LCOS LX 7.20

Addendum

10/2026

ROHDE&SCHWARZ
Make ideas real

Inhalt

1 Addendum zur LCOS LX-Version 7.20....4
2 Weitere Administratoren....5
2.1 Ergänzungen im Setup-Menü....5
2.1.1 Admins....5
3 Zeitautomatik via Cron-Job....8
3.1 Ergänzungen im Setup-Menü....9
3.1.1 Cron-Table....9
4 Client Management....13
4.1 Profile....14
4.2 Radio-Einstellungen....15
4.3 Ergänzungen im Setup-Menü....16
4.3.1 Client-Mgmt-Profile....16
4.3.2 Client-Management....16
4.3.3 Client-Management-Mode....19
5 Firewall....20
5.1 Host-Gruppen....21
5.2 Regeln....21
5.3 Ergänzungen im Setup-Menü....22
5.3.1 Firewall....22
6 End-to-End-Test....28
6.1 Testprofile....29
6.2 WLAN-Verbindung....30
6.3 WLAN-Authentifizierung....31
6.4 Statische IP-Parameter....32
6.5 DNS-Ziele....32
6.6 Ping-Ziele....33
6.7 HTTP-Ziele....33
6.8 Captive-Portal-Logins....34
6.9 Captive-Portal-Login-Daten....35
6.10 Ergänzungen im Setup-Menü....36
6.10.1 End2End-Test....36
7 SSH-Authentifizierung mit öffentlichem Schlüssel....56
7.1 Ergänzungen im Setup-Menü....57
7.1.1 Keys....57
8 Ergänzungen im Status-Menü....59
8.1 Syslog....59
8.1.1 Last-Messages....59

Copyright

© 2026 Rohde & Schwarz Networks and Cybersecurity GmbH, Würselen (Germany). Alle Rechte vorbehalten.

Hinweis zur Unternehmensbezeichnung: LANCOM Systems heißt seit dem 01.07.2026 **Rohde & Schwarz Networks and Cybersecurity**. Produktinformationen und Kommunikationsmaterialien werden entsprechend unter der neuen Unternehmensbezeichnung geführt.

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

Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhalts sind nur mit schriftlicher Erlaubnis von Rohde & Schwarz Networks and Cybersecurity gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

Windows® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

R&S und Rohde & Schwarz sind Marken der Rohde & Schwarz GmbH & Co. KG, die u. a. in Deutschland, EU, USA, China und weiteren Ländern eingetragen oder benutzt werden. Andere verwendete Namen oder Bezeichnungen können (registrierte) Marken von unterschiedlichen Firmen oder Inhabern sein. Dieses Dokument enthält zukunftsbezogene Aussagen zu Produkten und Produkteigenschaft. Der Herausgeber behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten oder Auslassungen.

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.rs-nc@rohde-schwarz.com*.

Produkte von Rohde & Schwarz Networks and Cybersecurity enthalten Software, die vom „OpenSSL Project“ für die Verwendung im „OpenSSL Toolkit“ entwickelt wurde (*www.openssl.org*).

Produkte von Rohde & Schwarz Networks and Cybersecurity enthalten kryptographische Software, die von Eric Young (*eay@cryptsoft.com*) geschrieben wurde.

Produkte von Rohde & Schwarz Networks and Cybersecurity enthalten Software, die von der NetBSD Foundation, Inc. und ihren Mitarbeitern entwickelt wurde.

Produkte von Rohde & Schwarz Networks and Cybersecurity enthalten das LZMA SDK, das von Igor Pavlov entwickelt wurde.

Rohde & Schwarz Networks and Cybersecurity GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

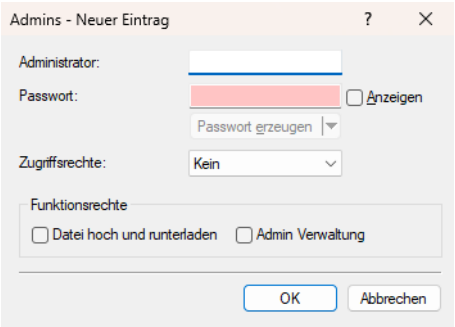
www.rohde-schwarz.com/networks-and-cybersecurity

1 Addendum zur LCOS LX-Version 7.20

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS LX-Version 7.20 gegenüber der vorherigen Version.

2 Weitere Administratoren

Nicht für jede Konfigurationstätigkeit benötigen Sie einen Administrator mit allen Rechten. Als Root-Administrator können sie Administratoren mit eingeschränkten Rechten anlegen. Somit muss das Hauptgerätepasswort nicht jedem Administrator bekannt sein. Die Konfiguration weiterer Administratoren erfolgt unter **Management** > **Admin** > **Admins**.



Administrator

Der Name des neuen Administrator-Accounts.

Passwort

Das Passwort des neuen Administrator-Accounts.

Zugriffsrechte

Wählen Sie eines der folgenden Zugriffsrechte:

- **Kein:** Die Konfiguration kann nicht gelesen oder geschrieben werden, aber ein CLI Login zum Ausführen von Kommandos ist möglich.
- **Admin-RO:** Die Konfiguration darf gelesen, aber nicht geschrieben werden.
- **Admin-RW:** Die Konfiguration darf gelesen und geschrieben werden.

Funktionsrechte

Wählen Sie aus den folgenden Funktionsrechten:

- **Datei hoch- und runterladen:** Dieses Funktionsrecht ist erforderlich, um Dateien, z. B. via scp, übertragen zu können - z. B. die Support-Info-Datei.
- **Admin-Verwaltung:** Dieses Funktionsrecht ist erforderlich, um weitere Administratoren auf dem Gerät konfigurieren zu können.

2.1 Ergänzungen im Setup-Menü

2.1.1 Admins

Legen Sie für Administratoren in dieser Tabelle an, die gegebenenfalls über eingeschränkte Rechte verfügen.

Der Administrator root hat immer alle Rechte.

SNMP-ID:

2.11.21

Pfad Konsole:

Setup > **Config**

2.1.1.1 Administrator

Anmeldename des Administrators in dieser Zeile der Tabelle.

SNMP-ID:

2.11.21.1

Pfad Konsole:

Setup > **Config** > **Admins**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][a-z][0-9]-.`

2.1.1.2 Function-Rights

Aktivieren Sie hier die Funktionsrechte des Administrators in dieser Zeile der Tabelle.

SNMP-ID:

2.11.21.3

Pfad Konsole:

Setup > **Config** > **Admins**

Mögliche Werte:

Basic
Admin-Management

2.1.1.3 Rights

Die Rechte des Administrators in dieser Zeile der Tabelle.

SNMP-ID:

2.11.21.5

Pfad Konsole:

Setup > **Config** > **Admins**

Mögliche Werte:

None
Admin-RO-Limit
Admin-RW-Limit
Admin-RO
Admin-RW
Supervisor

2.1.1.4 Hashed-Password

Hashwert des Passworts des Administrators in dieser Zeile der Tabelle.

SNMP-ID:

2.11.21.6

Pfad Konsole:

Setup > **Config** > **Admins**

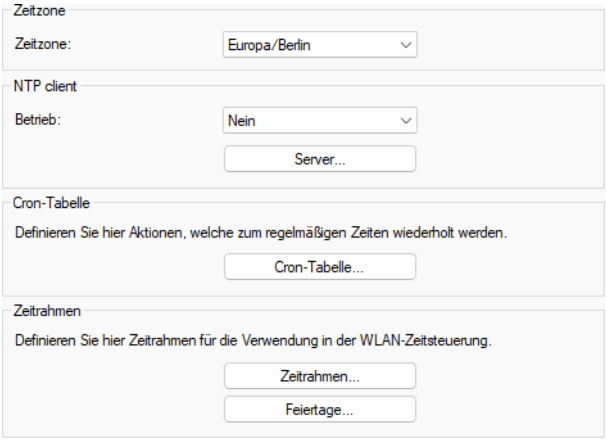
Mögliche Werte:

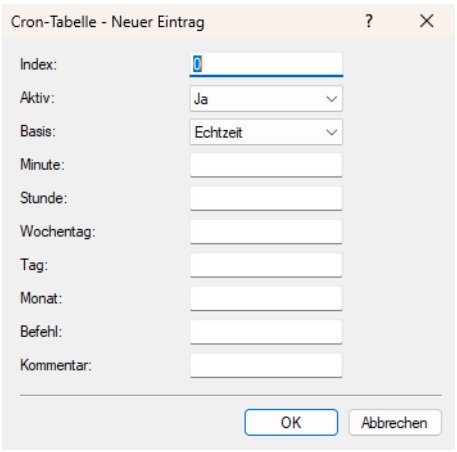
max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

3 Zeitautomatik via Cron-Job

Dieses Feature erlaubt dem Gerät, bestimmte Befehle zu bestimmten, benutzerdefinierten Zeitpunkten auszuführen. Die Funktionalität entspricht dabei dem unter UNIX bekannten Cron-Dienst. Ausgeführt werden kann dabei jede beliebige Kommandozeilenfunktion. Es können damit also alle Features mit einer zeitlichen Steuerung versehen werden.

Die Einstellungen zur Cron-Tabelle finden Sie unter **Datum / Zeit** > **Konfiguration**.





Die Funktion der einzelnen Felder entspricht weitestgehend der aus Linux/Unix bekannten Cron-Job-Konfiguration.

Index

Dient der Sortierung mehrerer Cron-Jobs.

Aktiv

Bestimmt, ob der Job ausgeführt wird oder nicht.

Basis

Die Zeitbasis bestimmt, ob LCOS LX die zeitliche Steuerung des Befehls auf Grundlage der Echtzeit oder der Systemlaufzeit (entspricht der seit dem Gerätestart vergangenen Zeit) des Gerätes ausführt.

Minute

Wird die hier angegebene Minute erreicht, wird der Befehl ausgeführt.

Stunde

Wird die hier angegebene Stunde erreicht, wird der Befehl ausgeführt.

Wochentag

Der Befehl wird an den hier per Zahlen angegebenen Wochentagen ausgeführt. Die Ziffern der Wochentage werden dabei durch Kommata voneinander getrennt. 0 entspricht Sonntag, 1 entspricht Montag, …, 6 entspricht Samstag

Tag

Der Befehl wird an den hier angegebenen Tagen des Monats (von 1 bis 31) ausgeführt.

Monat

Der Befehl wird an den hier angegebenen Monaten (von 1 bis 12) ausgeführt.

Befehl

Der auszuführende CLI-Befehl.

Kommentar

Ein Freitextfeld zum Hinterlegen eines beliebigen Kommentars.

3.1 Ergänzungen im Setup-Menü

3.1.1 Cron-Table

Dieses Feature erlaubt dem Gerät, bestimmte Befehle zu bestimmten, benutzerdefinierten Zeitpunkten auszuführen. Die Funktionalität entspricht dabei dem unter UNIX bekannten Cron-Dienst. Ausgeführt werden kann dabei jede beliebige Kommandozeilenfunktion. Es können damit also alle Features mit einer zeitlichen Steuerung versehen werden.

Die Funktion der einzelnen Felder entspricht weitestgehend der aus Linux/Unix bekannten Cron-Job-Konfiguration.

SNMP-ID:

2.11.20

Pfad Konsole:

Setup > **Config**

3.1.1.1 Index

Dient der Sortierung mehrerer Cron-Jobs.

SNMP-ID:

2.11.20.1

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

max. 5 Zeichen aus `[0-9]`

3.1.1.2 Active

Bestimmt, ob der Job ausgeführt wird oder nicht.

SNMP-ID:

2.11.20.2

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

Yes
No

3.1.1.3 Base

Die Zeitbasis bestimmt, ob LCOS LX die zeitliche Steuerung des Befehls auf Grundlage der Echtzeit oder der Systemlaufzeit (entspricht der seit dem Gerätestart vergangenen Zeit) des Gerätes ausführt.

SNMP-ID:

2.11.20.3

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

Real-Time
Operating-Time

3.1.1.4 Minute

Wird die hier angegebene Minute erreicht, wird der Befehl ausgeführt.

SNMP-ID:

2.11.20.4

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

max. 32 Zeichen aus `Range or comma-separated list between 0 and 59 (1,2,3 or 0-59 or 1-3,59)`

3.1.1.5 Hour

Wird die hier angegebene Stunde erreicht, wird der Befehl ausgeführt.

SNMP-ID:

2.11.20.5

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

max. 32 Zeichen aus `Range or comma-separated list between 0 and 23 (1,2,3 or 0-23 or 1-3,23)`

3.1.1.6 DayOfWeek

Der Befehl wird an den hier per Zahlen angegebenen Wochentagen ausgeführt. Die Ziffern der Wochentage werden dabei durch Kommata voneinander getrennt. 0 entspricht Sonntag, 1 entspricht Montag, …, 6 entspricht Samstag

SNMP-ID:

2.11.20.6

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

max. 32 Zeichen aus `Range or comma-separated list between 0 and 6 (1,2,3 or 0-6 or 1-3,6)`

3.1.1.7 Day

Der Befehl wird an den hier angegebenen Tagen des Monats (von 1 bis 31) ausgeführt.

SNMP-ID:

2.11.20.7

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

max. 32 Zeichen aus `Range or comma-separated list between 1 and 31 (1,2,3 or 1-7 or 1-3,7,8-9)`

3.1.1.8 Month

Der Befehl wird an den hier angegebenen Monaten (von 1 bis 12) ausgeführt.

SNMP-ID:

2.11.20.8

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

max. 32 Zeichen aus `Range or comma-separated list between 1 and 12 (1,2,3 or 1-7 or 1-3,7,8-9)`

3.1.1.9 Command

Der auszuführende CLI-Befehl.

SNMP-ID:

2.11.20.9

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

3.1.1.10 Comment

Ein Freitextfeld zum Hinterlegen eines beliebigen Kommentars.

SNMP-ID:

2.11.20.10

Pfad Konsole:

Setup > **Config** > **Cron-Table**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

4 Client Management

Ab LCOS LX 7.20 wird Client Management basierend auf IEEE 802.11k und IEEE 802.11v unterstützt. Die aus LCOS LX <7.20 bekannte Variante des Client Management (reines Band Steering) bleibt weiterhin optional verfügbar. Die Konfiguration wurde in den Bereich „WLAN Band-Steering Einstellungen“ verlagert.

Client Management dient dazu, WLAN-Clients innerhalb eines Netzwerks lastabhängig auf die zur Verfügung stehenden Access Points zu verteilen. In High-Density-Szenarien kann dies zu einer gleichmäßigeren Auslastung der WLAN-Ressourcen (u. a. AP-Kapazität und Kanalkapazität) führen.

Client Management basiert auf zwei Basistechnologien - RRM (Radio Resource Management / IEEE 802.11k) und WNM (Wireless Network Management (IEEE 802.11v).

RRM

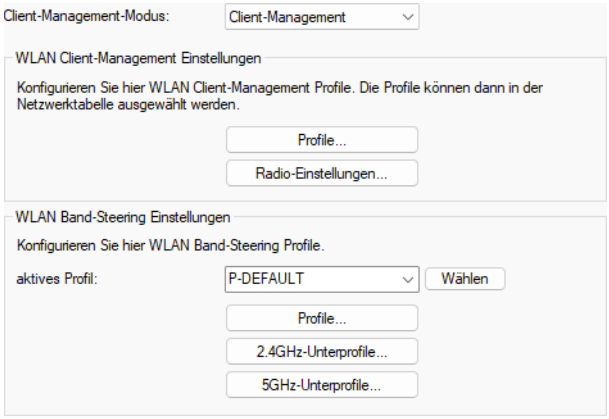
Client Management unterstützt RRM Neighbor Reports. Clients können einen Neighbor Report Request an den AP senden; dieser antwortet mit einem Neighbor Report, der eine Liste von in Frage kommenenden Roaming-Kandidaten beinhält. Der AP ermittelt diese Roaming-Kandidaten mittels eines Umgebungs-Scan, der automatisiert einmal täglich erfolgt, die Funkumgebung nach Kandidaten scannt und via IAPP prüft, dass die ermittelten APs tatsächlich LCOS LX APs des selben Netzwerks sind. Neben der reinen Liste der Kandidaten wird auch eine Priorität der einzelnen Kandidaten übermittelt (BSS Transition Candidate Preference), welcher die aktuelle Anzahl der am Kandidaten-AP eingebuchten Clients zugrunde liegt (weniger Clients = höhere Priorität).

WNM

Client Management unterstützt WNM BSS Transition Management (BTM). Clients können BTM Queries an den AP senden, der wiederum einen BTM Request mit einem oder mehreren sinnvollen Roaming-Kandidaten sendet. Dies ist prinzipiell ähnlich wie vorab für RRM beschrieben, es kommt lediglich ein anderes Protokoll zum Einsatz.

Um einen Client seitens des AP mit dem Wechsel zu einem anderen AP zu beauftragen, kann der AP dem Client auch unverlangt BTM Requests senden. Dies erfolgt, sobald die im weiteren Verlauf beschriebenen Schwellenwerte erreicht werden. Diese Schwellenwerte werden bei jedem Einbuchen eines neuen Client überprüft. Beim Erreichen dieser wählt das Client Management zufällig einen eingebuchten Client aus, der schon länger als 5 Minuten eingebucht ist und sendet diesem einen BTM Request, um ihn zum Wechsel auf einen (nicht ausgelasteten) AP zu bewegen. Clients, die für weniger als 5 Minuten eingebucht sind, oder die in den letzten 5 Minuten bereits einen BTM Request von diesem AP bekommen haben, werden nicht kontaktiert, um mehrere Roaming-Vorgänge innerhalb kurzer Zeit zu verhindern.

Die Einstellungen zum Client Management für WLAN-Netzwerke finden Sie unter **Wireless-LAN** > **Client-Management**.



Client-Management-Modus

Entscheiden Sie hier, ob Client-Management, reines Band-Steering oder keins der Features genutzt werden soll.

4.1 Profile

Definieren Sie unter **Wireless-LAN** > **Client-Management** > **Profile** Konfigurationsprofile für das Client-Management, oder verwenden Sie eines der vordefinierten Profile:

Vorhandene Profile

DEFAULT

Aktiviert RRM, aber nicht WNM/BSS Transition Management.

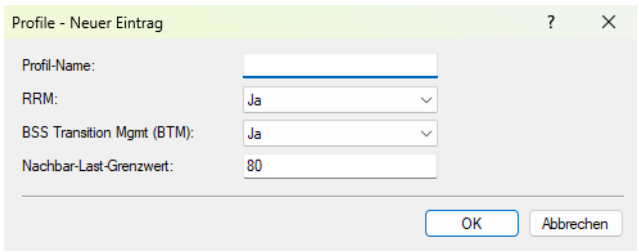
DISABLED

Deaktiviert sowohl RRM als auch WNM/BTM.

RRM+BTM

Aktiviert RRM und WNM/BTM.

Das gewünschte Profil weisen Sie unter **Wireless-LAN** > **WLAN-Netzwerke** > **Netzwerke** > **Client-Mgmt-Profil** zu.



Profil-Name

Name dieses Profils.

RRM

Aktivieren Sie hier die Verwendung von RRM.

BSS Transition Mgmt (BTM)

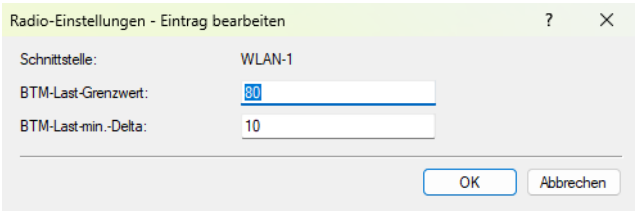
Aktivieren Sie hier die Verwendung von WNM/BTM.

Nachbar-Last-Grenzwert

Der prozentuale Wert, bis zu dem APs ausgelastet sein dürfen, um noch als Roaming-Ziele in Frage zu kommen. 100% entsprechen dabei aktuell 80 eingebuchten Clients, es wird nicht zwischen verschiedenen AP-Modellen unterschieden. Der Wert wird für RRM und WNM/BTM verwendet.

4.2 Radio-Einstellungen

Definieren Sie unter **Wireless-LAN** > **Client-Management** > **Radio-Einstellungen** die Radio-Einstellungen des Client-Managements.



Schnittstelle

Die WLAN-Schnittstelle, für die die folgenden Einstellungen gültig sind.

BTM-Last-Grenzwert

Wenn die Last dieser WLAN-Schnittstelle des APs den Grenzwert überschreitet, sendet der AP BTM-Requests an eingebuchte Clients, um diese auf andere APs zu steuern.

BTM-Last-min.-Delta

Dies ist ein dynamischer Schwellenwert: er ist relativ zur eigenen Last dieses APs. Der hier konfigurierte Wert stellt die minimale Lastdifferenz gegenüber unserer eigenen Last dar: Nur Nachbar-APs, deren Last mindestens um BTM-Last-min.-Delta niedriger ist als unsere eigene Last, werden an Clients empfohlen. Alle anderen werden als „nicht verwenden“ markiert. Beispiel: BTM-Last-Grenzwert beträgt 80, BTM-Last-min.-Delta ist 10. Angenommen, unsere eigene Last liegt bei 85 – wir haben den Schwellenwert damit überschritten und versuchen, Clients über BTM-Anfragen an Nachbar-APs zu verlagern. Mit dem Min-Delta von 10 werden jedoch nur APs an Clients empfohlen, deren Last mindestens 10 Punkte niedriger ist als unsere eigene. In diesem Beispiel werden daher alle Nachbar-APs mit einer Last von 75 oder höher als „nicht verwenden“ markiert. (Hinweis: Der statische Schwellenwert aus der Profiltabelle gilt weiterhin unabhängig davon.)

Dieses „Min-Delta“ dient der Erzeugung einer Hysterese, um zu verhindern, dass zwei Nachbar-APs mit hoher Last – jeweils nahe ihrem eigenen Schwellenwert – Clients ständig zwischen ihnen hin und her wechseln lassen.

4.3 Ergänzungen im Setup-Menü

4.3.1 Client-Mgmt-Profile

Wählen Sie hier eines der Client-Management-Profile aus *2.20.18.2 Profiles* aus.

SNMP-ID:

2.20.1.43

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

4.3.2 Client-Management

Konfifurieren Sie hier das Client Management.

SNMP-ID:

2.20.18

Pfad Konsole:

Setup > **WLAN**

4.3.2.1 Profiles

Definieren Sie hier Konfigurationsprofile für das Client-Management. Die Profile können in der Netzwerktabelle ausgewählt werden.

SNMP-ID:

2.20.18.2

Pfad Konsole:

Setup > **WLAN** > **Client-Management**

4.3.2.1.1 Profile-Name

Name dieses Profils.

SNMP-ID:

2.20.18.2.1

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

4.3.2.1.2 RRM

Aktivieren Sie hier die Verwendung von RRM.

SNMP-ID:

2.20.18.2.2

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

No
Yes

4.3.2.1.3 BTM

Aktivieren Sie hier die Verwendung von WNM/BTM.

SNMP-ID:

2.20.18.2.3

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

No
Yes

4.3.2.1.4 Neighbor-Load-Threshold

Der prozentuale Wert, bis zu dem APs ausgelastet sein dürfen, um noch als Roaming-Ziele in Frage zu kommen. 100% entsprechen dabei aktuell 80 eingebuchten Clients, es wird nicht zwischen verschiedenen AP-Modellen unterschieden. Der Wert wird für RRM und WNM/BTM verwendet.

SNMP-ID:

2.20.18.2.4

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

0 … 100

4.3.2.2 Radio-Settings

Definieren Sie hier die Radio-Einstellungen des Client-Managements.

SNMP-ID:

2.20.18.3

Pfad Konsole:

Setup > **WLAN** > **Client-Management**

4.3.2.2.1 Ifc

Die WLAN-Schnittstelle, für die die folgenden Einstellungen gültig sind.

SNMP-ID:

2.20.18.3.1

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Radio-Settings**

Mögliche Werte:

max. 9 Zeichen aus `WLAN-1,WLAN-1-2,...`

4.3.2.2.2 BTM-Load-Threshold

Wenn die Last dieser WLAN-Schnittstelle des APs den Grenzwert überschreitet, sendet der AP BTM-Requests an eingebuchte Clients, um diese auf andere APs zu steuern.

SNMP-ID:

2.20.18.3.2

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Radio-Settings**

Mögliche Werte:

0 … 100

4.3.2.2.3 BTM-Load-Min-Delta

Dies ist ein dynamischer Schwellenwert: er ist relativ zur eigenen Last dieses APs. Der hier konfigurierte Wert stellt die minimale Lastdifferenz gegenüber unserer eigenen Last dar: Nur Nachbar-APs, deren Last mindestens um BTM-Last-min.-Delta niedriger ist als unsere eigene Last, werden an Clients empfohlen. Alle anderen werden als „nicht verwenden“ markiert. Beispiel: BTM-Last-Grenzwert beträgt 80, BTM-Last-min.-Delta ist 10. Angenommen, unsere eigene Last liegt bei 85 – wir haben den Schwellenwert damit überschritten und versuchen, Clients über BTM-Anfragen an Nachbar-APs zu verlagern. Mit dem Min-Delta von 10 werden jedoch nur APs an Clients empfohlen, deren Last mindestens 10 Punkte niedriger ist als unsere eigene. In diesem Beispiel werden daher alle Nachbar-APs mit einer Last von 75 oder höher als „nicht verwenden“ markiert. (Hinweis: Der statische Schwellenwert aus der Profiltabelle gilt weiterhin unabhängig davon.)

Dieses „Min-Delta“ dient der Erzeugung einer Hysterese, um zu verhindern, dass zwei Nachbar-APs mit hoher Last – jeweils nahe ihrem eigenen Schwellenwert – Clients ständig zwischen ihnen hin und her wechseln lassen.

SNMP-ID:

2.20.18.3.3

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Radio-Settings**

Mögliche Werte:

0 … 100

4.3.3 Client-Management-Mode

Entscheiden Sie hier, ob Client-Management, reines Band-Steering oder keins der Features genutzt werden soll.

SNMP-ID:

2.20.19

Pfad Konsole:

Setup > **WLAN**

Mögliche Werte:

Client-Management
Band-Steering
Off

5 Firewall

Mit der Firewall kann Datenverkehr von und zu WLAN-Netzen auf IP-Ebene gefiltert werden. Es ist eine Deny-All-Strategie (jeglicher Verkehr wird verboten, bis auf konfigurierte Ausnahmen) oder eine Allow-All-Strategie (jeglicher Verkehr wird erlaubt, nur Ausnahmen werden verboten) möglich. Es können neben IP-Adressen auch Hostnamen / DNS-Namen als Ziel verwendet werden. Die Firewall liest dazu jegliche DNS-Anfragen von Clients im betroffenen WLAN-Netzwerk mit und speichert die aufgelösten IP-Adressen bis zum Erreichen der TTL (time-to-live) in einem internen Zwischenspeicher. Versucht ein Client anschließend die Verbindung zu einer so ermittelten IP-Adresse aufzubauen, kann diese - je nach Konfiguration - blockiert oder erlaubt werden.

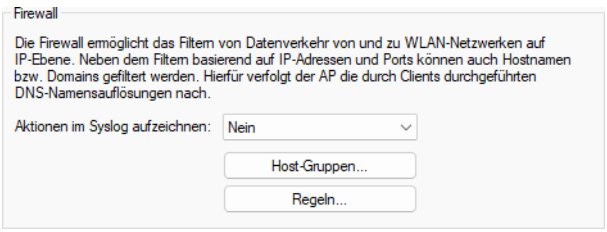
Das „mitlesen“ Der DNS-Anfragen ist nur bei unverschlüsseltem DNS möglich. Verwendet der Client verschlüsselte Verfahren wie z. B. DoT (DNS-over-TLS) oder DoH (DNS-over-HTTPS), können die DNS-Anfragen nicht inspiziert werden. In diesem Fall kann es sich anbieten, diese DNS-Verfahren ebenfalls mittels der Firewall zu blockieren. Für DoT kann eine Sperre erfolgen, indem der dafür verwendete Port 853 gesperrt wird. DoH verwendet den regulären HTTPS-Port 443 und kann daher nicht generell blockiert werden; allerdings erfolgt die Auflösung der DoH-Server in der Regel initial über reguläres DNS, so dass populäre DoH-Server-Domains unter Angabe ihres Namens mit der Firewall blockiert werden können.

Eine lückenlose Blockade von DoH ist prinzipbedingt nicht möglich; steht im Vordergrund, dass jeglicher unkontrollierter Traffic unterbunden werden muss, empfiehlt sich daher eine Deny-All-Strategie zu konfigurieren und erlaubte Dienste explizit freizuschalten.

Beim Roaming eines Client zwischen APs stellen die Applikationen des Clients normalerweise nicht als Reaktion darauf neue DNS-Anfragen. Dies erfolgt i.d.R. erst nach Ablauf der TTL (time-to-live). Die Firewall des AP, auf den geroamt wird, kann also keine DNS-Anfragen analysieren und die aufgelösten IP-Adressen lernen und daher den Datenverkehr des Clients eigentlich nicht blockieren.Um dies trotzdem zu ermöglichen, wird der DNS-Cache der Firewall zwischen APs, welche mit der oder den selben SSIDs konfiguriert sind, via IAPP übertragen und synchron gehalten. Dadurch erzeugen alle zusammengehörigen APs des Netzwerks das selbe effektive Firewall-Regelwerk und können den Datenverkehr basierend auf den IP-Adressen filtern, die ein beliebiger AP im Netzwerk aus den DNS-Anfragen des Clients ermittelt hat. Der aktuelle DNS-Cache lässt sich auf dem AP mittels des CLI-Befehls `ls /Status/DNS/Snooping-Results` einsehen.

Beachten Sie, dass lediglich der (flüchtige) DNS Cache synchronisiert wird. Die Konfiguration des AP, bestehend aus Host-Gruppen und Filter-Regeln, wird nicht synchronisiert und muss separat für alle APs identisch gehalten werden.

Die Einstellungen zur IP- und DNS-basierten Firewall finden Sie unter **Wireless-LAN** > **Firewall**.



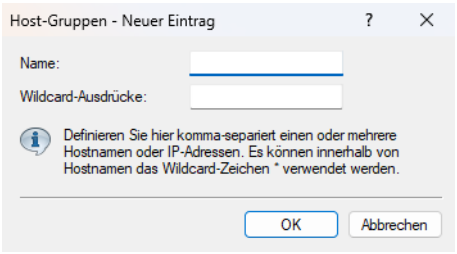
Aktionen im Syslog aufzeichnen

Wird eine Firewall-Regel durchlaufen, wird dazu ein Eintrag im Syslog erzeugt.

Je nach Datenaufkommen kann hierfür viel CPU-Leistung benötigt werden und sehr viele Syslog-Nachrichten erzeugt werden.

5.1 Host-Gruppen

Konfigurieren Sie hier Hostnamen oder IP-Adressen, die später in den Firewall-Regeln verwendet werden.



Name

Name der Gruppe.

Wildcard-Ausdrücke

Ein oder mehrere IP-Adressen oder Hostnamen, kommasepariert. Es kann das Wildcard-Zeichen * für beliebige Zeichen an dieser Stelle verwendet werden.

Die Syntax der Wildcard-Ausdrücke ist mit der der App-Definitionen des LCOS kompatibel.

5.2 Regeln

Konfigurieren Sie hier die Firewall-Regeln.

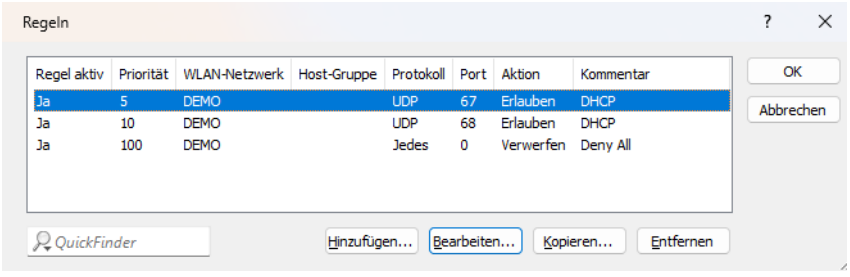
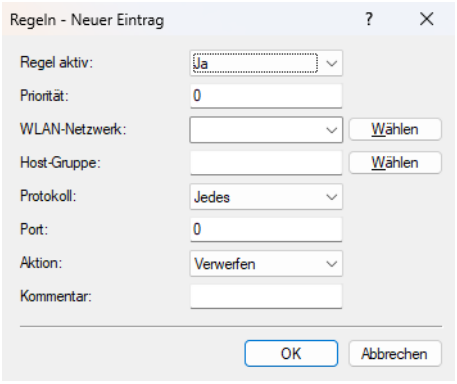


Abbildung 1: Beispiel Deny-All

Beachten Sie, dass die Deny-All-Regel **jeglichen** Datenverkehr blockiert. Es ist daher erforderlich, die entsprechenden Ports für DHCPv4 explizit zu erlauben, um den IPv4-Adressbezug zu ermöglichen.



Regel aktiv

Hier wird gesteuert, ob die Regel für die Firewall aktiv ist.

Priorität

Priorität der Regel. Regeln mit niedrigeren Werten werden vor Regeln mit höheren Werten verarbeitet.

WLAN-Netzwerk

Das WLAN-Netzwerk, für das die Regel aktiv ist.

Host-Gruppe

Eine oder mehrere zuvor konfigurierte Host-Gruppen, auf die als Ziel der Regel geprüft wird.

Protokoll

Konfiguriert, ob die Regel nur für TCP, UDP, oder jeglichen Traffic zutrifft.

Port

Wird als Protokoll TCP oder UDP eingetragen, kann hier zusätzlich eine Portnummer als Filter-Kriterium hinterlegt werden.

Aktion

Konfiguriert, ob bei Zutreffen der Regel die Verbindung erlaubt oder verworfen wird.

Kommentar

Ein Freitextfeld zum Hinterlegen eines beliebigen Kommentars.

5.3 Ergänzungen im Setup-Menü

5.3.1 Firewall

Mit der Firewall kann Datenverkehr von und zu WLAN-Netzen auf IP-Ebene gefiltert werden. Es ist eine Deny-All-Strategie (jeglicher Verkehr wird verboten, bis auf konfigurierte Ausnahmen) oder eine Allow-All-Strategie (jeglicher Verkehr wird erlaubt, nur Ausnahmen werden verboten) möglich.

Es können neben IP-Adressen auch Hostnamen / DNS-Namen als Ziel verwendet werden. Die Firewall liest dazu jegliche DNS-Anfragen von Clients im betroffenen WLAN-Netzwerk mit und speichert die aufgelösten IP-Adressen bis zum Erreichen der TTL (time-to-live) in einem internen Zwischenspeicher. Versucht ein Client anschließend die Verbindung zu einer so ermittelten IP-Adresse aufzubauen, kann diese - je nach Konfiguration - blockiert oder erlaubt werden.

Das „mitlesen“ Der DNS-Anfragen ist nur bei unverschlüsseltem DNS möglich. Verwendet der Client verschlüsselte Verfahren wie z. B. DoT (DNS-over-TLS) oder DoH (DNS-over-HTTPS), können die DNS-Anfragen nicht inspiziert werden. In diesem Fall kann es sich anbieten, diese DNS-Verfahren ebenfalls mittels der Firewall zu blockieren. Für DoT kann eine Sperre erfolgen, indem der dafür verwendete Port 853 gesperrt wird. DoH verwendet den regulären HTTPS-Port 443 und kann daher nicht generell blockiert werden; allerdings erfolgt die Auflösung der DoH-Server in der Regel initial über reguläres DNS, so dass populäre DoH-Server-Domains unter Angabe ihres Namens mit der Firewall blockiert werden können.

Eine lückenlose Blockade von DoH ist prinzipbedingt nicht möglich; steht im Vordergrund, dass jeglicher unkontrollierter Traffic unterbunden werden muss, empfiehlt sich daher eine Deny-All-Strategie zu konfigurieren und erlaubte Dienste explizit freizuschalten.

Beim Roaming eines Client zwischen APs stellen die Applikationen des Clients normalerweise nicht als Reaktion darauf neue DNS-Anfragen. Dies erfolgt i.d.R. erst nach Ablauf der TTL (time-to-live). Die Firewall des AP, auf den geroamt wird, kann also keine DNS-Anfragen analysieren und die aufgelösten IP-Adressen lernen und daher den Datenverkehr des Clients eigentlich nicht blockieren.Um dies trotzdem zu ermöglichen, wird der DNS-Cache der Firewall zwischen APs, welche mit der oder den selben SSIDs konfiguriert sind, via IAPP übertragen und synchron gehalten. Dadurch erzeugen alle zusammengehörigen APs des Netzwerks das selbe effektive Firewall-Regelwerk und können den Datenverkehr basierend auf den IP-Adressen filtern, die ein beliebiger AP im Netzwerk aus den DNS-Anfragen des Clients ermittelt hat. Der aktuelle DNS-Cache lässt sich auf dem AP mittels des CLI-Befehls `ls /Status/DNS/Snooping-Results` einsehen.

Beachten Sie, dass lediglich der (flüchtige) DNS Cache synchronisiert wird. Die Konfiguration des AP, bestehend aus Host-Gruppen und Filter-Regeln, wird nicht synchronisiert und muss separat für alle APs identisch gehalten werden.

SNMP-ID:

2.47

Pfad Konsole:

Setup

5.3.1.1 Rules

Konfigurieren Sie hier die Firewall-Regeln.

SNMP-ID:

2.47.1

Pfad Konsole:

Setup > **Firewall**

5.3.1.1.1 Enabled

Hier wird gesteuert, ob die Regel für die Firewall aktiv ist.

SNMP-ID:

2.47.1.1

Pfad Konsole:

Setup > **Firewall** > **Rules**

Mögliche Werte:

No

Regel nicht aktiv.

Yes

Regel aktiv.

5.3.1.1.2 Priority

Priorität der Regel. Regeln mit niedrigeren Werten werden vor Regeln mit höheren Werten verarbeitet.

SNMP-ID:

2.47.1.2

Pfad Konsole:

Setup > **Firewall** > **Rules**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

5.3.1.1.3 Network

Das WLAN-Netzwerk, für das die Regel aktiv ist.

SNMP-ID:

2.47.1.3

Pfad Konsole:

Setup > **Firewall** > **Rules**

Mögliche Werte:

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

5.3.1.1.4 Host-Group

Eine oder mehrere zuvor konfigurierte Host-Gruppen, auf die als Ziel der Regel geprüft wird.

SNMP-ID:

2.47.1.4

Pfad Konsole:

Setup > **Firewall** > **Rules**

Mögliche Werte:

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

5.3.1.1.5 Protocol

Konfiguriert, ob die Regel nur für TCP, UDP, oder jeglichen Traffic zutrifft.

SNMP-ID:

2.47.1.5

Pfad Konsole:

Setup > **Firewall** > **Rules**

Mögliche Werte:

Any
TCP
UDP

5.3.1.1.6 Port

Wird als Protokoll TCP oder UDP eingetragen, kann hier zusätzlich eine Portnummer als Filter-Kriterium hinterlegt werden.

SNMP-ID:

2.47.1.6

Pfad Konsole:

Setup > **Firewall** > **Rules**

Mögliche Werte:

0 … 65535

5.3.1.1.7 Action

Konfiguriert, ob bei Zutreffen der Regel die Verbindung erlaubt oder verworfen wird.

SNMP-ID:

2.47.1.7

Pfad Konsole:

Setup > **Firewall** > **Rules**

Mögliche Werte:

Accept
Drop

5.3.1.1.8 Comment

Ein Freitextfeld zum Hinterlegen eines beliebigen Kommentars.

SNMP-ID:

2.47.1.99

Pfad Konsole:

Setup > **Firewall** > **Rules**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. ``

5.3.1.2 Host-Groups

Konfigurieren Sie hier Hostnamen oder IP-Adressen, die später in den Firewall-Regeln verwendet werden.

SNMP-ID:

2.47.2

Pfad Konsole:

Setup > **Firewall**

5.3.1.2.1 Name

Name der Gruppe.

SNMP-ID:

2.47.2.1

Pfad Konsole:

Setup > **Firewall** > **Host-Groups**

Mögliche Werte:

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

5.3.1.2.2 Hostnames

Ein oder mehrere IP-Adressen oder Hostnamen, kommasepariert. Es kann das Wildcard-Zeichen * für beliebige Zeichen an dieser Stelle verwendet werden.

Die Syntax der Wildcard-Ausdrücke ist mit der der App-Definitionen des LCOS kompatibel.

SNMP-ID:

2.47.2.2

Pfad Konsole:

Setup > **Firewall** > **Host-Groups**

Mögliche Werte:

max. 255 Zeichen aus `comma separated list of IP addresses, networks or hostnames (with wildcards)`

5.3.1.3 Log-Actions

Wird eine Firewall-Regel durchlaufen, wird dazu ein Eintrag im Syslog erzeugt.

Je nach Datenaufkommen kann hierfür viel CPU-Leistung benötigt werden und sehr viele Syslog-Nachrichten erzeugt werden.

SNMP-ID:

2.47.3

Pfad Konsole:

Setup > **Firewall**

Mögliche Werte:

No

Keinen Eintrag schreiben.

Yes

Eintrag schreiben.

6 End-to-End-Test

Mit dem WLAN End-to-End-Test lässt sich die Verfügbarkeit und Leistungsfähigkeit eines WLANs aus Sicht eines Endgeräts überprüfen – ganz ohne zusätzliches Testgerät vor Ort. Dazu wird ein vorhandener R&S®LANCOM Access Point vorübergehend in den Client-Modus versetzt und führt definierte Tests entlang des gesamten Verbindungswegs vom WLAN bis ins Internet aus.

Der Test erkennt unter anderem Probleme bei der WLAN-Authentifizierung, der IP-Adressvergabe per DHCP, der Namensauflösung über DNS, der Anmeldung an einem Captive Portal sowie bei Ping- und HTTP-Verbindungen. Die Testprofile können an die jeweilige Netzwerkumgebung angepasst werden. Nicht benötigte Tests lassen sich dabei aus dem Profil entfernen – beispielsweise der Captive-Portal-Test, wenn kein Hotspot betrieben wird.

Ein Testlauf kann bei Bedarf manuell durch einen Administrator gestartet oder über die interne Cron-Tabelle regelmäßig geplant werden. Die Ergebnisse werden in den entsprechenden Logtabellen gespeichert und zusätzlich an den Gerätesyslog weitergegeben. Von dort können sie beispielsweise an externe SIEM-Systeme weitergeleitet werden.

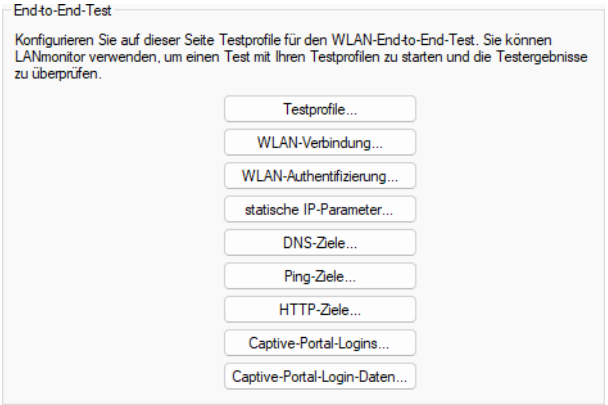
Während der Testausführung arbeitet der Access Point im Client-Modus. Dadurch steht er vorübergehend nicht für den normalen WLAN-Betrieb zur Verfügung und verbundene Clients werden getrennt. Nach Abschluss des Testlaufs wechselt der Access Point automatisch zurück in den normalen Betriebsmodus und nimmt die Versorgung der WLAN-Clients wieder auf.

Die Tests werden in einer festgelegten Reihenfolge ausgeführt:

1. WLAN-Verbindung
2. Netzwerkverbindung einschließlich DHCPv4, DHCPv6 und SLAAC
3. DNS-Auflösung
4. Captive Portal
5. Ping
6. HTTP-Verbindung

Diese Reihenfolge kann nicht verändert werden, da die einzelnen Prüfungen aufeinander aufbauen. Eine WLAN-Verbindung ist beispielsweise die Voraussetzung für die Netzwerkkommunikation, eine gültige IP-Adresse wird für DNS-Abfragen benötigt, und ein HTTP-Test ist gegebenenfalls erst nach erfolgreicher Anmeldung am Captive Portal möglich.

Die Einstellungen zum WLAN End-to-End-Test finden Sie unter **Wireless-LAN** > **End-to-End-Test**.



Testergebnisse

Die Ergebnisse der einzelnen Subtests werden jeweils in separaten Tabellen unter **Status** > **WLAN** > **End2End-Test** gespeichert. Zusätzlich gibt es eine eigene Historientabelle, in der die Ergebnisse aller Subtests chronologisch in einer gemeinsamen Tabelle aufgeführt werden. Die Historientabelle ist damit vergleichbar mit einem Syslog, enthält jedoch ausschließlich Einträge zum WLAN E2E-Test.

6.1 Testprofile

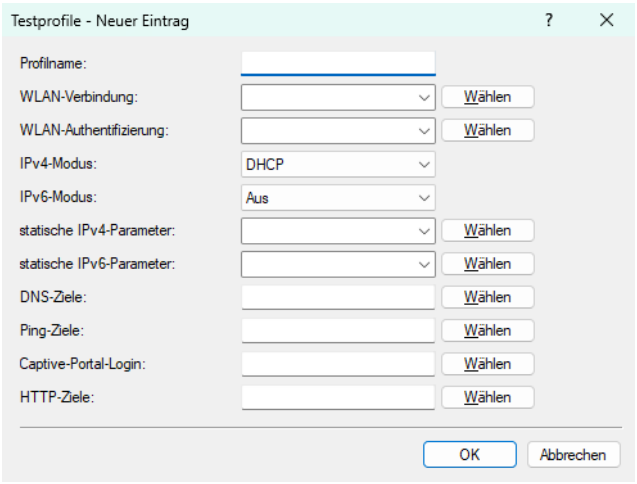
In diesem Menü werden Testläufe zusammengestellt. Ein Testlauf besteht aus mehreren Einzeltests, die gemeinsam ausgeführt werden.

Für jedes Testprofil muss mindestens ein Test der Kategorie **WLAN-Verbindung** konfiguriert werden. Weitere Einzeltests können optional hinzugefügt werden – abhängig davon, welche Prüfungen ausgeführt werden sollen.

Bleibt die **WLAN-Authentifizierung** leer, wird eine offene WLAN-Verbindung ohne Verschlüsselung verwendet. Die SSID muss in diesem Fall ein offenes Netzwerk bereitstellen.

Statische IPv4- oder IPv6-Parameter können leer bleiben, wenn im jeweiligen **IPvX-Modus** keine statischen Parameter ausgewählt wurden.

Pro Testprofil können mehrere Einzeltests derselben Kategorie ausgeführt werden. Hierzu werden die entsprechenden Tests durch Kommas getrennt angegeben.



Profilname

Der Name dieses Testprofils.

WLAN-Verbindung

Wählen Sie eine der vorhandenen WLAN-Verbindungen.

WLAN-Authentifizierung

Wählen Sie eine der vorhandenen WLAN-Authentifizierungen.

IPv4-Modus

Wählen Sie entweder DHCP oder statisch.

IPv6-Modus

Wählen Sie entweder Router Advertisement, DHCPv6, statisch oder Aus.

statische IPv4-Parameter

Wählen Sie ggf. die statischen IPv4-Parameter aus.

statische IPv6-Parameter

Wählen Sie ggf. die statischen IPv6-Parameter aus.

DNS-Ziele

Wählen Sie eines der vorhandenen DNS-Ziele.

Ping-Ziele

Wählen Sie eines der vorhandenen Ping-Ziele.

Captive-Portal-Login

Wählen Sie eines der vorhandenen Captive-Portal-Logins.

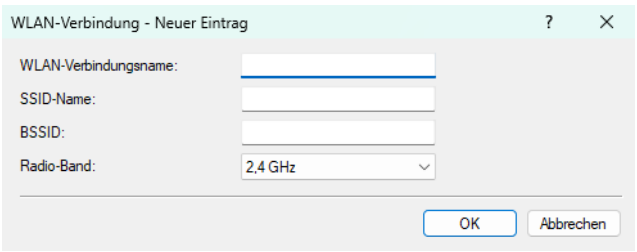
HTTP-Ziele

Wählen Sie eines der vorhandenen HTTP-Ziele.

6.2 WLAN-Verbindung

Legen Sie fest, mit welcher SSID die Verbindung hergestellt und die Tests ausgeführt werden sollen.

Optional kann eine bestimmte BSSID angegeben werden, wenn die Verbindung gezielt zu einem bestimmten Access Point hergestellt werden soll. Wird keine BSSID konfiguriert, wählt der Test automatisch einen Access Point mit der angegebenen SSID aus. Dabei wird der Access Point mit der besten Signalstärke bevorzugt.



WLAN-Verbindungsname

Geben Sie dieser Verbindung einen Namen.

SSID-Name

Die SSID für die Tests.

BSSID

Optionale BSSID für die Tests.

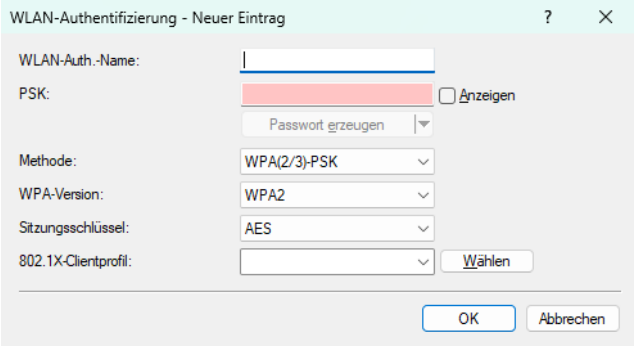
Radio-Band

Das Radio-Band für diese Verbindung.

6.3 WLAN-Authentifizierung

Der WLAN E2E-Test unterstützt sowohl die Authentifizierung per PSK als auch per IEEE 802.1X mit den üblichen Optionen auf Client-Seite.

Für die Verwendung von IEEE 802.1X muss zuvor ein passendes Supplicant-Profil konfiguriert werden.



WLAN-Auth.-Name

Geben Sie dieser WLAN-Authentifizierung einen Namen.

PSK

Geben Sie den PSK an.

Methode

Wählen Sie die Methode der WLAN-Authentifizierung aus.

WPA-Version

Wählen Sie die WPA-Version aus.

Sitzungsschlüssel

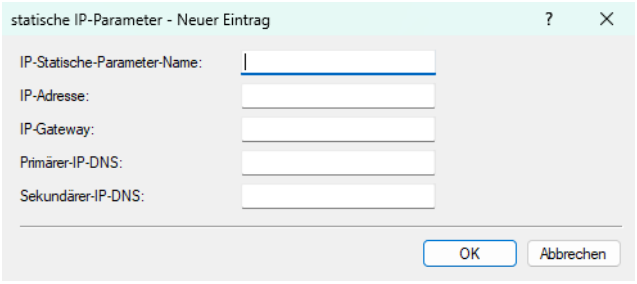
Wählen Sie den Typ des Sitzungsschlüssels aus.

802.1X-Clientprofil

Wählen Sie ein IEEE 802.1X-Clientprofil aus.

6.4 Statische IP-Parameter

Wenn für den Test eine statische IP-Konfiguration verwendet werden soll, tragen Sie die entsprechenden IP-Parameter in dieser Tabelle ein.



IP-Statische-Parameter-Name

Geben Sie dieser statischen IP-Konfiguration einen Namen.

IP-Adresse

Tragen sie die IP-Adresse ein.

IP-Gateway

Tragen sie den IP-Gateway ein.

Primärer IP-DNS

Tragen sie die IP-Adresse des primären DNS-Servers ein.

Sekundärer IP-DNS

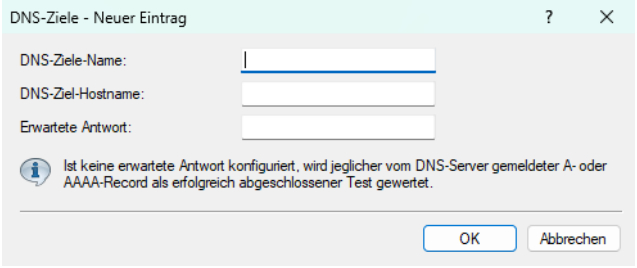
Tragen sie die IP-Adresse des sekundären DNS-Servers ein.

6.5 DNS-Ziele

Hier können Sie den DNS-Test konfigurieren. Im Feld **Erwartete Antwort** können Sie durch das Präfix „A:“ oder „AAAA:“ festlegen, dass ein bestimmter A- bzw. AAAA-Record erwartet wird.

Mehrere Records können als kommagetrennte Liste angegeben werden. Der Test gilt als erfolgreich, sobald einer der konfigurierten Records mit der empfangenen Antwort übereinstimmt.

Bleibt das Feld **Erwartete Antwort** leer, gilt jeder empfangene A- oder AAAA-Record als erfolgreiche Antwort.



DNS-Ziele-Name

Geben Sie diesen DNS-Zielen einen Namen.

DNS-Ziel-Hostname

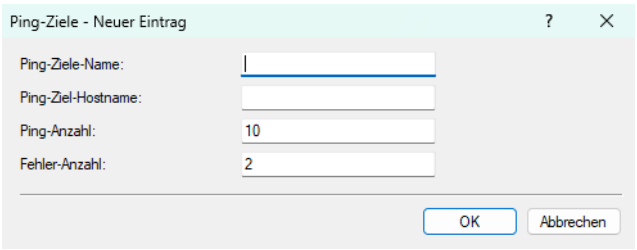
Geben Sie die Hostnamen an, die getestet werden sollen.

Erwartete Antwort

Geben Sie die für diesen Test erwartete Antwort ein.

6.6 Ping-Ziele

Hier können Sie den Ping-/ICMP-Test konfigurieren. Die Felder Ping- und Fehler-Anzahl sind mit den gezeigten Standardwerten vorbelegt und können bei Bedarf angepasst werden.



Ping-Ziele-Name

Geben Sie diesen Ping-Zielen einen Namen.

Ping-Ziel-Hostname

Geben Sie den Hostnamen an, der getestet werden sollen.

Ping-Anzahl

Geben Sie die Ping-Anzahl an.

Fehler-Anzahl

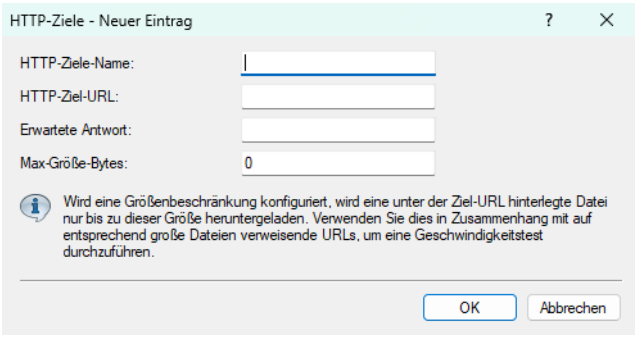
Geben Sie die Fehler-Anzahl an.

6.7 HTTP-Ziele

In dieser Tabelle können Sie eine HTTP-Verbindung testen. Der E2E-Test ruft die konfigurierte **HTTP-Ziel-URL** ab und vergleicht den empfangenen HTTP-Statuscode mit dem im Feld **Erwartete Antwort** angegebenen Wert.

Der HTTP-Test kann zusätzlich als Geschwindigkeitstest verwendet werden, wenn über die HTTP-Ziel-URL eine ausreichend große Datei heruntergeladen werden kann. Damit eine aussagekräftige Durchsatzmessung möglich ist, sollte in diesem Fall auch **Maximale Größe (Bytes)** konfiguriert werden. Wird kein Maximalwert angegeben, wird die Datei vollständig heruntergeladen.

Der gemessene Durchsatz wird in den Testergebnissen immer angezeigt. Aussagekräftig ist dieser Wert jedoch nur, wenn eine ausreichend große Datei heruntergeladen wird und der TCP-/HTTP-Download eine realistische Übertragungsgeschwindigkeit erreichen kann.



HTTP-Ziele-Name

Geben Sie diesen HTTP-Zielen einen Namen.

HTTP-Ziel-URL

Geben Sie die URL an, die getestet werden soll.

Erwartete Antwort

Geben Sie die erwartete Antwort an.

Max-Größe-Bytes

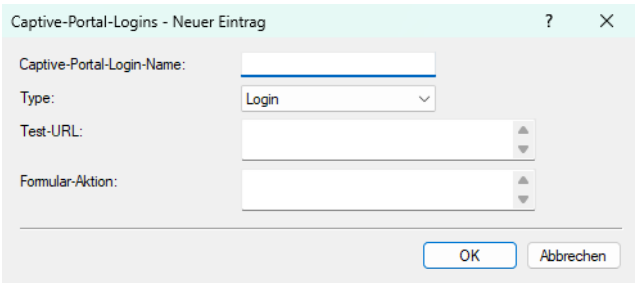
Optionale Größenbeschränkung.

6.8 Captive-Portal-Logins

Wenn das zu testende Netzwerk durch ein Captive Portal geschützt ist, können Sie die erforderlichen Anmeldeparameter hier konfigurieren.

Der E2E-Test ruft zunächst die konfigurierte Test-URL auf, um zu prüfen, ob das Captive Portal eine Weiterleitung durchführt. Wird eine Weiterleitung erkannt, erstellt der Test eine HTTP-POST-Anfrage mit den Einträgen aus der Tabelle Captive-Portal-Login-Daten und sendet diese an die im Feld Formular-Aktion angegebene URL.

Anschließend wird die Test-URL erneut aufgerufen. Erfolgt nun keine Weiterleitung mehr, gilt die Anmeldung als erfolgreich und der Test wird bestanden.



Captive-Portal-Login-Name

Geben Sie diesem Captive-Portal-Login einen Namen.

Type

Hier kann entweder „Login“ oder „Logout“ ausgewählt werden.

Je nach Captive Portal kann es sinnvoll sein, den Benutzer nach Abschluss des Tests wieder abzumelden. Dadurch lassen sich beispielsweise Ressourcen auf dem Captive-Portal-Gateway schonen oder erneute Anmeldungen mit denselben Zugangsdaten bei späteren Testläufen ermöglichen.

Legen Sie hierzu einen zusätzlichen Eintrag mit dem Typ „Logout“ an. Konfigurieren Sie dabei die **Formular-Aktion** so, dass sie die Abmeldeaktion des Captive Portals ausführt. Die URL für die Abmeldung kann sich von der URL des Anmeldeformulars unterscheiden. Analysieren Sie hierzu den HTML-Code des jeweiligen Portals.

Viele moderne Captive Portals mit Click-through-Anmeldung bieten jedoch keine Abmeldefunktion. Die Benutzersitzung wird in diesem Fall erst nach einem Timeout beendet. Ein regelmäßig in kurzen Abständen ausgeführter Captive-Portal-Test kann dann möglicherweise erfolgreich sein, ohne die Anmeldung tatsächlich zu prüfen, da die MAC-Adresse des testenden Access Points noch im Captive Portal zwischengespeichert ist.

Wenn Sie das Captive Portal selbst verwalten, kann eine spezielle Testfunktion sinnvoll sein. Beispielsweise könnte ein verstecktes Formular im HTML-Code eine dedizierte Testsitzung starten, die bereits nach kurzer Zeit automatisch abläuft.

Test-URL

Dies ist die URL, die der E2E-Test aufruft, um festzustellen, ob das Captive Portal eine Weiterleitung durchführt. Sie kann auf jede URL zeigen, die zuverlässig mit einem HTTP-Statuscode aus dem Bereich „200“ antwortet. Idealerweise wird eine URL verwendet, die mit „200“ oder „204“ antwortet.

Das Feld ist standardmäßig leer, da keine URL eines externen Drittanbieters fest vorgegeben werden kann. Es muss daher eine geeignete URL konfiguriert werden.

Formular-Aktion

Dies ist die URL, an die die Anmeldedaten per HTTP POST übertragen werden. Beim klassischen LCOS-Public Spot kann dies beispielsweise eine URL wie die Folgende sein:

```
https://pspot.lancom.de:443/authen/login/
```

Bleibt dieses Feld leer, verwendet der E2E-Test automatisch die URL, zu der das Captive Portal beim ersten Aufruf der Success-URL weitergeleitet hat. Bei R&S®LANCOM Management Cloud-basierten Hotspots funktioniert die Anmeldung dadurch in der Regel ohne zusätzliche Konfiguration dieser URL.

6.9 Captive-Portal-Login-Daten

In dieser Tabelle werden die Formularelemente konfiguriert, die für eine Anmeldung oder Abmeldung per HTTP POST an das Captive Portal übertragen werden.

Bei einem klassischen, auf LCOS basierenden Public Spot können die Formulardaten beispielsweise wie folgt aussehen:

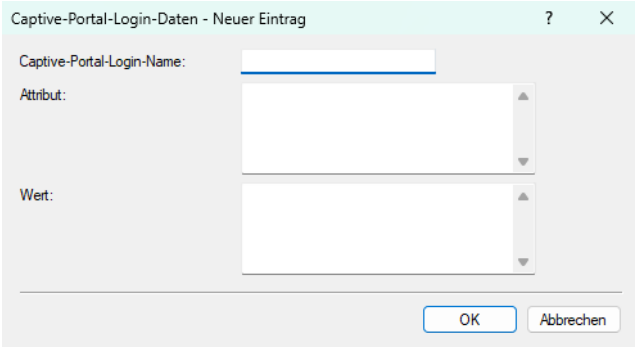
Attribut	Wert
AGB	checked
password	geheim

Attribut	Wert
userid	rsnc

Wenn zusätzlich die Logout-Funktion verwendet wird, müssen in dieser Tabelle auch die entsprechenden Attribute für den Logout-Test hinterlegt werden.

Jedes Captive Portal verwendet eine eigene Formularstruktur. Ermitteln Sie daher anhand des HTML-Quellcodes des Portals das korrekte Formular sowie die benötigten Attribute und Werte.

Bei sehr einfachen Portalseiten, die beispielsweise nur ein einziges Formularattribut – etwa eine Schaltfläche für den Click-through-Login – enthalten, versucht der E2E-Test, dieses Attribut automatisch per POST zu übertragen. In diesem Fall ist keine zusätzliche Konfiguration in dieser Tabelle erforderlich. Dies funktioniert derzeit beispielsweise beim One-Button-Login des R&S®LANCOM Management Cloud-Hotspots.



Captive-Portal-Login-Name

Geben Sie diesem Captive-Portal-Login einen Namen.

Attribut

Geben Sie hier die benötigten Attribue an.

Wert

Geben Sie hier die Werte zu den konfigurierten Attribuen an.

6.10 Ergänzungen im Setup-Menü

6.10.1 End2End-Test

Mit dem WLAN End-to-End-Test lässt sich die Verfügbarkeit und Leistungsfähigkeit eines WLANs aus Sicht eines Endgeräts überprüfen – ganz ohne zusätzliches Testgerät vor Ort. Dazu wird ein vorhandener R&S®LANCOM Access Point vorübergehend in den Client-Modus versetzt und führt definierte Tests entlang des gesamten Verbindungswegs vom WLAN bis ins Internet aus.

Der Test erkennt unter anderem Probleme bei der WLAN-Authentifizierung, der IP-Adressvergabe per DHCP, der Namensauflösung über DNS, der Anmeldung an einem Captive Portal sowie bei Ping- und HTTP-Verbindungen. Die Testprofile können an die jeweilige Netzwerkumgebung angepasst werden. Nicht benötigte Tests lassen sich dabei aus dem Profil entfernen – beispielsweise der Captive-Portal-Test, wenn kein Hotspot betrieben wird.

Ein Testlauf kann bei Bedarf manuell durch einen Administrator gestartet oder über die interne Cron-Tabelle regelmäßig geplant werden. Die Ergebnisse werden in den entsprechenden

Logtabellen gespeichert und zusätzlich an den Gerätesyslog weitergegeben. Von dort können sie beispielsweise an externe SIEM-Systeme weitergeleitet werden.

Während der Testausführung arbeitet der Access Point im Client-Modus. Dadurch steht er vorübergehend nicht für den normalen WLAN-Betrieb zur Verfügung und verbundene Clients werden getrennt. Nach Abschluss des Testlaufs wechselt der Access Point automatisch zurück in den normalen Betriebsmodus und nimmt die Versorgung der WLAN-Clients wieder auf.

Die Tests werden in einer festgelegten Reihenfolge ausgeführt:

1. WLAN-Verbindung
2. Netzwerkverbindung einschließlich DHCPv4, DHCPv6 und SLAAC
3. DNS-Auflösung
4. Captive Portal
5. Ping
6. HTTP-Verbindung

Diese Reihenfolge kann nicht verändert werden, da die einzelnen Prüfungen aufeinander aufbauen. Eine WLAN-Verbindung ist beispielsweise die Voraussetzung für die Netzwerkkommunikation, eine gültige IP-Adresse wird für DNS-Abfragen benötigt, und ein HTTP-Test ist gegebenenfalls erst nach erfolgreicher Anmeldung am Captive Portal möglich.

SNMP-ID:

2.20.20

Pfad Konsole:

Setup > **WLAN**

6.10.1.1 Test-Profiles

In diesem Menü werden Testläufe zusammengestellt. Ein Testlauf besteht aus mehreren Einzeltests, die gemeinsam ausgeführt werden.

Für jedes Testprofil muss mindestens ein Test der Kategorie **WLAN-Verbindung** konfiguriert werden. Weitere Einzeltests können optional hinzugefügt werden – abhängig davon, welche Prüfungen ausgeführt werden sollen.

Bleibt die **WLAN-Authentifizierung** leer, wird eine offene WLAN-Verbindung ohne Verschlüsselung verwendet. Die SSID muss in diesem Fall ein offenes Netzwerk bereitstellen.

Statische IPv4- oder IPv6-Parameter können leer bleiben, wenn im jeweiligen **IPvX-Modus** keine statischen Parameter ausgewählt wurden.

Pro Testprofil können mehrere Einzeltests derselben Kategorie ausgeführt werden. Hierzu werden die entsprechenden Tests durch Kommas getrennt angegeben.

SNMP-ID:

2.20.20.1

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

6.10.1.1.1 Profile-Name

Der Name dieses Testprofils.

SNMP-ID:

2.20.20.1.1

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

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

6.10.1.1.2 WLAN-Connection

Wählen Sie eine der vorhandenen WLAN-Verbindungen.

SNMP-ID:

2.20.20.1.2

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

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

6.10.1.1.3 WLAN-Authenticationn

Wählen Sie eine der vorhandenen WLAN-Authentifizierungen.

SNMP-ID:

2.20.20.1.3

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

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

6.10.1.1.4 IPv4-Mode

Wählen Sie entweder DHCP oder statisch.

SNMP-ID:

2.20.20.1.4

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

DHCP
static

6.10.1.1.5 IPv6-Mode

Wählen Sie entweder Router Advertisement, DHCPv6, statisch oder Aus.

SNMP-ID:

2.20.20.1.5

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

Router-Advertisement
DHCPv6
static
Off

6.10.1.1.6 IPv4-Static-Parameters

Wählen Sie ggf. die statischen IPv4-Parameter aus.

SNMP-ID:

2.20.20.1.6

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

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

6.10.1.1.7 IPv6-Static-Parameters

Wählen Sie ggf. die statischen IPv6-Parameter aus.

SNMP-ID:

2.20.20.1.7

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

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

6.10.1.1.8 DNS-Targets

Wählen Sie eines der vorhandenen DNS-Ziele.

SNMP-ID:

2.20.20.1.8

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. `

6.10.1.1.9 Ping-Targets

Wählen Sie eines der vorhandenen Ping-Ziele.

SNMP-ID:

2.20.20.1.9

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. `

6.10.1.1.10 Captive-Portal-Login

Wählen Sie eines der vorhandenen Captive-Portal-Logins.

SNMP-ID:

2.20.20.1.10

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

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

6.10.1.1.11 HTTP-Targets

Wählen Sie eines der vorhandenen HTTP-Ziele.

SNMP-ID:

2.20.20.1.11

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Test-Profiles**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

6.10.1.2 WLAN-Connection

Legen Sie fest, mit welcher SSID die Verbindung hergestellt und die Tests ausgeführt werden sollen.

Optional kann eine bestimmte BSSID angegeben werden, wenn die Verbindung gezielt zu einem bestimmten Access Point hergestellt werden soll. Wird keine BSSID konfiguriert, wählt der Test automatisch einen Access Point mit der angegebenen SSID aus. Dabei wird der Access Point mit der besten Signalstärke bevorzugt.

SNMP-ID:

2.20.20.2

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

6.10.1.2.1 WLAN-Connection-Name

Geben Sie dieser Verbindung einen Namen.

SNMP-ID:

2.20.20.2.1

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Connection**

Mögliche Werte:

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

6.10.1.2.2 SSID-Name

Die SSID für die Tests.

SNMP-ID:

2.20.20.2.2

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Connection**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. ``

6.10.1.2.3 BSSID

Optionale BSSID für die Tests.

SNMP-ID:

2.20.20.2.3

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Connection**

Mögliche Werte:

max. 17 Zeichen aus `mac address (xx:xx:xx:xx:xx:xx)`

6.10.1.2.4 Radio-Band

Das Radio-Band für diese Verbindung.

SNMP-ID:

2.20.20.2.4

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Connection**

Mögliche Werte:

2.4GHz
5GHz
6GHz

6.10.1.3 WLAN-Authentication

Der WLAN E2E-Test unterstützt sowohl die Authentifizierung per PSK als auch per IEEE 802.1X mit den üblichen Optionen auf Client-Seite.

Für die Verwendung von IEEE 802.1X muss zuvor ein passendes Supplicant-Profil konfiguriert werden.

SNMP-ID:

2.20.20.3

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

6.10.1.3.1 WLAN-Authentication-Name

Geben Sie dieser WLAN-Authentifizierung einen Namen.

SNMP-ID:

2.20.20.3.1

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Authentication**

Mögliche Werte:

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

6.10.1.3.2 Encryption-Key

Geben Sie den PSK an.

SNMP-ID:

2.20.20.3.2

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Authentication**

Mögliche Werte:

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

6.10.1.3.3 Method

Wählen Sie die Methode der WLAN-Authentifizierung aus.

SNMP-ID:

2.20.20.3.3

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Authentication**

Mögliche Werte:

802.11i-WPA-PSK
802.11i-WPA-802.1X
Enhanced-Open
802.11i-WPA-802.1X-192-Bits

6.10.1.3.4 WPA-Version

Wählen Sie die WPA-Version aus.

SNMP-ID:

2.20.20.3.4

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Authentication**

Mögliche Werte:

WPA1
WPA2
WPA1/2
WPA3
WPA2/3

6.10.1.3.5 Session-Keytypes

Wählen Sie den Typ des Sitzungsschlüssels aus.

SNMP-ID:

2.20.20.3.5

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Authentication**

Mögliche Werte:

TKIP
AES
TKIP/AES

6.10.1.3.6 802.1X-Client-Profile

Wählen Sie ein IEEE 802.1X-Clientprofil aus.

SNMP-ID:

2.20.20.3.6

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **WLAN-Authentication**

Mögliche Werte:

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

6.10.1.4 IP-Static-Parameters

Wenn für den Test eine statische IP-Konfiguration verwendet werden soll, tragen Sie die entsprechenden IP-Parameter in dieser Tabelle ein.

SNMP-ID:

2.20.20.4

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

6.10.1.4.1 IP-Static-Parameters-Name

Geben Sie dieser statischen IP-Konfiguration einen Namen.

SNMP-ID:

2.20.20.4.1

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **IP-Static-Parameters**

Mögliche Werte:

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

6.10.1.4.2 IP-Address

Tragen sie die IP-Adresse ein.

SNMP-ID:

2.20.20.4.2

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **IP-Static-Parameters**

Mögliche Werte:

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

6.10.1.4.3 IP-Gateway

Tragen sie den IP-Gateway ein.

SNMP-ID:

2.20.20.4.3

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **IP-Static-Parameters**

Mögliche Werte:

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

6.10.1.4.4 Primary-IP-DNS

Tragen sie die IP-Adresse des primären DNS-Servers ein.

SNMP-ID:

2.20.20.4.4

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **IP-Static-Parameters**

Mögliche Werte:

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

6.10.1.4.5 Secondary-IP-DNS

Tragen sie die IP-Adresse des sekundären DNS-Servers ein.

SNMP-ID:

2.20.20.4.5

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **IP-Static-Parameters**

Mögliche Werte:

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

6.10.1.5 DNS-Targets

Hier können Sie den DNS-Test konfigurieren. Im Feld **Erwartete Antwort** können Sie durch das Präfix „A:“ oder „AAAA:“ festlegen, dass ein bestimmter A- bzw. AAAA-Record erwartet wird.

Mehrere Records können als kommagetrennte Liste angegeben werden. Der Test gilt als erfolgreich, sobald einer der konfigurierten Records mit der empfangenen Antwort übereinstimmt.

Bleibt das Feld **Erwartete Antwort** leer, gilt jeder empfangene A- oder AAAA-Record als erfolgreiche Antwort.

SNMP-ID:

2.20.20.5

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

6.10.1.5.1 DNS-Targets-Name

Geben Sie diesen DNS-Zielen einen Namen.

SNMP-ID:

2.20.20.5.1

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **DNS-Targets**

Mögliche Werte:

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

6.10.1.5.2 DNS-Target-Hostname

Geben Sie die Hostnamen an, die getestet werden sollen.

SNMP-ID:

2.20.20.5.2

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **DNS-Targets**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9].-`

6.10.1.5.3 Expected-Response

Geben Sie die für diesen Test erwartete Antwort ein.

SNMP-ID:

2.20.20.5.3

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **DNS-Targets**

Mögliche Werte:

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

6.10.1.6 Ping-Targets

Hier können Sie den Ping-/ICMP-Test konfigurieren. Die Felder Ping- und Fehler-Anzahl sind mit den gezeigten Standardwerten vorbelegt und können bei Bedarf angepasst werden.

SNMP-ID:

2.20.20.6

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

6.10.1.6.1 Ping-Targets-Name

Geben Sie diesen Ping-Zielen einen Namen.

SNMP-ID:

2.20.20.6.1

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Ping-Targets**

Mögliche Werte:

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

6.10.1.6.2 Ping-Target-Hostname

Geben Sie den Hostnamen an, der getestet werden sollen.

SNMP-ID:

2.20.20.6.2

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Ping-Targets**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9].-:%`

6.10.1.6.3 Ping-Count

Geben Sie die Ping-Anzahl an.

SNMP-ID:

2.20.20.6.3

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Ping-Targets**

Mögliche Werte:

max. 5 Zeichen aus `[0-9]`

Default-Wert:

10

6.10.1.6.4 Fail-Count

Geben Sie die Fehler-Anzahl an.

SNMP-ID:

2.20.20.6.4

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Ping-Targets**

Mögliche Werte:

max. 5 Zeichen aus `[0-9]`

Default-Wert:

2

6.10.1.7 Captive-Portal-Logins

Wenn das zu testende Netzwerk durch ein Captive Portal geschützt ist, können Sie die erforderlichen Anmeldeparameter hier konfigurieren.

Der E2E-Test ruft zunächst die konfigurierte Test-URL auf, um zu prüfen, ob das Captive Portal eine Weiterleitung durchführt. Wird eine Weiterleitung erkannt, erstellt der Test eine HTTP-POST-Anfrage mit den Einträgen aus der Tabelle Captive-Portal-Login-Daten und sendet diese an die im Feld Formular-Aktion angegebene URL.

Anschließend wird die Test-URL erneut aufgerufen. Erfolgt nun keine Weiterleitung mehr, gilt die Anmeldung als erfolgreich und der Test wird bestanden.

SNMP-ID:

2.20.20.7

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

6.10.1.7.1 Captive-Portal-Login-Name

Geben Sie diesem Captive-Portal-Login einen Namen.

SNMP-ID:

2.20.20.7.1

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Logins**

Mögliche Werte:

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

6.10.1.7.2 Type

Hier kann entweder „Login“ oder „Logout“ ausgewählt werden.

Je nach Captive Portal kann es sinnvoll sein, den Benutzer nach Abschluss des Tests wieder abzumelden. Dadurch lassen sich beispielsweise Ressourcen auf dem Captive-Portal-Gateway schonen oder erneute Anmeldungen mit denselben Zugangsdaten bei späteren Testläufen ermöglichen.

Legen Sie hierzu einen zusätzlichen Eintrag mit dem Typ „Logout“ an. Konfigurieren Sie dabei die **Formular-Aktion** so, dass sie die Abmeldeaktion des Captive Portals ausführt. Die URL für die Abmeldung kann sich von der URL des Anmeldeformulars unterscheiden. Analysieren Sie hierzu den HTML-Code des jeweiligen Portals.

Viele moderne Captive Portals mit Click-through-Anmeldung bieten jedoch keine Abmeldefunktion. Die Benutzersitzung wird in diesem Fall erst nach einem Timeout beendet. Ein regelmäßig in kurzen Abständen ausgeführter Captive-Portal-Test kann dann möglicherweise erfolgreich sein, ohne die Anmeldung tatsächlich zu prüfen, da die MAC-Adresse des testenden Access Points noch im Captive Portal zwischengespeichert ist.

Wenn Sie das Captive Portal selbst verwalten, kann eine spezielle Testfunktion sinnvoll sein. Beispielsweise könnte ein verstecktes Formular im HTML-Code eine dedizierte Testsitzung starten, die bereits nach kurzer Zeit automatisch abläuft.

SNMP-ID:

2.20.20.7.2

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Logins**

Mögliche Werte:

Login
Logout

6.10.1.7.3 Test-URL

Dies ist die URL, die der E2E-Test aufruft, um festzustellen, ob das Captive Portal eine Weiterleitung durchführt. Sie kann auf jede URL zeigen, die zuverlässig mit einem HTTP-Statuscode aus dem Bereich „200“ antwortet. Idealerweise wird eine URL verwendet, die mit „200“ oder „204“ antwortet.

Das Feld ist standardmäßig leer, da keine URL eines externen Drittanbieters fest vorgegeben werden kann. Es muss daher eine geeignete URL konfiguriert werden.

SNMP-ID:

2.20.20.7.3

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Logins**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

6.10.1.7.4 Form-Action

Dies ist die URL, an die die Anmeldedaten per HTTP POST übertragen werden. Beim klassischen LCOS-Public Spot kann dies beispielsweise eine URL wie die Folgende sein:

```
https://pspot.lancom.de:443/authen/login/
```

Bleibt dieses Feld leer, verwendet der E2E-Test automatisch die URL, zu der das Captive Portal beim ersten Aufruf der Success-URL weitergeleitet hat. Bei R&S®LANCOM Management Cloud-basierten Hotspots funktioniert die Anmeldung dadurch in der Regel ohne zusätzliche Konfiguration dieser URL.

SNMP-ID:

2.20.20.7.4

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Logins**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

6.10.1.8 HTTP-Targets

In dieser Tabelle können Sie eine HTTP-Verbindung testen. Der E2E-Test ruft die konfigurierte **HTTP-Ziel-URL** ab und vergleicht den empfangenen HTTP-Statuscode mit dem im Feld **Erwartete Antwort** angegebenen Wert.

Der HTTP-Test kann zusätzlich als Geschwindigkeitstest verwendet werden, wenn über die HTTP-Ziel-URL eine ausreichend große Datei heruntergeladen werden kann. Damit eine aussagekräftige Durchsatzmessung möglich ist, sollte in diesem Fall auch **Maximale Größe (Bytes)** konfiguriert werden. Wird kein Maximalwert angegeben, wird die Datei vollständig heruntergeladen.

Der gemessene Durchsatz wird in den Testergebnissen immer angezeigt. Aussagekräftig ist dieser Wert jedoch nur, wenn eine ausreichend große Datei heruntergeladen wird und der TCP-/HTTP-Download eine realistische Übertragungsgeschwindigkeit erreichen kann.

SNMP-ID:

2.20.20.8

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

6.10.1.8.1 HTTP-Targets-Name

Geben Sie diesen HTTP-Zielen einen Namen.

SNMP-ID:

2.20.20.8.1

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **HTTP-Targets**

Mögliche Werte:

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

6.10.1.8.2 HTTP-Target-URL

Geben Sie die URL an, die getestet werden soll.

SNMP-ID:

2.20.20.8.2

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **HTTP-Targets**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

6.10.1.8.3 Expected-Response

Geben Sie die erwartete Antwort an.

SNMP-ID:

2.20.20.8.3

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **HTTP-Targets**

Mögliche Werte:

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

6.10.1.8.4 Max-Size-Bytes

Optionale Größenbeschränkung.

SNMP-ID:

2.20.20.8.4

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **HTTP-Targets**

Mögliche Werte:

max. 20 Zeichen aus `[0-9]`

6.10.1.9 Captive-Portal-Login-Data

In dieser Tabelle werden die Formularelemente konfiguriert, die für eine Anmeldung oder Abmeldung per HTTP POST an das Captive Portal übertragen werden.

Bei einem klassischen, auf LCOS basierenden Public Spot können die Formulardaten beispielsweise wie folgt aussehen:

Attribut	Wert
AGB	checked
password	geheim
userid	rsnc

Wenn zusätzlich die Logout-Funktion verwendet wird, müssen in dieser Tabelle auch die entsprechenden Attribute für den Logout-Test hinterlegt werden.

Bei sehr einfachen Portalseiten, die beispielsweise nur ein einziges Formularattribut – etwa eine Schaltfläche für den Click-through-Login – enthalten, versucht der E2E-Test, dieses Attribut automatisch per POST zu übertragen. In diesem Fall ist keine zusätzliche Konfiguration in dieser Tabelle erforderlich. Dies funktioniert derzeit beispielsweise beim One-Button-Login des R&S®LANCOM Management Cloud-Hotspots.

SNMP-ID:

2.20.20.9

Pfad Konsole:

Setup > **WLAN** > **End2End-Test**

6.10.1.9.1 Captive-Portal-Login-Name

Geben Sie diesem Captive-Portal-Login einen Namen.

SNMP-ID:

2.20.20.9.1

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Login-Data**

Mögliche Werte:

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

6.10.1.9.2 Attribute

Geben Sie hier die benötigten Attribue an.

SNMP-ID:

2.20.20.9.2

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Login-Data**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. `

6.10.1.9.3 Value

Geben Sie hier die Werte zu den konfigurierten Attribuen an.

SNMP-ID:

2.20.20.9.3

Pfad Konsole:

Setup > **WLAN** > **End2End-Test** > **Captive-Portal-Login-Data**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_. `

6.10.1.10 Run-Tests

Mit dieser Aktion starten Sie die Tests.

Beispiel: `do Run-Tests`

SNMP-ID:

2.20.20.20

Pfad Konsole:

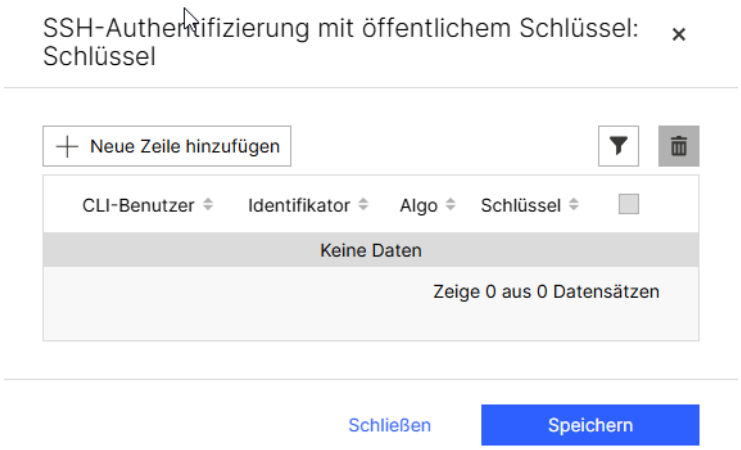
Setup > **WLAN** > **End2End-Test**

7 SSH-Authentifizierung mit öffentlichem Schlüssel

Konfigurieren Sie hier in der WEBconfig (**Systemkonfiguration** > **Konfiguriere SSH-Authentifizierung mit öffentlichem Schlüssel** die Einstellungen für die SSH-Authentifizierung mit öffentlichem Schlüssel.

Schlüssel

Zusätzlich zur interaktiven Authentifizierung mittels Benutzername und Passwort kann auch die Public-Key-Authentifizierung verwendet werden.



CLI-Benutzer

Der Benutzer, für den der in Folge eingetragene Public Key gültig sein soll. Dies kann entweder der Benutzer „root“ sein, oder ein optional zusätzlich eingerichteter Administrator (siehe *Weitere Administratoren*).

Identifikator

Der Identifikator wird verwendet, um mehrere Public Keys für den selben CLI-Benutzer verwenden zu können, z. B. wenn für jeden SSH-Client ein eigener Public Key erzeugt wurde, aber der Login im LCOS LX mit dem selben Benutzer-Account erfolgen soll. In diesem Fall wird der selbe CLI-Benutzer eingetragen, aber ein abweichender Identifikator.

Algo

Der Algorithmus, mit welchem der Public Key generiert wurde.

Schlüssel

Der zu verwendende Public Key.

7.1 Ergänzungen im Setup-Menü

7.1.1 Keys

Zusätzlich zur interaktiven Authentifizierung mittels Benutzername und Passwort kann auch die Public-Key-Authentifizierung verwendet werden. Diese kann hier konfiguriert werden.

SNMP-ID:

2.11.52.5

Pfad Konsole:

Setup > **Config** > **SSH**

7.1.1.1 CLI-User

Der Benutzer, für den der in Folge eingetragene Public Key gültig sein soll. Dies kann entweder der Benutzer „root“ sein, oder ein optional zusätzlich eingerichteter Administrator (siehe *Weitere Administratoren*).

SNMP-ID:

2.11.52.5.1

Pfad Konsole:

Setup > **Config** > **SSH** > **Keys**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

7.1.1.2 Identifier

Der Identifikator wird verwendet, um mehrere Public Keys für den selben CLI-Benutzer verwenden zu können, z. B. wenn für jeden SSH-Client ein eigener Public Key erzeugt wurde, aber der Login im LCOS LX mit dem selben Benutzer-Account erfolgen soll. In diesem Fall wird der selbe CLI-Benutzer eingetragen, aber ein abweichender Identifikator.

SNMP-ID:

2.11.52.5.2

Pfad Konsole:

Setup > **Config** > **SSH** > **Keys**

Mögliche Werte:

max. 254 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

7.1.1.3 Algo

Der Algorithmus, mit welchem der Public Key generiert wurde.

SNMP-ID:

2.11.52.5.3

Pfad Konsole:

Setup > **Config** > **SSH** > **Keys**

Mögliche Werte:

ssh-rsa
ssh-dss
ssh-ed25519
ecdsa-sha2-nistp256
ecdsa-sha2-nistp384
ecdsa-sha2-nistp521
rsa-sha2-256
rsa-sha2-512
sk-ecdsa-sha2-nistp256-openssh
sk-ssh-ed25519-openssh

7.1.1.4 Key

Der zu verwendende Public Key.

SNMP-ID:

2.11.52.5.4

Pfad Konsole:

Setup > **Config** > **SSH** > **Keys**

Mögliche Werte:

max. 1400 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.``

8 Ergänzungen im Status-Menü

8.1 Syslog

In diesem Menü finden Sie einige Statusinformationen zum Syslog.

SNMP-ID:

1.62

Pfad Konsole:

Status

8.1.1 Last-Messages

In dieser Tabelle finden Sie die Nachrichten des Syslog. Beispiel:

```
Id Time           Priority  Message                                              LMC-Message-ID
===-------------------------------------------------------------------------------------------------
0  1786102398625  err       "lxcron[6204]: Service temporarily not available"  5c9f6e94-e39a-...
1  1786102399918  notice    "mcastds: Entering evloopRun"                      4276b3ac-bfc9-...
2  1786102403656  err       "lxcron[7226]: Service temporarily not available"  38b0a6cc-e95b-...
```

SNMP-ID:

1.62.1

Pfad Konsole:

Status > **Syslog**

8.1.1.1 Id

ID einer Syslog-Nachricht.

SNMP-ID:

1.62.1.1

Pfad Konsole:

Status > **Syslog** > **Last-Messages**

Mögliche Werte:

max. 5 Zeichen aus `[0-9]`

8.1.1.2 Time

Zeitstempel einer Syslog-Nachricht.

SNMP-ID:

1.62.1.2

Pfad Konsole:

Status > **Syslog** > **Last-Messages**

Mögliche Werte:

max. 20 Zeichen aus `[0-9]`

8.1.1.3 Priority

Stufe einer Syslog-Nachricht.

SNMP-ID:

1.62.1.3

Pfad Konsole:

Status > **Syslog** > **Last-Messages**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

8.1.1.4 Message

Text einer Syslog-Nachricht.

SNMP-ID:

1.62.1.4

Pfad Konsole:

Status > **Syslog** > **Last-Messages**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

8.1.1.5 LMC-Message-ID

LMC-Message-ID einer Syslog-Nachricht.

SNMP-ID:

1.62.1.5

Pfad Konsole:

Status > **Syslog** > **Last-Messages**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`