LCOS LX 7.20

Addendum

10/2026

ROHDE&SCHWARZ
Make ideas real

Contents

1 Addendum to LCOS LX version 7.20....4
2 Additional Administrators....5
2.1 Additions to the Setup menu....5
2.1.1 Admins....5
3 Time Automation via Cron Job....8
3.1 Additions to the Setup menu....9
3.1.1 Cron-Table....9
4 Client Management....13
4.1 Profiles....14
4.2 Radio Settings....15
4.3 Additions to the Setup menu....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-Groups....21
5.2 Rules....21
5.3 Additions to the Setup menu....22
5.3.1 Firewall....22
6 End-to-End Test....28
6.1 Test Profiles....29
6.2 WLAN Connection....30
6.3 WLAN Authentication....30
6.4 Static IP parameters....31
6.5 DNS Targets....32
6.6 Ping Targets....33
6.7 HTTP Targets....33
6.8 Captive Portal Logins....34
6.9 Captive Portal Login Data....35
6.10 Additions to the Setup menu....36
6.10.1 End2End-Test....36
7 SSH Public Key Authentication....55
7.1 Additions to the Setup menu....56
7.1.1 Keys....56
8 Additions to the Status menu....58
8.1 Syslog....58
8.1.1 Last-Messages....58

Copyright

© 2026 Rohde & Schwarz Networks and Cybersecurity GmbH, Würselen (Germany). All rights reserved.

Notice on the company name: Since July 1, 2026, LANCOM Systems has been named **Rohde & Schwarz Networks and Cybersecurity**. Product information and communication materials are accordingly issued under the new company name.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. Rohde & Schwarz Networks and Cybersecurity shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from Rohde & Schwarz Networks and Cybersecurity. We reserve the right to make any alterations that arise as the result of technical development.

Windows® and Microsoft® are registered trademarks of Microsoft, Corp.

R&S and Rohde & Schwarz are trademarks of Rohde & Schwarz GmbH & Co. KG, registered or used, among others, in Germany, the EU, the USA, China, and other countries. Other names or designations used may be registered trademarks of different companies or owners. This document contains forward-looking statements regarding products and product features. The publisher reserves the right to change these at any time without stating reasons. No liability is accepted for technical inaccuracies or omissions.

This product contains separate open-source software components. These are subject to their own licenses, in particular the General Public License (GPL). License information relating to the device firmware (LCOS LX) is available on the CLI by using the command `show 3rd-party-licenses`. If the respective license demands, the source files for the corresponding software components will be made available on request. Please contact us via e-mail under *gpl.rs-nc@rohde-schwarz.com*.

Products from Rohde & Schwarz Networks and Cybersecurity include software developed by the “OpenSSL Project” for use in the “OpenSSL Toolkit” (*www.openssl.org*).

Products from Rohde & Schwarz Networks and Cybersecurity include cryptographic software written by Eric Young (*eay@cryptsoft.com*).

Products from Rohde & Schwarz Networks and Cybersecurity include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from Rohde & Schwarz Networks and Cybersecurity contain the LZMA SDK developed by Igor Pavlov.

Rohde & Schwarz Networks and Cybersecurity GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

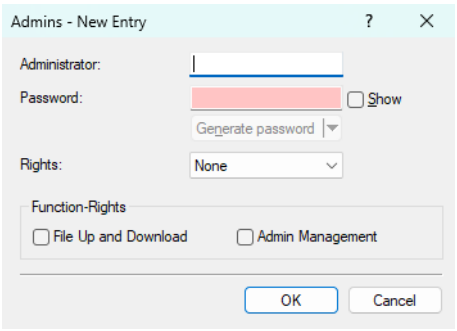
www.rohde-schwarz.com/networks-and-cybersecurity

1 Addendum to LCOS LX version 7.20

This document describes the changes and enhancements in LCOS LX version 7.20 since the previous version.

2 Additional Administrators

Not every configuration task requires an administrator with full permissions. As a root administrator, you can create administrators with restricted permissions. This means that the main device password does not have to be known to every administrator. Additional administrators are configured under **Management** > **Admin** > **Admins**.



Administrator

The name of the new administrator account.

Password

The password of the new administrator account.

Rights

Select one of the following access rights:

- **None:** The configuration cannot be read or written, but a CLI login for executing commands is possible.
- **Admin-RO:** The configuration can be read but not written.
- **Admin-RW:** The configuration can be read and written.

Function-Rights

Select from the following function rights:

- **File Up and Download:** This function right is required to transfer files, for example via SCP, such as the support information file.
- **Admin Management:** This function right is required to configure additional administrators on the device.

2.1 Additions to the Setup menu

2.1.1 Admins

Use this table to create administrators with restricted rights.

The root administrator always has all rights.

SNMP ID:

2.11.21

Console path:

Setup > **Config**

2.1.1.1 Administrator

Login name of the administrator in this row of the table.

SNMP ID:

2.11.21.1

Console path:

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

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-.`

2.1.1.2 Function-Rights

Here you activate the administrator's function rights in this row of the table.

SNMP ID:

2.11.21.3

Console path:

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

Possible values:

Basic
Admin-Management

2.1.1.3 Rights

The rights of the administrator in this row of the table.

SNMP ID:

2.11.21.5

Console path:

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

Possible values:

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

2.1.1.4 Hashed-Password

Hash value of the administrator password in this row of the table.

SNMP ID:

2.11.21.6

Console path:

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

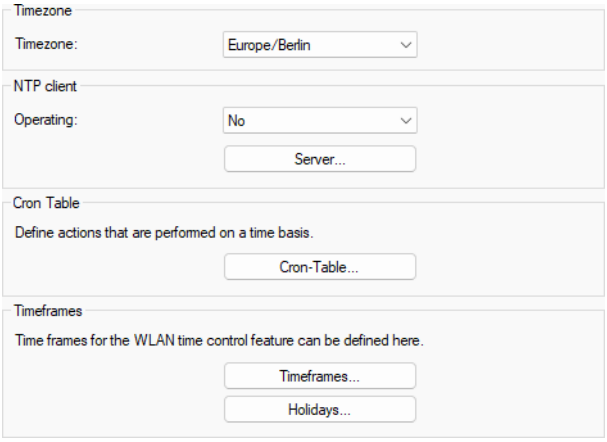
Possible values:

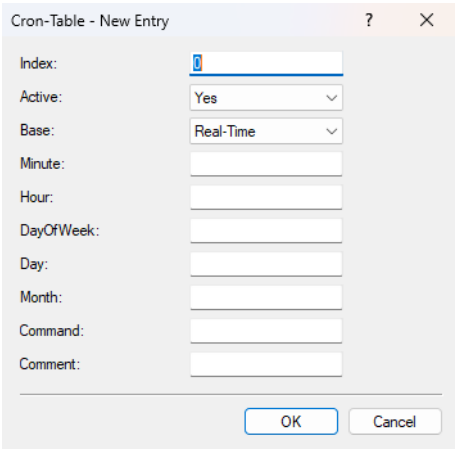
Max. 255 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

3 Time Automation via Cron Job

This feature enables the device to execute specific commands at specific, user-defined times. The functionality corresponds to the Cron service known from UNIX. Any command-line function can be executed. This means that all features can be controlled based on a schedule.

You can find the settings for the cron table under **Date / Time** > **Configuration**.





The function of the individual fields largely corresponds to the Cron job configuration known from Linux/Unix.

Index

Used to sort multiple Cron jobs.

Active

Determines whether the job is executed.

Base

The time base determines whether LCOS LX executes the command based on the device's real time or system uptime, that is, the time elapsed since the device was started.

Minute

The command is executed when the minute specified here is reached.

Hour

The command is executed when the hour specified here is reached.

DayOfWeek

The command is executed on the days of the week specified here using numbers. The digits representing the days of the week are separated by spaces. 0 represents Sunday, 1 represents Monday, …, and 6 represents Saturday.

Day

The command is executed on the days of the month specified here (from 1 to 31).

Month

The command is executed in the months specified here (from 1 to 12).

Command

The CLI command to be executed.

Comment

A free-text field for entering any comment.

3.1 Additions to the Setup menu

3.1.1 Cron-Table

This feature enables the device to execute specific commands at specific, user-defined times. The functionality corresponds to the Cron service known from UNIX. Any command-line function can be executed. This means that all features can be controlled based on a schedule.

The function of the individual fields largely corresponds to the Cron job configuration known from Linux/Unix.

SNMP ID:

2.11.20

Console path:

Setup > **Config**

3.1.1.1 Index

Used to sort multiple Cron jobs.

SNMP ID:

2.11.20.1

Console path:

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

Possible values:

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

3.1.1.2 Active

Determines whether the job is executed.

SNMP ID:

2.11.20.2

Console path:

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

Possible values:

Yes
No

3.1.1.3 Base

The time base determines whether LCOS LX executes the command based on the device's real time or system uptime, that is, the time elapsed since the device was started.

SNMP ID:

2.11.20.3

Console path:

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

Possible values:

Real-Time
Operating-Time

3.1.1.4 Minute

The command is executed when the minute specified here is reached.

SNMP ID:

2.11.20.4

Console path:

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

Possible values:

Max. 32 characters from `Range or comma-separated list between 0 and 59 (1,2,3 or 0-59 or 1-3,59)`

3.1.1.5 Hour

The command is executed when the hour specified here is reached.

SNMP ID:

2.11.20.5

Console path:

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

Possible values:

Max. 32 characters from `Range or comma-separated list between 0 and 23 (1,2,3 or 0-23 or 1-3,23)`

3.1.1.6 DayOfWeek

The command is executed on the days of the week specified here using numbers. The digits representing the days of the week are separated by spaces. 0 represents Sunday, 1 represents Monday, …, and 6 represents Saturday.

SNMP ID:

2.11.20.6

Console path:

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

Possible values:

Max. 32 characters from `Range or comma-separated list between 0 and 6 (1,2,3 or 0-6 or 1-3,6)`

3.1.1.7 Day

The command is executed on the days of the month specified here (from 1 to 31).

SNMP ID:

2.11.20.7

Console path:

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

Possible values:

Max. 32 characters from `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

The command is executed in the months specified here (from 1 to 12).

SNMP ID:

2.11.20.8

Console path:

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

Possible values:

Max. 32 characters from `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

The CLI command to be executed.

SNMP ID:

2.11.20.9

Console path:

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

Possible values:

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

3.1.1.10 Comment

A free-text field for entering any comment.

SNMP ID:

2.11.20.10

Console path:

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

Possible values:

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

Default:

empty

4 Client Management

As of LCOS LX 7.20, client management based on IEEE 802.11k and IEEE 802.11v is supported. The variant of client management known from LCOS LX <7.20 (pure band steering) remains optionally available. The configuration has been moved to the “WLAN Band Steering Settings” section.

Client management is used to distribute WLAN clients within a network across the available access points based on load. In high-density scenarios, this can result in a more even utilization of WLAN resources, including AP capacity and channel capacity.

Client management is based on two core technologies: RRM (Radio Resource Management / IEEE 802.11k) and WNM (Wireless Network Management (IEEE 802.11v).

RRM

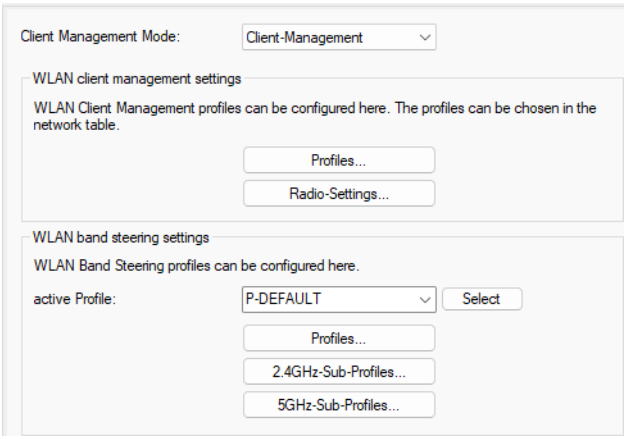
Client management supports RRM Neighbor Reports. Clients can send a Neighbor Report Request to the AP; the AP responds with a Neighbor Report containing a list of potential roaming candidates. The AP determines these roaming candidates by means of an automated environmental scan that is performed once a day, scans the radio environment for candidates, and uses IAPP to verify that the identified APs are in fact LCOS LX APs belonging to the same network. In addition to the list of candidates, a priority for each candidate is transmitted (BSS Transition Candidate Preference). This priority is based on the current number of clients associated with the candidate AP (fewer clients = higher priority).

WNM

Client management supports WNM BSS Transition Management (BTM). Clients can send BTM Queries to the AP, which in turn sends a BTM Request with one or more suitable roaming candidates. In principle, this is similar to the process described above for RRM; only a different protocol is used.

To instruct a client to switch to another AP, the AP can also send unsolicited BTM Requests to the client. This occurs as soon as the thresholds described below are reached. These thresholds are checked each time a new client associates. When a threshold is reached, Client Management randomly selects an associated client that has been associated for more than 5 minutes and sends it a BTM Request to encourage it to switch to a non-overloaded AP. Clients that have been associated for less than 5 minutes or that have already received a BTM Request from this AP within the last 5 minutes are not contacted in order to prevent multiple roaming processes within a short period of time.

You can find the Client Management settings for WLAN networks under **Wireless LAN** > **Client Management**.



Client Management Mode

Specify whether to use Client Management, band steering only, or neither feature.

4.1 Profiles

Under **Wireless LAN** > **Client management** > **Profiles**, define configuration profiles for client management or use one of the predefined profiles:

Existing Profiles

DEFAULT

Enables RRM, but not WNM/BSS Transition Management.

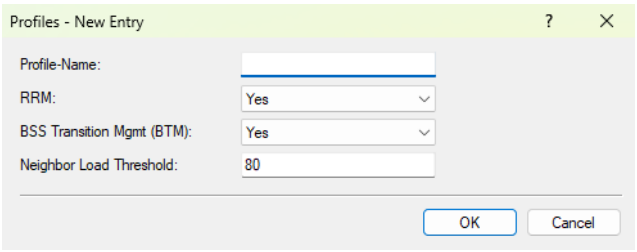
DISABLED

Disables both RRM and WNM/BTM.

RRM+BTM

Enables RRM and WNM/BTM.

Assign the desired profile under **Wireless-LAN** > **WLAN-Networks** > **Networks** > **Client-Mgmt-Profile**.



Profile-Name

Name of this profile.

RRM

Enable the use of RRM here.

BSS Transition Mgmt (BTM)

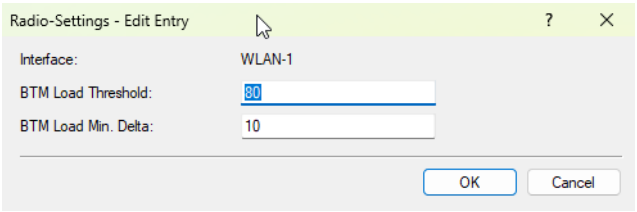
Enable the use of WNM/BTM here.

Neighbor Load Threshold

The percentage up to which APs may be loaded and still be considered as roaming targets. Currently, 100% corresponds to 80 associated clients; different AP models are not distinguished. The value is used for RRM and WNM/BTM.

4.2 Radio Settings

Under **Wireless-LAN** > **Client management** > **Radio-Settings**, define the radio settings for client management.



Interface

The WLAN interface to which the following settings apply.

BTM Load Threshold

When the load on this WLAN interface of the AP exceeds the threshold, the AP sends BTM requests to associated clients to steer them to other APs.

BTM Load Min. Delta

This is a dynamic threshold: it is relative to the load of the AP itself. The value configured here specifies the minimum load difference compared to our own load: only neighboring APs whose load is at least BTM Load Min. Delta lower than our own load are recommended to clients. All others are marked as “do not use”. Example: BTM Load Threshold is 80, and BTM Load Min. Delta is 10. Assume that our own load is 85—we have exceeded the threshold and attempt to move clients to neighboring APs using BTM requests. However, with a minimum delta of 10, only APs whose load is at least 10 points lower than our own are recommended to clients. In this example, all neighboring APs with a load of 75 or higher are therefore marked as “do not use”. (Note: The static threshold from the profile table continues to apply independently.)

This “minimum delta” is used to create hysteresis and prevent two neighboring APs with a high load—each close to its own threshold—from continuously moving clients back and forth between them.

4.3 Additions to the Setup menu

4.3.1 Client-Mgmt-Profile

Select one of the Client Management profiles from *2.20.18.2 Profiles* on page 16 here.

SNMP ID:

2.20.1.43

Console path:

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

Possible values:

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

4.3.2 Client-Management

Configure client management here.

SNMP ID:

2.20.18

Console path:

Setup > **WLAN**

4.3.2.1 Profiles

Define configuration profiles for client management here. You can select the profiles in the network table.

SNMP ID:

2.20.18.2

Console path:

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

4.3.2.1.1 Profile-Name

Name of this profile.

SNMP ID:

2.20.18.2.1

Console path:

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

Possible values:

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

4.3.2.1.2 RRM

Enable the use of RRM here.

SNMP ID:

2.20.18.2.2

Console path:

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

Possible values:

No
Yes

4.3.2.1.3 BTM

Enable the use of WNM/BTM here.

SNMP ID:

2.20.18.2.3

Console path:

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

Possible values:

No
Yes

4.3.2.1.4 Neighbor-Load-Threshold

The percentage up to which APs may be loaded and still be considered as roaming targets. Currently, 100% corresponds to 80 associated clients; different AP models are not distinguished. The value is used for RRM and WNM/BTM.

SNMP ID:

2.20.18.2.4

Console path:

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

Possible values:

0 … 100

4.3.2.2 Radio-Settings

Define the radio settings for client management here.

SNMP ID:

2.20.18.3

Console path:

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

4.3.2.2.1 Ifc

The WLAN interface to which the following settings apply.

SNMP ID:

2.20.18.3.1

Console path:

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

Possible values:

Max. 9 characters from `WLAN-1,WLAN-1-2,...`

4.3.2.2.2 BTM-Load-Threshold

When the load on this WLAN interface of the AP exceeds the threshold, the AP sends BTM requests to associated clients to steer them to other APs.

SNMP ID:

2.20.18.3.2

Console path:

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

Possible values:

0 … 100

4.3.2.2.3 BTM-Load-Min-Delta

This is a dynamic threshold: it is relative to the load of the AP itself. The value configured here specifies the minimum load difference compared to our own load: only neighboring APs whose load is at least BTM Load Min. Delta lower than our own load are recommended to clients. All others are marked as “do not use”. Example: BTM Load Threshold is 80, and BTM Load Min. Delta is 10. Assume that our own load is 85—we have exceeded the threshold and attempt to move clients to neighboring APs using BTM requests. However, with a minimum delta of 10, only APs whose load is at least 10 points lower than our own are recommended to clients. In this example, all neighboring APs with a load of 75 or higher are therefore marked as “do not use”. (Note: The static threshold from the profile table continues to apply independently.)

This “minimum delta” is used to create hysteresis and prevent two neighboring APs with a high load—each close to its own threshold—from continuously moving clients back and forth between them.

SNMP ID:

2.20.18.3.3

Console path:

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

Possible values:

0 … 100

4.3.3 Client-Management-Mode

Specify whether to use Client Management, band steering only, or neither feature.

SNMP ID:

2.20.19

Console path:

Setup > **WLAN**

Possible values:

Client-Management
Band-Steering
Off

5 Firewall

The firewall can be used to filter traffic to and from WLAN networks at the IP level. A deny-all strategy (all traffic is blocked except for configured exceptions) or an allow-all strategy (all traffic is allowed, and only exceptions are blocked) can be used. In addition to IP addresses, hostnames / DNS names can also be used as destinations. To do this, the firewall monitors all DNS requests from clients in the affected WLAN and stores the resolved IP addresses in an internal cache until the TTL (time-to-live) expires. If a client subsequently attempts to establish a connection to an IP address identified in this way, the connection can be blocked or allowed, depending on the configuration.

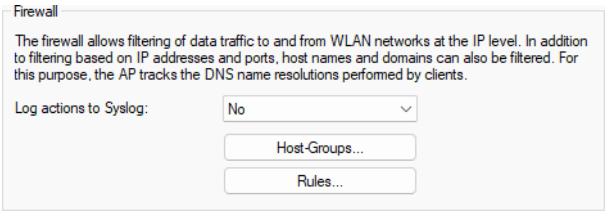
Monitoring DNS requests is only possible with unencrypted DNS. If the client uses encrypted methods such as DoT (DNS-over-TLS) or DoH (DNS-over-HTTPS), the DNS requests cannot be inspected. In this case, it may be advisable to block these DNS methods using the firewall as well. DoT can be blocked by blocking the port used for it, port 853. DoH uses the regular HTTPS port 443 and therefore cannot be blocked in general; however, DoH servers are usually initially resolved using regular DNS, so popular DoH server domains can be blocked by specifying their names in the firewall.

It is not possible to block DoH completely by design. If preventing all uncontrolled traffic is the priority, it is therefore recommended to configure a deny-all strategy and explicitly allow permitted services.

When a client roams between APs, the client's applications normally do not issue new DNS requests in response. This usually occurs only after the TTL (time-to-live) expires. The firewall of the AP to which the client has roamed therefore cannot analyze DNS requests or learn the resolved IP addresses and, as a result, cannot actually block the client's traffic. To enable this nevertheless, the firewall's DNS cache is transferred and kept synchronized via IAPP between APs configured with the same SSID or SSIDs. This causes all associated APs in the network to generate the same effective firewall rule set and filter traffic based on the IP addresses that any AP in the network has identified from the client's DNS requests. The current DNS cache can be viewed on the AP using the CLI command `ls /Status/DNS/Snooping-Results`.

Note that only the (volatile) DNS cache is synchronized. The AP configuration, consisting of host groups and filter rules, is not synchronized and must be kept identical separately for all APs.

The settings for the IP- and DNS-based firewall are available under **Wireless LAN** > **Firewall**.



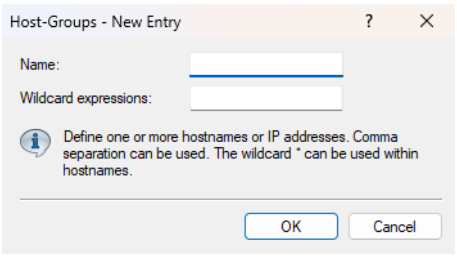
Log Actions to Syslog

When a firewall rule is processed, an entry is created in Syslog.

Depending on the amount of traffic, this may require significant CPU resources and generate a large number of Syslog messages.

5.1 Host-Groups

Configure hostnames or IP addresses here for use in the firewall rules later.



Name

Name of the group.

Wildcard expressions

One or more comma-separated IP addresses or hostnames. You can use the wildcard character * in this field to represent any characters.

The syntax of the wildcard expressions is compatible with that of the app definitions for LCOS.

5.2 Rules

Configure the firewall rules here.

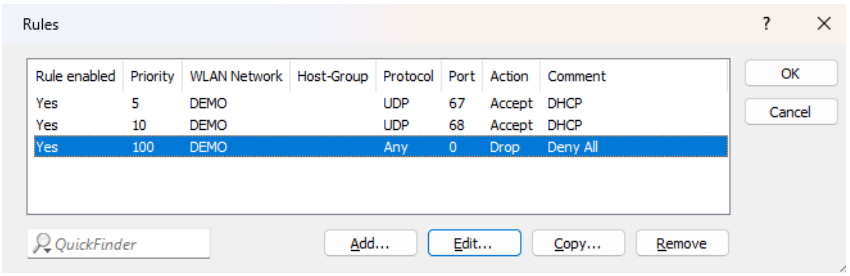
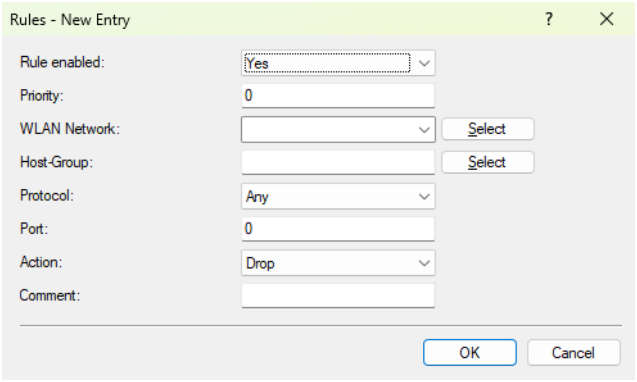


Figure 1: Deny-All Example

Note that the deny-all rule blocks **all** traffic. Therefore, you must explicitly allow the appropriate ports for DHCPv4 to enable IPv4 address assignment.



Rule enabled

Specifies whether the rule is active for the firewall.

Priority

Priority of the rule. Rules with lower values are processed before rules with higher values.

WLAN Network

The WLAN network for which the rule is active.

Host-Group

One or more previously configured host groups against which the destination of the rule is checked.

Protocol

Configures whether the rule applies only to TCP, UDP, or all traffic.

Port

If TCP or UDP is entered as the protocol, you can additionally specify a port number here as a filter criterion.

Action

Configures whether the connection is allowed or discarded when the rule applies.

Comment

A free-text field for entering any comment.

5.3 Additions to the Setup menu

5.3.1 Firewall

The firewall can be used to filter traffic to and from WLAN networks at the IP level. A deny-all strategy (all traffic is blocked except for configured exceptions) or an allow-all strategy (all traffic is allowed, and only exceptions are blocked) can be used. In addition to IP addresses, hostnames / DNS names can also be used as destinations. To do this, the firewall monitors all DNS requests from clients in the affected WLAN and stores the resolved IP addresses in an internal cache until

the TTL (time-to-live) expires. If a client subsequently attempts to establish a connection to an IP address identified in this way, the connection can be blocked or allowed, depending on the configuration.

Monitoring DNS requests is only possible with unencrypted DNS. If the client uses encrypted methods such as DoT (DNS-over-TLS) or DoH (DNS-over-HTTPS), the DNS requests cannot be inspected. In this case, it may be advisable to block these DNS methods using the firewall as well. DoT can be blocked by blocking the port used for it, port 853. DoH uses the regular HTTPS port 443 and therefore cannot be blocked in general; however, DoH servers are usually initially resolved using regular DNS, so popular DoH server domains can be blocked by specifying their names in the firewall.

It is not possible to block DoH completely by design. If preventing all uncontrolled traffic is the priority, it is therefore recommended to configure a deny-all strategy and explicitly allow permitted services.

When a client roams between APs, the client's applications normally do not issue new DNS requests in response. This usually occurs only after the TTL (time-to-live) expires. The firewall of the AP to which the client has roamed therefore cannot analyze DNS requests or learn the resolved IP addresses and, as a result, cannot actually block the client's traffic. To enable this nevertheless, the firewall's DNS cache is transferred and kept synchronized via IAPP between APs configured with the same SSID or SSIDs. This causes all associated APs in the network to generate the same effective firewall rule set and filter traffic based on the IP addresses that any AP in the network has identified from the client's DNS requests. The current DNS cache can be viewed on the AP using the CLI command `ls /Status/DNS/Snooping-Results`.

Note that only the (volatile) DNS cache is synchronized. The AP configuration, consisting of host groups and filter rules, is not synchronized and must be kept identical separately for all APs.

SNMP ID:

2.47

Console path:

Setup

5.3.1.1 Rules

Configure the firewall rules here.

SNMP ID:

2.47.1

Console path:

Setup > **Firewall**

5.3.1.1.1 Enabled

Specifies whether the rule is active for the firewall.

SNMP ID:

2.47.1.1

Console path:

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

Possible values:

No

Rule is inactive.

Yes

Rule is active.

5.3.1.1.2 Priority

Priority of the rule. Rules with lower values are processed before rules with higher values.

SNMP ID:

2.47.1.2

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

5.3.1.1.3 Network

The WLAN network for which the rule is active.

SNMP ID:

2.47.1.3

Console path:

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

Possible values:

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

5.3.1.1.4 Host-Group

One or more previously configured host groups against which the destination of the rule is checked.

SNMP ID:

2.47.1.4

Console path:

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

Possible values:

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

5.3.1.1.5 Protocol

Configures whether the rule applies only to TCP, UDP, or all traffic.

SNMP ID:

2.47.1.5

Console path:

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

Possible values:

Any
TCP
UDP

5.3.1.1.6 Port

If TCP or UDP is entered as the protocol, you can additionally specify a port number here as a filter criterion.

SNMP ID:

2.47.1.6

Console path:

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

Possible values:

0 … 65535

5.3.1.1.7 Action

Configures whether the connection is allowed or discarded when the rule applies.

SNMP ID:

2.47.1.7

Console path:

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

Possible values:

Accept
Drop

5.3.1.1.8 Comment

A free-text field for entering any comment.

SNMP ID:

2.47.1.99

Console path:

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

Possible values:

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

5.3.1.2 Host-Groups

Configure hostnames or IP addresses here for use in the firewall rules later.

SNMP ID:

2.47.2

Console path:

Setup > **Firewall**

5.3.1.2.1 Name

Name of the group.

SNMP ID:

2.47.2.1

Console path:

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

Possible values:

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

5.3.1.2.2 Hostnames

One or more comma-separated IP addresses or hostnames. You can use the wildcard character * in this field to represent any characters.

The syntax of the wildcard expressions is compatible with that of the app definitions for LCOS.

SNMP ID:

2.47.2.2

Console path:

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

Possible values:

Max. 255 characters from `comma separated list of IP addresses, networks or hostnames (with wildcards)`

5.3.1.3 Log-Actions

When a firewall rule is processed, an entry is created in Syslog.

Depending on the amount of traffic, this may require significant CPU resources and generate a large number of Syslog messages.

SNMP ID:

2.47.3

Console path:

Setup > **Firewall**

Possible values:

No

Do not write an entry.

Yes

Write an entry.

6 End-to-End Test

The WLAN end-to-end test can be used to check the availability and performance of a WLAN from the perspective of an end device—without requiring an additional test device on site. To do this, an existing R&S®LANCOM access point is temporarily switched to client mode and performs defined tests along the entire connection path from the WLAN to the Internet.

The test detects, among other things, problems with WLAN authentication, IP address assignment via DHCP, name resolution via DNS, logging in to a captive portal, and ping and HTTP connections. Test profiles can be adapted to the respective network environment. Tests that are not required can be removed from the profile, such as the captive portal test if no hotspot is operated.

An administrator can start a test run manually when required or schedule it regularly using the internal cron table. The results are stored in the corresponding log tables and are also forwarded to the device Syslog. From there, they can be forwarded, for example, to external SIEM systems.

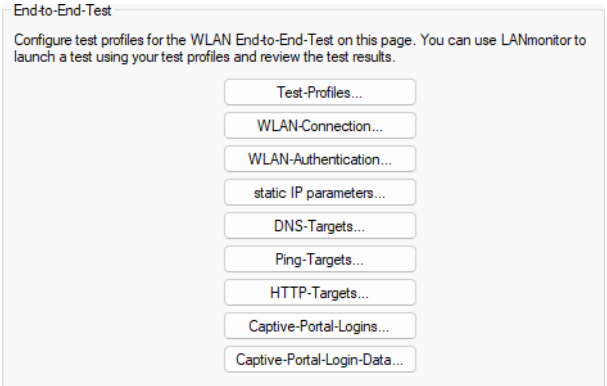
During test execution, the access point operates in client mode. As a result, it is temporarily unavailable for normal WLAN operation, and connected clients are disconnected. After the test run is complete, the access point automatically switches back to normal operating mode and resumes serving the WLAN clients.

The tests are executed in a defined order:

1. WLAN connection
2. Network connection, including DHCPv4, DHCPv6, and SLAAC
3. DNS resolution
4. Captive portal
5. Ping
6. HTTP connection

This order cannot be changed because the individual tests build on one another. For example, a WLAN connection is required for network communication, a valid IP address is required for DNS queries, and an HTTP test may be possible only after successfully logging in to the captive portal.

The settings for the WLAN end-to-end test are available under **Wireless-LAN** > **End-to-End Test**.



Test Results

The results of the individual subtests are stored in separate tables under **Status** > **WLAN** > **End2End-Test**. In addition, there is a separate history table that lists the results of all subtests chronologically in a single table. The history table is therefore comparable to a Syslog, but contains only entries for the WLAN E2E test.

6.1 Test Profiles

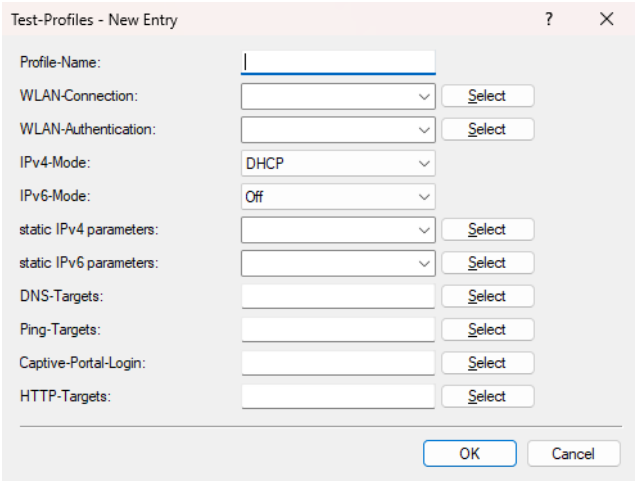
This menu is used to compile test runs. A test run consists of multiple individual tests that are executed together.

At least one test in the **WLAN-Connection** category must be configured for each test profile. Additional individual tests can be added optionally, depending on which tests are to be performed.

If **WLAN-Authentication** is left empty, an open WLAN connection without encryption is used. In this case, the SSID must provide an open network.

Static IPv4 or IPv6 parameters can be left empty if no static parameters were selected in the respective **IPvX-Mode**.

Multiple individual tests of the same category can be executed per test profile. To do this, specify the corresponding tests separated by commas.



Profile-Name

The name of this test profile.

WLAN-Connection

Select one of the available WLAN connections.

WLAN-Authentication

Select one of the available WLAN authentication configurations.

IPv4-Mode

Select either DHCP or Static.

IPv6-Mode

Select either Router Advertisement, DHCPv6, Static, or Off.

static IPv4 parameters

If required, select the static IPv4 parameters.

static IPv6 parameters

If required, select the static IPv6 parameters.

DNS-Targets

Select one of the available DNS targets.

Ping-Targets

Select one of the available ping targets.

Captive-Portal-Login

Select one of the available captive portal logins.

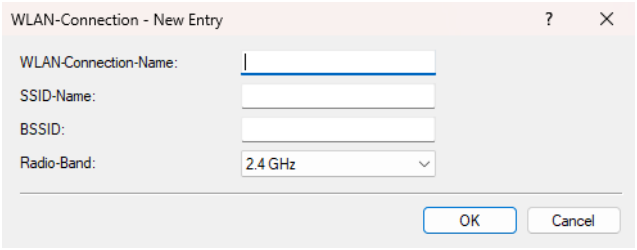
HTTP-Targets

Select one of the available HTTP targets.

6.2 WLAN Connection

Specify the SSID to which the connection is established and on which the tests are performed.

Optionally, you can specify a particular BSSID if the connection should be established to a specific access point. If no BSSID is configured, the test automatically selects an access point with the specified SSID. The access point with the strongest signal is preferred.



WLAN-Connection-Name

Enter a name for this connection.

SSID-Name

The SSID for the tests.

BSSID

Optional BSSID for the tests.

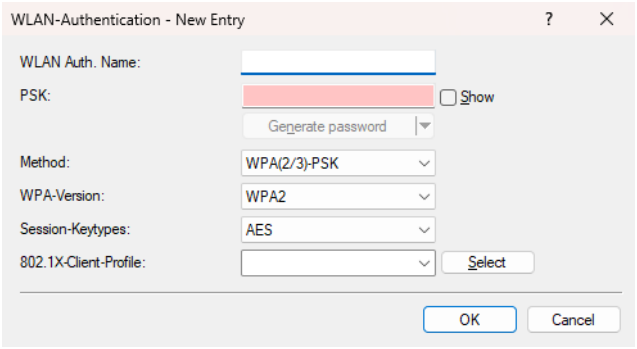
Radio-Band

The radio band for this connection.

6.3 WLAN Authentication

The WLAN E2E test supports both PSK authentication and IEEE 802.1X authentication with the usual client-side options.

To use IEEE 802.1X, you must first configure a suitable supplicant profile.



WLAN-Auth.-Name

Enter a name for this WLAN authentication configuration.

PSK

Enter the PSK.

Method

Select the WLAN authentication method.

WPA-Version

Select the WPA version.

Session-Keytypes

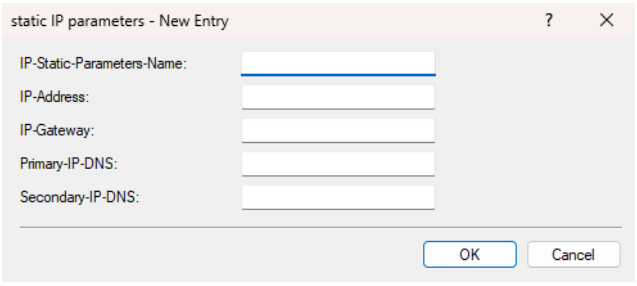
Select the session key type.

802.1X-Client-Profile

Select an IEEE 802.1X client profile.

6.4 Static IP parameters

If a static IP configuration is to be used for the test, enter the corresponding IP parameters in this table.



IP-Static-Parameters-Name

Enter a name for this static IP configuration.

IP-Address

Enter the IP address.

IP-Gateway

Enter the IP gateway.

Primary-IP-DNS

Enter the IP address of the primary DNS server.

Secondary-IP-DNS

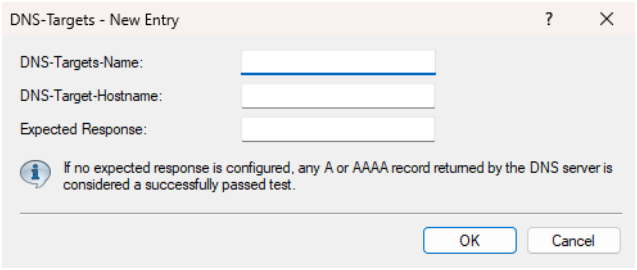
Enter the IP address of the secondary DNS server.

6.5 DNS Targets

Configure the DNS test here. In the **Expected Response** field, you can use the prefix “A:” or “AAAA:” to specify that a particular A or AAAA record is expected.

You can specify multiple records as a comma-separated list. The test is considered successful as soon as one of the configured records matches the received response.

If the **Expected Response** field is left empty, any received A or AAAA record is considered a successful response.



DNS-Targets-Name

Enter a name for this DNS target.

DNS-Targets-Hostname

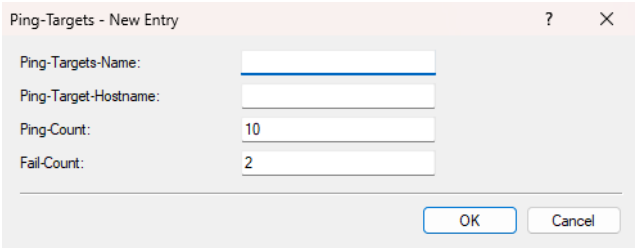
Enter the hostnames to be tested.

Expected Response

Enter the response expected for this test.

6.6 Ping Targets

Configure the ping/ICMP test here. The Ping Count and Failure Count fields are prepopulated with the displayed default values and can be adjusted as needed.



Ping-Targets-Name

Enter a name for this ping target.

Ping-Targets-Hostname

Enter the hostname to be tested.

Ping-Count

Enter the number of pings.

Failure-Count

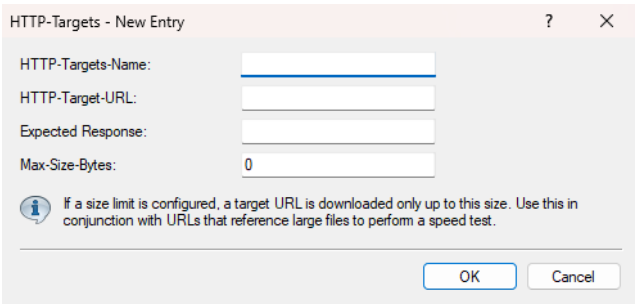
Enter the number of failures.

6.7 HTTP Targets

You can test an HTTP connection in this table. The E2E test accesses the configured **HTTP-Target-URL** and compares the received HTTP status code with the value specified in the **Expected Response** field.

The HTTP test can also be used as a speed test if a sufficiently large file can be downloaded from the HTTP target URL. To enable a meaningful throughput measurement, **Max-Size-Bytes** should also be configured in this case. If no maximum value is specified, the entire file is downloaded.

The measured throughput is always displayed in the test results. However, this value is meaningful only if a sufficiently large file is downloaded and the TCP/HTTP download can reach a realistic transfer speed.



HTTP-Targets-Name

Enter a name for this HTTP target.

HTTP-Target-URL

Enter the URL to be tested.

Expected Response

Enter the expected response.

Max-Size-Bytes

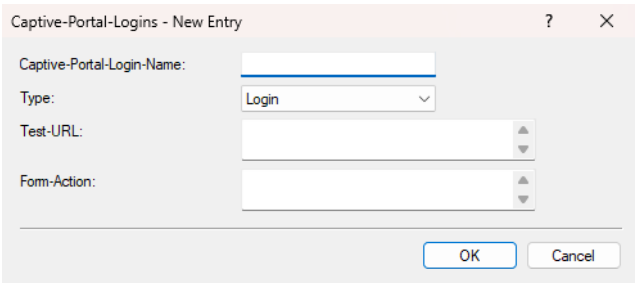
Optional size limit.

6.8 Captive Portal Logins

If the network being tested is protected by a captive portal, you can configure the required login parameters here.

The E2E test first accesses the configured test URL to check whether the captive portal redirects the request. If a redirect is detected, the test creates an HTTP POST request with the entries from the Captive Portal Login Data table and sends it to the URL specified in the Form Action field.

The test URL is then accessed again. If no redirect occurs, the login is considered successful and the test passes.



Captive-Portal-Login-Name

Enter a name for this captive portal login.

Type

You can select either “Login” or “Logout” here.

Depending on the captive portal, it may be useful to log the user out again after the test is completed. This can, for example, conserve resources on the captive portal gateway or allow the same credentials to be used for subsequent test runs.

To do this, create an additional entry with the type “Logout”. Configure the **Form Action** so that it performs the logout action of the captive portal. The logout URL may differ from the URL of the login form. Analyze the HTML code of the respective portal for this purpose.

However, many modern captive portals with click-through login do not provide a logout function. In this case, the user session is terminated only after a timeout. A captive portal test that runs regularly at short intervals may then succeed without actually checking the login, because the MAC address of the testing access point is still cached in the captive portal.

If you manage the captive portal yourself, a special test function may be useful. For example, a hidden form in the HTML code could start a dedicated test session that automatically expires after a short time.

Test-URL

This is the URL that the E2E test accesses to determine whether the captive portal redirects the request. It can point to any URL that reliably responds with an HTTP status code in the “200” range. Ideally, use a URL that responds with “200” or “204”.

This field is empty by default because no URL from an external third party can be specified as a fixed default. Therefore, you must configure a suitable URL.

Form-Action

This is the URL to which the login credentials are transmitted via HTTP POST. For a classic LCOS Public Spot, this could be a URL such as the following:

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

If this field remains empty, the E2E test automatically uses the URL to which the captive portal redirected the request when the Success URL was accessed for the first time. For R&S®LANCOM Management Cloud-based hotspots, this usually enables login without additional configuration of this URL.

6.9 Captive Portal Login Data

This table is used to configure the form elements that are transmitted to the captive portal via HTTP POST for logging in or logging out.

For a classic Public Spot based on LCOS, the form data could look as follows:

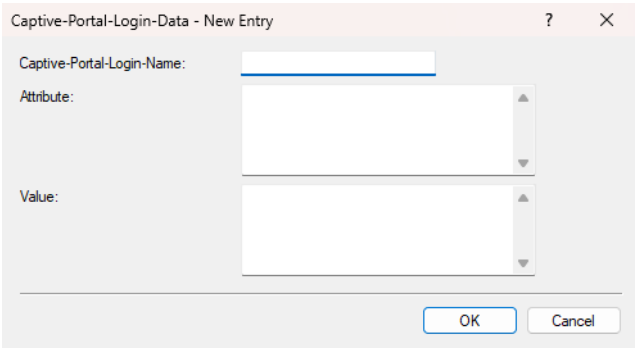
Attribute	Value
AGB	checked
password	secret
userid	rsnc

If the logout function is also used, the corresponding attributes for the logout test must also be stored in this table.

Each captive portal uses its own form structure. Therefore, use the portal's HTML source code to determine the correct form and the required attributes and values.

For very simple portal pages that contain only a single form attribute, such as a button for click-through login, the E2E test attempts to transmit this attribute automatically via POST. In this

case, no additional configuration in this table is required. This currently works, for example, with the One-Button login of the R&S®LANCOM Management Cloud hotspot.



Captive-Portal-Login-Name

Enter a name for this captive portal login.

Attribute

Enter the required attributes here.

Value

Enter the values for the configured attributes here.

6.10 Additions to the Setup menu

6.10.1 End2End-Test

The WLAN end-to-end test can be used to check the availability and performance of a WLAN from the perspective of an end device—without requiring an additional test device on site. To do this, an existing R&S®LANCOM access point is temporarily switched to client mode and performs defined tests along the entire connection path from the WLAN to the Internet.

The test detects, among other things, problems with WLAN authentication, IP address assignment via DHCP, name resolution via DNS, logging in to a captive portal, and ping and HTTP connections. Test profiles can be adapted to the respective network environment. Tests that are not required can be removed from the profile, such as the captive portal test if no hotspot is operated.

An administrator can start a test run manually when required or schedule it regularly using the internal cron table. The results are stored in the corresponding log tables and are also forwarded to the device Syslog. From there, they can be forwarded, for example, to external SIEM systems.

During test execution, the access point operates in client mode. As a result, it is temporarily unavailable for normal WLAN operation, and connected clients are disconnected. After the test run is complete, the access point automatically switches back to normal operating mode and resumes serving the WLAN clients.

The tests are executed in a defined order:

1. WLAN connection
2. Network connection, including DHCPv4, DHCPv6, and SLAAC
3. DNS resolution
4. Captive portal
5. Ping

6. HTTP connection

This order cannot be changed because the individual tests build on one another. For example, a WLAN connection is required for network communication, a valid IP address is required for DNS queries, and an HTTP test may be possible only after successfully logging in to the captive portal.

SNMP ID:

2.20.20

Console path:

Setup > **WLAN**

6.10.1.1 Test-Profiles

This menu is used to compile test runs. A test run consists of multiple individual tests that are executed together.

At least one test in the **WLAN-Connection** category must be configured for each test profile. Additional individual tests can be added optionally, depending on which tests are to be performed.

If **WLAN-Authentication** is left empty, an open WLAN connection without encryption is used. In this case, the SSID must provide an open network.

Static IPv4 or IPv6 parameters can be left empty if no static parameters were selected in the respective **IPvX-Mode**.

Multiple individual tests of the same category can be executed per test profile. To do this, specify the corresponding tests separated by commas.

SNMP ID:

2.20.20.1

Console path:

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

6.10.1.1.1 Profile-Name

The name of this test profile.

SNMP ID:

2.20.20.1.1

Console path:

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

Possible values:

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

6.10.1.1.2 WLAN-Connection

Select one of the available WLAN connections.

SNMP ID:

2.20.20.1.2

Console path:

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

Possible values:

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

6.10.1.1.3 WLAN-Authentication

Select one of the available WLAN authentication configurations.

SNMP ID:

2.20.20.1.3

Console path:

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

Possible values:

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

6.10.1.1.4 IPv4-Mode

Select either DHCP or Static.

SNMP ID:

2.20.20.1.4

Console path:

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

Possible values:

DHCP
Static

6.10.1.1.5 IPv6-Mode

Select either Router Advertisement, DHCPv6, Static, or Off.

SNMP ID:

2.20.20.1.5

Console path:

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

Possible values:

Router-Advertisement
DHCPv6
static
Off

6.10.1.1.6 IPv4-Static-Parameters

If required, select the static IPv4 parameters.

SNMP ID:

2.20.20.1.6

Console path:

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

Possible values:

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

6.10.1.1.7 IPv6-Static-Parameters

If required, select the static IPv6 parameters.

SNMP ID:

2.20.20.1.7

Console path:

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

Possible values:

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

6.10.1.1.8 DNS-Targets

Select one of the available DNS targets.

SNMP ID:

2.20.20.1.8

Console path:

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

Possible values:

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

6.10.1.1.9 Ping-Targets

Select one of the available ping targets.

SNMP ID:

2.20.20.1.9

Console path:

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

Possible values:

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

6.10.1.1.10 Captive-Portal-Login

Select one of the available captive portal logins.

SNMP ID:

2.20.20.1.10

Console path:

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

Possible values:

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

6.10.1.1.11 HTTP-Targets

Select one of the available HTTP targets.

SNMP ID:

2.20.20.1.11

Console path:

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

Possible values:

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

6.10.1.2 WLAN-Connection

Specify the SSID to which the connection is established and on which the tests are performed.

Optionally, you can specify a particular BSSID if the connection should be established to a specific access point. If no BSSID is configured, the test automatically selects an access point with the specified SSID. The access point with the strongest signal is preferred.

SNMP ID:

2.20.20.2

Console path:

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

6.10.1.2.1 WLAN-Connection-Name

Enter a name for this connection.

SNMP ID:

2.20.20.2.1

Console path:

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

Possible values:

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

6.10.1.2.2 SSID-Name

The SSID for the tests.

SNMP ID:

2.20.20.2.2

Console path:

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

Possible values:

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

6.10.1.2.3 BSSID

Optional BSSID for the tests.

SNMP ID:

2.20.20.2.3

Console path:

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

Possible values:

Max. 17 characters from `mac address (xx:xx:xx:xx:xx:xx)`

6.10.1.2.4 Radio-Band

The radio band for this connection.

SNMP ID:

2.20.20.2.4

Console path:

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

Possible values:

2.4GHz
5GHz
6GHz

6.10.1.3 WLAN-Authentication

The WLAN E2E test supports both PSK authentication and IEEE 802.1X authentication with the usual client-side options.

To use IEEE 802.1X, you must first configure a suitable supplicant profile.

SNMP ID:

2.20.20.3

Console path:

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

6.10.1.3.1 WLAN-Authentication-Name

Enter a name for this WLAN authentication configuration.

SNMP ID:

2.20.20.3.1

Console path:

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

Possible values:

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

6.10.1.3.2 Encryption-Key

Enter the PSK.

SNMP ID:

2.20.20.3.2

Console path:

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

Possible values:

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

6.10.1.3.3 Method

Select the WLAN authentication method.

SNMP ID:

2.20.20.3.3

Console path:

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

Possible values:

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

Select the WPA version.

SNMP ID:

2.20.20.3.4

Console path:

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

Possible values:

WPA1
WPA2
WPA1/2
WPA3
WPA2/3

6.10.1.3.5 Session-Keytypes

Select the session key type.

SNMP ID:

2.20.20.3.5

Console path:

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

Possible values:

TKIP
AES
TKIP/AES

6.10.1.3.6 802.1X-Client-Profile

Select an IEEE 802.1X client profile.

SNMP ID:

2.20.20.3.6

Console path:

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

Possible values:

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

6.10.1.4 IP-Static-Parameters

If a static IP configuration is to be used for the test, enter the corresponding IP parameters in this table.

SNMP ID:

2.20.20.4

Console path:

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

6.10.1.4.1 IP-Static-Parameters-Name

Enter a name for this static IP configuration.

SNMP ID:

2.20.20.4.1

Console path:

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

Possible values:

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

6.10.1.4.2 IP-Address

Enter the IP address.

SNMP ID:

2.20.20.4.2

Console path:

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

Possible values:

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

6.10.1.4.3 IP-Gateway

Enter the IP gateway.

SNMP ID:

2.20.20.4.3

Console path:

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

Possible values:

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

6.10.1.4.4 Primary-IP-DNS

Enter the IP address of the primary DNS server.

SNMP ID:

2.20.20.4.4

Console path:

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

Possible values:

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

6.10.1.4.5 Secondary-IP-DNS

Enter the IP address of the secondary DNS server.

SNMP ID:

2.20.20.4.5

Console path:

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

Possible values:

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

6.10.1.5 DNS-Targets

Configure the DNS test here. In the **Expected Response** field, you can use the prefix “A:” or “AAAA:” to specify that a particular A or AAAA record is expected.

You can specify multiple records as a comma-separated list. The test is considered successful as soon as one of the configured records matches the received response.

If the **Expected Response** field is left empty, any received A or AAAA record is considered a successful response.

SNMP ID:

2.20.20.5

Console path:

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

6.10.1.5.1 DNS-Targets-Name

Enter a name for this DNS target.

SNMP ID:

2.20.20.5.1

Console path:

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

Possible values:

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

6.10.1.5.2 DNS-Target-Hostname

Enter the hostnames to be tested.

SNMP ID:

2.20.20.5.2

Console path:

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

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9].-`

6.10.1.5.3 Expected-Response

Enter the response expected for this test.

SNMP ID:

2.20.20.5.3

Console path:

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

Possible values:

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

6.10.1.6 Ping-Targets

Configure the ping/ICMP test here. The Ping Count and Failure Count fields are prepopulated with the displayed default values and can be adjusted as needed.

SNMP ID:

2.20.20.6

Console path:

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

6.10.1.6.1 Ping-Targets-Name

Enter a name for this ping target.

SNMP ID:

2.20.20.6.1

Console path:

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

Possible values:

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

6.10.1.6.2 Ping-Target-Hostname

Enter the hostname to be tested.

SNMP ID:

2.20.20.6.2

Console path:

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

Possible values:

Max. 255 characters from `[A-Z][a-z][0-9].-:%`

6.10.1.6.3 Ping-Count

Enter the number of pings.

SNMP ID:

2.20.20.6.3

Console path:

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

Possible values:

Max. 5 characters from `[0-9]`

Default:

10

6.10.1.6.4 Fail-Count

Enter the number of failures.

SNMP ID:

2.20.20.6.4

Console path:

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

Possible values:

Max. 5 characters from `[0-9]`

Default:

2

6.10.1.7 Captive-Portal-Logins

If the network being tested is protected by a captive portal, you can configure the required login parameters here.

The E2E test first accesses the configured test URL to check whether the captive portal redirects the request. If a redirect is detected, the test creates an HTTP POST request with the entries from the Captive Portal Login Data table and sends it to the URL specified in the Form Action field.

The test URL is then accessed again. If no redirect occurs, the login is considered successful and the test passes.

SNMP ID:

2.20.20.7

Console path:

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

6.10.1.7.1 Captive-Portal-Login-Name

Enter a name for this captive portal login.

SNMP ID:

2.20.20.7.1

Console path:

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

Possible values:

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

6.10.1.7.2 Type

You can select either “Login” or “Logout” here.

Depending on the captive portal, it may be useful to log the user out again after the test is completed. This can, for example, conserve resources on the captive portal gateway or allow the same credentials to be used for subsequent test runs.

To do this, create an additional entry with the type “Logout”. Configure the **Form Action** so that it performs the logout action of the captive portal. The logout URL may differ from the URL of the login form. Analyze the HTML code of the respective portal for this purpose.

However, many modern captive portals with click-through login do not provide a logout function. In this case, the user session is terminated only after a timeout. A captive portal test that runs regularly at short intervals may then succeed without actually checking the login, because the MAC address of the testing access point is still cached in the captive portal.

If you manage the captive portal yourself, a special test function may be useful. For example, a hidden form in the HTML code could start a dedicated test session that automatically expires after a short time.

SNMP ID:

2.20.20.7.2

Console path:

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

Possible values:

Login
Logout

6.10.1.7.3 Test-URL

This is the URL that the E2E test accesses to determine whether the captive portal redirects the request. It can point to any URL that reliably responds with an HTTP status code in the “200” range. Ideally, use a URL that responds with “200” or “204”.

This field is empty by default because no URL from an external third party can be specified as a fixed default. Therefore, you must configure a suitable URL.

SNMP ID:

2.20.20.7.3

Console path:

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

Possible values:

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

6.10.1.7.4 Form-Action

This is the URL to which the login credentials are transmitted via HTTP POST. For a classic LCOS Public Spot, this could be a URL such as the following:

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

If this field remains empty, the E2E test automatically uses the URL to which the captive portal redirected the request when the Success URL was accessed for the first time. For R&S®LANCOM Management Cloud-based hotspots, this usually enables login without additional configuration of this URL.

SNMP ID:

2.20.20.7.4

Console path:

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

Possible values:

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

6.10.1.8 HTTP-Targets

You can test an HTTP connection in this table. The E2E test accesses the configured **HTTP-Target-URL** and compares the received HTTP status code with the value specified in the **Expected Response** field.

The HTTP test can also be used as a speed test if a sufficiently large file can be downloaded from the HTTP target URL. To enable a meaningful throughput measurement, **Max-Size-Bytes** should also be configured in this case. If no maximum value is specified, the entire file is downloaded.

The measured throughput is always displayed in the test results. However, this value is meaningful only if a sufficiently large file is downloaded and the TCP/HTTP download can reach a realistic transfer speed.

SNMP ID:

2.20.20.8

Console path:

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

6.10.1.8.1 HTTP-Targets-Name

Enter a name for this HTTP target.

SNMP ID:

2.20.20.8.1

Console path:

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

Possible values:

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

6.10.1.8.2 HTTP-Target-URL

Enter the URL to be tested.

SNMP ID:

2.20.20.8.2

Console path:

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

Possible values:

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

6.10.1.8.3 Expected-Response

Enter the expected response.

SNMP ID:

2.20.20.8.3

Console path:

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

Possible values:

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

6.10.1.8.4 Max-Size-Bytes

Optional size limit.

SNMP ID:

2.20.20.8.4

Console path:

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

Possible values:

Max. 20 characters from `[0-9]`

6.10.1.9 Captive-Portal-Login-Data

This table is used to configure the form elements that are transmitted to the captive portal via HTTP POST for logging in or logging out.

For a classic Public Spot based on LCOS, the form data could look as follows:

Attribute	Value
AGB	checked
password	secret
userid	rsnc

If the logout function is also used, the corresponding attributes for the logout test must also be stored in this table.

For very simple portal pages that contain only a single form attribute, such as a button for click-through login, the E2E test attempts to transmit this attribute automatically via POST. In this case, no additional configuration in this table is required. This currently works, for example, with the One-Button login of the R&S®LANCOM Management Cloud hotspot.

SNMP ID:

2.20.20.9

Console path:

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

6.10.1.9.1 Captive-Portal-Login-Name

Enter a name for this captive portal login.

SNMP ID:

2.20.20.9.1

Console path:

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

Possible values:

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

6.10.1.9.2 Attribute

Enter the required attributes here.

SNMP ID:

2.20.20.9.2

Console path:

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

Possible values:

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

6.10.1.9.3 Value

Enter the values for the configured attributes here.

SNMP ID:

2.20.20.9.3

Console path:

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

Possible values:

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

6.10.1.10 Run-Tests

Use this action to start the tests.

Example: `do Run-Tests`

SNMP ID:

2.20.20.20

Console path:

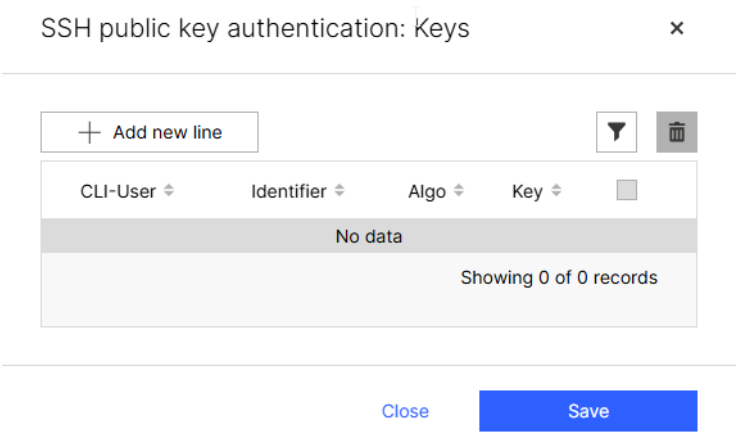
Setup > **WLAN** > **End2End-Test**

7 SSH Public Key Authentication

In WEBconfig, configure the settings for SSH public key authentication under **System configuration** > **Configure SSH public key authentication**.

Keys

In addition to interactive authentication using a user name and password, public key authentication can also be used.



CLI-User

The user for whom the public key entered below is to be valid. This can be either the “root” user or an optionally configured additional administrator (see *Additional Administrators* on page 5).

Identifier

The identifier is used to allow multiple public keys for the same CLI user, for example, if a separate public key was generated for each SSH client, but the login to LCOS LX should be performed using the same user account. In this case, enter the same CLI user but a different identifier.

Algo

The algorithm used to generate the public key.

Key

The public key to be used.

7.1 Additions to the Setup menu

7.1.1 Keys

In addition to interactive authentication using a user name and password, public key authentication can also be used. You can configure it here.

SNMP ID:

2.11.52.5

Console path:

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

7.1.1.1 CLI-User

The user for whom the public key entered below is to be valid. This can be either the “root” user or an optionally configured additional administrator (see *Additional Administrators* on page 5).

SNMP ID:

2.11.52.5.1

Console path:

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

Possible values:

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

7.1.1.2 Identifier

The identifier is used to allow multiple public keys for the same CLI user, for example, if a separate public key was generated for each SSH client, but the login to LCOS LX should be performed using the same user account. In this case, enter the same CLI user but a different identifier.

SNMP ID:

2.11.52.5.2

Console path:

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

Possible values:

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

7.1.1.3 Algo

The algorithm used to generate the public key.

SNMP ID:

2.11.52.5.3

Console path:

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

Possible values:

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

The public key to be used.

SNMP ID:

2.11.52.5.4

Console path:

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

Possible values:

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

8 Additions to the Status menu

8.1 Syslog

This menu provides status information about Syslog.

SNMP ID:

1.62

Console path:

Status

8.1.1 Last-Messages

This table displays the Syslog messages. Example:

```
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

Console path:

Status > **Syslog**

8.1.1.1 Id

ID of a Syslog message.

SNMP ID:

1.62.1.1

Console path:

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

Possible values:

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

8.1.1.2 Time

Timestamp of a Syslog message.

SNMP ID:

1.62.1.2

Console path:

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

Possible values:

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

8.1.1.3 Priority

Severity level of a Syslog message.

SNMP ID:

1.62.1.3

Console path:

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

Possible values:

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

8.1.1.4 Message

Message text of a Syslog message.

SNMP ID:

1.62.1.4

Console path:

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

Possible values:

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

8.1.1.5 LMC-Message-ID

LMC message ID of a Syslog message.

SNMP ID:

1.62.1.5

Console path:

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

Possible values:

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