SECURE. **NETWORKS.**

LCOS LX 5.20

Addendum

05/2020

LANCOM
Systems

Contents

Copyright

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems 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 LANCOM Systems. 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.

LANCOM, LANCOM Systems, LANcommunity and Hyper Integration are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and/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@lancom.de*.

Products from LANCOM Systems include software developed by the “OpenSSL Project” for use in the “OpenSSL Toolkit” (*www.openssl.org*).

Products from include cryptographic software written by Eric Young (*eay@cryptsoft.com*).

Products from LANCOM Systems include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from LANCOM Systems contain the LZMA SDK developed by Igor Pavlov.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen, Germany

Germany

www.lancom-systems.com

1 Addendum to LCOS LX version 5.20

This document describes the changes and enhancements in LCOS LX version 5.20 since the previous version.

2 WLAN controller support

As of LCOS LX 5.20, LCOS LX-based access points can be managed by a LANCOM WLAN controller (WLC). Like LCOS-based access points, they use the CAPWAP protocol.

The prerequisite for this is a LANCOM WLAN controller with LCOS version 10.40 or higher.

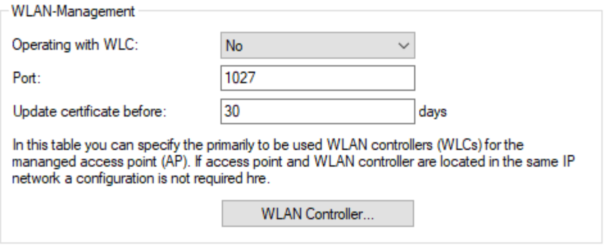
For background information on WLAN management with LANCOM WLAN controllers, see the section “WLAN management” in the LCOS reference manual.

In their factory default settings, LCOS LX-based access points search the local network for a WLAN controller. They also query the DNS name “WLC-Address” to try to reach a WLAN controller.

An access point will not try to contact the LANCOM Management Cloud if it is already being managed by a WLC.

If the access point is managed by the LANCOM Management Cloud and a WLAN configuration is rolled out to the access point by the LMC in this context, the access point will no longer attempt to contact a WLC.

This make it possible to use zero-touch commissioning, which means that no further configuration of the access point is necessary. A manual configuration may still be necessary in certain circumstances. This can be done using LANconfig in the device configuration under **Wireless LAN** > **WLC**.



WLAN-Management

Operating with WLC: No

Port: 1027

Update certificate before: 30 days

In this table you can specify the primarily to be used WLAN controllers (WLCs) for the mananged access point (AP). If access point and WLAN controller are located in the same IP network a configuration is not required hre.

Operating with WLC

This configures whether an access point actively searches for a WLC and can be managed by one.

This option should be deactivated for operation in stand-alone mode.

Port

Configures the port used to attempt to reach a WLC. The default value of 1027 is the default port used by the CAPWAP protocol. By default, LANCOM WLCs also use this port.

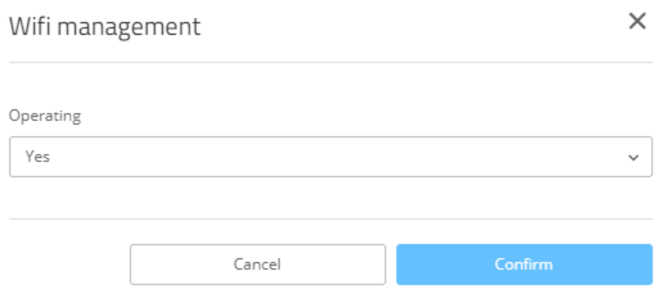
Update certificate before

Configures how many days before its expiry that the device certificate used by the access point to authenticate at the WLC is renewed.

WLAN Controller

Configures user-specified WLAN controllers. This may be necessary if a WLC cannot be found via the local network (e.g. with routed connections) and also the DNS name “WLC-Address” cannot be used to inform the access point about the address of the WLC.

In WEBconfig, this is done using settings in the area **System configuration** under **Wifi management**:



Wifi management

Operating

Yes

Operation

This configures whether an access point actively searches for a WLC and can be managed by one.

This option should be deactivated for operation in stand-alone mode.

2.1 Supported features

LCOS LX supports the following features for WLC operations:

Area	Feature	Supported?
In general	Password synchronization	Yes
	WLC tunnel	No
	WLAN scheduling	Yes
Logical WLAN configuration	VLAN tagging	Yes
	WPA2	Yes
	WPA3	Yes
	Enhanced Open	Yes
	Enhanced Open Transitional	No
	802.1X	Yes
	RADIUS profile	Yes
	Standalone mode	Yes
	802.11u/Hotspot 2.0	No
	OKC	No
	MAC check	Yes
	RADIUS accounting	Yes
	Inter-station traffic	Yes
	Fast roaming	Yes
	Base rate adjustable	No
	Client bridge support	No

Area	Feature	Supported?
	Bandwidth limitation per SSID	Yes
	Bandwidth limitation per client	No
	Maximum count of clients	Yes
	Min. client signal strength	Yes
	Client disassociation signal strength	No
	LBS	No
	Convert to unicast	No
	Transmit only unicasts	No
	U-APSD	Activated permanently
	Encrypt mgmt frames	Yes
Physical WLAN parameters	Country setting	Yes
	Configure 2.4-GHz mode	Yes
	Configure 5-GHz mode	Yes
	Configure 5-GHz sub-bands	Yes
	Set DTIM period	No
	Set the background scan interval	No
	Set antenna gain	Yes
	Set TX power reduction	No
	Activate the VLAN module [1]	–
	ARC: Client steering	Yes [2]
	ARC: Adaptive RF Optimization	No
	Enable QoS according to 802.11e (WME)	Activated permanently
	Indoor-only mode activated	Yes
	Report seen unknown clients	No
General/profile	Specify alternative WLCs	No
	Configuration delay	No
	LED profiles	Yes
	Wireless ePaper	No
	Wireless IDS	No
	AutoWDS	No
	IP parameter profiles	Yes
	Firmware management	Yes

[1] Unnecessary with LCOS LX.

[2] Currently, only AP-based band steering is supported. The settings **Preferred frequency band** and **Probe request age-out time** have no influence.

Area	Feature	Supported?
	Script management	No
	LEPS-U	Yes
	LEPS-MAC	Yes
	Assignment of a VLAN ID via LEPS-MAC (Dynamic VLAN)	Yes
	ARC: RF optimization	No

2.2 Additions to the Setup menu

2.2.1 WLAN-Management

LCOS LX-based access points can be managed by a LANCOM WLAN controller (WLC). Like LCOS-based access points, they use the CAPWAP protocol.

! The prerequisite for this is a LANCOM WLAN controller with LCOS version 10.40 or higher.

In their factory default settings, LCOS LX-based access points search the local network for a WLAN controller. They also query the DNS name “WLC-Address” to try to reach a WLAN controller.

i If an access point is already being managed by a WLC, it will no longer try to contact the LANCOM Management Cloud.

This make it possible to use zero-touch commissioning, which means that no further configuration of the access point is necessary. In certain cases it may still be necessary to carry out a manual configuration. This can be done in the device configuration here.

SNMP ID:

2.59

Console path:

Setup

Static-WLC-Configuration

Configures user-specified WLAN controllers. This may be necessary if a WLC cannot be found via the local network (e.g. with routed connections) and also the DNS name “WLC-Address” cannot be used to inform the access point about the address of the WLC.

SNMP ID:

2.59.1

Console path:

Setup > **WLAN-Management**

IP-Address

Set the IP address or DNS name of a WLAN controller.

SNMP ID:

2.59.1.1

Console path:

Setup > **WLAN-Management** > **Static-WLC-Configuration**

Possible values:

Max. 44 characters from `` [A-Za-z0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.` ``

Port

Configures the port used to attempt to reach a WLC.

SNMP ID:

2.59.1.2

Console path:

Setup > **WLAN-Management** > **Static-WLC-Configuration**

Possible values:

0 … 65535

Default:

1027

Operating

This configures whether an access point actively searches for a WLC and can be managed by one.

ⓘ This option should be deactivated for operation in stand-alone mode.

SNMP ID:

2.59.2

Console path:

Setup > **WLAN-Management**

Possible values:

No

The search for a WLC is disabled.

Yes

A WLC is actively searched for.

Default:

Yes

Update-Cert-Before

Configures how many days before its expiry that the device certificate used by the access point to authenticate at the WLC is renewed.

SNMP ID:

2.59.3

Console path:

Setup > **WLAN-Management**

Possible values:

Max. 4 characters from `[0-9]`

Default:

30

Capwap-Port

Configures the port used to attempt to reach a WLC. The default value of 1027 is the default port used by the CAPWAP protocol. LANCOM By default, WLCs also use this port.

SNMP ID:

2.59.4

Console path:

Setup > **WLAN-Management**

Possible values:

0 … 65535

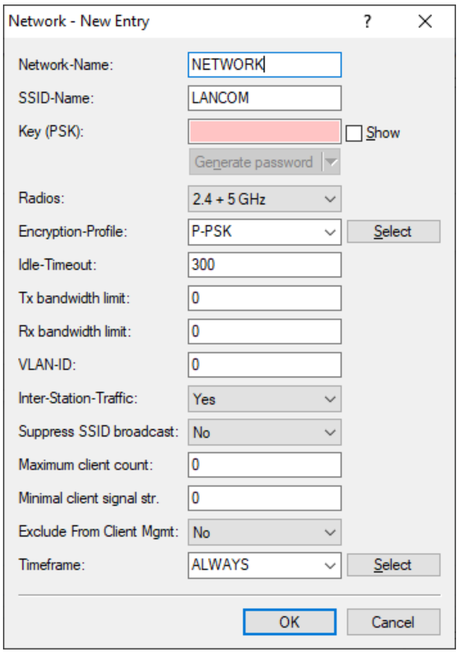
Default:

1027

3 WLAN scheduling

From LCOS LX 5.20, LCOS LX-based access points allow individual SSIDs to be switched on and off according to a schedule. To do this, you define a schedule in the Timeframe section. See also *Timeframes* on page 11.

Under **Wireless-LAN** > **WLAN-Networks** > **Network** you then assign this schedule to an SSID.



Network-Name: NETWORK
SSID-Name: LANCOM
Key (PSK): □ Show
Radios: 2.4 + 5 GHz
Encryption-Profile: P-PSK
Idle-Timeout: 300
Tx bandwidth limit: 0
Rx bandwidth limit: 0
VLAN-ID: 0
Inter-Station-Traffic: Yes
Suppress SSID broadcast: No
Maximum client count: 0
Minimal client signal str.: 0
Exclude From Client Mgmt: No
Timeframe: ALWAYS

Timeframe

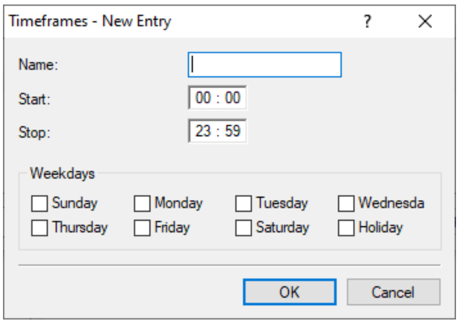
Enter the name of a *Timeframe* here. This is used to schedule when this SSID is switched on or off.

3.1 Timeframes

Timeframes are used to switch individual SSIDs on and off according to a schedule. One profile may contain several rows with different timeframes. Add the time frame to the logical WLAN settings for it to be used with the corresponding SSID.

As an example, a number of timeframes have already been set up here to illustrate a configuration for a school day. There are two timeframes with the same name “Lessons” – but with different start and stop times in order to allow a 45-minute break between these two timeframes. This is defined in the time frame “Break”. Timeframes can be restricted to certain days of the week. Holidays are also taken into account as long as they are entered in the *Holidays table*. Summertime/wintertime is also observed based on the time zone setting.

Predefined timeframes are ALWAYS and NEVER. You can configure additional timeframes in LANconfig under **Date/Time** > **Configuration** > **Timeframes**. This section also allows you to specify public holidays for the timeframes.



Timeframes - New Entry

Name:

Start: 00 : 00

Stop: 23 : 59

Weekdays

□ Sunday □ Monday □ Tuesday □ Wednesda

□ Thursday □ Friday □ Saturday □ Holiday

Name

Enter the name of the time frame so that it can be referenced from the WLAN SSID. Several entries with the same name result in a common profile.

Start

The start time (time of day) can be specified in the format HH:MM (default: 00:00), from which the selected profile becomes valid.

Stop

The stop time (time of day) can be specified in the format HH:MM (default: 00:00), from which the selected profile ceases to be valid.

> ⓘ A stop time of HH:MM usually runs until HH:MM:00. The stop time 00:00 is an exception, since this is interpreted as 23:59:59.

Weekdays

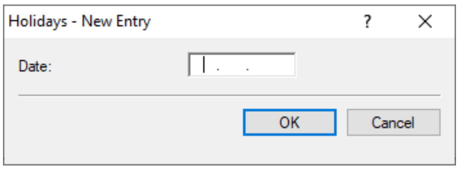
Here you select the weekday on which the timeframe is to be valid.

Possible values:

- Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Holiday

You can form a time schedule with the same name but with different times extending over several rows.

Holidays



Holidays - New Entry

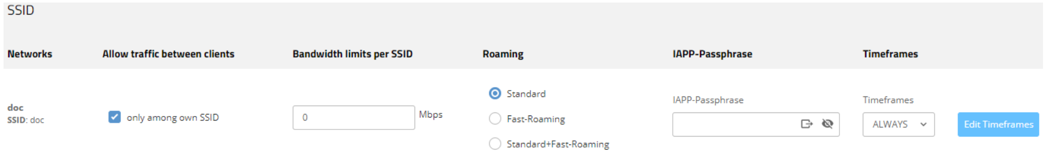
Date: . .

Enter the public holidays to be observed in the time frame.

> ⓘ The year 0 stands for any year.

3.2 WEBconfig

In WEBconfig, this is done using settings in the area **SSID** for the particular SSID under **Wi-Fi configuration**:



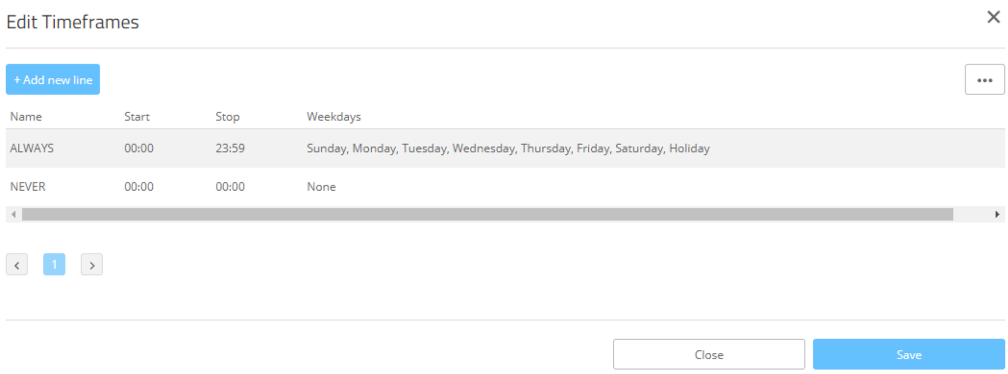
SSID

Networks	Allow traffic between clients	Bandwidth limits per SSID	Roaming	IAPP-Passphrase	Timeframes
doc SSID: doc	☑ only among own SSID	0 Mbps	● Standard ○ Fast-Roaming ○ Standard+Fast-Roaming	IAPP-Passphrase	Timeframes ALWAYS Edit Timeframes

Timeframe

Time frames are used to switch individual SSIDs on and off according to a schedule. One profile may contain several rows with different time frames. Add the time frame here so that it is observed for this SSID.

Edit Timeframes



Edit Timeframes

Name	Start	Stop	Weekdays
ALWAYS	00:00	23:59	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Holiday
NEVER	00:00	00:00	None

Name

Enter the name of the time frame so that it can be referenced from the WLAN SSID. Several entries with the same name result in a common profile. Predefined time frames are ALWAYS and NEVER.

Home

The start time (time of day) can be specified in the format HH:MM (default: 00:00), from which the selected profile becomes valid.

Stop

The stop time (time of day) can be specified in the format HH:MM (default: 00:00), from which the selected profile ceases to be valid.

ⓘ A stop time of HH:MM usually runs until HH:MM:00. The stop time 00:00 is an exception, since this is interpreted as 23:59:59.

Weekdays

Here you select the weekday on which the timeframe is to be valid.

Possible values:

- Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday, Holiday

You can form a time schedule with the same name but with different times extending over several rows.

3.3 Additions to the Setup menu

3.3.1 Holidays

In this table, configure the public holidays for use in timeframes, for example.

SNMP ID:

2.14.15

Console path:

Setup > **Time**

Date

In this table, configure the public holidays for use in timeframes, for example.

SNMP ID:

2.14.15.1

Console path:

Setup > **Time** > **Holidays**

Possible values:

Max. 10 characters from `mm/dd/yyyy`

Special values:

yyyy = 0

Represents any year.

3.3.2 Timeframes

Timeframes are used to switch individual SSIDs on and off according to a schedule. One profile may contain several rows with different timeframes. Add the time frame to the logical WLAN settings for it to be used with the corresponding SSID.

SNMP ID:

2.14.16

Console path:

Setup > **Time**

Name

Enter the name of the time frame for referencing from the logical WLAN settings.

SNMP ID:

2.14.16.1

Console path:

Setup > **Time** > **Timeframe**

Possible values:

Max. 31 characters from `` [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ` ``

Default:

empty

Home

Here you set the start time (time of day) in the format HH:MM when the selected profile becomes valid.

SNMP ID:

2.14.16.2

Console path:

Setup > **Time** > **Timeframes**

Possible values:

Max. 5 characters from `hh:mm`

Default:

00:00

Stop

Here you set the end time (time of day) in the format HH:MM when the selected profile ceases to be valid.

ⓘ A stop time of HH:MM usually runs until HH:MM:00. The stop time 00:00 is an exception, since this is interpreted as 23:59:59.

SNMP ID:

2.14.16.3

Console path:

Setup > **Time** > **Timeframes**

Possible values:

Max. 5 characters from `hh:mm`

Default:

00:00

Weekdays

Here you select the weekday on which the timeframe is to be valid.

SNMP ID:

2.14.16.4

Console path:

Setup > **Time** > **Timeframes**

Possible values:

None
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Holiday

All days specified in the table *2.14.15 Holidays* on page 14.

3.3.3 Timeframe

Enter the name of a *Timeframe* here. This is used to schedule when this SSID is switched on or off.

SNMP ID:

2.20.1.18

Console path:

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

Possible values:

Max. 31 characters from `` [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ` ``

Default:

empty

4 LANCOM Enhanced Passphrase Security (LEPS)

As of LCOS LX 5.20, MAC addresses can be assigned **individual** passphrases consisting of any sequence of 8 to 63 ASCII characters. Authentication at the access point is only possible with the correct combination of passphrase and MAC address.

This combination makes the spoofing of the MAC addresses futile—and LEPS thus shuts out a potential attack on the ACL. If WPA2 is used for encryption, the MAC address can indeed be intercepted—but this method never transmits the passphrase over wireless. This greatly increases the difficulty of attacking the WLAN, because knowledge of both the MAC address and the passphrase is required before encryption can be negotiated.

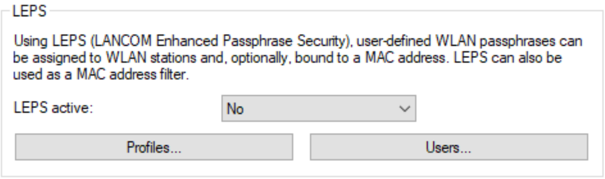
Compared to LEPS for users, the administrative overhead is slightly higher because the MAC address has to be entered for each device.

For technical reasons, LEPS is only compatible with WPA version WPA2.

Note that with WPA2/3 encryption mode, the client can use both WPA versions, which can lead to unexpected behavior when used with LEPS.

4.1 Stations/LEPS

The configuration of the **Profiles** and **Users** for LANCOM Enhanced Passphrase Security (LEPS) are located in LANconfig under **Wireless LAN** > **Stations/LEPS** > **LEPS**. The switch **LEPS active** enables the LEPS feature.



LEPS

Using LEPS (LANCOM Enhanced Passphrase Security), user-defined WLAN passphrases can be assigned to WLAN stations and, optionally, bound to a MAC address. LEPS can also be used as a MAC address filter.

LEPS active: No

When configured in LEPS, each user who should be able to authenticate client devices on the WLAN receives an individual passphrase. LEPS profiles are used to avoid having to repeat all of the settings for every new user. You then create the LEPS users with their individual passphrases and link them to one of the LEPS profiles created previously.

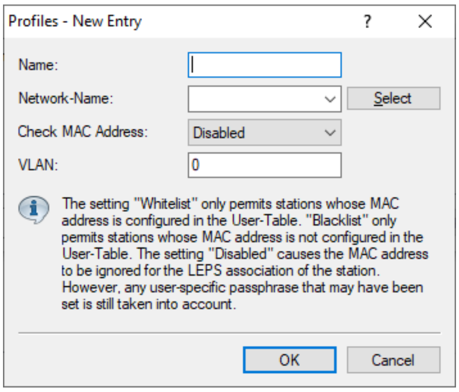
Alternatively, you can link the passphrase to a MAC address to set up a MAC address filter.

For technical reasons, LEPS is only compatible with WPA version WPA2.

Note that with WPA2/3 encryption mode, the client can use both WPA versions, which can lead to unexpected behavior when used with LEPS.

4.1.1 Profiles

Configure LEPS profiles here and link them to an SSID. You can then assign the LEPS profiles to the LEPS users.



The setting "Whitelist" only permits stations whose MAC address is configured in the User-Table. "Blacklist" only permits stations whose MAC address is not configured in the User-Table. The setting "Disabled" causes the MAC address to be ignored for the LEPS association of the station. However, any user-specific passphrase that may have been set is still taken into account.

Name

Enter a unique name for the LEPS profile here.

Network name

Here you select the SSID or, in the case of a WLC, the logical WLAN network for which the LEPS profile applies. The only users who can authenticate at the SSID or, in the case of a WLC, at the logical WLAN network are those who are connected to it via the LEPS profile.

Check MAC address

Possible values:

Disabled

The MAC address plays no role during LEPS authentication. If any user-specific passphrase has been set, this will be checked.

Whitelist

Only clients whose MAC address is known are admitted.

Blacklist

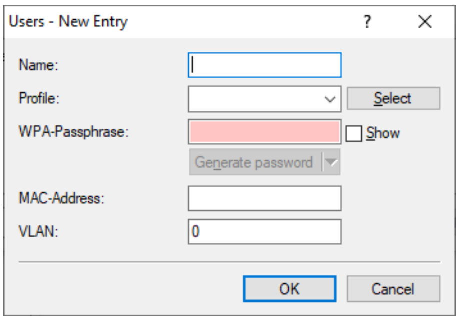
Only clients whose MAC address is not known are admitted.

VLAN

Here you specify which VLAN is assigned to a LEPS user or client who is connected to this profile.

4.1.2 Users

Create individual LEPS users here. Each LEPS user must be linked with a previously created profile and assigned an individual WPA passphrase. Any client can then use this passphrase to authenticate at the SSID specified in the corresponding profile. The passphrase identifies the user, who is assigned to the VLAN specified in this table. If no VLAN is specified here, the user is assigned to the VLAN configured in the profile. Settings for the individual user thus take priority over settings in the profile.



Users - New Entry

Name:

Profile:

WPA-Passphrase: □ Show

MAC-Address:

VLAN: 0

Name

Enter a unique name for the LEPS user here.

Profile

Select the profile for which the LEPS user is valid. The only LEPS users who can authenticate at the SSID are those who are connected to it via the LEPS profile.

WPA-Passphrase

Here you can specify the passphrase to be used by LEPS users to authenticate at the WLAN.

The passphrase can be a string of 8 to 64 characters. We recommend that the passphrases consist of a random string at least 32 characters long.

MAC-Address

Optionally specify a MAC address for a MAC filter. The setting in the profile decides whether this entry is ignored or whether the client devices listed in this table only are able to log on (whitelist). Using a blacklist, the MAC filter works the other way round: the specified MAC addresses cannot log on.

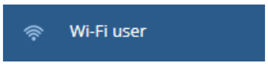
Compared to simply assigning a passphrase to a user, managing a passphrase for each MAC address requires a bit more work, but you have greater control over the devices in the network.

VLAN

Here you specify which VLAN is assigned to the LEPS user. If no VLAN is configured here, the VLAN configured in the LEPS profile (if any) applies. If a VLAN is configured in both the LEPS profile and for the LEPS user, the VLAN configured here takes priority.

4.2 WLAN users

You reach this section in WEBconfig by means of the **Wi-Fi user** item in the sidebar.

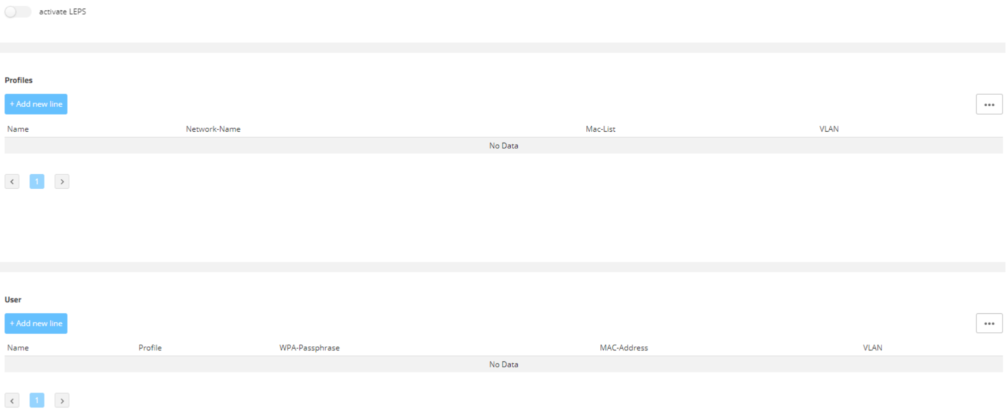


4.2.1 LEPS

When configured in LEPS, each user who should be able to authenticate client devices on the WLAN receives an individual passphrase. LEPS profiles are used to avoid having to repeat all of the settings for every new user. You then create the LEPS users with their individual passphrases and link them to one of the LEPS profiles created previously.

Alternatively, you can link the passphrase to a MAC address to set up a MAC address filter.

Here you configure the **Profiles** and **User** for the LANCOM Enhanced Passphrase Security (LEPS). The switch **Activate LEPS** enables the LEPS feature.



Profiles

Name	Network-Name	Mac-List	VLAN
No Data			

User

Name	Profile	WPA-Passphrase	MAC-Address	VLAN
No Data				

Profiles

Configure LEPS profiles here and link them to an SSID. You can then assign the LEPS profiles to the LEPS users.

Name

Enter a unique name for the LEPS profile here.

Network-Name

Here you select the SSID or, in the case of a WLC, the logical WLAN network for which the LEPS profile applies. The only users who can authenticate at the SSID or, in the case of a WLC, at the logical WLAN network are those who are connected to it via the LEPS profile.

Mac-List

Possible values:

Disabled

The MAC address plays no role during LEPS authentication. If any user-specific passphrase has been set, this will be checked.

Whitelist

Only clients whose MAC address is known are admitted.

Blacklist

Only clients whose MAC address is not known are admitted.

VLAN

Here you specify which VLAN is assigned to a LEPS user or client who is connected to this profile.

Users

Create individual LEPS users here. Each LEPS user must be linked with a previously created profile and assigned an individual WPA passphrase. Any client can then use this passphrase to authenticate at the SSID specified in the corresponding profile. The passphrase identifies the user, who is assigned to the VLAN specified in this table. If no VLAN is specified here, the user is assigned to the VLAN configured in the profile. Settings for the individual user thus take priority over settings in the profile.

Name

Enter a unique name for the LEPS user here.

Profile

Select the profile for which the LEPS user is valid. The only LEPS users who can authenticate at the SSID are those who are connected to it via the LEPS profile.

WPA-Passphrase

Here you can specify the passphrase to be used by LEPS users to authenticate at the WLAN.

> ! The passphrase can be a string of 8 to 64 characters. We recommend that the passphrases consist of a random string at least 32 characters long.

MAC-Address

Optionally specify a MAC address for a MAC filter. The setting in the profile decides whether this entry is ignored or whether the client devices listed in this table only are able to log on (whitelist). Using a blacklist, the MAC filter works the other way round: the specified MAC addresses cannot log on.

Compared to simply assigning a passphrase to a user, managing a passphrase for each MAC address requires a bit more work, but you have greater control over the devices in the network.

VLAN

Here you specify which VLAN is assigned to the LEPS user. If no VLAN is configured here, the VLAN configured in the LEPS profile (if any) applies. If a VLAN is configured in both the LEPS profile and for the LEPS user, the VLAN configured here takes priority.

4.3 Additions to the Setup menu

4.3.1 LEPS

LANCOM Enhanced Passphrase Security (LEPS) lets you assign custom passphrases to WLAN stations without having to pre-register stations by their MAC address. An alternative is to implement a MAC address filter.

SNMP ID:

2.20.133

Console path:

Setup > **WLAN**

Operating

Switches LEPS on or off. When switched off, LEPS users are ignored during WLAN client authentication.

SNMP ID:

2.20.133.1

Console path:

Setup > **WLAN** > **LEPS**

Possible values:

No
Yes

Default:

No

Profiles

Configure LEPS profiles here and link them to an SSID. You can then assign the LEPS profiles to the LEPS users. You can overwrite the profile values for any particular user with individual values.

SNMP ID:

2.20.133.2

Console path:

Setup > **WLAN** > **LEPS**

Name

Enter a unique name for the LEPS profile here.

SNMP ID:

2.20.133.2.1

Console path:

Setup > **WLAN** > **LEPS** > **Profiles**

Possible values:

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

Network-Name

Here you select the SSID or, in the case of a WLC, the logical WLAN network for which the LEPS profile applies. The only users who can authenticate at the SSID or, in the case of a WLC, at the logical WLAN network are those who are connected to it via the LEPS profile.

SNMP ID:

2.20.133.2.2

Console path:

Setup > **WLAN** > **LEPS** > **Profiles**

Possible values:

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

Mac-List

Here you specify if and how MAC addresses are checked.

SNMP ID:

2.20.133.2.3

Console path:

Setup > **WLAN** > **LEPS** > **Profiles**

Possible values:

Disabled

The MAC address plays no role during LEPS authentication. If any user-specific passphrase has been set, this will be checked.

Whitelist

Only clients whose MAC address is known are admitted.

Blacklist

Only clients whose MAC address is not known are admitted.

VLAN

Here you specify which VLAN is assigned to a LEPS user who is connected to this profile.

SNMP ID:

2.20.133.2.5

Console path:

Setup > **WLAN** > **LEPS** > **Profiles**

Possible values:

0 … 4095

Users

Create individual LEPS users here. Every LEPS user must be connected to a profile that was created previously.

SNMP ID:

2.20.133.3

Console path:

Setup > **WLAN** > **LEPS**

Name

Enter a unique name for the LEPS user here.

SNMP ID:

2.20.133.3.1

Console path:

Setup > **WLAN** > **LEPS** > **Users**

Possible values:

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

Profiles

Select the profile for which the LEPS user is valid. The only LEPS users who can authenticate at the SSID are those who are connected to it via the LEPS profile.

SNMP ID:

2.20.133.3.2

Console path:

Setup > **WLAN** > **LEPS** > **Users**

Possible values:

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

WPA-Passphrase

Here you can specify the passphrase to be used by LEPS users to authenticate at the WLAN.

SNMP ID:

2.20.133.3.3

Console path:

Setup > **WLAN** > **LEPS** > **Users**

Possible values:

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

VLAN

Here you specify which VLAN is assigned to the LEPS user. If no VLAN is configured here, the VLAN configured in the LEPS profile (if any) applies. If a VLAN is configured in both the LEPS profile and for the LEPS user, the VLAN-ID configured for the LEPS user takes priority.

SNMP ID:

2.20.133.3.4

Console path:

Setup > **WLAN** > **LEPS** > **Users**

Possible values:

0 … 4095

MAC-Address

Optionally specify a MAC address for a MAC filter. The setting in the profile decides whether this entry is ignored or whether the client devices listed in this table only are able to log on (whitelist). Using a blacklist, the MAC filter works the other way round: the specified MAC addresses cannot log on.

SNMP ID:

2.20.133.3.7

Console path:

Setup > **WLAN** > **LEPS** > **Users**

Possible values:

MAC address in the format `xx:xx:xx:xx:xx:xx`

5 Dynamic VLAN for 802.1X

The RADIUS server uses dynamic VLAN to assign a VLAN ID to the WLAN client for 802.1X authentication. This assigns clients to the required VLAN without the need to operate a separate SSID for each VLAN.

The RADIUS server must send the following attributes in the accept message:

ID	Name	Meaning	Possible values in LCOS LX
64	Tunnel-Type	Defines the tunneling protocol which will be used for the session.	13 (VLAN)
65	Tunnel-Medium-Type	Defines the transport medium over which the tunneled session will be established.	6 (IEEE 802)
81	Tunnel-Private-Group-ID	Specifies a required VLAN ID.	1 – 4096