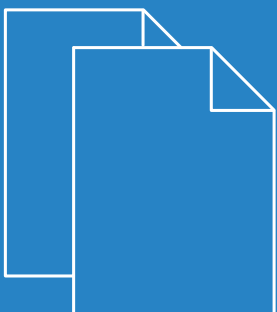


LCOS LX 5.20

Addendum



Inhalt

1 Addendum zur LCOS LX-Version 5.20.....	4
2 WLAN-Controller-Unterstützung.....	5
2.1 Unterstützte Features.....	6
2.2 Ergänzungen im Setup-Menü.....	8
2.2.1 WLAN-Management.....	8
3 WLAN-Zeitsteuerung.....	11
3.1 Zeitrahmen.....	11
3.2 WEBconfig.....	13
3.3 Ergänzungen im Setup-Menü.....	14
3.3.1 Holidays.....	14
3.3.2 Timeframes.....	14
3.3.3 Timeframe.....	16
4 LANCOM Enhanced Passphrase Security (LEPS).....	17
4.1 Stationen / LEPS.....	17
4.1.1 Profile.....	18
4.1.2 Benutzer.....	18
4.2 WLAN-Benutzer.....	19
4.2.1 LEPS.....	19
4.3 Ergänzungen im Setup-Menü.....	21
4.3.1 LEPS.....	21
5 Dynamic VLAN für 802.1X.....	26

Copyright

© 2020 LANCOM Systems GmbH, Würselen (Germany). Alle Rechte vorbehalten.

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

Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhalts sind nur mit schriftlicher Erlaubnis von LANCOM Systems gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

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

LANCOM, LANCOM Systems, LCOS, LANcommunity und Hyper Integration sind eingetragene Marken. Alle anderen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein. Dieses Dokument enthält zukunftsbezogene Aussagen zu Produkten und Produkteigenschaften. LANCOM Systems behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten und / oder Auslassungen.

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

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

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

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

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

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Addendum zur LCOS LX-Version 5.20

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS LX-Version 5.20 gegenüber der vorherigen Version.

2 WLAN-Controller-Unterstützung

Ab LCOS LX 5.20 können LCOS LX-basierte Access Points von einem LANCOM WLAN-Controller (WLC) verwaltet werden. Wie bei LCOS-basierten Access Points kommt hierzu das Protokoll CAPWAP zum Einsatz.

! Voraussetzung ist ein LANCOM WLAN-Controller mit LCOS-Version 10.40 oder höher.

i Für Hintergrundinformationen zum WLAN-Management mit LANCOM WLAN-Controllern, konsultieren Sie den Abschnitt „WLAN-Management“ im LCOS-Referenzhandbuch.

Im Auslieferungszustand suchen LCOS LX-basierte Access Points im lokalen Netzwerk nach einem WLAN-Controller. Ebenso wird unter dem DNS-Namen „WLC-Address“ versucht, einen WLAN-Controller zu erreichen.

i Wurde der Access Point in die Verwaltung durch einen WLC aufgenommen, wird dieser Access Point nicht weiter versuchen, die LANCOM Management Cloud zu kontaktieren.

i Wird der Access Point von der LANCOM Management Cloud verwaltet und in diesem Zusammenhang durch die LMC eine WLAN-Konfiguration auf den Access Point ausgerollt, wird dieser nicht weiter versuchen, einen WLC zu kontaktieren.

Auf diese Weise ist eine Zero-Touch-Inbetriebnahme möglich, bei der keine weitere Konfiguration des Access Points notwendig ist. In besonderen Fällen kann es dennoch erforderlich sein, eine manuelle Konfiguration vorzunehmen. Dies ist in der Gerätekonfiguration mit LANconfig unter **Wireless-LAN > WLC** möglich.

WLAN-Management

Betrieb mit WLC aktiv:

Port:

Gerätezeit. vor Ablauf anfordern: Tage

In dieser Tabelle können Sie die WLAN-Controller (WLC) angeben, mit denen dieser gemanagte Access-Point (AP) vornehmlich Verbindung aufnehmen soll. Befinden sich Access-Point und WLAN-Controller im gleichen IP-Netzwerk ist hier keine Einstellung erforderlich.

Betrieb mit WLC aktiv

Konfiguriert, ob ein Access Point aktiv nach einem WLC sucht und von diesem verwaltet werden kann.

i Für den Stand-Alone-Betrieb empfiehlt es sich, diese Option abzuschalten.

Port

Konfiguriert den Port, unter dem versucht wird, einen WLC zu erreichen. Der Standardwert von 1027 ist der Standardport des CAPWAP-Protokolls. LANCOM WLCs verwenden standardmäßig ebenfalls diesen Port.

Gerätezertifikat vor Ablauf anfordern

Konfiguriert, wie viele Tage vor dem Ablaufdatum das Gerätezertifikat erneuert wird, mit dem sich der Access Point am WLC authentifiziert.

WLAN-Controller

Konfiguriert benutzerdefinierte WLAN-Controller. Dies kann notwendig sein, wenn ein WLC nicht über das lokale Netzwerk (z. B. bei gerouteten Verbindungen) gefunden wird und auch der DNS-Name „WLC-Address“ nicht verwendet werden kann, um dem Access Point die Adresse des WLCs mitzuteilen.

In WEBconfig ist dies über die Einstellungen im Bereich **Systemkonfiguration** unter **WLAN-Management** möglich:

WLAN Management ✕

Betrieb

Nein ▼

Abbrechen
Übernehmen

Betrieb

Konfiguriert, ob ein Access Point aktiv nach einem WLC sucht und von diesem verwaltet werden kann.

Für den Stand-Alone-Betrieb empfiehlt es sich, diese Option abzuschalten.

2.1 Unterstützte Features

In LCOS LX werden folgende Features im Rahmen des WLC-Betriebs unterstützt:

Bereich	Feature	Unterstützt?
Allgemein	Passwortsynchronisation	Ja
	WLC-Tunnel	Nein
	WLAN-Zeitsteuerung	Ja
Logische WLAN-Konfiguration	VLAN-Tagging	Ja
	WPA2	Ja
	WPA3	Ja
	Enhanced Open	Ja
	Enhanced Open Transitional	Nein
	802.1X	Ja
	RADIUS-Profile	Ja
	Autarker Modus	Ja
	802.11u/Hotspot 2.0	Nein
	OKC	Nein
	MAC-Prüfung	Ja
	RADIUS-Accounting	Ja
	Inter-Station-Traffic	Ja
	Fast Roaming	Ja
	Basisrate einstellbar	Nein
Client-Bridge-Unterstützung	Nein	

Bereich	Feature	Unterstützt?
	Bandbreitenbegrenzung per SSID	Ja
	Bandbreitenbegrenzung per Client	Nein
	Maximalzahl der Clients	Ja
	Min. Client-Signalstärke	Ja
	Client-Trennen-Signalstärke	Nein
	LBS	Nein
	In Unicast konvertieren	Nein
	Nur Unicasts übertragen	Nein
	U-APSD	Dauerhaft eingeschaltet
	Mgmt-Frames verschlüsseln	Ja
Physikalische WLAN-Parameter	Landeseinstellung	Ja
	2,4 GHz-Modus konfigurieren	Ja
	5 GHz-Modus konfigurieren	Ja
	5 GHz-Unterbänder konfigurieren	Ja
	DTIM-Periode einstellen	Nein
	Background-Scan-Intervall einstellen	Nein
	Antennen-Gewinn einstellen	Ja
	Sendeleistungs-Reduktion einstellen	Nein
	VLAN-Modul aktivieren ¹	–
	ARC: Client Steering	Ja ²
	ARC: Adaptive RF Optimization	Nein
	QoS nach 802.11e einschalten	Dauerhaft eingeschaltet
	Indoor-Only-Modus aktivieren	Ja
	Unbekannte gesehene Clients melden	Nein
Allgemein/Profil	Angabe alternativer WLCs	Nein
	Konfigurations-Verzögerung	Nein
	LED-Profil	Ja
	Wireless ePaper	Nein
	Wireless IDS	Nein
	AutoWDS	Nein
	IP-Parameter-Profil	Ja
	Firmware-Management	Ja

¹ Bei LCOS LX nicht notwendig.

² Aktuell wird nur AP-basiertes Band Steering unterstützt. Die Einstellungen **bevorzugtes Frequenzband** und **Ablaufzeit Probe Requests** haben keinen Einfluss.

Bereich	Feature	Unterstützt?
	Skript-Management	Nein
	LEPS-U	Ja
	LEPS-MAC	Ja
	Zuweisung einer VLAN ID via LEPS-MAC (Dynamic VLAN)	Ja
	ARC: Funkfeldoptimierung	Nein


2.2 Ergänzungen im Setup-Menü

2.2.1 WLAN-Management

LCOS LX-basierte Access Points können von einem LANCOM WLAN-Controller (WLC) verwaltet werden. Wie bei LCOS-basierten Access Points kommt hierzu das Protokoll CAPWAP zum Einsatz.

 Voraussetzung ist ein LANCOM WLAN-Controller mit LCOS-Version 10.40 oder höher.

Im Auslieferungszustand suchen LCOS LX-basierte Access Points im lokalen Netzwerk nach einem WLAN-Controller. Ebenso wird unter dem DNS-Namen „WLC-Address“ versucht, einen WLAN-Controller zu erreichen.

 Wurde der Access Point in die Verwaltung durch einen WLC aufgenommen, wird dieser Access Point nicht weiter versuchen, die LANCOM Management Cloud zu kontaktieren.

Auf diese Weise ist eine Zero-Touch-Inbetriebnahme möglich, bei der keine weitere Konfiguration des Access Points notwendig ist. In besonderen Fällen kann es dennoch erforderlich sein, eine manuelle Konfiguration vorzunehmen. Dies ist in der Gerätekonfiguration hier möglich.

SNMP-ID:

2.59

Pfad Konsole:

Setup

Static-WLC-Configuration

Konfiguriert benutzerdefinierte WLAN-Controller. Dies kann notwendig sein, wenn ein WLC nicht über das lokale Netzwerk (z. B. bei gerouteten Verbindungen) gefunden wird und auch der DNS-Name „WLC-Address“ nicht verwendet werden kann, um dem Access Point die Adresse des WLCs mitzuteilen.

SNMP-ID:

2.59.1

Pfad Konsole:

Setup > WLAN-Management

IP-Address

Geben Sie die IP-Adresse oder den DNS-Namen eines WLAN-Controllers an.

SNMP-ID:

2.59.1.1

Pfad Konsole:

Setup > WLAN-Management > Static-WLC-Configuration

Mögliche Werte:

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

Port

Konfiguriert den Port, unter dem versucht wird, einen WLC zu erreichen.

SNMP-ID:

2.59.1.2

Pfad Konsole:

Setup > WLAN-Management > Static-WLC-Configuration

Mögliche Werte:

0 ... 65535

Default-Wert:

1027

Operating

Konfiguriert, ob ein Access Point aktiv nach einem WLC sucht und von diesem verwaltet werden kann.

 Für den Stand-Alone-Betrieb empfiehlt es sich, diese Option abzuschalten.

SNMP-ID:

2.59.2

Pfad Konsole:

Setup > WLAN-Management

Mögliche Werte:**No**

Die Suche nach einem WLC ist ausgeschaltet.

Yes

Es wird aktiv nach einem WLC gesucht.

Default-Wert:

Yes

Update-Cert-Before

Konfiguriert, wie viele Tage vor dem Ablaufdatum das Gerätezertifikat erneuert wird, mit dem sich der Access Point am WLC authentifiziert.

SNMP-ID:

2.59.3

Pfad Konsole:**Setup > WLAN-Management****Mögliche Werte:**

max. 4 Zeichen aus [0-9]

Default-Wert:

30

Capwap-Port

Konfiguriert den Port, unter dem versucht wird, einen WLC zu erreichen. Der Standardwert von 1027 ist der Standardport des CAPWAP-Protokolls. LANCOM WLCs verwenden standardmäßig ebenfalls diesen Port.

SNMP-ID:

2.59.4

Pfad Konsole:**Setup > WLAN-Management****Mögliche Werte:**

0 ... 65535

Default-Wert:

1027

3 WLAN-Zeitsteuerung

Ab LCOS LX 5.20 lassen sich einzelne SSIDs bei LCOS LX-basierten Access Points anhand eines Zeitplans ein- und ausschalten. Dazu definieren Sie einen Zeitplan im Bereich Zeiträumen. Siehe hierzu [Zeiträumen](#) auf Seite 11.

Unter **Wireless-LAN > WLAN-Netzwerke > Netzwerke** können Sie dann diesen Zeitplan einer SSID zuweisen.

Zeiträumen

Geben Sie hier den Namen eines [Zeiträumens](#) an, über den diese SSID zeitgesteuert an- bzw. abgeschaltet wird.

3.1 Zeiträumen

Zeiträumen werden verwendet, um einzelne SSIDs anhand eines Zeitplans ein- und auszuschalten. Zu einem Profil kann es auch mehrere Zeilen mit unterschiedlichen Zeiträumen geben. Fügen Sie den Zeiträumen bei den logischen WLAN-Einstellungen hinzu, damit er für die entsprechende SSID beachtet wird.

Beispielhaft sind hier bereits mehrere Zeiträumen angelegt, die eine Konfiguration für einen Unterrichtstag an einer Schule zeigen sollen. Es existieren zwei Zeiträumen mit dem identischen Namen „Unterricht“ – aber mit unterschiedlicher Start- und Stoppzeit, um zwischen diesen beiden Zeiträumen eine 45-minütige Pause realisieren zu können. Diese ist wiederum in dem Zeiträumen „Pause“ definiert. Zeiträumen können auf bestimmte Wochentage eingeschränkt werden. Feiertage, sofern sie in der [Feiertage-Tabelle](#) hinterlegt wurden, werden ebenfalls beachtet. Sommer / Winterzeit wird ebenfalls anhand der eingestellten Zeitzone beachtet.

Voreingestellt sind die Zeiträume ALWAYS und NEVER. Weitere Zeiträume können Sie in LANconfig konfigurieren unter **Datum/Zeit > Konfiguration > Zeiträume**. Im gleichen Bereich finden Sie auch die Möglichkeit, für die Zeiträume Feiertage vorzugeben.

Name


Hier muss der Name des Zeitrahmens angegeben werden, über den dieser bei einer WLAN-SSID referenziert wird. Mehrere Einträge gleichen Namens ergeben dabei ein gemeinsames Profil.

Startzeit

Hier kann die Startzeit (Tageszeit) im Format HH:MM (Default: 00:00) angegeben werden, ab der das gewählte Profil gelten soll.

Stopzeit

Hier kann die Stopzeit (Tageszeit) im Format HH:MM (Default: 00:00) angegeben werden, ab der das gewählte Profil nicht mehr gültig sein soll.

 Eine Stopzeit von HH:MM geht normalerweise bis HH:MM:00. Eine Ausnahme ist die Stopzeit 00:00, die als 23:59:59 interpretiert wird.

Wochentage

Hier können Sie die Wochentage auswählen, an denen der Zeitrahmen gültig sein soll.


Mögliche Werte:

> Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag, Feiertag

Zeitschemata lassen sich mit gleichem Namen, aber unterschiedlichen Zeiten auch über mehrere Zeilen hinweg definieren.

Feiertage

Geben Sie hier die Feiertage an, die in Zeiträumen berücksichtigt werden sollen.

 Das Jahr 0 steht für ein beliebiges Jahr.

3.2 WEBconfig

In WEBconfig ist dies über die Einstellungen im Bereich **SSID** bei der jeweiligen SSID in der **WLAN-Konfiguration** möglich:

SSID

Netzwerke	Kommunikation von Endgeräten untereinander erlauben	Bandbreitenlimits pro SSID	Roaming	IAPP-Passphrase	Zeitraumen
doc SSID: doc	<input checked="" type="checkbox"/> nur innerhalb der eigenen SSID	<input type="text" value="0"/> MBit/s	<input checked="" type="radio"/> Standard <input type="radio"/> Fast-Roaming <input type="radio"/> Standard+Fast-Roaming	<input type="text" value="IAPP-Passphrase"/>	Zeitraumen <input type="text" value="ALWAYS"/>

Zeitraumen

Zeitraumen werden verwendet, um einzelne SSIDs anhand eines Zeitplans ein- und auszuschalten. Zu einem Profil kann es auch mehrere Zeilen mit unterschiedlichen Zeitraumen geben. Fügen Sie den Zeitraumen hier hinzu, damit er für diese SSID beachtet wird.

Zeitraumen bearbeiten

Zeitraumen bearbeiten

+ Neue Zeile hinzufügen

Name	Start	Stop	Wochentage
ALWAYS	00:00	23:59	Sonntag, Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Feiertag
NEVER	00:00	00:00	Keine

Schließen Speichern

Name

Hier muss der Name des Zeitraumens angegeben werden, über den dieser bei einer WLAN-SSID referenziert wird. Mehrere Einträge gleichen Namens ergeben dabei ein gemeinsames Profil. Voreingestellt sind die Zeitraumen ALWAYS und NEVER.

Start

Hier kann die Startzeit (Tageszeit) im Format HH:MM (Default: 00:00) angegeben werden, ab der das gewählte Profil gelten soll.

Stopp

Hier kann die Stoppzeit (Tageszeit) im Format HH:MM (Default: 00:00) angegeben werden, ab der das gewählte Profil nicht mehr gültig sein soll.



Eine Stoppzeit von HH:MM geht normalerweise bis HH:MM:00. Eine Ausnahme ist die Stoppzeit 00:00, die als 23:59:59 interpretiert wird.

Wochentage

Hier können Sie die Wochentage auswählen, an denen der Zeitraumen gültig sein soll.

Mögliche Werte:

- > Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag, Feiertag

Zeitschemata lassen sich mit gleichem Namen, aber unterschiedlichen Zeiten auch über mehrere Zeilen hinweg definieren.

3.3 Ergänzungen im Setup-Menü

3.3.1 Holidays

Konfigurieren Sie in dieser Tabelle die Feiertage, die z. B. in Zeitrahmen verwendet werden können.

SNMP-ID:

2.14.15

Pfad Konsole:

Setup > Time

Date

Konfigurieren Sie in dieser Tabelle die Feiertage, die z. B. in Zeitrahmen verwendet werden können.

SNMP-ID:

2.14.15.1

Pfad Konsole:

Setup > Time > Holidays

Mögliche Werte:

max. 10 Zeichen aus `mm/dd/yyyy`

Besondere Werte:

yyyy = 0

Steht für ein beliebiges Jahr.

3.3.2 Timeframes

Zeitrahmen werden verwendet, um einzelne SSIDs anhand eines Zeitplans ein- und auszuschalten. Zu einem Profil kann es auch mehrere Zeilen mit unterschiedlichen Zeitrahmen geben. Fügen Sie den Zeitrahmen bei den logischen WLAN-Einstellungen hinzu, damit er für die entsprechende SSID beachtet wird.

SNMP-ID:

2.14.16

Pfad Konsole:

Setup > Time

Name

Hier muss der Name des Zeitrahmens angegeben werden, über den er in den logischen WLAN-Einstellungen referenziert wird.

SNMP-ID:

2.14.16.1

Pfad Konsole:

Setup > Zeit > Zeitrahmen

Mögliche Werte:

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

Default-Wert:

leer

Start

Hier kann die Startzeit (Tageszeit) im Format HH:MM angegeben werden, ab der das gewählte Profil gelten soll.

SNMP-ID:

2.14.16.2

Pfad Konsole:

Setup > Time > Timeframes

Mögliche Werte:

max. 5 Zeichen aus hh:mm

Default-Wert:

00:00

Stop

Hier kann die Endzeit (Tageszeit) im Format HH:MM angegeben werden, bis zu der das gewählte Profil gelten soll.



Eine Stoppzeit von HH:MM geht normalerweise bis HH:MM:00. Eine Ausnahme ist die Stoppzeit 00:00, die als 23:59:59 interpretiert wird.

SNMP-ID:

2.14.16.3

Pfad Konsole:

Setup > Time > Timeframes

Mögliche Werte:

max. 5 Zeichen aus hh:mm

Default-Wert:

00:00

Weekdays

Hier können Sie die Wochentage auswählen, an denen der Zeitrahmen gültig sein soll.

SNMP-ID:

2.14.16.4

Pfad Konsole:

Setup > Time > Timeframes

Mögliche Werte:

None
 Sunday
 Monday
 Tuesday
 Wednesday
 Thursday
 Friday
 Saturday
 Holiday

Alle in der Tabelle [2.14.15 Holidays](#) auf Seite 14 definierten Tage.

3.3.3 Timeframe

Geben Sie hier den Namen eines *Zeitrahmens* an, über den diese SSID zeitgesteuert an- bzw. abgeschaltet wird.

SNMP-ID:

2.20.1.18

Pfad Konsole:

Setup > WLAN > Network

Mögliche Werte:

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

Default-Wert:


leer


4 LANCOM Enhanced Passphrase Security (LEPS)

Ab LCOS LX 5.20 lassen sich auch MAC-Adressen **individuelle** Passphrasen zuordnen – eine beliebige Folge aus 8 bis 63 ASCII-Zeichen. Nur die Verbindung von Passphrase und MAC-Adresse erlaubt dann die Anmeldung am Access Point.

Da Passphrase und MAC-Adresse verknüpft sind, ist auch das Spoofing der MAC-Adressen wirkungslos – LEPS schließt damit auch einen möglichen Angriffspunkt gegen die ACL aus. Wenn als Verschlüsselungsart WPA2 verwendet wird, kann zwar die MAC-Adresse abgehört werden – die Passphrase wird bei diesem Verfahren jedoch nie über die WLAN-Strecke übertragen. Angriffe auf das WLAN werden so deutlich erschwert, da durch die Verknüpfung von MAC-Adresse und Passphrase immer beide Teile bekannt sein müssen, um eine Verschlüsselung zu verhandeln.

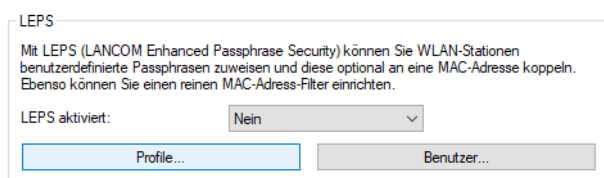
Im Vergleich zu LEPS für Benutzer ist der Verwaltungsaufwand etwas höher, da für jedes Gerät die MAC-Adresse eingetragen werden muss.

 Aus technischen Gründen ist LEPS nur mit der WPA-Version WPA2 kompatibel.

 Beachten Sie, dass bei dem Verschlüsselungsmodus WPA2/3 der Client beide WPA-Versionen verwenden kann, was in Verbindung mit LEPS zu unvorhergesehenem Verhalten führen kann.


4.1 Stationen / LEPS


Die Konfiguration der **Profile** und **Benutzer** für LANCOM Enhanced Passphrase Security (LEPS) finden Sie in LANconfig unter **Wireless-LAN > Stationen / LEPS > LEPS**. Über den Schalter **LEPS aktiviert** wird LEPS eingeschaltet.



Bei der Konfiguration von LEPS wird jedem Benutzer, der sich mit Clients im WLAN anmelden können soll, eine individuelle Passphrase zugeordnet. Dazu werden LEPS-Profilen angelegt, damit einige Einstellungen nicht bei jedem Benutzer erneut vorgenommen werden müssen. Anschließend legen Sie die LEPS-Benutzer mit der zugehörigen individuellen Passphrase an und verknüpfen diesen mit einem der vorher angelegten LEPS-Profilen.

Alternativ können Sie die Passphrase mit einer MAC-Adresse verbinden und auf diese Weise einen MAC-Adress-Filter einrichten.

 Aus technischen Gründen ist LEPS nur mit der WPA-Version WPA2 kompatibel.

 Beachten Sie, dass bei dem Verschlüsselungsmodus WPA2/3 der Client beide WPA-Versionen verwenden kann, was in Verbindung mit LEPS zu unvorhergesehenem Verhalten führen kann.

4.1.1 Profile

Konfigurieren Sie hier LEPS-Profile und verbinden Sie sie mit einer SSID. Anschließend können die LEPS-Profile den LEPS-Benutzern zugeordnet werden.

Profile - Neuer Eintrag

Name:

Netzwerkname: Wählen

MAC-Adresse prüfen: nicht prüfen

VLAN: 0

Die Einstellung "Whitelist" bewirkt, dass nur Stationen zugelassen werden, deren MAC-Adresse erfasst ist. "Blacklist" bewirkt, dass nur Stationen zugelassen werden, deren MAC-Adresse nicht erfasst ist. Die Einstellung "nicht prüfen" bewirkt, dass die MAC-Adresse für die LEPS-Anmeldung nicht beachtet wird. Eine ggf. gesetzte nutzerspezifische Passphrase wird aber weiterhin beachtet.

OK Abbrechen

Name

Vergeben Sie hier einen eindeutigen Namen für das LEPS-Profil.

Netzwerkname

Wählen Sie hier die SSID bzw. beim WLC das logische WLAN-Netzwerk aus, für die das LEPS-Profil gültig sein soll. Es können sich nur LEPS-Benutzer an der SSID bzw. beim WLC an dem logischen WLAN-Netzwerk anmelden, mit der sie über das LEPS-Profil verbunden sind.

MAC-Adresse prüfen

Mögliche Werte:

Nicht prüfen

Die MAC-Adresse wird für die LEPS-Anmeldung nicht beachtet. Eine ggf. gesetzte benutzerspezifische Passphrase wird hingegen geprüft.

Whitelist

Nur die Clients werden zugelassen, deren MAC-Adresse bekannt ist.

Blacklist

Nur die Clients werden zugelassen, deren MAC-Adresse nicht bekannt ist.

VLAN

Hier können Sie festlegen, welchem VLAN ein LEPS-Benutzer bzw. -Client, der mit diesem Profil verbunden ist, zugewiesen wird.

4.1.2 Benutzer

Legen Sie hier einzelne LEPS-Benutzer an. Jeder LEPS-Benutzer muss mit einem zuvor angelegten Profil verbunden werden und eine individuelle WPA-Passphrase zugewiesen bekommen. Mit dieser Passphrase kann sich dann ein beliebiger Client an der SSID anmelden, für die der Benutzereintrag durch die Verknüpfung des Profils gültig ist. Der Benutzer wird anhand der verwendeten Passphrase identifiziert und dem in dieser Tabelle konfigurierten VLAN zugewiesen. Wird hier

kein VLAN zugewiesen, wird er dem am Profil konfigurierten VLAN zugewiesen. Einstellungen am einzelnen Benutzer haben somit Priorität gegenüber Einstellungen am Profil.

Name


Vergeben Sie hier einen eindeutigen Namen für den LEPS-Benutzer.

Profil

Wählen Sie hier das Profil aus, für das der LEPS-Benutzer gültig sein soll. Es können sich nur LEPS-Benutzer an der SSID anmelden, mit der sie über das LEPS-Profil verbunden sind.

WPA-Passphrase

Vergeben Sie hier die Passphrase, mit der sich der LEPS-Benutzer am WLAN anmelden soll.

 Als Passphrase können Zeichenketten mit 8 bis 64 Zeichen verwendet werden. Wir empfehlen als Passphrasen zufällige Zeichenketten von mindestens 32 Zeichen Länge.

MAC-Adresse

Optionale Angabe einer MAC-Adresse für einen MAC-Filter. Abhängig von der Einstellung im Profil wird dieser Eintrag nicht beachtet oder es können sich dann nur die in dieser Tabelle aufgeführten Clientgeräte anmelden (Whitelist). Mittels Blacklist funktioniert der MAC-Filter genau anders herum – die angegebenen MAC-Adressen können sich nicht anmelden.

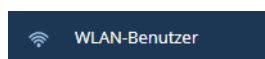
Im Vergleich zur reinen Zuweisung einer Passphrase an einen Benutzer ist die Verwaltung einer Passphrase pro MAC-Adresse etwas aufwändiger bei gleichzeitig höherer Kontrolle über die Geräte im Netz.

VLAN

Hier können Sie festlegen, welchem VLAN der LEPS-Benutzer zugewiesen wird. Wird hier kein VLAN konfiguriert, gilt eine eventuelle, im LEPS-Profil konfigurierte VLAN. Wird sowohl im LEPS-Profil als auch beim LEPS-Benutzer ein VLAN konfiguriert, gilt die hier konfigurierte VLAN.

4.2 WLAN-Benutzer

Sie erreichen diesen Bereich in der WEBconfig über den Punkt **WLAN-Benutzer** in der Sidebar.



4.2.1 LEPS

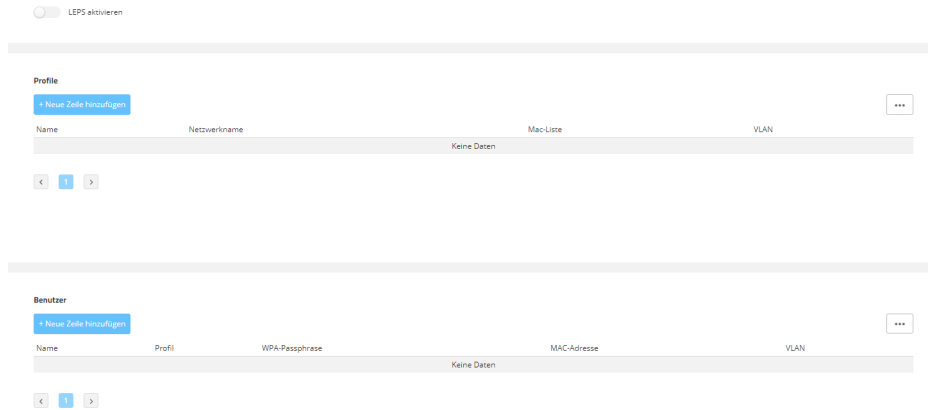
Bei der Konfiguration von LEPS wird jedem Benutzer, der sich mit Clients im WLAN anmelden können soll, eine individuelle Passphrase zugeordnet. Dazu werden LEPS-Profile angelegt, damit einige Einstellungen nicht bei jedem Benutzer erneut

4 LANCOM Enhanced Passphrase Security (LEPS)

vorgenommen werden müssen. Anschließend legen Sie die LEPS-Benutzer mit der zugehörigen individuellen Passphrase an und verknüpfen diesen mit einem der vorher angelegten LEPS-Profile.

Alternativ können Sie die Passphrase mit einer MAC-Adresse verbinden und auf diese Weise einen MAC-Adress-Filter einrichten.

Hier konfigurieren Sie die **Profile** und **Benutzer** für LANCOM Enhanced Passphrase Security (LEPS). Über den Schalter **LEPS aktivieren** wird LEPS eingeschaltet.



Profile

Konfigurieren Sie hier LEPS-Profile und verbinden Sie sie mit einer SSID. Anschließend können die LEPS-Profile den LEPS-Benutzern zugeordnet werden.

Name

Vergeben Sie hier einen eindeutigen Namen für das LEPS-Profil.

Netzwerkname

Wählen Sie hier die SSID bzw. beim WLC das logische WLAN-Netzwerk aus, für die das LEPS-Profil gültig sein soll. Es können sich nur LEPS-Benutzer an der SSID bzw. beim WLC an dem logischen WLAN-Netzwerk anmelden, mit der sie über das LEPS-Profil verbunden sind.

MAC-Liste

Mögliche Werte:

Nicht prüfen

Die MAC-Adresse wird für die LEPS-Anmeldung nicht beachtet. Eine ggf. gesetzte benutzerspezifische Passphrase wird hingegen geprüft.

Whitelist

Nur die Clients werden zugelassen, deren MAC-Adresse bekannt ist.

Blacklist

Nur die Clients werden zugelassen, deren MAC-Adresse nicht bekannt ist.

VLAN

Hier können Sie festlegen, welchem VLAN ein LEPS-Benutzer bzw. -Client, der mit diesem Profil verbunden ist, zugewiesen wird.

Benutzer

Legen Sie hier einzelne LEPS-Benutzer an. Jeder LEPS-Benutzer muss mit einem zuvor angelegten Profil verbunden werden und eine individuelle WPA-Passphrase zugewiesen bekommen. Mit dieser Passphrase kann sich dann ein beliebiger Client an der SSID anmelden, für die der Benutzereintrag durch die Verknüpfung des Profils gültig ist. Der Benutzer wird anhand der verwendeten Passphrase identifiziert und dem in dieser Tabelle konfigurierten VLAN zugewiesen. Wird hier kein VLAN zugewiesen, wird er dem am Profil konfigurierten VLAN zugewiesen. Einstellungen am einzelnen Benutzer haben somit Priorität gegenüber Einstellungen am Profil.

Name

Vergeben Sie hier einen eindeutigen Namen für den LEPS-Benutzer.

Profil

Wählen Sie hier das Profil aus, für das der LEPS-Benutzer gültig sein soll. Es können sich nur LEPS-Benutzer an der SSID anmelden, mit der sie über das LEPS-Profil verbunden sind.

WPA-Passphrase

Vergeben Sie hier die Passphrase, mit der sich der LEPS-Benutzer am WLAN anmelden soll.



Als Passphrase können Zeichenketten mit 8 bis 64 Zeichen verwendet werden. Wir empfehlen als Passphrasen zufällige Zeichenketten von mindestens 32 Zeichen Länge.

MAC-Adresse

Optionale Angabe einer MAC-Adresse für einen MAC-Filter. Abhängig von der Einstellung im Profil wird dieser Eintrag nicht beachtet oder es können sich dann nur die in dieser Tabelle aufgeführten Clientgeräte anmelden (Whitelist). Mittels Blacklist funktioniert der MAC-Filter genau anders herum – die angegebenen MAC-Adressen können sich nicht anmelden.

Im Vergleich zur reinen Zuweisung einer Passphrase an einen Benutzer ist die Verwaltung einer Passphrase pro MAC-Adresse etwas aufwändiger bei gleichzeitig höherer Kontrolle über die Geräte im Netz.

VLAN

Hier können Sie festlegen, welchem VLAN der LEPS-Benutzer zugewiesen wird. Wird hier kein VLAN konfiguriert, gilt eine eventuelle, im LEPS-Profil konfigurierte VLAN. Wird sowohl im LEPS-Profil als auch beim LEPS-Benutzer ein VLAN konfiguriert, gilt die hier konfigurierte VLAN.

4.3 Ergänzungen im Setup-Menü

4.3.1 LEPS

Mit LANCOM Enhanced Passphrase Security (LEPS) können Sie WLAN-Stationen benutzerdefinierte Passphrasen zuweisen, ohne die Stationen vorher anhand ihrer MAC-Adresse erfassen zu müssen. Alternativ lässt sich auch ein MAC-Adress-Filter realisieren.

SNMP-ID:

2.20.133

Pfad Konsole:

Setup > WLAN

Operating

Schaltet LEPS ein oder aus. Im ausgeschalteten Zustand werden die angelegten LEPS-Benutzer bei der Anmeldung von WLAN-Clients nicht beachtet.

SNMP-ID:

2.20.133.1

Pfad Konsole:

Setup > WLAN > LEPS

Mögliche Werte:

No
yes

Default-Wert:

No

Profiles

Konfigurieren Sie hier LEPS-Profile und verbinden Sie sie mit einer SSID. Anschließend können die LEPS-Profile den LEPS-Benutzern zugeordnet werden. Dabei können Sie für einen Benutzer die Profilwerte durch individuelle Werte überschreiben.

SNMP-ID:

2.20.133.2

Pfad Konsole:

Setup > WLAN > LEPS

Name

Vergeben Sie hier einen eindeutigen Namen für das LEPS-Profil.

SNMP-ID:

2.20.133.2.1

Pfad Konsole:

Setup > WLAN > LEPS > Profiles

Mögliche Werte:

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

Network-Name

Wählen Sie hier die SSID bzw. beim WLC das logische WLAN-Netzwerk aus, für die das LEPS-Profil gültig sein soll. Es können sich nur LEPS-Benutzer an der SSID bzw. beim WLC an dem logischen WLAN-Netzwerk anmelden, mit der sie über das LEPS-Profil verbunden sind.

SNMP-ID:

2.20.133.2.2

Pfad Konsole:**Setup > WLAN > LEPS > Profiles****Mögliche Werte:**

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

Mac-List

Hier können Sie angeben, ob und wie die MAC-Adressen überprüft werden sollen.

SNMP-ID:

2.20.133.2.3

Pfad Konsole:**Setup > WLAN > LEPS > Profiles****Mögliche Werte:****Disabled**

Die MAC-Adresse wird für die LEPS-Anmeldung nicht beachtet. Eine ggf. gesetzte benutzerspezifische Passphrase wird hingegen geprüft.

Whitelist

Nur die Clients werden zugelassen, deren MAC-Adresse bekannt ist.

Blacklist

Nur die Clients werden zugelassen, deren MAC-Adresse nicht bekannt ist.

VLAN

Hier können Sie festlegen, welchem VLAN ein LEPS-Benutzer, der mit diesem Profil verbunden ist, zugewiesen wird.

SNMP-ID:

2.20.133.2.5

Pfad Konsole:**Setup > WLAN > LEPS > Profiles****Mögliche Werte:**

0 ... 4095

Users

Legen Sie hier einzelne LEPS-Benutzer an. Jeder LEPS-Benutzer muss mit einem zuvor angelegten Profil verbunden werden.

SNMP-ID:

2.20.133.3

Pfad Konsole:

Setup > WLAN > LEPS

Name

Vergeben Sie hier einen eindeutigen Namen für den LEPS-Benutzer.

SNMP-ID:

2.20.133.3.1

Pfad Konsole:

Setup > WLAN > LEPS > Users

Mögliche Werte:

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

Profile

Wählen Sie hier das Profil aus, für das der LEPS-Benutzer gültig sein soll. Es können sich nur LEPS-Benutzer an der SSID anmelden, mit der sie über das LEPS-Profil verbunden sind.

SNMP-ID:

2.20.133.3.2

Pfad Konsole:

Setup > WLAN > LEPS-U > Users

Mögliche Werte:

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

WPA-Passphrase

Vergeben Sie hier die Passphrase, mit der der LEPS-Benutzer sich am WLAN anmelden soll.

SNMP-ID:

2.20.133.3.3

Pfad Konsole:

Setup > WLAN > LEPS > Users

Mögliche Werte:

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

VLAN

Hier können Sie festlegen, welchem VLAN der LEPS-Benutzer zugewiesen wird. Wird hier kein VLAN konfiguriert, gilt eine eventuelle, im LEPS-Profil konfigurierte VLAN. Wird sowohl im LEPS-Profil als auch am LEPS-Benutzer ein VLAN konfiguriert, gilt die am LEPS-Benutzer konfigurierte VLAN-ID.

SNMP-ID:

2.20.133.3.4

Pfad Konsole:

Setup > WLAN > LEPS > Users

Mögliche Werte:

0 ... 4095

MAC-Address

Optionale Angabe einer MAC-Adresse für einen MAC-Filter. Abhängig von der Einstellung im Profil wird dieser Eintrag nicht beachtet oder es können sich dann nur die in dieser Tabelle aufgeführten Clientgeräte anmelden (Whitelist). Mittels Blacklist funktioniert der MAC-Filter genau anders herum – die angegebenen MAC-Adressen können sich nicht anmelden.

SNMP-ID:

2.20.133.3.7

Pfad Konsole:

Setup > WLAN > LEPS > Users

Mögliche Werte:

MAC-Adresse im Format `xx:xx:xx:xx:xx:xx`

5 Dynamic VLAN für 802.1X

Mit Dynamic VLAN kann der RADIUS-Server im Rahmen einer 802.1X-Anmeldung die VLAN-ID für den WLAN-Client zuweisen. Clients lassen sich somit dem gewünschten VLAN zuweisen, ohne dafür je VLAN eine separate SSID bereitstellen zu müssen.

Der RADIUS-Server muss dazu folgende Attribute in der Accept-Nachricht mitsenden:

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS LX
64	Tunnel-Type	Definiert das Tunneling-Protokoll, welches für die Sitzung verwendet wird.	13 (VLAN)
65	Tunnel-Medium-Type	Definiert das Transportmedium, über das eine getunnelte Sitzung hergestellt wird.	6 (IEEE 802)
81	Tunnel-Private-Group-Id	Definiert die gewünschte VLAN-ID.	1-4096