LCOS LX 7.10

Addendum

08/2025

LANCOM SYSTEMS

Contents

Copyright

© 2025 LANCOM Systems GmbH, Würselen (Germany). All rights reserved.

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, LCOS, LANcommunity, LANCOM Service LANcare, LANCOM Active Radio Control, and AirLancer 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

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Würselen, Germany

Germany

www.lancom-systems.com

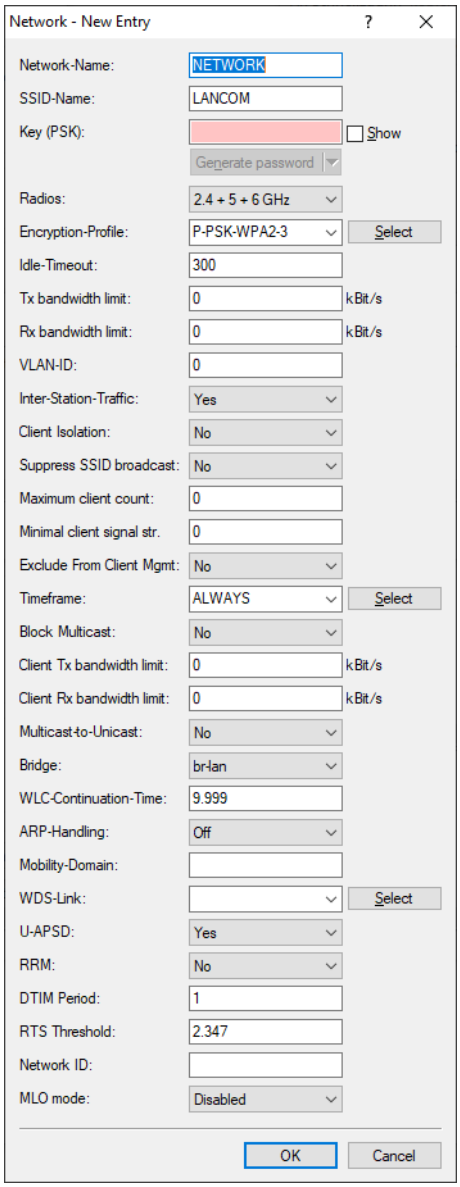
1 Addendum to LCOS LX version 7.10

This document describes the changes and enhancements in LCOS LX version 7.10 since the previous version.

2 Multi-Link Operation (MLO)

As of LCOS LX 7.10, Multi-Link Operation (MLO) is supported. For this purpose, the configuration has been extended with the options described below.

Under **Wireless-LAN** > **WLAN-Networks** > **Network** you will find the new option **MLO mode**.



MLO mode

With Multi-Link Operation (MLO), Wi-Fi 7-capable WLAN clients can manage multiple associations with the same access point simultaneously. This increases throughput and reduces latency.

For WLAN clients with only one radio module, it is possible to switch quickly between the better-quality frequency bands. This significantly reduces disconnections in high-density wireless environments and provides more stable WLAN connectivity.

WLAN clients with multiple radios can use several frequency bands simultaneously to maximize data throughput.

Ccertain encryption settings are mandatory for standards-compliant Wi-Fi 7 and Multi Link Operation:

- The WPA session key type must include AES-GCMP-256
- The Group Mgmt Cipher must be BIP-GMAC-256
- The SAE/OWE-DH groups must include DH-19, DH-20, and DH-21
- Protected Management Frames (IEEE 802.11w) must be enabled
- Beacon Protection must be enabled

To simplify the use of these settings, the additional encryption profile "P-PSK-WiFi7" is included in the configuration as of LCOS LX 7.10 and can be used.

Since some of these settings may cause compatibility issues with existing (legacy) clients, we recommend configuring a separate SSID for Wi-Fi 7, MLO, and the above-mentioned encryption settings, and using it exclusively with Wi-Fi 7 clients.

Possible values:

Auto

MLO is enabled for all Wi-Fi 7 / IEEE 802.11be-capable radios where the SSID is broadcast.

Single-Link

Each Wi-Fi 7 / IEEE 802.11be-capable radio is treated as a standalone MLD (Multi-Link Device). In this case, the MLO "infrastructure" is used, but the radios remain separated. This mode may be useful in cases of compatibility issues.

Disabled

MLO is not used. The radios are not configured as MLDs.

2.1 Additions to the Setup menu

2.1.1 MLO-Mode

With Multi-Link Operation (MLO), Wi-Fi 7-capable WLAN clients can manage multiple associations with the same access point simultaneously. This increases throughput and reduces latency.

For WLAN clients with only one radio module, it is possible to switch quickly between the better-quality frequency bands. This significantly reduces disconnections in high-density wireless environments and provides more stable WLAN connectivity.

WLAN clients with multiple radios can use several frequency bands simultaneously to maximize data throughput.

Ccertain encryption settings are mandatory for standards-compliant Wi-Fi 7 and Multi Link Operation:

- The WPA session key type must include AES-GCMP-256
- The Group Mgmt Cipher must be BIP-GMAC-256
- The SAE/OWE-DH groups must include DH-19, DH-20, and DH-21
- Protected Management Frames (IEEE 802.11w) must be enabled
- Beacon Protection must be enabled

To simplify the use of these settings, the additional encryption profile “P-PSK-WiFi7” is included in the configuration as of LCOS LX 7.10 and can be used.

Since some of these settings may cause compatibility issues with existing (legacy) clients, we recommend configuring a separate SSID for Wi-Fi 7, MLO, and the above-mentioned encryption settings, and using it exclusively with Wi-Fi 7 clients.

SNMP ID:

2.20.1.42

Console path:

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

Possible values:

Auto

MLO is enabled for all Wi-Fi 7 / IEEE 802.11be-capable radios where the SSID is broadcast.

Single-Link

Each Wi-Fi 7 / IEEE 802.11be-capable radio is treated as a standalone MLD (Multi-Link Device). In this case, the MLO “infrastructure” is used, but the radios remain separated. This mode may be useful in cases of compatibility issues.

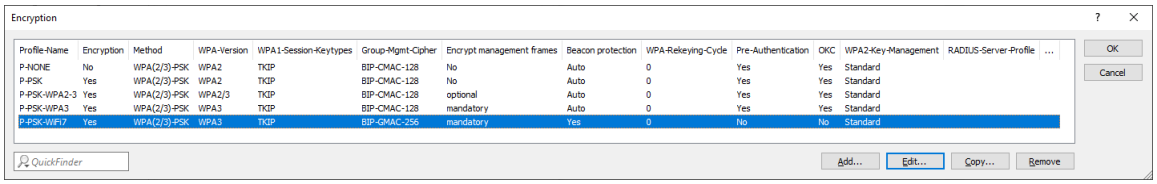
Disabled

MLO is not used. The radios are not configured as MLDs.

3 Encryption Profile for Wi-Fi 7 and MLO Operation

Standards-compliant Wi-Fi 7 certified operation according to the specifications of the Wi-Fi Alliance requires specific encryption settings. A new, dedicated encryption profile makes this easy to configure as of LCOS LX 7.10.

Under **Wireless LAN** > **WLAN Networks** > **Encryption**, the new encryption profile "P-PSK-WiFi7" is now available.



P-PSK-WiFi7

Ccertain encryption settings are mandatory for standards-compliant Wi-Fi 7 and Multi Link Operation:

- The WPA session key type must include AES-GCMP-256
- The Group Mgmt Cipher must be BIP-GMAC-256
- The SAE/OWE-DH groups must include DH-19, DH-20, and DH-21
- Protected Management Frames (IEEE 802.11w) must be enabled
- Beacon Protection must be enabled

To simplify the use of these settings, the additional encryption profile "P-PSK-WiFi7" is included in the configuration as of LCOS LX 7.10 and can be used.

Since some of these settings may cause compatibility issues with existing (legacy) clients, we recommend configuring a separate SSID for Wi-Fi 7, MLO, and the above-mentioned encryption settings, and using it exclusively with Wi-Fi 7 clients.

4 Default Encryption Profile

As of LCOS LX 7.10, the default encryption profile for newly created WLAN networks has been changed from P-PSK to P-PSK-WPA2-3.