

RELEASE NOTES

LCOS LX

7.14 RU1

Table of contents

02	1. Preface
02	2. The release tag in the software name
03	3. Device-specific compatibility to LCOS LX
03	4. Notes on LCOS LX
03	Information on default settings
03	5. Known restrictions
04	6. History LCOS LX
04	LCOS LX - improvements 7.14.0036 RU1
05	LCOS LX - improvements 7.14.0026 Rel
06	7. General notes
06	Disclaimer
06	Backing up the current configuration

1. Preface

The LCOS family of operating systems—LCOS, LCOS SX, LCOS LX, and LCOS FX—forms the trusted basis for the entire R&S®LANCOM range of products. Within the scope of the hardware specified by the products, the latest firmware version is available for all R&S®LANCOM products and is offered by Rohde & Schwarz Networks and Cybersecurity for download free of charge.

Rohde & Schwarz Networks and Cybersecurity keeps program libraries used in LCOS firmware up to date with the latest security patches and fixes security vulnerabilities even if they cannot be exploited in the firmware.

This document describes the innovations within LCOS LX software release 7.14 RU1, as well as the improvements since the previous version.

Before upgrading the firmware, please pay close attention to chapter 7 „General notes“ of this document.

Latest support notes and known issues regarding the current LCOS LX version can be found in the [support area of our website](#).

2. The release tag in the software name

Release Candidate (RC)

A Release Candidate has been extensively tested by Rohde & Schwarz Networks and Cybersecurity and includes new LCOS features. It is suitable for testing and is not recommended for use in productive environments.

Release Version (REL)

The release version has been extensively and successfully tested in practice. It contains new features and improvements over previous operating system versions and is therefore recommended for use in productive environments.

Release Update (RU)

A release update is a further development of an initial release version in productive environments and contains minor improvements, security fixes, bug fixes and smaller features.

Security Update (SU)

Contains important security fixes for the respective operating system version and ensures that your security level remains very high on an ongoing basis in your productive environment.

3. Device-specific compatibility to LCOS LX

R&S®LANCOM products regularly receive major firmware releases throughout their lifetime which provide new features and bugfixes. LCOS LX release updates including bugfixes and general improvements are available on a regular basis for devices which do not support the latest LCOS LX version. You can find an overview of the latest supported LCOS LX version for your device under [Lifecycle policies](#).

4. Notes on LCOS LX

Information on default settings

Devices delivered with LCOS LX automatically connect to the R&S®LANCOM Management Cloud (R&S®LMC). This functionality provides zero-touch installation for new devices. In case you do not want to use the R&S®LMC, this feature can be disabled while running the default setup wizard for the initial configuration, or at any time from within LANconfig under Management > LMC. You can manually re-enable the usage of the R&S®LMC whenever you want.

5. Known restrictions

- ▶ Local configuration changes are not transferred to the R&S®LMC.
- ▶ The scripting of the device from the R&S®LMC is currently not supported, but the use of add-ins is.

6. History LCOS LX

LCOS LX - improvements 7.14.0036 RU1

New features

- ▶ Support for the Wireless Client Explorer in the R&S®LANCOM Management Cloud

Bugfixes / improvements

- ▶ In scenarios involving a large number of simultaneously active R&S®LMC hotspot clients, communication with the R&S®LMC might be disrupted

LCOS LX - improvements 7.14.0026 Rel

New features

- ▶ A TACACS+ server can now be accessed via IPv6, too.
- ▶ A syslog server can now be accessed via IPv6, too.
- ▶ The LMC-based hotspot can now also be used via L2TPv3 tunnels.
- ▶ BLE 5.4/LBS scanning is now supported on the LANCOM LX-7200, LX-7200E, and LX-7400 devices.

Bugfixes / improvements

- ▶ If a configured TACACS+ server is accessible and responds to requests, local fallback is no longer possible.
- ▶ The OpenSSL library has been updated to version 1.1.1zf.
- ▶ No SSID names were displayed in the WEBconfig menu 'Wi-Fi configuration > Bridge' in the 'Networks' column.
- ▶ If the IPv6 address source was configured to Router Advertisement (default setting) in the Access Point configuration in the 'IP Configuration > LAN Interfaces' menu, it took several minutes to obtain an IPv6 address.
- ▶ When configuring an encryption profile for Enhanced Open, the access point required a password (passphrase) to be assigned, even though this is not intended for Enhanced Open. As a result, the configuration could not be written to the access point.
- ▶ When roaming using fast roaming (802.11r), the status 'No' might have been displayed incorrectly instead of 'Yes' in the station table 'Status > WLAN > Station Table' under 'Fast Roaming'.
- ▶ After changing the SSID name via the LMC, the old SSID continued to be broadcast.
- ▶ Authentication via 802.1X as a LAN supplicant is only possible on the main port with PoE support (usually LAN1). However, on the LANCOM OW-602, authentication only worked on the LAN2 port.
- ▶ In a scenario with a WLAN controller, when a wireless client initially connected to an access point while using both fast roaming (802.1X SSID) and dynamic VLAN, the client was assigned the correct VLAN ID. However, the access point did not store this VLAN ID in its FT cache. After the wireless client roamed from another access point back to the initial access point, this resulted in the client being assigned either no VLAN ID or the VLAN ID stored statically in the logical wireless profile, depending on the configuration.
- ▶ If the WLC tunnel operating mode was used on a WLAN controller in a Wi-Fi network, the SSID remained active even when the WLAN controller was unavailable.
In addition, the SSID continued to be broadcast permanently when autonomous operation was active and the connection type was 'LAN at AP', even though the configured time had already been exceeded.

7. General notes

Disclaimer

Rohde & Schwarz Networks and Cybersecurity does not take any guarantee and liability for software not developed, manufactured or distributed by Rohde & Schwarz Networks and Cybersecurity, especially not for shareware and other extraneous software.

Backing up the current configuration

Before upgrading your R&S®LANCOM devices to a new LCOS LX version it is essential to backup the configuration data!

Due to extensive features it is **not possible to downgrade** to a previous firmware without using the backup configuration.

Please see the LCOS LX reference manual for instructions on how to upgrade the firmware.

We strongly recommend updating productive systems in client environment only after internal tests.

Despite intense internal and external quality assurance procedures possibly not all risks can be eliminated by Rohde & Schwarz Networks and Cybersecurity.

Rohde & Schwarz Networks and Cybersecurity GmbH
Adenauerstr. 20/B2
52146 Wuersele | Germany
info.rs-nc@rohde-schwarz.com | www.rohde-schwarz.com/networks-and-cybersecurity

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.

ROHDE & SCHWARZ
Make ideas real

