RELEASE NOTES

# LCOS
## 11.00 RC1

## Table of contents


02 **1. Preface**

02 **2. The release tag in the software name**

03 **3. Device-specific compatibility to LCOS 11.00**
03 R&S®LANCOM devices without support as of LCOS 11.00

04 **4. Advices regarding LCOS 11.00**
04 General notes on the update
04 Information on default settings
04 Removed features

05 **5. Feature overview LCOS 11.00**

05 **5.1 Feature highlights**
05 Future-proof VPN encryption with post-quantum cryptography
05 VRRP for high-availability VoIP environments

06 **6. History LCOS 11.00**
06 LCOS improvements 11.00.0043 RC1

08 **7. General advice**
08 Disclaimer
08 Backing up the current configuration
08 Using converter firmwares to free up memory


ROHDE&SCHWARZ
Make ideas real

## 1. Preface

The LCOS family of operating systems—LCOS, LCOS SX, LCOS LX, and LCOS FX—forms the trusted asis 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 software release 11.00 RC1, as well as the improvements since the previous version.

**Before upgrading the firmware, please pay close attention to chapter 7 "General advice" of this document.**

**Latest support notes and known issues** regarding the current LCOS 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 featurses. 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 11.00

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

### R&S®LANCOM devices without support as of LCOS 11.00

- 883+ VoIP
- 1640E
- 1784VA
- 1790VA
- 1790VAW
- 1790VA-4G
- 1790VA-4G+
- IAP-4G+
- LN-1700B
- LN-1702B
- R884VA
- WLC-1000
- WLC-30

## 4. Advices regarding LCOS 11.00

### General notes on the update

As of LCOS 10.90, the CLI menu for VRRP has been moved from '/Setup/IP-Router/VRRP/' to '/Setup/VRRP/'. The table structure and the associated OID path have also changed due to the support for VRRPv3 and IPv6.

Please note that add-ins for the R&S®LMC and any existing scripts for VRRP must be adapted for LCOS 10.90 and higher. Existing scripts for VRRP are not compatible with LCOS 10.90 and higher.

### Information on default settings

Devices delivered with LCOS 10.00 or higher 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.

### Removed features

For new devices, the use of the ePaper USB flash drive (End of Sale) is no longer supported.

# 5. Feature overview LCOS 11.00

## 5.1 Feature highlights

### Future-proof VPN encryption with post-quantum cryptography

With this update, IKEv2 VPN connections can already be prepared for future threats posed by powerful quantum computers. To achieve this, LCOS uses modern post-quantum mechanisms for key exchange. Traditional encryption methods can be combined with the quantum-resistant ML-KEM algorithm. This creates a hybrid approach that combines established security mechanisms with additional protection for the future. The ML-KEM groups DH35, DH36, and DH37 are available.

### VRRP for high-availability VoIP environments

To improve failover reliability in telephony infrastructures, the Voice Call Manager in R&S®LANCOM SD-WAN VoIP gateways can now also be operated redundantly using VRRP (Virtual Router Redundancy Protocol). Multiple physical R&S®LANCOM SD-WAN VoIP gateways act as a single virtual gateway, allowing a standby device to take over network communication if the active device fails. For this purpose, the Voice Call Manager is specifically bound to the corresponding virtual network. SIP endpoints register using the gateway's virtual IP address and can re-register with the new master device after a failover. This ensures that telephony functions are quickly restored even in the event of a failure.

**You can find further features within the individual builds sections in chapter 6 "History LCOS 11.00".**

# 6. History LCOS 11.00

## LCOS improvements 11.00.0043 RC1

### New features

#### General

- Support for TLS in TACACS+ acc. to RFC 9887
- The Voice Call Manager can be used in conjunction with VRRP.
- For AON fiber-optic connections using the R&S®LANCOM SFP-AON-1, there is now a dedicated status menu under ‚/Status/AON/'.
- When using the R&S®LANCOM SFP-AON-1, the WEBconfig dashboard now displays status information for the AON module.
- Support for RFC 5709 OSPFv2 HMAC-SHA cryptographic authentication.
- LMC Client: The behavior for zero-touch claiming is now configurable.
- Adjustment of default menu settings for IPv6 Router advertisements and DHCPv6 to align with the recommendations in RFC 9096
- If a DHCPv6-PD prefix is deactivated on the WAN, the DHCPv6 server on the LAN now initiates a reconfiguration using a 'Renew' message type for DHCPv6 clients that have negotiated reconfiguration.
- The PPPoE server now supports the framed route (IETF #22) and LCS-DNS server-IPv4-address (Vendor 2356, Attribute #21) attributes for RADIUS authentication.
- The DHCPv6 server supports the transmission of DHCPv6 options via a vendor-specific RADIUS attribute (IKEv2 and PPPoE servers).
- IKEv2 and PPPoE servers support RADIUS Accounting On and RADIUS Accounting Off messages.
- The PPPoE server now supports RADIUS accounting and a configurable sender address.
- The 'Loadfirmware' command on the CLI now also supports loading firmware files from a USB flash drive connected to the router.
- TR-069 (data model TR-181) now supports AON and GPON status information.
- IPv6 addresses can now also be specified for HTTP tunnels.
- Support for the PQ algorithms 'mlkem768nistp256-sha256' and 'mlkem1024nistp384-sha384' in SSH

#### VPN

- Support for RFC 9242 Intermediate Exchange in IKEv2
- Support for RFC 9370 Multiple Key Exchanges in IKEv2
- Support for the post-quantum DH groups ML-KEM DH35, DH36, and DH37 in the IKEv2 key exchange
- The type of the WireGuard remote node (WAN or VPN) can be configured.

#### LANconfig

- Wireless ePaper management has been removed and is no longer supported.

## Bug fixes

### General

- The eSIM client in mobile routers did not support ‘chunked encoding‘ If an eSIM server used ‘chunked encoding‘, this prevented the eSIM profile from being retrieved.
- Security vulnerabilities with the following CVE numbers have been fixed in the PCRE2 program library:
  - CVE-2026-89157
  - CVE-2026-89158
  - CVE-2026-89161
- The Apache Thrift framework has been updated to version 0.24, thereby addressing security vulnerabilities with the following CVE numbers:
  - CVE-2026-58662
  - CVE-2026-55971
  - CVE-2026-55970

## 7. General advice

### 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 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.

If you want to upgrade devices which are only accessible via router connections or Wi-Fi bridges, please keep in mind to upgrade the remote device first and the local device afterwards. Please see the LCOS 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.

### Using converter firmwares to free up memory

Due to numerous new functions within the LCOS firmware it may not be possible in some circumstances for older devices to keep two fully-featured firmware versions at the same time in the device. To gain more free memory, a smaller firmware with less functionality has to be uploaded to the device first. As a result, significantly more memory will be available for a second firmware.

This installation has to be done only once by using a “converter firmware“.

After having installed the converter firmware, the firmsafe function of the R&S®LANCOM device is only available on a limited scale. The update to a new firmware is furthermore possible without any problems.

However, after a failed update the R&S®LANCOM device works with the converter firmware which only allows local device access. Any advanced functionality, particularly the remote administration, is not available as long as the converter firmware is active.

Rohde & Schwarz Networks and Cybersecurity GmbH
Adenauerstr. 20/B2
52146 Wuerselen | 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. 11/2026

ROHDE&SCHWARZ
Make ideas real