Release Notes

LCOS 10.72 Rel

Table of contents

December 07th, 2022, CBuersch

1. Preface

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

This document describes the innovations within LCOS software release 10.72 Rel, 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
www.lancom-systems.com/service-support/instant-help/common-support-tips

2. The release tag in the software name

Release Candidate (RC)

A Release Candidate has been extensively tested by LANCOM and includes new LCOS featurses. It is suitable for testing and is not recommended for use in productive environments.

Release-Version (REL)

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

Release Update (RU)

This is a further development of an initial release version and contains minor improvements, bug fixes and smaller features.

Security Update (SU)

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

3. Device-specific compatibility to LCOS 10.72

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 under www.lancom-systems.com/products/firmware/lifecycle-management/product-tables

Support for the following devices is no longer available as from LCOS 10.72:

→ LANCOM 1781EF+
→ LANCOM 1783VA
→ LANCOM 1781VAW
→ LANCOM 1783VA-4G
→ LANCOM R883VAW
→ Business LAN R800A

4. Advices regarding LCOS 10.72

Information on default settings

Devices delivered with LCOS 10.00 or higher automatically connect to the LANCOM Management Cloud (LMC). This functionality provides zero-touch installation for new devices. In case you do not want to use the 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 LMC whenever you want.

5. Feature overview LCOS 10.72

5.1 Feature highlights 10.72

Advanced Mesh VPN

With classic, star-shaped VPN site networks, in which all branches are only connected via the headquarters and not directly to each other, the Internet line of the headquarters quickly becomes the bottleneck of the entire communication. With Advanced Mesh VPN, the branch offices are now directly interconnected, resulting in significantly less traffic at the headquarters and thus higher performance. The VPN tunnels are established dynamically as soon as data traffic is transported from one branch office to another. If there is no more communication, the VPN connection is terminated dynamically as well

5.2 Further features 10.72

Protection of minors according to official regulations

With LCOS 10.70 RC1, you can now maximize the protection of underage end users, e.g. in schools or youth facilities. For example, the official website list of the “Bundesprüfstelle für jugendgefährdende Medien” (German Federal Review Board, BPjM) is now also part of the LANCOM Content Filter Option or available separately via the software extension LANCOM BPjM Filter Option (as of LCOS 10.70 Rel). This means that domains whose content is officially classified as harmful are not accessible to the relevant target group in Germany. Continuous updates and extensions of this list are guaranteed.

Two-factor authentication – double security for your VPN

Whenever a high level of security for your sensitive data is required or, for example, compliance guidelines in your company demand it, double protection of network access via your LANCOM Advanced VPN Client is ideal. Thanks to two-factor authentication (IKEv2 EAP-OTP), you can now protect VPN access and thus also your network from unauthorized access. You can specify that users can only log in via the LANCOM Advanced VPN Client if they use two-factor authentication when logging in. In this case, the VPN password is supplemented by a time-based one-time password, which can be generated in an authentication app (e.g. Google Authenticator) on the cell phone. This feature can be used with all devices that have at least 25 VPN tunnels (either already integrated or upgraded with LANCOM VPN Option).

You can find further features within the individual builds sections in chapter 6 “History LCOS 10.72”.

6. History LCOS 10.72

LCOS improvements 10.72.0015 Rel

New features

→ Support for Q-in-Q VLAN on WAN interfaces

→ Support of a sender address for the update process of the signature file at the BPJM filter

→ Master holddown time switch in VRRP

→ Support for RADSEC certificates in the SCEP client

→ In WEBConfig, there is a link to the Wi-Fi station table in the dashboard under Wi-Fi.

→ A LANCOM WLC supports the selection of the LANCOM LX-6500 in the firmware management.

→ Support for LANCOM ARC 2.0 together with the LMC

Bug fixes / improvements

General

→ Although no Content Filter option was active on a router, the 'Content Filter' menu was displayed in WEBconfig. However, the configuration dialogs were empty.

→ In WEBconfig, the configuration settings for the time server adjustment method were missing in the 'Date/Time / Synchronization' menu.

→ In the WEBconfig menu 'Setup Wizard / Manage Public Spot Users', users were displayed as 'unauthenticated' although they were successfully connected to the Public Spot.

→ In a WWAN connection where the address reference was configured via DHCP, the LANCOM DHCP client sent ARP requests, although these were not required for the WWAN connection.

→ The DNS servers stored in the 'IPv4 / Addresses' menu are bound to the LAN interface. If the local IP address of the router was stored as DNS server in this menu and a default route was created which pointed to the IP address of an upstream router in the same IP address range, this led to an immediate restart of the router.

Wi-Fi

- If another user was to be added when the RADIUS user table was full, a page with JavaScript code was displayed instead of an error message.
- In LCOS 10.70 it could happen that an incorrect reference to the MAC address of the connected Wi-Fi device was stored in the address table of the WLC tunnel used. As a result, communication via the WLC tunnel no longer worked.

7. General advice

Disclaimer

LANCOM Systems GmbH does not take any guarantee and liability for software not developed, manufactured or distributed by LANCOM Systems GmbH, especially not for shareware and other extraneous software.

Backing up the current configuration

Before upgrading your 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 LANCOM Systems.

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 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 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.