Release Notes

LCOS
10.34 SU6

Table of contents

03 **1. Preface**

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

04 **3. Device-specific compatibility to LCOS 10.34**

04 **4. Advices regarding LCOS 10.34**
04 Information on default settings

05 **5. Feature overview LCOS 10.34**

05 **5.1 Feature highlights 10.34**
05 SD-WAN – Application Routing
05 SD-WAN – Layer-7 Application Control in the firewall
05 WLC functions in the vRouter (vWLC)

06 **5.2 Further features**
06 Flexible and future-proof telephony at all locations
06 TLS 1.3
06 Elliptic Curve Digital Signature Algorithm (ECDSA)
06 IKEv2 split DNS
06 IKEv2 fragmentation
06 Enhanced client reservations in the DHCPv6 server
06 Double the number of Public Spot users

07 **6. History LCOS 10.34**
07 LCOS improvements 10.34.03xx SU6

08 LCOS improvements 10.34.0308 SU5
09 LCOS improvements 10.34.0305 SU4
09 LCOS improvements 10.34.0304 RU3
11 LCOS improvements 10.34.0168 RU2
12 LCOS improvements 10.34.0162 RU1
13 LCOS improvements 10.34.0100 Rel

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

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 10.34 SU6 , 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 https://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 version has been extensively and successfully tested in practice. It contains new features and improvements over previous LANCOM 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 LANCOM 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 10.34

LANCOM products regularly receive major firmware releases throughout their life-time 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 https://www.lancom-systems.com/products/firmware/lifecycle-management/product-tables/

Support for the following devices is no longer available as from LCOS 10.34:

- → LANCOM 831A
- → LANCOM IAP-322
- → LANCOM L-451agn
- → LANCOM L-452agn
- → LANCOM L-460agn
- → LANCOM OAP-3G

4. Advices regarding LCOS 10.34

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 10.34

5.1 Feature highlights 10.34

SD-WAN – Application Routing

Enjoy significant performance gains when you operate modern business applications in the cloud (e.g. Office 365, SalesForce, etc). SD-WAN Application Routing detects cloud-based applications and routes them directly to the Internet (local break-out). This relieves the VPN path to the headquarters as well as the headquarters' Internet line.

SD-WAN – Layer-7 Application Control in the firewall

Keep control of which applications can operate on your network. Defining application-related rules in the firewall allows you to decide which Internet applications are allowed, blocked, limited or prioritized.

WLC functions in the vRouter (vWLC)

You decide which role your LANCOM vRouter should play: VPN gateway or WLAN controller. The LANCOM vRouter now supports the role of a virtual WLC (vWLC). This fully virtualizes the functions of a WLAN controller on virtualization platforms such as VMWare ESXi or Microsoft Hyper-V. The number of managed access points depends on the vRouter license category.

5.2 Further features

Flexible and future-proof telephony at all locations

With the release version LCOS 10.34 you can now use your LANCOM routers with VoIP functionality in conjunction with a CompanyFlex line from Deutsche Telekom. This means that in the future you can combine all your previous telephone numbers in just one SIP line, even if they come from different previous ISDN connections. This means that you can continue to use your existing telephone system or terminal equipment while enjoying all the advantages of a new IP-based connection. In addition, you can flexibly integrate different company locations and allocate number blocks and services as required in all branches.

TLS 1.3

Support of the new TLS 1.3 protocol increases the security of device access via WEBconfig.

Elliptic Curve Digital Signature Algorithm (ECDSA)

IKEv2 now supports the Elliptic Curve Digital Signature Algorithm (ECDSA) authentication method. Shorter keys combined with high-efficiency encryption provide the same security.

IKEv2 split DNS

Split DNS allows DNS to resolve specific internal domains to a VPN tunnel, with other DNS requests using a public DNS server.

IKEv2 fragmentation

Fragmentation of IKEv2 messages (per RFC 7383) is handled by the VPN router itself, eliminating the need for the transport network to fragment IKE packets.

Enhanced client reservations in the DHCPv6 server

In the DHCPv6 server, client addresses or prefixes can now be assigned either by means of DUID, MAC address, interface ID (as per RFC 3315) or remote ID (as per RFC 4649).

Double the number of Public Spot users

For the LANCOM 178x and 179x series with the Public Spot Option, the number of users is increased from 64 to 128.

You can find further features within the individual builds sections in chapter 6 “History LCOS 10.34”.

6. History LCOS 10.34

LCOS improvements 10.34.03xx SU6

Bug fixes / improvements

General

→ A security vulnerability in the web interface has been fixed, which allowed unauthenticated attackers to cause an unexpected device restart (DoS attack) by sending a manipulated packet. This affected administrative access via WEBconfig from the LAN and the WAN (if management access via HTTP/HTTPS from the WAN was enabled), as well as the web services IPSec-over-HTTPS, SCEP, OCSP server/responder, and the Public Spot. In the default configuration, access to the router from the WAN is disabled, meaning the router was not affected by this vulnerability in such cases. The TR-069 protocol was also not affected by the vulnerability.

LCOS improvements 10.34.0308 SU5

Bug fixes / improvements

General

→ A vulnerability in the OpenSSL library has been fixed (CVE-2022-0778).

→ A vulnerability in the zlib library has been fixed (CVE-2018-25032).

→ The WEBconfig or TLS device certificate of a LANCOM device operated with LCOS was not automatically extended by the device beyond the expiration date in 2024.

LCOS improvements 10.34.0305 SU4

Bug fixes / improvements

General

→ If H.323 is enabled in the configuration (default setting), this will be disabled after an upgrade to LCOS 10.34 SU4. If the protocol is reactivated in the configuration, a message is generated in the syslog protocol.

LCOS improvements 10.34.0304 RU3

Bug fixes / improvements

General

→ In the table for entering services that can be used in the Bonjour proxy's network list, a comma was not accepted as a separator for multiple services.

→ The length check of ICMPv6 packets in the IPv6 firewall did not work correctly. This could cause ICMPv6 packets to be dropped by the router with the message "intruder detection".

→ The certificate management buttons were not displayed in WEBconfig. Thus, it was not possible to create a new certificate, revoke a certificate or declare a certificate as valid.

Wi-Fi

→ The IEEE 802.11u parameters 'Include-in-Beacon-OUI' and 'Additional-OUI' only allowed lowercase letters to be entered on the console. In LANconfig, however, uppercase letters were also allowed for these parameters. Upper case letters are now converted to lower case letters.

→ Due to an error in the management of 'Circuit IDs', Wi-Fi clients could experience login problems in a Public Spot scenario.

→ Changes in the 'E-mail domains' table in the 'Public Spot / E-mail' menu were not applied without restarting the device.

→ When managing Public Spot users via WEBconfig in the 'Setup Wizards / Manage Public Spot Users' menu, a message with the content "DataTables warning (table id = 'pbspotTable'):" could occur if a user's password contained a backslash character '\'.

VoIP

→ In an incoming SIP telephone call, the calling party (in this case the provider) represents the UAC (user agent client), and the accepting party (in this case the LANCOM router) represents the UAS (user agent server). If there is a change in negotiation (e.g. due to an UPDATE or RE-INVITE), the direction changes. The provider thus becomes the UAS and the LANCOM router becomes the UAC.
In the 'Session-Expires' header the calling participant tells how long the negotiated session may initially last and whether the UAC or the UAS will update the session (the 'refresher'). The 'refresher' usually remains the same (e.g. the provider), therefore the role changes from UAC to UAS and has to be adjusted in an UPDATE or RE-INVITE.
If an incoming call containing the 'Session-Expires' header with the 'refresher' UAC resulted in a change of codecs, the LANCOM router sent a RE-INVITE to the provider with the 'refresher' UAC contained in the initial 'Session-Expires' header instead of UAS. The LANCOM router would have had to send the 'refresh request' to the provider, but this is not intended. Thus no session refresh took place.
This caused the phone call to terminate after the 'Session-Expires' timer expired (e.g. after 30 minutes).

→ When forwarding calls via 'Semi-Attended Transfer' the router used placeholders for the 'Call-ID', the 'from' tag and the 'to' tag. As a result, the destination could not assign the call and aborted the call forwarding with the error message "481 Call Leg/Transaction Does Not Exist".

→ Incoming SIP update packets via SDP were answered by the LANCOM router without SDP. As a result, calls in connection with a downstream PBX failed.

→ If an incoming telephone call contained an 'UPDATE' in the Allow header, but this was no longer transmitted by the provider in the message "200 OK", the router sent an UPDATE to the provider instead of a RE-INVITE. This resulted in the telephone call being terminated by the provider.

LCOS improvements 10.34.0168 RU2

Bug fixes / improvements

VoIP

→ A LANCOM router used as Session Border Controller (SBC) did not perform call routing to an alternate line if the original line returned the error message “488 Not Acceptable”.

→ If a soft client is connected behind an Octopus Netphone PBX and makes an outgoing call, Netphone sends a “REFER” message to the LANCOM router when the call is accepted. However, the LANCOM router immediately responded with a “Re-Invite” to Netphone instead of first sending a “202 Accepted” to Netphone. As a result, a call did not come through.

→ If another update process was triggered by a CWMP server (CPE WAN Management Protocol) during a firmware update, this could mean that no running LCOS could be started after restarting the LANCOM router.

→ In a scenario in which a LANCOM router was used as a Session Border Controller (SBC), call forwarding to a mobile VoLTE could fail. As a result, the call was hung up on the VoLTE terminal device after acceptance.

→ For longer telephone calls (e.g. 15 minutes) the provider sends an UPDATE message to the Voice Call Manager. If the UPDATE message was forwarded to a connected SIP PBX, the Voice Call Manager did not count up a sequence number. The SIP PBX acknowledged this with the message ‘500 server internal error’.
This caused the call to be disconnected after the time (e.g. 30 minutes) stored in the ‘session-expire header’.

→ In a scenario with a Swyx / Netphone Media Bridge a Re-INVITE was sent to the provider during an outgoing call to a mobile phone subscriber of the Telekom (VoLTE) and was acknowledged by the provider with the message ‘491 Request Pending’. Due to an incorrect handling of the message ‘491 Request Pending’, the RTP data stream was interrupted after a short time and the telephone call was terminated.

LCOS improvements 10.34.0162 RU1

Bug fixes / improvements

General

→ Layer-7 application detection did not work if it was restricted to a specific VLAN via the associated VLAN table ‘Setup/Layer-7-App-Detection/VLAN’.

→ If automatic license activation was used on the command line, the process would remain in ‘Processing’ status after the command line command was entered. The respective license was not activated on the device.

VoIP

→ If immediate call forwarding was configured in the user settings of a SIP user and a ‘clip no screening’ phone number was specified as a user-defined, signaled phone number, the LANCOM router transmitted an incorrect signaled phone number.

→ If the router received DTMF tones during the ‘Early Media Phase’ and converted them into a SIP info packet, a new transaction ID was used. After successful completion of this transaction (200 OK) the transaction ID of the SIP info packet was used for the already existing INVITE transaction and for Provisional Responses. This caused the telephone call to terminate.

→ If the router received the message ‘491 Request Pending’ from the provider after a refresh request for the session timer, the call was disconnected instead of repeating or forwarding the refresh request.

→ The Voice Call Manager starts the RTP monitoring in the ‘Early Media Phase’. After the timer has expired, RTP monitoring is deactivated if RTP packets are detected. In this case, the Voice Call Manager expects an external ring tone. If the RTP data stream was interrupted, the Voice Call Manager did not recognize this and therefore could not generate a local ring tone.

→ Outgoing calls with suppressed phone number could not be set up because the call could not be assigned to a user.

→ For an incoming call with forwarding to a call group, the ‘Allow Header’ was removed from the router to the provider. This could cause some SIP phones to stop transmitting voice data and terminate the call if the SIP phone did not correctly support session timer renewal via REINVITE.

→ In a scenario with a Netphone PBX in bridge mode, a phone call was only possible with the codec G.711, although G.722 was used in the first Invite.

→ In a scenario with a Swyx PBX in combination with the CTI+ option, the call is first established with the CTI+ device and then forwarded to the target subscriber via a REFER. No ring tone was audible on the CTI+ device because the used codec (G.711 or G.722) was not negotiated correctly. Furthermore the LANCOM router sent a RINGING to the Swyx PBX after session progress, although the call was already established.
→ It could happen that the LANCOM router sent the flag 'Require: 100rel' to the provider in the '183 Session Progress' although the connected SIP participant did not support this and had not announced it in the RINGING. The SIP participant acknowledged this with the error message '500 Server Internal Error', which caused the telephone call to be aborted.
→ When the error codes SIP 403 or SIP 500 are received from the provider, the router automatically switches to another dynamic SIP line.

LCOS improvements 10.34.0100 Rel

New Features

→ Support for "Telekom Company Flex"
→ Calls can be dynamically distributed to multiple SIP lines.
→ The maximum number of parallel calls for one SIP line is now configurable.
→ Support for Early Media

Bug fixes / improvements

General

→ If a script which set a single value in a table row was transferred to a router by the rollout wizard, a sudden device restart occured.
→ Port forwarding did not work with the vRouter if a map port was used which did not match the specified port.
→ On a vRouter with configured port forwarding for TFTP GRE packets could not be allocated to the PPTP session. As a result, GRE packets were not forwarded and port forwarding for a PPTP connection did not work.
→ If the vRouter was operated on a Hyper-V system or Microsoft Azure, packet loss could occur when sending multiple big aggregated packets. Furthermore, a packet buffer was filled up and no longer cleared.
This could generally lead to transmission issues. Particularly on VPN connections the IKE negotiation and data transmission was faulty after some time.

VPN

→ If an IKE packet had to be retransmitted while negotiating IKE on a router, the router sent the message ‘ICMP port unreachable‘ immediately after retransmission.
The message ‘ICMP port unreachable‘ is no longer sent after a retransmission.

Wi-Fi

→ For all access points with IEEE 802.11ac Wi-Fi module the parameter ‘excessive retries’ has been added to the feature ’Adaptive RF Optimization’. If packets have to be transferred to the Wi-Fi device more than once, the access point recognizes this and thus can change the Wi-Fi channel.

VoIP

→ On devices of the 1783 series WEBconfig showed all analog- and dial interfaces for an analog user as selected, if the user entry was saved with the analog- and dial interface 2 only.

→ With Telekom VoIP connections it could happen that no “ring” was signalled on the line for fixed line calls initiated by SIP clients, because the provider sent a “Ringing” without Session Description Protocol (SDP). As a result, the call establishment remained unsignalled until call answering.

→ In a scenario with a SIP phone system connected by a gateway line the session ID in the SDP information was not increased by the LANCOM device. This resulted in phone calls being cancelled when the call was answered.

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.

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info@lancom.de | lancom-systems.com