Release Notes

LCOS SX

3.34 RU6

Table of contents

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.

LCOS SX 3.32 / 3.34 is the operating system for all LANCOM switches of the GS-1300 / GS-2300 series.

The LCOS SX 5.x operating system is available for all LANCOM switches of the XS series.
The LCOS 4.x operating system is available for all LANCOM switches of the GS-3000 series.
The release notes for these device series can be found as usual on the LANCOM website in the download area of the respective switch.

This document describes the new features of the LCOS SX software release 3.34 RU6 as well as the changes and improvements to the previous version.

Before upgrading your device to a new firmware it is essential to **backup your device's configuration**.
Due to extensive features it is **not possible to downgrade** to a previous firmware without using the backup configuration.
Please note that different firmware files might be available for your device.

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. Note on the firmware update

Never disconnect the switch from the power supply during a firmware update, as the device will not start properly if the update process is aborted.

Please make sure to **back up your configuration files** before updating your LANCOM devices to a new firmware version!
Due to the partly extensive feature enhancements, a **downgrade** to the old firmware is **no longer possible** automatically **without such a backup**.
Please note that different firmware files may be available for your device.

4. New features, improvements, and history

LANCOM GS-2300 series only:

Devices delivered with LCOS SX 3.30 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 at any time on the device's WEBconfig under > Configuration > LMC. You can manually re-enable the usage of the LMC whenever you want.

LANCOM GS-1300 / GS-2300 series improvements 3.34.0323 RU6

Bugfixes / improvements

→ A switch managed by the LMC with LCOS SX 3.34 RU5 and a static IP address could no longer contact the LMC after a rollout.

→ In the course of fixing the 'Terrapin' security vulnerability, the 'strict-kex' mode was introduced. Instead of negotiating this mode for each SSH connection individually, the switch used it for all connections. As a result, encryption negotiation was no longer possible for remote peers without strict-kex support and SSH sessions could not be established.

→ After an update to LCOS SX 3.34 RU5, it could happen that the switch generated an SSH key with the wrong size. This caused the SSH service to terminate and the switch to freeze.

LANCOM GS-1300 / GS-2300 series improvements 3.34.0320 RU5

Bugfixes / improvements

→ After a firmware update, the information of inserted SFP modules was no longer displayed in the configuration.

→ The maximum for processing 802.1X identities was 39 characters. This maximum has now been increased to 253 characters.

→ It could happen that a switch performed an unmediated restart when accessed via SSH.

→ After three failed ‘Auto Negotiations’, the port speed was set by the switch to a maximum of 100 Mbps (default setting) using a downshift function. In some scenarios, this caused negotiated faster port speeds to fall back to 100 Mbps, e.g. when a client was in standby mode. The downshift function can now be disabled with the command ‘downshift <port-list> disable’.

→ After a ‘DHCP Renew’, the switch disconnected all HTTP connections. In an LMC scenario, this also disconnected the connection to LMC monitoring, which led to an immediate restart of the switch.

→ In individual cases, it could happen in an LMC scenario that the switch did not send any monitoring data to the LMC.

→ When using the Hybrid tagging mode and ‘Port-based 802.1X’ on a port at the same time, the switch only learned the MAC addresses of the devices connected via the port for VLAN 1 (untagged VLAN). If a connected device in a tagged VLAN switched to another port secured by ‘Port-based 802.1X’ (e.g. by roaming to another access point), the switch was unable to correctly assign the MAC address to the new port. As a result, communication in the tagged VLAN no longer worked after changing the port.

→ A query carried out in WEBconfig for existing user profiles returned the password in plain text in addition to general user data. The password is now no longer sent.

→ The use of CBC encryption algorithms has been deactivated, which means that all 3DES encryption variants have also been deactivated.

→ The use of the hash algorithms

- diffie-hellman-group14-sha1,
- diffie-hellman-group1-sha1,
- hmac-sha1-96,
- hmac-sha1

has been deactivated.

→ A session cookie is set after a user logs in to the web interface. This incorrectly contained the user's login data (Base64-encoded).

→ The SSH service Dropbear has been updated. In the new version, outdated algorithms have been deactivated and security patches have been implemented.

- Support for the DSA (SSH-DSS) algorithm has been removed.
- Support for Diffie-Hellman group 1 has been removed.
- Support for SSH-RSA (SHA1) has been removed and replaced by SSH-RSA-SHA2-256.

→ The local user database now uses the Argon2 hash algorithm.

LANCOM GS-1300 / GS-2300 series improvements 3.34.0205 RU4

New features

→ Extension of the Radius Supplicant feature by a software switch that changes the MAC address used by the 802.1X Supplicant to the system MAC address. This simplifies the use of single and multi-auth modes.

LANCOM GS-1300 / GS-2300 series improvements 3.34.0204 RU3

New features

→ The LMC CLI and WebGUI tunnel has been added similarly to the other switch series.
→ The switch can now be authenticated as a ‘supplicant’ on the RADIUS server.
→ SYSLOG support according to RFC-5424 has been implemented.
→ SYSLOG messages now include the hostname instead of the IP address.
→ Access Control List entries can now be completely deleted via CLI command <delete all> in the ACL menu.

Bugfixes / improvements

→ Fallback from 802.1X authentication to MAC-based authentication failed when the client responded to the EAP requests with ‘EAP logoff’ packets to reject 802.1X authentication.
→ If an ACL rule (Access Control List) for IPv4 with frame type ‘255.255.255/32’ was created via the switch’s command line, this value was not accepted.
→ In syslog messages the IP address was displayed instead of the host name, which could make the exact identification of the device difficult. Now the host name is displayed.
→ When a LANCOM GS-2310x was supposed to authenticate as a RADIUS supplicant via its MAC address to a RADIUS server and the switch was connected via one of the combo ports, the switch counted up the MAC address on the combo ports. This resulted in an incorrect MAC address being reported to the RADIUS server and authentication failing.
→ A login via a CLI tunnel did not generate an entry in the syslog of the switch.
→ In scenarios where the switch was used as an authenticator, the RADIUS packet did not contain an IP address in the ‘NAS’ field after a switch reboot. As a result, the authenticated clients did not receive an IP address.
→ The automatic refresh of the configuration interface was functionless and could not be deactivated after an activation.

LANCOM GS-1300 / GS-2300 series improvements 3.34.0101 RU2

New features

→ RADIUS MAC address bypass / fallback has been added - e.g. if 802.1X authentication is rejected, the MAC-based request is sent after an optionally definable waiting time.

→ RADIUS assigned VLANs are now also supported for multi-client modes ‘Multi 802.1X’.

Bugfixes / improvements

→ The port configuration of a ‘Mac-based Single’ client authentication in combination with port security could lead to an endless boot loop of the switch, which could only be fixed by pulling the connection cable to the client.

LANCOM GS-1300 / GS-2300 series improvements 3.34.0006 RU1

Bugfixes / improvements

→ After a reboot, the switch did not forward the VLAN tags for a short time. This meant that network subscribers connected to an ‘access’ port were briefly assigned an IP address from the untagged management network via DHCP. An IP address from the correct network was only assigned after the DHCP lease expired.

LANCOM GS-1300 / GS-2300 series improvements 3.34.0003 RelI

New Features

→ The Spanning Tree Protocol (STP) can now be configured from the LMC.

→ The persistent event and boot logs can be erased from the debug menu (debug; erase persistent-logs).

→ In the IP Source Guard configuration, a ‘mouseover’ in the description column provides convenient port detail information.

Bugfixes / improvements

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

→ A vulnerability in the zlib library has been fixed(CVE-2018-25032).
When using 802.1X with ‘MAC-based Auth.’ authentication mode, the ‘RADIUS-Assigned VLAN Enabled’ feature could not be enabled.
A new authentication mode ‘MAC-based single Auth.’ has been implemented which allows the use of the ‘RADIUS-Assigned VLAN Enabled’ feature.

→ If a Sunday was specified as the time changeover day in the time changeover configuration (CET/CEST), the switch displayed an incorrect time after the time changeover if an NTP time server was set as ‘Clock Source’.

→ The OID value ‘Serial’ was output with the incorrect value ‘System MAC: <MAC address>’ in monitoring tools.

→ When transmitting LLDP data, the IP address was missing in the ‘Management Address IPv4’ value. The address 0.0.0.0 was always entered there.

→ When specifying the firmware information in the LMC in the menu ‘Devices / <device name> / System information’, the switch only transmitted the version information. However, the date information behind the version number was missing.

→ When the firmware is upgraded to LCOS SX 3.34 RelI, new RSA SSH host keys are automatically generated in the switch configuration.

→ When using protocols with port-bound packets (e.g. STP or LLDP), a GS-2300 series switch used its management MAC address instead of a separate MAC address per port.

→ If the syntax in the switch configuration was not specified correctly and the configuration was uploaded to the switch, this could lead to an immediate restart of the switch. An error message was not issued in this case.

→ When importing a switch configuration, it is first checked for syntax errors and then read in. However, the PoE tree was read in directly without performing a syntax check. This could lead to an incorrect PoE configuration.

→ A scan with a vulnerability scanner could lead to crashes of individual processes of an SSH service. The switch could then no longer be reached via SSH.

→ When using DHCP snooping and simultaneously configuring LACP or spanning tree on the trusted ports, DHCP packets were sent on all trusted ports and thus duplicated or even multiplied. This could lead to DHCP flooding in the network.

→ Individual functions require certain privileges for editing ('Privilege Level'). The settings for the 'Easyport' function could not be edited with a user with 'Privilege Level' 12, but only with a user with Level 15. Furthermore, the configuration of the 'LLDP-MED' function required a user with Privilege Level 6 (same level as the 'LLDP' function) instead of Privilege Level 5.
When using DHCP option 43 in the network with a 'Value Size' larger than 127 bytes, the switch could not process the DHCP packets correctly and therefore could not obtain an IP address via DHCP.
DHCP packets with option 43 can now be processed up to a size of 255 bytes.

→ If configuration changes were made via WEBconfig or command line during a firmware update, the switch started with the new firmware after the update, but without the changed configuration. It is now no longer possible to make configuration changes during the firmware update.

→ In the configuration of a switch name, any configured name was always prefixed with "LANCOM-".

→ If single authentication with active guest VLAN was configured on a switch port, the switch placed the clients without authentication into the appropriate VLAN for the guest network according to the MAC table, but the clients did not receive an IP address via DHCP.

→ When multiple clients are connected on an 802.1X multi-client port, the last client seen determines whether broadcasts are allowed on the port. However, if the last client seen was one that was not allowed on the port, the switch turned off broadcasts on the port.

→ In the RADIUS server table, only one IP address could be entered in the 'Hostname' field.

Only GS-2300 series:

→ If a password with 32 characters was configured for the switches of the GS-2300 series, it was no longer possible to log in to the WEBconfig of the switch with this password. In the LMC, a password with 32 characters caused an error message to be displayed when the detailed configuration was called up and the detailed configuration could no longer be used.

→ The console command ‘startlmc’ can be used in LCOS to pair with the LMC by specifying the serial number and the cloud pin. When executing the command ‘startlmc’ on LCOS SX, an activation code from the LMC was also requested by mistake.

→ With the sFlow function, the switch sent only ‘counters sample’ packets and no ‘flow sample’ packets when the mode option was enabled (status: enabled). As a result, information gaps could occur when monitoring the devices with monitoring tools from other manufacturers (e.g. PRT).

→ It could occasionally happen that the pairing process of a switch with the LMC or the rollout process of a configuration by the LMC to the switch failed due to an incorrect parameter, although this parameter was not configured on the switch. In this case, the error message “Not accepted” was output in the LMC.
As of LCOS SX 3.32 RU7, the service type ‘Call-Check’ is used for authentication requests to switch ports.
According to best practice in RFC 3580, the service type ‘Framed’ is now used for ‘802.1X’ requests and the service type ‘Call-Check’ for ‘MAC-based’ requests.

→ On LANCOM GS-2300 series switches, the Telnet protocol is now disabled by default in the factory state.

→ In the swich port configuration, it is now possible for a voice VLAN and MAC-based authentication to be routed over one port to clients in two different VLANs.

→ The boot log as well as the event log could not be deleted. This could cause the logs to become very large and slow to load.
The logs can now be deleted on the console in the debug menu (debug) with the command ‘erase persistent-logs’.

LANCOM GS-1300 / GS-2300 series improvements 3.32.0222 RU7

Bugfixes / improvements

→ With MAC-based 802.1X authentication against a RADIUS server, a client was authenticated although the RADIUS authentication was answered with a 'RADIUS Reject' and 'EAP Success'. However, the 'Success' type EAP packet only refers to successful EAP communication.

→ The switch only interpreted the EAP part, but not the contents of the RADIUS packet (the 'RADIUS Reject'). Therefore a client that was not known on the RADIUS server was also successfully authenticated.

→ The switch is now able to transmit the RADIUS attributes 'NAS Identifier' and 'Service Type=Call Check'.

→ The maximum length of an SSH hostkey has been extended from 1024 bits to 2048 bits.

→ A MAC-based 802.1X authentication against a RADIUS server was passed as a RADIUS request without EAP components and with the MAC address as user name.

→ When using 802.1X authentication with the 'Single 802.1X,' 'Multi 802.1X' and 'MAC-based Auth.' modes, the MAC addresses were not transferred to the MAC address table after the terminal devices successfully logged in.

LANCOM GS-1300 / GS-2300 series improvements 3.32.0221 SU6

Bugfixes / improvements

→ Special user input via the web interface was not validated correctly. This could provoke a sudden restart of the device.

LANCOM GS-1300 / GS-2300 series improvements 3.32.0210 RU5

Bugfixes / improvements

→ When operating LANCOM switches of the GS-1300 / GS-2300 series, it could happen that devices lost their serial number and MAC address after a restart and were also unable to obtain an IP address. The devices continued to operate, but the affected switches could no longer be reached via their IP address.

LANCOM GS-1300 / GS-2300 series improvements 3.32.0208 RU4

New features

→ In the ‘Authentication Method Configuration’ it is now possible to configure the protocols HTTP and HTTPS separately.

→ Simplification of the VLAN port marking

→ A warning is now displayed in the ‘System Log Configuration’ for insecure ‘SNMPv2 Get community’ configuration.

Bugfixes / improvements

→ The passwords stored in the configuration files are now stored encrypted.

→ When using 802.1X with the ‘Mac-based Auth.’ authentication mode, the ‘RADIUS-Assigned VLAN Enabled’ feature could not be enabled.

→ A new ‘MAC-based single Auth.’ authentication mode has been implemented to allow the use of the ‘RADIUS-Assigned VLAN Enabled’ feature.

→ Although access to the web interface was blocked in the configuration, the login page of the web interface was displayed when an access attempt was made. However, a login was not possible.

→ After disabling ‘Web’ in the ‘Authentication Method Configuration’, port 80 was displayed as open, but access to the web interface was not possible.

→ When using the feature ‘Port Based 802.1X’ and the VLAN mode ‘Trunk’ a connected device could be authenticated, but a data transmission was not possible.

→ If a Voice VLAN was configured on the switch, the MAC address of individual connected network devices was sporadically no longer included in the MAC address table after the ‘Voice VLAN Aging Time’ had expired. This caused these devices to no longer being able to communicate in the network. Only devices in VLANs that did not correspond to the Voice VLAN were affected.

→ When setting a static MAC table entry in the menu ‘Filtering Data Base / Configuration‘, the switch restarted abruptly.

→ If a port-based VLAN was configured and an additional configuration for MAC-based VLAN was added, only the MAC-based settings worked; the advanced settings were ignored.

→ The ‘Limit Control’ function in the ‘Security / Port Security’ menu could only be activated via the web interface. If an attempt was made to activate the function via the console, the error message “Port Security Limit Control Configuration of easyport must be preserved” was displayed.

→ **GS-2300 only:** In the SNMP MIB of a LANCOM GS-2310(P)(+), 13 ports were listed in the LLDP tree when LACP was active, although the switch only has 12 ports.

→ **GS-2300 only:** The (admin) password, user name and privilege level could not be configured via SNMP using the existing admin account.

→ **GS-2300 only:** On the console, there was no way to enable multiple protocols to access the switch simultaneously (e.g. SNMP & TELNET/SSH). Either all protocols could be activated at once or only one protocol could be activated.

LANCOM GS-2300 series improvements 3.32.0135 SU3

Bugfixes / improvements

→ The random generator for generating SSH keys did not generate enough different host keys.

To make sure that after upgrading to firmware LCOS SX 3.32 SU3 enough different SSH host keys are available in the switch, you need to do the following:

- Open the switch’s web interface.
- Navigate to the menu ‘Security / SSH’.
- Click on the button ‚Regenerate hostkey‘.
- In the menu ‘Maintenance / Save/Restore‘ save the configuration with the option ‘Save Start‘.
- Restart the switch with the option ‘Maintenance / Restart Device‘.

New SSH host keys are generated when the switch is restarted.

See also https://support.lancom-systems.com/knowledge/x/AoCCAg.

LANCOM GS-2300 series improvements 3.32.0114 RU2

Bugfixes / improvements

→ Switches which were connected to the LANCOM Management Cloud (LMC) could in seldom cases experience an SSL connection error which resulted in devices which could no longer be managed by the LMC. Only the monitoring was functional.

→ If the LANCOM switch detected a network loop, until now only the timestamp and blocked port have been logged to a syslog message. The network loop detection now additionally logs the number of the second involved port, and also shows an information about which port was the sender and which one was the receiver of the loop protection frame.

LANCOM GS-1300 / GS-2300 series improvements 3.32.0110 RU1

New features

→ Extension of the device logs

→ Extension of PoE Detection (Legacy Mode)

→ New switch for sFlow (Always On)

Bugfixes / improvements

→ The LANCOM switches transmitted MAC addresses (e. g. from supplicants with 802.1X on a RADIUS server) exclusively using small letters (e. g. 00-10-a4-23-19-c0). However, according to RFC-3580, upper case letters must be used (e.g. 00-10-A4-23-19-C0), which is now the case.

→ The automatic conversion of the time to Central European Summer Time (CEST) was one week too early.

→ Due to a too small internal data buffer, too large TLV (Type-Length-Value) packets were discarded. As a result, the authentication of a client via 802.1X to a RADIUS server failed.

→ If the web interface of the switch was prompted via an IPv6 address, the online help display did not work.

→ **GS-2300 only:** If a fixed IP address was assigned to a switch managed by LMC using an add-in script, this resulted in a sudden restart of the switch.

→ **GS-2300 only:** If you created a script saving from a switch of type LANCOM GS-2352x, in which a PVID is entered for 26 ports, this script saving could not be loaded into the device.

- → **GS-2300 only:** If the LLDP function was used for automatic device recognition on a LANCOM GS-2300 series switch managed in the LMC, the switch could restart abruptly.
- → **GS-2300 only:** A ping to the IP address of a GS-2352(P) was not answered by the switch if a management VLAN other than 1 was used.
- → **GS-2300 only:** When transferring a GS-2300 to the LANCOM Management Cloud, “Forbidden VLANs” were not transferred to the LMC configuration.
- → **GS-2300 only:** Debug information for analyzing a sudden restart (“watchdog”) could not be read out completely via SSH and Telnet.
- → **GS-2300 only:** An open SSH, Telnet or Web session on a switch managed via the LMC was not terminated immediately if a new main device password was rolled out to the switch via the LMC.
- → **GS-2300 only:** A reboot event triggered via SNMP or the LMC was not written to the syslog.
- → **GS-2300 only:** The pairing of a switch with the LMC via LANconfig using an activation code was not successfully completed. As a result, the switch was in an endless loop. The identical process via the web interface or the claiming via PIN, however, worked.
- → **GS-2300 only:** The configuration item “Unregistered ICMPv6 Flooding” under MLD-Snooping was without function on models of the GS-2328 and GS-2352 series.
- → **GS-2300 only:** A faulty sFlow configuration caused a switch to send “Counter Samples” instead of “Flow Samples” after some time and the sFlow Collector no longer received any data.
- → **GS-2300 only:** A GS-2310(P) provided the same port ID for both CU and SFP ports 9 and 10 when queried via SNMP. Now the port IDs 9A and 10A for the CU ports and 9B and 10B for the SFTP ports are delivered.

LANCOM GS-1300 / GS-2300 series improvements 3.32.0012 Rel

New features

→ For SSL and TLS configurations, the minimum SSL and TLS versions to be applied are now selectable from a drop down list.

→ Added a hint for a not yet saved configuration to the configuration interface

→ **GS-2300 only:** Scripting ability via the LANCOM Management Cloud

Bugfixes / improvements

→ If STP was activated on the switch ports, and this configuration was saved as “Start configuration”, it could happen that after a cold boot the displayed uptime value in the menu “configuration > port status” was stated with 2627 days.

→ When saving a configuration to an *.xml file, PoE configuration parameters for “Power delay”, “Auto checking” and “Scheduling” were missing.

→ Switch ports with configured 802.1X Single-/ multi mode port authentication were blocked after 4-6 minutes and re-released after a further 4-6 minutes. The port status was always (even with blocked status) shown as “Authorized”.

→ In the web configuration the error string of an error message was not scaled to the size of the message area.

→ Descriptions for configuration options for individual switch types were missing in the online help for the function “Configured link speed” (in the menu “Port configuration”).

→ When using the function MAC-based authentication for connected access points, a change of the switch ports due to Wi-Fi roaming caused a sudden switch restart, if the MAC address of the Wi-Fi clients was deposed on the RADIUS server.

→ When using multiple switches with activated RSTP in a ring structure, and simultaneously activated DHCP snooping 100% CPU load was generated on a big amount of clients (more than 500).

→ General stability improvements

→ **GS-2300 only:** A main device password which was configured via the LANCOM Management Cloud was not included in an *.xml configuration file export.

→ **GS-2300 only:** No online help was available for the switch’s system information “LMC pairing state”, “LMC control state”, “Largest free mem block”, and “Free memory”, as well as for the functions “Configuration save” and “Configuration upload”.

→ **GS-2300 only:** The automatic completion of “show” commands using the tab key failed on the command line due to the spelling of the command “show-3rd-party-licenses” for all managed switches.

→ **GS-2300 only:** It was possible that no ICMPv6 packets were transmitted on particular ports of the GS-2352x switches.

→ **GS-2300 only:** Communication problems with IPv6 packets could occur with activated MLD snooping, if the network connection to the client was cut and reconnected afterwards. A high amount of packet losses could occur when using IPv6, too.

5. Common 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.

Support notes & known issues

Latest support notes and known issues regarding the current LCOS SX version can be found in the download area of our website: Common support hints

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

LANCOM, LANCOM Systems, LCOS, LANcommunity and Hyper Integration 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. 04/2024