Release Notes

LCOS FX
11.1 RU4

Table of contents

02 **1. Preface**

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

03 **3. Supported hardware**

04 **4. History LCOS FX**
04 LCOS FX improvements 11.1 RU4
05 LCOS FX improvements 11.1 RU3
06 LCOS FX improvements 11.1 RU2
08 LCOS FX improvements 11.1 RU1
10 LCOS FX improvements 11.1 Rel
12 LCOS FX improvements 11.1 RC1

14 **5. Further information**

14 **6. Disclaimer**

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 software release LCOS FX 11.1 RU4.

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. Supported hardware

Version 11.1 RU4 supports the following hardware appliances:

→ LANCOM R&S®Unified Firewalls
UF-50/60/60 LTE/T-60/100/160/200/260/300/360/500/760/900/910/1060
→ R&S®UF-50/100/200/300/500/800/900/1000/1200/2000
→ R&S®UF-T10
→ R&S®UTM+100/200/300/500/800/1000/2000/2500/5000
→ R&S®NP+200/500/800/1000/2000/2500/5000
→ R&S®GP-U 50/100/200/300/400/500
→ R&S®GP-E 800/900/1000/1100/1200
→ R&S®GP-S 1600/1700/1800/1900/2000
→ R&S®GP-T 10

Version 11.1 RU4 supports the following virtual appliances:

→ LANCOM vFirewall S, M, L, XL
→ R&S®UVF-200/300/500/900

Version 11.1 RU4 supports the following hypervisors:

→ VMware ESXi
→ Microsoft Hyper-V
→ Oracle VirtualBox
→ KVM

4. History LCOS FX

LCOS FX improvements 11.1 RU4

Bugfixes

→ Each time Let's Encrypt certificates were renewed, a new log file was created instead of overwriting the existing one.
Now only one log file is created and overwritten if necessary.

→ For LTA users who were to be assigned exactly 128 authorization profiles, the assignment of the authorization profiles failed. This meant that access to the assigned resources was not possible.

→ When rolling out networks and IPSec connections via the LMC, a rule was created in the nftables chain 'forward.prefilter.ipsec' for each combination of source object, target object, and protocol. If a large number of networks were rolled out, this led to a significantly increased CPU load during data transmission via the Internet connection, which resulted in a significantly reduced transmission speed.

→ The 'gpNetworkd' service created a new iptables rule each time a connection was established, even if it already existed. If the Internet connection was repeatedly established and terminated (e.g. when flapping), this could lead to a significantly increased CPU load by the 'ksoftirqd' service.

→ After an update to LCOS FX 11.1 Rel, the service for the HTTPS proxy (Squid) could crash when URL Sanitize or Safesearch was active. This meant that websites could no longer be accessed until the HTTPS proxy was restarted.

LCOS FX improvements 11.1 RU3

New features

→ The Voice-over-IP helper is now configurable.

Bugfixes

→ After updating to LCOS FX 11.1 RU1, every time an IPSec connection was established or terminated (including rekeying), all rules for incoming data traffic (nftables input rules) were reloaded. This caused packet loss and high CPU load, resulting in performance degradation.

→ If the firewall's antivirus function was active but the antispam function was deactivated, antivirus definition updates were performed successfully. However, the web interface permanently displayed the message "Running" under "Updates."

→ In some cases, not all warning messages from the alarm log appeared in the LMC API and the SIEM service (Security Information and Event Management). As a result, these messages were not forwarded to the SIEM system.

→ When using PPPoE or WWAN connections, DHCP leases were sometimes not transmitted to the LMC and thus not displayed there.

→ In LCOS FX 11.1 RU2, the VoIP helper was introduced and always active by default. In scenarios where SIP devices (e.g., PBXs or SBCs) used their own NAT helpers, this could lead to issues with SIP signaling or voice transmission. The VoIP helper is now deactivated by default and can be enabled if needed in the "Advanced Settings" menu.

→ After updating to LCOS FX 11.1 RU2, the IPv4 address was either not forwarded or forwarded with a significant delay to the DynDNS service of the LMC. As a result, access via the DynDNS name (e.g., an incoming VPN connection) was either not possible or only possible after a delay.

LCOS FX improvements 11.1 RU2

New features

→ Support for the LANCOM R&S®Unified Firewall UF-560

→ The firewall sends the reason for the last restart to the LMC so that it appears in the LMC device logs.

Bugfixes

→ After updating to LCOS FX 11.1 RU1, a LANCOM R&S®Unified Firewall UF-50 could not establish a connection to the LMC.

→ With enabled Application Filter and activated logs in the LANCOM R&S®Unified Firewall, no statistics were kept or log entries created.

→ If a DHCP relay was deleted on a LANCOM R&S®Unified Firewall, this was displayed correctly in the web interface; however, the entry was still present in the backend.

→ After an update to LCOS FX 11.1 Rel, the 'Wake on LAN' function, which is provided for certain users via the Unified Firewall, could no longer be used. Users were also no longer able to log in correctly to the internal portal and a connection error was displayed.

→ If the mail proxy was used in LCOS FX 11.1 Rel or LCOS FX 11.1 RU1, the address filter 'Whitelist' in the mail filter settings had no function.

→ When using the whitelist for the mail proxy, e-mails were also sent that were not included in the whitelist.

→ The antivirus service (bdamserver) saved information in a single log file instead of saving it in another log after reaching a certain file size and compressing the old log (logrotate). This resulted in the log file becoming very large after some time.

→ Members of a host group on the desktop were displayed twice under 'Additional objects', whereby the UUID was displayed as the name for the duplicate entries.

→ User-defined services were not displayed in the desktop configuration of the executive report. This also applied to user-defined objects that were created in the LMC.

→ If the API documentation of the Unified Firewall was to be called via an LMC web tunnel, an error message occurred and the API documentation was not displayed.

→ Checking an IPv6 Internet connection with the 'curl' application did not work.

→ Licensing of a vFirewall which was installed on a kernel-based virtual machine (KVM) from the manufacturer Hetzner, could not be carried out because the system did not generate a serial number for the firewall.

→ A WAN connection test with type ‘tcp_probe’ or ‘tcp_probev6’ and the preset default arguments (53 8.8.8.8 or 2001:4860:4860::8888) did not work.

→ In a scenario with traffic shaping, in which limits were specified for the WAN interface, it could happen that a configured outbound download limit for a client was not observed and as a result an unlimited download was used.

→ In a scenario with traffic shaping, two WAN connections and rule-based routing for HTTP and HTTPS traffic, it could happen that an incorrect limit value was used for the HTTP traffic of a client via the second WAN connection.

→ When creating an IPv6 connection to a VLAN interface, an error message appeared during interface selection stating that the selected connection type was invalid.

→ There were duplicates of some parameters in the ‘openapi.json’ file, which could lead to problems when using the OpenAPI command line or OpenAPI diff tools.

→ If the ‘HAProxy’ service was not configured, it could happen that it restarted regularly.

LCOS FX improvements 11.1 RU1

New features

→ **TCP Load Balancer**

TCP load balancers can be used to distribute any TCP connection to several backend servers behind the firewall. Thanks to active server monitoring, connections are only ever forwarded to functional servers.

Bugfixes

→ After an update to LCOS FX 11.1 Rel, the Unified Firewall used port 0 instead of the standard port 22 for the automatic backup via SCP. As a result, the automatic backup no longer worked.

→ If a network was created that should use a GPON interface, an error message was displayed when selecting the interface, stating that the selected interface was already being used in a bridge. As a result, no connection could be configured.

→ If a static IPv6 WAN connection was active on a Unified Firewall, the DNS function no longer worked for DHCPv4 connections configured on the same interface.

→ In LCOS FX 11.1 Rel, it could happen that a timeout occurred when creating a reverse proxy entry with LetsEncrypt when creating the LetEncrypt certificate. This could also occur when renewing a certificate via the web interface.

→ If there were a large number of entries in the reverse proxy list and these were made available via the external web interface, some entries could not be displayed there because scrolling was not possible.

→ The LMC device certificate saved during the backup of an LMC-managed Unified Firewall is only transferred during the re-import if there is no LMC device certificate in the Unified Firewall.

→ After updating to LCOS FX 11.1 Rel, the data of the updated device was no longer displayed in the Command Center.

→ No default route was created for a configured DHCPv6 WAN connection. As a result, the connection was not functional.

→ After setting up an Internet connection with IPv6 and address assignment via DHCP, the default route was no longer available after restarting the Unified Firewall. As a result, communication with the Internet via IPv6 was no longer possible.

→ Groups that contained other groups with users (nested groups) were not supported by the SAML implementation and could therefore not be synchronized.

→ When assigning a VLAN interface to a DHCPv6 connection, the error message “The connection type is invalid for the selected interface.” was displayed. As a result, the connection could not be saved.

→ If a user tried to access the stored website without authorization for the reverse proxy frontend, a redirect to the login page took place. The login page was reloaded again and again.

→ If the ‘Synchronize now’ button was clicked after configuring the SAML parameters without first saving the configuration, this had no effect.
By clicking on the ‘Synchronize now’ button, the configuration is now validated and saved and the synchronization is then carried out.

→ On a LANCOM Unified Firewall UF-60 LTE it could happen that processes were not terminated correctly and the memory was not released. This led to an immediate restart of the Unified Firewall.

→ The encryption algorithms used in the security profile ‘LANCOM LCOS Default IKEv2’ did not match the default settings in LCOS. As a result, when using this profile, VPN connections with LANCOM routers with LCOS and with the LANCOM Advanced VPN Client did not work or the connection was interrupted.

→ If a DHCP relay sent data via a VPN connection whose Internet connection obtained the IP parameters via PPP, the DHCP relay no longer worked after a restart of the Unified Firewall.

→ In a shaping configuration for traffic shaping, entered values were displayed multiplied by 1000 after saving (e.g. 5 Mbit entered, 5,000 Mbit displayed). This was merely a display error.

→ If the option ‘Block incorrectly scanned files’ was active in the antivirus settings (default setting), it could sporadically happen that even correctly scanned websites without malware were blocked by the antivirus engine. The error message “The request has been blocked. The requested URL could not be retrieved due to an anti virus engine failure.” was displayed.

LCOS FX improvements 11.1 RelI

Improvements

→ In addition to traffic groups, traffic shaping can also be set directly for source interfaces.

→ Performance optimization of the reverse proxy

→ The engine for application filter and application-based routing recognizes doctolib.

Bugfixes

→ In the alarm and system log of the firmware version LCOS FX 11.1 RC1, the name of the detected virus was not displayed in an antivirus incident.

→ If the antivirus option ‘Block files if scan fails’ was deactivated in firmware version LCOS FX 11.1 RC1, password-protected files were still blocked by the Unified Firewall.

→ On the notification page for a detected virus, the name of the detected virus was not included for firmware version LCOS FX 11.1 RC1.

→ After renaming a VPN SSL connection, the ‘Activate’ button in the menu bar of the Unified Firewall was not colored blue.

→ No description text was displayed in the host / network groups in firmware version LCOS FX 11.1 RC1 if objects were added that were not in the list.

→ After a Unified Firewall was reset to factory settings via the web client, no more settings could be made in the LetsEncrypt configuration dialog.

→ In LCOS FX 11.1 RC1, not all buffer contents were taken into account for IDS / IPS. As a result, some data traffic was not checked by IDS / IPS.

→ The IP protocols 61, 63, 68, 99, 114, and 253 have not been assigned a name in the user-defined services. Furthermore, a manually entered service name was not transferred to the menu bar.

→ A proxy exception configured in LCOS FX 11.1 RC1 for a specific website in a routing profile for application management was not applied. This resulted in the website being blocked by the content filter.

→ It was not possible to create an additional administrator in the Unified Firewall via an LMC add-in. The rollout was acknowledged with the error message “None Type has no attribute username”.

→ If the ‘suricata’ service (responsible for the IDS / IPS) was terminated abruptly, local services such as DNS could be accessed and used externally.

→ An IPv6 address stored in LCOS FX 11.1 RC1 for the default gateway was not displayed in the status information of the Internet object.

→ When using the HTTP(S) proxy with activated Antivirus, it could happen sporadically that websites were blocked.

It is now possible to activate an automated restart of the HTTP(S) proxy at midnight via script. Please contact LANCOM Support to receive the script file.

→ When creating a management report with the Unified Firewall, the number of packets blocked by IDS / IPS was not displayed graphically in the diagram.

→ If a DHCP relay server was stored for an interface on a Unified Firewall and then another entry was stored for another interface with a different DHCP server, only the new entry worked.

→ If a user-defined service was created in firmware version LCOS FX 11.1 RC1 and only one source port was to be specified, this did not work if only a port number was entered in the ‘Source port from’ field and the ‘To’ field remained empty.

→ No host names could be stored in the DNS server settings. As a result, it was not possible to store the host name ‘wlc-address’, for example.

→ If the reverse proxy was very heavily utilized, it could happen that the reverse proxy stopped forwarding packets after some time.

→ The SSO client (Single Sign On) could no longer connect to the Unified Firewall with LCOS FX 11.1 RC1 because port 6789 was blocked by the packet filter. As a result, Single Sign On no longer worked.

→ In the LCOS FX 11.1 RC1 firmware, the mail proxy did not work with the default certification authority.

→ With LCOS FX 11.1 RC1, it could happen in an HA cluster that the PostgreSQL database on the backup firewall was no longer functional. This caused the synchronization of the log database between the master and backup firewall to stop. Furthermore, the hard disk of the backup firewall was filled up.

LCOS FX improvements 11.1 RC1

New features

→ **IPv6 WAN**

The firewall can be operated on pure IPv6 connections or mixed IPv4/IPv6 connections. IPSec VPN tunnels and Wireguard VPN tunnels can be set up via IPv6. In addition, reverse proxy frontends can be offered via IPv6 and the firewall's web client and SSH can be accessed via IPv6.

→ **SAML authentication**

In addition to local users and the LDAP connection, the firewall can use SAML authentication to authenticate users for user- or group-specific rules. Keycloak and Microsoft Entra ID are supported as IDP.

→ **Reverse proxy authentication**

Services offered by the firewall via the reverse proxy can be restricted to certain users or groups. Local as well as LDAP and SAML users and groups are supported.

→ **HA cluster handover in the event of a network interface failure**

If a network interface on the active cluster node fails, the other firewall takes over, provided the interface on the second machine is working.

→ **New anti-virus engine**

Bitdefender will be used for the anti-virus functionality, as it has already been for anti-spam and Content Filter.

→ **REST API documentation via OpenAPI**

The REST API of the configuration interface is documented using OpenAPI. The documentation can be viewed live via the browser.

→ **Support for general IP protocols**

With user-defined services, it is possible to create services for any IP protocols.

→ **User-defined services with restriction of the source port**

With user-defined services, it is also possible to restrict the permitted source ports for TCP- or UDP-based services.

Improvements

→ The UF-260 supports the GPON module LANCOM SFP-GPON-1.

→ On the 'rules' desktop, groups can refer directly to network and host objects in order to avoid double configuration of IP addresses.

→ The reverse proxy now supports websockets.

→ A timeout towards the backend server can be configured for the reverse proxy.

→ HostHeader Preservation can be configured for the reverse proxy.

→ Any ACME server is supported.
→ It is possible to bind reverse proxy frontends to Wireguard connections.
→ It is possible to bind the external portal to Wireguard connections.

Further information

→ The VoIP proxy has been removed.
→ The import of configuration backups is only supported from version 9.8.
→ Please note that the reverse proxy is not included in a Basic license. Use of the Reverse Proxy within the Basic license is therefore outside the contractual scope of the license. As of version 11.1, it will no longer be possible to use the Reverse Proxy with the Basic license. Please perform an upgrade to a Full license in time, so that the Reverse Proxy can still be used.
→ The Outlook Anywhere option of the reverse proxy has been removed, as it is no longer required for current Microsoft Outlook / Exchange versions.

Bugfixes

→ A user with “Read-Only” authorization could not export the backup or a VPN-SSL connection.
The export of the backup and the export of a VPN SSL connection is now also possible with “Read-Only” authorization.
→ If a Unified Firewall with active IDS/IPS was shut down unexpectedly (e.g. due to a power failure), the connection tracking service (conntrackd) could no longer start. As a result, IDS/IPS no longer functioned. Furthermore, a sudden restart could occur when IDS/IPS tried to access the connection tracking service.
→ The Netfilter service (nftd) tried to write the firewall rules again and again, which resulted in increased RAM utilization. This could also lead to firewall rules not being written.
→ When using multi-WAN weighting with multiple Internet connections, the Internet connections were not prioritized correctly and the majority of traffic was sent over the connection with the lower weighting.
→ In an HA cluster, sporadic packet losses could occur during communication via the firewall.

5. Further information

→ Backups of versions 9.8 und 10.X are supported.
→ Devices with less than 4 GB of RAM can not execute all UTM features simultaneously.

6. 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.

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