Release Notes

# LCOS FX
## 11.2 RU2

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.

This document describes the innovations within software release LCOS FX 11.2 RU2.

## 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 11.2 RU2 supports the following hardware appliances:**

→ LANCOM R&S®Unified Firewalls
UF-50/60/60 LTE/T-60/100/160/200/260/300/360/500/560/760/900/910/1060
→ 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 11.2 RU2 supports the following virtual appliances:**

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

**Version 11.2 RU2 supports the following hypervisors:**

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

# 4. History LCOS FX

## LCOS FX improvements 11.2 RU2

### New features

→ LCOS FX now supports the OSPF protocol for dynamic routing.

## LCOS FX improvements 11.2 RU1

### Bugfixes

→ If the `x-lmc-configd.json` file contained UUIDs for non-existent desktop connections, a configuration rollout via LMC would fail.

→ In the LMC device overview, no information about the Internet connection was displayed if a PPPoE or mobile connection was configured on the Unified Firewall.

→ If the Let's Encrypt certificates for the reverse proxy could not be generated correctly, the reverse proxy would not function. Furthermore, in this case, the reverse proxy frontends could no longer be deactivated.
In such cases, the faulty certificate is now deleted and regenerated.

→ A SAG (Secure Application Gateway) license could not be activated on a Unified Firewall running LCOS FX 11.2 REL.

→ Certificates without the 'basicConstraints' attribute could not be imported into the Unified Firewall.

→ If an additional VPN tunnel was rolled out via LMC to a unified firewall with many configured VPN tunnels, this could cause the VPN tunnels to disconnect. Additionally, this could result in the rollout taking longer than usual.

→ A series of security vulnerabilities in the Linux tool AppArmor allowed arbitrary AppArmor profiles to be loaded, replaced, or deleted, enabling attackers with basic privileges to gain root privileges through local privilege escalation (CrackArmor).

## LCOS FX improvements 11.2 RelI

### Improvements

→ Support for SAG (SPLA) licenses

→ Update Support IPs for Webclient and SSH access

### Bugfixes

→ After updating to LCOS FX 11.2 RC2, a unified firewall managed by LMC could lose its connection to LMC because the certificate and private key for authentication were no longer available on the device.

→ When the application filter was active and used in a connection (e.g., LAN to WAN with a blacklist), the editor for creating new interfaces (e.g., VLAN or Wireguard interfaces) timed out and could no longer be closed. However, the new interface was created.

→ Traffic Shaping did not function properly due to malfunctions in the service responsible for it.

→ If a SAML user was a member of multiple desktop groups and logged in to the internal portal of the Unified Firewall, only the defined rules of one group were applied.

→ A security vulnerability has been fixed that allowed logged-in administrators with backup creation privileges to execute code.

→ With a unified firewall running LCOS FX 11.2 RC2 in factory condition, the second rollout might fail after configuration via LMC.

→ When exporting the configuration, the Docker containers are also exported. If symbolic links were contained in the Docker containers, this caused the export of the Docker containers and thus the entire configuration export to fail.

→ If a rollback occurred on a unified firewall managed by LMC with a user-defined packet filter rule with at least one desktop object created by LMC after a failed rollout, the user-defined rule was deleted but could not be restored by the rollback. This resulted in restricted communication.

## LCOS FX improvements 11.2 RC2

### Improvements

→ It is now possible to create desktop connections between local and LMC objects.

→ The reverse proxy can enforce Outlook Basic Auth.

→ The LDAP/AD connection now supports paging when querying users and groups to improve collaboration with Active Directory for more than 1,000 items.

→ The Docker connection now also supports logging in to Azure and Docker Hub to download Docker images.

### Bugfixes

→ After a configuration rollout via LMC, the list of configured syslog servers was deleted. As a result, system events were no longer sent to the syslog servers.

→ Rules for user groups that authenticate via SAML were not written. This resulted in no communication being possible for the users included in the group.

→ VLAN interfaces generated by the LMC could not be used to create desktop objects in the web interface of the Unified Firewall because they were grayed out.

→ When the HA cluster service (gpHAd) on the master firewall did not receive a response from the license management service (gpLicensed), it sent an empty serial number to the slave firewall. The slave firewall then removed the license because the serial number did not match the license. When switching roles from slave to master, this meant that not all features were available and communication was therefore only possible to a limited extent.

→ With Chromium-based browsers (e.g., Google Chrome or Microsoft Edge), desktop interactions in the web client could sometimes be delayed.

→ In a routing table with many entries, the ‘Delete’ button was overlaid by a scroll bar in the web client. As a result, the button could not be used.

→ It could happen that during external communication from a Microsoft Outlook client via the firewall’s reverse proxy, a password prompt was constantly displayed.

## LCOS FX improvements 11.2 RC1

### New features

→ **Docker container management*:**

**Introduction of support for the management and execution of Docker containers via the REST API**

**Key features**

- Managing Docker containers: creating, deleting, and updating containers
- Managing Docker networks: creating, deleting, and updating networks and attaching containers to these networks
- Container lifecycle management: starting, stopping, and restarting containers
- Defining firewall rules for Docker networks
- Persistent Docker volumes: Volumes are preserved by firewall backups.
- Retrieving Docker images from upstream registries
- Real-time monitoring: access to container logs via REST API and events via WebSockets

**Benefits**

- Improved security and control over Docker containers and networks
- Simplified management and provision of containers
- Improved monitoring and logging functions
- Seamless integration into existing firewall functions
- Simplified handling of containers: optimized management and deployment via LMC add-ins

**API documentation**

- The interactive REST API documentation is available in the Web GUI.

→ **Local editing of LMC objects**

- Distinction between two types of settings, depending on the scenario configured in the LMC: Those that are vital to the scenario configured by the LMC, and additional settings that are not strictly necessary to be set to specific values.
- The additional settings can be configured via firewall Web GUI to meet the administrator's needs.
- Depending on the scenario, additional settings maybe things like NAT settings, IDPS exemptions, extra firewall rules etc.
- To avoid loss of settings on subsequent config rollouts, the Firewall will merge existing additional settings with the changes coming in from the LMC.

* To use the Docker container functionality, you must activate a SAG Basic or SAG Full license (Secure Application Gateway) on your hardware firewall.

  - Instead of always recreating changed objects and their dependents, the Firewall will now try to change existing objects. This improves rollout speeds and allows to keep more of an administrator's customizations.
  - Changes are reviewable in the audit log.

→ Network interfaces created by the LMC can be used for own desktop objects

→ Integration of SICCT proxy for secure operation of card readers in the healthcare sector (telematics infrastructure)

→ Updating and expanding Bitdefender content filter categories analogous to the LCOS operating system

→ Central syslog collection in the LANCOM Management Cloud (LMC)

→ SAML: It is possible to select a primary group. This means that only groups and users within this group are synchronized, in order to speed up synchronization in large organizations.

→ SAML: It is possible to use the TrustStore to verify the IDP certificate.

→ SAML: The IDP certificate/CA is selected from a drop-down menu.

→ Let's encrypt: The type and length of the key are adjustable: RSA 2048 (legacy), RSA 4096, ECDSA (recommended)

→ The menu item Proxy CAs has been renamed TrustStore.

**Bugfixes**

→ With a newly installed HA cluster, synchronization between the firewalls might not have worked.

→ The configured IP address of the SICCT proxy (Secure Interoperable Chip Card Terminal) was only assigned to the network interface after the proxy had been started. This meant that the SICCT proxy could not use this IP address and communication was therefore not possible.

→ When a configuration change was made that involved a host object with more than 300 entries (e.g., changing a rule that contained this object), the web interface froze. This condition could only be resolved by restarting the firewall.

→ If the DMZ port was stored in a firewall rule and this entry was removed so that no port was stored anymore, the rule set could no longer be written.

→ It is possible to assign an LMC license to Unified Firewalls if they are operated in an LMC project with the SPLA (Services Provider Licensing Agreement) license type. The Unified Firewall system log displayed the warning message "could not read SPLA license file!" every 5 minutes if the device was used either in an LMC project without SPLA support or in standalone mode.

→ After deactivating a WireGuard connection, if the Unified Firewall was restarted, the WireGuard service (x-wireguardd) ignored the deactivated connection and did not create the associated interface and peer configuration. After reactivating the WireGuard connection, the peer configuration was created, but not the WireGuard interface. As a result, the WireGuard connection was not functional.

→ If a DHCP option was specified in a DHCP interface in the ‘Manufacturer-specific options’ tab without specifying the ‘Manufacturer ID’, the configuration could not be created, but no warning message was displayed. After logging out and then logging back in to the web interface, the DHCP interface with the incorrect DHCP configuration was still present. If ‘Create’ was clicked multiple times, several DHCP interfaces for the same network were then present (one DHCP interface for each click on ‘Create’). The DHCP service was then no longer functional.

→ If a PPP interface with configured traffic shaping was deleted, the shaping configuration remained in the device and could not be deleted afterwards.

→ When clicking on the ‘Help’ icon in an LTA group, the error message “404 Not Found” was displayed instead of the corresponding chapter from the manual.

## 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