LANCOM Release Notes

LCOS FX

10.6 RU4

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

Internet: http://www.lancom-systems.com

October 4th, 2021, MKoser

Table of Contents

LANCOM Systems

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 FX software release 10.6 RU4, as well as the improvements since the previous version.

2. Supported hardware

Version 10.6 RU4 supports the following hardware appliances:

- LANCOM R&S®Unified Firewalls UF-50/60/T-60/100/200/300/360/500/900/910
- 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 10.6 RU4 supports the following virtual appliances:

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

Version 10.6 RU4 supports the following hypervisors:

- Vmware ESX
- Microsoft HyperV
- Oracle Virtualbox
- KVM

3. History LCOS FX

LCOS FX improvements 10.6 RU4

Improvements

- Stability improvements of the LMC connection

LCOS FX improvements 10.6 RU3

New features

- **Cloud-managed Firewall**[1]

  The current release provides completely new configuration options for cloud-managed firewalls in conjunction with the LANCOM Management Cloud. The one-click security package includes comprehensive control of the application filter, content filter, SSL inspection, and anti-virus/anti-malware functions (including whitelist options). An initial configuration can be easily rolled out to all devices, sites, and networks.

  LCOS FX 10.6 RU3 also expands the range of uses for the cloud-managed firewall, so that the LANCOM R&S®Unified Firewalls can now be used both as a VPN gateway and as a central-site VPN gateway, e.g. for networking different sites. All this with just a few clicks in the LANCOM Management Cloud via Auto-VPN.

- **IDS/IPS and anti-virus exceptions**

  Specific hosts and networks can be excluded from scanning by the IDS/IPS or anti-virus engine via settings in the respective desktop object.

Further improvements

- For SSL VPN connections, since LCOS FX 10.6 REL it is possible to select a CA on the server side, whereby the Unified Firewall accepts any client that has a certificate signed by this CA. Thus, it is not necessary to configure a separate VPN connection for each VPN client. As of LCOS FX 10.6 RU3, this now also works for VPN-SSL in bridging mode.

Bugfixes

- In some cases, it was not possible to log in to the web configuration interface. This could be the case during operation or after an initial installation or configuration of the Unified Firewall.
- The counter for unsuccessful admin logins on the web configuration interface did not work.
- If the communication port for the web configuration interface was not equal to the default port 3438, a configuration could not be rolled out to the Unified Firewall after pairing with the LMC.
- An online firmware upgrade from LCOS FX 10.5 to 10.6 on Unified Firewalls operating in a High Availability (HA) cluster failed.

1 Support of these features in the LANCOM Management Cloud will follow soon.

- When configuring an e-mail notification, the password for accessing the e-mail inbox in use was in plain text.
- When importing a backup created under LCOS FX 9.6, a port specification changed for access to the internal portal was not included in the webserver.ini file.
- Desktop icons from the LMC were still displayed after a rollout via the LMC and setting a filter to hide these icons.
- In rare cases an empty dns.ini file in the path '/opt/gateprotect/etc/' could cause the web client not to work after a firmware upgrade to LCOS FX 10.6 RU2.
- After importing a configuration backup, Subject Alternative Name (SAN) identifiers present in the IPSec configuration were no longer displayed.
- When all traffic was transferred over an IPSec connection (both client-to-site and site-to-site) and a web page was accessed, some web servers ignored path MTU handling via ICMP. This meant that the web pages could not be accessed due to an excessively large MTU.
  For IPSec connections, TCP MSS clamping is now performed to ensure that the MTU is selected appropriately.
- Although the synchronization of an HA cluster was successful, the status of the cluster in the configuration interface was indicated as 'Out of sync'.
- An IPSec VPN connection was not automatically re-established by the initiator after a connection failure, but only when a data transmission was taking place.
- In a management report exported in CSV format (report_data.csv), the time specification 'Statistics Period' was not included.
- In the connection configuration dialog, it could happen that the button for removing the rule was missing in the 'Application Management' tab for an added routing profile.
- A user with configured 'Wake on LAN' could no longer log in to the 'internal portal'.

LCOS FX improvements 10.6 RU2

Bugfixes

- Minor improvements for LCOS FX 10.6 RU1

LCOS FX improvements 10.6 RU1

New features

- Support of the LANCOM R&S®Unified Firewall UF-360 with a massive performance boost compared to the predecessor model UF-300: Doubled performance, doubled storage capacity, module expansion slot, and two 10 Gbps SFP+ interfaces for completely new application scenarios.
- Conversion of the VPN tunnel limitation of the UF-60 / UF-160 / UF-260 into a recommendation for customer orientation.

Further improvements

- **CSV export of the executive report**
  The executive report can now also be exported to CSV format for easier machine processing.

Bugfixes

- German texts / terms were displayed in the English dialog for exporting SSL VPN configurations.
- If an entry was added in the 'Network / DNS / Network spec. settings' menu and the entry was to be changed after the first save, the change could not be saved.
- After changing the port for the local web client in the menu 'Firewall / Firewall access / Web client settings' it was not possible to log in to the web interface with the changed port.
  If an administrative user was created, which had the monitoring right 'Read / Open' in the web client rights (menu 'Firewall /Administrators / Web client rights'), it was not possible to view the list of DHCP leases in the menu 'Monitoring & statistics / DHCP leases' with this user account. The user received the "403 Forbidden" error instead.
- After a reboot it could happen that the connection to the LMC could not be established anymore.
- If DNS settings were made for a specific network in the menu 'Network / DNS / Network specific settings', no DNS queries were answered for this network.
- When two branch offices were connected to a central site using VPN-SSL with bridge, the two branch offices could not communicate with each other via the central site.

LCOS FX improvements 10.6 Rel

New features

- **Extended feature set for cloud-managed firewalls** [2]

  LANCOM FX 10.6 upgrades the LANCOM R&S®Unified Firewalls with many additional functions for operation with the LANCOM Management Cloud (LMC) and turns them into a fully-fledged stand-alone VPN gateway for branch offices: From now on, secure VPN networking of sites, including network virtualization, is fully automated. Thanks to the support of LMC's DynDNS service, firewalls are also easily reached via a self-selected subdomain. Furthermore, applications can now also be blocked by the firewall in stand-alone mode at layer 7 level.

- **Zone management for DNS**

  From now on, the LANCOM R&S®Unified Firewalls support different DNS servers for different zones. In addition, the DNS configuration for individual networks can be adjusted separately. This allows separate DNS configuration for individual networks so that, for example, local zones can be accessed exclusively from the employee network and not from the guest network.

Further improvements

- **VPN-SSL CA Auth**

  For a VPN SSL client-to-site connection, a CA can be selected for authentication. All clients whose certificate has been signed by this CA can connect to this site.

Bugfixes

- With LCOS FX 10.6, a security vulnerability (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31538) of the LANCOM R&S®Unified Firewall has been fixed. This affects all devices with LCOS FX 10.5 versions. LCOS FX 10.4 versions and lower are not affected by the security vulnerability.
- When using the internal user portal, if a user logon was performed while the background process x-rulesd was starting, this caused the background process to terminate and no user logon via the internal portal was possible anymore.
- When creating a new client-to-site connection with SSL VPN, the button to export the VPN configuration was grayed out and thus not usable.
- When a new SSL VPN connection was configured, data compression was enabled by default and the TCP protocol was always used by default. Data compression is now disabled by default and the UDP protocol is used for the VPN tunnel by default.
- If the profile of an IPSec VPN client connection where the password contained special characters (e.g. #) was exported to an AVC profile file (*.ini file), the exported profile could not be imported into the LANCOM Advanced VPN Client.
- In an HA cluster, changed administrator passwords and a changed support password were not synchronized from the master device to the slave device.

2 Support of these features in the LANCOM Management Cloud will follow soon.

- Installations with a very large number of client-to-site connections (SSL VPN) may experience frequent logins and logouts of the VPN clients. The memory reserved by the processes responsible for logging in and logging out the VPN clients was no longer released in the process. This caused the 'OOM' (Out Of Memory) process to be called, which terminated processes required for operation, so that the function was no longer given. This could only be remedied by a restart.
- If a backup was created via the 'Veeam' software when IDS/IPS was active, the IDS/IPS service kept reserving memory and no longer released it. This led to an immediate reboot.
- If a DHCP configuration with the same DHCP address range was duplicated after an update to LCOS FX 10.5.3 (for example by migrating an IP address range to another interface without removing the DHCP configuration), the DHCP service could not be started due to the address conflict.
  Incorrect DHCP configurations are now ignored during a firmware update.
- Switching the HTTP proxy between 'Transparent' and 'Intransparent' modes caused the proxy to subsequently stop working until the rules were re-enabled.
- When a user accessed the login page of the 'Internal Portal' for authentication, but did not accept the SSL certificate of the login page, this resulted in high processor utilization of the Unified Firewall.
- For the purpose of checking the Internet connection, a ping to a stored IP address is performed via a heartbeat test. Previously, the Google DNS server 8.8.8.8 was stored by default. If a ping failed, the Internet connection switched to the offline status.
  The following DNS servers are now used for the heartbeat tests. Three ping packets are sent in each case, at least one of which must be answered.
  - 8.8.8.8
  - 9.9.9.9
  - 1.1.1.1

LCOS FX improvements 10.5 RU3

New features

- **Support for the LANCOM R&S®Unified Firewall UF-60**
  Full UTM performance in small installations
- **DHCP Refresh**
  - DHCP Lease Monitoring: The currently assigned DHCP leases can be viewed.
  - New DHCP server options: Routes, PXE- and proxy settings can be pushed to the client.
  - Mixed operation of DHCP server and relay possible: It can be configured separately for each network interface whether DHCP server or relay should be active.
- **mDNS Relay**
  For device discovery within the network, the Unified Firewall can forward mDNS requests between local networks.
- **Route-based IPsec**
  Tunnels with identical policies can be set up and selected via routes.
- **License expiration behavior**
  - Transition phase until 30 days after license expiration: The configuration remains editable, a warning is issued for each change.
  - From 30 days before license expiration LCOS FX warns in the header and when logging into the administration interface.
  - Configurable behavior of UTM features upon license expiration: Web and mail traffic can be blocked or allowed without UTM filters.
  - When the license expires: A note about the expired license appears in the header of the administration interface. After the expiration of the transition phase, the configuration is still readable, but no longer editable.

Bugfixes

- With a VPN client connection that sent all traffic through the firewall and also used the content filter, no firewall block page was displayed for blocked web pages.
- If VLANs were bridged to Ethernet interfaces in a firewall configuration, this could lead to the ‘gpNetworkd’ service no longer starting when restoring a backup configuration. As a result, access to the firewall was no longer possible.
- When using the mail proxy, it could happen that e-mails with certain characters in the subject (e.g. hearts or stars) could not be retrieved via POP3 or POP3s.
  It could also happen that the mail proxy could not decode received e-mails and then not forward them.
- After importing a backup configuration, a window appeared at the first login prompting to either close the previous session or open the configuration in ‘read only’ mode. This message has been removed and normal configuration access to the firewall is possible.
- An e-mail containing special unicode characters could cause the virus scan for that e-mail to fail.

- When querying the SNMP IDs of the mail proxy for the ‘spam’ and ‘virus’ counters, the value ‘0’ was always returned.
- If e-mails with characters that are not contained in the ASCII character set and could not be converted to Unicode (e.g. Cyrillic or e-mails with umlauts) were received when the mail proxy was activated, these e-mails could not be retrieved via POP3 or POP3s. This resulted in all subsequent e-mails also not being retrieved via POP3.
- A certificate request could not be created, because a click on ‘Create’ showed no reaction.
- In scenarios with special combinations of desktop objects and firewall rules, the service responsible for the firewall (xrulesd) completely utilized the CPU after the firewall rules were changed. Furthermore, the service used more and more memory and did not release it. After some time, this led to an abrupt restart of the firewall.

LCOS FX improvements 10.5 RU2

New features

- **Support for the LANCOM R&S®Unified Firewalls UF-160 and UF-260**
  The new generation of desktop LANCOM R&S®Unified Firewalls with a significant leap in performance enables the use of all UTM features already from the UF-160. The UF-260 is the first desktop LANCOM R&S®Unified Firewall with a dedicated SFP port.
- **Executive Report**
  The new Executive Report enables a regular tabular and/or graphical overview via PDF or HTML. In addition to the current desktop configuration and the display of all rules, security statistics can also be included (e.g. blocked connections/contents, accessed/blocked domains/traffic per source).
- **License expiration behavior**
  - From 30 days before license expiration LCOS FX warns in the header area and when logging into the administration interface
  - Configurable behavior of UTM features at license expiration:
    Web and mail traffic can be blocked or allowed without UTM filter.
  - On license expiration:
    A note about the expired license appears in the header area of the administration interface.
    The configuration is still readable, but can no longer be edited.
  - From LCOS FX 10.5 RU 3 onwards, transition period up to 30 days after license expiration:
    The configuration remains editable, a warning will be issued for each change.

Further improvements

- Implementation of the LANCOM and R&S® co-branding
- Improved user guidance and default settings in the initial setup wizard
- After completing the initial setup wizard, a check for firmware updates is performed immediately.
- Customized info area in the web client with the option to call up the settings dialogs directly
- Entries in the HTTP(S) proxy whitelist can be grouped and include an optional description.
- Certificate export with .crt extension for direct import under Windows

Bugfixes

- In the ‘User Authentication / Unassigned’ menu, the word ‘User Authentication’ in the header of the configuration dialog was only half readable when minimized.
- The content filter categories were displayed in English in the German user interface.
- Importing administrator accounts for access to the Web client failed if the accounts were exported from a previous firmware version.
- After a firmware update from LCOS FX 10.5 to LCOS FX 10.5 RU1, a list previously filled with entries in the ‘UTM / Reverse Proxy / Frontends’ menu no longer contained any entries.
- When using the SMTP proxy, incoming E-mail messages may not be forwarded. The proxy then issued the error message “UnicodeDecodeError: ‘utf-8’ codec can’t decode byte xxx in position”.
- If access via SSH was allowed for a VPN tunnel (IPSec), the TFTP protocol was enabled for all connections (including WAN connections).
- The performance has been raised to the level of the previous firmware version.
- In a scenario with a VPN SSL bridging server, only the first VPN SSL bridging client could establish a connection to a remote peer. Other VPN SSL bridging clients could not connect to the same remote site.
- When using the IMAP proxy, it could happen that e-mails retrieved via IMAP were delivered incorrectly encoded and, as a result, existing file attachments were not readable.

LCOS FX improvements 10.5 RU1

Behavior on license expiration

As before, no changes can be made to the firewall configuration after the user license has expired. However, the firewall configuration can still be viewed. In addition, a clear dialog has been integrated into the interface, which contains a direct link to the license extension.

New features

- **VPN profile portal**

  The new external user portal offers a simple and secure method of making VPN profile files available to employees. From home or on the road, employees can log on to the firewall with their usual Active Directory or LDAP login and download their VPN profile file.
- **Wake-On-LAN**

  The firewall can now wake up PCs within the internal network via Wake-On-Lan. This is useful, for example, for home office employees who access dedicated PCs within the company network from home via VPN. The WoL packets are sent when logging on to the internal user portal.
- **LDAP-TLS**

  Connections between the firewall and an ActiveDirectory- or LDAP server can now be secured using the TLS protocol.

Bugfixes

- To avoid errors, there is a check whether the remote network of an IPSec connection collides with the local network. It could happen that a collision with the default route (0.0.0.0/0) was detected and a corresponding error message was issued.
- If an application filter profile was stored in a desktop object, it could happen that not all firewall rules were created. As a result, communication was not possible or only possible to a limited extent.
- If large files were transferred via SMB with IDS/IPS enabled, the memory consumption continued to increase and was not released. This could lead to a sudden restart or freezing of the device.
- When using a VLAN on a bridge and the HTTP proxy simultaneously, no connection to the Internet was possible.
- When creating a desktop rule via the alarm log it could happen in some cases that the wrong source object was suggested.
- In the alarm log it was not possible to create an IDS/IPS rule from an alarm message.
- The content filter rules for LDAP groups using a non-transparent proxy and client authentication were non-functional.
- When the firewall was restarted, the certificates for communication with the LMC were deleted. As a result, the firewall was displayed as 'Offline' in the LMC after the restart and could no longer be managed and monitored by the LMC.
- A code to override the content filter, which was created in the English user interface, was functionless.
- No changes to the time settings or time tables for desktop rules could be saved.
- In the Sysinfo output of a UF-910 the raid status was given, too. This made the sysinfo output very confusing.
- A 10-digit signature ID could not be ignored with activated IDS/IPS because the system only allowed 9-digit signature IDs.
- In rare cases, it could happen that the antivirus service could not start because another service prevented it from starting. As a result, the web proxy was not functional.
- In some configuration fields the placeholder texts with suggestions for input were missing or the texts were incorrect.
- If the list of configured IPSec VPN connections was expanded, some icons (e.g. the delete icon) might not be displayed.
- The configuration interface showed WAN connections using DHCP as offline, although they were established.

LCOS FX improvements 10.5

New features

- **IMAP proxy**

  As of LCOS FX 10.5, complete e-mail security is also available for the IMAP protocol. Both IMAP with STARTTLS and IMAPS are supported. This means that in particular smaller end customers who do not host their e-mails themselves can make full use of the usual e-mail security with anti-malware and anti-spam.

- **Application based routing**

  Application based routing enables the routing of recognized protocols and applications to be determined on the basis of the PACE2 DPI engine. There are three options: The selection of a specific outgoing connection in multi-WAN scenarios (e.g. streaming services via the slower line, VPN via the faster one), the exclusion of specific applications from the proxy (e.g. trusted cloud applications), and the exclusion of specific applications from IPSec tunnels (e.g. for branch offices that send all Internet traffic to the central office but want to exclude certain trusted applications from it).

Further improvements

- **Desktop search**

  The desktop tags filter is extended to become the desktop filter. You can search for desktop objects as well as desktop connections. Objects / connections that do not apply are hidden. A variety of parameters can be searched for, including name, IP address, corresponding VPN connection or proxy flag.

- **Create rules from the log**

  You can create rules for denied access directly from the alarm and system log. If the firewall with the current set of rules blocks desired network traffic, you can add a new rule for this network traffic directly from within the log with a few clicks. This makes both the initial rule creation and maintenance much easier and faster.

- **Multiple logged-on administrators**

  Multiple administrators can be logged on to the LANCOM R&S®Unified Firewall web client at the same time. The administrator logged on first has write permissions, i.e. he can make changes to the configuration. Other administrators have read-only rights. If the first administrator logs off, the write permission is passed on to the next one. This significantly simplifies the administration of LANCOM R&S®Unified Firewalls in larger administration teams.

- **Restore points**

  Restore points make it possible to reset the LANCOM R&S®Unified Firewall to the original version after an upgrade.

- **Content Filter override codes**

  The administration of the content filter has been extended by codes that allow users to view blocked pages within certain times by entering the respective code. These exception codes can be created by end users in the end user portal if the administrator has enabled them to do so. For example, supervisors can enable exceptions to the content filter for their area if required.

- **VPN-SSL bridging**

  By means of VPN-SSL bridging it is possible to connect two or more networks at different locations securely and reliably on Layer-2, e.g. to enable communication via non-IP-based protocols.

Bugfixes

- After importing a backup configuration file and then restarting the firewall, it could happen that the application filter settings were not loaded.
- After importing a backup configuration file and then restarting the firewall, it could happen that the category list was missing in the application filter.
- After updating to firmware version 10.4 RU1, a GP-NP-200 firewall only accepted the license for a UF-900 type firewall.
- In individual cases, when the application filter was deactivated, the memory consumption of the responsible service (gpAppFilterd) could increase continuously.
- When using the 'Single Sign On' function, no firewall rules were created for users with an umlaut or the letter "ß" in their name.
- A configuration backup could be imported into a device with an older firmware version. This usually resulted in a non-functional configuration.

  During the import process the version is now checked and the import is rejected if the firmware version of the device is older than the configuration backup.
- If a VPN profile was created and exported for the Advanced VPN Client, a VPN connection could not be established with this profile because the string "email:" was inserted before the 'Local Identifier' during export.

4. Installation instructions for updating to LCOS FX 10.6 RU4

Note 1:

If there is not yet a working 10.2.0 firewall installation, please setup a simple 10.2.0 firewall installation with Internet connection first (see document „First installation steps“). An Internet connection is mandatory to receive updates.

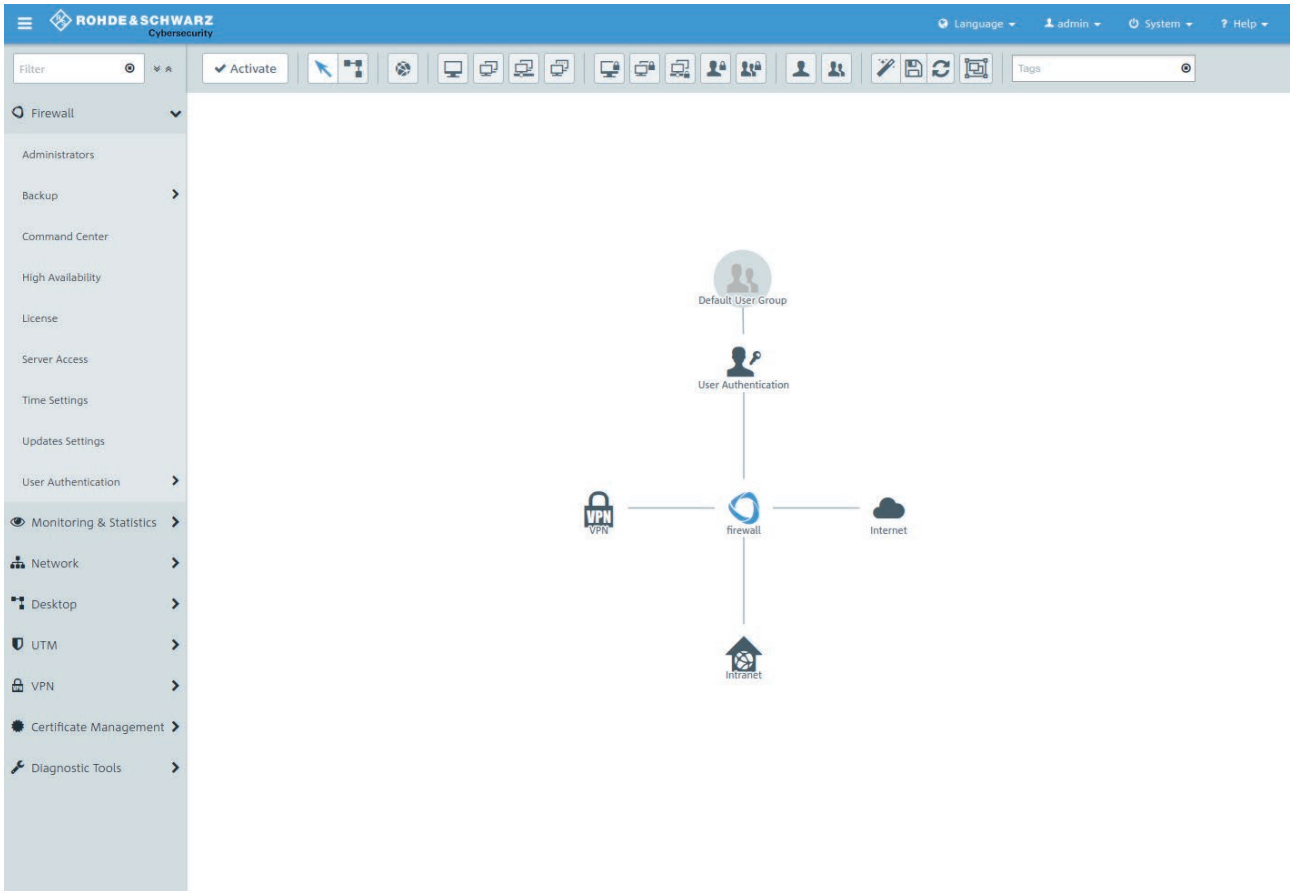
Via the auto updater on the web interface of your LANCOM R&S®Unified Firewall the respectively newer minor update version is available for step-by-step updating.

Please follow the subsequently described steps in this manual to update your device to the latest LCOS FX version.

Note 2:

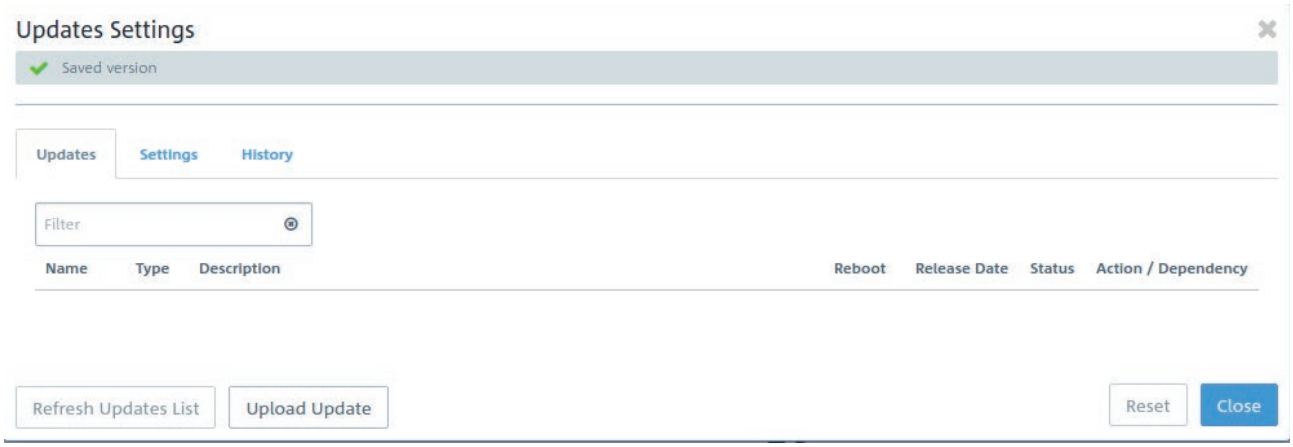
In order to not hinder any workflows, please first install the update in a testing environment and not in a productive setting.

In the navigation bar on the left side, select “Updates Settings“ under the first item “Firewall“.

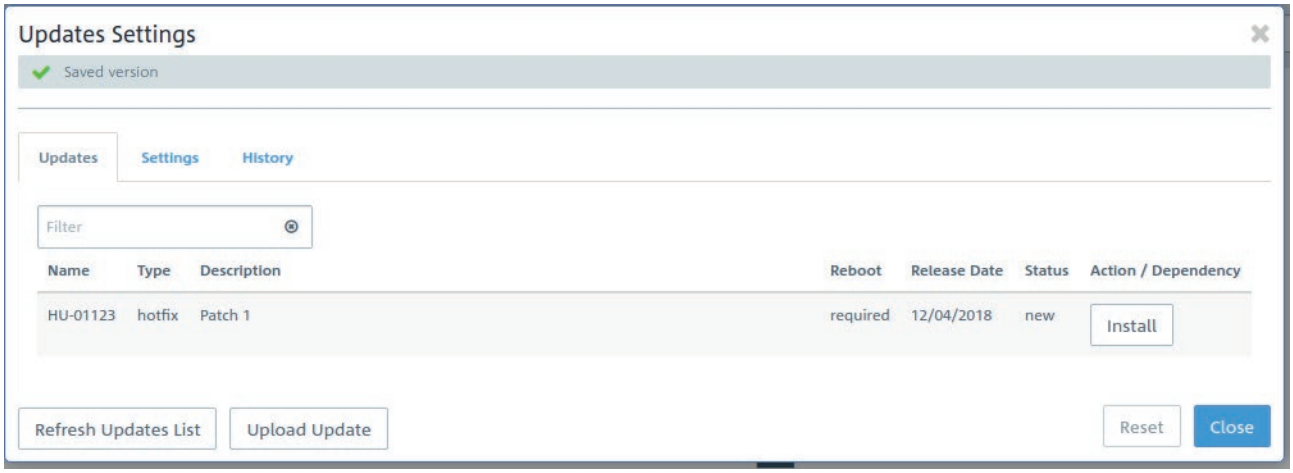


LANCOM Systems

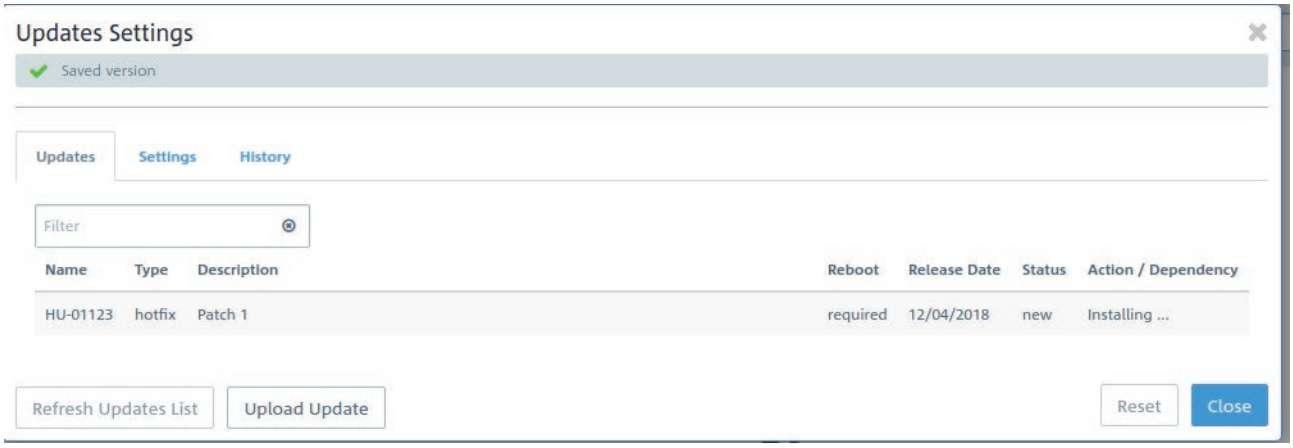
In the opening window “Updates Settings“ press the button “Refresh Updates List” under the tab “Updates“.



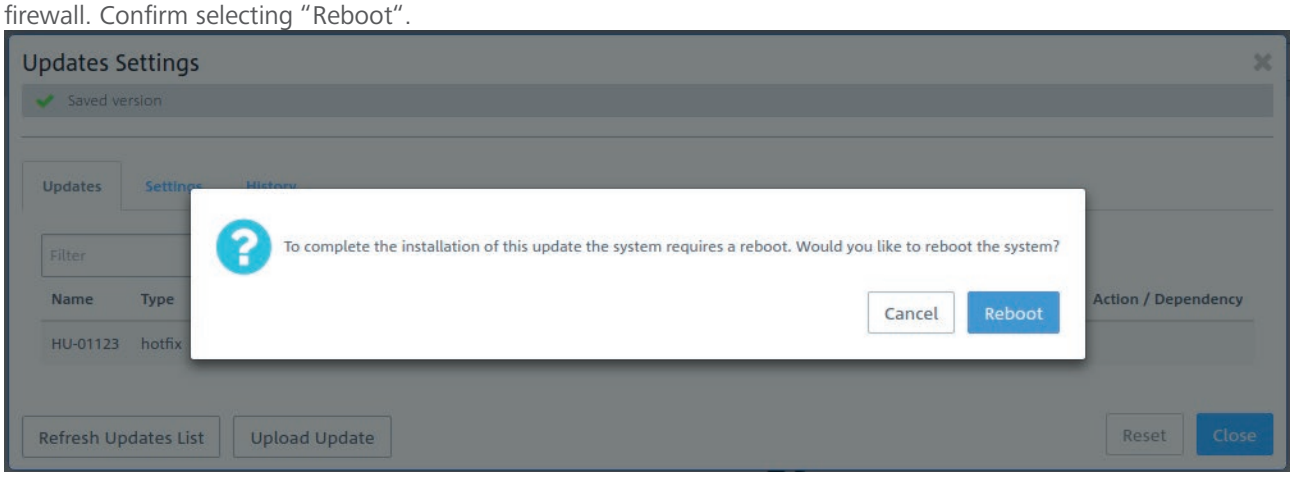
From the list, select the firmware file to install and press the “Install” button.



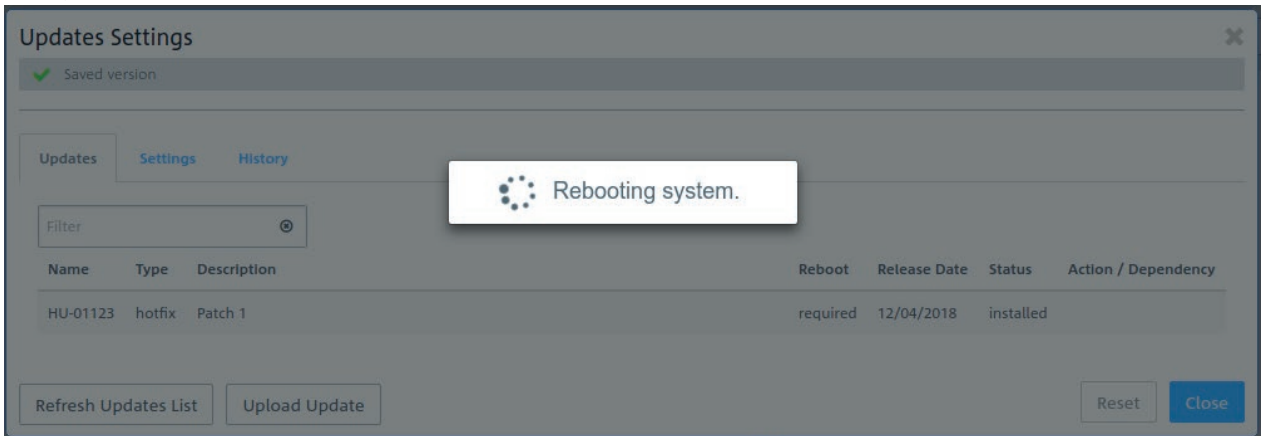
The status of the action changes to “Installing...“



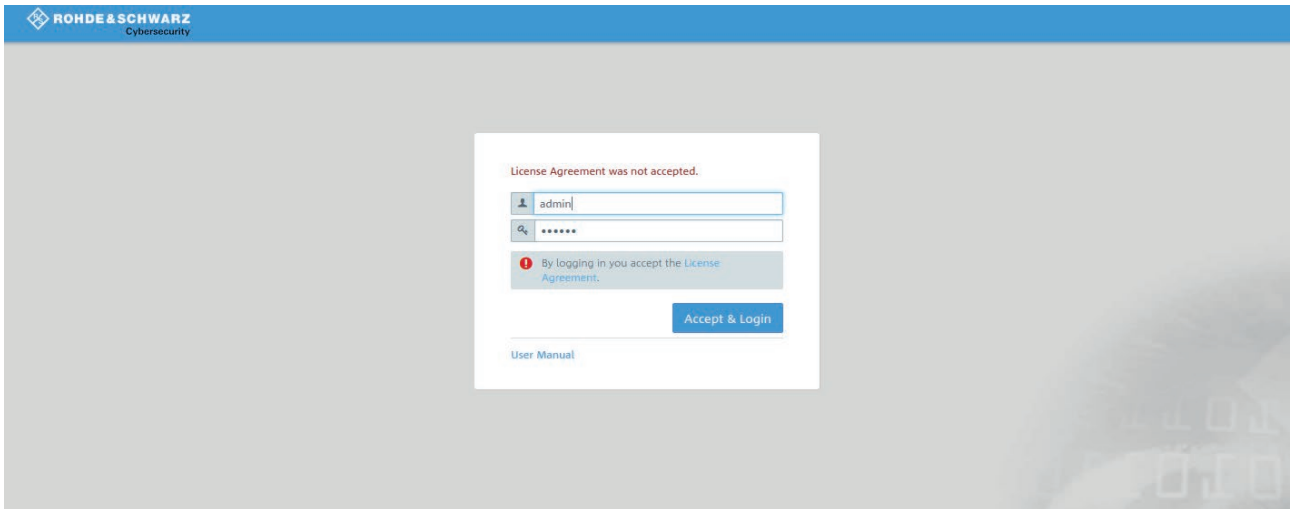
After the installation has completed a popup dialogue window appears displaying a request for rebooting the firewall. Confirm selecting “Reboot“.



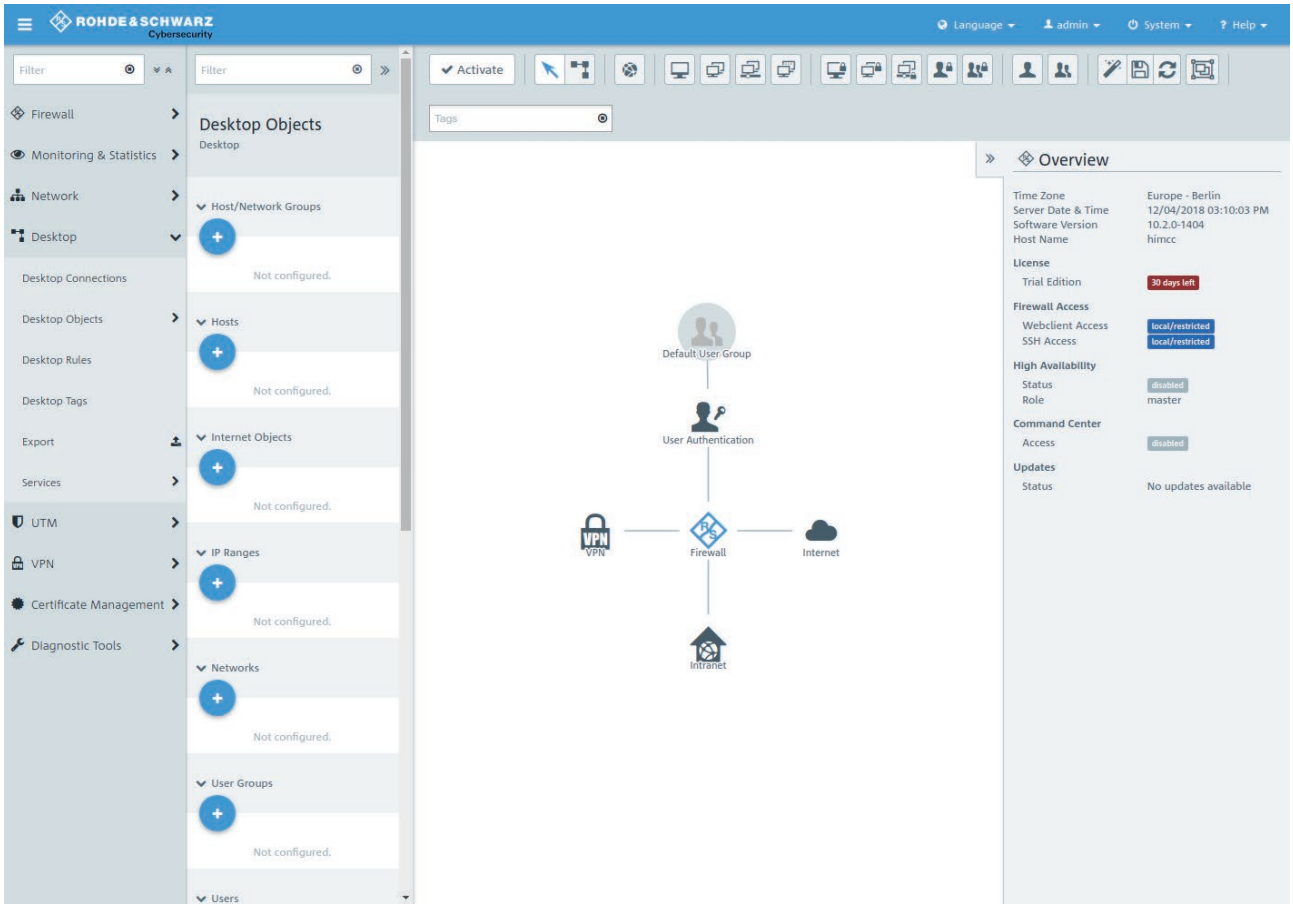
The system is rebooted.



After the firewall reboot the login window appears. When typing in your login credentials you are asked to accept the license agreement.



After having logged in, the desktop of your LANCOM R&S®Unified Firewall opens. You will notice the info bar on the right side. Here you can see information about the current software version and others.



5. Further information

- Backups of versions 9.6, 9.8 und 10.X are supported.
- Devices with less than 4 Gbytes of RAM can not execute all UTM features simultaneously.

6. Known issues

- System- and audit protocols are not synced when operating in high availability mode.
- Some monitoring information is not yet available:
  - User login status
  - Network interfaces load

7. 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.