LANCOM Release Notes

LCOS FX

10.5 RU1

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

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

July 30th, 2020, CBuersch

Table of Contents

1. Preface 2
2. Supported hardware 2
3. History LCOS FX 3
LCOS FX improvements 10.5 RU1 3
LCOS FX improvements 10.5 5
LCOS FX improvements 10.4 RU3 6
LCOS FX improvements 10.4 RU2 7
LCOS FX improvements 10.4 RU1 8
LCOS FX improvements 10.4 8
LCOS FX improvements 10.3.3 10
LCOS FX improvements 10.3.2 11
LCOS FX improvements 10.3.1 11
LCOS FX improvements 10.3.0 11
LCOS FX improvements 10.2.3 12
LCOS FX improvements 10.2.2 13
LCOS FX improvements 10.2.1 13
LCOS FX 10.2.0 13
4. Installation instructions for updating to LCOS FX 10.5 RU1 15
5. Further information 19
6. Known issues 19
7. Disclaimer 19

1. Preface

LCOS FX is the operating system for all LANCOM R&S®Unified Firewalls. In the context of the hardware given by the products the at a time latest LCOS FX version is available for all LANCOM R&S®Unified Firewalls and is available free of charge for download from LANCOM Systems.

This document describes the innovations within LCOS FX software release 10.5 RU1, as well as the improvements since the previous version.

2. Supported hardware

Version 10.5 RU1 supports the following hardware appliances:

- LANCOM R&S®Unified Firewalls UF-50/100/200/300/500/900/910
- 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 10.5 RU1 supports the following virtual appliances:

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

Version 10.5 RU1 supports the following hypervisors:

- Vmware ESX
- Microsoft HyperV
- Oracle Virtualbox
- KVM

3. History LCOS FX

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.

LCOS FX improvements 10.4 RU3

Improvements

- Preparation of the option to restore the old version after a firmware update. Configuration under 'Firewall / Update settings / Automatic recovery'. This feature will only become active for the future update from LCOS FX 10.4 to LCOS FX 10.5.

Bugfixes

- After a firmware update to LCOS FX 10.4 RU1 the following describers and texts have been replaced by the respective UUID (Universally Unique Identifier) of the parameter:
  - the names of some services, even within a service group
  - the description of firewall rules
- Desktop objects created by the LMC could not be copied.
- It could happen that the Unified Firewall listed a user as 'logged in', even though the user was already logged out from the firewall. As a result, the user-specific rules for IP addresses were written.
- If a configuration backup contained a VPN connection with an expired certificate, all subsequent VPN tunnels could not be loaded during import from the IPSec service.
  This could cause a VPN connection with an expired certificate to fail to load all VPN tunnels.
- After a VPN certificate expired, the corresponding VPN connection could not be deactivated.
- If a configuration backup was imported, it could happen that VPN connections could not be deactivated and the name of the connection could not be edited.

LCOS FX improvements 10.4 RU2

Improvements

- The IPSec EAP configuration options have been extended to allow EAP on connections with the LANCOM Advanced VPN Client, Windows 10, and iOS.
- Support for the LANCOM R&S®Unified Firewall UF-910

Bugfixes

- After a firmware upgrade to LCOS FX 10.4.1 VPN hosts were displayed without icons.
- A PSK with a maximum of 63 characters for an IPSec VPN connection prevented the establishment of the VPN connection.
- If a local IP address was specified in the field 'Listening IP addresses' for an IPSec VPN connection, and a network connection with multiple local IP addresses was used, the unified firewall used all specified local IP addresses as listening addresses.
  Listening addresses are now handled with priority.
- The DPD behaviour was realized by "trap policies", so that VPN tunnels could only be re-established if data should be sent through the tunnel. This behaviour caused malfunction in some VPN scenarios. The DPD behaviour is now realized by a "restart policy". If the unified firewall determines a non-answering remote site by DPD, it tries to re-establish the VPN tunnel.
- If configuration changes have been made on a network interface which could cause no access to the unified firewall via web client, no warning message appeared.
- If a new VPN connection was configured in the menu "VPN/IPSec/Connections", a template was selected, and subsequently the menu was closed by the escape key, the menu was empty when recalling it by the menu bar in the window header.
- In the menu"Network/Connections/Network connections" the gateway could be erroneously specified in CIDR (Classless Inter Domain Routing) notation, but the configuration could not be written.
- After a unified firewall license expiration the firewall lost the connection to the LANCOM Management Cloud, so that no access to the web interface was possible via the LMC's detail configuration, and thus no new license could be uploaded.
- In the menu "Monitoring & Statistics/Statistics" no scrolling was possible in the statistics for blocked contents and blocked connections, so that not all data could be displayed.
- If a network object with a network range was created on the desktop which was not known by the unified firewall, the firewall displayed a warning message stating that the created network could possibly not be reachable via the used interface.
  The warning message is no longer displayed.
- Although LDAP groups were configured in the unified firewall, only single users could be selected from a user group on the desktop, but not the existing user groups.

LCOS FX improvements 10.4 RU1

Improvements

- The webclient behavior after connection loss to the firewall has been improved.
- After the auto logout from the webclient the previously edited dialog is re-opened.

Bugfixes

- An issue has been fixed that after restoring a backup the initial setup wizard was started in some cases.
- An issue with Serpent and Twofish Ciphers and IPSec has been fixed.
- The number of IPSec retransmission retries has been decreased.
- An issue regarding collision warnings on IPSec connections has been fixed.
- An issue has been fixed that requests on port 3439 were answered.
- An issue with converting VPN network desktop objects has been fixed.
- Fix for the use of Network Discovery Tools
- The number of log messages from the anti-malware engine has been decreased.

LCOS FX improvements 10.4

New features

Initial setup wizard

Setup your firewall in less than 5 minutes, including Internet access, local networks, and UTM features.

In 4 simple steps the wizard configures:

- Firewall hostname
- Internet access
- Local networks
  - IP addresses
  - DHCP servers
  - Internet access rules
- UTM features (anti-malware, IDS/IPS, URL- and Content-Filter)

Integration to the LANCOM Management Cloud

- **SD-SECURITY**
  - Enables cross-site application managment
  - Configure application access only once per network for easy rollout to all sites
- **Monitoring**
  - Device status (hardware load, interface throughput, ..)
  - Security status (blocked connections, blocked contents like malware)
- **Webclient tunnel**
  - Easy access to the complete firewall management interface

- **Cloud-ready**
  - As from LCOS FX 10.4 all newly delivered Unified Firewalls are cloud-ready.
  - Simply connect and manage instantly via the LMC

New IPSec implementation

- Comfortable handling due to reusable security profiles for IKE and ESP
- Predefined profiles for common clients (Windows 10, iOS, Android, LANCOM Advanced VPN Client) and servers (LCOS FX 10.4, LCOS 10.30 or newer)
- Configuration export for the LANCOM Advanced VPN Client
- Configuration of multiple networks in one connection to reduce configuration efforts
- Option for connecting external DHCP- and RADIUS servers
- Support for Hub-and-Spoke architectures
- Option to specifically configure the external tunnel IP address

E-mail notifications

- Direct information about important events by e-mail, optionally immediate or time-aggregated (configurable per event type)
- Events
  - Internet connection broken / reconnected
  - IPSec Site-to-Site tunnel broken / reconnected
  - High availability switch-over
  - Firewall restart expected / unexpected
- Optional: delivery via mail relay
- Optional: encrypted delivery using SMIME

Improvements

- User-specific application filter rules
  - Combination of user authentication and application filter
  - Specific application profiles for single users or groups
    Connection to active directory (assignment to a group / department directly creates the appropriate application filter rules)
- Configuration and logs can be reset to delivery condition.
- Linux kernel updated to 4.19.69
- SNMP statistics show virtual network interfaces too, e.g. VLANs.
- SNMP statistics show firewall alarms.
- The browser reloads the webclient automatically after the connection has been lost.
- The automatic webclient logout is reset on mouse movement, too.
- The currently active license can now be downloaded under Firewall > License.

Bugfixes

- Fixed an issue within the memory management which could cause unexpected restarts.
- Fixed stability issues with a high amount of IPSec tunnels.
- A Kerberos-Ticket is now created accurately even with capital letters within the hostname.
- Timeout to small for TCP connections
- Statistics are working after disabling the high avalibility mode.
- The high avalability mode has been modified for installations without DNS resolve.
- The 'web proxy did not start' issue has been fixed.
- Improvements for the timeout handling of the user authentication at weblogin
- Stability issues with particular VPNSSL site-to-site connections have been fixed.
- The Anti-virus on the UF-50 is now accurately disabled in all cases.
- Some redundant log entries have been removed.
- The handling of DNS servers which have been obtained by DHCP has been corrected.
- The stability of the weblogin service for user authentication has been improved.
- The Internet connection can be selected from the Internet object right after deleting.
- All firewall services ignore disconnected Internet connections.
- Removed an automatic rule for blocking TCP connections with MSS less than 512.

Additional Information

- Stronger password guidelines for webclient administrators and for the console password
  - minimum of 8 characters
  - minimum of 3 character types (upper case, lower case, digits, special characters)
- Modified standard backup for delivery and initial installation
  - eth0 obtains the IP address and default gateway by DHCP
  - eth1 to eth3 enable the DHCP server for simplified initial setup
- Added the LANCOM support IPs to the preconfigured IPs for webclient- and SSH access.
- Custom scripts are disabled when upgrading.

LCOS FX improvements 10.3.3

Improvements

- Added German manual
- Updated manual to V10.3
- Added support for new UF-100/200 hardware revision

Bugfixes

- Fixed issue which could result in hardware appliances displaying virtual machine UUID in license dialog
- Fixed issue which could result in failing synchronization in High Availability
- Fixed issue in mailproxy if client side closes connection too early
- Fixed issue which lead to already installed patches being installable again

LCOS FX improvements 10.3.2

Bugfixes

- Fixed problem with license handling which could result in an appliances losing the license
- Status of IPsec site-to-site is correctly recognized in all cases
- DNS server is correctly restarted after receiving DHCP lease
- Removed verbose mailproxy logging
- High availability now handles Umlauts in network connections correctly

LCOS FX improvements 10.3.1

Improvements

- Linux kernel security update to version 4.19.53 to fix the vulnerability CVE-2019-11477

LCOS FX improvements 10.3.0

New features

- Alert log
  - Alerts are logged separately
    Covers blocked connections, finished connections, malware, IDS/IPS, web filter, URL/Content filter, anti-spam and the application filter
  - Easy-to-build complex filter queries with AND, OR, NOT operators
    Smart filter proposals allow for constructing precise queries, matching specific alert attributes such as port numbers and source IP addresses
- Online updates are possible in HA mode
- Linux kernel security update to version 4.19.29

Improvements

- Licenses compatible across versions
- Improved performance of log view
- Network interface drop-down lists show attached connections and IP addresses.
- Updated pre-defined services
- Improved usability of DMZ rule creation
- Automatic log-out from web client after 10 minutes
- Configurable end-of-license behavior
- Improved stability of IPSec tunnels

- Improved stability and performance of mail proxy
- Pending changes on the rule desktop are saved on log-out
- Log database size is now capped at approx. 8 Gbyte to ensure system stability; the oldest log entries are deleted.

Additional information

- The end-of-license behavior changed compared to V9.X.
  If you migrate from version V9.X, navigate to "Firewall" > "License" to adapt the end-of-license behavior.
- By default, LANCOM R&S®Unified Firewalls check for software updates once per day. Navigate to "Firewall" > "Updates Settings" to change this interval.
- Backup import supports the migration from versions V9.4 to V9.8 and V10.0, V10.1 and V10.2.
- Devices with less than 4 Gbyte RAM do not support all UTM features to be activated simultaneously.

Discontinued features

The following features are no longer available in LANCOM R&S®Unified Firewalls version 10.3.0:

- PPTP VPN connections
- E-Mail reporting
- LAN accounting
- VPN SSL bridges
- Desktop notes
- Dynamic routing
- Connection-specific DNS servers
- Centralized management of the LANCOM R&S®Unified Firewalls using the gateprotect Command Center. Instead, use the LANCOM R&S®UF Command Center.

LCOS FX improvements 10.2.3

Improvements

- Allow Outlook Anywhere to traverse the reverse proxy
- Administrators can adjust upstream ciphers that are accepted by the HTTP proxy.
- Linux kernel security update to version 4.14.103
- Improved handling of large content filter blacklists
- Increased responsiveness of the Info area
- Increased mail proxy performance
- Reduced hard disk write-load
- Improved backup compatibility
- Improved import of multi-tier certificate chains

LCOS FX improvements 10.2.2

Improvements

- Optimized web-proxy logfile handling
- Improved backup migration

LCOS FX improvements 10.2.1

Improvements

- Fine-grained IP-based access control for SSH and webclient management interfaces
- Configurable listening ports for SSH and webclient management interfaces
- Info area to show detailed information on desktop nodes
- Whitelist for e-mail proxy to exclude particular senders/receivers from virus scan
- Configurable HTTPS certificate for the webclient
- SSL proxy support dropped for various outdated ciphers

LCOS FX 10.2.0

New features

- Integration of Avira Antivirus:
  - Avira Protection Cloud: machine learning and sandboxing
- IDS/IPS:
  - Improved performance thanks to a new IDS/IPS engine
  - Simplified IDS/IPS configuration including a rule exception list for eliminating false-positive results
- Statistics:
  - Security messages
  - Traffic counter
- Protocols:
  - Security messages
- Web proxy upgrade:
  - Improved HTTPS support
  - Improved performance
- FTP proxy upgrade
- Reverse proxy upgrade
- Support for link aggregation/bonding of ethernet interfaces

Improvements

- Searchable description field for desktop objects and firewall rules
- Services can be grouped.
- Desktop objects for "Host-/Network groups" can contain hosts and networks.
- Desktop objects can be tagged and filtered by tags.
- Desktop configurations (i.e. an overview of the dektop objects and firewall rules) can be exported to the file formats PDF and HTML.
- Realtime connection tracking
- DNS search domains can be pushed vie DHCP.
- The webclient supports the offline upload of updates.

4. Installation instructions for updating to LCOS FX 10.5 RU1

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.

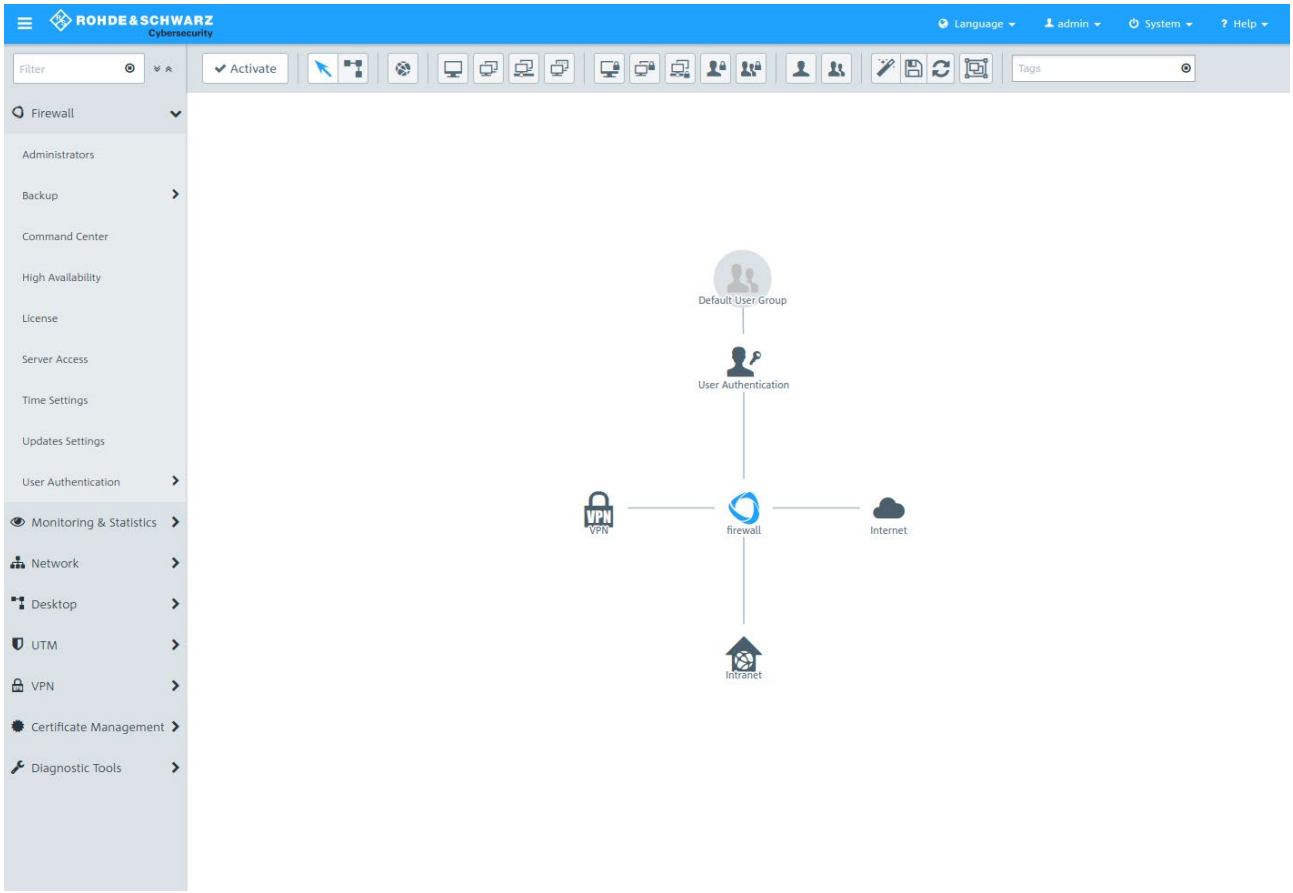
Via the auto updater on the web interface of your LANCOM R&S®Unified Firewall the respectively newer minor update version is available for step-by-step updating.

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

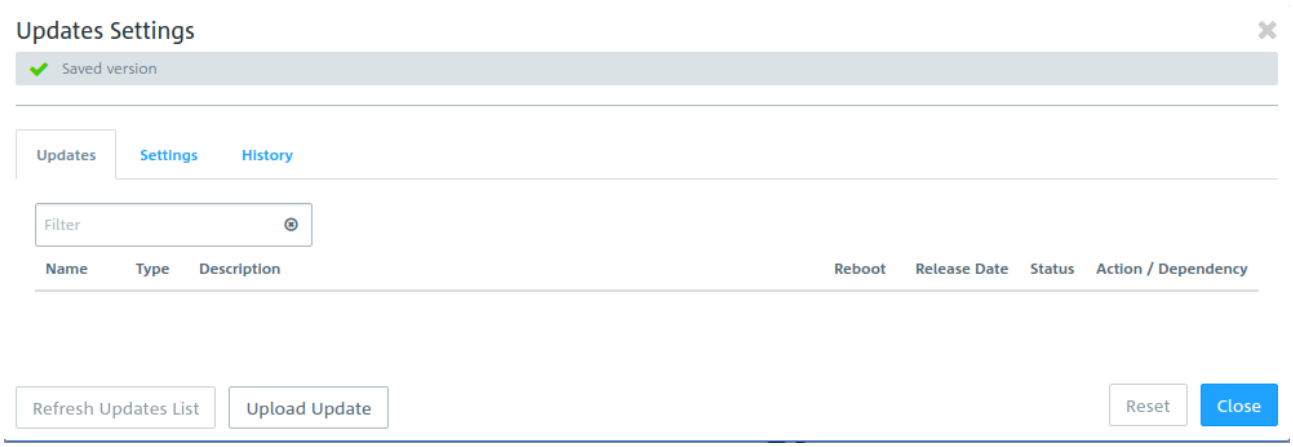
Note 2:

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

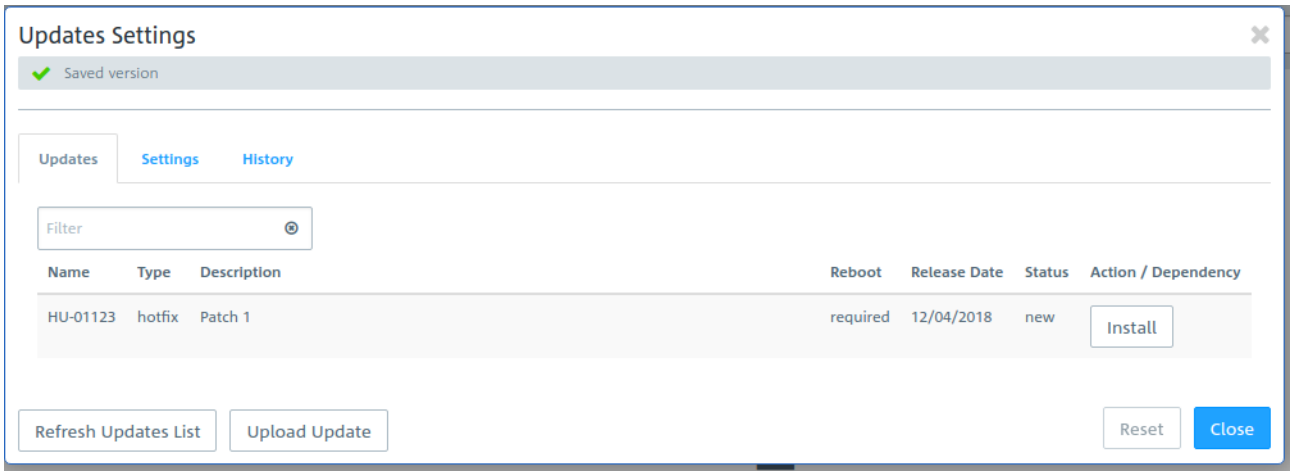
In the navigation bar on the left side, select “Updates Settings“ under the first item “Firewall“.



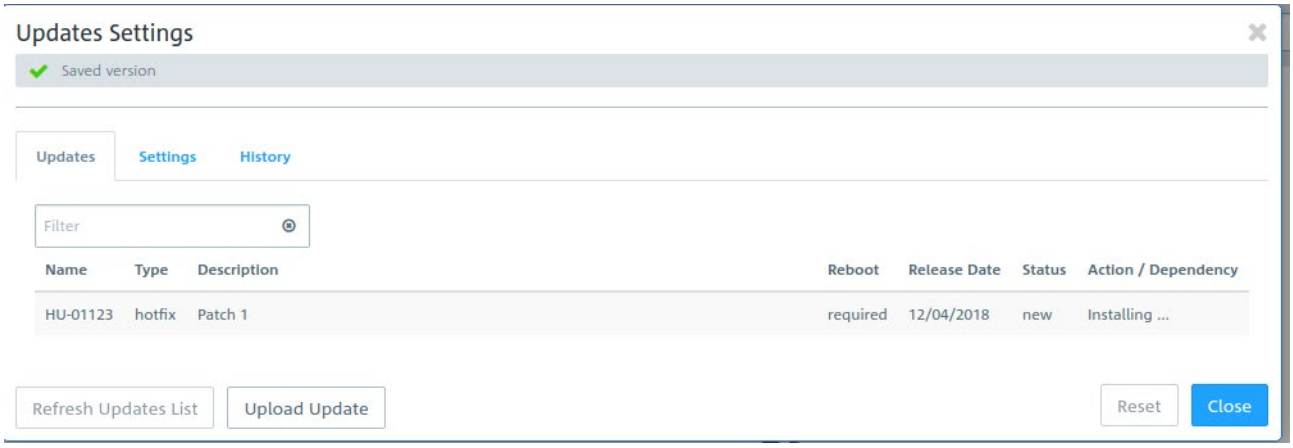
In the opening window “Updates Settings“ press the button “Refresh Updates List“ under the tab “Updates“.



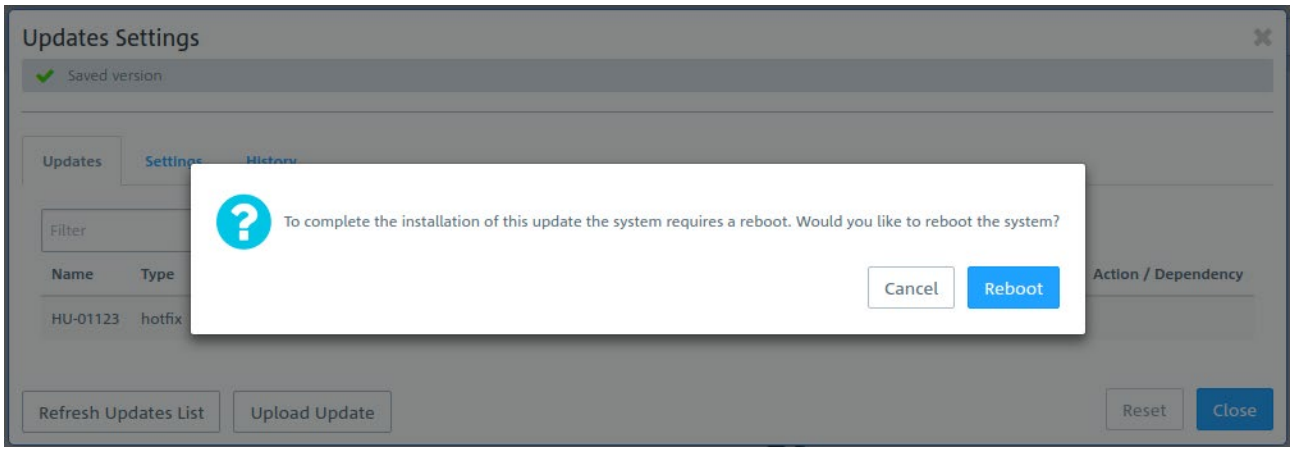
From the list, select the firmware file to install and press the “Install” button.



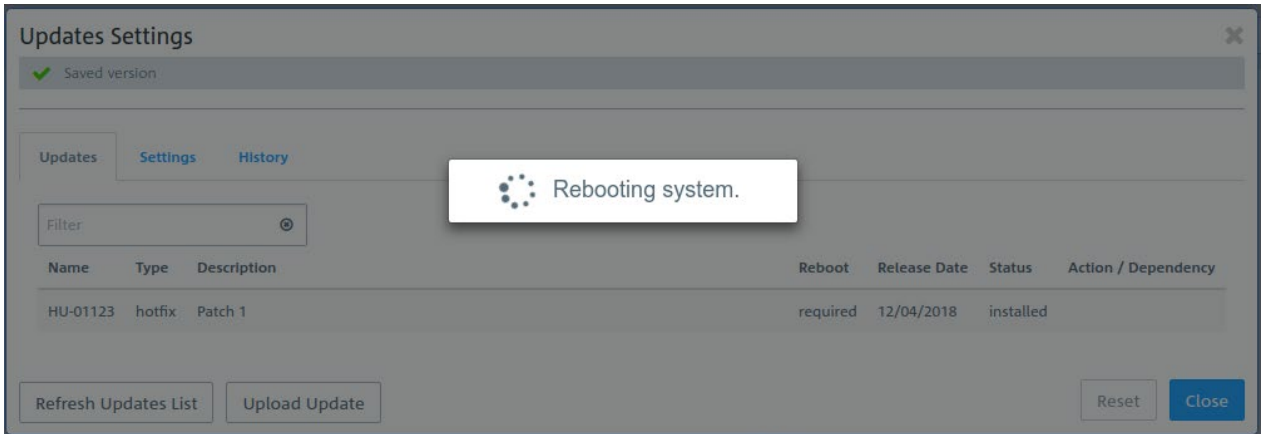
The status of the action changes to “Installing...”



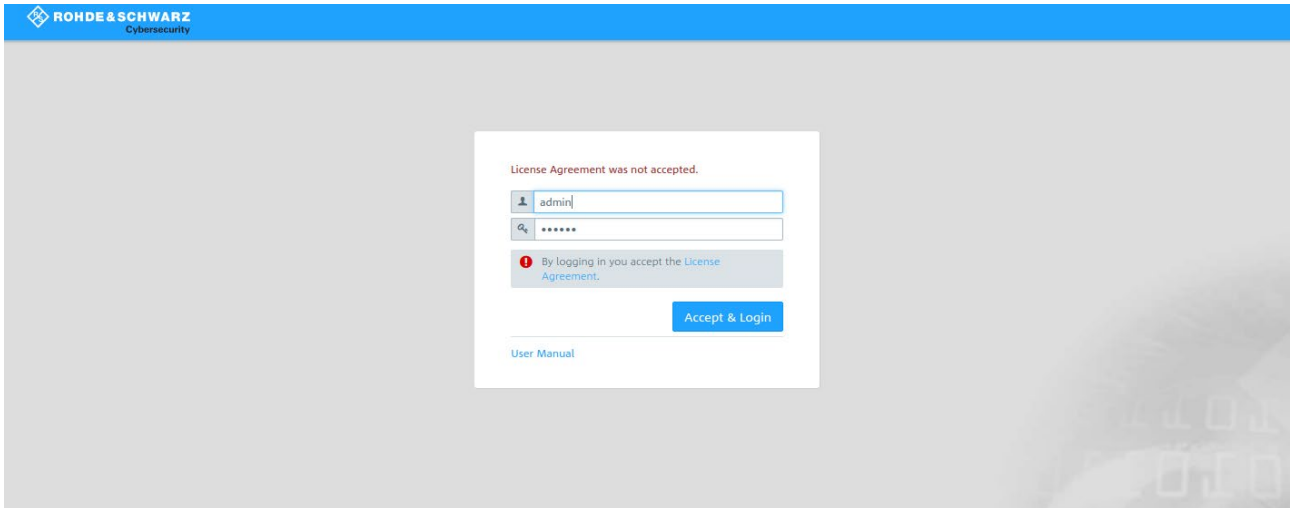
After the installation has completed a popup dialogue window appears displaying a request for rebooting the firewall. Confirm selecting “Reboot”.



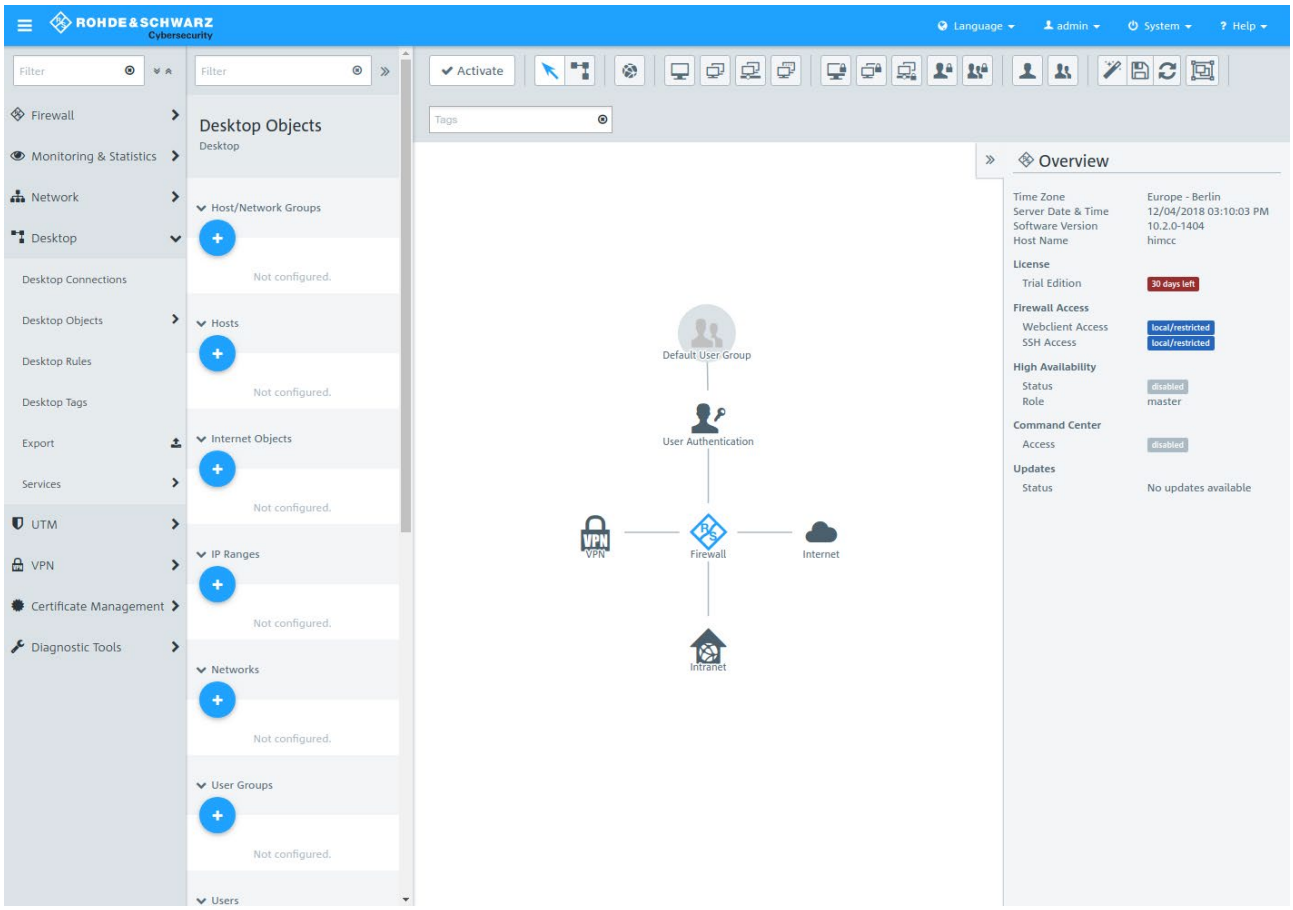
The system is rebooted.



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.


ROHDE&SCHWARZ
Cybersecurity
Language
admin
System
Help
Activate
Tags
Filter
Firewall
Monitoring & Statistics
Network
Desktop
Desktop Connections
Desktop Objects
Desktop Rules
Desktop Tags
Export
Services
UTM
VPN
Certificate Management
Diagnostic Tools
Desktop Objects
Desktop
Host/Network Groups
Not configured.
Hosts
Not configured.
Internet Objects
Not configured.
IP Ranges
Not configured.
Networks
Not configured.
User Groups
Not configured.
Users
Default User Group
User Authentication
VPN
Firewall
Internet
Intranet
Overview
Time Zone
Europe - Berlin
Server Date & Time
12/04/2018 03:10:03 PM
Software Version
10.2.0-1404
Host Name
himcc
License
Trial Edition
30 days left
Firewall Access
Webclient Access
local/restricted
SSH Access
local/restricted
High Availability
Status
disabled
Role
master
Command Center
Access
disabled
Updates
Status
No updates available

5. Further information

- Backups of versions 9.4 to 9.8, 10.0, 10.1, and 10.2 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.