



**SECURE USER GUIDANCE
FOR
LANCOM R&S® UNIFIED FIREWALL UF-360
WITH LANCOM SYSTEMS OPERATING SYSTEM
LCOS FX 10.11 RU4**

Version 1.4



TABLE OF CONTENTS

1.	General description	3
2.	Disclaimer	3
3.	Documentation.....	3
3.1	Device documentation LCOS FX 10.11 RU4	3
3.2	Acronym Table.....	3
4.	Environment.....	4
5.	Configuration	4
5.1	WebConfig.....	4
5.2	Firmware Download and Installation	4
5.3	Physical Port Configuration	4
5.4	Initial Configuration.....	5
6.	Configuration of the LANCOM R&S®Unified Firewall UF-360.....	10
6.1	Menu “Firewall → Administrators”	10
6.2	Menu “Firewall → Backup”	10
6.3	Menu “E-Mail Settings”	10
6.4	Menu “Firewall → Executive Report”	11
6.5	Menu “Firewall → Firewall Access”	11
6.6	Menu “Firewall → License”	11
6.7	Menu “Firewall → Time Settings”	11
6.8	Menu “Firewall → Update Settings”	11
6.9	Menu “Monitoring & Statistics”	11
6.10	Menu “Network → Interfaces”	13
6.11	Menu “Network → Connections”	13
6.12	Menu “DHCP Interfaces”	13
6.13	Menu “DNS”	13
6.14	Menu “Traffic Shaping”	13
6.15	Menu “Routing → Routing Rules”	13
6.16	Menu “Routing → Routing Tables”	13
6.17	Menu “Desktop”	13
6.18	Menu “VON → IPSec”	14
6.19	Menu “Certificate Management”	17
6.20	Menu “Diagnostics”	17
7.	Decommissioning	17



1. GENERAL DESCRIPTION

This document is the Secure User Guidance for the BSZ certification of the "LANCOM R&S@Unified Firewall UF-360" with LANCOM Systems Operating System "LCOS FX 10.11 RU4" and "IPSec VPN" (Target of Evaluation, TOE) at the BSI.

This document describes the requirements to operate the TOE in a secure manner. Deviations from these requirements are subject to the risk management of the administrator.

2. DISCLAIMER

This product is targeted at professional users who have the experience and knowledge to operate network components in a secure manner.

3. DOCUMENTATION

3.1 Device documentation LCOS FX 10.11 RU4

Beside this Secure User Guidance there is an additional user manual available. This document can be downloaded from the address below:

www.lancom-systems.de/download/documentation/manuals/MA_LCOS-FX-10-11-User-Manual_DE.pdf

3.2 Acronym Table

Acronym

BSI	Bundesamt für Sicherheit in der Informationstechnik
BSZ	Beschleunigte Sicherheitszertifizierung
CLI	Command Line Interface
DNS	Domain Name Service
DHCP	Dynamic Host Configuration Protocol
USB	Universal Serial Bus
LMC	LANCOM Management Cloud
UTM	Unified Threat Management
SSH	Secure Shell
SNMP	Simple Network Management Protocol
IPSec	IP security
LAN	Local Area Network
LCOS FX	LANCOM Systems Operating System; the operating system of LANCOM R&S@Unified Firewalls
NAT	Network Address Translation
PPP	Point-to-Point Protocol
TOE	Target of Evaluation
VPN	Virtual Private Network



VLAN	Virtual Local Area Network
------	----------------------------

WebConfig	Web-based management interface
-----------	--------------------------------

4. ENVIRONMENT

- 1 The administrator must ensure that physical access to the LANCOM R&S®Unified Firewall is only possible for authorized personnel and every physical access is securely logged.
- 2 The USB port of the LANCOM R&S®Unified Firewall must not be used except for reinstallation.
- 3 The serial port must not be used.

5. CONFIGURATION

5.1 WebConfig

For the management of the LANCOM R&S®Unified Firewall UF-360 the web-based management has to be used. By default, it runs on port 3438. It can only be accessed via HTTPS using TLS 1.3. Supported browsers are up-to-date versions of Google Chrome and Mozilla Firefox. In the following it is called WebConfig.

5.2 Firmware Download and Installation

- 1 Use the download area in the License portal in myLANCOM to download the LCOS FX 10.11 RU4 ISO file and the USB installer to create a bootable USB flash drive.
- 2 Check the hash values of the ISO file and the USB installer.
 - 2.1 LCOSFX 10.11 RU4 ISO sha256sum:
5A53A703200B8833B3E101D83082BE6FA40914BF6889921F1FDC9B13AD4D5651
 - 2.2 USB Installer sha256sum:
c0c084927e46465cd377d5a81f4b226c878595435e0de12e70a4777ffd448030
- 3 Use a secure USB flash drive and a secure Windows Laptop or Desktop PC to create a bootable USB flash drive with LCOS FX using the default backup as initial configuration.
- 4 Plug the USB flash drive into the LANCOM R&S®Unified Firewall and switch it on. The installation takes several minutes.
- 5 At the end of the installation, the LANCOM R&S®Unified Firewall shuts down. Unplug the USB flash drive and switch the LANCOM R&S®Unified Firewall on again.

The procedure is also described in [this Knowledge Base article](#).

5.3 Physical Port Configuration

In the certified state it is not allowed to use NIC extension modules.

For the onboard SFP+ ports only the official LANCOM SFP-SX-LC10 may be used.

The firewall must be the only physical connection between the networks which are to be protected / regulated.



5.4 Initial Configuration

- 1 Connect a secure client (Laptop or PC) directly via Ethernet to port eth1.
- 2 Open a web browser and enter the address <https://192.168.1.254:3438/> to connect to the LANCOM R&S@Unified Firewall via WebConfig.
- 3 Enter 'admin' as username and password.

admin
.....
Login
User Manual

- 4 WebConfig then asks for a new admin password to access WebConfig and for a new support password. The support password is necessary for direct access to the LCOS FX operating system via SSH or serial console. Select two different strong passwords according to the [BSI guidelines](#).

Admin password needs to be changed.
Console password needs to be changed.
License Agreement was not accepted.

admin
.....

New Admin Password
.....
.....
 Show Password

New Support Password
.....
.....
 Show Password

i The support password is the password the technical support can use to access the backend of your firewall. Please keep it safe and secure.

i By logging in you accept the License Agreement.

Cancel Accept & Login
User Manual

- 5 Start the setup wizard and follow the steps. The procedure is also described in [this Knowledge Base article](#).



5a Configure Internet access.

Internet Access LANCOM R&S®Unified Firewalls

Please set up your firewall's internet access, so that LCOS FX system updates and UTM signature updates can be downloaded. In the next steps of the wizard, you can configure how the internet connection is shared with your local networks.

Internet Interface

Internet Access

- DHCP**
The firewall is behind a router or cable modem and get assigned an IP address.
- Static Configuration**
The firewall is behind a router or cable modem that connects to the Internet.
- ADSL/SDSL**
The firewall is behind a DSL modem that connects to the Internet.
- VDSL**
The firewall is behind a VDSL modem that connects to the Internet.

5b Configure the local networks. Please note, that one physical port must be reserved for administrative access to the firewall.

LAN LANCOM R&S®Unified Firewalls

Set up the firewall for your LAN.

Active	Interface	IP and Prefix Length	Enable DHCP Server	Allow Internet Access*
<input checked="" type="checkbox"/>	eth0	This interface is used to access the internet.		
<input checked="" type="checkbox"/>	eth1	<input type="text" value="192.168.1.254/24"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Web <input checked="" type="checkbox"/> Mail
<input checked="" type="checkbox"/>	eth2	<input type="text" value="192.168.2.254/24"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Web <input checked="" type="checkbox"/> Mail
<input checked="" type="checkbox"/>	eth3	<input type="text" value="192.168.3.254/24"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Web <input checked="" type="checkbox"/> Mail

* Allowing internet access of type "Mail" will allow SMTP, POP3 and IMAP connections. Type "Web" will allow HTTP connections. The SSL/TLS variants of these protocols will be allowed too.



5c Deactivate all UTM features.

Security LANCOM R&S®Unified Firewalls

Which security features should be enabled?

Anti-Virus

The anti-virus engine monitors mail and web traffic. It protects you against malicious software from the internet using state-of-the-art machine learning and sandboxing technology.

IDS

The IDS engine monitors the network traffic between your local networks and the internet. Malicious traffic will be detected and logged.

Content Filter

The content filter makes sure no unwanted web sites are accessible. The default setting will block advertisements as well as pornographic, criminal and violent web sites.

i For the use of the security features outside of the trial period you require an appropriate license.

Cancel Wizard Step 4 of 5 Back Next

5d A summary of the settings is shown. Complete the setup wizard by clicking 'Finish'. Afterwards the settings are applied and you are logged out automatically.

Summary LANCOM R&S®Unified Firewalls

Please review your input.

General		Internet Access			Security		
Firewall Hostname	firewall	Type	DHCP	Anti-Virus	✗		
Time Zone	Europe - Berlin			IDS	✗		
Send Usage Statistics	✓			Content Filter	✗		
Send Diagnostic Reports	✓						

LAN		LAN			LAN				
	IP and Prefix Length	DHCP	Web	Mail		IP and Prefix Length	DHCP	Web	Mail
eth0	This interface is used to access the internet.				eth2	192.168.2.254/24	✓	✓	✓
eth1	192.168.1.254/24	✓	✓	✓	eth3	192.168.3.254/24	✓	✓	✓

Cancel Wizard Step 5 of 5 Back Finish



- 6 Login to the Unified Firewall again and deactivate SSH access in the menu 'Firewall → Firewall Access → SSH Settings' by clicking on the slider in the top left corner.

Allow	Title	Source
<input checked="" type="checkbox"/>	Local Networks	LAN
<input type="checkbox"/>	Internet	WAN
<input type="checkbox"/>	VPN Tunnels	VPN
<input type="checkbox"/>	LANCOM Customer Support 1	212.117.89.9/32
<input type="checkbox"/>	LANCOM Customer Support 2	217.6.21.90/32
<input type="checkbox"/>	LANCOM Customer Support 3	213.238.47.128/29
<input type="checkbox"/>	Rohde & Schwarz Internet Gateway	80.246.32.0/24
<input checked="" type="checkbox"/>	Private Networks Class C	192.168.0.0/16
<input checked="" type="checkbox"/>	Private Networks Class B	172.16.0.0/12
<input checked="" type="checkbox"/>	Private Network Class A	10.0.0.0/8

- 7 Create a new WebConfig certificate in the menu 'Certificate Management → Certificates'. In the new WebConfig certificate, enter the IP address of the administrative interface as the 'Subject Alternative Name'. The procedure is also described in [this Knowledge Base article](#).

Allow	Title	Source
<input checked="" type="checkbox"/>	Local Networks	LAN
<input type="checkbox"/>	Internet	WAN
<input type="checkbox"/>	VPN Tunnels	VPN
<input type="checkbox"/>	LANCOM Customer Support 1	212.117.89.9/32
<input type="checkbox"/>	LANCOM Customer Support 2	217.6.21.90/32
<input type="checkbox"/>	LANCOM Customer Support 3	213.238.47.128/29
<input type="checkbox"/>	Rohde & Schwarz Internet Gateway	80.246.32.0/24
<input checked="" type="checkbox"/>	Private Networks Class C	192.168.0.0/16
<input checked="" type="checkbox"/>	Private Networks Class B	172.16.0.0/12
<input checked="" type="checkbox"/>	Private Network Class A	10.0.0.0/8



- 8 Restrict WebConfig access to the administrative network (in this example 192.168.1.0/24) in the menu 'Firewall → Firewall Access → Webclient Settings'. Also, select the new WebConfig certificate created in the last step.

Webclient Settings

Modified version - changes will be preserved until you reset or log out.

Port: 3438

Webclient Certificate: WEBconfig-Certificate
Algorithm: RSA, Key Size: 4096, Hash: sha384

Private Key Password: [REDACTED]

Access Restrictions

Allow	Title	Source	
<input type="checkbox"/>	Local Networks	LAN	
<input type="checkbox"/>	Internet	WAN	
<input type="checkbox"/>	VPN Tunnels	VPN	
<input type="checkbox"/>	LANCOM Customer Support 1	212.117.89.9/32	
<input type="checkbox"/>	LANCOM Customer Support 2	217.6.21.90/32	
<input type="checkbox"/>	LANCOM Customer Support 3	213.238.47.128/29	
<input type="checkbox"/>	Rohde & Schwarz Internet Gateway	80.246.32.0/24	
<input type="checkbox"/>	Private Networks Class C	192.168.0.0/16	
<input type="checkbox"/>	Private Networks Class B	172.16.0.0/12	
<input type="checkbox"/>	Private Network Class A	10.0.0.0/8	
<input checked="" type="checkbox"/>	Administrative Network	192.168.1.0/24	

Reset Save

- 9 Deactivate the LMC connectivity in the menu 'Firewall → LMC Settings' by clicking the slider in the top left corner.

LMC Settings Firewall

Modified version - changes will be preserved until you reset or log out.

LMC Domain: cloud.lancom.de

Activation Code: [REDACTED]

Reset Save

- 10 Finally create at least one personified administrator account in the menu 'Firewall → Administrators'.

After the initial configuration, the administrator account with the name 'admin' must only be used to create personal administrator accounts.

Management of the LANCOM R&S@Unified Firewall must be conducted using personal administrator accounts, which can be unambiguously related to one specific person.



The screenshot shows a configuration dialog titled "Admin-Meier Administrator". At the top, a yellow star icon indicates a new configuration, with the text: "New - changes will be preserved until you cancel this dialog or log out." Below this, the "Name" field contains "Admin-Meier" and the "Description" field contains "Personal Administrator for Mr. Meier". There are two tabs: "Client Access" (selected) and "Webclient Permissions". Under "Client Access", the "Web Client Access" checkbox is checked. Below it are two password fields, both masked with dots. There are two checkboxes: "Show Password" (unchecked) and "Require password change after next login" (unchecked). At the bottom right, there are "Cancel" and "Create" buttons.

6. CONFIGURATION OF THE LANCOM R&S@UNIFIED FIREWALL UF-360

In the evaluated state, only the features and services described in this chapter may be used plus features and services which are active in the default configuration and which were not disabled during the initial configuration.

For the involved risks and guidance for secure configuration when using features which were not evaluated see the manual of the firewall (accessible via WebConfig -> Help), the Knowledge Base (<https://knowledgebase.lancom-systems.de/display/KBEN>) and the general security information (<https://www.lancom-systems.com/service-support/general-security-information>).

6.1 Menu "Firewall → Administrators"

The administrative user account must be created as described in Chapter 5.3, Step 10. It is mandatory that one administrative user account per person exists in the configuration of the Unified Firewall.

6.2 Menu "Firewall → Backup"

There are no restrictions on the use of the functions in this configuration menu. Please ensure that the backups created are kept in a safe and secure place or storage.

6.3 Menu "E-Mail Settings"

There are no restrictions on the use of the functions in this configuration menu.

6.4 Menu “Firewall → Executive Report”

There are no restrictions on the use of the functions in this configuration menu.

6.5 Menu “Firewall → Firewall Access”

The access to the LANCOM R&S@Unified Firewall via WebConfig must be restricted as described in Chapter 5.3, Step 7.

6.6 Menu “Firewall → License”

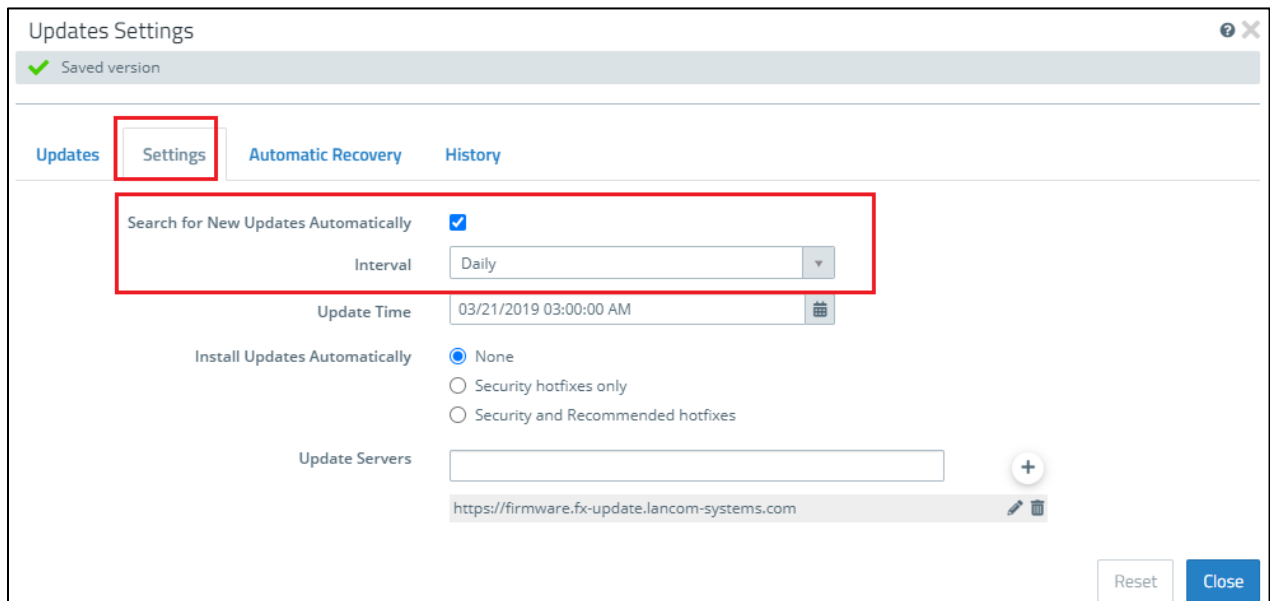
There are no restrictions on the use of the functions in this configuration menu.

6.7 Menu “Firewall → Time Settings”

There are no restrictions on the use of the functions in this configuration menu.

6.8 Menu “Firewall → Update Settings”

There are no restrictions on the use of the functions in this configuration menu. Please make sure to check for new updates in the update settings on a regular basis.



6.9 Menu “Monitoring & Statistics”

It is recommended to regularly check all three available logs:

- **System Log:** The System Log creates and displays a list of recent system events.
- **Alert Log:** In the Alert Log editing window, you can see what traffic is blocked by your LANCOM R&S@Unified Firewall or how traffic was transmitted through the firewall.
- **Audit Log:** The Audit Log creates records about every configuration change made on your LANCOM R&S@Unified Firewall (e.g. updating the VPN settings), executed actions (e. g. importing a backup) and what caused the change or action.

Further information on the configuration of the logs can be found in chapter 3.4.2.8 of the user manual.



6.9.1 Usage of SNMP

SNMP is allowed only by using SNMPv3 with a secure password.

SNMP Settings

Modified version - changes will be preserved until you reset or log out.

Listening IP: 0.0.0.0

Listening Port: 161

Protocol Version: v3

Username: testuser

Authentication Protocol: SHA

Authentication Password:

Show Authentication Password

Privacy Protocol: AES

Privacy Password:

Show Privacy Password

Location: _____

Contact: _____

Reset Save

6.9.2 E-Mail Notifications

The use of E-Mail Notifications is allowed. Be aware that emails contain sensitive information and must therefore be transmitted in encrypted form (e.g. via SMIME encryption) and received and stored in a secure location.

6.9.3 External Syslog

The use of an external Syslog-Server is only allowed by using a secure IPSec VPN tunnel to the server.



6.10 Menu “Network → Interfaces”

The following interfaces can be used without any restrictions. The use of interfaces that are not listed is not permitted for BSI-compliant use of the LANCOM R&S®Unified Firewall.

- Ethernet interfaces
- VLAN interfaces
- Bond interfaces
- Bridge interfaces
- PPP interfaces

Attention: The use of VLANs on Bridge interfaces is forbidden because Bridges can use VLAN interfaces as bridge ports.

Attention: The firewall must be the only logical connection between the networks which are to be protected / regulated.

6.11 Menu “Network → Connections”

The following connections can be used without any restrictions:

- Network connections
- PPP connections

6.12 Menu “DHCP Interfaces”

There are no restrictions on the use of the functions in this configuration menu.

6.13 Menu “DNS”

There are no restrictions on the use of the functions in this configuration menu.

6.14 Menu “Traffic Shaping”

There are no restrictions on the use of the functions in this configuration menu.

6.15 Menu “Routing → Routing Rules”

There are no restrictions on the use of the functions in this configuration menu. Please be aware that triangular routing has to be avoided for the connection tracking to function properly.

6.16 Menu “Routing → Routing Tables”

There are no restrictions on the use of the functions in this configuration menu. Please be aware that triangular routing has to be avoided for the connection tracking to function properly.

6.17 Menu “Desktop”

The following desktop objects can be used without any restrictions:

- Internet Objects
- VPN Networks
- VPN Hosts
- VPN Groups



- Network
- Hosts
- Host Groups

6.17.1 Desktop Connections

In desktop connections, the following items are allowed to be used:

- Protocol/port-based filter
- NAT
- URL/Content Filter

The use of the following items is forbidden:

- Application filter
- Application-based routing.

6.18 Menu “VON → IPSec”

- 1 When creating VPN connections, it is mandatory to use the existing BSI security profile.

Headquarter Connection

★ New - changes will be preserved until you cancel this dialog or log out.

Name: Headquarter

Template: (empty)

Security Profile: BSI TR-02102-3 IKEv2 recommended until 20...
IKEv2

Connection: eth0 WAN Connection

All configured IP addresses of this connection are used.



- Secure passwords and certificates with a secure key length (see [BSI technical guideline](#)) must be used in the Authentication tab.

Headquarter Connection

★ New - changes will be preserved until you cancel this dialog or log out.

Name:

Template:

Security Profile:
IKEv2

Connection Tunnels **Authentication** Routing Traffic Shaping

Authentication Type:

Local

PSK (Preshared Key):

Local Certificate:
Algorithm: RSA, Key Size: 4096, Hash: sha384

Private Key Password:

Local Identifier:



6.18.1 Access to the Administration Client via IPSec

- 1 In the menu 'VPN → IPSec → Virtual IP Pools' create a new virtual IP pool with a network that is not used anywhere else in the network.

Admin Virtual-IP pool Virtual IP Pool

New - changes will be preserved until you cancel this dialog or log out.

Changes to the IP pool will be activated in the related connections only when they are manually restarted. All related connections can be restarted via the entry of the IP pool list.

Name: Admin Virtual-IP pool

Used in: -

IP Pool: 192.168.99.0/24

Preferred DNS Server: 8.8.8.8

Alternate DNS Server:

Preferred WINS Server:

Alternate WINS Server:

DNS Search Domains: +

Cancel Create

- 2 Go to the menu 'VPN → IPSec → Connections' and create a dedicated IPSec connection for an administrator using the new virtual IP pool. Please also refer to chapter 6.18 regarding the creation of IKEv2 connections.

Admin-Meier Connection

New - changes will be preserved until you cancel this dialog or log out.

Name: Admin-Meier

Template:

Security Profile: BSI TR-02102-3 IKEv2 recommended until 20...
IKEv2

Connection Tunnels Authentication Routing Traffic Shaping

Local Networks: 192.168.1.0/24

Remote Networks: +

Virtual IP Pool: Admin Virtual-IP pool
IP Pool: 192.168.99.0/24

Virtual IP:

IKEv2 Compatibility Mode:

Cancel Create

- 3 Finally, add the Virtual IP pool in the menu ‘Firewall → Firewall Access → Webclient Settings’.

Webclient Settings

Modified version - changes will be preserved until you reset or log out.

Port: 3438

Webclient Certificate: WEBconfig-Certificate
 Algorithm: RSA, Key Size: 4096, Hash: sha384

Private Key Password:

Access Restrictions

Allow	Title	Source
<input type="checkbox"/>	Local Networks	LAN
<input type="checkbox"/>	Internet	WAN
<input type="checkbox"/>	VPN Tunnels	VPN
<input type="checkbox"/>	LANCOM Customer Support 1	212.117.89.9/32
<input type="checkbox"/>	LANCOM Customer Support 2	217.6.21.90/32
<input type="checkbox"/>	LANCOM Customer Support 3	213.238.47.128/29
<input type="checkbox"/>	Rohde & Schwarz Internet Gateway	80.246.32.0/24
<input type="checkbox"/>	Private Networks Class C	192.168.0.0/16
<input type="checkbox"/>	Private Networks Class B	172.16.0.0/12
<input type="checkbox"/>	Private Network Class A	10.0.0.0/8
<input checked="" type="checkbox"/>	Administrative Network	192.168.1.0/24
<input checked="" type="checkbox"/>	Administrative VPN	192.168.99.0/24

Reset Save

6.19 Menu “Certificate Management”

- 1 Let's Encrypt must not be used for BSI-compliant operation of the Unified Firewall.
- 2 There are no restrictions on the use of the other functions in this configuration menu.
- 2a Always use strong passwords.
- 2b Use a key length according to BSI technical guideline.

6.20 Menu “Diagnostics”

There are no restrictions on the use of the functions in this configuration menu.

7. DECOMMISSIONING

To decommission a LANCOM R&S®Unified Firewall, the following steps must be carried out:

- 1 Perform a factory reset and make sure, the option “Delete Logs” is checked.

Resetting system to factory settings

Delete Logs

Cancel Reset and Reboot

- 2 If the LANCOM R&S®Unified Firewall is to be scrapped, please open the unit and destroy the built-in hard disk or have it destroyed by a specialist data destruction company. No logs or configuration data are stored outside the hard disk.