SECURE. **NETWORKS.**

LCOS FX 10.6

Addendum

08/2021

LANCOM
Systems

Contents

Copyright

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and/or omissions.

This product contains separate open-source software components which are subject to their own licenses, in particular the General Public License (GPL). If the respective license demands, the source files for the corresponding software components will be provided on request. Please send an e-mail to *gpl@lancom.de*.

Products from LANCOM Systems include software developed by the "OpenSSL Project" for use in the "OpenSSL Toolkit" (*www.openssl.org*).

Products from LANCOM Systems include cryptographic software written by Eric Young (*eay@cryptsoft.com*).

Products from LANCOM Systems include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from LANCOM Systems contain the LZMA SDK developed by Igor Pavlov.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom-systems.com

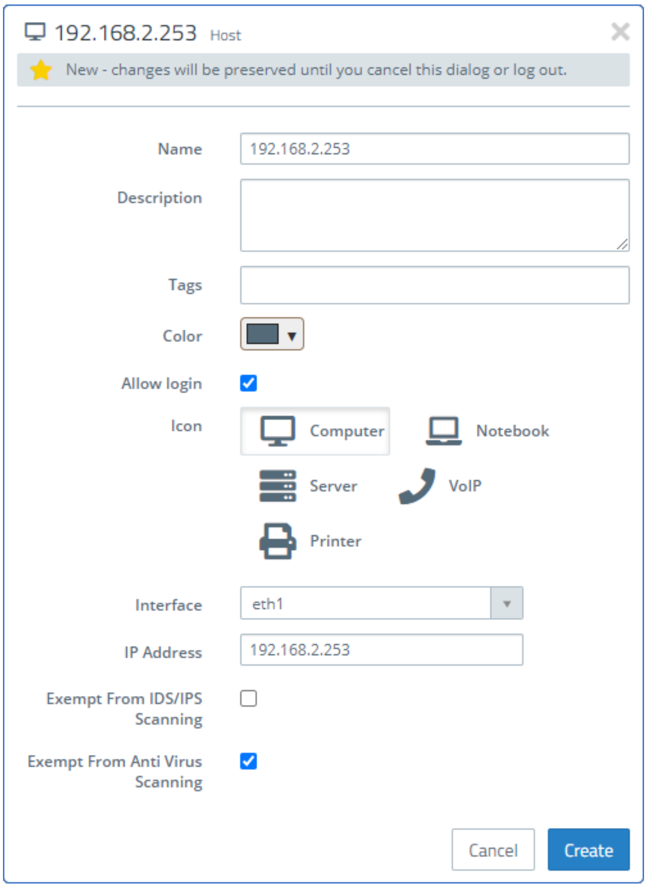
1 Addendum to LCOS FX version 10.6

This document describes the changes and enhancements in LCOS FX version 10.6 since the previous version.

2 IDS / IPS and anti virus per network

As of LCOS FX version 10.6 RU3, individual hosts or networks can now be specifically excluded from scanning by the IDS / IPS and the anti virus functions of the LANCOM R&S®Unified Firewall. The settings for this are made in the respective desktop objects (host 🖥, network 🖧 host / network group objects 🗗).

The settings look the same for hosts and networks, shown here using the example of a host object:



🖥 192.168.2.253 Host

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

Name: 192.168.2.253

Description:

Tags:

Color: ▾

Allow login: ☑

Icon: Computer, Notebook, Server, VoIP, Printer

Interface: eth1

IP Address: 192.168.2.253

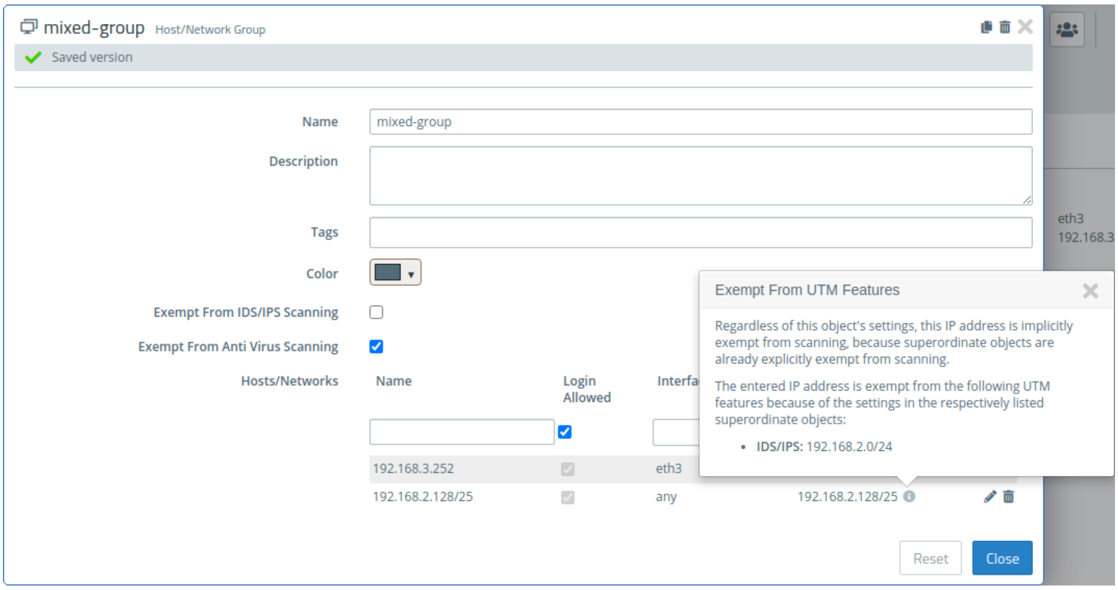
Exempt From IDS/IPS Scanning: □

Exempt From Anti Virus Scanning: ☑

Figure 1: Host object

The lower two check marks can be used to explicitly exclude the object from being checked by the respective feature. An object can also be implicitly excluded from the check. This is the case if it is located in a network area that has already been explicitly excluded from the check by a higher-level object. In this case, a corresponding note appears below the checkbox, which also lists the names of the objects from which the setting was “inherited”.

Exclusion from scanning is done in the same way for host / network groups with a corresponding check mark. However, the individual group members must be considered individually for displaying a corresponding notice regarding the implicit exclusion from the IDS / IPS and anti virus features.



mixed-group Host/Network Group

✓ Saved version

Name: mixed-group

Description:

Tags:

Color:

Exempt From IDS/IPS Scanning □

Exempt From Anti Virus Scanning ☑

Hosts/Networks

Name	Login Allowed	Interfa
	☑	
192.168.3.252	☑	eth3
192.168.2.128/25	☑	any 192.168.2.128/25 ℹ

Exempt From UTM Features

Regardless of this object's settings, this IP address is implicitly exempt from scanning, because superordinate objects are already explicitly exempt from scanning.

The entered IP address is exempt from the following UTM features because of the settings in the respectively listed superordinate objects:

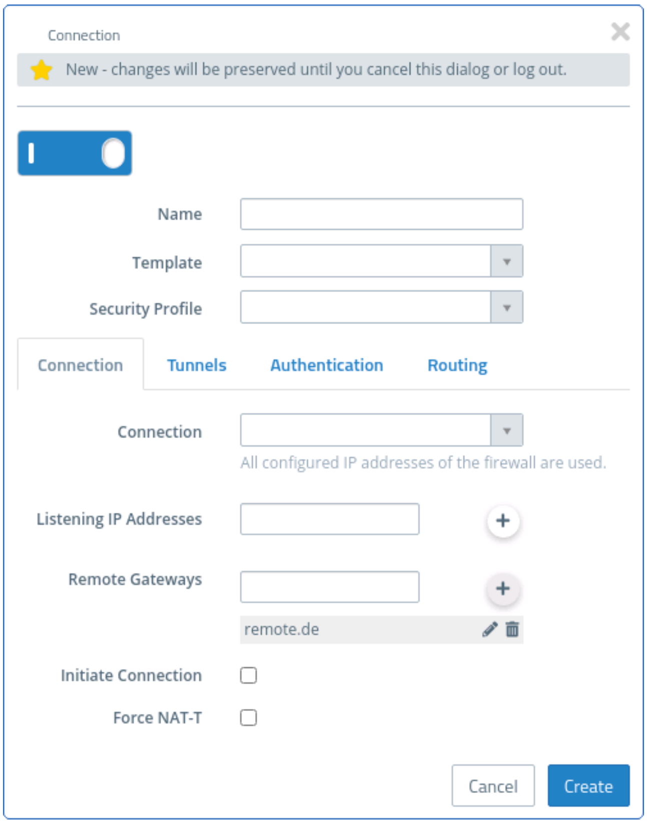
- **IDS/IPS:** 192.168.2.0/24

Figure 2: Group object

If a group member is already implicitly excluded from the check, a small ℹ icon appears to the right of the IP address. Clicking on this then opens a small popover with an explanation as well as a list of the UTM features from which the group member is excluded and from which parent objects this setting was inherited.

3 IPsec connection settings

As of LCOS FX version 10.6 RU3, the remote gateway settings have changed. Instead of just one remote gateway, a list of gateways can now be entered. This change affects both the settings of an IPsec connection (**VPN** > **IPsec** > **Connections**) and those of a connection template (**VPN** > **IPSec** > **Templates**).

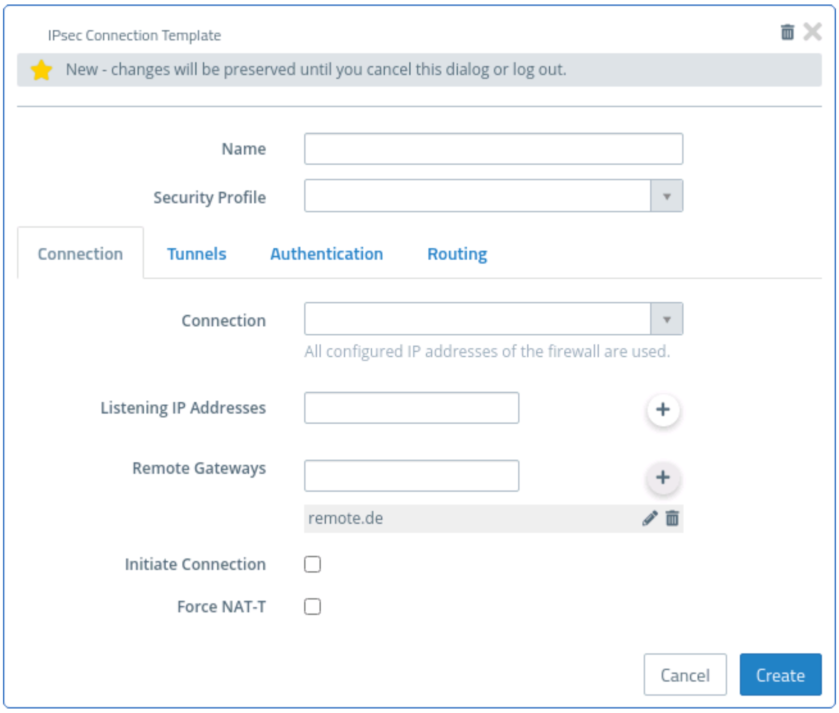

Connection

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

All configured IP addresses of the firewall are used.

remote.de

Figure 3: IPsec connection



IPsec Connection Template

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

Name

Security Profile

Connection

All configured IP addresses of the firewall are used.

Listening IP Addresses

Remote Gateways

remote.de

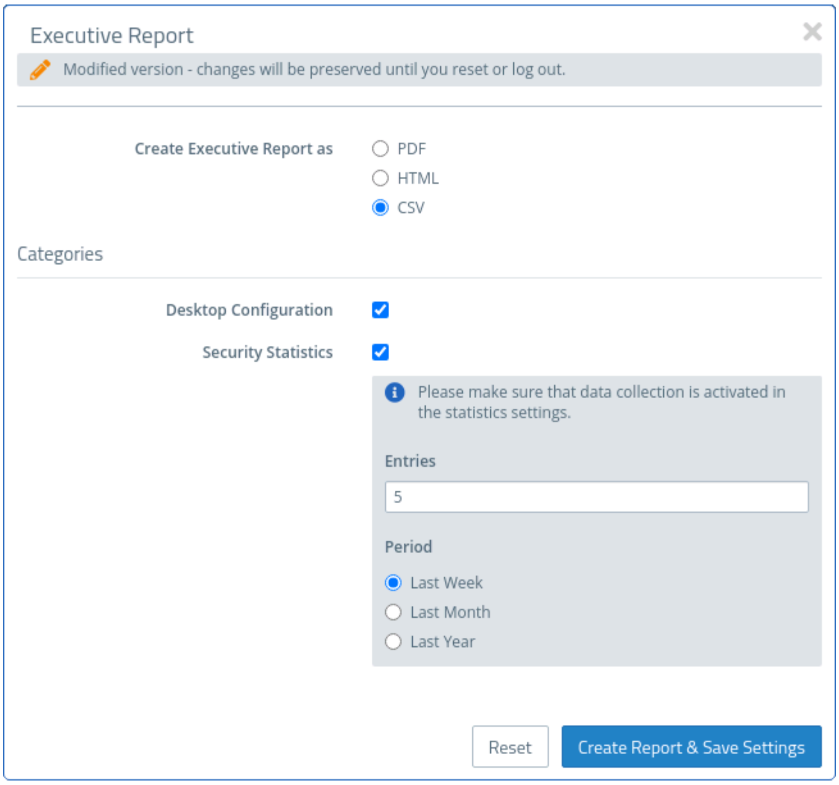
Initiate Connection □

Force NAT-T □

Figure 4: IPsec connection template

4 Executive report as CSV export

From LCOS FX version 10.6 RU1 the Executive report can also be exported in CSV format.



Executive Report

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

Create Executive Report as ○ PDF ○ HTML ● CSV

Categories

Desktop Configuration ☑

Security Statistics ☑

Please make sure that data collection is activated in the statistics settings.

Entries: 5

Period: ● Last Week ○ Last Month ○ Last Year

With the CSV format, the tables are created as individual `csv` files and packed together as a ZIP file for saving. This simplifies any further processing of the data.

5 DNS settings

From LCOS FX version 10.6 the DNS settings are now divided between two menu items under **Network** > **DNS Settings**. One for the global settings (**General Settings**), which apply if no network-specific settings override them. And one for the network-specific settings (**Network-Specific Settings**), in which settings can be made depending on the source network from which DNS requests originate.

5.1 General settings

Navigate to **Network** > **DNS Settings** > **General Settings** to configure the global DNS settings for your LANCOM R&S®Unified Firewall.

The DNS server settings are usually specified by the WAN connection. You should only need to configure the DNS server settings if you cannot obtain them over the WAN connection.

In the **General Settings** editing window you can modify the following parameters:

Input box	Description
Acquired Servers	Listed here are the DNS servers that have been learned via DHCP and PPP connections or similar.
DNS Servers	This table allows the configuration of 1 to 2 DNS servers per zone. A zone is a specific DNS area like "*.company.intern". The default zone "*" is the zone that every DNS address falls into that doesn't fall into a specifically defined zone. The setting "AUTO" is valid for the default zone only. It cannot be used in combination with manually specified IP addresses; it must stand alone. If set to "AUTO", the automatically learned DNS servers listed above are used. You can sort the table according to your needs, with the exception of the default zone which is always the last element and cannot be deleted.
Multicast-DNS-Relay	Activate the multicast DNS relay here. Multicast DNS (mDNS) is an alternative to conventional DNS for resolving host names in (small) networks. Here, rather than requesting the name resolution from a server, a request is sent to and processed by all of the hosts that can be reached through the multicast address. Popular implementations of mDNS are Bonjour (Apple) and Avahi (Linux), which enable various devices (e.g. network printers) to be networked without having to perform any configurations beforehand.

If you change any settings, click **Save** to store your changes or **Reset** to discard them. Then click **Close** to quit the editing window.

Click ✔ **Activate** in the toolbar at the top of the desktop to apply your configuration changes.

5.2 Network-specific settings

Navigate to **Network** > **DNS Settings** > **Network-Specific Settings** to make alternative configurations based on the source network of DNS queries.

In the **Network-Specific Settings** editing window you can modify the following parameters:

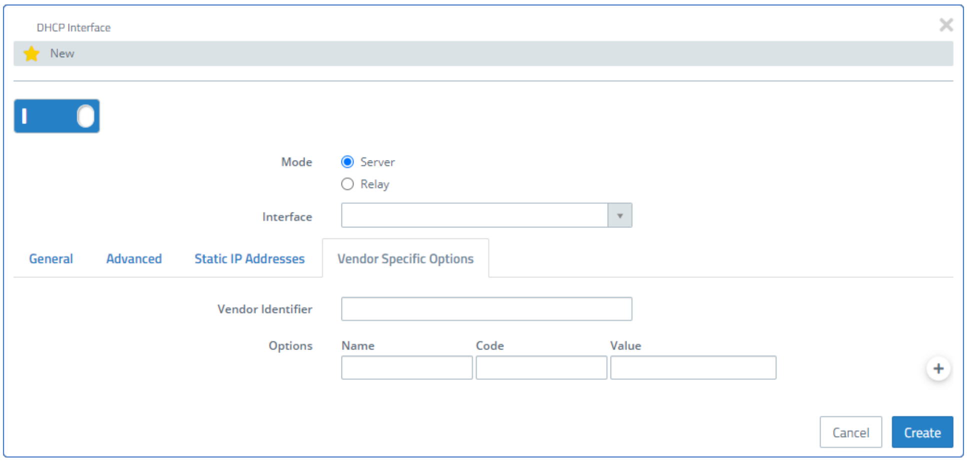
Input box	Description
I/0	A slider button indicates whether this collection of settings is currently enabled (**I**) or disabled (**0**). Click on the slider button to change this. A new collection of settings is enabled by default.
Name	Give these network-specific settings a name here.
Source Networks	Enter a list of the subnets for which this entry should apply. ❗ The different collections of settings must have unique names, and the source networks must not be used multiple times, nor may they overlap.
DNS Servers	This table allows the configuration of 1 to 2 DNS servers per zone. A zone is a specific DNS area like "*.company.intern". Unlike with the global settings, it is not strictly necessary to set the default zone "*". If a DNS request is received for a name that is not in one of the listed zones, name resolution is performed using the global settings. ⓘ The setting "AUTO" cannot be used here, you have to use specific DNS server addresses.
Global Settings	The currently valid global settings are listed here. The table cannot be edited here and merely serves to provide an overview when creating network-specific tables.

If you change any settings, click **Save** to store your changes or **Reset** to discard them. Then click **Close** to quit the editing window.

Click ✔ **Activate** in the toolbar at the top of the desktop to apply your configuration changes.

6 DHCP options

From LCOS FX version 10.6 the DHCP settings include the option to configure manufacturer-specific options (DHCP option 43). A new tab has been added to the DHCP interface settings for this purpose. This is used by the LANCOM Management Cloud to distribute the LMC domain, project ID and location to other LANCOM devices, such as access points.



DHCP Interface

New

Mode ● Server ○ Relay

Interface

Vendor Identifier

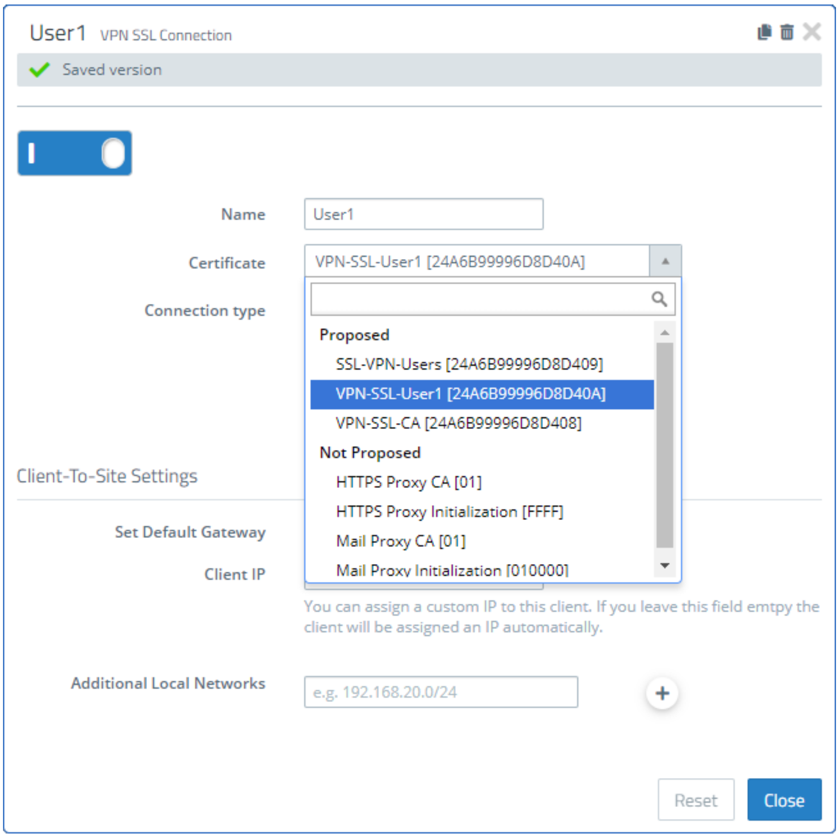
Options Name Code Value

Manufacturer-specific options on the tab:

Input box	Description
Vendor Identifier	Here you can configure manufacturer-specific options (DHCP option 43). The ID has a maximum of 64 characters consisting of a-z, A-Z, 0-9 and _. This is used by the LANCOM Management Cloud to distribute the LMC domain, project ID and location to other LANCOM devices, such as access points.
Options	› **Name** The name of the option. This has a maximum of 64 characters consisting of a-z, A-Z, 0-9 and _. › **Code** Number of the option that should be sent to the DHCP client. The option number describes the information transmitted, e.g. “43” for manufacturer-specific options. ! You can find a list of all DHCP options in *RFC 2132 – DHCP Options and BOOTP Vendor Extensions* of the Internet Engineering Task Force (IETF). › **Value** With this field you define the contents of the DHCP option. IP addresses are specified with the usual notation for IPv4 addresses, e.g. as “123.123.123.100”, integer types are entered as normal decimal numbers, and strings as simple text. Multiple values in a single field are separated with commas, e.g. “123.123.123.100, 123.123.123.200”. The maximum length of the field is 64 characters.

7 Recommended certificates for VPN SSL connections

From LCOS FX version 10.6 the VPN SSL connection settings now also show which CAs are “Recommended” and can be used for a VPN SSL connection.


User1 VPN SSL Connection

Saved version

Name: User1

Certificate: VPN-SSL-User1 [24A6B99996D8D40A]

Proposed
- SSL-VPN-Users [24A6B99996D8D409]
- VPN-SSL-User1 [24A6B99996D8D40A]
- VPN-SSL-CA [24A6B99996D8D408]

Not Proposed
- HTTPS Proxy CA [01]
- HTTPS Proxy Initialization [FFFF]
- Mail Proxy CA [01]
- Mail Proxy Initialization [010000]

Connection type

Client-To-Site Settings

Set Default Gateway

Client IP

You can assign a custom IP to this client. If you leave this field emtpy the client will be assigned an IP automatically.

Additional Local Networks: e.g. 192.168.20.0/24

An advantage of using the CA is that several connections can be exported that only need to be defined once on the firewall. You do this in the VPN-SSL connections export dialog by selecting a CA certificate under **Remote Certificate**.

In the case of a CA connection, the user must select a certificate that was signed by the configured CA. With normal certificate connections, the configured certificate is preselected and the field is deactivated.

If additional local networks are to be transmitted to the clients, they have to be configured globally in the VPN-SSL settings dialog. A notice for users has also been added to the connection dialog for the additional local networks.