LCOS FX 10.13

Addendum

09/2023

LANCOM
SYSTEMS

Contents

1 Addendum to LCOS FX version 10.13..4
2 Rule inheritance...5
3 LANCOM Trusted Access...6
4 Sending alerts to the LANCOM Management Cloud..............................8
5 MTU for route-based IPsec connections...9
6 curl heartbeats for WAN connections..10

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.

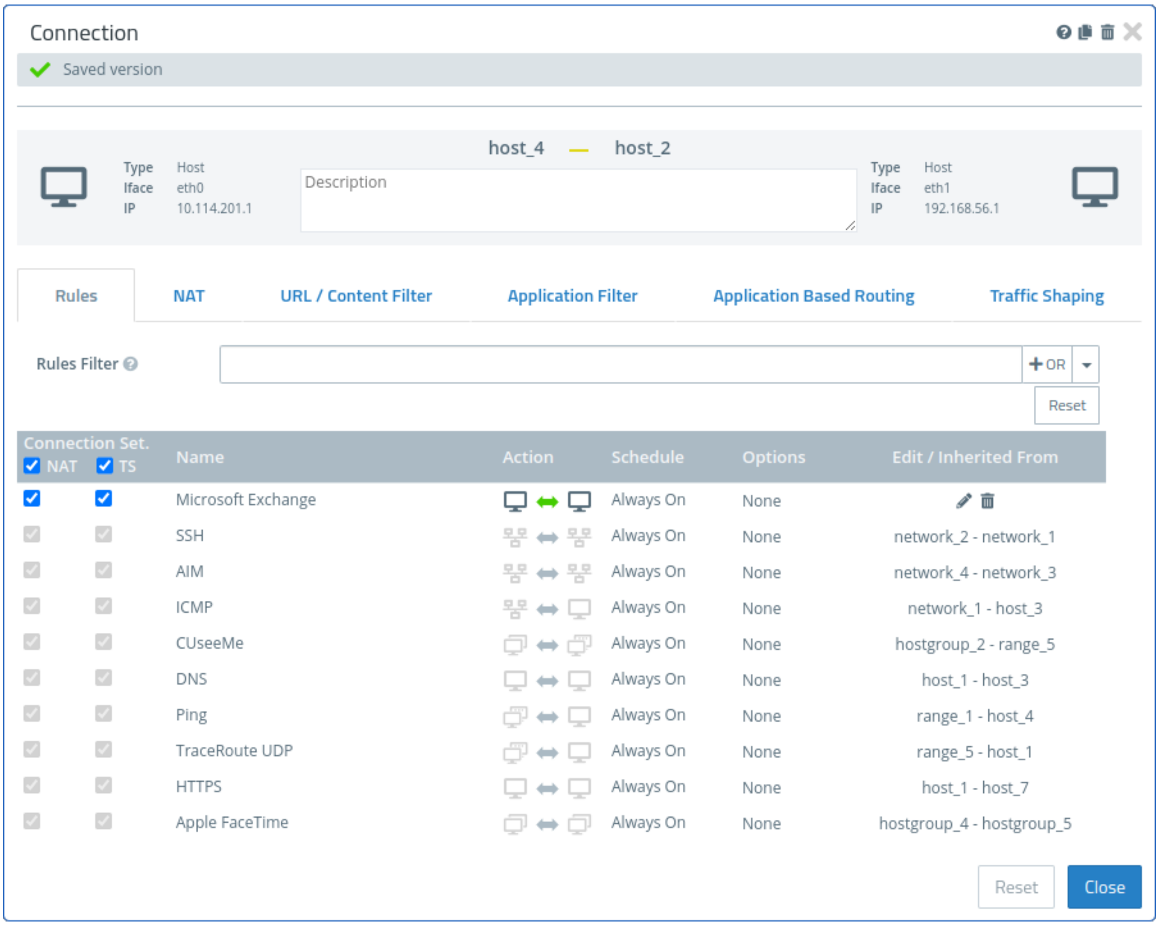
LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Wuerselen
Germany
www.lancom-systems.com

1 Addendum to LCOS FX version 10.13

This document describes the changes and enhancements in LCOS FX version 10.13 since the previous version.

2 Rule inheritance

The dialog for a connection between two desktop objects has been revised and extended with new functions. Additional information for the connected desktop objects is displayed in the upper area. e.g. interface used or IP address.



Connection

✓ Saved version

host_4 — host_2

Type	Host
Iface	eth0
IP	10.114.201.1

Description

Type	Host
Iface	eth1
IP	192.168.56.1

Rules Filter

Connection Set. ☑ NAT	 ☑ TS	Name	Action	Schedule	Options	Edit / Inherited From
☑	☑	Microsoft Exchange	↔	Always On	None	✎ 🗑
☑	☑	SSH	↔	Always On	None	network_2 - network_1
☑	☑	AIM	↔	Always On	None	network_4 - network_3
☑	☑	ICMP	↔	Always On	None	network_1 - host_3
☑	☑	CUseeMe	↔	Always On	None	hostgroup_2 - range_5
☑	☑	DNS	↔	Always On	None	host_1 - host_3
☑	☑	Ping	↔	Always On	None	range_1 - host_4
☑	☑	TraceRoute UDP	↔	Always On	None	range_5 - host_1
☑	☑	HTTPS	↔	Always On	None	host_1 - host_7
☑	☑	Apple FaceTime	↔	Always On	None	hostgroup_4 - hostgroup_5

Figure 1: Connection between desktop objects

As before, the selected services are displayed in the table in the **Rules** tab. In addition, the rules configured between parent objects are now also displayed. These inherited rules cannot be edited directly. However, by clicking on the rule name, the settings for these rules can be viewed. In the **Edit / Inherited from** column, instead of the edit buttons, the names of the connections from which these rules are used are displayed. By clicking on these names, the corresponding connection can be opened directly.

You can use the filter function to limit the display of rules so that you can more quickly determine whether a particular rule already exists. Filter criteria are

- Text for names, rule names, connection names and protocols
- Numbers for port and port ranges
- Booleans e.g. for DMZ, proxy or NAT

3 LANCOM Trusted Access

In the context of LANCOM Trusted Access (LTA) there are some additions to be able to display the settings coming from the LANCOM Management Cloud in a meaningful way. For LANCOM Trusted Access, the access rules are configured in the LANCOM Management Cloud. Rules are always created between a user group and a connection target.

LANCOM Trusted Access is the trusted network access security solution for enterprise networks. It enables secure and scalable access to enterprise applications for employees in the office, at home, or on the road, protecting modern hybrid working from anywhere, anytime. The LANCOM Trusted Access solution adapts to increasing security requirements in your organization and enables both cloud-managed VPN client networking for access to entire networks and the move to a zero trust security architecture for comprehensive network security. Based on granular access rights, users are only granted access to applications that have been assigned to them (zero trust principle). Existing systems for managing users and user groups (Active Directory) can be fully integrated into the (LMC). For smaller networks, the LMC alternatively offers internal user management. LANCOM Trusted Access 100% GDPR compliant and scales for small businesses as well as for very large networks with several thousand users.

LTA user groups

To distinguish LTA user groups from local/LDAP groups, a new group type has been added: LTA groups. A new desktop icon represents LTA user groups.

Icon / button	Description
👥	Create a LANCOM Trusted Access user group.

Create desktop objects for LTA user groups (LANCOM Trusted Access). Normally, these are only displayed here because they are managed via the LANCOM Management Cloud.

Navigate to **Desktop** > **Desktop Objects** > **LTA Group** to display the list of LTA user group objects currently created in the system in the Object bar.

The **LTA Group** configuration dialog allows you to configure the following elements:

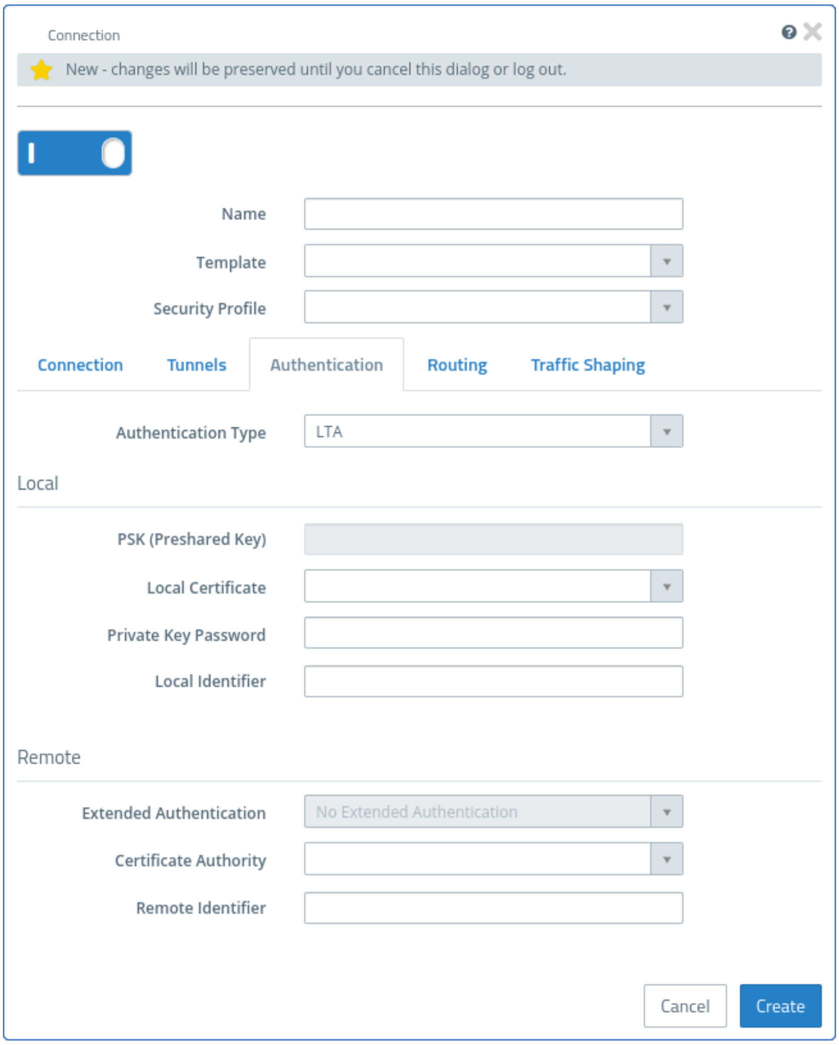
Input box	Description
Name	Specify a name for the LTA user group.
Description	Optional: Enter additional information on the LTA user group object for internal use.
Group ID	The group ID used in the user's certificate.
Tags	Optional: From the drop-down list, select the desktop tags that you want to assign to the LTA user group.
Color	Select the color to be used for this object on the desktop.

The buttons at the bottom right of the editor panel depend on whether you add a new LTA user group or edit an existing group. For a newly configured group, click **Create** to add the group to the list of available LTA user groups or **Cancel** to discard your changes. To edit an existing group, click **Save** to store the reconfigured group or **Reset** to discard your changes. You can click **Close** to shut the editor panel as long as no changes have been made on it.

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

LTA authentication for IPSec

For IPSec connections, there is a new authentication type called LTA.



Connection

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

Name

Template

Security Profile

Authentication Type: LTA

Local

PSK (Preshared Key)

Local Certificate

Private Key Password

Local Identifier

Remote

Extended Authentication: No Extended Authentication

Certificate Authority

Remote Identifier

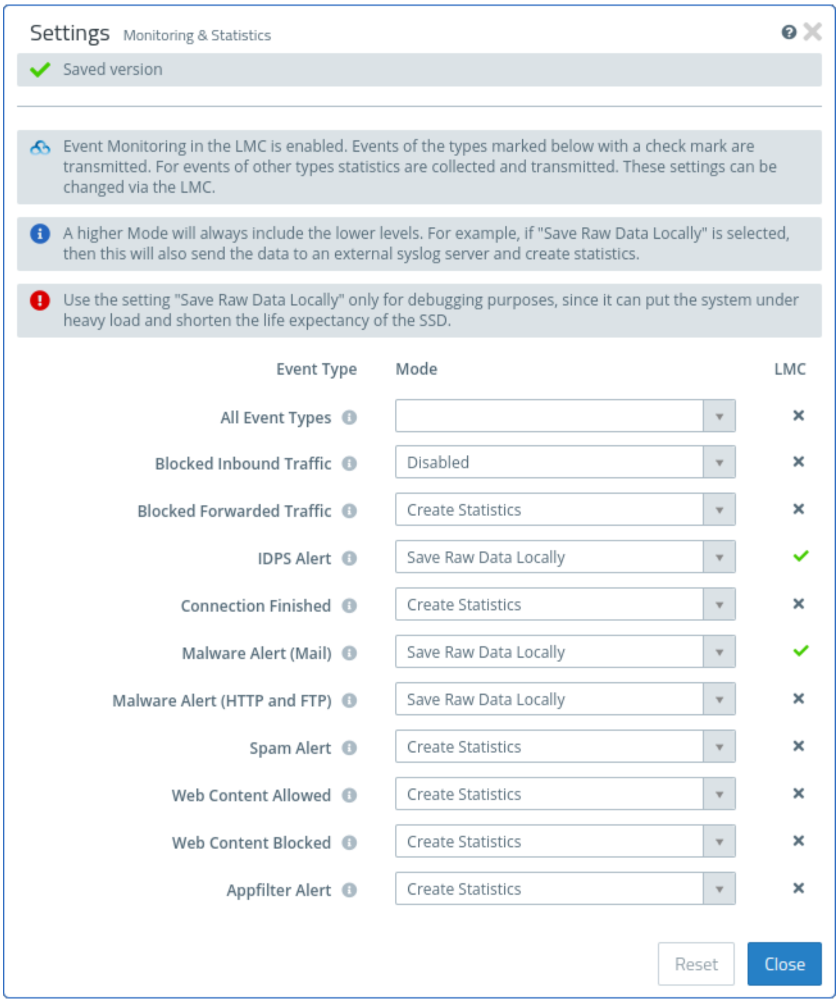
Figure 2: VPN > IPsec > Connections

Table 1: Authentication

Input box	Description
Authentication type	Specify the authentication type. Possible values: › … › LTA – in LANCOM Trusted Access mode, a client certificate is always expected and the groups of the connecting user are read from this client certificate in order to activate the matching rules.

4 Sending alerts to the LANCOM Management Cloud

The LANCOM Management Cloud can be used to configure the forwarding of alerts generated on the LANCOM R&S®Unified Firewall. If this function has been activated via the LANCOM Management Cloud, the settings made there are made transparent in the web client.



✓ Saved version

Event Monitoring in the LMC is enabled. Events of the types marked below with a check mark are transmitted. For events of other types statistics are collected and transmitted. These settings can be changed via the LMC.

A higher Mode will always include the lower levels. For example, if "Save Raw Data Locally" is selected, then this will also send the data to an external syslog server and create statistics.

Use the setting "Save Raw Data Locally" only for debugging purposes, since it can put the system under heavy load and shorten the life expectancy of the SSD.

Event Type	Mode	LMC
All Event Types		✕
Blocked Inbound Traffic	Disabled	✕
Blocked Forwarded Traffic	Create Statistics	✕
IDPS Alert	Save Raw Data Locally	✓
Connection Finished	Create Statistics	✕
Malware Alert (Mail)	Save Raw Data Locally	✓
Malware Alert (HTTP and FTP)	Save Raw Data Locally	✕
Spam Alert	Create Statistics	✕
Web Content Allowed	Create Statistics	✕
Web Content Blocked	Create Statistics	✕
Appfilter Alert	Create Statistics	✕

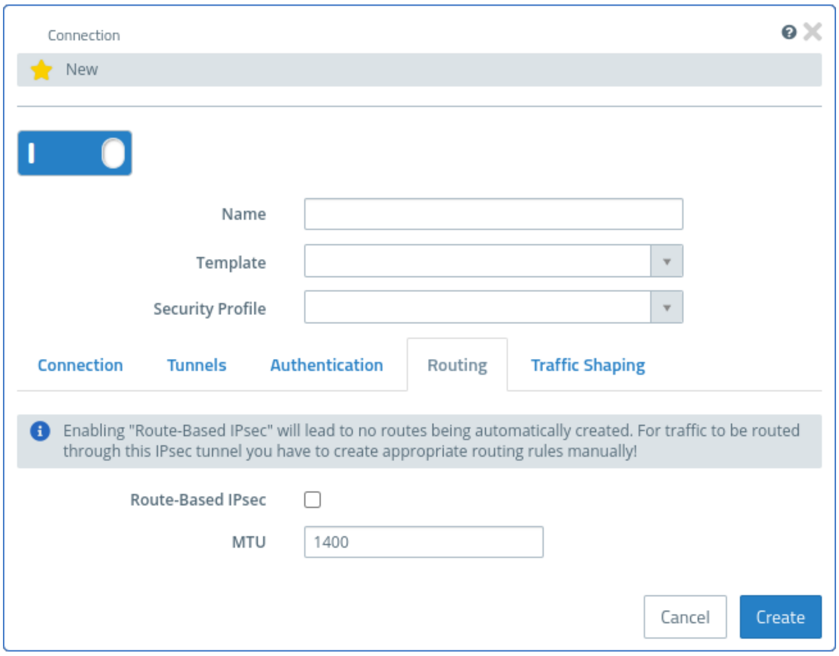
Figure 3: Monitoring & Statistics > Settings

The **LMC** column shows if the forwarding of generated messages to event types has been set in the LANCOM Management Cloud. All event types sent to the LANCOM Management Cloud are displayed with a green check mark. For the event types with an X, no individual events are transmitted, but the number of events that occurred is still sent to the LANCOM Management Cloud.

These settings cannot be changed directly via the LANCOM R&S®Unified Firewall. This is only possible via the LANCOM Management Cloud. The settings are only displayed here for the sake of transparency.

5 MTU for route-based IPsec connections

For route-based IPsec connections, the MTU can now be set for both connections and templates.



Enabling "Route-Based IPsec" will lead to no routes being automatically created. For traffic to be routed through this IPsec tunnel you have to create appropriate routing rules manually!

Route-Based IPsec ☐

MTU 1400

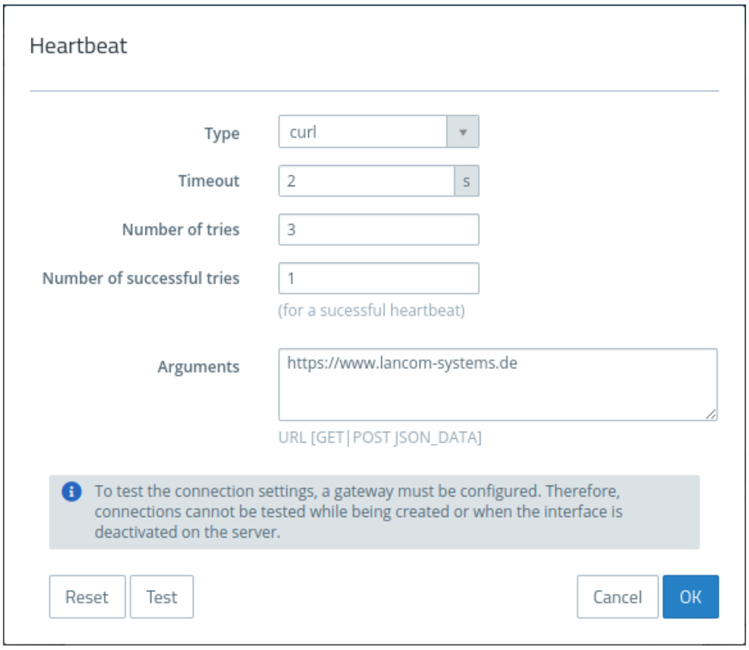
Figure 4: VPN > IPsec > Connections / VPN > IPSec > Templates

Table 2: Routing

Input box	Description
MTU	Here you can set the MTU (Maximum Transmission Unit), i.e. the maximum size of an unfragmented data packet. By default, it is 1400.

6 curl heartbeats for WAN connections

In addition to “ping” and “tcp_probe”, there is now also the option to set up “curl” heartbeats for WAN connections for which a default gateway is set up.



Heartbeat

Type: curl

Timeout: 2 s

Number of tries: 3

Number of successful tries: 1

(for a sucessful heartbeat)

Arguments: https://www.lancom-systems.de

URL [GET|POST JSON_DATA]

To test the connection settings, a gateway must be configured. Therefore, connections cannot be tested while being created or when the interface is deactivated on the server.

Figure 5: Network > Connections > Network Connections > Failover > Heartbeat

Under Type you can set the new mode “curl”. This mode allows the HTTP request methods GET and POST. POST can be used to pass data to be sent to the specified endpoint in JSON format.