LCOS FX 10.12

Addendum

04/2023

LANCOM SYSTEMS

Contents

Copyright

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom-systems.com

1 Addendum to LCOS FX version 10.12

This document describes the changes and enhancements in LCOS FX version 10.12 since the previous version.

2 Extension of the desktop overview with hardware monitoring data

In the notification area of the desktop, the overview now also shows some basic data of the hardware monitoring. This gives you a quick overview of the following data at any time:

- **Uptime**: Elapsed time since the firewall was started
- **CPU**: Average utilization of all CPUs in percent
- **RAM**: Usage of the main memory in percent
- **var Partition**: The usage of this partition is used here because data for logs or statistics are stored on this partition, among other things.

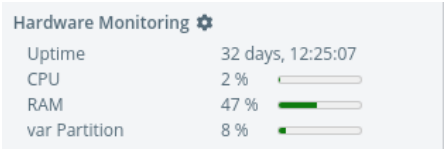


Figure 1: Übersicht > Hardware Monitoring

Click on the title to go directly to the section *Hardware Monitoring* on page 6.

3 Hardware Monitoring

In the **Hardware Monitoring** edit window, you can view the current status of your LANCOM R&S®Unified Firewall. Data on the following areas is displayed:

- System Information
- CPU utilization
- Process list
- Network utilization

Users must have the "Monitoring (Read/Open)" permission to view this data.

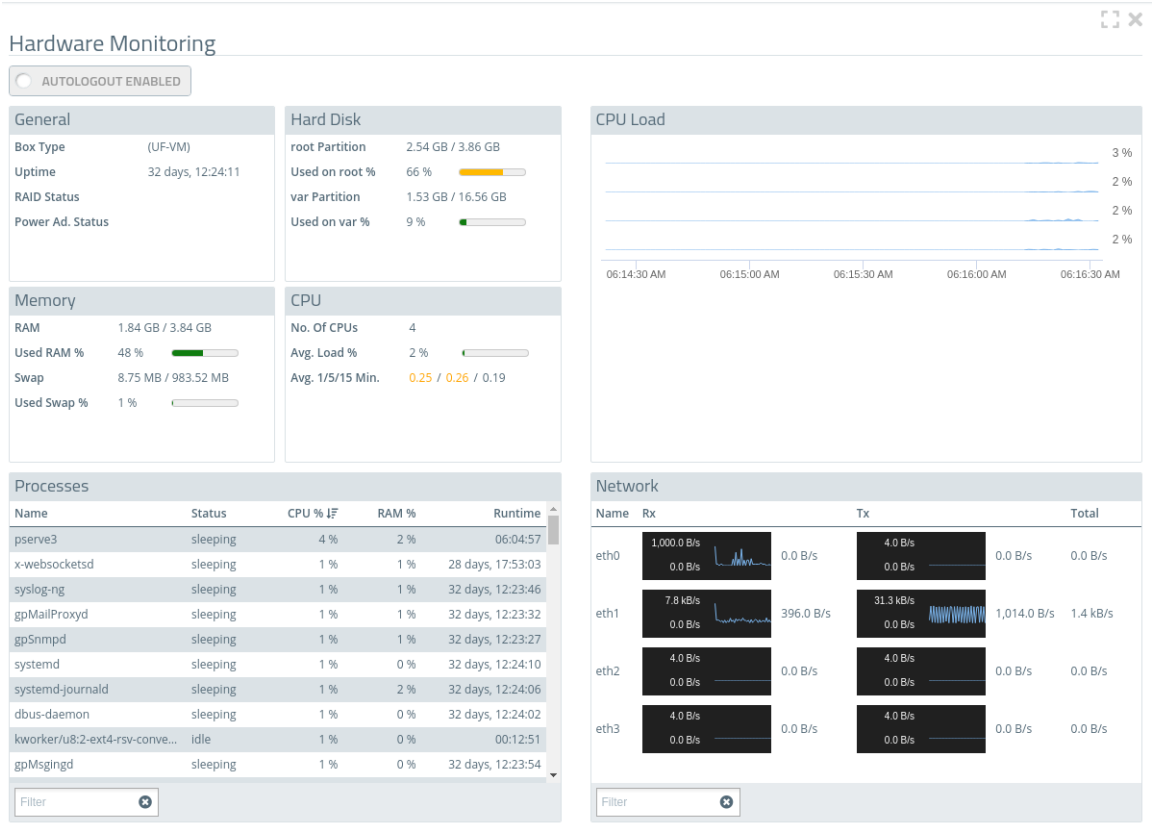


Figure 2: Monitoring & Statistics > Hardware Monitoring

Input field	Description
Autologout enabled / disabled	You can use this switch to enable or disable the automatic logout of the web client. This allows you to track the monitoring data over a longer period of time. This disables a security function of the web client. Therefore, in this case, use a user account to be created by you, which only has the authorization "Monitoring (read/open)".
	Display the monitoring dialog in full screen.

3.1 System Information

The system information is displayed in the upper left area. Information on the following topics is displayed:

- **General**: information about the firewall box type, firewall uptime, RAID status (if present), and power supply status (if present).
- **Hard Disk**: Usage of the root and var partitions, each in absolute and percentage values.
- **Memory**: Usage of RAM and swap, each in absolute and percentage values.
- **CPU**: Number of available logical CPUs, average utilization of all CPUs in percent and the average CPU utilization of the last 1, 5 and 15 minutes. The displayed utilization can also be higher than 1. In this case, more than one CPU core is being utilized. As long as the value is below the number of CPUs, the system is not fully utilized. Values above the number of available CPUs are displayed in red.

  The average CPU utilization of the last 1 or 5 minutes is displayed in yellow if:

  - 1 min value: the average CPU utilization of the last minute is above the utilization average of the last 5 or 15 minutes.
  - 5 min value: the average CPU utilization of the last 5 minutes is above the utilization average of the last 15 minutes.

3.2 CPU Load

The CPU load is displayed in the upper right area. Here the utilization of individual CPUs is displayed over a period of up to 5 minutes. (For more than 10 CPUs two columns are displayed, for more than 20 CPUs the maximum of 3 columns).

If the average of the last 10 values of the utilization of a CPU is above 50%, the color of the graph of this CPU changes to orange. If the average of the last 10 values is above 75%, the graph changes to red.

3.3 Processes

The processes are displayed in the lower left area. The following information is displayed for each process:

- **Name**
- **Status**
- **CPU utilization in percent**
- **RAM utilization in percent**
- **Process runtime**

All columns can be sorted in ascending or descending order.

Additionally, the table can be filtered by process name. The filter also supports only the part of a name.

The list of available processes in the filter is loaded only once when opening the hardware monitoring, thus newly starting processes are not listed.

3.4 Network

The network load is displayed in the lower right area. The current load of all available Ethernet ports is displayed with the following information:

- **Name**
- **Rx**: Bytes received
- **Tx**: Bytes sent
- **Total**: Rx + Tx

Via the filter individual Ethernet ports can be filtered by name.

4 Executive Report

The **Executive Report** menu item has been moved from **Firewall** to **Monitoring & Statistics** and now contains two sub-items **Current Report** and **Mail Report**. The current report corresponds to the previous executive report.

Navigate to **Monitoring & Statistics** > **Executive Report** to create a report about the current desktop configuration and some statistics and transfer it to your computer. Alternatively, you can also send it by e-mail.

4.1 Current Report

By navigating to **Monitoring & Statistics** > **Executive Report** > **Current Report**, you can generate a report on your current desktop configuration and various statistics, and transfer these to your computer.

In the **Executive Report** window you can choose between the file formats PDF, HTML and CSV by selecting the appropriate radio button. 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.

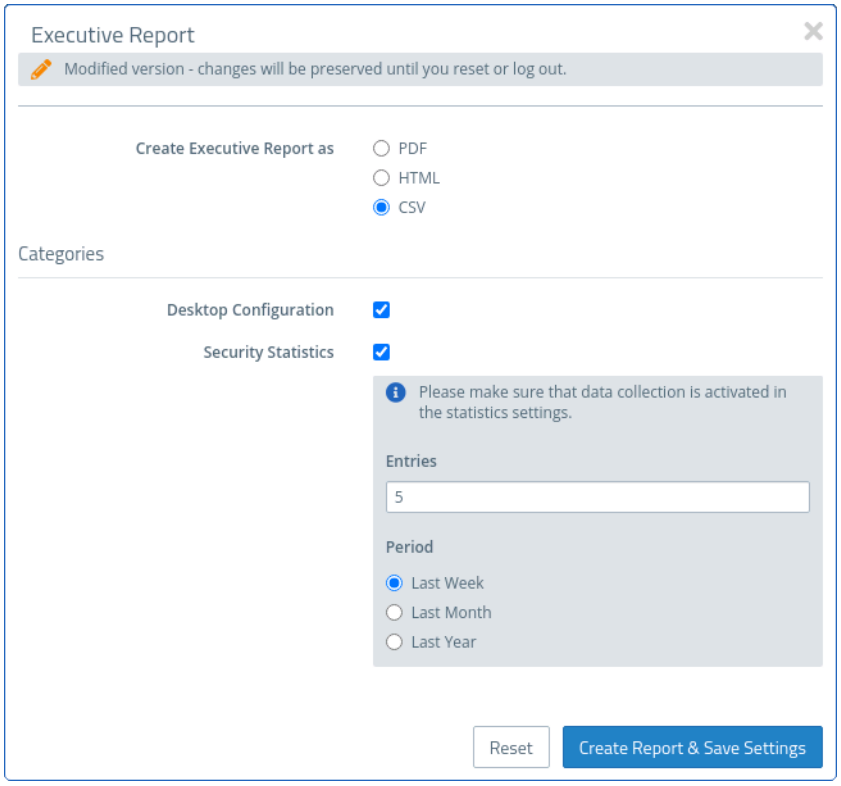


Figure 3: Executive Report – settings

In the **Categories** section you can configure the following elements:

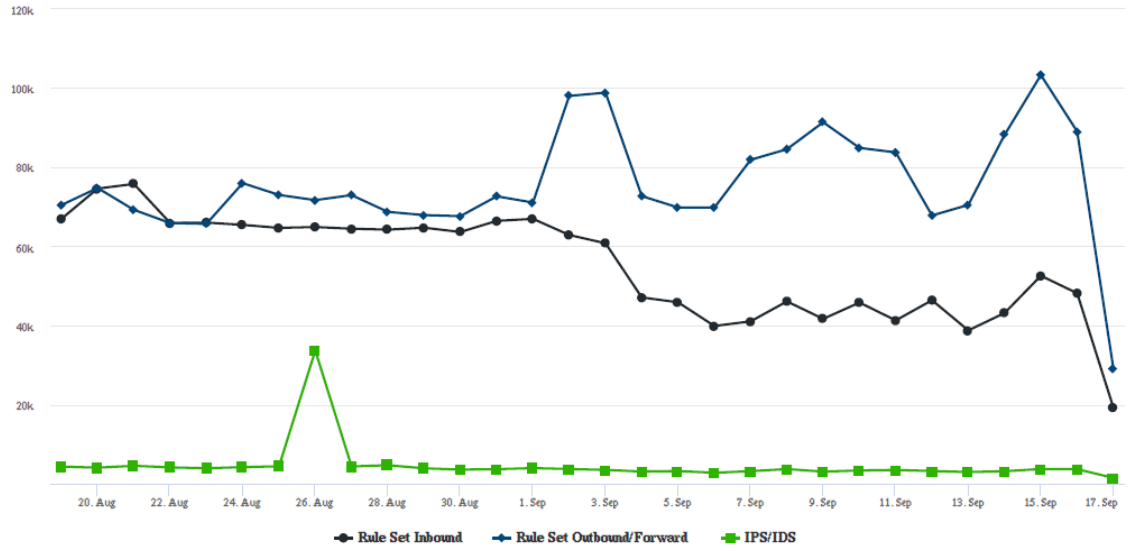
Input box	Description
Desktop configuration	The export file contains a table with all of the configured firewall rules, including additional information such as NAT, DMZ, IP addresses of the host objects and the content of the description fields for the configured desktop objects and connections.

Input box	Description
	Desktop objects are only included if they are connected to other desktop objects.
Security statistics	In order for statistics to be generated, the value under **Monitoring & Statistics** > **Settings** must at least be set to “Create Statistics” for the event types. Contains the statistics that are also available under the menu item **Monitoring & Statistics** > **Statistics** > **Overview**, both as a graph and as a table: › Blocked connections › Blocked content › Top viewed domains › Top blocked domains › Top traffic per source If security statistics are activated, further settings are available: › Number of entries (this setting applies to the top lists only) › Period, definition of the period to be recorded starting with the current point in time

Click on **Create Report** if you want to create and transfer the export file. Your settings are saved and a file name with a date prefix (YYYY-MM-DD_HH-mm) is suggested. Otherwise click **Reset** to reset the settings to the last saved settings.

LANCOM Systems ROHDE&SCHWARZ

Blocked Connections



Date	Rule Set Inbound	Rule Set Outbound/Forward	IPS/IDS
17. Sep	19272	29097	1559
16. Sep	48169	88978	3784
15. Sep	52570	103212	3815
14. Sep	43177	88127	3261
13. Sep	38790	70447	3052

Figure 4: Sample from an Executive Report

LANCOM Systems ROHDE&SCHWARZ

Source	Action	NAT	Destination	Service	Rule Settings	Connection Settings
eth2 LAN Connection 10.10.21.0/24	➡	➡	WAN eth0 WAN Connection	IMAP4 143 TCP	Proxy: IMAP4	Webfilter: Sex: Content Filter Kriminelles: Content Filter Werbung: Content Filter
	➡	➡		POP3s 995 TCP	Proxy: POP3S	
	➡	➡		SMTP 25 TCP	Proxy: SMTP	
	➡	➡		IMAP4s 993 TCP	Proxy: IMAP4S	
	➡	➡		POP3 110 TCP	Proxy: POP3	
	➡	➡		SMTPs 465 TCP	Proxy: SMTPS	
	➡	➡		HTTPS 443 TCP	Proxy: HTTPS	
	➡	➡		HTTP 80 TCP	Proxy: HTTP	
eth1 LAN Connection 10.10.20.0/24	➡	➡	WAN eth0 WAN Connection	HTTPS 443 TCP	Proxy: HTTPS	Webfilter: Sex: Content Filter Kriminelles: Content Filter Werbung: Content Filter
	➡	➡		HTTP 80 TCP	Proxy: HTTP	

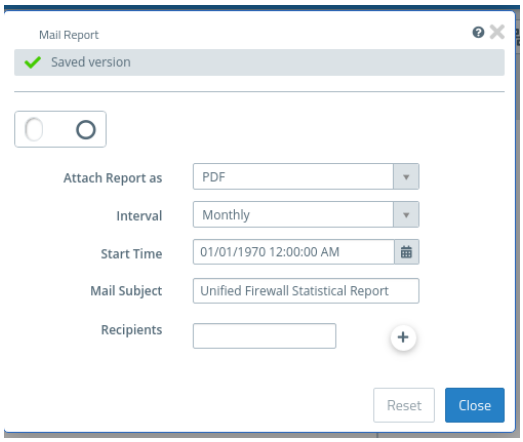
Figure 5: Sample from an Executive Report

4.2 Mail Report

Navigate to **Monitoring & Statistics** > **Executive Report** > **Mail Report** to create a regular report about the current desktop configuration and some statistics and send it via email. Unlike the **Current Report**, the **Mail Report** always includes both the desktop configuration and the statistics.

The mail report uses the firewall-internal mail system. Therefore, the basic settings must be configured under **Firewall** > **E-mail settings** so that e-mails can be sent.

Figure 6: Mail Report – Report settings



Input field	Description
I/**0**	A slide switch indicates whether sending a regularly generated report is currently active (**I**), or inactive (**0**). You can change the status by clicking on the slide switch.
Attach Report as	Choose one of the possible formats PDF, HTML or CSV.
Interval	Specify whether the report should be sent weekly or monthly.
Start Time	Specify the time for sending the report for the first time.
Mail Subject	Specify your own subject for the report email.
Recipients	In this list, specify all email addresses that should receive the report.

The buttons at the bottom right of the edit box depend on whether you have made changes. To apply the changes, click **Save** to save the changes or **Reset** to discard your changes. You can click **Close** to close the editing window as long as no changes have been made in it.

5 LLDP

As of LCOS FX 10.12 LLDP is supported.

LLDP (Link Layer Discovery Protocol) is used to exchange information such as interface MAC addresses or system descriptions with directly connected neighbor devices. Each interface sends and receives information separately. For example, the local interface eth1 only sends information about itself to neighbors to which the local device on this interface is connected. The same applies to receiving. Information is exchanged only with immediate neighbors and can be used to assist in cabling devices, for example.

The following sections provide more detailed information about LLDP.

5.1 LLDP settings

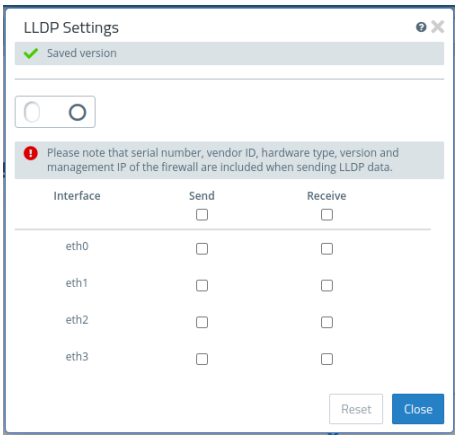


Figure 7: Network > LLDP > LLDP Settings

Under **Network** > **LLDP** > **LLDP Settings** you can configure the following items:

Input field	Description
I/**0**	A slide switch indicates whether the LLDP service is currently active (I), or inactive (0). You can change the status by clicking on the slide switch.
Interface	Activate for each existing interface whether LLDP data should be sent or received separately. You can also set this for all interfaces simultaneously in the table header. Note that when you send, various information about the firewall is sent: Serial number, vendor ID, hardware type, version, and management IP of the firewall.

The buttons at the bottom right of the edit box depend on whether you have made changes. To apply the changes, click **Save** to save the changes or **Reset** to discard your changes. You can click **Close** to close the editing window as long as no changes have been made in it.

5.2 LLDP information

Navigate to **Monitoring & Statistics** > **LLDP** to open a window to view the Link Layer Discovery Protocol (LLDP) information that was received.

Column	Description
Port ID (Local)	Local interface of the firewall on which the LLDP message was received.
Chassis ID	The MAC address of the neighboring device.
System Description	A description of the device, e.g. operating system, version, etc.
System Capabilities	A listing of capabilities that the neighboring device has.
Port ID (Remote)	Remote interface of the neighbor from which the LLDP message was sent.
Port Description	Description of the remote neighbor port.
Management Address	Address where more information about the neighbor can be found.
TTL	Time To Live, duration of the validity of the neighbor information in seconds.

All columns can be sorted in ascending or descending order based on one of the columns.

6 WireGuard

The WireGuard protocol has been added for VPN connections. You can now set up a corresponding interface for this. You can then use this to set up connections and display the status of these connections.

6.1 WireGuard Interfaces

You can use the settings under **WireGuard Interfaces** to set up interfaces secured by WireGuard.

The following sections provide more detailed information about WireGuard interfaces.

6.1.1 WireGuard interface settings

Under **Network** > **Interfaces** > **WireGuard Interfaces** you can add a new WireGuard interface or edit an existing one.

In the **WireGuard Interface** editing window, you can view the following information and configure the following items:

Input field	Description
I/0	A slide switch indicates whether the WireGuard interface is active (**I**) or inactive (**0**). You can change the status of the WireGuard interface by clicking on the slide switch. Newly created WireGuard interfaces are activated by default.
Name	Displays the name of the WireGuard interface. The name is generated automatically according to the scheme wg<*x*>.
Used by	Displays the network components (e.g. connections, other interfaces, etc.) that use the WireGuard interface.
Status	Displays the current status of the WireGuard interface.
MTU	Set the maximum packet size in bytes.

The buttons at the bottom right of the edit box depend on whether you are adding a new WireGuard interface or editing an existing WireGuard interface. For a newly configured WireGuard interface, click **Create** to add it to the list of available WireGuard interfaces or **Cancel** to discard your changes. To edit an existing WireGuard interface, click **Save** to save the newly configured WireGuard interface or **Reset** to discard your changes. You can click **Close** to close the editing window as long as no changes have been made in it.

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

6.2 WireGuard

Set up VPN connections secured by WireGuard under **VPN** > **WireGuard**.

6.2.1 WireGuard Connection

Under **VPN** > **WireGuard** you can manage WireGuard VPN connections.

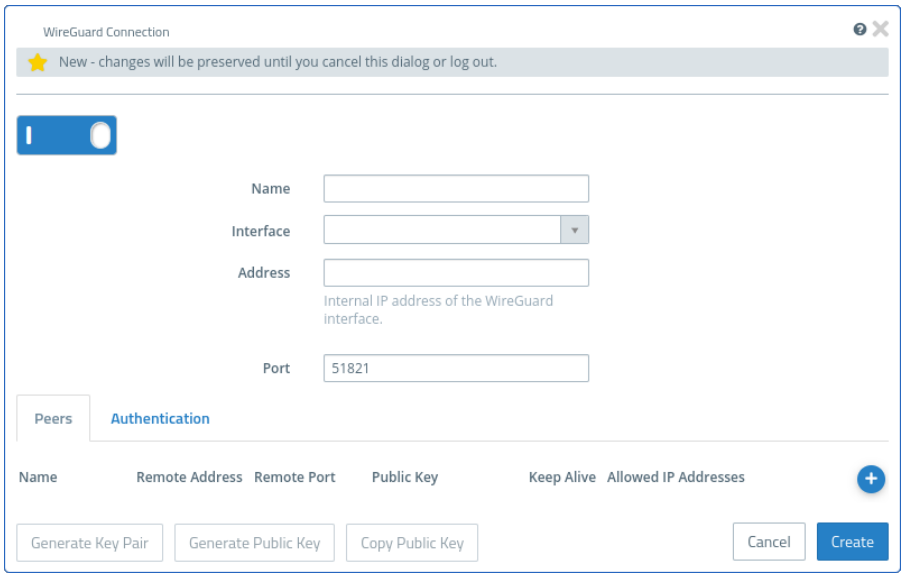


Abbildung 8: VPN > WireGuard > WireGuard Connection

Input field	Description
I/0	A slide switch indicates whether this WireGuard connection is active (**I**) or inactive (**0**). Clicking on the slide switch changes the status of this option.
Name	Give this WireGuard connection a name.
Interface	Selection list in which WireGuard interfaces can be selected. See *WireGuard Interfaces* auf Seite 15.
Address	Enter the IP address of the WireGuard interface here. This can be both an implicit IP address (/32 prefix length) and an IP address with prefix length less than 32.
Port	Port on the firewall over which the WireGuard connection can be established by the remote peer. For the first connection, the default port 51820 is suggested, then for each additional connection, the port is incremented or the next unused port is suggested.

Remote peers can be configured under the **Peers** tab. Click on ⊕ to open the peer dialog.

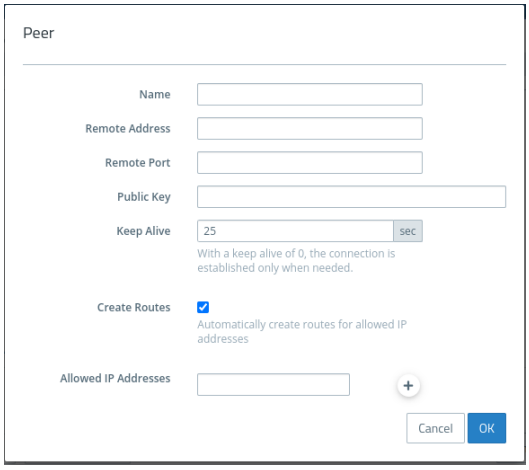


Abbildung 9: VPN > WireGuard > WireGuard Connection > Peers

Tabelle 1: Peers

Input field	Description
Name	Give this remote station a name.
Remote Address	Optional external address of the remote terminal that can thus be reached via the Internet. Can also be a domain name. If specified, then the firewall will attempt to initiate the connection. The specification is required if a remote port is specified.
Remote Port	Optional port through which the connection is to be established. Required if a remote address is specified.
Public Key	The base64-encoded public key of the remote peer.
Keep Alive	Interval in seconds for sending packets to maintain the connection, default 25, with a value of 0 the connection is established only when needed.
Create Routes	If enabled, then all IP addresses under **Allowed IP Addresses** are automatically added to the routing table 201. Otherwise, you must create the routes manually.
Allowed IP Addresses	IP addresses or networks with subnet mask that are to be accessible via the WireGuard connection.

Under the **Authentication** tab, a private/public key pair can be created. These are used by WireGuard instead of certificates.

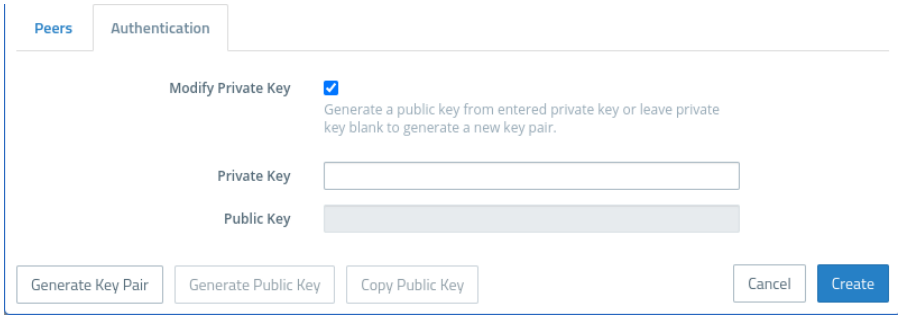


Abbildung 10: VPN > WireGuard > WireGuard Connection > Authentication

Tabelle 2: Authentication

Input field	Description
Modify Private Key	This option is intended to prevent overwriting a key that has already been entered. Checking this box also enables the **Generate Key Pair** button.
Private Key	Either enter a Base64 string as the private key or leave the field empty.
Public Key	The public key for the private key. If necessary, generate it using **Generate Key Pair**.
Generate Key Pair	With a click on this button you create a private / public key pair. If a private key already exists, then you will receive a confirmation prompt.
Generate Public Key	With a click on this button you generate a public key for an already entered private key.
Copy Public Key	Copy the public key to the clipboard. The copied key can then be entered on the remote site, or sent to the remote site admin.

The buttons at the bottom right of the edit box depend on whether you are adding a new connection or editing an existing one. For a newly configured connection, click **Create** to add it to the list of available connections or **Cancel** to discard your changes. To edit an existing connection, click **Save** to save the newly configured connection or **Reset** to discard your changes.

6.3 WireGuard Status

The status of the WireGuard connections can be monitored under **Monitoring & Statistics** > **WireGuard Status**. WireGuard does not display whether a connection has actually been established.

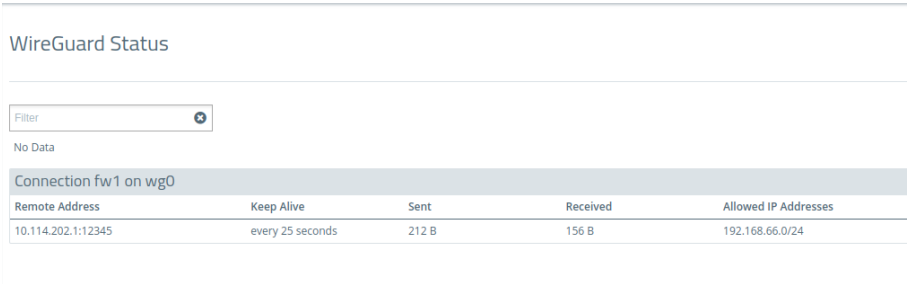


Abbildung 11: Monitoring & Statistics > WireGuard Status

Column	Description
Remote Address	The remote address of this WireGuard connection. You can filter by this column.
Keep Alive	The set Keep Alive value of this WireGuard connection.
Sent	Bytes sent over this connection.
Received	Bytes received over this connection.
Allowed IP Addresses	The configured allowed IP addresses of this WireGuard connection. You can filter by this column.

7 Export logs

Audit, alarm and system logs can now be exported in PDF, HTML and CSV formats. For this purpose, a new export dropdown has been added or the existing one has been extended. The export of the logs takes into account all the filters that have been set.

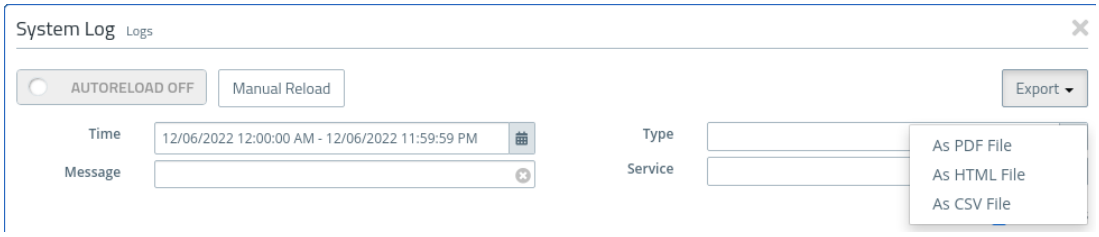


Figure 12: Monitoring & Statistics > Logs > System Log

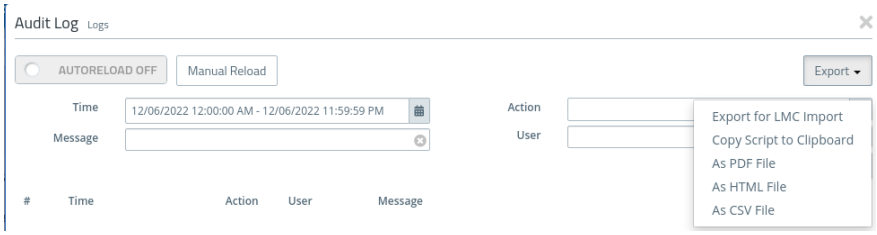


Figure 13: Monitoring & Statistics > Logs > Audit Log

8 DNS based rules

It is now possible to configure host objects and objects in host groups with domain names in addition to IP addresses, so that rules can be generated dynamically for these objects.

For this, two dialogs were adjusted in the frontend.

- In the host dialog, the **IP Address** field has been renamed to **Host**
- In the host group dialog, the column header has been renamed from **Host/Network IP** to **Host/Network**

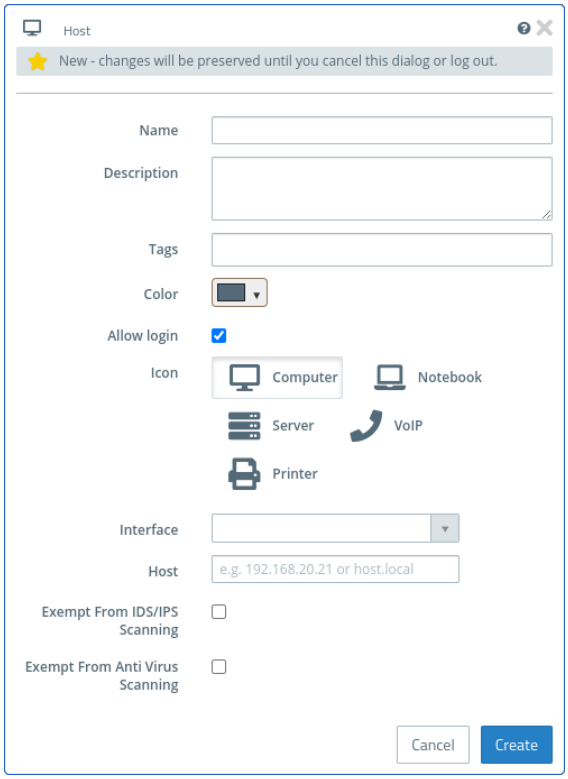


Figure 14: Desktop > Desktop Objects > Hosts

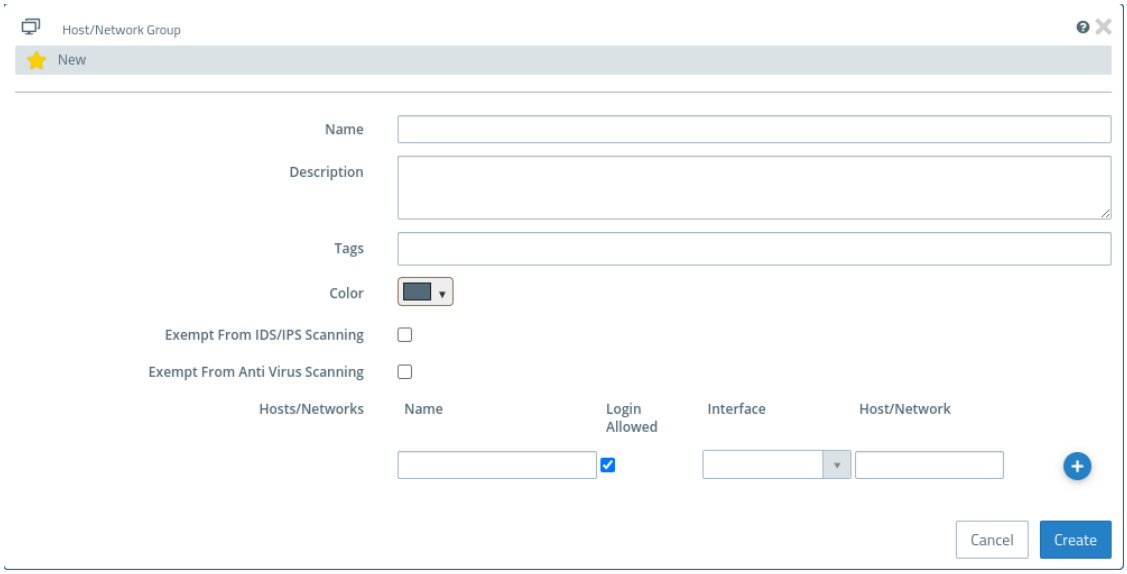


Figure 15: Desktop > Desktop Objects > Host/Network Groups

9 BGP extension

Two new settings have been added to the BGP configuration.

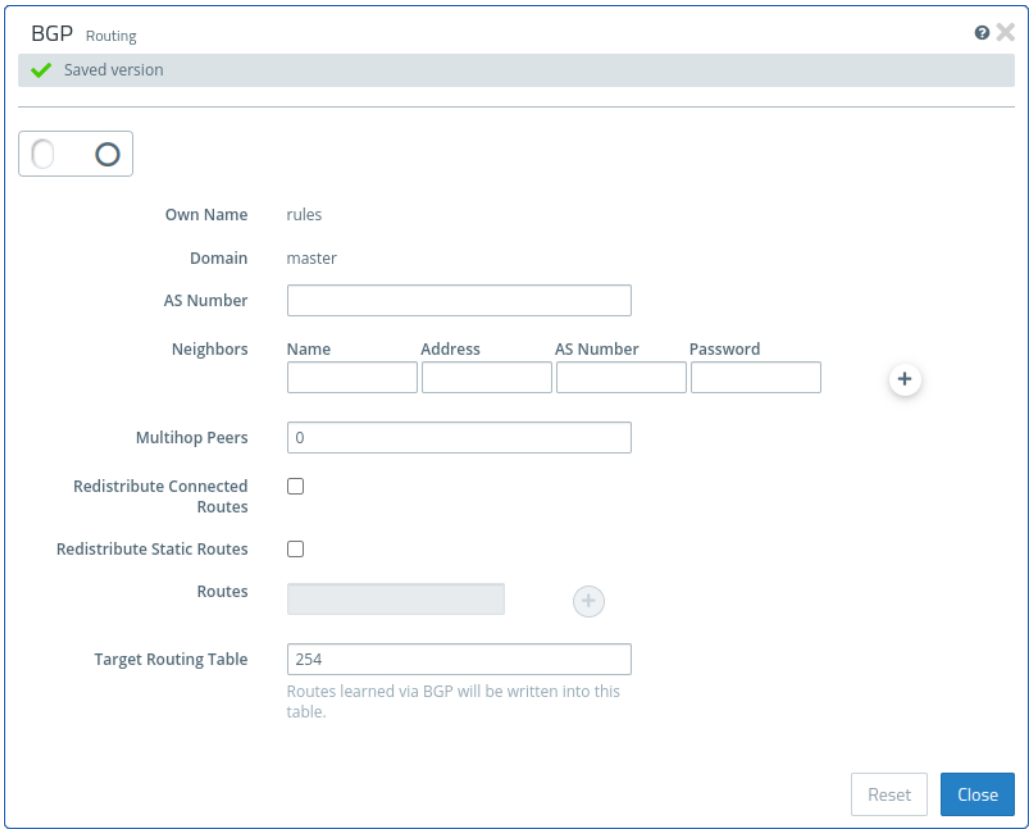


Abbildung 16: Network > Routing > BGP

Input field	Description
Multihop Peers	Set the max. number of hops over which a peer can be reached. Possible values: 0 to 255 (at 0 only directly connected peers are considered).
Target Routing Table	Routing table into which the learned routing entries are to be written. Possible values: 254 (Main table) or 512 to 65535 (user-defined tables).