LCOS FX 10.10

Addendum

01/2023

LANCOM
SYSTEMS

Contents

Copyright

1 Addendum to LCOS FX version 10.10

This document describes the changes and enhancements in LCOS FX version 10.10 since the previous version.

2 Antivirus settings

With LCOS FX version 10.10 the antivirus service in the backend has been optimized and the following changes or new features have been added:

The settings

> **Scan archived files**
> **Enable Cloud Scan**
> **Heuristic Analysis**

now apply to all scanners.
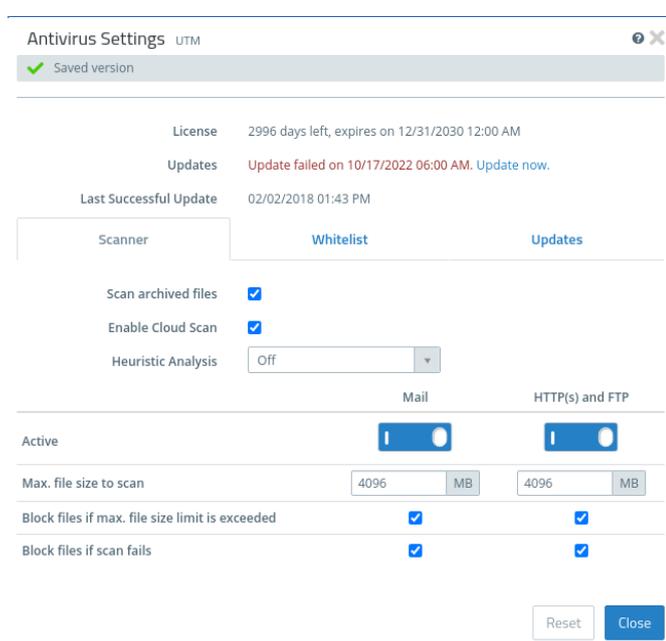
Figure 1: UTM > Antivirus Settings

The following settings can now be set separately for **Mail**, **HTTP(s) and FTP** for each scanner.

Input field	Description
Active	Two slide switches indicate whether the virus scanner for e-mail and/or HTTP(S) and FTP is currently active (**I**) or inactive (**0**). Clicking the respective slide switch changes the status of this option. These options are enabled by default for all services.
Max. file size to scan	Set the maximum file size to scan in MB (Min: 1 MB, Max: 4096 MB).
Block files if max. file size limit is exceeded	If a file exceeds the maximum file size for a file to be scanned, then it can be blocked. If you uncheck this option, then the files will be downloaded without antivirus scan.
Block files if scan fails	Activate this check box to block e-mails and/or the download of HTTP(S) and FTP files that the virus scanner could not check successfully.
	If an error occurs during the check, the e-mail will be blocked and the recipient will be informed. If you clear the check box, the recipient will receive a substitute e-mail with the original e-mail as an encrypted attachment, together with the password to decrypt it.

3 VPN Groups

With LCOS FX version 10.10, multiple remote networks can be specified within a VPN group for individual IPsec connections contained in the group. The individual entries can now also be configured more flexibly, essentially analogously to the desktop objects under **VPN Network**. The settings per group item have been moved to a separate subwindow and are now no longer edited directly in the group item table.
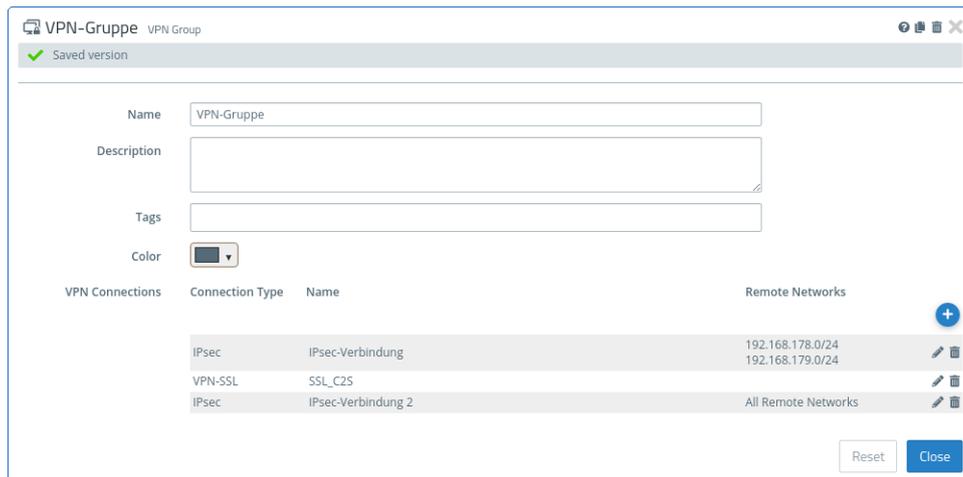

Figure 2: Desktop > Desktop Objects > VPN Groups

Input box	Description
VPN Connections	To add VPN connections to the VPN group, click ⊕. A window opens where you can select or edit the VPN connection. **Figure 3: Window for editing a group element**
	VPN Connection Type — Select the type of VPN connection by selecting the appropriate radio button.
	IPsec Connection / **VPN-SSL Connection** — This field depends on the selected connection type. From the drop-down list, select the VPN connection you want to assign to the VPN network object.

| Input box	Description	
	Remote Networks	If you have selected an IPSec connection, you can either use all of the configured remote networks or explicitly add the remote networks to be used.
	(!)	VPN connections can be assigned to multiple VPN groups.

4 Export of audit log entries for the LANCOM Management Cloud

To simplify the use of AddIns in the LANCOM Management Cloud, as of LCOS FX version 10.10 the audit log can be exported in the appropriate format. This allows to quickly and easily multiply the ideal configuration from one Unified Firewall to any number of Unified Firewalls managed by the LANCOM Management Cloud (LMC). There are two options to choose from:

> **Export for LMC Import**: A json file is generated which can later be uploaded to the LANCOM Management Cloud using the appropriate import function.

> **Copy Script to Clipboard**: The AddIn function is copied to the clipboard and can then be pasted directly.

The export takes the current filter settings into account.
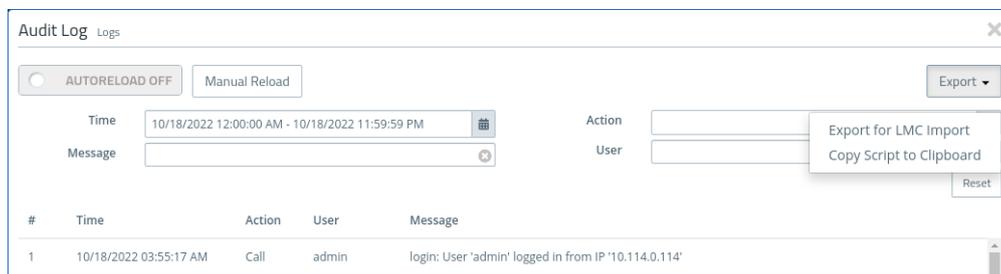
Figure 4: Monitoring & Statistics > Logs > Audit Log

Click on ⚙ in a line on the right to export this audit entry as an LMC function call.

5 Let's Encrypt

With the settings under **Let's Encrypt** you can use Let's Encrypt certificates. In addition to a Let's Encrypt account, only a few settings on the firewall are required for this.

5.1 Let's Encrypt Settings

In the **Certificate Management** > **Let's Encrypt** editing window, you can make settings for Let's Encrypt certificates. The following items can be specified:

Figure 5: Certificate Management > Let's Encrypt

Input field	Description
E-Mail Address	Enter the e-mail address with which the Let's Encrypt account will be registered.

If you have modified these settings, use the buttons at the bottom right of the editor panel to confirm (**Save**) or to discard your changes (**Reset**). Otherwise, you can close the dialog (**Close**).

The certificates created using Let's Encrypt are displayed under **Certificate Management** > **Certificates** under **Let's Encrypt certificates**.These certificates can only be "Renewed", "Viewed" and "Exported". "Revoking", "Deleting" and also "Renewing" when the end of the validity period is reached are performed automatically.

5.2 Use Let's Encrypt certificates

The Let's Encrypt certificates can be used in the Reverse Proxy Frontend with SSL mode enabled and in the external Portal of user authentication.

Figure 6: UTM > Reverse Proxy > Frontends

Input field	Description
Use Let's Encrypt	Use a Let's Encrypt certificate. The certificates used are automatically generated and automatically renewed when their validity expires. See *Let's Encrypt* on page 9.

Figure 7: User Authentication > External Portal > Settings

Input field	Description
Use Let's Encrypt	Use a Let's Encrypt certificate. See *Let's Encrypt* on page 9.
	ⓘ One limitation of using Let's Encrypt is that no IP addresses can be used in the **Domain or IP address** field, only domain names.

6 Connection-specific DNS server

With LCOS FX version 10.10 you can now specify for each DNS server entry in both the global and the network-specific DNS settings which connection can be used to reach the entered servers. A new **Connection** column has been created for this purpose, in which an existing connection can be selected.

Network > **DNS Settings** > **General Settings**

Specify here which connection can be used to reach the entered servers. For the DNS server entry with "AUTO" as the assigned server, the **Aquired Servers** are used. If a connection has been assigned to this entry, e.g. dsl, then all obtained servers are displayed, but only the servers obtained via the connection "dsl" are used. If no connection is selected for the "AUTO" entry, then all obtained servers are used.

Figure 8: Network > DNS Settings > Network-Specific Settings

7 Notification Settings

With LCOS FX version 10.10 you can now use the **Omit Mails Without Notifications** option in the notification settings to specify whether notification mails should be sent that contain no or no new notifications.

Monitoring & statistics > **Notification settings**

8 Redirect HTTP to HTTPS

With LCOS FX version 10.10 you can enable the **Redirect HTTP to HTTPS** option in the settings for a reverse proxy frontend. This redirects HTTP requests to the configured domain or IP address to HTTPS.

UTM > **Reverse Proxy** > **Frontends**