

LCOS FX 10.10

Addendum

01/2023

Inhalt

1 Addendum zur LCOS FX-Version 10.10.....	4
2 Antivirus-Einstellungen.....	5
3 VPN-Gruppen.....	7
4 Export von Audit-Log-Einträgen für die LANCOM Management Cloud.....	9
5 Let's Encrypt.....	10
5.1 Einstellungen für Let's Encrypt.....	10
5.2 Let's Encrypt-Zertifikate verwenden.....	11
6 Verbindungsspezifische DNS-Server.....	13
7 Benachrichtigungs-Einstellungen.....	14
8 HTTP auf HTTPS umleiten.....	15

Copyright

© 2023 LANCOM Systems GmbH, Würselen (Germany). Alle Rechte vorbehalten.

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. LANCOM Systems haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhaltes sind nur mit schriftlicher Erlaubnis von LANCOM Systems gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

Windows® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

LANCOM, LANCOM Systems, LCOS, LANcommunity und Hyper Integration sind eingetragene Marken. Alle übrigen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein. Dieses Dokument enthält zukunfts- bezogene Aussagen zu Produkten und Produkteigenschaften. LANCOM Systems behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten und / oder Auslassungen.

Das Produkt enthält separate Komponenten, die als sogenannte Open Source Software eigenen Lizenzen, insbesondere der General Public License (GPL), unterliegen. Sofern die jeweilige Lizenz dies verlangt, werden Quelldateien zu den betroffenen Software-Komponenten auf Anfrage bereitgestellt. Bitte senden Sie eine E-Mail an gpl@lancom.de.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project“ für die Verwendung im „OpenSSL Toolkit“ entwickelt wurde (www.openssl.org).

Produkte von LANCOM Systems enthalten kryptographische Software, die von Eric Young (eay@cryptsoft.com) geschrieben wurde.

Produkte von LANCOM Systems enthalten Software, die von der NetBSD Foundation, Inc. und ihren Mitarbeitern entwickelt wurde.

Produkte von LANCOM Systems enthalten das LZMA SDK, das von Igor Pavlov entwickelt wurde.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Addendum zur LCOS FX-Version 10.10

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS FX-Version 10.10 gegenüber der vorherigen Version.

2 Antivirus-Einstellungen

Mit LCOS FX-Version 10.10 wurde der Antiviren-Dienst im Backend optimiert und folgende Änderungen bzw. Neuerungen hinzugefügt:

Die Einstellungen

- > **Archivdateien scannen**
- > **Cloud-Scan aktivieren**
- > **Heuristische Analyse**

gelten nun für alle Scanner.

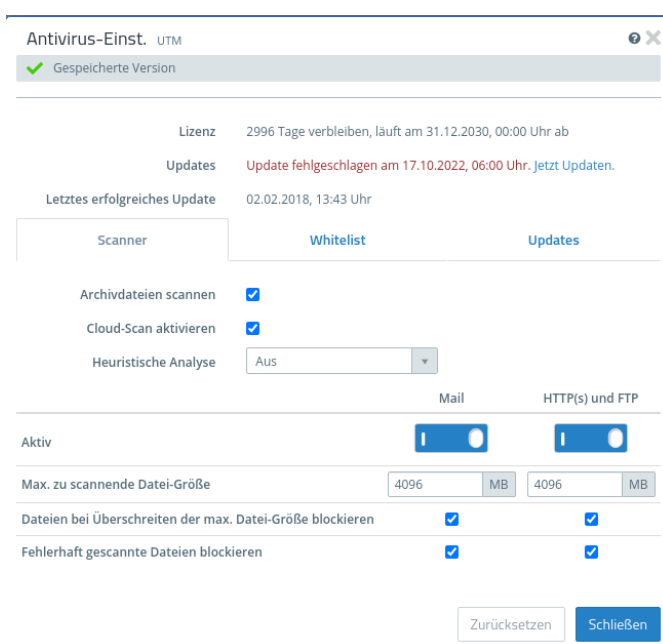


Abbildung 1: UTM > Antivirus-Einstellungen

Die folgenden Einstellungen sind nun jeweils für **Mail** bzw. **HTTP(s) und FTP** getrennt je Scanner einstellbar.

Eingabefeld	Beschreibung
Aktiv	Zwei Schiebeschalter geben an, ob der Virenschanner für E-Mail und/oder HTTP(S) und FTP derzeit aktiv (I) oder inaktiv (O) ist. Mit einem Klick auf den jeweiligen Schiebeschalter ändern Sie den Status dieser Option. Diese Optionen sind für alle Dienste standardmäßig aktiviert.
Max. zu scannende Datei-Größe	Stellen Sie die maximal zu scannende Datei-Größe in MB ein (Min: 1 MB, Max: 4096 MB).
Dateien bei Überschreiten der max. Datei-Größe blockieren	Falls eine Datei die maximale Datei-Größe für eine zu scannende Datei überschreitet, dann kann sie blockiert werden. Wenn Sie diese Option deaktivieren, dann werden die Dateien ohne Antiviren-Scan heruntergeladen.
Fehlerhaft gescannte Dateien blockieren	Setzen Sie dieses Häkchen, um E-Mails zu blockieren und/oder den Download von Dateien in HTTP(S) und FTP abzubrechen, falls der Virenschanner deren Überprüfung nicht erfolgreich abschließen konnte. Falls also während der Überprüfung ein Fehler auftritt, wird die E-Mail blockiert und der Empfänger wird darüber informiert. Wenn Sie das Häkchen entfernen, erhält der Empfänger

2 Antivirus-Einstellungen

Eingabefeld	Beschreibung
	eine Ersatz-E-Mail, die die Original-E-Mail als verschlüsselten Anhang zusammen mit dem zur Entschlüsselung benötigten Passwort enthält.

3 VPN-Gruppen

Mit LCOS FX-Version 10.10 können innerhalb einer VPN-Gruppe mehrere Remote-Netze für einzelne in der Gruppe enthaltene IPsec-Verbindungen angegeben werden. Die einzelnen Einträge können nun auch flexibler konfiguriert werden, im wesentlichen analog zu den Desktop-Objekten unter **VPN-Netzwerk**. Die Einstellungen pro Gruppen-Element sind in ein eigenes Unterfenster ausgelagert worden und werden nun nicht mehr direkt in der Tabelle der Gruppen-Elemente bearbeitet.

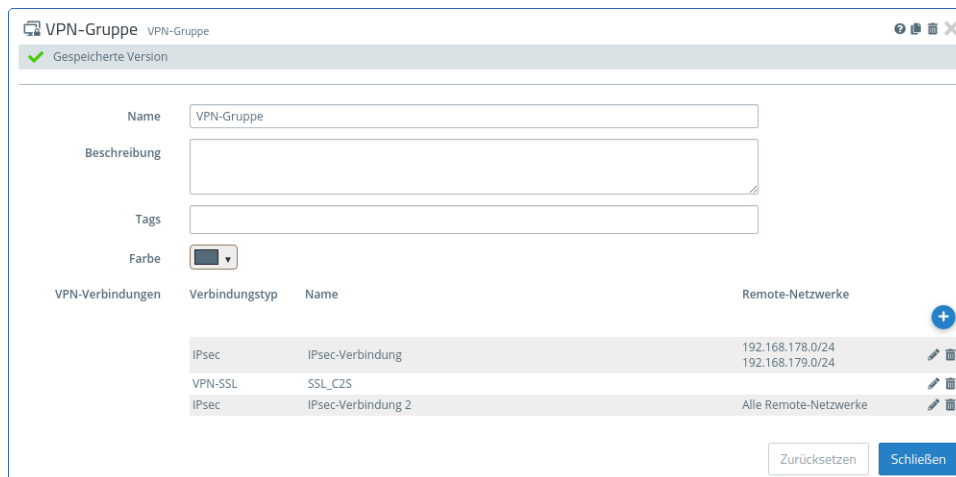



Abbildung 2: Desktop > Desktop-Objekte > VPN-Gruppen

Eingabefeld	Beschreibung
VPN-Verbindungen	<p>Um VPN-Verbindungen zur VPN-Gruppe hinzuzufügen, klicken Sie auf +.</p> <p>Es öffnet sich ein Fenster, in dem Sie die VPN-Verbindung auswählen bzw. bearbeiten.</p> <p>IPsec-Verbindung VPN-Gruppen-Eintrag</p> <p>Verbindungstyp <input checked="" type="radio"/> IPsec <input type="radio"/> VPN-SSL</p> <p>IPsec-Verbindung <input type="text" value="IPsec-Verbindung"/></p> <p>i Bei der Einstellung "Alle konfigurierten Remote-Netzwerke verwenden" haben URL/Content Filter-Regeln keinen Effekt.</p> <p>Remote-Netzwerke <input type="radio"/> Alle konfigurierten Remote-Netzwerke verwenden <input checked="" type="radio"/> Remote-Netzwerke konfigurieren</p> <p><input type="text"/></p> <p>192.168.178.0/24 <input type="text"/></p> <p>192.168.179.0/24 <input type="text"/></p> <p>Abbrechen <input type="button" value="OK"/></p>
Verbindungstyp	Wählen Sie den Typ der VPN-Verbindung aus, indem Sie die entsprechende Optionsschaltfläche auswählen.
IPsec-Verbindung / VPN-SSL-Verbindung	Dieses Feld hängt vom gewählten Verbindungstyp ab. Wählen Sie aus der Drop-down-Liste die VPN-Verbindung aus, die Sie der VPN-Gruppe zuweisen möchten.

Abbildung 3: Fenster zum Bearbeiten eines Gruppen-Elements

Eingabefeld	Beschreibung	
	Remote Netzwerke	Falls Sie eine IPsec-Verbindung ausgewählt haben, dann können Sie entweder alle konfigurierten remote Netzwerke verwenden oder die zu verwendenden remote Netzwerke explizit hinzufügen.
	 VPN-Verbindungen können mehreren VPN-Gruppen zugewiesen werden.	

4 Export von Audit-Log-Einträgen für die LANCOM Management Cloud

Zur Vereinfachung der Verwendung von AddIns in der LANCOM Management Cloud kann ab LCOS FX-Version 10.10 das Auditprotokoll im passenden Format exportiert werden. Damit lassen sich schnell und einfach Konfigurationen von einer Unified Firewall auf beliebig viele von der LANCOM Management Cloud (LMC) gemanagte Unified Firewalls multiplizieren. Dabei kann zwischen zwei Optionen gewählt werden:

- > **Für LMC-Import exportieren:** Eine json-Datei wird erzeugt, die später in der LANCOM Management Cloud über die entsprechende Import-Funktion hochgeladen werden kann.
- > **Script in Zwischenablage kopieren:** Die AddIn-Funktion wird in die Zwischenablage kopiert und kann dann direkt eingefügt werden.

Der Export berücksichtigt hierbei die gegenwärtigen Filter-Einstellungen.

#	Zeit	Aktion	Benutzer	Meldung
1	18.10.2022 03:55:17	Aufruf	admin	login: User 'admin' logged in from IP '10.114.0.114'
2	18.10.2022 03:29:27	Erstellen	admin	INSERT 'network' on 'networks'.

Abbildung 4: Monitoring & Statistiken > Protokolle > Auditprotokoll

Klicken Sie rechts in einer Zeile auf , um diesen Audit-Eintrag als LMC-Funktionsaufruf zu exportieren.

5 Let's Encrypt

Mit den Einstellungen unter **Let's Encrypt** können Sie Let's Encrypt-Zertifikate verwendet werden. Dazu werden neben einem Let's Encrypt Account nur wenige Einstellungen auf der Firewall benötigt.

5.1 Einstellungen für Let's Encrypt

Im Bearbeitungsfenster **Zertifikatsverwaltung > Let's Encrypt** können Sie Einstellungen für Let's Encrypt-Zertifikate vornehmen. Die folgenden Elemente können vorgegeben werden:

Abbildung 5: Zertifikatsverwaltung > Let's Encrypt

Eingabefeld	Beschreibung
E-Mail-Adresse	Geben Sie die E-Mail-Adresse ein, mit welcher der Let's Encrypt-Account registriert wird.

Wenn Sie Änderungen vorgenommen haben, können Sie diese mit den Schaltflächen unten rechts im Bearbeitungsfenster speichern (**Speichern**) oder verwerfen (**Zurücksetzen**). Andernfalls können Sie das Fenster schließen (**Schließen**).

Die mittels Let's Encrypt erstellten Zertifikate werden unter **Zertifikatsverwaltung > Zertifikate** unter **Let's Encrypt-Zertifikate** angezeigt. Diese Zertifikate können nur „Erneuert“, „Angesehen“ und „Exportiert“ werden. „Revozieren“, „Löschen“ und auch das „Erneuern“, sobald das Ende des Gültigkeitszeitraums erreicht wird, werden automatisch durchgeführt.

5.2 Let's Encrypt-Zertifikate verwenden

Die Let's Encrypt-Zertifikate können im Reverse Proxy Frontend bei aktiviertem SSL-Modus und im externen Portal der Benutzerauthentifizierung verwendet werden.

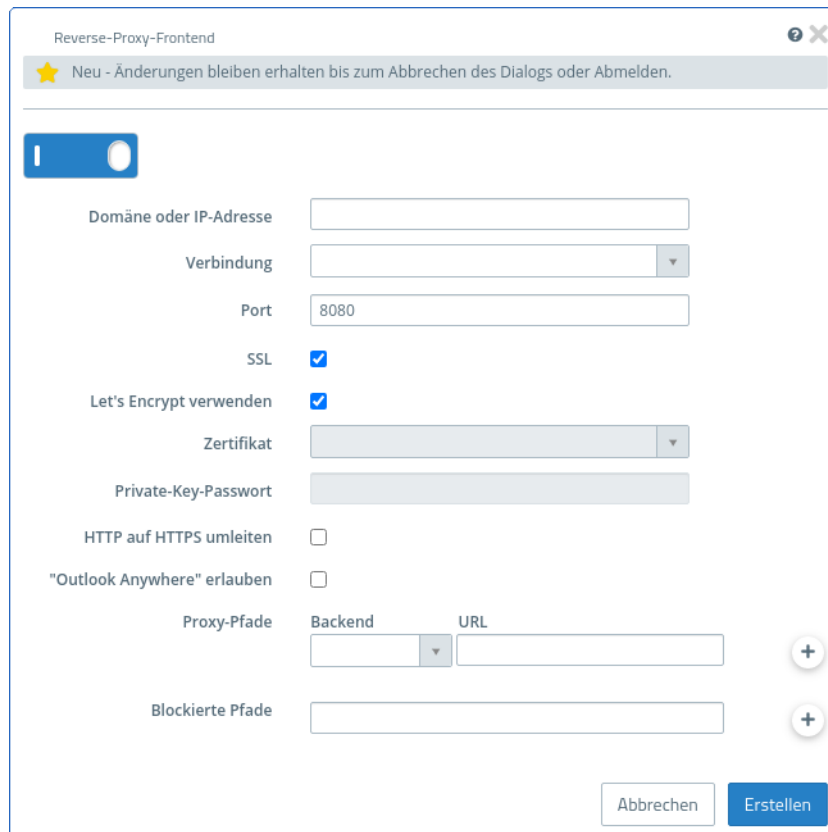


Abbildung 6: UTM > Reverse-Proxy > Frontends

Eingabefeld	Beschreibung
Let's Encrypt verwenden	Verwendet ein Let's Encrypt-Zertifikat. Die verwendeten Zertifikate werden automatisch erzeugt und bei Ablauf der Gültigkeit automatisch verlängert. Siehe Let's Encrypt auf Seite 10.

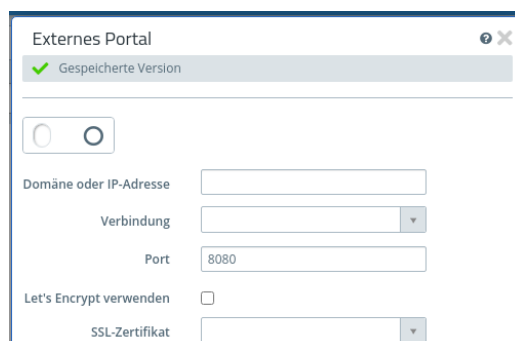



Abbildung 7: Benutzerauthentifizierung > Externes Portal > Einstellungen

Eingabefeld	Beschreibung
Let's Encrypt verwenden	<p>Verwendet ein Let's Encrypt-Zertifikat. Siehe Let's Encrypt auf Seite 10.</p> <hr/> <p> Eine Einschränkung bei der Verwendung von Let's Encrypt ist, dass keine IP-Adressen im Feld Domäne oder IP-Adresse verwendet werden können, sondern ausschließlich Domännennamen.</p>

6 Verbindungsspezifische DNS-Server

Mit LCOS FX-Version 10.10 können Sie bei den DNS-Server-Einträgen sowohl in den globalen als auch in den netzwerkspezifischen DNS-Einstellungen nun je Eintrag festlegen, über welche Verbindung die eingetragenen Server erreicht werden können. Dafür wurde eine neue Spalte **Verbindung** erstellt, in der eine vorhandene Verbindung ausgewählt werden kann.

Netzwerk > DNS-Einstellungen > Allgemeine Einstellungen

Allgemeine Einstellungen 🔍 ✕

✓ Gespeicherte Version

Bezogene Server 8.8.8.8 (dsl), 192.168.44.5 (dhcp)
Nur Server, die über die Verbindung "dsl" bezogen werden, werden aktuell für die "AUTO"-Einstellung verwendet.

DNS-Server	Zone	Zugewiesene Server	Verbindung
*.lancom.de	192.168.55.5		eth1 LAN Connection
*	AUTO		dsl

Multicast-DNS-Relay

Zurücksetzen Schließen

Legen Sie hier fest, über welche Verbindung die eingetragenen Server erreicht werden können. Für den DNS-Server-Eintrag mit „AUTO“ als zugewiesenen Server, werden die **Bezogenen Server** verwendet. Wurde diesem Eintrag eine Verbindung zugewiesen, z. B. dsl, dann werden zwar alle bezogenen Server angezeigt, aber nur die Server verwendet, die über die Verbindung „dsl“ bezogen wurden. Wenn keine Verbindung für den „AUTO“-Eintrag gewählt wird, dann werden alle bezogenen Server verwendet.

test Netzwerk-spezifische Einst. 🔍 🗑️ ✕

✓ Gespeicherte Version

Name test

Quell-Netzwerke

DNS-Server	Zone	Zugewiesene Server	Verbindung
*.dd	192.168.66.5		eth1 LAN Connection

Globale Einstellungen

DNS-Server	Zone	Zugewiesene Server	Verbindung
*.lancom.de	192.168.55.5		eth1 LAN Connection
*	AUTO		dsl

Zurücksetzen Schließen

Abbildung 8: Netzwerk > DNS-Einstellungen > Netzwerk-spezifische Einstellungen

7 Benachrichtigungs-Einstellungen

Mit LCOS FX-Version 10.10 können Sie bei den Benachrichtigungs-Einstellungen nun über die Option **Mails nicht senden, die keine Benachrichtigungen enthalten** festlegen, ob Benachrichtigungs-Mails gesendet werden sollen, die keine bzw. keine neuen Benachrichtigungen enthalten.

Monitoring & Statistiken > Benachrichtigungs-Einstellungen

⊞ ✕
Benachrichtigungs-Einstellungen

✎ Bearbeitete Version - Änderungen bleiben erhalten bis zum Zurücksetzen oder Abmelden.

○
○

Benachrichtigungs-Einstellungen

Allgemein

Benachrichtigungssprache Deutsch ▼

Betreff-Vorlage Unified Firewall Notification

Empfänger +

Aggregierte Benachrichtigungen

Aggregations-Intervall 60 Min.

Max. Anzahl Benachrichtigungen Pro Mail 10000

Mails nicht senden, die keine Benachrichtigungen enthalten

Sofort-Benachrichtigungen

Max. Anzahl Mails Pro Stunde 10

8 HTTP auf HTTPS umleiten

Mit LCOS FX-Version 10.10 können Sie in den Einstellungen für ein Reverse-Proxy-Frontend die Option **HTTP auf HTTPS umleiten** aktivieren. Damit werden HTTP-Anfragen an die konfigurierte Domain oder IP-Adresse auf HTTPS umgeleitet.

UTM > Reverse-Proxy > Frontends

Reverse-Proxy-Frontend ⓘ ✕

★ Neu - Änderungen bleiben erhalten bis zum Abbrechen des Dialogs oder Abmelden.

I 0

Domäne oder IP-Adresse

Verbindung

Port

SSL

Let's Encrypt verwenden

Zertifikat

Private-Key-Passwort

HTTP auf HTTPS umleiten

"Outlook Anywhere" erlauben

Proxy-Pfade

Backend	URL
<input type="text" value="⌵"/>	<input type="text"/>

Blockierte Pfade

+ +