

LANCOM Release Notes

LCOS

10.42 Rel

Copyright (c) 2002-2021 LANCOM Systems GmbH, Würselen (Germany)

LANCOM Systems GmbH
Adenauerstraße 20 / B2
52146 Würselen
Germany

Internet: <http://www.lancom-systems.de>

20.01.2021, CBuersch

Inhaltsübersicht

1. Einleitung	2
2. Gerätespezifische Kompatibilität zu LCOS 10.42	2
3. Hinweise zu LCOS 10.42	2
Informationen zu Werkseinstellungen	2
1. Feature-Übersicht LCOS 10.42	3
1.1 Feature-Highlight 10.42	3
Dynamic Path Selection	3
1.2 Weitere Features LCOS 10.42	4
Dynamic DNS Service für die Public Cloud	4
Cloud-managed Hotspot	4
BLE API für die Realisierung innovativer Location-based Services	4
2. Historie LCOS 10.42	5
LCOS-Änderungen 10.42.277 Rel	5
LCOS-Änderungen 10.42.212 RC3	7
LCOS-Änderungen 10.42.155 RC2	8
LCOS-Änderungen 10.42.037 RC1	10
3. Allgemeine Hinweise	11
Haftungsausschluss	11
Sichern der aktuellen Konfiguration	11
Verwendung einer Minimalfirmware zur Vergrößerung des Speicherplatzes	11

1. Einleitung

LCOS („LANCOM Operating System“) ist das bewährte LANCOM Betriebssystem für Router, Access Points und WLAN-Controller. Im Rahmen der von den Produkten vorgegebenen Hardware ist die jeweils aktuelle LCOS-Version für LANCOM Produkte verfügbar und wird von LANCOM Systems kostenlos zum Download angeboten.

Dieses Dokument beschreibt die Neuerungen der LCOS Software Release 10.42 Rel sowie die Änderungen und Verbesserungen zur Vorversion.

Beachten Sie vor der Durchführung des Firmware-Update unbedingt die Hinweise im Kapitel 3 „Allgemeine Hinweise“ dieses Dokumentes.

Aktuelle Support-Hinweise und sowie Informationen über bekannte Einschränkungen zur aktuellen LCOS-Version finden Sie im Support-Bereich unserer Webseite

<https://www.lancom-systems.de/service-support/soforthilfe/aktuelle-support-hinweise/>

2. Gerätespezifische Kompatibilität zu LCOS 10.42

Grundsätzlich werden alle LANCOM Produkte über die gesamte Lebenszeit regelmäßig mit Major Releases bedient, welche neue Features und Bugfixes beinhalten.

Auch für Geräte, die keine aktuelle LCOS-Version unterstützen, werden in regelmäßigen Abständen LCOS Release Updates inklusive Bugfixes und allgemeinen Verbesserungen bereitgestellt. Eine Übersicht über die aktuell unterstützte LCOS-Version für Ihr Gerät finden Sie unter

<https://www.lancom-systems.de/produkte/firmware/lifecycle-management/produkttabellen/>

Mit LCOS 10.42 entfällt die Unterstützung für folgende Geräte

- > LANCOM 1780EW-4G
- > LANCOM 1781A-4G
- > LANCOM L-322E
- > LANCOM L-1302acn
- > LANCOM L-1310acn

3. Hinweise zu LCOS 10.42

Informationen zu Werkseinstellungen

Geräte, die mit LCOS 10.00 oder größer ausgeliefert werden, kontaktieren automatisch die LANCOM Management Cloud (LMC). Diese Funktionalität ermöglicht eine Zero-Touch-Inbetriebnahme von neuen Geräten. Falls die LMC nicht verwendet werden soll, kann diese Funktionalität über den Grundeinstellungs-Wizard bei der Erstinstallation oder im LANconfig jederzeit unter Management > LMC deaktiviert werden. Eine spätere Verwendung der LMC ist jederzeit wieder manuell aktivierbar.

1. Feature-Übersicht LCOS 10.42

1.1 Feature-Highlight 10.42

Dynamic Path Selection

Mit dem neuen Highlight-Feature Dynamic Path Selection routen Sie in Ihrem SD-WAN geschäftskritische Business-Anwendungen stets über die qualitativ beste Leitung. Das Feature überwacht dabei kontinuierlich Ihre WAN-Verbindungen in Bezug auf Last, Paketverlust, Latenz oder Jitter und entscheidet in Abhängigkeit der aktuellen Verbindungsqualität dynamisch über die optimale Leitung für bestimmte Anwendungen. Welche Leistungskriterien Sie für eine Anwendung an die WAN-Verbindung stellen, definieren Sie dabei flexibel selbst. Somit profitieren Sie in großen SD-WAN-Infrastrukturen mit mehreren WAN-Verbindungen im Active/Active-Modus von maximaler Performance und Ausfallsicherheit.

1.2 Weitere Features LCOS 10.42

Dynamic DNS Service für die Public Cloud

Die LANCOM Management Cloud (Public) wird zum DynDNS-Provider! Weisen Sie in den Standort-Einstellungen den dort eingesetzten Gateways einfach eine feste, selbstgewählte Sub-Domain zu (mycompany.dyndns-lmc.de). Diese Sub-Domain kann daraufhin beispielsweise in VPN-Gegenstellen wie dem LANCOM Advanced VPN Client hinterlegt werden. Somit bleiben mit der neuen LCOS 10.42 RC3 auch Gateways mit dynamischen WAN-IP-Adressen jederzeit über diesen Domain-Namen erreichbar.

Cloud-managed Hotspot

Erstellen Sie mit wenigen Klicks einen einfachen WLAN-Hotspot – direkt aus der LMC heraus. Ein zusätzliches Gateway oder ein WLAN-Controller mit LANCOM Public Spot Option sind hierfür nicht erforderlich. Über ein intuitiv zu bedienendes Menü individualisieren Sie Ihren Hotspot-Begrüßungsbildschirm mit Ihrem Logo sowie Ihren Unternehmensfarben und integrieren wichtige Informationen wie Impressum und Nutzungsrichtlinien für Ihre Hotspot-Benutzer. Anschließend weisen Sie das neue Hotspot-Netz den gewünschten Standorten zu und schon steht er Ihren Besuchern zur Verfügung.

BLE API für die Realisierung innovativer Location-based Services

Ob für die Innenraumlokalisierung von Patienten in Krankenhäusern, die Auswertung von Kundenaufkommen im Einzelhandel oder Asset Tracking im Logistik-Bereich: Für alle LANCOM Access Points mit Bluetooth Low Energy-Modul (BLE) steht nun eine neue API-Schnittstelle (REST) für die Einbindung ortsbezogener Dienste zur Verfügung. In Zusammenarbeit mit Drittanbietern ermöglicht diese die Realisierung einer Vielzahl ortsbezogener Dienste (Location-based Services, LBS) und innovativer IoT-Anwendungen.

Weitere Features finden Sie in den Abschnitten zu den einzelnen Builds im Kapitel 2 „Historie LCOS 10.42“.

2. Historie LCOS 10.42

LCOS-Änderungen 10.42.277 Rel

Korrekturen / Anpassungen

Allgemein

- Anfragen von LANCOM-internen Diensten (z.B. ICMP-Anfragen oder ICMP-Messungen im DPS) ins WAN, welche eine lokale Absender-Adresse aufwiesen (z.B. „ping -a INTRANET 8.8.8.8“), wurden unmaskiert gesendet, wenn in der Routingtabelle ausschließlich Routen für Loadbalancer eingetragen waren und Routen für die jeweils einzelnen WAN-Verbindungen fehlten. In der Folge schlug die Anfrage fehl.
- Das Laden einer LANCOM Routerkonfiguration von einem USB-Stick, welcher in ein unkonfiguriertes Gerät eingesteckt war, schlug fehl.
- Der Datensatz für Netzwerke im Konsolen-Pfad ‚Status / DHCP-Client / LAN-IP-List‘ wurde immer mit der maximalen statt der tatsächlichen Länge angelegt.
Dies führte dazu, dass bei Auswahl eines Interfaces (z.B. INTRANET) in WEBconfig im Menü ‚Extras / LCOS-Menübaum / Status / DHCP-Client / LAN-IP-Liste / Ifc‘ eine leere Seite ausgegeben und die Fehlermeldung „404 Not found“ angezeigt wurde. Auch per Konsole konnten die Informationen nicht ausgelesen werden.
- Bei der Protokollierung von DNS-Auflösungen wurde das Syslog über Port 512 statt Port 514 gesendet. In der Folge erreichten die Meldungen einen externen Syslog-Server nicht.
- Der Voice-Call-Manager im LANCOM Router versendete E-Mails in einer Textcodierung, in welcher z.B. Umlaute unleserlich ausgegeben wurden. Die E-Mails werden jetzt UTF-8-codiert versendet.
- Wurde auf der Konsole ein Ping mit einer Größe kleiner als 16 Byte ausgeführt (mit dem Parameter -s), führte dies zu einem unvermittelten Neustart, da die minimale Paketgröße bei 16 Byte liegt.
- Brauchte ein Prozess auf dem vRouter sehr lange (ausgelöst durch einen Mangel an CPU-Ressourcen), konnte dies zu einem unvermittelten Neustart führen.
- Die Längen-Prüfung von ICMPv6-Paketen in der IPv6-Firewall funktionierte nicht korrekt. Dies konnte dazu führen, dass ICMPv6-Pakete vom Router mit der Meldung „intruder detection“ verworfen wurden.

WLAN

- Die 802.11u-Parameter ‚Include-in-Beacon-OUI‘ und ‚Additional-OUI‘ ließen auf der Konsole lediglich die Eingabe von Kleinbuchstaben zu. In LANconfig wurden für diese Parameter aber auch Großbuchstaben zugelassen. Großbuchstaben werden jetzt in Kleinbuchstaben konvertiert.
- Bei Verwendung von 802.11u in Verbindung mit Passpoint R2 wurde der NAI-Realm nicht an das Endgerät übertragen, sodass dieses keine Verbindung aufbauen konnte.

VPN

- › Forderte der VPN-Partner mehrere Phase-1-Proposals zur parallelen Bearbeitung an statt wie sonst üblich sequenziell, kam es zu einem unvermittelten Neustart des Routers.
- › Nach einer Firmware-Aktualisierung auf LCOS 10.42 RC3 konnte es vorkommen, dass IKEv2-VPN-Verbindungen per EAP-Authentifizierung nicht mehr aufgebaut wurden, wenn in diesen kein Remote-Gateway angegeben war und als Remote-ID ‚No-Identity‘ verwendet wurde.
- › Nach dem Aufbau einer Dial-In-VPN-Verbindung von einer Außenstelle wurden die Routen vom annehmenden Router (Zentrale) gelöscht und direkt wieder hinzugefügt. Dies führte dazu, dass auch bestehende Sessions gelöscht wurden und die Kommunikation über diese Session nicht mehr möglich war (z.B. RDP).

VoIP

- › Sendete ein SIP-Provider ein INVITE mit einem zu kleinen Session Timer, antwortete der Router mit der Fehlermeldung „422 Session Interval Too Small“. Sendete der SIP-Provider dann kein neues INVITE mit einem angepassten Session Timer, wurde das Telefonat abgebaut und der Anrufer hörte kein Rufzeichen. Die Meldung „422 Session Interval Too Small“ wird jetzt nur noch bei Verwendung einer ‚Gateway-Leitung‘ zur Anbindung einer SIP-TK-Anlage versendet.
- › Sendete eine SIP-TK-Anlage in der Meldung „200 OK“ das Merkmal für SDP in Kleinbuchstaben (rtp/avp) an den Router, erkannte dieser das SDP nicht und sendete das „200 OK“ ohne SDP an den Provider. Der Provider antwortete darauf mit einem BYE und der Fehlermeldung „488 Not Acceptable Here“. Dies führte dazu, dass in einem solchen Fall das Telefonat nicht zustande kam.
- › Wenn ein SIP-Teilnehmer im INVITE in der SIP-URI das Protokoll in Kleinschreibung an den Router schickte (z.B. udp), lehnte der Router das Paket mit der Fehlermeldung „404 Not Found“ ab. Der Router ignoriert jetzt Groß- bzw. Kleinschreibung.

LCOS-Änderungen 10.42.212 RC3

Neue Features

Routing & VPN

- › IPv6-Source-Adressfilter für IKEv2 VPN-Verbindungen

Korrekturen / Anpassungen

Allgemein

- › Die Tabelle für die Mobilfunk-Historie im Pfad ‚Status / Modem-Mobilfunk / Historie‘ blieb leer, unabhängig davon, ob eine Mobilfunk-Verbindung genutzt wurde oder nicht, da der Standardwert zur Erfassung der Historie im Pfad ‚Setup / Schnittstellen / Mobilfunk / Protokollierungsintervall‘ auf ‚0‘ (ausgeschaltet) stand. Das Standardintervall wurde nun auf 300 Sekunden (5 Minuten) geändert.
- › Die Tabelle ‚Status / Last-Admin-Logins‘ wies eine fehlerhafte Struktur auf, da die erste Spalte (die einzige Index-Spalte) die IP-Adresse enthielt und nicht, wie üblich, einen eindeutigen Index-Wert (z.B. eine fortlaufende Nummer).
- › Der Konfigurations-Bezug per TR-069 bei Verwendung einer IPv6-Adresse schlug fehl, da die eigene IPv6-Adresse vom TR-069-Prozess des Routers in eckige Klammern gesetzt und daher nicht korrekt erkannt wurde. Es wurde in diesem Fall ein Fallback per IPv4 durchgeführt.

WLAN

- › In der Tabelle ‚Setup / WLAN-Management / AP-Configuration / IEEE802.11u / General‘ konnte für ein 802.11u-Standortprofil ein Profilname mit max. 32 Zeichen eingegeben werden. Der gleiche Parameter wurde jedoch in der Tabelle der WLAN-Profile mit einer Namenslänge von max. 31 Zeichen geführt. In der Folge konnte ein Profilname mit 32 Zeichen in der WLAN-Profil-Tabelle nicht konfiguriert werden, da die maximal zulässige Zeichenanzahl von 31 Zeichen überschritten wurde.
- › In einem WLAN-Controller-Szenario wurde die Domain ID aus dem Menü ‚WLAN-Controller / 802.11u / Hotspot 2.0 Profile‘ von den Access Points nicht übernommen, weshalb der Platzhalter ‚0‘ verwendet wurde. Dadurch wurde eine falsche Domain ID an anfragende WLAN-Teilnehmer übergeben.
- › Wurde auf einem WLAN-Controller im Konsolen-Pfad ‚Setup / WLAN-Management / AP-Configuration / IEEE802.11u / General‘ für den ‚Venue-Name‘ ein nicht unterstützter regulärer Ausdruck (RegEx) eingetragen, führte dies zu einem unvermittelten Neustart des Gerätes.
- › Bei der Verwendung einer eigenen Start-Seite im Public Spot wurde beim Aufruf derselben lediglich eine weiße Seite angezeigt, da bei der Weitergabe der Redirect-URI (Uniform Resource Identifier) an den Public Spot Teilnehmer eine falsche IP-Adresse enthalten war.

LCOS-Änderungen 10.42.155 RC2

Neue Features

Allgemein

- › Der 802.1X-Authenticator für Ethernet-Ports ist nun in allen Geräten enthalten.
- › Der 802.1X-Authenticator kann nun optional statt einer 802.1X-Verhandlung sofort eine Prüfung der MAC-Adresse des angeschlossenen Ethernet-Geräts mit einem RADIUS-Server durchführen.
- › In Neukonfigurationen ist die MAC-Adresse von Bundle-Interfaces nun ‚0‘ und wird im Betrieb auf die systemweite, gerätespezifische MAC-Adresse umgesetzt. Dies erleichtert die Portierung von Konfigurationen.
- › Die HTTP(S)-Hit-Liste der Layer-7-Erkennung wurde aktualisiert.
- › Für die Verbindung mit einem Wireless ePaper-Server kann nun das ThinAP2.0/TLS-Protokoll verwendet werden.
- › In Neukonfigurationen sind die Management-Protokolle Telnet und Telnet-over-SSL nun standardmäßig deaktiviert.

Routing & VPN

- › Der Linecode des xDSL-Modems der LANCOM 179x-Serie wurde aktualisiert.

WLAN

- › Unterstützung für Stanley-AeroScout RTLS Tags
- › Besteht das Ergebnis der Kanalbeurteilung der automatischen WLAN-Kanalwahl aus mehreren gleich guten Kanälen, wird daraus ein Kanal anhand der systemweiten MAC-Adresse gewählt. Dies verbessert Szenarien, in denen mehrere benachbarte Access Points zeitgleich eine automatische Kanalwahl durchführen.
- › Unterstützung einer JSON-API zur Ausleitung von BLE- und WLAN-Lokationsdaten
- › Die standardmäßige WLAN-Passphrase ist nun leer. Zur Aktivierung einer verschlüsselten WLAN-SSID ist das Setzen einer benutzerdefinierten Passphrase notwendig.
- › Unterstützung der Konfiguration von PassPoint R2 via WLC

VoIP

- › Für SIP-Leitungen kann die Übergabe einer fixen PPI oder PAI konfiguriert werden.
- › Für SIP-PBX-Leitungen kann nun eine Loopback-Adresse konfiguriert werden.
- › Die Voice-Call-Manager-Tabelle ‚Benutzer-Einstellungen‘ kann nun beliebig viele Einträge beinhalten.

Korrekturen / Anpassungen

Allgemein

- › Beim LANCOM OAP-1702B fehlte im LCOS die spezifische Angabe für die PoE-Leistung, welche per LLDP bei einem PoE-fähigen Switch angefordert wurde.
- › Bei LANCOM Routern traten sporadisch CPU-Auslastungen bis zu 100% auf, welche auf ein Problem mit der Session-Anzahl in der IPv4-Maskierungstabelle der Geräte zurückzuführen waren. In der Folge kam es durch die hohe CPU-Last u.a. zu Problemen beim IPv4-Routing.
- › Die Kommunikation mit einem externen Syslog-Server über einen benutzerdefinierten Port (ungleich 514) war unabhängig vom genutzten Protokoll (TCP oder UDP) nicht möglich. Der Router ignorierte die Einstellung und nutzte weiterhin den Port 514.
- › Die Konfiguration konnte auf einen durch die LMC verwalteten Router nicht ausgerollt werden, wenn gleichzeitig ein neues Objekt in der DNS-Ziel-Liste angelegt und dieses in einer neuen Firewall-Regel referenziert wurde.
- › Wenn für einen GRE-Tunnel ein Routing-Eintrag erstellt wurde, welcher auf eine IP-Adresse aus einem lokalen Netzwerk verwies, konnte der GRE-Tunnel nicht aufgebaut werden.
- › Bei einer Änderung des Hauptgeräte-Passwortes per Konsolen-Befehl ‚passwd -n‘, welches das EscapeZeichen ‚\‘ beinhaltete, wurden weitere Zeichen vor dem Passwort eingefügt. Dies führte dazu, dass mit diesem Passwort kein Zugriff auf das Gerät möglich war und das Passwort mit dem Befehl ‚passwd -n‘ nicht erneut gesetzt werden konnte.
- › Es konnte bei aktivierter ‚Dynamic Path Selection‘ während des Ausroll-Vorgangs einer komplexen Konfiguration über die LMC zu einem unvermittelten Neustart kommen.

LCOS-Änderungen 10.42.037 RC1

Neue Features

Allgemein

- › Die HTTP-/HTTPS-Tracking-Liste der Layer-7-Anwendungserkennung wurde aktualisiert.

Routing & VPN

- › Unterstützung für SD-WAN Dynamic Path Selection

WLAN

- › Entfall der standardmäßigen WLAN-Passphrase
- › Ein LANCOM WLC konfiguriert das erste WLAN-Modul (2,4 GHz) eines verwalteten Access Points nun per Default für 20 MHz Kanalbreite. Dies betrifft nur neu in die Verwaltung aufgenommene Access Points.

3. Allgemeine Hinweise

Haftungsausschluss

Die LANCOM Systems GmbH übernimmt keine Gewähr und Haftung für nicht von der LANCOM Systems GmbH entwickelte, hergestellte oder unter dem Namen der LANCOM Systems GmbH vertriebene Software, insbesondere nicht für Shareware und sonstige Fremdsoftware.

Sichern der aktuellen Konfiguration

Bitte sichern Sie vor dem Update Ihrer LANCOM-Geräte auf eine neue LCOS-Version unbedingt Ihre Konfigurationsdateien!

Wegen umfangreicher Feature-Erweiterungen ist ohne eine Sicherung der Konfigurationsdaten eine Rückkehr auf die alte Firmware **nicht mehr automatisch möglich**.

Wenn Sie Geräte, die Sie über eine Router-Verbindung oder WLAN-Punkt-zu-Punkt-Verbindung erreichen können, aktualisieren möchten, bedenken Sie bitte, dass Sie zuerst das entfernte LANCOM Gerät und anschließend das lokale LANCOM Gerät aktualisieren. Eine Anleitung zur Firmware-Aktualisierung erhalten Sie im LCOS-Referenzhandbuch.

Wir empfehlen zudem, dass produktive Systeme vor dem Einsatz in der Kundenumgebung erst einem internen Test unterzogen werden, da trotz intensivster interner und externer Qualitätssicherungsmaßnahmen ggf. nicht alle Risiken durch LANCOM Systems ausgeschlossen werden können.

Verwendung einer Minimalfirmware zur Vergrößerung des Speicherplatzes

Durch zahlreiche neue Funktionen in der LCOS-Firmware ist es bei älteren LANCOM Geräten unter Umständen nicht mehr möglich, zwei vollwertige Firmware-Versionen gleichzeitig zu speichern. Um mehr Platz im Speicher zu schaffen, muss dann statt einer vollwertigen Firmware zunächst eine eingeschränkte, kleinere Firmware eingerichtet werden. Hierdurch steht für die andere Firmware im Gerät erheblich mehr Speicher zur Verfügung.

Diese Einrichtung ist nur einmalig erforderlich und wird mit einer „Minimalfirmware“ durchgeführt.

Nach dem Einspielen der Minimalfirmware steht die Firmsafe-Funktion des LANCOM nur noch in eingeschränktem Umfang zur Verfügung. Das Update auf eine neuere Firmware ist weiterhin problemlos möglich.

Das LANCOM Gerät arbeitet nach einem fehlgeschlagenen Update jedoch mit einer Minimalfirmware, die Ihnen ausschließlich den lokalen Zugriff auf das Gerät erlaubt. Alle erweiterten Funktionalitäten, insbesondere die Remote Administration, sind nicht verfügbar, solange die Minimalfirmware aktiv ist.