

A Addendum zur LCOS-Version 8.0

A.1 Übersicht

- 'IPSec over HTTPS' →Seite 1
- 'Basic HTTP Fileserver für LCOS 8.0' →Seite 3
- 'Automatisches Laden von Firmware oder Konfiguration von externen Datenträgern' →Seite 4
- 'SSH-Client' →Seite 7
- 'Alternative Boot-Config' →Seite 10
- 'Alternative DHCP-Server zur Weiterleitung' →Seite 13
- 'Kanallastanzeige im WLC-Betrieb' →Seite 14
- 'Änderungen in LANconfig' →Seite 15
- '802.1x-Accounting im WLAN-Controller für logische WLANs aktivieren' →Seite 16
- 'LANCOM Content Filter' →Seite 17
- 'DFS3' →Seite 35
- 'Alternative URLs für CRLs' →Seite 36
- 'Broken-Link-Detection' →Seite 36

A.2 IPSec over HTTPS

A.2.1 Einleitung

In manchen Umgebungen ist es nicht möglich, über eine vorhandene Internetverbindung eine geschützte VPN-Verbindung aufzubauen, weil in den Einstellungen einer vorgeschalteten Firewall die von IPSec genutzten Ports gesperrt sind. Um auch in einer solchen Situation eine IPSec-geschützte VPN-Verbindung aufbauen zu können, unterstützen LANCOM VPN-Router die IPSec over HTTPS-Technologie.

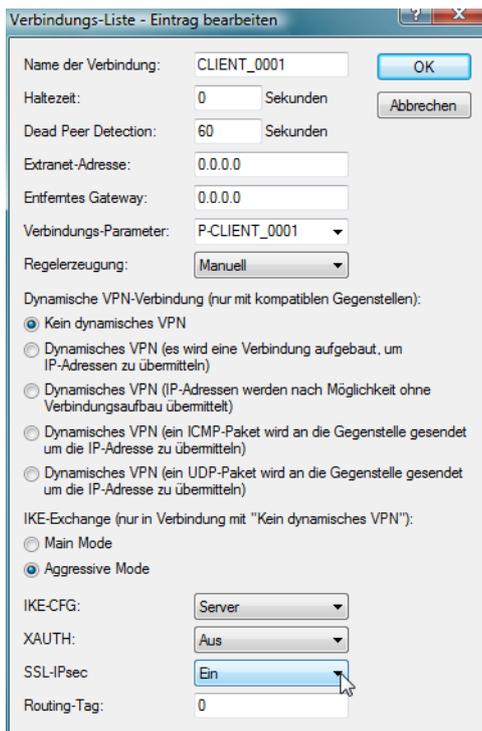
Dabei wird zunächst eine Datenübertragung über Standard-IPSec versucht. Kommt diese Verbindung nicht zustande (z.B. weil der IKE Port 500 in einem Mobilfunknetz gesperrt ist), so wird automatisch ein Verbindungsaufbau versucht, bei dem das IPSec VPN mit einem zusätzlichen SSL-Header (Port 443, wie bei https) gekapselt wird.

Bitte beachten Sie, dass die IPSec over HTTPS-Technologie nur genutzt werden kann, wenn beide Gegenstellen diese Funktion unterstützen und die entsprechenden Optionen aktiviert sind. IPSec over HTTPS ist verfügbar in LANCOM VPN-Routern mit LCOS 8.0 oder höher sowie im LANCOM Advanced VPN Client 2.22 oder höher.

A.2.2 Konfiguration der IPSec over HTTPS-Technologie

Für den aktiven Verbindungsaufbau eines LANCOM-VPN-Geräts zu einer anderen VPN-Gegenstelle mit Hilfe der IPSec over HTTPS-Technologie aktivieren Sie die Option im entsprechenden Eintrag für die Gegenstelle in der VPN-Namenliste.

- LANconfig: VPN ► Allgemein ► Verbindungsliste
- WEBconfig: LCOS-Menübaum ► Setup ► VPN ► VPN-Gegenstellen



■ **SSL-IPsec**

Mit dieser Option aktivieren Sie die Nutzung der IPsec over HTTPS-Technologie beim aktiven Verbindungsaufbau zu dieser Gegenstelle.

Mögliche Werte:

- Ein, Aus

Default:

- Aus

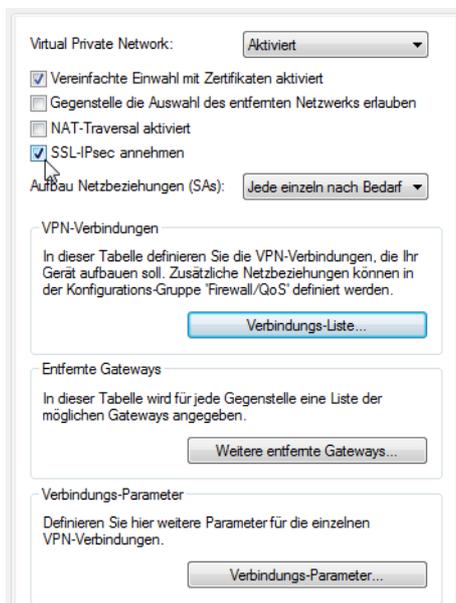


Bitte beachten Sie, dass bei eingeschalteter IPsec over HTTPS-Option die VPN-Verbindung nur aufgebaut werden kann, wenn die Gegenstelle diese Technologie ebenfalls unterstützt und die Annahme von passiven VPN-Verbindungen mit IPsec over HTTPS bei der Gegenstelle aktiviert ist.

Für den passiven Verbindungsaufbau zu einem LANCOM-VPN-Gerät von einer anderen VPN-Gegenstelle mit Hilfe der IPsec over HTTPS-Technologie (LANCOM-VPN-Gerät oder LANCOM Advanced VPN Client) aktivieren Sie die Option in den allgemeinen VPN-Einstellungen.

- LANconfig: VPN ► Allgemein

- WEBconfig: LCOS-Menübaum ► Setup ► VPN



■ **SSL-IPsec annehmen**

Mit dieser Option aktivieren Sie die Annahme von passiven Verbindungsaufbauten, wenn die Gegenstelle die IPsec over HTTPS-Technologie nutzt.

Mögliche Werte:

- Ein, Aus

Default:

- Aus



Der LANCOM Advanced VPN Client unterstützt einen automatischen Fallback auf IPsec over HTTPS. In dieser Einstellung versucht der VPN-Client zunächst eine Verbindung **ohne** die zusätzliche SSL-Kapselung aufzubauen. Falls diese Verbindung nicht aufgebaut werden kann, versucht das Gerät im zweiten Schritt eine Verbindung **mit** der zusätzlichen SSL-Kapselung aufzubauen.

A.2.3 Statusanzeigen der IPsec over HTTPS-Technologie

Die Statusanzeigen zu jeder aktiven VPN-Verbindung zeigen an, ob für die jeweilige Verbindung die IPsec over HTTPS-Technologie (SSL-Encaps.) genutzt wird.

- WEBconfig: LCOS-Menübaum ▶ Status ▶ VPN ▶ Verbindungen

Verbindungen																
Gegenstelle	Status	Letzter-Fehler	Mode	SH-Zeit	phys.-Verb.	B1-HZ	Entferntes-Gw	Nat-Erkennung	SSL-Encaps.	Krypt-Alg	Krypt-Laenge	Hash-Alg	Hash-Laenge	Hmac-Alg	Hmac-Laeng	
CLIENT_0004	Verbindung (none)		passiv	0		NETCOLOGN	9999	91.114.240.66	no-nat	nein	AES	128	HMAC_MD5	128	(none)	0
LCS	Verbindung (none)		aktiv	9999		NETCOLOGN	9999	213.217.69.77	no-nat	nein	AES	128	HMAC_MD5	128	(none)	0

A.3 Basic HTTP Fileserver für LCOS 8.0

A.3.1 Einleitung

Der eingebaute HTTP-Server in LCOS bietet die Möglichkeit, Dateien von einem externen Speichermedium über das HTTP-Protokoll bereitzustellen und arbeitet so als einfacher Dateiserver.

Diese Funktion wird von allen LANCOM-Geräten mit USB-Anschluss unterstützt.

A.3.2 Vorbereitung des USB-Speichermediums

So bereiten Sie ein USB-Medium für den Einsatz an einem LANCOM-Gerät vor:

- Dateisystem: Formatieren Sie das USB-Medium mit FAT16 oder FAT32 Dateisystem.
- Basisverzeichnis: Erstellen Sie auf dem USB-Medium ein Verzeichnis `public_html`. Der HTTP-Server von LCOS greift nur auf Dateien in diesem Verzeichnis und den evtl. vorhandenen Unterverzeichnissen zu. Alle anderen Dateien auf dem USB-Medium werden ignoriert.
- USB-Verbindung: Verbinden Sie das Massenspeichergerät mit dem USB-Anschluss des LANCOM-Gerätes.

A.3.3 Einhängepunkt des USB-Mediums im LCOS ermitteln

Beim Anschließen eines USB-Mediums an ein LANCOM-Gerät wird automatisch ein Einhängepunkt erzeugt, der von LCOS zur internen Verwaltung des Mediums verwendet wird. Dieser Einhängepunkt bleibt für ein bestimmtes USB-Medium immer gleich, auch nach einem Reboot oder Neustart. Verschiedenen Medien wird jeweils ein eigener, eindeutiger Einhängepunkt zugewiesen.

Um auf die Daten des USB-Mediums zugreifen zu können, muss der zugehörige Einhängepunkt bekannt sein. Den Einhängepunkt der USB-Medien können Sie über die Statustabelle ermitteln:

- WEBconfig: LCOS-Menübaum ▶ Status ▶ Dateisystem ▶ Volumes

Volumes					
ID	Mountpunkte	Dateisystem	Entmountbar?	Frei	Groesse
BlkDev-1	/PKBACK#.001, /usb	FAT32	1	53382 KB	122 MB
MiniFs	/minifs	MiniFs	0	209 KB	256 KB

Die Statustabelle zeigt alle Datenträger ("Volumes"), die dem Gerät bekannt sind.

- MiniFs ist das eingebaute Flash-Dateisystem, das es auf fast allen Geräten gibt.

- BlkDev-n bezeichnen die bekannten USB-Medien. Wenn nur ein USB-Massenspeichergerät angeschlossen ist, wird es BlkDev-1 genannt und ist eingehängt unter /usb.

A.3.4 Zugriff auf die Dateien eines USB-Mediums

Um auf die Dateien auf dem USB-Medium über den HTTP-Server im LCOS zuzugreifen, verwenden Sie die folgende URL:

- `http://<IP address of device>/filesrv/<mount point>/<file name>`

Wenn z. B. eine Datei `coupon.jpeg` benannt ist und auf dem einzigen USB-Medium im Basisverzeichnis unter `\public_html` gespeichert ist, dann können Sie mit folgendem Link darauf zugreifen:

`http://<IP address of device>/filesrv/usb/coupon.jpeg`



Der Zugriff kann auch über HTTPS anstatt HTTP erfolgen.

A.3.5 Unterstützte Inhaltstypen

Der HTTP-Server im LCOS nutzt die Dateierweiterung, um den MIME-Inhaltstyp zu bestimmen, der für die korrekte Darstellung der Inhalte im Browser benötigt wird. Momentan sind die folgenden Erweiterungen bekannt und werden in einen korrekten MIME-Inhaltstyp übersetzt:

- `.htm` und `.html` für HTML-Dateien
- `.gif`, `.jpg`, `.jpeg`, `.png`, `.bmp`, `.pcx` für entsprechende Formate der Bilddateien
- `.ico` für Icon-Dateien
- `.pdf` für Adobe Acrobat PDF-Dateien
- `.css` für Cascading-Style-Sheet-Dateien

A.3.6 Verzeichnisstruktur

Das Verzeichnis `public_html` kann Unterverzeichnisse beinhalten. Der HTTP-Server im LCOS hat bestimmte Regeln für den Zugriff auf Verzeichnisse:

- Wenn eine Datei `'index.html'` in dem Unterverzeichnis existiert, dann wird diese zum HTTP-Client übertragen; andernfalls:
- Wenn eine Datei `'index.htm'` in dem Unterverzeichnis existiert, dann wird diese zum HTTP-Client übertragen; andernfalls:
- Der Fileserver erstellt eine einfache Liste aller Dateien und Unterverzeichnisse im Hauptverzeichnis.

A.4 Automatisches Laden von Firmware oder Konfiguration von externen Datenträgern

A.4.1 Einleitung

LANCOM-Geräte mit USB-Anschluss können mit Hilfe eines externen Datenträgers sehr komfortabel in Betrieb genommen werden. Firmware-Dateien und Loader können ebenso wie vollständige Konfigurationen oder Skripte automatisch von einem USB-Medium in das Gerät geladen werden.

A.4.2 Automatisches Laden von Loader- und/oder Firmware-Dateien

Wenn die Funktion aktiviert ist, sucht das Gerät beim Mounten eines USB-Mediums nach Loader- und/oder Firmware-Dateien im Verzeichnis "Firmware". In diesem Verzeichnis werden alle Dateien mit der Dateiendung ".upx" für den automatischen Ladevorgang in Betracht gezogen, die zum aktuellen Gerätetyp passen. Dazu wird zunächst der Header der Dateien ausgelesen, die Dateien werden anschließend nach folgenden Regeln verwendet:

- Wird mindestens eine upx-Datei mit Loader gefunden, wird der Loader mit der höchsten Versionsnummer geladen, sofern im Gerät nicht schon ein Loader mit höherer Versionsnummer vorhanden ist.
- Wird mindestens eine Firmware-Datei gefunden, wird die Firmware mit der höchsten Versionsnummer geladen, wenn die Version ungleich der im Gerät aktiven oder inaktiven Firmwareversionen ist.

Während des automatischen Ladevorgangs blinken die Power- und die Online-LED am Gerät abwechselnd. Wenn zunächst ein Loader geladen wird, erfolgt nach dem Ladevorgang ein Neustart des Geräts und anschließend evtl. ein zweiter automatischer Ladevorgang für eine Firmware. Auch bei dem zweiten Ladevorgang blinken die Power- und die Online-LED am Gerät abwechselnd.

□ Automatisches Laden von Firmware oder Konfiguration von externen Datenträgern

An den automatischen Ladevorgang von Loader- und/oder Firmware-Dateien können sich evtl. noch weitere Ladevorgänge für Konfigurations- und/oder Skript-Dateien anschließen.

Wenn der automatische Ladevorgang vollständig abgeschlossen ist, leuchten alle LEDs des Geräts für 30 Sekunden grün. Das USB-Medium kann dann entfernt werden.

A.4.3 Automatisches Laden von Konfigurations- und/oder Skript-Dateien

Wenn die Funktion aktiviert ist, sucht das Gerät beim Mounten eines USB-Mediums nach Konfigurations- und/oder Skript-Dateien im Verzeichnis "Config". In diesem Verzeichnis werden alle Dateien mit der Dateiendung ".lcs" oder ".lcf" für den automatischen Ladevorgang in Betracht gezogen, die zum aktuellen Gerätetyp passen. Dazu wird zunächst der Header der Dateien ausgelesen, die Dateien werden anschließend nach folgenden Regeln verwendet:

- Eine Voll-Konfiguration ".lcf" wird immer vor einem Skript ".lcs" geladen. Es werden nur Voll-Konfigurationen geladen, deren Gerätetyp-Eintrag gleich dem Typ des ladenden Geräts ist und deren Firmware-Version-Eintrag im Header gleich der im ladenden Gerät aktiven Firmware ist. Liegen mehrere passende Voll-Konfigurationen vor, so wird die Auswahl nach den folgenden Kriterien in dieser Reihenfolge vorgenommen:
 - Der Konfigurationsheader enthält eine Geräte-Seriennummer und diese stimmt mit der Seriennummer des ladenden Gerätes überein.
 - Der Konfigurationsheader enthält eine MAC-Adresse und diese stimmt mit der MAC-Adresse des ladenden Gerätes überein.
 - Sollten danach mehrere Konfigurationsdateien ohne die zuvor genannten Kriterien verbleiben, wird die Konfiguration mit dem aktuellsten Datum verwendet.

 Die Header-Parameter für Konfigurationsdateien können manuell im Datei-Dialog von LANconfig als Meta-Parameter gesetzt werden, wenn eine Offline-Konfiguration gespeichert wird.

- Sollte keine Voll-Konfiguration vorliegen, wird eine eventuell vorhandene Skript-Datei (".lcs") herangezogen. Liegen mehrere passende Skripte vor, so wird die Auswahl nach den folgenden Kriterien in dieser Reihenfolge vorgenommen:
 - Der Skript-Header enthält eine Geräte-Seriennummer und diese stimmt mit der Seriennummer des ladenden Gerätes überein.
 - Der Skript-Header enthält eine MAC-Adresse und diese stimmt mit der MAC-Adresse des ladenden Gerätes überein.
 - Der Skript-Header enthält eine Firmware-Version und diese stimmt mit der Firmware-Version des ladenden Gerätes überein.
 - Sollten danach mehrere Skripte ohne die zuvor genannten Kriterien verbleiben, wird das Skript mit der neuesten Versionsnummer bzw. mit dem aktuellsten Datum verwendet.

 Die Header-Parameter für Skripte können manuell in einem Text-Editor in den entsprechenden Skript-Dateien durch die Angabe "SERIAL:" und/oder "MAC:" und ggf. einer Firmwareversion gesetzt werden.

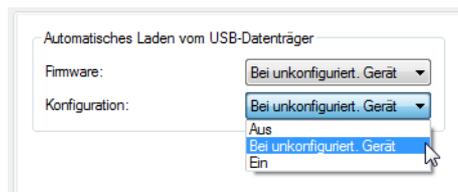
Während des automatischen Ladevorgangs blinken die Power- und die Online-LED am Gerät abwechselnd.

Wenn der automatische Ladevorgang vollständig abgeschlossen ist, leuchten alle LEDs des Geräts für 30 Sekunden grün. Das USB-Medium kann dann entfernt werden.

A.4.4 Konfiguration

Die Konfiguration für das automatische Laden finden Sie in folgendem Menü:

- LANconfig: Management ► USB-Datenträger



- WEBconfig: LCOS-Menübaum ► Setup ► Automatisches-Laden

Automatisches-Laden

-   Firmware-und-Loader wenn-unkonfiguriert
-   Konfiguration-und-Skript wenn-unkonfiguriert

■ Firmware

Mit dieser Option aktivieren Sie das automatische Laden von Loader- und/oder Firmware-Dateien von einem angeschlossenen USB-Medium.

Mögliche Werte:

- Aus

Das automatische Laden von Loader- und/oder Firmware-Dateien für das Gerät ist deaktiviert.

- Ein

Das automatische Laden von Loader- und/oder Firmware-Dateien für das Gerät ist aktiviert.

Beim Mounten eines USB-Mediums wird versucht, eine passende Loader- und/oder Firmware-Datei in das Gerät zu laden. Das USB-Medium wird beim Einstecken in den USB-Anschluss am Gerät oder beim Neustart gemountet.

- Bei unkonfiguriert. Gerät

Das automatische Laden von Loader- und/oder Firmware-Dateien für das Gerät wird nur dann aktiviert, wenn sich das Gerät im Auslieferungszustand befindet. Durch einen Konfigurations-Reset kann ein Gerät jederzeit wieder auf den Auslieferungszustand zurückgesetzt werden.

Default:

- Bei unkonfiguriert. Gerät



Durch den Assistenten für Sicherheitseinstellungen bzw. für Grundeinstellungen wird diese Option auf "inaktiv" gesetzt.

■ Konfiguration

Mit dieser Option aktivieren Sie das automatische Laden von Konfigurations- und/oder Skript-Dateien von einem angeschlossenen USB-Medium.

Mögliche Werte:

- Aus

Das automatische Laden von Konfigurations- und/oder Skript-Dateien für das Gerät ist deaktiviert.

- Ein

Das automatische Laden von Konfigurations- und/oder Skript-Dateien für das Gerät ist aktiviert.

Beim Mounten eines USB-Mediums wird versucht, eine passende Konfigurations- und/oder Skript-Dateien in das Gerät zu laden. Das USB-Medium wird beim Einstecken in den USB-Anschluss am Gerät oder beim Neustart gemountet.

- Bei unkonfiguriert. Gerät

Das automatische Laden von Konfigurations- und/oder Skript-Dateien für das Gerät wird nur dann aktiviert, wenn sich das Gerät im Auslieferungszustand befindet. Durch einen Konfigurations-Reset kann ein Gerät jederzeit wieder auf den Auslieferungszustand zurückgesetzt werden.

Default:

- Bei unkonfiguriert. Gerät



Durch den Assistenten für Sicherheitseinstellungen bzw. für Grundeinstellungen wird diese Option auf "inaktiv" gesetzt.

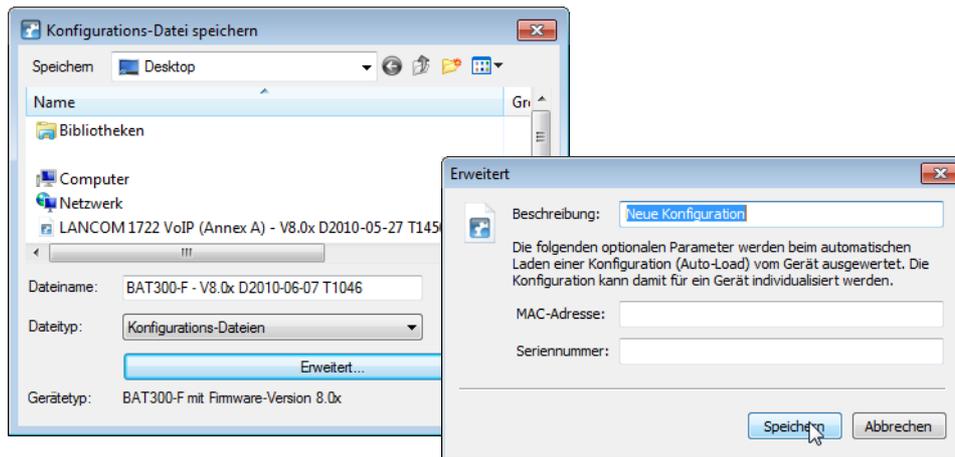


Wenn Sie verhindern wollen, dass ein Gerät durch manuellen Reset auf Werkseinstellungen und Einstecken eines USB-Datenträgers mit einer unerwünschten Konfiguration versehen werden kann, müssen Sie den Reset-Schalter deaktivieren.

A.4.5 Meta-Daten für Konfigurationsdateien

Für das automatische Laden von einem USB-Datenträger können Konfigurationsdateien mit der Seriennummer und/oder der MAC-Adresse eines Geräts gekennzeichnet werden. Die Geräte laden mit der Auto-Load-Funktion dann nur die Konfiguration bzw. das Script, bei denen die eingetragene Geräte-Seriennummer mit der Seriennummer des ladenden Gerätes übereinstimmt.

LANconfig bietet beim Speichern einer Konfiguration die Möglichkeit, diese Informationen als Meta-Parameter zu erfassen. Wählen Sie dazu beim Speichern der Konfiguration aus LANconfig die Schaltfläche **Erweitert**:



A.5 SSH-Client

A.5.1 Einleitung

Neben dem SSH-Server, der eine sichere und authentifizierte Einwahl in ein LANCOM-Gerät ermöglicht, stellt LCOS auch einen SSH-Client zur Verfügung. Über diesen SSH-Client können von einem LANCOM-Gerät aus SSH-Verbindungen zu einem entfernten Server – z.B. ein weiteres LANCOM-Gerät oder ein Unix-Server – aufgebaut werden. Diese Funktion ist sehr nützlich, wenn eine direkte Verbindung zu dem entfernten System nicht möglich ist, aber eine indirekte Verbindung über das LANCOM-Gerät existiert, das aus beiden Subnetzen erreicht werden kann.

Der SSH-Client kann über einfache Befehle auf der Kommandozeile gestartet werden, ähnlich dem OpenSSH-Client auf einem Linux- oder Unix-System.

A.5.2 CLI-Argumente für den SSH-Client

Die SSH-Verbindung zu einem entfernten System wird mit dem folgenden Befehl gestartet:

- `ssh [-?] [-h] [-b/-a loopback-address] [-p port] [-C] [-j interval] [user@]host [command]`
 - `-?`, `-h`: zeigen eine kurze Hilfe der möglichen Argumente
 - `-b`, `-a`: ermöglicht die Angabe der Absenderadresse (Loopback-Adresse). Diese Option ist besonders im Zusammenhang mit ARF wichtig.
 - `-p`: gibt den zu verwendenden Port an. Wird der Port nicht angegeben, wird der TCP-Port 22 verwendet.
 - `command`: der SSH-Client kann entweder eine interaktive Shell auf dem entfernten System starten oder nur einen einzelnen Befehl ausführen. Wird kein Befehl angegeben, wird eine interaktive Shell gestartet.
 - `user`: Benutzername für die Anmeldung am entfernten System. Nur wenn kein expliziter Benutzername angegeben ist, wird der aktuelle Nutzer der Anmeldung an der LCOS CLI verwendet.
 - `-C`: Wenn diese Option angegeben wird, versucht der SSH-Client eine Datenkompression über den zlib-Algorithmus mit dem entfernten System auszuhandeln. Wenn das entfernte System diese Kompression nicht unterstützt, werden die Daten ohne Kompression übertragen. Der Einsatz der Kompression ist in den meisten Fällen nur auf langsamen Verbindungen (z.B. über ISDN) sinnvoll. Auf schnellen Verbindungen ist der zusätzliche Overhead der Kompression meistens größer als der Gewinn durch die Datenreduzierung.
 - `-j interval`: Wenn die Verbindung zu dem entfernten System über einen NAT-Router oder eine Firewall geführt wird, ist es möglicherweise sinnvoll, die Verbindung dauerhaft aufrecht zu erhalten. Bei einer interaktiven SSH-Sitzung werden phasenweise keine Daten übertragen, was zu einer Unterbrechung der Verbindung im Gateway aufgrund von Timeouts führen kann. In diesen Fällen kann der SSH-Client regelmäßig Keep-Alive-Pakete senden, die vom entfernten System als Leerlaufprozess interpretiert werden, die dem Gateway aber das Fortbestehen der Verbindung signalisieren. Mit diesem Argument wird das Intervall in Sekunden angegeben, in dem die Keep-Alive-Pakete verschickt werden. Die Keep-Alive-Pakete werden dabei nur versendet, wenn der SSH-Client für die Dauer des Intervalls keine anderen Daten an das entfernte System schicken muss.

A.5.3 CLI-Argumente für den Telnet-Client

Alternativ zum SSH-Client kann auch über Telnet eine Verbindung zu einem entfernten System mit dem folgenden Befehl gestartet werden:

- `telnet [-?] [-h] [-b loopback-address] host [port]`

□ SSH-Client

- `-?`, `-h`: zeigen eine kurze Hilfe der möglichen Argumente
- `-b`: ermöglicht die Angabe der Absenderadresse (Loopback-Adresse). Diese Option ist besonders im Zusammenhang mit ARF wichtig.
- `port`: gibt den zu verwendenden Port an. Wird der Port nicht angegeben, wird der TCP-Port 23 verwendet.

A.5.4 Öffentliche Schlüssel für die Authentifizierung

SSH nutzt für die Authentifizierung öffentliche Schlüssel, die vom entfernten System übermittelt werden. Wenn ein SSH-Client eine Verbindung zu einem SSH-Server aufbauen will, übermittelt der Server den öffentlichen Schlüssel an den Client, der diesen Schlüssel dann in seinen Dateien sucht. Die folgenden Situationen können dabei auftreten:

- Der SSH-Client findet den Schlüssel in seiner Liste der bekannten Server-Schlüssel, und der Schlüssel ist dem entsprechenden Hostnamen bzw. der IP-Adresse zugeordnet. Die SSH-Verbindung kann dann ohne weitere Benutzeraktivität aufgebaut werden.
- Der SSH-Client findet den Schlüssel **nicht** in seiner Liste der bekannten Server-Schlüssel, und auch keinen anderen Schlüssel vom gleichen Typ (RSA bzw. DSS) für den entsprechenden Hostnamen bzw. die IP-Adresse. Der SSH-Client geht davon aus, dass es die erste Verbindung zu diesem Server ist und zeigt den öffentlichen Schlüssel und den zugehörigen Fingerabdruck an. Der Anwender kann den Schlüssel mit einer auf anderem Wege übermittelten Version verifizieren und entscheiden, ob der Server in der Liste der bekannten SSH-Server gespeichert werden darf. Wenn der Anwender diese Verifizierung ablehnt, wird die SSH-Verbindung sofort beendet.
- Der SSH-Client findet einen Schlüssel für den entsprechenden Hostnamen bzw. die IP-Adresse, dieser weicht aber von dem aktuell verwendeten Schlüssel ab. Beide Schlüssel werden angezeigt, dann wird die SSH-Verbindung beendet, weil der SSH-Client eine Man-in-the-middle-Attacke vermutet. Sofern das entfernte System den öffentlichen Schlüssel kürzlich geändert hat, muss der Administrator den veralteten Eintrag aus der Liste der bekannten Server löschen.

Nach der erfolgreichen Verifikation des Server-Schlüssels kann der Administrator das Passwort zur Anmeldung am entfernten System eingeben. Das Passwort kann nicht direkt über den Kommandozeilenbefehl eingegeben werden. SSH-Verbindungen werden üblicherweise durch den Server beendet, z.B. durch Eingabe von "Exit" in der Shell. In manchen Fällen ist es nötig, die SSH-Verbindung durch den Client zu beenden, z.B. wenn die Anwendung auf der Server-Seite gestört ist. Der SSH-Client im LCOS verwendet die gleiche Zeichenfolge wie OpenSSH zum Beenden einer Verbindung, also die Folge Tilde – Punkt.



Wenn die LCOS CLI-Sitzung selbst durch einen OpenSSH-Client geöffnet wurde, wird die Folge Tilde – Tilde – Punkt verwendet, da ansonsten die falsche Verbindung beendet wird.

A.5.5 Erzeugung von SSH-Schlüsseln

Die SSH-Authentifizierung unterstützt zwei unterschiedliche Verfahren:

- interaktiv mit der Passwordeingabe über die Tastatur
- mit dem Austausch von öffentlichen Schlüsseln

Die Schlüssel müssen individuell und anwenderbezogen erstellt werden, es gibt keine vordefinierten Standardschlüssel. Im Auslieferungszustand unterstützen die LANCOM-Geräte daher nur die Authentifizierung über Passwort.

Die Erzeugung von Schlüsseln wird über den Befehl `sshkeygen` an der CLI des Gerätes gestartet, auf dem der Administrator den SSH-Client nutzen möchte. Dabei gilt folgende Syntax:

- `sshkeygen [-?] [-h] [-t dsa|rsa] [-b bits] [-f output-file]`
 - `-?`, `-h`: zeigen eine kurze Hilfe der möglichen Argumente
 - `-t`: dieses Argument bestimmt den Typ des Schlüssels.

SSH unterstützt zwei Typen von Schlüsseln:

RSA-Schlüssel sind am weitesten verbreitet und haben eine Länge von 512 bis zu 16384 Bit. Verwenden Sie nach Möglichkeit Schlüssel mit einer Länge von 1024 bis 2048 Bit.

DSS-Schlüssel folgen dem Standard des National Institute of Standards and Technology (NIST) und werden z.B. in Umgebungen eingesetzt, die eine Compliance mit dem Federal Information Processing Standard (FIPS) erfordern. DSS-Schlüssel haben immer eine Länge von 1024 Bit, sind aber langsamer als die entsprechenden RSA-Schlüssel.

Wird kein Typ angegeben, wird ein Schlüssel vom Typ RSA erzeugt.

- `-b`: dieses Argument bestimmt die Länge des Schlüssels in Bit für RSA-Schlüssel.
Wird keine Länge angegeben, wird ein Schlüssel mit einer Länge von 1024 Bit erzeugt.
- `-f`: ermöglicht die Angabe eines Dateinamens für den Schlüssel.

Nachdem der Schlüssel erzeugt wurde, muss der öffentliche Teil auf das entfernte System übertragen werden. Der öffentliche Teil des Schlüssels kann mit dem folgenden Befehl angezeigt werden:

```
■ show ssh idkeys
```

Diese Befehl erzeugt eine Ausgabe ähnlich der folgenden:

```
Configured Client-Side SSH Host Keys For User 'root':
ssh-rsa AAAAB3NzaC1yc2EAAAABEQAQAQEA2
8BtNFFInAi8I5B1a0wq5g2YfwIX2O/vMX+9SLZ
AJVAhFnhdOG4wjTpLVuaQRNlITpBESPaWPLqoA
...
wd0T0nkuNQ== root@sshctest
```

Bitte beachten Sie, dass es sich um einen einzelnen Schlüssel handelt, auch wenn die Ausgabe in mehrere Zeilen aufgeteilt wird, der aus drei Teilen besteht:

- Der erste Teil zeigt den Typ des Schlüssels (ssh-rsa oder ssh-dss).
- Der zweite Teil ist die binäre Ausgabe des Schlüssels selbst, kodiert als Base64.
- Der dritte Teil enthält den Hostnamen, der mehr als Kommentar gedacht ist.

Die Datei kann mit einer Funktion von WEBconfig komfortabel bearbeitet werden (WEBconfig ► Extras ► Liste erlaubter öffentlicher SSH-Schlüssel bearbeiten). Kopieren Sie den ersten und zweiten Teil und ersetzen Sie den dritten Teil mit einer Liste von Anwendern, um die Nutzung dieses Schlüssels auf einen Teil der LCOS-Administratoren einzugrenzen.

A.5.6 Bearbeitung der Dateien

Während des Betriebs nutzt der SSH-Client verschiedene Dateien, die ggf. manuell bearbeitet werden müssen.

Die Liste der bekannten SSH-Server

Der SSH-Client nutzt die Liste der bekannten SSH-Server zum Speichern der entsprechenden Schlüssel. Diese Datei wird jedesmal verändert, wenn erstmalig eine Verbindung zu einem SSH-Server aufgebaut wird und der Administrator den angezeigten Schlüssel des entfernten Systems akzeptiert.

Jeder Schlüssel ist in dieser Datei in einer Zeile gespeichert und enthält drei Felder:

- Der Name oder die IP-Adresse des entfernten Systems, so wie es beim Aufbau der Verbindung im SSH-Befehl eingegeben wird.
- Der Typ des Schlüssels, also ssh-rsa oder ssh-dss.
- Die binäre Ausgabe des Schlüssels selbst, kodiert als Base64.



Wenn ein Administrator den öffentlichen Schlüssel eines SSH-Servers akzeptiert hat, gilt dieser Eintrag für alle LCOS-Administratoren, es findet keine benutzerbezogene Unterscheidung statt.

Die Dateien `ssh_id_rsa` und `ssh_id_dsa`

Diese Dateien enthalten die Schlüssel, die mit dem Befehl `sshkeygen` erzeugt wurden, also die Schlüssel zur Authentifizierung der entfernten SSH-Server im PEM-Format. Die Schlüssel für alle LCOS-Administratoren sind in einer zentralen Datei gespeichert und nur für den root-Administrator über secure copy zugänglich, das Hoch- bzw. Herunterladen über WEBconfig ist jedoch nicht möglich.

Die ID-Dateien entsprechen dem folgenden Aufbau, der die Nutzung eines Schlüssels für einen bestimmten LCOS-Administrator definiert:

```
*** User xyz
Schlüssel
*** End
```

A.5.7 Prioritäten für die SSH-Authentifizierung

Die Reihenfolge der SSH-Authentifizierung folgen einer festen Prioritätenfolge:

- Als erste Methode wird immer die Authentifizierung über öffentliche Schlüssel versucht, es sei denn, das entfernte System unterstützt diese Methode nicht oder der aktuelle LCOS-Administrator besitzt keine öffentlichen Schlüssel.
- Als zweite Methode wird die interaktive Authentifizierung über die Tastatur verwendet, wenn die Authentifizierung über öffentliche Schlüssel prinzipiell nicht verwendet werden kann oder wenn das entfernte System alle öffentlichen Schlüssel des aktuellen LCOS-Administrators abgelehnt hat. Die interaktive Authentifizierung kann

je nach Anwendung aus dem Austausch mehrerer Nachrichten zwischen SSH-Client und SSH-Server bestehen, im einfachsten Fall reicht ggf. nur ein Eingabe des Passworts.

A.5.8 Berechtigung zur Nutzung des SSH-Clients

Das Recht zur Nutzung des SSH-Clients kann für jeden einzelnen Administrator der LANCOM-Geräte separat eingeräumt werden.

Die Rechte für die Administratoren finden Sie in folgendem Menü:

- LANconfig: Management ▶ Admin ▶ Weitere Administratoren
- WEBconfig: LCOS-Menübaum ▶ Setup ▶ Config ▶ Admins



A.6 Alternative Boot-Config

A.6.1 Einleitung

Das Verhalten der LANCOM-Geräte im Betrieb wird durch die Konfiguration bestimmt. Diese benutzerdefinierte Konfiguration wird in einem speziellen Bereich des Flash-Speichers abgelegt, der auch bei einem Neustart des Gerätes erhalten bleibt (Konfigurationsspeicher). Im Auslieferungszustand ist der Konfigurationsspeicher leer, da das Gerät noch nicht über eine benutzerdefinierte Konfiguration verfügt. Im späteren Betrieb kann der Konfigurationsspeicher bei Bedarf durch einen Konfigurations-Reset wieder gelöscht werden. Wird ein Gerät mit leerem Konfigurationsspeicher gestartet oder gebootet, werden die Werte aus einer Boot-Konfiguration verwendet, welche die Standardwerte für das jeweilige Modell enthält.

Erst bei der Änderung von mindestens einem Konfigurationsparameter wird der Konfigurationsspeicher beschrieben. Dabei wird die komplette Konfiguration im Konfigurationsspeicher abgelegt. Auch wenn z.B. nur der Gerätename geändert wird, werden alle für das jeweilige Modell verfügbaren Parameter mit aktuellen Werten in der benutzerdefinierten Konfiguration gespeichert. Die Werte für die Parameter, die nicht geändert wurden, werden dabei aus einer Boot-Konfiguration übernommen.

LANCOM-Geräte können drei verschiedene Boot-Konfigurationen nutzen:

- LANCOM-Werkseinstellungen: Diese enthält die Standardwerte für das jeweilige Modell im Auslieferungszustand, also den LANCOM-Standard. Die Standard-Boot-Konfiguration ist in der jeweiligen Firmware des Gerätes enthalten.
- Kundenspezifische Standardeinstellungen: Diese enthält die kundenspezifischen Standardwerte für das jeweilige Modell für den Fall, dass der Konfigurationsspeicher leer ist, der LANCOM-Standard aber nicht verwendet werden soll. Mit dieser Funktion werden LANCOM-Geräte persistent (über beliebig viele Boot-/Reset-Vorgänge hinweg) mit kundenspezifischen Vorgabewerten für den Neustart versehen. Die kundenspezifischen Standardeinstellungen werden bei einem Konfigurations-Reset **nicht** gelöscht. Die kundenspezifischen Standardeinstellungen werden auf dem ersten Boot-Speicherplatz abgelegt.
- Rollout-Konfiguration: Diese Konfiguration wird in größeren Roll-Out-Szenarien verwendet, wenn für zahlreiche Geräte eine vom LANCOM-Standard abweichende Boot-Konfiguration verwendet werden soll. Die Rollout-Konfiguration muss durch eine entsprechende Bedienung des Reset-Tasters aktiviert werden. Die spezielle Rollout-Konfiguration wird auf dem zweiten Boot-Speicherplatz abgelegt.

A.6.2 Verwenden der Boot-Konfigurationen

Bei einem normalen Start nutzen die LANCOM-Geräte die möglichen Konfigurationen in einer definierten Reihenfolge:

- Benutzerdefinierte Konfiguration (im Konfigurationsspeicher)
- Kundenspezifische Standardeinstellungen (auf dem ersten Boot-Speicherplatz)
- LANCOM-Werkseinstellungen (in der Firmware des Gerätes)

Die kundenspezifischen Standardeinstellungen werden also automatisch und vorrangig vor den LANCOM-Werkseinstellungen verwendet, wenn der Konfigurationsspeicher leer ist.

Die Verwendung der Rollout-Konfiguration wird über den Reset-Taster ausgelöst. Der Reset-Taster hat verschiedene Funktionen, die durch unterschiedlich lange Betätigungszeiten des Tasters ausgelöst werden:

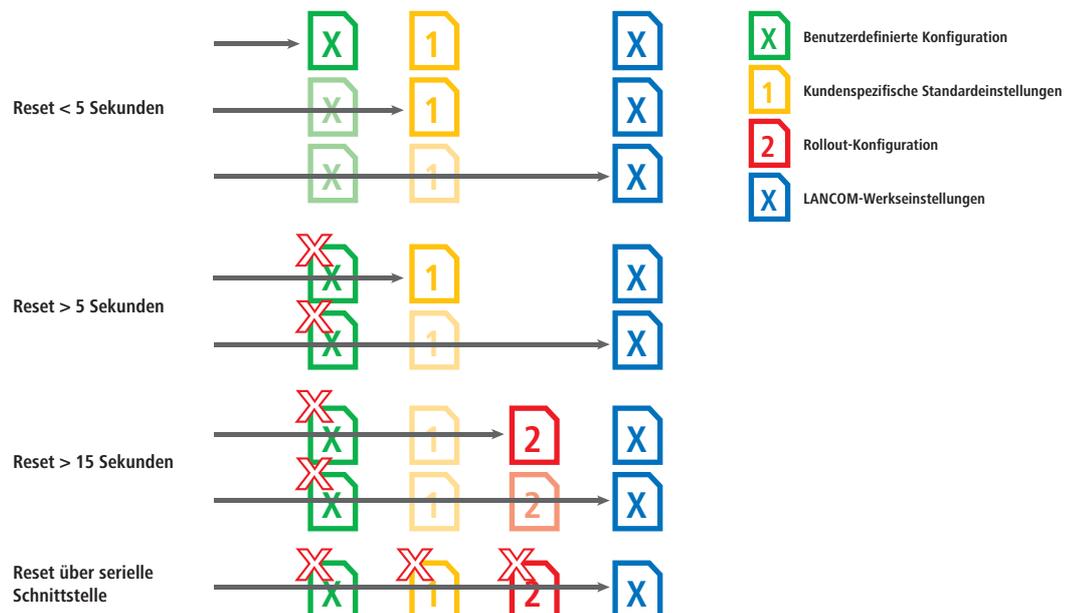
- weniger als 5 Sekunden: Booten (Neustart), dabei wird die benutzerdefinierte Konfiguration aus dem Konfigurationsspeicher geladen. Wenn die benutzerdefinierte Konfiguration leer ist, werden die kundenspezifischen Standardeinstellungen (erster Speicherplatz) geladen. Das Laden der kundenspezifischen Standardeinstellungen wird angezeigt, indem alle LEDs des Geräts einmal kurzzeitig rot aufleuchten. Wenn auch der erste Speicherplatz leer ist, werden die LANCOM Werkseinstellungen geladen.
- mehr als 5 Sekunden bis zum **ersten** Aufleuchten aller LEDs am Gerät: Konfigurations-Reset (Löschen des Konfigurationsspeichers) und anschließender Neustart. Damit werden die kundenspezifischen Standardeinstellungen (erster Speicherplatz) geladen. Das Laden der kundenspezifischen Standardeinstellungen wird angezeigt, indem alle LEDs des Geräts einmal kurzzeitig rot aufleuchten. Wenn der erste Speicherplatz leer ist, werden die LANCOM Werkseinstellungen geladen.
- mehr als 15 Sekunden bis zum **zweiten** Aufleuchten aller LEDs am Gerät: Aktivieren der Rollout-Konfiguration und Löschen der benutzerdefinierten Konfiguration. Nach dem Neustart wird die Rollout-Konfiguration (zweiter Speicherplatz) geladen. Das Laden der Rollout-Konfiguration wird angezeigt, indem alle LEDs des Geräts zweimal kurzzeitig rot aufleuchten. Wenn der zweite Speicherplatz leer ist, werden die LANCOM Werkseinstellungen geladen.

Die Rollout-Konfiguration wird jeweils nur einmalig direkt nach dem Neustart verwendet, wenn der Reset-Taster für mehr als 15 Sekunden gedrückt wurde. Nach dem nächsten Neustart gilt automatisch wieder die normale Boot-Reihenfolge (benutzerdefinierte Konfiguration, kundenspezifische Standardeinstellungen, LANCOM Werkseinstellungen).

 Wenn der Reset-Button in der Konfiguration deaktiviert ist (Einstellung 'Ignorieren' oder 'Nur-Booten') wird das Laden der Rollout-Konfiguration unmöglich gemacht.

Die folgende Grafik zeigt, welche Konfiguration bei unterschiedlichen Reset-Vorgängen je nach Zustand des Gerätes geladen wird. Beispiele:

- Bei Drücken des Reset-Buttons für weniger als 5 Sekunden wird die benutzerdefinierte Konfiguration geladen, wenn die nicht vorhanden ist die kundenspezifischen Standardeinstellungen, wenn die auch nicht vorhanden sind die LANCOM-Werkseinstellungen.
- Bei Drücken des Reset-Buttons für mehr als 15 Sekunden wird immer die benutzerdefinierte Konfiguration, dann die Rollout-Konfiguration geladen, wenn die nicht vorhanden ist die LANCOM-Werkseinstellungen.



A.6.3 Wiederherstellen der LANCOM Werkseinstellungen über seriellen Zugang

Wenn beide Speicherplätze mit kundenspezifischen Standardeinstellungen **und** Rollout-Konfiguration belegt sind, kann das Gerät nicht mehr über den Reset-Taster auf die LANCOM Werkseinstellungen zurückgesetzt werden. Wenn ein Zugriff auf die Konfiguration nicht mehr möglich ist (z.B. weil das Kennwort nicht mehr vorliegt), können die LANCOM Werkseinstellungen nur über den seriellen Zugang wieder hergestellt werden.

Über die serielle Schnittstelle kann eine Firmware in das Gerät geladen werden. Wenn Sie dabei statt des Konfigurations-Passwortes die Seriennummer verwenden, wird die Konfiguration des Gerätes wie bei einem Reset vollständig auf den Auslieferungszustand zurückgesetzt. Auf diese Weise können Sie sich Zugang zu einem Gerät verschaffen, wenn die LANCOM Werkseinstellungen nicht auf einem anderen Weg wieder hergestellt werden können.

- ① Schließen Sie das Gerät über das serielle Konfigurationskabel an einen Rechner an.
- ② Starten Sie auf diesem Rechner ein Terminal-Programm, z. B. Hyperterminal.
- ③ Starten Sie eine Verbindung mit den Einstellungen 115200bps, 8n1, Hardware-Handshake (RTS/CTS).
- ④ Drücken Sie im Begrüßungsbildschirm des Terminal-Programms die Return-Taste, bis die Aufforderung zur Eingabe des Passwortes erscheint.
- ⑤ Geben Sie als Passwort die Seriennummer ein, die unter der Firmware-Version angezeigt wird und drücken Sie erneut Return.

```

Outband-115200 Bit/s OK
#
| LANCOM L-54ag Wireless
| Ver. 7.26.0002 / 19.09.2007
| SN. 013020600159
| Copyright (c) LANCOM Systems
|
Connection No.: 001 (Outband-115200 Bps)
Password:
System is going down ...
@W@
| FLASHROM-Upload
| LANCOM L-54ag Wireless
| Copyright (C) LANCOM Systems
| Ver. 2.06.0001 / 22112006 / 16:30
|
Start Xmodem Upload
$_
    
```

- ⑥ Das Gerät erwartet nun den Firmware-Upload. Klicken Sie dazu z. B. unter Hyperterminal auf **Übertragung ► Datei senden** und wählen Sie X-Modem als Übertragungsprotokoll aus.

 Bei diesem Firmware-Upload wird die Konfiguration inklusive der Boot-Konfigurationen vollständig gelöscht und auf den Auslieferungszustand zurückgesetzt! Dabei werden alle im Gerät abgelegten Dateien gelöscht, z.B. auch vorhandene Rollout-Zertifikate. Nutzen sie diese Möglichkeit daher nur, wenn Sie keinen anderen Zugang zum Gerät herstellen können. Die Konfiguration und die Boot-Konfigurationen werden auch dann gelöscht, wenn der Firmware-Upload abgebrochen wird.

A.6.4 Speichern und Hochladen der Boot-Konfigurationen

Kundenspezifische Standardeinstellungen oder Rollout-Konfiguration werden in einem komprimierten Format gespeichert. Über die Kommandozeile kann die aktuelle Konfiguration eines Gerätes als kundenspezifische Standardeinstellung oder Rollout-Konfiguration gespeichert werden. Nutzen Sie dazu den folgenden Befehl:

■ `bootconfig --savecurrent [1,2, all] oder bootconfig -s [1,2, all]`

Mit der entsprechenden Ziffer wird entweder der erste Boot-Speicherplatz für die kundenspezifischen Standardeinstellungen oder der zweite Boot-Speicherplatz für die Rollout-Konfiguration ausgewählt. Mit der Angabe des Parameters "all" wird die aktuelle Konfiguration gleichzeitig in beide Speicherplätze geschrieben.

Auch über WEBconfig können die kundenspezifischen Standardeinstellungen oder die Rollout-Konfiguration in das Gerät geladen werden:

■ WEBconfig: LCOS-Menübaum ► Dateimanagement ► Konfiguration hochladen

Konfiguration hochladen

Geben Sie den Pfad und Dateinamen der Konfigurations-Datei ein.

Speichere Konfiguration als erste alternative Bootkonfiguration
 Speichere Konfiguration als zweite alternative Bootkonfiguration
 Dateiname:

Wählen Sie die zu verwendene Konfigurationsdatei aus und aktivieren Sie den Verwendungszweck als kundenspezifische Standardeinstellungen und/oder Rollout-Konfiguration.



Wenn beide Speicherplätze mit kundenspezifischen Standardeinstellungen **und** Rollout-Konfiguration belegt sind, kann das Gerät nicht mehr über den Reset-Taster auf die LANCOM Werkseinstellungen zurückgesetzt werden. Verwenden Sie in diesem Fall die Funktion 'Wiederherstellen der LANCOM Werkseinstellungen über seriellen Zugang' →Seite 12.

A.6.5 Löschen der Boot-Konfigurationen

Die alternative und die spezielle Boot-Konfiguration können nicht über die normalen Datei-Funktionen gelöscht werden. Nutzen Sie dazu den folgenden Befehl:

■ `bootconfig --remove [1,2, all] oder bootconfig -r [1,2, all]`

Mit der entsprechenden Ziffer wird zu löschende Boot-Speicherplatz ausgewählt. Mit der Angabe des Parameters "all" werden gleichzeitig beide Speicherplätze gelöscht.

A.6.6 Verwendung von Zertifikaten

Für die Nutzung durch VPN und SSL/TLS nach einem Konfigurations-Reset kann ein Standardzertifikat als PKCS#12-Container im Gerät gespeichert werden. Dieses Standardzertifikat wird nur von den kundenspezifischen Standardeinstellungen und der Rollout-Konfiguration verwendet:

- Wenn die kundenspezifischen Standardeinstellungen geladen werden, wird das Standardzertifikat in den normalen Zertifikatsspeicher für VPN und SSL/TLS kopiert, somit steht es auch nach einem Reboot zur Verfügung.
- Wenn die Rollout-Konfiguration geladen wird, wird das Standardzertifikat für VPN verwendet, aber nicht kopiert, d.h. nach einem Neustart (auch ohne Konfigurations-Reset) kann das Gerät darauf nicht mehr zugreifen.

Das Standardzertifikat können Sie über WEBconfig in das Gerät hochladen.

- WEBconfig: LCOS-Menübaum ▶ Dateimanagement ▶ Zertifikat oder Datei hochladen

Zertifikat oder Datei hochladen

Wählen Sie aus, welche Datei Sie hochladen wollen sowie deren Namen, dann klicken Sie auf 'Upload starten'. Bei PKCS12-Dateien kann eine Passphrase erforderlich sein.

Dateityp:
 Dateiname:
 Passphrase (falls benötigt):

Achtung: Beim Upload einer Datei (ggfs. mit falscher Passphrase) wird diese nicht auf inhaltliche Korrektheit überprüft. Diese Überprüfung findet später in den jeweiligen Modulen statt, die die Dateien verwenden. Beim Upload von Zertifikaten können Sie unmittelbar nach dem Upload entsprechende Fehlermeldungen im VPN-Status-Trace sehen.

Wählen Sie das zu verwendene Zertifikat aus und starten Sie den Vorgang des Hochladens mit **Upload starten**.

A.7 Alternative DHCP- Server zur Weiterleitung

A.7.1 Einleitung

Der DHCP-Server erlaubt verschiedene Betriebsarten. Im Weiterleitungs-Modus agiert das Gerät im lokalen Netz als DHCP-Relay und leitet Anfragen an einen oder mehrere konfigurierte DHCP-Server weiter. Diese Einstellung erlaubt den Betrieb von zentralen DHCP-Servern in einem anderen Netz.

Alle DHCP-Nachrichten, welche die DHCP-Clients als Broadcast senden, werden an alle konfigurierten DHCP-Server weitergeleitet. Der Client wählt dann den ersten Server der antwortet und sendet alle weiteren Nachrichten als Unicast, die gezielt an den zuständigen Server weitergeleitet werden. Falls der gewählte Server nicht erreichbar ist, sendet der Client erneut Broadcast-Nachrichten und wählt einen anderen DHCP-Server.

A.7.2 Konfiguration

Die Konfiguration der DHCP-Server zur Weiterleitung finden Sie in folgendem Menü:

- LANconfig: TCP/IP ► DHCP ► DHCP-Netzwerke
- WEBconfig: LCOS-Menübaum ► Setup ► DHCP ► Netzliste

■ Adresse des 1. Servers

Hier wird die IP-Adresse des übergeordneten DHCP-Servers eingetragen, an den DHCP-Anfragen weitergeleitet werden, wenn für das Netzwerk die Betriebsart 'Anfragen Weiterleiten' gewählt wurde.

Mögliche Werte:

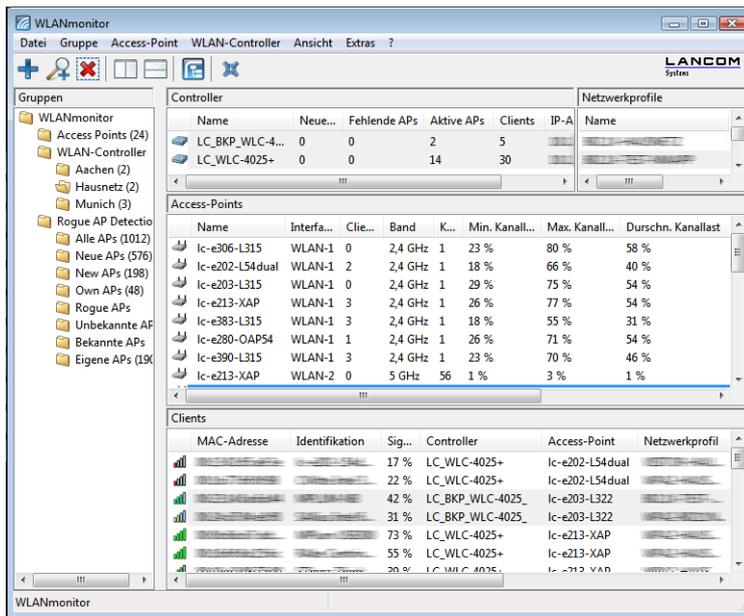
- IP-Adresse oder die Broadcast-Adresse des Netzes, in dem der Server steht. Die Broadcast-Adresse ist die höchste Adresse in einem IP-Netz. Alle Pakete an diese Adresse werden von allen Hosts empfangen.

Default:

- 0.0.0.0

A.8 Kanallastanzeige im WLC-Betrieb

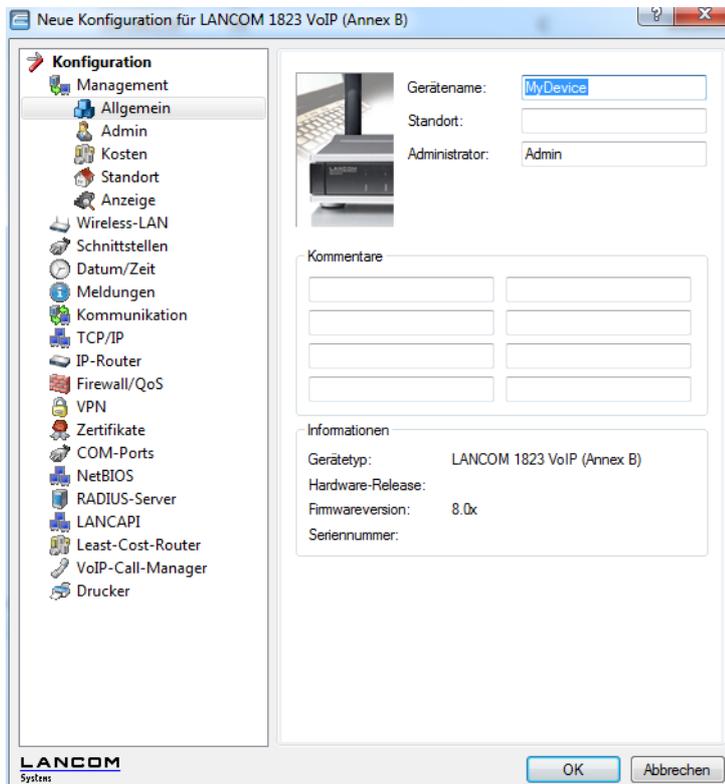
Für die von einem WLAN Controller verwalteten Access Points wird die Last auf den verwendeten Kanälen in drei Werten als minimale, maximale und durchschnittliche Kanallast angezeigt. Die angezeigten Werte werden in einem Messintervall von drei Minuten ermittelt. Die ersten Werte werden demnach auch erst nach drei Minuten angezeigt.



A.9 Änderungen in LANconfig

A.9.1 Konfigurationsbaum

Ab der Version 8.00 werden die beiden obersten Ebenen der Konfigurationsmenüs in LANconfig als "Konfigurationsbaum" permanent sichtbar in einem eigenen Bereich angezeigt. Diese neue Struktur erleichtert die Orientierung, erlaubt eine leichte Navigation und den schnellen Wechsel zwischen den Haupt-Konfigurationsbereichen.



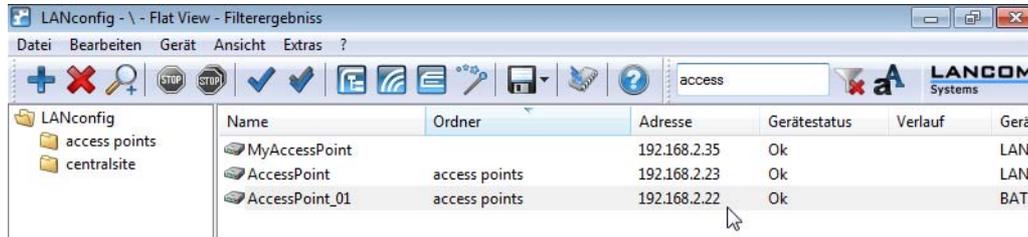
A.9.2 Dynamischer Filter

Mit dem dynamischen Filter in LANconfig können Sie sehr komfortabel die Anzeige auf die Geräte mit bestimmten Eigenschaften einschränken. Tragen Sie in das Filterfeld das gewünschte Filterkriterium ein. Als Filterkriterien können Sie alle angezeigten Eigenschaften verwenden, also z. B. Gerätenamen, Ordner, IP-Adresse, Gerätestatus, Gerätetyp, Seriennummer etc.

LANconfig reduziert die gewählte Ordneransicht auf die Einträge, welche das Filterkriterium an beliebiger Stelle (auch innerhalb von Begriffen) enthalten. Mit dem Filtersymbol neben dem Filterfeld können Sie den Filter zurück-

□ 802.1x-Accounting im WLAN-Controller für logische WLANs aktivieren

setzen. Mit dem Symbol für die Groß-Klein-Schreibung können Sie die exakte Übereinstimmung der Schreibweise des Filterkriteriums mit den aufgefundenen Stellen in den Eigenschaften erzwingen (Default: aus), andernfalls bleibt die Groß-Klein-Schreibung unbeachtet. Die Ordneransicht wird bei Verwendung des dynamischen Filters sofort bei der Eingabe angepasst. Der dynamische Filter bezieht sich immer auf den aktuell ausgewählten Ordner. Er kann auch mit der Ansicht "Flat View Modus" kombiniert werden, sodass zum ausgewählten Order auch alle Inhalte der untergeordneten Ordner hinzugezogen werden.



A.9.3 Zugriff auf Web-Server-Dienste einschränken

Der Zugriff auf ein Gerät über HTTP für die Konfiguration kann generell erlaubt, nicht erlaubt oder auf nur lesen eingeschränkt werden. Unabhängig davon kann der Zugriff auf die Web-Server-Dienste separat geregelt werden, z. B. um die Kommunikation von CAPWAP über HTTP zu ermöglichen, auch wenn der HTTP-Zugang generell nicht erlaubt ist.

- LANconfig: Management ► Admin ► Zugriff auf Web-Server-Dienste

■ HTTP-Port

Für jeden Zugriffsweg (je nach Gerät LAN, WAN, WLAN) stellen Sie hier das Zugriffsrecht von Web-Server-Diensten des Gerätes auf den HTTP-Server-Port ein.

Mögliche Werte:

- Automatisch: Der HTTP-Server-Port ist offen, solange ein Dienst angemeldet ist (z.B. CAPWAP). Ist kein Dienst mehr angemeldet, wird der Server-Port geschlossen.
- Aktiviert: Der HTTP-Server-Port ist immer offen, auch wenn der Zugriff auf die Konfiguration über HTTP nicht erlaubt ist. Hiermit kann der direkte Konfigurationszugriff unterbunden werden, jedoch die automatische Konfiguration von APs über einen WLAN-Controller weiterhin erlaubt werden.
- Deaktiviert: Der HTTP-Server-Port ist geschlossen, so dass kein Dienst den Web-Server benutzen kann. Wenn der Zugriff auf die Konfiguration über HTTP erlaubt ist, wird mit der entsprechenden Meldung quittiert, dass der Web-Server nicht erreichbar ist.

Default:

- Die Standardeinstellung für alle Zugangswege ist "Automatisch".



A.10 802.1x-Accounting im WLAN-Controller für logische WLANs aktivieren

Die Konfiguration der logischen WLAN-Netzwerke finden Sie in folgendem Menü:

- LANconfig: WLAN-Controller ► Profile ► Logische WLAN-Netzwerke (SSIDs)
- WEBconfig: LCOS-Menübaum ► Setup ► WLAN-Management ► AP-Konfiguration ► Netzwerkprofile

 Ab LCOS 8.0 ist die Aktivierung des RADIUS-Accounting mit 802.1x individuell pro SSID möglich. In vorherigen Firmware-Versionen konnte das RADIUS-Accounting mit 802.1x nur global für alle SSIDs eingestellt werden.

Logisches WLAN-Netzwerk aktiviert OK
 Name: LOG-1 Abbrechen
 Vererbung
 Erbt Werte von Eintrag: Vererbte Werte
 Netzwerk-Name (SSID): WLAN-1
 VLAN-ID: 0
 Verschlüsselung: 802.11i (WPA)-PSK
 Schlüssel 1/Passphrase: Anzeigen
Passwort erzeugen
 Zulässige Freq.-Bänder: 2,4/5 GHz (802.11a)
 Autarker Weiterbetrieb: 0 Minuten
 MAC-Prüfung aktiviert
 SSID-Broadcast unterdrücken
 RADIUS-Accounting aktiviert

■ RADIUS-Accounting aktiviert

Stellen Sie hier ein, ob das RADIUS-Accounting in diesem logischen WLAN-Netzwerk aktiviert werden soll.

Mögliche Werte:

ja, nein

Default:

nein

 Die Access Points, die der WLAN-Controller mit diesem logischen WLAN-Netzwerk konfiguriert, müssen eine LCOS-Version 8.00 oder höher verwenden.

A.11 LANCOM Content Filter

A.11.1 Einleitung

Mit dem LANCOM Content Filter können Sie bestimmte Inhalte in Ihrem Netzwerk filtern und dadurch den Zugriff auf z.B. illegale, gefährliche oder anstößige Internetseiten verhindern. Weiterhin können Sie das private Surfen auf bestimmten Seiten während der Arbeitszeit unterbinden. Das steigert nicht nur die Produktivität der Mitarbeiter und die Sicherheit des Netzwerks, sondern sorgt auch dafür, dass die volle Bandbreite ausschließlich für Geschäftsprozesse zur Verfügung steht.

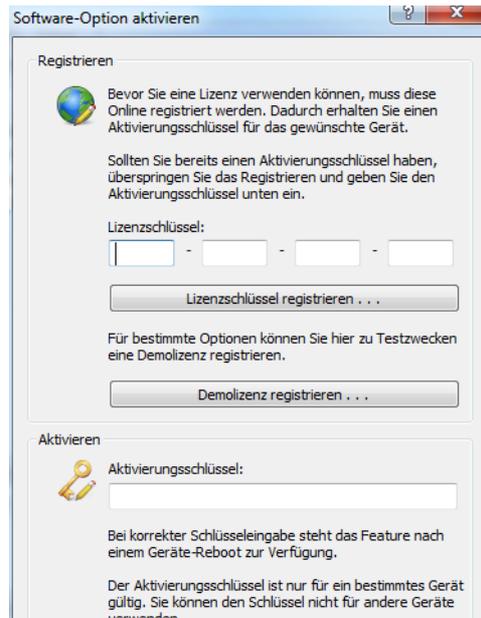
Der LANCOM Content Filter ist ein intelligenter Content-Filter und arbeitet dynamisch. Er kontaktiert einen Bewertungsserver, der gemäß den von Ihnen ausgewählten Kategorien die Bewertung der Internetseiten zuverlässig und korrekt vornimmt.

Die Funktion des LANCOM Content Filters basiert auf der Überprüfung der IP-Adressen, die anhand der eingegebenen URL ermittelt werden. Innerhalb einer Domain wird bei vielen Seiten außerdem nach dem Pfad unterschieden, so dass bestimmte Bereiche einer URL unterschiedlich bewertet werden können.

 Die Anwender können die Prüfung der aufgerufenen Webseiten durch den LANCOM Content Filter nicht umgehen, indem sie die IP-Adresse zu einer Webseite ermitteln und diese in den Browser eingeben. Der LANCOM Content Filter prüft nur unverschlüsselte Webseiten über HTTP.

Die von Ihnen erworbene Lizenz für den LANCOM Content Filter gilt für eine bestimmte Anzahl Benutzer und einen bestimmten Zeitraum (jeweils für ein Jahr oder drei Jahre). Sie werden rechtzeitig über den Ablauf Ihrer Lizenz informiert. Die Anzahl der aktuellen Benutzer wird im Gerät geprüft, dabei werden die Benutzer über die IP-Adresse identifiziert. Sie können das Verhalten bei Lizenzüberschreitung einstellen: Entweder wird der Zugriff verboten oder es wird eine ungeprüfte Verbindung hergestellt.

 Sie können den LANCOM Content Filter auf jedem Router testen, der diese Funktion unterstützt. Hierfür müssen Sie für jedes Gerät einmalig eine zeitlich befristete 30-Tage Demo-Lizenz aktivieren. Demo-Lizenzen werden direkt aus LANconfig heraus erstellt. Klicken Sie mit der rechten Maustaste auf das Gerät, wählen Sie im Kontextmenü den Eintrag **Software-Option aktivieren** und im folgenden Dialog die Schaltfläche **Demo-Lizenz registrieren**. Sie werden automatisch mit der Webseite des LANCOM-Registrierungsservers verbunden, auf der Sie die gewünschte Demo-Lizenz auswählen und für das Gerät registrieren können.



Über die Kategorieprofile speichern Sie alle Einstellungen bezüglich der Kategorien. Dabei wählen Sie aus vordefinierte Haupt- und Unterkategorien in Ihrem LANCOM Content Filter: 58 Kategorien sind zu 14 Gruppen thematisch zusammengefasst, z.B. "Pornographie/Nacktheit", "Einkaufen" oder "Kriminelle Aktivitäten". Für jede dieser Gruppen lassen sich die enthaltenen Kategorien aktivieren oder deaktivieren. Die Unterkategorien für "Pornographie/Nacktheit" sind z.B. "Pornographie/Erotik/Sex", "Bademoden/Dessous".

Zusätzlich kann der Administrator bei der Konfiguration für jede dieser Kategorien die Option des Override aktivieren. Bei aktivem Override kann der Benutzer den Zugriff auf eine verbotene Seite durch einen Klick auf eine entsprechende Schaltfläche für eine bestimmte Zeitspanne freischalten – allerdings erhält der Administrator in diesem Fall eine Benachrichtigung per E-Mail, Syslog und/oder SNMP-Trap.

Mit dem von Ihnen erstellten Kategorieprofil, der Whitelist und der Blacklist können Sie ein Content-Filter-Profil anlegen, welches über die Firewall gezielt Benutzern zugeordnet werden kann. Beispielsweise können Sie das Profil "Mitarbeiter_Abteilung_A" anlegen, welches dann allen Computern der entsprechenden Abteilung zugeordnet wird.

Bei der Installation des LANCOM Content Filters werden sinnvolle Standardeinstellungen automatisch eingerichtet, die für den ersten Start nur aktiviert werden müssen. In weiteren Schritten können Sie das Verhalten des LANCOM Content Filters weiter an Ihren speziellen Anwendungsfall anpassen.

A.11.2 Voraussetzungen für die Benutzung des LANCOM Content Filters

Folgende Voraussetzungen müssen erfüllt sein, damit Sie den LANCOM Content Filter benutzen können:

- 1 Die LANCOM Content Filter Option ist aktiviert.
- 2 Die Firewall muss aktiviert sein und mit einer entsprechenden Firewall-Regel das Content-Filter-Profil auswählen.
- 3 Das Content-Filter-Profil muss für jeden Zeitraum des Tages ein Kategorieprofil und nach Wunsch eine White- und/oder Blacklist festlegen. Um die verschiedenen Zeiträume abzudecken, kann ein Content-Filter-Profil aus mehreren Einträgen bestehen.

Wird ein bestimmter Zeitraum des Tages nicht über einen Eintrag abgedeckt, so ist in diesem Zeitraum ein unprüfter Zugriff auf die Webseiten möglich.

 Wenn das Content-Filter-Profil nachträglich umbenannt wird, muss die Firewallregel ebenfalls angepasst werden.

A.11.3 Quickstart

Nach der Installation des Content Filters sind alle Einstellungen für eine schnelle Inbetriebnahme vorbereitet.

 Der Betrieb des Content Filters kann durch die Datenschutzrichtlinien in Ihrem Land oder Betriebsvereinbarungen in Ihrem Unternehmen eingeschränkt sein. Bitte prüfen Sie vor Inbetriebnahme die geltenden Regelungen.

Aktivieren Sie den Content Filter in den folgenden Schritten:

- 1 Rufen Sie für das entsprechende Gerät den Setup-Assistenten auf.
- 2 Wählen Sie den Setup-Assistenten zur Konfiguration des Content Filters.



- 3 Wählen Sie eines der vordefinierten Sicherheitsprofile (Basis-Profil, Firmen-Profil, Jugendschutz-Profil):
 - Basis-Profil: Diese Profil sperrt im Wesentlichen den Zugang zu den Kategorien Pornografie, illegale, gewalttätige oder diskriminierende Inhalte, Drogen, SPAM und Phishing
 - Firmen-Profil: Über die Einstellungen des Basis-Profiles hinaus sperrt dieses Profil zusätzlich die Kategorien Einkaufen, Jobsuche, Spiele, Musik, Radio und bestimmte Kommunikationsdienste wie Chat.
 - Jugendschutz-Profil: Über die Einstellungen des Basis-Profiles hinaus gelten in diesem Profil verschärfte Sperren für Nacktheit oder Waffen/Militär.

Falls die Firewall ausgeschaltet ist, schaltet der Assistent die Firewall ein. Dann prüft der Assistent, ob die Firewall-Regel für den Content-Filter richtig eingestellt ist und korrigiert diese, sofern nötig. Mit diesen Schritten haben Sie den Content-Filter aktiviert, es gelten immer die Standardeinstellungen für alle Stationen im Netzwerk mit dem ausgewählten Content-Filter-Profil und den noch leeren Black- und Whitelists. Passen Sie diese Einstellungen ggf. an Ihre Bedürfnisse an.

 Detaillierte Informationen über die manuelle Konfiguration des Content-Filters finden Sie im Content-Filter-Handbuch als PDF als Download von www.lancom.de.

A.11.4 Die Standardeinstellungen im LANCOM Content Filter

In der Standardeinstellung sind im LANCOM Content Filter folgende Elemente angelegt:

- Eine Firewall-Regel
- Drei Firewall-Aktions-Objekte
- Drei Content-Filter-Profile
- Zwei Zeitrahmen
- Eine Blacklist
- Eine Whitelist
- Drei Kategorieprofile

Firewall-Regel

Die voreingestellte Firewall-Regel hat den Namen CONTENT-FILTER und verwendet das Aktionsobjekt CONTENT-FILTER-BASIC.

Firewall-Aktions-Objekte

Es existieren drei Firewall-Aktions-Objekte: CONTENT-FILTER-BASIC, CONTENT-FILTER-WORK und CONTENT-FILTER-PARENTAL-CONTROL. Diese Aktionsobjekte greifen auf die entsprechenden Content-Filter-Profile zurück.

Content-Filter-Profile

Es existieren drei Content-Filter-Profile. Alle Content-Filter-Profile nutzen den zeitrahmen ALWAYS, die Blacklist MY-BLACKLIST und die Whitelist MY-WHITELIST. Jedes Content-Filter-Profil nutzt eines der vordefinierten Kategorie-Profile:

- CF-BASIC-PROFILE: Dieses Content-Filter Profil verfügt nur über geringe Einschränkungen und nutzt das Kategorie-Profil BASIC-CATEGORIES.
- CF-PARENTAL-CONTROL-PROFILE: Mit diesem Content-Filter-Profil können Minderjährige (Auszubildende) vor ungeeigneten Internetinhalten geschützt werden, es nutzt das Kategorie-Profil PARENTAL-CONTROL.

□ LANCOM Content Filter

- **CF-WORK-PROFILE:** Dieses Content-Filter-Profil ist für den Einsatz in Unternehmen gedacht und sperrt z.B. die Kategorien Jobsuche oder Chat, es nutzt das Kategorie-Profil WORK-CATEGORIES.

Name	Zeitraumen	Blacklisted	Whitelisted	Kategorie-Profil
CF-BASIC-PROFILE	ALWAYS	MY-BLACKLIST	MY-WHITELIST	BASIC-CATEGORIES
CF-PARENTAL-CONTROL-PROFILE	ALWAYS	MY-BLACKLIST	MY-WHITELIST	PARENTAL-CONTROL
CF-WORK-PROFILE	ALWAYS	MY-BLACKLIST	MY-WHITELIST	WORK-CATEGORIES

Zeitraumen

Es gibt zwei definierte Zeitraumen:

- ALWAYS: 00.00-23.59 Uhr
- NEVER: 00.00-0.00 Uhr

Blacklist

Die voreingestellte Blacklist hat den Namen "MY-BLACKLIST" und ist leer. Tragen Sie hier optional die URLs ein, die für Ihre Anwendung verboten werden sollen.

Whitelist

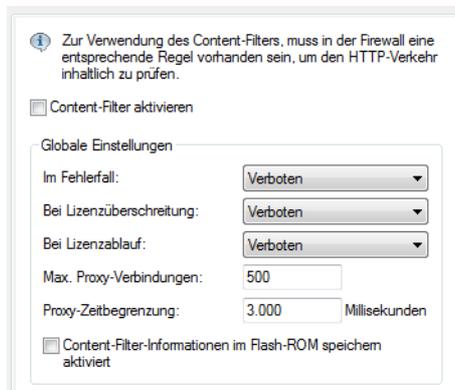
Die voreingestellte Whitelist hat den Namen "MY-WHITELIST" und ist leer. Tragen Sie hier optional die URLs ein, die für Ihre Anwendung erlaubt werden sollen.

Kategorieprofile

Es existieren drei Kategorieprofile: BASIC-CATEGORIES, WORK-CATEGORIES und PARENTAL-CONTROL. Das Kategorie-Profil enthält die Angaben darüber, welche Kategorien erlaubt und verboten sind und für welche ein sogenannter Override aktiviert ist.

A.11.5 Allgemeine Einstellungen

Die globalen Einstellungen des LANCOM Content Filters nehmen Sie hier vor:



LANconfig: Content-Filter ► Allgemein

WEBconfig: LCOS-Menübaum ► Setup ► UTM ► Content-Filter ► Globale-Einstellungen

■ **Content-Filter aktivieren**

Hier können Sie den LANCOM Content Filter aktivieren.

■ **Im Fehlerfall:**

Hier können Sie bestimmen, was bei einem Fehler passieren soll. Kann der Bewertungsserver beispielsweise nicht kontaktiert werden, kann der Benutzer in Folge dieser Einstellung entweder ungehindert surfen oder aber es wird der komplette Webzugriff verboten.

Mögliche Werte:

- verboten, erlaubt

Default:

- verboten

■ **Bei Lizenzüberschreitung:**

Hier können Sie bestimmen, was bei Überschreitung der lizenzierten Benutzeranzahl passieren soll. Die Benutzer werden über die IP-Adresse identifiziert. Das heißt, dass die IP-Adressen, die eine Verbindung durch den

LANCOM Content Filter aufbauen, gezählt werden. Baut z.B. bei einer 10er Option ein elfter Benutzer eine Verbindung auf, findet keine Prüfung mehr durch den LANCOM Content Filter statt. Der Benutzer, für den keine Lizenz mehr zur Verfügung steht, kann in Folge dieser Einstellung entweder ungehindert surfen oder aber es wird der komplette Webzugriff verboten.

Mögliche Werte:

verboten, erlaubt

Default:

verboten



Die Benutzer des Content-Filters werden automatisch aus der Benutzerliste entfernt, wenn von dieser IP-Adresse seit 24 Stunden keine Verbindung durch den Content-Filter mehr aufgebaut wurde.

■ Bei Lizenzablauf:

Die Lizenz zur Nutzung des LANCOM Content Filters gilt für einen bestimmten Zeitraum. Sie werden 30 Tage, eine Woche und einen Tag vor Ablauf der Lizenz an die auslaufende Lizenz erinnert (an die E-Mailadresse, die konfiguriert ist unter LANconfig: Meldungen ► Allgemein).

Hier können Sie bestimmen, was bei Ablauf der Lizenz passieren soll (blockieren oder ungeprüft durchlassen). Der Benutzer kann in Folge dieser Einstellung nach Ablauf der für ihn verwendeten Lizenz entweder ungehindert surfen oder aber es wird der komplette Webzugriff verboten.

Mögliche Werte:

verboten, erlaubt

Default:

verboten

■ Max. Proxy-Verbindungen

Stellen Sie hier die Anzahl der Proxy-Verbindungen ein, die maximal gleichzeitig aufgebaut werden dürfen. Die Last kann somit auf dem System eingeschränkt werden. Es wird eine Benachrichtigung ausgelöst, wenn diese Anzahl überschritten wird.

Mögliche Werte:

0 bis 999999 Verbindungen

Default:

geräteabhängig

■ Proxy-Zeitbegrenzung

Stellen Sie hier die Zeit in Millisekunden ein, die der Proxy maximal für die Bearbeitung benötigen darf. Wird diese Zeit überschritten, wird dies durch eine entsprechende Zeitüberschreitungs-Fehlerseite quittiert.

Mögliche Werte:

0 bis 999999 Millisekunden

Default:

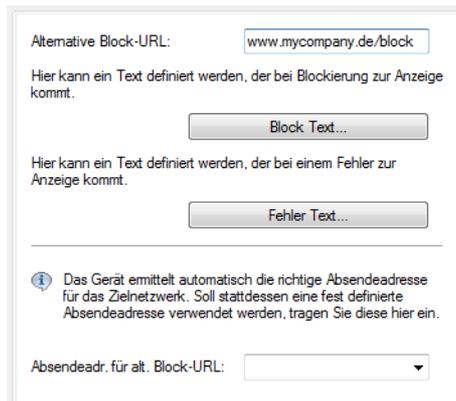
3000 Millisekunden

Besondere Werte:

Der Wert 0 steht für keine Zeitbegrenzung. Werte kleiner als 100 Millisekunden sind nicht sinnvoll.

A.11.6 Einstellungen für das Blockieren

Die Einstellungen für das Blockieren von Webseiten nehmen Sie hier vor:



LANconfig: Content-Filter ▶ Blockieren

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Globale-Einstellungen

■ **Alternative Block-URL:**

Hier können Sie eine alternative URL-Adresse eintragen. Im Falle des Blockierens wird dann statt der Standard-Webseite die hier eingetragene URL aufgerufen. In der externen HTML-Seite können Sie z.B. das Corporate Design Ihres Unternehmens abbilden oder weitere Funktionen wie JavaScript etc. nutzen. Außerdem können hier auch die gleichen HTML-Tags wie im Blocktext verwendet werden. Wenn Sie an dieser Stelle keinen Eintrag vornehmen, wird die im Gerät hinterlegte Standard-Webseite aufgerufen.

Mögliche Werte:

- gültige URL-Adresse

Default:

- leer

■ **Absendeadr. für alt. Block-URL:**

Hier können Sie optional eine Absende-Adresse konfigurieren, die statt der ansonsten automatisch für die Ziel-Adresse gewählten Absende-Adresse verwendet wird. Falls Sie z.B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absende-Adresse angeben.

Mögliche Werte:

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ (Achtung: wenn es eine Schnittstelle Namens "DMZ" gibt, dann wird deren Adresse genommen)
- LB0 ... LBF für die 16 Loopback-Adressen
- GUEST
- Beliebige IP-Adresse in der Form x.x.x.x

Default:

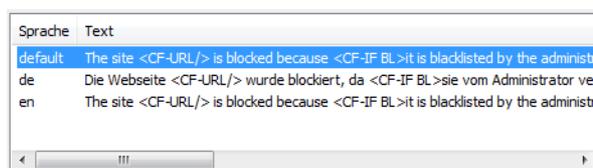
- leer



Die hier eingestellte Absende-Adresse wird für jede Gegenstelle unmaskiert verwendet.

Block-Text

Hier können Sie einen Text definieren, der bei Blockierung angezeigt wird. Für unterschiedliche Sprachen kann jeweils ein eigener Blocktext definiert werden. Die Auswahl des verwendeten Blocktextes wird anhand des übermittelten Spracheinstellung des Browsers (User Agents) vorgenommen.



■ Sprache

Damit der Anwender alle Meldungen in seiner voreingestellten Browser-Sprache erhält, kann hier der entsprechende Country-Code eingetragen werden. Wird der im Browser eingestellten Country-Code hier gefunden, kommt der dazu passende Text zur Anzeige.

Weitere Sprachen können nach Belieben hinzugefügt werden.

Der Country-Code sieht dafür z.B. folgendermaßen aus:

- de-DE: Deutschsprachig-Deutschland
- de-CH: Deutschsprachig-Schweiz
- de-AT: Deutschsprachig-Österreich
- en-GB: Englischsprachig-Großbritannien
- en-US: Englischsprachig-Vereinigte Staaten



Der Country-Code muss genau der Spracheinstellung des Browsers entsprechen, z.B. muss für Deutsch "de-DE" eingegeben werden (es reicht nicht "de"). Wird der im Browser eingestellte Country-Code in dieser Tabelle nicht gefunden oder der dafür hinterlegte Text gelöscht, so wird der bereits vordefinierten Standardtext (Default) verwendet. Den Default-Text können Sie bearbeiten.

Mögliche Werte:

- 10 alphanumerische Zeichen

Default:

- leer

■ Text

Geben Sie hier den Text ein, der als Blocktext für diese Sprache verwendet werden soll.

Mögliche Werte:

- 254 alphanumerische Zeichen

Default:

- leer

Besondere Werte:

Sie können für den Blocktext auch spezielle Tags verwenden, wenn Sie unterschiedliche Seiten anzeigen wollen, je nachdem aus welchem Grund (z.B. Verbotene Kategorie oder Eintrag in der Blacklist) die Seite verboten wurde.

Für die einzusetzenden Werte können Sie folgende Tags verwenden:

- <CF-URL/> für die verbotene URL
- <CF-CATEGORIES/> für die Liste der Kategorien aufgrund der die Webseite verboten wurde
- <CF-PROFILE/> für den Profilnamen
- <CF-OVERRIDEURL/> für die URL zum Freischalten des Overrides (diese kann in ein einfaches <a>-Tag oder einen Button eingebaut werden)
- <CF-LINK/> fügt einen Link zum Freischalten des Overrides ein
- <CF-BUTTON/> für einen Button zum Freischalten des Overrides

Zum Ein- und Ausblenden von Teilen des Html-Dokuments wird ein Tag mit Attributen verwendet: <CF-IF att1 att2> ... </CF-IF>.

Attribute sind:

- BLACKLIST: wenn die Seite verboten wurde, weil sie auf der Blacklist des Profils steht
- CATEGORY: wenn die Seite aufgrund einer ihrer Kategorien verboten wurde
- ERR: wenn ein Fehler aufgetreten ist.

Da es getrennte Texttabellen für die Blockseite und die Fehlerseite gibt, ist das Tag nur sinnvoll, wenn Sie eine alternative Block-URL konfiguriert haben.

- OVERRIDEOK: wenn dem Benutzer ein Override erlaubt wurde (in diesem Fall sollte die Seite eine entsprechende Schaltfläche anzeigen)

Werden in einem Tag mehrere Attribute angegeben, dann wird der Bereich eingeblendet, wenn mind. eine dieser Bedingungen erfüllt ist. Alle Tags und Attribute lassen sich mit den jeweils ersten zwei Buchstaben abkürzen (z.B. CF-CA oder CF-IF BL). Das ist notwendig, weil der Blocktext nur maximal 254 Zeichen lang sein darf.

- Beispiel:
`<CF-URL/>` wird wegen der Kategorien `<CF-CA/>` verboten.
Ihr Contentfilterprofil ist `<CF-PR/>`.
<CF-IF OVERRIDEOK>
<CF-BU/></CF-IF>



Die hier beschriebenen Tags können auch in externen HTML-Seiten (alternative Block-URL) verwendet werden.

Fehler-Text

Hier können Sie einen Text definieren, der bei einem Fehler zur Anzeige kommt.

Sprache	Text
default	<code><CF-URL/></code> is blocked, because the following error occurred: <CF-ERROR/>
de	<code><CF-URL/></code> wird blockiert, weil folgender Fehler aufgetreten ist: <CF-ERROR/>
en	<code><CF-URL/></code> is blocked, because the following error occurred: <CF-ERROR/>

■ Sprache

Damit der Anwender alle Meldungen in seiner voreingestellten Browser-Sprache erhält, kann hier der entsprechende Country-Code eingetragen werden. Wird der im Browser eingestellten Country-Code hier gefunden, kommt der dazu passende Text zur Anzeige.

Weitere Sprachen können nach Belieben hinzugefügt werden.

Der Country-Code sieht dafür z.B. folgendermaßen aus:

- de-DE: Deutschsprachig-Deutschland
- de-CH: Deutschsprachig-Schweiz
- de-AT: Deutschsprachig-Österreich
- en-GB: Englischsprachig-Großbritannien
- en-US: Englischsprachig-Vereinigte Staaten



Der Country-Code muss genau der Spracheinstellung des Browsers entsprechen, z.B. muss für Deutsch "de-DE" eingegeben werden (es reicht nicht "de"). Wird der im Browser eingestellte Country-Code in dieser Tabelle nicht gefunden oder der dafür hinterlegte Text gelöscht, so wird der bereits vordefinierte Standardtext (Default) verwendet. Den Default-Text können Sie bearbeiten.

Mögliche Werte:

- 10 alphanumerische Zeichen

Default:

- leer

■ Text

Geben Sie hier den Text ein, der als Fehlertext für diese Sprache verwendet werden soll.

Mögliche Werte:

- 254 alphanumerische Zeichen

Default:

- leer

Besondere Werte:

Sie können für den Fehlertext auch HTML-Tags verwenden.

Für die einzusetzenden Werte können Sie folgende Empty-Element-Tags verwenden:

- `<CF-URL/>` für die verbotene URL
- `<CF-PROFILE/>` für den Profilnamen
- `<CF-ERROR/>` für die Fehlermeldung
- Beispiel:
`<CF-URL/>` wird verboten, weil ein Fehler aufgetreten ist:
<CF-ERROR/>

A.11.7 Override-Einstellungen

Die Override-Funktion ermöglicht eine Webseite zu öffnen, obwohl sie zu einer verbotenen Kategorie gehört. Wenn die verbotene Seite geöffnet werden soll, muss der Benutzer dies mit einem Klick auf den Override-Button bestäti-

gen. Sie können die Konfiguration so einstellen, dass der Administrator bei Klick auf den Override-Button eine Benachrichtigung erhält (LANconfig: Content-Filter ► Optionen).



Durch den Klick auf den Override-Button schaltet der Benutzer, wenn der Override-Typ "Kategorie" aktiviert ist, **alle** Kategorien frei, zu denen die aufgerufene URL gehört. Auf der zunächst angezeigten Blockseite wird nur eine Kategorie angezeigt, aufgrund derer der Zugriff auf die URL gesperrt werden soll. Nach dem Klick auf den Override-Button werden alle freigeschalteten Kategorien angezeigt. Wenn der Override-Typ "Domain" aktiviert ist wird die Domain freigeschaltet.

Die Einstellungen für die Override-Funktion finden Sie hier:

LANconfig: Content-Filter ► Override

WEBconfig: LCOS-Menübaum ► Setup ► UTM ► Content-Filter ► Globale-Einstellungen

■ **Override aktiviert**

Hier können Sie die Override-Funktion aktivieren und weitere Einstellungen für diese Funktion vornehmen.

■ **Override-Dauer:**

Der Override kann hier zeitlich begrenzt werden. Nach Ablauf der Zeitspanne wird jedes Betreten der gleichen Domain und/oder Kategorie wieder verboten. Mit einem erneuten Klick auf den Override-Button kann die Seite wieder für die Override-Dauer betreten werden, der Administrator erhält je nach Einstellung eine erneute Benachrichtigung.

Mögliche Werte:

- 1-1440 (Minuten)

Default:

- 5 (Minuten)

■ **Override-Typ:**

Hier können Sie den Override-Typ einstellen, für den der Override gelten soll. Er kann für die Domain oder die Kategorie der zu blockierenden Seite oder für beides erlaubt werden.

Mögliche Werte:

- Kategorie: Während der Override-Dauer sind alle URLs erlaubt, die unter die angezeigten Kategorien fallen (zuzüglich derer, die auch ohne den Override schon erlaubt gewesen wären).
- Domain: Während der Override-Dauer sind alle URLs unter der besuchten Domain erlaubt, egal zu welchen Kategorien sie gehören.
- Kategorie und Domain: Während der Override-Dauer sind alle URLs erlaubt, die sowohl zu dieser Domain als auch zu den freigeschalteten Kategorien gehören. Dies ist die stärkste Einschränkung.

Default:

- Kategorie und Domain

■ **Alternative Override-URL:**

Hier können Sie eine alternative URL-Adresse eintragen. Im Falle des Override wird dann statt der Standard-Webseite die hier eingetragene URL aufgerufen. In der externen HTML-Seite können Sie z.B. das Corporate Design Ihres Unternehmens abbilden oder weitere Funktionen wie JavaScript etc. nutzen. Außerdem können hier auch die gleichen Tags wie im Override-Text verwendet werden. Wenn Sie an dieser Stelle keinen Eintrag vornehmen, wird die im Gerät hinterlegte Standard-Webseite aufgerufen.

Mögliche Werte:

- gültige URL-Adresse

Default:

- leer

■ **Override-Absende-IP-Adresse:**

Hier können Sie optional eine Absende-Adresse konfigurieren, die statt der ansonsten automatisch für die Ziel-Adresse gewählten Absende-Adresse verwendet wird. Falls Sie z.B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absende-Adresse angeben.

Mögliche Werte:

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ (Achtung: wenn es eine Schnittstelle Namens "DMZ" gibt, dann wird deren Adresse genommen)
- LB0 ... LBF für die 16 Loopback-Adressen
- GUEST
- Beliebige IP-Adresse in der Form x.x.x.x

Default:

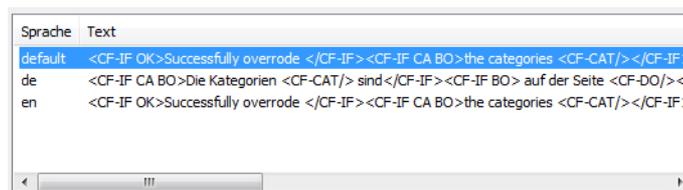
- leer



Die hier eingestellte Absende-Adresse wird für jede Gegenstelle unmaskiert verwendet.

■ **Override Text**

Hier können Sie einen Text definieren, der als Bestätigung für den Benutzer bei einem Override angezeigt wird.



■ **Sprache**

Damit der Anwender alle Meldungen in seiner voreingestellten Browser-Sprache erhält, kann hier der entsprechende Country-Code eingetragen werden. Wird der im Browser eingestellten Country-Code hier gefunden, kommt der dazu passende Text zur Anzeige.

Weitere Sprachen können nach Belieben hinzugefügt werden.

Der Country-Code sieht dafür z.B. folgendermaßen aus:

- de-DE: Deutschsprachig-Deutschland
- de-CH: Deutschsprachig-Schweiz
- de-AT: Deutschsprachig-Österreich
- en-GB: Englischsprachig-Großbritannien
- en-US: Englischsprachig-Vereinigte Staaten



Der Country-Code muss genau der Spracheinstellung des Browsers entsprechen, z.B. muss für Deutsch "de-DE" eingegeben werden (es reicht nicht "de"). Wird der im Browser eingestellte Country-Code in dieser Tabelle nicht gefunden oder der dafür hinterlegte Text gelöscht, so wird der bereits vordefinierten Standardtext (Default) verwendet. Den Default-Text können Sie bearbeiten.

Mögliche Werte:

- 10 alphanumerische Zeichen

Default:

- leer

■ **Text**

Geben Sie hier den Text ein, der als Override Text für diese Sprache verwendet werden soll.

Mögliche Werte:

- 254 alphanumerische Zeichen

Default:

- leer

Besondere Werte:

Sie können für den Blocktext auch HTML-Tags verwenden, wenn Sie unterschiedliche Seiten anzeigen wollen, je nachdem aus welchem Grund (z.B. Verbotene Kategorie oder Eintrag in der Blacklist) die Seite verboten wurde.

Für die einzusetzenden Werte können Sie folgende Tags verwenden:

- <CF-URL/> für die ursprünglich verbotene URL, die jetzt aber freigeschaltet ist
- <CF-CATEGORIES/> für die Liste der Kategorien, die durch diesen Override freigeschaltet sind (außer bei Domain-Override).
- <CF-BUTTON/> zeigt einen Override-Button, der auf die ursprünglich aufgerufene URL weiterleitet.
- <CF-LINK/> zeigt einen Override-Link an, der auf die ursprünglich aufgerufene URL weiterleitet.
- <CF-HOST/> oder <CF-DOMAIN/> zeigen den Hostteil bzw. die Domain der freigeschalteten URL an. Die Tags sind gleichwertig und können wahlweise verwendet werden.
- <CF-ERROR/> erzeugt eine Fehlermeldung, falls der Override fehlschlägt.
- <CF-DURATION/> zeigt die Override-Dauer in Minuten.

Zum Ein- und Ausblenden von Teilen des Html-Dokuments wird ein Tag mit Attributen verwendet: <CF-IF att1 att2> ... </CF-IF>.

Attribute können sein:

- CATEGORY wenn der Override-Typ "Kategorie" ist und der Override erfolgreich war
- DOMAIN wenn der Override-Typ "Domain" ist und der Override erfolgreich war
- BOTH wenn der Override-Typ "Kategorie und Domain" ist und der Override erfolgreich war
- ERROR falls der Override fehlgeschlagen ist
- OK falls entweder CATEGORY oder DOMAIN oder BOTH zutreffend sind

Werden in einem Tag mehrere Attribute angegeben, dann sollte der Bereich eingeblendet werden, wenn mind. eine dieser Bedingungen erfüllt ist. Alle Tags und Attribute lassen sich mit den jeweils ersten zwei Buchstaben abkürzen (z.B. CF-CA oder CF-IF BL). Das ist notwendig, weil der Text nur maximal 254 Zeichen lang sein darf.

- Beispiel:

```
<CF-IF CA BO>Die Kategorien <CF-CAT/> sind</CF-IF><CF-IF BO> in der Domain <CF-DO/></CF-IF><CF-IF DO>Die Domain <CF-DO/> ist</CF-IF><CF-IF OK> f&uuml;r <CF-DU/> Minuten freigeschaltet.<br><CF-LI/></CF-IF><CF-IF ERR>Override-Fehler:<br><CF-ERR/></CF-IF>
```

A.11.8 Profile des LANCOM Content Filters

Hier können Sie Content-Filter-Profile erstellen, die zur Überprüfung von Webseiten auf nicht zugelassene Inhalte genutzt werden. Ein Content-Filter-Profil hat immer einen Namen und ordnet verschiedenen Zeitabschnitten das jeweils gewünschte Kategorieprofil sowie optional eine Black- und eine Whitelist zu.

Um verschiedene Zeiträume unterschiedlich zu definieren, werden mehrere Content-Filter-Profileinträge mit dem gleichen Namen angelegt. Das Content-Filter-Profil besteht dann aus der Summe aller Einträge mit dem gleichen Namen.

Das Content-Filter-Profil wird über die Firewall angesprochen.



Bitte beachten Sie, dass Sie zur Nutzung der Profile im LANCOM Content Filters entsprechende Einstellungen in der Firewall vornehmen müssen.

Profile

Die Einstellungen für die Profile finden Sie hier:



LANconfig: Content-Filter ▶ Profile ▶ Profile

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profile ▶ Profile

■ **Name**

Hier muss der Name des Profils angegeben werden, über das es in der Firewall referenziert wird.

Mögliche Werte:

- Name eines Profils

Default:

- leer

■ **Zeitraumen**

Wählen Sie den Zeitraum für das folgende Kategorieprofil und optional die Blacklist und die Whitelist. Voreingestellt sind die Zeiträume "Always" und "Never". Weitere Zeiträume können Sie konfigurieren unter:

LANconfig: Datum/Zeit ▶ Allgemein ▶ Zeiträume

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Zeit ▶ Zeiträume

Zu einem Profil kann es auch mehrere Zeilen mit unterschiedlichen Zeiträumen geben.

Mögliche Werte:

- Always
- Never
- Name eines Zeitraumprofils

Default:

- leer

 Wenn sich bei der Verwendung von mehreren Einträgen für ein Content-Filter-Profil die Zeiträume überlappen, werden in diesem Zeitraum alle Seiten gesperrt, die durch einen der aktiven Einträge erfasst werden. Bleibt bei der Verwendung von mehreren Einträgen für ein Content-Filter-Profil ein Zeitraum undefiniert, ist in diesem Zeitraum der ungeprüfte Zugriff auf alle Webseiten möglich.

■ **Blacklisted**

Name des Blacklist-Profiles das für dieses Content-Filter-Profil während dieser Zeit gelten soll. Es kann ein neuer Name eingegeben oder ein vorhandener aus der Blacklist-Tabelle ausgewählt werden.

Mögliche Werte:

- Name eines Blacklist-Profiles
- Neuer Name

Default:

- leer

■ **Whitelisted**

Name des WhiteList-Profiles das für dieses Content-Filter-Profil während dieser Zeit gelten soll. Es kann ein neuer Name eingegeben oder ein vorhandener aus der Whitelist-Tabelle ausgewählt werden.

Mögliche Werte:

- Name eines Whitelist-Profiles
- Neuer Name

Default:

- leer

■ Kategorie-Profil

Name des Kategorie-Profiles das für dieses Profil während dieser Zeit gelten soll. Es kann ein neuer Name eingegeben oder ein vorhandener aus der Kategorietabelle ausgewählt werden.

Mögliche Werte:

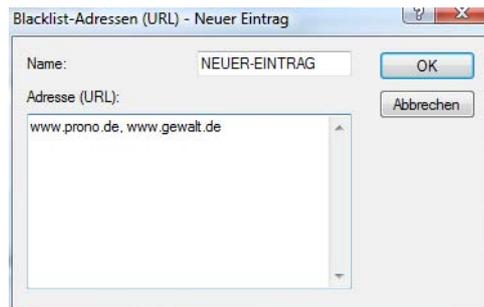
- Name eines Kategorie-Profiles
- Neuer Name

Default:

- leer

Blacklist-Adressen (URL)

Hier können Sie Webseiten konfigurieren, die anschließend verboten werden sollen.



LANconfig: Content-Filter ▶ Profile ▶ Blacklist-Adressen (URL)

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profile ▶ Blacklists

■ Name

Hier muss der Name der Blacklist angegeben werden, über den sie im Content-Filter-Profil referenziert wird.

Mögliche Werte:

- Name einer Blacklist

Default:

- leer

■ Adresse (URL)

Hier werden die URLs eingetragen, die über diese Blacklist verboten werden sollen.

Mögliche Werte:

- gültige URL-Adresse

Es können auch folgende Wildcards zum Einsatz kommen:

- * für mehrere beliebige Zeichen (z.B. findet www.lancom.* die Webseiten www.lancom.de, www.lancom.eu, www.lancom.es etc.)
- ? für ein beliebiges Zeichen (z.B. findet www.lancom.e* die Webseiten www.lancom.eu und www.lancom.es)



Bitte geben Sie die URL **ohne** führendes http:// ein. Beachten Sie, dass bei vielen URLs häufig automatisch ein Schrägstrich am Ende der URL angehängt wird, z.B. www.mycompany.de/. Daher empfiehlt sich für die Eingabe an dieser Stelle die Form: www.mycompany.de*.

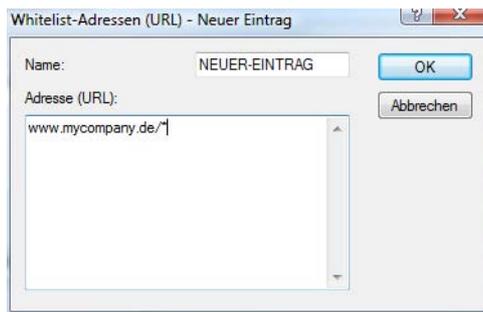
Einzelne URLs werden mit Leerzeichen getrennt.

Default:

- leer

Whitelist-Adressen (URL)

Hier können Sie Webseiten konfigurieren, die gezielt erlaubt werden sollen.



LANconfig: Content-Filter ▶ Profile ▶ Whitelist-Adressen (URL)

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profile ▶ Whitelists

■ **Name**

Hier muss der Name der Whitelist angegeben werden, über den sie im Content-Filter-Profil referenziert wird.

Mögliche Werte:

- Name einer Whitelist

Default:

- leer

■ **Adressen (URL)**

Hier können Sie Webseiten konfigurieren, die lokal geprüft und anschließend akzeptiert werden sollen.

Mögliche Werte:

- gültige URL-Adresse

Es können auch folgende Wildcards zum Einsatz kommen:

- * für mehrere beliebige Zeichen (z.B. findet www.lancom.* die Webseiten www.lancom.de, www.lancom.eu, www.lancom.es etc.)
- ? für ein beliebiges Zeichen (z.B. findet www.lancom.e* die Webseiten www.lancom.eu und www.lancom.es)



Bitte geben Sie die URL **ohne** führendes http:// ein. Beachten Sie, dass bei vielen URLs häufig automatisch ein Schrägstrich am Ende der URL angehängt wird, z.B. www.mycompany.de/. Daher empfiehlt sich für die Eingabe an dieser Stelle die Form: www.mycompany.de*.

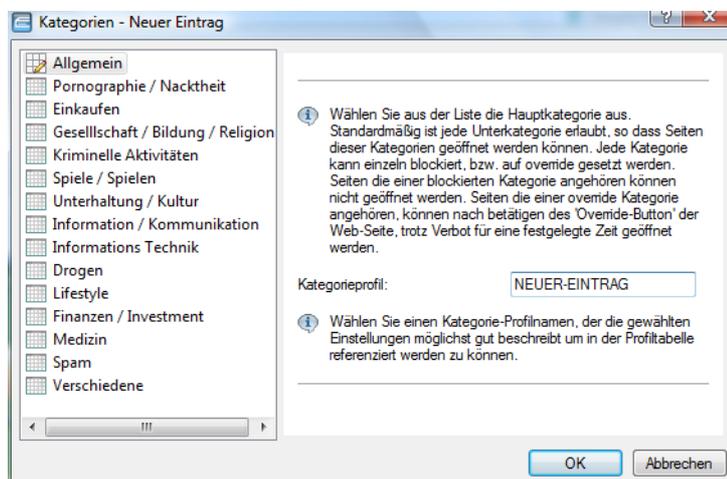
Einzelne URLs werden mit Leerzeichen getrennt.

Default:

- leer

Kategorien

Hier erstellen Sie ein Kategorieprofil und legen fest, welche Kategorien bzw. Gruppen bei der Bewertung der Webseiten berücksichtigt werden. Für jede Gruppe können Sie die einzelnen Kategorien erlauben, verbieten oder die Override-Funktion aktivieren.



LANconfig: Content-Filter ▶ Profile ▶ Kategorien

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Profile ▶ Kategorieprofile

■ Kategorieprofil

Hier wird der Name der Kategorieprofils angegeben, über den sie im Content-Filter-Profil referenziert wird.

Mögliche Werte:

- Name eines Kategorieprofils

Default:

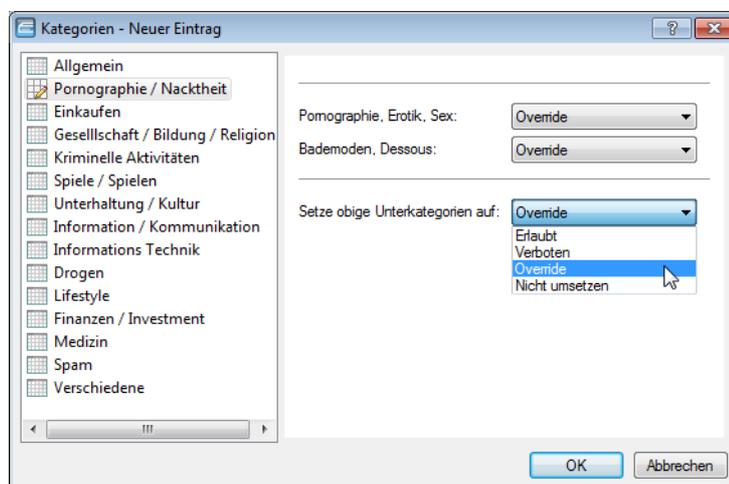
- leer

■ Kategorieeinstellungen

Für jede Hauptkategorie bzw. die zugeordneten Unterkategorien kann separat festgelegt werden, ob die zugehörigen URLs erlaubt, verboten oder nur mit Override erlaubt werden sollen.

Folgende Hauptkategorien können konfiguriert werden:

- Pornographie/ Nacktheit
- Einkaufen
- Gesellschaft/ Bildung/ Religion
- Kriminelle Aktivitäten
- Spiele/ Spielen
- Unterhaltung/ Kultur
- Information/ Kommunikation
- Informationstechnik
- Drogen
- Lifestyle
- Finanzen/ Investement
- Medizin
- Spam
- Verschiedene



Das Kategorieprofil muss anschließend einem Content-Filter-Profil zugewiesen werden (zusammen mit einem Zeitrahmen) um aktiv zu werden.

Mögliche Werte:

- Erlaubt, Verboten, Override

Default:

- Override

A.11.9 Optionen des LANCOM Content Filters

Hier können Sie einstellen, ob Sie über Ereignisse benachrichtigt werden und an wo die Informationen des LANCOM Content Filters gespeichert werden sollen.

Benachrichtigung über Ereignisse

Hier definieren Sie, in welcher Form Sie über bestimmte Ereignisse informiert werden möchten.

Ereignisse...

E-Mail Empfänger:

Informationen speichern

Geben Sie an, ob das Gerät regelmäßig ein Abbild der gesammelten Content-Filter-Daten (Snapshot) speichern soll.

Content-Filter-Snapshot aktiviert

Intervall:

Montagstag:

Wochentag:

Tageszeit:

LANconfig: Content-Filter ▶ Optionen

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Globale-Einstellungen

■ **Ereignisse:**

Hier definieren Sie, in welcher Form Sie über bestimmte Ereignisse informiert werden. Die Benachrichtigung kann erfolgen durch E-Mail, SNMP oder SYSLOG. Für verschiedene Ereignisse kann separat definiert werden, über welchen Weg Meldungen ausgegeben werden sollen.

Fehler:

- Bei SYSLOG: Quelle "System", Priorität "Alarm".
- Default: Benachrichtigung SNMP

Lizenzablauf:

- Bei SYSLOG: Quelle "Verwaltung", Priorität "Alarm".
- Default: Benachrichtigung SNMP

Lizenz überschritten:

- Bei SYSLOG: Quelle "Verwaltung", Priorität "Alarm".
- Default: Benachrichtigung SNMP

Override angewandt:

- Bei SYSLOG: Quelle "Router", Priorität "Alarm".
- Default: Benachrichtigung SNMP

Proxy-Begrenzung:

- Bei SYSLOG: Quelle "Router", Priorität "Info".
- Default: Benachrichtigung SNMP

Grund	E-Mail	SNMP	SYSLOG
Fehler	Aus	Ein	Aus
Lizenzablauf	Aus	Ein	Aus
Lizenz überschritten	Aus	Ein	Aus
Override angewandt	Aus	Ein	Aus
Proxy Begrenzung	Aus	Ein	Aus

Ereignisse - Eintrag bearbeiten

Benachrichtigung bei: Lizenzablauf

Benachrichtigung durch:

E-Mail

SNMP

SYSLOG

■ **E-Mail Empfänger:**

Um die E-Mail Benachrichtigungsfunktion zu nutzen, muss ein SMTP-Client entsprechend konfiguriert sein. Sie können den Client in diesem Gerät dazu verwenden oder einen anderen Ihrer Wahl.



Wenn kein E-Mail Empfänger angegeben wird, dann wird keine E-Mail verschickt.

WEBconfig: LCOS-Menübaum ▶ Setup ▶ UTM ▶ Content-Filter ▶ Globale-Einstellungen ▶ Schnappschuss

■ Content-Filter-Snapshot

Hier können Sie den Content-Filter-Snapshot aktivieren und bestimmen wann und wie häufig er stattfindet. Der Schnappschuss kopiert die Tabelle der Kategoriestatistik in die Letzter-Schnappschuss-Tabelle, dabei wird der alte Inhalt der Schnappschuss-Tabelle überschrieben. Die Werte der Kategoriestatistik werden dann auf 0 gesetzt.

■ Intervall

Wählen Sie hier, ob der SnapShot monatlich, wöchentlich oder täglich angefertigt werden soll.

Mögliche Werte:

- monatlich
- wöchentlich
- täglich

Default:

- monatlich

■ Montagstag:

Ist eine monatliche Ausführung des SnapShot gewünscht, wählen Sie hier den Tag an dem der SnapShot angefertigt werden soll.

Mögliche Werte:

- max. 2 Zeichen

Default:

- 1



Wählen Sie als Montagstag sinnvollerweise eine Zahl zwischen 1 und 28, damit der Tag in jedem Monat vorkommt.

■ Wochentag:

Ist eine wöchentliche Ausführung des SnapShot gewünscht, selektieren Sie hier den Wochentag, an dem der SnapShot angefertigt werden soll.

Mögliche Werte:

- Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag

Default:

- Montag

■ Tageszeit:

Ist eine tägliche Ausführung des SnapShot gewünscht, tragen Sie hier die Tageszeit in Stunden und Minuten ein.

Mögliche Werte:

- max. 5 Zeichen, Format HH:MM

Default:

- 00:00

A.11.10 Zusätzliche Einstellungen für den LANCOM Content Filter

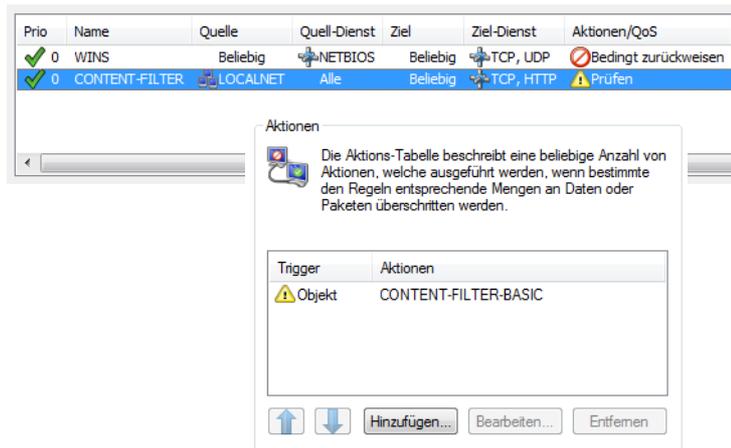
Firewall-Einstellungen für den Content-Filter

Die Firewall muss aktiviert sein, damit der LANCOM Content Filter arbeiten kann. Sie aktivieren die Firewall unter:

LANconfig: Firewall/QoS ► Allgemein

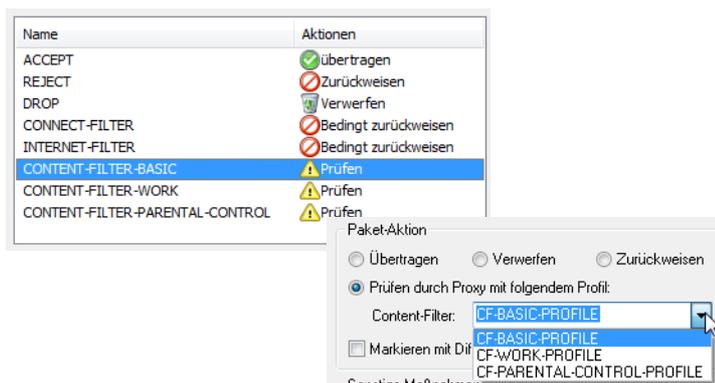
WEBconfig: LCOS-Menübaum ► Setup ► IP-Router ► Firewall

In der Default-Einstellung finden Sie die Firewall-Regel CONTENT-FILTER, die auf das Aktionsobjekt CONTENT-FILTER-BASIC zurückgreift:



i Die Firewall-Regel sollte auf den Zieldienst "http" beschränkt werden, damit nur ausgehende HTTP-Verbindungen erfasst werden. Ohne diese Einschränkung werden alle Pakete über den Contentfilter geprüft, was zu einer Beeinträchtigung der Performance im Gerät führt.

Eine Firewall-Regel für den Content-Filter muss ein spezielles Aktionsobjekt verwenden, das über die Paket-Aktionen die Daten mit einem Content-Filter-Profil prüft. In der Default-Einstellung finden Sie die Aktionsobjekte CONTENT-FILTER-BASIC, CONTENT-FILTER-WORK und CONTENT-FILTER-PARENTAL-CONTROL, die auf jeweils passende Content-Filter-Profile zurückgreifen:

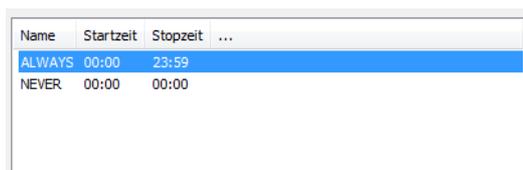


Beispiel: Beim Öffnen einer Webseite durchlaufen die Datenpakete die Firewall und werden von der Regel CONTENT-FILTER erfasst. Das Aktionsobjekt CONTENT-FILTER-BASIC prüft die Datenpakete mit dem Content-Filter-Profil CONTENT-FILTER-BASIC.

Zeitrahmen

Zeitrahmen werden verwendet, um die Gültigkeitsdauer von Content-Filter-Profilen zu definieren. Zu einem Profil kann es auch mehrere Zeilen mit unterschiedlichen Zeitrahmen geben. Dabei sollten sich die Zeitrahmen unterschiedlicher Zeilen ergänzen, d.h. wenn Sie eine ARBEITSZEIT festlegen, wollen Sie wahrscheinlich auch einen Zeitrahmen FREIZEIT festlegen, der die Zeit außerhalb der Arbeitszeit umfasst.

Voreingestellt sind die Zeitrahmen "ALWAYS" und "NEVER". Weitere Zeitrahmen können Sie konfigurieren unter:



LANconfig: Datum/Zeit ► Allgemein ► Zeitrahmen

WEBconfig: LCOS-Menübaum ► Setup ► Zeit ► Zeitrahmen

■ Name

Hier muss der Name des Zeitrahmens angegeben werden, über den er im Content-Filter-Profil referenziert wird.

Mögliche Werte:

- Name eines Zeitrahmens

Default:

- leer

■ Startzeit

Hier kann die Startzeit (Tageszeit) angegeben werden, ab der das gewählte Profil gelten soll.

Mögliche Werte:

- max. 5 Zeichen, Format HH:MM

Default:

- 00:00

■ Endzeit

Hier kann die Endzeit (Tageszeit) angegeben werden, ab der das gewählte Profil nicht mehr gültig sein soll.

Mögliche Werte:

- max. 5 Zeichen, Format HH:MM

Default:

- 23:59

■ Wochentage

Hier können Sie die Wochentage auswählen, an denen der Zeitrahmen gültig sein soll.

Mögliche Werte:

- Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag

Default:

- Aktiviert für Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag

Zeitschemata lassen sich mit gleichem Namen, aber unterschiedlichen Zeiten auch über mehrere Zeilen hinweg definieren:

Name	Startzeit	Stopzeit	...
ALWAYS	00:00	23:59	
FREIZEIT	00:00	07:00	
FREIZEIT	12:01	13:00	
FREIZEIT	17:01	23:59	
NEVER	00:00	00:00	

A.12 DFS3

A.12.1 Einleitung

Mitte 2010 tritt eine neue Version (1.5.1) der EN 301 893 in Kraft, die einige Veränderungen für die Nutzung von WLAN-Frequenzen im Bereich 5,25 bis 5,35 und 5,47 bis 5,725 GHz mit sich bringt. Die neue EN 301 893-V1.5 regelt das DFS-Verfahren (Dynamic Frequency Selection) für diese Frequenzbereiche, mit dem Radarstationen vor dem Einfluss durch WLAN-Systeme geschützt werden. Bei der Erkennung von bestimmten Mustern in den empfangenen Funksignalen können WLAN-Systeme mit Hilfe von DFS die Radarstationen erkennen und einen automatischen Wechsel der verwendeten Kanäle durchführen. Im Unterschied zu den bisherigen Regelungen in EN 301 893-V1.3 (DFS2) wird DFS nach EN 301 893-V1.5 kurz als "DFS3" bezeichnet.

Generell wird ein Radarmuster durch die Werte Pulsrate, Pulsbreite und Anzahl der Pulse beschrieben. Nach den bisherigen DFS-Verfahren wurden nur feste Radarmuster geprüft, die durch definierte Kombinationen verschiedener Pulsraten und Pulsbreiten im WLAN-Gerät hinterlegt sind. Nach DFS3 müssen nun auch Muster aus wechselnden Pulsraten und Pulsbreiten als Radarmuster erkannt werden. Außerdem können innerhalb eines Radarsignals zwei oder drei unterschiedliche Pulsraten verwendet werden.



Für die Erkennung von Wetterradaren (Kanäle 120, 124 und 128 im Frequenzbereich 5,6 bis 5,65 MHz) gelten besondere Nutzungsbedingungen. Die DFS-Implementierung im LCOS unterstützt die verschärften Erkennungsbedingungen nicht, deshalb werden diese drei Kanäle von neueren LCOS-Versionen ausgespart.

A.12.2 Konfiguration

Alle WLAN-Systeme, die nach Inkrafttreten der EN 301 893-V1.5 in Betrieb genommen werden, müssen im 5 GHz-Band DFS3 verwenden. Um DFS3 in ihrem WLAN-Gerät zu aktivieren, wählen Sie folgenden Menüeintrag:

WEBconfig: LCOS-Menübaum ► Setup ► Schnittstellen ► WLAN ► Radioeinstellungen

- Bevorzugtes-DFS-Schema

□ Alternative URLs für CRLs

Hier haben Sie die Möglichkeit zwischen DFS2 (EN 301 893-V1.3) und DFS3 (EN 301 893-V1.5) zu wählen.

- Mögliche Werte:
EN 301 893-V1.5
EN 301 893-V1.3
- Default:
EN 301 893-V1.5

Bei einem Upgrade von einer Firmware vor LCOS-Version 8.00 auf eine LCOS-Version 8.00 oder höher wird die vorherige Einstellung DFS2 (EN 301 893-V1.3) beibehalten.



Die Auswahl ist nicht möglich für WLAN-Geräte, die fest auf DFS3-Betrieb eingestellt sind, deren Prozessor die DFS3-Technologie nicht unterstützt oder die nur auf dem 2,4 GHz-Band senden.

A.13 Alternative URLs für CRLs

A.13.1 Einleitung

Die Adresse, von der eine Certificate Revocation List (CRL) abgeholt werden kann, wird normalerweise innerhalb der Zertifikate (als `crlDistributionPoint`) angegeben. Im LCOS können in einer Tabelle alternative URLs angegeben werden. Nach dem Systemstart werden die entsprechenden CRLs automatisch von diesen URLs abgeholt und zusätzlich zu den in den Zertifikaten angegebenen Listen verwendet.

A.13.2 Konfiguration

Die Tabelle für die alternativen CRL-URLs finden Sie auf folgenden Pfaden:

LANconfig: Zertifikate ▶ CRL-Client ▶ Alternative-URLs

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Zertifikate ▶ CRLs ▶ Alternative-URL-Tabelle

■ Alternative-URL

Geben Sie hier die URL an, von der eine CRL abgeholt werden kann.

- Mögliche Werte:
Gültige URL, max. 251 Zeichen.
- Default:
Leer

A.14 Broken-Link-Detection

Wenn ein Access Point keine Verbindung zum kabelgebundenen LAN hat, kann er in den meisten Fällen seine wesentliche Aufgabe – den eingebuchten WLAN-Clients einen Zugang zum LAN zu ermöglichen – nicht mehr erfüllen. Mit der Funktion der Broken-Link-Detection (Link-Fehler-Erkennung) können die WLAN-Module eines Geräts deaktiviert werden, wenn die LAN-Verbindung verloren geht. So können die beim Access Point eingebuchten Clients einen anderen Access Point (mit ggf. schwächerem Signal) suchen und sich mit diesem verbinden.

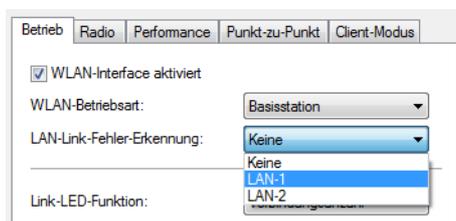
Bis zur LCOS-Version 7.80 bezog sich die Aktivierung der Link-Fehler-Erkennung immer auf LAN-1, auch wenn das Gerät über mehrere LAN-Interfaces verfügte. Außerdem wirkte sich die Deaktivierung auf alle verfügbaren WLAN-Module des Gerätes aus.

Ab LCOS-Version 8.00 kann die Link-Fehler-Erkennung gezielt an ein bestimmtes LAN-Interface gebunden werden.

Die Einstellung für die Link-Fehler-Erkennung finden Sie auf folgenden Pfaden:

LANconfig: Wireless-LAN ▶ Allgemein ▶ Physikalische WLAN-Einst. ▶ Betrieb

WEBconfig: LCOS-Menübaum ▶ Setup ▶ Schnittstellen ▶ WLAN ▶ Betriebs-Einstellungen



■ LAN-Link-Fehler-Erkennung

Mit dieser Funktion werden die WLAN-Module des Geräts deaktiviert, wenn das zugeordnete LAN-Interface nicht über einen Link zum LAN verfügt.

Mögliche Werte:

- Nein: Link-Fehler-Erkennung wird nicht genutzt.
- LAN-1 bis LAN-n (je nach verfügbaren LAN-Interfaces im Gerät): Alle WLAN-Module des Geräts werden deaktiviert, wenn das hier angegebene LAN-Interface keine Verbindung zum kabelgebundenen LAN hat.

Default:

- Nein



Die Interface-Bezeichnungen LAN-1 bis LAN-n repräsentieren die logischen LAN-Schnittstellen. Die verfügbaren physikalischen Ethernet-Ports des Geräts müssen zur Nutzung dieser Funktion ggf. auf die entsprechenden Werte LAN-1 bis LAN-n eingestellt werden.



Die Link-Fehler-Erkennung kann auch für WLAN-Geräte in der Betriebsart als WLAN-Client genutzt werden. Bei eingeschalteter Link-Fehler-Erkennung werden die WLAN-Module eines WLAN-Clients nur dann aktiviert, wenn die entsprechenden LAN-Schnittstellen eine Verbindung zum kabelgebunden LAN haben.