

LCOS LX 6.12

Addendum

07/2023

Contents

- 1 Addendum to LCOS LX version 6.12.....4**
- 2 LED signaling in case of insufficient power supply.....5**
- 3 Client mode for flexible integration of Ethernet-capable devices in wireless networks.....6**
 - 3.1 Links.....6
 - 3.2 RADIUS Client.....8
 - 3.3 Roaming.....8
 - 3.4 WDS (Wireless Distribution System) / Point-to-point links.....9
 - 3.4.1 Links.....9
 - 3.4.2 RADIUS client profiles.....10
 - 3.4.3 Roaming profiles.....11
 - 3.4.4 Client certificate.....11
 - 3.5 Additions to the Setup menu.....12
 - 3.5.1 Mode.....12
 - 3.5.2 Encryption-Profile.....12
 - 3.5.3 Encryption-Key.....13
 - 3.5.4 LCOS-Client-Bridge-Support.....13
 - 3.5.5 Roaming-Profile.....13
 - 3.5.6 RADIUS-Client-Profile.....14
 - 3.5.7 Roaming.....14
 - 3.5.8 Delete-WLAN-Supplicant-Certificates.....15
 - 3.5.9 WLAN-Supplicant.....16

Copyright

© 2023 LANCOM Systems GmbH, Würselen (Germany). All rights reserved.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from LANCOM Systems. We reserve the right to make any alterations that arise as the result of technical development.

Windows® and Microsoft® are registered trademarks of Microsoft, Corp.

LANCOM, LANCOM Systems, LANcommunity and Hyper Integration are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and/or omissions.

This product contains separate open-source software components. These are subject to their own licenses, in particular the General Public License (GPL). License information relating to the device firmware (LCOS LX) is available on the CLI by using the command `show 3rd-party-licenses`. If the respective license demands, the source files for the corresponding software components will be made available on request. Please contact us via e-mail under gpl@lancom.de.

Products from LANCOM Systems include software developed by the "OpenSSL Project" for use in the "OpenSSL Toolkit" (www.openssl.org).

Products from include cryptographic software written by Eric Young (ey@cryptsoft.com).

Products from LANCOM Systems include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from LANCOM Systems contain the LZMA SDK developed by Igor Pavlov.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen, Germany
Germany
www.lancom-systems.com

1 Addendum to LCOS LX version 6.12

This document describes the changes and enhancements in LCOS LX version 6.12 since the previous version.

2 LED signaling in case of insufficient power supply

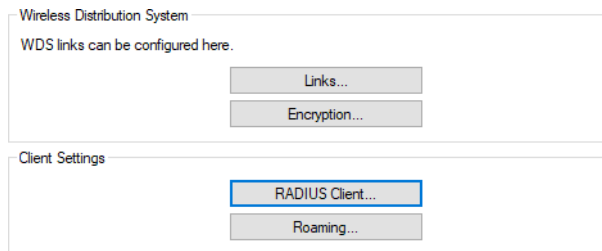
As of LCOS LX 6.12, an insufficient power supply is indicated.

For devices that require PoE 802.3bt for full functionality (e.g. activation of all WLAN streams), a permanently lit yellow power LED indicates that there is insufficient power supply.

3 Client mode for flexible integration of Ethernet-capable devices in wireless networks

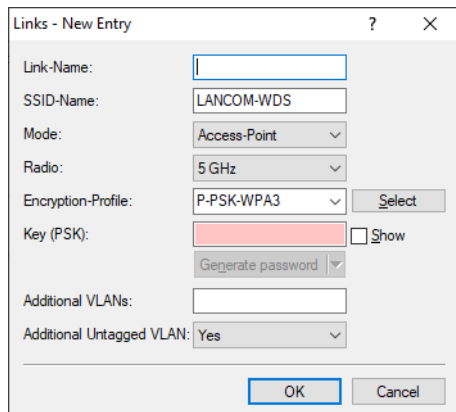
Your LCOS LX-based access points now support client mode. From now on, you can use your LCOS LX-based access points flexibly to integrate a wide range of Ethernet-capable devices into existing WLAN networks - regardless of the operating system and thus regardless of the manufacturer. For tailored security, choose between certificate-based encrypted communication via IEEE 802.1X or via WPA2/3-PSK.

WLAN client connections are technically similar to WDS connections and are therefore configured in the same place. For this purpose there are the following changed or new settings in LANconfig under **Wireless-LAN > WDS**.



3.1 Links

General settings relating to the WDS connection are configured under **Wireless-LAN > WDS > Links**. Add a line to the table for each WDS connection. By default, the table is empty.



Link-Name

The name of the link. Used for further referencing in the device configuration.

SSID-Name


The name of the special SSID used for the WDS link. This name must match at both ends of the connection.


Mode

In the context of a WDS connection, there are three roles: Access Point, Client, Legacy Client. The partner configured as a client searches for a partner configured as an access point using the SSID configured above

and initiates the connection. The access point configured as a legacy client can log into the SSID of any access point

In a point-to-multipoint scenario, multiple clients can connect to an access point.

 The number of regular configured SSIDs for the client connection plus number of the configured WDS links cannot exceed the total number of SSIDs supported by the device—in a sense, it all comes from the same “SSID budget”.

 Any number of WDS links can be operated in access-point mode (up to the technical maximum number of SSIDs supported by the device mentioned above). In station mode, however, only one WDS link can operate per device. Connections in access-point mode and station mode (of the latter, only one) can operate simultaneously on the same device.

Note that for a point-to-multipoint scenario, a single connection in AP mode on the “distribution node” is usually sufficient.

Radio

The frequency band to be used for the WDS link. For capacity reasons, we recommend the use of 5 GHz or 6 GHz (depending on the hardware capabilities of the device).

Encryption-Profile

The encryption profile to be used for the WDS link.

Key (PSK)

The WPA-PSK used for the WDS link. When using an encryption profile with 802.1X, this field can be left empty.

Additional VLANs

The WLAN configuration allows individual SSIDs to be associated with WDS links. These are then made available as a bridge via the WDS connection. If additional VLANs, e.g. transported via Ethernet, are also to be transmitted, they can be entered here (comma-separated list of VLAN IDs [0-4095]).

Additional Untagged VLAN

Untagged packets are to be transmitted.

LCOS Client Bridge Support

If the LCOS LX access point in client mode is connected to an LCOS access point in base station mode, 4-address frames can still be used for this, which enables the transmission of VLANs or MAC addresses. This mode cannot be used if the LCOS LX access point is operated in base station mode and an LCOS access point is logged in to it in client mode.

Roaming profile

Here you can enter a roaming profile if the access point is in client or legacy client mode.

Optionally configure an encryption profile under [Encryption](#).

If you want to establish a client connection using 802.1X, please configure a RADIUS client profile first. See [RADIUS Client](#) on page 8

Create a roaming profile if required. See [Roaming](#) on page 8

3.2 RADIUS Client

The settings for logging in using 802.1X are configured under **Wireless-LAN > WDS > Client Settings > RADIUS Client**.

Profile name

Use a unique profile name, which you specify later in the encryption profile.

Method

Select a method that suits your requirement. When using "TLS", uploading a certificate is necessary.

Username

Enter the RADIUS user name here. When using the "TLS" method, no entry is necessary here.

Password

Enter the RADIUS password here. When using the "TLS" method, no entry is necessary here.

Certificate

You can accept the RADIUS server's certificate automatically or have the uploaded certificate verified. We always recommend uploading a certificate to verify the integrity of the RADIUS server. The certificate upload is only possible in WEBconfig. See [Client certificate](#) on page 11.

3.3 Roaming

Settings relating to the roaming profile are configured under **Wireless-LAN > WDS > Client Settings > Roaming**.

Profile name

Use a unique profile name, which you specify later in the WDS connection.

Signal strength threshold

Enter the threshold value from which the scan interval of the access point should change. Values from 0 to 100 specify a percentage value. Values from -100 to 0 are in dbm.

Good signal scan interval

If the signal strength is above the limit, a scan is performed in seconds during this time to check if a better access point becomes available to connect.

Bad signal scan interval

If the signal strength falls to the specified limit, a scan is triggered directly to search for a better access point. If no better access point is available, the search continues in the specified time in seconds until a connection to an access point with a better signal strength could be connected or the signal with the connected access point has improved again.


3.4 WDS (Wireless Distribution System) / Point-to-point links

You can reach this area in WEBconfig via the **WDS** item in the sidebar.



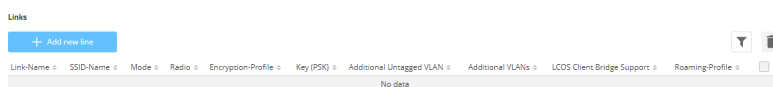
WDS can be used to set up point-to-point WLAN links between access points. These connections serve as a wireless backhaul, allowing remote access points to be connected to the rest of the network. This allows WLAN coverage to be provided even in areas where access points cannot be connected via Ethernet, for example.

These access points optionally offer SSIDs for connecting WLAN clients ("repeater" mode) or for connecting the wireless backhaul to its Ethernet port (wireless bridge).

 With LCOS LX 6.10, WDS operation is validated over a maximum distance of 300 meters.

3.4.1 Links

Configure here general settings relating to the WDS connection. Add a line to the table for each WDS connection. By default, the table is empty.

**Link-Name**

The name of the link. Used for further referencing in the device configuration.

SSID-Name

The name of the special SSID used for the WDS link. This name must match at both ends of the connection.

Mode

In the context of a WDS connection, there are three roles: Access Point, Client, Legacy Client. The partner configured as a client searches for a partner configured as an access point using the SSID configured above and initiates the connection. The access point configured as a legacy client can log into the SSID of any access point

In a point-to-multipoint scenario, multiple clients can connect to an access point.

i The number of regular configured SSIDs for the client connection plus number of the configured WDS links cannot exceed the total number of SSIDs supported by the device—in a sense, it all comes from the same “SSID budget”.

i Any number of WDS links can be operated in access-point mode (up to the technical maximum number of SSIDs supported by the device mentioned above). In station mode, however, only one WDS link can operate per device. Connections in access-point mode and station mode (of the latter, only one) can operate simultaneously on the same device.

Note that for a point-to-multipoint scenario, a single connection in AP mode on the “distribution node” is usually sufficient.

Radio

The frequency band to be used for the WDS link. For capacity reasons, we recommend the use of 5 GHz or 6 GHz (depending on the hardware capabilities of the device).

Encryption-Profile

The encryption profile to be used for the WDS link.

Key (PSK)

The WPA-PSK used for the WDS link. When using an encryption profile with 802.1X, this field can be left empty.

Additional VLANs

The WLAN configuration allows individual SSIDs to be associated with WDS links. These are then made available as a bridge via the WDS connection. If additional VLANs, e.g. transported via Ethernet, are also to be transmitted, they can be entered here (comma-separated list of VLAN IDs [0-4095]).

Additional Untagged VLAN

Untagged packets are to be transmitted.

LCOS Client Bridge Support

If the LCOS LX access point in client mode is connected to an LCOS access point in base station mode, 4-address frames can still be used for this, which enables the transmission of VLANs or MAC addresses. This mode cannot be used if the LCOS LX access point is operated in base station mode and an LCOS access point is logged in to it in client mode.

Roaming profile

Here you can enter a roaming profile if the access point is in client or legacy client mode.

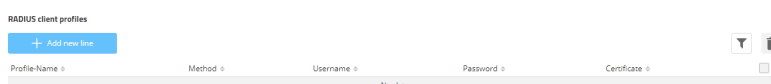
Optionally configure an encryption profile under [Encryption](#).

If you want to establish a client connection using 802.1X, please configure a RADIUS client profile first under [RADIUS client profiles](#) on page 10.

If required, create a roaming profile under [Roaming profiles](#) on page 11.

3.4.2 RADIUS client profiles

If you want to establish a client connection using 802.1X, please configure a RADIUS client profile here first.



Profile name

Use a unique profile name, which you specify later in the encryption profile.

Method

Select a method that suits your requirement. When using "TLS", uploading a certificate is necessary.

Username

Enter the RADIUS user name here. When using the "TLS" method, no entry is necessary here.

Password

Enter the RADIUS password here. When using the "TLS" method, no entry is necessary here.

Certificate

You can accept the RADIUS server's certificate automatically or have the uploaded certificate verified. We always recommend uploading a certificate to verify the integrity of the RADIUS server. See [Client certificate](#) on page 11 for the certificate upload.

3.4.3 Roaming profiles

If required, create a roaming profile here.

Roaming profiles

[+ Add new item](#)

| Profile-Name | Signal-Strength-Threshold | Good-Signal-Scan-Interval | Bad-Signal-Scan-Interval | |
|--------------|---------------------------|---------------------------|--------------------------|--------------------------|
| P-DEFAULT | 32 | 300 | 30 | <input type="checkbox"/> |
| P-STATIC | 0 | 600 | 600 | <input type="checkbox"/> |

Showing 2 of 2 records

Profile name

Use a unique profile name, which you specify later in the WDS connection.

Signal-Strength-Threshold

Enter the threshold value from which the scan interval of the access point should change.

Good-Signal-Scan-Interval

If the signal strength is above the limit, a scan is performed in seconds during this time to check if a better access point becomes available to connect.

Bad-Signal-Scan-Interval

If the signal strength falls to the specified limit, a scan is triggered directly to search for a better access point. If no better access point is available, the search continues in the specified time in seconds until a connection to an access point with a better signal strength could be connected or the signal with the connected access point has improved again.

3.4.4 Client certificate

Manage the client certificates for the WDS connections here.

Client certificate

Upload a new PKCS12 certificate

Select file No file selected

PKCS12 password

[Start upload](#) [Delete certificate](#)


Select a PKCS12 container and specify the associated password. Use **Start upload** to upload the certificate to the device. You can delete any existing certificates via **Delete certificate**.


3.5 Additions to the Setup menu

3.5.1 Mode

In the context of a WDS connection, there are three roles: Access Point, Client, Legacy Client. The partner configured as a client searches for a partner configured as an access point using the SSID configured above and initiates the connection. The access point configured as a legacy client can log into the SSID of any access point

In a point-to-multipoint scenario, multiple clients can connect to an access point.

 The number of regular configured SSIDs for the client connection plus number of the configured WDS links cannot exceed the total number of SSIDs supported by the device—in a sense, it all comes from the same “SSID budget”.

 Any number of WDS links can be operated in access-point mode (up to the technical maximum number of SSIDs supported by the device mentioned above. In station mode, however, only one WDS link can operate per device. Connections in access-point mode and station mode (of the latter, only one) can operate simultaneously on the same device.

Note that for a point-to-multipoint scenario, a single connection in AP mode on the “distribution node” is usually sufficient.

SNMP ID:

2.20.13.1.3

Console path:

Setup > WLAN > WDS > Links

Possible values:

Access point
Station

3.5.2 Encryption-Profile

The encryption profile to be used for the WDS link.

SNMP ID:

2.20.13.1.5

Console path:

Setup > WLAN > WDS > Links

Possible values:

Max. 128 characters from [A-Z] [a-z] [0-9] #@ { | } ~ ! \$ % & ' () * + - , / : ; < = > ? [\] " ^ _ . `

3.5.3 Encryption-Key

The WPA-PSK used for the WDS link. When using an encryption profile with 802.1X, this field can be left empty.

SNMP ID:

2.20.13.1.6

Console path:

Setup > WLAN > WDS > Links

Possible values:

Max. 63 characters from [A-Z] [a-z] [0-9] #@{|}~!\$%&'()*+,-./:;<=>?[\] "^_`~`

3.5.4 LCOS-Client-Bridge-Support

If the LCOS LX access point in client mode is connected to an LCOS access point in base station mode, 4-address frames can still be used for this, which enables the transmission of VLANs or MAC addresses. This mode cannot be used if the LCOS LX access point is operated in base station mode and an LCOS access point is logged in to it in client mode.

SNMP ID:

2.20.13.1.9

Console path:

Setup > WLAN > WDS > Links

Possible values:

No
Yes

Default:

Yes

3.5.5 Roaming-Profile

Here you can enter a roaming profile if the access point is in client or legacy client mode.

Optionally configure an encryption profile.

If you want to establish a client connection using 802.1X, please configure a RADIUS client profile first.

If required, create a roaming profile.

SNMP ID:

2.20.13.1.11

Console path:

Setup > WLAN > WDS > Links

Possible values:

Max. 128 characters from [A-Z] [a-z] [0-9] #@{|}~!\$%&'()*+,-./:;<=>?[\]"^_`~

3.5.6 RADIUS-Client-Profile

Specify a RADIUS client profile here if necessary.

SNMP ID:

2.20.13.2.6

Console path:

Setup > WLAN > WDS > Encryption

Possible values:

Max. 128 characters from [A-Z] [a-z] [0-9] #@{|}~!\$%&'()*+,-./:;<=>?[\]"^_`~

3.5.7 Roaming

Configure the settings for the roaming profile here.

SNMP ID:

2.20.13.3

Console path:

Setup > WLAN > WDS

3.5.7.1 Profile-Name

Use a unique profile name, which you specify later in the WDS connection.

SNMP ID:

2.20.13.3.1

Console path:

Setup > WLAN > WDS > Roaming

Possible values:

Max. 128 characters from [A-Z] [a-z] [0-9] #@{|}~!\$%&'()*+,-./:;<=>?[\]"^_`~

3.5.7.2 Signal-Strength-Threshold

Enter here the threshold value from which the scan interval of the access point should change. Values from 0 to 100 specify a percentage value. Values from -100 to 0 are in dbm.

SNMP ID:

2.20.13.3.2

Console path:**Setup > WLAN > WDS > Roaming****Possible values:**Max. 4 characters from `-[0-9]`

3.5.7.3 Good-Signal-Scan-Interval

If the signal strength is above the limit, a scan is performed in seconds during this time to check if a better access point becomes available to connect.

SNMP ID:

2.20.13.3.3

Console path:**Setup > WLAN > WDS > Roaming****Possible values:**

0 ... 4,294,967,295 Seconds

3.5.7.4 Bad-Signal-Scan-Interval

If the signal strength falls to the specified limit, a scan is triggered directly to search for a better access point. If no better access point is available, the search continues in the specified time in seconds until a connection to an access point with a better signal strength could be connected or the signal with the connected access point has improved again.

SNMP ID:

2.20.13.3.4

Console path:**Setup > WLAN > WDS > Roaming****Possible values:**

0 ... 4,294,967,295 Seconds

3.5.8 Delete-WLAN-Supplicant-Certificates

With this action you delete all existing certificates of the WLAN supplicants.

SNMP ID:

2.30.4

Console path:

Setup > RADIUS > RADIUS-Server

Possible arguments:

none

3.5.9 WLAN-Supplicant

Here you will find the settings for the 802.1X supplicant functionality to authenticate the device WLAN-side to an infrastructure secured with 802.1X.

SNMP ID:

2.30.12

Console path:

Setup > RADIUS

3.5.9.1 Profile-Name

Use a unique profile name, which you specify later in the encryption profile.

SNMP ID:

2.30.12.1

Console path:

Setup > RADIUS > WLAN-Supplicant

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#{|}~!$%&'()*+,-./:;<=>?[\]"^_``

3.5.9.2 Method

Select a method that suits your requirement. When using TLS, uploading a certificate is necessary.

SNMP ID:

2.30.12.2

Console path:

Setup > RADIUS > WLAN-Supplicant

Possible values:

none
 MD5
 TLS
 TTLS/MD5
 TTLS/PAP
 TTLS/CHAP
 TTLS/MSCHAPv2
 TTLS/MSCHAP
 PEAP/GTC
 PEAP/MSCHAPv2

3.5.9.3 Username

Enter the RADIUS user name here. When using the "TLS" method, no entry is necessary here.

SNMP ID:

2.30.12.3

Console path:

Setup > RADIUS > WLAN-Supplicant

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]"^_`~``

3.5.9.4 Password

Enter the RADIUS password here. When using the "TLS" method, no entry is necessary here.

SNMP ID:

2.30.12.4

Console path:

Setup > RADIUS > WLAN-Supplicant

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+,-./:;<=>?[\]"^_`~``

3.5.9.5 Certificate

You can accept the RADIUS server certificate automatically or have the uploaded certificate verified. We always recommend uploading a certificate to verify the integrity of the RADIUS server.

3 Client mode for flexible integration of Ethernet-capable devices in wireless networks

SNMP ID:

2.30.12.5

Console path:

Setup > RADIUS > WLAN-Supplicant

Possible values:

Auto-accept

Accept certificate automatically.

Container

Check uploaded certificate.