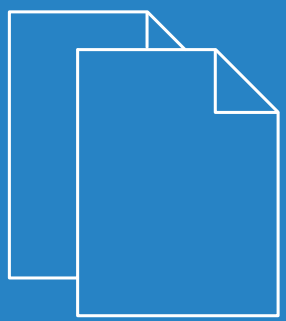
SECURE. NETWORKS.

LCOS LX 5.30

Addendum



01/2021

LANCOM Systems

Contents

Copyright

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 (*eay@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

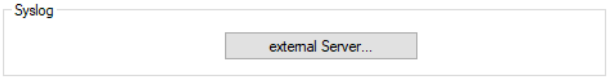
1 Addendum to LCOS LX version 5.30

This document describes the changes and enhancements in LCOS LX version 5.30 since the previous version.

2 Syslog

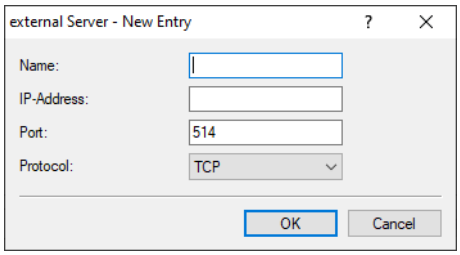
For diagnostic purposes, the syslog of a LCOS LX-based device can be sent to an external syslog server.

The settings for this can be found under **Management** > **Extended** > **Syslog**.



Configure one or more syslog servers in the **External Server** table. Messages can be sent via TCP or UDP.

Note that syslog messages are unencrypted and may contain sensitive information about your network. For this reason they should only be transmitted for diagnostic purposes over a secure network.



Name

Name of the external syslog server.

IP address

IP address of the external syslog server.

Port

Port of the external syslog server.

Protocol

Protocol (TCP/UDP) used to communicate with the external syslog server.

2.1 Additions to the Setup menu

2.1.1 Syslog

For diagnostic purposes, the syslog of a LCOS LX-based device can be sent to an external syslog server.

You can adjust the relevant settings here.

SNMP ID:

2.22

Console path:

Setup

Server

Configure one or more syslog servers in this table. Messages can be sent via TCP or UDP.

Note that syslog messages are unencrypted and may contain sensitive information about your network. For this reason they should only be transmitted for diagnostic purposes over a secure network.

SNMP ID:

2.22.2

Console path:

Setup > **Syslog**

Server

Name of the external syslog server.

SNMP ID:

2.22.2.1

Console path:

Setup > **Syslog** > **Server**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

IP-Address

IP address of the external syslog server.

SNMP ID:

2.22.2.7

Console path:

Setup > **Syslog** > **Server**

Possible values:

Max. 32 characters from `IPv4 address: a.b.c.d`

Port

Port of the external Syslog server.

SNMP ID:

2.22.2.8

Console path:

Setup > **Syslog** > **Server**

Possible values:

Max. 5 characters from `[0-9]`

Default:

514

Protocol

Protocol (TCP/UDP) used to communicate with the external syslog server.

SNMP ID:

2.22.2.9

Console path:

Setup > **Syslog** > **Server**

Possible values:

TCP
UDP

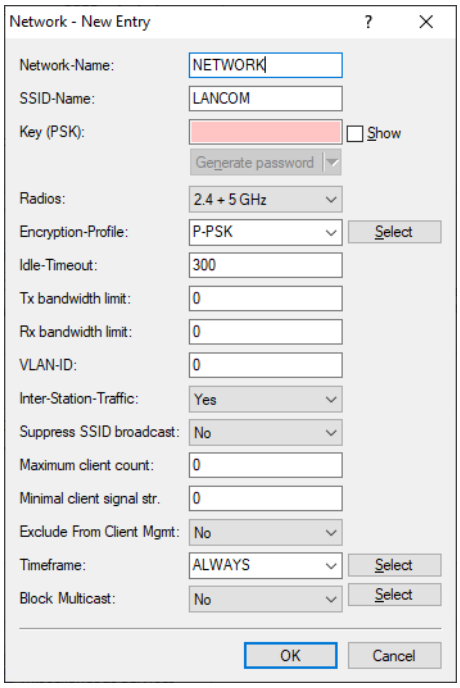
Default:

TCP

3 SSID-specific multicast filter

From LCOS LX 5.30 you can activate a multicast filter for each SSID.

Configure this under **Wireless-LAN** > **WLAN-Networks** > **Network**.



Block Multicast

This can be used to block multicasts sent or received by WLAN clients. A distinction can be made between IPv4 and IPv6.

ICMPv6 packets are not blocked in order for IPv6 address referencing to continue to work.

The LW-500 does not support this feature.

3.1 Additions to the Setup menu

3.1.1 Block-Multicast

This can be used to block multicasts sent or received by WLAN clients. A distinction can be made between IPv4 and IPv6.

ICMPv6 packets are not blocked in order for IPv6 address referencing to continue to work.

The LW-500 does not support this feature.

SNMP ID:

2.20.1.25

Console path:

Setup > **WLAN** > **Network**

Possible values:

No

Do not block multicasts.

IPv4-only

Block IPv4 multicasts only.

IPv6-only

Block IPv6 multicasts only.

Both

Block both IPv4 and IPv6 multicasts.

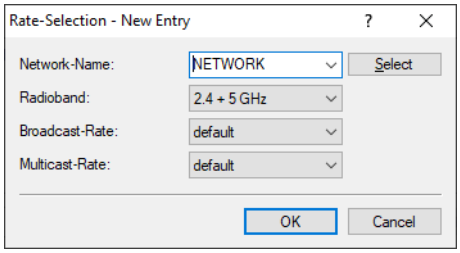
Default:

No

4 Configurable broadcast and multicast data rates

Increasing the broadcast and multicast data rates can help to reduce the load on the medium. Broadcasts and multicasts are usually sent at the lowest possible rate in order to reach distant clients; however, this means that they occupy a large slice of medium time. Adjusting this setting can be particularly useful in large networks with a high density of access points.

Configure the broadcast and multicast data rates under **Wireless-LAN** > **WLAN-Networks** > **Rate-Selection**.



Network name

The network or SSID to which the rates configured here should apply. The name must match with a name of a network set up in *Networks*.

Radio band

The band that the rates configured here apply to. This can be further limited to a specific band.

Broadcast-Rate

The rate to use for sending broadcasts.

Multicast-Rate

The rate to use for sending multicasts.

4.1 Additions to the Setup menu

4.1.1 Rate-Selection

Increasing the broadcast and multicast data rates can help to reduce the load on the medium. Broadcasts and multicasts are usually sent at the lowest possible rate in order to reach distant clients; however, this means that they occupy a large slice of medium time. Adjusting this setting can be particularly useful in large networks with a high density of access points. You can set the rates for the WLAN networks in this table.

SNMP ID:

2.20.1111

Console path:

Setup > **WLAN**

Network-Name

The network or SSID to which the rates configured here should apply. The name must match with a name of a network set up in *2.20.1 Network*.

SNMP ID:

2.20.1111.1

Console path:

Setup > **WLAN** > **Rate-Selection**

Possible values:

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

Broadcast-Rate

The rate to use for sending broadcasts.

SNMP ID:

2.20.1111.23

Console path:

Setup > **WLAN** > **Rate-Selection**

Possible values:

default
1MBit
2MBit
5.5MBit
6MBit
9MBit
11MBit
12MBit
18MBit
24MBit
36MBit
48MBit
54MBit

Default:

default

Multicast-Rate

The rate to use for sending multicasts.

SNMP ID:

2.20.1111.24

Console path:

Setup > **WLAN** > **Rate-Selection**

Possible values:

default
1MBit
2MBit
5.5MBit
6MBit
9MBit
11MBit
12MBit
18MBit
24MBit
36MBit
48MBit
54MBit

Default:

default

Radio-Band

The band that the rates configured here apply to. This can be further limited to a specific band.

SNMP ID:

2.20.1111.101

Console path:

Setup > **WLAN** > **Rate-Selection**

Possible values:

2.4GHz+5GHz
2.4 GHz
5 GHz
None

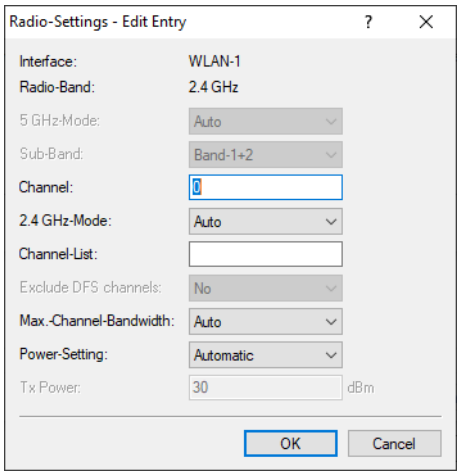
Default:

2.4GHz+5GHz

5 Setting target TX power

From LCOS LX 5.30 you can set the desired target transmission power.

Configure this with LANconfig under **Wireless LAN** > **WLAN-Networks** > **Radio-Settings**.



Power setting

This setting regulates whether to use the maximum permitted transmission power that the access-point hardware can achieve ("Automatic") or to specify the desired target transmission power in manual mode ("Manual"). This is done in dBm in the field **TX Power**.

TX Power

Depending on the setting in the field **Power setting**, you set the transmission power in dBm here.

If the hardware of the access point is not capable of the desired transmission power, the maximum possible value is set automatically.

Under no circumstances will the access point exceed the regulatory limits for transmission power. These are always respected automatically, regardless of the settings made here.

5.1 Additions to the Setup menu

5.1.1 Power-Setting

This setting regulates whether to use the maximum permitted transmission power supported by the hardware of the access point ("Automatic") or whether the desired target transmission power can be specified in the manual mode ("Manual"). This is done in dBm under *2.20.8.34 EIRP* on page 14.

SNMP ID:

2.20.8.33

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

Automatic

Use the maximum permitted transmission power that can be realized by the hardware of the access point.

Manual:

Use the target transmission power specified in dBm under *2.20.8.34 EIRP* on page 14.

If the hardware of the access point is not capable of the desired transmission power, the maximum possible value is set automatically.

Under no circumstances will the access point exceed the regulatory limits for transmission power. These are always respected automatically, regardless of the settings made here.

Default:

Automatic

5.1.2 EIRP

Depending on the setting in *2.20.8.33 Power-Setting* on page 13, you set the transmission power in dBm here.

If the hardware of the access point is not capable of the desired transmission power, the maximum possible value is set automatically.

Under no circumstances will the access point exceed the regulatory limits for transmission power. These are always respected automatically, regardless of the settings made here.

SNMP ID:

2.20.8.34

Console path:

Setup > **WLAN** > **Radio-Settings**

Possible values:

Max. 2 characters from `[0-9]`

6 Wireless ePaper

LANCOM Wireless ePaper Displays provide a variety of options for displaying information. You can automatically and remotely update the calendar schedule for your conference rooms, you can create dynamic notices and direction signs, or you can control the price labels of goods on your shelves from a central location in real time. The wide range of different settings allows you to set up your very own customized use case.

The settings for operating Wireless ePaper Displays are to be found in LANconfig under **Tools** > **Options** > **Wireless ePaper**. Under IP/hostname you enter the IP address and the port of the Wireless ePaper Server. The recommended port number is 8001.

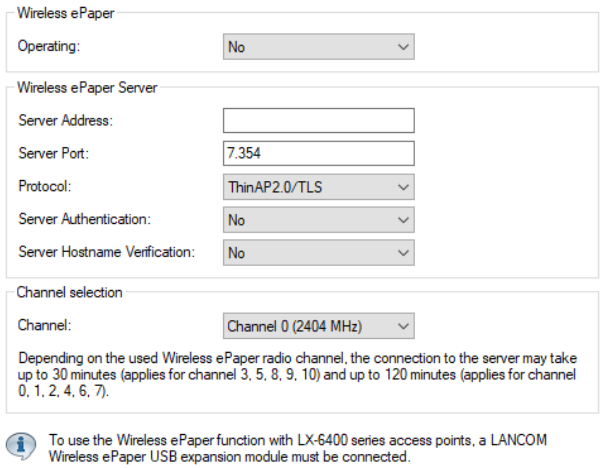
You invoke the Wireless ePaper management in LANconfig under **Tools** > **Start Wireless ePaper management**.

6.1 Settings for Wireless ePaper via LANconfig

Wireless ePaper Displays from LANCOM offer state-of-the-art digital signage for a wide range of applications. The Displays are controlled by an innovative wireless technology with extremely low power consumption.

ePaper operations require the use of a USB-connected LANCOM Wireless ePaper USB expansion module for each device. This is currently supported by the devices LX-6400 and LX-6402.

Activate the Wireless ePaper radio module in LANconfig under **IoT** > **Wireless ePaper**,



Operation

Use this to activate the Wireless ePaper feature in the access point.

The server must be configured for the connection type ThinAP2.0/TCP. Please refer to the *LANCOM Support Knowledge Base* for further information. Use the same method to set the following two configuration options to enable communication between the server and LCOS LX access points:

```
accessPointUseThinMode?value=true
accessPointThinUseOutboundMode?value=true
```

This can be done, for example, with “curl” as follows:

```
curl -X PUT http://localhost:8001/service/configuration/accessPointUseThinMode?value=true
curl -X PUT http://localhost:8001/service/configuration/accessPointThinUseOutboundMode?value=true
```

The legacy connection mode via UDP is not supported by LCOS LX.

Server address

Here you configure the IP address of the Wireless ePaper Server that the access point should contact.

Server port

The TCP destination port to be used for communication with the server.

Protocol

The protocol used to communicate with the server.

Server Authentication

Optionally, the access point can check the server certificate of the Wireless ePaper Server when it connects to it. If this option is enabled, a corresponding CA certificate (or certificate chain) in PEM format must also be loaded onto the access point via WEBconfig.

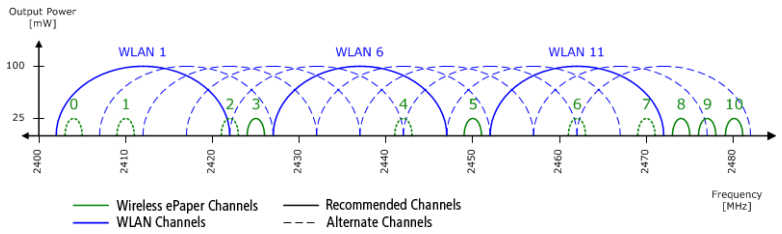
Server Hostname Verification

In connection with the **Server Authentication** option, this setting decides whether the "Common Name" specified in the certificate is checked for a match with the host name of the addressed Wireless ePaper Server.

Channel

Configure the radio channel to be used for controlling the Wireless ePaper Displays.

Depending on the radio channel used, connecting the server to a Display can take up to 30 minutes (channels 3, 5, 8, 9, 10) or up to 120 minutes (channels 0, 1, 2, 4, 6, 7). If possible, you should prefer the channels 3, 5, 8, 9 and 10, as Wireless ePaper Displays scan them more frequently and they do not interfere with the popular Wi-Fi channels 1, 6, and 11.

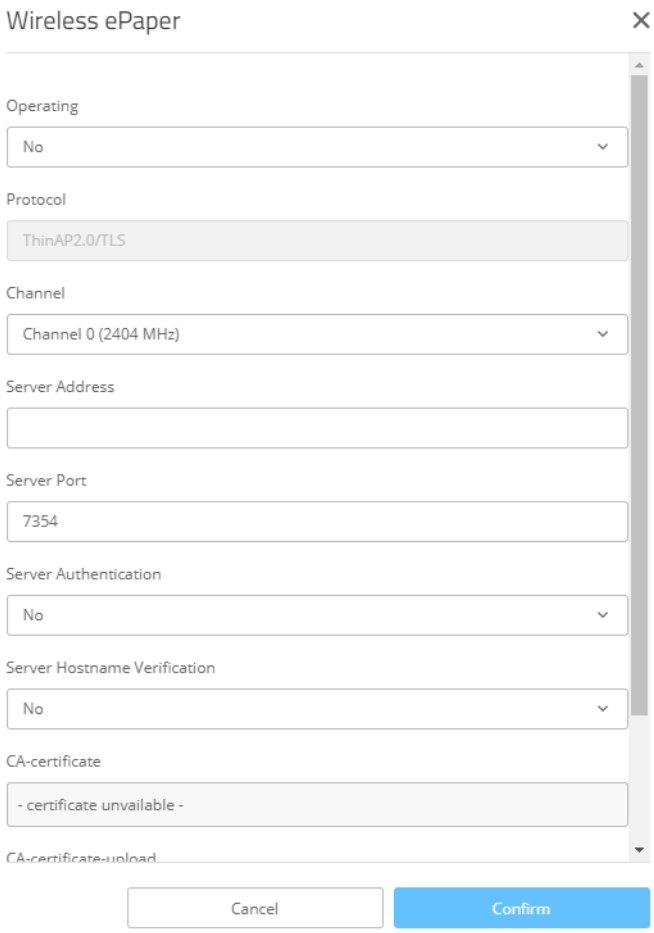


Do not select the same channel for two access points that are in the same area. This causes interference and prevents Displays from joining the network. It is possible to set the same channel on two access points if you are sure that each display is only within range of one of these access points.

6.2 Settings for Wireless ePaper via WEBconfig

LANCOM Wireless ePaper Displays provide a variety of options for displaying information. You can automatically and remotely update the calendar schedule for your conference rooms, you can create dynamic notices and direction signs, or you can control the price labels of goods on your shelves from a central location in real time. The wide range of different settings allows you to set up your very own customized use case.

The settings of the Wireless ePaper in WEBconfig are located under **System configuration** > **Wireless ePaper**.



Operation

Use this to activate the Wireless ePaper feature in the access point.

The server must be configured for the connection type ThinAP2.0/TCP. Please refer to the *LANCOM Support Knowledge Base* for further information. Use the same method to set the following two configuration options to enable communication between the server and LCOS LX access points:

```
accessPointUseThinMode?value=true
accessPointThinUseOutboundMode?value=true
```

This can be done, for example, with "curl" as follows:

```
curl -X PUT http://localhost:8001/service/configuration/accessPointUseThinMode?value=true
curl -X PUT http://localhost:8001/service/configuration/accessPointThinUseOutboundMode?value=true
```

The legacy connection mode via UDP is not supported by LCOS LX.

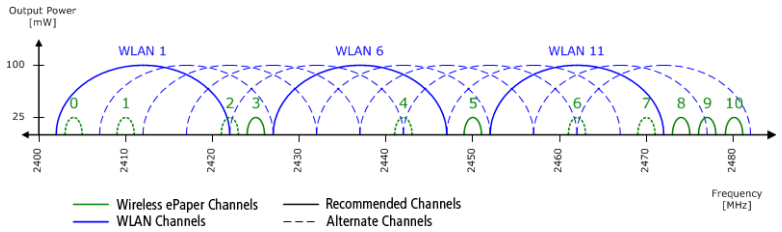
Protocol

The protocol used to communicate with the server.

Channel

Configure the radio channel to be used for controlling the Wireless ePaper Displays.

Depending on the radio channel used, connecting the server to a Display can take up to 30 minutes (channels 3, 5, 8, 9, 10) or up to 120 minutes (channels 0, 1, 2, 4, 6, 7). If possible, you should prefer the channels 3, 5, 8, 9 and 10, as Wireless ePaper Displays scan them more frequently and they do not interfere with the popular Wi-Fi channels 1, 6, and 11.



Do not select the same channel for two access points that are in the same area. This causes interference and prevents Displays from joining the network. It is possible to set the same channel on two access points if you are sure that each display is only within range of one of these access points.

Server address

Here you configure the IP address of the Wireless ePaper Server that the access point should contact.

Server port

The TCP destination port to be used for communication with the server.

Server Authentication

Optionally, the access point can check the server certificate of the Wireless ePaper Server when it connects to it. If this option is enabled, a corresponding CA certificate (or certificate chain) in PEM format must also be loaded onto the access point via WEBconfig.

Server Hostname Verification

In connection with the **Server Authentication** option, this setting decides whether the "Common Name" specified in the certificate is checked for a match with the host name of the addressed Wireless ePaper Server.

CA certificate

If you have uploaded a certificate to the device for server authentication, it will be displayed here.

CA-certificate-upload

If you use server authentication, a CA certificate for server verification must also be uploaded to the device. You can do this here by selecting the certificate file and then uploading it.

6.3 Additions to the Setup menu

6.3.1 IoT

Settings for IoT technologies supported by LCOS LX, such as Wireless ePaper and Bluetooth Low Energy.

SNMP ID:

2.111

Console path:

Setup

Wireless ePaper

Configure the settings for the Wireless ePaper module here.

SNMP ID:

2.111.88

Console path:

Setup > **IoT**

Operating

Use this to activate the Wireless ePaper feature in the access point.

The server must be configured for the connection type ThinAP2.0/TCP. Please refer to the *#unique_30/unique_30_Connect_42_ThinAP2.0TCP* for further information. The legacy connection mode via UDP is not supported by LCOS LX.

SNMP ID:

2.111.88.1

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

No

The Wireless ePaper feature is not enabled.

Yes

The Wireless ePaper feature is enabled.

Default:

No

Channel

Configure the radio channel to be used for controlling the Wireless ePaper Displays.

Depending on the radio channel used, connecting the server to a Display can take up to 30 minutes (channels 3, 5, 8, 9, 10) or up to 120 minutes (channels 0, 1, 2, 4, 6, 7). If possible, you should prefer the channels 3, 5, 8, 9 and 10, as Wireless ePaper Displays scan them more frequently and they do not interfere with the popular Wi-Fi channels 1, 6, and 11.

Do not select the same channel for two access points that are in the same area. This causes interference and prevents Displays from joining the network. It is possible to set the same channel on two access points if you are sure that each display is only within range of one of these access points.

SNMP ID:

2.111.88.2

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

2404 MHz
2410 MHz
2422 MHz
2425 MHz
2442 MHz
2450 MHz
2462 MHz
2470 MHz
2474 MHz
2477 MHz
2480 MHz

Default:

2404 MHz

Server-Address

IP address of the Wireless ePaper Server.

SNMP ID:

2.111.88.3

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

Max. 128 characters from `[A-Z][a-z][0-9].-:%`

Server port

The TCP destination port to be used for communication with the server.

SNMP ID:

2.111.88.4

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

0 … 65535

Default:

7354

Protocol

The protocol used to communicate with the server.

SNMP ID:

2.111.88.5

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

ThinAP2.0/TLS

Default:

ThinAP2.0/TLS

Server-Authentication

Optionally, the access point can check the server certificate of the Wireless ePaper Server when it connects to it. If this option is enabled, a corresponding CA certificate (or certificate chain) in PEM format must also be loaded onto the access point via WEBconfig.

SNMP ID:

2.111.88.6

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

No
Yes

Default:

No

Server-Hostname-Verification

In connection with the option *2.111.88.6 Server-Authentication* on page 21, this setting decides whether the "Common Name" specified in the certificate is checked for a match with the host name of the addressed Wireless ePaper Server.

SNMP ID:

2.111.88.7

Console path:

Setup > **IoT** > **Wireless-ePaper**

Possible values:

No
Yes

Default:

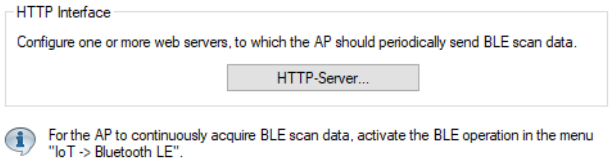
No

7 Location-based services (LBS)

LANCOM access points are able to work as LBS clients with an LBS server. In this case, they report any BLE clients within range to the LBS server, which can then offer location-based services to those clients. As of LCOS LX 5.30, an HTTP interface is supported.

Using the HTTP interface, access points can send LBS data directly to a freely configurable HTTP endpoint. The data is sent in JSON format, which ensures easy processing at the receiving end.

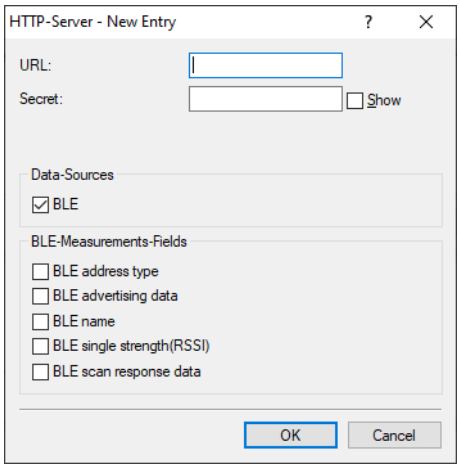
LANconfig: **Miscellaneous Services** > **Location Based Services**



In order for the access point to collect BLE data, the BLE feature has to be switched on separately. Please refer to *Bluetooth Low Energy (BLE)* on page 25 or *Location based services* on page 26.

7.1 HTTP-Server

Under **HTTP-Server** you configure the HTTP endpoints for the LBS data.



URL

Configure the URL of the HTTP endpoint here.

HTTP and HTTPS are supported. If you use HTTPS, a CA certificate for server verification must also be uploaded to the device. This can be done using WEBconfig. See *Location based services* on page 26.

Secret

The secret (key) is transmitted from the access point to the end point in the JSON messages and can additionally be used for message authentication.

Data-Sources

Here you configure the types of LBS data that should be sent. Only BLE is currently available.

BLE-Measurements-Fields

Here you configure which measurement fields or data from the access point should be included in the messages to the HTTP endpoint. In order to minimize the data volume, we recommend that you limit this to essential data only.

Data format of the messages sent to the endpoint

› For **BLE**:

```
{
    "deviceMac": "00A0574C49EB",
    "measurements": [
        {
            "addressType": "Random",
            "deviceAddress": "70CE7B7014EC",
            "name": "",
            "rssi": -93,
            "seenTime": 1599208076493
        },
        {
            "addressType": "Random",
            "deviceAddress": "70CE7B7014EC",
            "name": "",
            "rssi": -93,
            "seenTime": 1599208076494
            "advertisingData": "1eff0600010920024bab81ba8815c5dc61c38449a886740a1ddb09b9e2ad8e",
            "scanResponseData": "050974657374"
        }
    ],
    "secret": "",
    "type": "BLE",
    "version": "1.0"
}
```

version

The version of the API being used. Currently this is always 1.0.

secret

The HTTP server secret specified in the access point configuration.

type

The type of data sent. Can be either WLAN or BLE.

deviceMac

The LAN MAC address of the access point.

measurements

This contains at least one measured value. This could also be a number of measurements.

deviceAddress

The address of the BLE device or client.

seenTime

The time stamp (in Unix time) when the BLE frame from the client was received by the access point.

addressType

The type of BLE address. The following address types are available: `Public` or `Random`.

rssi

The signal strength in dBm of the received BLE frame.

name

The name submitted by the BLE device. Only transmitted if the BLE scanner is activated in the BLE operational settings.

advertisingData

The complete advertisement transmitted by the BLE device.

scanResponseData

The complete scan response transmitted by the BLE device. Only transmitted if the BLE scanner is activated in the BLE operational settings.

7.1.1 Bluetooth Low Energy (BLE)

The settings for Bluetooth Low Energy are located here.

The specific settings for BLE are made in LANconfig under **IoT** > **Bluetooth LE**.

Operation

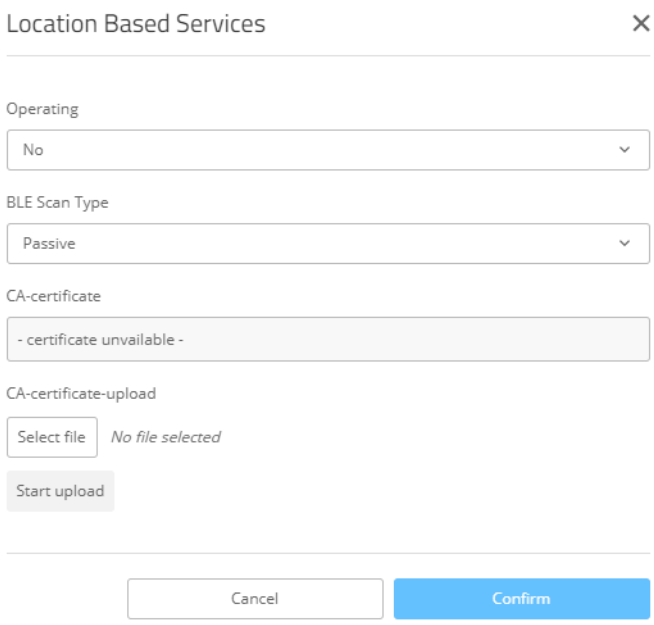
By turning on the BLE radio here, data about the BLE environment is collected continuously.

BLE Scan Type

Choose between a passive and an active scan. The BLE name and a scan response can only be detected in the active scan. Note that BLE clients answering scan requests can increase power consumption.

7.2 Location based services

The settings of the Location Based Services in WEBconfig are located under **System configuration** > **Location Based Services**.



Operation

By turning on the BLE radio here, data about the BLE environment is collected continuously.

BLE Scan Type

Choose between a passive and an active scan. The BLE name and a scan response can only be detected in the active scan. Note that BLE clients answering scan requests can increase power consumption.

CA certificate

If you have uploaded a certificate for the HTTPS protocol to the device, it will be displayed here.

CA-certificate-upload

If you use HTTPS, a CA certificate for server verification must also be uploaded to the device. You can do this here by selecting the certificate file and then uploading it.

7.3 Additions to the Setup menu

7.3.1 LBS

LANCOM access points are able to work as LBS clients with an LBS server. In this case, they report any connected clients to the LBS server, which can then offer location-based services to those clients. As of LCOS LX 5.30, an HTTP interface is supported.

Using the HTTP interface, access points can send LBS data directly to a freely configurable HTTP endpoint. The data is sent in JSON format, which ensures easy processing at the receiving end.

SNMP ID:

2.99

Console path:

Setup

HTTP-Server

Configure the HTTP endpoints for the LBS data here.

SNMP ID:

2.99.1

Console path:

Setup > **LBS**

URL

Configure the URL of the HTTP endpoint here.

HTTP and HTTPS are supported. If you use HTTPS, a CA certificate for server verification must also be uploaded to the device. This can be done using WEBconfig.

SNMP ID:

2.99.1.1

Console path:

Setup > **LBS** > **HTTP-Server**

Possible values:

Max. 251 characters from `URL with http or https`

Secret

The secret (key) is transmitted from the access point to the end point in the JSON messages and can additionally be used for message authentication.

SNMP ID:

2.99.1.3

Console path:

Setup > **LBS** > **HTTP-Server**

Possible values:

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

Data-Sources

Here you configure the types of LBS data that should be sent. Only BLE is currently available.

SNMP ID:

2.99.1.4

Console path:

Setup > **LBS** > **HTTP-Server**

Possible values:

BLE

BLE-Measurements-Fields

Here you configure which measurement fields or data from the access point should be included in the messages to the HTTP endpoint. In order to minimize the data volume, we recommend that you limit this to essential data only.

SNMP ID:

2.99.1.5

Console path:

Setup > **LBS** > **HTTP-Server**

Possible values:

None
BLE-Address-Type-Transmit
BLE-Advertising-Data-Transmit
BLE-Name-Transmit
BLE-RSSI-Transmit
BLE-Scan-Response-Data-Transmit

Operating

By turning on the BLE radio here, data about the BLE environment is collected continuously.

SNMP ID:

2.99.2

Console path:

Setup > **LBS**

Possible values:

No
BLE radio switched off.

Yes
BLE radio switched on.

Default:

No

LBS-Server-Type

Configure the LBS server type here. Currently, only the HTTP API with data packets in JSON format is supported.

SNMP ID:

2.99.3

Console path:

Setup > **LBS**

Possible values:

HTTP-JSON

BLE-Scan-Type

Choose between a passive and an active scan. The BLE name and a scan response can only be detected in the active scan. Note that BLE clients answering scan requests can increase power consumption.

SNMP ID:

2.99.4

Console path:

Setup > **LBS**

Possible values:

Passive
Active

Run-Bluetooth-Scan

Use this action to run a Bluetooth scan.

Example: `do Run-Bluetooth-Scan`

SNMP ID:

2.99.5

Console path:

Setup > **LBS**

Delete-CA-Certificate

This action allows you to delete the certificate used for communication with an HTTPS server.

Example: `do Delete-CA-Certificate`

SNMP ID:

2.99.6

Console path:

Setup > **LBS**

Delete-Scan-Results

Use this action to delete the values of the last Bluetooth scan.

Example: `do Delete-Scan-Results`

SNMP ID:

2.99.7

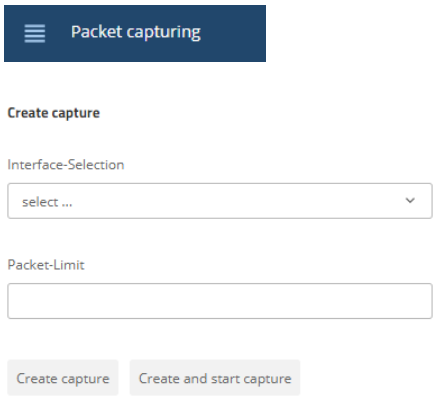
Console path:

Setup > **LBS**

8 Packet capturing in WEBconfig

This item allows you to capture Wireshark-compatible packets.

You reach this section from the sidebar under **Diagnosis** > **Packet capturing**.

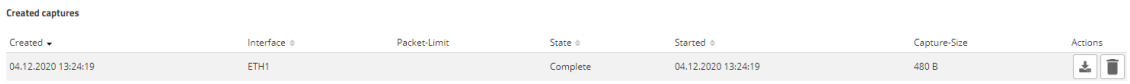


In the section "Created captures" you can specify the interface where packets are to be captured and whether the capture size should be limited by the number of captured packets.

The interfaces available for selection include all Ethernet interfaces as well as active WLAN SSIDs (separated according to frequency band).

Click on **Create capture** and a capture job is created with the chosen settings, but it is not yet started. The capture can then be started at any time from the "Created captures" list. Click on **Create and start capture** to create a capture job with the chosen settings and start it immediately.

Using the "Created captures" list you can start, stop and download captures as a .pcap file.



Capture data is streamed directly from the access point or WEBconfig into the browser's cache. Please note that a capture job that has been started is aborted when you close WEBconfig.

Different capture jobs can be started in parallel.