SECURE. **NETWORKS.**

LCOS LX 5.10

Addendum

02/2020

LANCOM
Systems

Contents

Copyright

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 (*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 5.10

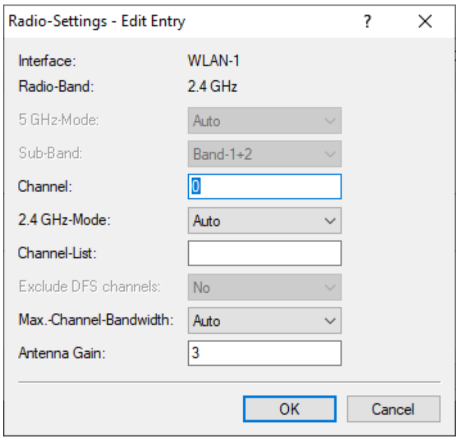
This document describes the changes and enhancements in LCOS LX version 5.10 since the previous version.

2 Wi-Fi 6

WLAN is everywhere these days—the number of users is increasing just as rapidly as the potential applications. Wi-Fi 6 provides not only more speed here, but above all a real increase in average throughput per Wi-Fi client. Thanks to a more efficient use of the available bandwidths and channels, Wi- Fi 6 brings more stability and reliability to intensively used wireless LANs.

LCOS LX access points with Wi-Fi 6 hardware, such as a LANCOM LX-6400, support this standard without further adjustments.

In LANconfig, all settings relating to the physical radio parameters are configured under **Wireless LAN** > **WLAN networks** > **Radio settings**. By default, there is an entry in the table for every physical WLAN radio for modification as required. The following options are relevant to Wi-Fi 6:



Radio-Settings - Edit Entry

Interface:	WLAN-1
Radio-Band:	2.4 GHz
5 GHz-Mode:	Auto
Sub-Band:	Band-1+2
Channel:	0
2.4 GHz-Mode:	Auto
Channel-List:	
Exclude DFS channels:	No
Max.-Channel-Bandwidth:	Auto
Antenna Gain:	3

5 GHz-Mode

Here you configure the mode used for 5-GHz radio operation. This directly affects the available data rates. If a restriction is set here, a client attempting to login triggers a check to see whether the modes used by the client match with those configured here. Depending on this, the login is allowed or denied. The following modes are available:

Auto

All modes supported by the device are used.

11an-mixed

The modes 802.11a and 802.11n are used.

11anac-mixed

The modes 802.11a, 802.11n and 802.11ac are used.

11nac-mixed

The modes 802.11n and 802.11ac are used.

11ac-only

Only the 802.11ac mode is used.

11anacax-mixed

The modes 802.11a, 802.11n, 802.11ac and 802.11ax (Wi-Fi 6) are used.

ⓘ Maximum compatibility and performance is available by setting the mode to **Auto**.

2.4-GHz mode

Here you configure the mode used for 2.4-GHz radio operation. This directly affects the available data rates. If a restriction is set here, a client attempting to login triggers a check to see whether the modes used by the client match with those configured here. Depending on this, the login is allowed or denied. The following modes are available:

Auto

All modes supported by the device are used.

11bg-mixed

The modes 802.11b and 802.11g are used.

11g-only

Only the 802.11g mode is used.

11bgn-mixed

The modes 802.11b, 802.11g and 802.11n are used.

11gn-mixed

The modes 802.11g and 802.11n are used.

11bgnax-mixed

The modes 802.11b, 802.11g, 802.11n and 802.11ax (Wi-Fi 6) are used.

11gnax-mixed

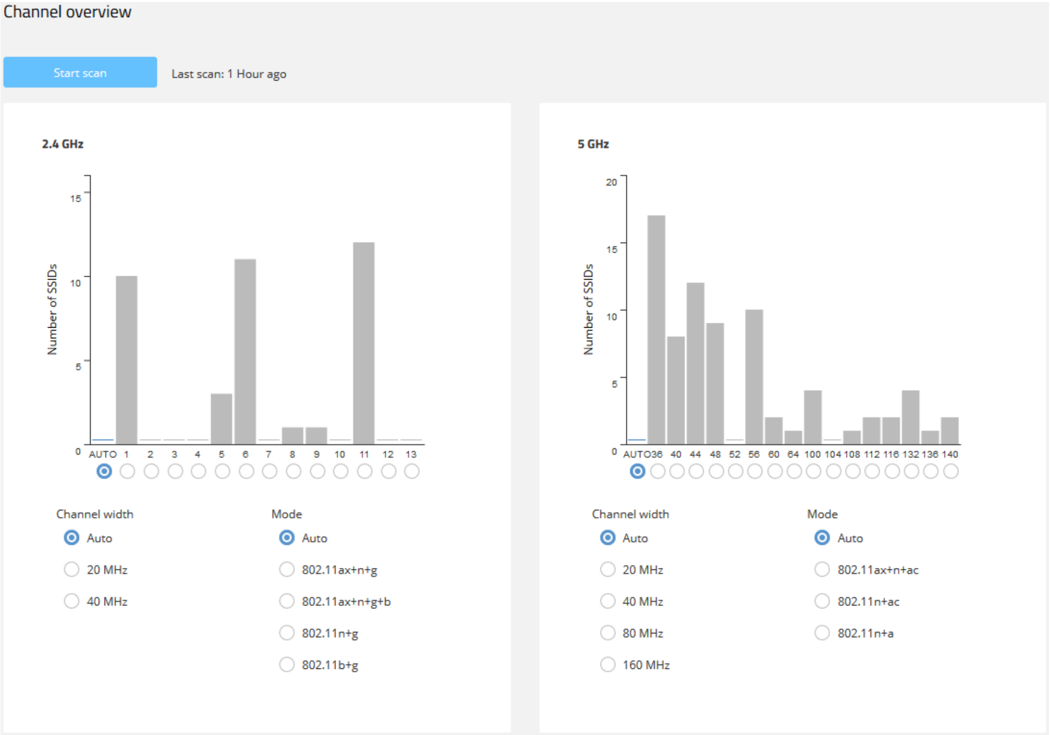
The modes 802.11g, 802.11n and 802.11ax (Wi-Fi 6) are used.

ⓘ Maximum compatibility and performance is available by setting the mode to **Auto**.

In WEBconfig, this is done using settings in the area **Technology** for the particular SSID under **Wi-Fi configuration**:

The **Technology** page offers the option to set fixed channels for the 2.4- and 5-GHz bands, to specify the available channel width and to determine which radio mode is used. The default setting for all options is automatic selection.

The physical settings that can be configured here apply to the entire frequency band and are not SSID-specific.



Channel overview

Start scan

Last scan: 1 Hour ago

2.4 GHz: ● AUTO

Channel width

● Auto

○ 20 MHz

○ 40 MHz

Mode

● Auto

○ 802.11ax+n+g

○ 802.11ax+n+g+b

○ 802.11n+g

○ 802.11b+g

5 GHz: ● AUTO

Channel width

● Auto

○ 20 MHz

○ 40 MHz

○ 80 MHz

○ 160 MHz

Mode

● Auto

○ 802.11ax+n+ac

○ 802.11n+ac

○ 802.11n+a

The two bar charts visualize how many SSIDs the device detected on the various 2.4- and 5-GHz channels, which can represent the potential load on the channels.

The bar charts only contain information if a neighborhood scan has been performed under **Neighborhood**.

2.1 Additions to the Setup menu

2.1.1 5GHz-Mode

Here you configure the mode used for 5-GHz radio operation. This directly affects the available data rates. If a restriction is set here, a client attempting to login triggers a check to see whether the modes used by the client match with those configured here. Depending on this, the login is allowed or denied. The following modes are available:

Maximum compatibility and performance is available by setting the mode to **Auto**.

SNMP ID:

2.20.8.3

Console path:

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

Possible values:

11an-mixed
The modes 802.11a and 802.11n are used.

11anac-mixed
The modes 802.11a, 802.11n and 802.11ac are used.

11nac-mixed
The modes 802.11n and 802.11ac are used.

11ac-only
Only the 802.11ac mode is used.

11anacax-mixed
The modes 802.11a, 802.11n, 802.11ac and 802.11ax (Wi-Fi 6) are used.

Auto
All modes supported by the device are used.

2.1.2 2.4GHz-Mode

Here you configure the mode used for 2.4-GHz radio operation. This directly affects the available data rates. If a restriction is set here, a client attempting to login triggers a check to see whether the modes used by the client match with those configured here. Depending on this, the login is allowed or denied.

ⓘ Maximum compatibility and performance is available by setting the mode to **Auto**.

SNMP ID:

2.20.8.9

Console path:

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

Possible values:

11bg-mixed
The modes 802.11b and 802.11g are used.

11g-only
Only the 802.11g mode is used.

11bgn-mixed
The modes 802.11b, 802.11g and 802.11n are used.

11gn-mixed
The modes 802.11g and 802.11n are used.

11bgnax-mixed
The modes 802.11b, 802.11g, 802.11n and 802.11ax (Wi-Fi 6) are used.

11gnax-mixed
The modes 802.11g, 802.11n and 802.11ax (Wi-Fi 6) are used.

Auto
All modes supported by the device are used.

3 Fast Wi-Fi roaming

Fast roaming as per the WLAN standard IEEE 802.11r allows clients to roam quickly between access points for an optimal wireless LAN user experience.

By operating authentication according to the IEEE 802.1X standard and key management according to the IEEE 802.11i standard, modern WLAN installations offer a high degree of security and confidentiality for the transmitted data. However, these standards require transmission of additional data packets during the connection negotiation as well as additional computing power on the client and server.

IEEE 802.11 originally required up to six data packets to establish a data connection between a WLAN client and an access point. The standard extension IEEE 802.11i improved on weak points of WEP encryption; however, depending on the authentication method, it substantially increased the length of the login process.

This extra time for the WLAN client to login to the access point is not a problem for non-time-critical applications. However, for smooth, loss-free roaming of a WLAN client from one access point to the next, a delay of more than 50 ms is not acceptable. Examples include Voice-over-IP (VoIP) or the application in real-time industrial environments. In this context, roaming means that the network connection passes from one access point to the other without interruption.

Methods such as pair-wise master key caching (PMK caching), pre-authentication, opportunistic key caching (OKC) and the use of central WLAN controllers (WLC) for key management improve the time for the key negotiation between the WLAN client and access point during login. Despite this, the comparatively long time required for key negotiation between the WLAN client and the access point has still not been reduced to a viable extent.

Along with the improved encryption protocols, IEEE 802.11e makes it possible to reserve additional bandwidth with the access point. This allows the WLAN client to prevent interruptions, for example for VoIP connections at times of high network loads at the access point. For roaming from one access point to the next, the WLAN client must again reserve this additional bandwidth on the new access point. However, the additional management frames required for this considerably increase the login time.

The IEEE 802.11r standard provides a simplified authentication process for mobile WLAN clients to roam trouble-free from one access point to the next. The goal is to once again reduce the number of data packets for the login on the access point to the four to six packets known from IEEE 802.11.

Similar to opportunistic key caching (OKC), a centralized key management (preferably by a WLC) supplies the access points connected to it with the credentials of the WLAN clients. In contrast to OKC, the WLAN client performing fast roaming can detect whether the access point supports IEEE 802.11r

Access points managed by the WLC transmit the “mobility domain information element (MDIE)” to inform WLAN clients within range about, among other things, which “mobility group” the access point belongs to. Based on this information, the WLAN client detects whether it belongs to the same domain and can therefore authenticate without delay. This mobility domain is announced to a WLAN client the first time it authenticates at an access point.

The domain identifier and other special keys generated during the initial authentication and transmitted to all managed access points now reduce the stages of negotiation to the desired four to six steps when authenticating at a new access point.

To avoid futile and thus time-wasting login attempts with expired PMKs, IEEE 802.11r provides additional information about the validity periods of keys. In this manner, the client negotiates a new PMK while connected to the current access point. This is also valid on the access point that the WLAN client wants to connect to next.

Additionally, IEEE 802.11r uses “resource requests” to reserve additional bandwidth on the new access point, so that there is no need to cause added delay by transferring unnecessary data packets during the IEEE 802.11e authentication.

ⓘ Older WLAN clients may have trouble establishing a connection to an SSID with enabled 802.11r. Therefore, it is advisable to use two SSIDs here: One SSID for older clients without 802.11r support and another SSID with enabled 802.11r for clients that support 802.11r.

Fast roaming is possible between devices based on LCOS and LCOS LX.

Fast roaming by Inter Access Point Protocol (IAPP)

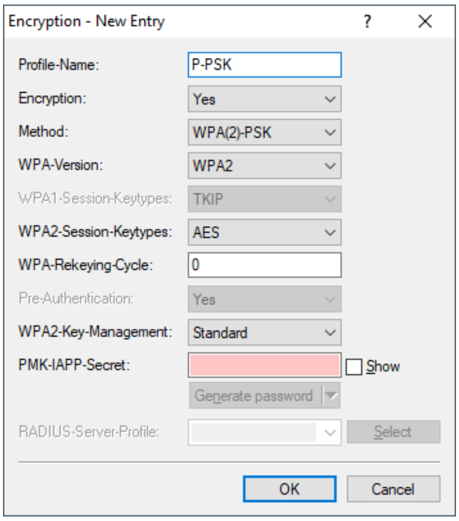
In order to use fast roaming with IAPP, you need to assign an individual IAPP passphrase in the WLAN encryption settings for each interface. This is used to encrypt the pairwise master keys (PMKs). Access points that share a matching IAPP passphrase (PMK-IAPP secret) are able to exchange PMKs between one another and ensure uninterrupted connections. When a client switches to another access point, the new access point sends a handover request to the former access point. The former access point then deletes the client from its station table. The handover request contains the client's MAC address, so that devices in the LAN are informed about the new routing and can update their mapping table.

To enter the IAPP passphrase in LANconfig, navigate to **Wireless LAN** > **General** > **Encryption** > **PMK-IAPP secret**.

Please note that to use Fast Roaming by IAPP, it is necessary to select Fast Roaming in the encryption settings under WPA2 key management.

Configuring fast roaming

In LANconfig the settings for encryption and authentication on the Wi-Fi networks are configured under **Wireless LAN** > **WLAN networks** > **Encryption**.



Profile-Name:	P-PSK
Encryption:	Yes
Method:	WPA(2)-PSK
WPA-Version:	WPA2
WPA1-Session-Keytypes:	TKIP
WPA2-Session-Keytypes:	AES
WPA-Rekeying-Cycle:	0
Pre-Authentication:	Yes
WPA2-Key-Management:	Standard
PMK-IAPP-Secret:	□ Show
	Generate password
RADIUS-Server-Profile:	Select

WPA2 key management

Here you specify which standard the WPA2 key management should follow. Possible values:

Standard

Enables key management according to the IEEE 802.11i standard without Fast Roaming and with keys based on SHA-1. Depending on the configuration, the WLAN clients in this case must use opportunistic key caching, PMK caching or pre-authentication.

Fast roaming

Enables fast roaming according to the IEEE 802.11r standard.

Fast roaming is possible between devices based on LCOS and LCOS LX.

Standard+Fast-Roaming

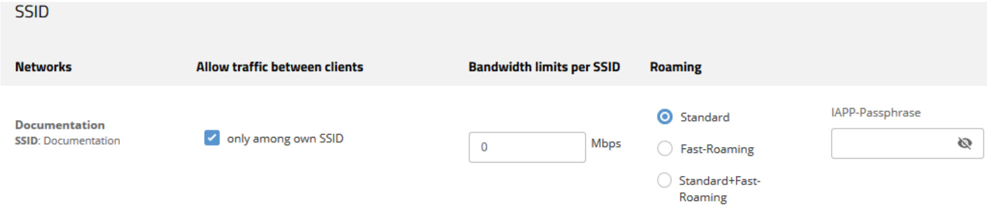
Combination of standard and fast roaming

Although it is possible to make multiple selections, this is advisable only if you are sure that the clients attempting to login to the access point are compatible. Unsuitable clients may refuse a connection if an option other than Standard is enabled.

PMK-IAPP-Secret

This passphrase is used to implement encrypted opportunistic key caching. This is required to use Fast Roaming over IAPP. Each interface must be assigned an individual IAPP passphrase in the WLAN connection settings. This is used to encrypt the pairwise master keys (PMKs). Access points that share a matching IAPP passphrase (PMK-IAPP secret) are able to exchange PMKs between one another and ensure uninterrupted connections. You should therefore ensure that this passphrase is identical on all of the access points that should operate fast roaming.

In WEBconfig, this is done using settings in the area **SSID** under **Wi-Fi configuration**:



SSID

Networks	Allow traffic between clients	Bandwidth limits per SSID	Roaming	
Documentation SSID: Documentation	☑ only among own SSID	0 Mbps	● Standard ○ Fast-Roaming ○ Standard+Fast-Roaming	IAPP-Passphrase

Roaming

Settings for switching a client from one access point to another access point that broadcasts the same SSID.

Standard

Enables key management according to the IEEE 802.11i standard without Fast Roaming and with keys based on SHA-1. Depending on the configuration, the WLAN clients in this case must use opportunistic key caching, PMK caching or pre-authentication.

Fast roaming

Enables fast roaming according to the IEEE 802.11r standard.

Fast roaming is possible between devices based on LCOS and LCOS LX.

Standard+Fast-Roaming

A combination of standard behavior and Fast Roaming.

Although it is possible to make multiple selections, this is advisable only if you are sure that the clients attempting to login to the access point are compatible. Unsuitable clients may refuse a connection if an option other than Standard is enabled.

IAPP passphrase

This passphrase is used to implement encrypted opportunistic key caching. This is required to use Fast Roaming over IAPP. Each interface must be assigned an individual IAPP passphrase in the WLAN connection settings. This is used to encrypt the pairwise master keys (PMKs). Access points that share a matching IAPP passphrase (PMK-IAPP secret) are able to exchange PMKs between one another and ensure uninterrupted connections. You should therefore ensure that this passphrase is identical on all of the access points that should operate fast roaming.

3.1 Additions to the Setup menu

3.1.1 WPA2-Key-Management

Here you specify which standard the WPA2 key management should follow.

SNMP ID:

2.20.3.19

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

Standard

Enables key management according to the IEEE 802.11i standard without Fast Roaming and with keys based on SHA-1. Depending on the configuration, the WLAN clients in this case must use opportunistic key caching, PMK caching or pre-authentication.

Fast roaming

Enables fast roaming according to the IEEE 802.11r standard.

Standard+Fast-Roaming

Combination of standard and fast roaming

Although it is possible to make multiple selections, this is advisable only if you are sure that the clients attempting to login to the access point are compatible. Unsuitable clients may refuse a connection if an option other than Standard is enabled.

3.1.2 PMK-IAPP-Secret

This passphrase is used to implement encrypted opportunistic key caching. This is required to use Fast Roaming over IAPP. Each interface must be assigned an individual IAPP passphrase in the WLAN connection settings. This is used to encrypt the pairwise master keys (PMKs). Access points that share a matching IAPP passphrase (PMK-IAPP secret) are able to exchange PMKs between one another and ensure uninterrupted connections. You should therefore ensure that this passphrase is identical on all of the access points that should operate fast roaming.

SNMP ID:

2.20.3.20

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

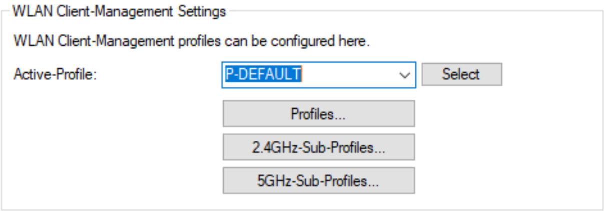
Max. 64 characters from `` [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.` ``

4 Band steering – full bandwidth through intelligent client steering

Band steering offers optimized load balancing across the Wi-Fi by actively redirecting clients to the less congested and higher performance 5-GHz frequency band. Depending on the capabilities of the Wi-Fi client, the access point steers it to the best available frequency band—almost seamlessly thanks to the modern 802.11v technology.

4.1 Client Management

The band steering settings for Wi-Fi networks can be found under **Wireless LAN** > **Client Management**.



WLAN Client-Management Settings

WLAN Client-Management profiles can be configured here.

Active-Profile: P-DEFAULT

Active profile

Here you select the profile with the settings for the band-steering module.

P-DEFAULT

Steering is based on the load on the medium and the interference detected on the current channel and is preferably performed with 802.11v. If the client does not support 802.11v, steering is induced by deliberately disassociating the client. Steering can be performed before association and, if necessary, once the client is already associated. This is the recommended profile.

P-DISABLED

No steering is performed. The client decides independently which frequency band to use.

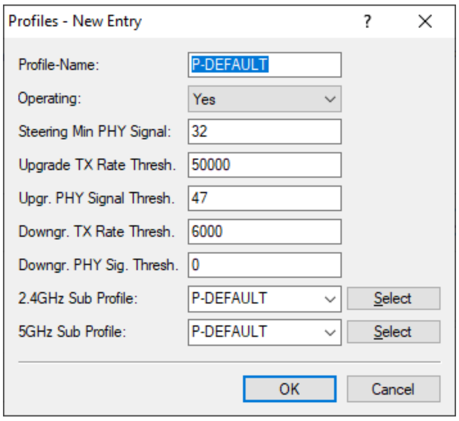
P-LEGACY

Steering is performed before the client associates by deliberately withholding probe responses. Regardless of the load, the 5-GHz band is always preferred.

4.1.1 Profiles

Adjust the detailed settings of the steering profiles or create a new profile under **Wireless LAN** > **Client Management** > **Profiles**.

LANCOM recommends using the preset profiles.



Profiles - New Entry

Profile-Name:	P-DEFAULT
Operating:	Yes
Steering Min PHY Signal:	32
Upgrade TX Rate Thresh.	50000
Upgr. PHY Signal Thresh.	47
Downgr. TX Rate Thresh.	6000
Downgr. PHY Sig. Thresh.	0
2.4GHz Sub Profile:	P-DEFAULT
5GHz Sub Profile:	P-DEFAULT

Profile name

Give this profile a name.

Operation

Controls whether band steering is active for this profile.

Steering min. PHY signal

Specifies the client signal strength (in dB) below which client steering is initiated.

Upgrade TX rate threshold

Specifies the limit value of the transmission rate (in kbps), at which the client should potentially be steered to the 5-GHz band.

Upgrade PHY signal threshold

Specifies the client signal strength (in dB) required as a minimum before the client is considered for steering to the 5-GHz band.

Downgrade TX rate threshold

Specifies the limit value of the transmission rate (in kbps), at which the client should potentially be steered to the 2.4-GHz band.

Downgrade PHY signal threshold

Specifies the client signal strength (in dB) that must be exceeded before the client is considered for steering to the 2.4-GHz band.

For steering to 2.4 GHz (downgrade), the signal strength has to fall below the value configured here and also below the **Downgrade TX rate threshold** value.

2.4-GHz sub-profile

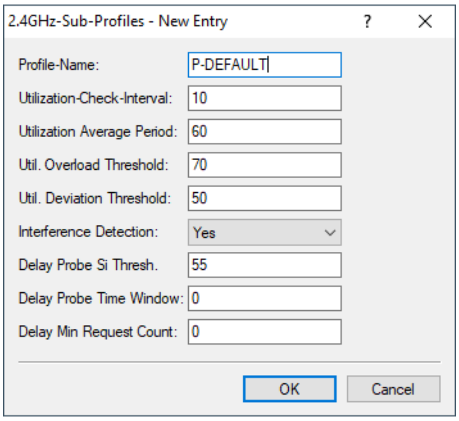
Here you configure which 2.4-GHz sub-profile is used.

5-GHz sub-profile

Here you configure which 5-GHz sub-profile is used.

4.1.2 2.4-GHz sub-profiles

The settings for the 2.4-GHz sub-profiles are located under **Wireless LAN** > **Client Management** > **2.4GHz sub-profiles**.



2.4GHz-Sub-Profiles - New Entry

Profile-Name:	P-DEFAULT
Utilization-Check-Interval:	10
Utilization Average Period:	60
Util. Overload Threshold:	70
Util. Deviation Threshold:	50
Interference Detection:	Yes
Delay Probe Si Thresh.	55
Delay Probe Time Window:	0
Delay Min Request Count:	0

Profile name

Give this 2.4-GHz sub-profile a descriptive name.

Utilization check interval

Configures the interval (in seconds) for checking media utilization.

Utilization average period

Configures the period (in seconds) over which the media utilization is averaged. This value must always be higher than the value configured for the **Utilization check interval**.

Utilization overload threshold

Configures the media utilization (in percent) above which the current 2.4-GHz channel is assumed to be overloaded.

Utilization deviation threshold

Configures the media utilization (in percent) which, together with the expected media utilization, may be reached before any further downgrade steering is stopped (until the next measurement of medium utilization).

Interference detection

Configures whether interference on the configured 2.4-GHz channel is considered for steering decisions.

Delay probe signal threshold

Specifies the client signal strength (in dB) that must be reached before steering-related probe responses are delayed.

Delay probe time window

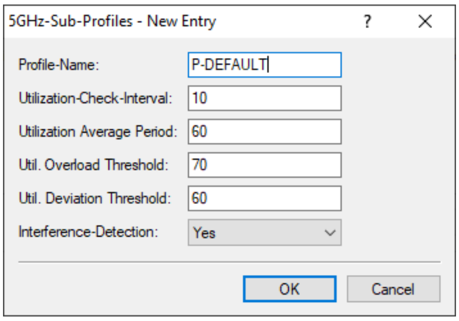
Configures the time window (in seconds) in which a client must receive at least the number of probe requests configured under **Delay min. request count** before it responds to them.

Delay min. request count

Configures the number of probe requests that a client must receive within the period configured under **Delay probe time window** before it responds to them.

4.1.3 5-GHz sub-profiles

The settings for the 5-GHz sub-profiles are located under **Wireless LAN** > **Client Management** > **5 GHz sub-profiles**.



5GHz-Sub-Profiles - New Entry

Profile-Name: P-DEFAULT

Utilization-Check-Interval: 10

Utilization Average Period: 60

Util. Overload Threshold: 70

Util. Deviation Threshold: 60

Interference-Detection: Yes

Profile name

Give this 5-GHz sub-profile a descriptive name.

Utilization check interval

Configures the interval (in seconds) for checking media utilization.

Utilization average period

Configures the period (in seconds) over which the media utilization is averaged. This value must always be higher than the value configured for the **Utilization check interval**.

Utilization overload threshold

Configures the media utilization (in percent) above which the current 5-GHz channel is assumed to be overloaded.

Utilization deviation threshold

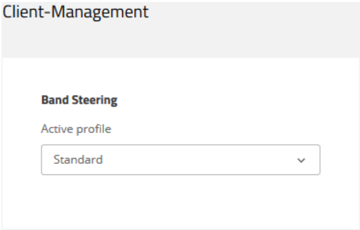
Configures the media utilization (in percent) which, together with the expected media utilization, may be reached before any further downgrade steering is stopped (until the next measurement of medium utilization).

Interference detection

Configures whether interference on the configured 5-GHz channel is considered for steering decisions.

4.2 Setting up client management via WEBconfig

In WEBconfig, this is done using settings in the area **Technology** for the particular SSID under **Wi-Fi configuration**:



Client-Management

Band Steering

Active profile: Standard

Active profile

Select the profile that defines the settings for the band steering module.

Standard

Steering is based on the medium load and the detected interference on the current channel and is preferably done using 802.11v. If the client does not support 802.11v, steering is performed by means of a targeted disassociation of the client. Steering is performed both before association and, if necessary, while the client is already associated. This is the recommended profile.

Ausgeschaltet

No steering is carried out at all. The client decides autonomously which frequency band to choose.

Legacy

Steering takes place before the client is associated by the targeted restraint of probe responses. The 5 GHz band is always preferred regardless of the workload.

4.3 Additions to the Setup menu

4.3.1 Client-Management

Configure the settings for band steering here. Using band steering, clients can be steered from the overloaded 2.4-GHz frequency band to the 5-GHz frequency band, so that more bandwidth is available for the individual client, and the user experience is improved. LCOS LX supports 802.11v standard, which has the option to steer clients to the frequency band that offers them the best signal. Even clients that do not support the 802.11v standard can be steered to the 5-GHz band by deliberately delaying probe responses or by deliberately disconnecting them from the WLAN.

SNMP ID:

2.20.4

Console path:

Setup > **WLAN**

Active-Profile

Here you select the profile with the settings for the band-steering module.

SNMP ID:

2.20.4.1

Console path:

Setup > **WLAN** > **Client-Management**

Possible values:

P-DEFAULT

Steering is based on the load on the medium and the interference detected on the current channel and is preferably performed with 802.11v. If the client does not support 802.11v, steering is induced by deliberately disassociating the client. Steering can be performed before association and, if necessary, once the client is already associated. This is the recommended profile.

P-LEGACY

Steering is performed before the client associates by deliberately withholding probe responses. Regardless of the load, the 5-GHz band is always preferred.

P-DISABLED

No steering is performed. The client decides independently which frequency band to use.

<Custom>

In addition to the existing profiles, you can also define your own profiles under **Profiles**.

Default:

P-DEFAULT

Profiles

Here you adjust the detailed settings of the steering profiles or you can create a new profile.

SNMP ID:

2.20.4.2

Console path:

Setup > **WLAN** > **Client-Management**

Profile-Name

The name of the profile.

SNMP ID:

2.20.4.2.1

Console path:

Setup > **WLAN** > **Client-Management** > **Profiles**

Possible values:

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

Operating

Controls whether band steering is active for this profile.

SNMP ID:

2.20.4.2.2

Console path:

Setup > **WLAN** > **Client-Management** > **Profiles**

Possible values:

No
Band steering is not active.

Yes
Band steering is active.

Steering-Min-PHY-Signal

Specifies the client signal strength (in dB) below which client steering is initiated.

SNMP ID:

2.20.4.2.3

Console path:

Setup > **WLAN** > **Client-Management** > **Profiles**

Possible values:

Max. 10 characters from `[0-9]`

Upgrade-TX-Rate-Threshold

Specifies the limit value of the transmission rate (in kbps), at which the client should potentially be steered to the 5-GHz band.

SNMP ID:

2.20.4.2.4

Console path:

Setup > **WLAN** > **Client-Management** > **Profiles**

Possible values:

Max. 10 characters from `[0-9]`

Upgrade-PHY-Signal-Threshold

Specifies the client signal strength (in dB) required as a minimum before the client is considered for steering to the 5-GHz band.

SNMP ID:

2.20.4.2.5

Console path:

Setup > **WLAN** > **Client-Management** > **Profiles**

Possible values:

Max. 10 characters from `[0-9]`

Downgrade-TX-Rate-Threshold

Specifies the limit value of the transmission rate (in kbps), at which the client should potentially be steered to the 2.4-GHz band.

SNMP ID:

2.20.4.2.6

Console path:

Setup > **WLAN** > **Client-Management** > **Profiles**

Possible values:

Max. 10 characters from `[0-9]`

Downgrade-PHY-Signal-Threshold

Specifies the client signal strength (in dB) that must be exceeded before the client is considered for steering to the 2.4-GHz band.

For steering to 2.4 GHz (downgrade), the signal strength has to fall below the value configured here and also below the **Downgrade TX rate threshold** value.

SNMP ID:

2.20.4.2.7

Console path:

Setup > **WLAN** > **Client-Management** > **Profiles**

Possible values:

Max. 10 characters from `[0-9]`

2.4GHz-Sub-Profile

Here you configure which 2.4-GHz sub-profile is used.

SNMP ID:

2.20.4.2.8

Console path:

Setup > **WLAN** > **Client-Management** > **Profiles**

Possible values:

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

5GHz-Sub-Profile

Here you configure which 5-GHz sub-profile is used.

SNMP ID:

2.20.4.2.9

Console path:

Setup > **WLAN** > **Client-Management** > **Profiles**

Possible values:

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

2.4GHz-Sub-Profiles

Configure the settings of the 2.4-GHz sub-profile here.

SNMP ID:

2.20.4.3

Console path:

Setup > **WLAN** > **Client-Management**

Profile-Name

The profile name of the 2.4-GHz sub-profile.

SNMP ID:

2.20.4.3.1

Console path:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Possible values:

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

Utilization-Check-Interval

Configures the interval (in seconds) for checking media utilization.

SNMP ID:

2.20.4.3.2

Console path:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Possible values:

Max. 10 characters from `[0-9]`

Utilization-Average-Period

Configures the period (in seconds) over which the media utilization is averaged. This value must always be higher than the value configured for the Utilization check interval.

SNMP ID:

2.20.4.3.3

Console path:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Possible values:

Max. 10 characters from `[0-9]`

Utilization-Overload-Threshold

Configures the media utilization (in percent) above which the current 2.4-GHz channel is assumed to be overloaded.

SNMP ID:

2.20.4.3.4

Console path:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Possible values:

0 … 100

Utilization-Deviation-Threshold

Configures the media utilization (in percent) which, together with the expected media utilization, may be reached before any further downgrade steering is stopped (until the next measurement of medium utilization).

SNMP ID:

2.20.4.3.5

Console path:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Possible values:

0 … 100

Interference-Detection

Configures whether interference on the configured 2.4-GHz channel is considered for steering decisions.

SNMP ID:

2.20.4.3.6

Console path:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Possible values:

No

Do not take interference into account.

Yes

Take interference into account.

Delay-Probe-PHY-Signal-Threshold

Specifies the client signal strength (in dB) that must be reached before steering-related probe responses are delayed.

SNMP ID:

2.20.4.3.7

Console path:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Possible values:

Max. 10 characters from `[0-9]`

Delay-Probe-Time-Window

Configures the time window (in seconds) in which a client must receive at least the number of probe requests configured under **Delay probe min. request count** before it responds to them.

SNMP ID:

2.20.4.3.8

Console path:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Possible values:

Max. 10 characters from `[0-9]`

Delay-Probe-Min-Request-Count

Configures the number of probe requests that a client must receive within the period configured under **Delay probe time window** before it responds to them.

SNMP ID:

2.20.4.3.9

Console path:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Possible values:

Max. 10 characters from `[0-9]`

5GHz-Sub-Profiles

Configure the settings of the 5-GHz sub-profile here.

SNMP ID:

2.20.4.4

Console path:

Setup > **WLAN** > **Client-Management**

Profile-Name

The profile name of the 5-GHz sub-profile.

SNMP ID:

2.20.4.4.1

Console path:

Setup > **WLAN** > **Client-Management** > **5GHz-Sub-Profiles**

Possible values:

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

Utilization-Check-Interval

Configures the interval (in seconds) for checking media utilization.

SNMP ID:

2.20.4.4.2

Console path:

Setup > **WLAN** > **Client-Management** > **5GHz-Sub-Profiles**

Possible values:

Max. 10 characters from `[0-9]`

Utilization-Average-Period

Configures the period (in seconds) over which the media utilization is averaged. This value must always be higher than the value configured for the Utilization check interval.

SNMP ID:

2.20.4.4.3

Console path:

Setup > **WLAN** > **Client-Management** > **5GHz-Sub-Profiles**

Possible values:

Max. 10 characters from `[0-9]`

Utilization-Overload-Threshold

Configures the media utilization (in percent) above which the current 5-GHz channel is assumed to be overloaded.

SNMP ID:

2.20.4.4.4

Console path:

Setup > **WLAN** > **Client-Management** > **5GHz-Sub-Profiles**

Possible values:

0 … 100

Utilization-Deviation-Threshold

Configures the media utilization (in percent) which, together with the expected media utilization, may be reached before any further downgrade steering is stopped (until the next measurement of medium utilization).

SNMP ID:

2.20.4.4.5

Console path:

Setup > **WLAN** > **Client-Management** > **5GHz-Sub-Profiles**

Possible values:

0 … 100

Interference-Detection

Configures whether interference on the configured 5-GHz channel is considered for steering decisions.

SNMP ID:

2.20.4.4.6

Console path:

Setup > **WLAN** > **Client-Management** > **5GHz-Sub-Profiles**

Possible values:

No

Do not take interference into account.

Yes

Take interference into account.

5 LANCOM Enhanced Passphrase Security User (LEPS-U)

LANCOM Enhanced Passphrase Security Users (LEPS-U) allows a set of passphrases to be configured and assigned to individual users or groups. This avoids having one global passphrase for an SSID. Instead, there are several passphrases, which can then be distributed individually.

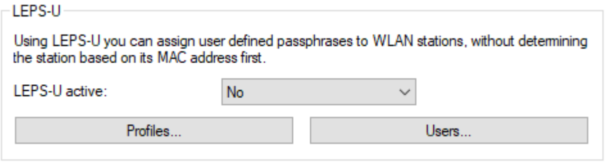
This is useful for onboarding devices into the network. For example, a network operator “onboarding” multiple WLAN devices into different areas of the network does not want to configure each specific device; instead this should done by the users of the devices themselves. In this case, users are given a preshared key for the company WLAN for use with their own devices. The configuration of LEPS-U takes place on the infrastructure side only, so assuring full compatibility to third-party products.

The security issue presented by global passphrases is fundamentally remedied by LEPS-U. Each user is assigned their own individual passphrase. If a passphrase assigned to a user should “get lost” or an employee with knowledge of their passphrase leaves the company, then only the passphrase of that user needs to be changed or deleted. All other passphrases remain valid and confidential.

For technical reasons, LEPS-U is only compatible with WPA version WPA2.

5.1 Stations/LEPS

The configuration of the **Profiles** and **Users** for LANCOM Enhanced Passphrase Security User (LEPS-U) are located in LANconfig under **Wireless LAN** > **Stations/LEPS** > **LEPS-U**. LEPS-U is enabled/disables with the switch **LEPS-U active**.


LEPS-U

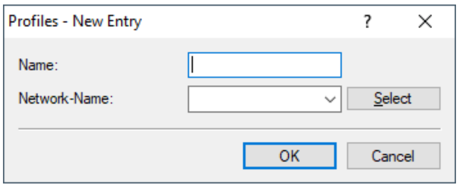
Using LEPS-U you can assign user defined passphrases to WLAN stations, without determining the station based on its MAC address first.

LEPS-U active: No

When configuring LEPS-U, each user who should be able to authenticate client devices on the Wi-Fi receives an individual passphrase. LEPS-U profiles are used to avoid having to repeat all of the settings for every new user. You then create the LEPS-U users with their individual passphrases and link them to one of the LEPS-U profiles created previously.

5.1.1 Profiles

Configure LEPS-U profiles here and link them to an SSID. You can then assign the LEPS-U profiles to the LEPS-U users.


Profiles - New Entry

Name:

Network-Name:

Name

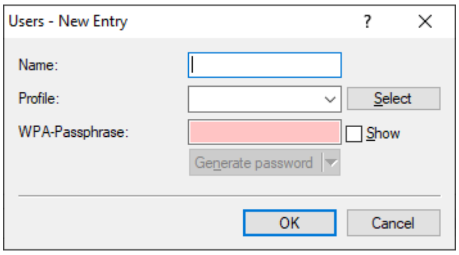
Enter a unique name for the LEPS-U profile here.

Network name

Here you select the SSID or, in the case of a WLC, the logical WLAN network for which the LEPS-U profile applies. The only users who can authenticate at the SSID or, in the case of a WLC, at the logical WLAN network are those who are connected to it via the LEPS-U profile.

5.1.2 Users

Create individual LEPS-U users here. Each LEPS-U user must be linked with a previously created profile and assigned an individual WPA passphrase. Any client can then use this passphrase to authenticate at the SSID specified in the corresponding profile. The user is identified by the passphrase used.



Name

Enter a unique name for the LEPS-U user here.

Profile

Select the profile for which the LEPS-U user is valid. The only users who can authenticate at the SSID are those who are connected to it via the LEPS-U profile.

WPA passphrase

Here you can specify the passphrase to be used by LEPS-U users to authenticate at the WLAN.

The passphrase can be a string of 8 to 64 characters. We recommend that the passphrases consist of a random string at least 32 characters long.

5.2 Additions to the Setup menu

5.2.1 LEPS-U

LANCOM Enhanced Passphrase Security User (LEPS-U) lets you assign custom passphrases to WLAN stations without having to pre-register stations by their MAC address.

SNMP ID:

2.20.133

Console path:

Setup > **WLAN**

Operating

Switches LEPS-U on or off. When switched off, LEPS-U users are ignored during WLAN client authentication.

SNMP ID:

2.20.133.1

Console path:

Setup > **WLAN** > **LEPS-U**

Possible values:

No
Yes

Default:

No

Profiles

Configure LEPS-U profiles here and link them to an SSID. You can then assign the LEPS-U profiles to the LEPS-U users. You can overwrite the profile values for any particular user with individual values.

SNMP ID:

2.20.133.2

Console path:

Setup > **WLAN** > **LEPS-U**

Name

Enter a unique name for the LEPS-U profile here.

SNMP ID:

2.20.133.2.1

Console path:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Possible values:

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

Network-Name

Here you select the SSID or, in the case of a WLC, the logical WLAN network for which the LEPS-U profile is valid. The only users who can authenticate at the SSID or, in the case of a WLC, at the logical WLAN network are those who are connected to it via the LEPS-U profile.

SNMP ID:

2.20.133.2.2

Console path:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Possible values:

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

Users

Create individual LEPS-U users here. Every LEPS-U user must be connected to a profile that was created previously.

SNMP ID:

2.20.133.3

Console path:

Setup > **WLAN** > **LEPS-U**

Name

Enter a unique name for the LEPS-U user here.

SNMP ID:

2.20.133.3.1

Console path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

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

Profiles

Select the profile for which the LEPS-U user is valid. The only users who can authenticate at the SSID are those who are connected to it via the LEPS-U profile.

SNMP ID:

2.20.133.3.2

Console path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

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

WPA-Passphrase

Here you can specify the passphrase to be used by LEPS-U users to authenticate at the WLAN.

SNMP ID:

2.20.133.3.3

Console path:

Setup > **WLAN** > **LEPS-U** > **Users**

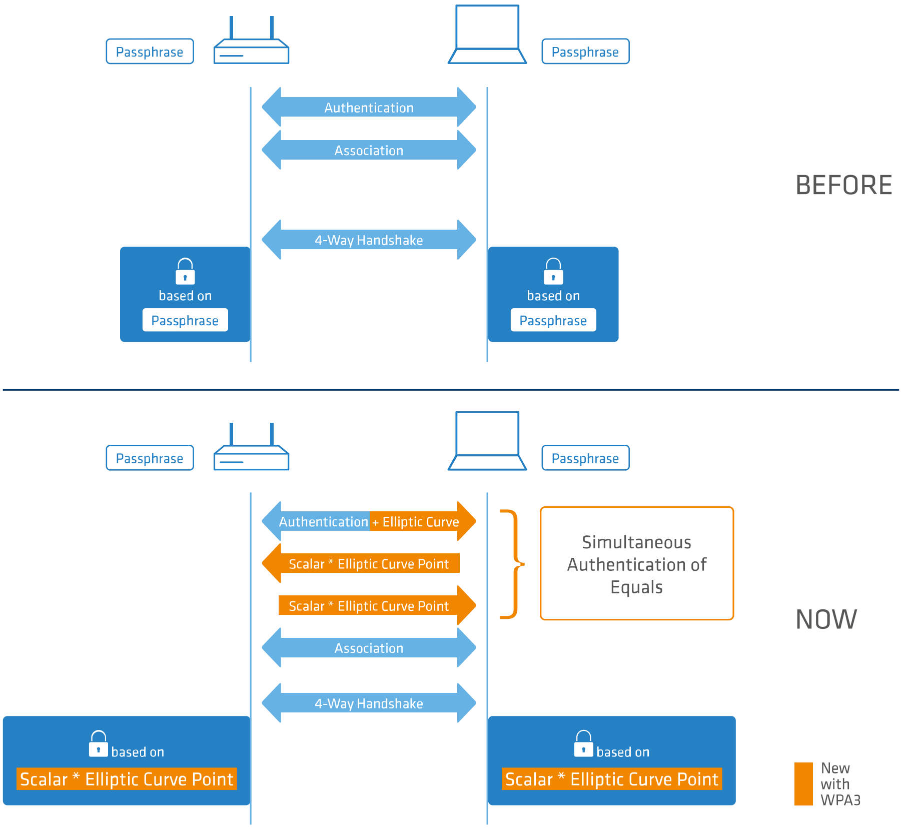
Possible values:

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

6 WPA3 (Wi-Fi Protected Access 3)

Compared to the predecessor standard WPA2 introduced by the Wi-Fi Alliance in 2004, the WPA3 standard introduced in 2018 offers improved security by combining various security methods. Like WPA2, WPA3 also exists in the versions WPA3-Personal and WPA3-Enterprise.

WPA3-Personal uses the Simultaneous Authentication of Equals (SAE) authentication method, which only requires a password for authentication but which prevents brute-force and dictionary attacks. Furthermore, for the first time this method offers forward secrecy, i.e. captured WPA3-secured traffic cannot be decrypted subsequently after the attacker gains knowledge of the pre-shared key.


Passphrase
Passphrase
Authentication
Association
4-Way Handshake
based on
Passphrase
based on
Passphrase
BEFORE
Passphrase
Passphrase
Authentication + Elliptic Curve
Scalar * Elliptic Curve Point
Scalar * Elliptic Curve Point
Simultaneous Authentication of Equals
Association
4-Way Handshake
NOW
based on
Scalar * Elliptic Curve Point
based on
Scalar * Elliptic Curve Point
New with WPA3

In addition, the WPA3-Enterprise uses the Commercial National Security Algorithm (CNSA) Suite B cryptography. Suite B ensures that all links in the encryption chain match with one another. Suite B forms classes of bit lengths for hashed, symmetric, and asymmetric encryption in order to provide suitable levels of protection. For example, an SHA-2 hash with 256 bits matches AES with 128 bits. Where Suite B is operated, the support of all other combinations is expressly excluded. Consequently, the encryption chain consists of links of equal strength.

Both variants now require the use of protected management frames (PMF) according to IEEE 802.11w. PMF prevents attackers from computing the WLAN password from captured material gained by using fake management frames to force a disassociation and then eavesdropping the re-authentication.

6.1 WPA3-Personal

In the WLAN encryption settings under **Wireless LAN** > **WLAN networks** > **Encryption**, the WPA versions **WPA3** and **WPA2/3** are available for selection.

With **WPA3** selected, only WLAN clients that support WPA3-Personal will be able to login. This configuration enforces authentication with the Simultaneous Authentication of Equals (SAE). Similarly, this SSID enforces the use of PMF (Protected Management Frames as per IEEE 802.11w), a mandatory part of WPA3.

By selecting **WPA2/3**, these two versions of WPA are offered in parallel. This option allows clients that only support WPA2 to operate in parallel with clients that already support WPA3. For WPA3-compatible WLAN clients, this configuration enforces the use of PMF; for WPA2-compatible WLAN clients, PMF is offered as an option for backwards compatibility.

6.2 WPA3-Enterprise

WPA3-Enterprise does not fundamentally change or replace the protocols defined in WPA2-Enterprise. Rather, it set out policies to ensure greater consistency in the application of these protocols and to assure the desired level of security.

In the WLAN encryption settings under **Wireless LAN** > **WLAN networks** > **Encryption**, the WPA versions **WPA3** and **WPA2/3** are available for selection.

By selecting **WPA3**, only WLAN clients that support WPA3-Enterprise will be able to log in. This SSID enforces the use of PMF (Protected Management Frames as per IEEE 802.11w), a mandatory part of WPA3.

By selecting **WPA2/3**, these two versions of WPA are offered in parallel. This option allows clients that only support WPA2 to operate in parallel with clients that already support WPA3. For WPA3-compatible WLAN clients, this configuration enforces the use of PMF; for WPA2-compatible WLAN clients, PMF is offered as an option for backwards compatibility.

Suite B cryptography

In addition, the WPA3-Enterprise uses the Commercial National Security Algorithm (CNSA) Suite-B cryptography. Suite B ensures that all links in the encryption chain match with one another. Suite B forms classes of bit lengths for hashed, symmetric, and asymmetric encryption in order to provide suitable levels of protection. For example, an SHA-2 hash with 256 bits matches AES with 128 bits. Where Suite B is operated, the support of all other combinations is expressly excluded. Consequently, the encryption chain consists of links of equal strength.

ⓘ Further information on CNSA Suite B can be found at the following link: *CNSA algorithm suite factsheet*

Use of the following EAP cipher suites are enforced:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

ⓘ Other cipher suites can no longer be used. Also enforced are a minimum key length of 3072 bits for the RSA and Diffie-Hellman key exchange, as well as 384 bits for the ECDSA and ECDHE key exchange. The session key type AES-GCMP-256 is also enforced.

! If these cipher suites are not supported by the WLAN clients or the remaining infrastructure (e.g. the RADIUS server), then no connection is possible!

ⓘ The RADIUS server integrated in the LCOS supports the cipher suites mentioned here.

6.3 Configuring WPA3

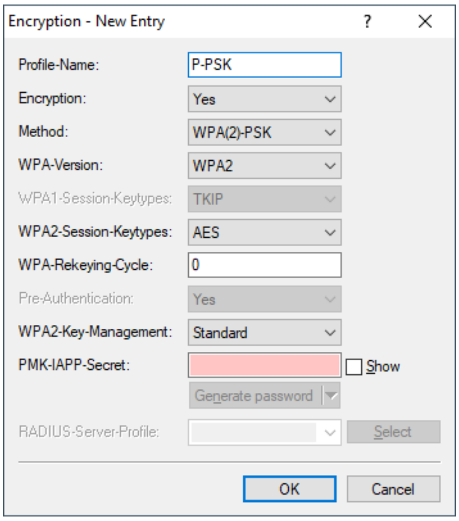
In LANconfig, all of the necessary settings for WPA3 are located under **Wireless LAN** > **WLAN Networks** > **Encryption**. The following encryption profiles have been added and are used to configure the Wi-Fi networks.

P-PSK-WPA2-3

The authentication method used is WPA2 and/or WPA3 with pre-shared key (PSK), also known as WPA-Personal. A key must be configured for the WLAN network.

P-PSK-WPA3

The authentication method used is WPA3 with pre-shared key (PSK), also known as WPA3-Personal. A key must be configured for the WLAN network.



Encryption - New Entry

Profile-Name:	P-PSK
Encryption:	Yes
Method:	WPA(2)-PSK
WPA-Version:	WPA2
WPA1-Session-Keytypes:	TKIP
WPA2-Session-Keytypes:	AES
WPA-Rekeying-Cycle:	0
Pre-Authentication:	Yes
WPA2-Key-Management:	Standard
PMK-IAPP-Secret:	□ Show
RADIUS-Server-Profile:	

Method

Here you configure the encryption method. The following methods are available:

WPA

- WPA(2/3)-PSK: WPA2 and/or WPA3 with pre-shared key (PSK), also known as WPA-Personal.
- WPA(2/3)-802.1X: WPA2 and/or WPA3 with 802.1X, also known as WPA-Enterprise

> Note that 802.1X requires a RADIUS server profile to be specified as well.

WEP

> The WEP process no longer provides adequate security and should only be used to integrate legacy clients that do not support a newer security method. If this is the case, we recommend that you isolate the WEP clients in their own VLAN to keep them separate from the rest of the WLAN infrastructure.

- WEP-40-Bits: WEP with 40-bits key length
- WEP-104-Bits: WEP with 104-bits key length
- WEP-128-Bits: WEP with 128-bits key length
- WEP-40-Bits-802.1X: WEP with 40-bits key length and 802.1X

! Note that 802.1X requires a RADIUS server profile to be specified as well.

- WEP-104-Bits-802.1X: WEP with 104-bits key length and 802.1X

! Note that 802.1X requires a RADIUS server profile to be specified as well.

- WEP-128-Bits-802.1X: WEP with 128-bits key length and 802.1X

! Note that 802.1X requires a RADIUS server profile to be specified as well.

WPA-Version

Wi-Fi Protected Access (WPA) is an encryption method. Here you configure the WPA version used for the encryption methods WPA(2)-PSK and WPA(2)-802.1X. The following versions are available:

- WPA1: WPA version 1 is used exclusively.
- WPA2: WPA version 2 is used exclusively.
- WPA3: WPA version 3 is used exclusively.
- WPA1/2: Whether the encryption method WPA 1 or 2 is used depends on the capabilities of the client.
- WPA2/3: Whether the encryption method WPA 2 or 3 is used depends on the capabilities of the client.

WPA2/3-Session-Keytypes

Here you configure the session key type to be used for WPA version 2 and 3. This also influences the encryption method used. The following types are available:

TKIP

TKIP encryption is used.

AES

AES encryption is used.

TKIP/AES

Whether the encryption method TKIP or AES is used depends on the capabilities of the client.

ⓘ Employing TKIP is only recommended for operating older WLAN clients which do not support AES.

ⓘ If a WLAN network uses only WEP or WPA with TKIP for encryption, the WLAN clients connected to it achieve a maximum gross data rate of 54 Mbps.

Encrypt management frames

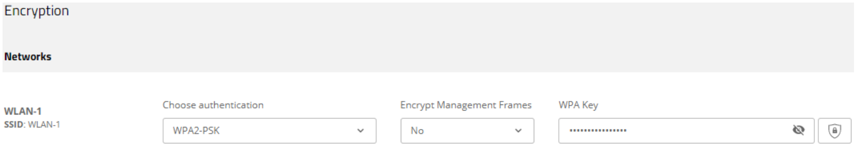
By default, the management information transmitted on a WLAN for establishing and operating data connections is unencrypted. Anybody within a WLAN cell can receive this information, even those who are not associated with an access point. Although this does not entail any risk for encrypted data connections, the injection of fake management information could severely disturb the communications within a WLAN cell.

The IEEE 802.11w standard encrypts this management information (protected management frames, PMF), meaning that potential attackers can no longer interfere with the communications if they don’t have the corresponding key.

ⓘ As of WPA3, management frames have to be encrypted, so this value is ignored there and is assumed to be set as “Mandatory”. For WPA2, this is optional.

In WEBconfig, this is done using settings in the area **Encryption** for the particular SSID under **Wi-Fi configuration**:

Here you can set the parameters for each SSID as follows:



Encryption

Networks

	Choose authentication	Encrypt Management Frames	WPA Key
WLAN-1 SSID: WLAN-1	WPA2-PSK	No	················

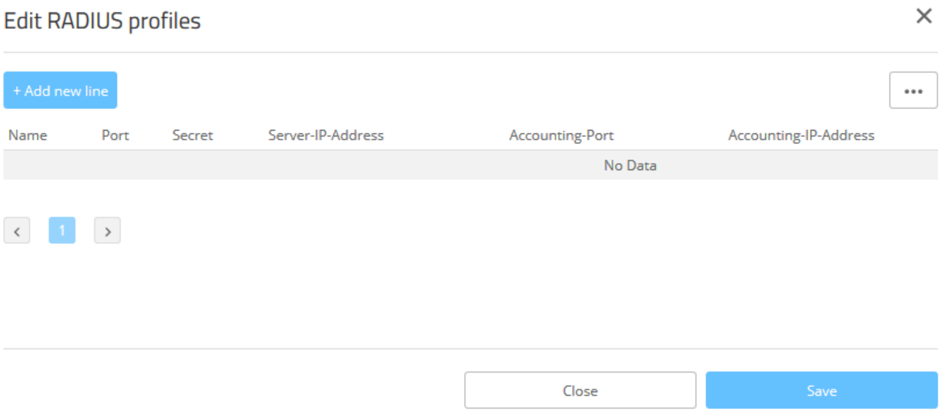
Select authentication

Change the encryption and authentication method here. WPA2-PSK (WPA2 with pre-shared key or WPA2-Personal) is preset by default. Optionally select **No encryption** or one of the following options:

- WPA3-PSK – WPA3 with pre-shared key or WPA3-Personal
- WPA(2+3)-PSK – WPA2 and/or WPA3 with pre-shared key
- WPA2-801.1X– WPA2 with 802.1X or WPA2-Enterprise
- WPA3-801.1X– WPA3 with 802.1X or WPA3-Enterprise
- WPA(2+3)-801.1X– WPA2 and/or WPA3 with 802.1X

ⓘ When using methods requiring a pre-shared key (PSK), you need to enter a **WPA key**. You can read the key by clicking on the crossed-out eye symbol. Depending on your needs, you can automatically generate a secure WPA key (⛉).

ⓘ In the case of 802.1X you have to create a RADIUS profile. To do this, click on **Edit RADIUS profile** and add a new line there.



Edit RADIUS profiles

Name	Port	Secret	Server-IP-Address	Accounting-Port	Accounting-IP-Address
		No Data			

Name

Choose a meaningful name for the RADIUS server profile here. This internal identifier is used to reference the RADIUS server profile from other parts of the configuration.

Port

Select the port (UDP) used to contact the RADIUS server.

ⓘ This is usually the port 1812 (RADIUS authentication).

Secret

Here you configure the secret used to encrypt the traffic between the device and the RADIUS server. This secret must also be stored on the RADIUS server.

Server IP address

Here you configure the host name or IP address where the RADIUS server is to be reached.

Accounting port

Select the port (UDP) used to contact the RADIUS accounting server.

This is usually the port 1813 (RADIUS accounting).

Accounting IP address

Here you configure the host name or IP address where the RADIUS accounting server is to be reached.

Please note that the RADIUS server generally has to be notified about the RADIUS client by means of an entry in its configuration.

Store your changes by clicking on **Save.**

Encrypt management frames

By default, the management information transmitted on a WLAN for establishing and operating data connections is unencrypted. Anybody within a WLAN cell can receive this information, even those who are not associated with an access point. Although this does not entail any risk for encrypted data connections, the injection of fake management information could severely disturb the communications within a WLAN cell.

The IEEE 802.11w standard encrypts this management information (protected management frames, PMF), meaning that potential attackers can no longer interfere with the communications if they don't have the corresponding key.

As of WPA3, management frames have to be encrypted, so the value there is ignored and is assumed to be set as **Mandatory**. For WPA2, this is optional.

6.4 Additions to the Setup menu

6.4.1 Method

Here you configure the encryption method.

The WEP process no longer provides adequate security and should only be used to integrate legacy clients that do not support a newer security method. If this is the case, we recommend that you isolate the WEP clients in their own VLAN to keep them separate from the rest of the WLAN infrastructure.

SNMP ID:

2.20.3.4

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

WEP-40-Bits

AES with 40 bits key length

WEP-104-Bits

AES with 104 bits key length

WEP-128-Bits

AES with 128 bits key length

WEP-40-Bits-802.1X

AES with 40 bits key length and 802.1X

! Note that 802.1X requires a RADIUS server profile to be specified as well.

WEP-104-Bits-802.1X

AES with 104 bits key length and 802.1X

! Note that 802.1X requires a RADIUS server profile to be specified as well.

WEP-128-Bits-802.1X

AES with 128 bits key length and 802.1X

! Note that 802.1X requires a RADIUS server profile to be specified as well.

802.11i-WPA-PSK

WPA(2) with Pre-Shared-Key

802.11i-WPA-802.1X

WPA(2) with 802.1X

! Note that 802.1X requires a RADIUS server profile to be specified as well.

Enhanced-Open

Until now, hotspots were mainly operated without encryption, meaning that the data transmitted over the wireless interface was open to inspection. What also offers only limited security is the widespread practice of securing a hotspot with WPA2-PSK and publicly announcing the shared key, for example, on a poster. Since WPA2-PSK does not offer Perfect Forward Secrecy, an attacker who knows this key can use it to subsequently decrypt recordings of secure data traffic. The Enhanced Open method minimizes these risks. Clients that support this method use encrypted communication to prevent other users in the same radio cell from eavesdropping on their communications. The threat of a man-in-the-middle attack remains, but the risk is much lower than when using an unencrypted open hotspot. Just set the encryption method. That is all you need to do to encrypt communications for clients that support this method.

6.4.2 WPA-Version

Here you configure the WPA version used for the encryption methods **802.11i WPA-PSK** and **802.11i WPA 802.1X**.

SNMP ID:

2.20.3.9

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

WPA1
WPA version 1 is used exclusively.

WPA2
WPA version 2 is used exclusively.

WPA3
WPA version 3 is used exclusively.

WPA1/2
Whether the encryption method WPA 1 or 2 is used depends on the capabilities of the client.

WPA2/3
Whether the encryption method WPA 2 or 3 is used depends on the capabilities of the client.

6.4.3 WPA2-3-Session-Keytypes

Here you configure the session key type to be used for WPA version 2. This also influences the encryption method used.

ⓘ Operating TKIP is only recommended when using older WLAN clients which do not support AES.

ⓘ If a WLAN network uses only WEP or WPA with TKIP for encryption, the WLAN clients connected to it achieve a maximum gross data rate of 54 Mbps.

SNMP ID:

2.20.3.13

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

TKIP
TKIP encryption is used.

AES
AES encryption is used.

TKIP/AES
Whether the encryption method TKIP or AES is used depends on the capabilities of the client.

6.4.4 Prot.-Mgmt-Frames

By default, the management information transmitted on a WLAN for establishing and operating data connections is unencrypted. Anybody within a WLAN cell can receive this information, even those who are not associated with an access point. Although this does not entail any risk for encrypted data connections, the injection of fake management information could severely disturb the communications within a WLAN cell.

The IEEE 802.11w standard encrypts this management information (protected management frames, PMF), meaning that potential attackers can no longer interfere with the communications if they don’t have the corresponding key.

As of WPA3, management frames have to be encrypted, so this value is ignored there and is assumed to be set as “Mandatory”. For WPA2, this is optional.

SNMP ID:

2.20.3.14

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

No

Do not use PMF.

optional

Offer PMF. The client decides whether to use them.

mandatory

Use PMF

6.4.5 SAE/OWE-Groups

Contains the selection of the available Diffie-Hellman groups as a bit mask used by the protocol partners to create a key for exchanging data. The available groups use elliptical curves

The authentication method SAE (Simultaneous Authentication of Equals) used by WPA3 uses these methods together with AES to generate a cryptographically strong key.

SNMP ID:

2.20.3.26

Console path:

Setup > **WLAN** > **Encryption**

Possible values:

DH-19

Bit 0x80000 (524288) – 256-bit random ECP group

DH-20

Bit 0x100000 (1048576) – 384-bit random ECP group

DH-21

Bit 0x200000 (2097152) – 521-bit random ECP group

Default:

DH-19

7 Auto updater – always up-to-date

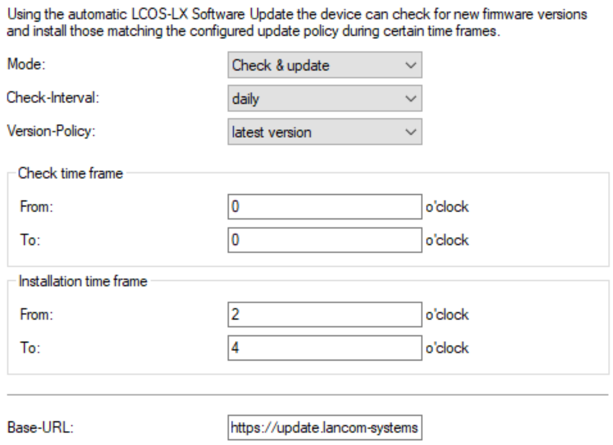
The Auto Updater keeps your installations up-to-date automatically: LCOS LX-based devices can search for new software updates, and download and install them without any user interaction. You can choose whether to install only security updates, release updates, or all updates automatically. If automatic updates are not desired, the feature can still be used to check for new updates, which can then be installed with a single click.

7.1 Software update

The LANCOM Auto Updater allows the automatic updating of on-site LANCOM devices without further user intervention. LANCOM devices can search for new software updates, and download and install them without any user interaction. You can choose whether to install security updates, release updates, or all updates automatically. If you choose not to use automatic updates, the feature can still be used to check for the availability of new updates.

The LANCOM Auto Updater contacts the LANCOM update server to check for updates and firmware downloads. Communication is based on HTTPS. When contacting the server, the LANCOM device uses previously installed TLS certificates for validation. Furthermore, the firmware files for current LANCOM devices are signed. The LANCOM Auto Updater validates this signature before uploading any firmware.

The configuration for the LANCOM Auto Updater in LANconfig is located under **Management** > **Software update**.



Using the automatic LCOS-LX Software Update the device can check for new firmware versions and install those matching the configured update policy during certain time frames.

Mode: Check & update

Check-Interval: daily

Version-Policy: latest version

Check time frame

From: 0 o'clock

To: 0 o'clock

Installation time frame

From: 2 o'clock

To: 4 o'clock

Base-URL: https://update.lancom-systems

Mode

Set the operating mode here. The following modes are supported:

Check & update

- The Auto Updater regularly checks the update server for new updates.
- The update server uses the **update policy** to find the most suitable update, it sets the time to download and install the update within a time frame configured by the user, and it sends the update to the Auto Updater.
- The firmware is installed in test mode. After installation, the Auto Updater performs a connection check. Here, the device checks whether a connection can be established to the update server to ensure that Internet access is still available. If the update server is contacted successfully, the test mode terminates and the firmware goes into regular operation. If the update server cannot be contacted, then Internet

access is assumed to be impossible and the second (i.e. the previously active) firmware will be started again.

Check

- The Auto Updater regularly checks the update server for new updates.
- The availability of a new update is signaled to the user in the LCOS LX menu tree and via syslog.
- Users can manually use the Auto Updater to initiate the latest available update.

ⓘ A manual update is started with the following entry on the command line:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Manual

- The Auto Updater only checks for new updates when prompted by the user.
- Users can manually use the Auto Updater to initiate the latest available update.

ⓘ A manual update is started with the following entry on the command line:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Check interval

This decides whether checks for an available update are performed daily or weekly.

Update policy

Latest version

Always the newest version, irrespective of the release version. Example: 10.20 Rel is installed; an update to 10.20 RU1 is performed, but also to 10.30 Rel. Updates always go to the latest version, but not back to a previous release.

Current version

The latest RU/SU/PR within a release. Example: 10.20 Rel is installed; an update to 10.20 RU1 is performed, but not to 10.30 Rel.

Security patches only

The latest SU within a release. Example: 10.20 Rel is installed; an update to 10.20 SU1 is performed, but not to 10.20 RU2.

Latest version w/o REL

The newest RU/SU/PR, irrespective of the release version. Updates are only performed if a RU is available. Example: Any version of 10.20 is installed; an update to 10.30 RU1 is performed, but not to 10.30 REL.

Check time frame

Set the time frame for checking and downloading new updates here. The daily start and end time for this time frame can be set to the hour. The default value for both of these is 0, so checks for updates and downloads can be started at any time of day. The Auto Updater schedules a random time for update checks and downloads within the configured time frame.

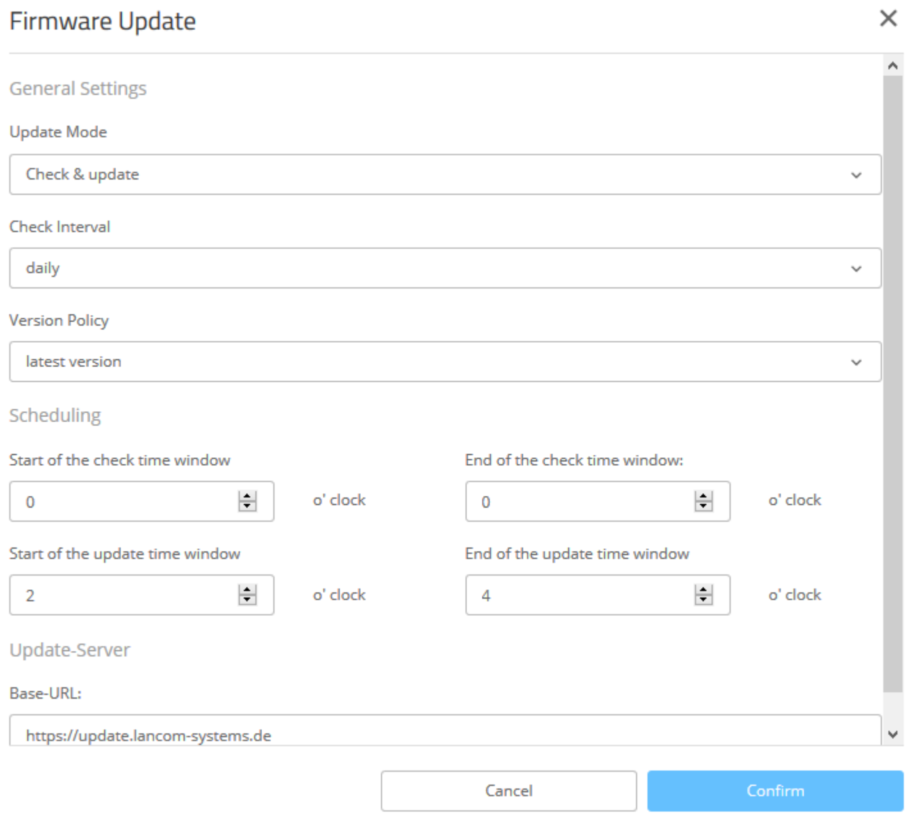
Installation time frame

Set the time frame for update installations here. The daily start and end time for this time frame can be set to the hour. The default setting specifies a time frame between 2:00 AM and 4:00 AM. If an update is found, it will be installed during this time and the device will be restarted to activate the update. The Auto Updater schedules a random time for the installation within the configured time frame.

Base URL

Specifies the URL of the server that provides the latest firmware versions.

7.2 Automatic firmware update



Firmware Update

General Settings

Update Mode: Check & update

Check Interval: daily

Version Policy: latest version

Scheduling

Start of the check time window: 0 o' clock

End of the check time window: 0 o' clock

Start of the update time window: 2 o' clock

End of the update time window: 4 o' clock

Update-Server

Base-URL: https://update.lancom-systems.de

Update mode

Set the operating mode here. The following modes are supported:

Check & update

- The Auto Updater regularly checks the update server for new updates.
- The update server uses the **update policy** to find the most suitable update, it sets the time to download and install the update within a time frame configured by the user, and it sends the update to the Auto Updater.
- The firmware is installed in test mode. After installation, the Auto Updater performs a connection check. Here, the device checks whether a connection can be established to the update server to ensure that Internet access is still available. These attempts continue for several minutes to allow for VDSL synchronization or WWAN connection setup. If the update server is contacted successfully, the test mode terminates and the firmware goes into regular operation. If the update server cannot be contacted, then Internet access is assumed to be impossible and the second (i.e. the previously active) firmware will be started again.

Check

- The Auto Updater regularly checks the update server for new updates.
- The availability of a new update is signaled to the user in the LCOS LX menu tree and via syslog.
- Users can manually use the Auto Updater to initiate the latest available update.

A manual update is started with the following entry on the command line:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Manual

- The Auto Updater only checks for new updates when prompted by the user.
- Users can manually use the Auto Updater to initiate the latest available update.

A manual update is started with the following entry on the command line:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Check interval

This decides whether checks for an available update are performed daily or weekly.

Update policy

Latest version

Always the newest version, irrespective of the release version. Example: 4.00 Rel is installed; an update to 4.00 RU1 is performed, but also to 5.00 Rel. Updates always go to the latest version, but not back to a previous release.

Current version

The latest RU/SU/PR within a release. Example: 4.00 Rel is installed; an update to 4.00 RU1 is performed, but not to 5.00 Rel.

Security patches only

The latest SU within a release. Example: 4.00 Rel is installed; an update to 4.00 SU1 is performed, but not to 4.00 RU2.

Latest version w/o REL

The newest RU/SU/PR, irrespective of the release version. Updates are only performed if a RU is available. Example: Any version of 4.00 is installed; an update to 5.00 RU1 is performed, but not to 5.00 REL.

Check time window

Set the time frame for checking and downloading new updates here. The daily start and end time for this time frame can be set to the hour. The default value for both of these is 0, so checks for updates and downloads can be started at any time of day. The Auto Updater schedules a random time for update checks and downloads within the configured time frame.

Update time window

Set the time frame for update installations here. The daily start and end time for this time frame can be set to the hour. The default setting specifies a time frame between 2:00 AM and 4:00 AM. If an update is found, it will be installed during this time and the device will be restarted to activate the update. The Auto Updater schedules a random time for the installation within the configured time frame.

Base URL

Specifies the URL of the server that provides the latest firmware versions.

7.3 Additions to the Setup menu

7.3.1 Automatic-Firmware-Update

The LANCOM Auto Updater allows on-site LANCOM devices to be updated automatically without further user intervention (unattended). LANCOM Devices can search for new software updates, and download and install them without any user interaction. You can choose whether to install security updates, release updates, or all updates automatically. If you choose not to use automatic updates, the feature can still be used to check for the availability of new updates.

The LANCOM Auto Updater contacts the LANCOM update server to check for updates and firmware downloads. Communication is based on HTTPS. When contacting the server, the LANCOM device uses previously installed TLS certificates for validation. Furthermore, the firmware files for current LANCOM devices are signed. The LANCOM Auto Updater validates this signature before uploading any firmware.

SNMP ID:

2.107

Console path:

Setup

Mode

Set the operating mode of the LANCOM Auto Updater.

SNMP ID:

2.107.1

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

manual

The Auto Updater only checks for new updates when prompted by the user.

Users can manually use the Auto Updater to initiate the latest available update.

check

The Auto Updater regularly checks the LANCOM update server for new updates. The availability of a new update is signaled to the user in the LCOS LX menu tree and via syslog. Users can manually use the Auto Updater to initiate the latest available update.

check-and-update

The Auto Updater regularly checks the LANCOM update server for new updates. The update server uses the version policy to find the most suitable update, it sets the time to download and install the update within a time frame configured by the user, and it sends the update to the Auto Updater. The firmware is installed in test mode. After installation, the Auto Updater performs a connection check. Here, the device checks whether a connection can be established to the update server to ensure that Internet access is still available. If the update server is contacted successfully, the test mode terminates and the firmware goes into regular operation. If the update server cannot be contacted, then Internet access is assumed to be impossible and the second (i.e. the previously active) firmware will be started again.

Default:

check-and-update

Check-Firmware-Now

This command triggers the device to check the LANCOM update server for new firmware.

SNMP ID:

2.107.2

Console path:

Setup > **Automatic-Firmware-Update**

Update-Firmware-Now

This command triggers the device to download and install the latest firmware from the LANCOM update server.

SNMP ID:

2.107.3

Console path:

Setup > **Automatic-Firmware-Update**

Cancel-Current-Action

This command triggers the device to abort any current actions by the Auto Updater. This applies to manually started and scheduled actions.

SNMP ID:

2.107.4

Console path:

Setup > **Automatic-Firmware-Update**

Reset-Updater-Config

This command resets the boot-persistent configuration files that are created by the Auto Updater. This includes the local blacklist of firmware versions that failed an automatic update.

SNMP ID:

2.107.5

Console path:

Setup > **Automatic-Firmware-Update**

Base-URL

Specifies the URL of the server that provides the latest firmware versions.

SNMP ID:

2.107.6

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

Max. 252 characters from `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

Default:

https://update.lancom-systems.de

Check-Interval

After booting, the Auto Updater sets a random time period within a day or a week for the check to be performed. The update itself is performed in the next time period between 02:00 - 04:00 (default).

SNMP ID:

2.107.7

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

daily
weekly

Default:

daily

Version-Policy

Set the version policy of the LANCOM Auto Updater. This controls which firmware versions are offered to update a device.

SNMP ID:

2.107.8

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

latest

Always the newest version, irrespective of the release version. Example: 4.00 Rel is installed; an update to 4.00 RU1 is performed, but also to 5.00 Rel. Updates always go to the latest version, but not back to a previous release.

current

The latest RU/SU/PR within a release. Example: 4.00 Rel is installed; an update to 4.00 RU1 is performed, but not to 5.00 Rel.

security-updates-only

The latest SU within a release. Example: 4.00 Rel is installed; an update to 4.00 SU1 is performed, but not to 4.00 RU2.

latest-without-REL

The newest RU/SU/PR, irrespective of the release version. Updates are only performed if a RU is available. Example: Any version of 4.00 is installed; an update to 5.00 RU1 is performed, but not to 5.00 REL.

Default:

security-updates-only

Check-Time-Begin

The hour of the day at the start of the time interval when checks are made to see whether a firmware update is available and, if applicable, downloaded. The start and end are 0 by default, so checks for updates and downloads can be started at any time of day. The Auto Updater schedules a random time for update checks and downloads within the configured time frame.

SNMP ID:

2.107.10

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

0 … 23

Default:

0

Check-Time-End

The hour of the day at the end of the time interval when checks are made to see whether a firmware update is available and, if applicable, downloaded. The start and end are 0 by default, so checks for updates and downloads can be started at any time of day. The Auto Updater schedules a random time for update checks and downloads within the configured time frame.

SNMP ID:

2.107.11

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

0 … 23

Default:

0

Install-Time-Begin

The hour of the day at the start of the time interval during which a firmware update is installed. The default is between 2 and 4 o'clock in the morning. After installation, the device reboots.

SNMP ID:

2.107.12

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

0 … 23

Default:

2

Install-Time-End

The hour of the day at the end of the time interval during which a firmware update is installed. The default is between 2 and 4 o'clock in the morning. After installation, the device reboots.

SNMP ID:

2.107.13

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

0 … 23

Default:

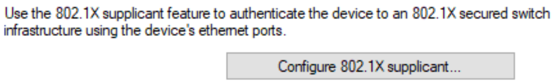
4

8 802.1X supplicant, LAN-side

As of LCOS LX 5.10 you can configure the access point so that it authenticates at a switch infrastructure secured by 802.1X.

8.1 802.1X supplicant

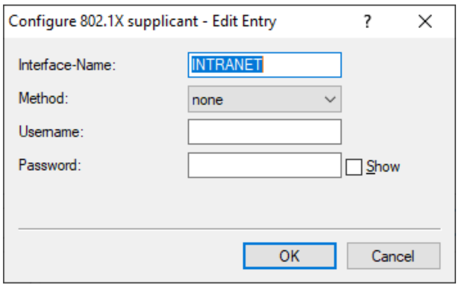
These are the settings for the 802.1X supplicant functionality, which authenticates the device towards the LAN at a switch infrastructure secured by 802.1X. These are located under **Management** > **802.1X supplicant**.



Use the 802.1X supplicant feature to authenticate the device to an 802.1X secured switch infrastructure using the device's ethernet ports.

8.1.1 Configuring the 802.1X supplicant

You configure the 802.1X supplicant functionality under **Management** > **802.1X supplicant** > **Configure 802.1X supplicant**.



Configure 802.1X supplicant - Edit Entry

Interface-Name: INTRANET

Method: none

Username:

Password: □ Show

Interface name

The name of the LAN interface. Currently there is only the interface INTRANET, and this cannot be changed.

Method

The EAP method used to authenticate at the 802.1X infrastructure.

User name

The user name to use to authenticate at the 802.1X infrastructure.

Password

The password to use to authenticate at the 802.1X infrastructure.

ⓘ Support for authentication by means of client certificates will follow in a future LCOS LX version.

8.2 Additions to the Setup menu

8.2.1 Supplicant-Ifc-Setup

These are the settings for the 802.1X supplicant functionality, which authenticates the device towards the LAN at a switch infrastructure secured by 802.1X.

SNMP ID:

2.30.11

Console path:

Setup > **IEEE802.1X**

Interface-Name

The name of the LAN interface. Currently there is only the interface INTRANET, and this cannot be changed.

SNMP ID:

2.30.11.1

Console path:

Setup > **IEEE802.1X** > **Supplicant-Ifc-Setup**

Possible values:

Max. 64 characters from `INTRANET`

Method

The EAP method used to authenticate at the 802.1X infrastructure.

SNMP ID:

2.30.11.2

Console path:

Setup > **IEEE802.1X** > **Supplicant-Ifc-Setup**

Possible values:

None
MD5
TTLS/MD5
TTLS/PAP
TTLS/CHAP
TTLS/MSCHAPv2
TTLS/MSCHAP
PEAP/GTC
PEAP/MSCHAPv2

Username

The user name to use to authenticate at the 802.1X infrastructure.

SNMP ID:

2.30.11.3

Console path:

Setup > **IEEE802.1X** > **Supplicant-Ifc-Setup**

Possible values:

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

Password

The password to use to authenticate at the 802.1X infrastructure.

SNMP ID:

2.30.11.4

Console path:

Setup > **IEEE802.1X** > **Supplicant-Ifc-Setup**

Possible values:

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

9 SNMPv3 with LANmonitor

SNMPv3 (Simple Network Management Protocol Version 3) with LANmonitor provides professional network monitoring. It offers convenient and yet high-security device monitoring thanks to encrypted data communication in LANmonitor.

If, after updating a LANCOM LW-500 from LCOS LX 4.00 to LCOS LX 5.10, the new SNMPv3 feature is to be used in conjunction with the root user (e.g. by LANmonitor), it is necessary to set the main device password on the device again. This can be done either via WEBconfig, LANconfig or the CLI. The background is that for use with SNMPv3, the main device password must be stored in the device in a form compatible with SNMPv3 as a hash value. This is done by setting the password again.

This process is only necessary once when upgrading from LCOS LX 4.00 to a higher version. This is not necessary for future upgrade steps. Especially to enable the use of LANmonitor, the described steps are required!

9.1 Simple Network Management Protocol (SNMP)

9.1.1 SNMPv3 basics

The SNMP protocol structure has changed significantly with version 3. SNMPv3 is now divided into a number of modules with clearly defined interfaces that communicate with one another. The three main elements in SNMPv3 are “Message Processing and Dispatch (MPD)”, “User-based Security Model (USM)” and “View-based Access Control Mechanism (VACM)”.

MPD

The MPD module is responsible for the processing and dispatch of inbound and outbound SNMP messages.

USM

The USM module manages security features that ensure the authentication of the users and the encryption and integrity of the data. SNMPv3 introduced the principle of the “security model”, so that the SNMP configuration in LCOS LX primarily uses the security model “SNMPv3”. However, for compatibility reasons it may be necessary to also take the versions SNMPv2c or even SNMPv1 into account, and to select these as the “security model” accordingly.

VACM

VACM ensures that the sender of an SNMP request is entitled to receive the requested information. The associated access permissions are found in the following settings and parameters:

SNMPv3-Views

“SNMPv3-Views” collect together the content, status messages, and actions of the Management Information Base (MIB) that are permitted to receive or execute an SNMP request. These views can be single values, but also complete paths of the MIB. This content is specified by the OIDs of the MIB entries.

In this way, a successfully authenticated sender of an SNMP request only has access to that data specified in the applicable SNMPv3 views.

SNMPv3-Groups

“SNMPv3-Groups” collect users with the same permissions into a specific group.

Security-Levels

“Security levels” relate to the exchange of SNMP messages. The following levels can be selected:

NoAuth-NoPriv

The SNMP request is valid without the use of specific authentication methods. Authentication merely requires the user to belong to an SNMP community (for SNMPv1 and SNMPv2c) or to specify a valid user name (for SNMPv3). Data transfer is not encrypted.

Auth-NoPriv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, but data transfer is not encrypted.

Auth-Priv

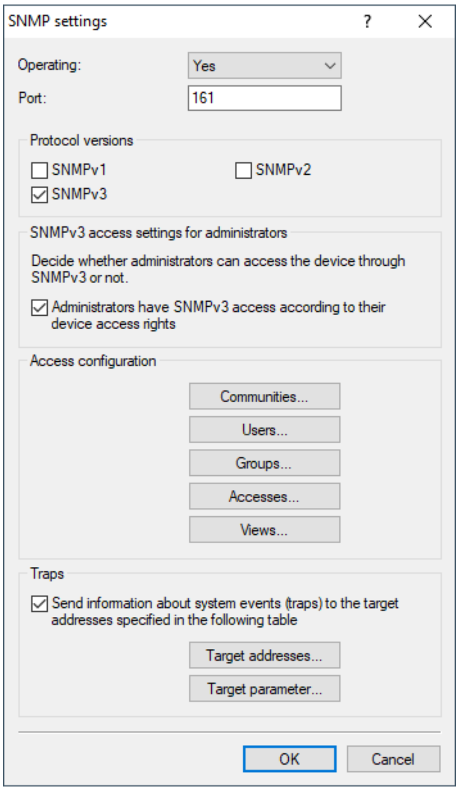
SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, and data transfer is encrypted by the DES or AES algorithm.

Context

“Context” is used to distinguish the various SNMP entities.

9.1.2 Configuring SNMP

The SNMP settings of the device can be found under **Management** > **Admin** > **SNMP** > **SNMP settings**.



SNMP settings

Operating: Yes

Port: 161

Protocol versions

□ SNMPv1 □ SNMPv2

☑ SNMPv3

SNMPv3 access settings for administrators

Decide whether administrators can access the device through SNMPv3 or not.

☑ Administrators have SNMPv3 access according to their device access rights

Access configuration

Traps

☑ Send information about system events (traps) to the target addresses specified in the following table

Operation

Enable SNMP for the SNMP protocol versions specified below, which the device should support for SNMP requests and SNMP traps.

Port

If necessary, adjust the port used for SNMP. Default: 161

Protocol versions

SNMPv1

Enables SNMPv1.

SNMPv2

Enables SNMPv2c.

SNMPv3

Enables SNMPv3.

SNMPv3 access settings for administrators

Administrators have SNMPv3 access according to their access rights

Enable this option if registered administrators, including the root user, should also have access via SNMPv3.

Access configuration

SNMP communities

Administrators of networks with SNMP management systems can precisely control the access rights to various access levels. SNMP of the versions v1 and v2 do this by encoding the access credentials as part of a “community”. Authentication is optionally handled

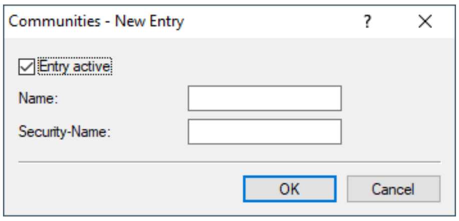
- by the `public` community (unlimited SNMP read access),
- by a master password (limited SNMP read access),
- or a combination of user name and password, separated by a colon (limited SNMP read access)

.

A community collects certain SNMP hosts into groups, in part so that it is easier to manage them. On the other hand, SNMP communities offer a certain degree of security because an SNMP agent only accepts SNMP requests from participants in a community that it knows.

By default, your device answers all SNMP requests that it receives from LANmonitor or another SNMP management system with the community `public`. Because this represents a potential security risk, especially with external access, LANconfig gives you the option of defining your own communities.

This configuration is relevant for the SNMP versions v1 and v2c only.



Entry active

Activates or deactivates this SNMP community.

Name

Enter a descriptive name for this SNMP community.

Security-Name

Here you enter the name for the access policy that specifies the access rights for all community members.

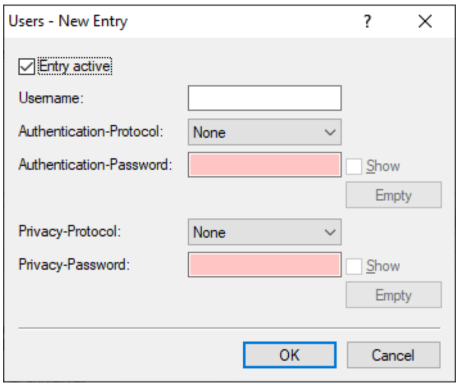
The SNMP community `public` is set up by default, and this provides unrestricted SNMP read access.

For SNMPv1 or SNMPv2c, you force the entry of login data for SNMP read-only access by disabling the `public` community in the list of the SNMP communities. This setting only allows information about the state of the device, current connections, reports, etc., to be read out via SNMP after the user authenticates at the device. Authorization can be conducted either with the administrator-account access credentials or an access account created for the individual SNMP community.

Disabling the community `public` has no effect on accessing for other communities created here. An individual SNMP read-only community always provides an alternative access path that is not tied to an administrator account.

Users

Individual users can be granted access to the device in addition to the administrators registered on it. Here you configure the authentication and encryption settings for these users when operating SNMPv3.



Users - New Entry

☑ Entry active

Username:

Authentication-Protocol: None

Authentication-Password: □ Show

Privacy-Protocol: None

Privacy-Password: □ Show

Entry active

Activates or deactivates this user.

User name

Enter a descriptive name for this user.

Authentication

Specify the method that the user is required to use to authenticate at the SNMP agent. The following options are available:

None

Authentication of the user is not necessary.

HMAC-MD5

Authentication is performed using the hash algorithm HMAC-MD5-96 (hash length 128 bits).

HMAC-SHA

Authentication is performed using the hash algorithm HMAC-SHA (hash length 160 bits).

HMAC-SHA224

Authentication is performed using the hash algorithm HMAC-SHA- 224 (hash length 224 bits).

HMAC-SHA256

Authentication is performed using the hash algorithm HMAC-SHA- 256 (hash length 256 bits).

HMAC-SHA384

Authentication is performed using the hash algorithm HMAC-SHA- 384 (hash length 384 bits).

HMAC-SHA512

Authentication is performed using the hash algorithm HMAC-SHA- 512 (hash length 512 bits).

Authentication password

Enter the user password necessary for authentication here and repeat it in the box below.

Encryption

Specify which encryption method is used for encrypted communication with the user. The following options are available:

None

Communication is not encrypted.

DES

Encryption is performed with DES (key length 56 bits).

AES128

Encryption is performed with AES128 (key length 128 bits)

AES192

Encryption is performed with AES192 (key length 192 bits)

AES256

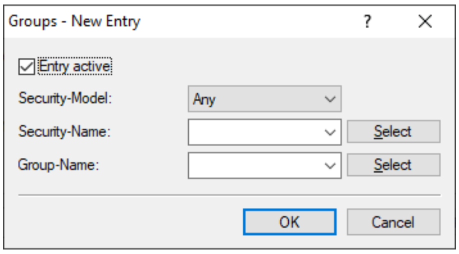
Encryption is performed with AES256 (key length 256 bits)

Privacy password

Enter the user password required by the encryption here and repeat it in the box below.

Groups

By configuring SNMP groups, it is easy to manage and assign the authentication and access rights of multiple users. By default, the configuration is set up for SNMP access via LANmonitor.



Groups - New Entry

☑ Entry active

Security-Model: Any

Security-Name:

Group-Name:

Entry active

Activates or deactivates this group.

Security model

SNMPv3 introduced the principle of the “security model”, so that the SNMP configuration in LCOS LX primarily uses the security model “SNMPv3”. However, for compatibility reasons it may be necessary to also take the versions SNMPv2c or even SNMPv1 into account, and to select these as the “security model” accordingly. Select one of the following entries accordingly:

Any

Any model is accepted.

SNMPv1

Data is transmitted by SNMPv1. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level “No authentication/No privacy”.

SNMPv2_C

Data is transmitted by SNMPv2c. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level “No authentication/No privacy”.

SNMPv3_USM

Data is transmitted by SNMPv3. Security levels for the user’s authentication and communication are possible, and these levels are activated with the **access rights**.

Security-Name

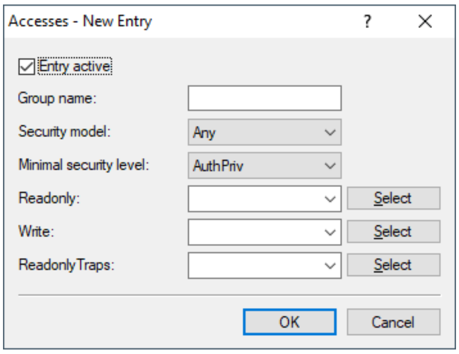
Here you select a security name you assigned to an SNMP community.

Group name

Here you select a group that you want to define under **Access rights**.

Access rights

This table brings together the different configurations for access rights, security models, and views.



Accesses - New Entry

☑ Entry active

Group name:	
Security model:	Any
Minimal security level:	AuthPriv
Readonly:	
Write:	
ReadonlyTraps:	

Entry active

Activates or deactivates this entry.

Group name

Enter a descriptive name for this group.

Security model

Activate the appropriate security model here.

Minimal security level

Specify the minimum security level for access and data transfer.

NoAuthNoPriv (No authentication/No privacy)

The authentication is performed by the specification and evaluation of the user name only. Data communication is not encrypted.

AuthNoPriv (Authentication/No privacy)

Authentication makes use of the hash algorithms set for the user. Data communication is not encrypted.

AuthPriv (Authentication and privacy)

Authentication makes use of the hash algorithms set for the user. Data communication is encrypted by DES or AES algorithms.

Read

Set the view of the MIB entries for which this group is to receive read rights. Available values are those defined under **Views**. Previously defined views are "Full Access". "LANmonitor Access". "Setup Access" and "Status Access".

Write

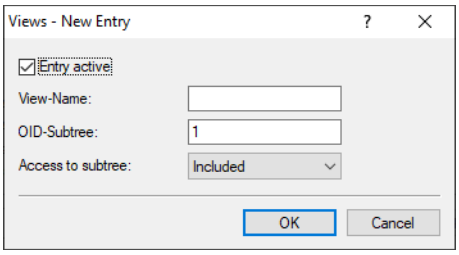
Set the view of the MIB entries for which this group is to receive write rights. Available values are those defined under **Views**. Previously defined views are "Full Access". "LANmonitor Access". "Setup Access" and "Status Access".

Read-only traps

Set the view of the MIB entries for which this group is to receive read rights for traps. Available values are those defined under **Views**. Previously defined views are "Full Access". "LANmonitor Access". "Setup Access" and "Status Access".

Views

Here you collect the different values or even entire branches of the device MIB, which each user is entitled to view or change in keeping with the corresponding access rights.



Views - New Entry

☑ Entry active

View-Name:

OID-Subtree: 1

Access to subtree: Included

Entry active

Activates or deactivates this view.

Name

Enter a descriptive name for this view.

OID subtree

Use a comma-separated list of the relevant OIDs to decide which values and actions from the MIB are included in or excluded from this view.

> The OIDs can be found in the device MIB, which you can download from *www.lancom-systems.com/downloads/*.

Access to subtree

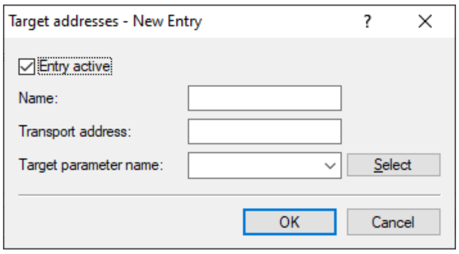
Here you decide whether the specified OID subtrees are "added" or "removed" from the view.

Traps

If you enable the option **Send information about system events (traps) to the target addresses specified in the following table**, the recipients configured under **Target addresses** and **Target parameters** will receive the corresponding information.

Target addresses

The list of target addresses is used to configure the addresses of the recipients to whom the SNMP agent sends the SNMP traps.



Entry active

Activates or deactivates this entry.

Name

Give the entry a descriptive name here.

Transport address

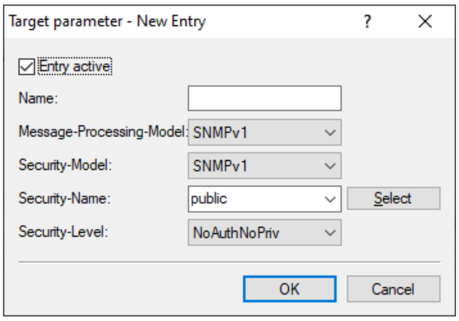
Configure the address of the recipient here. This address describes the IP address and port number of a recipient of an SNMP trap and is specified in the syntax "<IP address> : <Port>" (e.g. 128.1.2.3:162). UDP port 162 is used for SNMP traps.

Target parameter name

Here you select the desired entry from the list of recipient parameters.

Target parameter name

In this table you configure how the SNMP agent handles the SNMP traps that it sends to the recipient.



Target parameter - New Entry

☑ Entry active

Name:

Message-Processing-Model: SNMPv1

Security-Model: SNMPv1

Security-Name: public

Security-Level: NoAuthNoPriv

Entry active

Activates or deactivates this entry.

Name

Give the entry a descriptive name here.

Message processing model

Here you specify the protocol for which the SNMP agent structures the message.

Security model

SNMPv3 introduced the principle of the “Security Model”, so that the SNMP configuration in LCOS LX primarily uses the security model “SNMPv3”. However, for compatibility reasons it may be necessary to allow for the versions SNMPv2c or even SNMPv1, and to select these accordingly. Select one of the following entries accordingly:

Any

Any model is accepted.

SNMPv1

Data is transmitted by SNMPv1. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level “NoAuthNoPriv”.

SNMPv2_C

Data is transmitted by SNMPv2c. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level “NoAuthNoPriv”.

SNMPv3_USM

Data is transmitted by SNMPv3. This can only be selected together with SNMP users. The effective possible security level depends on the user's chosen authentication and encryption methods.

Security-Name

Here you select a security name you assigned to an SNMP community.

Security level

Set the security level that applies for the recipient to receive the SNMP trap.

NoAuthNoPriv (No authentication/No privacy)

The authentication is performed by the specification and evaluation of the user name only. Data communication is not encrypted.

AuthNoPriv (Authentication/No privacy)

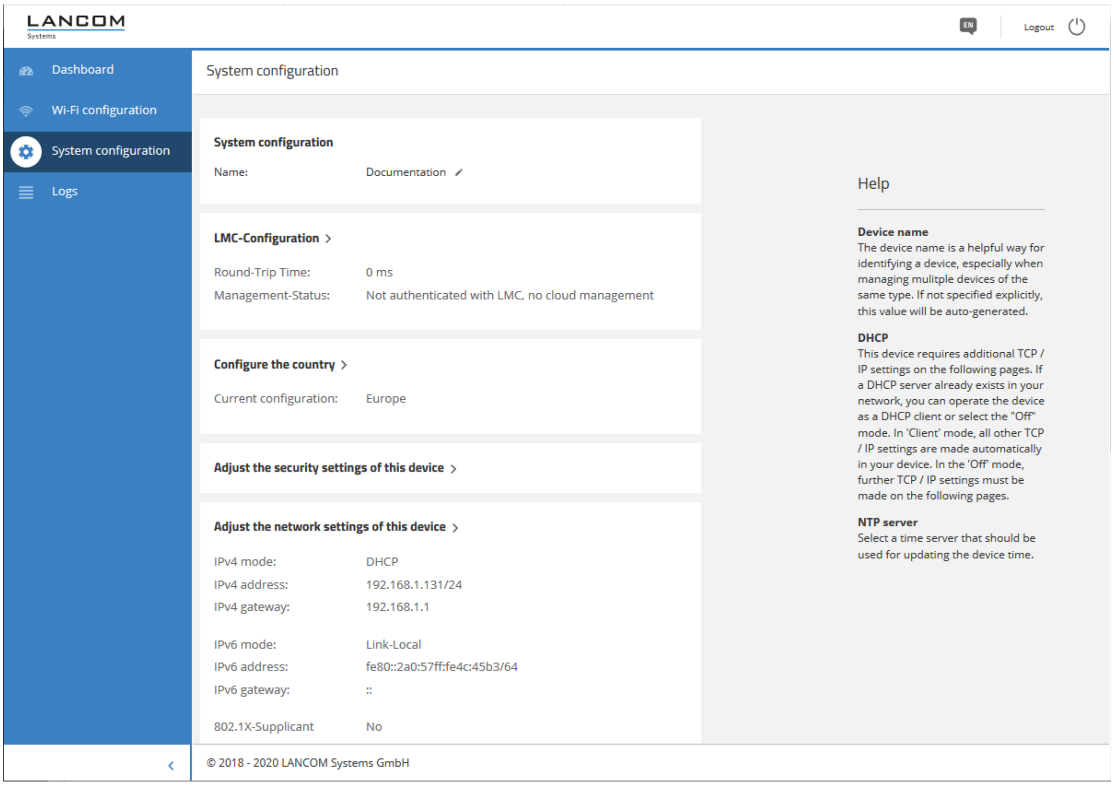
Authentication makes use of the hash algorithms set for the user. Data communication is not encrypted.

AuthPriv (Authentication and privacy)

Authentication makes use of the hash algorithms set for the user. Data communication is encrypted by DES or AES algorithms.

9.2 System configuration

This allows you to configure the basic parameters of your device, such as the device name or the IP settings for managing the device.



System configuration

Name: Documentation

LMC-Configuration >

Round-Trip Time: 0 ms
Management-Status: Not authenticated with LMC, no cloud management

Configure the country >

Current configuration: Europe

Adjust the security settings of this device >

Adjust the network settings of this device >

IPv4 mode: DHCP
IPv4 address: 192.168.1.131/24
IPv4 gateway: 192.168.1.1

IPv6 mode: Link-Local
IPv6 address: fe80::2a0:57ff:fe4c:45b3/64
IPv6 gateway: ::

802.1X-Supplicant No

Help

Device name
The device name is a helpful way for identifying a device, especially when managing mulitple devices of the same type. If not specified explicitly, this value will be auto-generated.

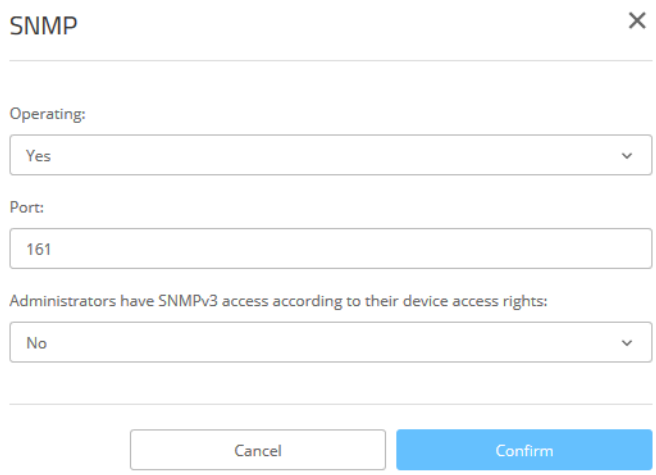
DHCP
This device requires additional TCP / IP settings on the following pages. If a DHCP server already exists in your network, you can operate the device as a DHCP client or select the "Off" mode. In 'Client' mode, all other TCP / IP settings are made automatically in your device. In the 'Off' mode, further TCP / IP settings must be made on the following pages.

NTP server
Select a time server that should be used for updating the device time.

© 2018 - 2020 LANCOM Systems GmbH

You can edit individual fields such as the system name by clicking on the check mark next to it. An edit mask for the various sections opens after clicking on the headline.

9.2.1 SNMP



SNMP

Operating:

Yes

Port:

161

Administrators have SNMPv3 access according to their device access rights:

No

Operation

Activate SNMP.

Port

If necessary, adjust the port used for SNMP. Default: 161

Administrators have SNMPv3 access according to their access rights

Enable this option if registered administrators, including the root user, should also have access via SNMPv3.

9.3 Additions to the Setup menu

9.3.1 SNMP

This menu contains the configuration of SNMP.

ⓘ The OIDs can be found in the device MIB, which you can download from *www.lancom-systems.com/downloads/*.

SNMP ID:

2.9

Console path:

Setup

Send-Traps

When serious errors occur, for example when an unauthorized attempt is made to access the device, it can send an error message to one or more SNMP managers automatically. Activate the option and, in the Target addresses table, add the targets where these SNMP managers are installed.

SNMP ID:

2.9.1

Console path:

Setup > **SNMP**

Possible values:

Yes
No

Default:

No

Port

Using this parameter, you specify the port which external programs such as LANmonitor use to access the SNMP service.

SNMP ID:

2.9.21

Console path:

Setup > **SNMP**

Possible values:

0 … 65535

Default:

161

Communities

SNMP agents and SNMP managers belong to SNMP communities. These communities collect certain SNMP hosts into groups, in part so that it is easier to manage them. On the other hand, SNMP communities offer a certain degree of security because an SNMP agent only accepts SNMP requests from participants in a community that it knows.

This table is used to configure the SNMP communities.

ⓘ The SNMP community `public` is set up by default, and this provides unrestricted SNMP read access.

SNMP ID:

2.9.27

Console path:

Setup > **SNMP**

Name

Enter a descriptive name for this SNMP community.

SNMP ID:

2.9.27.1

Console path:

Setup > **SNMP** > **Communities**

Possible values:

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

Default:

empty

Security-Name

Here you enter the name for the access policy that specifies the access rights for all community members.

SNMP ID:

2.9.27.3

Console path:

Setup > **SNMP** > **Communities**

Possible values:

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

Default:

empty

Status

This entry is used to enable or disable this SNMP community.

SNMP ID:

2.9.27.8

Console path:

Setup > **SNMP** > **Communities**

Possible values:

Active

The community is enabled.

inactive

The community is disabled.

Default:

Active

Groups

By configuring SNMP groups, it is easy to manage and assign the authentication and access rights of multiple users.

SNMP ID:

2.9.28

Console path:

Setup > **SNMP**

Security-Model

SNMPv3 introduced the principle of the "security model", so that the SNMP configuration in LCOS LX primarily uses the security model "SNMPv3". However, for compatibility reasons it may be necessary to also take the versions SNMPv2c or even SNMPv1 into account, and to select these as the "security model" accordingly.

You select a security model here as is appropriate.

SNMP ID:

2.9.28.1

Console path:

Setup > **SNMP** > **Groups**

Possible values:

Any

Any model is accepted.

SNMPv1

Data is transmitted by SNMPv1. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level "NoAuthNoPriv".

SNMPv2_C

Data is transmitted by SNMPv2c. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level "NoAuthNoPriv".

SNMPv3_USM

Data is transmitted by SNMPv3. Users can authenticate and communicate according to the following security levels:

NoAuthNoPriv

The authentication is performed by the specification and evaluation of the user name only. Data communication is not encrypted.

AuthNoPriv

The authentication is performed with the hash algorithm HMAC-MD5 or HMAC-SHA. Data communication is not encrypted.

AuthPriv

The authentication is performed with the hash algorithm HMAC-MD5 or HMAC-SHA. Data communication is encrypted by DES or AES algorithms.

Default:

SNMPv3_USM

Security-Name

Here you select a security name you assigned to an SNMP community. It is also possible to specify the name of an existing configured user.

SNMP ID:

2.9.28.2

Console path:

Setup > **SNMP** > **Groups**

Possible values:

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

Default:

empty

Group-Name

Enter a descriptive name for this group. You will use this name when you go on to configure the access rights.

SNMP ID:

2.9.28.3

Console path:

Setup > **SNMP** > **Groups**

Possible values:

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

Default:

empty

Status

Activates or deactivates this group configuration.

SNMP ID:

2.9.28.5

Console path:

Setup > **SNMP** > **Groups**

Possible values:

Active
inactive

Default:

Active

Accesses

This table brings together the different configurations for access rights, security models, and views.

SNMP ID:

2.9.29

Console path:

Setup > **SNMP**

Group-Name

Here you select the name of a group that is to receive these assess rights.

SNMP ID:

2.9.29.1

Console path:

Setup > **SNMP** > **Accesses**

Possible values:

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

Default:

empty

Security-Model

Activate the appropriate security model here.

SNMP ID:

2.9.29.3

Console path:

Setup > **SNMP** > **Accesses**

Possible values:

Any
Any model is accepted.

SNMPv1
SNMPv1 is used.

SNMPv2_C
SNMPv2c is used.

SNMPv3_USM
SNMPv3 is used.

Default:

Any

Read-View-Name

Set the view of the MIB entries for which this group is to receive read rights.

SNMP ID:

2.9.29.5

Console path:

Setup > **SNMP** > **Accesses**

Possible values:

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

Default:

empty

Write-View-Name

Set the view of the MIB entries for which this group is to receive write rights.

SNMP ID:

2.9.29.6

Console path:

Setup > **SNMP** > **Accesses**

Possible values:

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

Default:

empty

Notify-View-Name

Set the view of the MIB entries for which this group is to receive notify rights.

SNMP ID:

2.9.29.7

Console path:

Setup > **SNMP** > **Accesses**

Possible values:

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

Default:

empty

Status

Activates or deactivates this entry.

SNMP ID:

2.9.29.8

Console path:

Setup > **SNMP** > **Accesses**

Possible values:

Active
inactive

Default:

Active

Min-Security-Level

Specify the minimum security level for access and data transfer.

SNMP ID:

2.9.29.10

Console path:

Setup > **SNMP** > **Accesses**

Possible values:

NoAuthNoPriv

The SNMP request is valid without the use of specific authentication methods. Authentication merely requires the user to belong to an SNMP community (for SNMPv1 and SNMPv2c) or to specify a valid user name (for SNMPv3). Data transfer is not encrypted.

AuthNoPriv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, but data transfer is not encrypted.

AuthPriv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, and data transfer is encrypted by the DES or AES algorithm.

Default:

AuthPriv

Views

This table is used to collect the different values or even entire branches of the device MIB, which each user is entitled to view or change in keeping with their corresponding access rights.

SNMP ID:

2.9.30

Console path:

Setup > **SNMP**

View-Name

Give the view a descriptive name here.

SNMP ID:

2.9.30.1

Console path:

Setup > **SNMP** > **Views**

Possible values:

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

Default:

empty

OID-Subtree

Use a comma-separated list of the relevant OIDs to decide which values and actions from the MIB are included in this view.

> The OIDs can be found in the device MIB, which you can download from *www.lancom-systems.com/downloads/*.

SNMP ID:

2.9.30.3

Console path:

Setup > **SNMP** > **Views**

Possible values:

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

Default:

empty

Type

Here you decide whether the OID subtrees specified in the following are “Included” or “Excluded” from the view.

SNMP ID:

2.9.30.4

Console path:

Setup > **SNMP** > **Views**

Possible values:

Included

This setting outputs MIB values.

Excluded

This setting blocks the output of MIB values.

Default:

Included

Status

Activates or deactivates this view.

SNMP ID:

2.9.30.6

Console path:

Setup > **SNMP** > **Views**

Possible values:

Active
inactive

Default:

Active

Users

This menu contains the user configuration.

SNMP ID:

2.9.32

Console path:

Setup > **SNMP**

Username

Specify the SNMPv3 user name here.

SNMP ID:

2.9.32.2

Console path:

Setup > **SNMP** > **Users**

Possible values:

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

Default:

empty

Authentication-Protocol

Specify the method that the user is required to use to authenticate at the SNMP agent.

SNMP ID:

2.9.32.5

Console path:

Setup > **SNMP** > **Users**

Possible values:

None
Authentication of the user is not necessary.

HMAC-MD5
Authentication is performed using the hash algorithm HMAC-MD5-96 (hash length 128 bits).

HMAC-SHA
Authentication is performed using the hash algorithm HMAC-SHA-96 (hash length 160 bits).

HMAC-SHA224
Authentication is performed using the hash algorithm HMAC-SHA-224 (hash length 224 bits).

HMAC-SHA256
Authentication is performed using the hash algorithm HMAC-SHA-256 (hash length 256 bits).

HMAC-SHA384
Authentication is performed using the hash algorithm HMAC-SHA-384 (hash length 384 bits).

HMAC-SHA512
Authentication is performed using the hash algorithm HMAC-SHA-512 (hash length 512 bits).

Authentication-Password

Enter the user password necessary for authentication here.

Cleartext input is only possible if the parameter in *2.9.32.14 Authentication-Password-Type* on page 78 was changed.

SNMP ID:

2.9.32.6

Console path:

Setup > **SNMP** > **Users**

Possible values:

Max. 130 characters from `anything printable`

Default:

empty

Privacy-Protocol

Specify which encryption method is used for encrypted communication with the user.

SNMP ID:

2.9.32.8

Console path:

Setup > **SNMP** > **Users**

Possible values:

None

Communication is not encrypted.

DES

Encryption is performed with DES (key length 56 bits).

AES128

Encryption is performed with AES128 (key length 128 bits).

AES192

Encryption is performed with AES192 (key length 192 bits).

AES256

Encryption is performed with AES256 (key length 256 bits)

Privacy-Password

Enter the user password necessary for encryption here.

Cleartext input is only possible if the parameter in *2.9.32.15 Privacy-Password-Type* on page 78 was changed.

SNMP ID:

2.9.32.9

Console path:

Setup > **SNMP** > **Users**

Possible values:

Max. 130 characters from ``[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.` ``

Default:

empty

Status

Activates or deactivates this user.

SNMP ID:

2.9.32.13

Console path:

Setup > **SNMP** > **Users**

Possible values:

Active
inactive

Default:

Active

Authentication-Password-Type

The password in *2.9.32.6 Authentication-Password* on page 76 is always stored in encrypted format (type "Masterkey"). If you wish to enter a new password, for example from the command-line interface, you must first change the type to "Plaintext" here. You are then able to enter a password in plain text. LCOS LX will then encrypt the password and reset this value to "Masterkey".

SNMP ID:

2.9.32.14

Console path:

Setup > **SNMP** > **Users**

Possible values:

Plaintext
Masterkey

Privacy-Password-Type

The password in *2.9.32.9 Privacy-Password* on page 77 is always stored in encrypted format (type "Masterkey"). If you wish to enter a new password, for example from the command-line interface, you must first change the type to "Plaintext" here. You are then able to enter a password in plain text. LCOS LX will then encrypt the password and reset this value to "Masterkey".

SNMP ID:

2.9.32.15

Console path:

Setup > **SNMP** > **Users**

Possible values:

Plaintext
Masterkey

Target-Addresses

The list of target addresses is used to configure the addresses of the recipients to whom the SNMP agent sends the SNMP traps.

SNMP ID:

2.9.34

Console path:

Setup > **SNMP**

Name

Specify the target address name here.

SNMP ID:

2.9.34.1

Console path:

Setup > **SNMP** > **Target-Addresses**

Possible values:

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

Default:

empty

Transport-Address

The transport address describes the IP address and port number of a recipient of an SNMP trap and is specified in the syntax <IP address> : <Port> (e.g. 128.1.2.3:162). UDP port 162 is used for SNMP traps.

SNMP ID:

2.9.34.3

Console path:

Setup > **SNMP** > **Target-Addresses**

Possible values:

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

Default:

empty

Parameters-Name

Here you select the desired entry from the list of recipient parameters.

SNMP ID:

2.9.34.7

Console path:

Setup > **SNMP** > **Target-Addresses**

Possible values:

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

Default:

empty

Status

Activates or deactivates this target address.

SNMP ID:

2.9.34.9

Console path:

Setup > **SNMP** > **Target-Addresses**

Possible values:

Active
inactive

Default:

Active

Target-Params

In this table you configure how the SNMP agent handles the SNMP traps that it sends to the recipient.

SNMP ID:

2.9.35

Console path:

Setup > **SNMP**

Name

Give the entry a descriptive name here.

SNMP ID:

2.9.35.1

Console path:

Setup > **SNMP** > **Target-Params**

Possible values:

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

Default:

empty

Message-Processing-Model

Here you specify the protocol for which the SNMP agent structures the message.

SNMP ID:

2.9.35.2

Console path:

Setup > **SNMP** > **Target-Params**

Possible values:

SNMPv1
SNMPv2c
SNMPv3

Default:

SNMPv3

Security-Model

Use this entry to specify the security model.

SNMP ID:

2.9.35.3

Console path:

Setup > **SNMP** > **Target-Params**

Possible values:

Any
SNMPv1
SNMPv2_C
SNMPv3_USM

Default:

SNMPv3_USM

Security-Name

Here you select a security name you assigned to an SNMP community. It is also possible to specify the name of an existing configured user.

SNMP ID:

2.9.35.4

Console path:

Setup > **SNMP** > **Target-Params**

Possible values:

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

Default:

empty

Security-Level

Set the security level that applies for the recipient to receive the SNMP traps

SNMP ID:

2.9.35.5

Console path:

Setup > **SNMP** > **Target-Params**

Possible values:

NoAuthNoPriv

The SNMP message is valid without the use of specific authentication methods. Authentication merely requires the user to belong to an SNMP community (for SNMPv1 and SNMPv2c) or to specify a valid user name (for SNMPv3). Data transfer is not encrypted.

AuthNoPriv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, but data transfer is not encrypted.

AuthPriv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, and data transfer is encrypted by the DES or AES algorithm.

Default:

NoAuthNoPriv

Status

Activates or deactivates this entry.

SNMP ID:

2.9.35.7

Console path:

Setup > **SNMP** > **Target-Params**

Possible values:

Active
inactive

Default:

Active

Admitted-Protocols

Here you enable the SNMP versions supported by the device for SNMP requests and SNMP traps.

SNMP ID:

2.9.37

Console path:

Setup > **SNMP**

Possible values:

SNMPv1
SNMPv2
SNMPv3

Default:

SNMPv3

Allow-Admins

Enable this option if registered administrators (including the root user) should also have access via SNMPv3.

SNMP ID:

2.9.38

Console path:

Setup > **SNMP**

Possible values:

No
Yes

Default:

No

Operating

This entry enables or disables SNMP traps.

SNMP ID:

2.9.41

Console path:

Setup > **SNMP**

Possible values:

No

SNMP traps are switched off.

Yes

SNMP traps are enabled.

Default:

No