LCOS 10.94

Public Spot

01/2026

Contents

1 Public Spot....5
1.1 Introduction....5
1.1.1 What is a Public Spot?....5
1.1.2 Application scenarios....6
1.1.3 Overview of the Public Spot module....13
1.2 Setup and operation....15
1.2.1 Basic configuration....16
1.2.2 Security settings....39
1.2.3 Extended functions and settings....41
1.2.4 Alternative login methods....63
1.2.5 Internal and customized voucher and authentication pages (templates)....96
1.2.6 Viewing Public Spot clients....117
1.2.7 Displaying advertising to Public Spot users....117
1.3 Access to the Public Spot....118
1.3.1 Requirements for logging in....118
1.3.2 Logging in to the Public Spot....119
1.3.3 Session information....120
1.3.4 Logging out of the Public Spot....120
1.3.5 Advice and help....121
1.4 Tutorials for setting up and using Public Spots....122
1.4.1 Virtualization and guest access via WLAN controller with VLAN....122
1.4.2 Virtualization and guest access via WLAN controller without VLAN....132
1.4.3 Setting up a secure hotspot with Enhanced Open....146
1.4.4 Setting up an external RADIUS server for user administration....146
1.4.5 Internal and external RADIUS servers combined....147
1.4.6 Checking WLAN clients with RADIUS (MAC filter)....151
1.4.7 Setting up an external SYSLOG server....152
1.5 XML interface....153
1.5.1 Feature....154
1.5.2 Setting up the XML interface....155
1.5.3 Analyzing the XML interface using cURL....156
1.5.4 Commands....157
2 Appendix....164
2.1 Commonly transmitted RADIUS attributes....164
2.1.1 Messages to and from the authentication server....164
2.1.2 Messages to/from the accounting server....166
2.2 RADIUS attributes transmitted via WISPr....168
2.3 Dynamic authorization by RADIUS CoA (Change of Authorization)....169
2.3.1 Configuring dynamic authorization with LANconfig....169
2.4 Importing and exporting RADIUS user data by CSV file....171

2.4.1 Exporting RADIUS user data by CSV file....171
2.4.2 Importing RADIUS user data by CSV file....171
2.5 Expert settings for the PMS interface....172
2.5.1 Accounting....172
2.5.2 Login form....174
2.5.3 Guest-name-case-sensitive....177
2.5.4 Separator....178
2.5.5 Charset....178
2.6 Sending and receiving SMS text messages....179
2.6.1 Receiving SMS text messages....179
2.6.2 Basic configuration of the SMS module....179
2.6.3 Managing SMS text messages with LANmonitor....180
2.6.4 Sending SMS text messages with LANmonitor....181
2.6.5 URL placeholder for sending SMS....181
2.6.6 Character set for sending SMS....182
2.7 The SYSLOG module....183
2.7.1 Structure of SYSLOG messages....184
2.7.2 Configuring SYSLOG....185
2.7.3 Meaning of SYSLOG messages....192

Copyright

© 2026 LANCOM Systems GmbH, Würselen (Germany). All rights reserved.

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

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

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

LANCOM, LANCOM Systems, LCOS, LANcommunity, LANCOM Service LANcare, LANCOM Active Radio Control, and AirLancer 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 which are subject to their own licenses, in particular the General Public License (GPL). The license information for the device firmware (LCOS) is available on the device's WEBconfig interface under "Extras > License information". If the respective license demands, the source files for the corresponding software components will be made available on a download server upon request.

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

Products from LANCOM Systems 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

A Rohde & Schwarz Company

Adenauerstr. 20/B2

52146 Wuerselen

Germany

www.lancom-systems.com

1 Public Spot

1.1 Introduction

This chapter provides answers to the following two questions:

- What is a Public Spot?
- Which functions and properties apply to the Public Spot module?

1.1.1 What is a Public Spot?

Public Spots, also called hotspots, are places where users can connect their terminals – such as smartphones, tablet PCs or laptops – to a publicly accessible network. Normally, these networks provide connections to the Internet; however a Public Spot can also be limited to a local network in order to offer extra information to users visiting a museum or a trade show, for example. The term is usually synonymous to the devices with which the user can connect to the network, which is also why this manual does not differentiate between the location and the device.

The solution: (W)LAN technology

Public Spot scenarios make use of the widespread (W)LAN technologies based on the internationally established IEEE 802.11/802.3 standards:

- Access via WLANs provides fast, uncomplicated network access by radio. WLAN adapters are standard equipment for mobile devices and they support bandwidths that even allow the smooth playback of HD videos.
- With automatic address allocation via DHCP, access via LAN is similarly uncomplicated: Most notebooks feature a LAN adapter for the network cable.

When accessing via LAN the user loses mobility and uninterrupted flexibility. However, this access – assuming that a corresponding infrastructure is available – also provides stable network operation with the highest network load (for example, for multimedia content such as video-on-demand) and a higher number of users (for example, in a large hotel), where connections via WLAN may reach their limits sooner. It is also possible to add a Public Spot offering to an existing cable infrastructure (for example, in a college) with the use of a Public Spot via LAN.

Noteworthy issues of access using (W)LAN

Operating conventional WLAN access points or LAN routers as a Public Spot is made more difficult by the fact that user authentication is only possible by RADIUS/802.1X, which requires a corresponding configuration. For this reason, the use of devices without the Public Spot function is not practical, since these devices are not able to separate and log the specific network usage of authorized and unauthorized users of publicly accessible networks.

User authorization and authentication

As soon as an end device moves within range of an access point, the user can spontaneously established a connect to this access point. The same is true for open LAN connections. However, the problem is that access should not be available to the public in general, but only to certain selected users. Setting up restrictions of this type is the task of a Public Spot.

For this purpose, a Public Spot must be in a position to control access to the (W)LAN on a user basis. For simple Public Spot installations, user data can be locally stored and managed in the router or access point – or alternatively on a WLAN controller. Instead, complex installations employ a direct database connection to a central authentication server in the interests of detailed accounting or direct management. Central servers of this type generally work with RADIUS technology.

Accounting

If the Public Spot operator does not want to offer this service free of charge, connection data has to be collected and billed for each user. Typical methods include: Purchase of a limited amount of online time (pre-paid model), retrospective payment of consumed resources (post-paid model), or unrestricted access until a certain time (e.g. checking out of a hotel).

For smaller Public Spot installations, accounting functions should be as simple as possible, and they should be implemented locally in the device. Larger installations offer the facilities for billing via an external RADIUS server. For each application scenario, the connection to an external system can also be implemented using a software interface which has access to the accounting data and can control the user authentication (e.g. hotel reservation systems).

Logging

The Public Spot module provides suitable functions for recording user data with RADIUS accounting and SYSLOG.

Please note that operating a Public Spot (also referred to as a hotspot) can be subject to legal regulations in your country. Before installing a Public Spot, please inform yourself about any applicable regulations. You can also find information about this topic in the LANCOM techpaper "Public Spot" which is available at *www.lancom-systems.com*.

1.1.2 Application scenarios

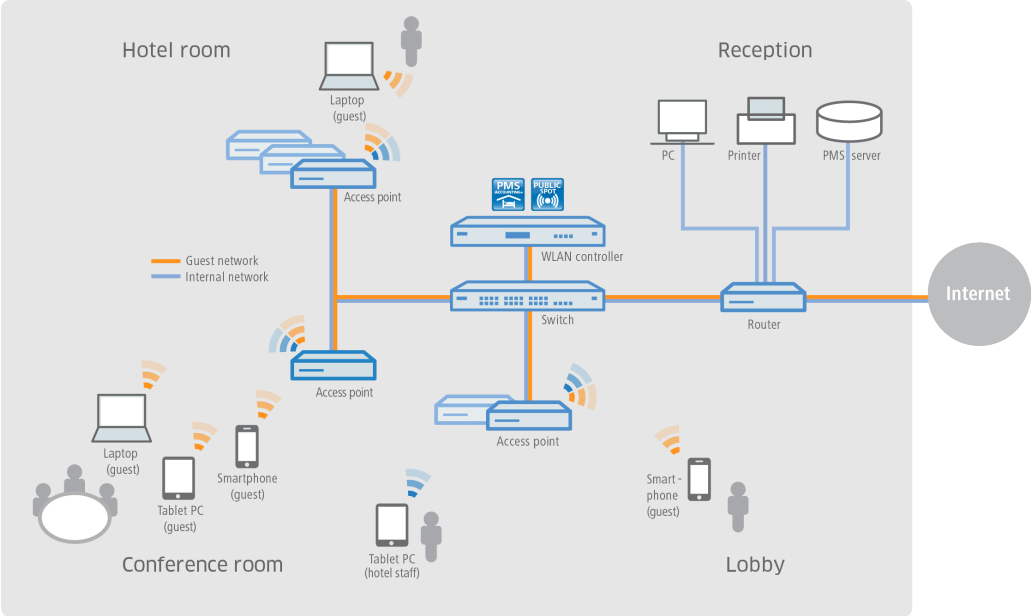
Guest access accounts in hotels

Wireless LAN makes it easier than ever for hotel operators to offer their guests convenient Internet access. Quick and easy to install, hotspot solutions from LANCOM enable guests to use their own laptop, tablet or smartphone to access the Internet via WLAN. Whether in the lobby, the conference room or in the hotel rooms—securely separated from the internal network, guest access can be provided anywhere it is desired.

The option LANCOM Public Spot PMS Accounting Plus is ideal for straightforward accounting: All Public Spot logins are automatically sent to the central PMS server where the hotel's accounting system is installed. In this way, guests can login to the hotspot using their room number and last name. For fee-based Internet access, the usage fees can be billed directly to the room. Needless to say, it is easy to set up free guest-access accounts in hotels, if desired.

- **Convenient setup and configuration** – a user-friendly setup and configuration wizard guarantees easy setup of the hotspot. For more details see the chapter *Basic installation of a Public Spot for simple scenarios* on page 16.
- **No access by unauthorized persons to internal data** – secure separation of the in-house and guest networks within a single infrastructure is ensured with VLAN or Layer 3 tunneling. Also, data can be securely encrypted on the wireless interface so that guests cannot penetrate the hotel network over the WLAN. For more details see the chapter *Virtualization and guest access via WLAN controller with VLAN* on page 122.
- **Simplified guest login on the WLAN** – The integrated Smart Ticket function ensures that the guest receives the login data for the Public Spot conveniently and automatically via text message (SMS) or e-mail. Alternatively, vouchers can also be printed out or guests can login with their room number and/or last name. For more details see the chapter *Alternative login methods* on page 63.

- **Simple billing of fee-based Internet access** – with the addition of the LANCOM Public Spot PMS Accounting Plus option, it is possible to connect to hotel accounting systems such as Micros Fidelio. For more details see the chapter *Interface for property management systems* on page 92.

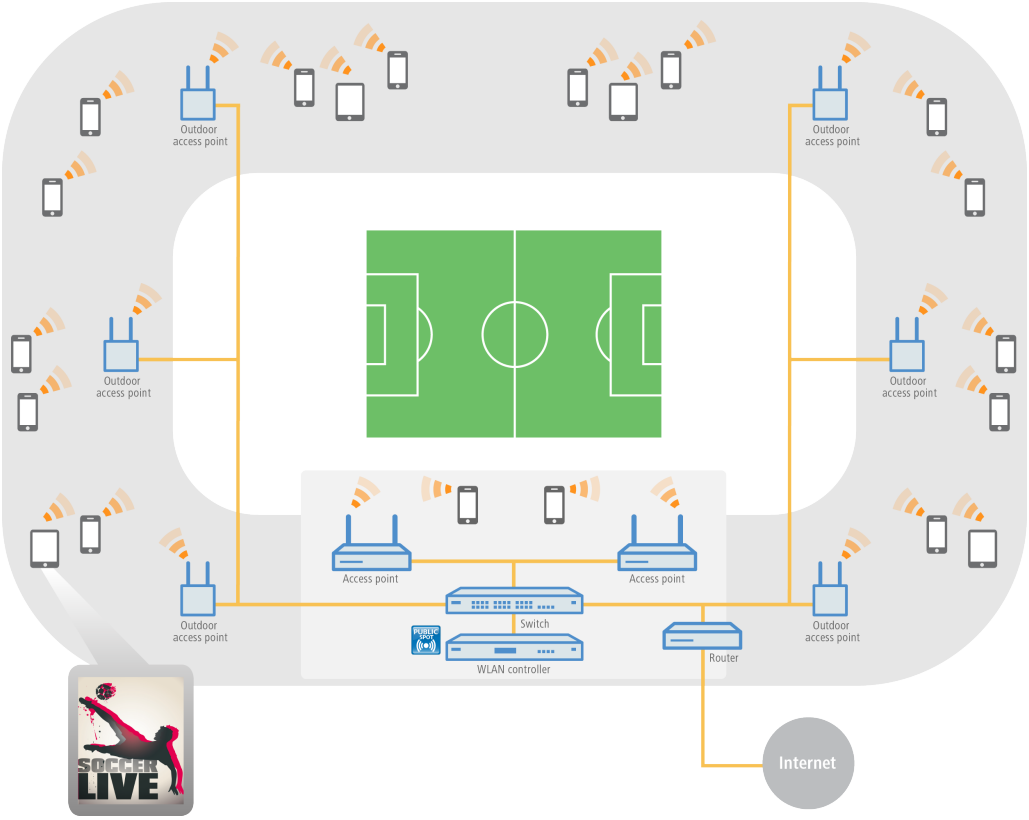


Guest access in sport arenas

Stadiums that host large sporting events increasingly offer a range of modern services. For example, they should allow very large numbers of spectators to use Internet access with their own end devices, for example to view live content about the event, or to surf online. In order to offer spectators an Internet connection that is faster than the overloaded cellular networks, a promising solution is to offload the data to the stadium Wi-Fi with the aid of LANCOM solutions. By connecting the clients to the stadium WLAN, the stadium operator has the possibility to create additional advertising space for sponsors—and thus additional sources of income. For example, the hotspot login page can be customized or sponsor websites can be invoked.

- **Multi-media fan experience** – with a WLAN Internet access, fans have the attractive option of watching current sports news live, and looking up information as well as watching replays.
- **New advertising spaces generate additional income** – additional, attractive advertising spaces can be made available to stadium operators by using the individual configuration options of the hotspot login page and also the configuration of pre-defined websites which do not require a login (walled garden function). For more details see the chapter *Open access networks (no login)* on page 42.

- **Convenient setup and configuration** – a user-friendly setup and configuration wizard guarantees easy setup of the hotspot. For more details see the chapter *Basic installation of a Public Spot for simple scenarios* on page 16.



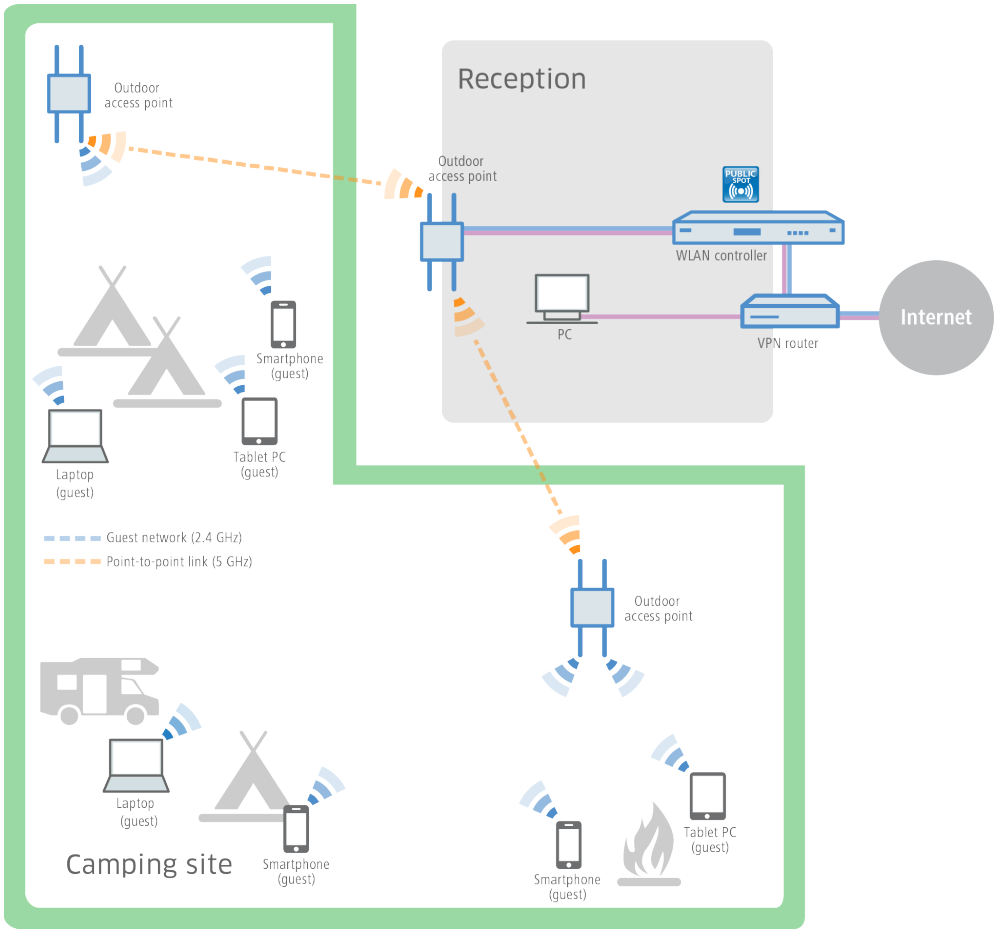
Guest access at camping grounds

Camping grounds are exposed to the weather and are often quite large. Nevertheless, people vacationing at modern camping grounds expect to have the convenience of Internet access from their own laptop, tablet or smartphone. Whether in a tent, a camper, or around the campfire, ubiquitously available Internet access is a real competitive advantage for camping ground operators.

With the robust, weather-proof outdoor devices from LANCOM and the LANCOM Public Spot option, even these demanding scenarios are implemented with ease—and without the laborious and costly need to lay cables. For example, in administration buildings for camping grounds, a WLAN controller (incl. LANCOM Public Spot option) is connected to a LANCOM dual-radio outdoor access point. This sends the signal via point-to-point connections in the 5-GHz frequency band to further outdoor access points, which provide WLAN coverage in the 2.4-GHz frequency band to the desired areas—such as campsites or recreational areas for guests. The secure separation of the guest and administrative networks is assured throughout, thanks to VLAN assignment.

- **Online convenience without laying cables** – even in wide-open areas, guests can be connected to the Internet without a costly and complicated installation.
- **Convenient setup and configuration** – a user-friendly setup and configuration wizard guarantees easy setup of the hotspot. For more details see the chapter *Basic installation of a Public Spot for simple scenarios* on page 16.
- **Simplified guest access** – The integrated Smart Ticket function ensures that the client receives the login data for the Public Spot conveniently and automatically via text message (SMS) or e-mail. Or as an alternative, vouchers can be printed out. For more details see the chapter *Alternative login methods* on page 63.

- **Reliable even in extreme conditions** – thanks to the robust IP66 outdoor housing and an extended temperature range, LANCOM outdoor devices are reliable and defy even extreme weather conditions from -33° to +70°C.



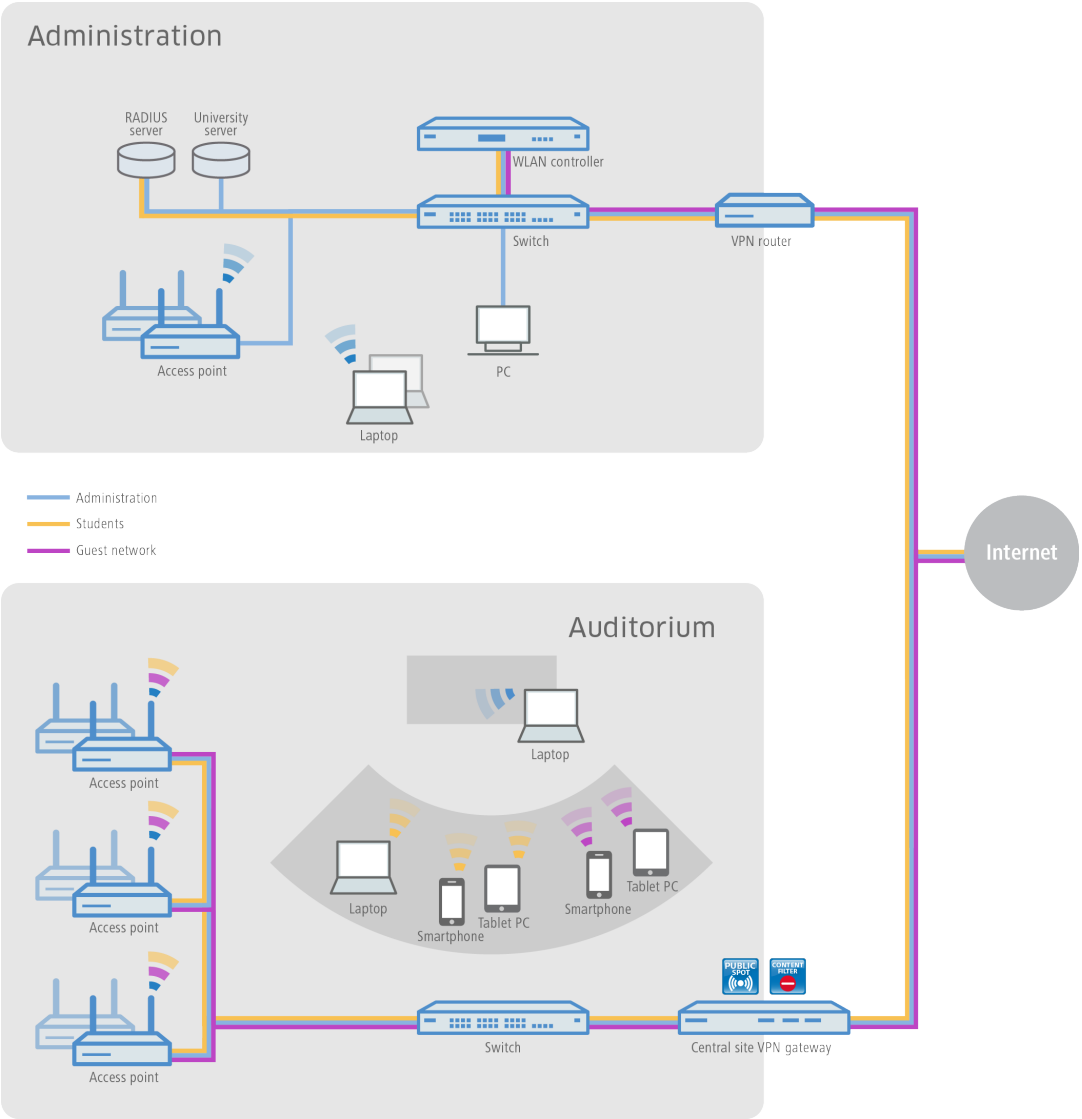
Guest access in schools and universities

Researching at home, learning for tests, preparing classes, or interactive design: The potential of Internet usage for students and pupils as well as teachers and staff of modern schools and universities is indispensable today—including at isolated buildings, preferably wireless, and with the users' own end devices.

With the help of LANCOM WLAN solutions, this is easy to implement. By configuring separate networks, the Internet access of the pupils and students is securely separated from the administrative access. Thanks to dynamic VLAN access, the different user groups are assigned to the VLANs that are intended for them, using just one SSID. For example, only staff have access to the university servers. At the same time, school and university students have the convenience of an extensive WLAN guest access, which is so important these days. The authentication in the pupil and student networks (e.g., Eduroam) can be implemented with IEEE 802.1X. This makes it possible for guest students from partner universities to connect to the WLAN of the host university. And even conference guests can be provided with a temporary guest access by means of a voucher.

- **Secure login for university affiliates** – professors, students and staff of universities can have access to the Internet and various online libraries over the securely encrypted WLAN.
- **No access by unauthorized persons to internal data** – secure separation of the administrative, students', and professors' and guests' networks within a single infrastructure is ensured with VLAN or Layer 3 tunneling. For more details see the chapter *Virtualization and guest access via WLAN controller with VLAN* on page 122.
- **No misuse of the network** – with the LANCOM Content Filter, professional, database-supported verification of websites is performed. Undesirable websites or web content can be made inaccessible to specified user groups.

- **Comfortable, cable-free Internet access** – even in large open areas, guests have Internet access with their WLAN-enabled end devices without a costly and complicated installation.



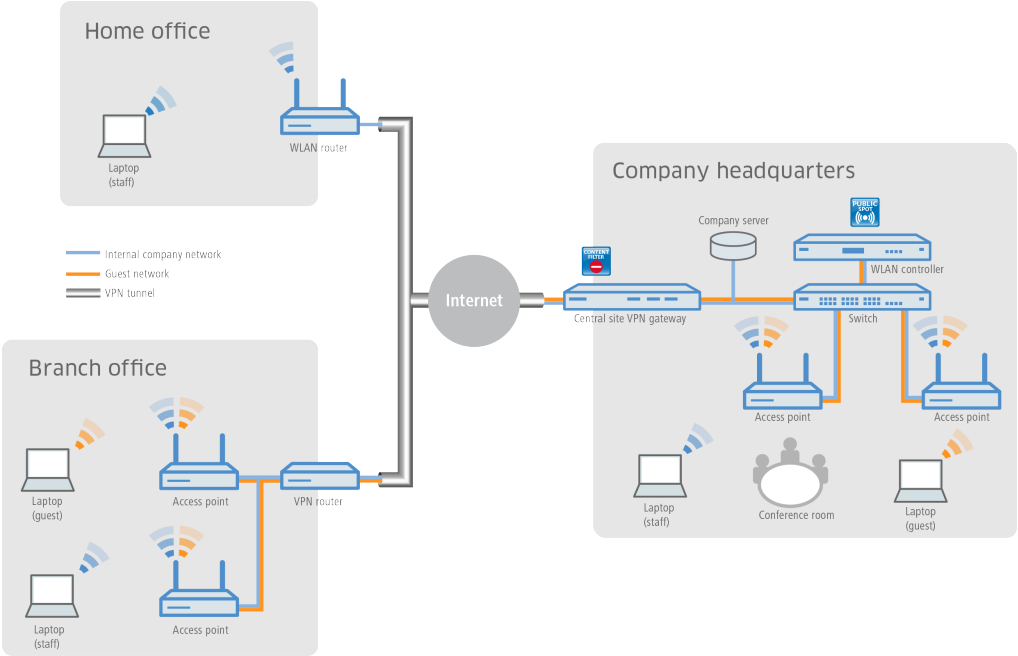
Guest access in companies

At any company with a complex network structure, the flexibility and stability of Internet access is vitally important. Branch offices must have cross-site access to the company network, and home office employees also need access to e-mail accounts and databases. In addition, customers and visitors should be offered a separate guess access.

With devices from LANCOM and the LANCOM Public Spot option, these scenarios are easy to implement. The sites are connected using a VPN tunnel. Companies can provide access to the Internet for their external guests on their own mobile devices ("Bring Your Own Device") using a separate guest network in the company main office and even at networked branch offices. Access to the company's internal data is reserved for authorized employees only.

- **Secure separation of company and guest networks** – the secure separation of employee and guess networks within a single infrastructure is achieved by using VLAN or a Layer 3 tunnel. This keeps internal data safe from unauthorized access. For more details see the chapter *Virtualization and guest access via WLAN controller with VLAN* on page 122.
- **User-friendly setup and configuration** – a LANCOM WLAN controller allows different user profiles to be defined and configurations to be uploaded to the different WLAN devices – including those at remote sites.

- **Easy guest access** – using vouchers, it is a simple task for your reception desk to provide guests with login data for the Public Spot so that they can use their own mobile clients ("Bring Your Own Device"). In this way, only registered users have access to the Internet and e-mail.
- **No misuse of the network** – with the LANCOM Content Filter, professional, database-supported verification of websites is performed. Undesirable websites or web content can be made inaccessible to specified user groups.



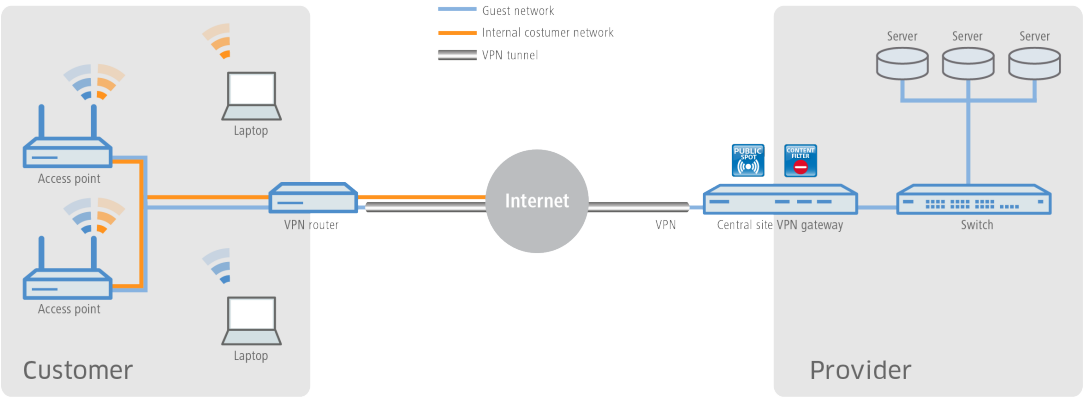
Guest access for providers

With the solutions from LANCOM, it is very easy for Internet providers to offer their customers a network with guest access. The provider receives all necessary network products from one source, LANCOM, and manages the networks of its clients centrally and conveniently—without a technician on site.

For the implementation, LANCOM access points are installed behind a LANCOM VPN router at the site of the provider's client (for example, a hotel, hospital or business). A separate internal network is given direct Internet access. The guest access is provided over a secure VPN tunnel to the central-site VPN gateway at the provider, who can log incoming requests on their internal servers. With the LANCOM Content Filter, the provider can also limit or block access to undesirable or illegal websites for customer guest-access accounts.

- **Simple and central management and roll-out** – even without a technician on site, the provider can centrally monitor and configure the networks for the customer. For more details see the chapter *Basic installation of a Public Spot for simple scenarios* on page 16.
- **Different redirect options** – network separation means that the hotspot services can be designed and implemented in various ways. For example, services offered to end customers can be limited to hotspot administration only, or they can include full-service administration, whereby all data traffic from the end customer is forwarded to the provider via a tunnel.
- **Connection of proprietary AAA systems** – LANCOM provides different interfaces (RADIUS, XML, FIAS) which can be combined with proprietary AAA servers. Custom authentication and login to the hotspot, as well as accounting, can be implemented specific to each provider. For more details see the chapter *Alternative login methods* on page 63.
- **Multi-provider support** – LANCOM devices are not locked into access via a specific provider. Hotspot service providers who cooperate with different providers can combine their software solutions over a variety of interfaces with the help of LANCOM devices. For more details see the chapter *Alternative login methods* on page 63.
- **No misuse of the network** – with the LANCOM Content Filter, professional, database-supported verification of websites is performed. Undesirable websites or web content can be made inaccessible to specified user groups.

- **Data offloading** – WLAN hotspots can provide effective relief for cellular networks by offloading data traffic to different infrastructures.

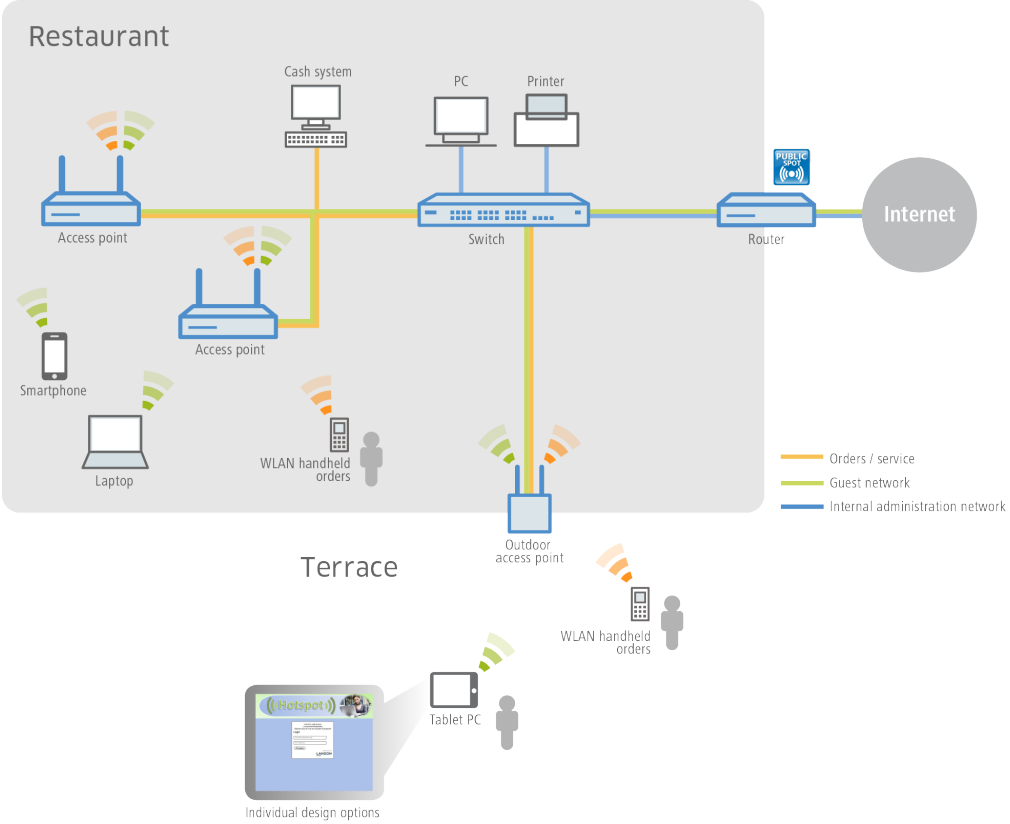


Guest access in gastronomy

Providing guests in a modern restaurant or café with a hotspot can significantly increase the appeal of any location. With the WLAN solutions from LANCOM, visitors benefit from a WLAN guest network in that they can make convenient use of the Internet with their mobile smartphones, tablet PCs or laptops—while being securely and completely separated from the internal administrative network. For a significant increase in efficiency in work processes, wait staff also have the option of taking orders with the help of a WLAN-enabled hand-held device, and transmitting the order directly to the checkout system, kitchen, or drink serving station. Needless to say, WLAN access for the guests and for taking orders can also be made available on the patio or outdoor areas of the restaurant, since a robust LANCOM outdoor access point is ideal for outdoor areas.

- **Customizable and flexible creative leeway** – whether with proprietary logos, texts or images—the welcome page of the Public Spot can be easily tailored to your own requirements. Even displaying pre-defined websites is possible (walled garden feature), so that, for example, the menu of the restaurant or its own website is shown to the guest without a prior login to the hotspot by the guest. For more details see the chapter *Internal and customized voucher and authentication pages (templates)* on page 96.
- **No access by unauthorized persons to internal data** – secure separation of the networks within a single infrastructure is ensured with VLAN or Layer 3 tunneling. For more details see the chapter *Virtualization and guest access via WLAN controller with VLAN* on page 122.
- **Convenient setup and configuration** – a user-friendly setup and configuration wizard guarantees the easy setup of hotspots. For more details see the chapter *Basic installation of a Public Spot for simple scenarios* on page 16.

- **Simplified guest access** – The integrated Smart Ticket function ensures that guests receive their login data for the Public Spot conveniently and automatically via text message (SMS) or e-mail. Or as an alternative, vouchers can be printed out. For more details see the chapter *Alternative login methods* on page 63.



1.1.3 Overview of the Public Spot module

The demands placed on devices operating Public Spots are as varied as the environments they are employed in. A Public Spot offers various functions which are described in more detail in the following sections.

Open User Authentication (OUA)

Open User Authentication (OUA) provides Web-based authentication by means of an online form and is ideal for Public Spot installations.

Typical procedure for an online session with OUA

1. The user of a W(LAN)-enabled end device is within reach of an access point or a network outlet in a Public Spot mode.
   - WLAN: After system startup, the WLAN adapter automatically logs on to the appropriate access point.
   - LAN: After system startup the user connects to the network with a suitable cable and is assigned an address by the DHCP server.

   Internet access or the use of chargeable services is not yet possible at this stage.
2. The user starts a web browser. The device offering the Public Spot service automatically directs the user to the login page of the Public Spot. This page provides detailed information on using the services.

   Alternatively, the user's client device automatically performs captive portal detection and presents the login page of the Public Spot immediately after associating with the WLAN.

Generally, the user purchases a voucher with login data that grants a limited amount of access time. Other login methods are also possible, such as login after confirming the provider's terms of use or independently requesting login data via e-mail or a text message (SMS).

3. In the case of a login using a voucher, the user enters his login data (username and password) on the login page. Depending on the configuration, the RADIUS server on the device (internal) or an external one checks the login data that was entered. If the login is successful, the user gains access to the Public Spot. Otherwise an error message will be displayed. If a prepaid model is employed, i.e. access is to be granted for a limited period of time only, then the RADIUS server additionally informs the Public Spot about the user's time credit.
4. The user can log off from the Public Spot at any time. The Public Spot can terminate a session itself if the time credit has expired, if a specified expiry date is reached, or if contact is lost for an extended period.

   During and at the end of a session the Public Spot provides the user with an overview of the session data. If required, the Public Spot can simultaneously transmit all important accounting information to the RADIUS server. This can be the device's internal server or an external server.

Security in the (W)LAN

Wireless LANs are potentially a significant security risk. Public Spots present similar risks to the operator and users.

Security for the operator

Operators of Public Spots are primarily interested in the security of their own network infrastructure. A Public Spot module provides operators with a range of security technologies and methods:

- **Multi-SSID** (only WLAN)**, VLAN and virtual routers**
  - The safe separation of public access can be achieved using one or more different radio cells for an access point (Multi-SSID).
  - VLAN technology can separate public access from the private network of the operator.
  - Virtual routing technology ARF (Advanced Routing and Forwarding) from LANCOM Systems supplies one SSID with its own security and QoS settings and only specific destinations are routed on it.

  This ensures that guest access over a Public Spot is securely and effectively separated from the productive network, even though they share the same infrastructure. The device's internal firewall can, for example, limit the available bandwidth in the WAN to max. 50 %, and access can be restricted to web pages (HTTP, port 80) and name resolutions (UDP 53).

  Further information on Multi-SSID, VLANs and ARF is available in the LCOS Reference Manual.

- **Traffic limit**

  To avoid denial-of-service (DoS) and brute-force attacks on the Public Spot you can restrict the permissible data transfer for non-authenticated Public Spot participants to a harmless volume.

- **Locking access to the configuration**

  You can lock access from your Public Spot network to device configurations (e.g., your access points, WLAN controllers or routers) so that access to configurations is only possible using other specified management interfaces.

Security for the user

The primary security concern for users of Public Spots is the confidentiality of their data. Users are also interested in security of user data to avoid misuse. Users are protected by the following security technologies:

- **Intra-cell blocking** (WLAN Only)

  Prevent communication between the WLAN clients in your Public Spot network. Along with the user's existing security mechanisms, this measure helps to prevent unauthorized access to the resources of your Public Spot users.

- **Encryption during the login phase**

If you have a digital certificate, you can load it on your device in order to secure usernames and passwords using an encrypted HTTPS method. The digital certificate should be signed by a recognized public authority so that browsers classify it as trustworthy and do not display security errors to the users. If there is no certificate, data is sent unencrypted.

The certificate merely secures the login process, as the data within a Public Spot network are normally not encrypted. This is true for LAN as well as WLAN connections. If your users wish to secure their regular data traffic as well, they will have to use their own encryption methods.

An exception to this are the WLAN connections via HotSpot 2.0: Since the HotSpot 2.0 standard is based on WPA2 (802.1X/802.11i), EAP and 802.11u, data packets are always encrypted for transmission, both for authentication and during the session.

LANCOM strongly recommends that sensitive user data should only ever be transferred via encrypted connections, such as the IPSec-based VPN tunnel with the LANCOM Advanced VPN Client or over normal encrypted data connections based on HTTPS. In addition to this, Public Spot users should ensure that a personal firewall is active on their end devices.

Setup wizard for Public Spots

The **Setup Public Spot** wizard helps you to setup and perform the initial configuration of your Public Spot. You can set up a functional Public Spot network with just a few clicks. The wizard groups the necessary settings together (e.g. assign an interface, choose an IP range, specify the access format and login procedure, logging) and offers you the option to create an administrator with limited rights who can only create and manage Public Spot users.

Wizard for creating and managing users

Using the setup wizard **Create Public Spot account** you can use WEBconfig to create temporary accesses to the Public Spot network with just a few clicks of the mouse. In the simplest case, you only need to enter the duration of access, the wizard assigns the username and password automatically and stores the credentials in the user database of the internal RADIUS server. The user receives a printed, personalized voucher, which the user can immediately use to login to the Public Spot network for the specified period.

Alternatively, a stock of vouchers can be created and printed out to speed up the voucher issue at peak times or to allow employees without access to the device to issue vouchers. In this case the Public Spot account is created with an online time duration that starts when the user logs in for the first time. You also set a maximum validity period for the access. After this time, the Public Spot automatically deletes the access account, even if the online time was not used up yet.

The setup wizard **Manage Public Spot account** displays all registered Public-Spot access accounts in a table on a web page. This gives you an overview of your most important user data, as well as a user-friendly way to extend or reduce the validity of an access account with a single click, or even delete user accounts completely. In addition, the administrator can call up information about the user account using the wizard, such as the password in cleartext, the authentication status, the IP address, the sent/received data volume or any restrictions that apply to the user account.

If several administrators are involved with the management of Public Spot accounts, you have the option of restricting the accounts that are displayed to those created by the respective administrator. As a result, the overview table only displays those accounts that were created by the administrator who is currently logged-in.

This restriction has no effect if an administrator account has a full name that is a part of the other administrator account names. "PSpot_Admin" for example sees the entries made by "PSpot_Admin1" and "PSpot_Admin2". "PSpot_Admin" acts as a super-admin in this scenario. All other administrators ("PSpot_AdminX"), however, do not see the entries made by the others.

1.2 Setup and operation

This chapter contains the main information required for setting up and operating a Public Spot.

- **1) step: Basic configuration**

  First, we describe the basic configuration. After completing the basic configuration, the Public Spot is operational and preconfigured for a simple application scenario (login using voucher).

- **2nd step: Security settings**

  This chapter describes in detail the security settings that impede attacks on your Public Spot network and promote stable operation. If you have not already made these settings during previous setup steps, you should pay close attention to the following pages.

- **3rd step: Extended functions and settings**

  Finally, we review the wide variety of available extended functions and settings. Detailed descriptions inform you on how to individually adapt your device to its task and its environment. In addition, this chapter informs you on how to keep an overview of the status and activities of your Public Spot.

Please note that operating a Public Spot (also referred to as a hotspot) can be subject to legal regulations in your country. Before installing a Public Spot, please inform yourself about any applicable regulations. You can also find information about this topic in the LANCOM techpaper "Public Spot" which is available at *www.lancom-systems.com*.

1.2.1 Basic configuration

The instructions for the basic settings are divided into several separate sections:

- The first section describes the setup of an operational Public Spot using a Wireless Router as an example.

  To set up a Public Spot for a simple application scenario, you can start the corresponding wizard, which assists you in configuring the Public Spot.

- The second section describes the configuration of the default values for the user wizard with which new employees can easily create and manage new Public Spot users without the need for general administrator rights. This also includes creating a limited access account with which your employees can access this wizard only.
- The third section describes user administration on the local RADIUS server, either using the user wizard or manually with LANconfig.

To a certain extent these sections are dependent on one another, and ideally you should work through them in sequence.

Basic installation of a Public Spot for simple scenarios

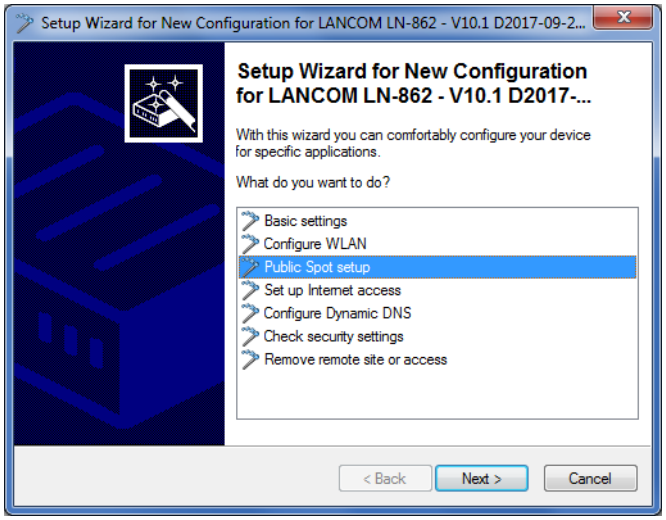
Installation using the setup wizards

The following tutorial describes how to use LANconfig's Public Spot setup wizard to perform a basic Public Spot installation.

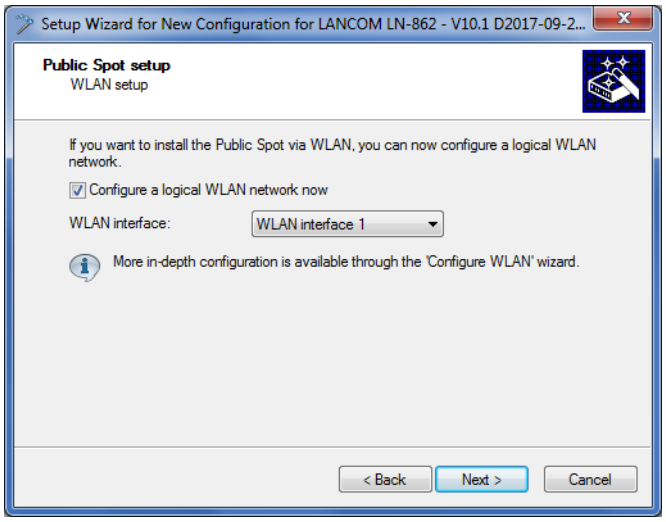
The wizard for the basic configuration of the Public Spot shows different dialogs depending on the device type and your previous choices. This tutorial is only an example.

1. To do this, start LANconfig and select the device on which you wish to set up the Public Spot, for example, an access point.

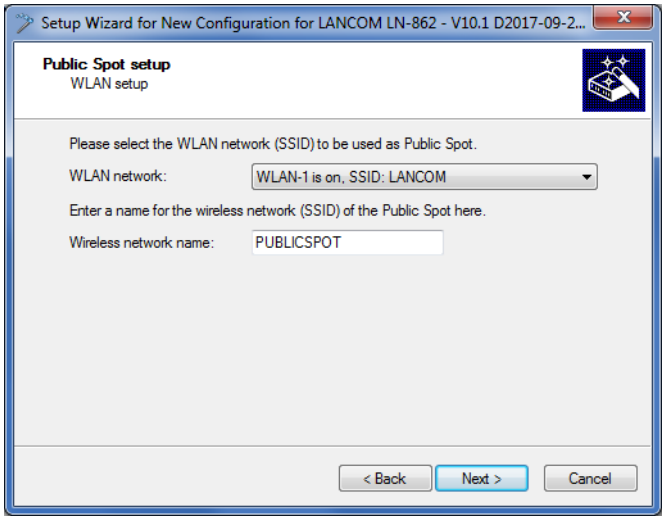
2. Start the Setup Wizard with **Device** > **Setup wizard**, select the action **Setup Public Spot** and then click **Next**.



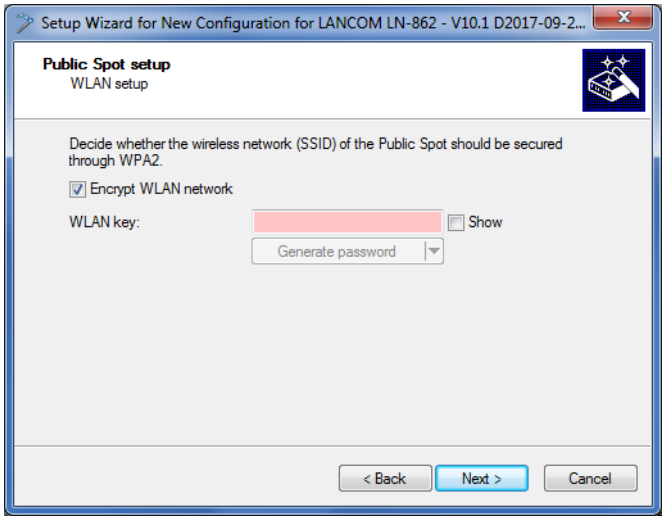
3. If you want the Public Spot to be available over WLAN, enable the corresponding option and then click **Next**.



4. Select the logical interface from the drop-down menu which the Public Spot should offer (e.g., WLAN-1), and enter a descriptive name for the wireless network (PUBLICSPOT). Click on **Next**.

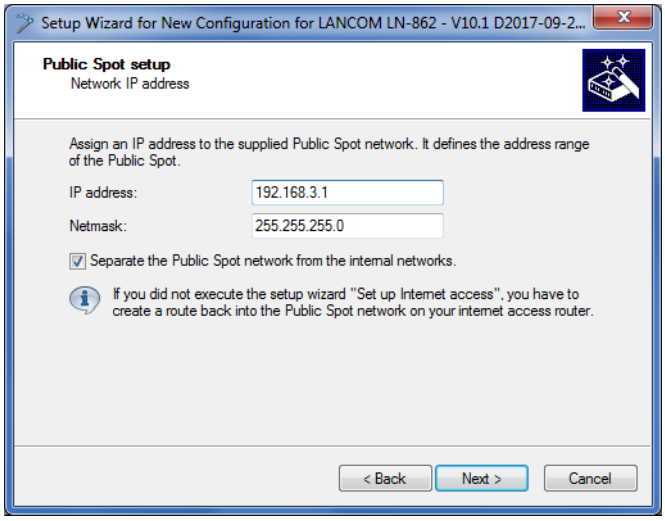


5. Specify whether the wireless network should be encrypted. In this case, specify a WLAN key or have it generated automatically.



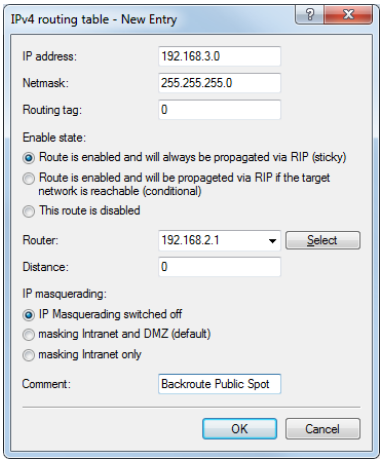
6. Assign the IP address and netmask to the device that your Public Spot network should specify and click **Next**.
   The Public Spot module has its own address on your network, which is independent from the address that you assigned to your device. For example, if you have a 192.168.0.0/24 network set up and your device has the IP address 192.168.2.1, you can assign the IP address `192.168.3.1` and the subnet mask `255.255.255.0`, as long as this IP address has not already been used elsewhere.

If you want to separate the Public Spot network from internal networks for security reasons, make sure that the corresponding option is enabled.



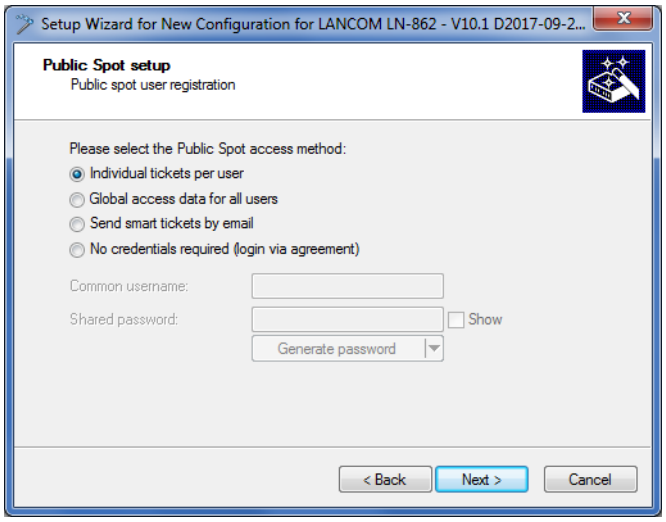
If your device is not directly connected to the Internet and you have a different address range for your Public Spot, you must set up a return route to your Public Spot network on your Internet gateway. If there is no return route, Public Spot users will see an HTTP error after they have successfully authenticated.

Please find the directions on how to set up a return route, in the documentation for your Internet gateway. In LANconfig you configure this under **IP router** > **Routing** > **IPv4 routing table**. To do this, create a new entry and enter the network address of your Public Spot network under **IP Address** and under **Router** enter the address of the Public Spot in your local network.

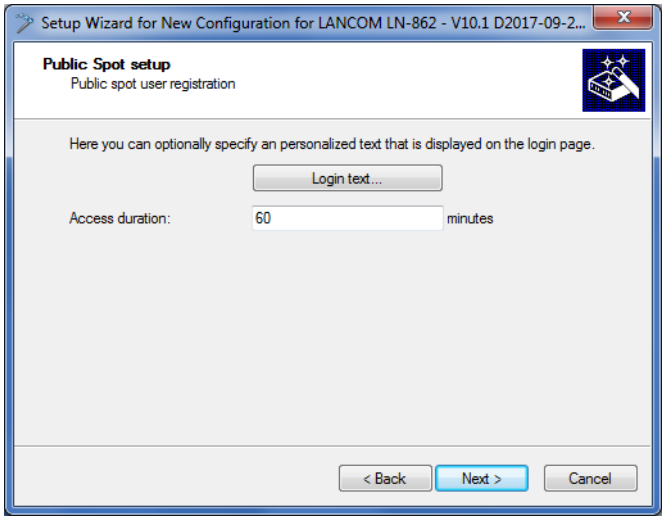


7. Specify which login data your users are to use to login to the Public Spot. Also, you can optionally add customized text to the login page. To continue, click on **Next**.

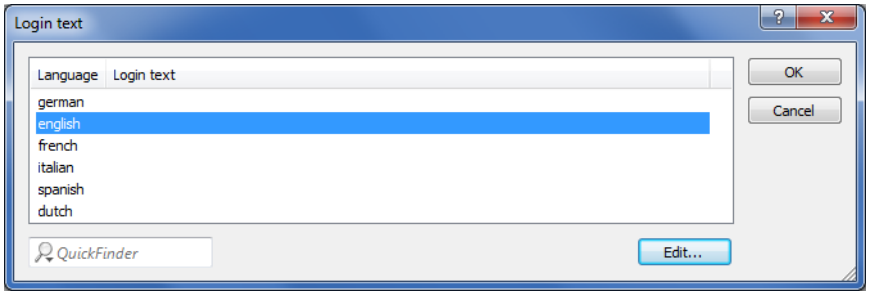
You can either give each user their own login data or set up a general account that all users use to access the Public Spot. If you issue vouchers later and would like to set up permanent user accounts, select the option **Individual tickets per guest**.

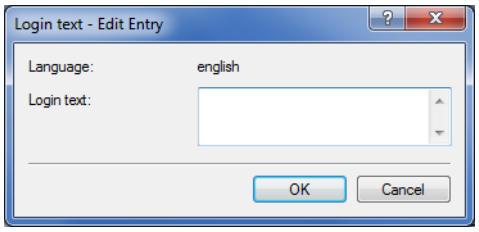


8. Here you can optionally select a login text, you set the access time and click **Next**.



Login text (optional):



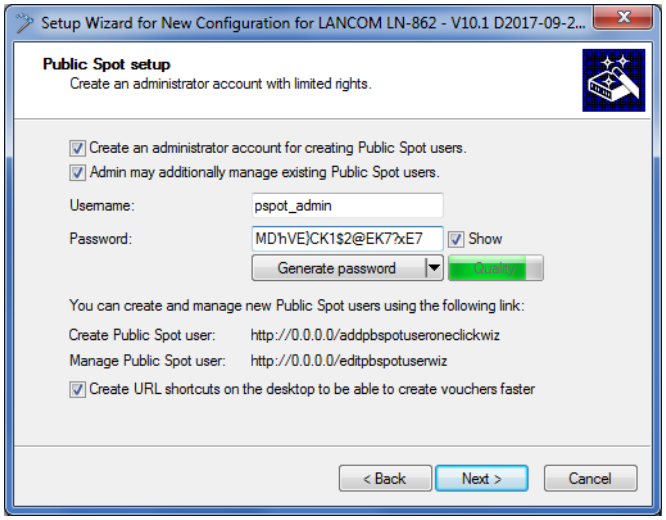


The login text is a customized text entered in HTML format, which appears on the login page inside the box on the registration form. You can manually add or edit this text at a later time (see the section *Customized text or login title for the login page* on page 99).

9. If necessary, create an administrator with limited rights who can use the setup wizards in WEBconfig to create and manage Public Spot users. To continue, click on **Next**.
   This type of administrator is useful when you want your employees to be able to manage user accounts themselves without the help of a device administrator. The right to create new accounts in WEBconfig enables the Create Public Spot account wizard, and administrator rights enable the Manage Public Spot account wizard.

   Using the user creation wizard **Create Public Spot account**, the administrator has the option of creating time-limited accounts for Public Spot users and print the corresponding login data on a voucher.

   The **Manage Public Spot accounts** wizard enable the administrator to manage the users. The administrator can extend or reduce the validity period of access, or completely delete a specific user account. In addition, the administrator can call up information about the user account using the wizard, such as the password in cleartext, the authentication status, the IP address, the sent/received data volume or any restrictions that apply to the account.

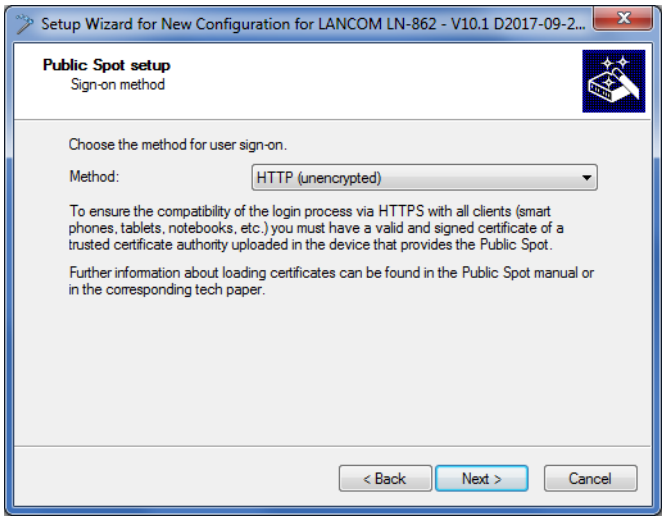


Make sure that the password you create is secure. The Setup Wizard will check the quality of the password you enter. For passwords that are not secure the input field appears in red, when it is more secure it changes to yellow, and when it is very secure the background turns green.

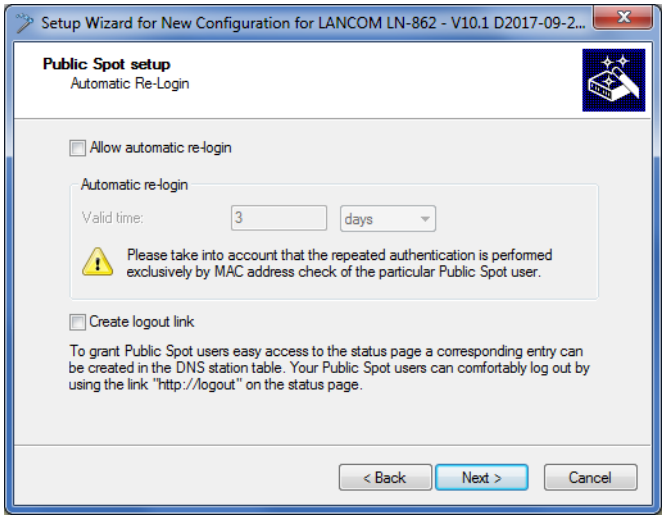
10. Select the procedure for user login. To continue, click on **Next**.

You can select **HTTP** or **HTTPS** in the drop-down list. Using a connection with HTTPS provides a secure connection for Public Spot users.

The use of HTTPS requires the installation of a suitable server certificate. Otherwise the user is presented the device's own certificate, which would cause the browser to issue a certificate warning.

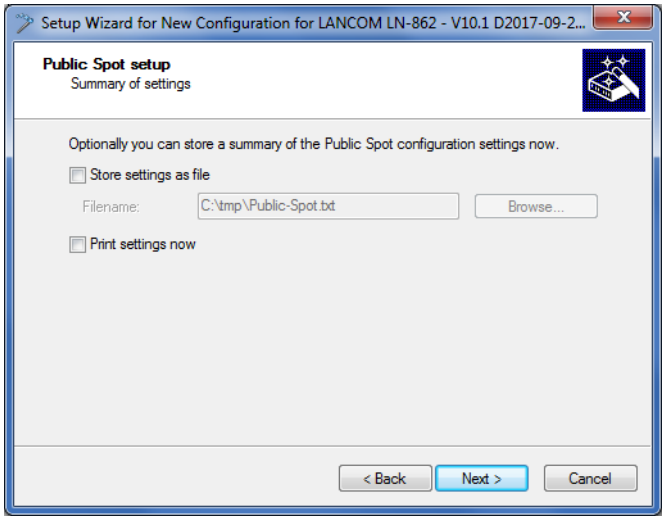


11. Determine whether automatic re-login is allowed for all Public-Spot users, and the maximum absence that is allowed before the user must login again on the Public Spot webpage. To continue, click on **Next**.
The **Automatic re-login** option is a convenience option that allows the Public Spot to automatically authenticate known users or devices. However, if known devices are to be recognized exclusively from the MAC address of the network adapter, the fact that MAC addresses can be falsified represents a potential security risk. For this reason this option is disabled by default.



12. Save your changes if necessary.

Before you save the configuration to your device, you have the option to save the configuration locally on your PC or to print a summary.



13. The click **Next** and finally **Finish** to complete the basic installation of the Public Spot. The Setup Wizard will now send the settings to the device.

That's it! You have completed configuration of your Public Spot module! Now, if you come within range of a Public Spot with a WLAN-capable device, the device can find the SSID that you set up as a public network and login to it.

Manual installation

The following configuration steps show you how to manually setup a Public Spot for simple scenarios. For the application scenario described here, you enable the Public Spot on an interface over which there is no other data traffic other than the Public Spot traffic – where Public Spot and normal WLAN users do not share the same network (dedicated SSID).

This tutorial is only an example. Depending on the device type (access point, WLAN controller, etc.) or complexity of the network configuration (e.g., use of VLAN or ARF), setting up a Public Spot may require different or additional steps. Since this type of network configuration can be highly customized, this tutorial concentrates specifically on a simple example, so that you can adapt the steps as needed.

1. To do this, start LANconfig and select the device on which you wish to set up the Public Spot, for example, an access point. Next, open the configuration menu for the device.
2. Check that the time is correct.

   To check the certificates and correctly record and bill session data, it is important for the Public Spot's time setting to be accurate. First make settings such as time zone and time changes (summer and standard time):

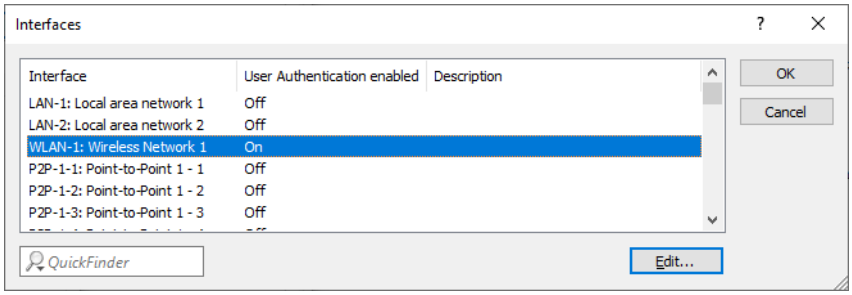
   › LANconfig: **Date/time** > **General**

   In order to ensure that the time of the Public Spot remains correct, the device should be set up as an NTP client. Enter the time server that is necessary for that under **Date/Time** > **Synchronization** > **Time server**. Open the "Add" window to show a list of possible server addresses.

3. Select the interfaces for the Public Spot operation.

   Here you activate the interfaces which will be available to registered users. Along with the logical WLAN interfaces which Public Spot users directly login to, the logical LAN interfaces (LAN-1, etc.), and the point-to-point connections (P2P-1, etc.) can also be selected. When connected via the LAN or P2P interface, additional access points can be integrated into the Public Spot provided by another device. For a single access point, on the other hand, you select, for example, the logical WLAN interface **WLAN-1**.

> LANconfig: **Public Spot** > **Server** > **Operation settings** > **Interfaces**

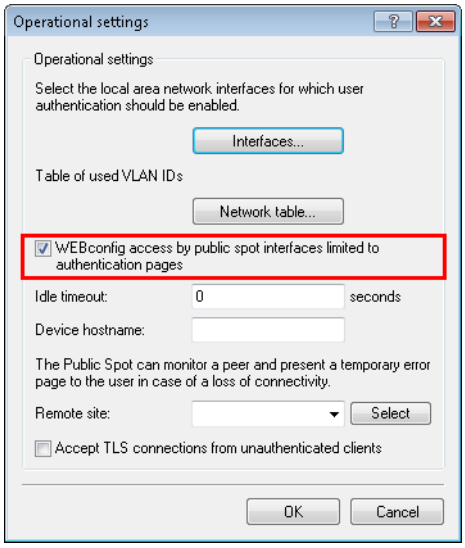


By activating the authentication for a WLAN interface, you automatically release the associated SSID for the Public Spot operation.

On a WLC you can enable certain Ethernet interfaces for the Public Spot. In this manner you can also set up selective restrictions for certain VLANs.

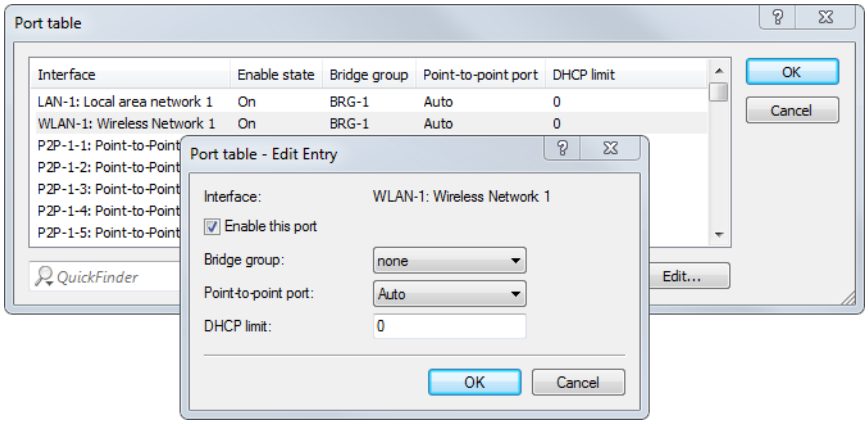
4. Access to your device from the Public Spot network should be restricted to the authentication pages.
   If you do not restrict access, Public Spot users will be able to access the configuration interface of your device (WEBconfig). For security reasons you should not permit this.

   > LANconfig: **Public Spot** > **Server** > **Operational settings** > **WEBconfig access by Public Spot interfaces limited to authentication pages**



5. Disconnect the interface which is to be used for Public Spot operations from the other network traffic.
   In order for end devices to be able to communicate with one another via the different interfaces of a Public Spot device (e.g., between LAN-1 and WLAN-1), these interfaces are logically connected to one another (bridged) within your device. However, in a Public Spot scenario this type of bridging may not be desirable for security reasons. In order to disconnect the communication between an interface (e.g., WLAN-1) assigned to a Public Spot and the rest of the network, you have to remove bridging. In the **Port table** set the **Bridge group** for the respective interface to `none`.

> LANconfig: **Interfaces** > **LAN** > **Port table**

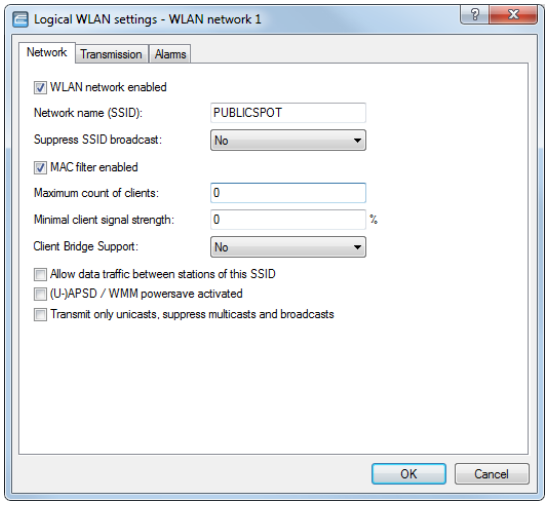


6. Enable the WLAN for the Public Spot.

   This setting does not affect: Routers, WLAN controllers, central-site gateways.

   Activate the logical WLAN which you enabled for the Public Spot login and assign a descriptive name to this network (SSID).

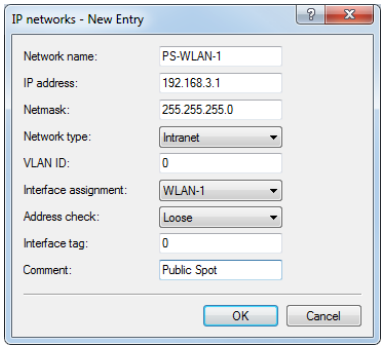
   > LANconfig: **Wireless LAN** > **General** > **Logical WLAN settings** > **WLAN network <number>** > **Network**



If you do not set up a private WLAN, you should disable the setting **Allow data traffic between stations with this SSID** for security reasons. This prohibits communication between the individual Public Spot users.

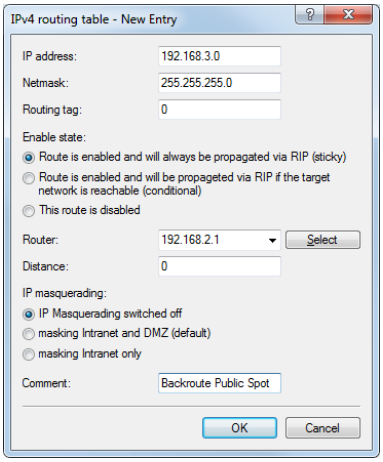
7. Assign the IP address and netmask to the device that your Public Spot network should specify.
   The Public Spot module has its own address on your network, which is independent from the address that you assigned to your device. For example, if you have a 192.168.0.0/24 network set up and your device has the IP address 192.168.2.1, you can assign the IP address `192.168.3.1` and the subnet mask `255.255.255.0`, as long as this IP address has not already been used elsewhere. Select the interface that you chose under **Interface assignment** e.g., `WLAN-1`.

> LANconfig: **IPv4** > **General** > **IP networks**



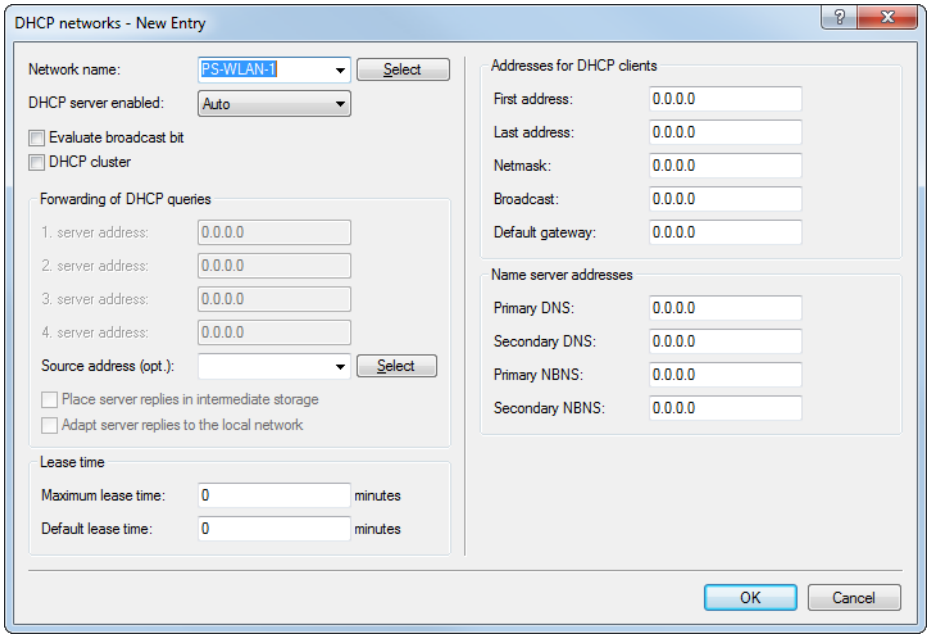
If your device is not directly connected to the Internet and you have a different address range for your Public Spot, you must set up a return route to your Public Spot network on your Internet gateway. If there is no return route, Public Spot users will see an HTTP error after they have successfully authenticated.

Please find the directions on how to set up a return route, in the documentation for your Internet gateway. In LANconfig you configure this under **IP router** > **Routing** > **IPv4 routing table**. To do this, create a new entry and enter the network address of your Public Spot network under **IP Address** and under **Router** enter the address of the Public Spot in your local network.



8. Configure the DHCP server settings for the Public Spot network.
Since the device has an IP network that is independent from the network where it is located, you must configure a DHCP server for this network. For the previously set up IP network (e.g., `PS-WLAN-1`), set the value for **DHCP server enabled** to `Yes`.

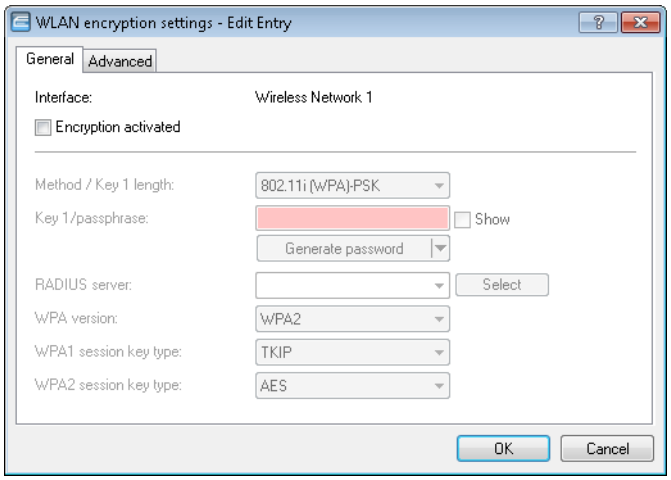
> LANconfig: **IPv4** > **DHCPv4** > **DHCP networks**



9. Disable the encryption for the interface that you are using for the Public Spot.

This setting does not affect: Routers, WLAN controllers, central-site gateways.

Encryption for all logical WLANs is enabled by default. In Public Spot applications, the payload data between the WLAN clients and the access point are usually transmitted unencrypted. For this reason, go to **Wireless LAN** > **Encryption** > **WLAN encryption settings** and disable encryption for the logical WLAN which you previously set up for the Public Spot login.

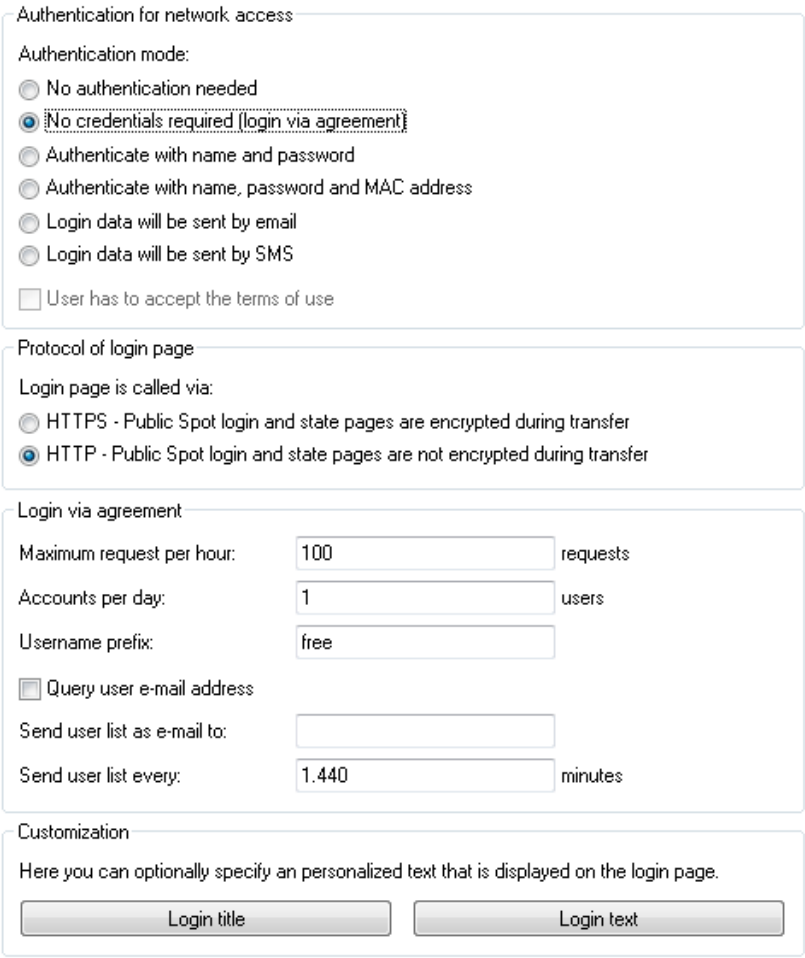


10. Select the authentication mode and the protocol used for the user login.

The authentication method that you select determines the information which users of the Public Spot WLAN must enter when logging in. Select **Authenticate with name and password** to allow your users the option to login with an individual username and password that you have previously assigned them. This setting also allows you to quickly provide Hotspot access to your guests using vouchers (tickets).

Use **HTTPS** as the protocol in order to be able to send encrypted login data to your users during login.

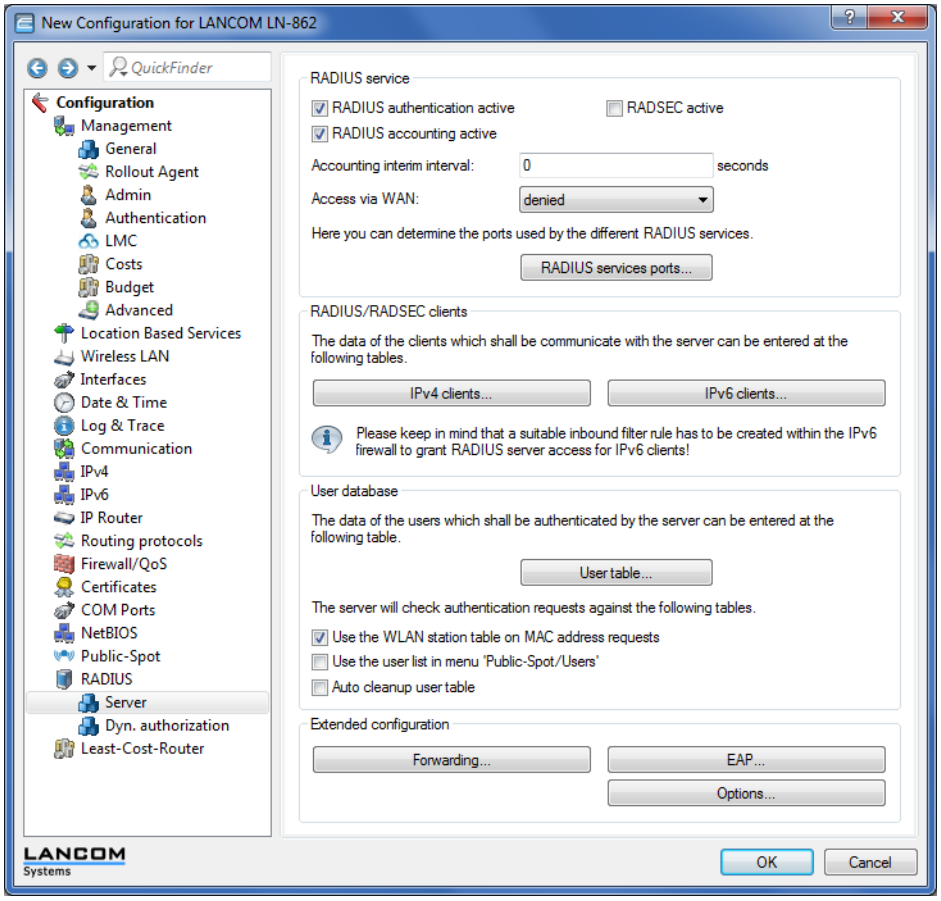
› LANconfig: **Public Spot** > **Authentication** > **Authentication mode**



Pay attention to the fact that, when you select the setting **No authentication needed**, unauthorized persons can have unlimited access to your Public Spot!

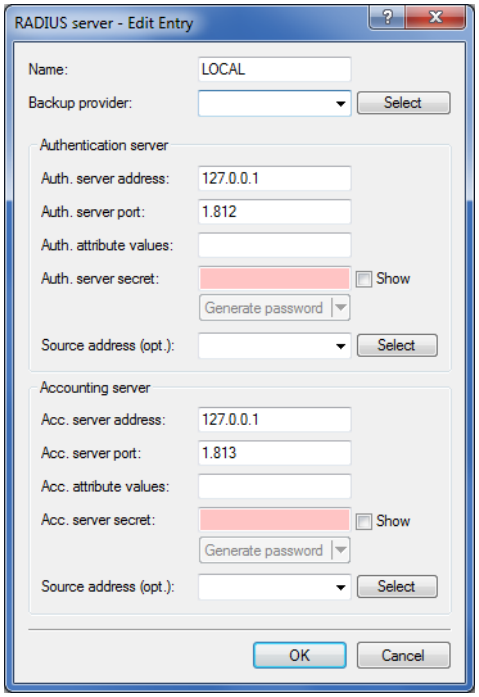
11. Activate the internal RADIUS server for user administration and accounting.
You store Public Spot access accounts in the user database on the device's own RADIUS server.

› LANconfig: **RADIUS** > **Server** > **User database**



12. By default, the Public Spot is preconfigured to use the internal RADIUS server.
The list entry is necessary in order for the Public Spot to recognize the address of the RADIUS server and so that it can authenticate Public Spot access on the internal RADIUS server.

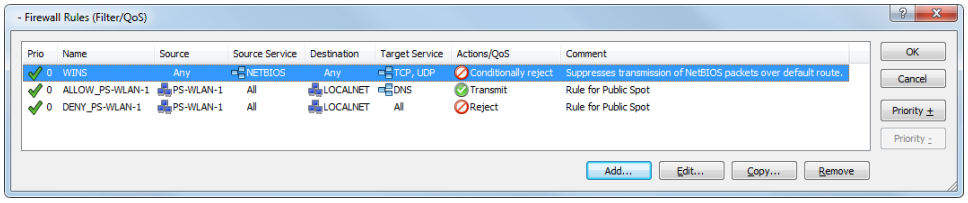
› LANconfig: **Public Spot** > **Users** > **Users and RADIUS servers** > **RADIUS server**

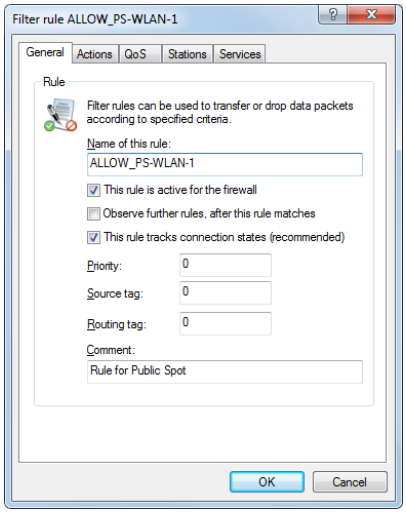


13. Set up filter rules in the Public Spot's firewall to secure your local network. In each case, create an "accept" rule (for example, `ALLOW_PS-WLAN-1`) and a "reject" rule (for example, `DENY_PS-WLAN-1`).

You use the accept rule when devices are to be able to send DNS requests from the Public Spot network to all local networks, e.g., your local intranet. On the other hand, with a reject rule you generally block all access or requests from the Public Spot network to your local network. The order – accept before reject – is essential, since the firewall applies rules from the top to bottom of the list.

› LANconfig: **Firewall/QoS** > **IPv4 Rules** > **Rules…**





› **Settings for the Accept rule:**

a) Enter the name of the rule in **General**, for example, `ALLOW_PS-WLAN-1`.

b) Remove all possible predefined action objects from the list and using **Actions** > **Add..** add an action object of type **ACCEPT**.

c) In **Stations** > **Connection source**, enable the option **Connections from the following stations** and select **Add...** > **Add custom station**.

d) In the Stations window that opens, select the option **All stations in local network** and for **Network name** select the name of your Public Spot IP network, e.g., `PS-WLAN-1`. **Close the dialog with** OK.

e) In **Stations** > **Connection destination**, enable the option **Connections to the following stations** and after selection **Add...** choose **LOCALNET**.

f) In **Services** > **Protocol/target services** enable the option **Following protocol/target services** and select **Add...** > **DNS**.

g) End the filter rule dialog with a final click on **OK**.
LANconfig then enters the allow rule into the rule table.

› **Settings for the Reject rule:**

a) Enter the name of the rule in **General**, for example, `DENY_PS-WLAN-1`.

b) Remove all possible predefined action objects from the list and using **Actions** > **Add..** add an action object of type **REJECT**.

c) In **Stations** > **Connection source**, enable the option **Connections from the following stations** and select **Add...** > **Add custom station**.

d) In the Stations window that opens, select the option **All stations in local network** and for **Network name** select the name of your Public Spot IP network, e.g., `PS-WLAN-1`. **Close the dialog with** OK.

e) In **Stations** > **Connection destination**, enable the option **Connections to the following stations** and after selection **Add...** choose **LOCALNET**.

f) End the filter rule dialog with a final click on **OK**.

LANconfig then enters the rejection rule in the rule table.

14. Store the configuration on your device.

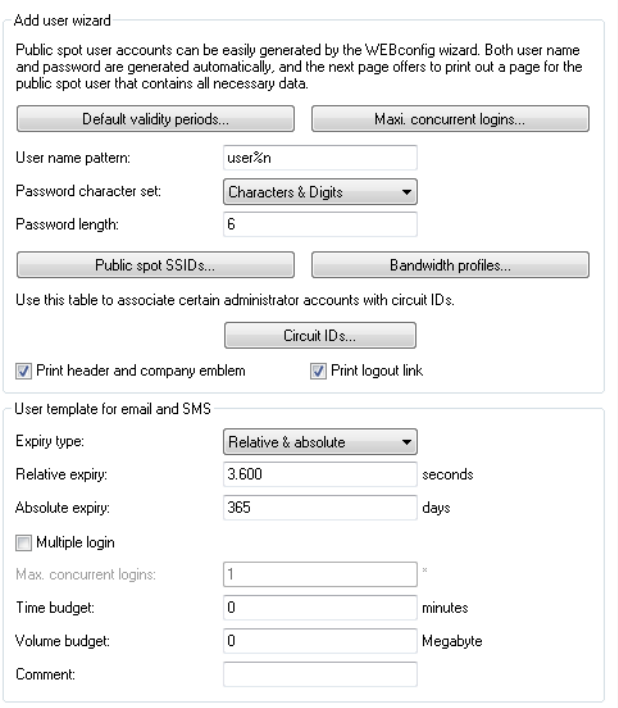
That's it! You have completed configuration of your Public Spot module! Now, if you come within range of a Public Spot with a WLAN-capable device, the device can find the SSID that you set up as a public network and login to it.

Setting default values for the Public Spot wizard

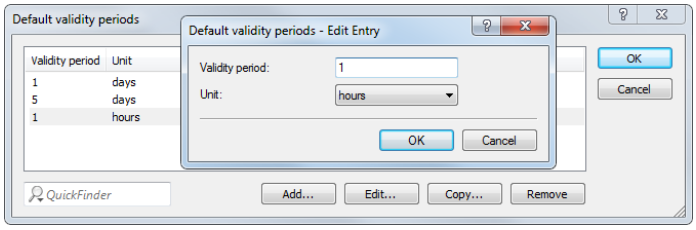
The following section describes how you define default values for the **New user wizard** (setup wizard **Create Public Spot account**) to meet your needs. Public Spot administrators can select the values defined here (e.g. for validity periods, bandwidth profiles, etc.) from selection lists when they are setting up new users and printing out vouchers.

Exceptions to this are the values for User name pattern and Password length shown in the dialog below, which only serve as default values for the device.

1. Start LANconfig and open the configuration dialog for the device.
2. Change the view to **Public Spot** > **Wizard**.

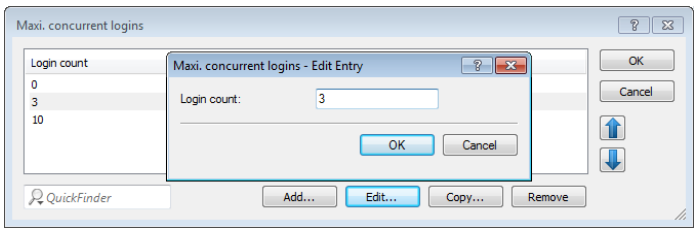


3. In **Default validity periods**, define which default validity periods for user accounts and vouchers are to be available by default.
   The new-user wizard takes the shortest validity period as the default.

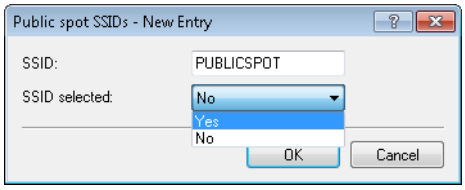


4. Under **Max. concurrent logins** you select the maximum number of devices that have access to the user account simultaneously.

The value 0 stands for 'unlimited'. Whether or not it is generally possible for a user to login with the multiple devices at the same time is determined by the Public Spot administrator with a separate setting in the wizard when creating a new user.



5. In **User name pattern** you specify the pattern used by the new user wizard to create usernames.
   You can enter up to 19 characters, whereby the wizard will automatically create a unique number for every user if you enter "%n". The default description `user%n` will be shown later on the voucher, for example, as `user12345`.
6. Using **Password length** you specify the length of the passwords that the new user wizard generates for Public Spot access.
   The default length is 6 characters. If you would like to have longer passwords, keep in mind that guests can make mistakes when entering them, which can cause unnecessary problems and complaints.
7. Optional: Under **Bandwidth profiles** you set the uplink and downlink limits for each Public Spot user.
   Learn more about this setting under *Manage bandwidth profiles* on page 49.
8. Public Spot via WLAN only: Using **Public Spot SSIDs** you specify the names of the Public Spot networks taken by default when you create new user accounts using the Create Public Spot account wizard.



   The Create Public Spot account wizard automatically marks the specified network names as **SSID selected** when creating a new Public Spot user. If you employ an access point or WLAN controller, you are able to select several network names as default values in order to give users access to different WLANs. When creating a new user and subsequently printing the voucher, these SSIDs are also printed out on the voucher.

   Using the arrow buttons, you can change the order in which the SSIDs are displayed. In this way, the most popular SSIDs can be placed at the top of the list.

That's it! This concludes the configuration of the default values for the Public Spot wizard.

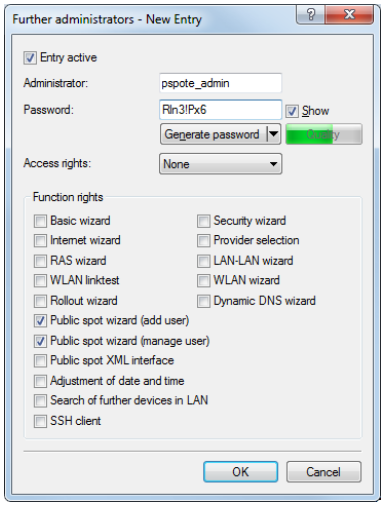
Setting up limited administrator rights for Public Spot managers

It is possible to allow employees to create and manage user accounts even though they do not have access rights to the device configuration. This is done by setting up a limited administrator, who only has the right to use the *Public Spot Wizard*. This tutorial describes the steps and the necessary access rights and privileges to do this in LANconfig.

The rights to use the Public Spot Wizards are configurable separately from one another, so it is possible to restrict a limited administrator to any single Wizard. In the case of the Public Spot setup wizard, the restricted administrator logging in to WEBconfig is automatically forwarded to the corresponding input mask.

1. In LANconfig, open the configuration dialog for the device you want to add a Public Spot administrator to.
   The Public Spot option has to be enabled on this device.
2. Navigate to the item **Management** > **Admin**. In the section **Device configuration**, click **Further administrators** and then click **Add**.

To allow an existing user to perform Public Spot management, you instead select the user's entry in the table and click on **Change**.

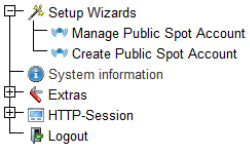


3. You activate the profile by checking the **Entry active** box.
4. Assign a descriptive name in the field **Administrator**.
5. Enter a **Password** and repeat it as a check.
6. Set the **Access rights** to **None**.
7. In the section **Function rights** enable the options **Public Spot wizard (add user)**, and **Public Spot wizard (manage user)** for the Public Spot setup wizard.

   The function right **Public Spot XML interface** is not required by a Public Spot administrator. The right is only relevant if you use the XML interface and should not be combined with the function rights described above for security reasons.

8. Save the new or modified administrator profile by clicking on **OK**.

If you have granted the feature rights to several Wizards, the limited administrator can navigate between these using the navigation bar in WEBconfig.



If you have set the function right for the **Public Spot Wizard (create user)** only, then a limited administrator can only navigate within this Wizard, and the navigation bar is hidden. In this case it is not possible to logout of WEBconfig manually. For security reasons, this means that the lifetime of the WEBconfig session is very short. In case of inactivity, the device automatically logs out the limited administrator.

For technical reasons, the Create Public Spot Account wizard does not update automatically after use of the **Create and CSV export** button. A limited administrator who wishes to set up additional users and print vouchers must invoke the Wizard again (e.g. via a URL or by refreshing the web page if the navigation bar is hidden).

Setting up and managing Public Spot users for simple scenarios

You can set up and manage Public Spot users either manually or by using the setup wizard. Setting up and managing the configuration options manually offers you more extensive options and allows you, for example, to create self-defined users with an unlimited lifetime.

On the other hand, the setup wizard allows you to create generic Public Spot users with automatically generated login data with limited lifetimes. The respective setup wizard is only accessible using WEBconfig, which allows you to quickly create users without requiring administrator permissions for the entire device. The only requirement is an administrator with limited permissions.

You naturally also have the option to initially create generic users with the aid of the setup wizard and then manually adapt them to your needs (e.g., change the usernames).

Setup and management using the Setup Wizard (WEBconfig)

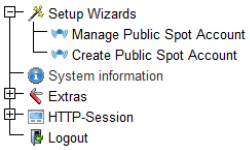
The Setup Wizards provide you with an easy method of managing Public Spot users.

Adding Public Spot users with a single click and voucher printing

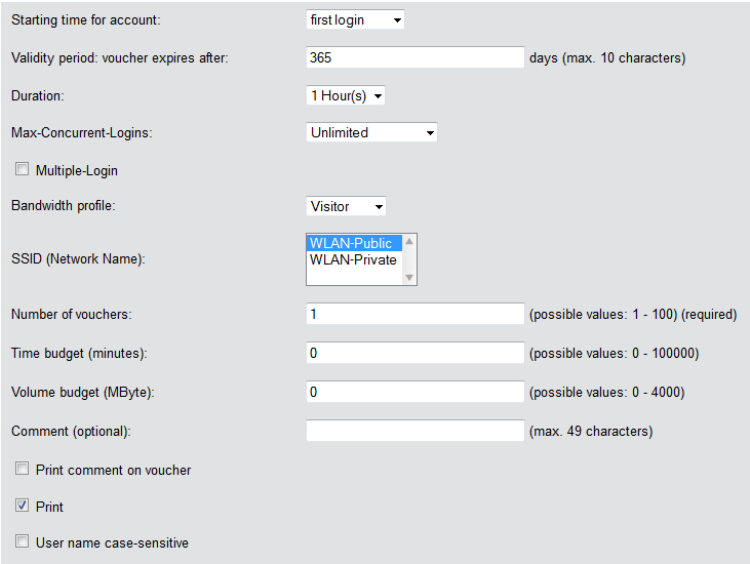
The following section describes the setup of a Public Spot user using WEBconfig and then printing a voucher. You can also prepare vouchers in advance.

You need the permissions for the **Public Spot Wizard (create user)**, in order to create a new Public Spot user.

1. Log on to the WEBconfig home page as an Administrator.
2. Start the setup wizard by clicking on **Setup wizards** > **Create Public Spot account**



3. The new user wizard starts with an input screen. The fields have default values.



The wizard automatically creates a username and a password. In the subsequent printout dialog you can select the voucher printer and print-out the voucher.

4. If necessary, you can change the default values before you print it.

   The following entries affect the appearance as well as the validity of the vouchers:

   - **Starting time for account**: Sets the time when the voucher becomes valid. With the setting **first login**, the access budget runs as of the first login; with the setting **immediately**, it applies as of the time that the user was created.

To a supply of vouchers in advance, select `First login` as the validity of the vouchers. That way the vouchers will still be valid even after a longer period.

- **Validity period: Voucher expires after**: Enter the overall time period within which the voucher can remain valid. If the access is to be valid immediately, it is not possible to enter a validity period.
- **Duration**: Set how long access is to be available after registration or the first login. The values listed here are managed in the **Default validity periods** table.
- **Max-Concurrent-Logins**: Select the maximum number of concurrent devices that can have access to the user account for the corresponding user. The values listed here are managed in the **Max. concurrent logins table**.
- **Multiple login**: Select this option in order to generally allow users to login with several devices using the same login data. The number of devices that can be logged on simultaneously is specified using the drop-down list **Max-concurrent-logins**.
- **Bandwidth profile**: Select a bandwidth profile from the list in order to selectively restrict the amount of bandwidth available to the user (uplink and downlink). Create a bandwidth profile in the **Bandwidth profile** table.
- **SSID (network name)**: Specify which wireless LAN network the access applies to. This SSIDs listed here are managed in the **SSID table**. By pressing the "Ctrl" button you have the option of selecting multiple entries. Default entries are already pre-selected.

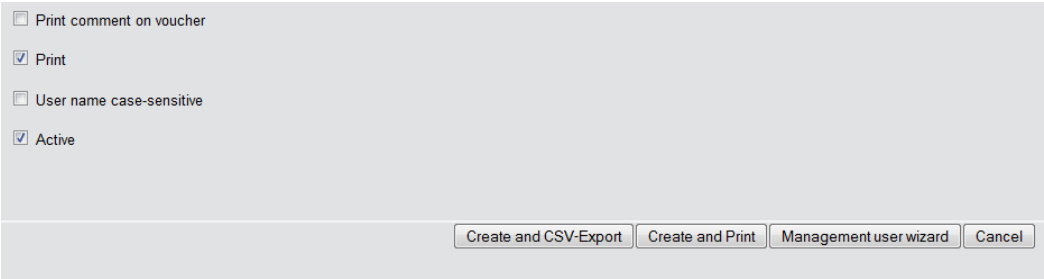
  If you have not defined any entries in the table, the wizard conceals this option.

- **Number of vouchers**: Specify how many vouchers you want to create at a time. If you set the login time as the access start time, you can print-out a supply of vouchers in advance.
- **Time budget (minutes)**: Specify the amount of time after which access to the Public Spot is closed. Depending on the chosen expiry method, access time is limited either to the time budget (incremental) or to the set voucher validity period (absolute).
- **Volume budget (MByte)**: Specify the available data volume after which access is closed.
- **Comment (optional)**: Enter a comment here. This comment can contain, for example, additional notes about the access duration or the telephone number of the receptionist in case of access problems.
- **Print comment on voucher**: Check this option if the comment is to appear on the voucher.
- **Print:** Check this option to print the vouchers as soon as they are registered.
- **User name case-sensitive**: Enable this option if Public Spot users have to pay attention to capitalization when entering their user name at login.

5. If you want to keep the default values or accept the new values without changing them, you click on **Save and print** at the end.

   If the **Print** option is disabled, the wizard displays a summary of the new Public Spot users after they have been registered. You then have the opportunity to print the vouchers again.

   The button **Manage User Wizard** button takes you to the **Manage Public Spot Account** Setup Wizard.



   You have the option to either show or hide this button. It is displayed by default.

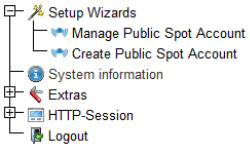
Wizard for Public Spot user management

The following section describes how to use WEBconfig to manage the registered Public Spot users.

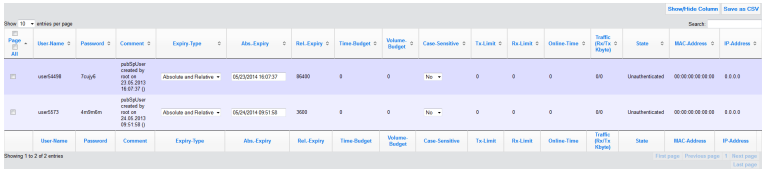
You need the **Public Spot wizard (user management)** permission, in order to manage a Public Spot account.

Unsaved changes are lost once you finish this wizard.

1. Log on to the WEBconfig home page as an Administrator.
2. Start the setup wizard by clicking on **Setup-Wizards** > **Manage Public Spot accounts**



3. The Public Spot wizard starts with a list of registered Public Spot users.



In the **Show... entries per page** drop-down list you set how many entries are displayed per page. The corresponding pages are accessed via the page navigation at the lower right:

- **First page**: Shows the page with the first entries.
- **Previous page**: Returns to the previous page.
- **Page numbers (1, 2, 3, ...)**: Goes directly to the chosen page.
- **Next page**: Goes to the next page.
- **Last page**: Shows the page with the latest entries.

With **Search** you can filter the displayed entries. The filter immediately searches for entered strings.

You export highlighted entries with **Save as CSV**.

The column headers have the following meaning:

- **Page/All**: This column is used to select the user for the desired action (print, delete, save). To select all entries on the current page, select **Page**. To select all of the entries, select **All**.
- **User name**: Manually or automatically displays the username generated by the system.
- **Password**: Manually or automatically displays the password generated by the system.
- **Comment**: Includes the comment entered at registration (in brackets) and any changes to the user data (automatically documented by the system).
- **Expiry type**: Indicates whether the validity period of this user account is absolute (e.g. expires on a set date) or relative (expires after the time has elapsed since the first successful login).
- **Abs.-Expiry**: If "absolute" has been selected as the expiry type, the user account becomes invalid at the time defined in this field.
- **Rel.-Expiry**: If "relative" has been selected as the expiry type, the user account becomes invalid after this time period has expired since the user logged in for the first time.
- **Time budget**: Specifies the maximum access time for this user account. The user can use this duration of access time until a relative or absolute expiry time (if set) is reached.
- **Volume budget**: Specifies the maximum data volume for this user account. The user can use this data volume until a relative or absolute expiry time (if set) is reached.
- **Case sensitive**: Indicates whether the login page takes capitalization of the user name into account.
- **Tx-Limit**: If a bandwidth profile was entered for the user, this entry shows the maximum transmission bandwidth available to that user.

- **Rx-Limit**: If a bandwidth profile was entered for the user, this entry shows the maximum receiving bandwidth available to that user.
- **Traffic (Rx/Tx Kbyte)**: Indicates the data volume in kilobytes that the user has received (Rx) or sent (Tx) so far.
- **State**: Displays the authentication status of each user, i.e. whether the user is currently logged on to the Public Spot (**Authenticated**) or not (**Unauthenticated**).
- **MAC address**: Indicates the physical address of the network adapter for the device with which the user is currently connected.
- **IP address**: This shows the IPv4 address that the system currently has allocated to the user.

The buttons at the bottom of the window have the following functions:

- **Print**: Print out the voucher for the selected user.
- **Delete**: Delete the selected user.
- **Save**: Save the changes.
- **Back to main page**: Return to the main page; all unsaved changes will be lost.

You can edit the following user information by changing the contents of the corresponding fields:

- **Expiry type**
- **Abs.-Expiry**
- **Rel.-Expiry**
- **Case sensitive**

4. Select the account that you want to edit in the first column.
5. Change the corresponding field values and click **Save** to apply the changes. Unsaved changes are lost once you finish this wizard.
6. If you would like to delete a user, mark the corresponding entry in the first column and click **Delete**.

The deletion takes place immediately without confirmation.

Hiding fields in WEBconfig

In the setup wizard "Manage Public Spot Account", the **Show/hide column** button enables you to display or conceal columns of the table. These changes are only temporary. Hidden columns are shown again after a page refresh or in a new session.

If you want to permanently hide specific fields, use the LCOS menu tree and navigate to the view **Setup** > **Public Spot module** > **Manage user wizard**. All of the fields are displayed by default. If you hide certain fields, for example to conceal the time budget, they will stay hidden in the wizard itself and also in the drop-down menu behind the button **Show/hide column** after reloading the page.

In order to delete authenticated Public Spot users, the columns "Calling station ID mask" and "Called station ID mask" need to be visible in the wizard. Unauthenticated users can be deleted even if these two columns are hidden.

Please note that hidden fields are not printed out when you press the **Print** button. On the other hand, exporting a CSV file includes all of the data. The **Save as CSV** button can optionally be hidden. To do this, use the LCOS menu tree to navigate to the view **Setup** > **Public Spot module** > **Add User Wizard** > **Hide CSV export** . Select "Yes" and save your entry.

Manual set up and management

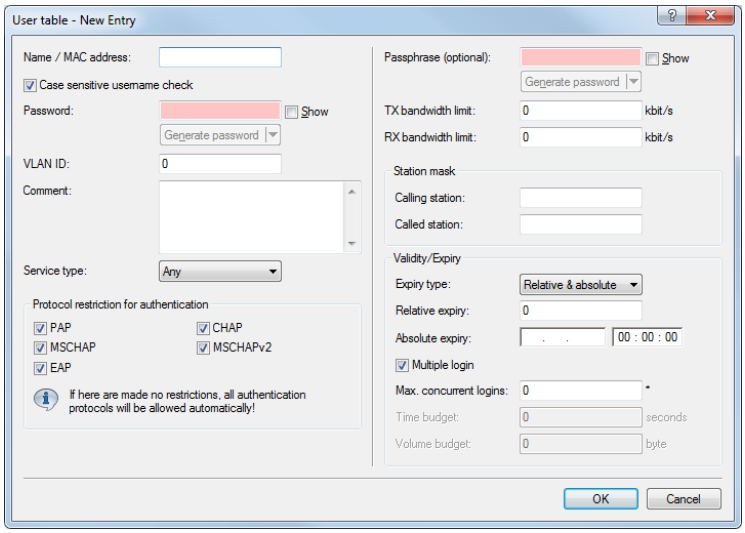
The following configuration steps show you how to use LANconfig to manually setup a Public Spot user for simple scenarios. You create and manage Public Spot users using the **User database** of the device's internal RADIUS server under **RADIUS** > **Server** > **User database**. Here you enter all of the users who should have access to the Public Spot – just as the setup wizard does as well.

For user administration, the Public Spot module also has its own internal list (found under **Public Spot** > **Users** > **User list**). During technical development, this list was replaced as of LCOS 7.70 by the user administration via RADIUS. For compatibility reasons, the device still evaluates the internal user list of the Public Spot module if it is enabled. However, for a new installation you should no longer use this list, since it prevents you from using many features (setup and administration using the wizard, bandwidth restrictions, accounting via RADIUS, VLAN IDs for Public Spot users, etc.).

1. In **Name** you enter the usernames of future users or the **MAC addresses** of their end devices.

   If you selected the authentication mode **Login with name and password**, enter the name of the username that the user employs to authenticate on the Public Spot. Entering a **password** is optional, however it is recommended for the authentication mode above.

   > LANconfig: **RADIUS** > **Server** > **User database** > **User table**



   If the authentication is performed using the MAC address (authentication modus **Authenticate with name, password and MAC address**), you define the MAC address using the field **Calling station** in the format `12:34:56:78:90:AB`.

2. Set the **Service-Type** to `Login`.

3. You remove all protocol restrictions by deselecting all check boxes.
   Two-phase authentication is not performed in a Public Spot scenario. This only makes sense for direct WLAN connections without Public Spot operations and the associated RADIUS users.

   If you do not completely remove the protocol restrictions, a user cannot log in using the login web page of your Public Spot!

4. Optional: On request, you can also, for example,

   > Enter a relative and/or absolute expiry date for the validity of the user account in the section **Validity/Expiry** (relative = validity in seconds after the first login);
   > Limit the uplink/downlink under **TX/RX bandwidth limit**;
   > Enable **Multiple login** and enter the **Max. concurrent logins** of end devices

5. Store the configuration on your device.

That's it! Your Public Spot users can now login with the credentials that you specified.

1.2.2 Security settings

The Public Spot has two additional safety mechanisms that effectively protect it against abuse.

Traffic limit option

In order for clients to login to the Public Spot via a browser, it must be possible for unauthorized users to transfer data packets (e.g. for DNS requests) to the access point. By default, there is no limit on this data. The following risks are associated with this:

- **Unauthorized use of the Public Spot:** Certain tools enable a user to pack data into a DNS packet (i.e. to establish a DNS tunnel) and to work with the Public Spot without logging in.
- **Denial-of-Service:** The attacker could send large amounts of data to the device and thus try to block the device or Public Spot.
- **Brute force:** The attacker could repeatedly try to access the base station by guessing the login data until successfully breaking in.

The traffic limit option can effectively eliminate these risks.

You enable the traffic limit option by setting a value other than "0". This value determines the maximum data quantity in bytes that can be transmitted between the base station and an unauthorized terminal device.

- LANconfig: **Public Spot** > **Server** > **Allow access without authentication** > **Maximum data volume**

When a terminal device exceeds this traffic volume, the Public Spot locks this device and drops all data received from it without inspection. This lock expires only when the device entry disappears from the station table.

For WLAN devices, this deletion can follow the general idle timeout, for example:

- WEBconfig: **Extras** > **LCOS menu tree** > **Setup** > **WLAN** > **Idle-Timeout**

Please keep in mind that if station monitoring is active, the lock may be removed earlier. If the mobile station cannot be reached for 60 seconds, the device removes its entry from the station table, and also the block.

The idle timeout for the Public Spot module has the same purpose as the idle timeout for WLANs, but it applies only to connections via Public Spots. If the idle timeout is set and no further data packets are received from a user, the device automatically logs the device out at the end of the specified time period.

- LANconfig: **Public Spot** > **Server** > **Idle timeout**

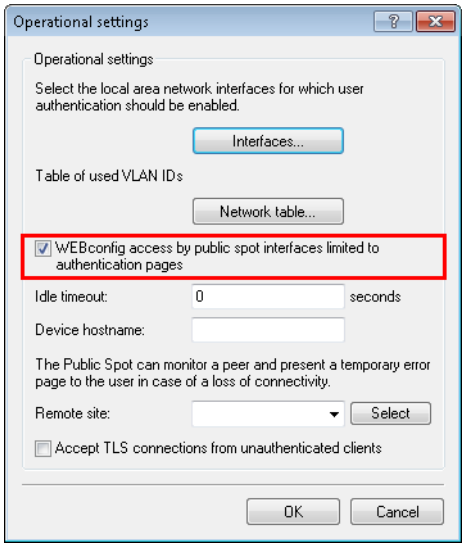
On the one hand the optimal value for traffic limit depends on the data volume of the login page. On the other hand, this value has a significant effect on the potential number of failed login attempts per user. Generally, a traffic limit of 60,000 bytes provides effective protection for a Public Spot but allows a sufficient number of login attempts. You can adjust this value to your individual needs, if necessary. The default value of "0" bytes allows an unlimited volume of data.

The traffic limit option only monitors the traffic before authentication. It does not take into account the traffic to and from a free Web server. This remains unlimited at all times.

Restricting access to the configuration

Public Spot access to a Public Spot network's configuration (WEBconfig) should always be prohibited for security reasons. A special switch allows access via the Public Spot interface to be restricted to the Public Spot authentication pages only. All other configuration protocols are automatically blocked.

- LANconfig: **Public Spot** > **Server** > **Operational settings** > **WEBconfig access by Public Spot interfaces limited to authentication pages**



Note that using permissions under **Management** > **Admin** > **Configurations access ways** > **Access rights** you cannot generally limit the access via HTTP(S) to the device.

1.2.3 Extended functions and settings

The Public Spot offers a wide range of extended functions, options and parameters, which can be used to adapt it to the specific requirements of the application at hand.

In the following sections you will find information about:

- Multiple logins

  By default, the use of login data is restricted to login with one device. Find out how you increase this limit or completely remove this limit for a user account.

- Open access networks (no login)

  Setup additional networks so that Public Spot users can also reach them without logging in to the Public Spot to provide the user with additional information (e.g., customer web sites inside the company, event calendars in a hotel).

- User administration using the Web API

  Use URLs to create and administrate Public Spot users with file links or scripts.

- Individual bandwidth limitation

  Individually set uplink and downlink restrictions for each Public Spot user.

- Automatic cleanup of user accounts and mobile stations

  Use the device's own functions to automatically delete expired Public Spot user accounts and improperly logged off mobile stations (WLAN only) from the device's internal databases.

- WLAN handover of sessions between devices

  Find out more about the roaming possibilities of mobile stations between access points, and what special configurations are necessary so that your users benefit from the seamless handover of WLAN sessions.

- Authentication via RADIUS

  Find out how you can provide multiple RADIUS servers for authentication and accounting, and how you can chain them, in order to forward the user data to the appropriate backup system in case individual systems are unavailable.

- Accounting for Public Spot connections for commercial operation

  Learn more about the accounting functions provided by the Public Spot for commercial operations. These billing functions can be roughly divided into two models:

  - Retrospective payment for the resources actually used (credit accounting)
  - Service use on a debit payment basis (PrePaid)

- Using multi-level certificates

  Find out how to load certificate chains on your device.

- Individual assignment of VLAN IDs

  Find out how to assign individual VLAN IDs to specific Public Spot users.

Multiple logins

You have the ability to allow Public Spot users to simultaneously sign in using one user account for multiple devices. This can be necessary for a group of people (for example, a family) that has multiple devices, which they would like to use to simultaneously access the Internet.

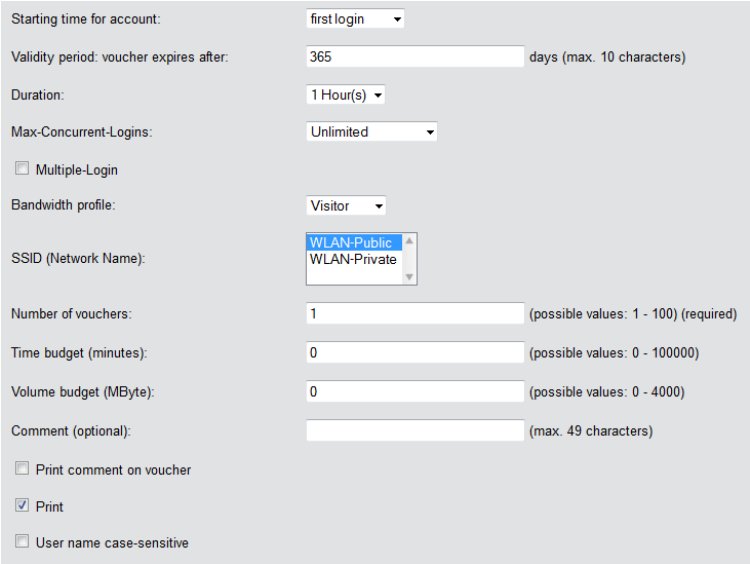
Setting default values

To use this feature, define the number of concurrent devices in the setup menu under **Public Spot module** > **Add user wizard** > **Max. concurrent logins table**. Enter the values here that you assigned in the second step with the **Create Public Spot account**. The value 0 stands for "unlimited".

Enabling multiple logins in the new user wizard

When you invoke the Wizard **Create Public Spot account**, you will see the menu item **Max concurrent logins**. The values shown here correspond to the numbers that you previously entered in the table of the same name. The values are shown within the phrase "Only ... device(s)".

Select the maximum number of concurrent devices that can have access to the user account for the corresponding user. Please note that to enable the feature in the wizard, the option **Allow multiple logins** must also be enabled.



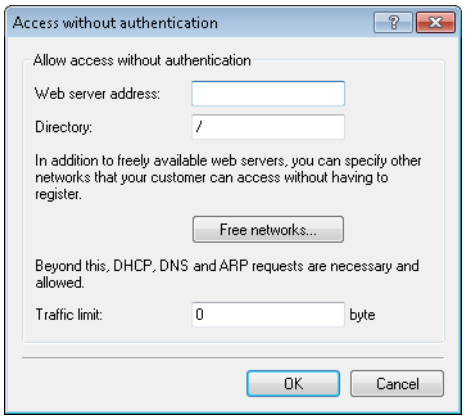
Open access networks (no login)

To provide users with access to important information without them having to login (e.g., important contact information) you can define any publicly available Web server.

> LANconfig: **Public Spot** > **Server** > **Access without authentication**

If you do not want to completely release this service, you can optionally define an alternative path to the web server.

> LANconfig: **Public-Spot** > **Server** > **Access without authentication** > **Directory**

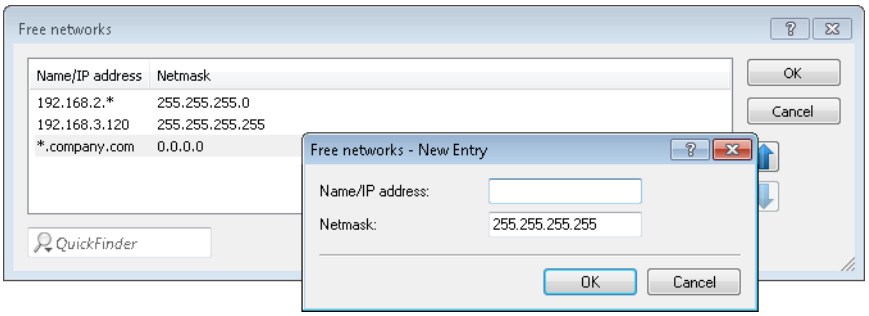


In addition to freely available web servers, you can define other networks and special sites which your customers can access without having to log on.

> **Public-Spot** > **Server** > **Access without authentication** > **Free networks**

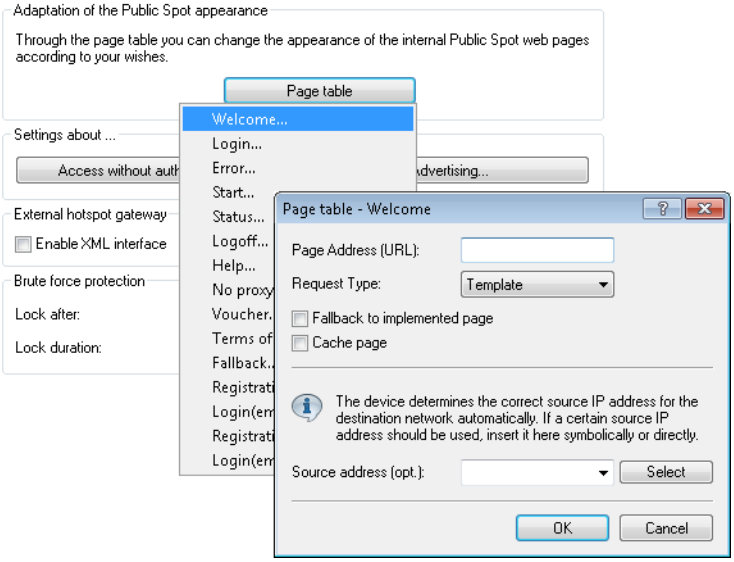
Enter the IP address of the server or of the network with its netmask, that your Public Spot users are to be given access to. Alternatively, you have the option of entering a domain name (with or without a wildcard "*"). Wildcards can be used, for example, to allow free access to all of the subdomains of a particular domain. The entry `*.company.com` allows the addresses `mail.company.com`, and `service.company.com`, etc.

If you wish to authorize a domain or just a single workstation with the address named earlier, set `255.255.255.255` as the netmask here. If you wish to authorize a whole IP network, specify the corresponding netmask. If you do not set a netmask (value `0.0.0.0`), the device ignores the table entry.



> **Public Spot** > **Server** > **Page table**

Enter the addresses (URLs) of the web pages to be displayed to users on the Public Spot in case of login, error, status display, etc. Read the chapter about *Default and customized authentication pages*.



DNS snooping

Web services with a high number of users distribute the requests for data to multiple servers for better utilization. This means that two DNS queries for the same hostname (e.g. "www.google.com") can lead to to two different IP addresses. If a Public Spot receives more than one valid IP address for the specified host name from the DNS server, it chooses one of them and stores it for future requests by Public Spot users. If a different IP address for the same host name is allocated to the user by a different server for a subsequent request, the Public Spot blocks this connection because this IP address is not stored as the authenticated one.

In order for Public Spot users to be able to connect to the requested host despite changing IP addresses, the Public Spot analyzes the user's DNS queries and stores the returned IP address with the host name, the valid time to live (TTL), the age and the data source as a free destination address in the table **Status** > **Public Spot** > **Free-Hosts** for subsequent use.

The entries in this table will expire after the time period defined in the DNS response (TTL). When the limits are very low (e.g. 5 seconds), you can avoid locking out Public Spot users immediately after a request by setting a minimum validity under **Setup** > **Public Spot-Module** > **Free-Hosts-Minimum-TTL**.

Managing Public Spot users via the web API

As an alternative to using the Setup Wizard, entering a special URL in the address bar gives you the option of displaying, creating or deleting Public-Spot users directly.

URL structure

The URL is structured as follows:

```
http://<Device-URL>/cmdpbspotuser/...?action=actiontodo&parameter1=value1&parameter2=value2
```

The following actions are available:

- **action=addpbspotuser**: Creates one or more new Public Spot users and then prints out the required number of vouchers.
- **action=delpbspotuser**: Deletes the Public Spot user with the specified user ID.
- **action=editpbspotuser**: Displays the Public Spot user with the specified user ID. You can then print out the user's voucher again.

The required parameters and their values depend on the action specified.

The Wizard ignores incorrect parameter information and accepts only the correct parameters. If you omit a required parameter or specify it incorrectly, the wizard displays an input mask. Enter the correct parameter values here.

Adding a Public Spot user

To register a new Public Spot user, simply enter the following URL:

```
http://<Geräte-URL>/cmdpbspotuser/
   ?action=addpbspotuser&parameter1=value1&parameter2=value2&...
```

The following parameters are available:

`comment`

Comment on the registered user

If it is possible to enter multiple comments for a Public Spot user, you can enter the comments and their corresponding comment-field names as follows:

```
&comment=<Content1>:<FieldName1>;<Content2>:<FieldName2>;...;<Content5>:<FeildName5>
```

If there is just one comment field per user, then the comment is entered as follows:

```
&comment=<Comment>
```

Special characters such as German umlauts are not supported.

The maximum number of characters for the comment parameter is 191 characters.

`print`

Automatic print-out of the voucher.

If this parameter is omitted, the wizard displays a button that you can use to print the voucher.

`printcomment`

Print the comment on the voucher.

If this parameter is omitted, no comment will appear on the voucher (default setting).

`nbGuests`

Number of Public Spot users to be created.

If this parameter is omitted, the wizard creates one user only (default setting).

`defaults`

Use default values

The wizard replaces missing or incorrect parameters with default values.

`expirytype`

Combined output of expiry type and, if applicable, the validity period of the voucher.

Specify this parameter as follows:

```
&expirytype=<Value1>+validper=<Value2>
```

The parameter values have the following meaning:

- `Value1`: Expiry type. Possible values are `absolute`, `relative`, `both`, and `none`.

- `Value2`: Time of the voucher's expiry if `expirytype` has the value `both`. In this case, you use `validper` to specify the voucher's maximum validity period in days for the absolute expiry type. For all other expiry types, the parameter `validper` is not set.

If a parameter is omitted or set with incorrect values the wizard will apply the default values.

`ssid`

Network name

If this parameter is omitted, the wizard uses the default network name (default setting).

`unit`

Access time

Specify this parameter as follows:

```
&unit=<Value1>+runtime=<Value2>
```

The parameter values have the following meaning:

- `Value1`: LIfetime units. Possible values are: Minute, hour, day
- `Value2`: Duration

`timebudget`

Time budget

If this parameter is omitted, the wizard uses the default value.

`volumebudget`

Volume budget

The following entries are allowed:

- `k` or `K`: Specified in kilobytes (kB), e.g. `volumebudget=1000k`.
- `m` or `M`: Specified in megabytes (MB), e.g. `volumebudget=1000m`.
- `g` or `G`: Specified in gigabytes (GB), e.g. `volumebudget=1g`.

Without a unit, the specification corresponds to a value in bytes (B).

If this parameter is omitted completely, the wizard uses the default value.

`multilogin`

Multiple logins

If you specify this parameter, the user can login multiple times with his/her user account. If this parameter is missing, multiple logins are disabled by default.

`maxconclogin`

Maximum number of concurrent logins

With this parameter you specify with how many different end devices a user can login to a Public Spot. Valid entries are integers such as `0, 1, 2, ....`

If this parameter is missing or if the parameter has the value `0`, this means that the number of devices is unlimited.

This parameter requires that multiple logins be enabled. Setting this parameter in isolation has no other effects.

casesensitive

Username case sensitive

If you enter this parameter, the Public Spot user must pay attention to capitalization when entering the user name at login. Valid values are:

- `0`: Case-sensitive username is disabled
- `1`: Case-sensitive username is enabled

If this parameter is omitted, the wizard uses the default value.

bandwidthprof

Bandwidth profile

With this parameter you assign a pre-defined bandwidth profile to a Public Spot user. Enter the valid value for this parameter as the line number of an existing profile name under **Setup** > **Public Spot module** > **Add user wizard** > **Bandwidth profiles**, such as

```
&bandwidthprof=1
```

to index the first entry in the table.

If this parameter is missing or the line number is invalid (for example, the table is empty), the wizard does not limit the bandwidth.

If the Public Spot administration contains no default values to replace missing parameters, the wizard opens a dialog. Enter the missing values here.

Modifying a Public Spot user

Modify one or more Public Spot users simply by entering the following URL:

```
http://<device-URL>/cmdpbspotuser/...?action=editpbspotuser&parameter1=value1&parameter2=value2&...
```

The following parameters are available:

pbspotuser

Name of the Public Spot user

Specify multiple users in the form `&=pbspotuser=<User1>+<User2>+....`

If the wizard cannot find the specified user, you have the option to search for a user.

After making your changes, accept these and print them out if necessary.

expirytype

Combined output of expiry type and, if applicable, the validity period of the voucher.

Specify this parameter as follows:

```
&expirytype=<Value1>+validper=<Value2>
```

The parameter values have the following meaning:

- `Value1`: Expiry type. Possible values are `absolute`, `relative`, `both`, and `none`.
- `Value2`: Time of the voucher's expiry if `expirytype` has the value `both`. In this case, you use `validper` to specify the voucher's maximum validity period in days for the absolute expiry type. For all other expiry types, the parameter `validper` is not set.

If a parameter is omitted or set with incorrect values the wizard will apply the default values.

unit

Access time

Specify this parameter as follows:

```
&unit=<Value1>+runtime=<Value2>
```

The parameter values have the following meaning:

- `Value1`: LIfetime units. Possible values are: Minute, hour, day
- `Value2`: Duration

timebudget

Time budget

If this parameter is omitted, the wizard uses the default value.

volumebudget

Volume budget

If this parameter is omitted, the wizard uses the default value.

print

Automatic print-out of the voucher.

If this parameter is omitted, the wizard displays a button. Use this to print out the voucher.

bandwidthprof

Bandwidth profile

With this parameter you assign a pre-defined bandwidth profile to a Public Spot user. Enter the valid value for this parameter as the line number of an existing profile name under **Setup** > **Public Spot module** > **Add user wizard** > **Bandwidth profiles**, such as

```
&bandwidthprof=1
```

to index the first entry in the table.

If this parameter is missing or the line number is invalid (for example, the table is empty), the wizard does not limit the bandwidth.

If the Public Spot administration contains no default values to replace missing parameters, the wizard opens a dialog. Enter the missing values here.

Deleting a Public Spot user

Delete one or more Public Spot users simply by entering the following URL:

```
http://<deviceURL>/cmdpbspotuser/...?action=delpbspotuser&pbSpotuser=<User1>+<User2>+...
```

If the wizard finds the specified user in the user list, the user is deleted and the wizard displays a confirming message.

If the wizard cannot find the specified user, it displays a table of registered Public Spot users. Mark the entries for deletion here.

Creating Public Spot users on a remote Public Spot gateway

With Smart Ticket operating, each user is given a Public Spot account on the RADIUS server of the local Public Spot gateway.

However, where multiple Public Spot gateways are in use but the user accounts should be managed by the RADIUS server of just one gateway, Smart Ticket causes the Public Spot account to be created on this central RADIUS server. To

implement this, the remote Public Spot gateway needs to be specified in the LCOS menu tree under **Setup** > **Public Spot module** > **Authentication modules**.

If no remote Public Spot gateway is defined, the Public Spot user accounts are created on the local Public Spot gateway.

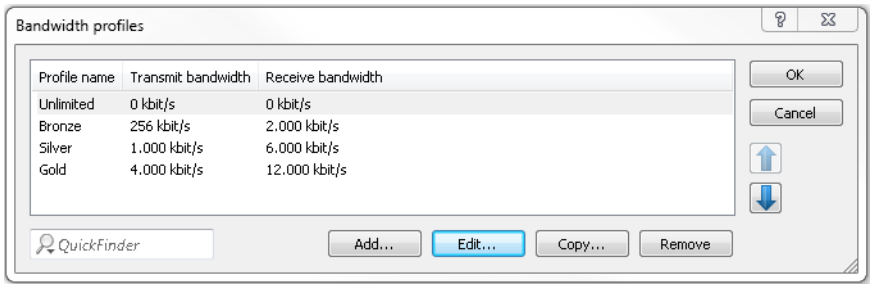
Bandwidth profile

Manage bandwidth profiles

Using the window **Public-Spot** > **Wizard** > **Bandwidth profiles**, you have the ability to set up profiles that limit the available bandwidth (uplink and downlink) for Public Spot users. You can select a predefined profile or create your own bandwidth profiles that meet your needs. These profiles can be assigned to new users when access is created for the Public Spot by calling the Setup-Wizard **Cerate Public Spot account** in WEBconfig.

Integrating predefined bandwidth profiles

From the four predefined profiles, select the bandwidth profile that closest meets your requirements:



Unlimited

No restriction in the transmit and receive bandwidth.

These values refer to the transmit bandwidth (TX) and receive bandwidth (RX) from the perspective of the client.

Bronze

The transmit (TX) bandwidth is 256 kbps, the receive (RX) bandwidth is 2 Mbps.

Silver

The transmit (TX) bandwidth is 1 Mbps, the receive (RX) bandwidth is 6 Mbps.

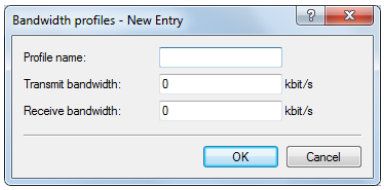
Gold

The transmit (TX) bandwidth is 4 Mbps, the receive (RX) bandwidth is 12 Mbps.

You have the option of customizing the predefined entries to meet your requirements. Select the profile for editing and click the button **Edit**. Alternatively, you can create your own profiles.

Creating your own bandwidth profiles

In order to add manual entries to the table **Bandwidth profiles**, click on the button **Add...**.



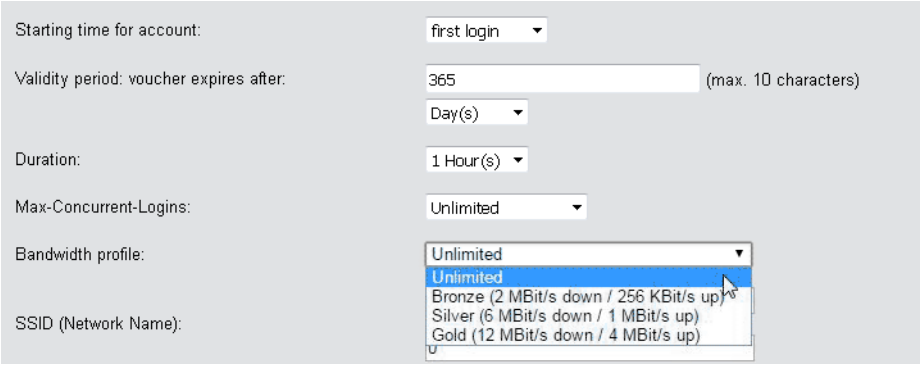
The entries in the edit window have the following meaning:

- **Profile name**: Enter the name for the bandwidth profile here.
- **TX bandwidth**: Enter the maximum uplink bandwidth (in kbps), which should be available to a Public Spot user. To limit the bandwidth, for example, to 1 Mbps, enter the value `1024`.
- **RX bandwidth**: Enter the maximum downlink bandwidth (in kbps), which should be available to a Public Spot user. To limit the bandwidth, for example, to 1 Mbps, enter the value `1024`.

Assigning bandwidth profiles

The following steps describe how you assign the available bandwidth profiles to a Public Spot user.

1. Open WEBconfig.
2. Start the add user wizard under **Setup Wizards** > **Create Public Spot account**.
3. Assign the new user an appropriate profile from the selection list **Bandwidth profile**.



When creating a new user, the RADIUS server automatically assigns the upper and lower boundaries of the bandwidth profile (not the bandwidth profile per se) to the associated account.

Auto cleanup user table

The device gives you the option to delete expired accounts for Public Spot users automatically.

Users of the Public Spot Wizard are generally administrators with restricted rights who are often unable to delete user table entries themselves. Because the user table has a limited number of entries, outdated entries could limit the capacity of the Public Spot. We strongly recommend that you activate this option.

If you use the internal RADIUS server for the administration of user accounts, enable automatic clean-up under **RADIUS** > **Server** > **User database** > **Auto cleanup user table**.

These settings have no effect on the user table on an external RADIUS server.

The following list offers you a general overview of which capacity limits apply to specific models. If you cannot find your device, please check the exact details in the product description.

Table 1: Size of the user table for specific LANCOM models

LANCOM model	User table size
with **Public Spot** option: - LANCOM LN-17xx serie - LANCOM L(N)-8xx - LANCOM LN-630acn - LANCOM L-3xx series - LANCOM IAP-4G+	64

LANCOM model	User table size
> LANCOM IAP-8xx series > LANCOM IAP-5G > LANCOM OAP-8xx series > LANCOM OAP-5G	
> LANCOM vRouter 50 > LANCOM 178x series > LANCOM 179x series > LANCOM 18xx series	128
> LANCOM 19xx series > LANCOM WLC-4006(+) > LANCOM vRouter 250 > LANCOM 2100 > LANCOM WLC-30 > LANCOM WLC-60	256
> LANCOM vRouter 500 > LANCOM vRouter 1000 > LANCOM vRouter unlimited with **Public Spot XL** option: > LANCOM ISG-1000 > LANCOM ISG-4000 > LANCOM ISG-5000 > LANCOM ISG-8000 > LANCOM WLC-1000 > LANCOM WLC-2000	unlimited*

*) No limitation on the table; however, an upper limit of max. 2,500 users is recommended.

Station monitoring

If station monitoring is activated, the Public Spot regularly checks to see if the associated end devices are still available. Lost end devices are automatically deleted from the local user table. If station monitoring is switched off, a user is not logged off until the validity period of the user's authentication expires.

Station monitoring is extremely important for Public Spots operating commercially on a time basis. In installations of this type, users must be assured that they are only paying for the time actually spent using the Public Spot services.

Configuration

Station monitoring for the Public Spot Module is disabled by default. You activate it by entering a value greater than 0 – this value disables the function – under **Public Spot** > **Server** > **Interface selection** > **Idle timeout**. From this point on, all end devices are automatically disconnected from the Public Spot after a specific time.

If your Public Spot device has WLAN, you also have the option of enabling station monitoring globally for all WLAN interfaces. You can find the corresponding settings under **Wireless LAN** > **Security** > **Monitor stations to detect inactive ones**. To do this, the device disconnects mobile stations after 60 seconds (default value). If WLAN station monitoring is disabled, by default this may take up to 15 minutes.

If you offer Public Spot via WLAN, please note that the station monitoring of the WLAN takes priority over that for the Public Spot, and a disconnection can occur earlier if the idle timeout for WLAN (configurable in the Setup menu under **WLAN** > **Idle timeout**) is less than that for the Public Spot.

Monitoring

You can monitor the Public Spot during operation using WEBconfig. The station table in the user authentication menu provides an overview of:

- Users currently logged in to the Public Spot and
- End devices in the WLAN which are not logged in.

You navigate to the Stations table in the Status menu under **Public Spot** > **Stations table**. Using the button **Monitor this table** you automatically refresh the table display at regular intervals.

WLAN handover of sessions between devices

Whenever a site equipped with WLAN hotspots expands, it may be necessary to deploy more than one access point to cover the whole area. One option would be to use a central device as an authentication gateway, enable the Public Spot option on this device only, and require all other access points to redirect requests to the central device. In this way, all other access points act as simple, transparent bridges, which connect to the central gateway using the Ethernet backbone. This allows clients to freely roam among the access points since all session information is kept in the central gateway.

This variant has two drawbacks, however:

- The central gateway is a single point of failure, and is not scalable. You can reduce the risk of failures by using VRRP to create a redundancy solution.

  This solution requires an external RADIUS server, since VRRP cannot synchronize configurations, e.g. the user database. However, this means that certain functions (such as the Public Spot wizards in WEBconfig) are no longer available.
- Roaming is only necessary when the Public Spot module is installed on the access points themselves. Using a WLC, the authentication can be forwarded to the central gateway. In this case, the roaming between access points is transparent to the WLAN controller.

An alternative to this type of centralized setup is to enable the Public Spot module in all of the access points. Authentication and page processing handling is thereby distributed over all devices, and a single point of failure is eliminated.

IAPP (inter access point protocol)

Since the Public Spot module is implemented as a "switchable" transparent bridge, there is no need for clients to acquire a new IP address after they roamed to another access point, so there is no need to terminate open connections. This results in the requirement that an already authenticated client does not have to re-authenticate after roaming to a new access point. Thus the authentication information should be carried over from the old to the new access point.

Access points use the IAPP (inter access point protocol) to share information about roaming clients: Whenever a wireless client decides to change to another access point, it has the option of informing the new AP about which AP it was previously connected to. This information, combined with regular Hello packets on the Ethernet backbone, enable the new access point to inform the old access point. The old access point can then remove the client from its station table and acknowledge the handover.

If a client does not use the corresponding Reassociate packet for connecting to the new access point, the new access point sends a handover request as a multicast on the backbone, instead of a directed packet to the old access point. This means that this handover also works for clients that do not support IAPP.

The main task of the IAPP in a WLAN is to tell the old access point not to send any more packets to the corresponding client in its wireless area, since it will no longer receive them. This type of behavior (based on the definition of the 802.11 frame exchange protocol) could otherwise cause problems with other clients that are connected with it.

In case of an enabled Public Spot module, the communication channel provided by IAPP is used to transport the session information of wireless clients. Whenever an access point receives a handover request for one of its wireless clients, and if a session record for this client is available in its station table, it will append state information about this client to the requesting access point. This information includes:

- The client’s current state (authenticated or not authenticated)

In case the client is authenticated, it also includes:

- The username used to authenticate
- The amount of data traffic generated by the client so far
- The session duration so far
- The IP address of the client
- Possible limits on the session duration and data volumes
- Possible information about idle timeouts

- If RADIUS accounting was used for the session:
  - The entry used for RADIUS accounting in the authentication server list, referenced by name
  - The accounting cycle used for interim updates

After a successful transfer, the old access point terminates the session, which, in the case of RADIUS accounting, means that it sends an accounting stop request to the RADIUS accounting server. This is necessary since a RADIUS server can use the NAS identification to associate requests with specific sessions, and these requests can no longer be associated with the correct sessions once the data packets for a session come from more than one device. If an access point receives this information in a handover reply, it immediately marks the client as authenticated and starts a new RADIUS accounting session, if possible.

Note that the new access point requires a corresponding entry in its **Authentication server** list in order to receive the necessary information. The specific part of the handover reply for the Public Spot module is protected by a shared secret, which is set in the setup menu under **Public-Spot-Module** > **Roaming-Secret**. These security measures should prevent falsification of handover replies. Without a password configured, the access point does not append the information above on a handover reply, which forces the client to authenticate again.

Authentication via RADIUS

RADIUS is an extensively accepted protocol for providing large groups of users access to a server. Although it was originally developed for dial-in server access over telephone lines, the concept is also useful for the hotspot authentication process. For that reason, it can be used in a more complex provider network, for example, to provide access for the same users via dial-in and hotspots. You configure RADIUS servers and their access parameters in the dialog **Public Spot** > **Users** > **Users and RADIUS servers** under **RADIUS server**.

In certain scenarios, it can be feasible to use more than one RADIUS server. In general, a RADIUS server is specified by its IP address, the UDP port the RADIUS service is bound to (typical ports are 1645 or 1812), and a so-called "shared secret". This is a random character string which acts as a password for access to the server. Only clients which know the shared secret can interact with the RADIUS server, since the password for the user account is hashed instead of being sent in cleartext.

If you operate your own external login portal, it is possible to change the attributes of Public Spot sessions after the user has authenticated. This is achieved with dynamic authorization by means of RADIUS CoA (Change of Authorization) (see *Dynamic authorization by RADIUS CoA (Change of Authorization)* on page 169 and *Enabling the acceptance of RADIUS CoA requests by the Public Spot* on page 53).

In theory, the simplest possible RADIUS transaction consists of the device sending the entered account data (user name + password) to the RADIUS server and the RADIUS server responding with either "yes" or "no". However, the RADIUS protocol also allows more complex responses and requests where the communication partners use a list of variables—so-called "attributes"—for requests and responses.

In the *Appendix* there is a list of which attributes a device can send to a RADIUS server and which attributes from a RADIUS response are understood by the device.

Enabling the acceptance of RADIUS CoA requests by the Public Spot

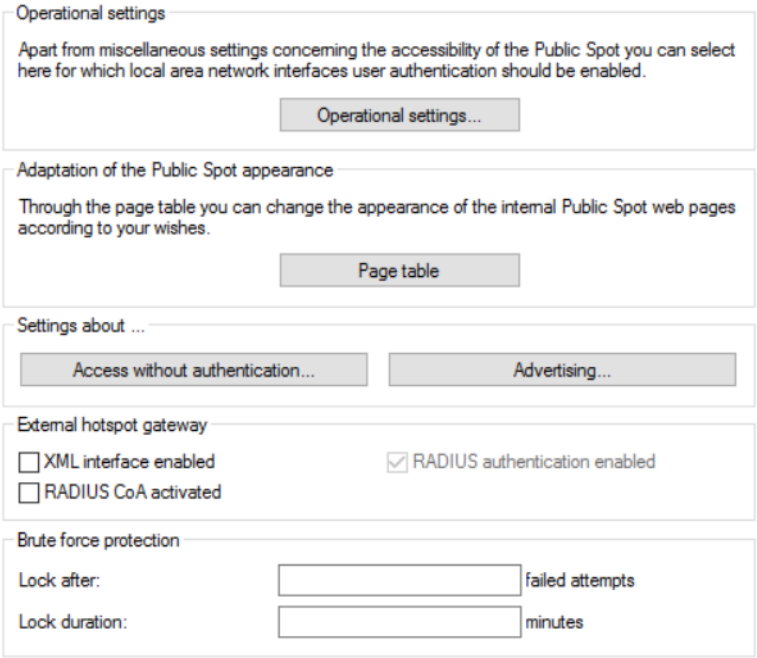
- The following steps assume that you have a functioning Public Spot that can be connected to an external hotspot gateway.

> The external hotspot gateway is located either in a freely accessible network provided by the Public Spot, or its address is included in the list of free hosts.

As an alternative to an XML-based `RADIUS_COA_REQUEST` via the XML interface, the Public Spot can also receive CoA requests by means of the RADIUS protocol from an external hotspot gateway or from an external RADIUS server. You have also have the option to use both forms of command transmission in parallel.

The following section explains how you enable RADIUS-CoA support as per RFC3576 in the Public Spot.

1. In LANconfig, open the device configuration and navigate to **Public Spot** > **Server**.



2. Set a checkmark under **RADIUS CoA activated**.
3. Now write the configuration back to the device.

From now on, the Public Spot processes any RADIUS CoA requests received from an external hotspot gateway.

Multiple authentication servers

As mentioned previously, the list of authentication servers can contain more than one entry. There may be situations where the hotspot provides access to the Internet for customers from different service providers. These providers may have separate user databases and their own RADIUS servers. The device must select which provider corresponds to the user based on the username.

Whenever the device does not find an entry for an authenticated user in its local table, it will first search through the authentication server list to find the provider that corresponds to the user. For example, user account names like `John.Doe@mydomain.com` contains the authentication server entry named `MYDOMAIN`. If the first allocation does not work, the device attempts to allocate the entry `DEFAULT` to the user. If this entry also does not exist, the device selects the authentication server that is first in the list. If the device does not find an entry (i.e., the list is empty), the user authentication fails.

Depending on the allocation of a user to a authentication server, your device always transmits the complete username to the selected RADIUS server. The selected RADIUS server is stored as the provider for the subsequent session and used for optional RADIUS accounting.

Chaining of backup servers

Internet access providers wish to provide a very high level of availability, and a common method to achieve this relies on redundancy. This redundancy is achieved using the backup servers which are needed when a request times out on the primary server, for example, because the server or another network component along the way was unavailable.

The requirements for backup servers varies widely among the different providers, which is why the list of authentication servers does not have a specific number of input fields. Instead, the device offers you a series of backup servers (backup chaining). Here, two or more entries in the authentication server table may be chained together to form a list of RADIUS servers. The device looks through the list of RADIUS servers one by one until the end of the list is reached (authentication failure due to server unavailability) or a response from a server (either positive or negative) is obtained.

You chain backup servers using the input field **Backup name** in the add/edit dialog under **Public Spot** > **Server** > **Authentication server**. Whenever a RADIUS request fails (i.e. times out), the device checks the backup field, and continues to try the RADIUS server specified in the entry that is referenced by the backup name. In general, an unlimited number of servers can be connected this way, which makes it possible for several providers to assign the same fallback server. The chain of backup servers is considered to be terminated if one of the following conditions occurs:

- Querying a RADIUS server failed and the corresponding authentication server table entry has an empty backup field.
- Querying a RADIUS server failed and the corresponding provider table entry has an invalid backup field, i.e. the entry referenced is not present in the authentication server list.
- Querying a RADIUS server failed and the corresponding authentication server list entry refers to an entry that has already been used in the query process. This avoids endless RADIUS requests due to circular references. It is possible to specify two RADIUS servers that reference each other as backups, with the primary server being selected by the user account name.

While the device is sending a RADIUS request, the TCP/HTTP connection to the client remains active. If the runtime of the chaining exceeds the lifetime of the TCP/HTTP connection, the client interrupts the login attempt. Therefore, it may be recommended to reduce the number of request retries to the individual backup servers as well as the time intervals between requests. You make these settings in the dialog **RADIUS** > **Server** > **Extended configuration** > **Options**.

Billing without a RADIUS accounting server

If user administration is performed using the internal user list of the Public Spot module, and you do not want to use a RADIUS accounting server, your only option is to use the expiry date of the user account for accounting purposes.

The use of the internal user list is no longer recommended. Instead, in order to take advantage of all of the options the Public Spot offers, you should use the internal RADIUS server for new installations.

For the purposes of billing by credit payment, the Public Spot can use SYSLOG to output detailed connection information to any computer in the network. Using the appropriate software on the destination computer allows you to precisely bill the resources that were actually used (such as connection times or transfer volumes).

Billing with a RADIUS accounting server

For the purposes of billing via a RADIUS server, you can set up the Public Spot so that it regularly supplies the current connection information for every active user to the specified accounting server. Accounting is started when a client is authenticated using RADIUS and a valid **Accounting server** is configured for the relevant **Authentication server** in the list of **Authentication servers**. It is possible to use different RADIUS servers for authentication and accounting.

Each of the regular message packets to the accounting server contains information about the resources (time, transferred data volumes, etc.) consumed by the user since the last message. This means that, even in the worst case of a Public Spot failure (e.g., due to a power outage or similar), only a small amount of accounting information will be lost.

Periodic messaging of accounting information to the accounting server (interim updates) is deactivated by default. It is activated by setting a value for the accounting cycle which is greater than 0.

- LANconfig: **Public Spot** > **Users** > **Accounting update cycle**

This cycle is defined in seconds. This sets the time interval of when your device regularly sends connection information to the accounting server. Setting the cycle to 0 deactivates this function. If this is the case, your device only sends accounting information at the beginning and end of the session.

When accounting on a prepaid basis, the RADIUS server monitors the restrictions on the users (limits on connection times or transfer volumes, expiry date). As soon as a user has used up the prepaid amount, the RADIUS server locks the user account. Your device rejects future login attempts for the user.

Time limits for prepaid models can be monitored by the Public Spot during active sessions. If a time limit is exceeded, the Public Spot automatically terminates the corresponding session. The monitoring of prepaid amounts is possible if the RADIUS server transmits the user's time credit to the Public Spot as the "Session timeout" attribute at the start of the session.

Request types

Your device is able to send different types of RADIUS requests to an accounting server. These requests differ according to a user's session state:

- An accounting start request is sent after a successful authentication.
- An accounting stop request is sent after a Public Spot session is terminated.
- Optional: Interim updates are sent throughout the session.

There are two types of interim updates: An initial update is sent immediately after the start request since some RADIUS servers need this in order to create a session in the accounting database. All further updates depend on whether an accounting cycle was created for the respective session (see **Public Spot** > **Users** > **Accounting update cycle**).

Alternatively, this value may be included in a RADIUS authentication response: The RADIUS server offers the RADIUS client (for example, your Public Spot) an interim accounting interval, which the client will use if it has the appropriate support for this and as long as no interval was set locally on the device itself.

If a local value was set, it will always be given a higher priority than the one received from a RADIUS server, which the RADIUS RFCs require by default!

In the *Appendix* there is a list of which attributes a device can send to a RADIUS server and which attributes from a RADIUS response are understood by the device.

Accounting backup

The backup solution for RADIUS accounting is the same as the one for RADIUS authentication, in that your device goes through the entries in the authentication server list one by one (see chapter *Chaining of backup servers*). The backup entries for the accounting server should be chosen with the same care as for the authentication server: If you are using multiple backups, you will probably have to reduce the timeout/try values for the requests in order to achieve reasonable response times for the entire system.

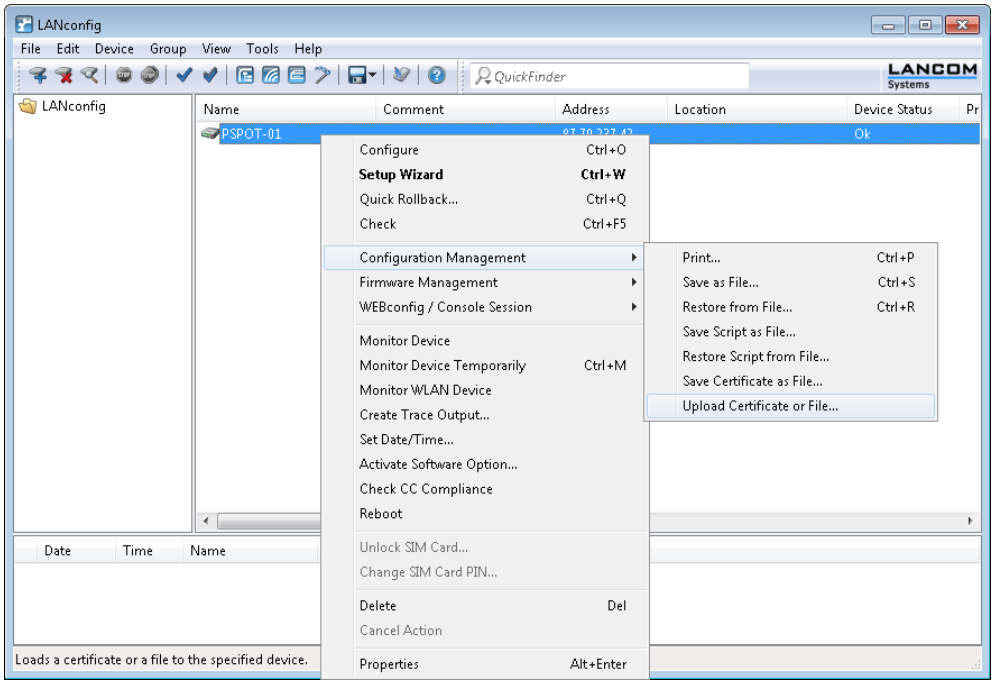
User sessions are not paused while the device sends accounting requests, which consumes additional resources in the device—in contrast to authentication. Please ensure that the time required for the selection of an accounting server* should be less than the length of an accounting cycle for interim update requests. This stops the requests from queuing up, which would result in a stack overflow.

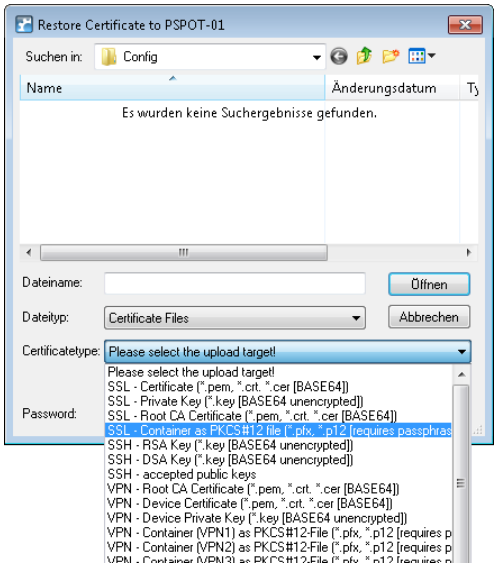
** Number of backups x (idle timeout + number of retries)*

Multi-level certificates for Public Spots

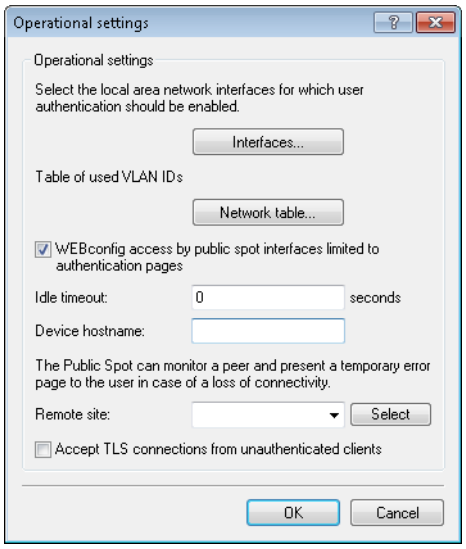
SSL certificate chains can be loaded into the device as a PKCS#12 container. These certificate chains can be used for Public Spot authentication pages by using the HTTPS server implemented in the device. Certificates from recognized trust centers are normally multi-level. Officially signed certificates in the Public Spot are necessary to avoid certificate-related error messages from the browser when authenticating at a Public Spot.

The certificate is loaded into the device for using LANconfig in File Management to upload the individual files of the root CA certificate or a PKCS#12 container:





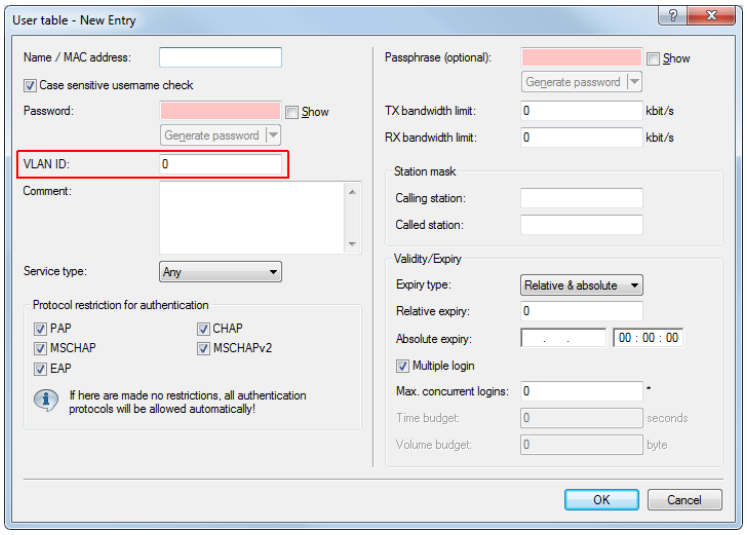
Certificates are normally issued for DNS names, so the Public Spot must specify the certificate's DNS name as the destination and not an internal IP address (enter in **Public Spot** > **Server** > **Operational settings** under **Device hostname**). This name has to be resolved by the DNS server to provide the corresponding IP address of the Public Spot.



Assigning users to individual VLANs

Regardless of the assignment of a VLAN ID for the entire Public Spot module, the device offers you the option of separately assigning individual VLAN IDs for individual Public Spot users. This ID is automatically assigned by the RADIUS server to your users after successful authentication. In this way it is possible, for example, to classify different Public Spot users in separate networks with different access rights and access options without having them login to separate SSIDs or requiring you to publicize the availability of various networks (e.g., networks for different customer types). The relevant rules can be realized via the firewall by specifying the VLAN ID of the respective user/the relevant user groups as the source tag.

An enabled VLAN module is a prerequisite for the functions described above.



> Open the **User table** in the dialog **RADIUS Server User database** and click **Add...** to create a new user.

- Assign an individual VLAN ID to the new user with the input field **VLAN-ID**. After authentication by the RADIUS server, the individual VLAN ID overwrites a global VLAN ID that a user would otherwise obtain from the interface. The value `0` disables the assignment of an individual VLAN ID.

For technical reasons, the assignment of a VLAN ID requires a new address assignment by the DHCP server. As long as a client is not yet assigned a new address after successful authentication, the client is still in the previous (e.g., untagged) network. In order for the clients to be transferred to the new network as quickly as possible, it is necessary to set the lease time of the DHCP server as low as possible under **IPv4** > **DHCPv4**. Possible values (in minutes) include, for example:

- **Maximum lease time:** `2`
- **Default lease time:** `1`

Take into account that a strong reduction in global lease time can flood your network with DHCP messages, and when there is a larger number of users, it leads to an increased network load! Alternatively, you have the option of using an external DHCP server or allowing your users to manually request a new address by using their client. In the Windows command line this is done, for example, using the commands `ipconfig /release` and `ipconfig /renew`.

By assigning a VLAN-ID, the user loses his connection after the initial DHCP lease expires. The connection only remains stable as of the second lease, i.e. after successfully assigning the VLAN-ID.

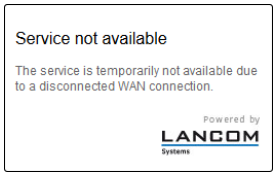
Error page in case of WAN connection failure

In addition to the general login error pages, you can also inform non-authenticated Public Spot users of a WAN connection error. Potential users are informed about the lack of network availability beforehand. This **Error** page is displayed whenever the Public Spot module registers a WAN link failure.

In order for the error page to be displayed properly, a corresponding remote site **must** be named, the connection to which is monitored by the Public Spot module. Make an appropriate entry in the dialog **Public Spot** > **Server Remote site**. The **Select** button allows you to assign an existing entry to the input field, or to create a new remote site.

If no remote site is named for monitoring, the Public Spot module disables the display of the connection error page. If the WAN connection fails, unauthenticated will not see an error page and their browsers will timeout instead.

On your custom error page, use the identifier `LOGINERRORMSG` to insert the error message issued by LCOS in case of a WAN link failure. In the event of a WAN link failure, the following error message is displayed:



Users who are already authenticated will see an appropriate error message from their browser.

AP-specific login to a central Public Spot

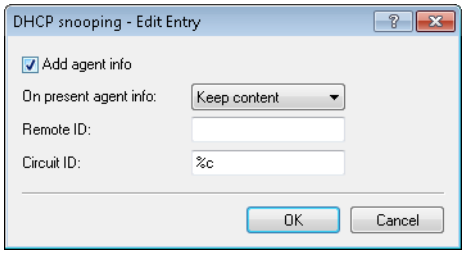
A central WLC manages a Public Spot in a distributed infrastructure. Accordingly, the configuration of the Public Spot (Public Spot SSID, security standards) is identical on all of the participating APs. This allows a Public Spot provider to offer an identical Public Spot at all of the different locations.

After receiving a voucher, customers would have access to this Public Spot at any branch. In order to limit access to the branch where the customer has received the voucher, the AP transmits its own identifier in addition to the user name and password. This identifier enables the voucher to be associated with this AP. To transfer the identifier, the AP attaches

the circuit ID (DHCP option 82) to the DHCP requests. These DHCP packets pass through the central Public Spot, which checks the identifier based on the entries in the RADIUS user table.

The Public Spot only allows a request if the voucher in the RADIUS user table is associated with this AP. Customers who have received a voucher at branch A cannot login to the same Public Spot at branch B, since the two APs transmit different identifiers.

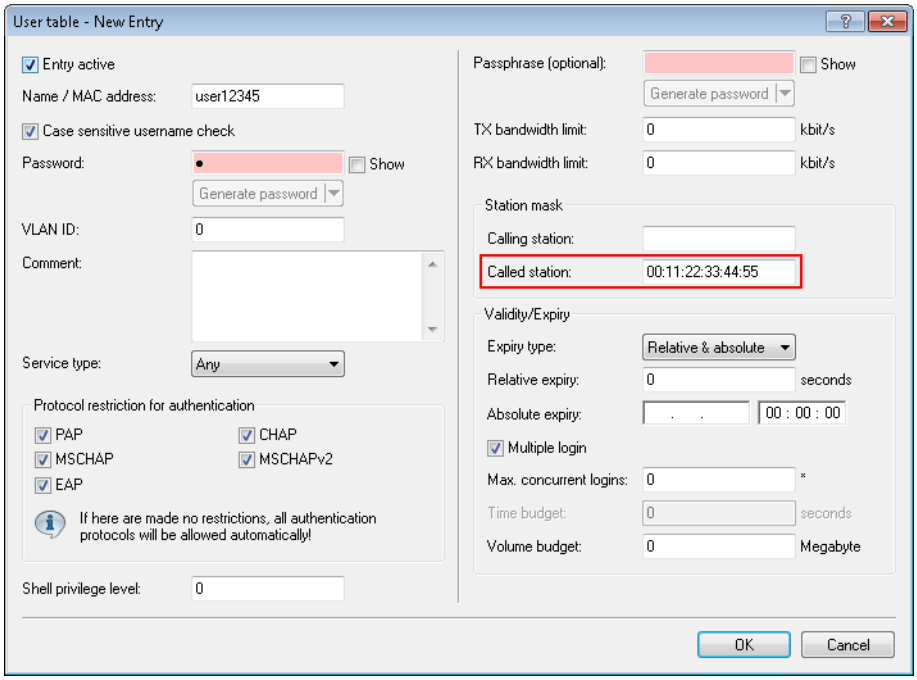
The AP identifier is configured as the circuit ID for the corresponding interface under **Interfaces** > **Snooping** > **DHCP snooping**.



You can use the following variables:

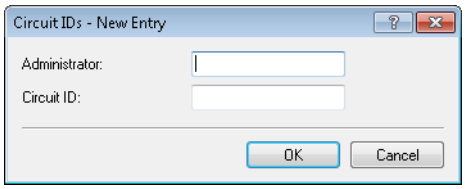
- **%%**: Inserts a percent sign.
- **%c**: Inserts the MAC address of the interface used by the Public Spot user to authenticate. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- **%c**: Inserts the name of the interface used by the Public Spot user to authenticate.
- **%n**: Inserts the name of the AP as specified under **Management** > **General**.
- **%v**: Inserts the VLAN ID of the DHCP request packet. This VLAN ID is sourced either from the VLAN header of the DHCP packet or from the VLAN ID mapping for this interface.
- **%p**: Inserts the name of the Ethernet interface that received the DHCP packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, **%p** and **%i** are identical.
- **%s**: Inserts the WLAN SSID if a WLAN client is used for the authentication. For other clients, this variable contains an empty string.
- **%e**: Inserts the serial number of the AP, to be found for example under **Management** > **General**.

On the WLC, you configure this identifier in the RADIUS user table under **RADIUS** > **Server** > **General** > **User table**.



As the “Called station”, you add the ID of the AP that should enable access by means of the corresponding voucher.

When setting up new Public Spot users, the Public Spot Setup Wizard automatically uses the ID of the device if this is configured under **Public Spot** > **Wizard** > **Circuit IDs**.



When you create a new Public Spot account, the setup wizard checks to see whether this table contains an entry for the logged-in **administrator**. If this is the case, the setup wizard inserts the **circuit ID** into the RADIUS user table as the “called station”.

Redirect for HTTPS connections

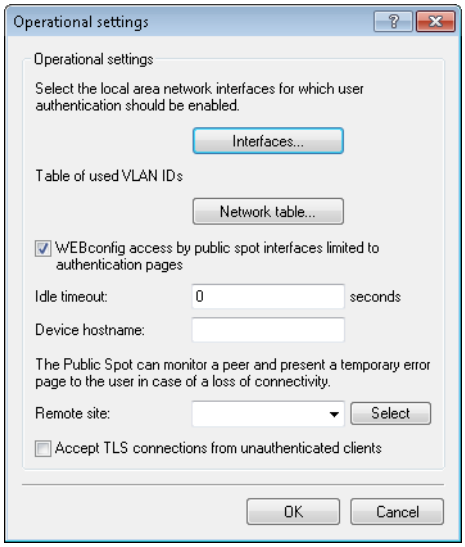
If an unauthenticated client attempts to access an HTTPS website via an interface operated by the Public Spot, the connection request is redirected to the Public Spot gateway itself, which then presents its login page to the user (as is also the case with HTTP). Usually, the user's browser displays a certificate warning, because the name or IP of the requested website is different from the name or IP address of the Public Spot. To prevent this and the increased load on the Public Spot from the HTTPS/TLS connections, this setting allows you to prevent HTTPS connections from being established for unauthenticated clients.

Once the client is authenticated, redirection is stopped and the client can establish any HTTP or HTTPS connection.

Modern clients carry out a "captive portal detection" via HTTP. The client attempts to access a certain URL via HTTP to check for the presence of a login page (from the Public Spot or other solutions). This mechanism is not affected by turning off the HTTPS redirect, since detection is usually via HTTP.

However, if unauthenticated WLAN clients should not perform connect requests over HTTP, this ineffective HTTPS redirect would place unnecessary load on the Public Spot gateway. For this reason it is possible to disable this HTTPS redirect. In this case, the user's browser displays a blank page.

In LANconfig, you configure the HTTPS redirect under **Public Spot** > **Server** > **Operational settings**.



To enable the HTTPS redirect, activate the option **Accept TLS connections from unauthenticated clients**. This option is disabled by default.

Protection against brute force attacks

Brute force attacks are the most common type of attack on networks. This method of attack tries out a variety of potential passwords in the shortest possible time, until the right one is found. One form of protection against brute-force attacks is to react to one or more successive failed attempts by delaying the time until the entry is allowed to be attempted again.

Configure the protection against brute-force attacks in LANconfig under **Public Spot** > **Server** in the section **Brute force protection**.

Lock after

Specify how many unsuccessful attempts are permitted before the entry lock takes effect.

Lock duration

Specify for how long the entry lock is to apply.

You can use the console to display the current status of the brute-force protection with the command `show pbbruteprotector`:

`show pbbruteprotector`

Shows all of the MAC addresses that are associated with the Public Spot.

`show pbbruteprotector [MAC address[ MAC address [ ...]]]`

Specifying one or more space-separated MAC addresses shows the status of all of the respective MAC addresses.

MAC addresses are specified in the format `11:22:33:44:55:66`, `11-22-33-44-55-66` or `112233445566`.

1.2.4 Alternative login methods

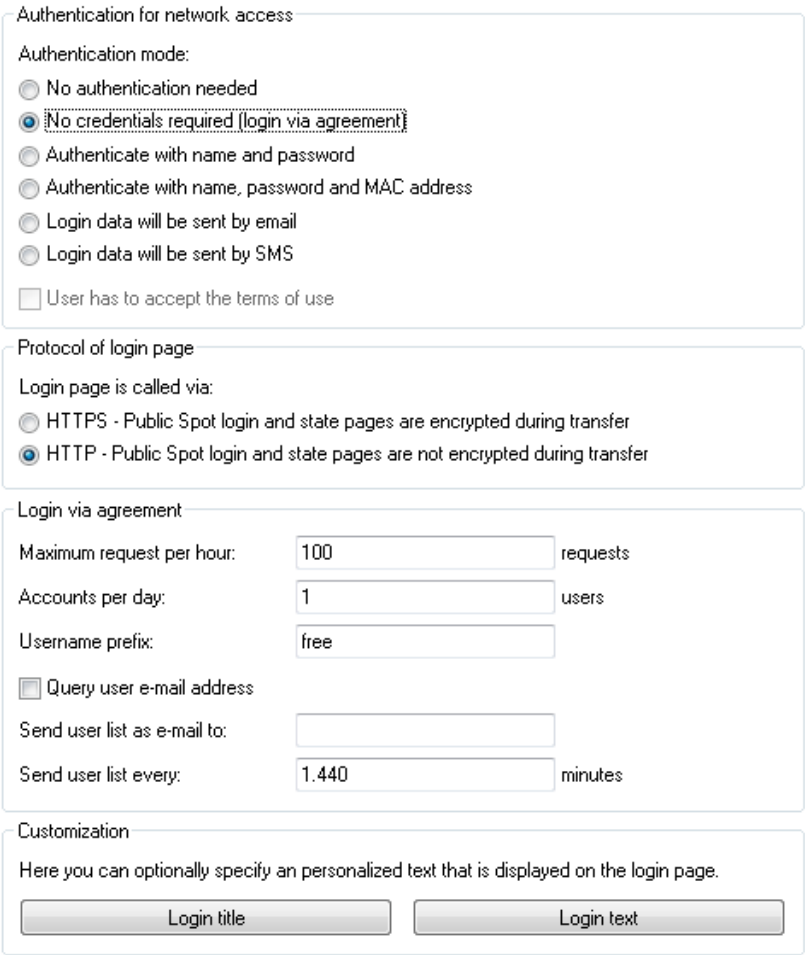
In addition to logging-in with previously provided credentials, your users can also independently request the receipt of login data via e-mail or text message (SMS), or by gaining instant access to the Public Spot by means of Login via agreement. Alternatively, in order to implement more complex or multi-level login scenarios, you can also link your Public Spot to other software systems using the XML or PMS interface (module optionally available).

You can also offer your users additional convenience by allowing, for example, automatic login processes (automatic login as well as re-login using a MAC address, login using WISPr, Hotspot 2.0), and also the related roaming services.

Hotspot 2.0 and roaming features are only available in conjunction with WLAN.

Overview of authentication modes

There are various ways to login to the Public Spot. The network access authentication setting is located in the dialog **Public Spot** > **Authentication**.



The following authentication modes are available:

- **No authentication required**

  Users get free access to the Public Spot, authentication is not required.

  Do not use this setting if your device has unlimited access to the Internet.

- **No credentials required (login after agreement)**

  Users get free access to the Public Spot after they agree to the operator's terms. With a RADIUS server, login is completely transparent for the user. The prerequisite is that you have set up an individual template page (a welcome page with a Login via agreement): In this case, the Public Spot initially forwards a user to the Welcome page. After the user agrees to the terms, the device automatically creates a user account in line with the default values set under **Public Spot** > **Wizard** and grants access to the connected network.

  Once you have select this login mode, the dialog section **Login via agreement** becomes available, where you can set additional conditions for the creation of free user accounts by the RADIUS server:

  - **Maximum requests per hour**: Specify how many users per hour can automatically create an account on the device. Decrease this value to reduce performance degradation caused by an excessive number of users.
  - **Accounts per day**: Specify how many accounts a user may create per day. If this value is reached and the user session has expired, a user can not automatically register and get authenticated on the Public Spot for the rest of the day.
  - **Username prefix**: Enter a prefix which can be used to identify the user in the RADIUS user table that the device created automatically after confirmation of the terms of use. This prefix is placed directly in front of the **User name pattern** specified under **Public Spot** > **Wizard**.
  - **Query user e-mail address**: Enable this check box in order to query the user's e-mail address as a requirement for using the Public Spot. The device automatically enters the e-mail address specified here into the comments box of the newly created RADIUS user. Once a day a list of all of the available addresses is stored in the flash memory of the device. This list is boot persistent.
  - **Send user list as e-mail to**: Enter the e-mail address where the address list is to be sent. Only new entries that have been added since the last submission are sent. The address list is transmitted as a CSV file.
  - **Send user list every**: This sets the interval at which the updated address list is sent to the specified e-mail address. This value is specified in minutes.

  The terms featured on the Welcome screen are not to be confused with the terms-of-use page itself. The **Terms of use** page is an extra page that becomes available when certain login modes are activated (see *Possible authentication pages* on page 97). If no Welcome page has been set up (see *Configuration of user-defined pages* on page 102), the device displays an error message when accessing the Public Spot.

- **Authenticate with name and password**

  Users log on to the Public Spot with their name and their password. Users get their login data from a network administrator as a voucher.

- **Authenticate with name, password and MAC address**

  Users log on to the Public Spot with their name and their password. Users get their login data from a network administrator as a voucher. For this login mode, the MAC address of the client must also match the one stored in the user list by the administrator.

- **Login data will be sent by e-mail**

  Users log on to the Public Spot with their name and their password. Users generate the credentials themselves, and the data is sent via e-mail. No action by an administrator is necessary. Learn more about this login mode under *Independent user authentication (Smart Ticket)* on page 65.

- **Login data will be sent by SMS (text message)**

  Users log on to the Public Spot with their name and their password. Users generate the credentials themselves, and the data is sent by SMS (text message). No action by an administrator is necessary. Learn more about this login mode under *Independent user authentication (Smart Ticket)* on page 65.

For some login modes, the option **User has to accept the terms of use** allows you to combine the login with an acceptance of the terms and conditions. In this case, the Public Spot login page displays an additional option, which prompts the user to accept the terms of use before registering or logging in. Users who do not explicitly agree to these terms and conditions are unable to login to the Public Spot.

Remember to upload a page with terms and conditions onto the device before you enable this option. Otherwise, the device will only show the user a placeholder instead of the terms and conditions.

Independent user authentication (Smart Ticket)

Devices operating a Public Spot provide users with time-limited access to certain networks, typically the Internet. In many scenarios, a limited administrator account is used for the creation of these accounts: For example, a hotel employee at the front desk can use an account that only has the functional rights to create and manage Public Spot users. With a few mouse clicks the employee can print a voucher for the hotel guests granting them network access.

However, the convenient voucher solution still requires action from an administrator. Alternatively, you can give the users the option to generate their own login data for the wireless network, and send it to themselves by e-mail or SMS (login by "Smart Ticket").

Login via agreement

Alternatively, the device gives you the ability to handle the login for Public Spot users transparently using a RADIUS server. In this case, the user login is preceded by a request to consent to the agreement before the user automatically receives access to the Public Spot. The creation of credentials by the user via e-mail or SMS does not apply for this authentication method. Learn more about this in the section under *Overview of authentication modes* on page 63—the "Login via agreement" is not a part of the Smart Ticket function.

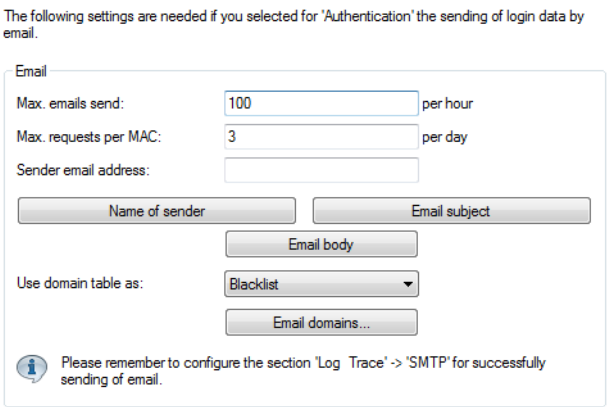
Configuring e-mail authentication

The settings for transmitting the login credentials to the e-mail address specified by the user are adjusted in the dialog **Public Spot** > **Email**. The following steps show you how to correctly configure e-mail authentication.

In order to successfully send access credentials as an e-mail, you must set up a valid SMTP account under **Log & Trace** > **SMTP account** and **Log & Trace** > **SMTP options**.

In addition, you can specify individual text blocks used by the device to send the login credentials; see *Customizing text message content* on page 68. By default, the device inserts predefined text modules; for an overview of these see *Standard texts for e-mail sender, subject line and body* on page 69.

1. Start LANconfig and open the configuration dialog for the device.
2. Change the view to **Public Spot** > **Authentication**.
3. Change the login mode to **Login data will be sent by email**.
4. Change the view to **Public Spot** > **Email**.



5. Under **Max. emails send** you enter the maximum number of e-mails that the Public Spot module may send per hour to users authenticating via e-mail. Lower the value to reduce the number of new users per hour.
6. Under **Max.requests per MAC** you specify how many different sets of credentials the device can provide to a MAC address within one day.
7. Under **Sender e-mail address** enter the return address that your Public Spot users will see when the e-mail is delivered, e.g. `support@providerX.org`.
8. Specify whether the device uses the table **Email domains** as a blacklist or whitelist with the selection item **Use domain table as**.

   This definition sets which e-mail addresses or domains may be entered by your Public Spot users in order to register.

   - **Blacklist**: Registration is permitted on all e-mail domains except those in this table.
   - **Whitelist**: Registration is possible only via the e-mail domains that are present in this table.

   Please note that a Public Spot operating with an empty whitelist will black-list (reject) all domains.

9. Use the **Email domains** table to define the e-mail domains that you allow or prohibit in the case of logins by your Public Spot users via e-mail. Enter domains in the format `web-domain.com`.
10. You can write the configuration back to the device.

Configuring SMS authentication

The settings for transmitting the login credentials as an SMS text message to the phone number specified by the user are adjusted in the dialog **Public Spot** > **SMS**. The choices available to you vary according to the device type:

- The credentials are sent as an SMS text message via the 3G/4G WWAN module in this device.
- The credentials are sent as an SMS text message via the 3G/4G WWAN module in another device.
- The access credentials are sent as an e-mail to an external E-Mail2SMS gateway, which then converts the e-mail to SMS.

LCOS checks the entered phone number for invalid characters. Only numbers between 0 and 9 are allowed. The user must enter 5 to 15 numbers (excluding the country code).

The following steps show you how to correctly configure the different variants of SMS authentication.

In order to send login data as a text message via a 3G/4G WWAN-capable device, the internal SMS module of this device must be set up under **Log & Trace** > **SMS messages**, see *Basic configuration of the SMS module* on page 179.

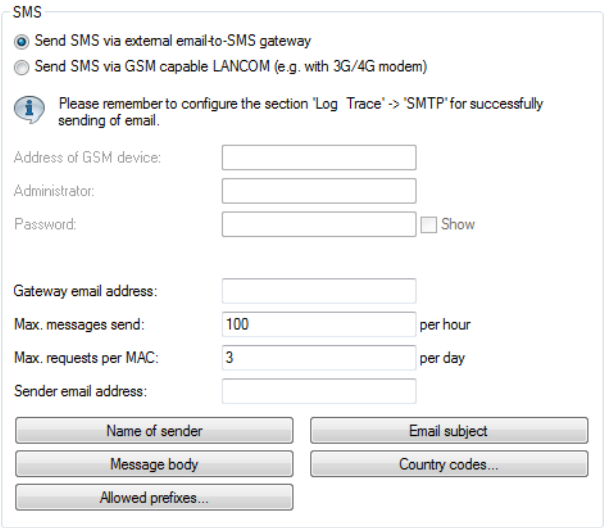
SMS transmission is suitable for installations with a maximum throughput of 10 SMS per minute.

In order to successfully send access credentials as an e-mail, you must set up a valid SMTP account under **Log & Trace** > **SMTP account** and **Log & Trace** > **SMTP options**.

In addition, you can specify individual text blocks used by the device to send the login credentials; see *Customizing text message content* on page 68. By default, the device inserts predefined text modules; for an overview of these see *Standard texts for e-mail sender, subject line and body* on page 69.

1. Start LANconfig and open the configuration dialog for the device.
2. Change the view to **Public Spot** > **Authentication**.
3. Change the login mode to **Login data will be sent by SMS**.

4. Navigate to the menu item **Public Spot** > **SMS**.



5. Specify how the device sends SMS text messages.

   - In order to send the login credentials as an SMS text message via the internal 3G/4G WWAN module, select **Send SMS via internal GSM modem** and then continue with the next main step in the configuration.
   - In order to send the login credentials as an SMS text message via the 3G/4G WWAN module of another device, you first carry out the steps in section *Operating devices with the 3G/4G WWAN module as an SMS gateway* on page 68 and then continue with the next main step in the configuration.
   - In order to send the login credentials to an external E-Mail2SMS gateway, select the setting **Send SMS via external e-mail-to-SMS gateway** and then continue with the next main step in the configuration.

   a) Under **Gateway e-mail address** you enter the IP address or the hostname of the gateway server, which converts the e-mail into SMS. If the provider expects to find the mobile phone number in the local part of the e-mail, you can use the variable `$PSpotUserMobileNo`.

   b) Under **Sender e-mail address** enter the return address that your Public Spot users will see when the SMS is delivered, e.g. `support@providerX.org`.

6. Under **Max. messages send** you enter the maximum number of SMS text messages that the Public Spot module may send per hour to users authenticating via SMS. Lower the value to reduce the number of new users per hour.
7. Under **Max.requests per MAC** you specify how many different sets of credentials the device can provide to a MAC address within one day.
8. Under **Country codes** you enter the international code numbers that the Public Spot will accept when sending data via SMS.
   Country codes can be entered directly or with a prefixed double-zero, for example for Germany `49` or `0049`.

   This table acts as a whitelist. You must define country codes in order for the login data to be delivered.

9. You can limit the transmission of SMS text messages to certain area codes for each country by entering the permissible codes followed by a '*' into a comma-separated list. An example for German mobile phone providers: `15*, 16*, 17*`.

   If you do not make an entry for a country in this table, all country codes will be allowed. Beforehand, an entry must have been created for this country in the Allowed-Country-Codes table.

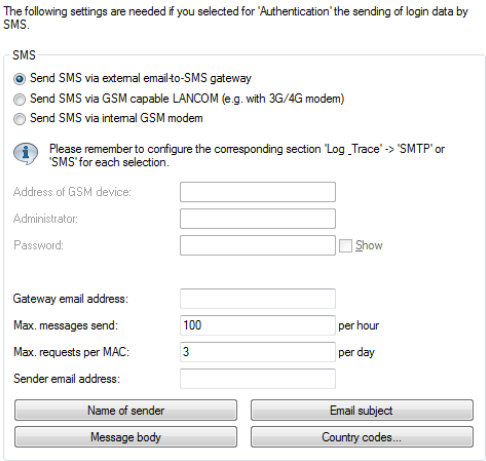
10. You can write the configuration back to the device.

Operating devices with the 3G/4G WWAN module as an SMS gateway

When using Public Spot authentication via SMS (Smart Ticket), you have the option of sending access credentials via the 3G/4G WWAN module in a further device instead of using an external E-Mail2SMS gateway. To use this option, you must store the address and the access credentials for the 3G/4G device on the device that provides the Public Spot. For the purpose of sending the SMS, the Public Spot module uses a URL call to send the credentials and the text message to the external 3G/4G device.

The option is available on devices both with and without their own 3G/4G WWAN module. These options allow you to chain multiple devices together and to set up your own transmitting device if you operate multiple Public Spots or use a device without a 3G/4G WWAN module.

1. Start LANconfig and set up the SMS module on the 3G/4G device that is to serve as an SMS gateway (see *Basic configuration of the SMS module* on page 179). In addition, we recommended that you create an administrator without access rights (select **None**) and with just one function right, **Send SMS**.
2. Open the configuration dialog for the device that provides the Public Spot.
3. Navigate to the menu item **Public Spot** > **SMS**.



4. Select the setting **Send SMS via GSM-capable device (e.g. with 3G/4G modem)**.
5. Enter the user name and password for the administrator on the other 3G/4G device under **Administrator** and **Password**.
6. In the field **Address of GSM device**, enter the IP address where the Public Spot is to reach the other 3G/4G device.

Customizing text message content

By default, the device uses predefined text modules as the content of the e-mails or SMS text messages. An overview of these standard texts is available under *Standard texts for e-mail sender, subject line and body* on page 69. You can also define your own texts.

If you do not specify any text for a language, the device automatically enters the internal default text.

1. Start LANconfig and open the configuration dialog for the device.
2. Depending on the selected authentication method, switch to the view **Public Spot** > **E-mail** or **SMS**.
3. Using the button **Name of sender**, enter a customized sender name for the e-mails or SMS text messages sent in the various languages, e.g. `Provider X`.
4. Use the **E-mail subject** button to enter a subject line for the e-mails sent in the various languages by the Public Spot module. Special control characters are available for this, described in more detail in the section *Variables and control characters* on page 69.

5. Use the **E-mail body** or **Message body** button to enter the content of the e-mails or SMS text messages sent in the various languages by the Public Spot module. Variables and special control characters are available for this, described in more detail in the section *Variables and control characters* on page 69.
6. Now write the configuration back to the device.

Variables and control characters

The message texts used for the Smart Ticket function can be customized with the use of variables and control characters. The variables are automatically populated with values when the Public Spot module sends the e-mail to the user or the SMS gateway.

Variables

The following variables are available in the input field **E-mail body**:

`$PSpotPasswd`

Placeholder for user-specific password for the Public Spot access.

`$PSpotLogoutLink`

Placeholder for the logout URL of the Public Spot in the form `http://<IP address of the Public Spot>/authen/logout`. This URL allows users to logout of the Public Spot if, after a successful login, the session window (which also contains this link) was blocked by the browser or closed by the Public Spot user.

Control characters

The following control characters may also be used in the text entered into the fields **E-mail subject** and **E-mail body**:

`\n`

CRLF (carriage return, line feed)

`\t`

Tabulator

`\<ASCII>`

ASCII code of the corresponding character

If the e-mail2SMS provider requires a variable which contains a backslash ("\"), you have to prefix this with another "\". This prevents the transformation of the "\" by LCOS.

Standard texts for e-mail sender, subject line and body

If you leave the dialogs **Public Spot** > **Email** or **SMS** blank, then the device automatically reverts to the standard texts in the corresponding language as stored in LCOS to generate the e-mail. The language used depends on the language setting of the browser used by the user for registration. If there are no default texts stored internally for a language, the device uses the English texts.

Table 2: Overview of the internal standard texts for authentication via e-mail/SMS

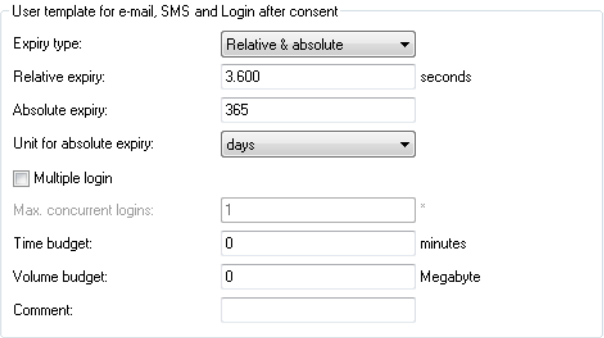
	Name of sender:	E-mail subject:	E-mail body:
Deutsch	Public Spot	Your login credentials for the Public Spot	Your password for the Public Spot: $PSpotPasswd $PSpotLogoutLink

	Name of sender:	E-mail subject:	E-mail body:
English	Public Spot	Your Public Spot account	Your password for the Public Spot: $PSpotPasswd $PSpotLogoutLink

Setting default values for the user templates

The following section describes how you adjust the default values for the **User templates** to meet your needs. The device uses the values set here as defaults when creating new users in Smart Ticket and when users login after confirming the terms and conditions. If you have so opted to send the login credentials via e-mail/SMS or you have activated the login after confirming the terms and conditions, each new user account is equipped with the permissions and constraints as defined by the user template.

1. Start LANconfig and open the configuration dialog for the device.
2. Change the view to **Public Spot** > **Wizard**.



3. Complete the input fields in the section **User template** according to your preferences:

   Expiry type

   Using this entry you define how an automatically created Public Spot user account expires. You can specify whether the validity period of a user account is absolute (e.g. expires on a set date) and/or relative (elapsed time since the first successful login). If you select both values, the expiry time depends on which case occurs first.

   Relative expiry

   Using this entry you define the relative expiry time of an automatically created user account (in seconds). The **Expiry-type** that you chose must include `relative` in order for this setting to work. The validity of the account terminates after the time period specified in this field from the time of the first successful login of the user.

   Absolute expiry

   Using this entry you define the absolute expiry time of an automatically created user account (in days). The **Expiry type** that you chose must include `absolute` in order for this setting to work. The validity of the account terminates at the time specified in this field, calculated from the day of the creation of the account.

   Unit for absolute expiry

   To configure shorter expiry times, use the drop-down menu to select the unit for absolute expiry. Adjust the value for the absolute expiry if necessary.

   Multiple login

   This entry allows you to generally allow or prohibit users with an automatically created account to login to the Public Spot using the same credentials with multiple devices at the same time. The number of devices that can be logged on simultaneously is specified using the input field **Max. concurrent logins**.

Maximum number

Using this entry you set the maximum number of devices which can concurrently login to an automatically created account. The value 0 stands for "unlimited". In order for this setting to work, the parameter **Multiple login** must be enabled.

Time budget

Using this entry you define the time budget which automatically created users are assigned. The value 0 deactivates the function.

Volume budget

Using this entry you define the volume budget which automatically created users are assigned. The value 0 deactivates the function.

Comment

Using this entry you specify a comment or informational text which the RADIUS server adds to an automatically created user account.

4. Optional: If necessary, change the **User name pattern** and the **Password length**. In the authentication modes mentioned above, the device uses the relevant *New user wizard default values* to automatically generate a user name and a password.
5. You can write the configuration back to the device.

Automatic re-login

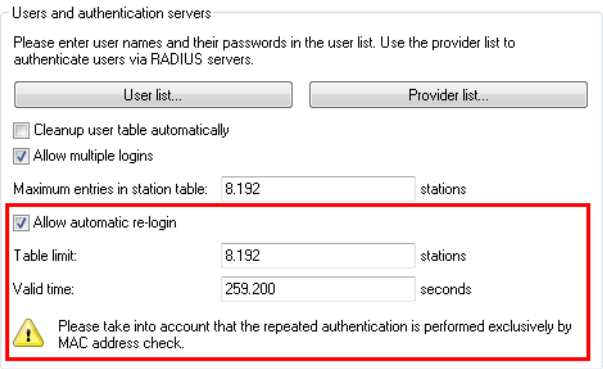
Mobile WLAN clients (e.g., smart phones and tablet PCs) automatically log in to known WLAN networks (SSID) when they reenter the cell. In this case, many apps automatically and directly access web content using the web browser in order to request current data (such as e-mails, social networks, weather reports, etc.) It is similar for mobile LAN clients (e.g., notebooks) which have to be disconnected from the network for a short time for a change of location (e.g., for changes from a lecture hall to a library in a college). In all of these cases, it is impractical to make the user manually log in to the Public Spot again in the browser.

With automatic re-login, the user only has to be identified on the Public Spot once. After a temporary absence, the user can seamlessly use the Public Spot again.

The Public Spot records the manual login and logout as well as a re-login in the SYSLOG. It stores the same login data for a re-login that a user had employed for initial authentication.

The authentication is only performed on the MAC address of the client when re-login is enabled. Since it can lead to security problems, re-login is disabled by default.

The settings for automatic re-login can be found in LANconfig in the device configuration under **Public Spot** > **Users** in the section **Users and authentication servers**.



The selection box **Allow automatic re-login** enables this function.

You specify the number of clients (maximum 65536) in the field **Automatic re-login table limit** that the re-login function may use.

In the field **Automatic re-login valid time** you specify how long the Public Spot stores the credentials of a client in the table for a re-login. After this period expires, the Public Spot user must log in again using the login page of the Public Spot in the browser.

Automatic authentication with the MAC address

After successful authentication, a Public Spot gives the user access to certain services. The Public Spot usually displays a login website so that users can authenticate. The user enters the authorization credentials into the login page and the Public Spot then redirects the user to the allowed sites.

In some applications, authentication via web site may not be desired or not possible, as the following examples illustrate:

- The end device does not have a browser and therefore cannot open the login page.
- Manually accessing the login page may be undesirable, such as when carrying out a performance test.

Automatic authentication on the Public Spot with a MAC address makes it possible to use the Public Spot without first opening the login page. The administrator enters the MAC addresses of the corresponding end device into the table of permissible MAC addresses under **Public Spot** > **Users** > **MAC authenticated users**.

MAC-address check procedure

When the device receives a request from a client, the Public Spot executes the following steps for the automatic authentication by MAC address:

- If the Public Spot has already authenticated the MAC address of the received data packets, the device forwards the data packets without further delay.
- If the MAC address is in the list of allowed clients, the Public Spot starts a new session for the user and forwards the corresponding data packets.
- If a provider has been defined for verification of the MAC addresses by RADIUS, and a positive, valid MAC address authentication is cached in the Public Spot, then the Public Spot starts a new session for that user and forwards the associated data packets.
- If a provider chooses to check the MAC address with the RADIUS server but there is no valid authentication for the MAC address cached in the Public Spot, the Public Spot initiates the authentication of the MAC address at the corresponding RADIUS server. After a positive response, the Public Spot starts a new session for that user and forwards the associated packets.
- If all of the above checks fail, the Public Spot directs the user to the login page.

Authentication of the MAC address by RADIUS

If the MAC address of a WLAN client requesting to associate is not included in the list of approved addresses, the Public Spot alternatively authenticates the address via a RADIUS server.

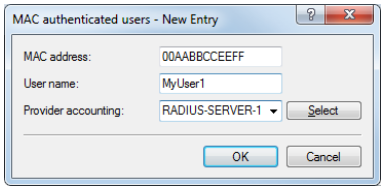
To enable RADIUS authentication, the administrator selects one of the RADIUS servers that has defined in the device and saved to the list of providers.

In addition, the administrator defines a lifetime for the rejected MAC addresses. The Public Spot uses this lifetime to prevent the RADIUS server from being flooded with repeated requests for MAC addresses that cannot be authenticated via the RADIUS server or MAC address table.

If a MAC address authentication is rejected by the RADIUS server, the Public Spot stores this rejection for the lifetime defined here. The Public Spot responds to further requests for the same MAC address directly and without forwarding them to the RADIUS server first.

Configuration by LANconfig

For the configuration in LANconfig, you find the parameters for the authentication of clients by MAC address in the dialog **Public Spot** > **Users** > **MAC authenticated users**.



Automatic authentication via WISPr

Your device provides an interface for authentication via WISPr. The **WISPr** standard is the technological predecessor of the 802.11u and Hotspot 2.0 specifications. The acronym stands for **Wireless Internet Service Provider roaming** and designates both a process and a protocol that allow users of WLAN enabled devices to roam seamlessly between the WLANs of different operators – and, therefore, between their Internet service providers. The idea behind it is similar to that of 802.11u and Hotspot 2.0; however, it requires more comprehensive support by the respective users.

Using the WISPr protocol, you can provide logins and network usage on your hotspot in a manner similar to Hotspot 2.0, even for end devices that no longer support Hotspot 2.0. The prerequisite is that your service provider provides the necessary infrastructure. Support for the user's device is provided either by the operating system or a suitable app (smart client). This client handles authentication to the hotspot for the user. If no credentials are available for the relevant network, the client queries the user for valid credentials at the system level. In any case, this eliminates the user having to log in via a login web page in the browser.

Because of its age, almost all current end devices with iOS, Android and Windows 8 support the WISPr protocol. In addition, larger WLAN Internet service providers often have their own apps to make the login for their clients easier: These apps include a preconfigured database of the provider's own hotspots and, optionally, those of their roaming partners. The authentication process corresponds to the following schema:

1. A customer installs his provider's hotspot app to act as a client, which provides a database of preconfigured hotspot SSIDs.
2. The client connects automatically with one of the hotspots and sends a HTTP-GET-Request to a random URL to test if direct Internet access is available or the Public Spot requires authentication.
3. In HTTP-Redirect the hotspot sends a WISPr-XML-Tag with the Login-URL.
4. The client sends its login data to the Login-URL in an HTTP-Post.

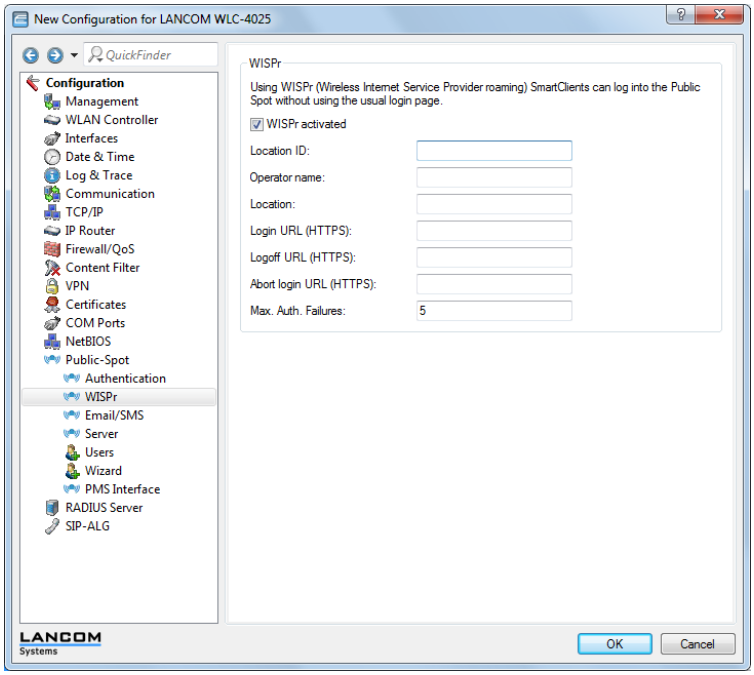
Example for an XML-Tag in redirect:

```
<HTML>
<?xml version="1.0" encoding="UTF-8"?>
  <WISPAccessGatewayParam xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccess GatewayParam.xsd">
    <Redirect>
      <AccessProcedure>1.0</AccessProcedure>
      <AccessLocation>Hotel Contoso Guest Network</AccessLocation>
      <LocationName>Hotel Contoso</LocationName>
      <LoginURL>https://captiveportal.com/login</LoginURL>
      <MessageType>100</MessageType>
      <ResponseCode>0</ResponseCode>
    </Redirect>
   </WISPAccessGatewayParam>
</HTML>
```

In order to use WISPr, the device must have an SSL certificate and a private key installed. The certificate must either be signed by a trusted authority or – if it is a self-signed certificate – be imported as a trusted certificate on the client. Otherwise the client will reject the login via WISPr. Further information about loading these objects on your device can be found in the LANCOM techpaper "Certificate Management in Public Spots" available from *www.lancom-systems.com*.

Configuring WISPr

Configure the WISPr function of your device in the menu **Public Spot** > **WISPr**.



In this window you have the following options:

- **WISPr activated**: Enable or disable the WISPr function for the device.
- **Location ID**: Use this ID to assign a unique location number or ID for your device, for example, in the format `isocc=<ISO_Country_Code>,cc=<E.164_Country_Code>,ac=<E.164_Area_Code>,network=<SSID/ZONE>`
- **Operator name**: Enter the name of the hotspot operator, e.g., `providerX`. This information helps the user to manually select an Internet service provider.
- **Location**: Describe the location of your device, e.g., `CafeX_Market3`. This helps to better identify a user in your hotspot.
- **Login URL (HTTPS)**: Enter the HTTPS address, that the WISPr client uses to transfer the credentials to your Internet service provider. Any external URL can be entered or the Public Spot itself. If the Public Spot should authenticate users using WISPr, enter the URL in the format `https://<Device-FQDN>/wisprlogin`. For "wisprlogin" in the example, any freely defined path can be used.
- **Logoff URL (HTTPS)**: Enter the HTTPS address that a WISPr client uses for logging off at your Internet service provider. The same rules apply as for the login URL.
- **Abort login URL (HTTPS)**: Enter the HTTPS address to which the device forwards a WISPr client if authentication fails. The same rules apply as for the login URL.

The three URLs must be different, if the Public Spot is used in the device domain, for example:

- Login-URL: https://<Device-FQDN>/wisprlogin
- Logoff-URL: https://<Device-FQDN>/wisprlogoff
- Abort-Login-URL: https://<Device-FQDN>/wisprabort

Finally, for test purposes, you can also configure an URL with IP addresses. In a production system, the client will check the FQDN of the certificate!

- **Max. auth. failures**: Enter the maximum number of failed attempts which the login page of your Internet service provider allows. If the Public Spot is used, the Public Spot rejects further login attempts by the specified client after this number of failed attempts.

IEEE 802.11u and Hotspot 2.0

Your device supports WLAN connections according to the IEEE 802.11u standard and the Hotspot 2.0 specification, which is based on it. Using 802.11u you have the option to implement automatic authorization and authentication of your users on a local WLAN network (for example, within your company) or a Public Spot network. The prerequisite for this is that the relevant stations (smartphones, tablet PCs, notebooks, etc.) also support connections for 802.11u and Hotspot 2.0. In detail, the following functions are offered:

- **Automatic network selection**

  In a 802.11u-enabled environment, the user does not have to manually detect and select an SSID. Instead, the client independently searches for and selects a suitable Wi-Fi network by automatically requesting and evaluating the operator and network data of all 802.11u- access points that are in range. A previous login to the access point is not required.

  Hotspot 2.0 stations also have the ability to retrieve information about the services available in a Wi-Fi network. If specific services that are relevant for a user (e.g., connections via HTTP, VPN or VoIP) are not available for a Wi-Fi network, any networks that do not meet the criteria are excluded from further searches. This ensures that users are always connected to the optimal network.

- **Automatic authentication and authorization**

  In 802.11u-enabled environments, the station automatically carries out the user's login if the necessary credentials are available. Authentication can be done, for example, using a SIM card, a username and password, or a digital certificate. Repetitive manual input of the credentials by the user in a login screen is no longer necessary. After successful authentication, the user can immediately use the desired services.

- **Seamless handover**

  Connections according to 802.11u and in conjunction with 802.21 facilitate the uninterrupted exchange of data connections between different network types. This enables users to switch their stations seamlessly from a cellular network to a WLAN network as soon as they get within range of a Hotspot 2.0 zone—and vice versa. The same is true for the transfer between two different operators if, for example, the user goes from one homogeneous network to another during a bus trip

- **Automatic roaming**

  Connections as per 802.11u facilitate roaming between different operator networks. If a user is in range of a Hotspot 2.0 zone of an operator for which he does not have any credentials, his station still has the option to switch to its home network. Authentication at a third-party Hotspot 2.0 zone is handled by the operator's roaming partner, which then allows the user to access the third-party Wi-Fi network. This is interesting not only in areas where there are only single network operators with access points, it is also especially attractive for people traveling abroad.

Example: For example, a user who is in transit in the city with his 802.11u-enabled smartphone (station) can enable the WLAN feature to browse the Internet. The station then starts trying to find all available Wi-Fi networks in the area. If any of the access points offer 802.11u, the station selects the one network that best fits the required service based on the operator and network information that was previously obtained, for example, from a hotspot offering Internet access from its own cellular network company. In this case, the subsequent authentication can be performed automatically via the SIM card so that the user does not need to intervene at any time during the process. The encryption method selected for the connection – e.g., WPA2 – is unaffected.

In summary, connections according to 802.11u and with Hotspot 2.0 enabled combine the security features and performance of classic Wi- Fi hotspots with the flexibility and simplicity of data cellular network connections. At the same time, they relieve the cellular networks by redistributing data traffic (and possibly also telephony) to the network connections and frequency bands offered by access points.

Passpoint® Release 2

As of LCOS 10.40 the extended Hotspot 2.0 feature in your WLAN device can be configured as per Passpoint® Release 2 as specified by the Wi-Fi Alliance. The RADIUS server in the LCOS has been equipped with the necessary features since 10.32 version RU4.

Passpoint® Release 2 simplifies the onboarding of devices into a network using the WPA2-Enterprise (802.1X) encryption method. A dedicated onboarding SSID allows a user with a device that supports Passpoint® Release 2 to install a profile and automatically switch to the encrypted network using the stored credentials. This helps to implement hotspots that provide encrypted wireless communication. An onboarding SSID can be used to give guests temporary access credentials.

Similarly, a mobile service provider can relieve the load on their cellular network by introducing Wi-Fi offloading and allowing mobile devices with a SIM card to automatically log into their WLAN network. Customers' devices find the WLAN network from the mobile service provider and automatically login to the operator's WLAN network using the user data stored on the SIM card.

Passpoint® Release 2 adds the following features to Hotspot 2.0:

- Online Sign-Up (OSU) – with Passpoint® Release 2, companies and network operators can use "Online Sign-Up" servers (OSU servers) to deliver profiles to their users. Using an open OSU SSID, users can identify various OSU servers by their icons and thus select the one that suits them best. The OSU server can optionally ask the user for credentials before providing a profile that best suits the user's device. In addition to the open OSU-SSID, an encrypted SSID can be used to exchange user data by means of "anonymous EAP-TLS". This requires the use of a RADIUS server that supports "anonymous EAP-TLS".

  An OSU server is not included with LCOS. However, solutions are available from LANCOM partners.

- OSU icons – icons corresponding to the supported OSU servers can be uploaded to the LCOS as files using the WEBconfig feature **File management**. We recommend PNG as the file format.
- Notification – the network can notify the user about an imminent logout from the RADIUS server. This may be the case if the user credentials have expired or if the specified connection duration has been reached.
- QoS Map – the "QoS Map Set" function enables an access point to instruct its clients to use a specific QoS map. This defines the values for the contention window (media access via EDCA) of the various access categories (voice, video, best effort and background data packets) and the corresponding DSCP parameters. At the same time, the access points also use the values stored in the QoS map.

  Currently available are the two QoS maps required by the Wi-Fi-Alliance and the default QoS map of the LCOS.

Hotspot operators and service providers

The Hotspot 2.0 specification of the Wi-Fi Alliance differentiates between hotspot operators and hotspot service providers: A **hotspot operator** only operates one Wi-Fi network, while a **hotspot service provider** (SP) provides the connection for the user to the Internet or a cellular network. Of course, it is possible for an operator to also be an SP. However, in all other cases, a hotspot operator requires the corresponding roaming agreements with an SP or a group of multiple SPs (called a roaming consortium). Only when an operator has made these agreements are the various roaming partners' customers able to authenticate with the hotspot operator. Each service provider operates its own AAA infrastructure. A hotspot communicates this list of possible roaming partners and the name of the hotspot operator using ANQP (see functional description).

Functional description

The 802.11u standard is the base standard of IEEE. This standard essentially expands access points or hotspots with the ability to broadcast so-called "ANQP data packets "(Advanced Message Queuing Protocol) in its broadcast signals. ANQP is a query/response protocol that a device can use to request a range of information about the hotspot. This includes both meta-data, such as information about the owner and the venue, as well as information on the underlying network, such as information on operator domains, roaming partners, authentication methods, forwarding addresses, etc. All 802.11u-enabled devices in range have the ability to request these data packets without a prior login to the access point in order to select a network based on the network information.

The Wi-Fi Alliance has added further ANQP elements to the standard, and markets this specification as **Hotspot 2.0**. This Hotspot 2.0 function merely adds additional elements to the standard, which the device can use as criteria for selecting its network. These criteria include, for example, information about the services and WAN metrics available at the hotspot. The associated certification program is called Passpoint®, which is available in different versions. Certain LANCOM access points are Wi-Fi Alliance Passpoint® CERTIFIED (Release 1 and/or 2).

The ANQP data packets are the central information element of the 802.11u standard. However, to signal the support for 802.11u and to transmit data packets, further elements are required for the operation of 802.11u:

- The signaling of 802.11u support in the beacons and probes of a hotspot are done by the element known as the **Interworking element**. In this element, the initial basic network information—such as the network classification, Internet availability (Internet bit) and the OI of the roaming consortium and/or of the operator—are already included. At the same time, it is used by 802.11u-enabled devices as an initial screening criterion when detecting a network.
- ANQP data packets are transferred within the so-called GAS containers. GAS stands for Generic Advertisement Service, and is the name of generic containers that allow a device to request additional internal and external information for the network selection from the hotspot, in addition to the information in the beacons. The GAS containers are transmitted on layer 2 by what are referred to as public action frames.

Login by an 802.11u-enabled client at a Hotspot 2.0

The following functional description schematically illustrates the selection and login process of an 802.11u-enabled device at a Hotspot 2.0.

Login via username/password or digital certificate

1. The hotspots reply with an ANQP response, which contains, among other things, the name of the hotspot operator and a list of NAI realms, which list all available roaming partners (service provider, abbreviated SP).
2. The device loads the locally stored credentials from the WLAN profiles or installed certificates that were set up by the user, and compares the local realms with the NAI realm lists obtained in (2).
   a. If the device successfully finds one, it knows that it can be authenticated successfully on the relevant Wi-Fi network.
   b. If the device successfully finds more than one, the selection of a Wi-Fi network is made based on the user's preference list. This list defines the preferred order of operators in conjunction with the potential roaming partners. In this case, the device compares the operator names listed under (2) with the list, and selects the operator with the highest priority.
3. The device authenticates itself with its local credentials at the hotspot of the preferred operator for the appropriate SP. The access point then transmits this data over its SSPN interface (Subscription Service Provider Network) to an AAA system responsible for authentication. The authentication is performed using the authentication method determined by the SP. The authentication via username/password uses EAP-TTLS, and authentication via digital certificate uses EAP-TLS.

Login via (U)SIM

1. In contrast to the login via username/password or digital certificate, a device with a (U)SIM does not request the list of NAI realms in its ANQP requests, but rather the 3GPP Cellular Network Information. The ANQP responses contain the cellular network information list of all cellular network providers for which the access point offers authentication.
2. The device loads the parameters for the cellular network from its local (U)SIM card, and compares it with the data retrieved from the cellular network information lists. The list comparison and selection of a preferred provider network is performed analogous to the login via username/password or digital certificate.
3. The device authenticates itself with its local credentials at the hotspot of the preferred operator for the appropriate cellular network company. The hotspot then transmits this data over its SSPN interface (Subscription Service Provider Network) to an AAA system responsible for the authentication. The presence of a (U)SIM card changes the possible authentication method for the device to EAP-SIM or EAP-AKA.

4. The AAA system verifies the credentials for authentication via the interface MAP (Mobile Application Part) at the HLR server (Home Location Register) of the cellular network company.

If authentication is successful, the device gets access to the WLAN network either via hotspot (credentials for the operator's network are available) or automatic roaming (credentials for the operator's network are not available).

If there are multiple authentication options available for the device (e.g., SIM card and username/password), it has the option of using the preferred EAP authentication method and, therefore, the preferred credentials based on the NAI realm or cellular network information list.

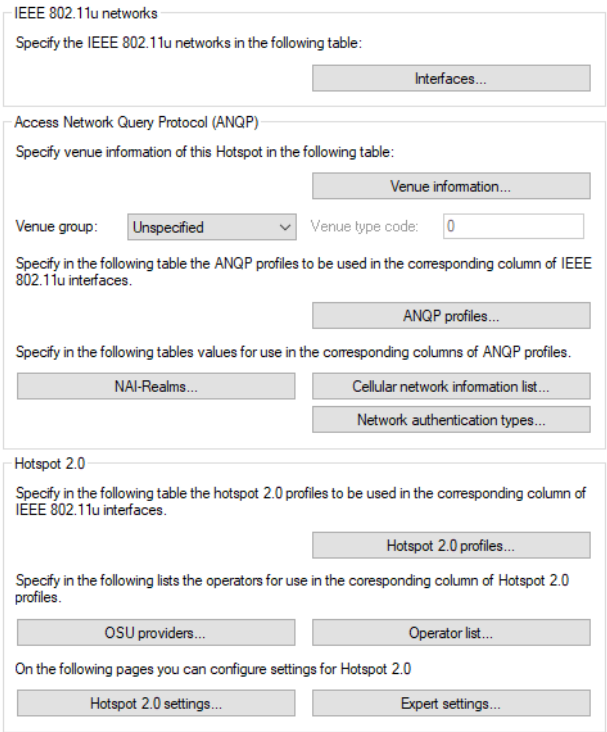
Recommended general settings

The Hotspot 2.0 specification recommends the following general settings for the 802.11u operator:

- WPA2-Enterprise Security (802.1X) enabled
- Authentication using EAP with the corresponding variant:
  - EAP-SIM/EAP-AKA for authentication with SIM / USIM card
  - EAP-TLS for authentication with a digital certificate
  - EAP-TTLS for authentication with a username and password
- Enabled and properly configured ARP proxy
- Disabled multicasts and broadcast in cellular networks
- Non-approved data traffic between the cellular network devices (Layer 2 traffic inspection and filtering). The corresponding settings can be found in LANconfig under **Wireless LAN** > **Security** > **Traffic between different SSIDs**.
- Enabled and implemented firewall on the access router, which provides Internet access

Configuration menu for IEEE 802.11u / Hotspot 2.0

The configuration menu for IEEE 802.11u and Hotspot 2.0 is located under **Wireless LAN** > **IEEE 802.11u**.



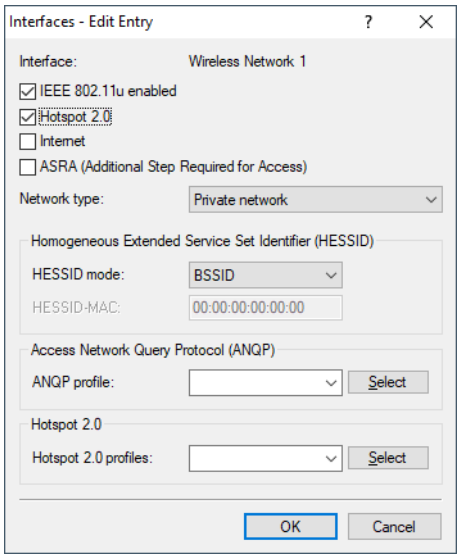
The device offers the ability to individually enable or disable and configure the support the IEEE 802.11u standard as well as the Hotspot 2.0 functionality for each logical WLAN interface using the button **Interfaces**.

Some parameters need to be configured in what are known as “Profiles”. Using profiles, you can group different rows in lists, which you only have to reference from the other windows. Essentially, these are profiles for ANQP data packets and Hotspot 2.0. The relationships between the profile lists is as follows:

```
| -- Interfaces
  |--ANQP profiles
    |--NAI realms
    |--Cellular network information list
    |--Network authentication types
  |--Hotspot 2.0 profiles
    |--Operator list
    |-- OSU providers
```

Activating interfaces

The table **Interfaces** is the highest administrative level for IEEE 802.11u and Hotspot 2.0. Here you have the option of enabling or disabling functions for each interface, assigning them different profiles, or modifying general settings.



Interface

Name of the logical WLAN interface that you are currently editing.

IEEE 802.11u enabled

Enable or disable support for connections according to IEEE 802.11u at the appropriate interface. If you enable support, the device sends the interworking element in beacons/probes for the interface or for the associated SSID, respectively. This element is used as an identifying feature for IEEE 802.11u-enabled connections: It includes, for example, the Internet bit, the ASRA bit, the HESSID, and the location group code and the location type code. These individual elements use 802.11u-enabled devices as the first filtering criteria for network detection.

Hotspot 2.0

Enable or disable the support for Hotspot 2.0 according to the Wi-Fi Alliance® at the appropriate interface. Hotspot 2.0 extends the IEEE standard 802.11u with additional network information, which stations can request using an ANQP request. These include, for example, the operator-friendly name, the connection capabilities, operating class and WAN metrics. Using this additional information, stations are in a position to make an even more selective choice of Wi-Fi network.

Internet

Select whether the Internet bit is set. The Internet-bit explicitly informs all stations that the Wi-Fi network allows Internet access. Enable this setting if services other than internal services are accessible via your device.

Using this function you only communicate the availability of an Internet connection. You configure the corresponding regulations on the firewall, irrespective of this option.

ASRA – Additional steps for access required

Select whether the ASRA bit (Additional Step Required for Access) is set. Using the ASRA bit explicitly informs all stations that further authentication steps are needed to access the Wi-Fi network. Enable this setting if you have, for example, set up online registration, additional authentication, or a consent form for your terms of use on your web site.

Please remember to specify a forwarding address in the **Network authentication types** table for the additional authentication and/or **WISPr** for the Public Spot module if you set the ASRA bit.

Network type

Select a network type from the available list which most closely describes the Wi-Fi network behind the selected interface. Based on the setting made here, the user has the option to limit network detection of their devices to specific network types. Possible values are:

Private network

Describes networks which are blocked to unauthorized users. Select this type, for example, for home networks or corporate networks where access is limited to employees.

Private with guest access

Similar to **Private network**, but with guest access for unauthorized users. Select this type, for example, for corporate networks where visitors may use the Wi-Fi network in addition to employees.

Chargeable public network

Describes public networks that are accessible to everyone and can be used for a fee. Information about fees may be available through other channels (e.g.: IEEE 802.21, HTTP/HTTPS or DNS forwarding). Select this type, for example, for hotspots in shops or hotels that offer fee-based Internet access.

Free public network

Describes public networks that are accessible to everyone and for which no fee is payable. Select this type, for example, for hotspots in public, local and long-distance transport, or for community networks where Wi-Fi access is an included service.

Personal device network

In general, it describes networks that connect wireless devices. Select this type, for example, for digital cameras that are connected to a printer via WLAN.

Emergency services only network

Describes networks that are intended for, and limited to, emergency services. Select this type, for example, for connected ESS or EBR systems.

Test or experimental

Describes networks that are set up for testing purposes or are still in the setup stage.

Wildcard

Placeholder for previously undefined network types.

HESSID mode

Specify where the device gets its HESSID for the homogeneous ESS. A homogeneous ESS is defined as a group of a specific number of access points, which all belong to the same network. The MAC address of a connected access point serves as a globally unique identifier (HESSID). The SSID can not be used as an identifier in this case, because different network service providers can have the same SSID assigned in a hotspot zone, e.g., by common names such as “HOTSPOT”. Possible values for the HESSID mode include:

BSSID

Select this item to set the BSSID of the device as the HESSID for your homogeneous ESS.

User

Select this item to manually assign a HESSID.

None

Select this item in order to not assign any homogeneous ESS and to isolate it from the device network.

HESSID-MAC

If you selected the setting `user` for the **HESSID mode**, enter the HESSID of your homogeneous ESS as a 6-octet MAC address. Select the BSSID for the HESSID for any access point in your homogeneous ESS in capital letters and without separators, e.g., "008041AEFD7E" for the MAC address 00:80:41:ae:fd:7e.

If your device is not present in multiple homogeneous ESS's, the HESSID is identical for all interfaces

ANQP profile

Select an ANQP profile from the list. You create ANQP profiles in the configuration menu using the button of the same name.

Hotspot 2.0 profiles

Select the Hotspot 2.0 profile from the list. You create the Hotspot 2.0 profiles in the configuration menu using the button of the same name.

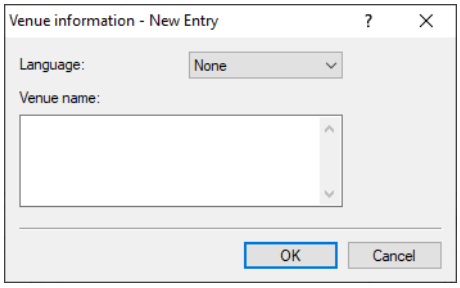
Configuring ANQP data packets

Venue information and group

Information about the access point's location is managed using the table **Venue information** and the subsequent dialogs **Venue group** and **Venue type code**.

In the event of a manual search, additional details on the **Venue information** help a user to select the correct hotspot. If more than one operator (e.g., multiple cafés) in a single hotspot zone uses the same SSID, the user can clearly identify the appropriate location using the venue information.

You can place your device in a predefined category using the **Venue group** and **Venue type code** – as opposed to the user-defined location information.



Language

You have the ability to specify custom information for the location of the access point for each language. The location name that matches your user's language will then be displayed. If a language is not available for a user, its station chooses one based, for example, on the default language.

Location name

Enter a short description of the location of your device for the selected language, for example:

```
Ice Café Valencia
123 Street
City, State 12345
```

The **Venue group** describes the environment where you operate the access point. You define them globally for all languages. The possible values, which are set by the "venue group code", are specified in the 802.11u standard.

Using the **Venue type code**, you have the option to specify the details for the venue group. These values are also specified by the standard. The possible type codes can be found in the following table.

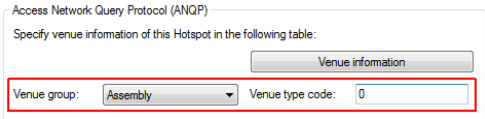


Table 3: Overview of possible values for venue groups and types

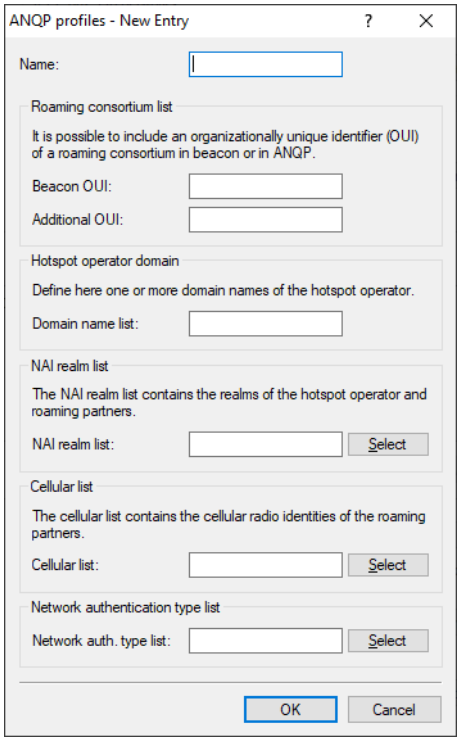
Venue group	Venue type code
Unspecified	
Assembly	> 0 = unspecified assembly > 1 = stage > 2 = stadium > 3 = passenger terminal (e.g., airport, bus station, ferry terminal, train station) > 4 = amphitheater > 5 = amusement park > 6 = place of worship > 7 = convention center > 8 = library > 9 = museum > 10 = restaurant > 11 = theater > 12 = bar > 13 = café > 14 = zoo, aquarium > 15 = emergency control center
Business	> 0 = unspecified business > 1 = doctor's office > 2 = bank > 3 = fire station > 4 = police station > 6 = post office > 7 = office > 8 = research facility > 9 = law firm
Educational:	> 0 = unspecified education > 1 = primary school > 2 = secondary school > 3 = college
Factory and industry	> 0 = unspecified factory and industry > 1 = factory

Venue group	Venue type code
Institutional	> 0 = unspecified institution > 1 = hospital > 2 = long-term care facility (e.g., nursing home, hospice) > 3 = rehabilitation clinic > 4 = organizational association > 5 = prison
Commerce	> 0 = unspecified commerce > 1 = retail store > 2 = food store > 3 = Automobile workshop > 4 = shopping center > 5 = gas station
Halls of residence	> 0 = unspecified residence hall > 1 = private residence > 2 = hotel or motel > 3 = student housing > 4 = guesthouse
Warehouse	> 0 = unspecified warehouse
Utility and miscellaneous	> 0 = unspecified service and miscellaneous
Vehicular	> 0 = unspecified vehicle > 1 = passenger or transport vehicles > 2 = aircraft > 3 = bus > 4 = ferry > 5 = ship or boat > 6 = train > 7 = motorcycle
Outdoor	> 0 = unspecified outdoor > 1 = municipal WLAN network > 2 = city park > 3 = rest area > 4 = traffic control > 5 = bus stop > 6 = kiosk

ANQP profiles

Using this table you manage the profile lists for ANQP. **ANQP profiles** offer you the ability to group certain ANQP elements and to assign them to mutually independent logical WLAN interfaces in the table **Interfaces**. These elements

include, for example, information about your OIs, domains, roaming partners and their authentication methods. Some of the elements are located in other profile lists.



Name

Assign a name for the ANQP 2.0 profile here. This name will appear later in the interfaces table in the selection for ANQP profiles.

Beacon OUI

Organizationally Unique Identifier, abbreviated as OUI, simplified as OI. As the hotspot operator, you enter the OI of the roaming partner with whom you have agreed a contract. If you are the hotspot operator as well as the service provider, enter the OI of your roaming consortium or your own OI. A roaming consortium consists of a group of service providers which have entered into mutual agreements regarding roaming. In order to get an OI, this type of consortium – as well as an individual service provider – must register with IEEE.

It is possible to specify up to 3 parallel OIs, in case you, as the operator, have roaming agreements with several partners. Multiple OIs can be provided in a comma-separated list, such as `00105E,00017D,00501A`.

This device transmits the specified OI(s) in its beacons. If a device should transmit more than 3 OIs, these can be configured under **Additional OUI**. However, additional OIs are not transferred to a station until after the GAS request. They are not immediately visible to the stations!

Additional OUI

Enter the OI(s) that the device also sends to a station after a GAS request. Multiple OIs can be provided in a comma-separated list, such as `00105E,00017D,00501A`.

Domain name list

Enter one or more domains that are available to you as a hotspot operator. Multiple domain names are separated by a comma separated list, such as `providerX.org,provx-mobile.com,wifi.mnc410.provX.com`. For subdomains it is

sufficient to specify only the highest qualified domain name. If a user configured a home provider on his device, e.g., providerX.org, this domain is also assigned to access points with the domain name wi-fi.providerX.org. When searching for suitable hotspots, a station always prefers a hotspot from his home provider in order to avoid possible roaming costs.

NAI realm list

Select an NAI realm profile from the list. You specify profiles for NAI realms in the configuration menu by clicking the button **NAI realms**.

Cellular list

Select the cellular network identity from the list. You set the identities for cellular networks – similar to profiles – in the configuration menu using the button **Cellular network information list**.

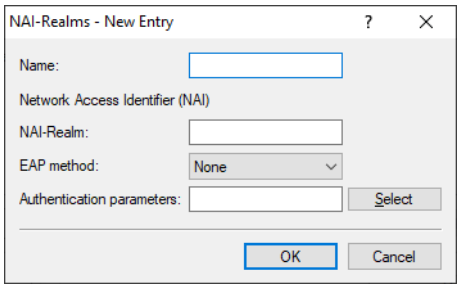
Network authentication type list

Select an authentication profile from the list. You specify profiles for network authentication in the configuration menu by clicking the button **Network authentication types**.

Additionally, the CLI provides the option to show the type of available IP addresses, which they can obtain from the network after successful authentication. You can access the relevant parameters **IPv4-Addr-Type** and **IPv6-Addr-Type** via the path **Setup** > **IEEE802.11u** > **ANQP-General**.

NAI realms

Using this table you manage the profile lists for the NAI realms. With these lists you have the ability to group certain ANQP elements. These include the realms of the hotspot operator and its roaming partners, as well as the associated authentication methods and parameters. Stations use the information stored in this list to determine whether they have the hotspot operator or one of its roaming partners have valid credentials.



Name

Assign a name for the NAI realm profile, such as the name of the service provider or service to which the NAI realm belongs. This name will appear later in the ANQP profile in the selection for **NAI realm list**.

NAI realm

Enter the realm for the Wi-Fi network. The identification of the NAI realm consists of the username and a domain, which can be extended using regular expressions. The syntax for an NAI realm is defined in *RFC 2486* and, in the simplest case, is `<username>@<realm>`. For `user746@providerX.org`, the corresponding realm is `providerX.org`.

EAP-Method

Select a language for the NAI realm from the list. EAP stands for the authentication profile (Extensible Authentication Protocol), followed by the corresponding authentication method Possible values are:

EAP-TLS

Authentication using Transport Layer Security (TLS). Select this setting when authentication via the relevant NAI realm is performed by a digital certificate that the user has to install.

EAP-SIM

Authentication via the Subscriber Identity Module (SIM). Select this setting when authentication via the relevant NAI realm is performed by the GSM Subscriber Identity Module (SIM card) of the station.

EAP-TTLS

Authentication via Tunneled Transport Layer Security (TTLS). Select this setting when authentication via the relevant NAI real is performed using a username and password. For security reasons, the connection is tunneled for this method.

EAP-AKA

Authentication using Authentication and Key Agreement (AKA). Select this setting when authentication via the relevant NAI realm is performed by the UMTS Subscriber Identity Module (USIM card) of the station.

None

Select this setting when the relevant NAI realm does not require authentication.

Authentication parameters

Click the authentication parameters that match the EAP method, e.g. for EAP-TTLS

`NonEAPAuth.MSCHAPV2,Credential.UserPass`

or for EAP-TLS `Credentials.Certificate`.

Possible values are:

Table 4: Overview of possible authentication parameters

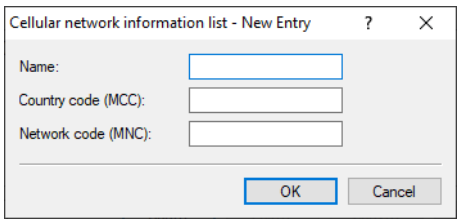
Parameter	Sub-Parameter	Comment
NonEAPAuth		Identifies the protocol that the realm requires for phase 2 authentication:
	PAP	Password Authentication Protocol
	CHAP	Challenge Handshake Authentication Protocol, original CHAP implementation, specified in *RFC 1994*
	MSCHAP	Implementation of Microsoft CHAP V1, specified in *RFC 2433*
	MSCHAPV2	Implementation of Microsoft CHAP V2, specified in *RFC 2759*
Credentials		Describes the type of authentication that the realm accepts:
	SIM	SIM card
	USIM	USIM card
	NFCSecure	NFC chip
	HWToken*	Hardware token
	SoftToken*	Software token
	Certificate	Digital certificate
	UserPass	Username and password

* The specific parameter or sub-parameter is reserved for future uses within the framework of Passpoint™ certification, but currently is not in use.

Parameter	Sub-Parameter	Comment
TunnelEAPCredentials.*	None	No credentials required
	SIM*	SIM card
	USIM*	USIM card
	NFCSecure*	NFC chip
	HWToken*	Hardware token
	SoftToken*	Software token
	Certificate*	Digital certificate
	UserPass*	Username and password
	Anonymous*	Anonymous login

Cellular network information list

Using this table you manage the identity lists for cellular networks. With these lists you have the ability to group certain ANQP elements. These include the network and country codes of the hotspot operator and its roaming partners. Based on the information stored here, stations with SIM or USIM cards use this list to determine if the hotspot operator belongs to their cellular network company or has a roaming agreement with their cellular network company.



Name

Assign a name for the cellular network identity, such as an abbreviation of the network operator in combination with the cellular network standard used. This name will appear later in the ANQP profile in the selection for **Cellular list**.

Country code (MCC)

Enter the Mobile Country Code (MCC) of the hotspot operator or its roaming partners, consisting of 2 or 3 characters, e.g., `262` for Germany.

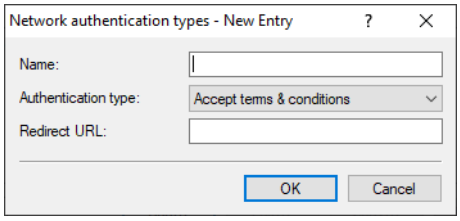
Network code (MNC)

Enter the Mobile Network Code (MNC) of the hotspot operator or its roaming partners, consisting of 2 or 3 characters.

Network authentication types

Using this table, you manage addresses to which the device forwards stations for an additional authentication step after the station has been successfully authenticated by the hotspot operator or any of its roaming partners. Only one forwarding entry is allowed for each authentication type.

Please remember to set the ASRA bit in the **Interfaces** table if you set up an additional authentication step.



Name

Assign a name for the table entry, for example `Accept Terms & Conditions`. This name will appear later in the ANQP profile in the selection for **Network auth. type list**.

Authentication type

Choose the context from the list, which applies before forwarding. Possible values are:

Accept terms & conditions

An additional authentication step is set up that requires the user to accept the terms of use.

Online enrollment

An additional authentication step is set up that requires the user to enroll online first.

HTTP redirection

An additional authentication step is set up to which the user is forwarded via HTTP.

DNS redirection

An additional authentication step is set up to which the user is forwarded via DNS.

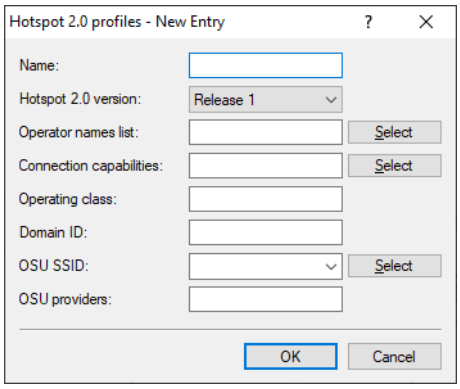
Redirect URL

Enter the address to which the device forwards stations for additional authentication.

Configuring Hotspot 2.0

Hotspot 2.0 profiles

Using this table you manage the profile lists for the Hotspot 2.0. **Hotspot 2.0 profiles** offer you the ability to group certain ANQP elements (from the Hotspot 2.0 specification) and to assign them to mutually independent logical WLAN interfaces in the table **Interfaces**. These include, for example, the operator-friendly name, the connection capabilities, operating class and WAN metrics. Some of the elements are located in other profile lists.



Name

Assign a name for the Hotspot 2.0 profile here. This name will appear later in the interfaces table in the selection for the Hotspot 2.0 profile.

Hotspot 2.0 version

Set the Hotspot-2.0 release supported by this profile.

A client must support this release in order to connect.

Operator names list

Select the profile of a hotspot operator from the list. You specify profiles for hotspot operators in the configuration menu by clicking the **Operator list**.

Connection capabilities

Select the connection capabilities for each service. Before joining a network, stations use the information stored in this list to determine whether your hotspot even allows the required services (e.g., Internet access, SSH, VPN). For this reason, the fewest possible entries should be entered with the status "unknown". Possible status values for each of these services are "closed" (`-C`), "open" (`-O`) or "unknown" (`-U`):

- `ICMP`: Specify whether to allow the exchange of information and error messages via ICMP.
- `TCP-FTP`: Specify whether to allow file transfers via FTP.
- `TCP-SSH`: Specify whether to allow encrypted connections via SSH.
- `TCP-HTTP`: Specify whether to allow Internet connections via HTTP/HTTPS.
- `TCP-TLS`: Specify whether to allow encrypted connections via TLS.
- `TCP-PPTP`: Specify whether to allow the tunneling of VPN connections via PPTP.
- `TCP-VOIP`: Specify whether to allow Internet telephony via VoIP (TCP).
- `UDP-IPSEC-500`: Specify whether to allow IPsec via UDP and port 500.
- `UDP-VOIP`: Specify whether to allow Internet telephony via VoIP (UDP).
- `UDP-IPSEC-4500`: Specify whether to allow IPsec via UDP and port 4500.
- `ESP`: Specify whether to allow ESP (Encapsulating Security Payload) for IPsec.

If you do not know if a service is available and its ports are open or closed on your network, or you consciously do not want to make any entry for the status, select a `-U` setting.

Using this dialog, you do not define permissions! The stations only use the entries to determine whether to join a network via your device. You configure specific access permissions for your network with other device functions, such as the firewall/QoS.

Operating class

Enter the code for the global operating class of the access point. Using the operating class, you inform a station about the frequency bands and channels that your access point is available on. Example:

- `81`: Operation at 2.4 GHz with channels 1-13
- `116`: Operation at 40 MHz with channels 36 and 44

Please refer to the IEEE standard 802.11- 2012, Appendix E, Table E-4, for the operating class that corresponds to your device: Global operating classes, available at *standards.ieee.org*.

Domain ID

The domain ID indicates which ANQP server is used. All access points and SSIDs with the same number/domain ID (16- value) use the same ANQP server.

A client sending an ANQP request to access points / SSIDs with the same domain ID would always receive the same response. To get different responses, the client would have to look for different domain IDs.

OSU SSID

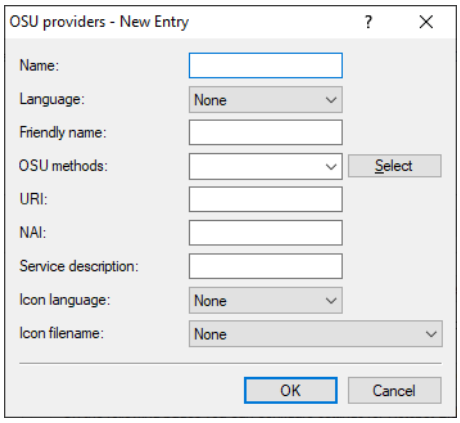
Name of the SSID that provides access to the OSU server.

OSU providers

List of OSU provider names in *OSU providers* on page 90 that are supported in the profile.

OSU providers

In this table, you configure the OSU providers for online sign-up with Passpoint® Release 2.



Name

Give this OSU provider a name so that you can reference it later. By using the same name repeatedly, this provider can be used for several languages.

Language

Set the language supported by this OSU provider.

Friendly name

Give this OSU provider a descriptive name.

OSU methods

Set the OSU methods used by this OSU provider. Options are “OMA-DM” or “SOAP-XML-SPP”.

Available methods with the online sign-up server with Passpoint® Release 2:

- OMA – Open Mobile Alliance
- DM – Device Management
- SOAP – Simple Object Access Protocol
- XML – eXtended Markup Language
- SPP – Subscription Provisioning Protocol

URI

Enter a URI where a client can reach the OSU server.

NAI

Enter the Network Access Identifier (NAI) for this OSU provider.

Service description

Enter a descriptive text for this service here.

Icon language

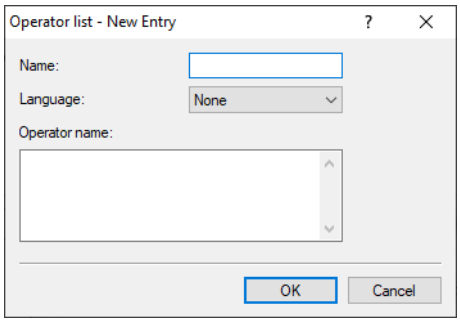
This item sets the language for the selected icon.

Icon-Filename

Select an icon for this OSU provider. Icons can be uploaded as files with WEBconfig. We recommend PNG as the file format.

Operator list

Using this table you manage the cleartext name of the hotspot operator. An entry in this table offers you the ability to send a user-friendly operator name to the stations, which they can then display instead of the realms. However, whether they actually do that depends on their implementation.



Name

Assign a name for the entry, such as an index number or combination of operator name and language.

Language

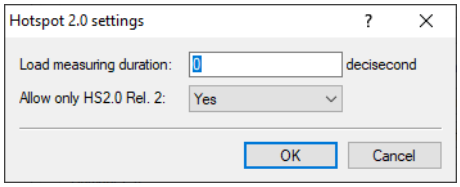
Select a language for the hotspot operator from the list.

Operator name

Enter the cleartext name of the hotspot operator.

Hotspot 2.0 settings

This table is used to configure particular settings for Hotspot 2.0.



Load measuring duration

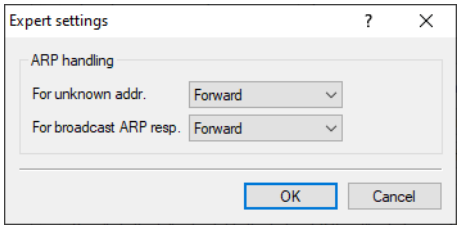
Measurement cycle for WAN downlink/uplink speeds in tenths of a second.

Allow only Hotspot 2.0 Release 2

A requirement of HotSpot 2.0 Release 2 is that it only allows Release 2 clients. This can be turned off with this switch.

Expert settings

This table is used to configure the expert settings for Hotspot 2.0. The settings in this menu are for suppressing ARP (IPv4) or Neighbor Solicitation (IPv6) between the clients within the SSID. An alternative solution would be to suppressing broadcast/multicasts via **Transmit only unicasts, suppress multicasts and broadcasts** in the logical WLAN network settings.



For unknown addresses

In case of an unknown address, the packet is either forwarded or discarded.

For broadcast ARP responses

In case of a broadcast, the packet is either forwarded or discarded.

Interface for property management systems

If you use a property management system (PMS), certain device types and series give you the option of connecting your Public Spot module with your PMS database via the PMS interface. If you operate a hotel, this offers you the possibility of automatically providing your guests with access to your Public Spot when they register. This access can optionally be free of charge or fee-based (using prepaid time credits), whereby all fees are charged to the guest's bill for their room. The last name, room number and, optionally, an additional security ID (for example, registration number or departure date) are used as login data.

In contrast to a voucher solution, using the PMS interface gives you the advantage of not requiring any additional administrative steps for the setup and management of a Public Spot user account. The device creates a user account by itself as soon as the user accesses the Public Spot and logs in with his registration data. Any future changes for this guest (room change, departure date change, check-out, etc.), which affect registration, are retrieved autonomously from your PMS.

The following login methods are currently supported:

1. Voucher
2. PMS login
3. PMS login and voucher
4. E-mail
5. SMS

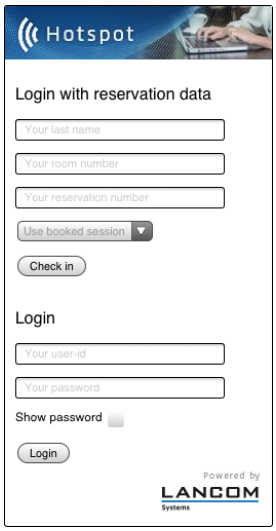
With login method (2), the login, for example, for hotel guests, can be based on the room number and last name, while you sell vouchers to your guests in your restaurant. Of course, even with the PMS interface enabled, you still have the option to issue vouchers, for example, for day guests or visitors.

The login method is configured globally for each device, and is thus the same for all SSIDs or networks.

The PMS interface currently only includes support for hotel property management systems from Micros Fidelio via TCP/IP.

Functional description

If you enable the PMS interface and provide a free or fee-based login page, the Public Spot portal page displays new input fields, which guests can use to authenticate by entering their surname, the room number and, if applicable, a further security identifier. The type of this identifier is set in the Setup menu; options include a registration number or the guest's arrival/departure date. If you have allowed access to your hotspot as a fee-based service, a drop-down menu additionally appears, which guests use to select the prepaid time quota or tariff/rate that they want to buy (e.g. 1 min for EUR 0.20, or 1 hours for EUR 1). The PMS working in the background automatically charges the costs to the room bill.



Every time a guest logs in to the Public Spot, the device initiates a comparison of the entered login data with that in the PMS. The PMS informs the device if it detects a valid match. The device then creates a new session for the guest and makes an entry in the corresponding accounting table (WEBconfig: **Status** > **PMS-Interface** > **Accounting**). The device records all hotel guests, and the corresponding prices, who have logged on via the PMS interface, irrespective of whether the connection is free or charged. The device then activates user access to the Internet.

A user with charged access can purchase additional time while logged on. Users who log off before the time quota expires can resume the session at a later time by selecting the corresponding field on the login page. The device stores the session until it becomes invalid, i.e. when the time quota is used up or when the PMS informs the device that the guest has departed. For a new login and synchronization with the PMS, the device recognizes that there is still a valid user account and continues using it instead of creating a new one.

If there is a change to the registration information (such as the room number), then an existing session initially remains unaffected. Only when the current session is closed an the guest logs on to the Public Spot again is it necessary to authenticate with the modified credentials. An exception occurs when a guest is checked-out of the PMS: In this case, the device immediately terminates an existing session.

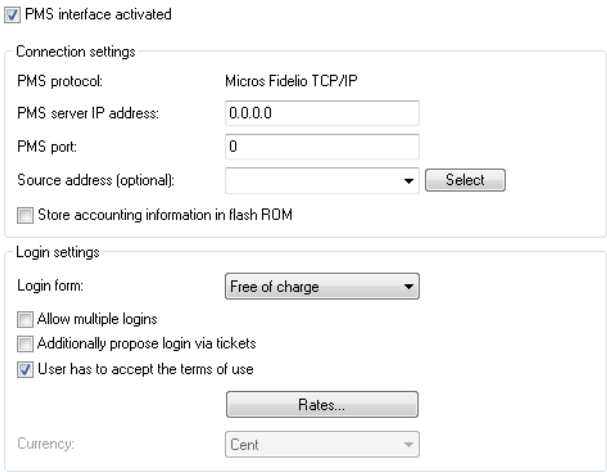
Your users should make sure that they log out properly from the Public Spot. Without a proper logout (caused by closing the browser, disconnecting the network, switching off the device, etc.) the user is considered to be still logged in. This can cause a problem for the user at login if you, as the Public Spot operator, have not allowed multiple logins.

Using *Station monitoring*, you can automatically log off these users after a specified idle time. This feature is off by default. However, for fee-based access, you absolutely should enable this. Otherwise, the device's automatic internal logout will only occur after the user account has expired, i.e., when the purchased time credit has been used up completely.

A temporary logout from the Public Spot does not change the expiry time of a purchased time quota. It is not possible to "pause" a previously purchased time credit in order to restart it at a later point in time. The countdown starts as of the purchase of the time credit regardless of the login status.

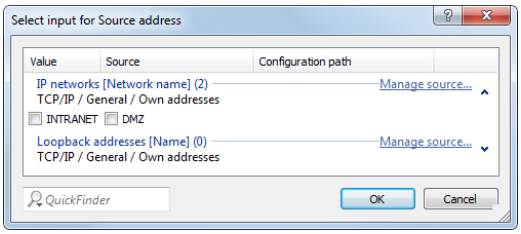
Configuring the PMS interface

Configure the PMS interface of your device in the menu **Public Spot** > **PMS-Interface**.



In this window you have the following options:

- **PMS interface activated**: Enable or disable the PMS interface for the device.
- **PMS protocol**: Identifies the protocol used by your property management system. Currently, the hotel property management systems from Micros Fidelio is supported only via TCP/IP.
- **PMS server IP address**: Enter the IPv4 address of your PMS server.
- **PMS port**: Enter the TCP port where your PMS server is accessible.
- **Source address**: Click on the **Select** button, in order to configure another address where your PMS server sends its reply messages. By default, the PMS server sends its replies back to the IP address of your device without having to enter it here.



Possible formats for entering the address include:

- Name of the IP network (ARF network), whose address should be used.
- `INT` for the address of the first Intranet
- `DMZ` for the address of the first DMZ

  If an interface with the name "DMZ" already exists, the device will select that address instead.

- `LB0`...`LBF` for one of the 16 loopback addresses or its name

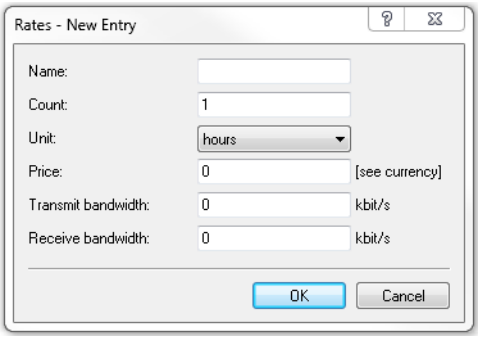
The device always uses **unmasked** loopback addresses, even on masked remote stations!

- Any IPv4 address

- **Store accounting information in flash ROM**: Enable or disable whether your device stores accounting information in regular intervals on the internal flash-ROM. By default this occurs hourly, but you can change the interval using the setup menu. Enable this option in order to prevent a complete loss of accounting information in case of a power outage.

Please note that frequent writing operations to this memory will reduce the lifetime of your device.

- **Login form**: Choose the login form that will be shown as a portal page for your PMS interface. Possible values are:
  - `free`: Choose this option if you offer your hotel guests free Internet access. Your hotel guests will still be required to authenticate on the hotspot on the portal page with their username, room number and, if required, an additional ID in order to prevent access to the Internet by unauthorized users.
  - `charge` Choose this option if you offer your hotel guests fee-based Internet access. Your hotel guests will be required to authenticate at the hotspot on the portal page with their username and room number, and also to select a rate.
- **Allow multiple logins**: Enable or disable this if you want to allow a hotel guest to use the same credentials to login to the hotspot with multiple devices.
- **Additionally propose login via tickets**: Enable or disable whether you also want to allow login with vouchers in addition to login with the combination of username/room number.
- **User has to accept the terms of use**: Enable this checkbox in order for hotel guests to accept the terms and conditions for the use of your hotspot.
- **Rates**: If you offer fee-based Internet access, this table is used to manage the tariff rates for the accounting.



  - **Name**: Specify a descriptive name for the rate here.
  - **Count**: Enter the rate for the time quota, for example, `1`. Combined with the unit, this is the value shown in the screenshot above, e.g., 1 hour.
  - **Unit**: Select the unit for the time quota from the list. Possible values are: `Minutes`, `Hours`, `Days`
  - **Price** Enter the amount charged for the time quota. In combination with the currency selected in the Login settings, the value amounts to 50 cents, for example.
  - **TX bandwidth**: Here you specify the maximum transmit bandwidth for this rate.
  - **RX bandwidth**: Here you specify the maximum receive bandwidth for this rate.

A temporary logout from the Public Spot does not change the expiry time of a purchased time quota. It is not possible to "pause" a previously purchased time credit in order to restart it at a later point in time. The countdown starts as of the purchase of the time credit regardless of the login status.

- **Currency**: If you offer fee-based Internet access, you set the currency used to bill your time quotas here (time quotas are set up using the Rates table). This unit is also displayed on the portal page. Please note that this currency must match the one on the PMS server. Possible values are:
  - `Cent`
  - `Penny`

Advanced settings

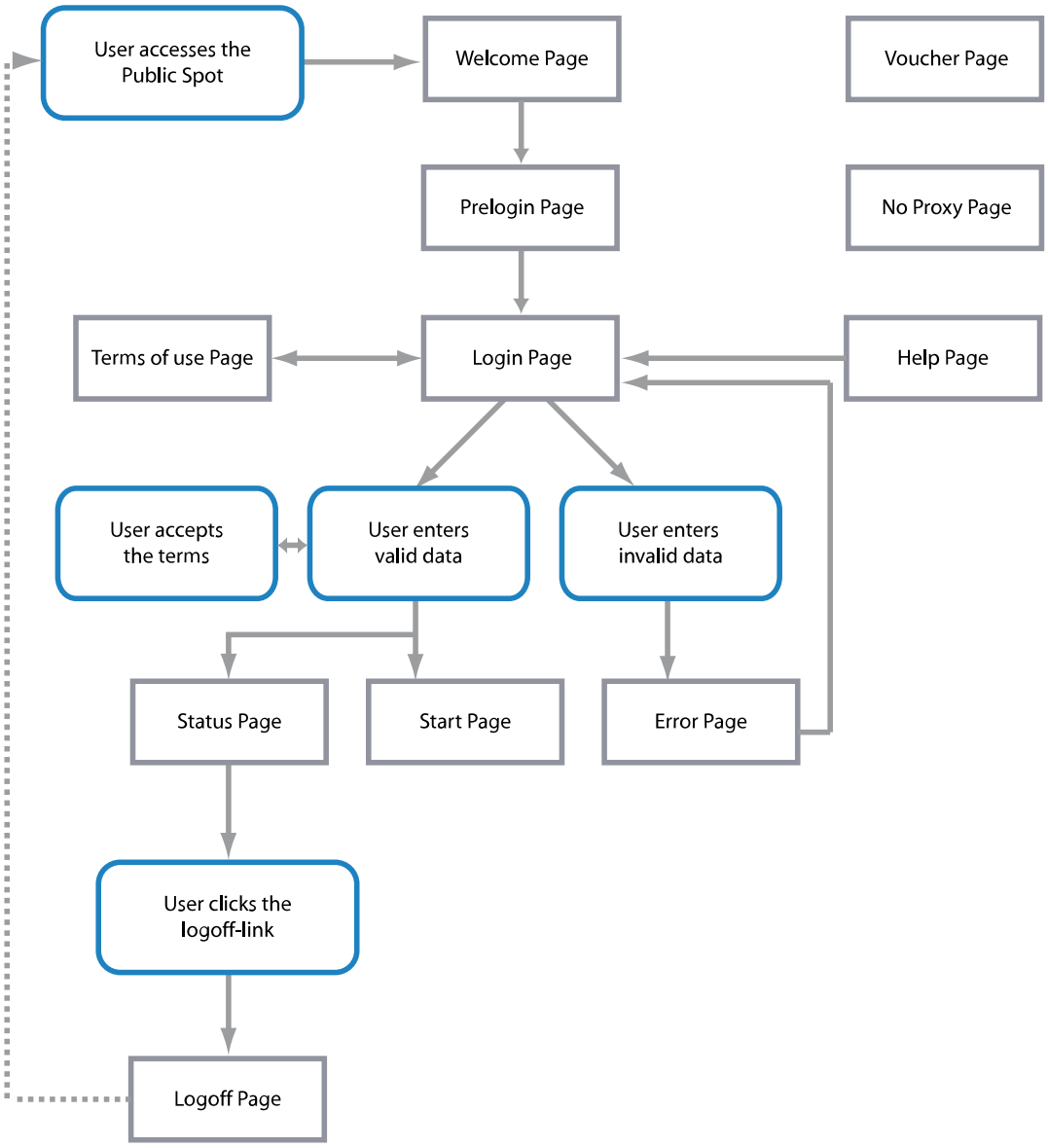
Advanced settings for the PMS interface are made on the console or in the setup menu. An overview of all additional parameters can be found in the *Appendix*.

1.2.5 Internal and customized voucher and authentication pages (templates)

By default, your device uses pre-installed templates for the login page and all other authentication pages that your user sees before, during and after a Public Spot session. However, you do have the option of adapting the individual web pages to your requirements and changing the design. You need basic HTML knowledge of DIV containers and cascading style sheets (CSS), in order to effectively change the structure and layout of the individual pages.

Possible authentication pages

The following flow-chart shows an overview and interaction of all authentication pages available with the Public Spot module: The chart takes the example of authentication using access credentials. Depending on the authentication mode and errors that can occur, the interaction may vary slightly:



The **Welcome** or **Login** pages are displayed to users when they access the Internet or the Public Spot for the first time.

- The **Welcome** page precedes the login page and is optional for most authentication modes: You can use this page, for example, to welcome a user, to provide information about the services available, or to provide instructions on how to use the Public Spot before continuing to the Start page with the login form. Only if you have selected the authentication mode "Login via agreement" is it compulsory for a customized Welcome page (containing the agreement) to be displayed, because it takes the place of the login form on the login page.

  The pre-installed default pages on your device do not include a Welcome page. If you set up this type of page without loading a template onto the device or an external server, the user either lands directly to the login page or receives an error message, depending on the login mode.

- **Authentication** includes the login form, assuming that Public Spot authentication requires the use of access credentials and that the latter have to be requested.

- The page with the **Terms of use** is only displayed if you require the confirmation of your terms of use for the selected authentication mode. In this case, a check box is displayed below the login form with an extra link that opens the terms in a pop-up.

The default pages installed on your device only include a placeholder and a generic Terms and Conditions page.

After the user has logged in with his login data (if necessary), the device checks that the information is correct and displays either an **Error** page, which sends the users back to the login page, or shows the **Start** page.

- Here, the **Error** page is only displayed to unauthenticated Public Spot users, which means that it is more or less directly associated with the login process. Typical situations in which a user sees the error page include unauthorized access to the Public Spot, when a user limit is exceeded, failed authentication due to the entry of incorrect credentials, or in case of failure of the authentication server. If you have set up monitoring of a remote site, the page could also appear whenever the Public Spot module registers a WAN link disconnection, as it provides advance notice to potential users about the lack of network availability (see *Error page in case of WAN connection failure* on page 59).

  Users who are already authenticated will see an appropriate error message from their browser.
- If there are no errors during login, the **Start** page verifies the successful login and after a few seconds redirects the user to the Internet page originally requested by user.

Additionally, a successful login is followed by a popup window with the **Status** page.

- The **Status** page shows the user the current information about his session (e.g., time used so far, sent/received data volumes, and validity period for his account). It also offers a link to close the session and stop the accounting. A user clicking on this link is redirected to the **Logout** page.
- The **Logout** page confirms to the user that the logout from the Public Spot was successful.

The remaining **Fallback error**, **Help** and **No-proxy** pages are isolated pages not related to the login process.

- The **Fallback error** page appears whenever the device cannot deliver a custom template page and the fallback to the LCOS internal default page is missing. Delivery can fail, for example, if you have specified an incorrect file path within the pages table, or if the template page does not exist on the device.
- The **No-proxy** page is displayed whenever a user tries to connect via HTTP on port 8080 instead of port 80. In intranets, port 8080 is typically used for HTTP proxies. Since this proxy is configured with a static IP address in the browser settings, but these cannot be configured via DHCP, the user would not be able to reach this proxy. The purpose of this page is just to instruct the user to disable the proxy before the user can proceed.
- The **Help** page is only a placeholder used to embed and display specific information (e.g., details about the login or where to get vouchers) on the remaining authentication pages (e.g. the Welcome page). The default pages contain neither a help page nor any link pointing to such a page. To use a help page, you must first create a custom template page.

The **Voucher** page is not one of the authentication pages: This is the graphic template for printing the vouchers. By uploading your own template, you can print tickets with the corporate design of your own company.

Pre-installed default pages

Ex-factory, your device comes pre-installed with all of the pages you need to setup an operational Public Spot.

The following table gives you a quick overview of the default pages included with LCOS:

Table 5: Overview of installed default pages

Page designation	Pre-installed?
Welcome…	No
Login...	Yes
Error...	Yes
Start…	Yes

Page designation	Pre-installed?
Status…	Yes
Logoff...	Yes
Help...	No
No proxy	No
Voucher…	Yes
Terms of use...	No
Fallback error	Yes
Login (e-mail)...	Yes
Prelogin (e-mail)...	Yes
Login (e-mail to SMS)...	Yes
Prelogin (e-mail to SMS)...	Yes

These pages were deliberately designed to be simple, not to use any fancy features like dynamic HTML or Java Script, and just to present the necessary elements as-is. The use of plain XHTML and CSS to produce the necessary elements only ensures that the pages appear correctly on a variety of browsers and screen sizes.

As the operator of a hotspot you may want to design more sophisticated pages or display a more neutral page without the manufacturer's logo. For that reason, the Public Spot module gives you the option to customize some of the default pages, or if necessary to replace them with your own design. The latter can be done either by using HTTP redirection or templates that you upload to the device and that the device processes like an intelligent HTML pre-processor. These template pages can be stored directly to the flash memory, so you can do without an external HTTP server.

Additional languages for the authentication pages

With LCOS8.84, the Public Spot module authentication pages (i.e. all pre-installed default pages except for the voucher page) support the languages French, Spanish, Italian and Dutch. This allows you to offer Public Spot access to a broader range of international users. The language displayed is determined by the settings in the Web browser used to access the Public Spot.

Multilingual support refers exclusively to the 8.84 internal default pages. You can implement multilingual customized template pages with an external server.

Customizing the standard pages

As an alternative to installing complete user-defined Web pages, the device provides the option of customizing the pre-installed default pages to a certain extent. This includes for example the input of a login text that is displayed to your users in the registration form, or replacing the header image (logo). In this way, you can quickly deploy a customized Public Spot without having to deal in-depth with the subject of the Web page authoring.

Customized text or login title for the login page

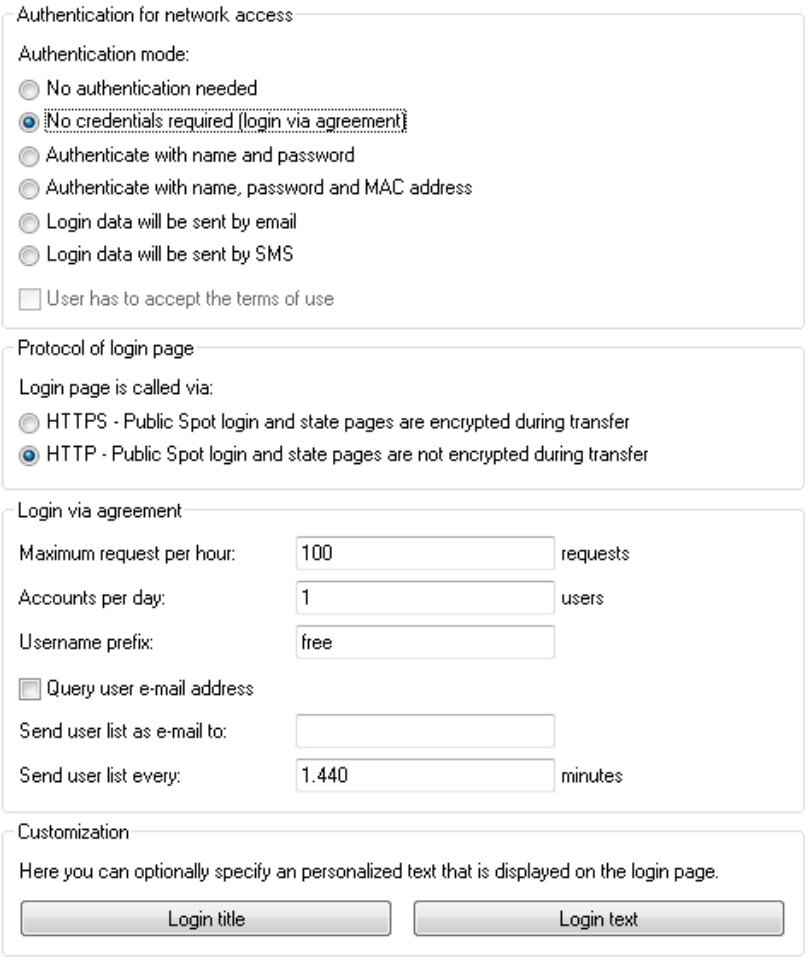
The Public Spot module gives you the option to specify customized **login text** and a **login title**, which appear on the login page in the box of the login form. The title and the text can be entered for a number of languages (English, German, French, Italian, Spanish and Dutch). The language displayed by the device depends on the language settings of the user's Web browser. If no customized login text or title is specified for a language, then the device falls back to the English login text (if available).

Please note that the login text and the login title are separate items.

Carry out the following steps to set up customized text or title on the login page.

1. In LANconfig, open the configuration dialog for the device.

2. Navigate to the dialog **Public Spot** > **Authentication**, click on the button **Login text** or **Login title** and select a language.



3. In the dialog that opens, enter the text that your Public Spot should display to users. You can enter an HTML string with max. 254 characters composed of:

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

LANconfig automatically transforms umlauts into their respective equivalents (`ü` to `ue`; `ß` to `ss`; etc.). To type umlauts, use their HTML equivalents (such as `ü` for `ü`), because the text is directly embedded in the Web page. You can also use HTML tags to structure and format the text. Example:

```
Welcome!<br/><i>Please complete this form.</i>)
```

4. Click **OK** to complete your entries and load the configuration back to the device.

Once the configuration has been written successfully, the new login text and login title appears the next time the Public Spot page is called.

Custom header images for variable screen widths

A component of the pre-installed pages in the device is a header image (logo), which is displayed to your users above the login form for the Public Spot. You can change this header image as you please, for example to reflect the application environment or your corporate design. There is no need for an external Web server; you can simply upload the image directly into the device via the file management in WEBconfig or the configuration management in LANconfig.

A special feature of the header image is that it is available in the device as two possible variants: One version is for large screens or browser windows with a horizontal resolution exceeding 800 px (normal monitors, laptops, tablet PCs, etc.), and one is a small picture for screens with a lower horizontal resolution (PDAs, mobile phones, etc.). This allows you to provide header images for different target groups and to provide them a login page that is appropriate for their device.

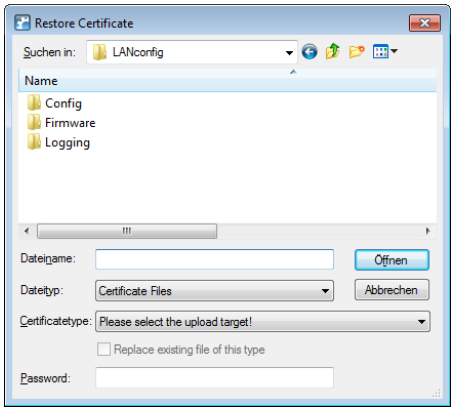
Figure 1: Login page for large screens

Figure 2: Login page for small screens

The available resolutions are set by the CSS file of the device. The pre-installed default graphics allow for 800x150 px for the large screen and 258x52 px for the small screen. The file type must be either JPG, GIF, or PNG.

To upload a new header image to the device either as a large or small version, follow the steps below.

1. Start LANconfig and highlight the device.
2. In the menu bar, click on **Device** > **Configuration management** > **Upload certificate or file**. The **Upload certificate** dialog opens.



3. Set the **File type** to **All files** and select the **Certificate type** that you want to upload.
   - **Public Spot - Header image of pages**: Certificate type for large screens
   - **Public Spot - Header image box**: Certificate type for small screens
4. Choose your custom header image and click on **Open**. LANconfig then starts the file upload.

After uploading successfully, the new header image appears the next time the Public Spot page is called.

You can check that the large and small header images are displayed by your Public Spot by setting your browser window width to >800 px and then reducing the width of the window. The CSS technology automatically switches between the large and small pictures.

Show/hide the vendor logo and header on the voucher

By default a voucher output by the device contains the header image and logo stored with the Public Spot homepage. The option **Public Spot** > **Wizard** > **Print header and company emblem** allows you to disable these graphics directly on the device without having to upload a customized version of the voucher template. In the case, the device outputs a neutral text voucher.

Configuration of user-defined pages

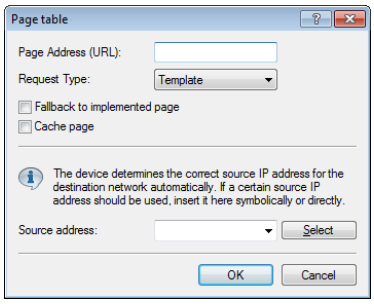
If you would like to replace the pre-installed pages with your own webpages, you can either store them directly on the device or on an external HTTP server. Sophisticated HTML pages may require more storage space than the space available on the device. There are additional advantages when using websites from an external server:

- Changes can be applied centrally. This reduces the effort required to change the login pages when using several devices.
- The server can dynamically provide the pages whose appearance is influenced by the information that the device provides. This information is discussed in more detail in the following chapters.

The storage location for the templates is entered in LANconfig in **Public Spot** > **Server** > **Page table** > **<Name of the template>** > **Page address (URL)**. There are currently three protocols available for the URL:

- `http://`...: Fetch the page via HTTP from an external server. TCP-port overrides and user/password specifications are possible.
- `https://`...: Similar to HTTP, but use HTTP over SSL for an encrypted connection.

> `file://`...: Retrieve the template from the given file in the device's local file system.



You can use any file name. If you decide to store the template pages in the device's local memory, they require the URLs reserved specially for this purpose. An internal standard page will be replaced by a new page loaded into the device by entering the local URL as the **Page address (URL)**.

Table 6: Overview of the reserved file names for template pages

Local URL on your device	Page designation
file://pbspot_template_welcome	Welcome…
file://pbspot_template_login	Login...
file://pbspot_template_error	Error...
file://pbspot_template_start	Start…
file://pbspot_template_status	Status…
file://pbspot_template_logoff	Logoff...
file://pbspot_template_help	Help...
file://pbspot_template_noproxy	No proxy
file://pbspot_template_voucher	Voucher…*
file://pbspot_template_agb	Terms of use...
file://pbspot_template_fallback	Fallback error
file://pbspot_template_reg_email	Prelogin (e-mail)...
file://pbspot_template_login_email	Login (e-mail)...
file://pbspot_template_reg_sms	Prelogin (e-mail to SMS)...
file://pbspot_template_login_sms	Login (e-mail to SMS)...

*) Template for printing vouchers, no authentication page

By uploading user-defined webpages, only the webpages that are pre-installed on the device are replaced, but not overwritten. They can be rolled back to the device's proprietary default pages at any time by deleting the local URL.

To provide the highest possible compatibility with earlier display devices and web browsers, you should avoid using frames, if possible. Also, specialized content such as JavaScript or plug-in elements can lead to an erroneous display.

Login pages depending on the login mode

The following table provides an overview of which login page is displayed by the device in the various authentication modes. If a login mode has no customized page template, the Public Spot module takes the default 8.84 page:

Table 7: Overview of login pages of each authentication mode

Authentication mode	Page designation
No authentication required	–
No credentials required (login after agreement)	Welcome…
Authenticate with name and password	Login...
Authenticate with name, password and MAC address	Login...
Login data will be sent by e-mail	> Prelogin (e-mail)... > Login (e-mail)...
Login data will be sent by SMS (text message)	> Prelogin (e-mail to SMS)... > Login (e-mail to SMS)...

Special template pages for Smart Ticket

The Public Spot module in LCOS versions prior to 8.84 used a central login page for all authentication modes. As of LCOS8.84, you can optionally equip the device with separate template pages for the Smart Ticket function (for self-sufficient user registration via e-mail/SMS). Two pages have to be configured for registration via e-mail/SMS: **Registration(...)** and **Login(...)**.

> On the registration page, users enter their personal data (e-mail address or mobile phone number) to register for the Public Spot and to request its login data.
> On the login page, users then enter their credentials in order to authenticate at the Public Spot.

The following table provides an overview of the related dependencies that you need to create your own page templates:

Table 8: Overview of dependencies of the SmartTicket login pages

Authentication mode	Page designation	Local URL on your device	Page template identifiers
Login data will be sent by e-mail	Prelogin (e-mail)...	file://pbspot_template_reg_email	<regemailform>
	Login (e-mail)...	file://pbspot_template_login_email	<loginemailform>
Login data will be sent by SMS (text message)	Prelogin (e-mail to SMS)...	file://pbspot_template_reg_sms	<regsmsform>
	Login (e-mail to SMS)...	file://pbspot_template_login_sms	<loginsmsform>

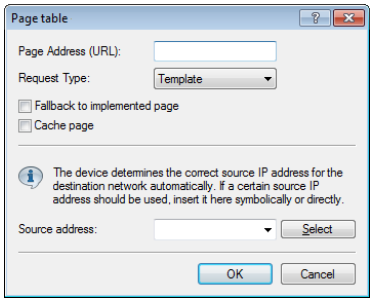
Setting up a customized template page

A custom template page allows you to replace the internal LCOS template pages with your own Web pages. This does not overwrite the LCOS templates, but just exchanges them for your own pages. If need be, you can fallback to the standard pages.

The steps below use the example of a **Login** page to show you how to set up a custom template page with the help of LANconfig.

1. You can load your customized error page either onto an external HTTP(S)-server or as the **Public Spot - Login page (* .html, * .htm)** into the memory of the device.
   Further information about uploading your own templates and sample files are available on the Internet in the *LANCOM Support Knowledgebase* under *Implementing your own websites for the LANCOM Public Spot option*.

2. Open the device configuration dialog in LANconfig, navigate to the **Public Spot** > **Server** dialog and select **Page table** > **Login**.



3. Enter the URL of the login page on the external server under **Page address (URL)** or the reference for a file on the local device (`file://pbspot_template_login`).

4. You can make these additional settings if necessary.
   - **Request type**: If you are using an external server, you can change the way in which the page is called. By default (in the setting **Template**) the device loads an externally stored HTM(L) page from the specified URL for further processing by the internal HTTP server. If you change the setting to **Redirect**, the device outsources the processing of the pages to the external server (also see *User-defined pages via HTTP redirect* on page 106).
   - **Fallback to implemented page**: If you use an external server and chose the template type **Request**, the Public Spot module is able to use the internal LCOS template in case of HTTP(S) errors (e.g. if the server is unavailable). This enables the Public Spot to continue operating (also see *Auto fallback* on page 107). If you do not activate this setting, the Public Spot displays the fallback error page instead.
   - **Cache page**: On some devices, you can write local and external templates to a cache. Learn more about under *Template caching* on page 105.
   - **Source address**: This setting allows you to specify the loopback address used by the device to connect to the external HTTP(S) server. By default, the server sends its replies back to the IP address of your device without having to enter it here. By entering an optional loopback address you change the source address and route used by the device to connect to the server. This can be useful, for example, when the server is available over different paths and it should use a specific path for its reply message.

5. Close this dialog and also the general configuration dialog each with click on **OK**. LANconfig then writes the new settings back to the device.

That's it!

Embedding graphics in user-created template pages

Images for your vouchers can now be uploaded into the device because a further five images slots (voucher image 1 to voucher image 5) are now available for your pages. These images are permanently stored in the flash memory of the device.

How to transfer the images into the device is described in the section *Custom header images for variable screen widths*. When uploading, set the **Certificate type** to "Public Spot - voucher image 1" to "Public Spot - voucher image 5".

Modify the HTML template of the relevant voucher (e.g. with a text editor such as Notepad++) and reference the uploaded images by including the following in the template: `<img src="/images/voucherimg1">` to `<img src="/images/voucherimg5">`. How to set up a custom template page is described in the section *Setting up a customized template page*.

Template caching

When configuring user-defined template pages on devices with sufficient memory (e.g., Public Spot gateways), you have the option to cache templates on the device. Caching improves the performance of the Public Spot module, particularly

in large-scale scenarios where the device internally caches templates and the HTML pages that were generated from them.

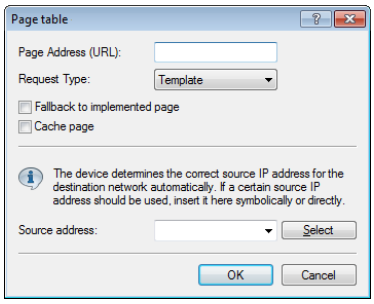
Caching is possible for:

- Templates stored in the local file system
- Templates stored on external HTTP(S) servers with static URLs

Templates on external servers that are referenced with template variables are not cached on the system.

Enable template caching

In LANconfig under **Public Spot** > **Server** > **Page table** > **<Name of the page template>**, caching for a page template is enabled by setting **Cache page**.



The corresponding parameter can be found under **Public Spot Module** > **Page table** > **Template cache**.

Delete template cache

The device automatically deletes or updates the templates stored in the cache once you load a new template file in the file system of your device (for local storage) or when the cache period for an HTTP(S) template runs out (for storage on an external server). The device evaluates the `Cache control` header of an HTTP(S) template in order to determine the maximum cache period.

If no `Cache control` header is set, the website is not cached and is immediately discarded. When setting up an individual template, ensure that you combine any META tag with a reasonable cache period (in seconds), for example, `<meta http-equiv="cache-control" content="max-age=60">`. The duration of the cache period depends on the scenario; there are no specific recommendations.

However, you do have the option of manually deleting the template cache with an action. In the status menu under **Public Spot** you can do this by starting the action **Flush template cache**.

User-defined pages via HTTP redirect

If you implement user-defined pages with redirection (request type: redirect), your device transforms it as follows: Whenever your device must send the respective page to a client, it will expand the URL according to the rules given in the previous chapter and will send an HTTP 307 (temporary redirect) response to the device, with this URL as the new location.

Redirects are particularly meaningful if you use a welcome page and all authentications should be performed on one external gateway. In this case, the clients can be immediately redirected to this gateway. This feature is often used with the external device controller.

User-defined pages via page templates

The device can alternatively act as a client and use the extended URL to download a user-defined page via an HTTP connection. The internal pre-processor takes of the processing of the page and subsequently sends the result to the Public Spot user. This pre-processor makes it possible to process session-specific data, although the server has a static

page available. The URL syntax understood by the device's built-in HTTP client is the syntax recognized by web browsers. However, only a subset of what is recognized by browsers is supported:

- The user authentication is performed using the form `user:password@host/...`
- The device is incapable of automatically resolving non-fatal HTTP errors such as redirects. Make sure that an access to this page will return the page directly.

Usage of symbolic names for the server's host instead of plain IP addresses is supported, given that DNS is properly configured. In many aspects, this mechanism can be considered like a proxy, which fetches HTML pages and then sends them to the client. The biggest difference is that the URL of the pages is determined by the device and not by the client of the Public Spot user.

Auto fallback

For every entry in the page table, it is possible to individually define whether a fallback should be used or not. This fallback feature is only meaningful if a page is defined as a template (request type: template), and not as a redirect (request type: redirect). While fetching a page via HTTP, various errors can appear:

- The DNS lookup for a host name may fail.
- The TCP/HTTP connection to the server may fail.
- The HTTP server may respond with an error code (e.g. 404 if an invalid URL was given).

By default, the device passes this type of error on to the user so that the user can start a new request or inform the provider of the Public Spot. Alternatively, the configuration of a fallback feature can ensure that the hotspot continues to function by using the default pages instead. You enable the fallback feature in LANconfig using the setting **Fallback to implemented page**.

Passed HTTP attributes

As mentioned above, in some respects the device may be seen as an HTTP proxy that fetches login and status pages for the client. HTTP proxies are obliged to keep certain HTTP attributes intact while forwarding a client request:

- The device forwards cookies between the client and the server. Client cookie values can also be sent transparently to the server and the server can set cookies on the client. Using cookies is necessary if the files that are sent from the server have ASP scripts, since ASP stores the session ID in a cookie.
- The device will forward the `User-Agent` value provided by the client. This allows a server to deliver different pages, based on the browser and system platform on the client side. PDAs and mobile phones for example call for web pages optimised for their small displays.
- The device inserts an `X-Forwarded-For` line into the HTTP request to report the device's IP address.
- WEBconfig generally attempts to use a tag named `Accept-Languages` provided by client browsers to match the request to one of the languages provided by its internal message tables (currently, only German and English). The selected language is communicated to the server via another `Accept-Languages` tag, in the hope that the server will provide a page in the appropriate language. When the server delivers the page, the device will check for a Language tag in the server's response to see if the server was actually capable of delivering a page in the requested language. If not, it will adapt the strings used in template expansion (see next section) to the actual language of the page.

URL placeholder (template variables)

The URLs specified in the page table do not need to be absolute strings. You have the option to integrate template variables in the address which are then filled-out with parameters from a Public Spot session when the device requests the pages from the server. Placeholders have a form similar to C format strings, e.g., a percent sign immediately followed by a single, lowercase character. The following placeholders are defined:

%a

Inserts the device's IP address. The placeholder only returns a value if the **Request type** in the **Page table** is set to `Template`.

Note that this placeholder cannot generate a reachable address if the device itself is located behind another router with activated NAT.

%c

Inserts the LAN MAC address of the Public Spot device as a 12-character hexadecimal string. The output is in the format 'aa:bb:cc:dd:ee:ff'.

%d

Enter the URL parameter '%d' as the circuit ID, for example `http://ipaddress/?circuit=%d&nas=%i`. The Public Spot module replaces this variable with the circuit ID that is detected in the client's DHCP request.

This requires "DHCP snooping" to be configured on the AP in such a way that the AP can query the circuit ID in the Public Spot station table of the WLC.

In this way it is possible for the Public Spot welcome page displayed on the clients to be customized by location.

%e

Inserts the device serial number.

%i

Inserts the NAS port ID. In this context, 'NAS' stands for 'Network Access Server'. This variable contains the interface of the device that the client used to login. For a WLC or router without WLAN this corresponds to a physical interface, such as `LAN-1`, or, for a standalone access point, it is the SSID.

%l

Inserts the device host name.

%m

Inserts the MAC address of the client as a 12-character hexadecimal string. The individual bytes are separated by colons.

%n

Inserts the name of the device the way it is configured in the setup menu under **Name**.

%o

Inserts the URL of the Internet page which the user initially requested. After successful authentication, the device forwards the user to this URL.

%p

Adds the IP address of the Public Spot device to the ARF context of the respective client.

Assuming that your device is active in various IP networks, you can use this variable to specify the IP address used by the device in the network where the client is also located.

%r

Adds the IP address of the client (from the perspective of the Public Spot device in the respective ARF context).

%s

If the client is connected to the device via a WLAN interface, this placeholder will insert the WLAN SSID used in the network that the client is connected to. This feature is particularly interesting when MultiSSID is used, since this gives the server the opportunity to display different pages based on the SSID. If the client is connected via another access point that connects to the device via a Point-2-Point connection, the SSID of the first WLAN will be inserted. If the client is connect via Ethernet, the placeholder remains empty.

%t

Inserts the routing tag which is appended to the client's data packets.

%v

If the requesting client is assigned an individual VLAN ID, this variable contains the source VLAN ID.

%0-9

Inserts a single number between 0 and 9.

%%

Inserts a single percent character.

In order to be able to use variables for a template, add the parameters to the **Page address (URL)** in the page table. In the following URLs the variable `%i` is replaced with `LAN-1` as described in the sample above:

Example: `http://192.168.1.1/welcome.php?nas=%i`

Example: `http://192.168.1.1/%i_welcome.html`

Tags and syntax of page templates

After the device receives the page from the server, it performs some transformations to the page template before sending it to the client. These transformations replace pre-defined HTML tag placeholders with data belonging to the client's current session (e.g. the current resource consumption in the status page). An HTML page delivered by the server could therefore better be described as a template for an actual HTML page displayed in the client's browser. HTML syntax was chosen for the placeholders to allow editing of page templates without interfering with syntax sensitive HTML editors.

In total, three placeholder tags are defined:

- `<pblink identifier>text</pblink>`

  Marks **text** as a clickable link to an **identifier**, typically to link to another page. Note that </pblink>is just an alias for , since this symmetrical definition causes less trouble with HTML syntax checkers. For example, the following fragment defines a link to the help page:

  ```
  Please click <pblink helplink>here</pblink>for help.
  ```

- `<pbelem identifier>`

  Insert the item specified by **identifier** at this place. For example, the following line inserts the user's time credit:

  ```
  Session will be ended in <pbelem sesstimeout>.
  ```

- `<pbcond identifier(s)>code</pbcond>`

  Only insert **code** into the page if all the identifiers are TRUE, i.e. numeric values are not equal to zero and string values are not empty. Note that the current implementation does not allow nested conditionals. Continuing from the previous example, the session timeout is only displayed if there is a time limit (a session without timeout internally has a session timeout of zero):

  ```
  <pbcond sesstimeout>Session will be terminated in <pbelem sesstimeout>seconds.</pbcond>
  ```

A set of sample page templates is available from LANCOM Systems. They are not meant to be used in productive systems, but instead to illustrate the use of page templates, and provide a starting point for your own creations.

Page template identifiers

The following identifiers can be used when designing customized template pages. The device does not differentiate between upper and lower case.

Please note that not all identifiers are available for all printouts! Not all identifiers are available on all pages.

ACCOUNTEND

Valid for: `<pbelem>`

This identifier supplements the voucher with information about the voucher's validity, i.e. from when and until when the created access account is valid.

APADDR

Valid for: `<pbelem>`

This identifier contains the Public Spot's IP address, as seen from the client's perspective. Can be used for user-defined login forms when the `LOGINFORM` element is not used.

AUTOPRINT

Valid for: `<pbelem>`

This identifier inserts a Java script into the page with the instruction to open the print dialog for printing the displayed page. Please note that in this case you **must** complete the `pbelem` tag with a separate `script`, e.g. `<pbelem autoprint></script>`.

BANDWIDTHPROFNAME

Valid for: `<pbelem>`

This identifier contains the bandwidth profile that the user is associated with.

This identifier is available from LCOS version 9.18 RU1. Templates featuring this identifier are not suitable for LCOS versions before 9.18 RU1.

COMMENT

Valid for: `<pbelem>`

This identifier adds an optional comment to the voucher, assuming that you have entered an appropriate text into the Setup Wizard.

HELPLINK

Valid for: `<pblink>`

This identifier contains the URL to the help page provided by the device.

LOGINEMAILFORM

Valid for: `<pbelem>`

For authentication via Smart Ticket, this identifier contains the HTML form for authenticating at the Public Spot with credentials provided by e-mail.

LOGINERRORMSG

Valid for: `<pbelem>`

This identifier returns the error message from LCOS in the case of a failed authentication or a WAN-connection failure. This identifier is only available on the general error page and the fallback error page.

To retrieve the error message from the RADIUS server in the event of a failed authentication, use the identifier **SERVERMSG**.

LOGINFORM

Valid for: `<pbelem>`

This identifier contains the HTML form for authentication at the Public Spot when authenticating with user name and password (and MAC address, if applicable).

LOGINLINK

Valid for: `<pblink>`

This identifier contains the URL to the login page provided by the device.

LOGINSMSFORM

Valid for: `<pbelem>`

For authentication via Smart Ticket, this identifier contains the HTML form for authenticating at the Public Spot with credentials provided by SMS.

LOGOFFLINK

Valid for: `<pblink>`

This identifier contains the URL to the logout page provided by the device.

ORIGLINK

Valid for: `<pbelem>` `<pblink>` `<pbcond>`

This identifier contains the URL originally requested by the user prior to the authentication process. If it is unknown, this value is empty.

PASSWORD

Valid for: `<pbelem>`

On a voucher, this identifier contains the password for Public Spot access.

REDIRURL

Valid for: `<pbelem>` `<pblink>` `<pbcond>`

This identifier holds a possible redirection URL contained in the RADIUS server's authentication response (if there was one). It is only defined for the error and start page.

REGEMAILFORM

Valid for: `<pbelem>`

For authentication via Smart Ticket, this identifier contains the HTML form for requesting the access credentials via e-mail (registration).

REGSMSFORM

Valid for: `<pbelem>`

For authentication via Smart Ticket, this identifier contains the HTML form for requesting the access credentials via SMS (registration).

RXBANDWIDTH

Valid for: `<pbelem>`

This identifier contains the maximum reception bandwidth of the bandwidth profile.

This identifier is available from LCOS version 9.18 RU1. Templates featuring this identifier are not suitable for LCOS versions before 9.18 RU1.

RXBYTES

Valid for: `<pbelem>`

This identifier contains the amount of data so far received by the device from the client in this session, expressed in bytes. It is zero for a station that is not logged in.

RXTXBYTES

Valid for: `<pbelem>`

This identifier contains the amount of data received by the device from the client so far, or sent to the client in this session, expressed in bytes. This means that it is the sum of TXBYTES and RXBYTES.

SERVERMSG

Valid for: `<pbelem>` `<pbcond>`

This identifier holds the reply message contained in the RADIUS server's authentication response (if there was one). Only applicable for the error and start pages. In the case of a failed authentication, this identifier contains the error message from the RADIUS server.

To retrieve the error message from the LCOS server in the event of a failed authentication, use the identifier **LOGINERRORMSG**.

SESSIONSTATUS

Valid for: `<pbelem>`

This identifier contains a textual representation of the current status of the client relative to the device (whether authenticated or not).

SESSIONTIME

Valid for: `<pbelem>`

This identifier contains the time that has passed since the login on the Public Spot.

SESSTIMEOUT

Valid for: `<pbelem>` `<pbcond>`

This identifier contains the remaining time for the current session. After this time, the device ends the current session automatically. This identifier is zero for a session with no time limit.

SSID

Valid for: `<pbelem>` `<pbcond>`

This identifier on a voucher contains the SSID to be used for Public Spot access.

STATUSLINK

Valid for: `<pbelem>` `<pblink>`

This identifier contains the URL to the logout page provided by the device. A reference that opens a new browser window is automatically generated within the `<pblink>` element.

TXBANDWIDTH

Valid for: `<pbelem>`

This identifier contains the maximum transmission bandwidth of the bandwidth profile.

This identifier is available from LCOS version 9.18 RU1. Templates featuring this identifier are not suitable for LCOS versions before 9.18 RU1.

TXBYTES

Valid for: `<pbelem>`

This identifier contains the amount of data transmitted by the device to the client so far in this session.

USER NAME

Valid for: `<pbcond>`

This identifier allows you to supplement the voucher page with conditional HTML code, which is only printed for certain users or administrators. `USER` is a prefix and **must** be placed before the user name (`NAME`) and a space. To generate HTML output specifically for the user 'root' when calling the voucher page, use the following syntax:

```
<pbcond USER root>Conditional HTML Code</pbcond>
```

When used in larger Public Spot scenarios with central administration, such as with a WLAN controller, this dependency can be used for the purpose of site localization: To do this, you create a Public Spot admin for each of the relevant access points and you specify a conditional voucher text for each administrator.

USERID

Valid for: `<pbelem>`

This identifier contains the user ID (in the form of the username) with which the current session was started. The identifier is not specified if the client is not (yet) logged in.

VOLLIMIT

Valid for: `<pbelem>` `<pbcond>`

This identifier contains the amount of data, expressed in bytes, that the client is still allowed to transfer before the device terminates the current session. This identifier is zero for a session with no data limit.

VOUCHERIMG

Valid for: `<pbelem>`

This identifier inserts the page banner image (in large size) into the page.

New placeholders from LCOS version 9.20:

These placeholders enable the page templates to be fine tuned. Unlike the placeholders mentioned above, these placeholders do not output any additional descriptive text, but their values only.

${SSID}

Returns the network name / SSID.

${USERID}

Returns the user name.

${PASSWORD}

Returns the user password.

${COMMENT}

Returns the comment.

${BandwidthProfName}

Returns the name of the bandwidth profile.

${TxBandwidth}

Returns the specified maximum bandwidth (transmit direction).

${RxBandwidth}

Returns the specified maximum bandwidth (receive direction).

${ACCOUNTEND}

This identifier returns the end of the ticket (date and time).

To use this placeholder, you need to include the jquery library in the template. To do this, add the following to the template:

```
<script src="/jquery/jquery.js" type="text/javascript"></script>
```

```
<script src="/jquery/jquery.tmpl.min.js" type="text/javascript"></script>
```

You also need to use the new placeholders inside a <script> block:

```
<script id="voucherTemplate" type="text/x-jquery-tmpl">

[... Contents ...]

</script>
```

Graphics in user-defined pages

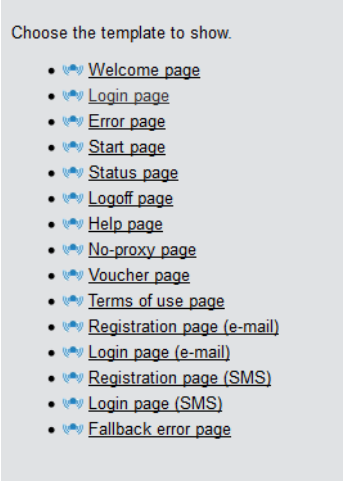
All but the simplest web pages contain images, which are fetched by the client's browser independent of the HTML page itself. The graphic files for the pre-installed page are also stored on the device. The device automatically adapts the necessary permissions so that even unauthorized clients have access to the images without problems. However, every access to the referenced (device-external) images for user-defined pages are treated like a normal Internet access, and would automatically send the user back to the welcome or start page.

In order to avoid this behavior, you should make sure that the servers where the graphics are stored are included in the **free servers**. Free servers are addresses that have unlimited access, and are therefore also accessible by unauthenticated clients, and are not billed by the accounting feature in the same way as the rest of the data traffic.

The chapter *Open access networks (no login)* on page 42 contains additional information about configuring free servers. Note that if a user-defined page is defined as a redirect, this of course has to be defined as a free IP address.

Template preview in WEBconfig

You can view the changes to the Public Spot templates in WEBconfig by switching to the view **Extras** > **Public Spot template preview**.

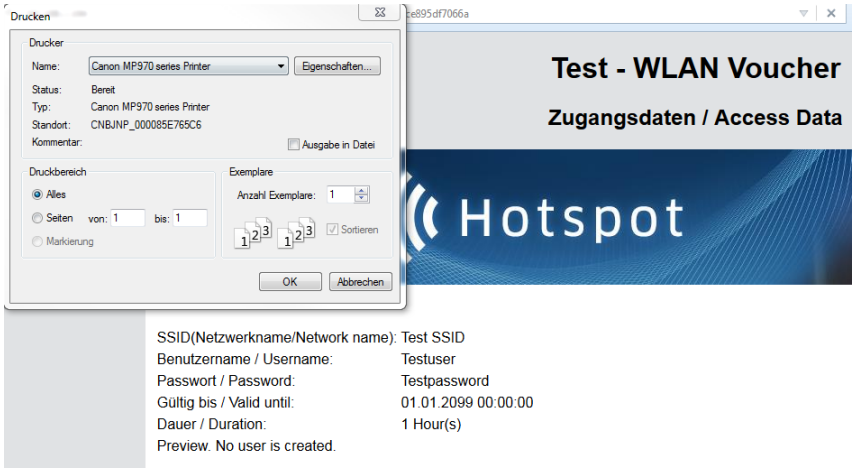


Select a template to display from the list.

The selected template is displayed in the same browser window. Use the "Back" function of your browser to return to WEBconfig.

Some templates contain JavaScript code. This code is executed when the template is invoked. For example, the "Voucher page" template contains code that starts a printout when the page is displayed.

This page contains test data. However, no user is created at this point. This allows you to test the template and print it out.



If a template does not exist or cannot be found, an error message is displayed by WEBconfig.

Public Spot Captive Portal API

The Public Spot supports the new Captive Portal API standard according to *RFC 8908*. The standard allows Wi-Fi clients in a hotspot to automatically find a captive portal or login page.

The client receives the URL of the portal page via DHCP and uses an API request to the hotspot to check whether a login is required or whether access is already permitted for the client. This significantly speeds up the user experience in a hotspot and, by defining a standard, now provides better manufacturer interoperability between hotspots and clients.

The following steps are required:

1. The use of TLS certificates in the Public Spot is mandatory. Without an HTTPS login, the client does not send a request to the portal.
2. The DHCP server must provide the Captive Portal DHCP option to the client.

The configuration in LANconfig is located under **Public-Spot** > **Server** > **Captive Portal API (RFC 8908)**.

Captive portal API enabled

Enables or disables the Captive Portal API function in the Public Spot.

User portal URL

(Optional) By default, the Captive Portal API supports TLS only. For this reason the device must have a trusted certificate and a DNS name. By default, the parameter can be left empty and it will be inserted automatically by the system. To do this, the device name must be configured in the Public Spot operating settings and agree with the TLS certificate. If an external hotspot server is used, a URL of this server can be entered here. Another requirement is that the clients in the hotspot must find the captive portal via DHCP option. For this purpose, the corresponding DHCP option according to *RFC 8910* must be configured for the hotspot network.

Venue URL

(Optional) URL (TLS) through which the operator can provide the user with additional information about the location of the hotspot, e.g. the website of the hotel with the hotspot.

Configure DHCPv4 option (according to RFC 8910)

In LANconfig, create a new table entry under **IPv4** > **DHCPv4** > **DHCP options**.

Option number

Number of the option that should be sent to the DHCP client. In this case 114.

Network name

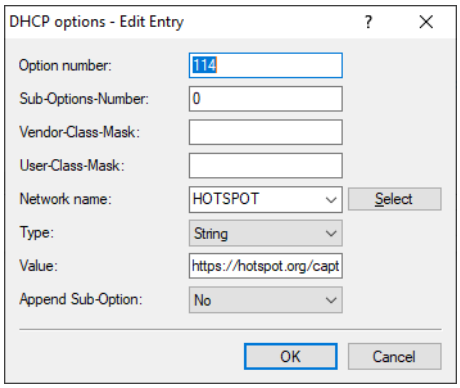
Name of the Public Spot network (see IPv4 networks)

Type

Entry type. In this case String.

Value

HTTPs URL of LANCOM router in the hotspot, e.g. “https://hotspot.org/captive-portal-api”. The DNS name, e.g. “hotspot.org”, is the device name of the router in the TLS certificate supplemented by the internal path of the Public Spot login page “captive-portal-api”. The hotspot client must be able to resolve the DNS name. Also, the device name must be configured in the Public Spot operating settings and agree with the TLS certificate.



Configure DHCPv6 option (according to RFC8910)

In LANconfig, create a new table entry under **IPv6** > **DHCPv6** > **DHCPv6 server** > **Additional options**.

Interface name/Relay IP

Name of the Public Spot network (see IPv6 networks)

Option code

103

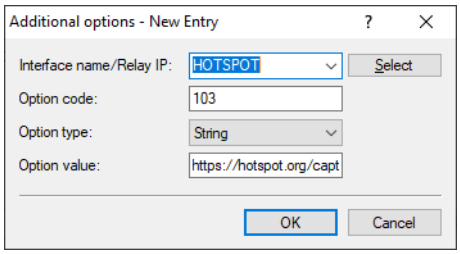
Option type

String

Option value

HTTPs URL of LANCOM router in the hotspot, e.g. “https://hotspot.org/captive-portal-api”. The DNS name, e.g. “hotspot.org”, is the device name of the router in the TLS certificate supplemented by the internal path of the Public Spot login page “captive-portal-api”. The hotspot client must be able to resolve the DNS name.

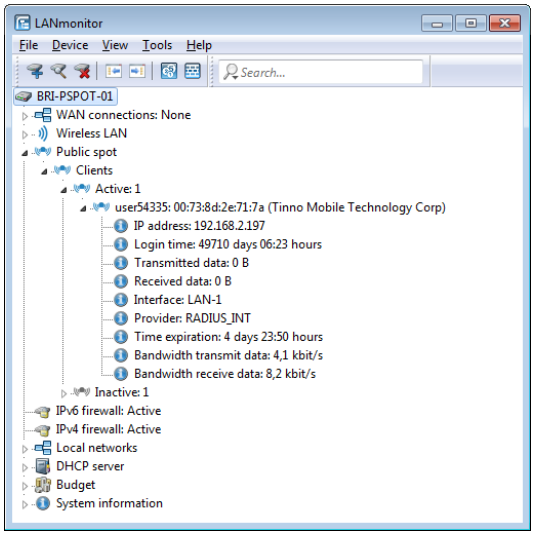
Also, the device name must be configured in the Public Spot operating settings and agree with the TLS certificate.



1.2.6 Viewing Public Spot clients

LANmonitor can optionally display detailed information about the clients associated with the Public Spot.

1. Open the menu item **Public Spot** > **Clients**.
2. Double-click on **Active** to display the active clients, or on **Inactive** to display inactive clients.
3. Double-click on a client to retrieve detailed information about it.



1.2.7 Displaying advertising to Public Spot users

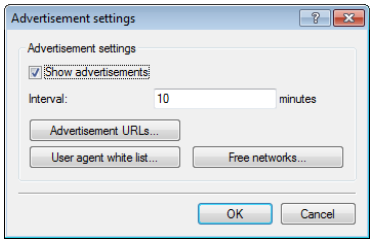
You can optionally display advertising to Public Spot users at configurable time intervals. The Public Spot shows the advertisement in the normal browser window of the user and not using a pop-up, since all modern browsers normally block pop-ups. In the Public Spot station table, a client can have one of three states:

- Authenticated: The client is logged on and can surf in Internet.
- Unauthenticated: The client is not logged on and cannot surf in Internet.
- Advertisement: The next time a client calls a URL, it is redirected to an advertisement URL.

You have the option to exclude certain networks and user agents from the display of advertisements by means of a whitelist.

1. In the device configuration, select the menu branch **Public Spot** > **Server** and click on **Advertisement settings**.

2. Enable the **Show advertisements** checkbox.



You can now change the interval between advertisement displays, and also other settings.

3. Under **Interval** you specify the time in minutes after which the Public Spot reroutes a user to an advertisement URL. With an interval of `0` forwarding occurs directly after login.
4. Click on **Advertisement URLs** to add an advertisement URL. If you add multiple URLs, the Public Spot displays them in sequence after the specified interval.
5. Optional: Click on **User agent white list** to add user agents, which the Public Spot excludes from the display of advertisements.
6. Optional: Click on **Free networks** to add networks, which the Public Spot excludes from the display of advertisements. This can be used in various ways, for example to enter the automatic search URLs used by the browser, e.g. `*.google.com`. Typically, a browser sends keyboard input at the address bar to a search engine; by setting the exception, the advertisement page does not responding to this.

   Login-free networks are generally ad-free networks. There is no need to explicitly include these networks into the whitelist.
7. Close all dialog windows by clicking on **OK**.

Public Spot users will be redirected to an advertisement URL after the specified time interval unless they are using a whitelisted user agent or they are located in a free network.

The timing of the advertisements refers to the session time of the active Public Spot clients. If a client stop sending data for a certain time, then the interval before the Public Spot displays advertising again will be delayed by this time.

1.3 Access to the Public Spot

1.3.1 Requirements for logging in

- Device with network adapter
- Operating systems supporting the TCP/IP protocol (automatic IP-address retrieval by DHCP active)
- Web browser (supporting JavaScript and Frames)
- Direct Internet access (use of proxy deactivated)
- WLAN access information (network name, encryption information)
- Valid user data (user identifier and password)

Information for WLAN access

A maximum of two pieces of information are required to access the WLAN:

- **The network name of the WLAN (SSID)**

  If the Public Spot's base stations are configured for operation as a closed network, the user must know the exact name of the wireless LAN, its SSID.
- **WLAN encryption**

Although it is possible to provide guest access via encrypted connections using, for example, WPA, Public Spots are not generally operated with WLAN encryption. Protection is provided in this case using authentication with a username and password. Data security when transmitting data on the Public Spot must be provided by the end user (e.g., using a VPN client).

Information for LAN access

If the IP addresses on your network are automatically assigned (for example, via DHCP), your users only need:

- a LAN socket that connects to the Public Spot.
- a LAN cable to connect their LAN adapter to the LAN socket.

Information for authentication

The user needs to have the following information to hand when logging in:

- User identifier
- Password
- MAC address

If you set the authentication mode for a Public Spot at the base station to "MAC+User+Password", you, as the operator, must know the MAC addresses of the end devices employed by your users. An end device automatically and continuously transmits its MAC address when communicating with a base station. The user does not have to manually enter this information when logging in, but instead it is communicated just once to the operator before attempting to login.

1.3.2 Logging in to the Public Spot

1. Log in to the WLAN of the Public Spot (for WLAN connections) or connect to the network using an Ethernet cable (for LAN connections).
   The different types of mobile devices and WLAN adapters offer various ways of entering the settings required for accessing the WLAN. Many devices require the network name (SSID) of the WLAN to be entered into the configuration program for the WLAN adapter. Some other products also provide an overview of all base stations in the vicinity, from which the user simply chooses the one they want to use.

   Depending on the configuration, the user receives the necessary settings for the LAN-adapter connection either automatically from the network or a connected DHCP server, or from the network administrator.

2. Start your Web browser.

   As soon as the Web browser attempts to access any Internet site, the Public Spot automatically intervenes and presents the login page. The login page, or the login form displayed within it, appear differently depending on which

firmware version you are using and which login mode you have selected. In the following, we assume a login with a voucher (or by user name and password).

Figure 3: Login page for large screens

3. Enter the complete **user ID** and **password** in the corresponding fields and confirm your entries with **Login**.

To login, you should use a Web browser with JavaScript support enabled to ensure that session status information can be displayed in a popup window.

If the login to the Public Spot is successful, an additional window pops up with the main information about the current session. This window is also used for the login. This window should be left open throughout the session (e.g., it can be minimized).

If the login fails, an error page opens with a request to return to the login page and to repeat the authentication. The form takes over a portion of the previously entered data as an aid to the user, e.g. in case of typos.

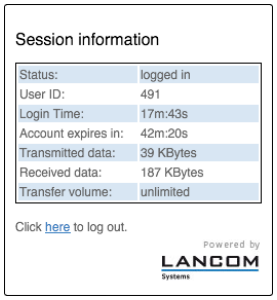
1.3.3 Session information

The window with session information is automatically updated at regular intervals. Along with the status and current user ID, the information displayed includes the connection time and the volume of transferred data.

If the session-information window is not open, you can open it by entering the following in the address line in the browser:

```
http://<IP address of the Public Spot>/authen/status
```

Alternatively, you can open the session page with the short URL `http://logout`.



1.3.4 Logging out of the Public Spot

The session information window can be used to logout from the Public Spot. Click on **here** in the bottom line of text in the window.

If the session-information window is not open, you can enter the following into the address line in the browser:

```
http://<IP address of the Public Spot>/authen/logout
```

Alternatively, you can open the session page with the short URL `http://logout` to logout from the Public Spot.

The operator can set up the Public Spot to automatically logoff users if they cannot be reached for 60 seconds. In case of doubt, please ask the Public Spot operator if automatic logoff (*Station monitoring*) is activated.

1.3.5 Advice and help

The following sections present solutions to the most common problems that may occur when operating a Public Spot.

The Public Spot login page is not displayed

- The Internet access must be set up so that it is directed via the network adapter and not via a dial-up networking connection. To check this, take a look at the connection settings for your Web browser. If you use Microsoft Internet Explorer, you must disable the dial-up configurations in **Tools** > **Internet Options** > **Connections**entered there.
- Internet access must be direct, i.e. without going via a proxy server. In Microsoft Internet Explorer, you can disable the use of a proxy server in the menu **Tools** > **Internet Options** > **Connections** > **LAN-Settings...**.
- If you are making the connection with a WLAN adapter: Ensure that your network adapter can in fact find the Public Spot. Your WLAN adapter gives you the option of searching for an access point.
- If you are making the connection with a WLAN adapter: Check if your network adapter has all of the necessary settings to access the Public Spot network:
  - You probably have to enter the network name for the WLAN.
  - When working with an encrypted Public Spots, you are also required to enter the corresponding WPA or WEP key.
- Check that your network adapter is set up for automatic retrieval of an IP address (DHCP). Your device should not have a fixed IP address.

If your network adapter is set up with a fixed IP address, adjusting it for automatic retrieval by DHCP may cause important configuration information to be lost. Ensure that you note all of the values listed in the network settings (IP address, standard gateway, DNS server, etc.).

Login not working

- Ensure that you enter the user data correctly and in full. Ensure that you use the correct capitalization for all entries.
- Is the CAPS-LOCK key activated on your device? This causes the capitalization to be reversed. Deactivate the CAPS-LOCK key and repeat the entry of your login data.
- The Public Spot operator may be checking more than just the user ID and password, but also the MAC address (physical address) of your network adapter as well. In this case, ensure that the Public Spot operator is informed of your correct MAC address.

It is no longer possible to login

If the Public Spot breaks off communications after a number of login attempts have failed, you should deactivate your WLAN adapter for at least 60 seconds (or your entire device) or disconnect the LAN adapter from the network, and then try again.

The session information window is not being displayed

To display the session-information window, enter the following line into the address line of your Web browser:

```
http://<IP address of the Public Spot>/authen/status
```

The Public Spot operator can supply you with the `<Public Spot's IP address>` upon request.

The Public Spot requests a new login for no reason (WLAN)

When moving into the signal coverage area of another access point (roaming), it is necessary to login again. If you are located in the overlap area between two access points, you may even experience a change of connection between the two access points at regular intervals. The task of the roaming secret is to allow Public Spot sessions to be passed between access points without the user having to login again.

- LANconfig: **Public Spot** > **Users** > **Roaming Secret**

1.4 Tutorials for setting up and using Public Spots

The following tutorials describe examples of how the Public Spot option can be implemented.

1.4.1 Virtualization and guest access via WLAN controller with VLAN

Many companies wish to offer Internet access to their visitors via WLAN. In larger installations the required settings apply to multiple access points, and these can be programmed centrally in the WLAN controller.

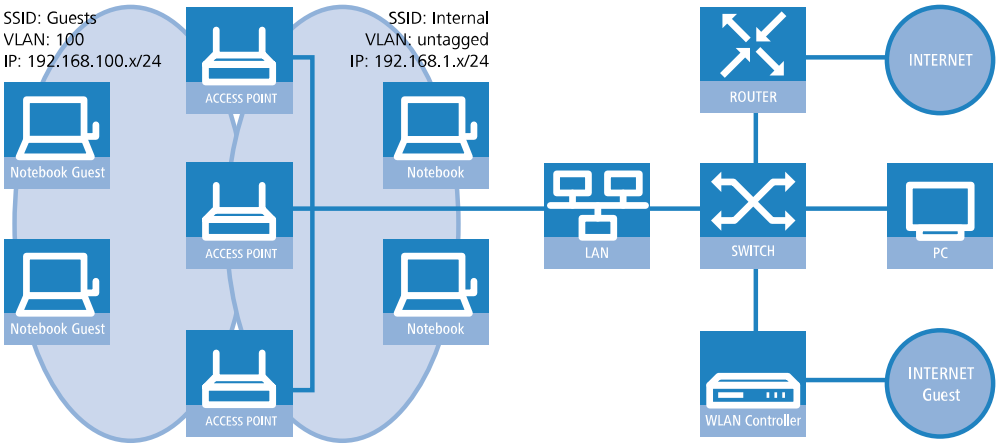
Targets

- Wireless LAN infrastructure available to internal employees and guests
- Shared physical components (cables, switches, access points)
- Separation of networks with VLAN and ARF
- Break-out of data streams to certain target networks:
  - Guests: Internet only
  - Internal employees: Internet, all local devices and services
- Guests login to the WLAN with a Web form.
- Internal employees use WLAN encryption for authentication.

Establish

- Management of the access points is handled by the WLC.
- The WLC serves as the DHCP server for the WLAN clients in the guest network.
- The guest network is provided with Internet access via the WLC (e.g. separate DSL access or Internet access via the company DMZ).
- The wired infrastructure is based on managed VLAN-capable switches:
  - Access point VLAN management is handled by the WLC.
  - The VLAN management of the switches is handled separately by the switch configuration.

> The access points operate within the internal VLANs.

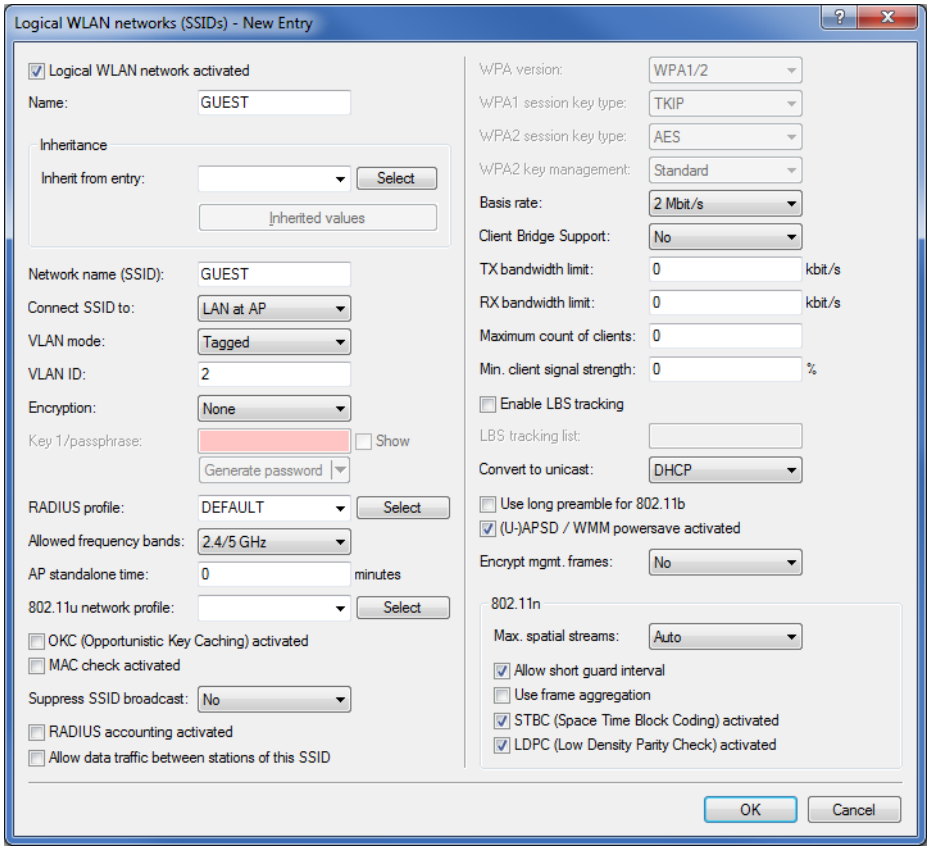


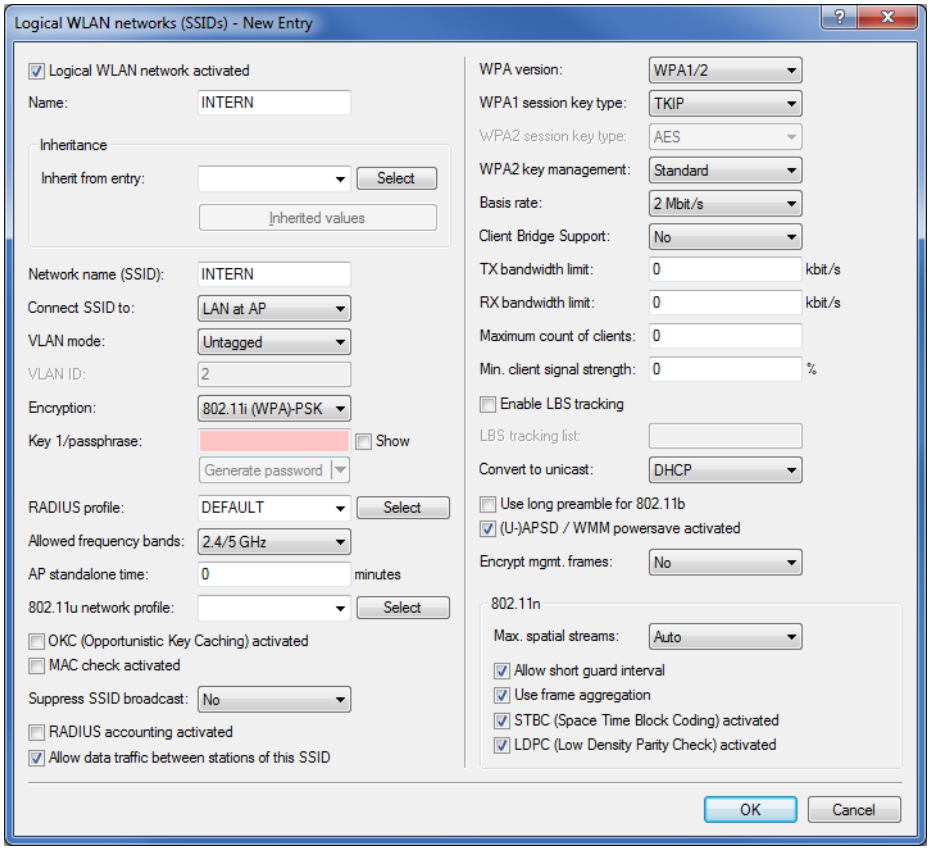
Wireless LAN configuration of the WLAN controllers

During the configuration of the WLAN, the necessary WLAN networks are defined and, along with the physical WLAN settings, are assigned to the access points managed by the controller.

1. Create a logical WLAN for guests and one for the internal employees:
   - The WLAN with the SSID `GUESTS` uses the VLAN ID `100` (VLAN operating mode **Tagged**) and uses **no** encryption.
   - The WLAN with the SSID `INTERNAL` receives no VLAN ID (VLAN operating mode **untagged**, i.e. packets are transferred in the Ethernet without a VLAN tag) and uses WPA encryption, e.g. **802 11i (WPA)-PSK**.

› LANconfig: **WLAN Controller** > **Profiles** > **Logical WLAN networks (SSIDs)**

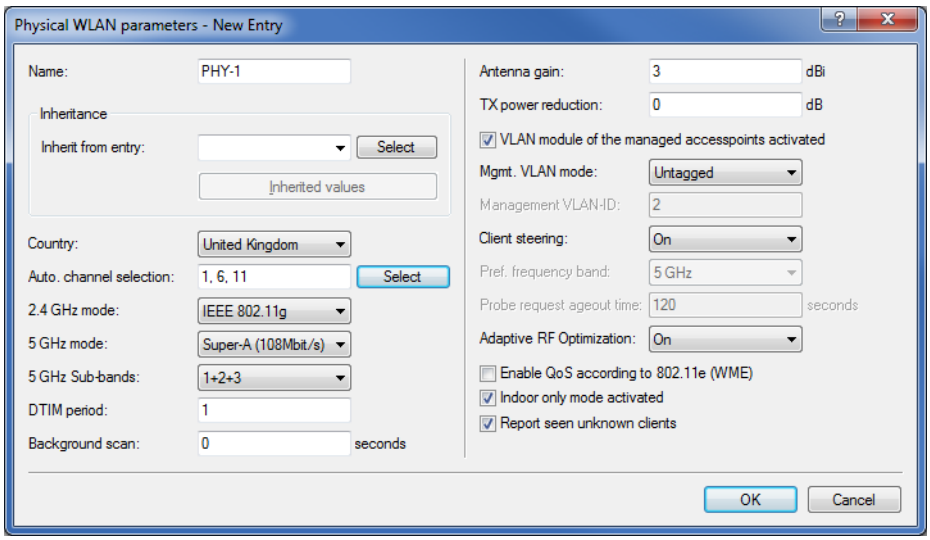




If you set the **VLAN mode** to **untagged**, LANconfig will gray-out the **VLAN ID** input field in the add/edit dialog shown above. However, the corresponding table **Logical WLAN networks (SSIDs)** still displays the assigned VLAN as a value in the grayed-out box. This entry is only of internal significance, as the acceptable range is between 2 and 4094. Ultimately it is the VLAN operating mode which is decisive: If this is set to **untagged**, then a VLAN ID is not transmitted under any circumstances.

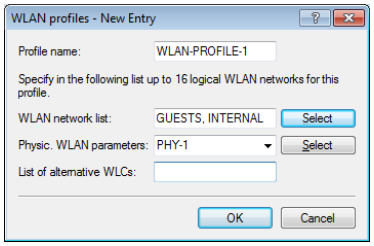
2. Create a set of physical parameters for the access points.
The management VLAN ID is set to `1`, which serves to activate the VLAN function (but without a separate management VLAN for the device; the management data traffic is transmitted untagged).

   › LANconfig: **WLAN-Controller** > **Profiles** > **Physical WLAN parameters**



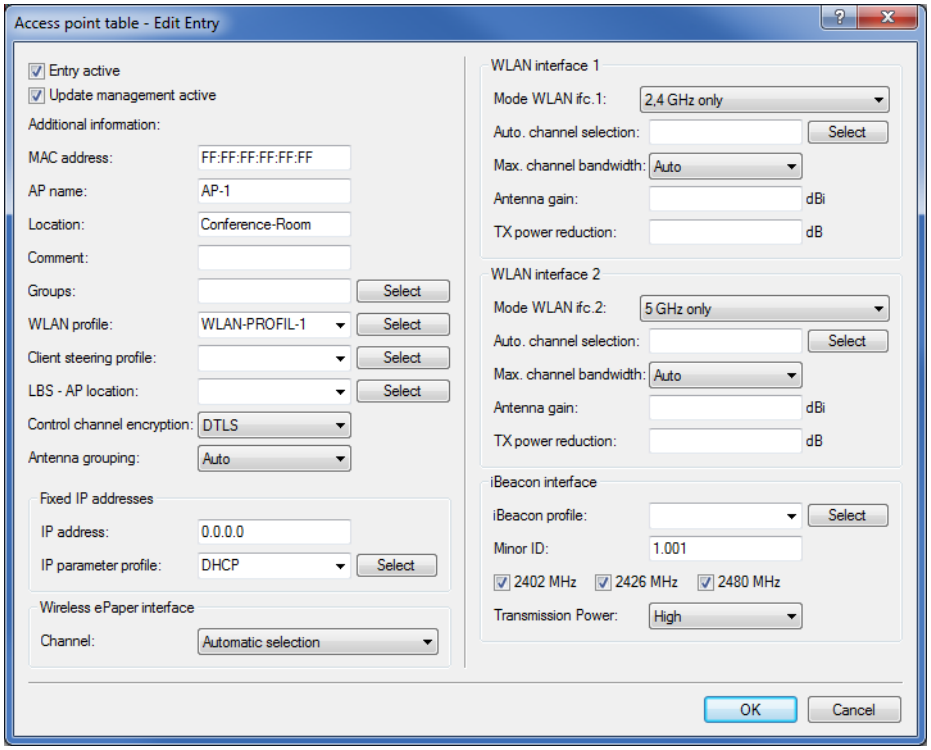
3. Create a WLAN profile that you can assign to the access points.
   The two logical WLAN networks and the set of physical parameters defined earlier are collected into this WLAN profile.

   › LANconfig: **WLAN-Controller** > **Profiles** > **WLAN-Profiles**



4. Assign this WLAN profile to the access points managed by the controller.
   Do this by entering each access point with its MAC address into the access point table. Alternatively you can use the **Default** button to create a default profile, which applies to all access points.

   › LANconfig: **WLAN controller** > **AP configuration** > **Access point table**



Configuring the switch (LANCOM GS-2326P)

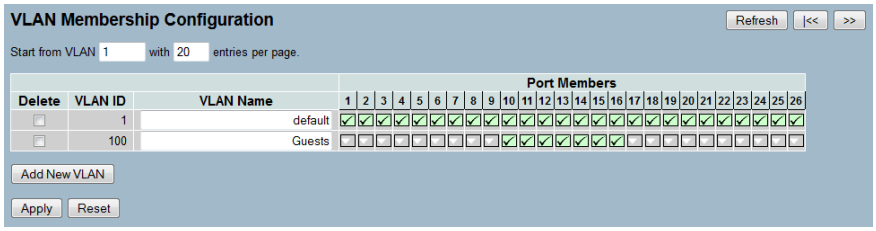
In this section we describe the configuration of the switch using the LANCOM GS-2326P as an example.

1. Under **Configuration** > **VLAN** > **VLAN-Membership**, create an additional VLAN group for the guest network.

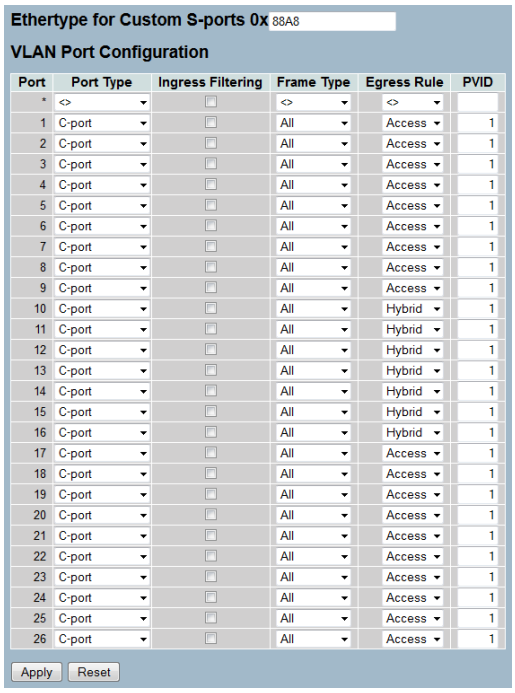
   To differentiate between the VLANs in the switch, two groups are used. The internal network for the employees is mapped to the group `default`, and that for the guests is mapped to the group `guests`.

   › The VLAN group for the internal employees uses the default VLAN ID `1`. This VLAN ID used for internal administration applies on all ports and is operated untagged, i.e. all untagged incoming data packets are given the VLAN ID 1 for internal routing, and this is removed again from outgoing data packets (see also "PVID" in the next step).

> The VLAN group for the guests uses the VLAN ID `100`, which you entered earlier when configuring the WLAN in the controller. This ID applies only to the ports which the WLAN controller and the access points are connected to (in this example: Port 10 to 16, green checkmarks for **Port members**). The switch does not remove tags from outgoing data packets. i.e. all tagged incoming packets with VLAN ID 100 retain this tag and are routed only to the ports that are members of the corresponding group.



2. Under **Configuration** > **VLAN** > **Ports** set the **Port Type** for all ports to **C-port**. See the documentation about your switch for details about this setting.
3. Configure the **Egress rule** for each port.
   > All ports except port 10 to 16 are given the **Access** rule. As a result, these ports forward only tagged packets and all others are dropped.
   > The ports 10 to 16 are given the rule **Hybrid**. As a result, these ports forward both untagged and tagged packets.



Port	Port Type	Ingress Filtering	Frame Type	Egress Rule	PVID
*	<>		<>	<>	
1	C-port		All	Access	1
2	C-port		All	Access	1
3	C-port		All	Access	1
4	C-port		All	Access	1
5	C-port		All	Access	1
6	C-port		All	Access	1
7	C-port		All	Access	1
8	C-port		All	Access	1
9	C-port		All	Access	1
10	C-port		All	Hybrid	1
11	C-port		All	Hybrid	1
12	C-port		All	Hybrid	1
13	C-port		All	Hybrid	1
14	C-port		All	Hybrid	1
15	C-port		All	Hybrid	1
16	C-port		All	Hybrid	1
17	C-port		All	Access	1
18	C-port		All	Access	1
19	C-port		All	Access	1
20	C-port		All	Access	1
21	C-port		All	Access	1
22	C-port		All	Access	1
23	C-port		All	Access	1
24	C-port		All	Access	1
25	C-port		All	Access	1
26	C-port		All	Access	1

Ensure that the **PVID** (port VLAN ID) for each port is set to a value of `1`. The PVID is the VLAN ID that a port assigns to incoming data packets which do not already have a VLAN tag; Therefore, the PVID corresponds to the VLAN ID of the `default` group.

4. OPTIONAL: If you wish to allow access to the guest network via Ethernet, go to **Configuration** > **VLAN** > **Ports** and, for example, set the **PVID** to `100` for ports 17 to 20 and, under **Configuration** > **VLAN** > **VLAN-Membership**, assign these ports to the group `Guests`. All untagged incoming data packets arriving at these ports are given VLAN ID 100.

Note that these data packets can only leave the switch via the ports of the guest network.

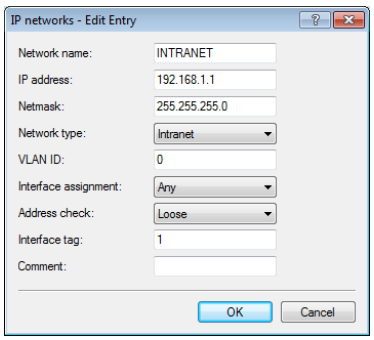
Configuring the IP networks in the WLAN controller

To separate the data streams on layer 3, two different IP networks are employed (ARF – Advanced Routing and Forwarding).

1. For the internal network, set the **INTRANET** to the address `192.168.1.1`.

   This IP network uses the **VLAN ID** `0`. This assigns all untagged data packets to this network (the VLAN module in the controller itself must be activated for this). The **interface tag** `1` is used for the subsequent break-out of data in the virtual router.

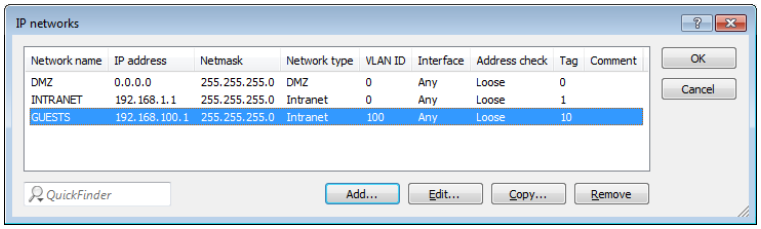
   › LANconfig: **TCP/IP** > **General** > **IP networks**



2. For guests, create a new IP network with the address `192.168.100.1`.

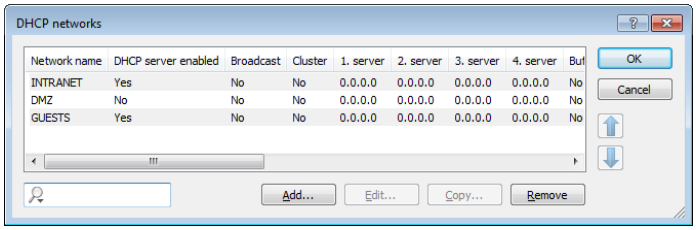
   This network uses the **VLAN ID** `100`. In this way, all data packets with this ID are assigned to the guest network. Here, too, the **interface tag** `10` is used later by the virtual router.

   › LANconfig: **TCP/IP** > **General** > **IP networks**

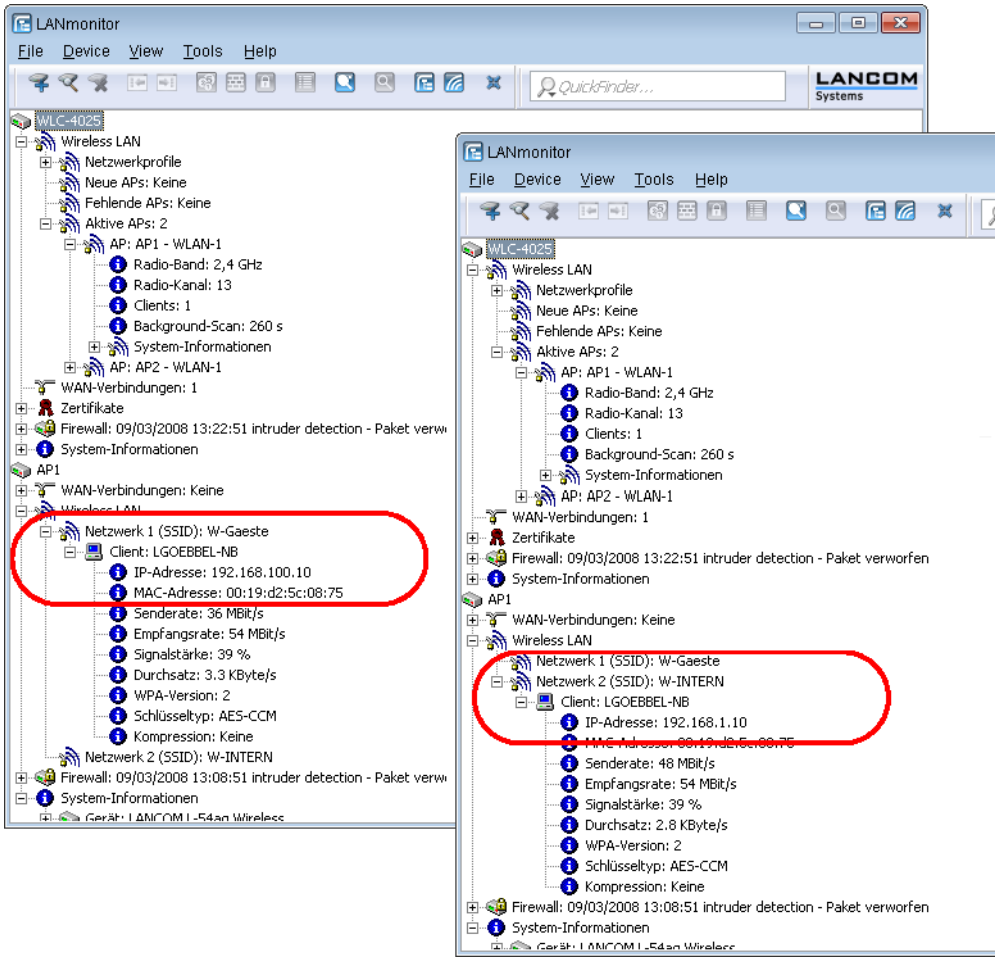


3. Enable the DHCP server for both IP networks.

   › LANconfig: **TCP/IP** > **General** > **IP networks**



With these settings, the WLAN clients of the internal employees and guests are assigned to the appropriate networks.

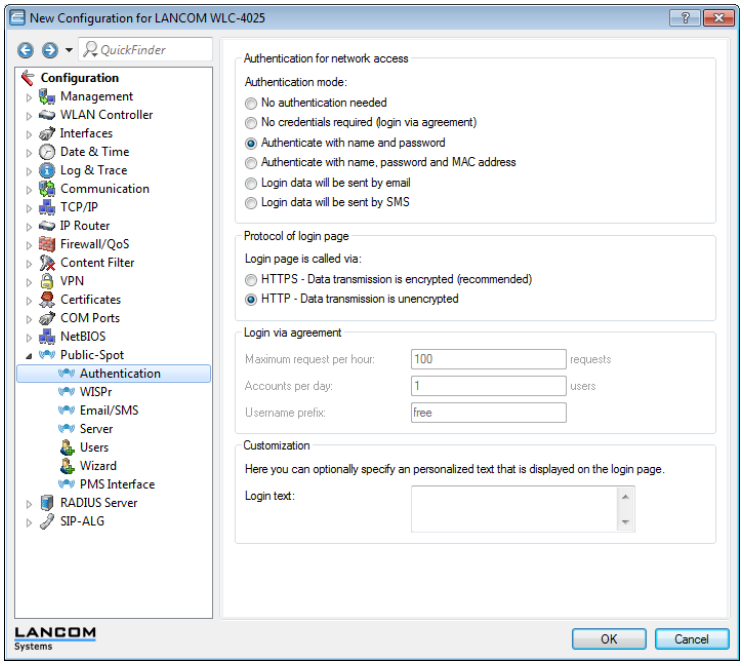


Configuring Public Spot access accounts

The Public Spot allows you to provide a strictly controlled point of access to your wireless LAN. Authentication is performed by requesting user information via a web interface. If necessary, you can can set a time limit for the access.

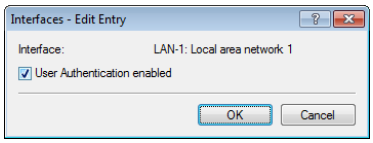
1. You should activate authentication for network access by name and password.

> LANconfig: **Public Spot** > **Authentication** > **Authentication for network access**



2. Activate user authentication for the controller's interface that is connected to the switch.

   > LANconfig: **Public Spot** > **Server** > **Operation settings** > **Interfaces**

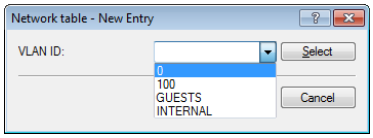


3. Restrict access to the Public Spot.

   You restrict use of the Public Spot to data packets from this virtual LAN by entering the VLAN ID of "100" for the guest network into VLAN table. Other data packets from other VLANs will be forwarded to the Public Spot without a login.

   ⓘ If the interface is not restricted to the VLAN ID, the controller will no longer be reachable at the specified physical Ethernet port!

   > LANconfig: **Public Spot** > **Server** > **VLAN table**



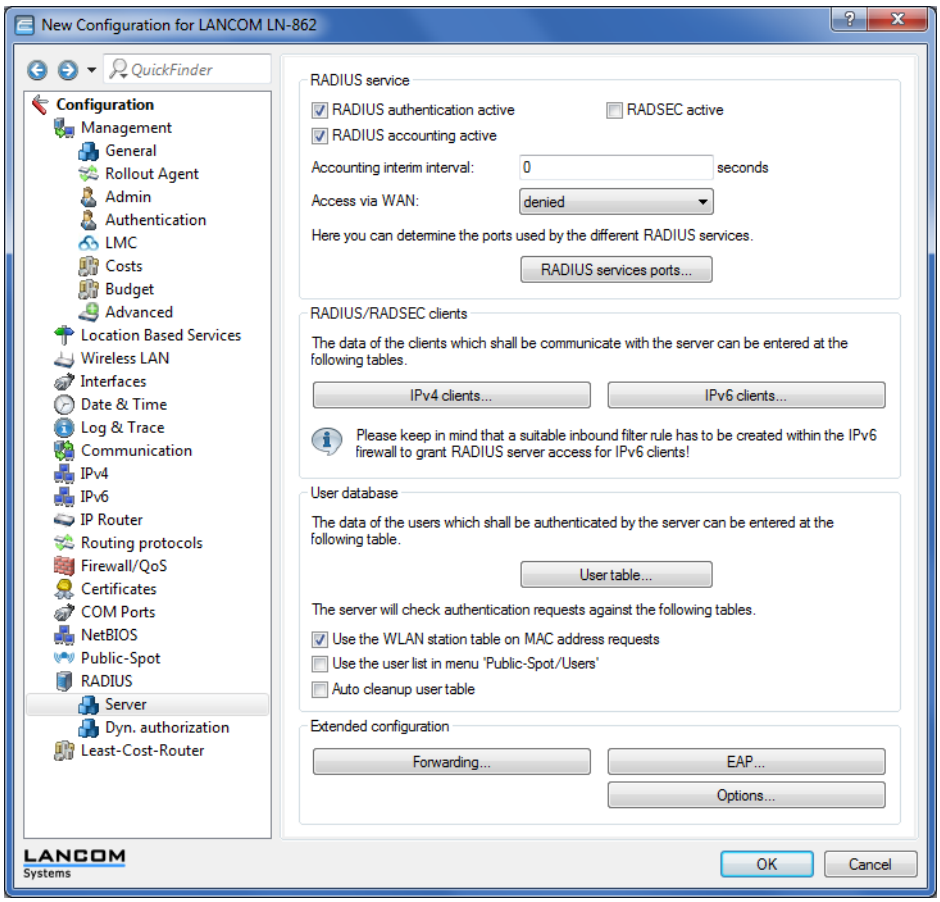
4. Enable the option to clean up the user table so that your device automatically deletes entries that are no longer needed.

   > LANconfig: **RADIUS** > **Server** > **User table** > **Auto cleanup user table**

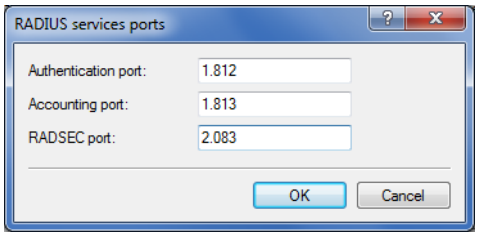
Configuring the internal RADIUS server for Public Spot operation

The Wizard stores the Public Spot access accounts in the user database of the internal RADIUS server. In order to use these Public Spot access accounts, the internal RADIUS server has been preconfigured with default values. You can inspect this setup in **LANconfig** as follows:

1. Navigate to **RADIUS** > **Server** > **RADIUS service**.
2. Ensure that checkmarks have been set for **RADIUS authentication active** and **RADIUS accounting active**.



3. Click the button **RADIUS services ports**.

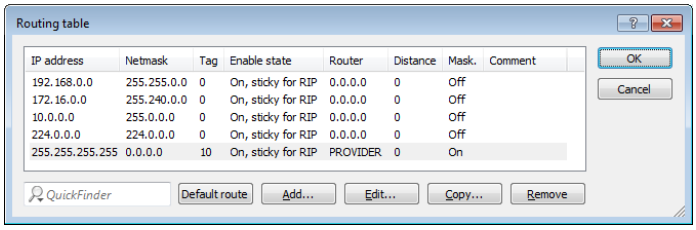


The default settings are available here for inspection.

Configuring Internet access for the guest network

1. In order to provide Internet access for guest network users, there is a wizard to set up access to a provider network.
2. Limit access to the provider network.
   In order for this access to be available to users of the guest network only, set the routing tag "10" for the corresponding route. This ensures that only data packets from the IP network "GUEST" with the interface tag "10" are transmitted to the provider's network. The different routing tag values ensure that data cannot be routed between the guest network and the internal network.

> LANconfig: **IP router** > **Routing** > **Routing table**



3. Optional: If necessary, use **Device** > **Configuration Management** > **Upload certificate or file** in LANconfig to upload an HTML template and an image as a template to the device for output of the voucher.
   The image can be a GIF, JPEG or PNG file of max. 64 KB in size.

1.4.2 Virtualization and guest access via WLAN controller without VLAN

Overlay network: Separating networks for access points without using VLAN

In many cases, networks in a shared physical infrastructure are separated by using VLANs. However, this method assumes that the switches operated in the network are VLAN-capable and that these are configured for VLAN operations. Consequently, the administrator has to rollout the VLAN configuration for the whole network.

WLCs enable you to separate the networks while minimizing the use of VLANs. The APs use a CAPWAP data tunnel to direct the payload from the WLAN clients straight to the WLC, which then assigns the data to the corresponding VLANs. In this situation, VLAN configuration is only required for the WLC and a single, central switch. All of the other switches in this example work without a VLAN configuration.

With this configuration, you reduce the VLAN to the core of the network structure (illustrated with a blue background). What's more, only 3 of the switch ports in use require a VLAN configuration.

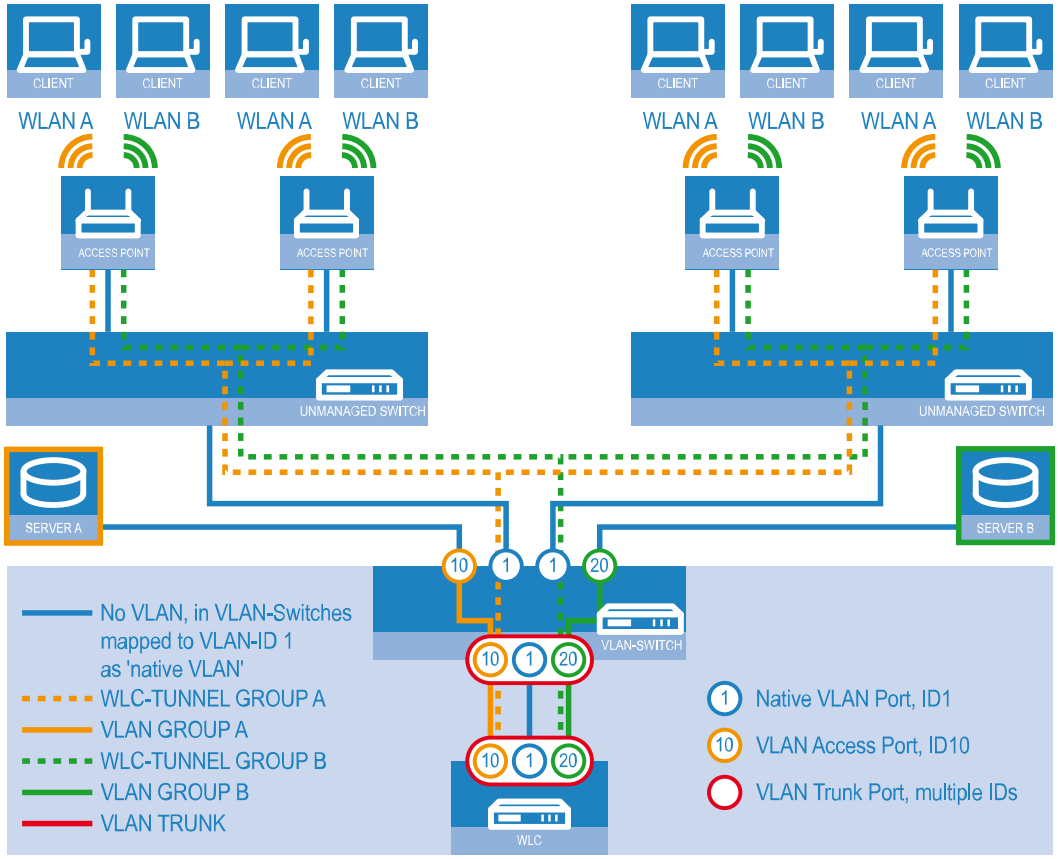


Figure 4: Example application: Overlay network

The diagram shows a sample application with the following components:

- The network consists of two segments, each with its own (not necessarily VLAN-capable) switch.
- Each segment contains several APs, each of which is connected to one of the switches.
- Each AP provides two SSIDs for the WLAN clients in two different user groups, shown in the diagram in green and orange.
- Each user group has access to its own dedicated server that is separated from other user group. The servers can only be accessed via the corresponding VLANs, i.e. through the access ports configured on the switch.
- A single WLC manages all of the APs in the network
- A central, VLAN-capable switch connects the switches in each segment, the servers for each group, and the WLC.

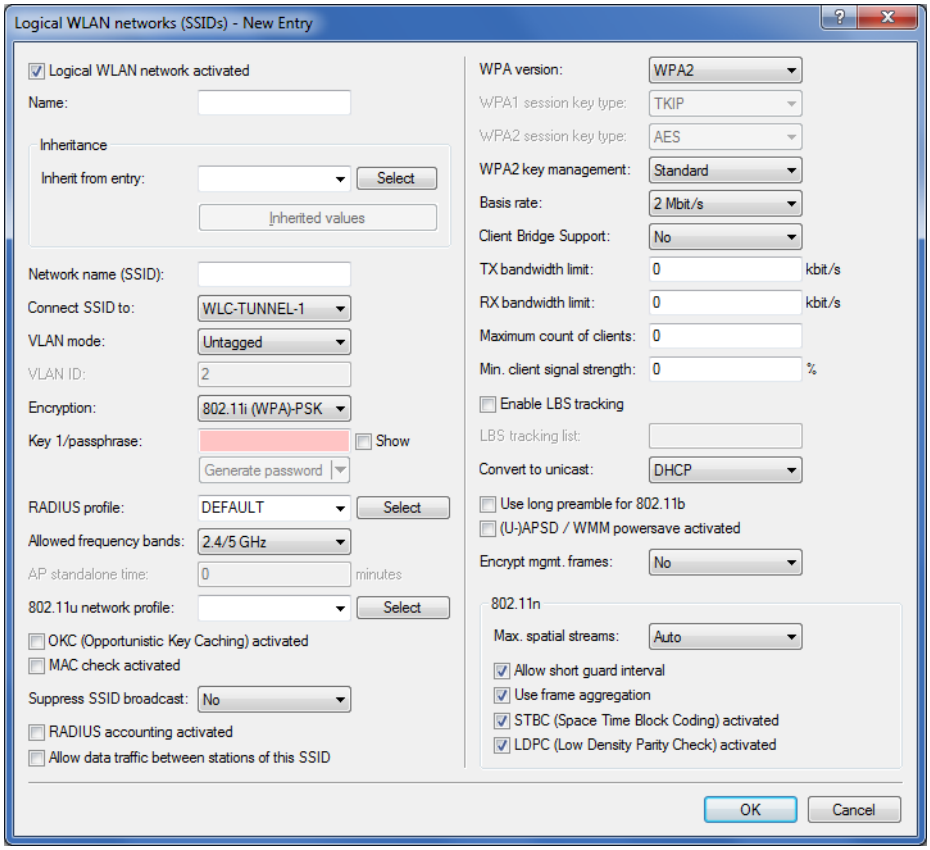
The aim of the configuration: A WLAN client that associates with an SSID is to have access to its "own" server, regardless of which AP is being used and regardless of the segment in which the client is located.

The following description assumes a working basic configuration of the WLC. The configuration of the VLAN switch is not part of this description.

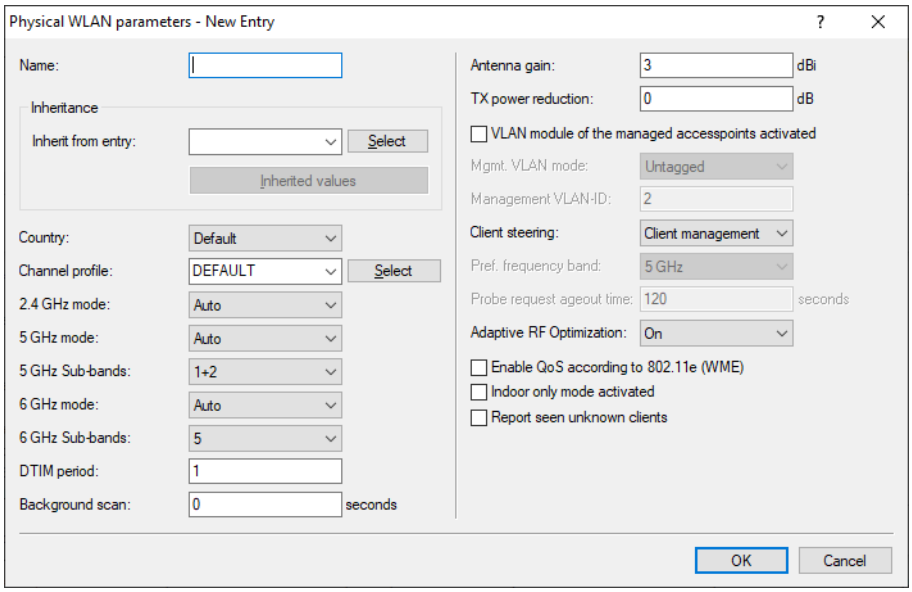
Configuring the WLAN settings

1. For each SSID, create an entry in the list of logical networks, each with a suitable name and the corresponding SSID. Connect the SSID to a WLC tunnel, for example the first SSID to "WLC-TUNNEL-1" and the second to "WLC-TUNNEL-2 ". Set the VLAN mode to 'tagged', set the VLAN ID '10' for the first logical network and the VLAN ID '20' for the

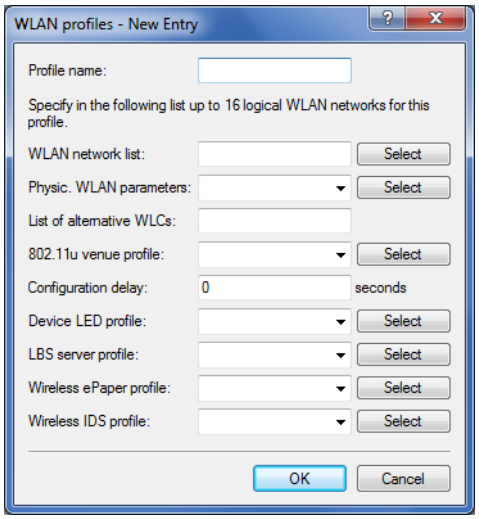
second logical network. In LANconfig you find these settings under **Configuration** > **WLAN Controller** > **Profiles** > **Logical WLAN networks (SSIDs)**.



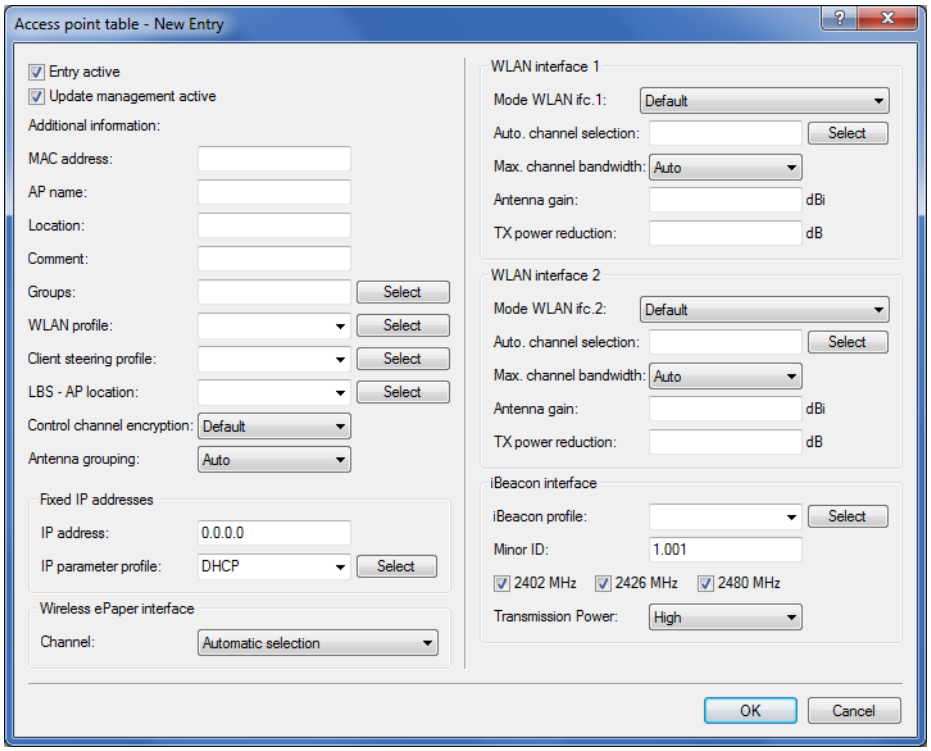
2. Create an entry in the list of physical WLAN parameters with the appropriate settings for your APs, such as the country 'Europe' with the channels 1, 6 and 11 in 802.11b/g/n and 802.11a/n in mixed mode. For this profile in the physical WLAN parameters, enable the option to turn on the VLAN module on the APs. Set the operating mode for the management VLAN in the APs to 'Untagged'. In LANconfig you find this setting under **Configuration** > **WLAN Controller** > **Profiles** > **Physical WLAN parameters**.



3. Create a WLAN profile and give it a suitable name. Then assign the logical WLAN networks and the physical WLAN parameters created previously to this WLAN profile. In LANconfig you find this setting under **Configuration** > **WLAN Controller** > **Profiles** > **WLAN profiles**.

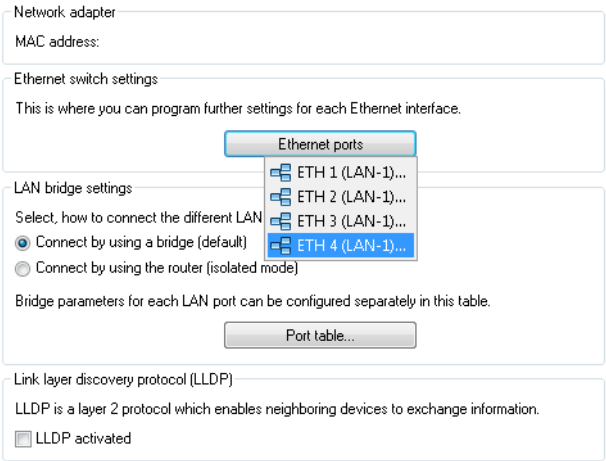


4. For each managed AP, create an entry in the AP table with a suitable name and the associated MAC address. Assign the previously created WLAN profile to this AP. In LANconfig you find these settings under **Configuration** > **WLAN Controller** > **AP config.** > **Access point table**.

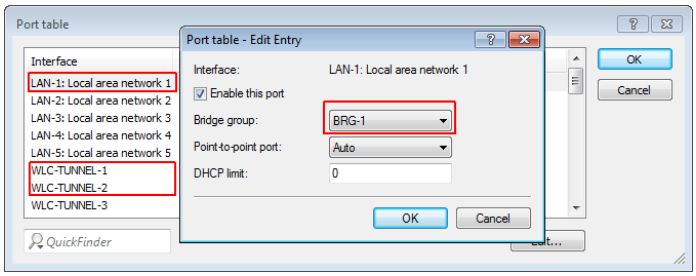


Configuring the interfaces on the WLC

5. Assign a separate logical LAN interface, e.g. 'LAN-1', to each physical Ethernet port. Make sure that the other Ethernet ports are not assigned to the same LAN interface. In LANconfig you find these settings under **Configuration** > **Interfaces** > **LAN** > **Ethernet ports**.

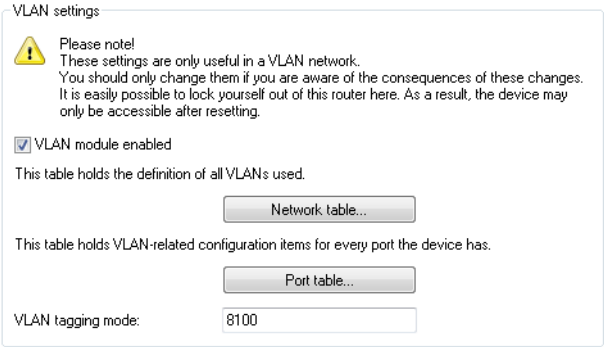


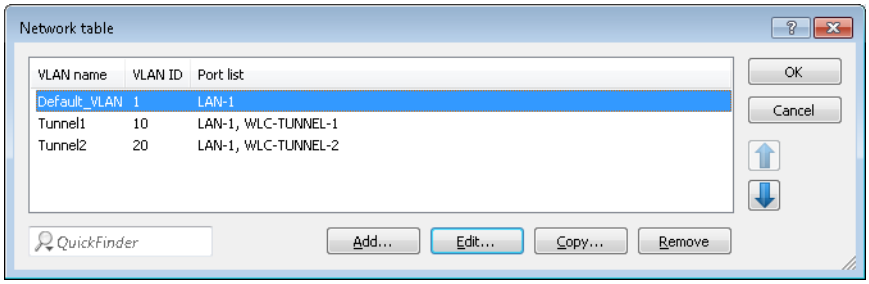
6. Assign the logical LAN interface 'LAN-1' and the WLC tunnels 'WLC-tunnel-1' and 'WLC-tunnel-2' to the bridge-group 'BRG-1'. Make sure that the other LAN ports are not assigned to the same bridge group. In LANconfig you find this setting under **Configuration** > **Interfaces** > **LAN** > **Port table**.



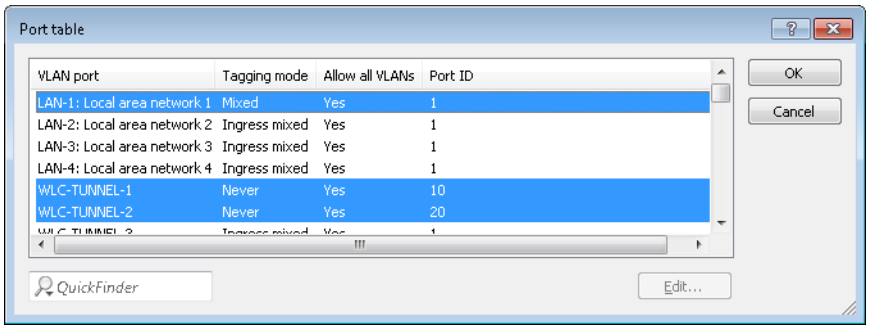
By default, the LAN interfaces and WLC tunnels do not belong to a bridge group. By assigning the LAN interface 'LAN-1' and the two WLC tunnels 'WLC-Tunnel-1' and 'WLC-Tunnel-2' to the bridge group 'BRG-1', the device transmits all data packets between LAN-1 and the WLC tunnels via the bridge.

7. Activate the VLAN module of the WLC under **Interfaces** > **VLAN** and, under **VLAN table**, assign the LAN port you selected above (LAN 1) and also the corresponding WLC tunnel to the desired VLAN.





8. Under **Interfaces** > **VLAN** > **Port table**, set the Tagging mode of the tunnel interface and the LAN interface, and set the corresponding port VLAN ID.



Depending on how the switch is configured, set the Tagging mode of the LAN interface to 'Mixed' or 'Always'.

In most cases the tunnel interfaces are operated with the mode 'Never', because packets here (from the WLAN) always arrive untagged and the WLC marks them with the port VLAN ID

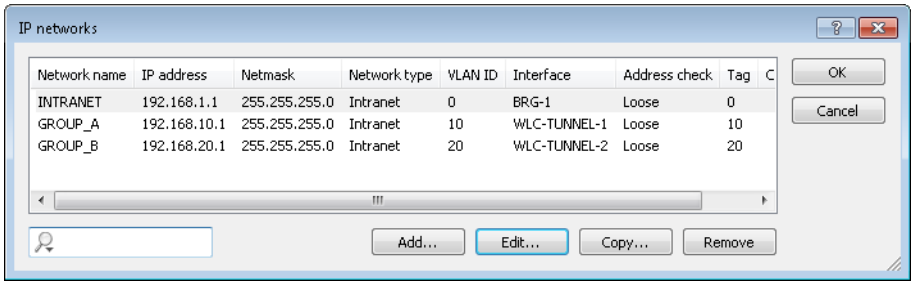
When you activate the VLAN module, please observe that the ARF networks configured on the WLC must be given a VLAN ID. In the VLAN configuration outlined above, you need to set the VLAN ID for the IP network to '1' in order for the WLC to reach the network without a VLAN tag.

A similar configuration is achieved by making the access point set a VLAN tag for packets that are to be sent via the tunnel, in which case the VLAN module of the WLC is not used.

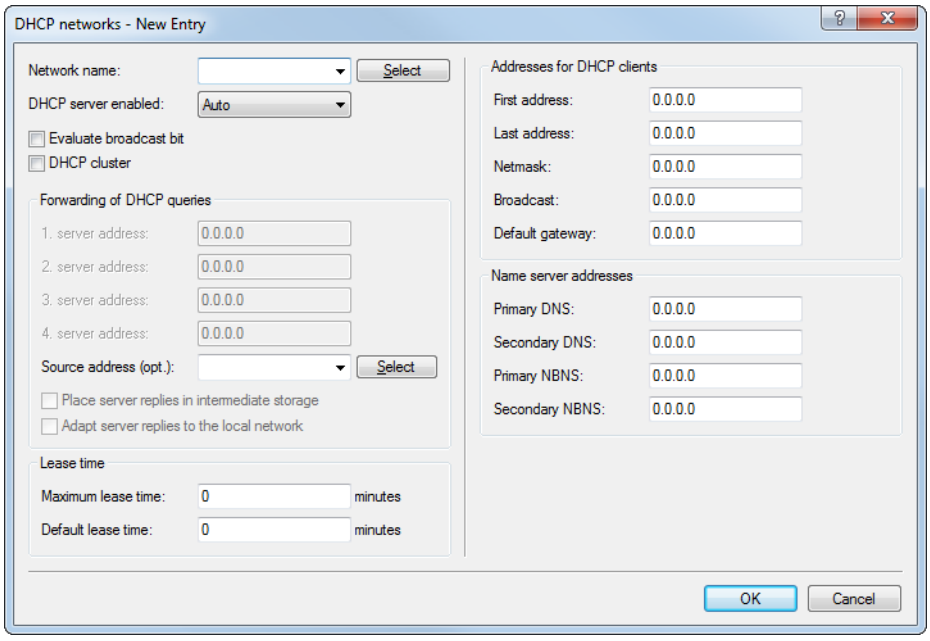
However, this bridging of the various WLC tunnels with one another causes broadcasts to be redirected into all of the tunnels; with a certain number of tunnels/SSIDs and APs, this can lead to load problems on the network and on the WLC. The VLAN module configuration presented here prevents this.

9. In addition you configure the IP settings for the networks that are separated on layer 2 under **IPv4** > **General** > **IP networks**.

To prevent the device from connecting these networks via layer 3, a separation must also be configured on layer 3, for example by using a port tag or by means of the firewall.



10. The WLC optionally acts as a DHCP server for the APs. To set this up, activate the DHCP server for the 'INTRANET'. In LANconfig you find these settings under **IPv4** > **DHCPv4** > **DHCP networks**.



WLAN controller with Public Spot

This scenario is based on the first scenario (overlay network) and enhances it to include specific settings for user authentication.

The configuration of a Public Spot can be greatly simplified if the payload data sent from the WLAN to the WLC is routed through a WLC tunnel. A Public Spot can, for example, provide guests with Internet access in parallel with, but separated from, an internal wireless LAN.

In this example, the employees of a company have access to a private WLAN (SSID), while the guests use a Public Spot to access the Internet. In all areas of the building, the APs provide two SSIDs, 'COMPANY' and 'GUESTS'.

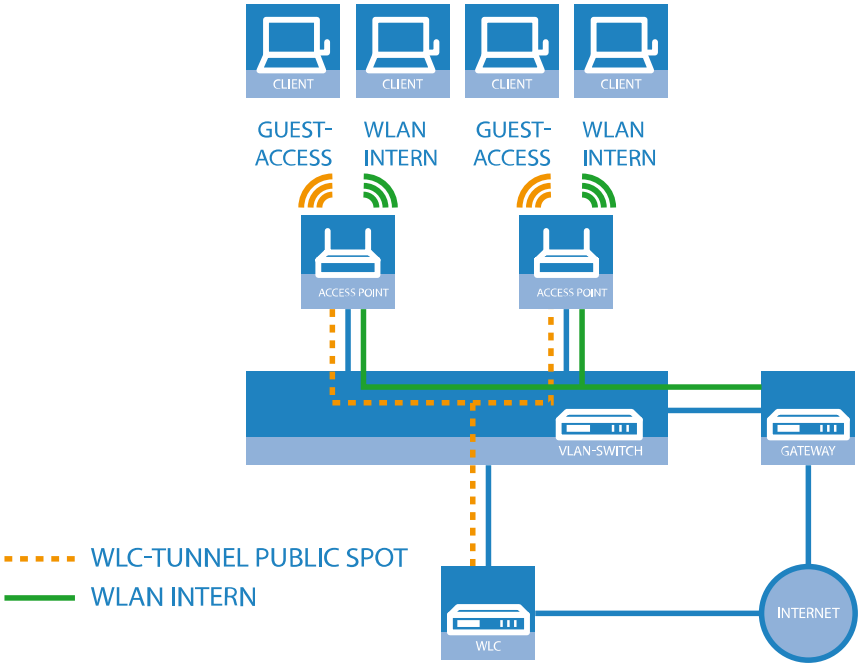
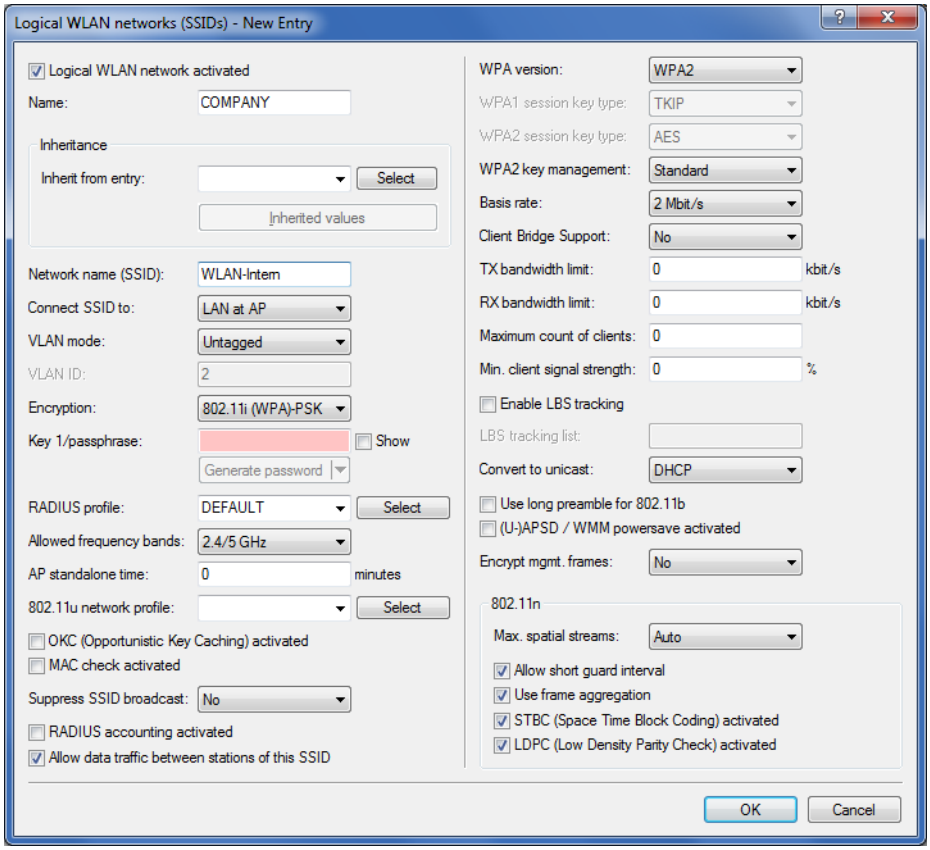


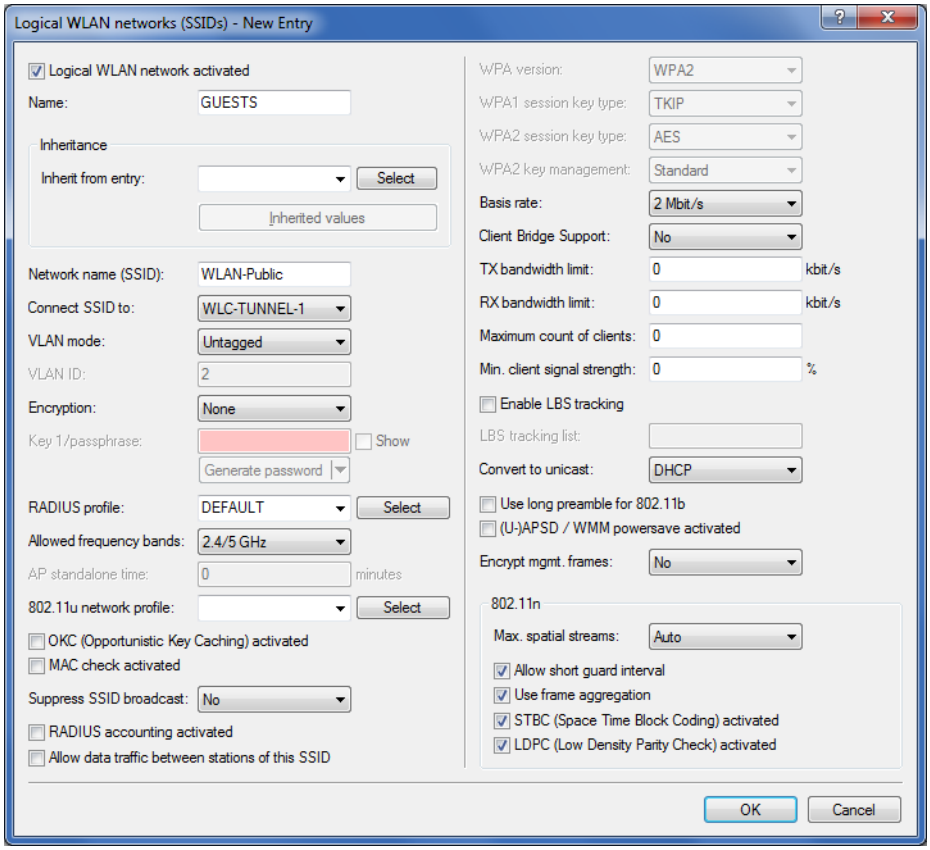
Figure 5: Example application: WLAN controller with Public Spot

The aim of the configuration: A WLAN client that associates with the internal SSID should have access to all internal resources and the Internet via the central gateway. The APs break-out the payload data from the internal clients locally and pass it on directly to the LAN. The guests' WLAN clients associate with the Public Spot. The APs send the payload data from the guest clients through a WLC tunnel directly to the WLC, which uses a separate WAN interface for Internet access.

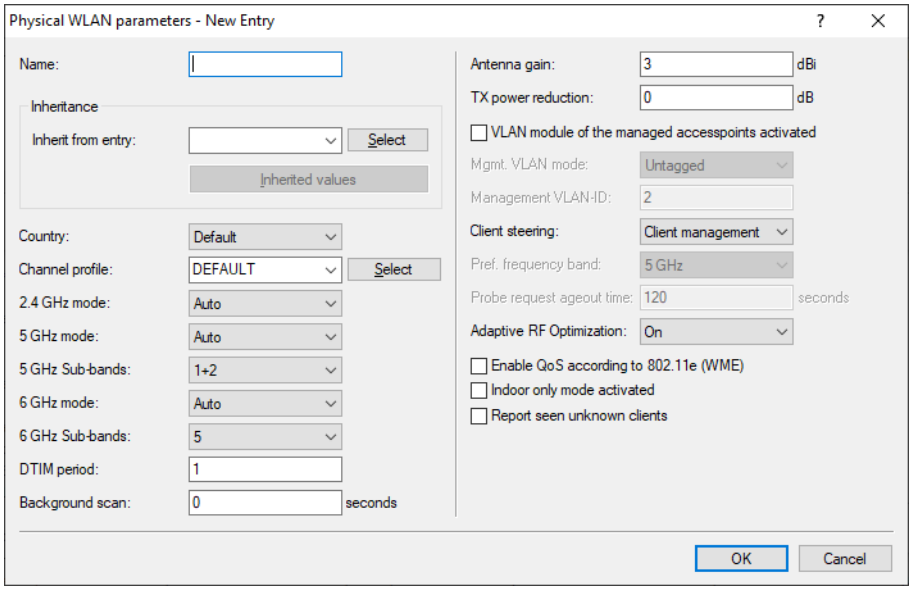
1. The internal WLAN and the guest WLAN each require an entry to be created in the list of logical networks, each with a suitable name and the corresponding SSID. Link the SSID for internal use with the 'LAN at AP', and the SSID for guests with (for example) 'WLC-TUNNEL-1'. Disable encryption for the guest network SSID so that the guests' WLAN

clients can associate with the Public Spot. You should also prevent inter-station traffic for this SSID. In LANconfig you find this setting under **Configuration** > **WLAN Controller** > **Profiles** > **Logical WLAN networks (SSIDs)**.

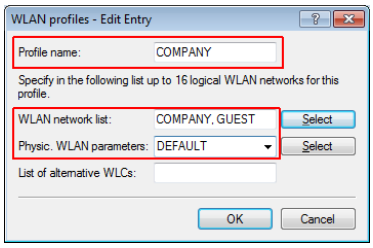




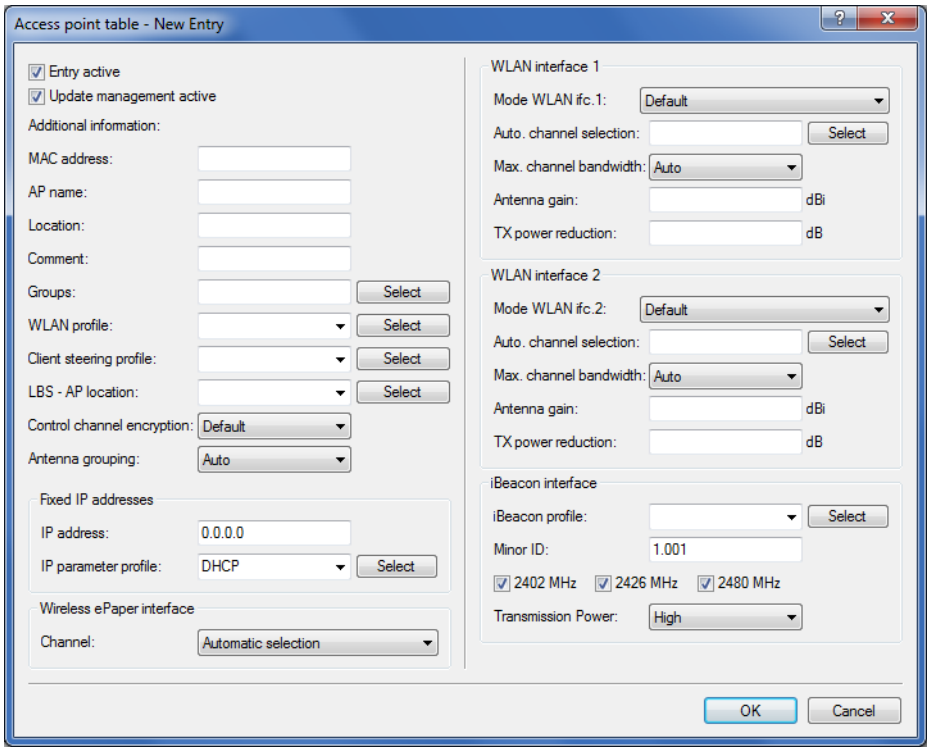
2. Create an entry in the list of physical WLAN parameters with the appropriate settings for your APs, such as the country 'Europe' with the channels 1, 6 and 11 in 802.11b/g/n and 802.11a/n in mixed mode. In LANconfig you find this setting under **Configuration** > **WLAN Controller** > **Profiles** > **Physical WLAN parameters**.



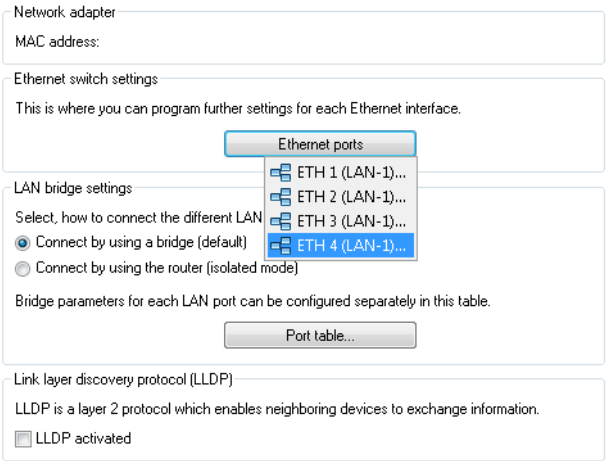
3. Create a WLAN profile and give it a suitable name. Then assign the logical WLAN networks and the physical WLAN parameters created previously to this WLAN profile. In LANconfig you find this setting under **Configuration** > **WLAN Controller** > **Profiles** > **WLAN profiles**.



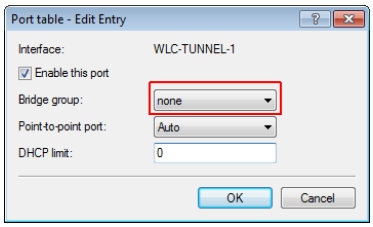
4. For each managed AP, create an entry in the AP table with a suitable name and the associated MAC address. Assign the previously created WLAN profile to this AP. In LANconfig you find this setting under **Configuration** > **WLAN Controller** > **AP config.** > **Access point table**.



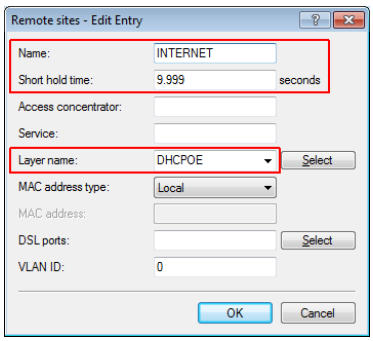
5. Assign a separate logical LAN interface, e.g. 'LAN-1', to each physical Ethernet port. Set the 4th Ethernet port to the logical LAN interface 'DSL-1'. The WLC then uses this LAN interface for the guest network Internet access. In LANconfig you find this setting under **Configuration** > **Interfaces** > **LAN** > **Ethernet ports**.



6. Verify that the logical LAN interface 'WLC-tunnel-1' is not allocated to a bridge group. This ensures that the other LAN interfaces do not transmit any data to the Public Spot. In LANconfig you find this setting under **Configuration** > **Interfaces** > **LAN** > **Port table**.

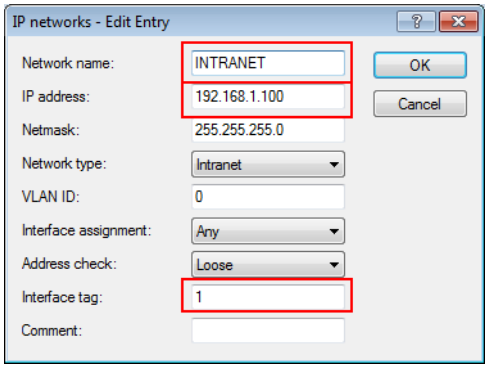


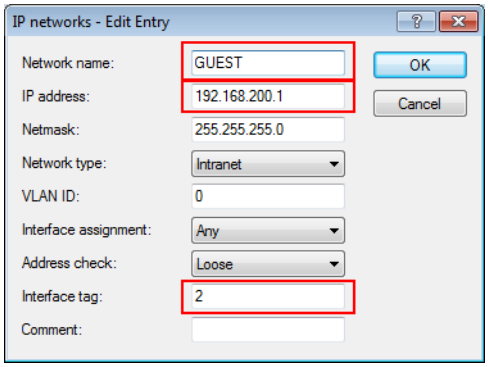
7. For the guest Internet access, create an entry in the list of DSL remote sites with the hold time '9999' and the pre-defined layer 'DHCPOE '. This example assumes that Internet access is provided by a router with DHCP server. In LANconfig you find this setting under **Configuration** > **Communications** > **Remote sites** > **Remote sites**.



8. For internal users, create the IP network 'INTRANET' with (for example) the IP address '192.168.1.100' and the interface tag '1'. For the guest access, create the IP network 'GUEST-ACCESS' with (for example) the IP address of

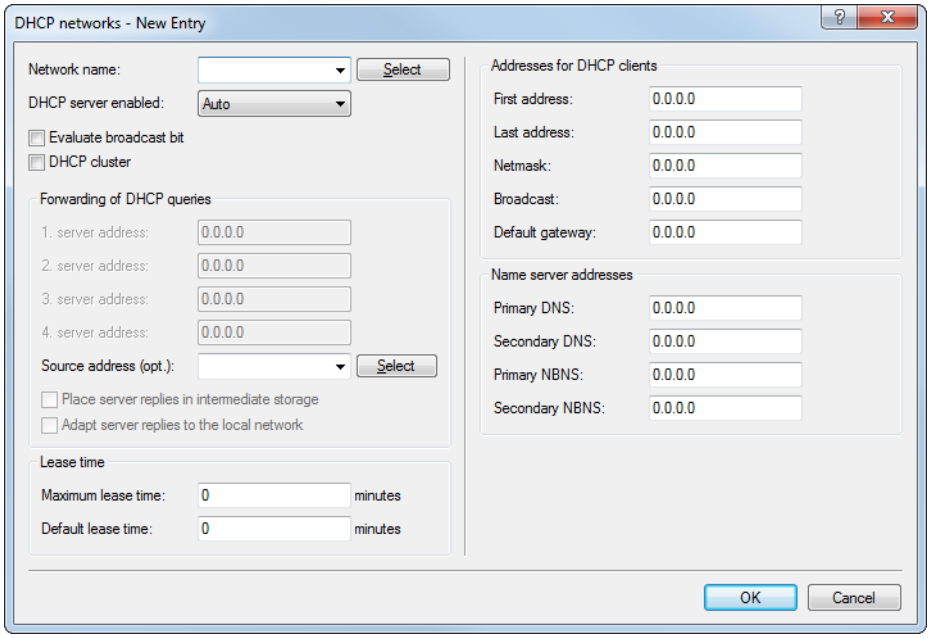
'192.168.200.1' and the interface tag '2'. The virtual router in the WLC uses the interface tags to separate the routes for the two networks. In LANconfig you find this setting under **Configuration** > **TCP/IP** > **General** > **IP networks**.



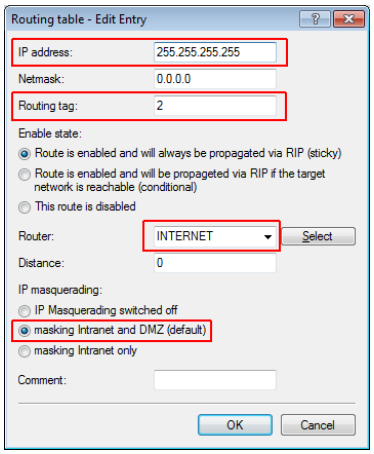


9. The WLC is able to act as a DHCP server for APs and the associated WLAN clients. To set this up, activate the DHCP server for the 'INTRANET' and the 'GUEST-ACCESS'. In LANconfig you find this setting under **Configuration** > **TCP/IP** > **DHCP** > **DHCP networks**.

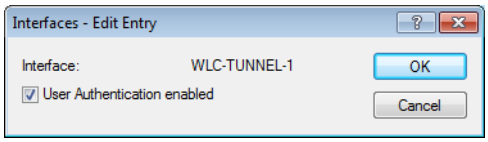
Activation of the DHCP server is obligatory for the guest network and optional for the internal network. There are other ways of realizing a DHCP server for the internal network.



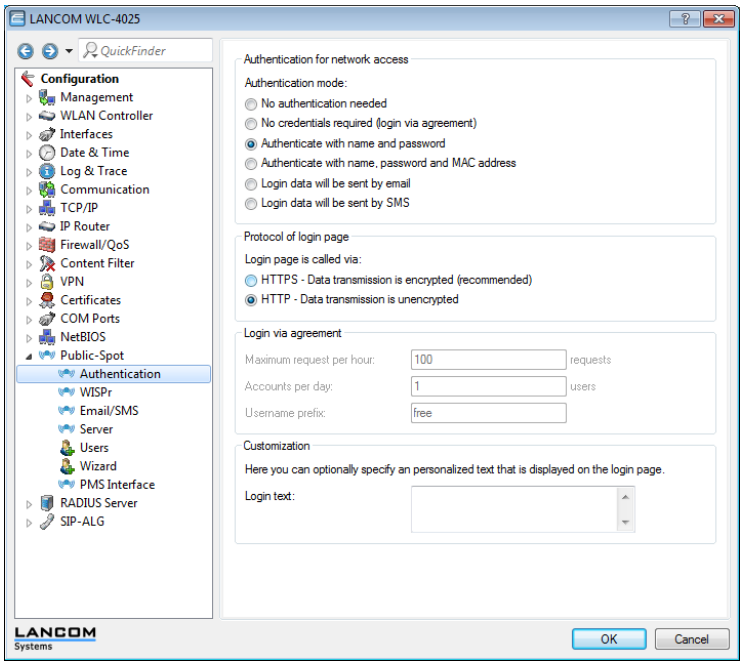
10. Create a new default route in the routing table to direct the data from the guest network to the Internet connection used by the WLC. Select the routing tag '2' and the router 'Internet'. Also activate the option 'Masking intranet and DMZ (default)'. In LANconfig you find this setting under **Configuration** > **IP router** > **Routing** > **Routing table**.



11. Activate the Public Spot user authentication for the logical LAN interface 'WLC-Tunnel-1'. In LANconfig you find this setting under **Configuration** > **Public Spot** > **Server** > **Operational settings** > **Interfaces**.



12. The final step is to enable authentication via the Public Spot for the WLC. In LANconfig you find this setting under **Configuration** > **Public Spot** > **Authentication**.



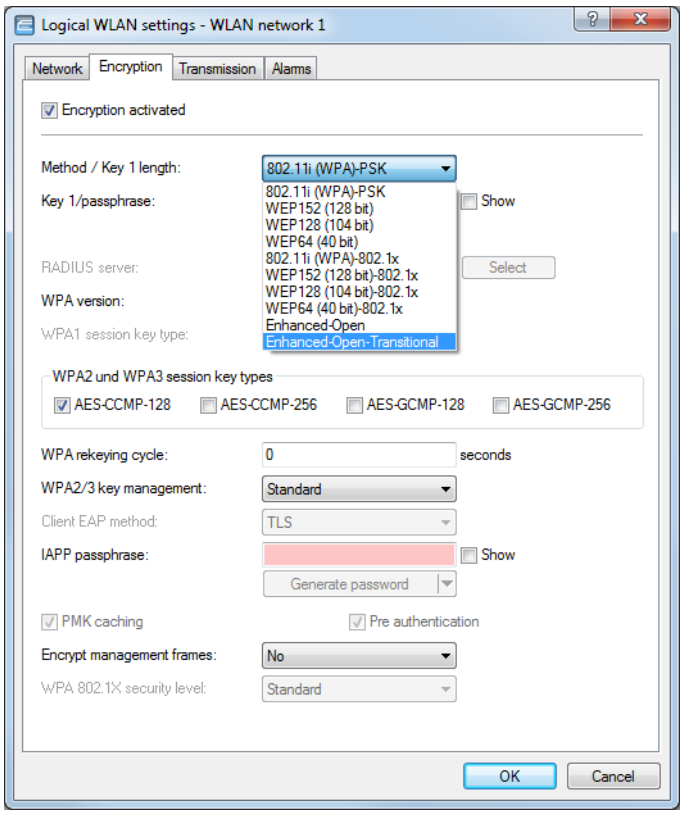
In addition to configuring the WLC, you must also configure the Public Spot either to use the internal user list or to use a RADIUS server, according to your needs.

1.4.3 Setting up a secure hotspot with Enhanced Open

Enhanced Open for the first time provides a way to offer a secure, yet easy-to-use hotspot.

Enhanced Open has been combined with the LANCOM Public Spot option.

The WLAN to be used for the hotspot is set up in the usual way with the exception that the encryption method is set to **Enhanced Open Transitional**:



Not only is entering a key not required, it is not even possible: A client enabled for Enhanced Open establishes an encrypted connection to the access point without any key having to be entered. To the user, it is just like using an unencrypted, open WLAN: There is no need to enter any previously communicated key as with WPA2-PSK.

The Transitional mode allows an SSID to be used concurrently by clients that support Enhanced Open as well as by clients that do not yet support Enhanced Open. For the latter clients, no encryption is used at all and the SSID works like an open, unencrypted SSID. Once Enhanced Open has become more widespread, you can switch from Transitional mode to regular Enhanced Open mode.

After this, you can proceed as usual with the configuration of the Public Spot module. Since the Public Spot module is independent of the encryption settings of the WLAN interfaces, all of the functions of the Public Spot module can be used without restriction in conjunction with Enhanced Open.

In summary, Enhanced Open is ideal for hotspot operation as it provides a higher level of security than the open hotspots used in the past. The optional Transitional mode ensures that even clients that do not yet support Enhanced Open can be connected in a way that is transparent to the user.

1.4.4 Setting up an external RADIUS server for user administration

Some applications user data is not stored on the device, but on an external, centralized RADIUS server. In this case, the Public Spot must communicate with the external RADIUS server to check the user data.

Please note that specific functions (such as the Public Spot wizards in WEBconfig) are not available to you if you use an external RADIUS server for user administration!

The following instructions assume that you know the IP address of a functional RADIUS server in the network.

The following configuration steps are used to set up a Public Spot that will be used with an external RADIUS server:

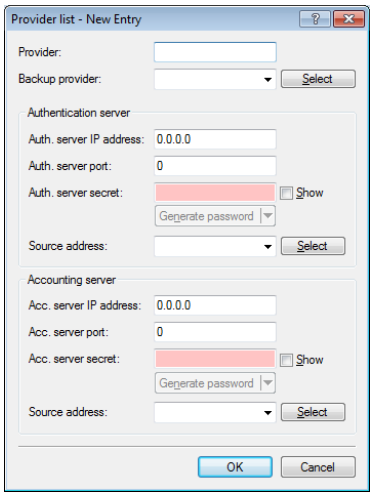
1. Follow the steps in the section *Manual Installation*.

   Among other things, the exact time on the device is necessary for the proper control of time-limited access.

   If authentication with an additional check of the physical address (MAC address) is enabled, the Public Spot transmits the MAC address of the end device to the RADIUS server. In this manner the Public Spot does not see whether the MAC address was actually checked or not. For MAC address checks to work without problem, the RADIUS server must be configured accordingly.

2. Enter the settings for the RADIUS server.

   When configuring a Public Spot, user registration data can be forwarded to one or more RADIUS servers. You configure these servers in LANconfig under **Public Spot** > **Users** > **Users and RADIUS servers** > **RADIUS server**. The registration data that individual RADIUS servers require from the clients is not important to the device that provides the Public Spot, since this data is transparently passed on to the RADIUS server.



   IP addresses specified here must be static. The Public Spot must be able to contact the specified destination addresses. For IP addresses outside of your own network, a router that has contact to the destination network must be specified as a gateway in the DHCP settings for the Public Spot. You have to define this gateway as the default route in the routing table.

   In order for the RADIUS server to record the connection data, the information on the accounting server must be specified in full. As an alternative to using a RADIUS accounting server, the connection information from the Public Spot can also be output by the SYSLOG function.

3. That's it!

   Your Public Spot is now ready for operation. All users with a valid account on the RADIUS server can use the Web interface to login to the Public Spot.

1.4.5 Internal and external RADIUS servers combined

Some companies use an external RADIUS server to authenticate users with IEEE801.1x. For applications with a WLAN controller and multiple access points, the access points initially address the WLAN controller as their RADIUS server. You define how the RADIUS requests are forwarded to the external RADIUS server on the WLAN controller.

The settings described below are only necessary if you are operating an external RADIUS server on your device in addition to the Public Spot in the external RADIUS server.

A Public Spot providing guest-access accounts requires the following settings:

- Authentication requests from internal employees are to be forwarded to an external RADIUS server.
- The authentication requests for Public Spot access accounts are to be handled by the internal RADIUS server.

Realm-tagging for RADIUS forwarding

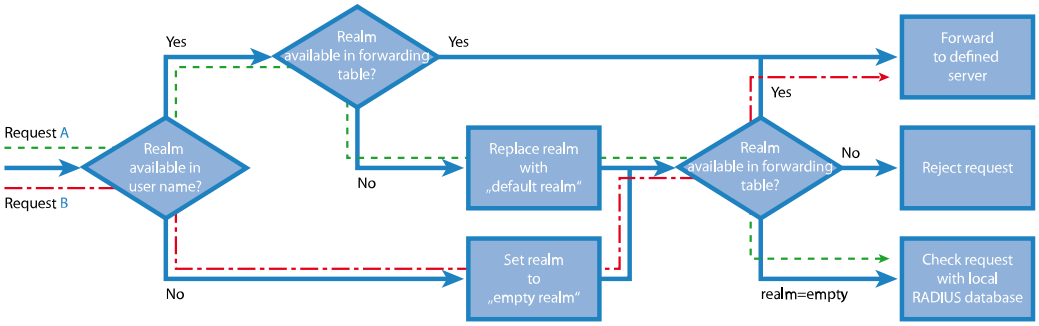
Authentication requests from the two user groups are to be handled separately. The WLAN controller uses what are known as "realms" to differentiate between these two groups. The purpose of realms is to address domains within which user accounts are valid. The WLAN controller can transmit the realms with authentication requests to the RADIUS server. Alternatively, the RADIUS server can change the realms in the user names for the purpose of RADIUS forwarding:

- The value defined for "Standard realm" replaces an existing realm of an incoming request if no forwarding is defined for that existing realm.
- The value defined under "Empty realm" is **only** used by the RADIUS server if the incoming user name **still does not** have a realm.

An entry in the forwarding table causes all authentication requests with a certain realm to be forwarded to a RADIUS server. If no matching entry exists in the forwarding table, the request is refused.

If the WLAN controller checks the realm and finds that it is empty, it **always** checks the authentication request with the internal RADIUS database.

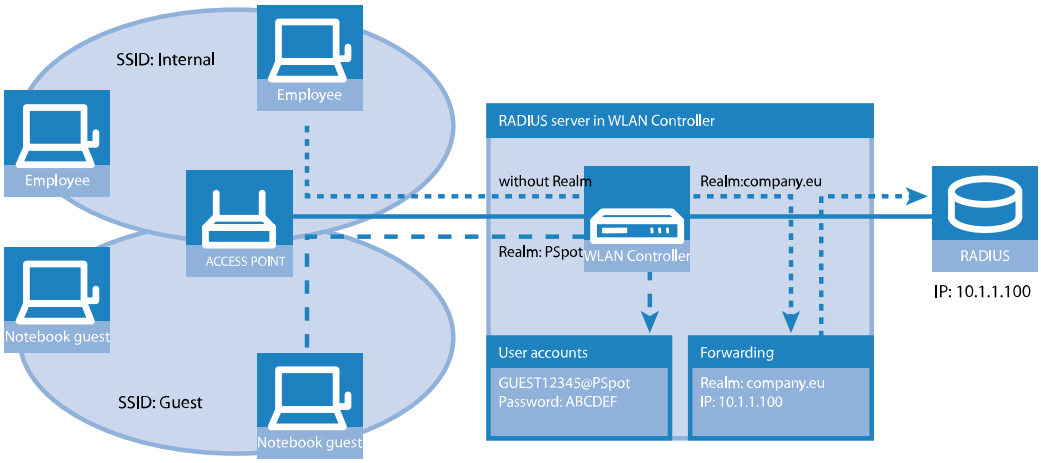
The following flow diagram illustrates the method used by the RADIUS server to process realms:



Using different realm tags allows different RADIUS servers to be targeted with requests. The way in which the device's RADIUS server makes decisions for the two requests is shown in the diagram:

1. Because the user names for guest access accounts are generated automatically, they are suffixed with an appropriate realm, such as "PSpot". Because the forwarding table does not contain this entry and the standard realm is empty, the WLAN controller forwards all authentication requests with this realm to the internal RADIUS server.
2. To limit the amount of work required for the configuration, internal users are listed without a realm. The RADIUS server in the device can automatically replace an empty realm with another realm in order to identify internal users. In this example, the empty realm is replaced by the domain of the company "company.eu". The information specified

in the forwarding table allows all authentication requests with this realm to be forwarded to the external RADIUS server.

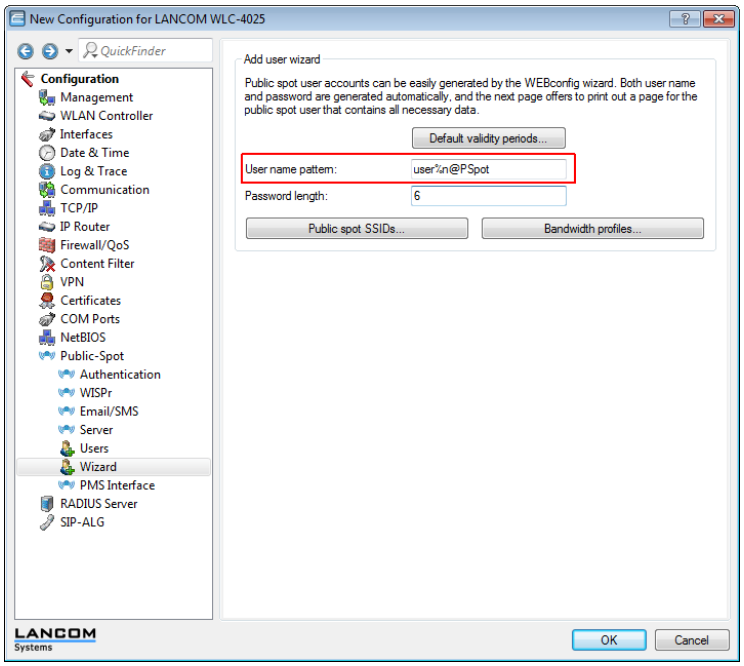


Configuring RADIUS forwarding

The following configuration steps allow you to specify the different manners in which internal users and guests are processed.

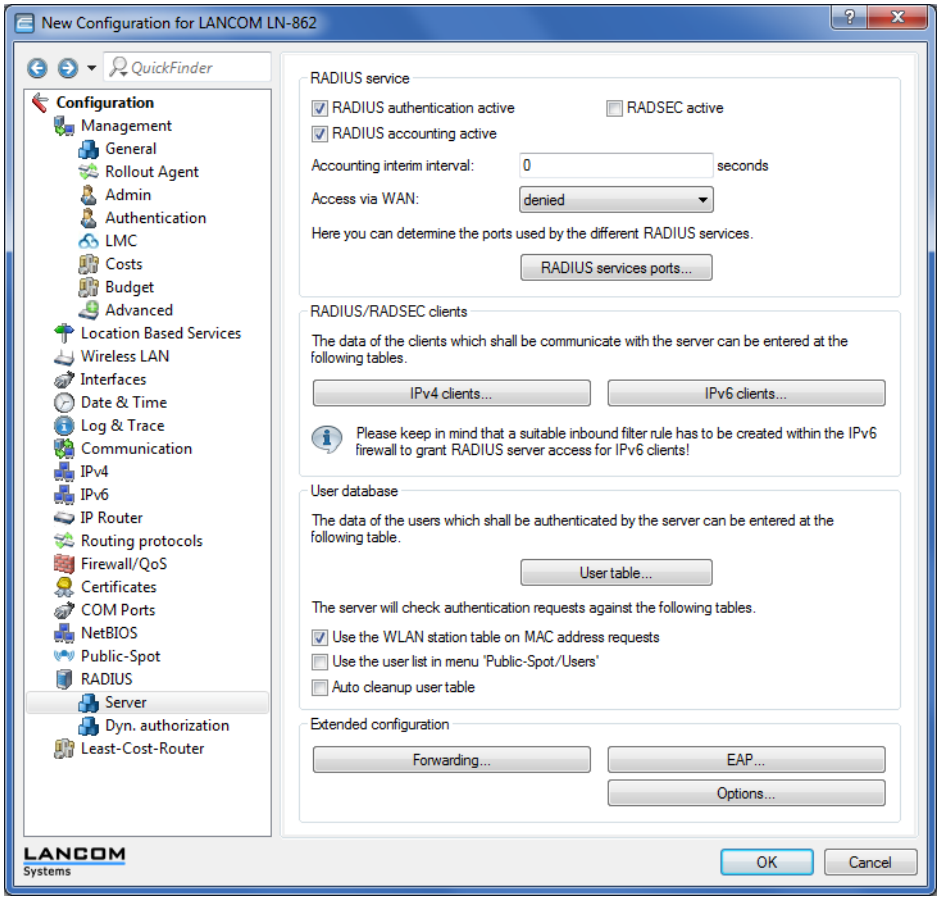
1. In the Public Spot, adapt the pattern of user names such that a unique realm can be suffixed.
   For example, if the pattern is "user%n@PSpot", the Public Spot generates usernames with the format "user12345@PSpot".

   › **LANconfig: Public-Spot** > **Wizard** > **Add user wizard**



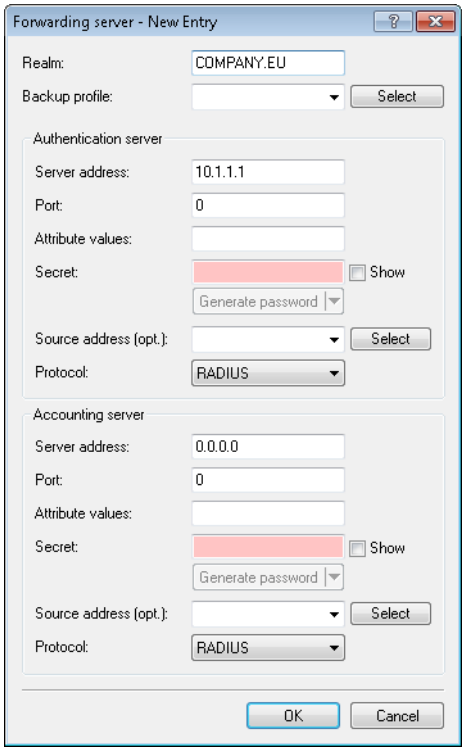
2. In the WLAN controller's RADIUS server, define an "empty realm" (e.g., "COMPANY.EU").
   This realm is attached to all user names which request authentication from the WLAN controller and which do not already have a realm. In this application, the internal users have no realm defined. In order to prevent the WLAN controller's RADIUS server from attaching a realm, you must leave the "Default realm" field blank.

> **LANconfig: RADIUS > Server > Extended configuration > Forwarding > RADIUS forwarding > Forwarding server**



3. In order for the WLAN controller to forward authentication requests from internal users to the external RADIUS server, suitable entries must be made in the forwarding settings.

All incoming RADIUS requests which have the realm "COMPANY.EU" will be forwarded to the specified IP address.



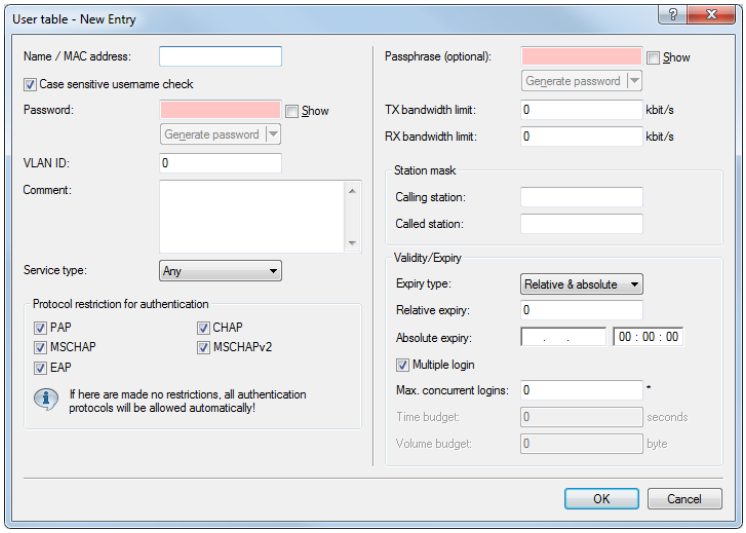
4. Authentication requests from Public Spot users have the realm "@PSpot" and are received by the WLAN Controller. With no forwarding defined for this realm, the usernames are automatically checked with the internal RADIUS database. Because the Public Spot access accounts created with the Wizard are stored in this database, these requests can be authenticated as required.

1.4.6 Checking WLAN clients with RADIUS (MAC filter)

To use RADIUS to only authenticate specific WLAN clients and grant them WLAN access based on their MAC address, an external RADIUS server can be used, as can the internal RADIUS user database of the WLAN controller.

Enter the MAC addresses in the RADIUS database using LANconfig, and enable all authentication methods. For **Name/MAC address** and **Password** select the corresponding MAC address in the format "AABBCC-DDEEFF".

> LANconfig: **RADIUS** > **server** > **User database** > **User table**



1.4.7 Setting up an external SYSLOG server

Depending on the use case, storage of the usage data is required for the operation of a Public Spot. This data can be stored to a SYSLOG server, for example. Some SYSLOG servers are available as free software.

To save user data from a Public Spot by means of SYSLOG, the external SYSLOG server has to be configured in the respective Public Spot. Once this is done, messages are sent for logging to the SYSLOG server whenever Public Spot user accounts are created or deleted, and at the beginning and end of Public Spot sessions. The message issued at the end of a session—with the source "Login" and the priority "Information"—also includes information on the transferred data volumes and the IP address used.

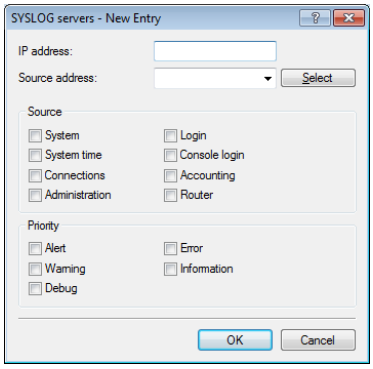
Further information on the configuration of SYSLOG is available in the section *The SYSLOG module*. You can find legal information about this topic in the LANCOM techpaper "Public Spot" which is available at *www.lancom-systems.com*.

Configuring an external SYSLOG server

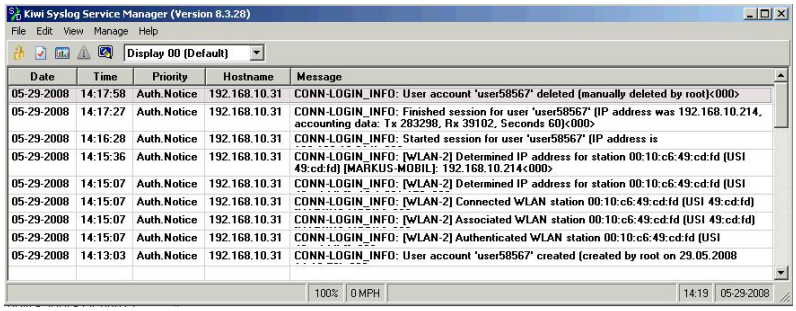
Your device is capable of logging the creation and deletion of Public Spot users, as well as their login and logout activities. You can also transfer this internally stored information to an external SYSLOG server. The following steps show you how you can set up logging with a program installed on an external SYSLOG server (in this example, "Kiwi").

1. Start LANconfig and open the configuration dialog for your device.
2. Change to the dialog **Log & Trace** > **General** and open the table **SYSLOG servers**.

3. Add a new entry. Specify the **IP address** of the computer where the SYSLOG client is installed (e.g., `192.168.10.237)`, and enter the **Source** (`Login`, `Accounting`) and the **Priority** (`Information`).



4. Close the dialog and store the configuration on your device.
5. Start the analysis program on your SYSLOG server (e.g., "Kiwi"). As soon as the program has started, it logs the creation and deletion of Public Spot accounts and also the user logins and logouts.



1.5 XML interface

In order to be able to cover a wide range of Public Spot scenarios, the default authentication method of name and password is not sufficient by itself. Access and accounting models based on social media, credit cards and other methods often require additional access data, which the Public Spot in this form would be unable to manage.

The implemented XML interface connects the Public Spot and an external gateway. It directs the user data only to the gateway that handles the authentication and accounting, and it only sends information about the duration and limits of the user access to the Public Spot.

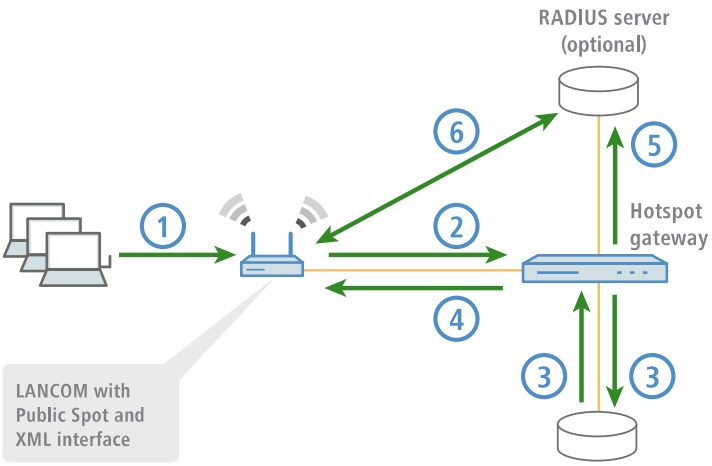
In this case, the Public Spot only performs the following tasks:

- Forward the user requests
- Restrict unauthorized access attempts
- Accept gateway commands to start and stop a session
- Accounting for sessions, if applicable

Since it is not realistic to implement all existing, and at times very specific scenarios with the associated gateway commands on the Public Spot, the XML interface was designed to be flexible and multi-purpose.

1.5.1 Feature

The communication between the XML interface and external gateway is processed as follows:



1. The user connects to the Public Spot's WLAN and sends an HTTP request to the Public Spot.
2. The Public Spot forwards the login procedure's HTTP request to the external hotspot gateway. The external hotspot gateway is located either in a freely accessible network provided by the Public Spot, or its address is included in the list of free hosts.

   The Public Spot forwards the MAC address of the requesting Public Spot client to the external gateway. To implement this, navigate to **Public-Spot-Module** > **Page-Table**, set the **Type** to "Redirect" and suffix the **URL** with the parameter `?myvar=%m`.

   Example: `http://192.168.1.1/?myvar=%m`

   In this case, `myvar` is a freely selectable variable. The variable `%m` is vital here, as the Public Spot replaces this with the client's MAC address when forwarding the request.

   Table 9: Variables

Variable	Meaning
%s	SSID name
%v	Source VLAN
%i	Interface (applies to LAN, WLAN, WLC-tunnel)
%t	Routing tag
%m	MAC address of the client
%c	MAC address of the Public Spot gateway
%r	Remote IP (client)
%p	Local IP (Public Spot gateway)
%o	Original URL called by the client
%n	Device name of the Public Spot gateway
%e	Serial number of the Public Spot gateway
%l	Host name of the Public Spot gateway
%0-9	Inserts a single number between 0 and 9
%%	Inserts a single percent character

3. The hotspot gateway checks the user's credentials and, if applicable, it can contact further systems to charging to credit card, for example.
4. The hotspot gateway sends an XML file with the user data to the Public Spot's XML interface. The external hotspot gateway contacts the device with the Public Spot XML interface using the URL `http://<Device-URL>/xmlauth`.

   The Public Spot's XML interface analyses this file and initiates the corresponding actions. In the case of a login request, the XML interface inserts the user and the corresponding MAC address into the list of logged-in Public Spot users. In the case of a logout request, the XML interface removes the user from this list again. At the same time, the XML interface confirms the request by sending a corresponding XML file to the hotspot gateway.

   In order for the Public Spot to be able to process the instructions in the XML file, a special administrator must be set up on the device who has the function right "Public-Spot -XML-interface". This hotspot gateway logs in to the Public Spot with this admin account.

   While the user is logged in to the Public Spot, the XML interface and hotspot gateway can exchange status information about the current session in the form of XML files.

   If the user has exhausted his online quota, the hotspot gateway will send a stop command to the XML interface, and then the Public Spot locks further access for that user. The XML interface also confirms that the login is blocked by sending the corresponding XML file to the hotspot gateway.
5. If the additional use of a RADIUS server is enabled, the hotspot gateway authenticates a user at a RADIUS server.
6. The Public Spot sends relevant data to the RADIUS server throughout the session, for example to facilitate the accounting of the Public Spot usage. By default, the Public Spot uses its internal RADIUS server for this. If necessary, you can configure the device running the Public Spot to use an external RADIUS server.

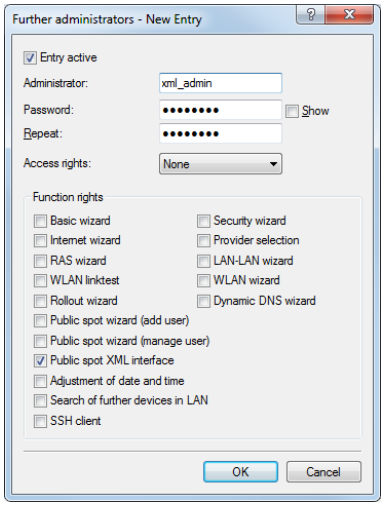
Communications between the Public Spot and a hotspot gateway with the use of XML is not standardized. Configure the hotspot gateway according to the instructions in the *Commands* section in order for the Public Spot and hotspot gateway exchange the XML messages in the required form. XML messages are exchanged invisibly without a graphical user interface. You can use tools such as *cURL* to test the exchange of messages.

1.5.2 Setting up the XML interface

The following section describes how to set up the XML interface.

1. Using **Management** > **Admin** > **Further administrators** you create a new administrator with the function right **Public Spot XML interface**.

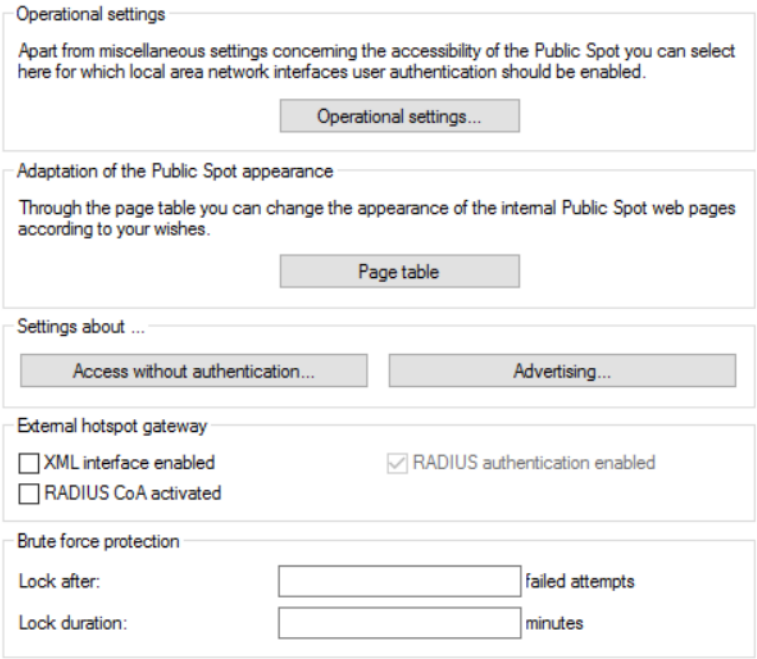
   This is the administrator account that the (external) gateway uses to send its XML requests to the Public Spot XML interface.



The new administrator should not have any further Public Spot function rights, since they represent a potential security risk in combination with the XML interface (e.g., if the communication between XML sender and device is unencrypted).

2. You enable the XML interface in **Public Spot** > **Server** in the section **External hotspot gateway** and RADIUS authentication.

   Incoming XML requests are forwarded by the Public Spot either to the internal RADIUS server or, if an external RADIUS server is used via a realm, to the external RADIUS server



3. In the section **Allow access without authentication** click on the button **Free Networks** and add a new network. Enter the **Name/IP address** of the login page. In **Netmask** enter `255.255.255.255`.

   When defined as a free network, the user has direct access to the login page of the gateway without having to login to the Public Spot first.

4. Configure the gateway so that it sends the user's session data to the Public Spot XML interface as an XML file. For questions about configuring the gateway, please refer to the applicable service provider.

1.5.3 Analyzing the XML interface using cURL

The following section describes the analysis of the XML interface with the open-source software cURL.

Client for URL, or cURL, is a command line application use for transferring files on a network without the use of a Web browser or FTP client. "cURL" is a component of many Linux distributions and is also available for other operating systems.

To analyze the XML interface using cURL, you need an administrator account with the function right "Public Spot XML interface" for the Public Spot.

1. First download cURL and install or unpack it.
2. Start cURL with the console command `curl -X POST -H "Content-Type:text/xml" -d @filename http://user:pass@myhost/xmlauth/`.

   The parameters have the following meaning:

filename

Path and name of the local XML file, e.g. the login request from the *examples*.

user

Username with the function right titled "Public Spot XML interface". The XML feature does not work without this authentication.

pass

User password.

myhost

IP address or DNS name of the device with the Public Spot XML interface

3. With Telnet you can use the command `trace # XML-Interface-PbSpot` to activate a trace that verifies whether XML requests were successful or error messages were received.

1.5.4 Commands

The XML interface can process three types of requests and responses:

- Login
- Logout
- Status

An XML file can contain several requests or answers.

Login

If the external gateway sends a "Login" request in an XML file, the Public Spot activates online access for the corresponding user. A "Login" request contains the attribute `COMMAND="RADIUS_LOGIN"`.

If the Public Spot does not use a RADIUS server, a "login" request prompts it to store the user and the associated MAC address directly in the internal Status table. As a result, the user is immediately authenticated in future, and there is no need to display a login page for entering the username and password.

When you operate a RADIUS server, a 'login' request can only be successfully processed if the login data of the corresponding user already exists on the RADIUS server.

The Web API in the Public Spot provides you with a convenient tool for creating new Public Spot users on the device's internal RADIUS server.

The XML interface can process the following XML elements in the **login request**:

`SUB_USER_NAME`

User name

`SUB_PASSWORD`

User password

`SUB_MAC_ADDR`

MAC address of the user device. Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

`VLAN_ID` (optional)

Custom VLAN ID assigned by the device to the Public Spot user upon login. After authentication by the RADIUS server, the individual VLAN ID overwrites a global VLAN ID that a user would otherwise obtain from the XML interface.

The value `0` disables use of a VLAN.

`SOURCE_VLAN` (optional, only in conjunction with authentication by RADIUS server)

The VLAN ID of the network from which a Public Spot user attempts to login (source VLAN). The Public Spot forwards the source VLAN in its access request to the internal or external RADIUS server. The Public Spot uses the RADIUS attribute 81 (**tunnel-private-group-ID**) together with the RADIUS attributes 64 (**tunnel-type**) and 65 (**tunnel-medium-type**). The RADIUS server uses the source VLAN to decide whether to accept or decline the access request from the Public Spot.

If the RADIUS server accepts the request, it returns the access-accept to the Public Spot along with the above-mentioned RADIUS attributes. The Public Spot then saves the source VLAN for the client and its station list and allows the user to access the Public Spot network.

Use the source VLAN in conjunction with the setup parameter *2.24.47*. This prevents Public Spot users in VLAN-separated Public Spot networks/SSIDs from authenticating once at the RADIUS server and then accessing all of the managed Public Spot networks/SSIDs.

The `SOURCE_VLAN` should not be confused with the `VLAN_ID`. The `VLAN_ID` is not sent to the RADIUS server. However, the Public Spot uses it to assign a VLAN ID provided by the gateway to a successfully authenticated user.

`PROVIDER` (occasionally required)

Name of the RADIUS server used by the Public Spot for user authentication and accounting. If you do not specify a RADIUS server, the Public Spot uses the server configured globally for the module.

This XML element is mandatory if you

- have configured multiple RADIUS servers for the Public Spot module.
- want to use the XML interface without RADIUS authentication but with RADIUS accounting.

Specifying this XML element is otherwise optional.

The referenced RADIUS server must be present in the configuration.

`TXRATELIMIT` (optional)

Maximum bandwidth (in kbps) provided to the Public Spot user for the uplink.

`RXRATELIMIT` (optional)

Maximum bandwidth (in kbps) provided to the Public Spot user for the downlink.

`SECONDSEXPIRE` (optional)

The maximum online time for a user account in seconds. The user can use this duration of access time until a relative or absolute expiry time (if set) is reached.

The value `0` switches off the monitoring of the time budget.

`TRAFFICEXPIRE` (optional)

The maximum data volume for a user account. The user can use this data volume until a relative or absolute expiry time (if set) is reached.

The following entries are allowed:

- `k` or `K`: Specified in kilobytes (kB), e.g. `<TRAFFICEXPIRE>1000k</TRAFFICEXPIRE>`.
- `m` or `M`: Specified in megabytes (MB), e.g. `<TRAFFICEXPIRE>100m</TRAFFICEXPIRE>`.
- `g` or `G`: Specified in gigabytes (GB), e.g. `<TRAFFICEXPIRE>1g</TRAFFICEXPIRE>`.

Without a unit, the specification corresponds to a value in bytes (B).

The value `0` switches off the monitoring of the data volume.

The XML interface then sends the gateway a "Login" response, which can contain the following XML elements:

SUB_USER_NAME

User name

SUB_STATUS

The current user status. The following values are possible:

- `RADIUS_LOGIN_ACCEPT`: Login successful
- `RADIUS_LOGIN_REJECT`: Login rejected

SUB_MAC_ADDR

MAC address of the user device. Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

PROVIDER

Name of the RADIUS server to be used for this user.

Some examples of XML files are given below:

Login request

The external gateway sends the data for the start of a session to the Public Spot:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_LOGIN">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_PASSWORD>5juchb</SUB_PASSWORD>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
    <PROVIDER>DEFAULT</PROVIDER>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

The Public Spot enables 'user2350' in the internal Status table.

Login response:

The XML interface sends a confirmation about the start of a session to the external gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
 <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
    <SUB_STATUS>RADIUS_LOGIN_ACCEPT</SUB_STATUS>
    <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <TXRATELIMIT>0</TXRATELIMIT>
```

```
    <RXRATELIMIT>0</RXRATELIMIT>
    <SECONDSEXPIRE>0</SECONDSEXPIRE>
    <TRAFFICEXPIRE>0</TRAFFICEXPIRE>
    <ACCOUNTCYCLE>0</ACCOUNTCYCLE>
    <IDLETIMEOUT>0</IDLETIMEOUT>
    </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

CoA

If a Public Spot user has to authenticate only and no further changes are required throughout the login, then the parameter `RADIUS_LOGIN` will meet your needs. On the other hand, if you need to change the attributes of an ongoing session for a Public Spot user, you have the option of using `RADIUS_CoA`. To implement a change, your external hotspot gateway sends a `RADIUS-CoA-Request` to the Public Spot, which directly transfers the changes in it to the **Station table** under **Status** > **Public-Spot**.

One application for CoA messages is the automatic throttling of bandwidth: If a Public Spot user has consumed his/her volume budget, an external hotspot gateway is able to throttle the user's bandwidth by evaluating the accounting data and sending a CoA message to the Public Spot.

The XML messages for negotiations between the hotspot gateway and the Public Spot appear as follows:

RADIUS-CoA-Request

The external gateway sends the data with the session change to the Public Spot. The Public Spot then changes the session data in the station table for the authenticated user 'user2350'.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_COA_REQUEST">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_PASSWORD>5juchb</SUB_PASSWORD>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
    <TXRATELIMIT>100</TXRATELIMIT>
    <RXRATELIMIT>100</RXRATELIMIT>
    <SECONDSEXPIRE>3600</SECONDSEXPIRE>
    <TRAFFICEXPIRE>10000000</TRAFFICEXPIRE>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

In the example above, the user is assigned a session duration of 3,600 seconds, a transferable data volume of 10,000,000 bytes, and a transmit and receive bandwidth of 100 kbps.

RADIUS-CoA-Response:

The XML interface sens a confirmation to the external hotspot gateway that the session data was changed:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
 <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
    <SUB_STATUS>RADIUS_COA_ACCEPT</SUB_STATUS>
    <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <TXRATELIMIT>100</TXRATELIMIT>
    <RXRATELIMIT>100</RXRATELIMIT>
    <SECONDSEXPIRE>3600</SECONDSEXPIRE>
    <TRAFFICEXPIRE>10000000</TRAFFICEXPIRE>
    <ACCOUNTCYCLE>0</ACCOUNTCYCLE>
    <IDLETIMEOUT>0</IDLETIMEOUT>
    </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

In case of throttling, the change to the user session always affects the quota that is still available to the user. For instance, if the user was logged on for one hour already, then a change of the time quota to six hours means that just five hours remain. If the time quota is less than the time the user is already logged on, the Public Spot logs out the user and sends a logout message to the hotspot gateway.

Logout

If the external gateway sends a "Logout" request in an XML file, the Public Spot blocks the corresponding user's online access. A "Logout" request contains the attribute `COMMAND="RADIUS_LOGOUT"`.

The XML interface can process the following XML elements for a request:

SUB_USER_NAME

User name

If the device receives this request and the Public Spot module discovers that this user is online with the corresponding MAC, then the Public Spot logs out this user.

SUB_MAC_ADDR

MAC address of the user device. Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

TERMINATION_CAUSE

Reason for the user to log off

The XML interface then sends the gateway a "Logout" response, which can contain the following XML elements:

SUB_USER_NAME

User name

SUB_STATUS

The current user status. The following values are possible:

- `RADIUS_LOGOUT_DONE`: Logout successful
- `RADIUS_LOGOUT_REJECT`: Logout rejected

SUB_MAC_ADDR

MAC address of the user device. Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

TERMINATION_CAUSE

Reason for blocking access

Some examples of XML files are given below:

Logout request

The external gateway sends the command for ending a session to the Public Spot:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_LOGOUT">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
    <TERMINATION_CAUSE>Check-Out</TERMINATION_CAUSE>
```

```
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Logout response:

The XML interface sends a confirmation about the end of a session to the external gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
   <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
     <SUB_STATUS>RADIUS_LOGOUT_DONE</SUB_STATUS>
     <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
     <SUB_USER_NAME>user2350</SUB_USER_NAME>
     <TERMINATION_CAUSE>User logout request</TERMINATION_CAUSE>
    </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Status

The external gateway queries the current status of a user from the Public Spot with a "Status" request. A "Status" request contains the attribute `COMMAND="RADIUS_Status"`.

The XML interface can process the following XML elements for a request:

`SUB_USER_NAME`

User name

`SUB_MAC_ADDR`

MAC address of the user device. Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

The XML interface then sends the gateway a "Status" response, which can contain the following XML elements:

`SUB_USER_NAME`

User name

`SUB_MAC_ADDR`

MAC address of the user device. Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

`SUB_STATUS`

The current user status. The following values are possible:

- `RADIUS_STATUS_DONE`: Status request successful
- `RADIUS_STATUS_REJECT`: Status request rejected, e.g. unknown user or MAC address

`SESSION_TXBYTES`

Current sent data volume

SESSION_RXBYTES

Current received data volume

SESSION_TXPACKETS

Number of data packets sent so far

SESSION_RXPACKETS

Number of data packets received so far

SESSION_STATE

Current status of the session

SESSION_ACTUAL_TIME

Current time

Some examples of XML files are given below:

Status request

The external gateway sends the command for a status request to the Public Spot:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_STATUS">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Status response:

The XML interface sends a status message to the external gateway:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
   <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
     <SUB_STATUS>RADIUS_STATUS_DONE</SUB_STATUS>
     <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
     <SUB_USER_NAME>user2350</SUB_USER_NAME>
     <SESSION_ID>2</SESSION_ID>
     <SESSION_TXBYTES>0</SESSION_TXBYTES>
     <SESSION_RXBYTES>0</SESSION_RXBYTES>
     <SESSION_TXPACKETS>0</SESSION_TXPACKETS>
     <SESSION_RXPACKETS>0</SESSION_RXPACKETS>
     <SESSION_STATE>Authenticated</SESSION_STATE>
     <SESSION_ACTUAL_TIME>0</SESSION_ACTUAL_TIME>
   </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

2 Appendix

2.1 Commonly transmitted RADIUS attributes

The RADIUS client module was implemented on the basis of RFCs no. 2865 and no. 2866.

These specifications define various attributes, some of which are an absolute necessity and some of which are optional. The following overview shows which attributes are transmitted/processed in messages between RADIUS servers and base stations.

2.1.1 Messages to and from the authentication server

Transferred attributes

As previously mentioned, your device transmits far more than just the username and password in a RADIUS request. RADIUS servers might choose to completely ignore these additional attributes, or only use a subset of these attributes. Many of these attributes are used for access to the server using dial-in, and are defined as standard attributes in the RADIUS RFCs. However, some important information for hotspot operation can not be represented with standard attributes. These additional attributes are manufacturer-specific with the manufacturer code 2356 (LANCOM Systems GmbH).

Table 10: Overview of the RADIUS attributes transmitted by the device to the authentication server

ID :	Name	Meaning	Possible values in LCOS
1	User name	The name entered by the user.	
2	User-Password	The password entered by the user.	
4	NAS-IP-Address	IP address of your device	<IPv4 address of the device>
6	Service-Type	Type of service that the user requested. The value “1” stands for Login.	
8	Framed-IP-Address	Specifies the IP address that is assigned to the client.	<IP address of the client>
30	Called-Station-Id	MAC address of your device	<nn:nn:nn:nn:nn:nn>
31	Calling-Station-Id	MAC address of the client The address is given byte-wise in hexadecimal notation with separators.	<nn:nn:nn:nn:nn:nn>
32	NAS identifier	Name of your device, if configured.	<Device-Name>
61	NAS-Port-Type	Type of physical port over which a user had requested authentication.	› **ID 19** denotes clients from WLAN. › **ID 15** denotes clients from Ethernet.
87	NAS-Port-Id	Description of the interface over which the client is connected to your device. This may be a physical and a logical interface. ⓘ Consider that more than one client may be connected to one interface at a time, so that, unlike dial-in servers, port numbers are not unique for clients.	For example › LAN-1 › WLAN-1-5 › WLC-TUNNEL-27

Processed attributes

Your device evaluates the authentication response of a RADIUS server for attributes that it may possibly process further. Most attributes however only have a meaning if the authentication response was positive, so that they influence the subsequent session:

Table 11: Overview of the supported RADIUS attributes

ID :	Name	Meaning	Possible values in LCOS
18	Reply-Message	An arbitrary string from the RADIUS server that may transport either a login failure reason or a user welcome message. This message may be integrated into user-defined start or error pages via the `SEVERMSG` element.	
25	Class	An arbitrary octet string that may contain data provided by the authentication/accounting backend. Whenever the device sends RADIUS accounting requests, they will contain this attribute as-is. Within an authentication response, this attribute can occur multiple times in order, for example, to transmit a string that is longer than 255 bytes. The device processes all occurrences in accounting requests in the order they appeared in the authentication response.	
26	Vendor 2356, Id 1 LCS-Traffic-Limit	Defines the data volume in bytes after which the device automatically ends the session. This value is useful for volume-limited accounts. If this attribute is missing in the authentication response, it is assumed that no volume limit applies. A traffic limit of 0 is interpreted as an account which is principally valid, however with a used-up volume budget. The device does not start a session in this case.	
26	Vendor 2356, Id 3 LCS-Redirection-URL	This can contain any URL that is offered as an additional link on the start page. This can be the start page of the user or a page with additional information about the user account.	
26	Vendor 2356, Id 5 LCS-Account-End	Defines an absolute point in time (measured in seconds since January 1, 1970 0:00:00) after which the account becomes invalid. If this attribute is missing, an unlimited account is assumed. The device does not start a session if its internal clock has not been set, or the given point in time is in the past.	
26	Vendor 2356, Id 7 LCS-Public-Spot-Username	Contains the name of a Public Spot user for auto-login. Auto-login refers to the table of MAC authenticated users who are automatically assigned usernames by the server.	
26	Vendor 2356, Id 8 LCS-TxRateLimit	Defines the maximum downstream rate in kbps. This restriction may be combined with the corresponding Public Spot function.	
26	Vendor 2356, Id 9 LCS-RxRateLimit	Defines the maximum upstream rate in kbps. This restriction may be combined with the corresponding Public Spot function.	
26	Vendor 2356, Id 13 LCS-Advertisement-URL	Specifies a comma-separated list of advertisement URLs.	
26	Vendor 2356, Id 14 LCS-Advertisement-Interval	Specifies the interval in minutes after which the Public Spot reroutes a user to an advertisement URL. With an interval of 0 forwarding occurs directly after login.	
27	Session-Timeout	Defines an optional maximum duration of the session, measured in seconds. If this attribute is missing in the response, an unlimited account is assumed. A Session	

ID :	Name	Meaning	Possible values in LCOS
		timeout of zero seconds is interpreted as an account which is principally valid, however with a used-up time budget. The device does not start a session in this case.	
28	Idle timeout	Defines a time period in seconds after which the device will terminate the session if no packets were received from the client. This value may possibly overwrite the idle timeout that is defined locally under **Public Spot** > **Server** > **Idle timeout**.	
64	Tunnel-Type	Defines the tunneling protocol which will be used for the session.	
65	Tunnel-Medium-Type	Defines the transport medium over which the tunneled session will be established.	
81	Tunnel-Private-Group-ID	Defines the group ID if the session is tunneled.	
85	Acct-Interim-Interval	Defines the amount of time between subsequent RADIUS accounting updates. This value is only evaluated if the RADIUS client does not have a local accounting interval defined, i.e. if you have not set an **Accounting update cycle** for the Public Spot module.	

Note that the LCS-Account-End and Session-Timeout attributes are mutually exclusive, and it therefore does not make sense to include both in the response. If both attributes are included in a response, the attribute that appears as the last one in the attribute list will define the session's time limit.

2.1.2 Messages to/from the accounting server

Transferred attributes

The set of RADIUS attributes transmitted to a RADIUS server in an accounting request is similar to the set of attributes transmitted in an authentication request. However, additional attributes specific to accounting will be added. The following attributes are present in all RADIUS accounting requests:

Overview of the RADIUS attributes transmitted by the device to the accounting server

1

User name

Name of the account that was used for authentication.

4

NAS-IP-Address

IP address of your device

8

Framed-IP-Address

IP address that was assigned to the client

25

Class

All class attributes that the RADIUS authentication server sent in its authentication response.

30

Called-Station-Id

MAC address of your device

31

Calling-Station-Id

MAC address of the client The address is given byte-wise in hexadecimal notation with separators (nn:nn:nn:nn:nn:nn).

32

NAS identifier

Name of your device, if configured.

40

Acct-Status-Type

Request type which signals the start or stop of accounting, or an interim update. Please refer to the section *Request types* for further information.

44

Acct-Session-Id

A series of characters that uniquely identify the client. It consists of the MAC address of the network adapter, the login timestamp (measured in seconds since January 1, 1970 0:00:00), and the session counter that your device manages locally.

61

NAS-Port-Type

Type of physical port over which a user had requested authentication.

- **ID 19** denotes clients from WLAN
- **ID 15** denotes clients from Ethernet

87

NAS-Port-Id

Description of the interface over which the client is connected to your device. This can be a physical as well as a logical interface, such as `LAN-1`, `WLAN-1-5` or `WLC-TUNNEL-27`.

Consider that more than one client may be connected to one interface at a time, so that, unlike dial-in servers, port numbers are not unique for clients.

In the case of an accounting stop request or an interim update, the request contains the following additional attribute:

42

Acct-Input-Octets

The sum of all data bytes received from the client in this session, modulo 2^{32}.

43

Acct-Output-Octets

The sum of all data bytes sent to the client in this session, modulo 2^{32}.

46

Acct-Session-Time

The total duration of the client's session in seconds.

If the session was ended due to an idle timeout, this value is reduced by the idle time.

47

Acct-Input-Packets

The number of data packets that your device received from the client during the session.

48

Acct-Output-Packets

The number of data packets that your device sent to the client during the session.

49

Acct-Terminate-Cause

The reason for termination or the end of the accounting session. This is sent if **Acct-Status-Type** has the value `Start` or `Stop`.

52

Acct-Input-Gigawords

The upper 32 bits of the sum of all data bytes received from the client during this session.

53

Acct-Output-Gigawords

The upper 32 bits of the sum of all data bytes sent to the client during this session.

55

Event-Timestamp

The elapsed time since this accounting request was submitted by the device, measured in seconds since January 1, 1970 0:00:00. This attribute is only present if your device's real time clock contains a valid value.

Note that the RADIUS accounting only starts accounting after a client successfully logs in, i.e. the time needed for authentication is not recorded. Using *Traffic-Limit-Option* you can limit the data traffic during the authentication phase. The final accounting stop request also contains the termination cause attribute (49). An overview of these attributes can be found in the LANCOM "Public Spot: Implementation Guide", available from *www.lancom-systems.com*.

Processed attributes

Your device currently does not process any attributes in responses sent by a RADIUS accounting server.

2.2 RADIUS attributes transmitted via WISPr

If you enable WISPr and you use an external RADIUS server, the Public Spot transmits the attributes (access request):

- **Location ID**
- **Location name**
- **Logoff URL**

These attributes are subset of the values configured in the previous section. The provider or roaming broker can use them to identify the location of the client for accounting purposes. Vendor Specific Attributes (VSA) are used with the IANA Private Enterprise Number (PEN) 14122.

The Public Spot processes the attributes (access accept) from an external RADIUS server:

- **Redirection URL**: URL to which a client should be redirected after login. This function is not supported by all smart clients.

- **Bandwidth max up**: Maximum uplink bandwidth available to the client.
- **Bandwidth max down**: Maximum downlink bandwidth available to the client.
- **Session terminate time**: Time when the client should be automatically de-authenticated. According to ISO 8601, the format is `YYYY-MM-DDThh:mm:ssTZD`. If "TZD" is not entered, the client is de-authenticated according to the local time on the Public Spot.
- **Session terminate end of day**: The value of this attribute can be either 0 or 1. It indicates whether the client is de-authenticated on the Public Spot at the end of the accounting day.

For accounting purposes, the Public Spot uses the following attributes:

- **Location ID**
- **Location name**

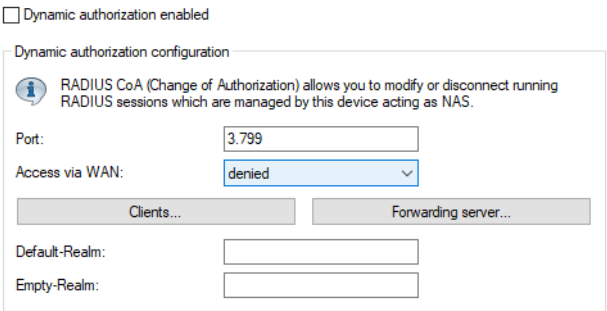
2.3 Dynamic authorization by RADIUS CoA (Change of Authorization)

Dynamic authorization provides the capability to modify current RADIUS sessions. A modification is initiated when the CoA client sends a CoA message to the NAS. This message contains the identifying characteristics for the session to be modified, the attributes to be modified, and their new values.

Another option is to disconnect the current session. This is done with a disconnect message (DM) sent to the NAS, whereupon the NAS terminates the connection.

2.3.1 Configuring dynamic authorization with LANconfig

In order to configure dynamic authorization (CoA) with LANconfig, navigate to **RADIUS** > **Dyn. Authorization**.



Dynamic authorization enabled

Activate or deactivate dynamic authorization here.

Port

Contains the default port where CoA messages are received.

Access via WAN

This entry specifies whether messages are accepted from the WAN, via VPN only, or prohibited.

Clients

Enter all of the CoA clients here that are permitted to send messages to the NAS.

Forwarding server

To forward CoA messages, the forwarding servers are specified here.

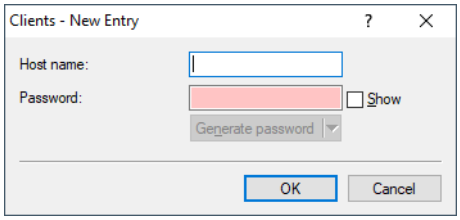
Default realm

This realm is used if the supplied username uses an unknown realm that is not in the list of forwarding servers.

Empty realm

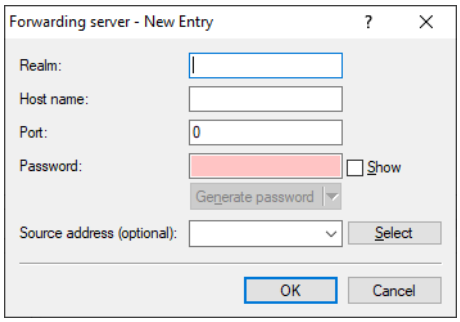
This realm is used when the specified username does not contain a realm.

To add CoA clients for dynamic authorization, click the button **Clients** and add a new entry to the table.



Enter a host name for the client and set a password for the client to access the NAS.

To add new forwarding servers for dynamic authorization, click the button **Forwarding server** and add a new entry to the table.



Realm

Here you enter the realm used by the RADIUS server to identify the forwarding destination.

If applicable, enter any existing forwarding servers that are specified under **RADIUS** > **Server** > **Extended configuration** > **Forwarding** > **Forwarding server**.

Host name

Specify the host name of the forwarding server.

Port

Specify the server port used to forward the requests.

Password

Set a password that is required by the client to access the RADIUS server.

Source address (optional)

Optionally, specify a source address.

Specify which logical WLAN interfaces should use dynamic authorization. You enable or disable them under **Wireless LAN** > **General** > **Logical WLAN settings** > **Network** with the checkbox **RADIUS CoA activated** for the appropriate interface.

2.4 Importing and exporting RADIUS user data by CSV file

The internal RADIUS server is basically a user database. Here we describe an easy way to import and export the user entries. This is particularly relevant for Public Spots, where users are generated in large numbers by an external system. For LEPS-MAC, too, this is an easy way to import the data. The format used for the data exchange is csv (comma separated values), whereby a semicolon serves as the default separator of the individual data fields.

2.4.1 Exporting RADIUS user data by CSV file

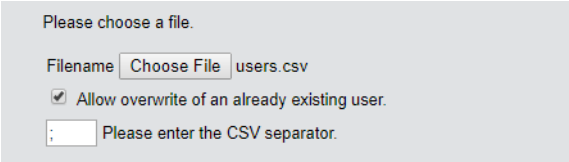
To export the user data of the RADIUS server via WEBconfig, proceed as follows.

Click on **Extras** > **Export RADIUS users**.<draft-comment author="mkoser">Englisch: Extras > Export RADIUS users</draft-comment>
The user data is downloaded as the file `users.csv`. The semicolon is the separator; the first row contains the identifiers of the database fields.

2.4.2 Importing RADIUS user data by CSV file

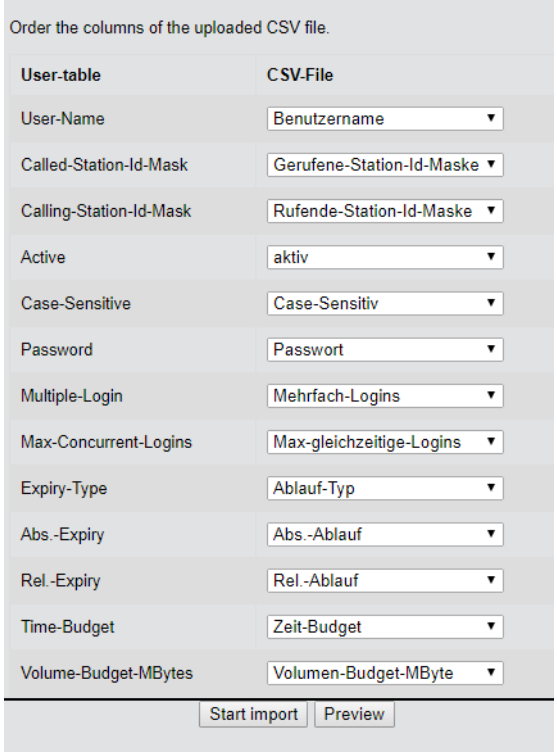
To import the user data of the RADIUS server via WEBconfig, proceed as follows.

1. Generate a file with the required header for the user data by performing an export of the user data as described in *Exporting RADIUS user data by CSV file* on page 171.
2. Create a CSV import file with a header containing the correct database field identifiers determined in the previous step. The import file does not have to contain all the columns.
3. Navigate to the menu item **Extras** > **Import RADIUS users**.
4. Use **Choose file** to select the CSV file to be imported.
5. Enter the CSV separator. By default this is already preset to ";".



6. Start the upload.

7. Now check that the columns detected in the CSV file are correctly aligned with the supported columns. You can adjust the alignment in this dialog. No adjustment should be necessary if you used the column names from the previously exported CSV file.



8. Click **Start import** to complete the process and accept the user data.

2.5 Expert settings for the PMS interface

In addition to the settings that LANconfig provides for the PMS interface, you have the possibility of configuring additional parameters in the setup menu. On one hand, these parameters encompass values that the device needs for internal synchronization with your PMS system, and that are normally not modified. On the other hand, you also find extended settings in the setup menu that you can use to increase the performance scope of the PMS interface, for example, by offering free access to an otherwise charged Public Spot access for your guests with VIP status.

The following pages offer you an overview of all parameters for the PMS interface that are not configured over LANconfig.

2.5.1 Accounting

In this menu you configure the transfer of accounting information from your device to your PMS.

SNMP ID:

2.64.10

Console path:

Setup > **PMS-Interface**

Cleanup-Accounting-Table-Period

Using this entry you configure the interval that the device uses to clean up expired sessions from the internal accounting table in the status menu.

SNMP ID:

2.64.10.3

Console path:

Setup > **PMS-Interface** > **Accounting**

Possible values:

0 … 4294967295 Seconds

Default:

60

Special values:

0

The value 0 disables the automatic cleanup.

Save-to-Flashrom-Period

Using this entry you configure the interval that the device uses to store collected accounting information to the internal flash ROM.

Please note that frequent writing operations to this memory will reduce the lifetime of your device.

SNMP ID:

2.64.10.2

Console path:

Setup > **PMS-Interface** > **Accounting**

Possible values:

0 … 4294967295 Seconds

Default:

15

Special values:

0

The value 0 deactivates the function.

Update-Accounting-Table-Period

Using this entry you configure the interval that the device uses to update the internal accounting table in the status menu.

SNMP ID:

2.64.10.4

Console path:

Setup > **PMS-Interface** > **Accounting**

Possible values:

0 … 4294967295 Seconds

Default:

15

Special values:

0

If the value is 0, the update is disabled and the status table does not display any values.

2.5.2 Login form

In this menu you make specific settings for the PMS for the login/portal pages which are displayed to your guests in case of unauthorized access attempts on the hotspot.

SNMP ID:

2.64.11

Console path:

Setup > **PMS-Interface**

Free-VIP-Status

In this table, you locally manage the VIP categories from your PMS.

SNMP ID:

2.64.11.6

Console path:

Setup > **PMS-Interface** > **Login-Form**

Status

Enter the VIP category from your PMS for the members that you want to provide with free Internet access.

For example, if you set up three VIP statuses (VIP1, VIP2, VIP3) for your PMS server, but you only want to offer hotel guests in category VIP2 free Internet access, enter the corresponding ID here.

SNMP ID:

2.64.11.6.1

Console path:

Setup > **PMS-Interface** > **Login-Form** > **Free-VIP-Status**

Possible values:

Max. 20 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.` ` `

Default:

empty

Fidelio-Free-Additional-check

Select the additional ID that a hotel guest uses – in addition to their username and room number – to authenticate on the Public Spot if you offer free Internet access. If you select `No-Check`, the device does not check for an additional ID.

SNMP ID:

2.64.11.3

Console path:

Setup > **PMS-Interface** > **Login-Form**

Possible values:

None
Reservation number
Arrival date
Departure date
First name
Profile number

Default:

None

Fidelio-Free-VIP-Additional-check

Select the additional ID used by a VIP – in addition to their username and room number – to authenticate on the Public Spot if you offer your VIPs free Internet access. If you select `No-Check`, the device does not check for an additional ID.

SNMP ID:

2.64.11.5

Console path:

Setup > **PMS-Interface** > **Login-Form**

Possible values:

None
Reservation number
Arrival date
Departure date
First name
Profile number

Default:

None

Fidelio-Charge-Additional-check

Select the additional ID used by a hotel guest – in addition to their username and room number – to authenticate on the Public Spot if you offer fee-based Internet access. If you select `No-Check`, the device does not check for an additional ID.

SNMP ID:

2.64.11.4

Console path:

Setup > **PMS-Interface** > **Login-Form**

Possible values:

None
Reservation number
Arrival date
Departure date
First name
Profile number

Default:

Reservation number

PMS-Login-Form

Choose the login page to be displayed by the portal page for your PMS interface.

SNMP ID:

2.64.11.2

Console path:

Setup > **PMS-Interface** > **Login-Form**

Possible values:

Free-of-charge
Choose this option if you offer your hotel guests free Internet access. Your hotel guests will still be required to authenticate on the hotspot on the portal page with their username, room number and, if required, an additional ID in order to prevent access to the Internet by unauthorized users.

charge
Choose this option if you offer your hotel guests fee-based Internet access. Your hotel guests will be required to authenticate at the hotspot on the portal page with their username and room number, and also to select a rate.

free-VIP
Select this setting, if you want to offer your otherwise fee-based Internet access free of charge to VIPs. Although your VIPs see the login screen for fee-based access, they will not be billed any fees.

Default:

Free-of-charge

PublicSpot-Login-Form

Enable or disable whether the portal page displays the Public Spot's own login screen. If you disable this setting, Public Spot users that use a combination of username and password as credentials (e.g., predefined or users with vouchers) can no longer login to the device.

SNMP ID:

2.64.11.1

Console path:

Setup > **PMS-Interface** > **Login-Form**

Possible values:

No
Yes

Default:

No

2.5.3 Guest-name-case-sensitive

Enable or disable whether the device checks the last name for capitalization (case sensitively) against the name of the guest in the PMS database during login. If this setting is enabled, the guest's Public Spot access is rejected if the spelling and capitalization of his name does not match that transferred by the hotel.

SNMP ID:

2.64.12

Console path:

Setup > **PMS-Interface**

Possible values:

No
Yes

Default:

Yes

2.5.4 Separator

Using this entry you configure the separator that your PMS uses to transfer data records to an API. The Micros Fidelio specification, e.g., uses the pipe symbol by default (|, hex 7C).

You should not change this value if at all possible. An incorrect separator can lead to your PMS being unable to read the transmitted data records, and the PMS interface not working!

SNMP ID:

2.64.6

Console path:

Setup > **PMS-Interface**

Possible values:

Max. 1 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.  `

Default:

|

2.5.5 Charset

Choose the character used by the PMS to transmit your guests' surnames to the device.

SNMP ID:

2.64.7

Console path:

Setup > **PMS-Interface**

Possible values:

CP850
W1252

Default:

CP850

2.6 Sending and receiving SMS text messages

If your device has a 3G/4G WWAN module, is capable of sending and receiving text messages via the Short Message Service (SMS).

In this case the SMS function is mainly used as a messaging and function-enhancing interface for the internal LCOS modules, but also for external instances such as routers, management solutions, accounting systems, and so on. You as a user also have the option to send SMS text messages using the corresponding *function in LANmonitor* or the `smssend` command at the command prompt. LANmonitor also provides you with convenient functions for *managing* sent and received messages.

The sending and receiving of SMS text messages must also be included in the SIM card's contract.

2.6.1 Receiving SMS text messages

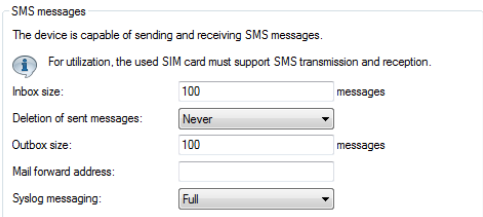
Your device uses the ETSI standard TS 127.005 to receive and request these SMS text messages, to store them and, if required, to log the receipt of an SMS to the SYSLOG. The entry in the SYSLOG counts as a "notice" to inform you about any important messages, such as a notification from an external instance, for example. An instance might be the accounting system of your provider:

If you connect to the Internet via a 3G/4G WWAN module and the contract with your Internet provider includes a volume limit, then depending on the contract your provider will throttle or stop data transfer once this volume limit has been reached. In countries with the appropriate legislation, this also applies when a charging limit for data roaming has been reached. Before the data transfer is throttled or stopped, many providers send an SMS text message informing the customer that the volume limit has been reached. With the corresponding notification settings in the SYSLOG and/or via e-mail, the device can immediately inform you about the reception of the SMS, so that you can respond promptly.

2.6.2 Basic configuration of the SMS module

The following steps show you the basic configuration of the SMS module in a 3G/4G WWAN-enabled device.

1. Start LANconfig and open the configuration dialog for the device.
2. Navigate to the menu item **Log & trace** > **SMS messages**.



3. Under **Inbox size** you set the maximum number of text messages stored in the device inbox.

If the preset number is exceeded, the oldest message will be deleted. In this case there is **no** SYSLOG entry. The value 0 disables the limit, i.e. an unlimited number of messages will be stored.

4. The item **Deletion of sent messages** decides how the device handles sent text messages.
   - **Immediately**: Sent messages are not saved.
   - **Never**: Sent messages are saved permanently.
5. Under **Outbox size** you set the maximum number of text messages stored in the device outbox.
   If the preset number is exceeded, the oldest message will be deleted. In this case there is **no** SYSLOG entry. The value 0 disables the limit, i.e. an unlimited number of messages will be stored.
6. Under **Syslog messaging** you specify if and how the arrival of text messages is logged to the SYSLOG.
   - **No**: Incoming text messages are not logged to SYSLOG.
   - **Only sender/no content**: The arrival of a text message is recorded to the SYSLOG together with the sender's phone number.
   - **Full**: The arrival of a text message is recorded to the SYSLOG together with the sender's phone number and the message in full.
7. Optional: Under **Mail forwarding address** you specify the e-mail address to which the device is to forward the incoming SMS text messages.

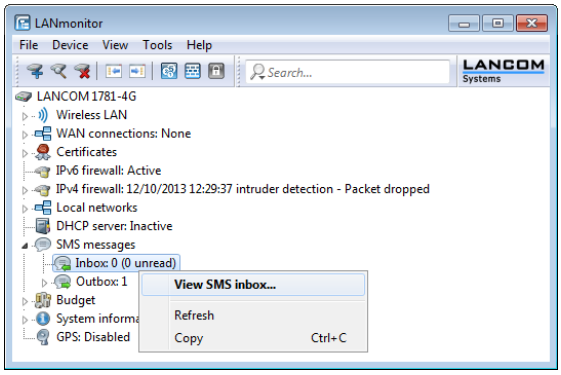
   E-mail routing will only work if a valid SMTP account is configured in the device.
8. Now write the configuration back to the device.

That's it! This concludes the basic configuration of the SMS module.

2.6.3 Managing SMS text messages with LANmonitor

The following section explains shows how you can use LANmonitor to read and delete text messages sent or received by a 3G/4G WWAN-enabled device.

1. Start LANmonitor and navigate to the menu tree of the respective device under **SMS messages** > **Inbox** or **Outbox**.
   If there are already text messages on the device, LANmonitor displays the last five received messages under **Inbox** and the last five sent messages under **Outbox**.
2. Open the context menu on the entry and choose **Show SMS inbox** or **Show SMS outbox**.



LANmonitor then displays a window listing all of the sent and received text messages and their status. In the **Inbox** you have the option to delete single or multiple selected messages, or to mark them as read/unread; the Status shows whether they have been read or not (**New** or **Read**). In the **Outbox**, the messages can only be deleted; the Status shows their send status (**Sent** or **Unsent**).

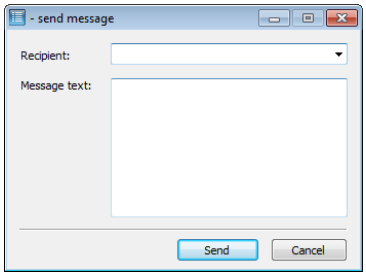
You can manage these messages by using the context menu. To delete all messages in the inbox or outbox, go to the menu bar under **Messages** and select the appropriate action.

You can easily toggle between the inbox and outbox by selecting **View** from the menu bar and selecting the desired option.

2.6.4 Sending SMS text messages with LANmonitor

The following section explains how you can use LANmonitor to send SMS text messages via a 3G/4G WWAN-enabled device.

1. Start LANmonitor and navigate to the menu tree of the respective device under **SMS messages**.
2. Open the context menu on the entry and select **Send message**.
3. In the Editor window that opens, enter the phone number of the recipient and the message content to be sent. The number of characters is limited to one SMS text message (max. 160 characters). For an overview of available characters, see the section *Character set for sending SMS* on page 182.



4. Click **Send** to send the message via the internal SMS module.

2.6.5 URL placeholder for sending SMS

You have the option of addressing the SMS module as an interface by means of a URL. By integrating predefined placeholders (parameters) into the URL, you can use the device to send SMS text messages by means of an HTTP(S) call. This makes LANCOM cellular routers ideal for use as an SMS gateway.

SMS transmission is suitable for installations with a maximum throughput of 10 SMS per minute.

You use your access credentials to authenticate at the device; just how these are Integrated into the URL is determined by your browser's requirements. The typical notation is `Username:Password@Host`.

Depending on the use case (for example, SMS gateway), we recommended that you create an administrator without access rights (**None**) and with just one function right, **Send SMS**.

Not all Web browsers support the transmission of credentials via the URL. This includes current versions of the Microsoft Internet Explorer, among others. In this case you should use another browser to send SMS via the URL.

The URL call uses the syntax:

```
(http|https)://<User>:<Password>@<Host>/sms/?<Param1>=<Value1>&…&oldauth
```

The parameter `oldauth` is **vital**, otherwise none of the available browsers will send the access credentials to the device. In addition, the following placeholders are defined:

`DestinationAddress`

Phone number to which the device should send the SMS. The same conventions apply as for normal telephone calls. Specify the parameters as follows:

```
&DestinationAddress=01511234567
&DestinationAddress=00491511234567
```

Content

Content of the text message. The number of characters is limited to one SMS text message (max. 160 characters). For an overview of available characters, see the section *Character set for sending SMS* on page 182.

Spaces and other special characters to be included into an SMS must be sent to the device in the URL-encoded form. For example, spaces are encoded with `%20` and full stops with `%2E`. Specify the parameters as follows:

```
&Content=This%20is%20a%20message%2E
```

Learn more about this topic on the Internet under the keyword "URL encoding" and also at *www.w3schools.com*.

Some browsers perform the URL encoding automatically. Despite this, we recommend that you encode the content yourself to ensure that all of the characters are converted correctly.

2.6.6 Character set for sending SMS

An SMS can contain a maximum of 160 characters (each of 7 bits = 1,120 bits). These are made up of the GSM basic character set (total of 128 characters) as well as selected characters from the extended GSM character set. Although the extended character set allows the use of some additional characters, these take up twice the space and correspondingly reduce the maximum number of characters that the SMS can contain. Characters not implemented in the SMS module are ignored by the device.

The following characters are defined in the **GSM basic character set**:

@	Δ	SP	0	¡	P	¿	p
£	_	!	1	A	Q	a	q
$	Φ	"	2	B	R	b	r
¥	Γ	#	3	C	S	c	s
è	Λ	¤	4	D	T	d	t
é	Ω	%	5	E	U	e	u
ù	Π	&	6	F	V	f	v
ì	Ψ	'	7	G	W	g	w
ò	Σ	(	8	H	X	h	x
Ç	Θ	)	9	I	Y	i	y
LF	Ξ	*	:	J	Z	j	z
Ø	ESC	+	;	K	Ä	k	ä
ø	Æ	,	<	L	Ö	l	ö
CR	æ	-	=	M	Ñ	m	ñ
Å	ß	.	>	N	Ü	n	ü
å	É	/	?	O	§	o	à

"SP" in the overview refers to the space character. "LF", "CR" and "ESC" refer to the control characters for the line feed, the carriage return and the escape in the extended GSM character set.

The following characters are implemented from the **extended GSM character set**:

{ | } [ ] ~ ^ \ €

2.7 The SYSLOG module

The SYSLOG module allows accessing of the device to be logged. This function is especially interesting for system administrators as it optionally records a complete history of all activities in the device.

A corresponding SYSLOG client or daemon is required to receive the SYSLOG messages. Logging under UNIX/Linux is generally performed by the SYSLOG daemon that is set up by default in these operating systems. The daemon either establishes contact with the CLI or writes its log to an appropriate SYSLOG file.

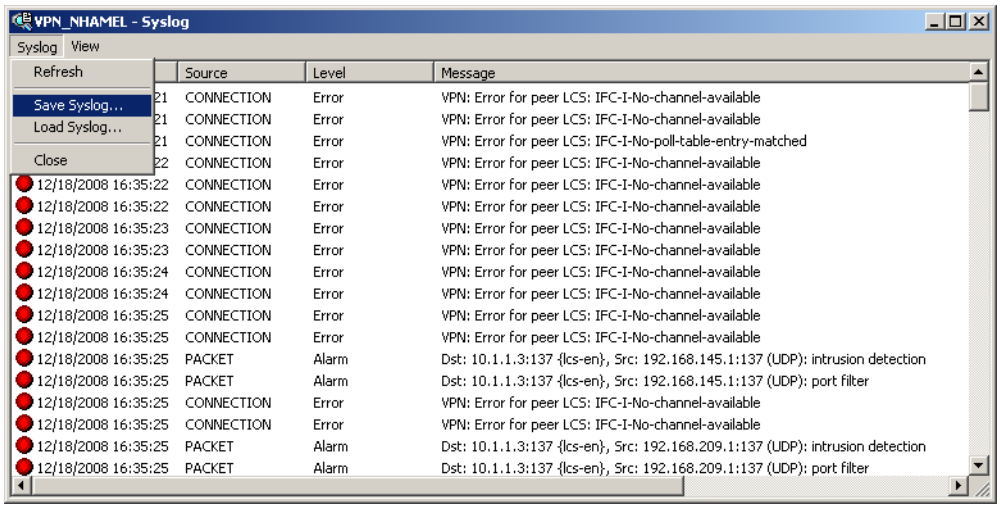
Under Linux, the file `/etc/syslog.conf` contains a definition of which facilities (service or component that issued the message) should be written to which log file. Please check your daemon's configuration to see if it explicitly listens to network connections.

Windows does not provide a corresponding system function. You require special software to provide the functionality of a SYSLOG daemon.

To extend the output of the SYSLOG information over an appropriate SYSLOG client, the most recent SYSLOG messages are stored in the device's RAM. Depending on the memory fitted, this can vary from 100 to 23,000 syslog messages. These internal syslogs can be viewed in various ways:

- In the device statistics on the command line
- In WEBconfig under /System information/Syslog
- LANmonitor additionally lets you export the syslog from the device and save it to a file. Simply click on the entry for the device with the right mouse button and select **View Syslog** from the context menu. A snapshot of the current status is displayed. Clicking on **Refresh** exports a copy of the current syslog and this is displayed in the window. **Save syslog...** stores the current display to a file. The content of syslog files can be viewed with **Load syslog...**.

SYSLOG messages will only be written to the device's internal memory if the device was entered as a SYSLOG client with the loopback address 127.0.0.1 or if boot-persistent storage is enabled. See *Boot-persistent SYSLOG, event log and boot log*.



Alternatively you can view the current SYSLOG messages on the first page of WEBconfig on the **SYSLOG** tab:

System data | Device status | Syslog

Idx.	Time	Source	Level	Message
743	11/11/2008 14:55:53	LOCAL3	Alarm	Dst: 10.1.1.5:139 {lcs-data}, Src: 192.168.8.1:14132 (TCP): port filter
744	11/11/2008 14:55:53	LOCAL3	Alarm	Dst: 10.1.1.5:139 {lcs-data}, Src: 192.168.202.1:14133 (TCP): intrusion detectic
745	11/11/2008 14:55:53	LOCAL3	Alarm	Dst: 10.1.1.5:139 {lcs-data}, Src: 192.168.202.1:14133 (TCP): port filter
746	11/11/2008 14:55:54	LOCAL3	Alarm	Dst: 10.1.1.5:139 {lcs-data}, Src: 192.168.8.1:14137 (TCP): intrusion detection
747	11/11/2008 14:55:54	LOCAL3	Alarm	Dst: 10.1.1.5:139 {lcs-data}, Src: 192.168.8.1:14137 (TCP): port filter
748	11/11/2008 14:55:54	LOCAL3	Alarm	Dst: 10.1.1.5:139 {lcs-data}, Src: 192.168.202.1:14138 (TCP): intrusion detectic
749	11/11/2008 14:55:54	LOCAL3	Alarm	Dst: 10.1.1.5:139 {lcs-data}, Src: 192.168.202.1:14138 (TCP): port filter
750	11/11/2008 15:13:34	LOCAL3	Alarm	Dst: 192.168.2.100:22338 {VPN_NHAMEL}, Src: 192.168.2.47:5000 {evb3-00a0
751	11/11/2008 15:13:34	LOCAL3	Alarm	Dst: 192.168.2.100:22338 {VPN_NHAMEL}, Src: 192.168.2.47:5000 {evb3-00a0
752	11/11/2008 15:13:34	LOCAL3	Alarm	Dst: 192.168.2.100:22338 {VPN_NHAMEL}, Src: 192.168.2.47:5000 {evb3-00a0
753	11/11/2008 15:13:34	LOCAL3	Alarm	Dst: 192.168.2.100:22339 {VPN_NHAMEL}, Src: 192.168.2.47:5001 {evb3-00a0
754	11/11/2008 16:37:19	LOCAL3	Alarm	Dst: 10.1.1.5:139 {lcs-data}, Src: 192.168.8.1:16446 (TCP): intrusion detection
755	11/11/2008 16:37:19	LOCAL3	Alarm	Dst: 10.1.1.5:139 {lcs-data}, Src: 192.168.8.1:16446 (TCP): port filter
756	11/11/2008 16:37:19	LOCAL3	Alarm	Dst: 10.1.1.5:139 {lcs-data}, Src: 192.168.202.1:16447 (TCP): intrusion detectic

2.7.1 Structure of SYSLOG messages

SYSLOG messages consist of three parts:

- Priority
- Header
- Contents

Priority

The priority in a SYSLOG message contains information about the the message severity and the facility (service or component that triggered the message).

The eight severity levels originally defined in SYSLOG have been reduced to five levels in the device. The table below shows the correlation between the alert level, the meaning and the SYSLOG severities.

Priority	Meaning	SYSLOG severity
Alert	This category includes all messages requiring the system administrator's close attention.	PANIC, ALERT, CRIT
Error	All error messages which can occur under normal conditions are communicated at this level; no special attention is required by the administrator (e.g. connection errors).	ERROR
Warning	This level communicates messages which do not compromise normal operating conditions.	WARNING
Information	At this level, all messages are sent that have a purely informational character (e.g. accounting information).	NOTICE, INFORM
Debug	Communication of all debug messages. Debug messages generate large data volumes and can compromise the device's operation. For this reason they should be disabled for normal operations and only used for troubleshooting.	DEBUG

The table below provides an overview of the meaning of all internal message sources that you can set in the device. The final column in the table also provides the default correlation between the internal sources of the device and the SYSLOG facilities. This mapping can be changed, if necessary.

Source	Meaning	Facility
System	System messages (boot events, timer system, etc.)	KERNEL

Source	Meaning	Facility
Logins	Messages about successful connection and disconnection as well as about login and logout of a user during PPP negotiation as well as errors that occur in the process	AUTH
System time	Messages about changes to the system time	CRON
CLI login	Messages about CLI logins (Telnet, Outband, etc.), logouts and any errors that occurred during this.	AUTHPRIV
Connections	Messages about any errors that occurred during establishment and termination of connections (display trace)	LOCAL0
Accounting	Accounting information stored after termination of a connection (user, online time, transfer volumes)	LOCAL1
Administration	Messages on changes to the configuration, remotely executed commands, etc.	LOCAL2
Router	Regular statistics about the most frequently used services (breakdown per port number) and messages about filtered packets, routing errors, etc.	LOCAL3

Header

The header contains the name or the IP address of the device which sent the SYSLOG message. The chronological sequence is also very important for evaluating the messages. Time information is only added to the messages at the SYSLOG client in order not to disturb their chronological consistency due to different device times.

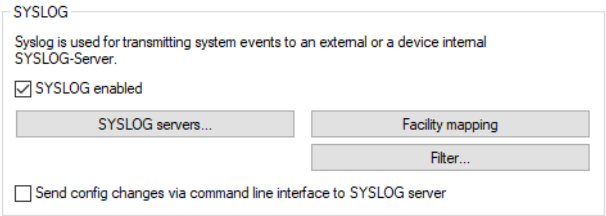
The devices must have a valid time stamp for the evaluation of the SYSLOG messages in internal memory.

Contents

The actual contents of the SYSLOG messages describe the event, for example a login occurrence, the establishment of a WAN connection, or firewall activities.

2.7.2 Configuring SYSLOG

In LANconfig you configure SYSLOG under **Logging/Monitoring** > **Protocols** in the section **SYSLOG**.



SYSLOG enabled

Activate the SYSLOG protocol.

Send config changes via command line interface to SYSLOG server

Configuration changes made via the command line interface are sent to the configured servers via SYSLOG.

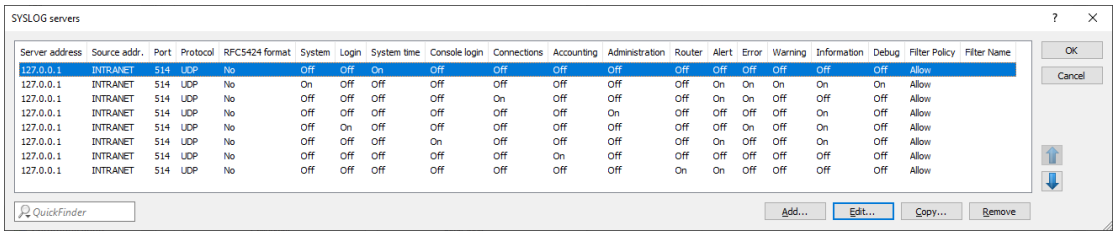
This protocol logs commands entered on the command line only. Configuration changes and actions made using LANconfig and WEBconfig are not logged.

SYSLOG server

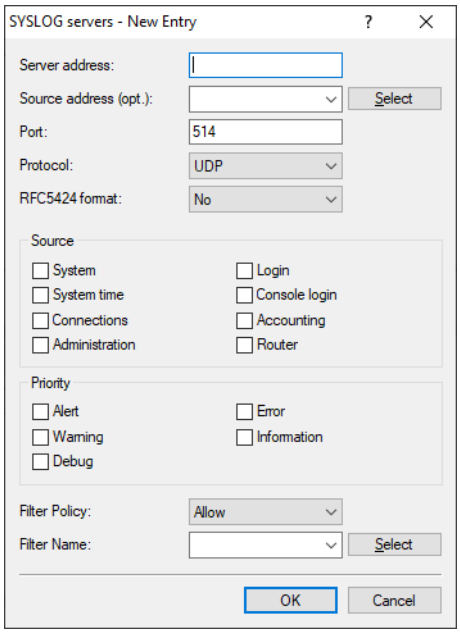
In LANconfig, you configure the settings for the SYSLOG server under **Logging/Monitoring** > **Protocols** > **SYSLOG** and clicking **SYSLOG servers**.

Click on **SYSLOG servers** to see the entries available for SYSLOG.

With the factory settings, the table of SYSLOG entries is set up to display important events which are relevant to diagnostics, and to save these to the internal SYSLOG memory. These settings correspond to the specifications in the UNIX world, where SYSLOG originates from. The following screenshot shows these pre-defined SYSLOG entries under LANconfig:



Click on **Add**, or select an entry and click **Edit**.



Server address

Used to set the IP address of the SYSLOG server. This can be specified as an IPv4 or IPv6 address, or as a host name.

Source address (optional)

You can optionally specify a source address that the SYSLOG client uses as the target address, instead of the one that would normally be selected automatically. If you have configured loopback addresses, you can specify them here as sender address.

Port

Specifies the port number (e.g. 514 for TCP/UDP).

Protocol

Defines the protocol used. Possible values:

UDP

User Datagram Protocol

TCP

Transmission Control Protocol

TLS

The syslog client supports three scenarios in TLS mode:

1. The syslog client accepts all TLS server certificates from the syslog server. For this purpose, no trusted CA certificate is stored in the router.
2. The syslog client only accepts server certificates signed by a trusted CA. To do this, the CA certificate must be uploaded to the corresponding certificate slot on the router.
3. The syslog client authenticates itself with the syslog server using a TLS client certificate and the syslog server authenticates itself with its CA certificate. To do this, both the TLS client certificate for the router and the CA certificate must be uploaded to the corresponding certificate slot on the router, e.g. in a container as a PKCS#12 file.

Certificates for syslog can be loaded into the device either via WEBconfig or LANconfig.

- **LANconfig**:**Right-click on the device** > **Configuration Management** > **Upload Certificate or File**
  - **Syslog - container as PKCS#12 file** or
  - **Syslog - Root CA Certificate**
- **WEBconfig**: **Extras** > **File management** > **Upload Certificate or File** > **File Type**
  - **Syslog - container as PKCS#12 file** or
  - **Syslog - Root CA Certificate**

RFC5424 format

Specifies whether the syslog client should send messages to the syslog server in RFC5424 format.

Source

The table below provides an overview of the meaning of all message sources that you can set in the device. The final column in the table also provides the correlation between the internal sources of the device and the SYSLOG facilities.

Source	Meaning	Facility
System	System messages (boot events, timer system, etc.)	KERNEL
Login	Messages concerning the user's login or logout during the PPP negotiation, and any errors that occur during this.	AUTH
System time	Messages about changes to the system time	CRON
Console login	Messages about CLI logins (Telnet, Outband, etc.), logouts and any errors that occurred during this.	AUTHPRIV
Connections	Messages about establishment and termination of connections and any errors that occurred (display trace)	LOCAL0
Accounting	Accounting information stored after termination of a connection (user, online time, transfer volumes)	LOCAL1
Administration	Messages on changes to the configuration, remotely executed commands, etc.	LOCAL2
Router	Regular statistics about the most frequently used services (breakdown per port number) and messages about filtered packets, routing errors, etc.	LOCAL3

Priority

The eight priority levels originally defined in SYSLOG have been reduced to five levels in the device. The table below shows the correlation between the alert level, the meaning and the SYSLOG priorities.

Priority	Meaning	SYSLOG priority
Alert	This category includes all messages requiring the system administrator's close attention.	PANIC, ALERT, CRIT
Error	All error messages which can occur under normal conditions are communicated at this level; no special attention is required by the administrator (e.g. connection errors).	ERROR
Warning	This level communicates messages which do not compromise normal operating conditions.	WARNING
Information	At this level, all messages are sent that have a purely informational character (e.g. accounting information).	NOTICE, INFORM
Debug	Communication of all debug messages. Debug messages generate large data volumes and can compromise the device's operation. For this reason they should be disabled for normal operations and only used for troubleshooting.	DEBUG

Filter Policy

If the syslog messages are transmitted to one or more servers by configuring settings for receiving certain messages, all configured messages are transmitted to the servers with the configured source and priority. However, it is sometimes desirable to filter out certain messages for the servers, to send only certain messages at all, or to change their source and priority if they should be weighted differently in the server log. The syslog filter allows the filtering of messages depending on the source, priority and/or message text. Here you determine whether messages, which are identified by the filter set in the following field, are allowed or denied.

Filter Name

Select one of the configured filters.

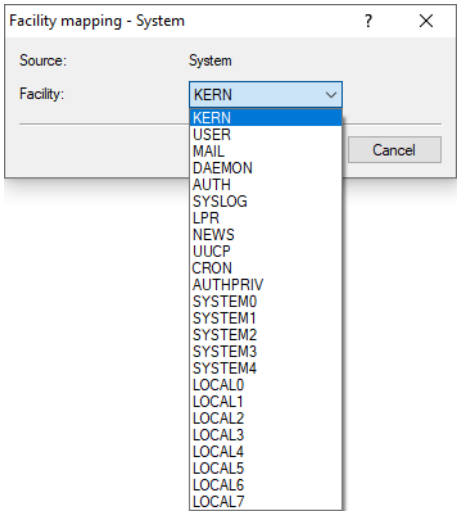
Once you have set all of the parameters, confirm your entries with **OK**. The SYSLOG table shows the SYSLOG client with its parameters.

SYSLOG facility mapping

The SYSLOG protocol uses certain designations for message sources, the so-called facilities. Each internal source in the devices that can generate a SYSLOG message must therefore be assigned to a SYSLOG facility.

The standard mapping can be changed, if necessary. In this way you can, for example, send all SYSLOG messages from a device with a specific facility (Local7). It is thus possible to collect all messages in a common log file by configuring the SYSLOG client appropriately.

Under **Logging/Monitoring** > **Protocols** in the section **SYSLOG** under **Facility mapping**, the internal sources can be assigned to the corresponding SYSLOG facilities.



Messages from the device are mapped to a facility, so that the SYSLOG client can write them to a special log file without any additional effort.

All facilities are set to 'local7'. Under Linux, the file `/etc/syslog.conf` with the entry

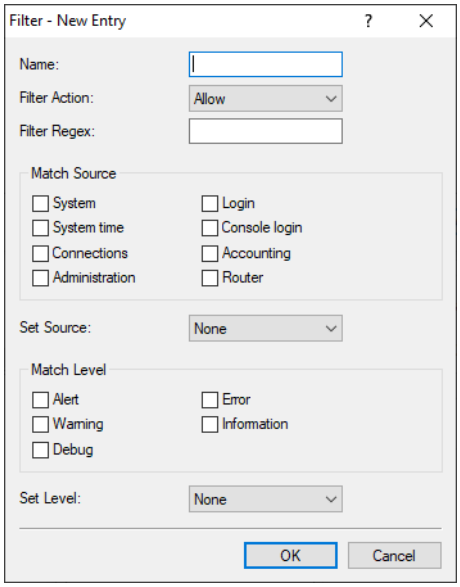
```
local7.* /var/log/lancom.log
```

writes all of the device output to the file `/var/log/lancom.log`.

Filter

If the syslog messages are transmitted to one or more servers by configuring settings for receiving certain messages, all configured messages are transmitted to the servers with the configured source and priority. However, it is sometimes desirable to filter out certain messages for the servers, to send only certain messages at all, or to change their source and priority if they should be weighted differently in the server log. The syslog filter allows the filtering of messages depending on the source, priority and/or message text. Configure these filters here, which you can then use for entries on the SYSLOG server.

In LANconfig, you configure the filter settings for the SYSLOG server under **Logging/Monitoring** > **Protocols** > **SYSLOG** and clicking **Filter**.



Name

Give the filter a descriptive name. Several rules can be created with the same filter name. These are then checked in the order in which they are created in the filter table when sending the messages. If there is no matching rule in this filter chain, the message is sent or discarded according to the server's default policy in the server table.

Filter action

Action when the rule applies; "Allow" enables messages to be sent to the server, "Deny" rejects the message.

Filter regex

Regular expression in Perl syntax (also see *Regular expressions in Perl*) to which the message text must apply. An empty string means that the message text is ignored, and therefore all message texts apply.

Match source

Source of the message to which this rule applies. The value "none" stands for any source.

Set source

New source of the message if the rule applies. The value "none" means that the source is not changed.

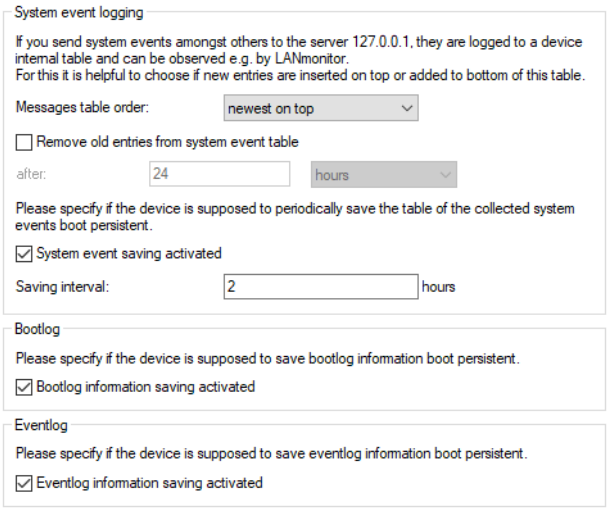
Match level

Priority of the message to which this rule applies. The value "none" stands for any priority.

Set level

New priority of the message if the rule applies. The value "none" means that the priority is not changed.

System event logging



Define for how long system events are saved

Under **Logging/Monitoring** > **System events** > **System event logging** you specify how long the device saves system events. To do so, select the option **Remove old entries from the system event table** and specify a time (0-9999) in hours, days or months.

In this case, a month is 30 days.

Boot-persistent SYSLOG, event log and boot log

The settings for the boot-persistent SYSLOG, event log and boot-log messages are to be found under **Logging/Monitoring** > **System events** (if available for your device). Activate the following options:

- SYSLOG: **System event saving activated**

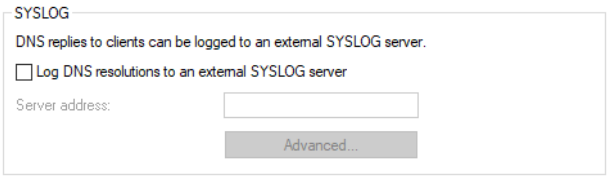
  Use the entry **Saving interval** to set the time in hours after which the SYSLOG system events are saved to boot-persistent memory.
- Bootlog: **Bootlog information saving activated**
- Eventlog: **Eventlog information saving activated**

Logging DNS requests and responses to external SYSLOG servers

The DNS server in LANCOM devices resolves the DNS queries from clients. SYSLOG provides an overview of the clients, the names they requested, and the responses they received.

It is not possible to use the router/access points own internal SYSLOG. For this reason it is necessary to employ an external SYSLOG server.

DNS logging is configured in LANconfig under **DNS** > **General** in the section **SYSLOG**.



Log the DNS resolutions on an external SYSLOG server

Select this option to enable the DNS logging.

This option is independent of the setting in the SYSLOG module. Even if the SYSLOG module is disabled (setting under **Logging/Monitoring** > **Protocols** in the section **SYSLOG**), DNS logging is carried out nevertheless.

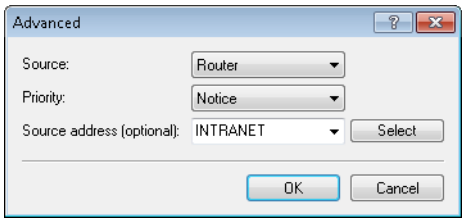
The corresponding SYSLOG message is structured as follows:

```
PACKET_INFO: DNS for <IP address>, TID {Hostname}: Resource record
```

Server address

Contains the IP address or the DNS name of the SYSLOG server.

The settings behind the button **Advanced** influence the content of SYSLOG messages.



Source

Contains the log source as displayed in the SYSLOG messages.

Priority

Contains the log level as displayed in the SYSLOG messages.

Source address (optional)

Contains the source address that is shown in the SYSLOG messages.

2.7.3 Meaning of SYSLOG messages

Extended status display of the login to the cellular network

In order to more quickly analyze connection problems in a cellular network, WWAN-capable routers report all logon procedures to the SYSLOG. In this manner, the user can recognize if and why the cellular service provider rejected the connection, for example.

The device generates a SYSLOG entry for each of the following events:

Status	Meaning	SYSLOG severity
WWAN: Currently not searching for network	The modem is not registered and is not searching for a cellular network.	INFORM
WWAN: Searching for network	The modem is not registered and is not searching for a cellular network.	INFORM
WWAN: Registered to home network	The modem has registered on its service provider's cellular network.	INFORM
WWAN: Registered to foreign network	The modem has successfully registered on the cellular network of the service provider's roaming partner.	INFORM

Status	Meaning	SYSLOG severity
WWAN: Unknown registration	Initial value. The modem has not yet received a response from the radio module regarding the registration status.	INFORM
WWAN: Network registration denied	The cellular service provider has rejected the login on the cellular network.	ERROR
WWAN: Lost network registration	The modem lost the connection to the registered cellular network.	NOTICE
WWAN: Failed to set network	The modem has replied to the command to assign the network with an error message. This error occurs if, for example, the network cannot be reached or does not exist, or an error has occurred on the device.	ERROR
WWAN: Failed to set network mode	The modem has replied to the command to assign the network mode with an error message. This error occurs if, for example, the network cannot be reached or does not exist, or an error has occurred on the device.	ERROR
WWAN: Using modem '...'.	Displays the modem in use.	INFORM
WWAN: Modem is gone.	Modem no longer available.	INFORM
WWAN: Resetting modem.	Re-init by modem reset	WARNING
WWAN: Local disconnect.	D-channel disconnect	INFORM
WWAN: Local disconnect (Release).	D-channel release	INFORM
WWAN: Force 2G mode at ... dB.	Modem starts the 2G fallback	NOTICE
WWAN: Ending forced 2G mode.	Modem ends the 2G fallback	INFO
WWAN: Forced 2G mode disabled.	The 2G fallback mode is disabled.	INFO
WWAN: PIN missing in profile.	PIN is missing from the profile.	ERROR
WWAN: PUK required.	Modem requires the PUK.	ERROR
WWAN: Invalid PIN.	Incorrect PIN	ERROR
WWAN: Failed to set APN	Error when setting the APN The modem has replied to the command to assign the APNs with an error message. This error occurs if, for example, the network cannot be reached or does not exist, or an error has occurred on the device.	ERROR
WWAN: Using profile '...'.	Name of the profile in use.	NOTICE
WWAN: Cannot find profile '...'.	Profile not available.	ERROR
WWAN: Disconnected.	Physical connection is terminated.	INFORM
WWAN: Connected: '...'.	The modem has established a data connection and can now transmit data over the cellular network.	INFORM
WWAN: Cell-ID is ..., Local Area Code is	Cell ID and country code.	INFORM
WWAN: Current Network is '...'.	Network (text)	INFORM
WWAN: Current Network is	Network (number)	INFORM
WWAN: Mode ..., Band '...'.	Display of network mode and band	INFORM

Status	Meaning	SYSLOG severity
WWAN: Mode ..., Band '...', Bandwidth in MHz: ..., Channel (Rx/Tx): .../....	Display of network mode, band, bandwidth and channel (transmit and receive direction).	INFORM
WWAN: Mode ..., Band '...', Channel (Rx/Tx): .../....	Display of network mode, band and channel (transmit and receive direction).	INFORM
WWAN: Max. Datarate (Ds/Us): .../....	Current QoS data rate (down/upstream)	INFORM
WWAN: Network mode is '...'.	Current mode. Possible values are: › GPRS › EDGE › UMTS › HSPA › LTE/4G	INFORM
WWAN: Signal strength is ... dBm.	Current signal strength	INFORM
WWAN: Using stored APN. APN: '...', PDP type:	Access point currently being used in the network.	INFORM
WWAN: Setting new APN. APN: '...', PDP type:	Change of network access point	INFORM
WWAN: Temperature is ...°C.	Current temperature of the module	INFORM
WWAN: Temperature status: '...'.	Current temperature status of the module. Possible values are: › Normal › High warning › High critical › Low critical	INFORM (normal), WARNING (high warning), CRITICAL (high critical, low critical)
WWAN: Closing device: '...'.	The device running the connection to the WAN is shutting down.	INFORM
WWAN: Hangup: '...'.	The modem terminates the network connection.	INFORM
WWAN: Error in modem init: '___'.	An error has occurred when initializing the modem.	ERROR

Documenting events on the xDSL interface

The device generates a SYSLOG entry for each of the following xDSL interface events:

Status	Meaning	SYSLOG severity
xDSL: Booting modem: ...	The modem is restarting.	NOTICE
xDSL: Set up line to <line mode>/<line type>	The xDSL module establishes the connection with the mode and type specified. The following values are possible: › Line mode: Disabled, auto and all modes configured in **Setup** > **Interfaces** > **ADSL or VDSL interface**. › Line type: POTS, ISDN	INFORM
xDSL: Line is up. DS-Rate: ..., US-Rate: ..., DS-Margin: ..., US-Margin: ...,	The modem connected successfully with the specified values.	NOTICE

Status	Meaning	SYSLOG severity
DS-Attn: ..., US-Attn: ..., Mode: ..., Profile:		
xDSL: Line data update. DS-Rate: ..., US-Rate: ..., DS-Margin: ..., US-Margin: ..., DS-Attn: ..., US-Attn: ..., Mode: ..., Profile: ...	After a synchronization, the modem and the DSLAM perform an optimization of the xDSL connection. This can lead to a change in the line values. After one minute, the modem transmits the current line values.	NOTICE
xDSL: Line data update.	After a synchronization, the modem and the DSLAM perform an optimization of the xDSL connection. After one minute, the modem transmits this message if the line values do not change after the synchronization.	NOTICE
xDSL: Line disconnected due to	The connection was disconnected for the specified reason. The following values are possible: > modem reboot > retrain > silence > high line error rate > protocol setting > line type setting > automode line type switch > modem timeout > VC parameter change	NOTICE
xDSL: SNR margin (dB, Down/Up): .../...	The value between the required and measured signal-noise ratio (SNR) has changed by more than 1dB.	INFORM