



User Guide Public Spot

LCOS
[LANCOM OPERATING SYSTEM]

LANCOM
Systems

Contents

1 Introduction.....	5
1.1 What is a Public Spot?.....	5
1.1.1 The solution: (W)LAN technology.....	5
1.1.2 User authorization and authentication	6
1.1.3 Accounting.....	6
1.1.4 Logging.....	6
1.2 Possible application scenarios.....	6
1.2.1 Guest access accounts in hotels.....	6
1.2.2 Guest access in sport arenas.....	7
1.2.3 Guest access at camping grounds.....	8
1.2.4 Guest access in schools and universities.....	9
1.2.5 Guest access in companies.....	10
1.2.6 Guest access for providers.....	11
1.2.7 Guest access in gastronomy.....	12
1.3 Overview of the Public Spot module.....	13
1.3.1 Open User Authentication (OUA).....	13
1.3.2 Security in the (W)LAN.....	14
1.3.3 Setup wizard for Public Spots.....	15
1.3.4 Wizard for creating and managing users.....	15
2 Enabling the Public Spot module.....	16
2.1 Installation prerequisites.....	16
2.1.1 Devices with optional Public Spot support.....	16
2.1.2 Package content.....	16
2.1.3 Configuration computer with the Windows operating system.....	17
2.1.4 Latest management software.....	17
2.1.5 Latest device firmware.....	17
2.2 Online registration.....	17
2.2.1 Necessary registration information.....	17
2.2.2 Online entry of registration information.....	17
2.2.3 Help in case of problems.....	18
2.3 Enabling the Public Spot module.....	18
2.4 Checking the activation.....	19
3 Setup and operation.....	20
3.1 Basic configuration.....	20
3.1.1 Basic installation of a Public Spot for simple scenarios.....	20
3.1.2 Setting default values for the Public Spot wizard.....	32
3.1.3 Setting up limited administrator rights for Public Spot managers.....	33
3.1.4 Setting up and managing Public Spot users for simple scenarios.....	34
3.2 Security settings.....	39
3.2.1 Traffic limit option.....	39

3.2.2 Restricting access to the configuration.....	40
3.3 Extended functions and settings.....	40
3.3.1 Multiple logins.....	41
3.3.2 Open access networks (no login).....	42
3.3.3 Managing Public Spot users via the web API.....	44
3.3.4 Bandwidth profile.....	48
3.3.5 Clear user list automatically.....	48
3.3.6 Station monitoring.....	49
3.3.7 WLAN handover of sessions between devices.....	50
3.3.8 Authentication via RADIUS	51
3.3.9 Billing without a RADIUS accounting server.....	52
3.3.10 Billing via RADIUS accounting server.....	52
3.3.11 Multi-level certificates for PublicSpots.....	53
3.3.12 Assigning users to individual VLANs.....	54
3.4 Alternative login methods.....	55
3.4.1 Overview of authentication modes.....	56
3.4.2 Independent user authentication (Smart Ticket).....	57
3.4.3 Automatic re-login.....	59
3.4.4 Automatic authentication with the MAC address.....	60
3.4.5 Automatic authentication via WISPr.....	61
3.4.6 IEEE 802.11u and Hotspot 2.0.....	63
3.4.7 XML interface.....	77
3.4.8 Interface for property management systems.....	84
3.5 Default and customized authentication pages.....	89
3.5.1 Possible pages.....	89
3.5.2 Pre-installed default pages.....	90
3.5.3 Customizing the standard pages.....	90
3.5.4 Configuration of user-defined pages.....	93
3.5.5 URL placeholder (template variables).....	94
3.5.6 User-defined pages via HTTP redirect.....	95
3.5.7 User-defined pages via page templates.....	95
3.5.8 Page template syntax	96
3.5.9 Page template identifiers.....	96
3.5.10 Graphics in user-defined pages.....	98
4 Access to the Public Spot.....	99
4.1 Requirements for logging in.....	99
4.2 Logging in to the Public Spot.....	100
4.3 Session information.....	100
4.4 Logging out of the Public Spot.....	101
4.5 Advice and help.....	101
4.5.1 The Public Spot login page is not displayed.....	101
4.5.2 Login not working.....	102
4.5.3 It is no longer possible to login.....	102
4.5.4 The session information window is not being displayed.....	102

4.5.5 The Public Spot requests a new login for no reason (WLAN).....	102
5 Tutorials for setting up and using Public Spots.....	103
5.1 Virtualization and guest access via WLAN controller with VLAN.....	103
5.1.1 Objectives.....	103
5.1.2 Establish.....	103
5.1.3 Wireless LAN configuration of the WLAN controllers.....	104
5.1.4 Configuring the switch (LANCOM ES-2126+).....	105
5.1.5 Configuring the switch (LANCOM GS-2326P).....	107
5.1.6 Configuring the IP networks in the WLAN controller.....	109
5.1.7 Configuring Public Spot access accounts.....	110
5.1.8 Configuring the internal RADIUS server for Public Spot operation.....	111
5.1.9 Configuring Internet access for the guest network.....	112
5.2 Virtualization and guest access via WLAN controller without VLAN.....	113
5.2.1 Overlay network: Separating networks for access points without using VLAN.....	113
5.2.2 WLAN controller with Public Spot.....	118
5.3 Setting up an external RADIUS server for user administration.....	124
5.4 Internal and external RADIUS servers combined.....	125
5.4.1 Realm tagging for RADIUS forwarding.....	125
5.4.2 Configuring RADIUS forwarding.....	126
5.5 Checking WLAN clients with RADIUS (MAC filter).....	128
5.6 Setting up an external SYSLOG server.....	129
5.6.1 Configuring an external SYSLOG server.....	129
6 Appendix.....	130
6.1 Commonly transmitted RADIUS attributes.....	130
6.1.1 Messages to/from the authentication server.....	130
6.1.2 Messages to/from the accounting server.....	133
6.2 RADIUS attributes transmitted via WISPr.....	135
6.3 Expert settings for the PMS interface.....	136
6.3.1 Accounting.....	136
6.3.2 Login form.....	137
6.3.3 Guest name case sensitive.....	140
6.3.4 Separator.....	140
6.3.5 Character set.....	140

1 Introduction

This chapter provides answers to the following two questions:

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

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.

Access via wireless LAN is widespread, however, it is also possible to access a Public Spot using a cabled LAN connection. The most popular demand for these services originally came from business travelers at airports, in hotels, or at other locations where their end devices require access to online content. The public rarely has access to modems, ISDN or broadband connections in areas like this. However, the recreational use of Public Spots by private persons has become very popular.

1.1.1 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. The user only needs a WLAN adapter for their mobile device, which, for modern devices, is usually part of the standard equipment or can be inexpensively added, usually with a USB interface. The bandwidth is sufficient for most applications, even when multiple users are simultaneously logged in to a Public Spot.
- With automatic address allocation via DHCP, access via LAN is similarly uncomplicated: In this case, the user only needs a LAN adapter and a suitable cable for their end device, in order to connect their device to the Public Spot network at a wall socket.

However, 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

It is difficult to employ a standard WLAN access point or LAN router as a Public Spot for two main reasons:

- User authentication is only possible by employing RADIUS/802.11x, so requiring the appropriate infrastructure and configuration.
- There is no facility for billing / accounting.

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.

1.1.2 User authorization and authentication

As soon as an end device moves within range of an access point, the user can spontaneously establish a connection 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 WLAN 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.

1.1.3 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 method), retrospective payment of consumed resources (credit payment), 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).

1.1.4 Logging

The operation of commercial telecommunications services is subject to national regulations. Certain information is to be recorded and presented to law enforcement agencies upon request.

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.de/en/publications/products.

1.2 Possible application scenarios

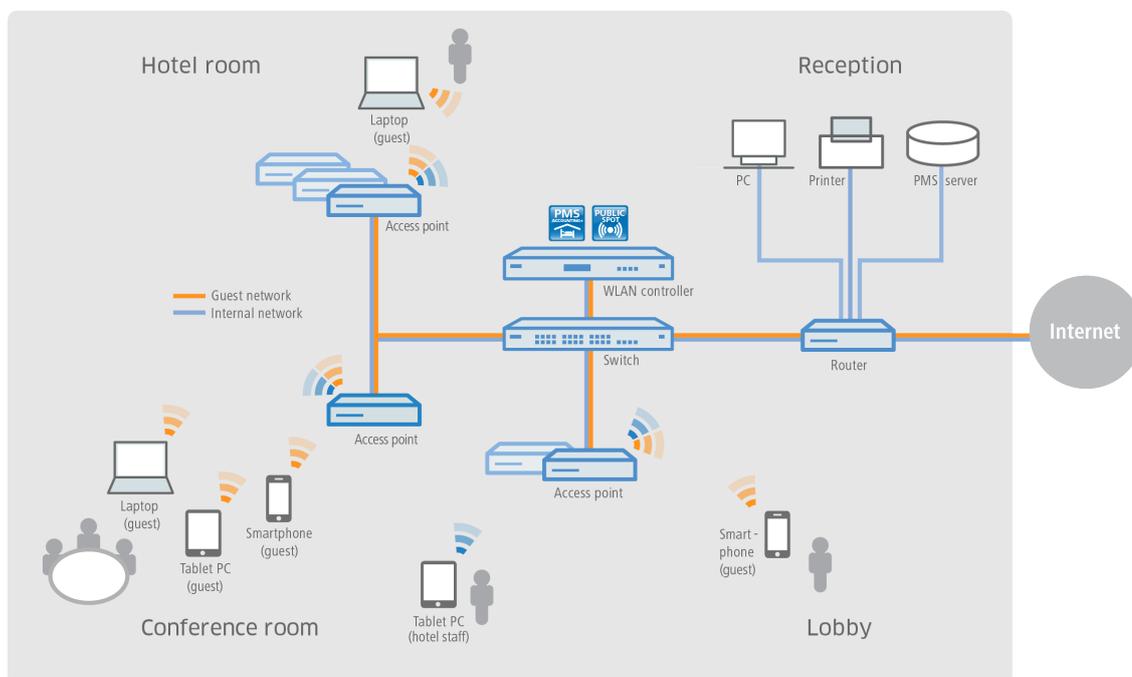
1.2.1 Guest access accounts in hotels

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 20.
- **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 103.

- **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 55.
- **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 84.

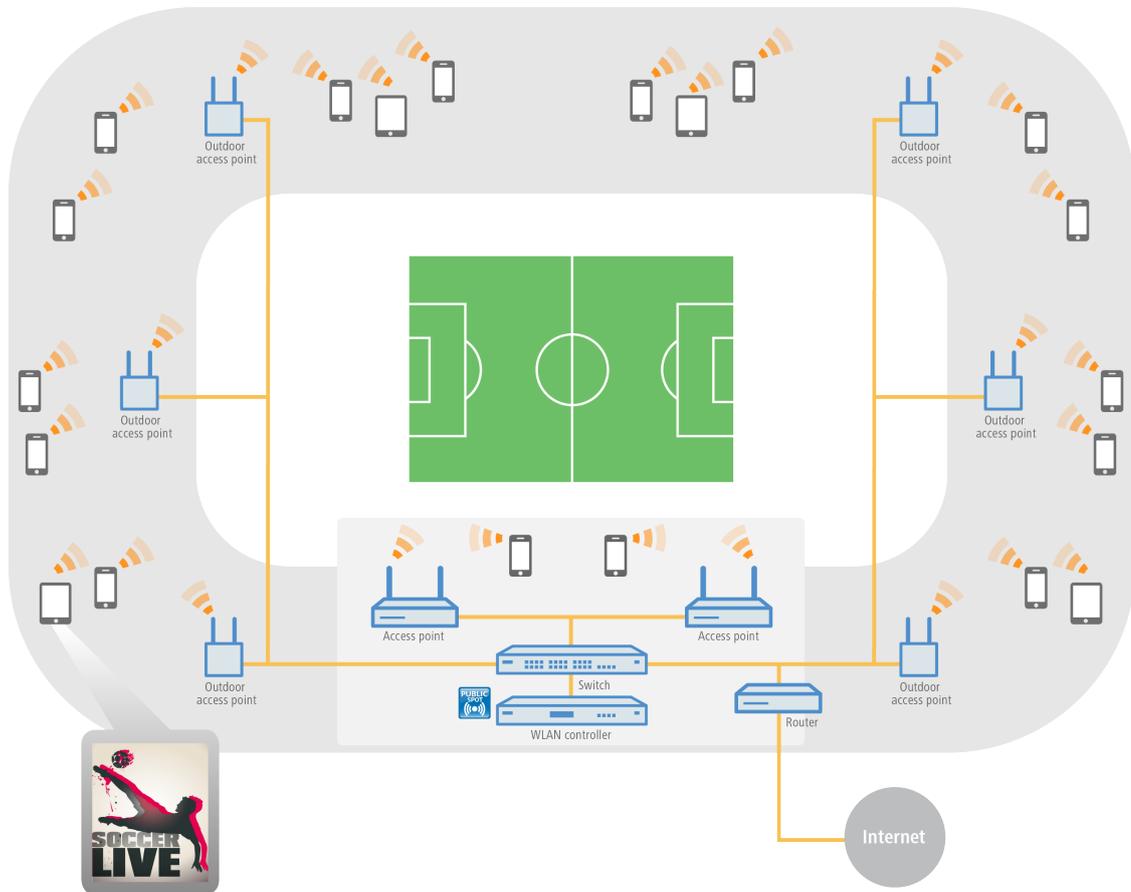


1.2.2 Guest access in sport arenas

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 WLAN 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 20.



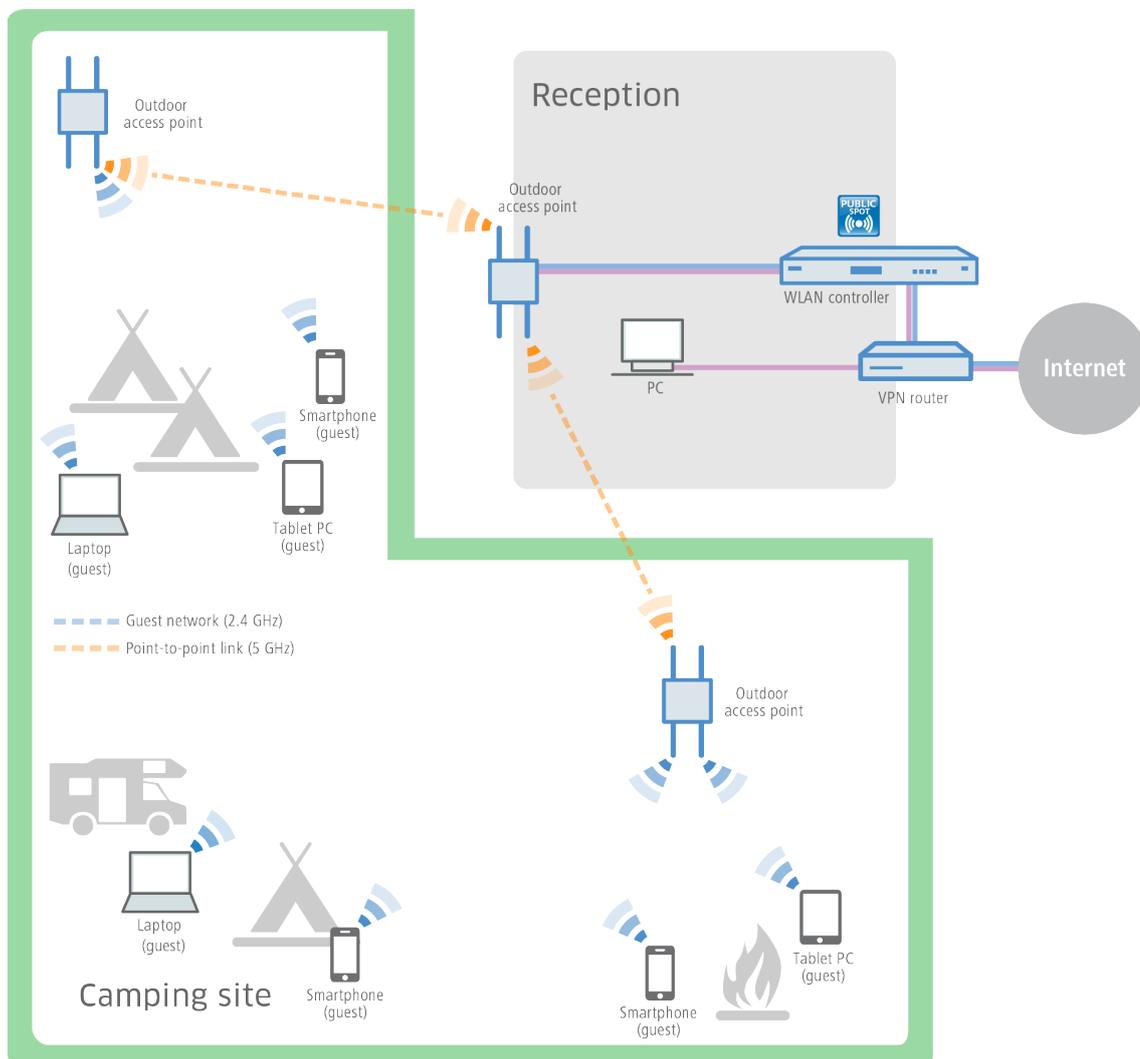
1.2.3 Guest access at camping grounds

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 can be 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 20.
- **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 55.

- **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.



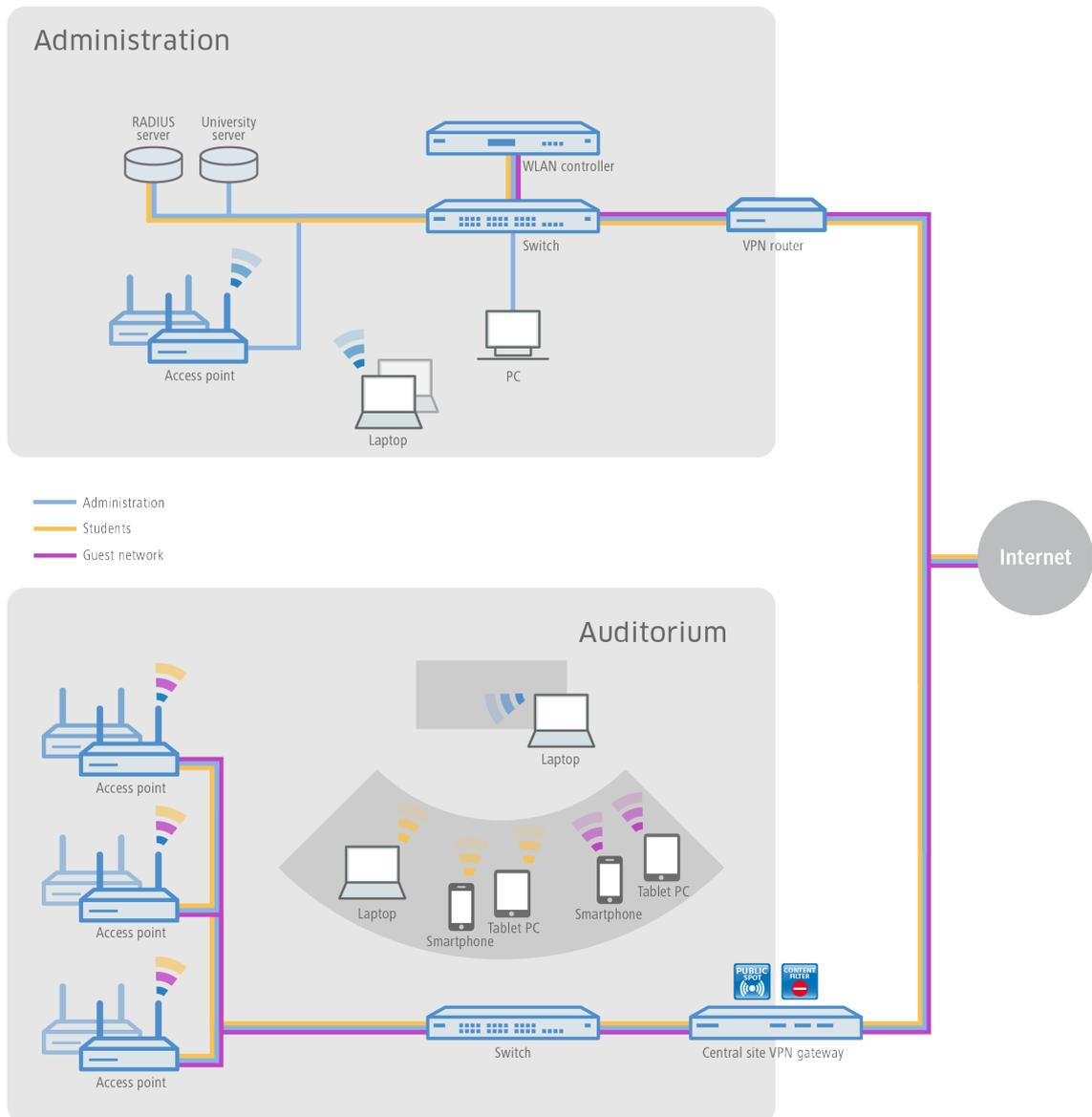
1.2.4 Guest access in schools and universities

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 103.
- **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.

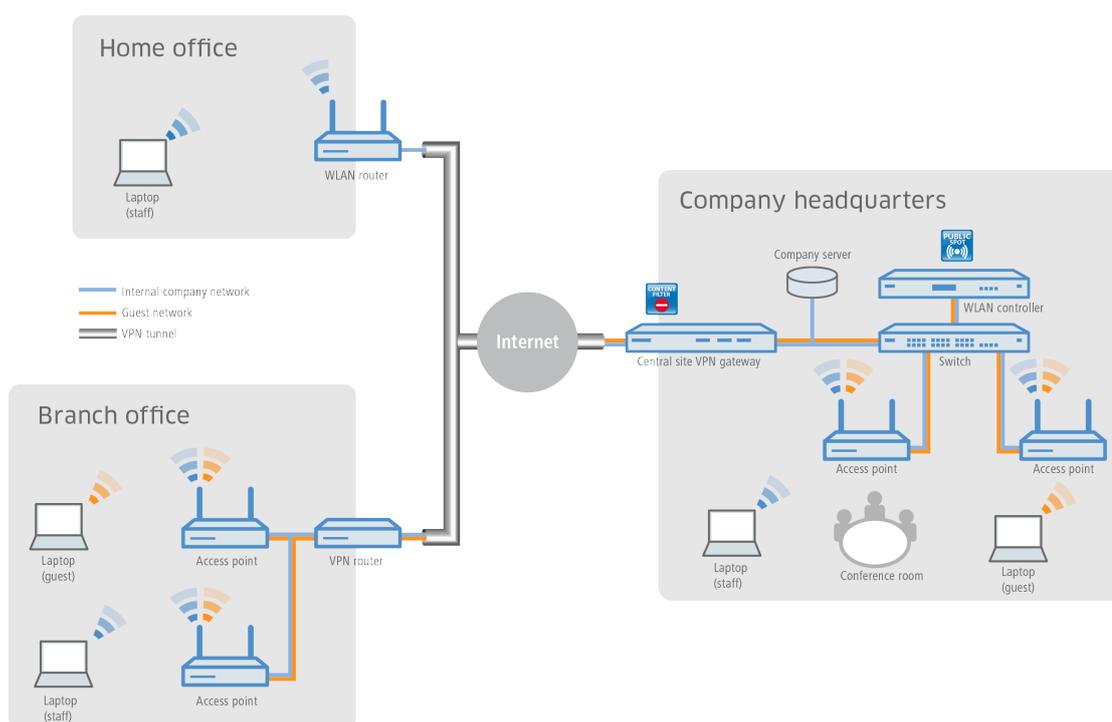


1.2.5 Guest access in companies

At any company with a complex network structure, the flexibility and stability of Internet access is extremely 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 guest 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 103.
- **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.



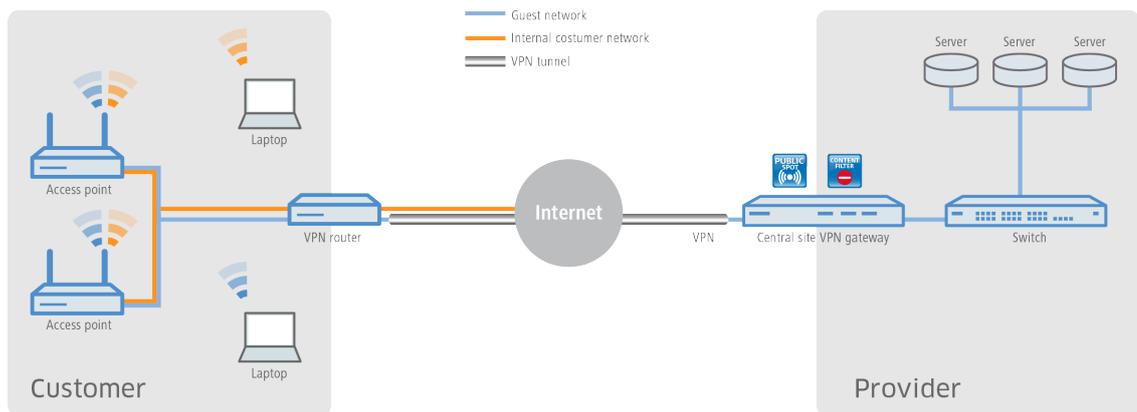
1.2.6 Guest access for providers

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). An individually separated 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 20.
- **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 55.
- **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 55.
- **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.

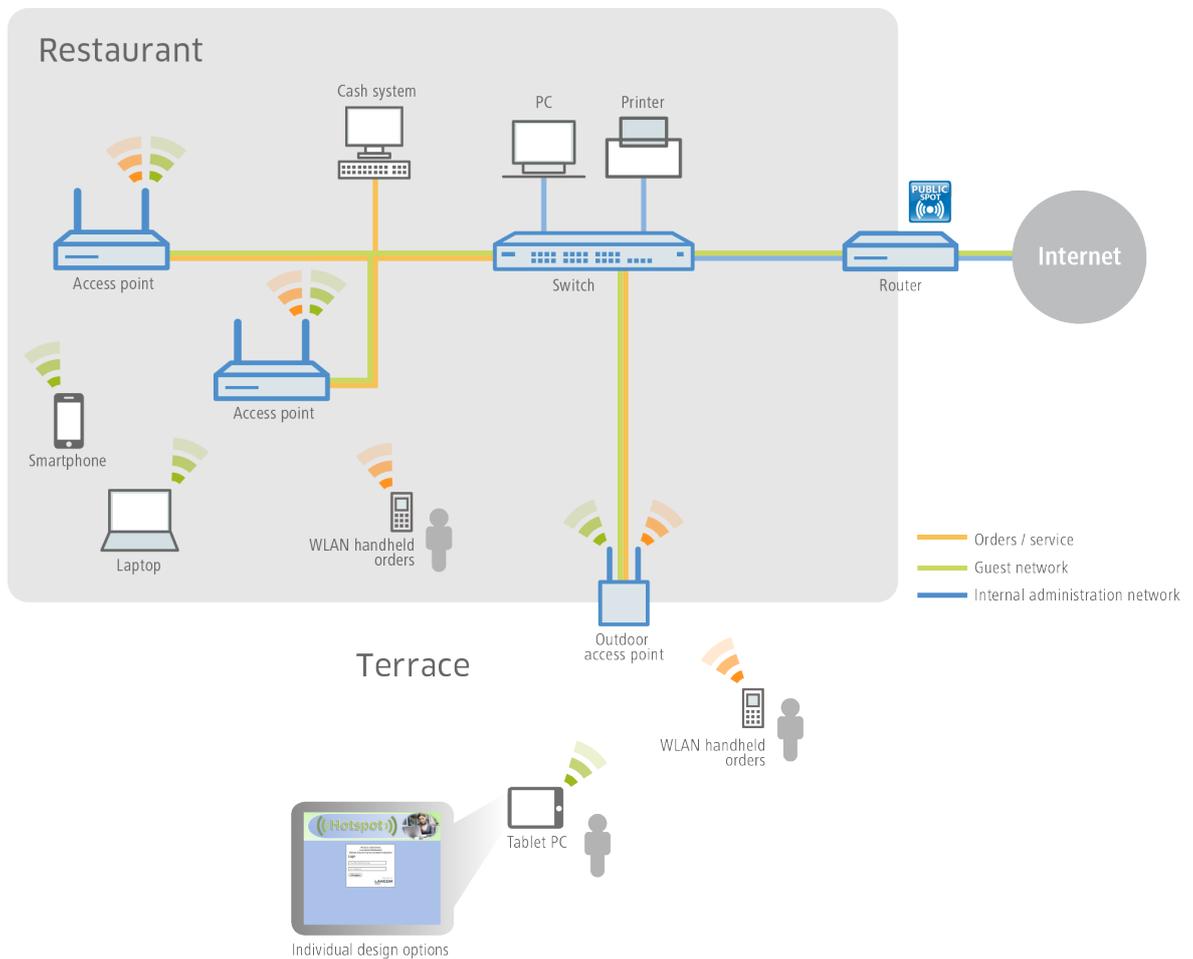


1.2.7 Guest access in gastronomy

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, guests benefit from a WLAN guest network in such a way that they can comfortably use 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 [Default and customized authentication pages](#) on page 89.
- **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 103.
- **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 20.

- **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 55.



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.

1.3.1 Open User Authentication (OUA)

Open User Authentication (OUA) is a method developed by LANCOM Systems. It 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.

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.

OUA can be employed universally

The big advantage of the OUA method is that it is completely based on standard protocols. This guarantees that OUA can be operated universally. It works with any (W)LAN adapter, can be seamlessly integrated in existing network infrastructures, and makes it possible to implement additional features, for example, when the WLAN is between cells during roaming.

1.3.2 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 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 Systems 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.

1.3.3 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.

1.3.4 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 use to login to the Public Spot network for the specified period.

The setup wizard **Manage Public Spot account** displays all registered Public-Spot user accounts in a table on a web page. With just one click you have the most important data for your users on one screen, and you can easily view the login status, information about login data and corresponding validity periods, extend a voucher, or delete a user account.

2 Enabling the Public Spot module

The Public Spot module is available by default on some devices, and the optional software can be purchased as an upgrade for the others. This chapter informs you how to activate the Public Spot module on your device at a later time. Activation takes place in four steps:

1. Ensuring that the prerequisites for installation are fulfilled
2. Online registration
3. Entry of the activating code
4. Checking the activation

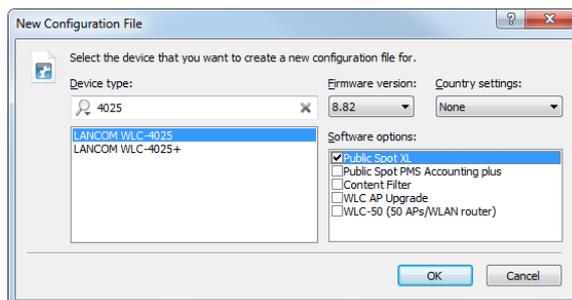
2.1 Installation prerequisites

2.1.1 Devices with optional Public Spot support

Make sure that all technical prerequisites are available to load the Public Spot module. Activation requires one of the following devices:

- LANCOM router
- LANCOM WLAN router
- LANCOM access point
- LANCOM WLAN controller
- LANCOM central-site gateway

If you are not sure whether your device fits the category listed, you can verify it using LANconfig: Click on the menu item **Edit > New configuration file...** and select the **Device type** from the window that opens. The **Software options** show you an overview of the optionally available modules.



For LANCOM routers, WLAN routers and access points, you will find the module under **Public Spot**. However, LANCOM WLAN controllers and central-site gateways use the designation **Public Spot XL**.

2.1.2 Package content

Please ensure that the Option package includes the following components:

- Data medium with management software (LANconfig, LANmonitor) and LCOS documentation
- Proof of license with a printed license number

2.1.3 Configuration computer with the Windows operating system

To activate the Public Spot module using LANconfig you need a computer with a Windows operating system. The computer must have access to the device that is to be configured. Access may be via the local network or even externally via remote access.

Alternatively you can also perform the activation using WEBconfig.

2.1.4 Latest management software

The latest version of LANconfig and LANmonitor are available for download from the LANCOM Systems homepage under www.lancom-systems.com/en/download. We recommend that you update these programs before continuing to the installation.

2.1.5 Latest device firmware

The latest firmware updates are available for download from the LANCOM Systems Web site under www.lancom-systems.com/en/download. Select your device from the list and download the firmware onto your computer.

 Detailed information about updating the firmware is available in the documentation for your LANCOM device.

2.2 Online registration

With the right firmware version, your device already has the complete Public Spot module installed, and it only has to be activated.

To activate the module you will need an activation code. The activation code is not included in the package. It will be sent to you on online registration. The delivery scope for the Public Spot module only contains the proof of license, where the license number is printed. You must register this license number once with LANCOM Systems and then you will receive an activation code.

 After successful online registration, the license number of your Public Spot module becomes invalid. The activation code that is sent to you can only be used with the LANCOM device as identified by the serial number which you provided at registration. Please ensure that you really only want to install the Public Spot option on the corresponding device. It is not possible to change to another device at a later date.

2.2.1 Necessary registration information

Please have the following information at the ready for your online registration:

- Exact designation of the module or the software option
- License number (from the proof of license)
- Serial number of your LANCOM (to be found on the underside of the device)
- Your customer data (company, name, postal address, e-mail address).

 Registration is anonymous and can be completed without specifying personal data. Any additional information may be of help to us in case of service and support. All information is of course treated in the strictest confidence.

2.2.2 Online entry of registration information

1. Start a web browser and access the LANCOM Systems web site under www.lancom.eu/routeroptions.

2 Enabling the Public Spot module

2. Enter the information as required and follow the instructions that follow. After entering all of the data, we will send you the activation code for your device and your customer data. If you submit an e-mail address, we will send you the data including the activation code via e-mail. Online registration is now complete.

 Make sure you store your activation code safely! You may need it at a later date to activate your Public Spot module again, for example after a repair.

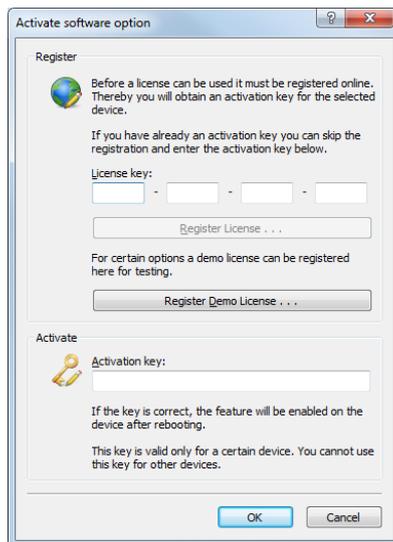
2.2.3 Help in case of problems

Help for problems registering your software option can be found in <http://www.lancom-systems.com/service-support>.

2.3 Enabling the Public Spot module

Enabling the Public Spot module is very simple. Please mark the desired device in LANconfig and in the menu select: **Device > Enable Software option...** Alternatively, click on the entry for the device with the right-hand mouse key and select **Enable Software option...** from the context menu.

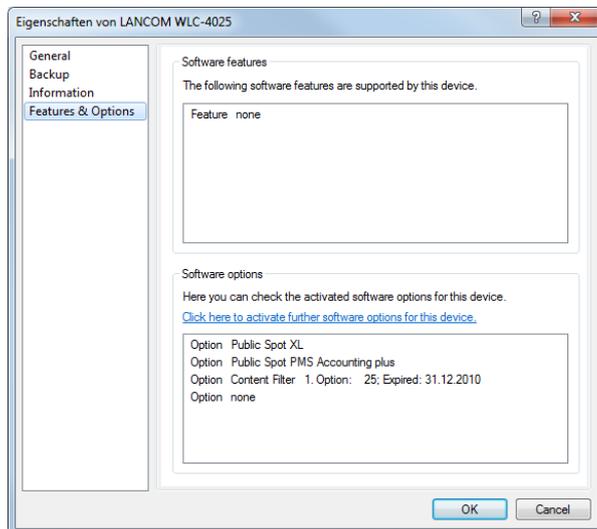
Under WEBconfig select the menu command **Extras > Enable Software option**.



In the following window, enter the activation code that you received with the previously described online registration. The device will then restart automatically.

2.4 Checking the activation

To check the successful activation of your Public Spot module, choose the device and in the menu select: **Device > Properties > Features & Options**. Here you can see a list of available software options.



For LANCOM routers, WLAN routers and access points, you will find the module under **Public Spot**. However, LANCOM WLAN controllers and central-site gateways use the designation **Public Spot XL**.

3 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 pre-configured for a simple application scenario (login using voucher).

- **2) 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.

- **3) 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.de/en/publications/products.

3.1 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.

3.1.1 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.

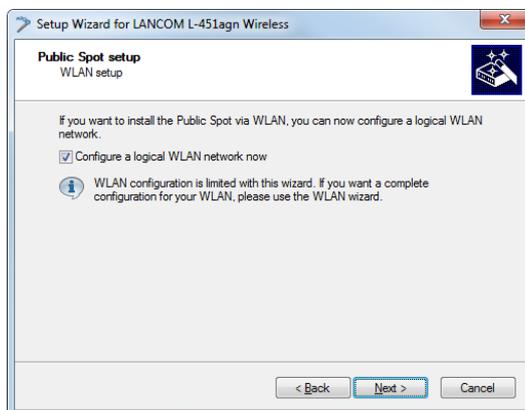
 The wizard for the basic configuration of the Public Spot shows different dialogs depending on the device type and your previous choices. This tutorial is only an example.

1. To do this, start LANconfig and select the device for which you want to set up the Public Spot, for example, a LANCOM access point.

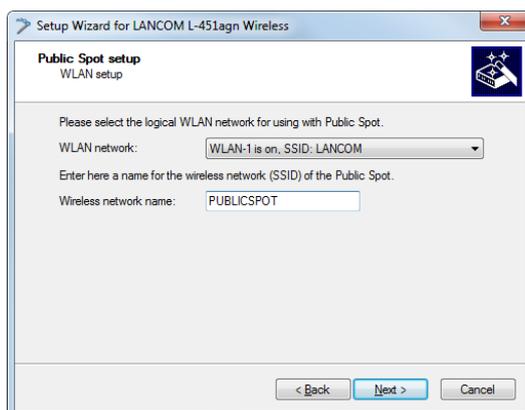
2. Start the Setup Wizard with **Device > Setup wizard**, select the action **Setup Public Spot** and then click **Next**.



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 (SSID). Click on **Next**.



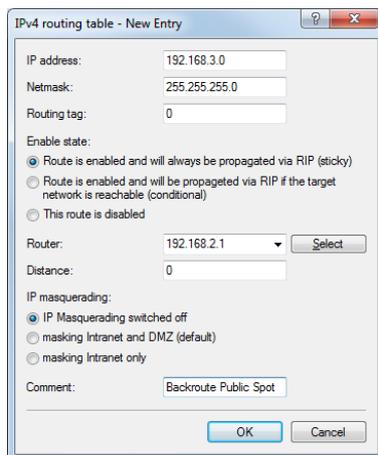
5. Assign the IP address and netmask to the device that your Public Spot network should specify and click **Next**. The Public Spot module has its own address on your network, which is independent from the address that you assigned to your device. For example, if you have a 192.168.0.0/24 network set 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.



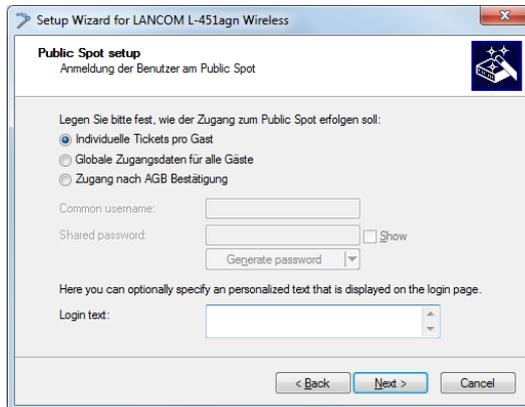
- ! If your device is not directly connected to the Internet and you have a different address range for your Public Spot, you must set up a return route to your Public Spot network on your Internet gateway. If there is no return route, Public Spot users will see an HTTP error after they have successfully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

Please find the directions on how to set up a return route, in the documentation for your Internet gateway. If it is a LANCOM device, you can configure it 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.



- 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**.

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 section [Customized text on the login page](#) on page 91).

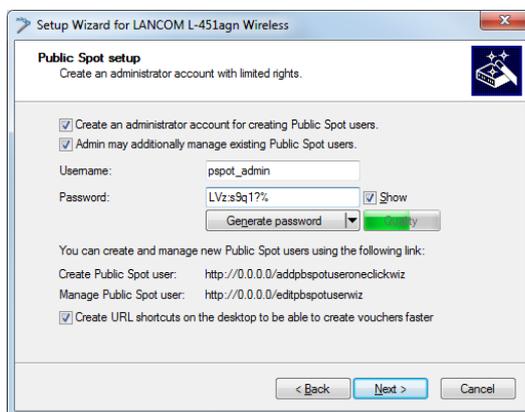


7. If necessary, create an administrator with limited rights who can use the setup wizards in WEBconfig to create and manage Public Spot users. To continue, click on **Next**.

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.

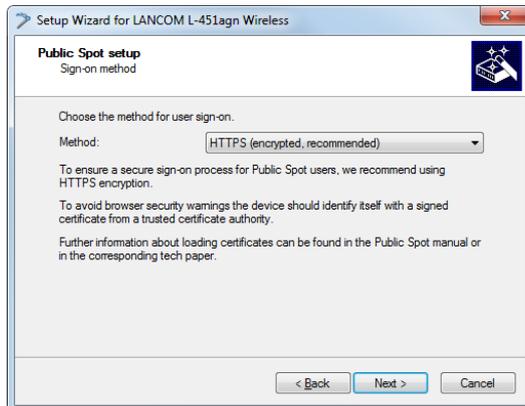
The **Manage Public Spot accounts** wizard enable the administrator to manage the users. The administrator can extend or reduce the validity period of access, or completely delete a specific user account. In addition, the administrator can call up information about the user account using the wizard,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



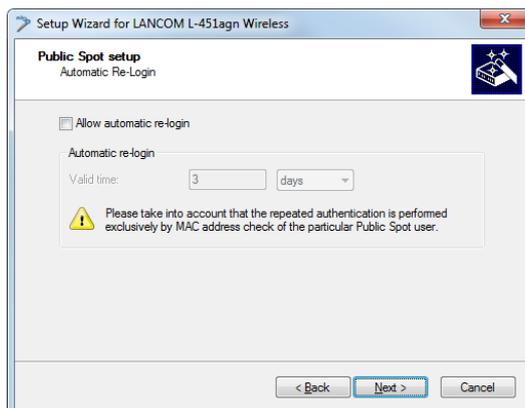
- ⚠ Make sure that the password you create is secure. The Setup Wizard will check the quality of the password you enter. For passwords that are not secure the input field appears in red, when it is more secure it changes to yellow, and when it is very secure the background turns green.

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

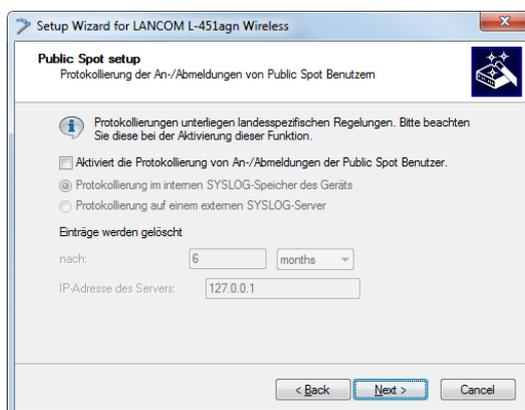
You can select **HTTPS** or **HTTP** in the drop-down list. Using a connection with HTTPS provides a secure connection for Public Spot users.



9. 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.

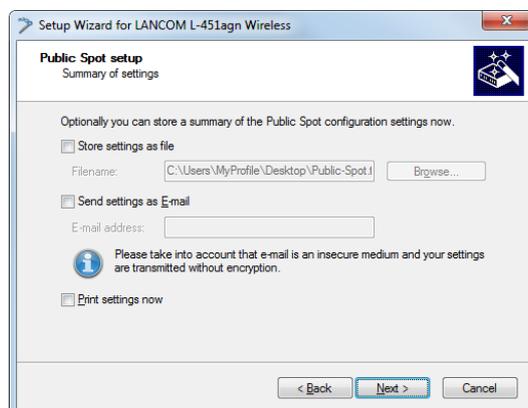


10. If needed, enable logging of logins and logouts for Public Spot users in the internal SYSLOG storage of your device. To continue, click on **Next**. Since the logs comply with country-specific regulations, this option is disabled by default. Before enabling this function, you need to determine what the data protection regulations are for your country in order to avoid any legal issues.



11. Save your changes if necessary.

Before you save the configuration to your device, you have the option of saving the configuration locally on your PC, sending it by e-mail, or printing a summary.

**12. 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, router, WLAN controller, etc.) or complexity of the network configuration (e.g., use of VLAN or ARF), different or additional steps may be required for setting up a Public Spot. 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 for which you want to set up the Public Spot, for example, a LANCOM 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):

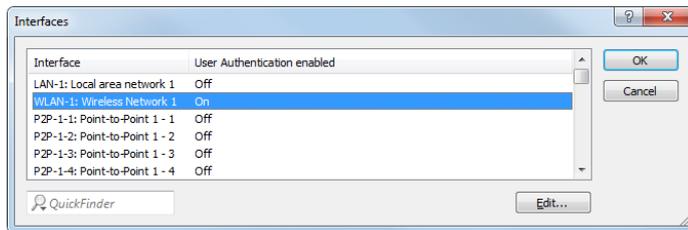
- LANconfig: **Date/time > General**

! 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, you can integrate additional access points into a LANCOM Wireless router Public Spot. For an access point select, for example, the logical WLAN interface **WLAN-1**.

- LANconfig: **Public Spot > Server > Interfaces**

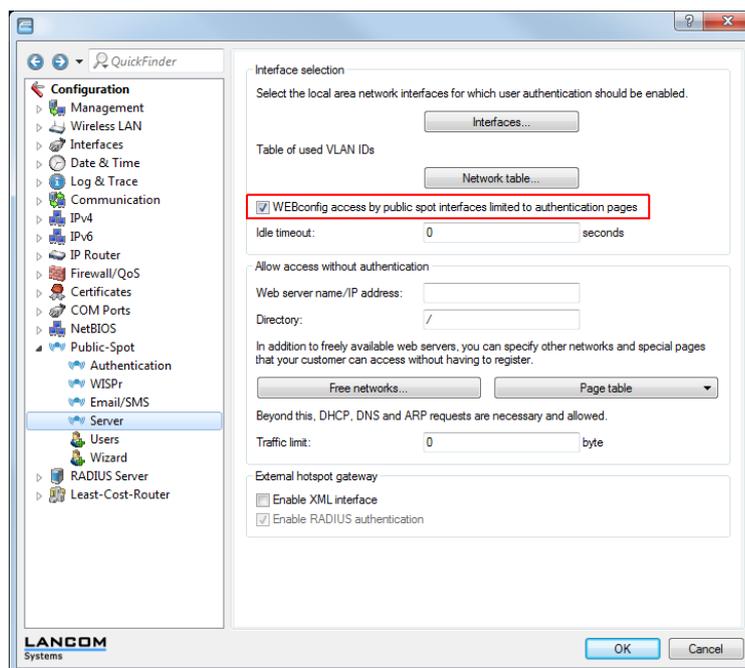


By activating the authentication for a WLAN interface, you automatically release the associated SSID for the Public Spot operation.

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

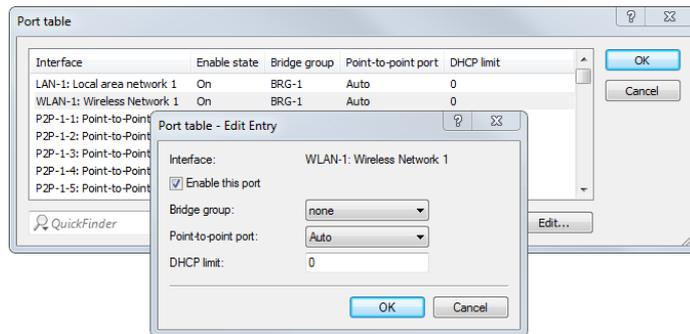
- Access to your device from the Public Spot network should be restricted to the authentication pages. If you do not restrict access, Public Spot users will be able to access the configuration interface of your device (WEBconfig). For security reasons you should not permit this.

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



- 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 each other using different interfaces of a LANCOM (e.g., between LAN-1 and WLAN-1), these interfaces are logically connected to each other (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**

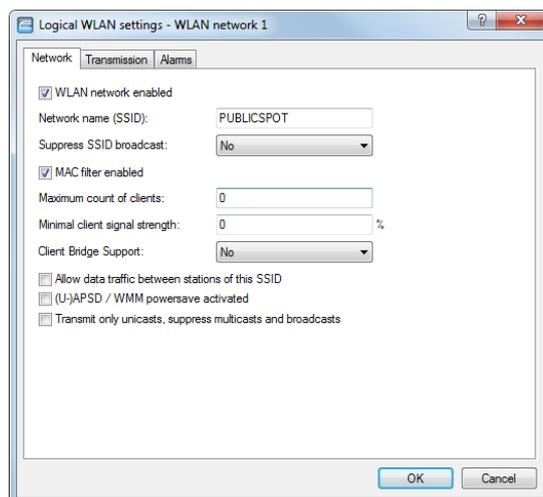


6. Enable the WLAN for the Public Spot.

This setting does not affect: LANCOM 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).

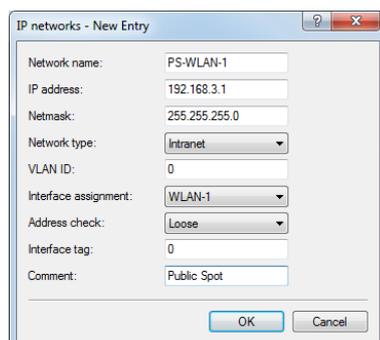
- LANconfig: **Wireless LAN > General > Logical WLAN settings > WLAN network <number> > Network**



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. If it is a LANCOM device, you can configure it 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.

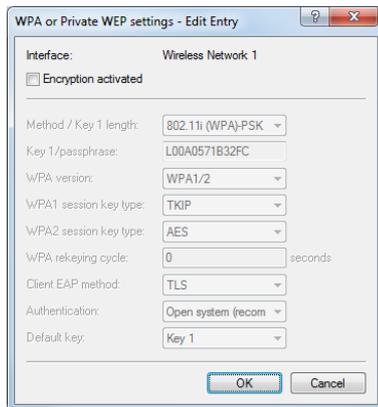
8. Configure the DHCP server settings for the Public Spot network.
Since the device has an IP network that is independent from the network where it is located, you must configure a DHCP server for this network. For the previously set up IP network (e.g., PS-WLAN-1), set the value for **DHCP server enabled**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

- LANconfig: **Wireless LAN > 802.11i/WEP > WPA or Private WEP settings**

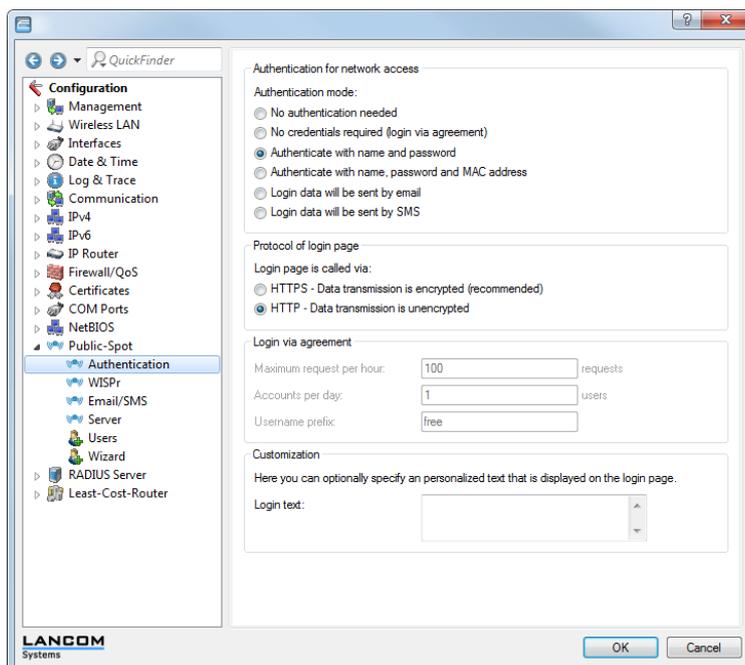


- Select the authentication mode and the protocol used for the user login.

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.

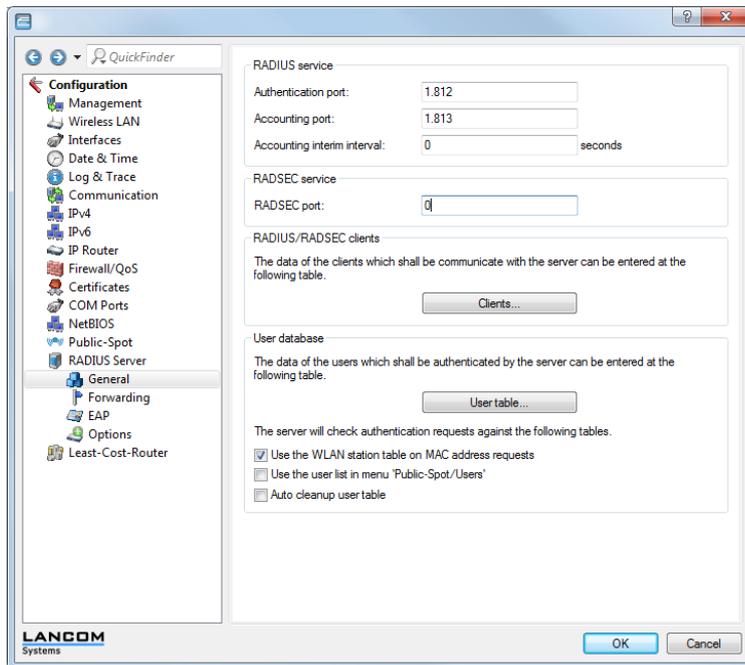
- LANconfig: **Public Spot > Authentication > Authentication mode**



- Specify the internal RADIUS server as the server responsible for user administration and accounting. To do this, enter the **Authentication port1 . 812** and **Accounting port1 . 813**.

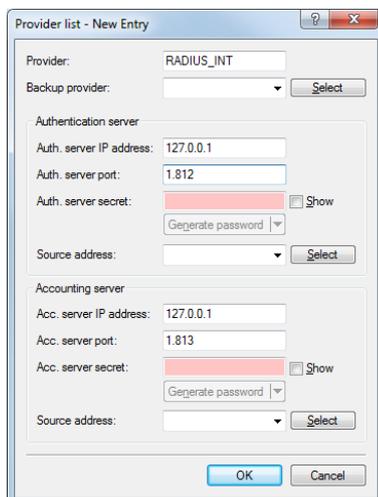
You store Public Spot access accounts in the user database on the device's own RADIUS server. In order to use Public Spot access accounts, you **must** configure the RADIUS server and the Public Spot module to use the RADIUS server.

- LANconfig: **RADIUS server > General**



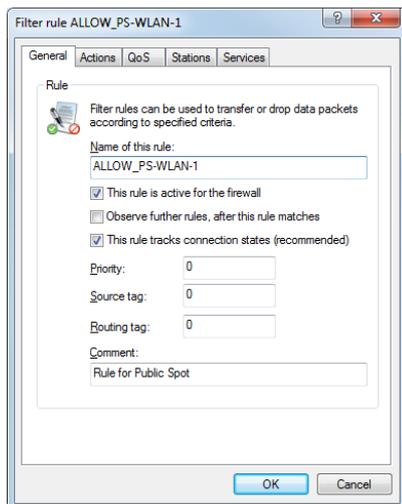
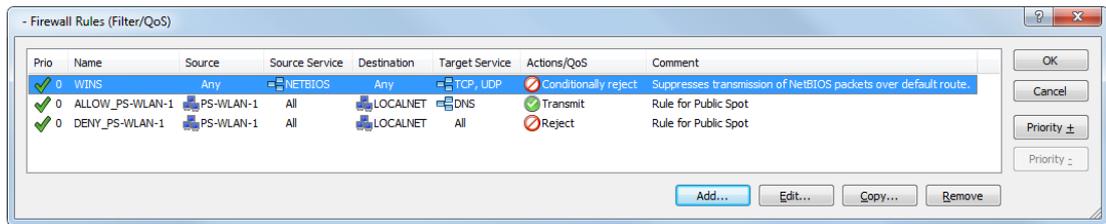
- Create an entry for the internal RADIUS server in the list of authentication servers of the Public Spot. Under **Auth. server IP address** and **Acc. server IP address** enter the loopback address 127.0.0.1. Use the **Auth. server port** and **Acc. server port** used for the authentication port and accounting port in the previous settings. 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 > Authentication servers**



- 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 top to bottom of the list.

- LANconfig: **Firewall/QoS > IPv4 Rules > Rules...**



- "Accept" rule settings:

- Enter the name of the rule in **General**, for example, `ALLOW_PS-WLAN-1`.
- Remove all possible predefined action objects from the list and using **Actions > Add..** add an action object of type **ACCEPT**.
- In **Stations > Connection source**, enable the option **Connections from the following stations** and select **Add... > Add custom station**.
- 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**.
- In **Stations > Connection destination**, enable the option **Connections to the following stations** and after selection **Add...** choose **LOCALNET**.
- In **Services > Protocol/target services** enable the option **Following protocol/target services** and select **Add... > DNS**.
- End the filter rule dialog with a final click on **OK**.
LANconfig then enters the allow rule into the rule table.

- "Reject" rule settings

- Enter the name of the rule in **General**, for example, `DENY_PS-WLAN-1`.
- Remove all possible predefined action objects from the list and using **Actions > Add..** add an action object of type **REJECT**.
- In **Stations > Connection source**, enable the option **Connections from the following stations** and select **Add... > Add custom station**.
- 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**.
- In **Stations > Connection destination**, enable the option **Connections to the following stations** and after selection **Add...** choose **LOCALNET**.
- End the filter rule dialog with a final click on **OK**.
LANconfig then enters the rejection rule in the rule table.

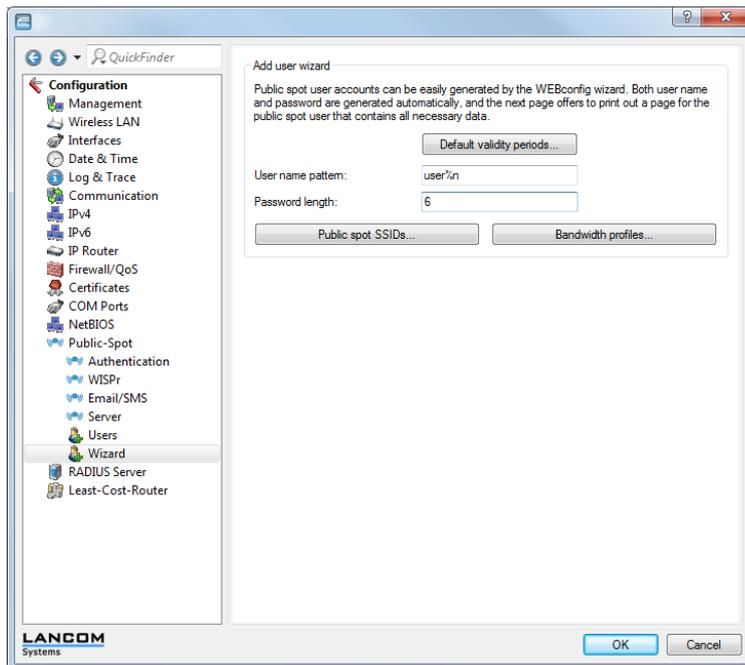
14. Store the configuration on your device.

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.

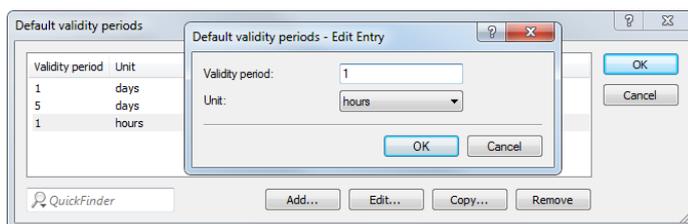
3.1.2 Setting default values for the Public Spot wizard

The following section describes how you define default values for the new-user wizard (**Create Public Spot account**).

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

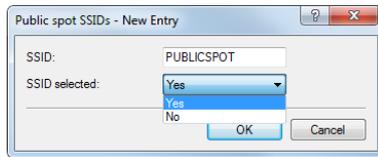


3. In **Default validity periods**, define which default validity periods for user accounts and vouchers are to be available by default.
The new-user wizard takes the shortest validity period as the default.



4. In **User name pattern** you indicate what pattern is 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`.
5. Using **Password length** you specify the length of the passwords that the new user wizard generates for Public Spot access. The default 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.

- 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, WLAN controller or WLAN router, for example, you can select several network names as default values in order to give users access to various different WLANs (e.g., for WLANs in the hotel lobby, the conference room, and floors where their rooms are located). 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 display order of the SSIDs. In this way, SSIDs that are used most often can be kept at the top of the list.

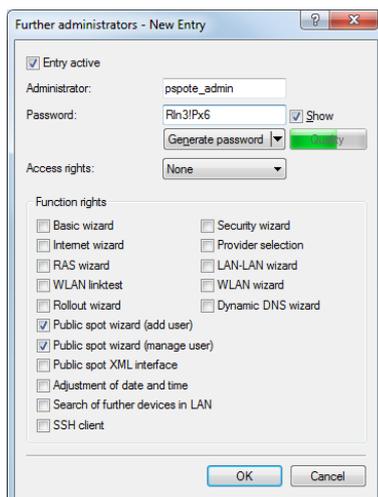
3.1.3 Setting up limited administrator rights for Public Spot managers

In order for employees to be able to manage a Public Spot on the device without further permissions, you can explicitly assign them the function rights to use the Public Spot wizard. This tutorial describes the steps to set up Public Spot function rights for employees without giving them additional administrator rights.

 You need to have the "Supervisor" permission to be able to assign Public Spot management to an employee.

- Start LANconfig.
- Open the configuration for the device for which you want to register a Public Spot administrator. The Public Spot option has to be enabled on this device.
- Change to the view **Management > Admin**, click in the section **Device configuration** on **Further administrators**, and then click on **Add**.

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



- You activate the profile by checking the **Entry enabled** box.
- Assign a descriptive name in the field **Administrator**.
- Enter a **password** and repeat it to be sure.
- Set the **Access rights** to **None**.

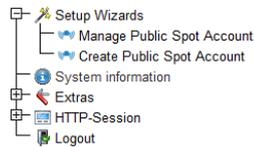
When you modify an existing user, you should not modify existing function rights.

- In the section **Function rights** enable the **Public Spot wizard (add user)**, and **Public Spot wizard (manage user)**.

When you modify an existing user, you should not modify existing function rights.

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

The Public Spot administrator is offered the Public-Spot wizards in the navigation when they log on using WEBconfig.



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.

Using the user management wizard **Manage Public Spot account**, the administrator has the option of managing these users as well as the users that you created as the main administrator using the RADIUS user database. 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 plain text, the authentication status, the IP address, the sent/received data volume or any restrictions that apply to the account.

 The function right **Public Spot XML interface** is not needed by a normal Public Spot admin. 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.

3.1.4 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**, in order to create a new Public Spot user.

- 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.

Starting time for account:	first login	
Validity period: voucher expires after:	365	days (max. 10 characters)
Duration:	1 Hour(s)	
Max-Concurrent-Logins:	Unlimited	
<input type="checkbox"/> Multiple-Login		
Bandwidth profile:	Visitor	
SSID (Network Name):	WLAN-Public	WLAN-Private
Number of vouchers:	1	(possible values: 1 - 100) (required)
Time budget (minutes):	0	(possible values: 0 - 100000)
Volume budget (MByte):	0	(possible values: 0 - 4000)
Comment (optional):		(max. 49 characters)
<input type="checkbox"/> Print comment on voucher		
<input checked="" type="checkbox"/> Print		
<input type="checkbox"/> User name case-sensitive		

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. Possible values are:
 - `First login`: Access is valid as of the user's initial login
 - `Immediately`: Access is valid as of the creation of the user's account

! 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. The pre-defined values are:
 - 1 Hour(s)
 - 1 Day(s)
 - 5 Day(s)
- **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**. The pre-defined values are:
 - Unlimited

- Only 3 device(s)
- Only 10 device(s)
- **Multiple login:** Select this option in order to allow a user 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.

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** 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.

Show 10 entries per page														Show/Hide Column	Save as CSV	
Page	User Name	Password	Comment	Expiry Type	Abs. Expiry	Rel. Expiry	Time Budget	Volume Budget	Case Sensitive	Tx.Limit	Rx.Limit	Online-Time	Traffic (Rx/Tx Kbyte)	State	MAC Address	IP Address
<input type="checkbox"/>	user5498	7cjd6	publicUser created by root on 23.05.2013 16:47:37 ()	Absolute and Relative	05/23/2014 16:07:37	0	0	0	No	0	0	0	0	Unauthenticated	00:00:00:00:00:00	0.0.0.0
<input type="checkbox"/>	user5573	4ndmfsm	publicUser created by root on 24.05.2013 09:51:58 ()	Absolute and Relative	05/24/2014 09:51:58	0	0	0	No	0	0	0	0	Unauthenticated	00:00:00:00:00:00	0.0.0.0

Showing 1 to 2 of 2 entries

First page Previous page 1 Next page Last page

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**.
- **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:** Shows the authentication status of the individual users. Possible values are:
 - **Unauthenticated:** The user is currently not logged on to the Public Spot.
 - **Authenticated:** The user is currently logged on to the Public Spot.
- **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**
 - **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.

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 > General**. 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 > General > User database**

❗ 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.

3.2 Security settings

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

3.2.1 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 a 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: **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 packages 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**

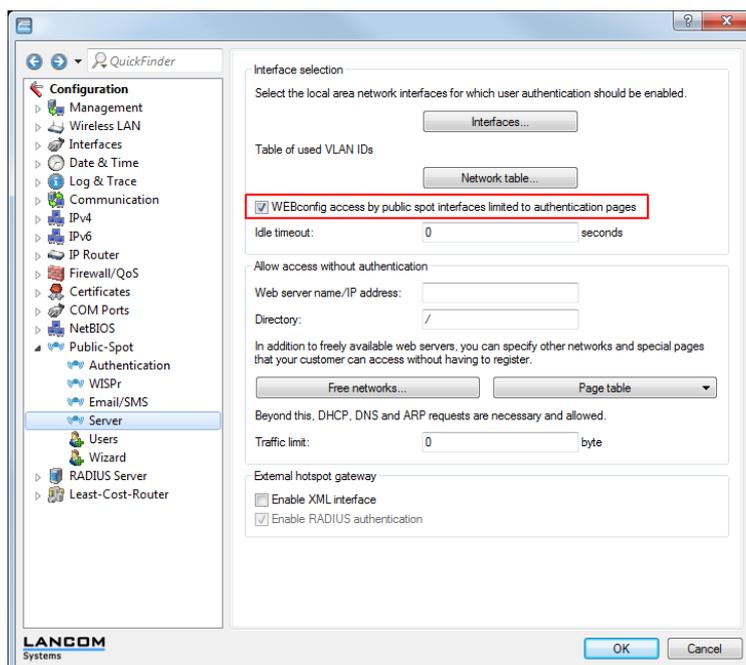
On the one hand the optimal value for traffic limit depends on the data volume of the login page. On the other hand, this value has a significant effect on the potential number of failed login attempts per user. Generally, a traffic limit of 60,000 bytes provides effective protection for a Public Spot 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.

3.2.2 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 > 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.

3.3 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.

3.3.1 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 **Add user wizard**. 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.

Starting time for account: first login

Validity period: voucher expires after: 365 days (max. 10 characters)

Duration: 1 Hour(s)

Max-Concurrent-Logins: Unlimited

Multiple-Login

Bandwidth profile: Visitor

SSID (Network Name): WLAN-Public
WLAN-Private

Number of vouchers: 1 (possible values: 1 - 100) (required)

Time budget (minutes): 0 (possible values: 0 - 100000)

Volume budget (MByte): 0 (possible values: 0 - 4000)

Comment (optional): (max. 49 characters)

Print comment on voucher

Print

User name case-sensitive

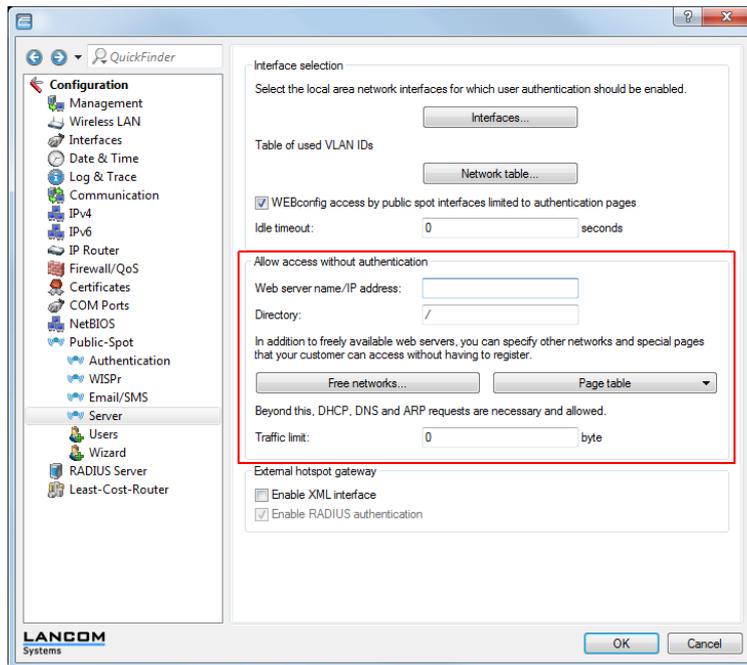
3.3.2 Open access networks (no login)

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 > Web server name/IP Address**

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 > Directory**



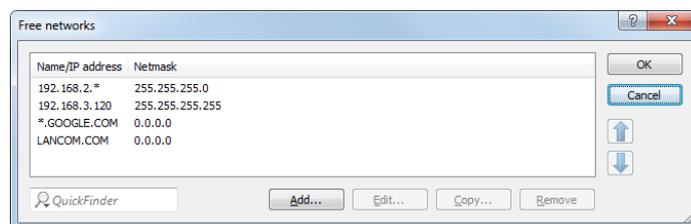
In addition to freely available web servers, you can define other networks and special sites which your customers can access without having to log on.

- LANconfig: **Public Spot > Server > Free networks or Page table**

- 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 `*.google.com` allows the addresses `mail.google.com`, and `maps.google.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.



- 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 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**.

3.3.3 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://<deviceURL>/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>:<FieldName5>
```

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.

expiretype

Combined output of expiry type and validity period of the voucher.

Specify this parameter as follows:

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

The parameter values have the following meaning:

- Value1: Expiry type (absolute, relative, absolute and relative, none)
- Value2: Voucher validity period

If these parameters are 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

If this parameter is omitted, 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.

maxconclgin

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

User name 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.

expiretype

Combined output of expiry type and validity period of the voucher.

Specify this parameter as follows:

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

The parameter values have the following meaning:

- Value1: Expiry type (absolute, relative, absolute and relative, none)
- Value2: Voucher validity period

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>/andpbspotuser/...?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.

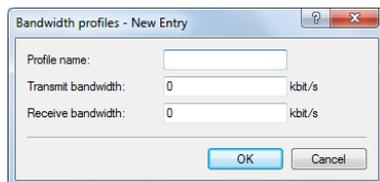
If the wizard cannot find the specified user, it displays a table of registered Public Spot users. Mark the entries for deletion here.

3.3.4 Bandwidth profile

As of LCOS 8.82 you have the option of setting up bandwidth profiles for Public Spot users.

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. These profiles can be assigned to new users when access is created for the Public Spot by calling the Setup-Wizard **Create Public Spot account** in WEBconfig.



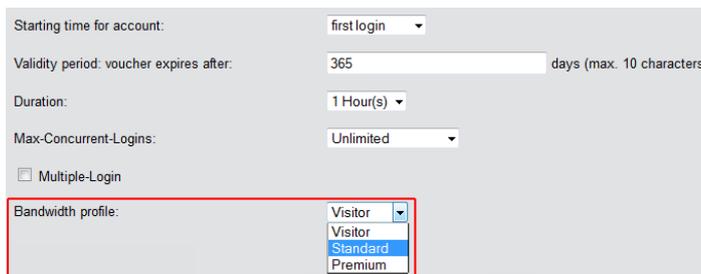
In order to edit the entries in the table **Bandwidth profiles**, click on the button **Add...**. The entries in the edit window have the following meaning:

- **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.

3.3.5 Clear user list automatically

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 > General > Clear user lists automatically**

! 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
<ul style="list-style-type: none"> ■ access points ■ Routers from the 178x series with "Public Spot" option	64
<ul style="list-style-type: none"> ■ WLC-4006(+) 	256
<ul style="list-style-type: none"> ■ WLC-4025 ■ WLC-4025(+) ■ WLC-4100 ■ 7100(+) VPN ■ 9100(+) VPN with "Public Spot XL" option	unlimited*

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

3.3.6 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 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, this may take up to an hour.

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.

Surveillance

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

3.3.7 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.

3.3.8 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 > Server** under **Authentication servers**.

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 plain text.

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.

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 `JohnDoe@lancom.de` contains the authentication server entry named `LANCOM`. 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 still exists. 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. These settings can be made in **RADIUS server > Options**.

3.3.9 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).

3.3.10 Billing via 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 > 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.

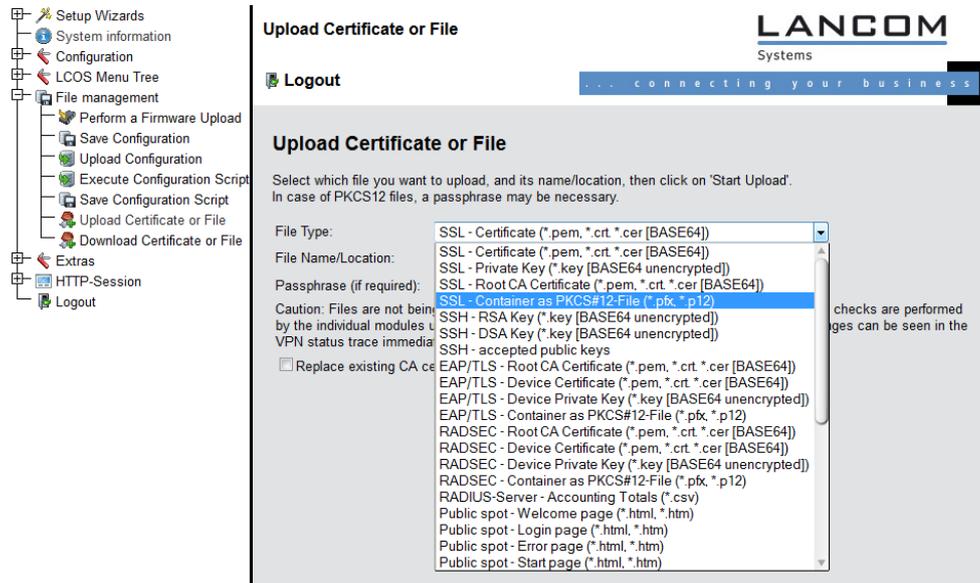
-
- ⓘ User sessions are not paused while the device sends accounting requests, which consumes additional resources in the device—in contrast to authentication. Please ensure that the time required for the selection of an accounting server* should be less than the length of an accounting cycle for interim 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)*

3.3.11 Multi-level certificates for PublicSpots

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 example by using WEBconfig 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 **Setup > Public Spot Module > Device Host Name**). This name has to be resolved by the DNS server to provide the corresponding IP address of the Public Spot.



3.3.12 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.

The screenshot shows a dialog box titled "User table - New Entry". It contains several input fields and checkboxes. The "VLAN ID" field is highlighted with a red rectangle and contains the value "0". Other fields include "Name / MAC address", "Password" (with a "Generate password" button and a "Show" checkbox), "Passphrase (optional)" (with a "Generate password" button and a "Show" checkbox), "TX bandwidth limit" and "RX bandwidth limit" (both set to "0 kbit/s"), "Station mask", "Calling station", and "Called station". There are also "Validity/Expiry" settings, including "Expiry type" (set to "Relative & absolute"), "Relative expiry" (set to "0"), and "Absolute expiry" (set to "00 : 00 : 00"). A "Multiple login" checkbox is checked. At the bottom, there are "OK" and "Cancel" buttons.

- Open the **User table** in the dialog **RADIUS server General** 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.

3.4 Alternative login methods

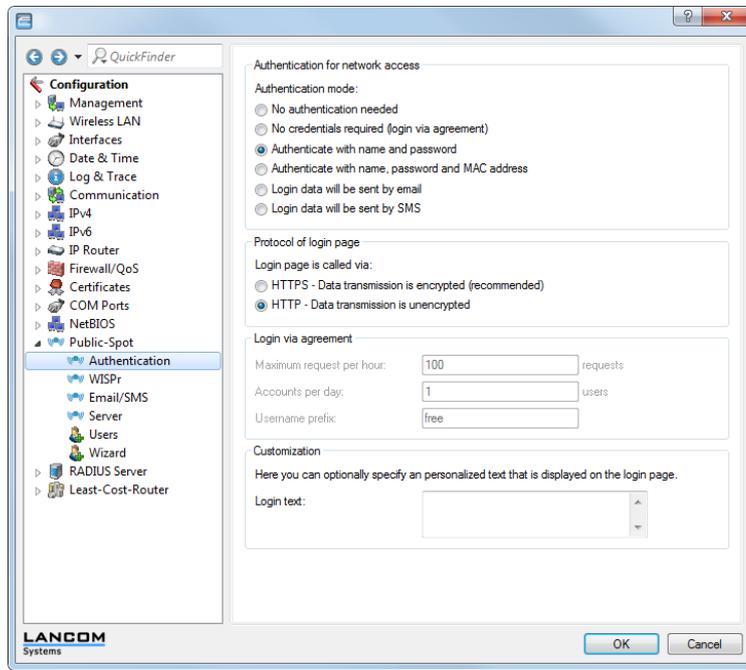
In addition to the login using the login data that was sent previously, your users can also request login data themselves via e-mail or text message (SMS), or by accepting the terms and conditions for the Public Spot (one-click login). Alternatively, in order to implement more complex or multi-level login scenarios, you can 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.

3.4.1 Overview of authentication modes

In this window, specify the settings for authentication to the network.



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 accept the operator's terms of use (one-click login). With a RADIUS server, login is completely transparent for the user. The prerequisite is that you have set up an individual welcome page with its own terms of use: In this case, the Public Spot initially forwards a user to the welcome page, where he must agree to the terms of use. After confirmation, the device automatically creates a user account according to the default values in the **Add user wizard** (under **Public-Spot > Wizard**) and provides access to the connected network.

Under **Login after agreement** you specify the framework 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.

 To load a custom welcome page (htm, html) on the device, use the upload function under **Device > Configuration management > Upload certificate or file** and reference this file under **Public-Spot >**

Server > Page-Table > Welcome in the field **Page address (URL)** with `file:///pbspot_template_welcome`. Templates for a welcome page and detailed information for uploading your own templates is available on the Internet in the LANCOM Support Knowledge Base under [Implementing your own websites](#).



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 a special page that is displayed only after a separate activation in connection with notification by e-mail/SMS.



If no welcome page is set up, 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.

- **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.

3.4.2 Independent user authentication (Smart Ticket)

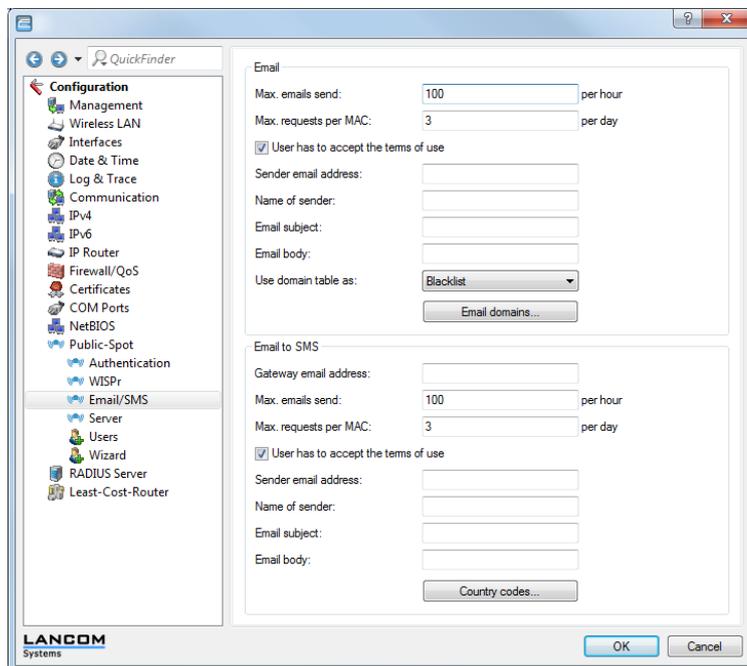
Devices operating a Public Spot provide users with time-limited access to wireless networks. Until now an administrator account was necessary to create a login on a device with the Public Spot. For employees at a hotel reception desk, for example, you can set up an administrator account that only has the function rights to create Public Spot users. With a few mouse clicks the employee can print a voucher for the hotel guests for access to the wireless network.

However, the easy 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 from the homepage of the Public Spot, and send it to themselves by e-mail or SMS (text message). In order to send e-mail, an SMTP account must be fully set up in the device settings. To send SMS/text messages the device uses an external SMS provider, which can charge fees to the Public-Spot operator or user, if desired.

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 checking the terms of use, whereby the user must first consent to the terms of use stored on the device before automatically receiving access to the Public Spot (one-click login). The creation of credentials by the user via e-mail or SMS does not apply for this authentication method.

Configuring e-mail/SMS authentication

You define the settings for sending the login credentials via e-mail or SMS in the dialog **Public Spot > E-mail/SMS**.



You have following configuration options:

- **Max. e-mails send:** Here, 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.
- **Max. requests per MAC:** Specify how many different sets of credentials the device can provide to a MAC address within one day.
- **User has to accept the terms of use:** If you select this option, the Public Spot login page displays an additional option, which prompts the user to accept the terms of use before registering via e-mail/SMS.



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.

- **Sender e-mail address:** Enter the e-mail address that your e-mail contains as the return address, e.g. `support@providerX.org`.
- **Name of sender:** Specify the name shown to your users as the sender of the e-mail, e.g. `Provider X`. If you leave this field blank, the device automatically enters the default text as described in the following section.
- **E-mail subject:** Type the subject line for the e-mail. If you leave this field blank, the device automatically enters the default text as described in the following section.
- **E-mail body:** Type the message text for the e-mail. You can use the following variables:

\$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 enables Public Spot users to log off from the Public Spot. This may be useful if the session window (which also contains this link) that is normally displayed after a successful login is blocked by the browser or closed by the user.

If you leave this field blank, the device automatically enters the default text as described in the following section.

- **Use domain table as:** Specify whether the device uses the table **E-mail domains** as a blacklist or whitelist. 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.
- **Gateway e-mail address:** Here 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`.
- **Country codes:** In this table, enter the country codes accepted by the device. 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.

Standard texts for sender, subject and body

If you leave the following input fields in the dialog **Public Spot > E-mail/SMS** blank, the device automatically reverts to the standard texts stored in LCOS when generating the e-mail. The language used depends on the language setting of the browser used by the user for registration.

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

	German	English
Name of sender	Public Spot	Public Spot
E-mail subject	Ihre Anmelde Daten für den Public Spot	Your Public Spot account
E-mail body	Ihr Passwort für den LANCOM Public Spot: <code>\$PSpotPasswd \$PSpotLogoutLink</code>	Your password for the LANCOM Public Spot: <code>\$PSpotPasswd \$PSpotLogoutLink</code>

3.4.3 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.

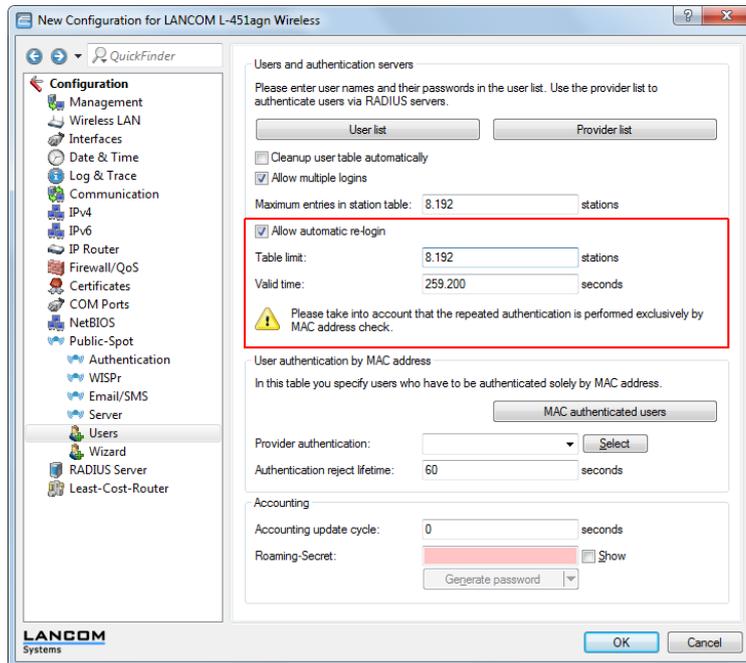
With automatic re-login, the user only has to be identified on the Public Spot once. After a temporary absence, the user can seamlessly use the Public Spot again.

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.

3.4.4 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 to allow users to authenticate themselves. 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**.

The 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 does not have a valid authentication for the MAC address saved in the cache of the Public Spot, the Public Spot starts authentication on the corresponding RADIUS server. After a positive response, the Public Spot starts a new session for that user and forwards the associated packages.
- All of the above checks are unsuccessful, 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 permissible addresses, the Public Spot can alternatively authenticate 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. This lifetime is used by the Public Spot to prevent the RADIUS server from being flooded with repeated requests for MAC addresses which cannot be authenticated (without login) via the RADIUS server or MAC address table.

If a MAC address authentication is rejected by the RADIUS server, the Public Spot saves 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 in LANconfig

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



3.4.5 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.

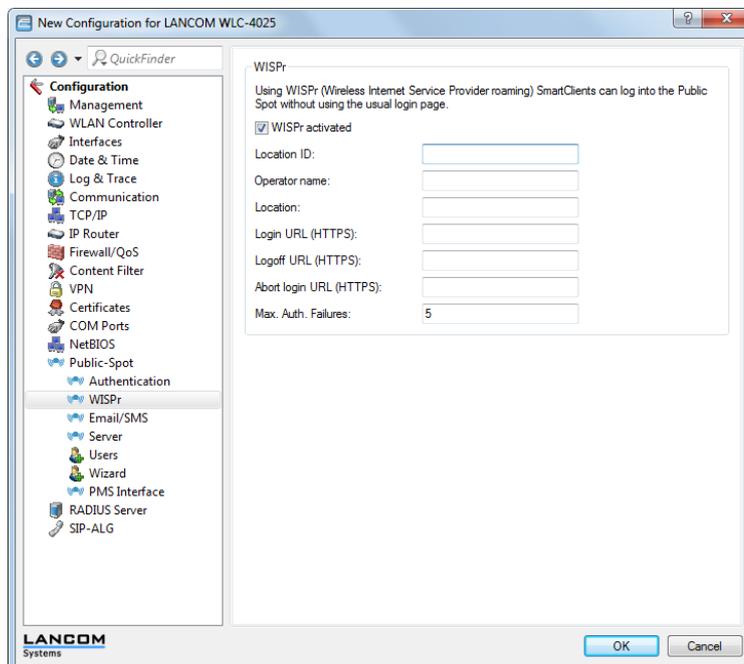
Example for an XML-Tag in redirect:

```
<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. Further information about loading these objects on your device can be found in the LANCOM techpaper "Certificate Management in Public Spots". 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.

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 LANCOM Public Spot itself. If the LANCOM Public Spot should authenticate users using WISPr, enter the URL in the format `https://<FQDN-of-the-LANCOM>/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 LANCOM domain, for example:

- Login URL: `https://<FQDN-of-the-LANCOM>/wisprlogin`
- Logoff URL: `https://<FQDN-of-the-LANCOM>/wisprlogoff`
- Abort-Login-URL: `https://<FQDN-of-the-LANCOM>/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.

3.4.6 IEEE 802.11u and Hotspot 2.0

As of LCOS 8.82, your device supports WLAN connections according to the IEEE 802.11u standard and—based on that—the Hotspot 2.0 specification. 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-enabled 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.

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 Pass Points™. Certain LANCOM access points are Passpoint™ CERTIFIED by the Wi-Fi Alliance.

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 802.11-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

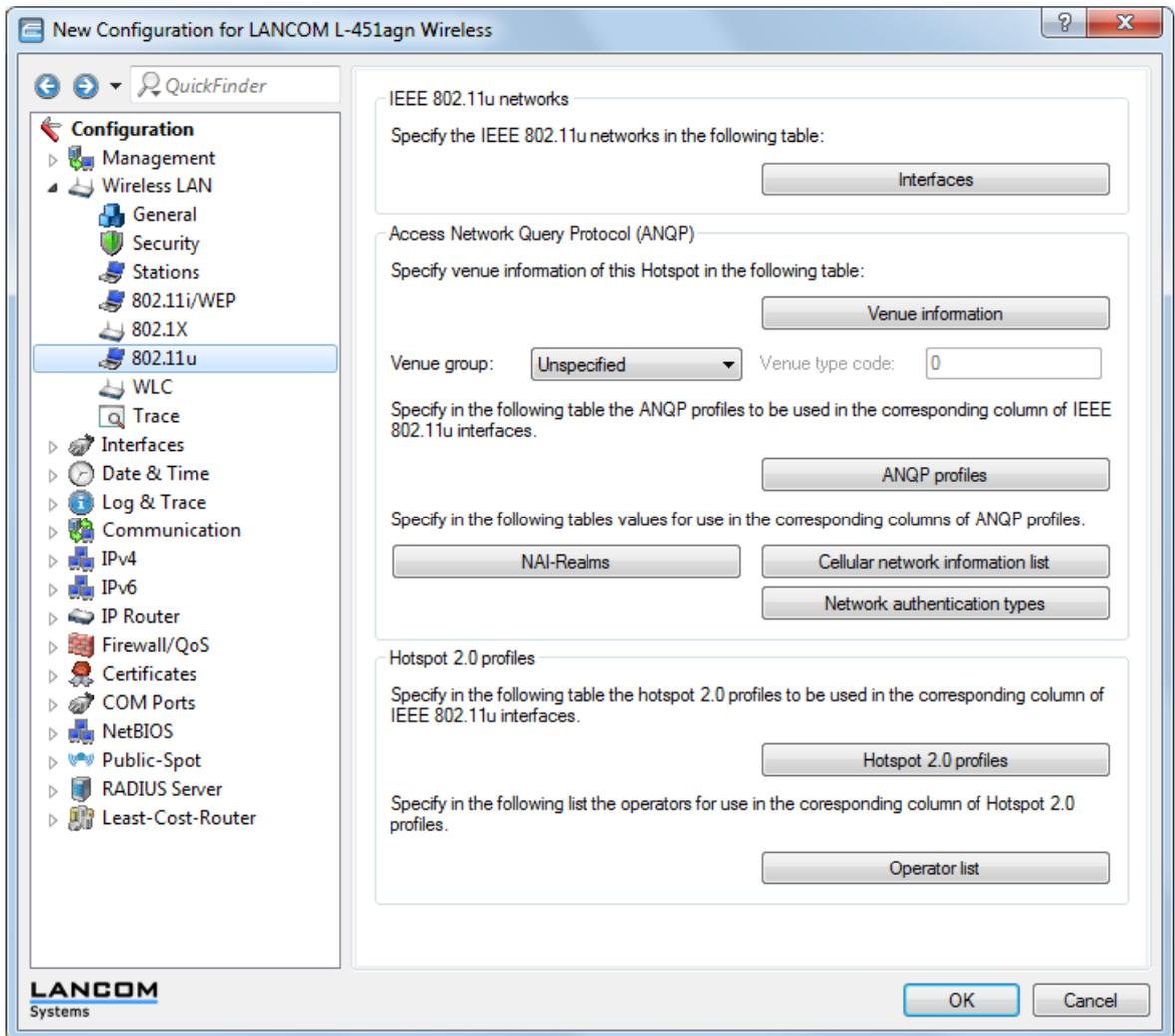
The Hotspot 2.0 specification recommends the following general settings for the 802.11u operator:

- 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 (new in LCOS 8.82)
- 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**.
- Enabled and implemented firewall on the access router, which provides Internet access

Configuration menu for IEEE 802.11u / Hotspot 2.0

You can find the configuration menu for IEEE 802.11u and Hotspot 2.0 under **Configuration > 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 of the parameters that need to be configured are located in so-called "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
```

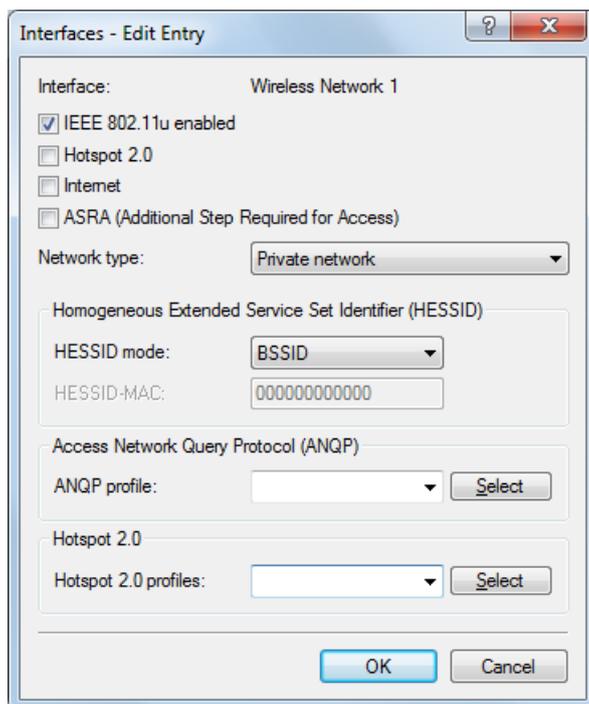
```

|-- Cellular-Network-Information-List
|-- Network-Authentication-Types
|-- Hotspot 2.0 Profiles
|-- Operator-List

```

Activating interfaces

The table **Interfaces** is the highest administrative level for 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.



In order to edit the entries in the table **Interfaces**, click on the button **Edit....** The entries in the edit window have the following meaning:

- **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 802.11-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. Over the Internet-bit, all stations are explicitly informed 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 include:
 - `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

Using the table **Venue information** and the following dialogs **Venue group** and **Venue type code**, you manage the information about the access point's location.

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.

In order to edit the entries in the table **Venue information**, click on the button **Add...** The entries in the edit window have the following meaning:

- **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.
- **Venue 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	Code = Venue type code
Unspecified	
Assembly	<ul style="list-style-type: none"> ■ 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

3 Setup and operation

Venue group	Code = Venue type code
	<ul style="list-style-type: none"> ■ 9 = museum ■ 10 = restaurant ■ 11 = theater ■ 12 = bar ■ 13 = café ■ 14 = zoo, aquarium ■ 15 = emergency control center
Business	<ul style="list-style-type: none"> ■ 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:	<ul style="list-style-type: none"> ■ 0 = unspecified education ■ 1 = primary school ■ 2 = secondary school ■ 3 = college
Factory and industry	<ul style="list-style-type: none"> ■ 0 = unspecified factory and industry ■ 1 = factory
Institutional	<ul style="list-style-type: none"> ■ 0 = unspecified institution ■ 1 = hospital ■ 2 = long-term care facility (e.g., nursing home, hospice) ■ 3 = rehabilitation clinic ■ 4 = organizational association ■ 5 = prison
Commerce	<ul style="list-style-type: none"> ■ 0 = unspecified commerce ■ 1 = retail store ■ 2 = food store ■ 3 = auto repair shop ■ 4 = shopping center ■ 5 = gas station
Halls of residence	<ul style="list-style-type: none"> ■ 0 = unspecified residence hall ■ 1 = private residence ■ 2 = hotel or motel ■ 3 = student housing ■ 4 = guesthouse
Warehouse	<ul style="list-style-type: none"> ■ 0 = unspecified warehouse
Utility and miscellaneous	<ul style="list-style-type: none"> ■ 0 = unspecified service and miscellaneous
Vehicular	<ul style="list-style-type: none"> ■ 0 = unspecified vehicle ■ 1 = passenger or transport vehicles ■ 2 = aircraft ■ 3 = bus ■ 4 = ferry ■ 5 = ship or boat ■ 6 = train

Venue group	Code = Venue type code
Outdoor	<ul style="list-style-type: none"> ■ 7 = motorcycle
	<ul style="list-style-type: none"> ■ 0 = unspecified outdoor
	<ul style="list-style-type: none"> ■ 1 = municipal Wi-Fi network (wireless mesh network)
	<ul style="list-style-type: none"> ■ 2 = city park
	<ul style="list-style-type: none"> ■ 3 = rest area
	<ul style="list-style-type: none"> ■ 4 = traffic control
	<ul style="list-style-type: none"> ■ 5 = bus stop
	<ul style="list-style-type: none"> ■ 6 = kiosk

ANQP profiles

Using this table you manage the profile lists for ANQP. **ANQP profiles** offers you the ability to group certain ANQP elements and to independently assign 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.

In order to edit the entries in the table **ANQP profiles**, click on the button **Add...**. The entries in the edit window have the following meaning:

- **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.

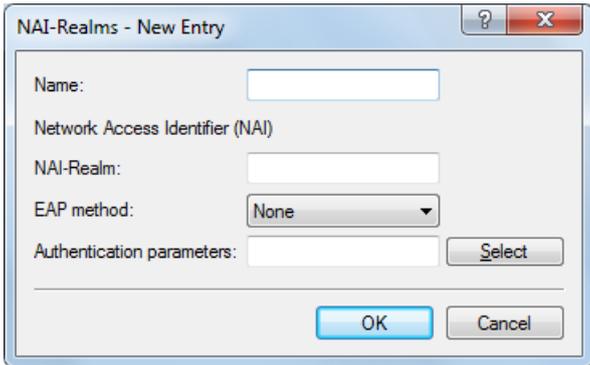
 This device transmits the specified OI(s) in its beacons. If a device should transmit more than 3 OIs, these can be configured under **Additional OUI**. However, additional OIs are not transferred to a station until after the GAS request. They are not immediately visible to the stations!

- **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, using the telnet console or setup menu, you have the option to also display the type of available IP addresses, which they can obtain from the network after a successful authentication. You can access the relevant parameters **IPv4-Addr-Type** and **IPv6-Addr-Type** via the telnet 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.

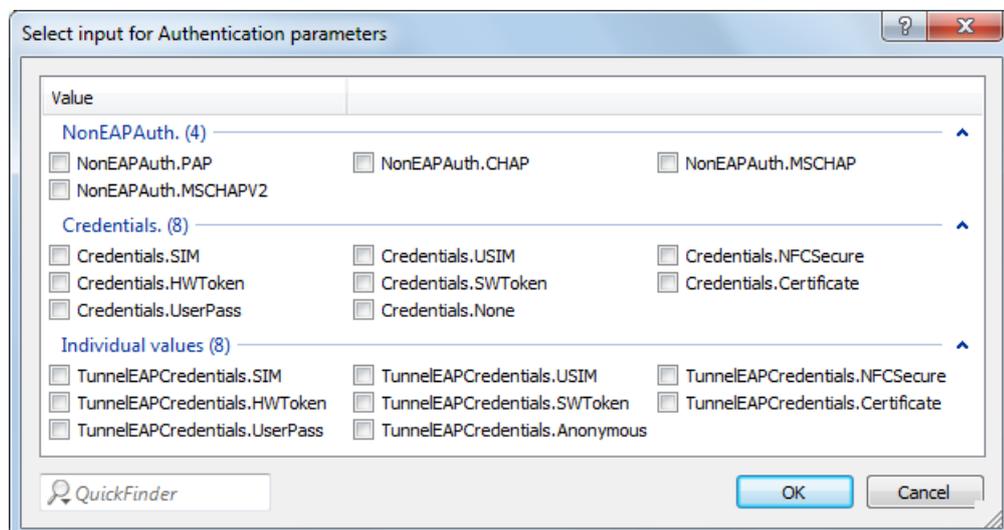


In order to edit the entries in the table **NAI realms**, click on the button **Add...**. The entries in the edit window have the following meaning:

- **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 IETF RFC 2486

and, in the simplest case, is <username>@<realm>, for user746@providerX.org, and therefore 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 include:
 - **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:**



In the window that opens when you click the **Select** button, select the appropriate authentication parameters for the EAP method, such as EAP-TTLS NonEAPAuth.MSCHAPV2, Credential.UserPass or for EAP-TLS Credentials.Certificate. Possible values include:

Table 4: Overview of possible authentication parameters

Parameters	Sub-parameters	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

Parameters	Sub-parameters	Comment
TunnelEAPCredentials.*	NFCSecure	NFC chip
	HWToken*	Hardware token
	SoftToken*	Software token
	Certificate	Digital certificate
	UserPass	Username and password
	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

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

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.

In order to edit the entries in the table **Cellular network information list**, click on the button **Add...** The entries in the edit window have the following meaning:

- **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.

In order to edit the entries in the table **Network authentication types**, click on the button **Add...** The entries in the edit window have the following meaning:

- **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 include:
 - `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 register 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.

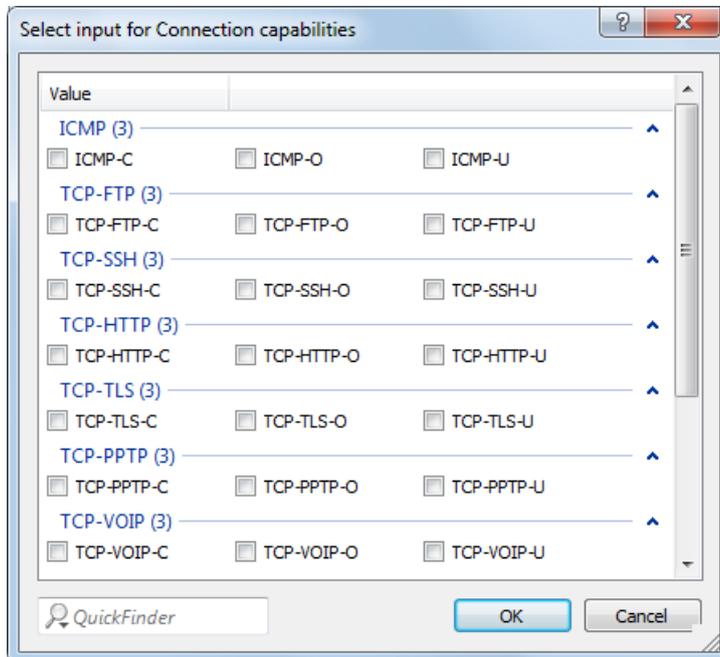
Configuring Hotspot 2.0

Hotspot 2.0 profiles

Using this table you manage the profile lists for the Hotspot 2.0. **Hotspot 2.0 profiles** offers you the ability to group certain ANQP elements (from the Hotspot 2.0 specification) and to independently assign 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.

In order to edit the entries in the table **Hotspot 2.0 profiles**, click on the button **Add...** The entries in the edit window have the following meaning:

- **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.
- **Operator name 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:**



Click the **Select** button and enter the connection capabilities for each service in the window that opens. 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 on which frequency bands and channels your access point is available. Example:
 - 81: Operation at 2.4 GHz with channels 1-13

- 1.1.6: 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.

Operator list

Using this table you manage the plain text 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.

In order to edit the entries in the table **Operator list**, click on the button **Add...** The entries in the edit window have the following meaning:

- **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 plain text name of the hotspot operator.

3.4.7 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 using key cards, dongles or prepaid credit cards 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.

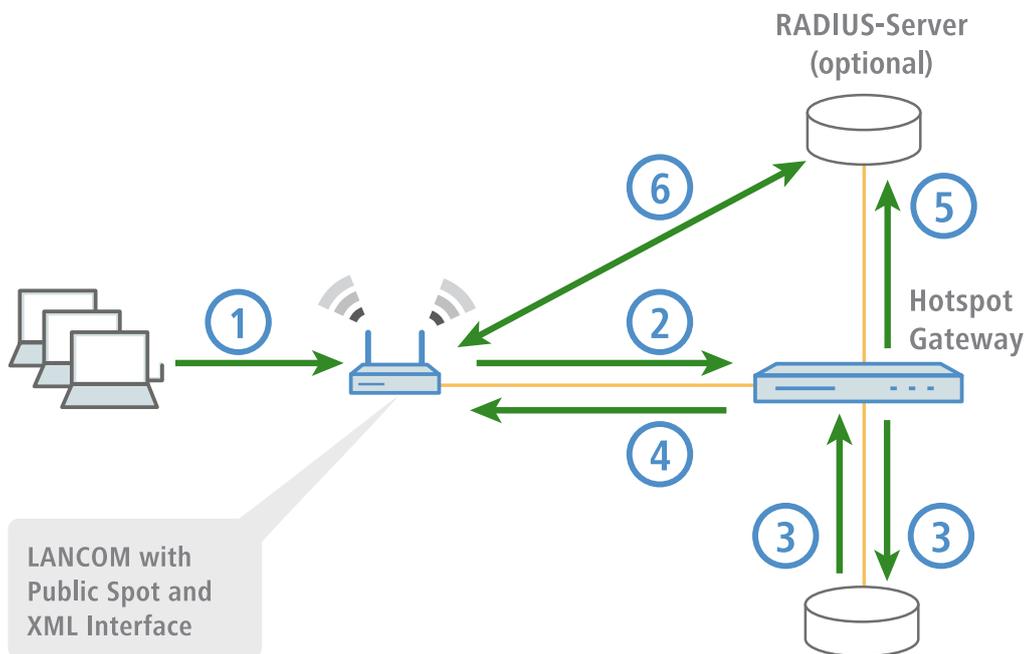
In this case, the Public Spot only performs the following tasks:

- 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.

Function

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.

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-on 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 optionally creates a user in 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 conduct forwarding to 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.

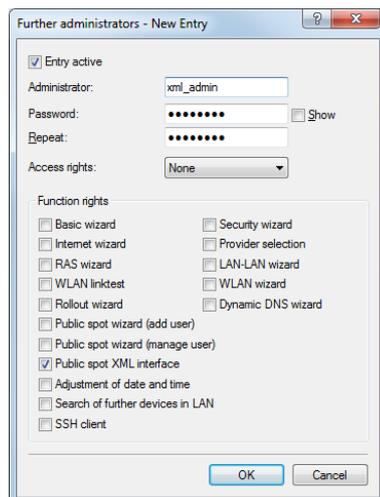
Setting up the XML interface

The following section describes how to set up the XML interface.

! You need to have the "Supervisor" permission in order to create another administrator account.

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 gateway uses to send XML files 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, if necessary, global RADIUS authentication for your Public Spot.
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.

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 LANCOM 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.

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 LANCOM's internal RADIUS server. Further information about this is available in the Reference Manual under the section "Public Spot".

The XML interface can process the following XML elements for a request:

SUB_USER_NAME

User name

SUB_PASSWORD

User password

SUB_MAC_ADDR

MAC address of the user's 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 "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's device Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

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>
  </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-4006_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>
```

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 LANCOM receives this request and the Public Spot module discovers that this user is online with the corresponding MAC, then this user is logged out.

SUB_MAC_ADDR

MAC address of the user's 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's 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_PASSWORD>5juchb</SUB_PASSWORD>
<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-4006_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's 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's 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-4006_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>
```

3.4.8 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.

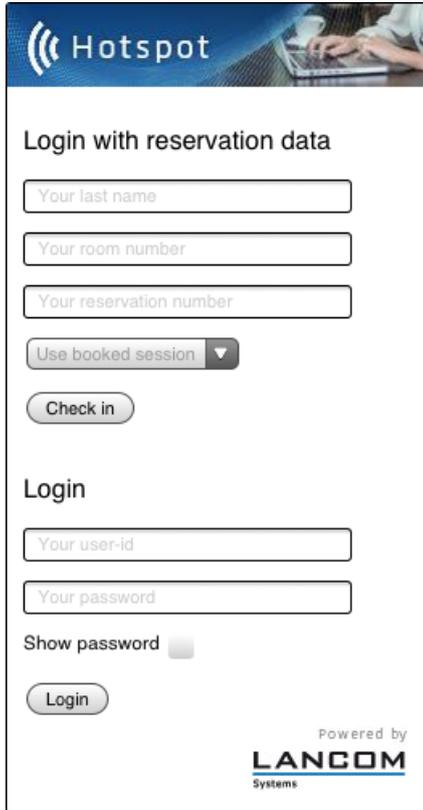
 Currently, the PMS interface is only available for the following device types and series:

- LANCOM 1780 series
- LANCOM 1781 series
- LANCOM WLC-4006
- LANCOM WLC-4006+
- LANCOM WLC-4025
- LANCOM WLC-4025+
- LANCOM WLC-4100
- LANCOM 7100 VPN
- LANCOM 7100+ VPN
- LANCOM 9100 VPN
- LANCOM 9100+ VPN

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 and 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.

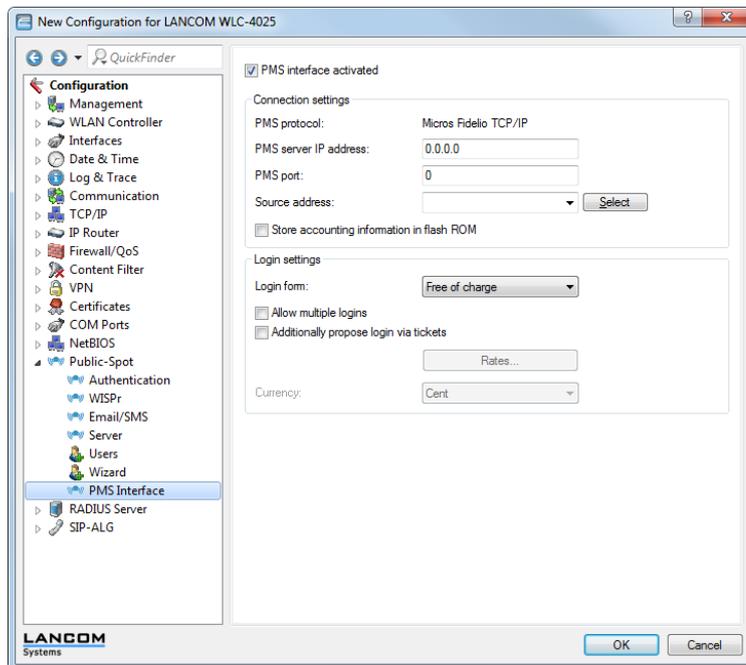
! Your users should make sure that they log out properly from the Public Spot. Without a proper logout (caused by closing the browser, disconnecting the network, switching off the device, etc.) the user is considered to be still logged in. This can cause a problem for the user at login if you, as the 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.

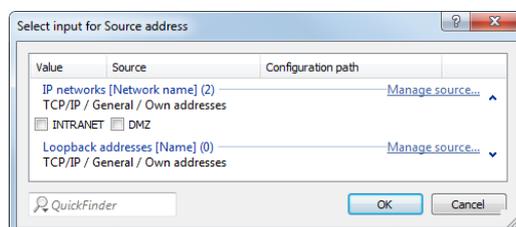
Configuring the PMS interface

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, only support for hotel property management systems from Micros Fidelio is available 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.
- **Sender 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...LB15` 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 include:
 - `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.
 - `Subject to charge`: Choose this option if you offer your hotel guests fee-based Internet access. Your hotel guests will be required to authenticate on the hotspot on the portal page with their username, room number and select a tariff.
- **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.
- **Rates:** If you offer fee-based Internet access, you manage the tariff rates for accounting using this table.

- **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 include: `Minutes`, `Hours`, `Days`
- **Price** Enter the amount charged for the time quota. Combined with the unit, this is the value shown in the screenshot above, e.g., 50 Cent.

! 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, select the currency that you use to bill the time quotas that you offer (time quotas are set up using the tariff 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 include:
 - `Cent`
 - `Penny`

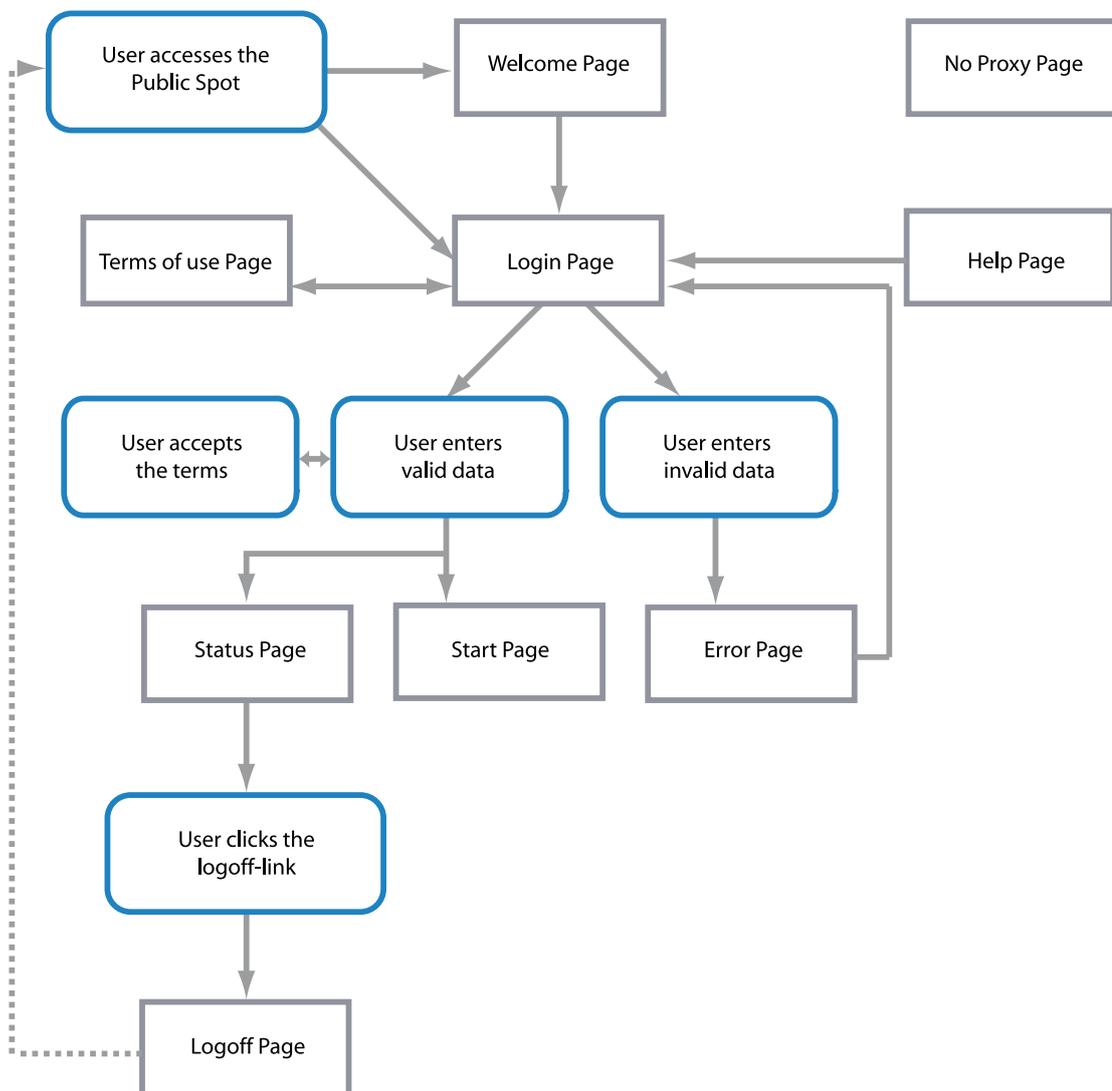
Advanced settings

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](#).

3.5 Default and customized authentication pages

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.

The following flow-chart shows an overview and interaction of all available authentication pages on your device:



3.5.1 Possible pages

The **Welcome** and **Login** pages are displayed to users when they access the Internet or the Public Spot for the first time. The welcome page has a higher priority than the login page and is often used for cosmetic reasons only: Some hotspot

providers like to welcome their users on a separate welcome page in order to present, for example, information about local offers or instructions for registration, while others prefer to provide the fastest possible access to the Internet. Alternatively, some providers use the welcome page to display customized terms of use, which users have to accept before they can go to the start page with the login form (e.g., "Login with name and password") or access the Internet ("Login after agreement").

This has nothing to do with the **Terms of use** page. This is displayed on the login page as an additional link if you selected login via e-mail or SMS, and if you also require confirmation of the terms of use.

 The pre-installed default pages on your device do not include a welcome page or the terms of use. If you invoke one of these pages without loading the corresponding template onto your device, your users will automatically be redirected to the login page (missing welcome page) or an error message will be displayed (missing terms of use).

After the user has logged in with his login data, 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. This page verifies the successful login and redirects the user after a few seconds to the Internet page that the user originally requested. Additionally, a small popup window is opened that holds the **Status** page. This 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 accounting. If a user clicks on this link, the user is sent to the **Logoff** page, which confirms the successful logout from the Public Spot.

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

- The **No-proxy** page is displayed whenever a user tries to connect via HTTP on port 8080 instead of port 80. This port is typically used in Intranets for an HTTP proxy. Since this proxy is configured with a static IP address in the browser settings, but these can not be configured via DHCP, the user would not be able to reach this proxy in any case. 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 in order to represent specific information (e.g., details about the login or where to get vouchers). The set of default pages built into the device does not contain a help 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.

3.5.2 Pre-installed default pages

As mentioned previously, your device contains a set of pre-installed pages on delivery, which you can use to setup an operational Public Spot. There are pages for

- HTTP redirection,
- Login/logout function,
- Status Information.

They were deliberately designed to be simple, not to use any fancy features like dynamic HTML, and just present the necessary elements as-is. By only using the absolutely necessary elements, the correct display in any browser and any size of screen can be assured.

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 offers you the possibility to replace all or some of the default pages with your own design. This 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. The templates can be directly loaded in the flash storage, which makes it possible to dispense with an external HTTP server (see chapter [User-defined pages via HTTP redirect](#)).

3.5.3 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 on the login page

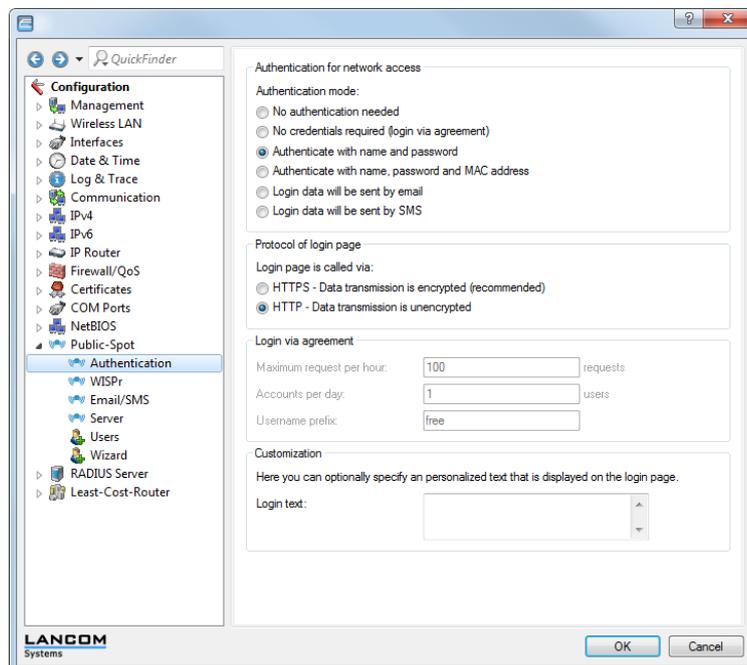
The Public Spot module gives you the option to specify customized text, which appears on the login page inside the box of the registration form. Do this by executing the following steps.

1. In LANconfig, open the configuration dialog for the device.
2. Navigate to the dialog **Public Spot > Authentication** and enter the text that you want your Public Spot users to see in the **Customization** section. You can enter an HTML string with max. 254 characters composed of:

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

LANconfig automatically transforms umlauts. To enter umlauts, you must use their HTML equivalents (e.g. ü for ü). You can also use HTML tags to structure and format the text. Example:

```
Herzlich Willkommen!<br/><i>Bitte füllen Sie das Formular aus.</i>
```



3. Click on **OK** to load the login text into the device.

Once the configuration has been written successfully, the new login text 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

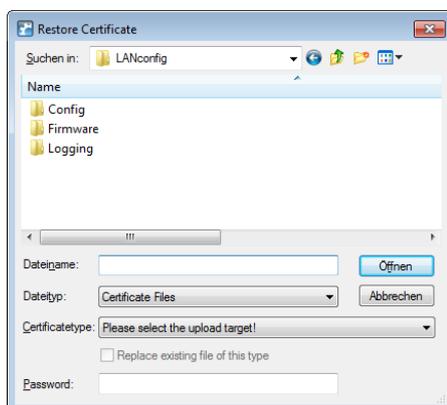


Figure 2: Login page for small screens

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.

3.5.4 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. Some file names are reserved for this purpose:

Table 5: Overview of the reserved file names for template pages

Local URL on your device	Page designation
<code>file://pbspot_template_welcome</code>	Welcome...
<code>file://pbspot_template_login</code>	Login...
<code>file://pbspot_template_error</code>	Error...
<code>file://pbspot_template_start</code>	Start...
<code>file://pbspot_template_status</code>	Status...
<code>file://pbspot_template_logoff</code>	Logoff...
<code>file://pbspot_template_help</code>	Help...
<code>file://pbspot_template_noproxy</code>	No proxy
<code>file://pbspot_template_voucher</code>	Voucher...*
<code>file://pbspot_template_agb</code>	Terms of use...

*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.

3.5.5 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.

%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 hexadecimal string of length 12. 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.

%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`

3.5.6 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.

3.5.7 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 care 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.

3.5.8 Page template syntax

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.

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. 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>
```

3.5.9 Page template identifiers

The following identifiers are currently defined.

 Please note that not all identifiers are available for all printouts! Not all identifiers are available on all pages.

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.

HELPLINK

Valid for: `<pbelem>`

This identifier contains the URL to the help page provided by the device.

LOGINERRORMSG

Valid for: `<pbelem>`

This identifier returns the error message from LCOS in the case of a failed authentication. It is only valid when used on the 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 refers to the HTML form for entering the user's name and password.

LOGINLINK

Valid for: <pbelem>

This identifier contains the URL to the login page provided by the device.

LOGOFFLINK

Valid for: <pbelem>

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.

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.

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.

SESTIMEOUT**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.

STATUSLINK**Valid for:** <pbelem><pbcond>

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.

TXBYTES**Valid for:** <pbelem>

This identifier contains the amount of data transmitted by the device to the client so far in this session.

USERID**Valid for:** <pbelem>

This identifier contains the user ID 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.

3.5.10 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 [Login-free servers and networks](#) 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.

4 Access to the Public Spot

4.1 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.

- **Wireless LAN 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.

4.2 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.

A screenshot of a web browser login page. The page has a white background and a thin black border. At the top left, the word "Login" is displayed. Below it are two input fields: the first is labeled "Your user-id" and the second is labeled "Your password". To the right of the password field is a "Show password" checkbox, which is currently unchecked. Below the input fields is a "Login" button. In the bottom right corner of the form, there is a logo for "LANCOM Systems" with the text "Powered by" above it.

- ⓘ Depending on the firmware version, the actual login page may vary from the one shown here. However it looks, the login page will always present the input fields for user ID and password.
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).

4.3 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/`

Session information	
Status:	logged in
User ID:	491
Login Time:	17m:43s
Account expires in:	42m:20s
Transmitted data:	39 KBytes
Received data:	187 KBytes
Transfer volume:	unlimited

Click [here](#) to log out.

Powered by
LANCOM
Systems

4.4 Logging out of the Public Spot

The session information window can be used to logout from the Public Spot. Simply click on the word **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`

The Public Spot operator can supply you with the <Public Spot 's IP address> upon request.



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.

4.5 Advice and help

The following sections present solutions to the most common problems that may occur when operating a Public Spot.

4.5.1 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.).

4.5.2 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.

4.5.3 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.

4.5.4 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.

4.5.5 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**

5 Tutorials for setting up and using Public Spots

The following tutorials describe examples of how the Public Spot option can be implemented.

5.1 Virtualization and guest access via WLAN controller with VLAN

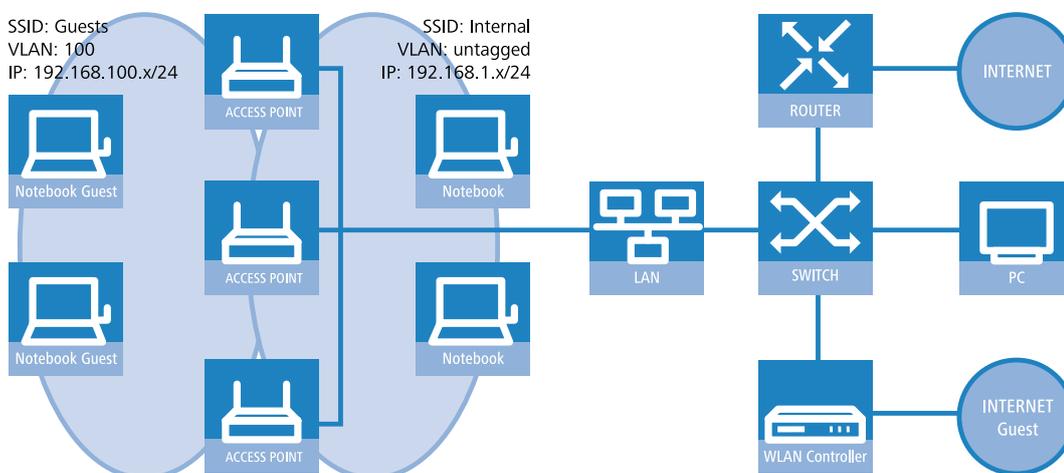
Many companies wish to offer Internet access to their visitors via WLAN. In larger installations the required settings apply to multiple access points, and these can be programmed centrally in the WLAN controller.

5.1.1 Objectives

- 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.

5.1.2 Establish

- Management of the access points is handled by the LANCOM WLC.
- The LANCOM WLC serves as the DHCP server for the WLAN clients in the guest network.
- The guest network is provided with Internet access via the LANCOM WLC (e.g. separate DSL access or Internet access via the company DMZ).
- The wired infrastructure is based on managed VLAN-capable switches:
 - The VLAN management of access points is handled by the LANCOM WLC.
 - The VLAN management of the switches is handled separately by the switch configuration.
- The access points operate within the internal VLANs.



5.1.3 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**

- 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**

- 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.

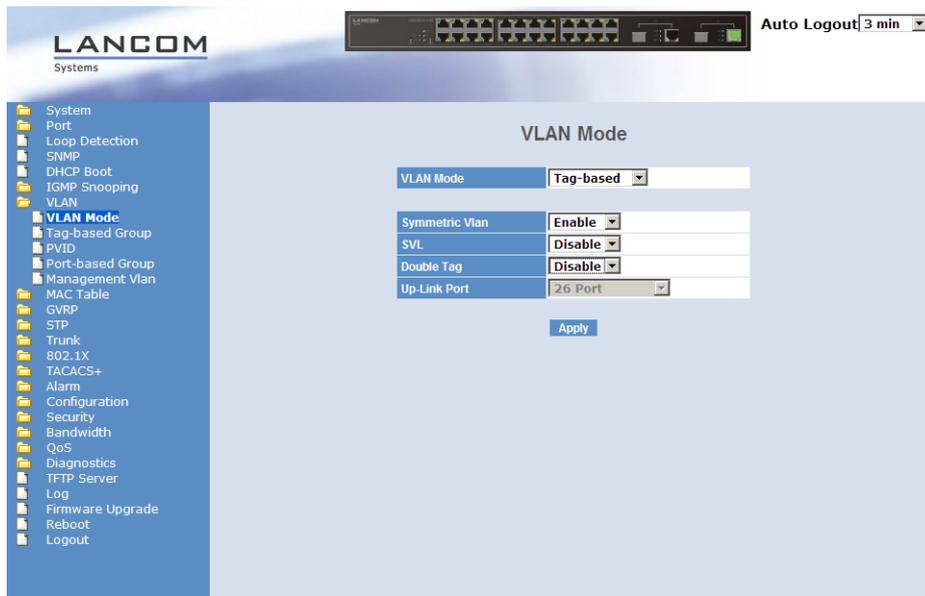
- LANconfig: **WLAN Controller > AP Config. > Access point table**

5.1.4 Configuring the switch (LANCOM ES-2126+)

In this section we describe the configuration of the switch using the LANCOM ES-2126+ as an example.

5 Tutorials for setting up and using Public Spots

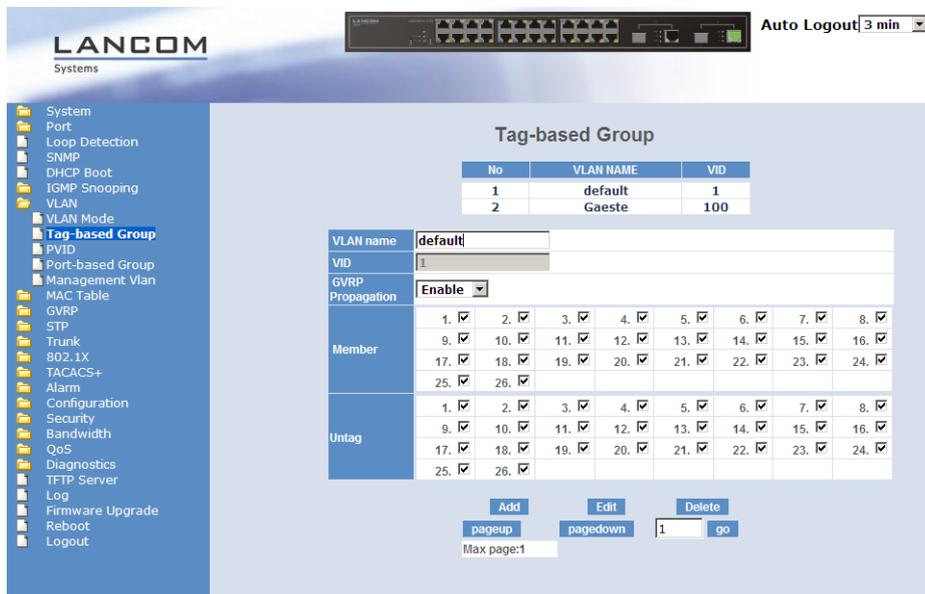
1. Set the VLAN mode to **Tagged**, as the access points handle the assignment of VLAN tags.



2. Set the group names of the VLANs.

To differentiate between the VLANs in the switch, two groups are used. The internal network for the employees is mapped to the default group (**default**), and a dedicated group (**guests**) is set up for the guests. The Groups use the corresponding VLAN IDs that you entered into the controller when configuring the VLANs.

The default VLAN is valid on all ports and remains untagged, i.e., the VLAN tags are removed from outgoing data packets for this group by the switch.



The guests' VLAN group uses the VLAN ID "100" and is valid only for the ports connected to the WLAN controller and access points (ports 10 to 16 in our example). The switch does not remove tags of outgoing data packets.

- Set the port VLAN ID (PVID) for all ports to "1".
This assigns all ports to the internal network so that the switch assigns the VLAN ID "1" to all untagged incoming data packets on these ports before forwarding them.

5.1.5 Configuring the switch (LANCOM GS-2326P)

In this section we describe the configuration of the switch using the LANCOM GS-2326P as an example.

- Under **Configuration > VLAN > VLAN-Membership**, create an additional VLAN group for the guest network.

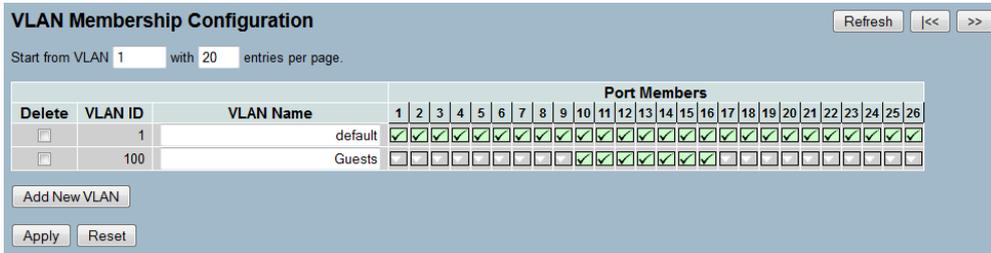
To differentiate between the VLANs in the switch, two groups are used. The internal network for the employees is mapped to the group `default`, and that for the guests is mapped to the group `guests`.

- 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

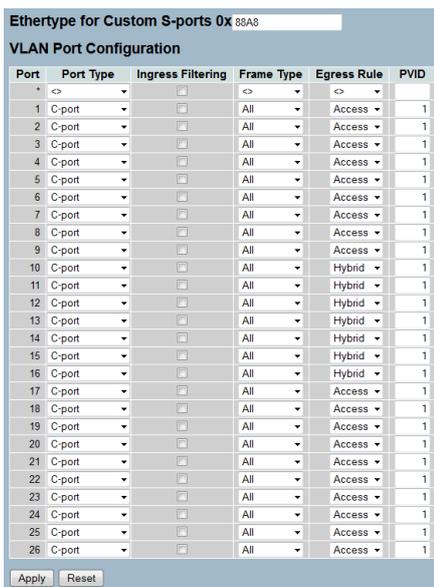
5 Tutorials for setting up and using Public Spots

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 VLAN 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.



⚠ 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.

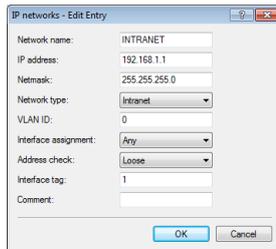
⚠ Note that these data packets can only leave the switch via the ports of the guest network.

5.1.6 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).

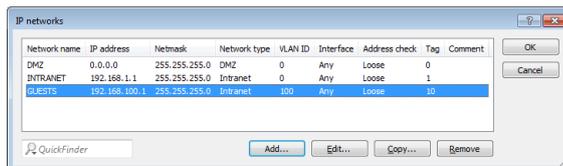
- For the internal network, set the **INTRANET** to the address 192.168.1.1.
This IP network uses the **VLAN ID** 0. This assigns all untagged data packets to this network (the VLAN module in the controller itself must be activated for this). The **interface tag** 1 is used for the subsequent break-out of data in the virtual router.

- LANconfig: **TCP/IP > General > IP networks**



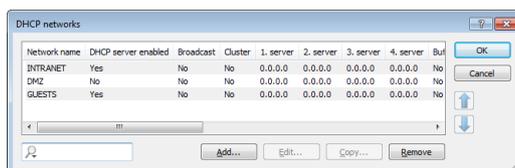
- For guests, create a new IP network with the address 192.168.100.1.
This network uses the **VLAN ID** 100. In this way, all data packets with this ID are assigned to the guest network. Here, too, the **interface tag** 10 is used later by the virtual router.

- LANconfig: **TCP/IP > General > IP networks**



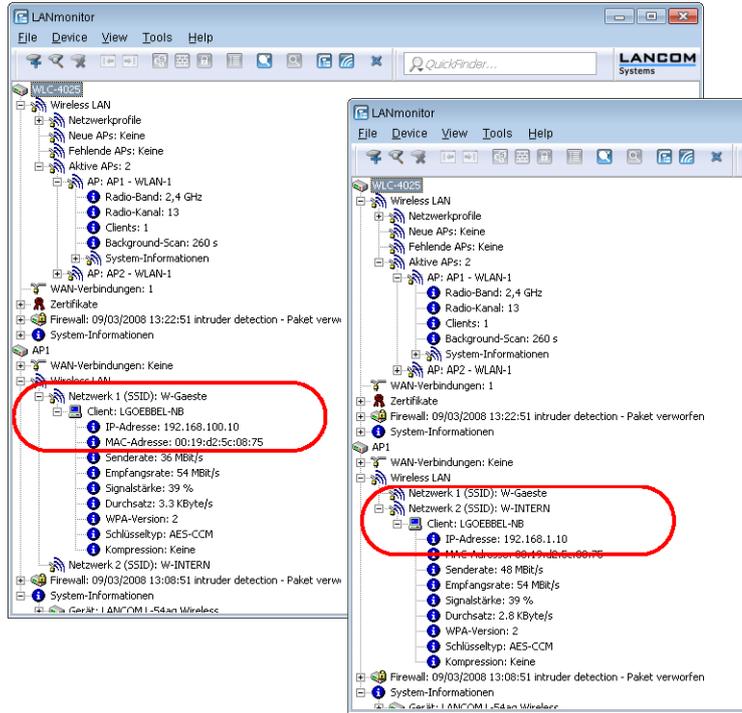
- Enable the DHCP server for both IP networks.

- LANconfig: **TCP/IP > General > IP networks**



5 Tutorials for setting up and using Public Spots

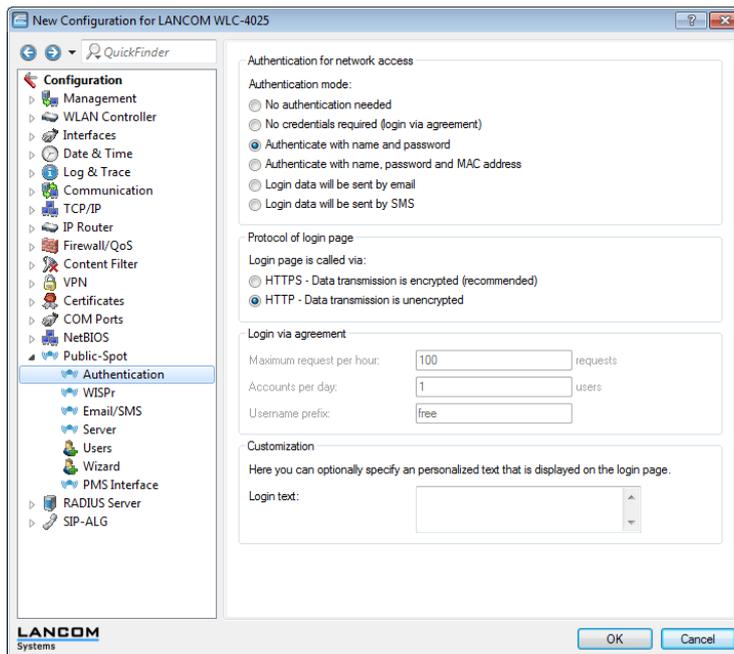
With these settings, the WLAN clients of the internal employees and guests are assigned to the appropriate networks.



5.1.7 Configuring Public Spot access accounts

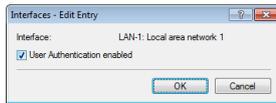
The Public Spot allows you to provide a strictly controlled point of access to your wireless LAN. Authentication is performed by requesting user information via a web interface. If necessary, you can set a time limit for the access.

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 > Interfaces**



- 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. Note that access to WEBconfig via the Public Spot interface is restricted to the authentication pages only (see [Limit configuration access](#)).

! 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**



- Enable the option to clean up the user table so that your device automatically deletes entries that are no longer needed.

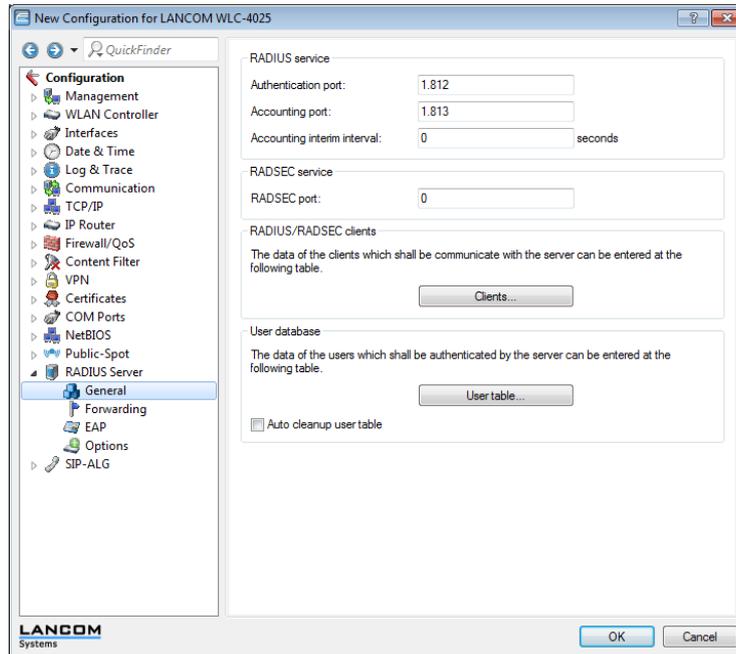
- LANconfig: **RADIUS server > General > Clear user lists automatically**

5.1.8 Configuring the internal RADIUS server for Public Spot operation

As of LCOS version 7.70, the Wizard stores the Public Spot access accounts in the user database of the internal RADIUS server. In order to use Public Spot access accounts, you **must** configure the RADIUS server and the Public Spot module to use the RADIUS server.

- Enable the RADIUS server by entering the authentication and accounting ports so that you can use the user database on the internal RADIUS server.
Use the **authentication port** 1,812 and the **accounting port** 1,813.

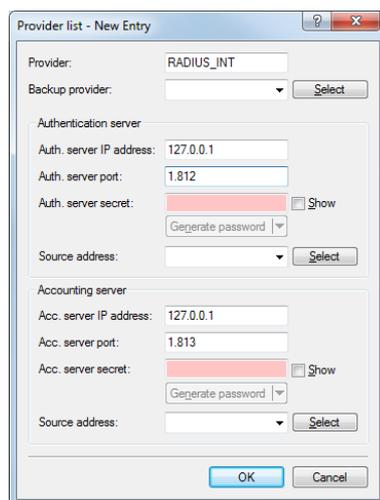
- LANconfig: **RADIUS server > General > RADIUS service**



- Create an entry in the **authentication server** list of the Public Spot for the internal RADIUS server under **Name**, so that the Public Spot has the address of the RADIUS server and can authenticate Public Spot access attempts on the internal RADIUS server of the LANCOM device.
Enter the IP address of the device as the authentication and accounting server where the RADIUS server was enabled. Also use the authentication and accounting port settings from the RADIUS server (1,812 and 1,813).

! If the Public Spot and the RADIUS server are provided by the same device, enter the device's internal loopback address (127.0.0.1) here.

- LANconfig: **Public Spot > Users > Authentication servers**

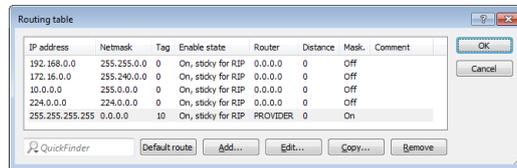


5.1.9 Configuring Internet access for the guest network

- In order to provide Internet access for guest network users, there is a wizard to set up access to a provider network.
- 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**



- 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.

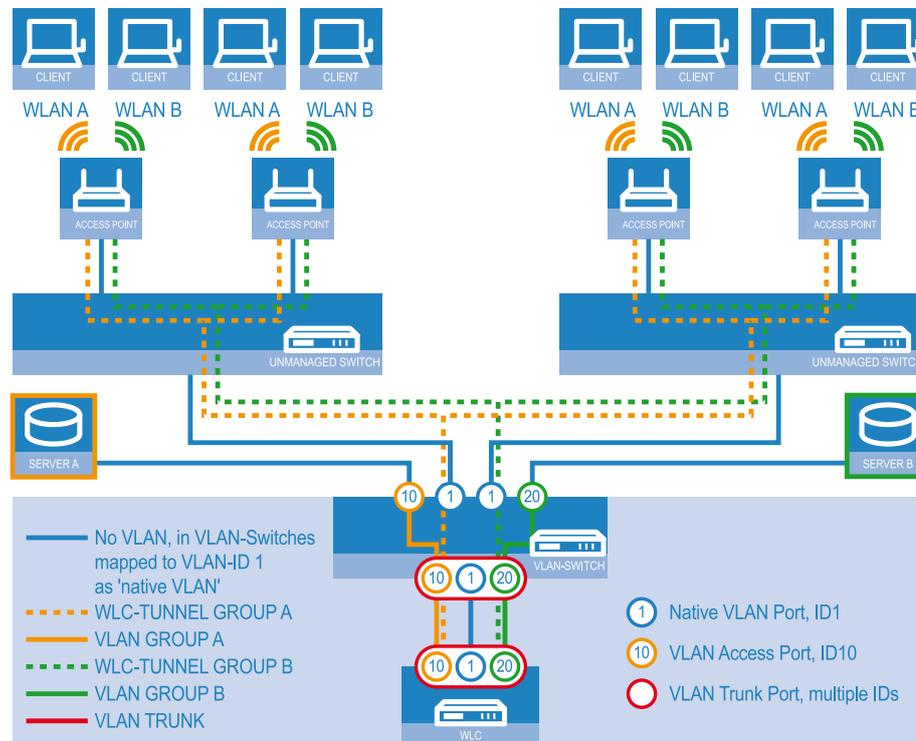
5.2 Virtualization and guest access via WLAN controller without VLAN

5.2.1 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.

WLAN controllers enable you to separate the networks while minimizing the use of VLANs. The access points use a CAPWAP data tunnel to direct the payload from the WLAN clients straight to the controller, which then assigns the data to the corresponding VLANs. In this situation, VLAN configuration is only required for the controller 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.



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 access points, each of which is connected to one of the switches.
- Each access point 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 WLAN controller manages all of the access points in the network.
- A central, VLAN-capable switch connects the switches in each segment, the servers for each group, and the WLAN controller.

The aim of the configuration: A WLAN client that associates with an SSID is to have access to its "own" server, regardless of which access point is being used and regardless of the segment in which the client is located.

! The following description assumes a working basic configuration of the WLAN controller. 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. This entry requires 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

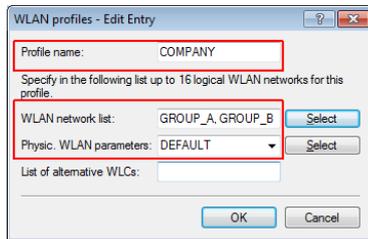
ID '20' for the second logical network. In LANconfig you find these settings under **Configuration > WLAN Controller > Profiles > Logical WLAN networks (SSIDs)**.

Logical WLAN networks for overlay networks

2. Create an entry in the list of physical WLAN parameters with the appropriate settings for your access points, 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 access points. Set the operating mode for the management VLAN in the access points to 'Untagged'. In LANconfig you find these settings under **Configuration > WLAN Controller > Profiles > Physical WLAN parameters**.

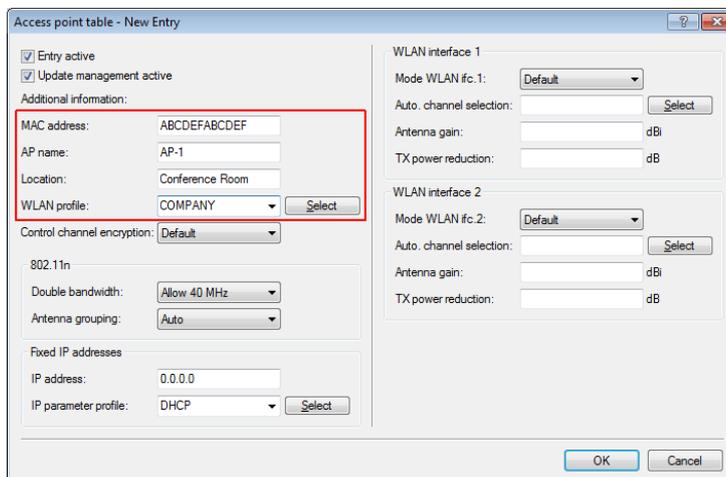
Physical WLAN parameters for overlay networks

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 these settings under **Configuration > WLAN Controller > Profiles > WLAN profiles**.



WLAN profiles for overlay networks

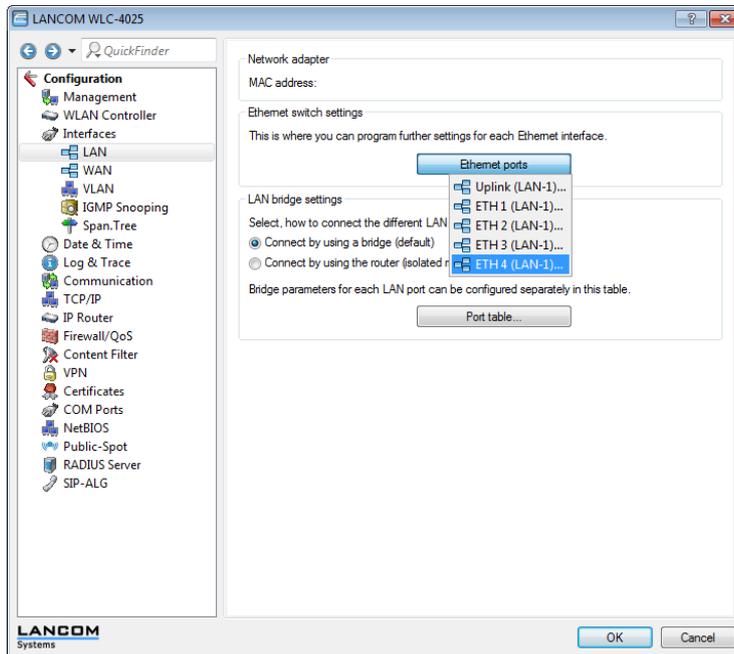
4. For each managed access point, create an entry in the access point table with a suitable name and the associated MAC address. Assign the WLAN profile created previously to this access point. In LANconfig you find these settings under **Configuration > WLAN Controller > AP config. > Access point table**.



Access point table for overlay networks

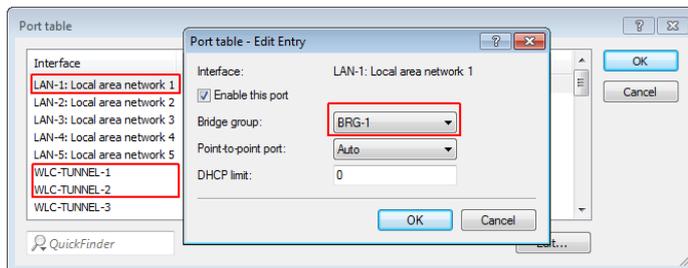
Configuring the interfaces on the WLC

- 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**.



Ethernet setting for overlay networks

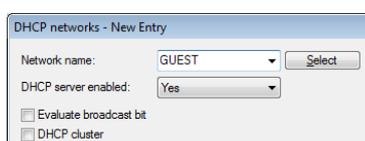
- Assign the logical LAN interface 'LAN-1' and the WLC tunnels 'WLC-tunnel-1' and 'WLC-tunnel-2' to the bridge-group 'BRG-1'. Make sure that the other LAN ports are not assigned to the same bridge group. In LANconfig you find these settings under **Configuration > Interfaces > LAN > Port table**.



Port settings for overlay networks

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.

- The WLAN controller can optionally act as a DHCP server for the access points. To set this up, activate the DHCP server for the 'INTRANET'. In LANconfig you find these settings under **Configuration > TCP/IP > DHCP > DHCP networks**.



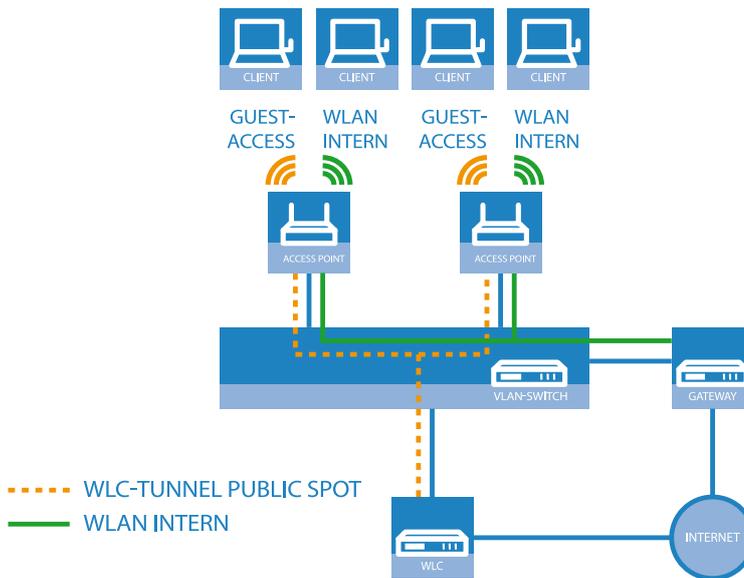
DHCP settings for overlay networks

5.2.2 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 controller 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 access points provide two SSIDs, 'COMPANY' and 'GUESTS'.



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 access points 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 access points send the payload data from the guest clients through a WLC tunnel directly to the WLAN controller, 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)**.

The screenshot shows the 'Logical WLAN networks (SSIDs) - Edit Entry' dialog box. The 'Logical WLAN network activated' checkbox is checked. The 'Name' field is 'COMPANY'. The 'Network name (SSID)' is 'WLAN-INTERNAL' and 'Connect SSID to' is 'LAN at AP'. The 'Encryption' is '802.11i (WPA)-PSK'. The 'Allow data traffic between stations of this SSID' checkbox is checked. Other settings include WPA version: WPA1/2, WPA1 session key type: TKIP, WPA2 session key type: AES, Basis rate: 2 Mbit/s, Client Bridge Support: No, Maximum count of clients: 0, Min. client signal strength: 0%, Use long preamble for 802.11b: unchecked, 802.11n Max. spatial streams: Auto, Allow short guard interval: checked, Use frame aggregation: checked, STBC (Space Time Block Coding) activated: checked, and LDPC (Low Density Parity Check) activated: checked.

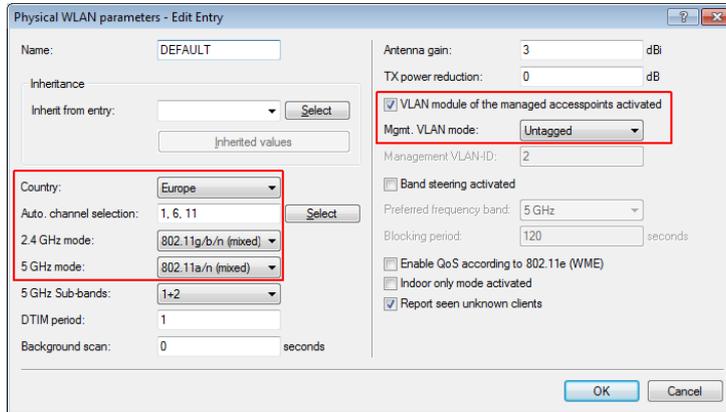
Logical WLAN networks for internal use

The screenshot shows the 'Logical WLAN networks (SSIDs) - Edit Entry' dialog box. The 'Logical WLAN network activated' checkbox is checked. The 'Name' field is 'GUEST'. The 'Network name (SSID)' is 'WLAN-PUBLIC' and 'Connect SSID to' is 'WLC-TUNNEL-1'. The 'Encryption' is 'None'. The 'Allow data traffic between stations of this SSID' checkbox is unchecked. Other settings include WPA version: WPA1/2, WPA1 session key type: TKIP, WPA2 session key type: AES, Basis rate: 2 Mbit/s, Client Bridge Support: No, Maximum count of clients: 0, Min. client signal strength: 0%, Use long preamble for 802.11b: unchecked, 802.11n Max. spatial streams: Auto, Allow short guard interval: checked, Use frame aggregation: checked, STBC (Space Time Block Coding) activated: checked, and LDPC (Low Density Parity Check) activated: checked.

Logical WLAN networks for guest access accounts

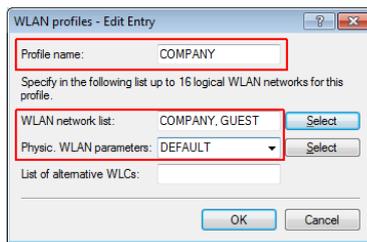
5 Tutorials for setting up and using Public Spots

2. Create an entry in the list of physical WLAN parameters with the appropriate settings for your access points, 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**.



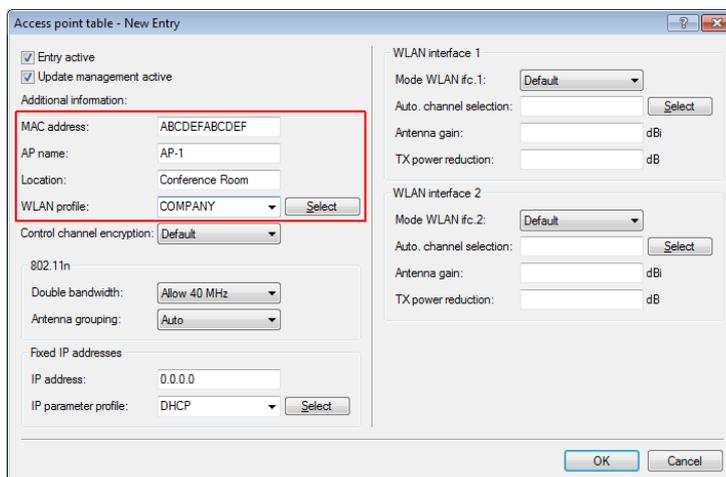
Physical WLAN parameters for Public Spot APs

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**.



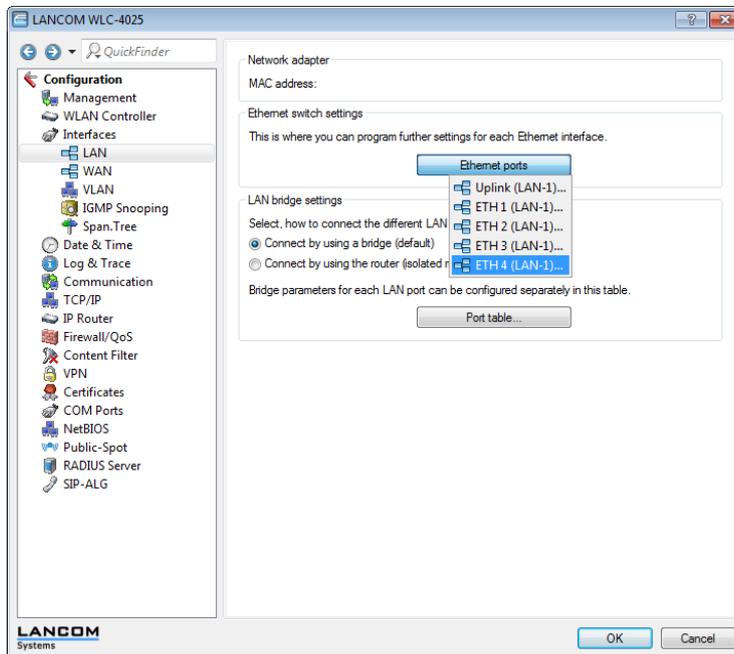
WLAN profiles for Public Spot APs

4. For each managed access point, create an entry in the access point table with a suitable name and the associated MAC address. Assign the WLAN profile created previously to this access point. In LANconfig you find this setting under **Configuration > WLAN Controller > AP config. > Access point table**.



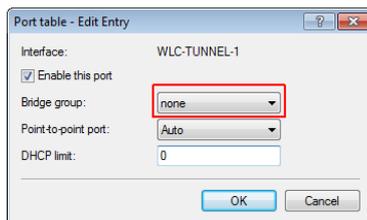
Access point table for Public Spot APs

- Assign a separate logical LAN interface, e.g. 'LAN-1', to each physical Ethernet port. Set the 4th Ethernet port to the logical interface 'DSL-1'. The WLAN controller will use this LAN interface for the guest network Internet access. In LANconfig you find this setting under **Configuration > Interfaces > LAN > Ethernet ports**.



Ethernet settings for Public Spot APs

- 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**.



Port settings for Public Spot APs

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 'DHCP'. 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**.

Remote sites - Edit Entry

Name: INTERNET

Short hold time: 9.999 seconds

Access concentrator:

Service:

Layer name: DHCP Select

MAC address type: Local

MAC address:

DSL ports: Select

VLAN ID: 0

OK Cancel

Remote site for Internet access

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 WLAN controller 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**.

IP networks - Edit Entry

Network name: INTRANET OK

IP address: 192.168.1.100 Cancel

Netmask: 255.255.255.0

Network type: Intranet

VLAN ID: 0

Interface assignment: Any

Address check: Loose

Interface tag: 1

Comment:

IP network for internal use

IP networks - Edit Entry

Network name: GUEST OK

IP address: 192.168.200.1 Cancel

Netmask: 255.255.255.0

Network type: Intranet

VLAN ID: 0

Interface assignment: Any

Address check: Loose

Interface tag: 2

Comment:

IP network for guest access

9. The WLAN controller can act as a DHCP server for access points 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.

DHCP network for guest access

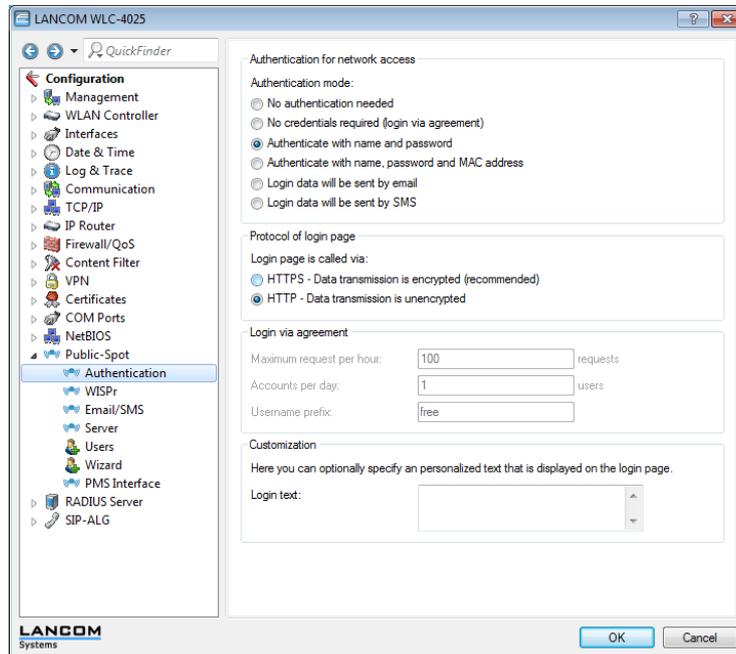
10. Create a new default route in the routing table to direct the data from the guest network to the Internet connection used by the WLAN controller. Select the routing tag '2' and the router 'Internet'. Also activate the option 'Masking intranet and DMZ (default)'. In LANconfig you find this setting under **Configuration > IP router > Routing > Routing table**.

Routing entry for Internet access

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 > Interfaces**.

Activation of user authentication for the WLC tunnel

12. The final step is to enable authentication via the Public Spot for the WLAN controller. In LANconfig you find this setting under **Configuration > Public Spot > Authentication**.



Activation of authentication via Public Spot

In addition to configuring the WLAN controller, you must also configure the Public Spot either to use the internal user list or to use a RADIUS server, according to your needs.

5.3 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.
 - LANconfig: **Public Spot > Users > Authentication servers**

When configuring a Public Spot, user registration data can be forwarded to one or more RADIUS servers. These servers are configured under **Public Spot > Users > Authentication servers**. 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.

5.4 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.

5.4.1 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:

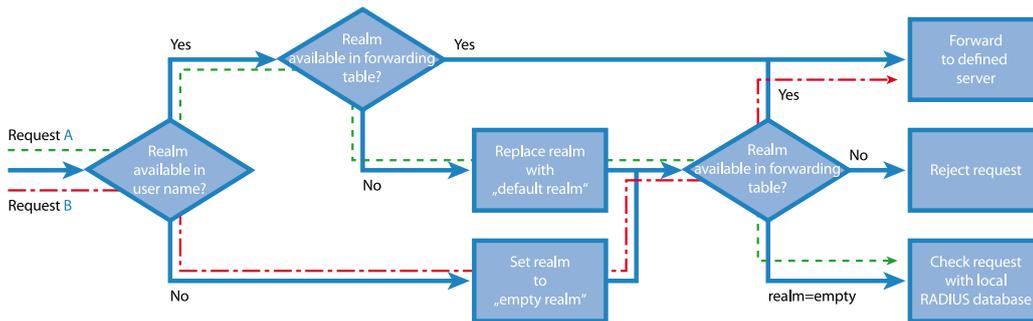
5 Tutorials for setting up and using Public Spots

- 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.

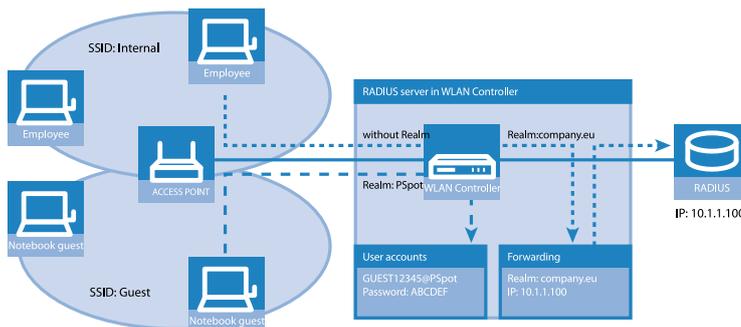
! If the WLAN controller checks the realm and finds that it is empty, it **always** checks the authentication request with the internal RADIUS database.

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 LANCOM'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 LANCOM 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.

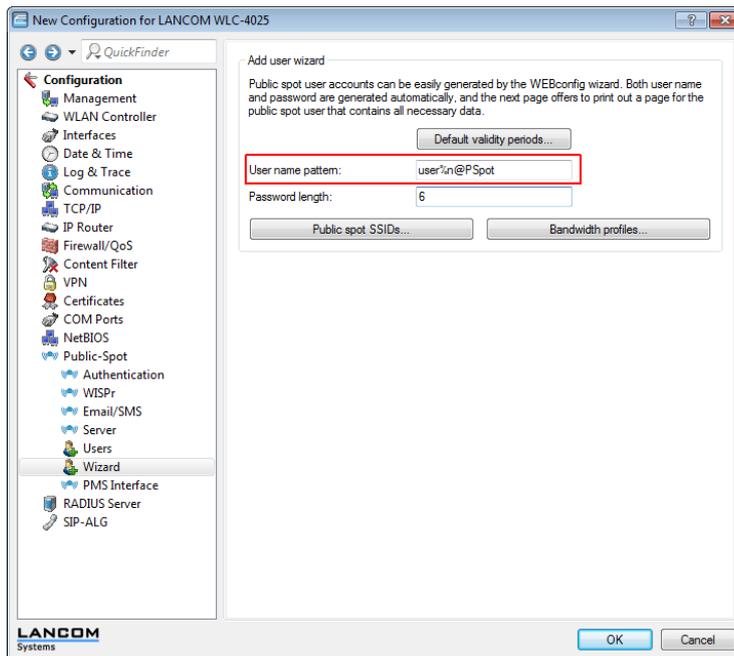


5.4.2 Configuring RADIUS forwarding

The following configuration steps allow you to specify the different manners in which internal users and guests are processed.

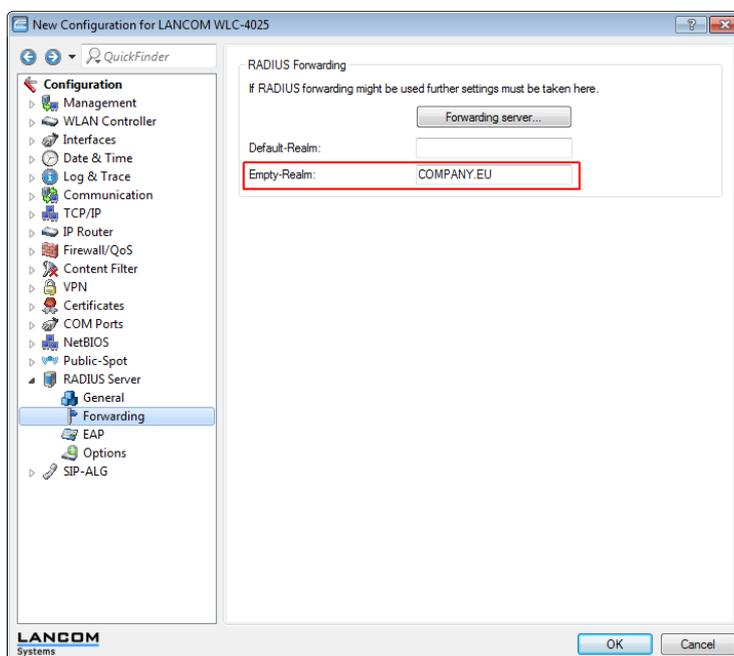
1. In the Public Spot, adapt the pattern of user names such that a unique realm can be suffixed. For example, if the pattern is "user%n@PSpot", the Public Spot generates usernames with the format "user12345@PSpot".

- LANconfig:Public Spot > Wizard > Add user wizard



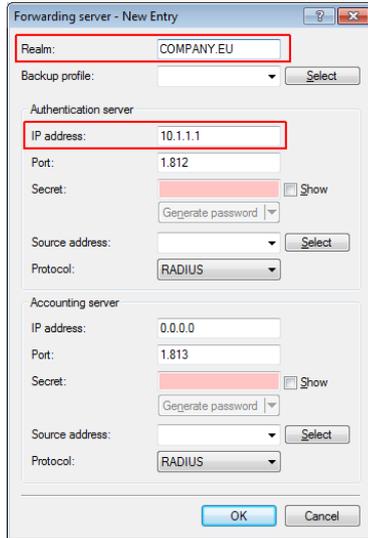
2. In the WLAN controller's RADIUS server, define an "empty realm" (e.g., "COMPANY.EU"). This realm is attached to all user names which request authentication from the WLAN controller and which do not already have a realm. In this application, the internal users have no realm defined. In order to prevent the WLAN controller's RADIUS server from attaching a realm, you must leave the "Default realm" field blank.

- LANconfig:RADIUS Server > 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.



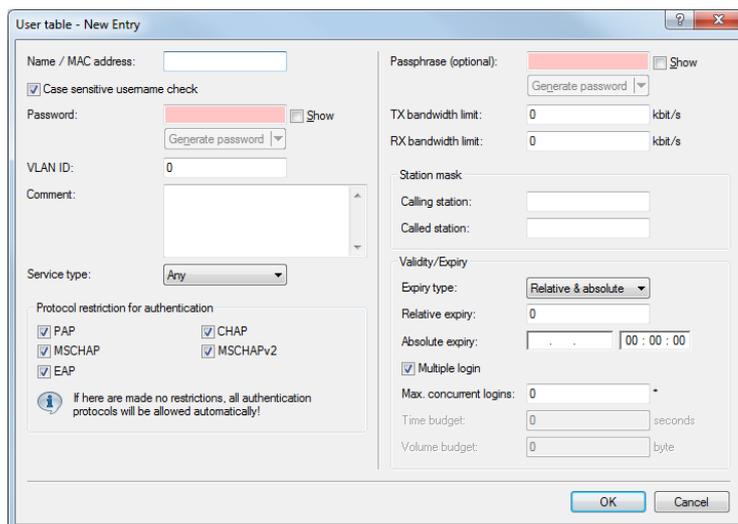
4. Authentication requests from Public Spot users have the realm "@PSpot" and are received by the WLAN Controller. With no forwarding defined for this realm, the usernames are automatically checked with the internal RADIUS database. Because the Public Spot access accounts created with the Wizard are stored in this database, these requests can be authenticated as required.

5.5 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 LANCOM 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 > General > User database**



5.6 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.

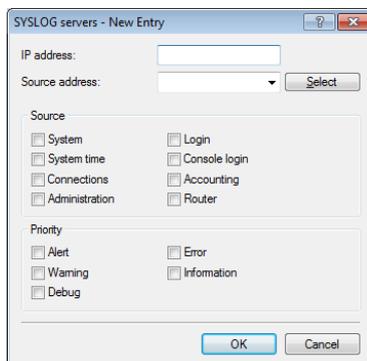
To save user data from a Public Spot by means of SYSLOG, the external SYSLOG server has to be configured in the respective Public Spot. Once this is done, messages are sent for logging to the SYSLOG server whenever Public Spot user accounts are created or deleted, and at the beginning and end of Public 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 to be found in the LCOS Reference Manual. You can find legal information about this topic in the LANCOM techpaper "Public Spot" which is available at www.lancom-systems.de/en/publications/products.

5.6.1 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.

The screenshot shows the "Kiwi Syslog Service Manager (Version 8.3.28)" application window. The main area displays a list of syslog messages with the following columns: Date, Time, Priority, Hostname, and Message.

Date	Time	Priority	Hostname	Message
05-29-2008	14:17:58	Auth.Notice	192.168.10.31	CONN-LOGIN_INFO: User account 'user58567' deleted [manually deleted by root]<000>
05-29-2008	14:17:27	Auth.Notice	192.168.10.31	CONN-LOGIN_INFO: Finished session for user 'user58567' (IP address was 192.168.10.214, accounting data: Tx:263298, Rx:39102, Seconds:60)<000>
05-29-2008	14:16:28	Auth.Notice	192.168.10.31	CONN-LOGIN_INFO: Started session for user 'user58567' (IP address is
05-29-2008	14:15:36	Auth.Notice	192.168.10.31	CONN-LOGIN_INFO: [WLAN-2] Determined IP address for station 00:10:c6:49:cd:fd (USI 49:cd:fd) [MARKUS-MOBIL]: 192.168.10.214<000>
05-29-2008	14:15:07	Auth.Notice	192.168.10.31	CONN-LOGIN_INFO: [WLAN-2] Determined IP address for station 00:10:c6:49:cd:fd (USI
05-29-2008	14:15:07	Auth.Notice	192.168.10.31	CONN-LOGIN_INFO: [WLAN-2] Connected WLAN station 00:10:c6:49:cd:fd (USI 49:cd:fd)
05-29-2008	14:15:07	Auth.Notice	192.168.10.31	CONN-LOGIN_INFO: [WLAN-2] Associated WLAN station 00:10:c6:49:cd:fd (USI 49:cd:fd)
05-29-2008	14:15:07	Auth.Notice	192.168.10.31	CONN-LOGIN_INFO: [WLAN-2] Authenticated WLAN station 00:10:c6:49:cd:fd (USI
05-29-2008	14:13:03	Auth.Notice	192.168.10.31	CONN-LOGIN_INFO: User account 'user58567' created [created by root on 29.05.2008

6 Appendix

6.1 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.

6.1.1 Messages to/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. For this reason LANCOM has chosen to provide these values as vendor-specific attributes, marked with LANCOM's enterprise ID (2356).

Overview of the RADIUS attributes transmitted by the device to the authentication server

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

6

Service-Type Id 1

Type of service that the user requested. The value 1 stands for **Login**.

8

Framed-IP-Address

IP address that was assigned to the client

26

Vendor 2356(LCS) ID 2

MAC address of the client if authentication using the MAC address is enabled. In contrast to the Calling-Station-Id, this value is transmitted as a 6-byte binary string. This attribute only exists for the login mode **Authenticate with name, password and MAC address**.

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.

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.

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:

Overview of the RADIUS attributes processed by the device

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(LCS) ID 1**Trafficlimit**

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(LCS) 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(LCS) 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(LCS) ID 8**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(LCS) 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(LCS) ID 9**LCS-RxRateLimit**

Defines the maximum upstream rate in kbps. This restriction may be combined with the corresponding Public Spot function.

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 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 overwrites in the locally defined idle timeout 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.

6.1.2 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".

Processed attributes

Your device currently does not process any attributes in responses sent by a RADIUS accounting server.

6.2 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**

6.3 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.

6.3.1 Accounting

In this menu you configure the transfer of accounting information from your device to your PMS.

SNMP ID:

2.64.10

Telnet path:**Setup > PMS-Interface**

Clean-up 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. If the value is 0, automatic clean-up is disabled.

SNMP ID:

2.64.10.3

Telnet path:**Setup > PMS-Interface > Accounting****Possible values:**

0 to 4294967295 seconds

Default:

60

Save to flash ROM 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

Telnet path:**Setup > PMS-Interface > Accounting****Possible values:**

0 to 4294967295 seconds

Default:

15

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. If the value is 0, the update is disabled and the status table does not display any values.

SNMP ID:

2.64.10.4

Telnet path:**Setup > PMS-Interface > Accounting****Possible values:**

0 to 4294967295 seconds

Default:

15

6.3.2 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

Telnet 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

Telnet 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

Telnet path:**Setup > PMS-Interface > Login-Form > Free-Of-Charge-VIP-Status****Possible values:**

String, max. 20 characters

Default:

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

Telnet path:**Setup > PMS-Interface > Login-Form****Possible values:**

none

Reservation number

Arrival date

Departure date

First name

Profile number

Default:

none

Fedelio 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

Telnet path:**Setup > PMS-Interface > Login-Form****Possible values:**

none

Reservation number

Arrival date

Departure date

First name

Profile number

Default:

none

Fedelio 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

Telnet 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

Telnet 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.
- **Subject to charge:** Choose this option if you offer your hotel guests fee-based Internet access. Your hotel guests will be required to authenticate on the hotspot on the portal page with their username, room number and select a tariff.
- **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

Telnet path:

Setup > PMS-Interface > Login-Form

Possible values:

No

Yes

Default:

No

6.3.3 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

Telnet path:**Setup > PMS-Interface****Possible values:**

No

Yes

Default:

Yes

6.3.4 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

Telnet path:**Setup > PMS-Interface****Possible values:**

String, max. 1 characters

Default:

|

6.3.5 Character set

Choose the character used by the PMS to transmit your guests' surnames to the device.

SNMP ID:

2.64.7

Telnet path:**Setup > PMS-Interface****Possible values:**

CP850

W1252

Default:

CP850