

# Introduction to bintec elmeg WLAN Controller

|   |    |
|---|----|
| 1 Functional overview .....   | 2  |
| 2 Project planning.....   | 3  |
| 2.1 Determining customer requirements.....  | 3  |
| 2.2 Recommended hardware installation on site .....                                   | 3  |
| 3 System requirements .....   | 4  |
| 3.1 WLAN Controller hardware .....  | 4  |
| 3.2 Access Point hardware .....   | 4  |
| 3.3 WLAN Controller software licences.....  | 5  |
| 4 Network configuration .....   | 5  |
| 4.1. Internal DHCP server .....   | 5  |
| 4.2. External DHCP server.....  | 5  |
| 4.3 No DHCP server – APs with static IP address settings.....                         | 6  |
| 5 WLAN rollout with the WLAN controller assistant.....                                | 6  |
| 5.1 Step 1: Activation of the WLAN Controller.....                                    | 6  |
| 5.2 Step 2: Setup of the internal WLAN .....  | 8  |
| 5.3 Step 3: Adding a guest WLAN.....  | 10 |
| 6 Details and optional customization of WLAN controller assistant configuration ..... | 11 |
| 6.1 Overview of rollout configuration from the WLAN controller assistant .....        | 12 |
| 6.2 LAN configuration details for the guest WLAN .....                                | 16 |
| 6.3 Important notes on VLAN.....  | 19 |
| 6.4 E-mail alert in case of access point failure .....                                | 20 |
| 7 Appendix.....   | 21 |
| 7.1 Configuration of a DHCP server on another bintec elmeg router.....                | 21 |
| 7.2 Configuration of a DHCP server on Windows Server 2003/2008.....                   | 21 |
| 7.3. Configuration of a DHCP server under Linux.....                                  | 25 |
| 7.4 Operation of APs with static IP address settings.....                             | 25 |

## 1 Functional overview

The bintec elmeg WLAN Controller offers you the following advantages for managing your WLAN infrastructure:

- Assistant-guided quick installation of your WLAN network in at most 3 steps.
- Fully automatic recognition and installation of new bintec elmeg access points with all settings of your (multi SSID) WLAN network as soon they are connected to the WLAN Controller via LAN.
- Centralized easy management and configuration of all access points:
  - Centralised firmware updates for all managed access points
  - Configuration is centrally saved in the WLAN Controller and is automatically reassigned to access points e.g., after loss of power.
  - Adding new SSIDs requires just a few clicks and is finished in seconds. Modifications to SSIDs and other settings are deployed to all associated access points equally fast.
- Parallel support of all WLAN generations including WiFi 6 (802.11ax) with optimised defaults, as well as display of functional range of a managed access point such as possible radio frequencies or if it supports WPA3.
- Multi SSID WLAN networks with secure separation via VLAN and firewall for guest networks and other scenarios, support of all common WLAN security standards including WPA3 and (in combination with an external Radius server) WPA Enterprise authentication (802.1X) of WLAN clients for high assurance solutions.
- Access Points installed at public locations no longer are a security risk:
  - ALL WLAN network settings, including passwords are kept in volatile RAM of the AP only and are not saved in AP. As soon as the online connection to the WLAN Controller is disrupted the AP automatically reboots and is again in factory defaults. WLAN passwords etc. and hence cannot fall into unauthorised hands through AP theft.
  - As soon as an access point is managed by the WLAN Controller, direct configuration and monitoring access to the AP is blocked. Thus, it cannot be read out by third parties during operation.
- Automated frequency management:
  - Integrated channel planning with predefined channels in every frequency band, for non-overlapping frequency assignment.
  - Interference reduction through intelligent frequency assignment which takes neighbour access points into account as well.
- Surveillance:
  - of access points including their radio modules with meaningful indicators.
  - of client activity including radio cell-based localisation of clients.
  - recognition and display of (undesired) access points access points in the neighbourhood (neighbour APs, rogue APs etc.)
  - E-mail alert in case of outage of a managed access point
  - scheduler based actions (e.g., overnight shutdown of the WLAN)

## 2 Project planning

### 2.1 Determining customer requirements

It all starts with the customers and determining what their needs really are. In most cases customers want a WLAN infrastructure with two separate WLAN networks for employees and visitors throughout offices and meeting rooms, allowing employees wireless connection to the company network and the Internet, and allowing visitors wireless access to the Internet only.

Next the question arises of whether a radio frequency site survey by a specialist needs to be performed. Because of the considerable expense involved, the radio frequency site survey is frequently skipped; instead APs are positioned at customer discretion and in consideration of the facility's spatial arrangement.

However, in case of complex buildings or if the customer requires a high-performance network with continuous coverage and “voice over WLAN” (VoWLAN) readiness, a radio frequency site survey is indispensable.

### 2.2 Recommended hardware installation on site

Next an electrician comes into play to install the access points in corridors and offices. If doing without a radio frequency site survey, APs should be mounted at 15-20 meters distance to each other: this rule usually results in a functional setup.

All APs should be connected to a PoE-capable switch over an Ethernet cable. Power supply via the Ethernet cable (PoE) avoids installation of a 230V socket and considerably simplifies setup.

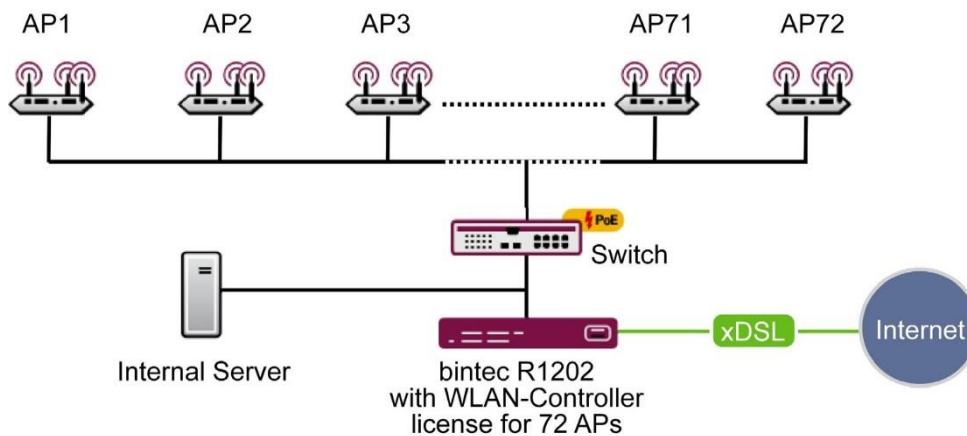


Figure 1: WLAN infrastructure

The electrician should document the locations and MAC addresses of the devices so that names or locations can later be assigned to the devices during configuration.

## 3 System requirements

### 3.1 WLAN Controller hardware

Almost all BOSS-based bintec elmeg devices with firmware versions 7.9.6 (published in October 2010) or higher can be used as WLAN controllers (supported devices with firmware versions lower than 7.9.6 need to be updated before installation).

It is recommended to use as WLAN controllers a device type for which a current BOSS firmware from 10.2.12 (published in September 2022) or higher is available:

- be.IP swift firmware is planned to have WLAN Controller support
- All BOSS firmware based routers of be.IP series (be.IP Plus V2, be.IP Plus, be.IP Plus World Edition, be.IP 4isdn, be.IP)
- All BOSS firmware-based routers of RSxx3 series (RS123, RS123w, RS123w-4G, RS353a, RS353aw, RS353awv-4G, RS353j, RS353j-4G, RS353jv, RS353jv-4G, RS353jw, RS353w-4G, RS353jwv, RS353jwv-4G)
- All BOSS firmware-based routers of RXL series (RXL12500 und RXL12100)
- All routers of Rxxx2 series (R1202, RT1202, R3002, RT3002, R3502, R3802, R4402, RT4202, RT4402)
- All access points of WIQ series (W2003ac, W2003ac-ext, WO2003ac, WO1003ac, APR222ac, W2004n, W2003n, W2003n-ext, W1001n, W1003n, WI1003n, WO2003n, WO1003n, W2002T-n)

For small installations up to 6 access points no dedicated WLAN controller hardware is needed and one of the access points (running as master access point) can take on the function of the WLAN controller. If a WLAN network with more than 6 access points is desired, a router is necessary as WLAN controller hardware.

### 3.2 Access Point hardware

The WLAN Controller can manage all OSDx firmware-based bintec elmeg access points as well all BOSS firmware-based bintec elmeg access points with firmware version 7.9.6 or higher, which support at least WiFi 4 (802.11n).

We recommend using OSDx firmware-based access points as well as BOSS firmware-based access points and routers with integrated WLAN for which a current BOSS firmware from 10.2.12 (published in September 2022) or higher is available:

- Router with integrated WLAN from be.IP series and RSxx3 series (these routers can manage itself and further access points, but cannot be managed from other routers)
- The OSDx firmware-based access points W2044ax, W2022ax, APR2044ax, W2022ac and W2022ac-ext
- All access points of WIQ series (W2003ac, W2003ac-ext, WO2003ac, WO1003ac, APR222ac, W2004n, W2003n, W2003n-ext, W1001n, W1003n, WI1003n, WO2003n, WO1003n, W2002T-n)

### 3.3 WLAN Controller software licences

From BOSS firmware version 10.2.12 or higher in any supported device the WLAN controller is activated with up to 6 freely manageable APs (namely without necessity to buy additional licenses up to that network size). In previous BOSS versions without additional licenses at most only a single access point could be managed via WLAN Controller.

With every additionally installed WLAN Controller license in the WLAN controller router 6 further access points can be managed. Up to eleven WLAN controller licences can be installed on an RSxx3 series router (e.g. RS123), allowing the management of a maximum of 72 access points. On central routers (e.g. RXL12100) up to 24 licenses can be installed, which allows for at maximum 150 managed access points.

Overview of minimum required WLAN controller hardware and licenses required in relation to the intended of number of access points:

|                              | Up to 6 AP                  | Up to 48 AP         | Up to 72 AP                         | Up to 150 AP      |
|------------------------------|-----------------------------|---------------------|-------------------------------------|-------------------|
| <b>Required WLC hardware</b> | None, runs on the master AP | be.IP series router | RSxx3 series or Rxxx2 series router | RXL series router |
| <b>WLC licenses</b>          | None                        | 7x                  | 11x                                 | 24x               |

## 4 Network configuration

### 4.1. Internal DHCP server

If there is no active DHCP server in your network, and if the WLAN controller device will also act as DHCP server (internal DHCP server) you can directly proceed with WLAN rollout with the WLAN controller assistant on page 6. The WLAN controller assistant includes the setup of all necessary DHCP server settings as well.

### 4.2. External DHCP server

For the access points to be manageable by the WLAN controller they must know the IP address of the WLAN controller. So, in addition to the required basic network settings such as device IP address, default gateway and nameserver, the DHCP server needs to provide the access point with the IP address of the WLAN controller. This is done via option 138 of the DHCP protocol. This option (also named CAPWAP Access Controller) must, therefore, be enabled on the DHCP server, and the IP address of the WLAN controller must be specified. In case:

- **Another bintec elmeg router is operating as DHCP server:** The required configuration steps are described in the appendix at page 21.
- **A Microsoft Server 2003 or Server 2008 is operating as DHCP server:** The required configuration steps are described in the appendix at page 21.
- **A Linux server is operating as DHCP server:** The required configuration steps are described in the appendix at page 25.
- **The router of a third-party provider is operating as DHCP server:** Please perform the configuration of DHCP option 138 according to the respective documentation.

### 4.3 No DHCP server – APs with static IP address settings

Occasionally, it may be necessary – however due to the high additional configuration effort it is not recommended – to operate a WLAN-controller-managed network with static IP address and network settings. Thus, each access point requires the manual configuration of IP and network settings. The necessary configuration steps for all access points are described in Appendix on page 25.

## 5 WLAN rollout with the WLAN controller assistant

The WLAN controller assistant guides you through configuration and rollout of your WLAN network in at most 3 steps. In the following example we assume that the WLAN Controller router is your internet access router as well.

### 5.1 Step 1: Activation of the WLAN Controller

Navigate in the GUI of your Wireless LAN Controller device to menu point “Assistants > WLAN (WLC)”. Only if the WLAN Controller in your device is not activated yet you will see the information page below with “Warning: Wireless LAN Controller is not activated.” In case you do not see this hint (e.g., on a “be.IP Plus” in factory defaults) the WLAN Controller is already active and you can directly skip to step 2.

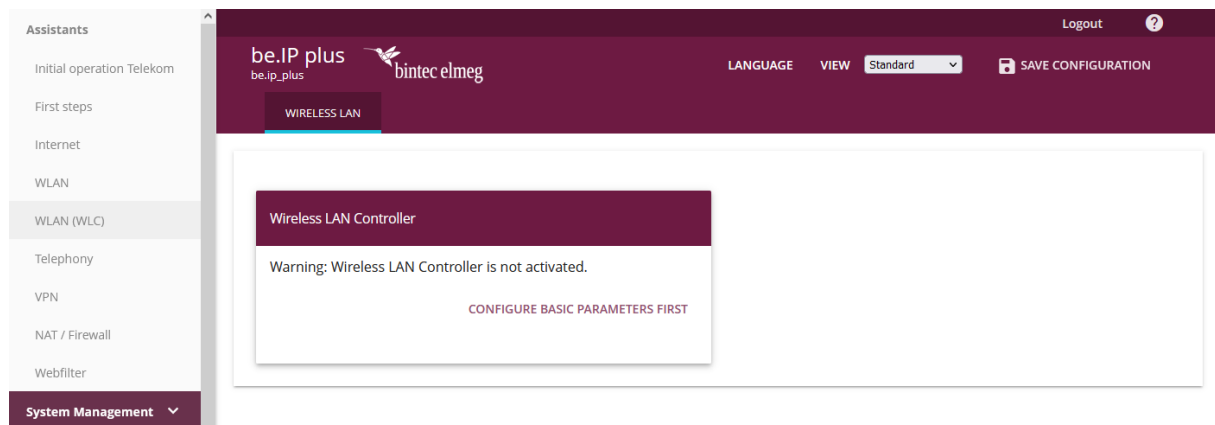


Figure 2: “Assistants > WLAN (WLC) > Wireless LAN Controller” WLAN Controller inactive

Click on the link “Configure basic parameters first”. You will be forwarded to the GUI page “Wireless LAN Controller > Controller Configuration > General”:

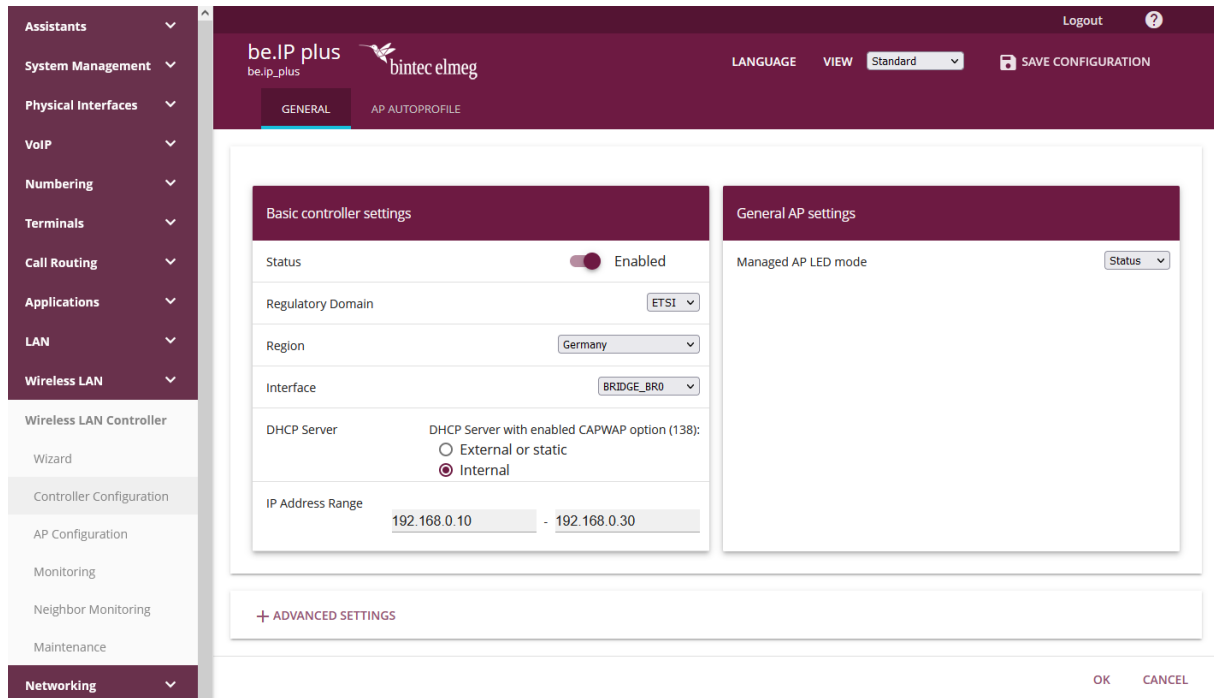


Figure 3: “Wireless LAN Controller > Controller Configuration > General” WLAN Controller enabled

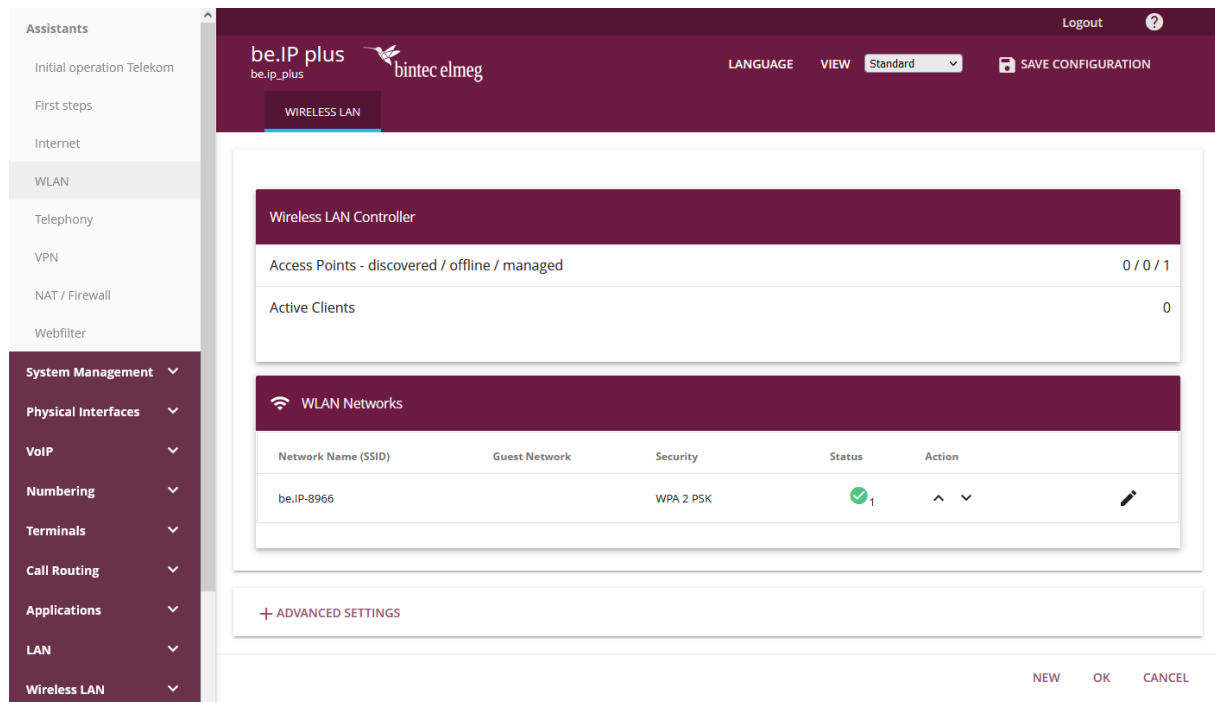
Here you define the basic characteristics of the WLAN Controller:

- **Status:** Set this status to “Enabled” to do the basic settings for the Wireless LAN Controller.
- **Regulatory Domain:** Here you can select the regulatory domain. It defines which frequencies are allowed for WLAN and needs to be identical to the factory-made fixed regulatory domain of your access points, otherwise the WLAN of your access points stays off. The default value is “ETSI” (European Telecommunications Standards Institute). Change this setting only if you have factory-made adapted access point for this purpose.
- **Region:** This setting adapts your WLAN network to the specific WLAN regulations of your region. You need to select the country where your access points are located.
- **Interface:** Defines over which interface the controller communicates with the APs (the IP of this interface is the WLAN Controller IP address configured in option 138 of the DHCP server).
- **DHCP Server:** Defines whether the “internal” or an “external” DHCP server is used for the access points. When using the internal DHCP server, all DHCP server settings including option 138 are made automatically. You'll find information on configuring an external DHCP server in appendix on page 21.
- **IP Address Range:** Defines the IP address range available to the internal DHCP server.

**Note:** If an external or internal DHCP server was already enabled at the time of AP installation, but DHCP option 138 was only subsequently enabled, the WLAN controller may fail to display the APs within your network. This can happen because the APs have already been assigned an IP address but have not yet received the WLAN controller IP address. This can be remedied by waiting for the expiration of the DHCP lease time or by restarting the APs.

## 5.2 Step 2: Setup of the internal WLAN

You are now on the overview page of the WLAN Controller assistant, which tells you how much access points are currently managed by the WLAN Controller, how many WLAN clients are connected in total over all configured WLAN networks and which WLAN networks are configured and on how many radio cells (one or two per AP, depending on hardware equipment of the AP) these WLAN networks are active. Per default on the “be.IP Plus” displayed here an internal WLAN is present, which is linked with your LAN network:



The screenshot shows the 'Wireless LAN Controller' overview page. The top navigation bar includes 'be.IP plus', 'bintec elmeg', 'LANGUAGE', 'VIEW Standard', and 'SAVE CONFIGURATION'. The left sidebar lists various system management options, with 'Wireless LAN' selected. The main content area is divided into two sections: 'Wireless LAN Controller' and 'WLAN Networks'. The 'Wireless LAN Controller' section shows 'Access Points - discovered / offline / managed' as 0 / 0 / 1 and 'Active Clients' as 0. The 'WLAN Networks' section contains a table with the following data:

| Network Name (SSID) | Guest Network | Security  | Status | Action            |
|---------------------|---------------|-----------|--------|-------------------|
| be.IP-8966          |               | WPA 2 PSK | 1      | ^ v [pencil icon] |

Below the table is a '+ ADVANCED SETTINGS' button. At the bottom right of the page, there are 'NEW', 'OK', and 'CANCEL' buttons.

Figure 4: "Assistants > WLAN (WLC) >Wireless LAN Controller" overview

You can edit this WLAN network with a click on the pencil:



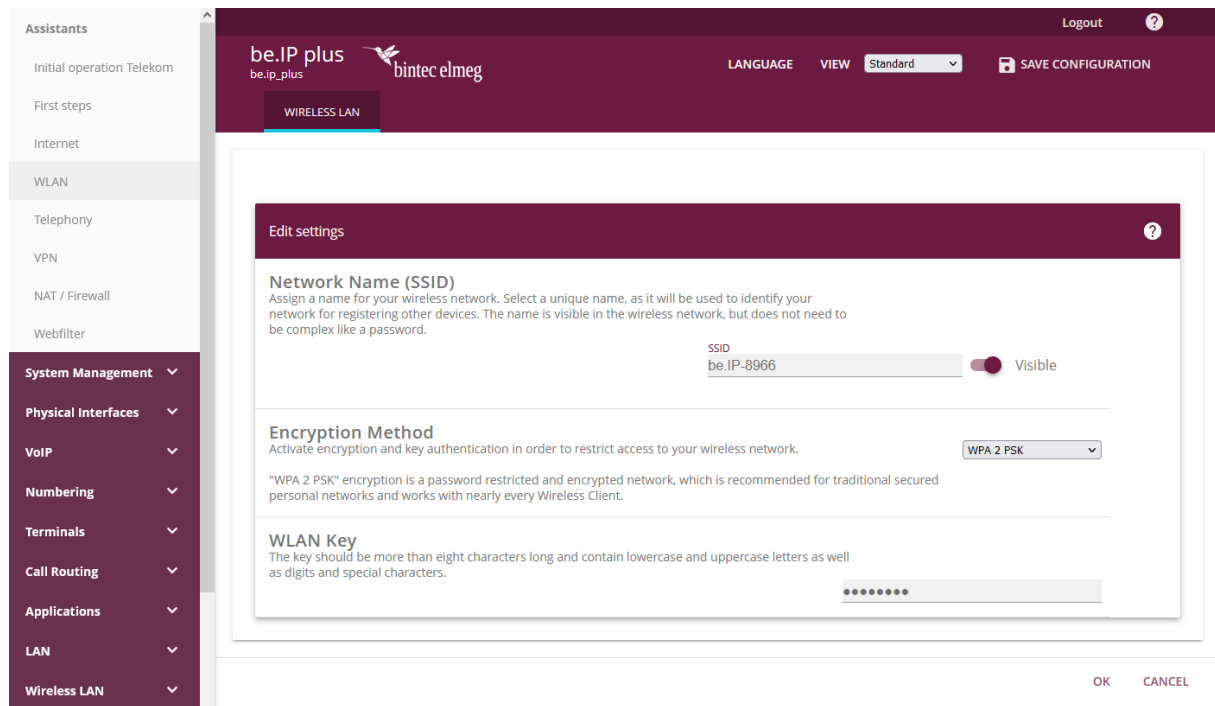


Figure 5: "Assistants > WLAN (WLC) >Wireless LAN Controller" edit WLAN network

Here you can setup your WLAN network:

- **Network Name (SSID):** Here you can assign a name to your WLAN by which it will be found by WLAN clients. Optionally you can define here that the WLAN name shall not be visible. At hidden WLAN networks WLAN user need to know the name and enter it manually into their WLAN client to be able connecting to the WLAN network.
- **Encryption Method:** The encryption method determines if and how users can access the WLAN network. Pre-set is "WPA 2 PSK", which is secure and as compatible as possible at the same time. You can choose out of a list of various methods from open unencrypted WLAN networks up to the high secure WPA 3. Concerning this matter please take note of the hints in the assistant, especially that the internal WLAN module of the bintec elmeg routers does not support WPA 3. You need W2022ac, W2022ac-ext, W2022ax or W2044ax access points with OSDx firmware version 2.4.1.1 or higher for WPA 3.
- **WLAN key:** The WLAN key needs to be at least 8 characters long and should be sufficiently complex to avoid that it can be figured out via trial and error by unauthorized persons.

With clicking on "OK" these settings are taken over immediately and rolled out to all access points on 2.4GHz band and (if available in the access point) on 5GHz band. Furthermore, access points added later automatically will be put into operation with these WLAN network settings immediately on connecting them to the LAN network. An extension of the WLAN network by further access points thus works fully automatic – except the mounting of the access points.

In the overview of page of the assistant you can check in summary (and more in detail on the detail menus explained further down in the text) if commissioning of the access points worked correctly.

Managed access points are locked by the WLAN controller and all direct access to them is prohibited. An access point can only be locally configured after the WLAN controller released the access point.

### 5.3 Step 3: Adding a guest WLAN

In the overview page of the WLAN Controller assistant, you can add further WLAN networks via clicking on “New” (in the lower right corner). You can setup up to 8 WLAN networks.

In this example we create a further WLAN network for guest access. After clicking on “New” you get a WLAN network configuration page with a further setting called “Guest Network”, which is available for newly created networks only. We setup our guest network analogue to the previous step with an own network name and WLAN key and additionally set the “Guest Network” to “Enabled”:

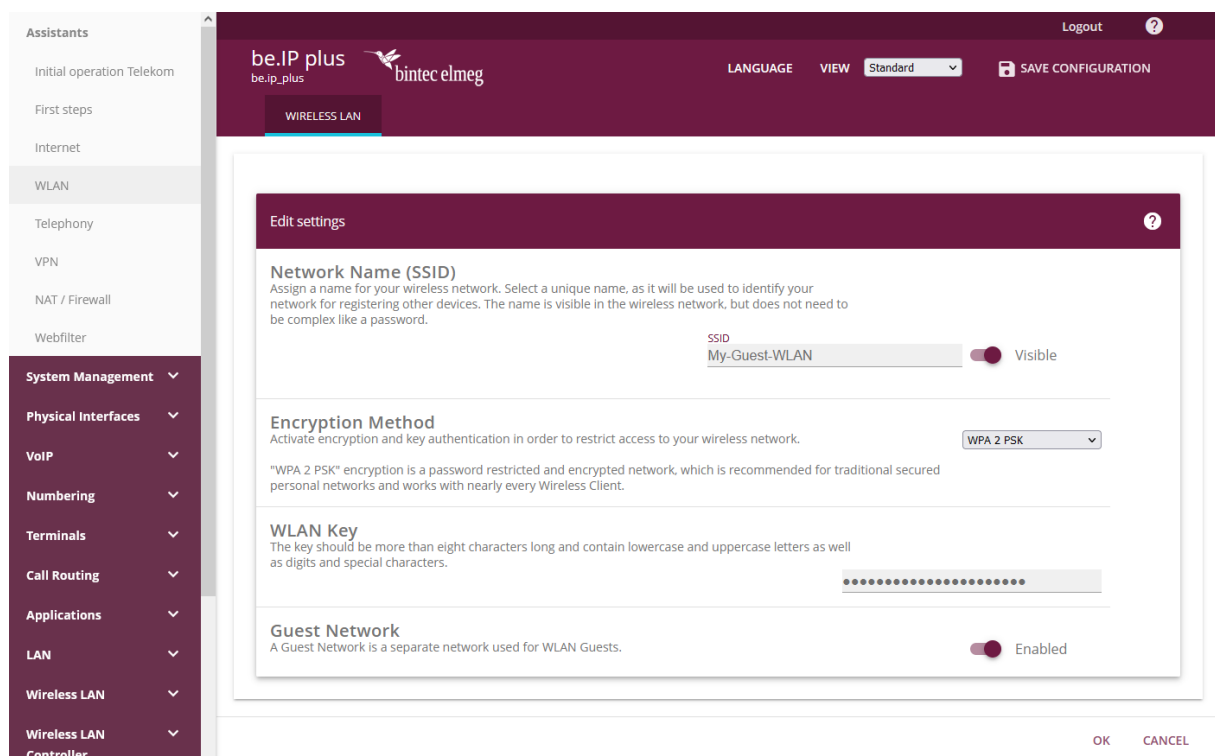


Figure: 6 "Assistants > WLAN (WLC) > Wireless LAN Controller" add guest WLAN network

In case the WLAN Controller router has no internet access configured via PPPoE (e.g. via xDSL) you will see on enabling the “Guest Network” function the warning message: “Attention! There is no Internet Connection over a PPPoE Interface configured, the Firewall settings for WLAN Guest Networks have to be set manually.” In the above example the Internet access is configured already. It is recommended to use the WLAN Controller router also as Internet access gateway especially in case of guest WLAN networks, as the firewall rules and further settings automatically rolled out by the assistant (also on the other router providing Internet access) would otherwise have to be created manually afterwards and adapted to the respective situation.

We leave that page with “OK” now and see afterwards the overview page of the WLAN Controller assistant with both networks:

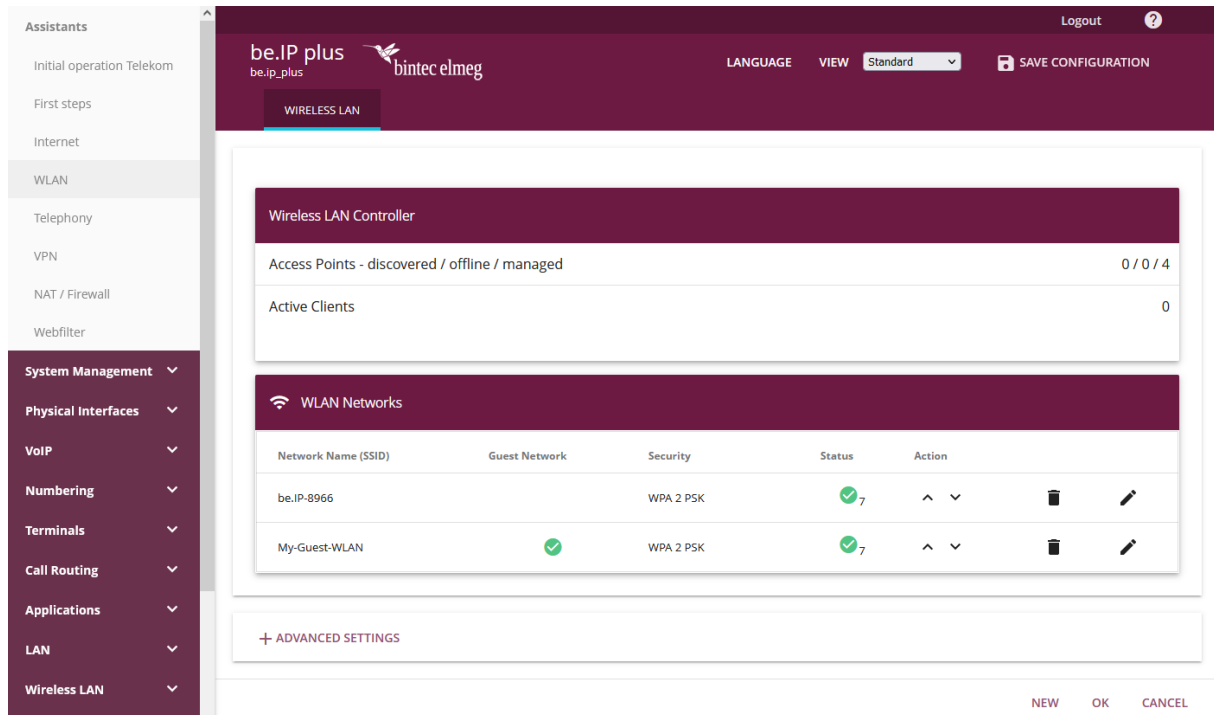


Figure 7: "Assistants > WLAN (WLC) >Wireless LAN Controller" overview of the finished configuration

The guest WLAN is automatically deployed like the internal WLAN on all current and later added access point (in the above example 3 further APs were added).

**The actual commissioning of the WLAN infrastructure with two separate WLAN networks for employees and guests is now successfully completed and you can use your WLAN. Please do not forget to save your successful configuration via the "Save configuration" button in the upper right corner.**

The access points themselves keep their current configuration in their volatile memory only and do not save it to their persistent memory. In the event of power failure, the configuration within the access points is lost and automatically re-loaded into the access point by the WLAN controller after power is restored. Keeping the configuration only in the volatile memory of the APs has the additional advantage that no sensitive access data (such as WLAN keys) can be compromised through theft of an access point installed at a public location.

Everything else is for a deeper understanding of the configuration rolled out by this assistant, for troubleshooting individual network components, and if you want to make adjustments that go beyond this assistant.

## 6 Details and optional customization of WLAN controller assistant configuration

In order to see the details of the configuration rolled out by the WLAN Controller assistant you need to switch on be.IP series routers the "View" to "Full Access" in the upper right corner first. On all other devices you do not need to do that intermediate step as they run in full access already.

## 6.1 Overview of rollout configuration from the WLAN controller assistant

In the left menu we now go to menu item “Wireless LAN Controller > Controller Configuration > General”. Either you know this page already from initial setup or in case the WLAN Controller was already active you now can view the basic settings of your WLAN Controller here.

In case you are distracted by the blinking of the access points you can globally set the LED status for all managed APs to “Off”. Please note: The access points now all look as if they are switched off. You can no longer see from the LED whether an AP is working or not. For BOSS based access points does this applies also after reboot and even in case it is not connected any longer to the WLAN Controller. You need to revert this setting (either via WLAN Controller or if the AP is not managed any longer via the internal GUI of the AP) to get the LED shining again.

We now go to the next tab “Wireless LAN Controller > Controller Configuration > AP Autoprofile”. There you find an auto profile, which was created (and extended) by the assistant and which automatically configures new access points with your WLAN settings:

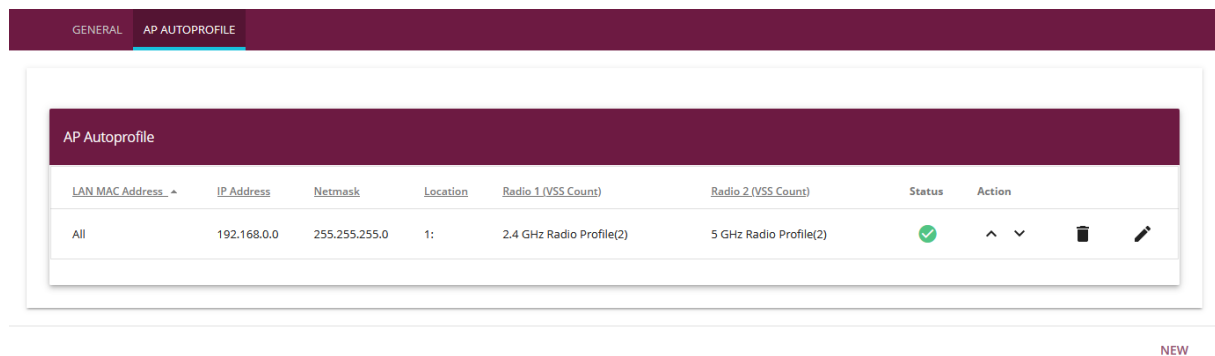





















Figure 8: Wireless LAN Controller > Controller Configuration > AP Autoprofile” overview

In menu item “Wireless LAN Controller > AP Configuration > Access Points” you see all found and managed access points with their status and configuration. On assignment of radio channels, the WLAN Controller takes care that APs use non-overlapping channels only and the managed access points take care that any interferences among each other are as low as possible.

To initiate a new tuning of the used channels after longer operation (e.g., if other neighbouring APs have been added) and thus minimize any WLAN interference, you can use the “Channel reallocation” function by clicking on “START”. While active the tuning causes unavoidable short interruptions in the operation of the WLAN at the APs (one after the other):

ACCESS POINTS
RADIO PROFILES
WIRELESS NETWORKS (VSS)

Access Points

| Location - Name ^ | IP Address    | LAN MAC Address   | Channel                          | Search Channel  | Status  | Action  |
|-------------------|---------------|-------------------|----------------------------------|---|---|---|
| 1-be.IP plus      | 192.168.0.251 | Elmegt_7f:01:54   | 5 HT20 (auto)                    |    |  Managed | ^ v   |
| 1-W2003ac         | 192.168.0.13  | BintecCo_49:10:f1 | 1 HT20 (auto) / 36 VHT40+ (auto) |   |  Managed | ^ v   |
| 1-W2022ac         | 192.168.0.15  | BintecCo_53:6a:06 | 9 HT20 (auto) / 56 VHT40- (auto) |   |  Managed | ^ v   |
| 1-W2044ax         | 192.168.0.17  | BintecCo_6e:60:1c | 13 HE20 (auto) / 44 HE40+ (auto) |   |  Managed | ^ v   |

Actions

Channel reallocation START

Figure 9: "Wireless LAN Controller > AP Configuration > Access Points" overview

Via the pencil icon you can see for every access point its hardware properties (number and characteristics of the radio module and if the access point for instance supports WPA3 or not), the radio profiles and wireless network profiles linked to it as well as further individual settings. Moreover, you can assign each device an individual location description here, which is recommended for a better overview in networks with many access points:

ACCESS POINTS
RADIO PROFILES
WIRELESS NETWORKS (VSS)

Access Point

|                 |                   |
|-----------------|-------------------|
| Device Type     | W2044ax           |
| Serial Number   | DAADZ-000190      |
| LAN MAC Address | 00:a0:f9:6e:60:1c |

Radio Module 1 supported features

Operation Band: 2.4 GHz @ ETSI  
Bandwidth: 20 MHz  
Wireless Mode: 802.11b/g/n/ax  
Spatial Streams: 4x4  
Data-rate trimming: Yes | WPA 3: Yes

Radio Module 2 supported features

Operation Band: 5 GHz @ ETSI  
Bandwidth: 20 MHz, 40 MHz, 80 MHz  
Wireless Mode: 802.11a/n/ac/ax  
Spatial Streams: 4x4  
Data-rate trimming: Yes | WPA 3: Yes

Access Point Settings

Location 1:

Name: W2044ax

Description 1:

Default Radius Server: None ▾

CAPWAP Encryption:  Enabled

Radio Module 1

Operation Mode:  On  Off

Active Radio Profile: 2.4 GHz Radio Profile ▾

Channel: Auto ▾

Channel in use: 13

Transmit Power: Max. ▾

Assigned Wireless Network (VSS)

| Profil              | MAC Address       | Status  |
|---------------------|-------------------|---|
| vss-1:be-IP-8966    | e2:a0:f9:6e:60:10 | <span style="color: green;">✔</span> <span style="color: gray;">🗑️</span> |
| vss-2:My-Guest-WLAN | e2:a0:f9:6e:60:11 | <span style="color: green;">✔</span> <span style="color: gray;">🗑️</span> |

Radio Module 2

Operation Mode:  On  Off

Active Radio Profile: 5 GHz Radio Profile ▾

Channel: Auto ▾

Channel in use: 52

Transmit Power: Max. ▾

Assigned Wireless Network (VSS)

| Profil              | MAC Address       | Status  |
|---------------------|-------------------|---|
| vss-1:be-IP-8966    | f2:a0:f9:6e:60:10 | <span style="color: green;">✔</span> <span style="color: gray;">🗑️</span> |
| vss-2:My-Guest-WLAN | f2:a0:f9:6e:60:11 | <span style="color: green;">✔</span> <span style="color: gray;">🗑️</span> |

OK CANCEL

Figure 10: “Wireless LAN Controller > AP Configuration > Access Points” edit page

In menu item “Wireless LAN Controller > AP Configuration > Radio Profiles” you will find two radio profiles, one for the 2.4GHz band and one for the 5GHz band, which are applied to the managed access points on their radio modules.

The 2.4GHz radio profile is optimized for best possible data throughput and frequency utilization in WLAN networks of more than one access point with default settings 802.11g/n/ax for wireless mode, 4 spatial streams, ETSI channel plan (1 – 5 – 9 – 13), enabled short guard interval and a beacon period of 100ms. The 5GHz radio profile has analogue default settings with a wider channel bandwidth and a channel plan optimized for 5GHz operation as there are more channels available.

Here you can customize radio frequencies, wireless mode, channel plans and more. Please note the context-sensitive online help and the online document linked in that page, which tells which settings are supported by what access point type. If an access point is configured by the WLAN controller with a setting that it does not support, it selects a setting that is closest to the transmitted configuration. Thanks to this “best effort approach” you can use even for different AP generations within the same

frequency band most times the same radio profile. Thus, you can keep the WLAN Controller configuration simple even in historically grown WLAN networks:

ACCESS POINTS
RADIO PROFILES
WIRELESS NETWORKS (VSS)

Please note that not all devices support all the options available in the WLAN Controller. A list which devices support which options can be found here: [http://system-update.eu/doc/misc/wlc\\_notes\\_en.pdf](http://system-update.eu/doc/misc/wlc_notes_en.pdf)

| Radio Profile Definition             | Performance Settings  |
|--------------------------------------|---|
| Description<br>2.4 GHz Radio Profile | Wireless Mode<br>802.11g/n/ax   |
| Operation Mode<br>Access Point       | Number of Spatial Streams<br>4  |
| Operation Band<br>2.4 GHz In/Outdoor | Airtime fairness<br><input checked="" type="checkbox"/> Enabled           |
|                                      | Cyclic Background Scanning<br><input checked="" type="checkbox"/> Enabled |

### Advanced Settings

| Frequency Settings  | Radio Timing                          |
|---|---------------------------------------|
| Channel Plan<br>ETSI Mode<br>(1, 5, 9, 13)                              | Beacon Period<br>100 ms               |
| Switch Channel on Jammer<br><input checked="" type="checkbox"/> Enabled | DTIM Period<br>2                      |
| Short Guard Interval<br><input checked="" type="checkbox"/> Enabled     | RTS Threshold<br>2347                 |
| Max. Transmission Rate<br>Auto  | Short Retry Limit<br>7                |
|   | Long Retry Limit<br>4                 |
|   | Fragmentation Threshold<br>2346 Bytes |

OK CANCEL

Figure 11: “Wireless LAN Controller > AP Configuration > Radio Profiles” edit page for „2.4GHz Radio Profile”

In menu item “Wireless LAN Controller > AP Configuration > Wireless Networks (VSS)” you will see the wireless network profiles for all WLAN networks, which you created previously via the WLAN Controller assistant. There you can do numerous customizations on detail settings and optimize them for your operation purpose, which were preallocated by the assistant with as general as possible values. Among others you can do there the security settings for WPA Enterprise, which are not selectable via the assistant (e.g., “WPA 3 Enterprise CNSA”, which is intended for high assurance networks), which especially are standard in WLAN networks of companies and agencies.

We now investigate the wireless network profile for the guest network. Guest networks are realized by the WLAN Controller via VLAN. In the edit page of the wireless network profile for the guest network you find the box “VLAN” further down in the page. There you see that VLAN is enabled and that the WLAN ID 3 has been assigned to it (every guest network created via the assistant gets an own VLAN ID in ascending order). That way all data from WLAN clients which are connected to that

guest network on an access point are tagged with VLAN ID 3 in Ethernet LAN. Thus, this network is securely separated from the untagged LAN network but still uses the same LAN cable infrastructure:

ACCESS POINTS
RADIO PROFILES
WIRELESS NETWORKS (VSS)

Please note that not all devices support all the options available in the WLAN Controller. A list which devices support which options can be found here: [http://system-update.eu/doc/misc/wlc\\_notes\\_en.pdf](http://system-update.eu/doc/misc/wlc_notes_en.pdf)

|  |  |
|--|--|
| <div style="background-color: #4a4a4a; color: white; padding: 5px; margin-bottom: 5px;"><b>Service Set Parameters</b></div> <p>Network Name (SSID)</p> <p><input type="text" value="My-Guest-WLAN"/> <input checked="" type="checkbox"/> Visible</p> <p>Intra-cell Repeating <input type="checkbox"/></p> <p>U-APSD <input type="checkbox"/></p> <p>IGMP Snooping <input checked="" type="checkbox"/> Enabled</p>  | <div style="background-color: #4a4a4a; color: white; padding: 5px; margin-bottom: 5px;"><b>Security Settings</b></div> <p>Security Mode <input type="text" value="WPA PSK"/></p> <p>WPA Mode <input type="text" value="WPA 2"/></p> <p>WPA2 Cipher <input checked="" type="radio"/> AES <input type="radio"/> TKIP <input type="radio"/> AES and TKIP</p> <p>Preshared Key <input type="text" value="••••••••"/></p> |
| <div style="background-color: #4a4a4a; color: white; padding: 5px; margin-bottom: 5px;"><b>Client load balancing</b></div> <p>Max. number of clients - hard limit <input type="text" value="32"/></p> <p>Max. number of clients - soft limit <input type="text" value="28"/></p> <p>Client steering <input type="text" value="Disabled - optimized for fast roaming"/></p> <p>Fast BSS Transition (802.11r) <input type="text" value="Disabled"/></p> <p>Radio Resource Management (802.11k) <input type="checkbox"/></p> <p>Network assisted Roaming (802.11v) <input type="checkbox"/></p> | <div style="background-color: #4a4a4a; color: white; padding: 5px; margin-bottom: 5px;"><b>MAC-Filter</b></div> <p>Access Control <input type="checkbox"/></p> <p>Dynamic blacklisting <input checked="" type="checkbox"/> Enabled</p> <p>Failed attempts per Time <input type="text" value="10"/> / <input type="text" value="60"/> Seconds</p> <p>Blacklist blocktime <input type="text" value="500"/> Seconds</p> |
| <div style="background-color: #4a4a4a; color: white; padding: 5px; margin-bottom: 5px;"><b>VLAN</b></div> <p>VLAN <input checked="" type="checkbox"/> Enabled</p> <p>VLAN ID <input type="text" value="3"/></p>  | <div style="background-color: #4a4a4a; color: white; padding: 5px; margin-bottom: 5px;"><b>Bandwidth limitation for each WLAN client</b></div> <p>Rx Shaping <input type="text" value="No limit"/></p> <p>Tx Shaping <input type="text" value="No limit"/></p>   |
| <div style="background-color: #4a4a4a; color: white; padding: 5px; margin-bottom: 5px;"><b>Data-rate trimming</b></div> <p>2.4 GHz band data rate profile <input type="text" value="All (Min. 1 MBit/s)"/></p> <p>5 GHz band data rate profile <input type="text" value="All (Min. 6 MBit/s)"/></p>  | <div style="background-color: #4a4a4a; color: white; padding: 5px; margin-bottom: 5px;"><b>Low RSSI threshold management</b></div> <p>RSSI threshold <input type="text" value="-110"/> dBm</p> <p>Grace time <input type="text" value="5"/> Seconds</p>  |

OK CANCEL

Figure 12: “Wireless LAN Controller > AP Configuration > Wireless Networks (VSS)” edit page for the guest WLAN network

## 6.2 LAN configuration details for the guest WLAN

However, a VLAN needs an own access interface as well, which deploys a separate IP network via DHCP, as well as services like DNS and which controls access to the Internet. For this purpose the WLAN Controller assistant has created in the WLAN Controller router an own virtual interface with VLAN ID 3, which is based on the interface of the WLAN Controller and which you can find in menu



item “LAN > IP Configuration”. In be.IP series this virtual interface is called “br0-1” in default settings (as the WLAN Controller interface is “br0” in default settings there). In the configuration of this virtual interface you see again the VLAN ID 3, as well as the IP address 192.168.3.1 (the penultimate block of the IP address is always assigned the same number as the VLAN ID by the assistant for a better overview) and that the security policy of this interface is set to “Untrusted”:

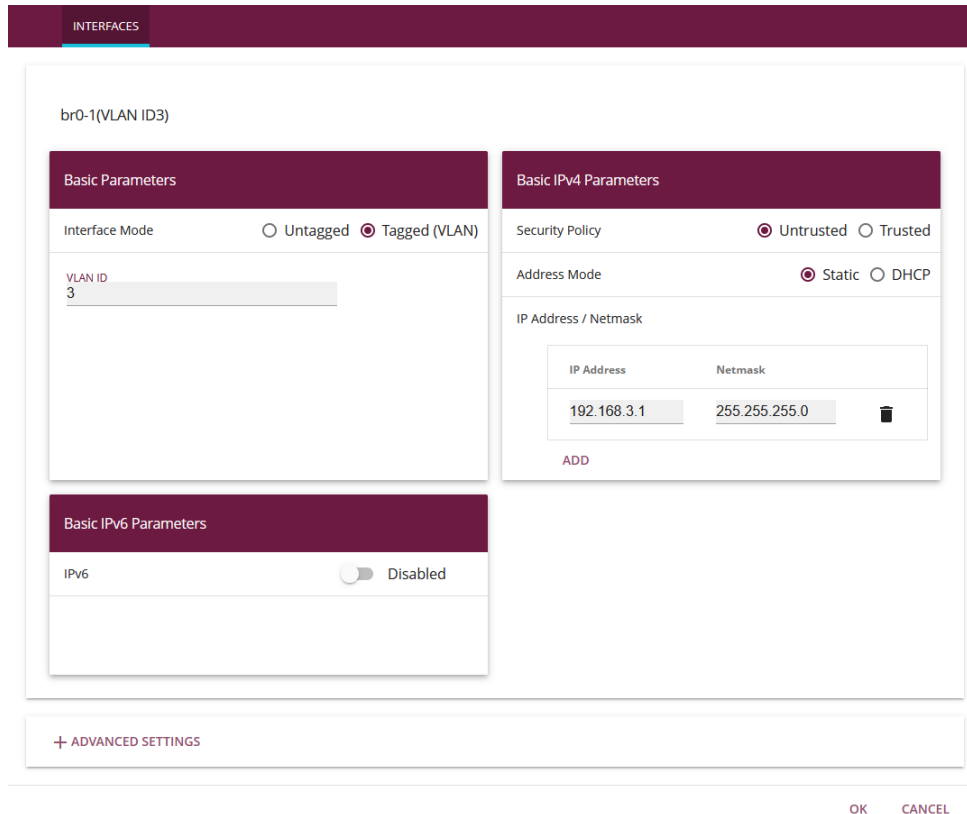


Figure 13: “LAN > IP Configuration” edit page for virtual interface “br0-1”

The DHCP server instance created by the WLAN controller assistant for the VLAN of the guest network can be found in the “Local Services > DHCP Server” menu. In the “Local Services > DHCP Server > IP Pool Configuration” page, you will find an IP pool from the 192.168.3.x network which name is identical to the network name assigned in the wizard for this guest WLAN:

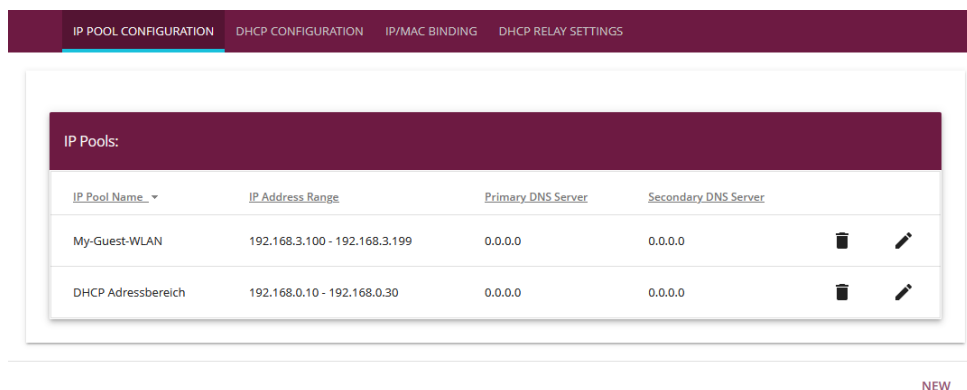


Figure 14: “Local Services > DHCP Server > IP Pool Configuration” overview

Finally, in the “Local Services > DHCP Server > DHCP Configuration” page, you will find the DHCP server instance for this pool, bound to the virtual interface for VLAN 3:

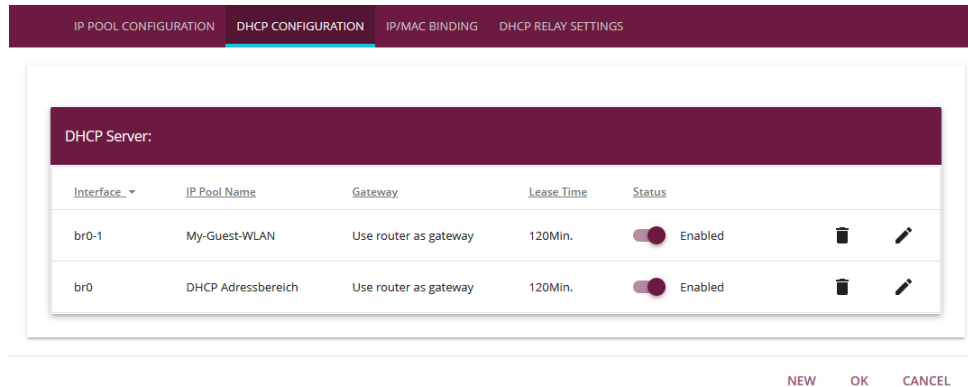


Figure 15: “Local Services > DHCP Server > DHCP Configuration” overview

In the “Firewall” menu, the WLAN controller assistant has created firewall rules that allow the devices in the guest network to access the Internet and which block access to all other local networks (including any other guest networks that may have been set up) and to the router itself. In the “Firewall > Policies > IPv4 Filter Rules” page, you can see three firewall rules created by the WLAN controller assistant for the virtual interface in VLAN 3 and a default filter rule:

1. The first rule allows access to essential services (DHCP and DNS) in the router, which are summarized in the service group “wlan-guest-local-access”.
2. The second rule is an optional rule (which you can subsequently disable via the check) that prevents IP telephony over the guest network.
3. The third rule allows access to the Internet interface and thus to the Internet for services, which are listed in the services group “Internet”.
4. Since the virtual interface for VLAN 3 – as mentioned above – is set to “Untrusted”, the fourth rule is the standard filter rule “n+2”, which discards all other data connections not covered by the above rules.

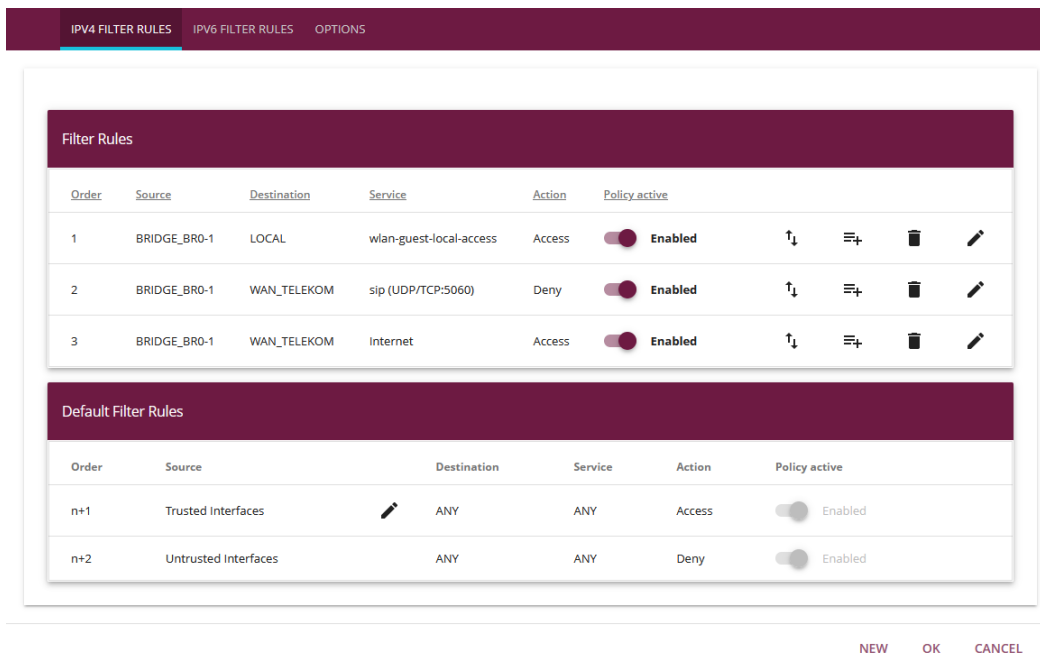


Figure 16: "Firewall > Policies > IPv4 Filter rules" overview

The service groups "wlan-guest-local-access" and "Internet" created by the assistant can be found in the GUI page "Firewall > Services > Groups". There you can view the network services allowed in the respective groups and subsequently adapt them to your needs:

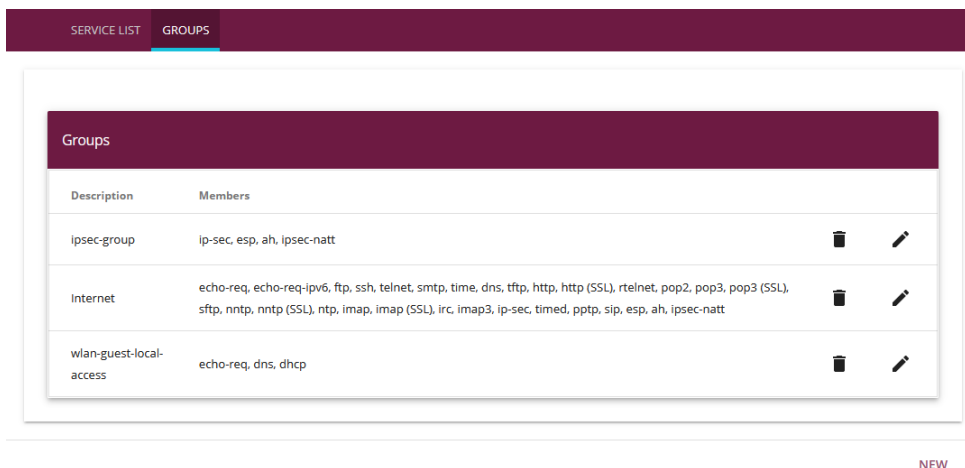


Figure 17: "Firewall > Services > Groups" overview

### 6.3 Important notes on VLAN

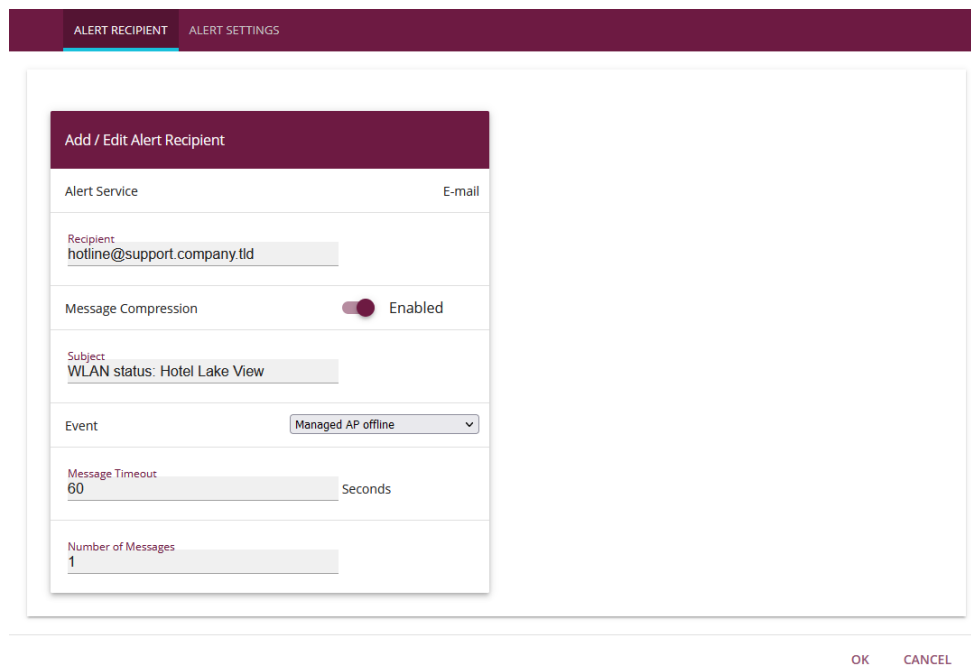
For the WLAN guest network and other VLAN-tagged WLAN networks to work on access points that are connected to the WLAN controller router through a network switch, your network switch must accept these VLAN IDs "tagged" on all ports to which the access points and WLAN controller router are connected. Most modern network switches discard any VLANs that are not explicitly allowed on the network switch.

In the event of a problem, your WLAN clients will see the WLAN guest network at the access points and can also log on to the WLAN, but they will not receive any network connection (and most smartphones will log off from the WLAN again immediately as a result, so that it looks as if the device cannot connect to the WLAN).

In this case, please configure your network switch to pass through the required VLANs according to the manual from your network switch manufacturer.

## 6.4 E-mail alert in case of access point failure

Starting with BOSS release 7.10.1 the WLAN Controller offers the option to send an e-mail in case one of the managed access points goes off or is no longer reachable. This is especially helpful in larger and complex WLAN infrastructures where this kind of failure does not become immediately apparent. The necessary configuration is done on the WLAN Controller device in the menu “External Reporting > E-mail Alert > E-mail Alert Recipient” (the server settings for e-mail alert are not described here). There you add a new entry:



The screenshot shows a configuration window titled "Add / Edit Alert Recipient". It contains the following fields and settings:

- Alert Service:** E-mail
- Recipient:** hotline@support.company.tld
- Message Compression:** Enabled (toggle switch)
- Subject:** WLAN status: Hotel Lake View
- Event:** Managed AP offline (dropdown menu)
- Message Timeout:** 60 Seconds
- Number of Messages:** 1

Buttons for "OK" and "CANCEL" are located at the bottom right of the window.

Figure 18: “External Reporting > E-mail Alert > E-mail Alert Recipient” adding an alert for a failed access point

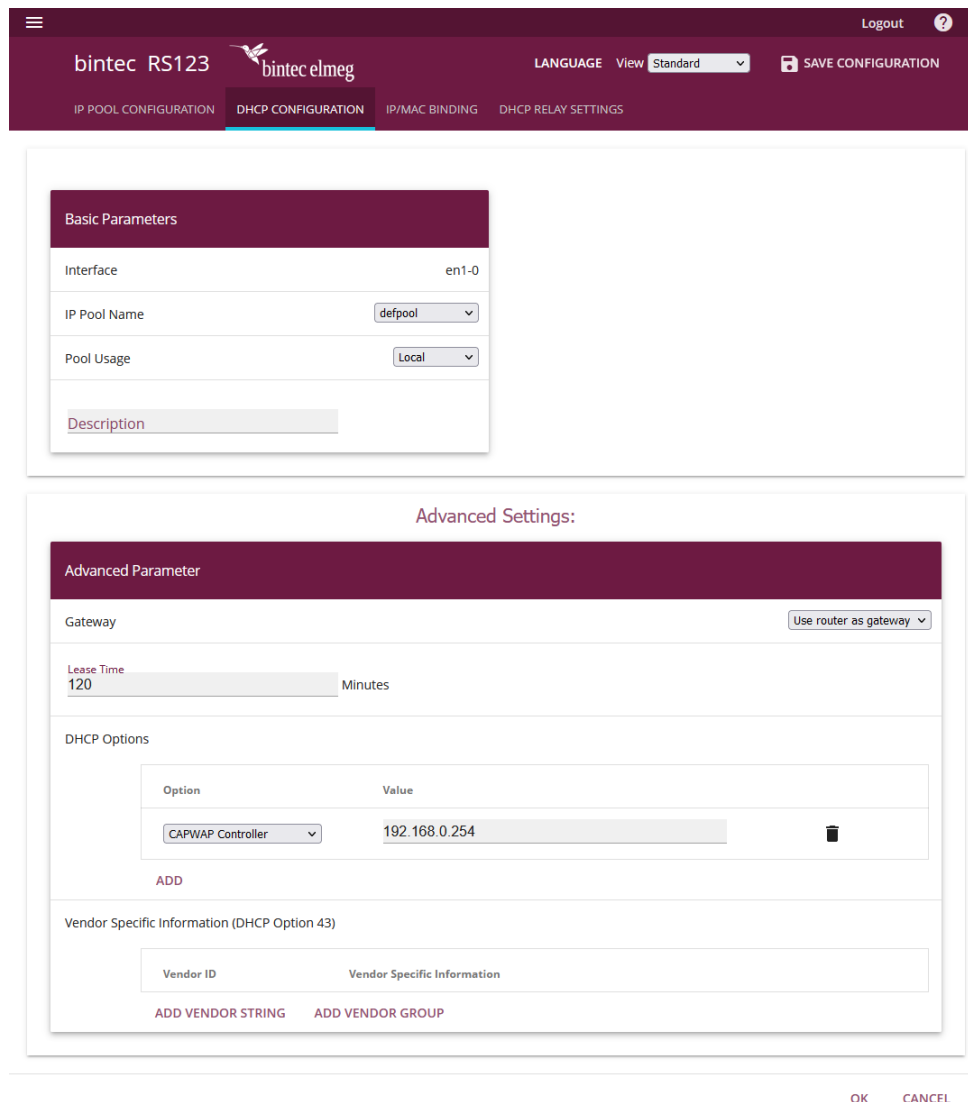
Here you define your desired e-mail alert:

1. **Recipient:** The email address of the mailbox that should receive this notification.
2. **Subject:** Select a suitable subject, so that you can assign the e-mail in your mailbox more easily.
3. **Event:** Select here the predefined event “Managed AP offline” from the drop-down list.

## 7 Appendix

### 7.1 Configuration of a DHCP server on another bintec elmeg router

The requirement is a bintec elmeg router with BOSS software release 7.9.5 Patch 4 or higher. Here the DHCP option “CAPWAP Controller” needs to be selected in edit page of GUI item “Local Services > DHCP Server > DHCP Configuration” and the IP address of the WLAN controller device needs to be entered in the “Value” field:



The screenshot displays the DHCP Configuration page in the bintec elmeg router GUI. The interface is divided into two main sections: Basic Parameters and Advanced Settings.

**Basic Parameters:**

- Interface: en1-0
- IP Pool Name: defpool
- Pool Usage: Local
- Description: (empty field)

**Advanced Settings:**

- Gateway: Use router as gateway
- Lease Time: 120 Minutes
- DHCP Options:
 

| Option            | Value         |
|-------------------|---------------|
| CAPWAP Controller | 192.168.0.254 |
- Vendor Specific Information (DHCP Option 43):
 

| Vendor ID | Vendor Specific Information |
|-----------|-----------------------------|
|           |                             |

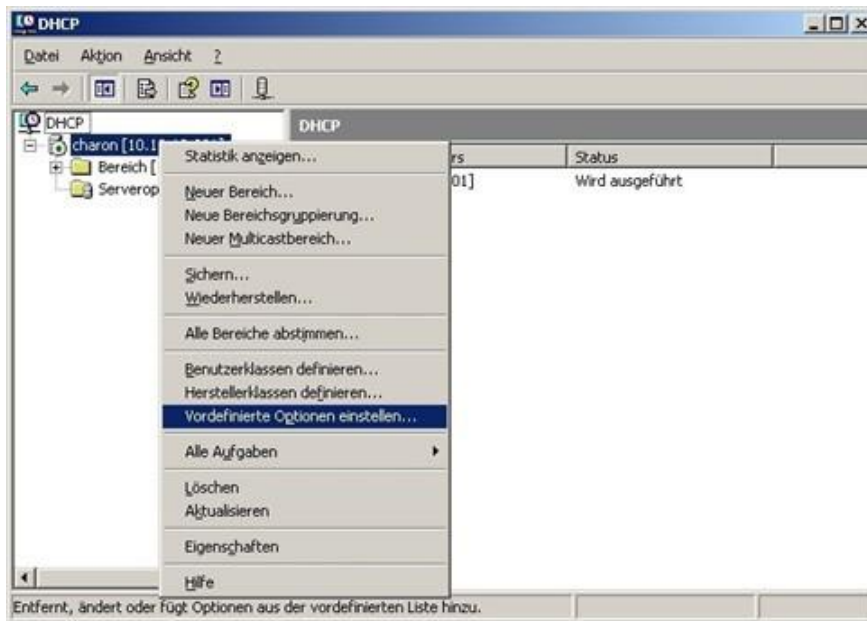
Buttons for 'ADD VENDOR STRING' and 'ADD VENDOR GROUP' are visible at the bottom of the Vendor Specific Information section. At the bottom right of the entire configuration area, there are 'OK' and 'CANCEL' buttons.

Figure 19: “Local Services > DHCP Server > DHCP Configuration” add “CAPWAP Controller” in edit page

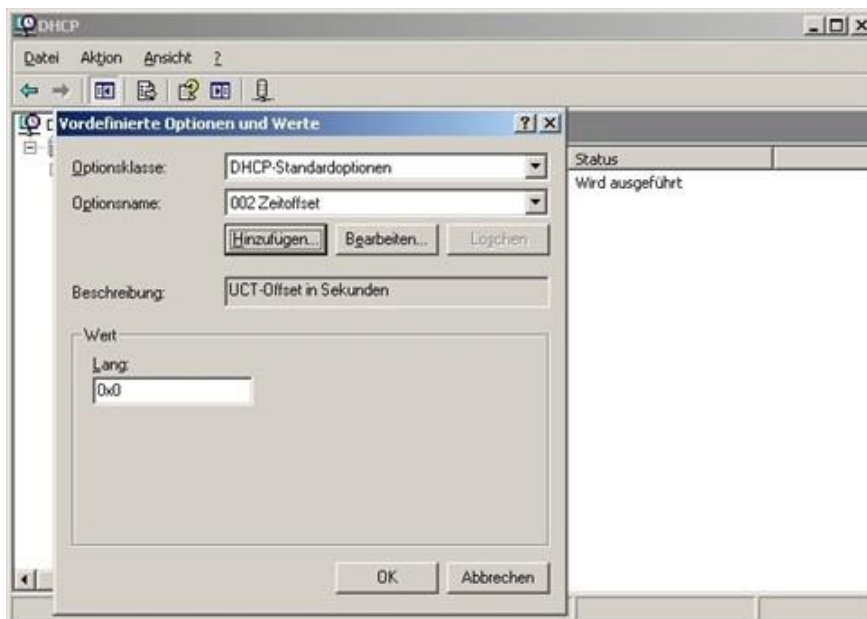
### 7.2 Configuration of a DHCP server on Windows Server 2003/2008

First, your Windows DHCP server service must receive a basic set up, i.e., the DHCP IP address range needs to be defined, and standard options such as DNS server and standard gateway need to be configured according to your network infrastructure.

In the DHCP service window (accessible via Control Panel, there under Administration), right-click on the existing DHCP service instance (you can identify it through the computer name and the IP address the DHCP service is linked to), then click on “Set Predefined Options” in the expanded context menu:



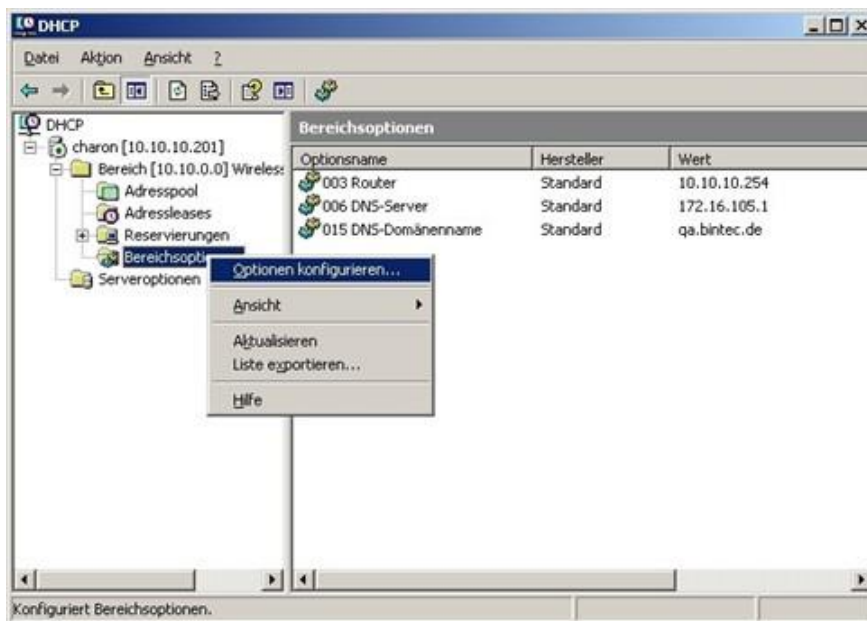
In the window which now opens, click “Add” to add the CAPWAP option, which is not predefined by default:



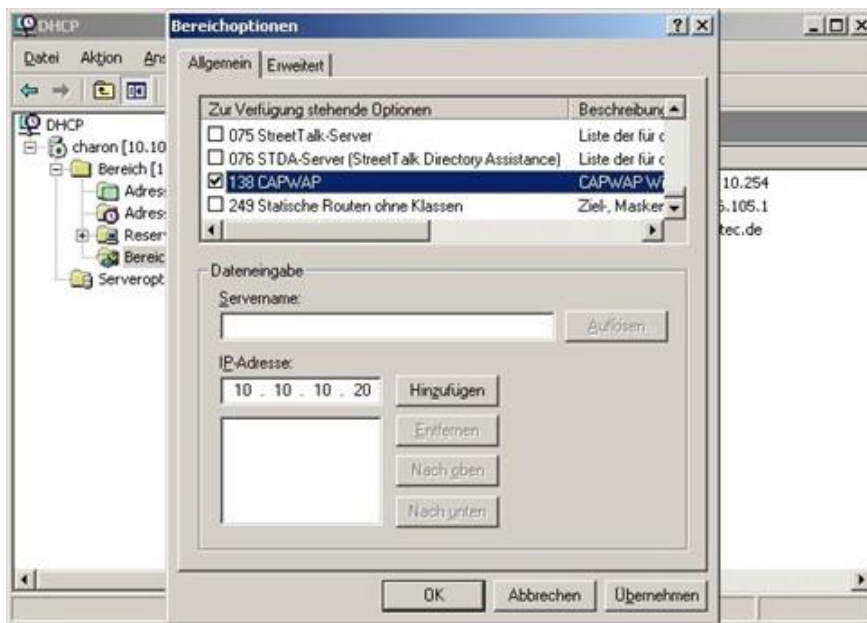
In the “Option Type” dialogue window, the CAPWAP option is now defined (but not yet activated). “Name” and “Description” can be freely selected but should be named plausible. The data type must be set to “IP address” and “Array” setting needs to be checked. In addition, “Code” must be set to “138”. If the code is already in use for another, self-defined DHCP option not matching the CAPWAP DHCP option, the pre-existing one must first be deleted. Close the dialogue and the previous window by clicking “OK”:



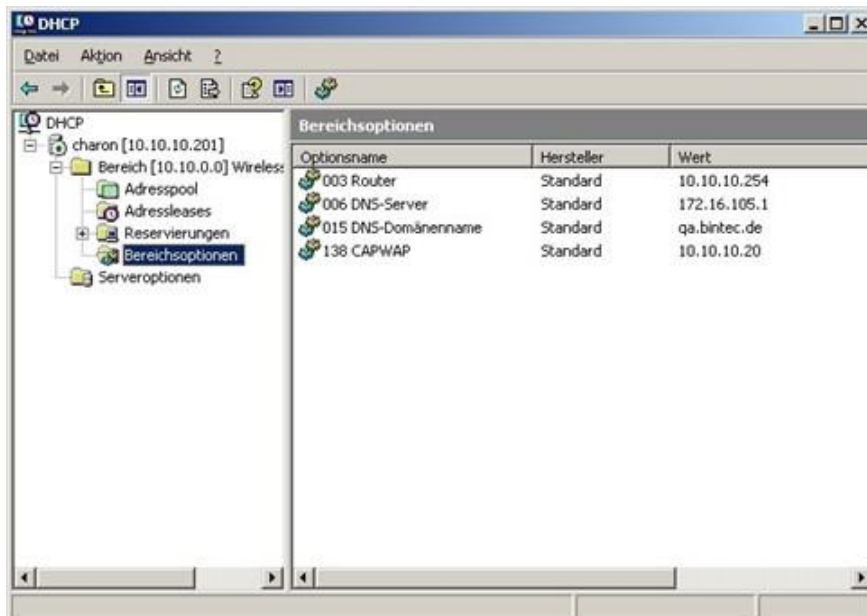
Now, in the IP address range of the DHCP service already configured for future access points, right-click "Range Options" and select "Configure Options" in the context menu:



In the expanding dialogue window, select option "138" in the list of "Available Options". In the "IP Address" entry field, enter the IP address of the WLAN controller; then, on the right, click "Add". Theoretically, it is possible to enter several WLAN controller IP addresses here. At present, however, only the first IP address is considered by the access points. Now leave this dialogue box by clicking "OK":



The DHCP service overview window should now also list the CAPWAP option. At this stage, the access points and the WLAN controller in the network for which the DHCP service has been configured, can go into operation:





### 7.3. Configuration of a DHCP server under Linux

In the configuration file “/etc/dhcp/dhcpd.conf”, add the following (of course adapted to your network):

```
# Format definition of DHCP CAPWAP option for WLAN Controller
option wlan-controller code 138 = array of ip-address;
# IP address range for managed Access Points
subnet 192.168.0.0 netmask 255.255.255.255 {
    range 192.168.0.10 192.168.0.200;
    option domain-name-servers mydnsserver.mydomain.tld;
    # IP address of your gateway for this network
    option router 192.168.0.1;
    option broadcast-address 192.168.0.255;
    default-lease-time 7200;
    max-lease-time 7200;
    # IP address of your WLAN Controller
    option wlan-controller 192.168.0.251
}
```

The lines beginning with option “wifi-controller” are the most crucial ones. The first of these two lines defines the data format of option 138, as it is not contained in the standard format definitions of the dhcpd. The second of these two lines specifies the IP address of the WLAN controller to which the individual access points connect to after they have received all necessary data (own IP address, WLAN controller IP address etc.) from the DHCP server.

All other specifications are standard for the definition of a DHCP pool: “subnet”, “range”, “domain-name-servers”, “routers” etc. need to be configured according to your requirements.

Once the configuration file is saved, you need to restart the DHCP server.

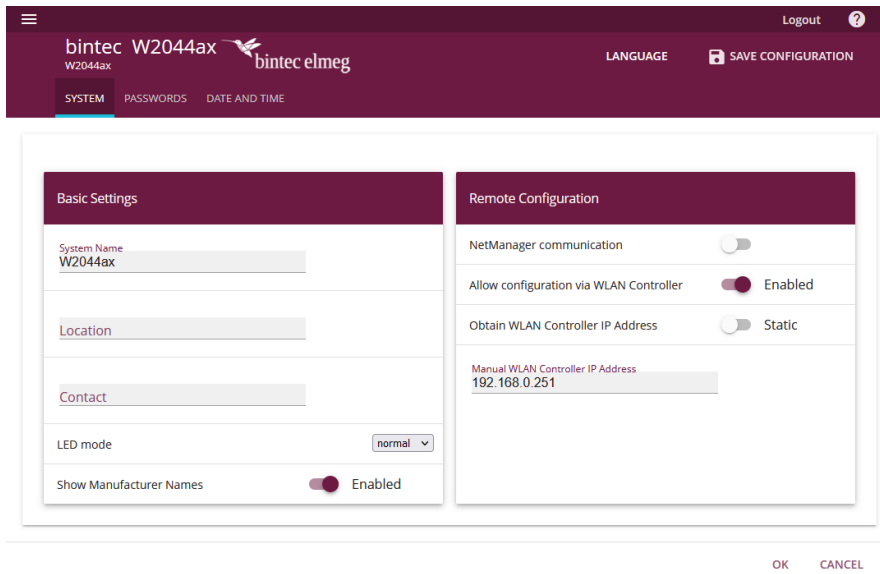
### 7.4 Operation of APs with static IP address settings


On the WLAN controller device, when starting the WLAN Controller assistant, make sure that “External or static” is selected in the first step of the configuration for the DHCP server.

As described in on page 5 the DHCP server not only assigns IP addresses but also provides the access points to be managed with the IP address of the WLAN Controller. In case of static IP address settings for access points it is necessary not only to specify an IP address and a netmask at each access point that is to be managed, but also to manually specify the IP address of the WLAN Controller.

On OSDx-based APs and on BOSS-based APs starting with release 7.10.1 you can find the necessary configuration parameter “Manual WLAN Controller IP Address” in the menu item “System Management > Global Settings > System”:

## WLAN Controller Introduction



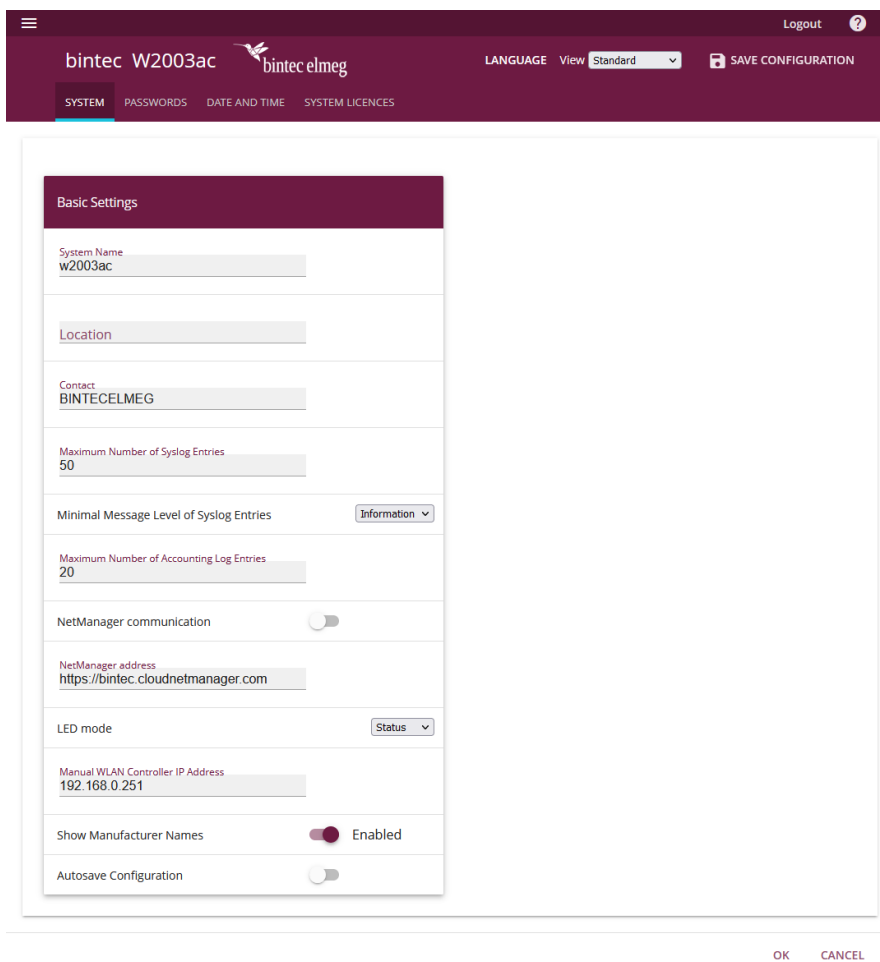
bintec W2044ax  Logout ?  
 LANGUAGE SAVE CONFIGURATION  
 SYSTEM PASSWORDS DATE AND TIME


**Basic Settings**  
 System Name: W2044ax  
 Location:  
 Contact:  
 LED mode: normal  
 Show Manufacturer Names: Enabled

**Remote Configuration**  
 NetManager communication:   
 Allow configuration via WLAN Controller:  Enabled  
 Obtain WLAN Controller IP Address:  Static  
 Manual WLAN Controller IP Address: 192.168.0.251

OK CANCEL

Figure 20: Configuration on an OSDx-based AP such as the W2044ax



bintec W2003ac  Logout ?  
 LANGUAGE View: Standard SAVE CONFIGURATION  
 SYSTEM PASSWORDS DATE AND TIME SYSTEM LICENCES

**Basic Settings**  
 System Name: w2003ac  
 Location:  
 Contact: BINTECELMEG  
 Maximum Number of Syslog Entries: 50  
 Minimal Message Level of Syslog Entries: Information  
 Maximum Number of Accounting Log Entries: 20  
 NetManager communication:   
 NetManager address: https://bintec.cloudnetmanager.com  
 LED mode: Status  
 Manual WLAN Controller IP Address: 192.168.0.251  
 Show Manufacturer Names: Enabled  
 Autosave Configuration:

OK CANCEL

Figure 21: Configuration on a BOSS-based AP such as the W2003ac