

Industrial Ethernet Training 24

Setting up a Weidmueller WiFi access point

Abstract:

A WiFi access point is a device that creates a wireless local area network, or WLAN. An access point connects to a network or a single device via an Ethernet cable (LAN), and projects a WiFi signal to a designated area. For example, if you want to have access to a machine or vehicle in your production hall via WiFi but the machine does not provide a wireless signal, you can install an access point to it and provide the production hall with a wireless signal for your computer/laptop to connect to. This application note shows how to configure the access point to connect to the network wirelessly.

Setting up a Weidmueller WiFi access point

Hardware reference

No.	Component name	Article No.	Hardware / Firmware version
1	IE-Training Kit-01	2881730000	1.1.2 (Build 125086)
2	Wireless Access Point/Client	2536600000	1.16.18 (Build 18081617)
3			

IE-Training Kit Content

No.	Component name	Article No.	Hardware / Firmware version
1	IE-SR-4TX	2751270000	1.4.7
2	IE-SW-AL08M-8TX	2682280000	1.08
3	IE-SW-AL05M-5TX	2682250000	1.14
4	IE-CS-MBGW-2TX-1COM	2682600000	3.11

Software reference

No.	Software name	Article No.	Software version
1			
2			
3			

File reference

No.	Name	Description	Version
1			
2			

Contact

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
www.weidmueller.com

For any further support please contact your
local sales representative:
<https://www.weidmueller.com/countries>

Content

1 Warning and Disclaimer..... 4

2 Prerequisites for doing..... 5

3 Factory default and firmware update..... 6

3.1 Default IP and credentials..... 6

3.2 Firmware update..... 6

4 Usage of an Access Point..... 7

4.1 Setting a new IP address for the Access Point..... 7

5 Configuring a new service set ID (SSID) and password for the WiFi access.....10

5.1 Configuring SSID.....10

5.2 Creating a password.....12

6 Results14

1 Warning and Disclaimer

Warning

Controls may fail in unsafe operating conditions, causing uncontrolled operation of the controlled devices. Such hazardous events can result in death and / or serious injury and / or property damage. Therefore, there must be safety equipment provided / electrical safety design or other redundant safety features that are independent from the automation system.

Disclaimer

This Application Note / Quick Start Guide / Example Program does not relieve you of the obligation to handle it safely during use, installation, operation and maintenance. Each user is responsible for the correct operation of his control system. By using this Application Note / Quick Start Guide / Example Program prepared by Weidmüller, you accept that Weidmüller cannot be held liable for any damage to property and / or personal injury that may occur because of the use.

Note

The given descriptions and examples do not represent any customer-specific solutions, they are simply intended to help for typical tasks. The user is responsible for the proper operation of the described products. Application notes / Quick Start Guides / Example Programs are not binding and do not claim to be complete in terms of configuration as well as any contingencies. By using this Application Note / Quick Start Guide / Example Program, you acknowledge that we cannot be held liable for any damages beyond the described liability regime. We reserve the right to make changes to this application note / quick start guide / example at any time without notice. In case of discrepancies between the proposals Application Notes / Quick Start Guides / Program Examples and other Weidmüller publications, like manuals, such contents have always more priority to the examples. We assume no liability for the information contained in this document. Our liability, for whatever legal reason, for damages caused using the examples, instructions, programs, project planning and performance data, etc. described in this Application Note / Quick Start Guide / Example is excluded.

Security notes

In order to protect equipment, systems, machines and networks against cyber threats, it is necessary to implement (and maintain) a complete state-of-the-art industrial security concept. The customer is responsible for preventing unauthorized access to his equipment, systems, machines and networks. Systems, machines and components should only be connected to the corporate network or the Internet if necessary and appropriate safeguards (such as firewalls and network segmentation) have been taken.

2 Prerequisites for doing

You need to have the following hardware and documentation

- Industrial Ethernet Training Kit including the WiFi Access Point device
- Application Note Industrial Ethernet Training 01 “Setting up default configuration of IE Training Kit” for applying default IP address configuration

3 Factory default and firmware update

3.1 Default IP and credentials

Number	Device	IPv4	Username	Password
1	IE-WL-BL-AP-CL-EU	192.168.1.110	admin	Detmold

Table 1: Default Credentials of the device

These are the default addresses and user credentials to access the access point in the default configuration.

Hint: If you cannot access the access point via the default IP (*192.168.1.110*) or made unwanted, irreversible changes, a reset might be necessary. To do that, you can refer to the manual to find the reset button on the device in our online catalogue.

3.2 Firmware update

We recommend updating the firmware of our access point. The device's latest firmware version can be found on our Weidmüller Online Catalogue at:

<https://catalog.weidmueller.com/>

4 Usage of an Access Point

Access points are used for making your wired network, for example a machine's local area network (LAN), accessible wirelessly. In fact, the access point is connected to your machine's network via an Ethernet cable, projecting the wired signal into a wireless signal for a computer to connect to. This is important when our computer/laptop is not stationary or the network we want to connect to, say from an automated guide vehicle (AGV), is moving and therefore a permanent access via cable is not possible.

4.1 Setting a new IP address for the Access Point

HINT: The IP-address range *192.168.1.1 - 192.168.1.254* is most common for consumer routers (e.g., DSL or TV cables internet access). If your local internet connection uses this IP range, disconnect your computer from the internet before accessing the WiFi Access Point.

1. To connect to the access point's web interface, type in the default IP "*192.168.1.110*" into the browser's URL field and log in with the default credentials mentioned in Table 1.



Figure 1: Login interface

Setting up a Weidmueller WiFi access point

2. To change the IP address, navigate to “*General Setup*” and then “*Network Settings*”. You should now see the following screen.

Weidmüller Wireless Device Configuration

Network Settings

IP address assignment: Static

IP address: 192.168.1.110

Subnet mask: 255.255.255.0

Gateway:

Primary DNS server:

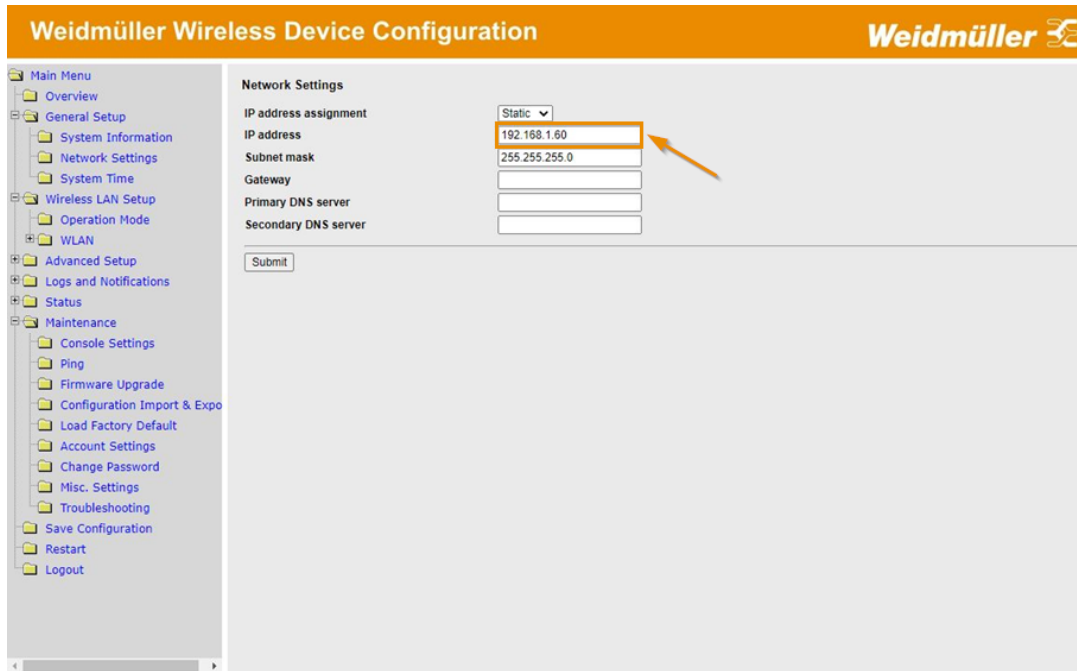
Secondary DNS server:

Submit

Figure 2: Network Settings

Setting up a Weidmueller WiFi access point

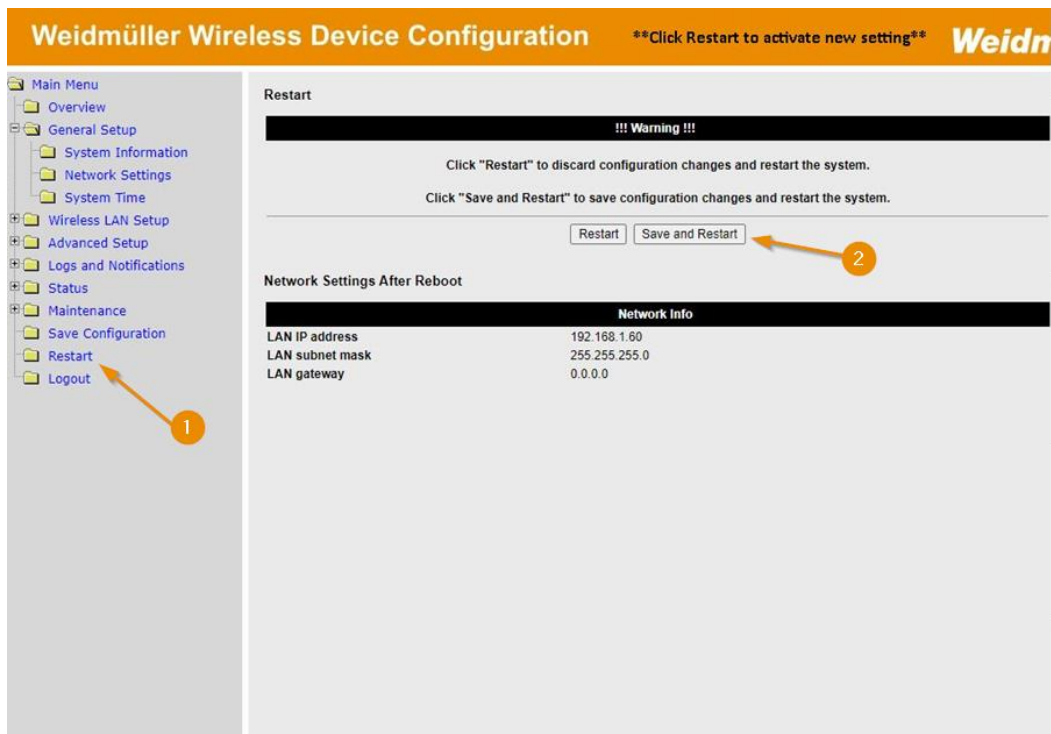
3. Type the following IP address: “192.168.1.60” into the “IP address assignment” field as seen below. Afterwards, submit the changes.



The screenshot shows the 'Weidmüller Wireless Device Configuration' interface. On the left is a 'Main Menu' tree with categories like Overview, General Setup, Wireless LAN Setup, Advanced Setup, Logs and Notifications, Status, and Maintenance. The 'Network Settings' page is active. It features a 'Static' dropdown for 'IP address assignment'. Below it are input fields for 'IP address' (containing '192.168.1.60'), 'Subnet mask' (containing '255.255.255.0'), 'Gateway', 'Primary DNS server', and 'Secondary DNS server'. A 'Submit' button is at the bottom. An orange arrow points to the 'IP address' field.

Figure 3: Changing the IP address

4. We are now asked to restart our device to activate our settings. To do that, navigate to “Restart” in the menu tree and select “Save and Restart”.



The screenshot shows the 'Restart' page in the 'Weidmüller Wireless Device Configuration' interface. A warning message states: 'Click "Restart" to discard configuration changes and restart the system. Click "Save and Restart" to save configuration changes and restart the system.' There are two buttons: 'Restart' and 'Save and Restart'. An orange arrow labeled '2' points to the 'Save and Restart' button. In the left menu tree, an orange arrow labeled '1' points to the 'Restart' option under the 'Maintenance' category. Below the buttons, a section titled 'Network Settings After Reboot' contains a table with network information.

Network Info	
LAN IP address	192.168.1.60
LAN subnet mask	255.255.255.0
LAN gateway	0.0.0.0

Figure 4: Save and Restart

5 Configuring a new service set ID (SSID) and password for the WiFi access

In this chapter, we are going to configure the SSID and a password for the WLAN. The service set ID (SSID) is your WiFi's public name. The WiFi access is configurable by either using the pre-existing SSID configuration *"Weidmueller"* or by configuring a new SSID. Furthermore, it is also very important to configure basic security settings like a password for the WLAN to protect it against unauthorized connections and access.

5.1 Configuring SSID

1. To configure an SSID, we have two options available: either using the pre-existing SSID settings from Weidmueller or create a new one.
The SSID settings can be found in the menu tree by selecting *"Wireless LAN Setup"* then *"WLAN"* and further select *"Basic WLAN Setup"*.

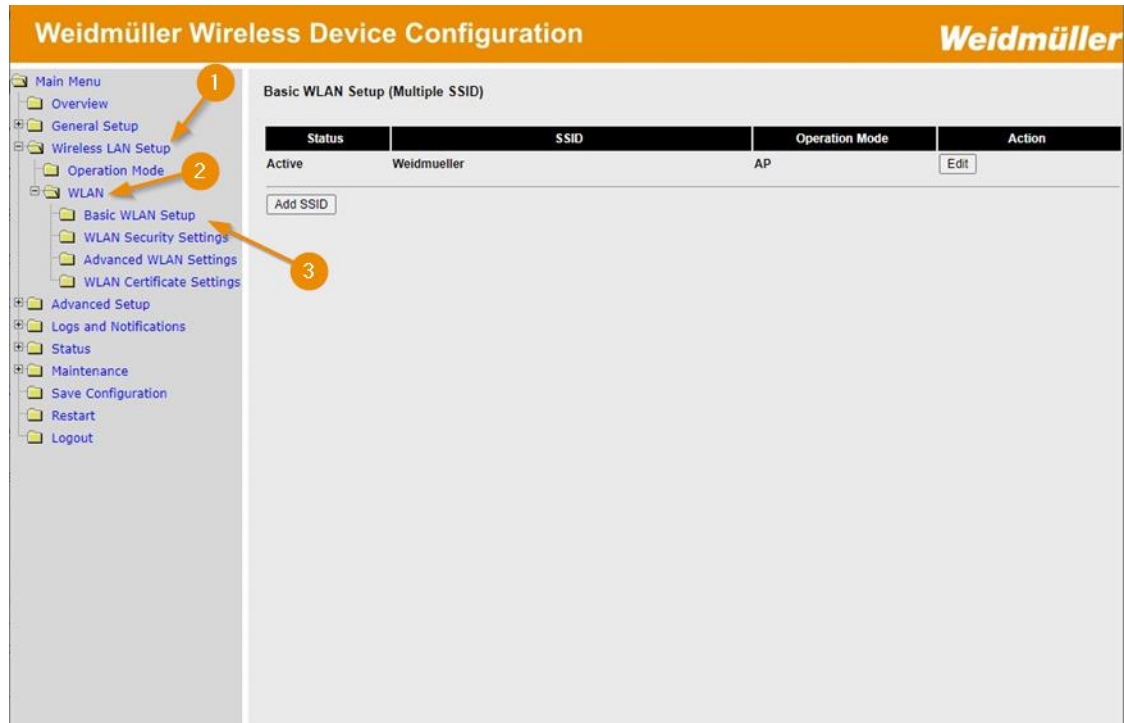


Figure 5: SSID settings

The screenshot above shows the currently active SSID from the access point, which comes with the default access point settings. As mentioned before, we can already connect to the access point with this pre-configured default SSID.

Setting up a Weidmueller WiFi access point

2. If we wish to add a different SSID, we can do this by clicking on the button “Add SSID” and then typing in a new name and saving the changes. For this test our SSID will be named test, but you can name it as you wish.

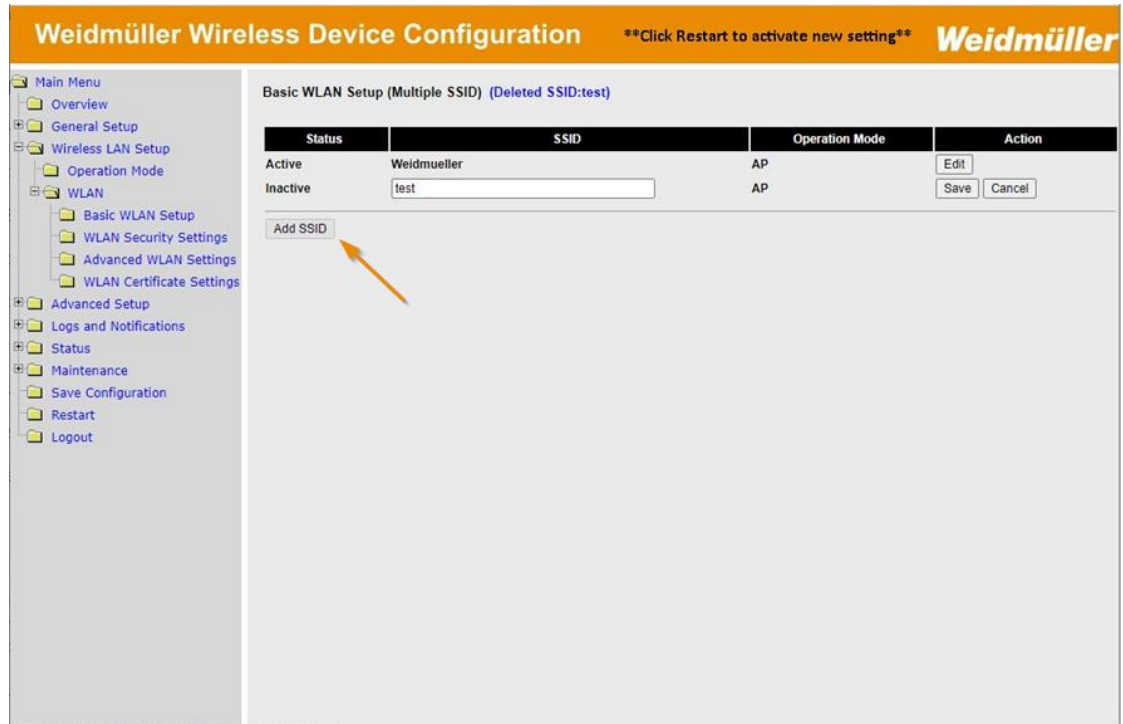


Figure 6: naming new SSID

The “*Edit*” option has more settings available, where we can change our SSID’s name, change the channel width or disable SSID broadcast. Changing the channel width can be helpful when experiencing low network speeds. A bigger channel width has more throughput but has a higher probability of interfering with different frequencies meaning it is less effective. Also, if we want to have an extra layer of security, we may disable “*SSID Broadcast*”. Deactivating it means, that we will have to type in our SSID manually when connecting to the network, as it will not be publicly visible if you scan for available WIFI networks.

5.2 Creating a password

1. For the sake of security, we should configure a password for our access point's WiFi. By doing so, we can prevent unauthorized access to the access point and thus the network, making it more secure to operate in the production network.

Please note that the password should not only contain trivial combinations like 1234 and should consist of at least 20 characters to ensure a good fundamental security of your network.

To find the security settings, we must navigate in the menu tree to *"Wireless LAN Setup"* then click *"WLAN"* and afterwards select the option *"WLAN Security Settings"*.

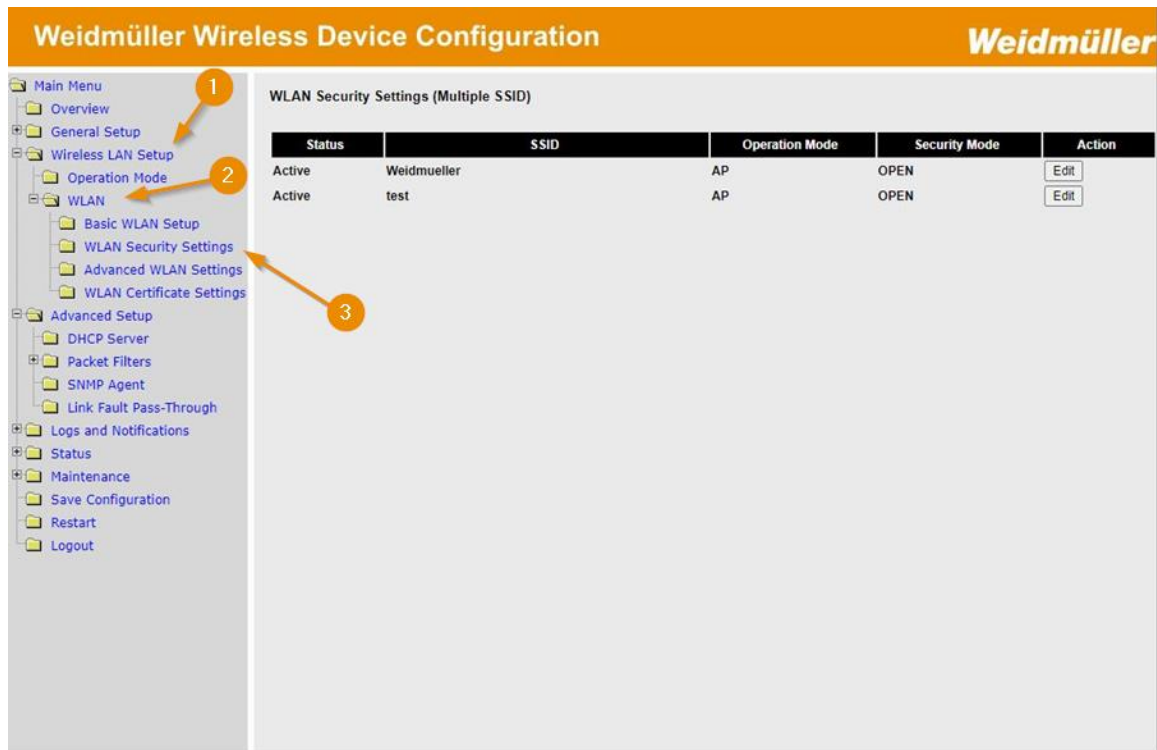


Figure 7: WLAN Security settings

- Now, click on “*Edit*” on the SSID (note: if you plan on using multiple SSIDs, make sure to edit every single one of them with the steps below, as a default SSID setting does not have any security measurements such as a password). First, you can choose between three different security modes:

- **Wired Equivalent Privacy (WEP):** an outdated standard for encryption used for old devices, not recommended.
- **WiFi protected access (WPA):** a more secure standard especially for older devices that are not compatible with WPA2’s AES encryption, recommended when using WPA2 incompatible devices
- **WiFi protected access 2 (WPA2):** WPA2 is based on WPA, uses AES encryption and is the standard secure encryption to use for a password as of now, WPA2 is recommended as a security mode (note: WPA3 more secure, but not yet standard)

The screenshot displays the 'Weidmüller Wireless Device Configuration' web interface. On the left is a navigation menu with options like Main Menu, Overview, General Setup, Wireless LAN Setup, and WLAN. The 'WLAN Security Settings' page is active, showing fields for SSID (set to 'test'), Security mode (WPA2), WPA type (Personal), Encryption method (AES), EAPOL version (1), Passphrase (empty), and Key renewal (3600 seconds). A 'Submit' button is at the bottom.

Figure 8: WLAN security mode

- After selecting a preferred security mode (we use WPA2), you can type in your passphrase (make sure to use a secure password).
We may now “*Save and Restart*” the device again.

6 Results

After implementing the steps, we can now use the access point to connect to a machine's or vehicle's wired network wirelessly. Furthermore, we are now able to change the IP, set up an SSID and define a password for the access point.