

## Application Note

# IP horn loudspeaker & IP amplifier module - Getting started – v1.2

This Application Note describes how to update the IP horn loudspeakers or the IP amplifier module and how to setup and configure some basic use cases.

### Related Products:

LHN-UC15L-SIP | LHN-UC15W-SIP | AMN-P15-SIP

### Severity:

- Immediate action required
- Action strongly recommended
- Informative

## Table of Contents

- 1. Introduction**
- 2. Unpacking and Powering**
- 3. Getting Started**
  - 3.1. Firmware Update
  - 3.2. IP address detection and hostname detection
  - 3.3. Logon with the web browser
- 4. Use Cases**
  - 4.1. Direct Bosch camera integration for automatic message playing
  - 4.2. SIP
    - 4.2.1. Peer-to-Peer connection
    - 4.2.2. SIP server connection
  - 4.3. Trigger message via noise (horn loudspeaker only)
- 5. Test/Rest button**
- 6. Document history**
- 7. Notice of liability**

## 1. Introduction

This Application Note describes how to get the IP horn loudspeakers and the IP amplifier module up and running. On the example of the wide angle IP horn loudspeaker, it will be described how to update the firmware and make some basic configuration. The long throw horn loudspeaker and the amplifier module can be configured in almost the same way.

### Products:

LHN-UC15L-SIP	=	SIP based long throw IP horn loudspeaker
LHN-UC15W-SIP	=	SIP based wide angle IP horn loudspeaker
AMN-P15-SIP	=	SIP based IP amplifier module

### **Notice!**

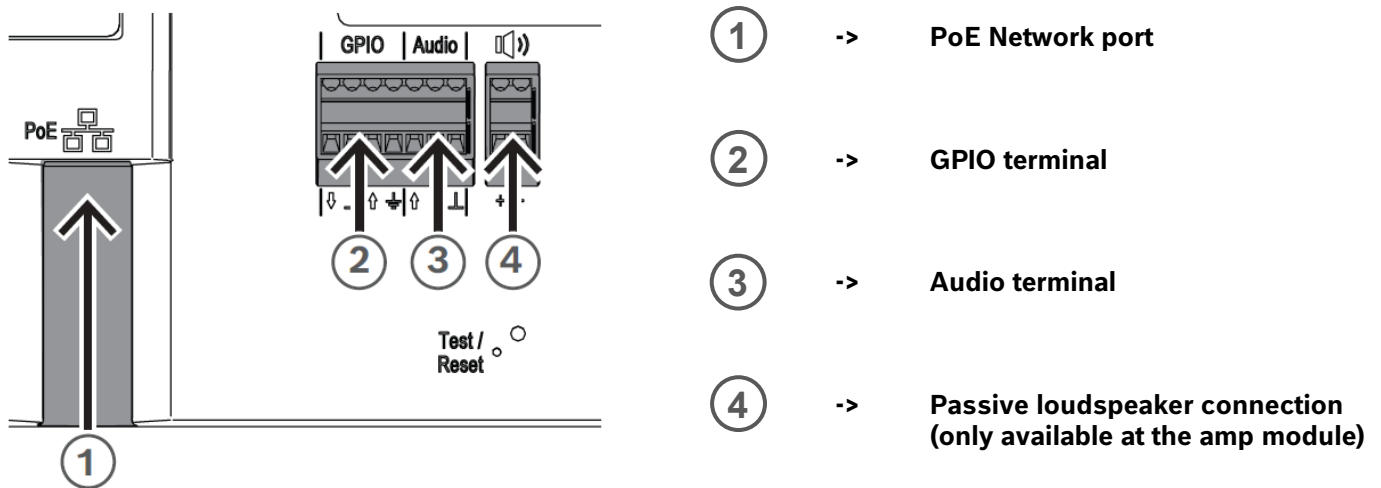
The screenshots of the IP horn WEB GUI were made with the firmware v2.1 (2.1.869).

## 2. Unpacking and Powering

To access the cable connections, do the following:

1. Using a T20 Torx screwdriver, remove the four cover screws.
2. Lift the cover from the chassis with care.

The back of the loudspeaker/amp module is shown as reference view bellow.



### Connecting to network

The IP horn loudspeaker and the IP amplifier module support PoE/PoE+ power supply mode. You need one Ethernet cable to connect to a PoE switch (e.g. PRA-ES8P2S) or an injector for a convenient installation. For the most reliable operation, always use shielded CAT-5e or higher class cables.

The network port LED turns on a few seconds after the network cable is connected, indicating that PoE/PoE+ power has been successfully applied.

There are two lights on the Ethernet jack:

- A solid green LED (right) indicates the port is operating at 1000 Mbps (1 Gbps). It flickers to indicate network activity.
- An orange/yellow LED (left) indicates a network link of 100 Mbps. It flickers to indicate network activity.

### Notice!

The cable gland has a small diameter that makes it impossible to feed a network cable with a connector crimped through the gland. Check the manual for detailed information.

### 3. Getting Started

The configuration of the loudspeaker and the module is done via WEB based GUI.

Before starting configuration and operation of the loudspeaker and the module, it is advised to do the following:

1. Download the latest firmware and update the IP horn/amp
2. IP address detection and hostname detection
3. Logon with the web browser

#### 3.1. Firmware Update

You can get the firmware from the product page at [www.boschsecurity.com](http://www.boschsecurity.com). It is recommended to use the latest firmware version.

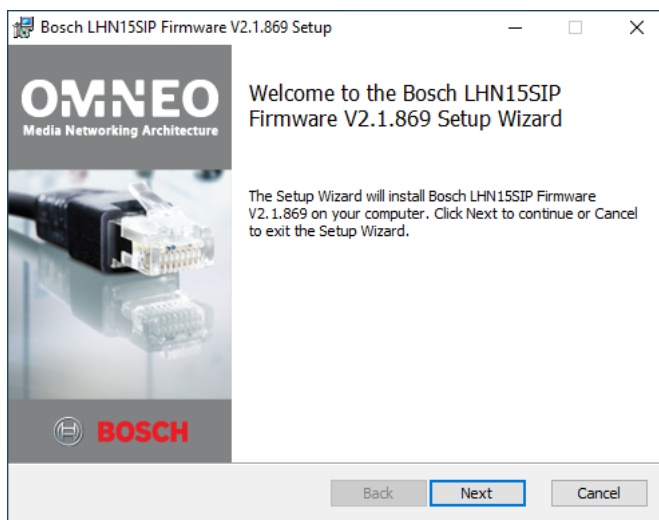
You perform firmware updates via the Firmware Upload Tool (FWUT) version 9.10 or above. You can the required Firmware Upload Tool (FWUT) from the product page on [www.boschsecurity.com](http://www.boschsecurity.com).

**To update the firmware of the device, do the following:**

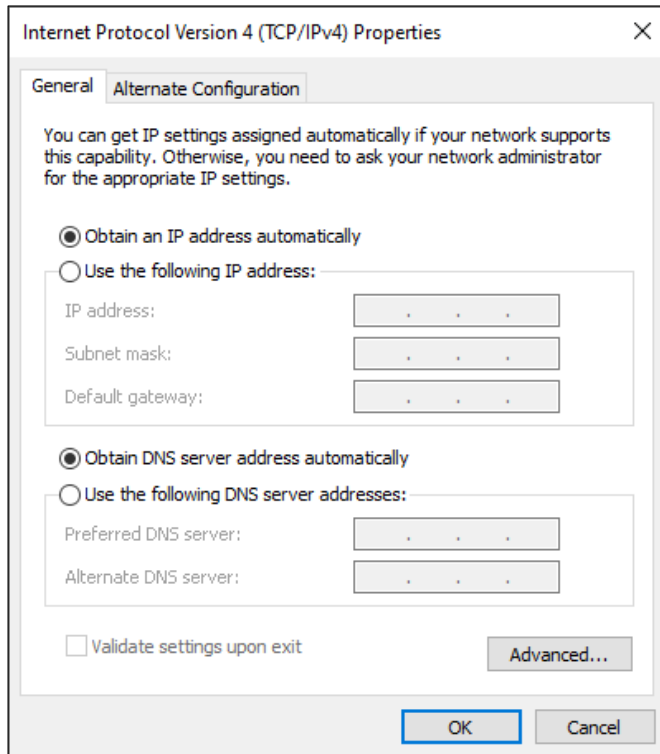
1. Click on the “Firmware.msi” file to start the Firmware Setup Wizard. There is one installation file for the two IP horn loudspeakers and one installation file for the IP amplifier module.



It will copy the firmware in the folder C:\ProgramData\Bosch\OMNEO\Firmware. Notice, that the FWUT needs to be installed upfront.

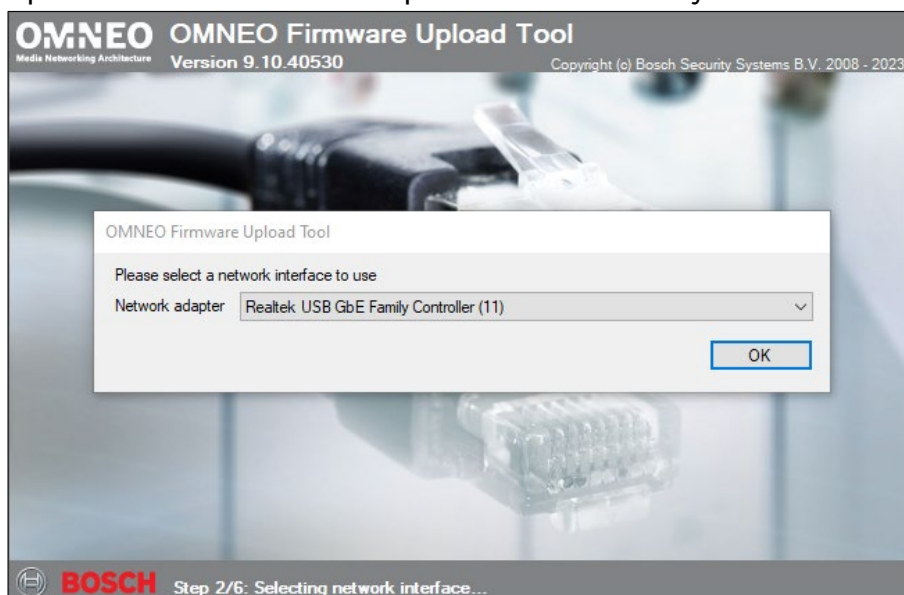


- Set your PC's network adapter to DHCP to automatically obtain an IP address.

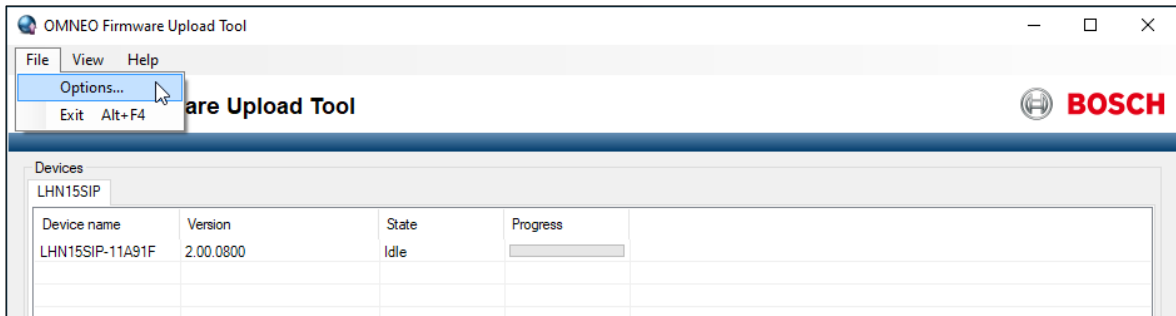
**Notice!**

By default, the IP horn/amp is set to DHCP and thus you will get an IP address in the same range.

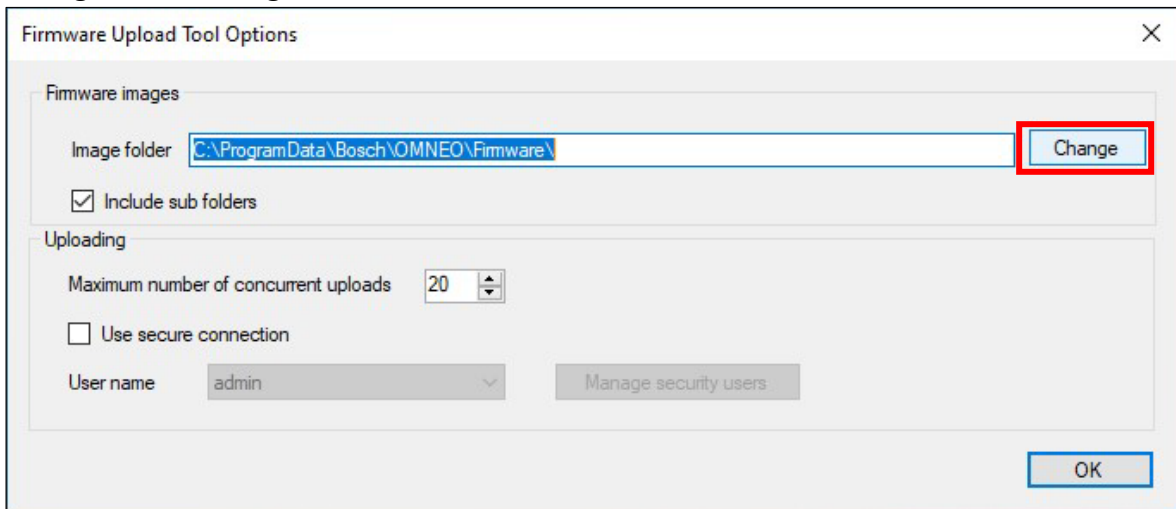
- Connect your PC to the same network/switch as the IP horn/amp. Attention, the IP horn/amp and the PC must be in the same subnet.
- Open the OMNEO Firmware Upload Tool and select your network adapter.



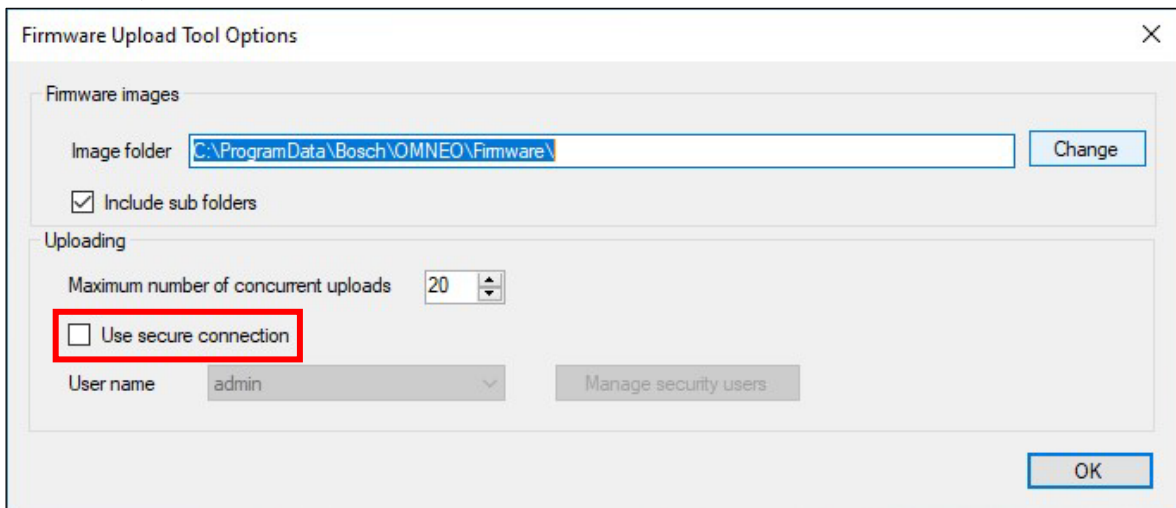
- 5. From the File menu, select Options.



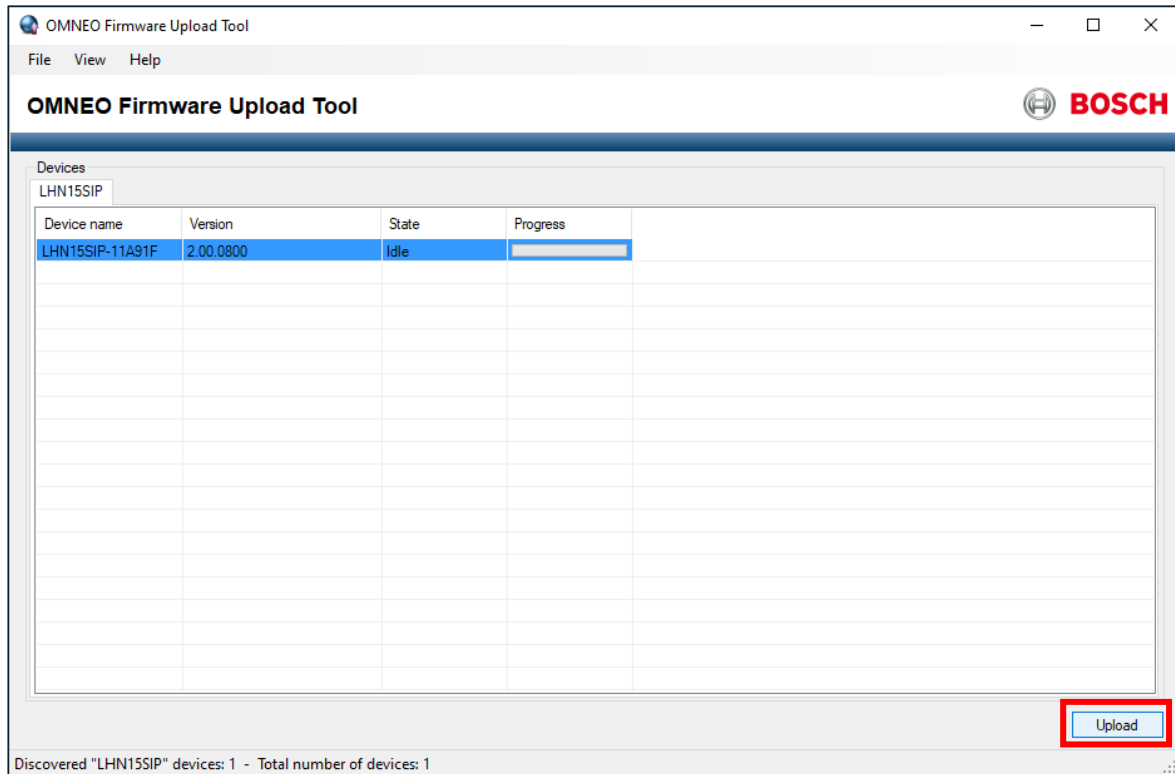
- 6. Check if the Image folder is “C:\ProgramData\Bosch\OMNEO\Firmware”. If not, click the Change button, navigate to the folder where the firmware is and click OK.



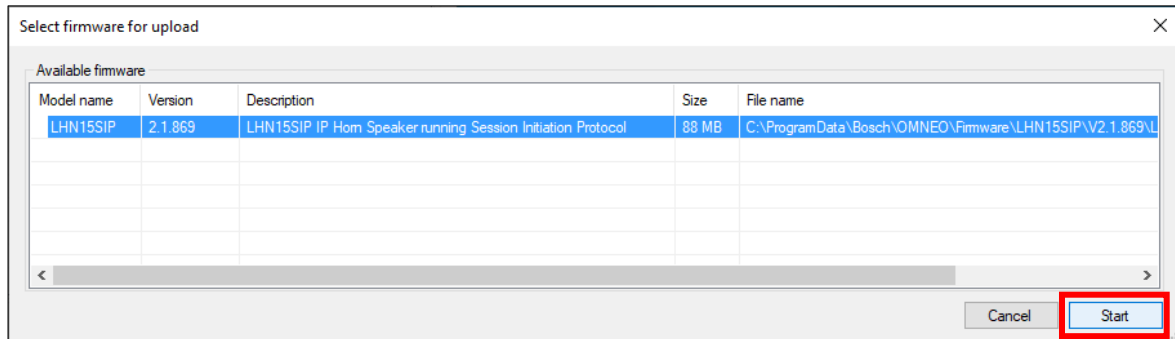
- 7. Make sure, that “Use secure connection” is unchecked and click OK.



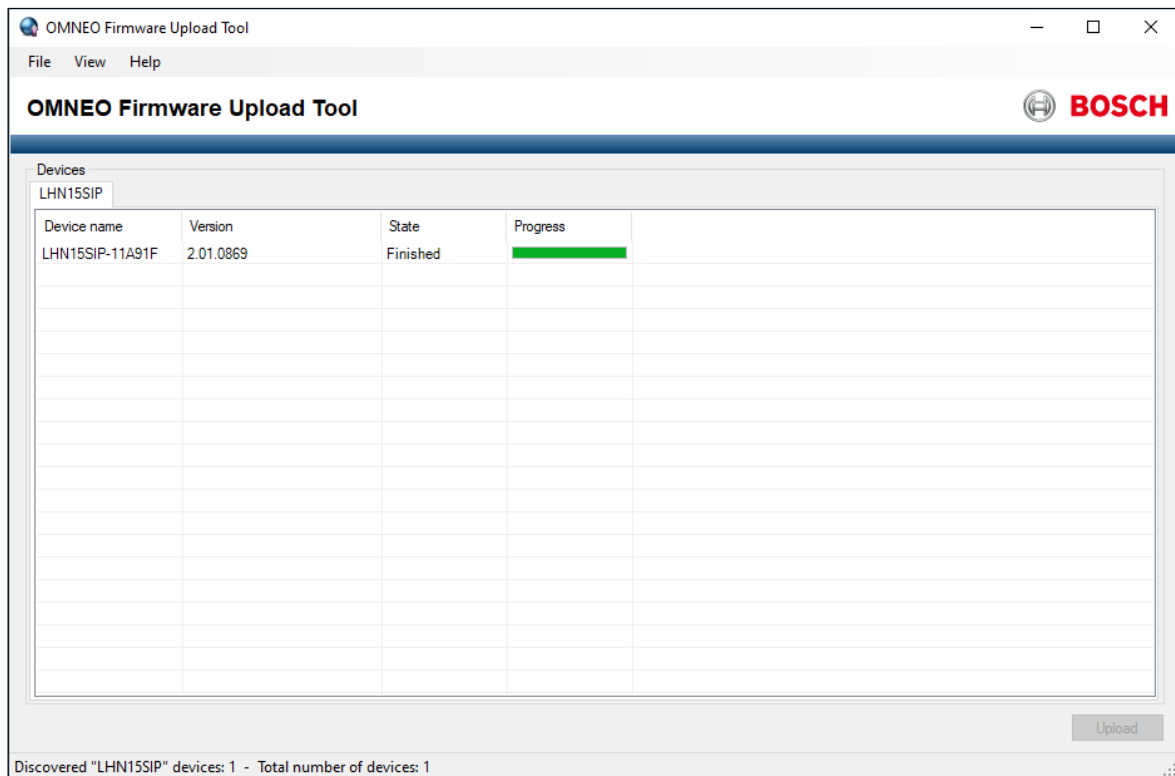
8. Select the device to update and click the Upload button.



9. From the list of firmware, select a firmware and click the Start button.



10. When the upload is completed, the State tab displays “Finished” and your device is ready to be used.



### Notice!

Do not disconnect the device while the update is running. If the update fails, disconnect the device and connect it again. Repeat the update process.

### Firmware Update troubleshooting:

- The IP horn/amp does not show up in the Firmware Upload Tool:
  - Check if you have selected the correct network adapter. This is only asked during startup of the Firmware Upload tool.
  - Make sure, that “Use secure connection” is unchecked.
  - Your PC needs to have an IP address in the same range as the IP horn/amp. Set your PC to DHCP and reset the IP settings of the IP horn/amp by pressing and holding the physical reset button for 6 - 10 seconds: the IP address of the IP horn/amp will reset to factory default (DHCP). For more details, please go to chapter 5.
  - Deactivate all other network adapters (e.g. WIFI).
  - Check firewall settings (FWUT needs to have the right to communicate through the firewall: Windows -> Allow an app through firewall).
- The update fails:
  - Disconnect the device and connect it again. Repeat the update process.
  - If the update fails, it may show 1.0 as Version. If this happens the IP horn/amp is in a kind of failsafe mode and you can restart the firmware update.
  - Don't use WIFI. Always use an Ethernet cable connection for firmware update.
  - The “Downloads” folder should not be used. Use a folder where you have read and write access rights.
- The IP horn/amp is shown in the FWUT, but greyed out:
  - Use Firmware Upload Tool V9.1 or later.
- The firmware is not visible in the FWUT:
  - First start the Firmware Setup Wizard (or copy the firmware into a folder) and then start the FWUT and select the corresponding folder.

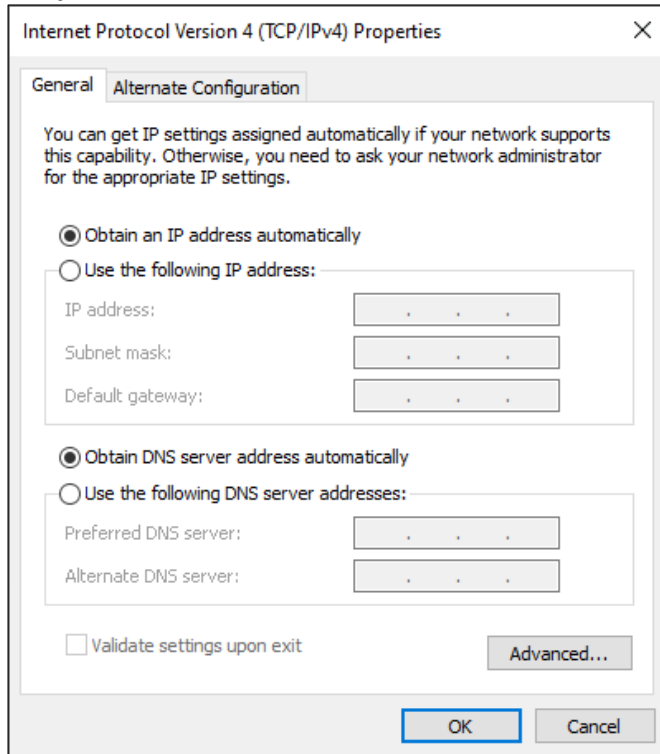


## 3.2. IP address detection and hostname detection

### IP address detection with the Firmware Upload Tool

The OMNEO Firmware Upload Tool can be used to discover the IP address of the IP horn/amp.

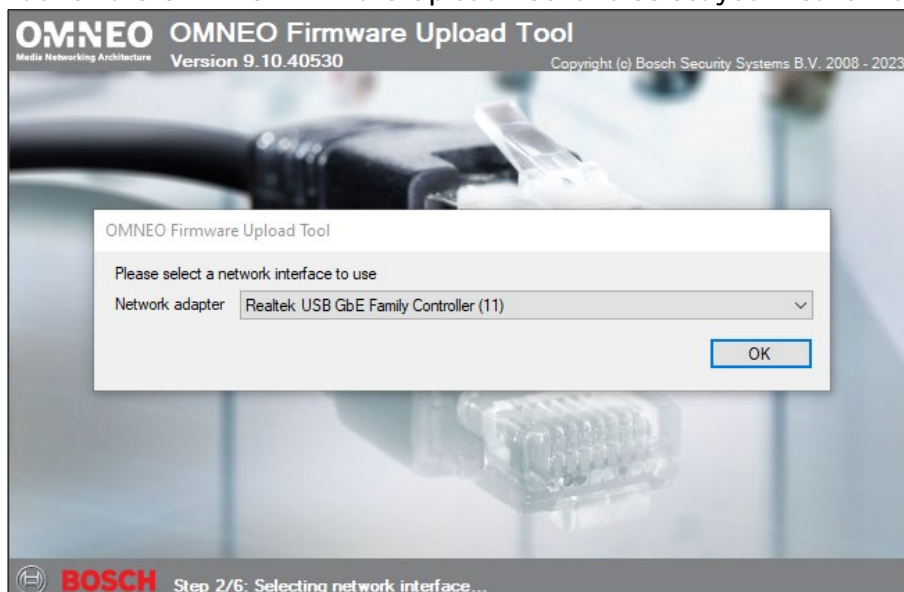
1. Set your PC's network card to DHCP to automatically obtain an IP address.



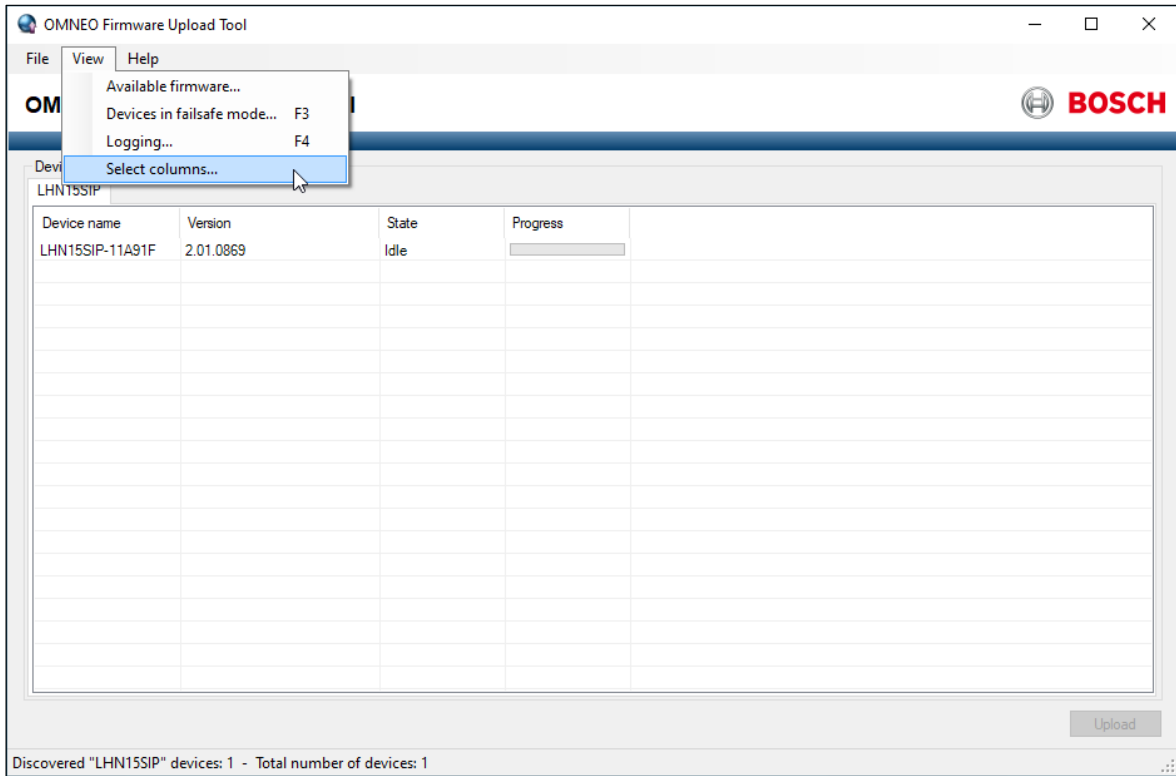
#### Notice!

By default, the IP horn/amp is set to DHCP and thus you will get an IP address in the same range.

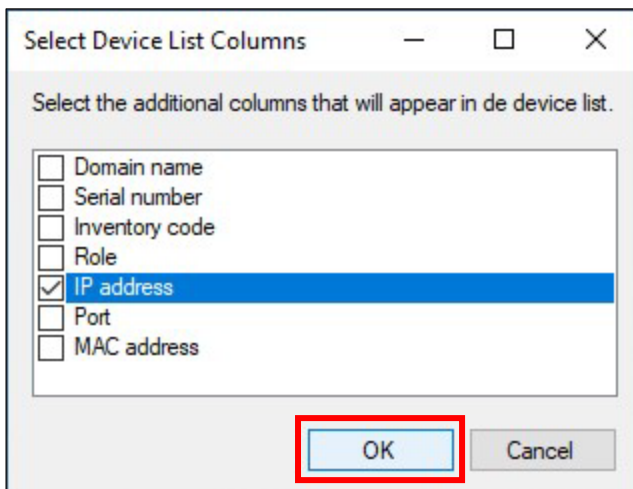
2. Connect your configuration PC to the same network/switch as the IP horn/amp. Attention, the IP horn/amp and the PC must be in the same subnet.
3. Launch the OMNEO Firmware Upload Tool and select your network adapter.



- Click in the View menu on Select columns.



- Select IP address and click OK.





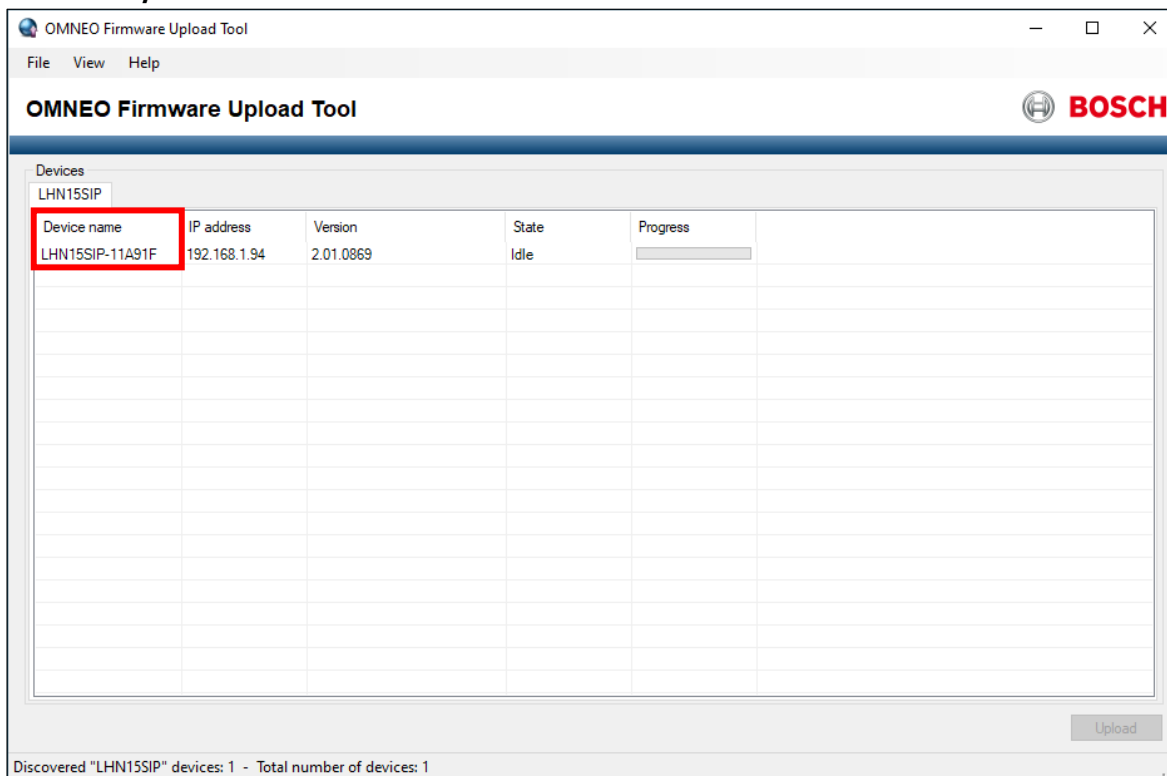
### Hostname detection

The hostname is a combination of the product type and the last 6 digits of the MAC address. The MAC address can be found on the device label. The hostname is displayed in the FWUT or can be assembled as shown below.

- General: https://HOSTNAME.local
- Horn loudspeaker: https://lhn15sip-11a91f.local
- Amplifier module: https://amn15sip-11a97a.local

https	Secure and encrypted connection
lhn15/amn15	Product type
6 digits	Last 6 digits of the MAC address
.local	Domain name (local)

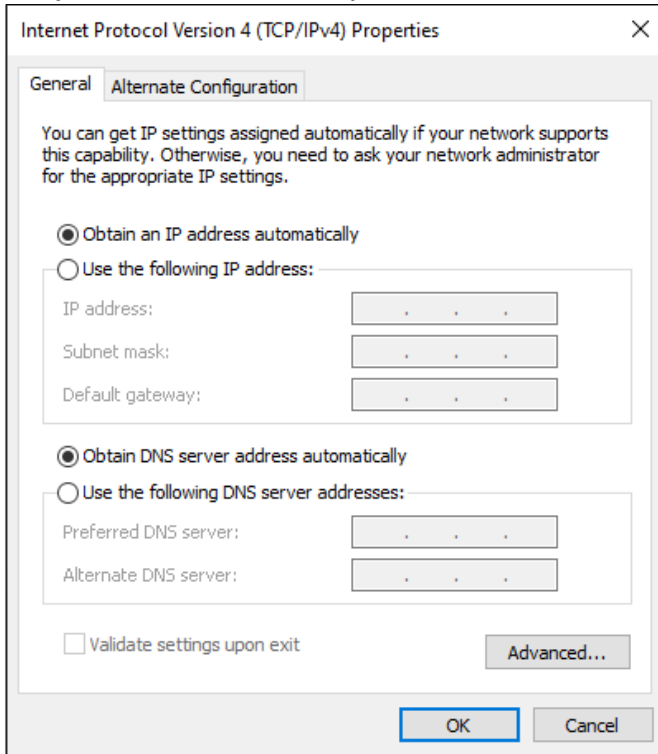
### Hostname/Device name in the FWUT



## IP address detection with the Bosch Configuration Manager

The Bosch Configuration Manager provides various functions for configuration of video cameras including a Network Scan. The Network Scan automatically detects all compatible devices present in a network, including the IP horn/amp. You can download the Bosch Configuration Manager from <https://downloadstore.boschsecurity.com>.

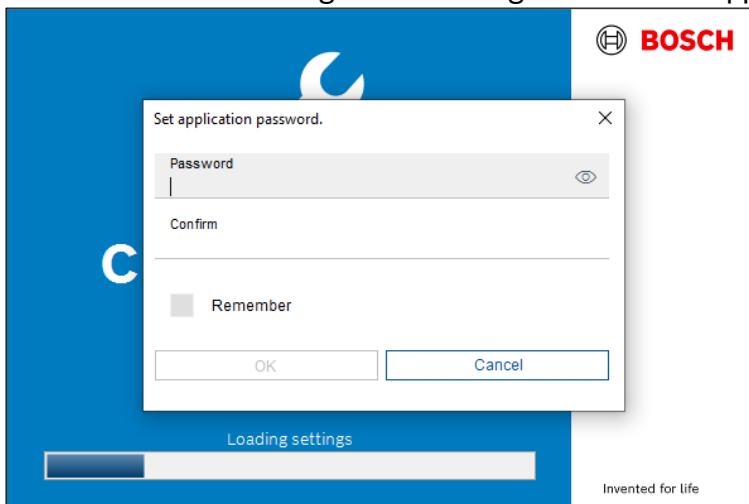
1. Set your PC's network adapter to DHCP to automatically obtain an IP address.




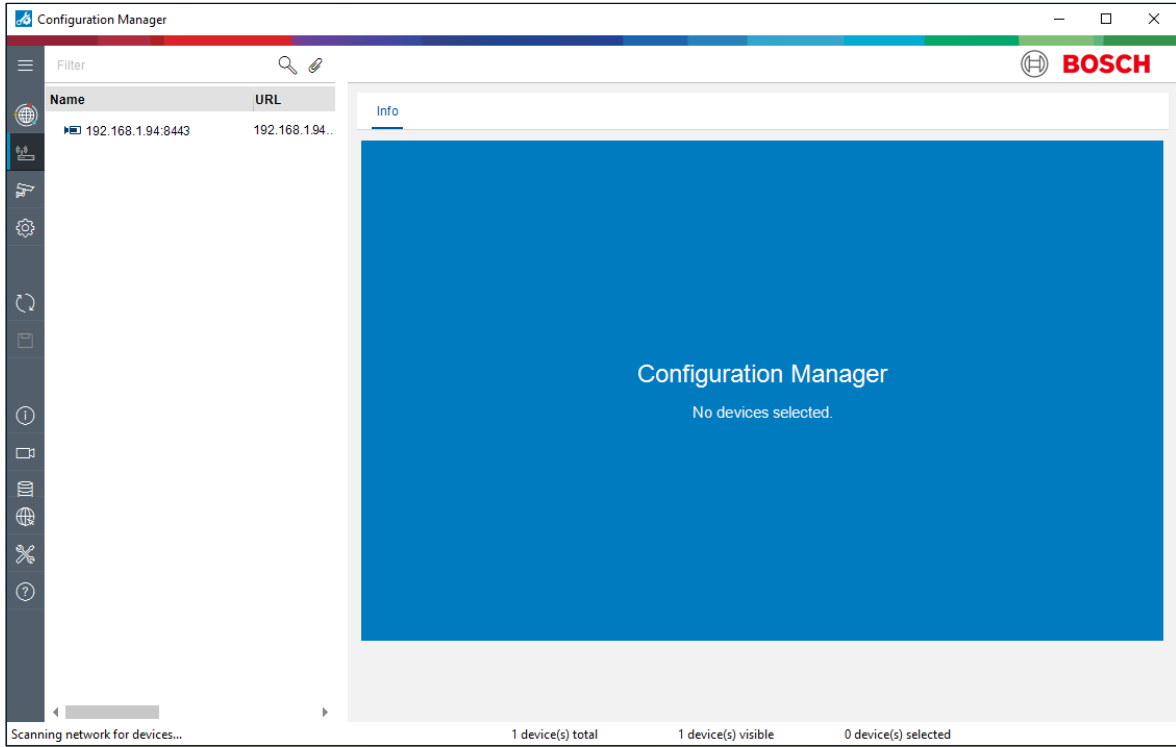
### Notice!

By default, the IP horn/amp is set to DHCP and thus you will get an IP address in the same range.

2. Connect your configuration PC to the same network/switch as the IP horn/amp. Attention, the IP horn/amp and the PC must be in the same subnet.
3. Launch the Bosch Configuration Manager and set an application password if not yet done.

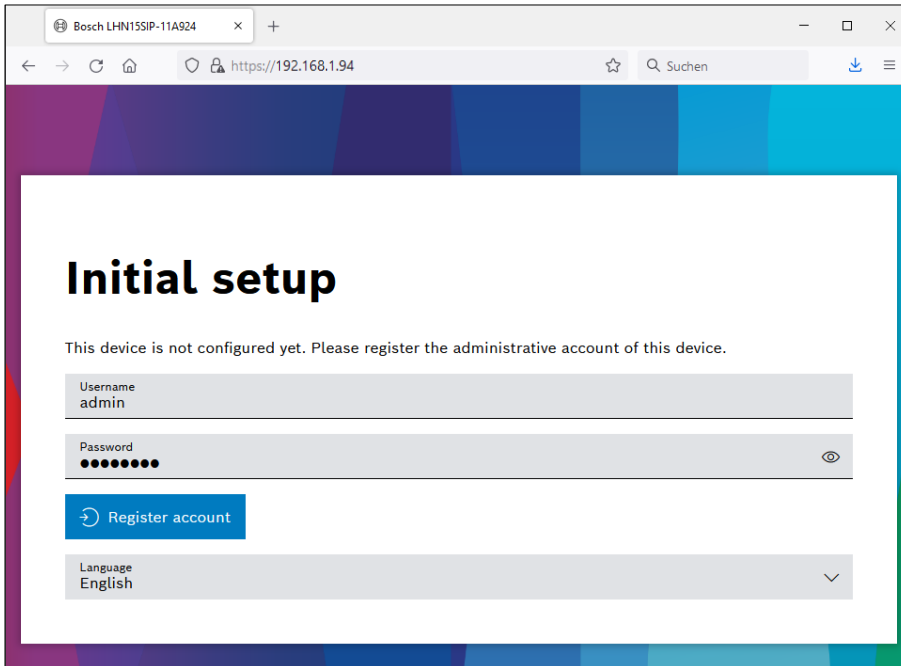


4. You can quickly discover the IP address of your device using the Network Scan  .



### 3.3. Logon with the web browser

1. Open a browser and enter the IP address (<https://IPaddress>) or the host name (<https://HOSTNAME.local>) of the device. Accept the risk for the self-signed certificate. There is no default password. This requires you to register the administrative account for the device.
  - Enter a unique username. The username must be 4 - 64 characters long.
  - Enter a unique strong password for the user. The password must be 8 - 64 characters long.
  - Choose the language of the interface. Later you can change your preference in *Generic settings*.
  - Register the administrative account.



**Initial setup**

This device is not configured yet. Please register the administrative account of this device.

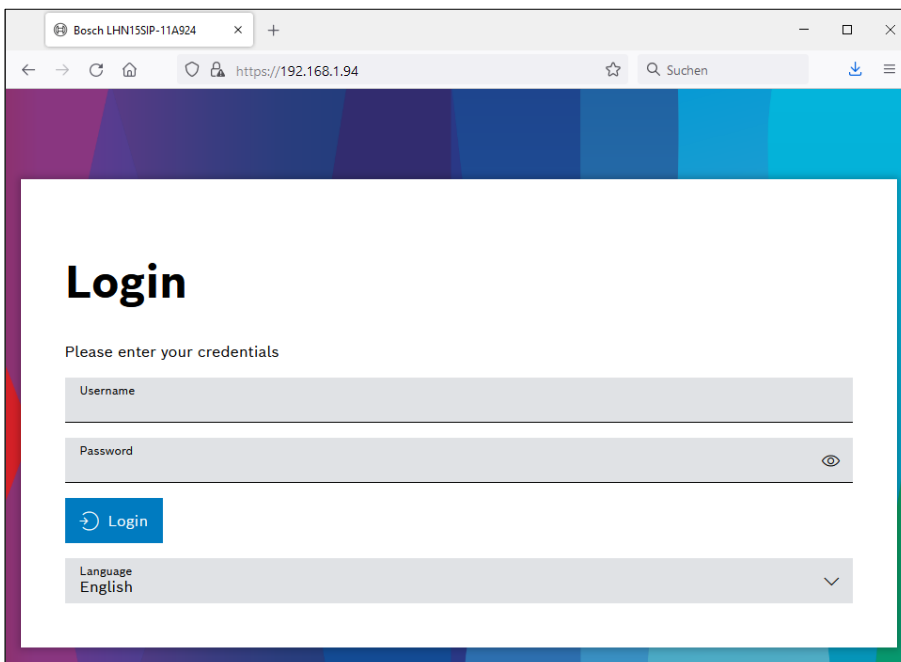
Username  
admin

Password  
●●●●●●●●

Register account

Language  
English

2. The administrative account is now registered and you can login with your Username and Password.



**Login**

Please enter your credentials

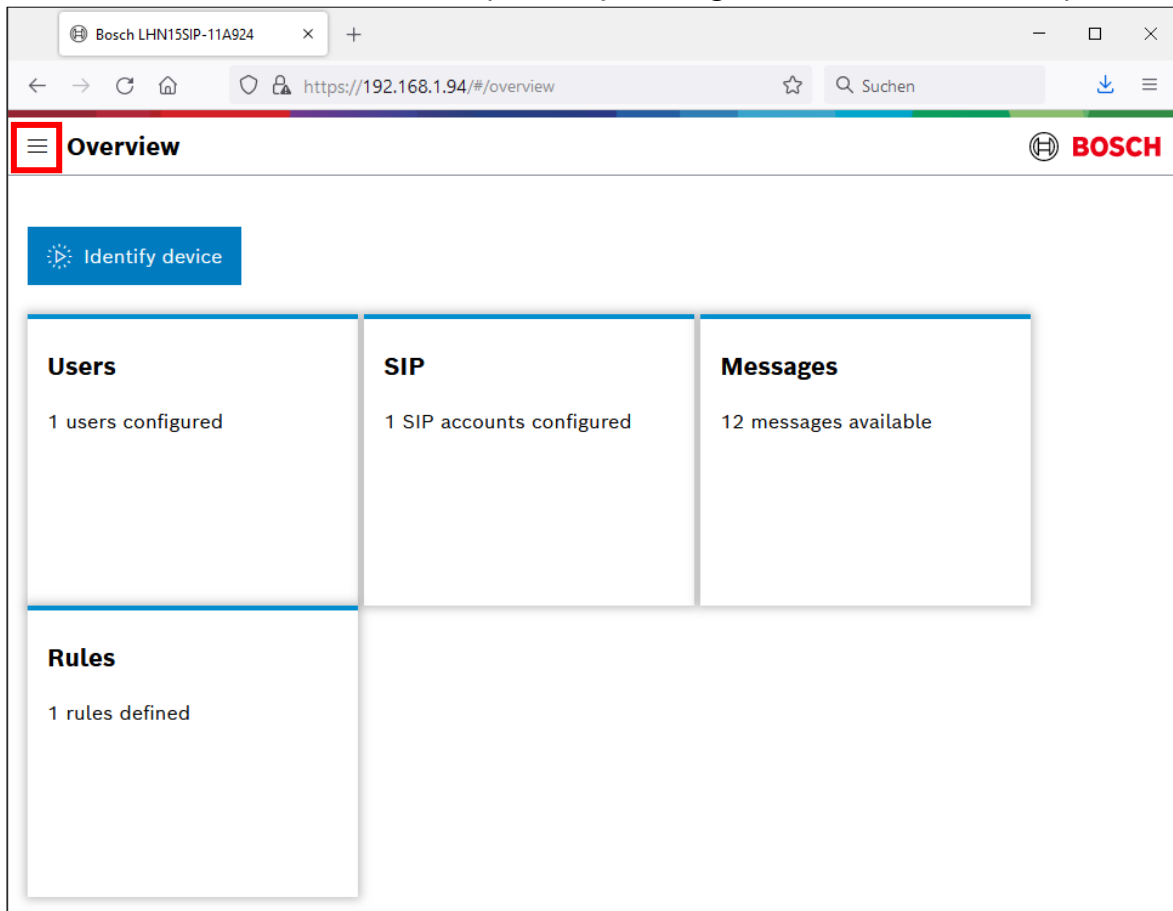
Username

Password  
●●●●●●●●

Login

Language  
English

3. Now you are on the GUI landing page *Overview*. Use the *Overview* menu to view the main functions of the web interface and to navigate to these functions in the system using the informative graphical tiles. Each tile displays configuration data and real-time status information of the device. The menu can be opened by clicking on the menu icon in top left corner.



### Supported browsers

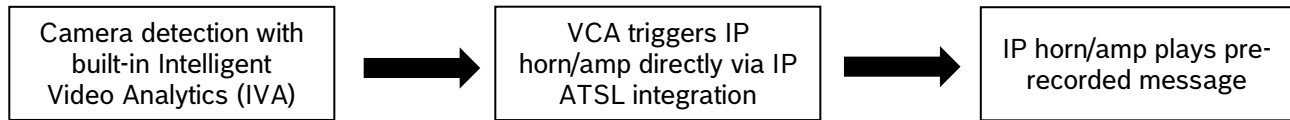
- Chrome
- Safari
- Firefox
- Microsoft Edge



## 4. Use Cases

### 4.1. Direct Bosch camera integration for automatic message playing

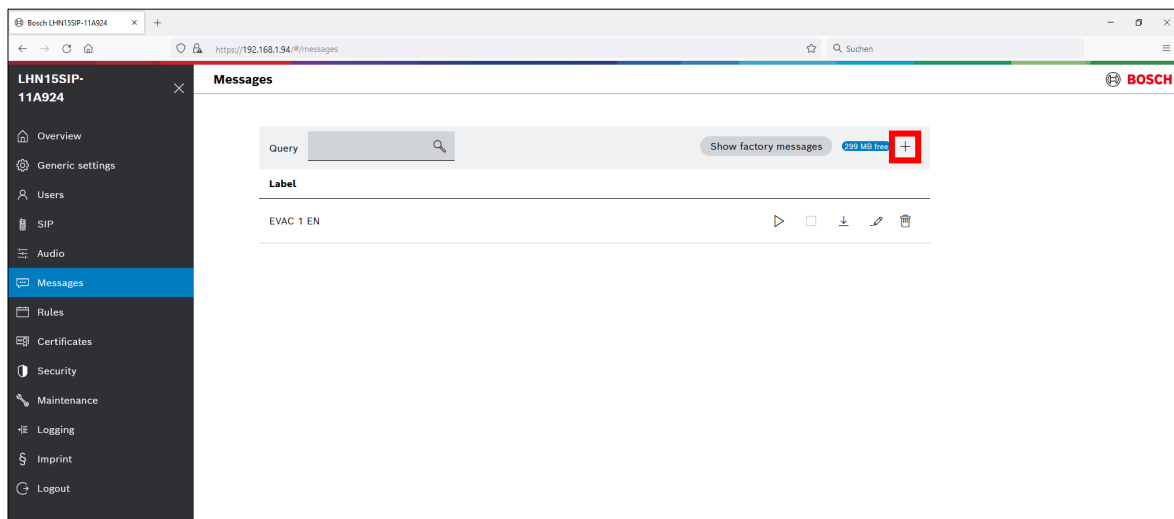
You may want to link a Bosch camera to the IP horn/amp so that it plays a message when an action occurs. To do this you need to create a special API profile and a rule at the IP horn/amp. Then you need to create a script in the camera using ATSL (Alarm Task Scripting Language) and configure the areas that trigger the alarm at the camera.



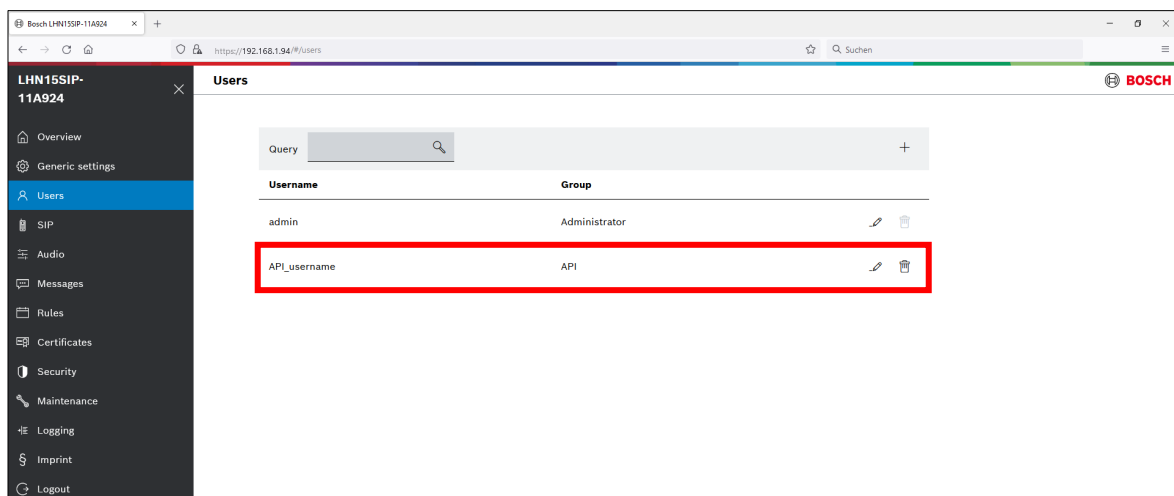
To link a Bosch camera with the IP horn/amp, the following steps are necessary:

#### At the IP horn/amp:

1. You can upload your own messages by using the + or you can use a factory message. Supported file formats are listed in the data sheet.

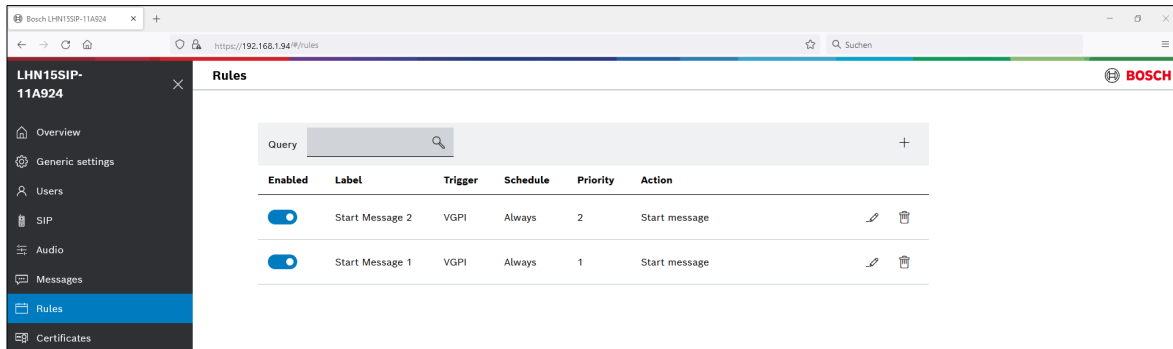


2. Create an API account dedicated for the camera.



3. Create a Rule that leads VGPIs (Virtual General Purpose Inputs) to start the action “activation of messages” and select the message you would like to play with the settings of repeat, abort/stop behavior.

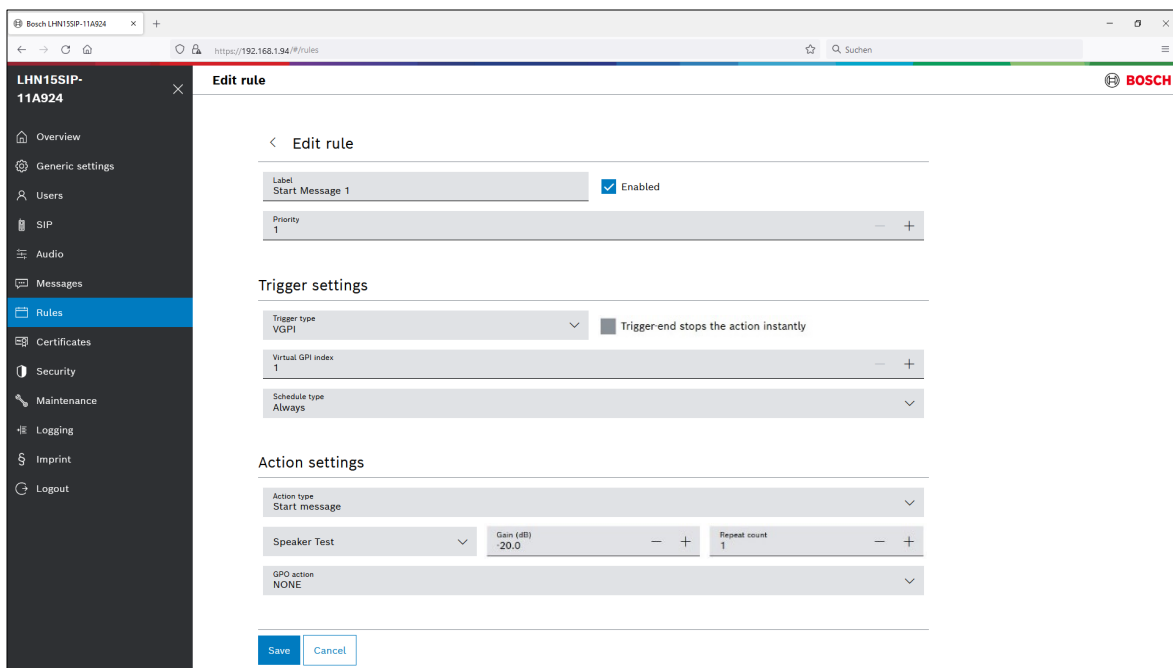
### Overview



### Details

### rule

1



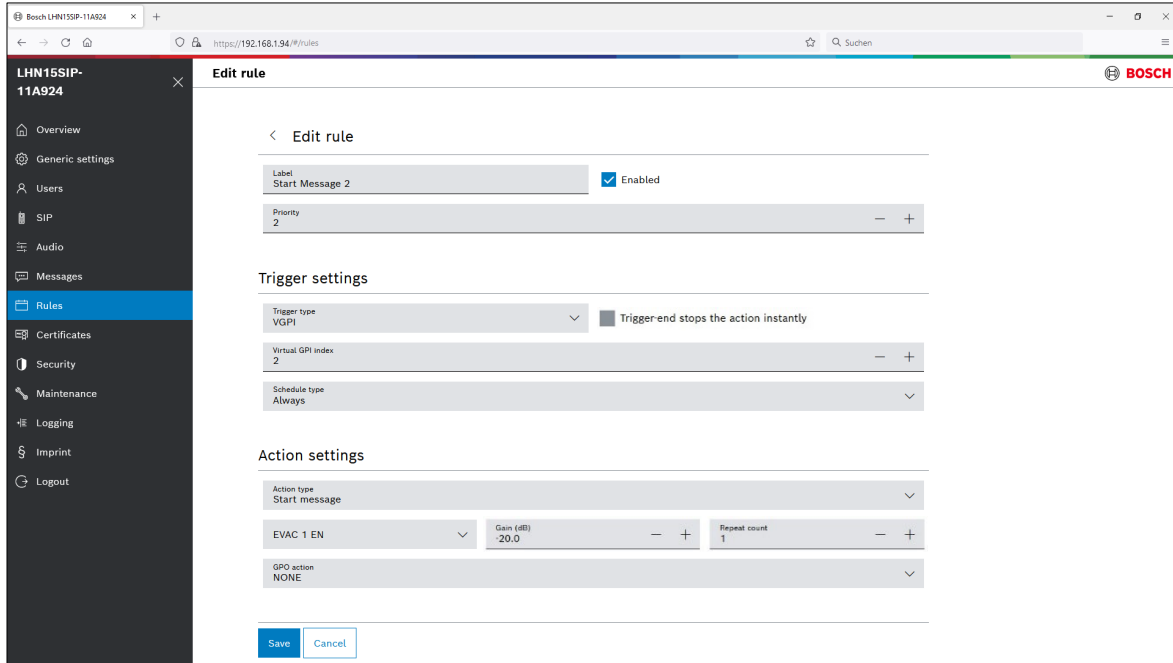
### Notice!

It is a good practice to make sure that the “Trigger-end stops the action instantly” check box is unchecked in the rule settings. This ensures that the message plays until the end of the loop.

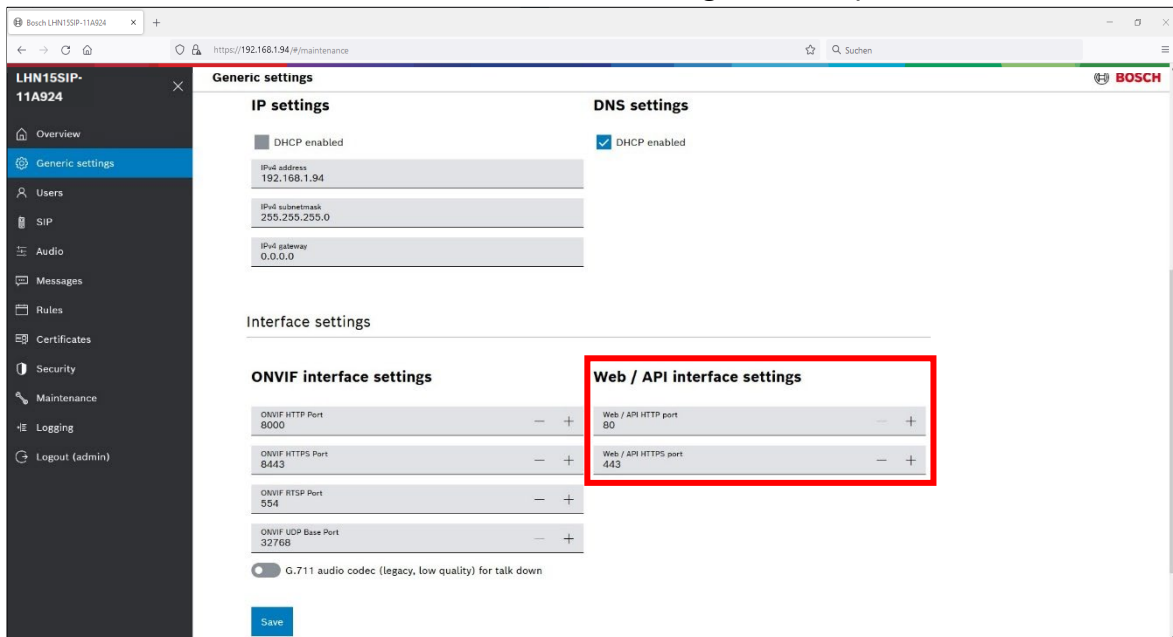
Details

rule

2

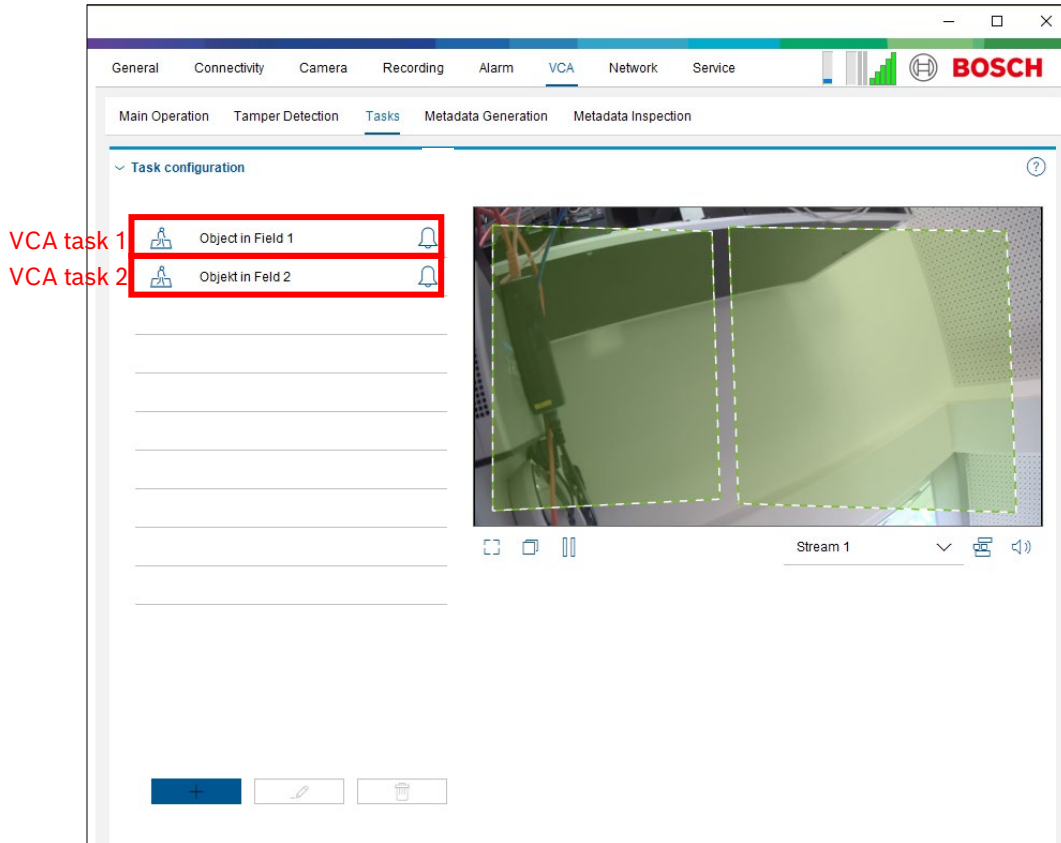


4. On the *Generic settings* page you can find the ports used for the connection via the API. Please be aware, that the Web and the API interface are using the same ports.

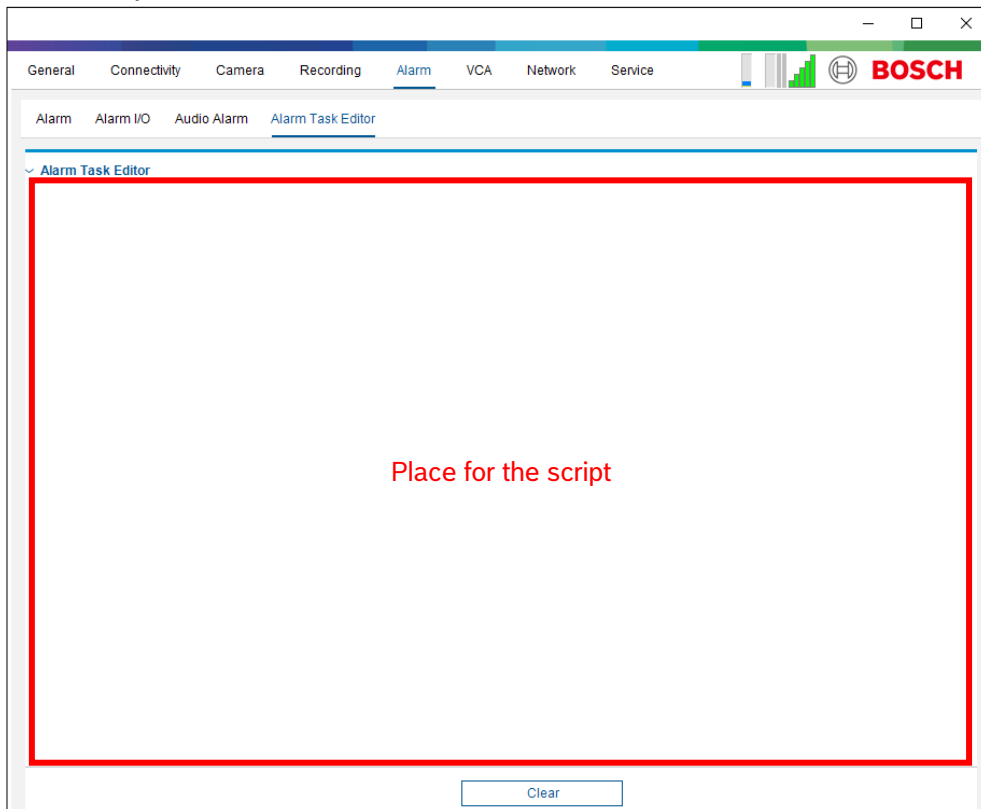


**At the camera:**

1. Set areas, using VCA task (Video Content Analysis tasks), that will trigger an Alarm Task Script.



2. Add a script at the Alarm Task Editor.



This script will trigger a Virtual General Purpose Input (VGPI) of the IP horn/amp. In the Alarm Task Script example below, it uses VCA task 1 (first rule) and VCA task 2 (second rule). If you are using another VCA task to trigger the IP horn/amp, make sure the VCA(1,x) is correctly defined.

The username and password for both the Alarm Task Editor Script (camera) and the API user account (IP horn/amp) must match. Also the IP address of the IP horn/amp needs to be adapted in the script below.

### Example Script

In this example, the camera defines two areas, that in turn activate two different messages via VGPIs at the speaker/module.

```
HttpCommand sendHttpOn:={
Command("api/ext/v1/vgpis/1")SSL(true)Port(443)IP("192.168.1.94")
Password("pwd12345")UserName("API_username")Method(POST)ForceBasicAuth(true)
ContentType("application/json")
Payload("true")
Name("Http Command 1")
};
```

```
HttpCommand sendHttpOff:={
Command("api/ext/v1/vgpis/1")SSL(true)Port(443)IP("192.168.1.94")
Password("pwd12345")UserName("API_username")Method(POST)ForceBasicAuth(true)
ContentType("application/json")
Payload("false")
Name("Http Command 1")
};
```

```
HttpCommand sendHttp_2On:={
Command("api/ext/v1/vgpis/2")SSL(true)Port(443)IP("192.168.1.94")
Password("pwd12345")UserName("API_username")Method(POST)ForceBasicAuth(true)
ContentType("application/json")
Payload("true")
Name("Http Command 2")
};
```

```
HttpCommand sendHttp_2Off:={
Command("api/ext/v1/vgpis/2")SSL(true)Port(443)IP("192.168.1.94")
Password("pwd12345")UserName("API_username")Method(POST)ForceBasicAuth(true)
ContentType("application/json")
Payload("false")
Name("Http Command 2")
};
```

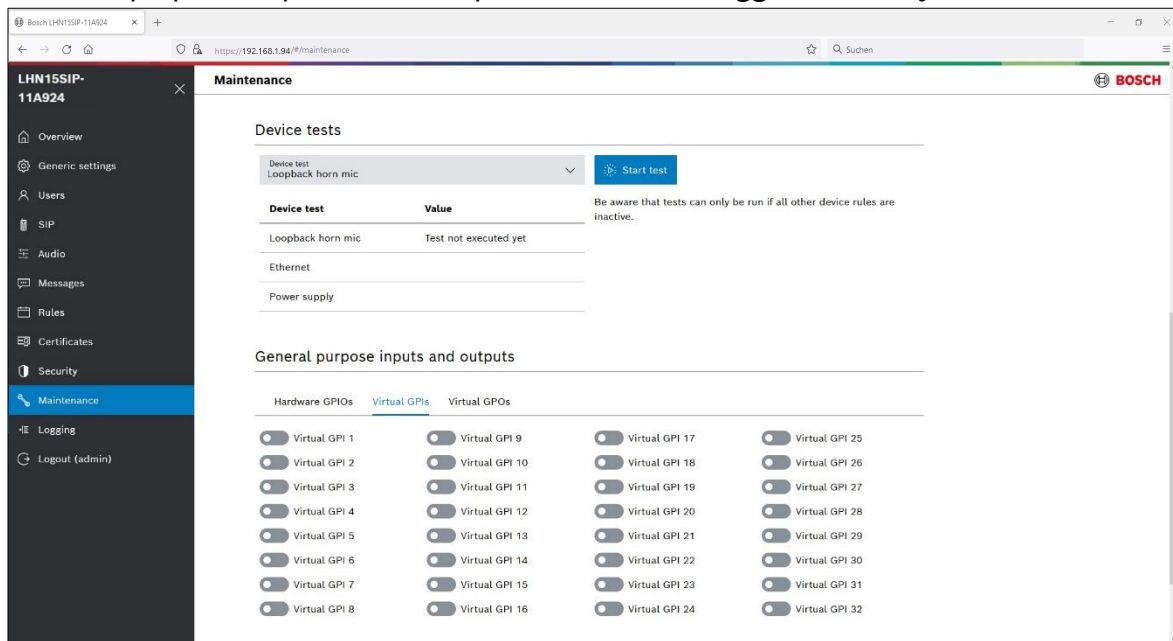
```
if(VCARule(1,1)) then sendHttpOn else sendHttpOff;
if(VCARule(1,2)) then sendHttp_2On else sendHttp_2Off;
```

## Notice!

The Alarm Task script will send an HTTP “On” command to the IP horn/amp when the VCA task is true. After a few seconds time delay, it will send an HTTP “Off” command to the IP horn/amp. Not sending the “OFF” command will result in the IP speaker continue to play the audio file in loop. This behavior can be adapted in the Action Settings of the Rule in the IP horn/amp.

## Testing

- The message should play when the VCA task becomes active in the camera (e.g. somebody enters the defined area)
- It is also possible to trigger the VGPI in the IP horn/amp. It can be used to test the IP horn/amp part independent from the camera. You can find this option on the maintenance page under *General purpose inputs and outputs*. With the toggle switch you can set it on/off.



## 4.2. SIP

The Session Initiation Protocol (SIP) is a signaling protocol used to manage (initiate, maintain and terminate) communication sessions involving voice, video and messages. This application protocol can be used to transmit all types of digital media. So, it is a specific technology that can be used for VoIP (Voice over IP).

Use the SIP accounts page of the IP horn/amp to provide information on the current existing accounts for this device. From this page, you can enable and disable existing SIP accounts and add, modify, or delete accounts.

You can create two types of accounts:

- **P2P account** - applicable for direct SIP phone to SIP device (IP horn/amp) communication. To set up a P2P account, two parameters are mandatory:
  - Username (Label)
  - Transport protocol.
- **Registrar account** - applicable if the device (IP horn/amp) connects to a SIP server. To set up a Registrar account:
  - The Username and Password need to match to the SIP server's dedicated account for the device.
  - You must select the Transport protocol.
  - You must assign an IP address of the SIP server in the Registrar.

### Additional considerations when using SIP

- **SIP audio codecs:**

The IP horn/amp supports the audio codecs G.711 (u-law and a-law), G.722, Opus. Ensure, that at least one of these codecs is enabled in the settings of the SIP server or SIP phone.
- **SIP account:**

For each SIP Rule a separate SIP account is needed.
- **Server certificate (optional):**

Server certificates are digital authorizations that allow secure transmissions between the SIP server and the speaker/module. When you select the Verify server certification check box, the device verifies the SIP server is authorized to transmit and receive audio and data by checking the digital certificate. Select the proper certificate from the Certificate for this device drop down menu. Manage the available certificates on the *Certificates* page.
- **Certificates (optional):**
  - Use the *Certificates* page to create and manage the certificates the device uses for secure transmissions within the system. Certificates are digital authorizations that allow devices to communicate with each other over secure communication lines.
  - The CA certificate allows secure SIP communication (transport protocol TLS) between a SIP server and the speaker/module. Selection of this certificate is done from the SIP server when TLS is enabled as the transport protocol. For more information, see the SIP page. To add this certificate, select CA cert and upload the certificate file via the select file button.
- **Advanced SIP configuration settings (optional):**

Under SIP settings or SIP accounts, further configuration settings can be adapted to match the SIP server or SIP phone requirements.

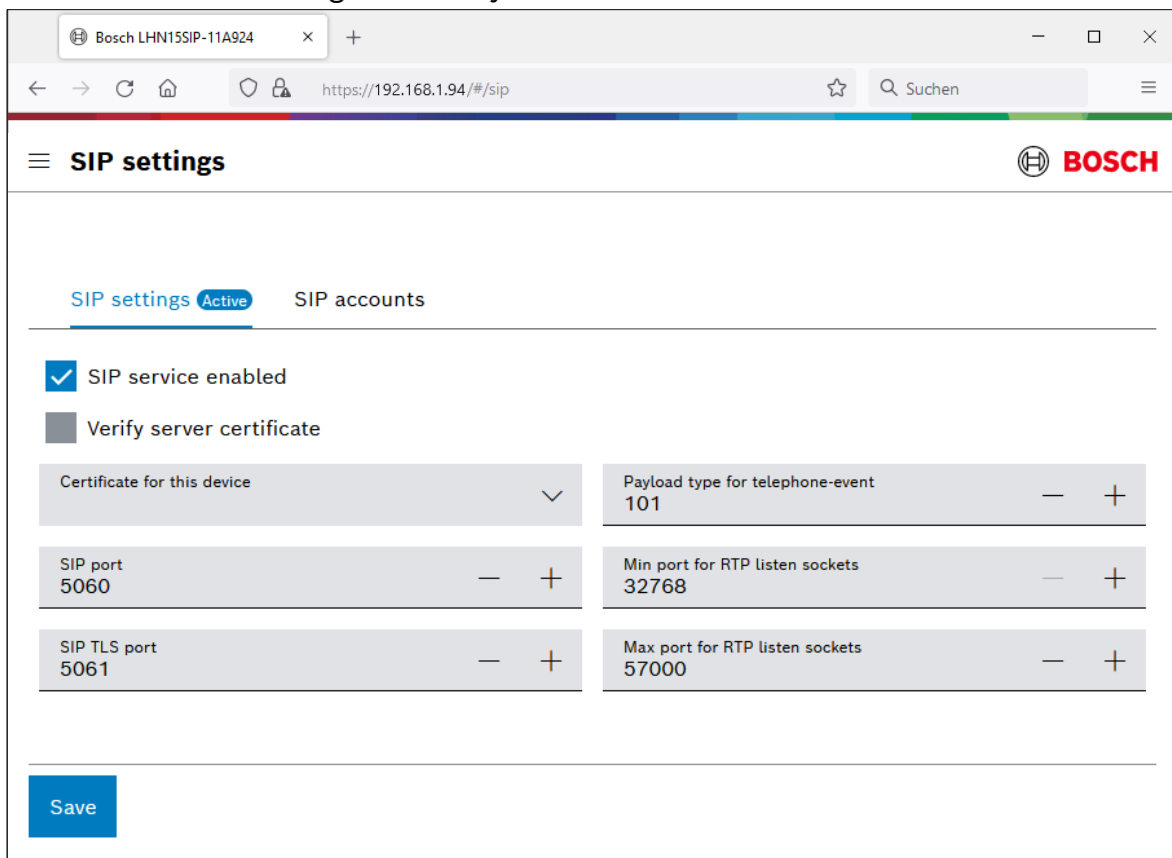
**Notice!**

There is no possibility to initiate a SIP call from the IP horn/amp to another SIP device. The IP horn/amp is unable to establish a direct connection with an online SIP proxy. Use SIP trunking to connect to the public telephone network via a SIP provider.

**4.2.1. Peer-to-Peer connection**

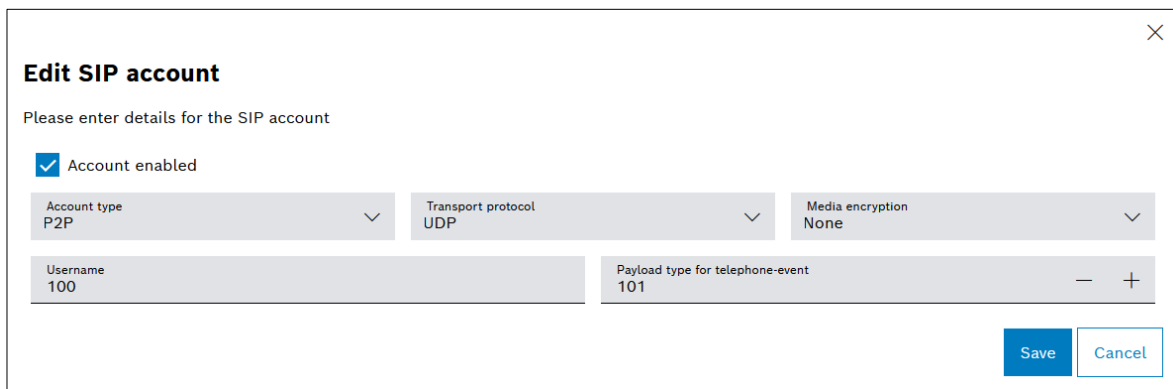
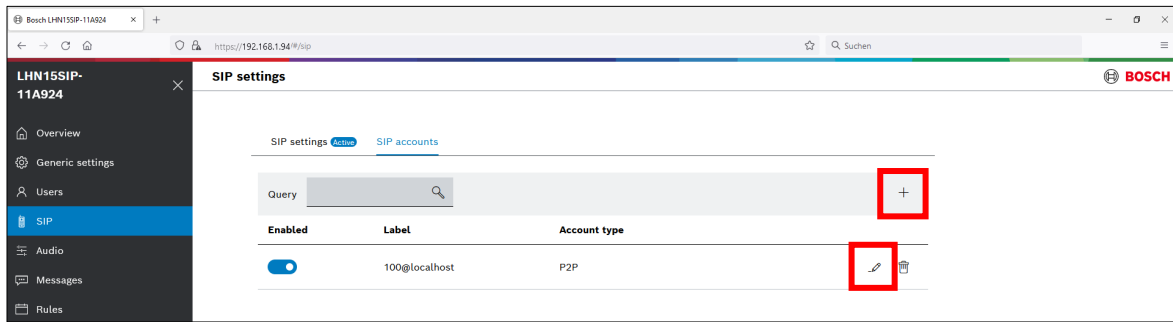
In case of having only one source from a fixed location a Peer-to-Peer connection between a SIP phone and an IP horn/amp could be set up without using a PBX server. In this example we are using MicroSIP as SIP phone.

1. Go to “SIP” -> “SIP settings” and verify that SIP service is enabled.





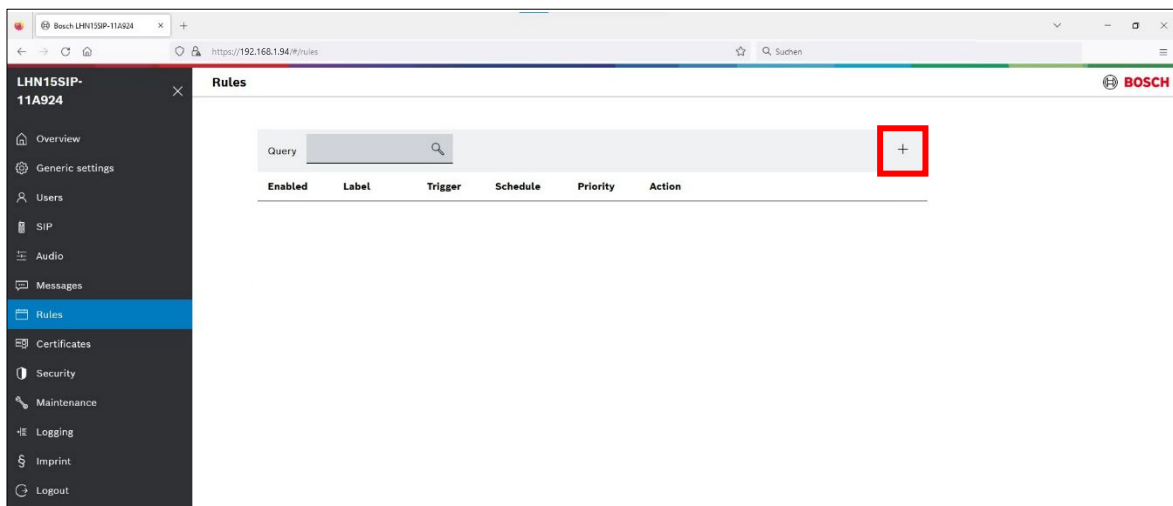
2. Go to “SIP” -> “SIP accounts” and create a SIP account by clicking the + or modifying an default one.



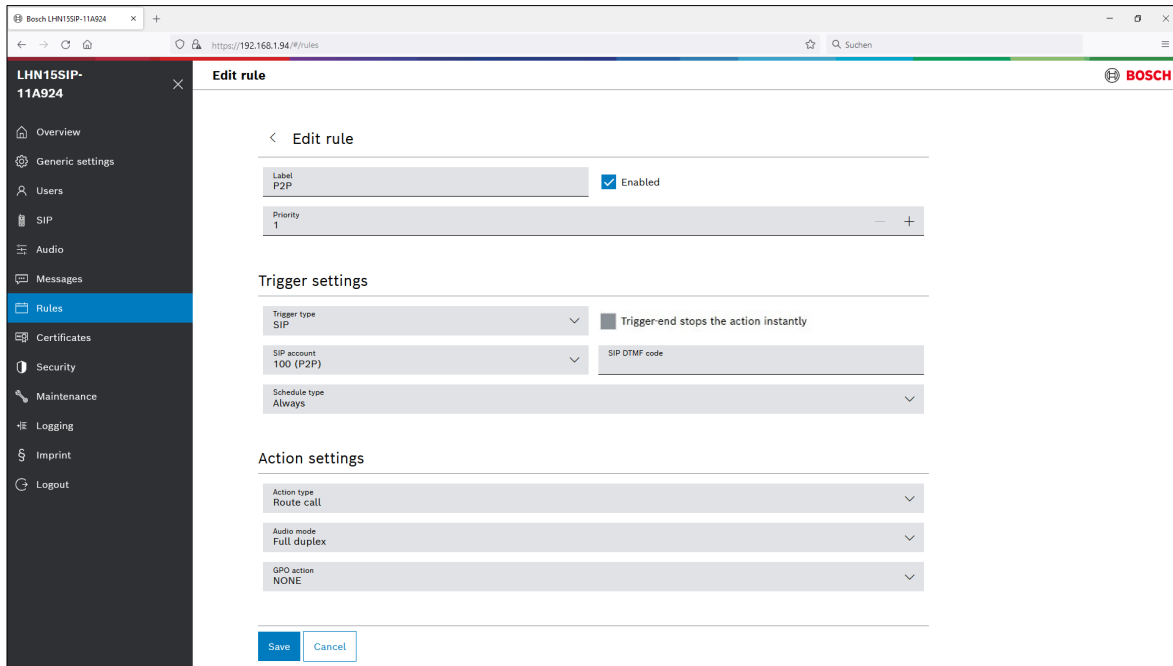
**Notice!**

The transfer protocol needs to be the same as in the SIP phone.

3. Go to “Rules” and click on the + to add a new rule.

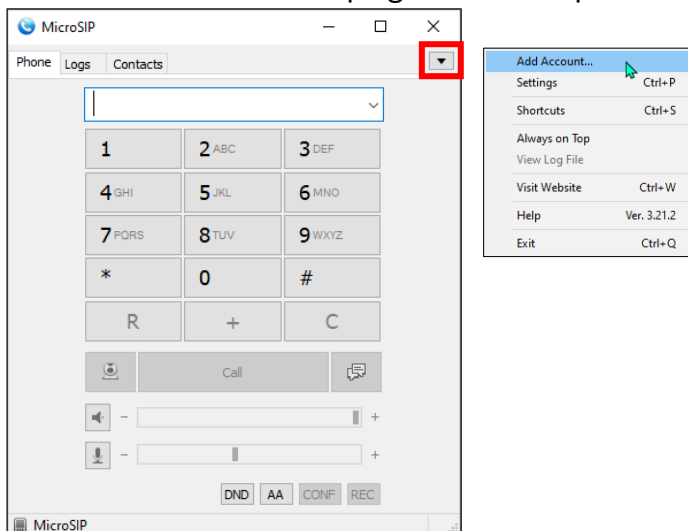


4. Make the following settings:
  - Trigger type: SIP
  - Select the P2P SIP account.
  - Action type: Route call



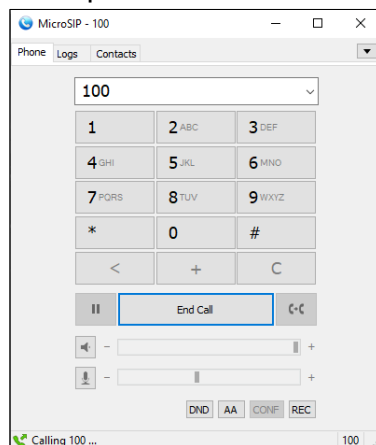
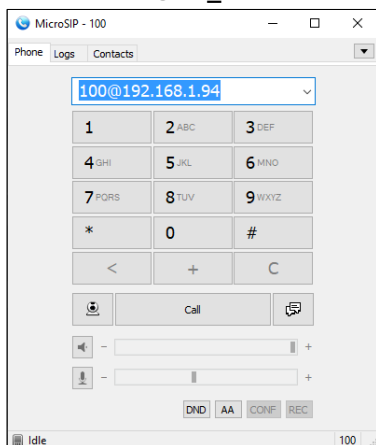
5. Open the configuration side of your SIP phone (in this example MicroSIP).

Click on the arrow in the top right corner to open the dropdown menu and click “Add Account...”.



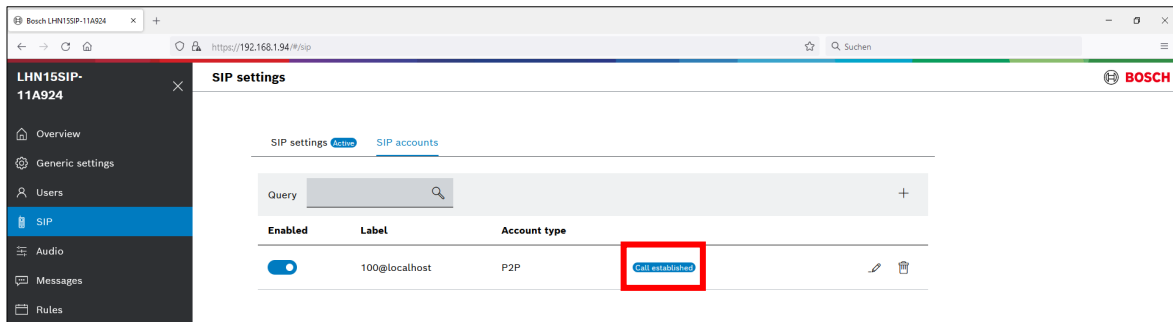
- Enter a Username and a Domain (IP address of the IP horn/amp), select the Transport protocol (UDP/TCP/TLS) and click Save.

- You can use now the SIP phone (in this example MicroSIP) to start a call. Dial “Username” or “Username@IP\_AddressOfHorn” and press the Call button. Press End Call to stop the call.

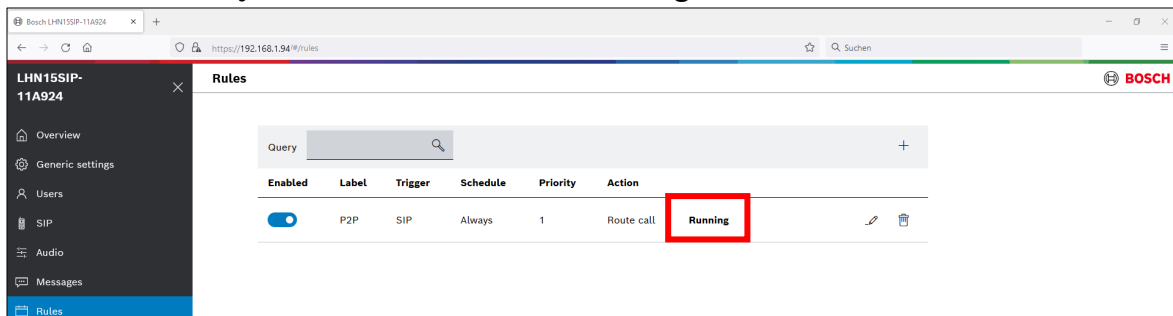


8. Very connectivity and rule activity:

In the SIP menu under SIP accounts you can check if the call is established.

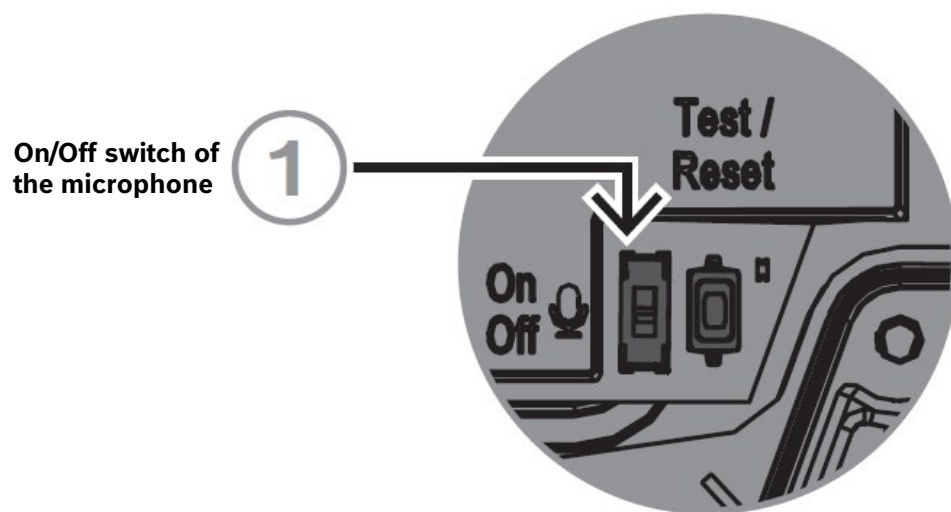


In the rules menu you can check if the rule is running.



**Notice!**

If you want to use two-way SIP communication, make sure that the microphone of the IP horn is activated.



## 4.2.2. SIP server connection

A 3rd party SIP PBX (Private Branch Exchange) Server is required for being able to call the IP horn/amp from multiple telephones.

The customer is responsible for the support and protection of the PBX against any security or fraud threats.

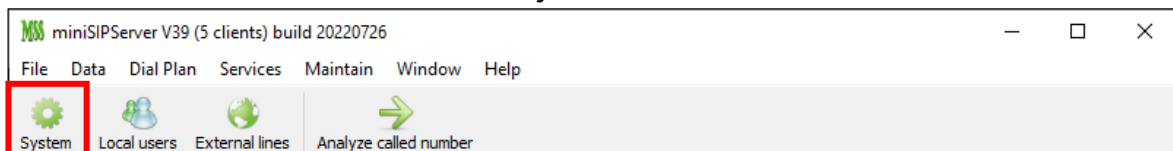
The IP horn/amp can subscribe as a SIP Client to the SIP PBX Server. It will have a phone number which can be called like any other VoIP client.

### Notice!

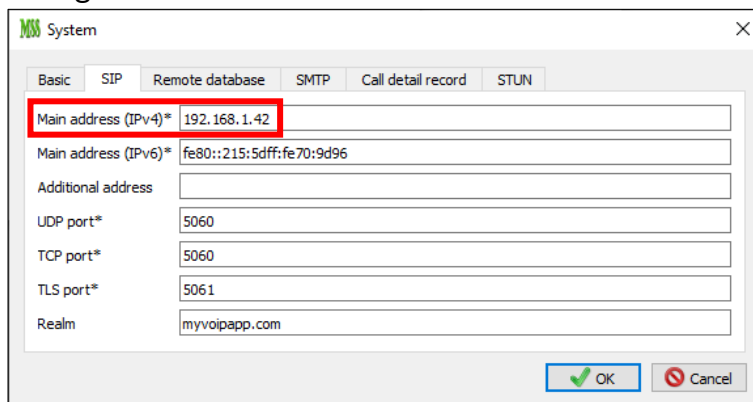
Server configuration depends upon the brand and model of the SIP PBX Server. Please consult the server-side documentation for this. In this example we are using the miniSIPServer.

Shown below is a server configuration supposing that the IP horn/amp, the SIP phone and the SIP server are in the same local network, that all three are in the same network subnet and that the SIP server network address is 192.168.1.42.

1. Launch the miniSIPServer and click on System.



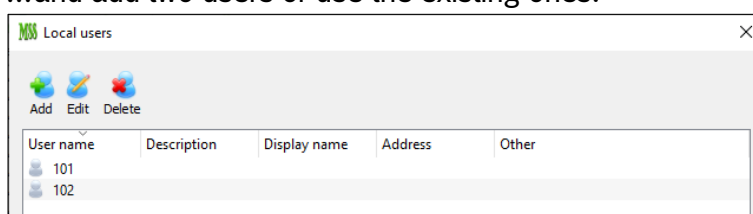
2. Change the Main address on the SIP tab to an address which is in the range of the IP horn/amp.



3. Click on local users...



...and add two users or use the existing ones.



User 101 is the MicroSIP phone (Username and Password = 101).

The screenshot shows a 'Local user' configuration window with the following fields and options:

- User name:** 101
- User password:** 101
- Description:** (empty)
- IP address authorization
- IP address:** (empty)
- Port:** 0

At the bottom right, there are 'OK' and 'Cancel' buttons.

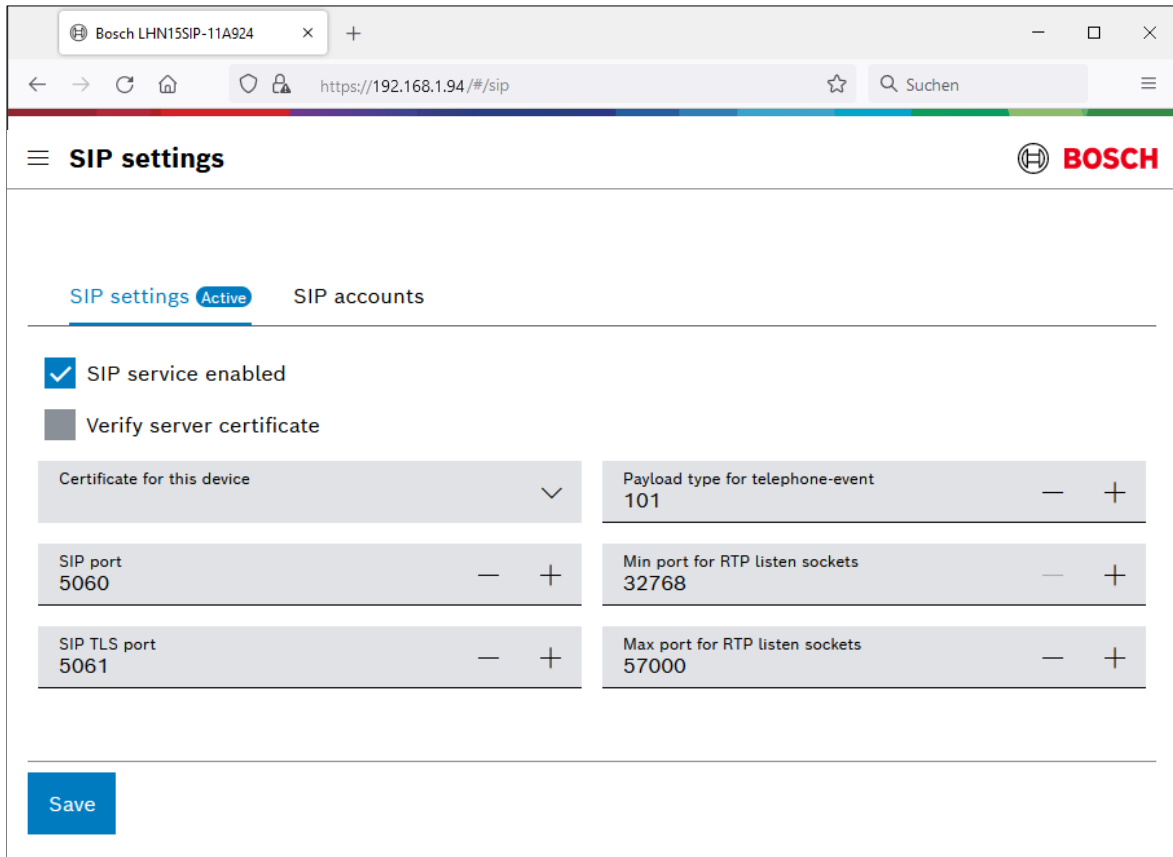
User 102 is the IP horn/amp (Username and Password = 102).

The screenshot shows a 'Local user' configuration window with the following fields and options:

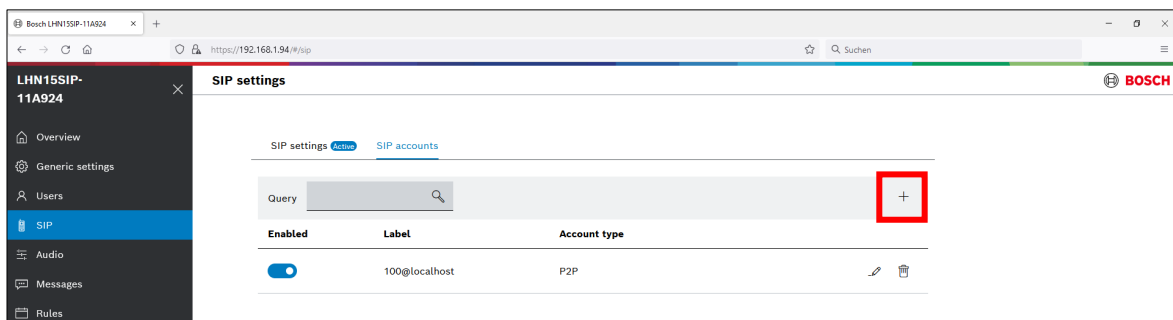
- User name:** 102
- User password:** 102
- Description:** (empty)
- IP address authorization
- IP address:** (empty)
- Port:** 0

At the bottom right, there are 'OK' and 'Cancel' buttons.

4. Logon to the IP horn/amp and go to “SIP” -> “SIP settings” and verify that SIP service is enabled.



5. Go to “SIP” -> “SIP accounts” and create a SIP account by clicking the + or modifying an existing one.



6. Do the following settings and click Save:
  - Account type: Registrar
  - Transport protocol: TCP, UDP, TLS
  - Username and Password: 102 (need to match the settings in the SIP server)
  - Registrar: IP address of the SIP server

### Add SIP account ✕

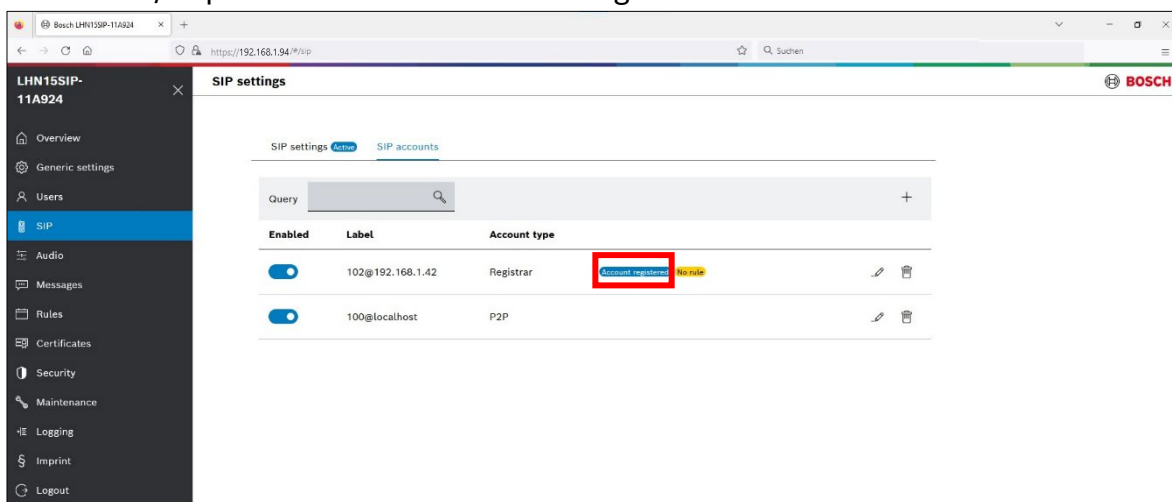
Please enter details for the SIP account 192.168.1.42

Account enabled

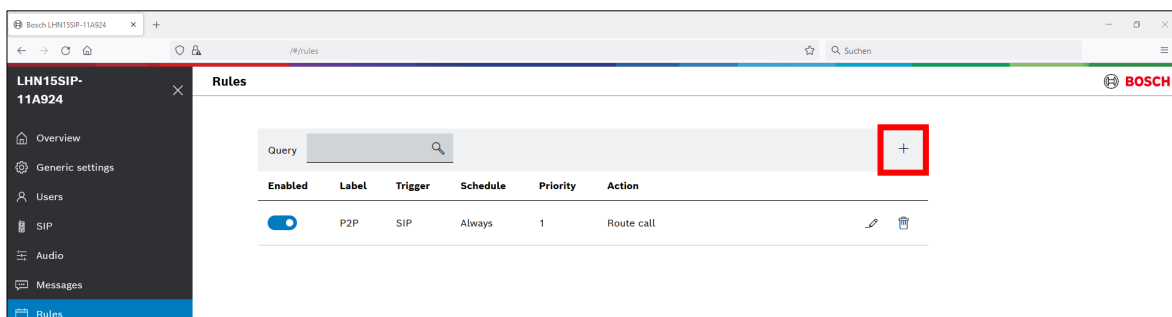
Account type Registrar	Transport protocol TCP	Media encryption None
Username 102	Password ●●●	Registrar 172.24.112.1
Payload type for telephone-event 101	NAT traversal method None	Registration expiry 30
Fallback registration expiry 0	Registration priority 0	Relative registration wait delay (%) 5
Proxy 1 IP	Proxy 1 username	Proxy 1 password
Proxy 2 IP	Proxy 2 username	Proxy 2 password

Save
Cancel

7. The IP horn/amp should show now “Account registered”.



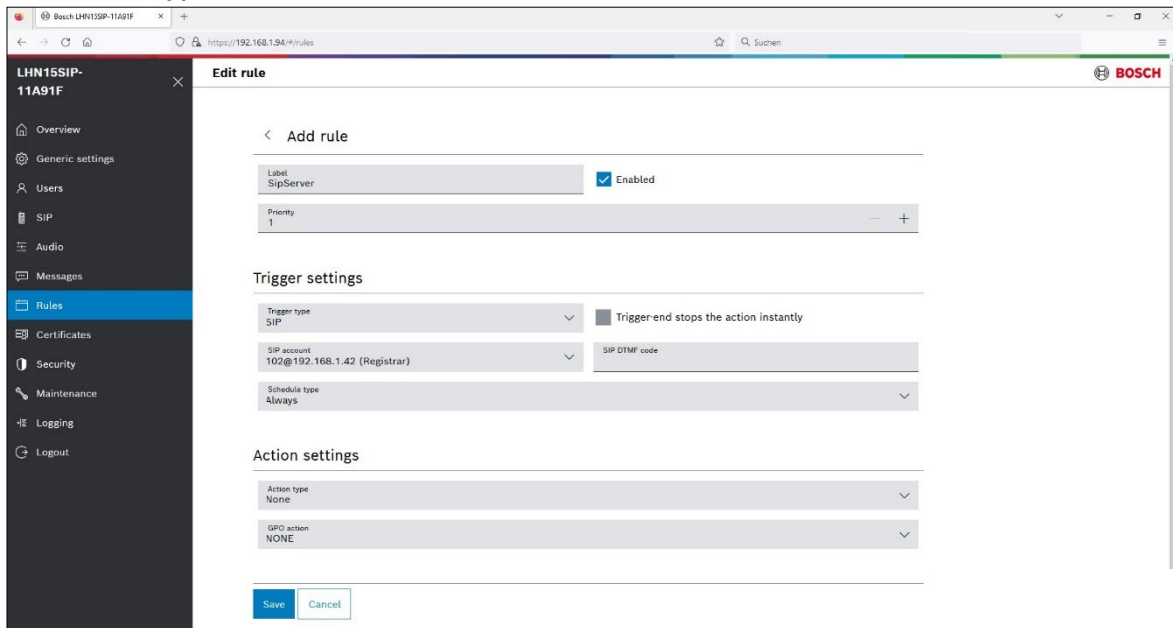
8. Go to “Rules” and click on the + to add a new rule.





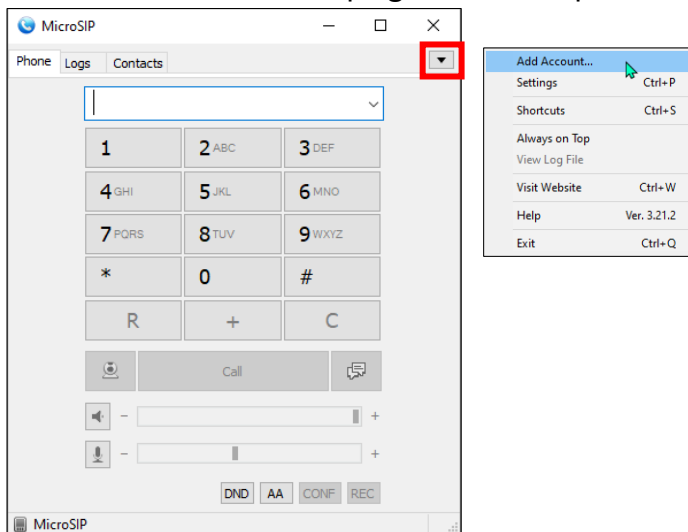
9. Make the following settings and click Save.

- Trigger type: SIP
- Select the Registrar SIP account.
- Action type: Route call



10. Open the configuration side of your SIP phone (in this example MicroSIP).

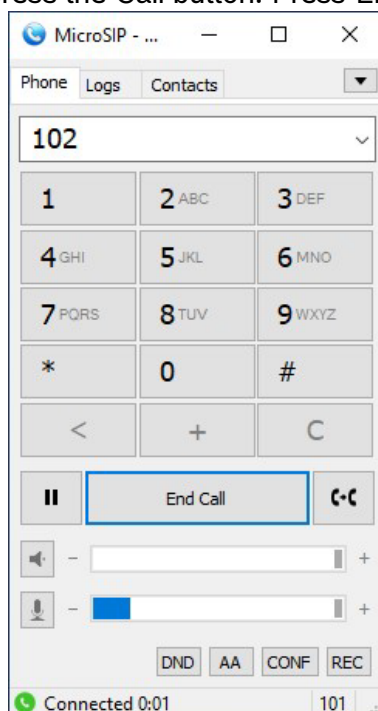
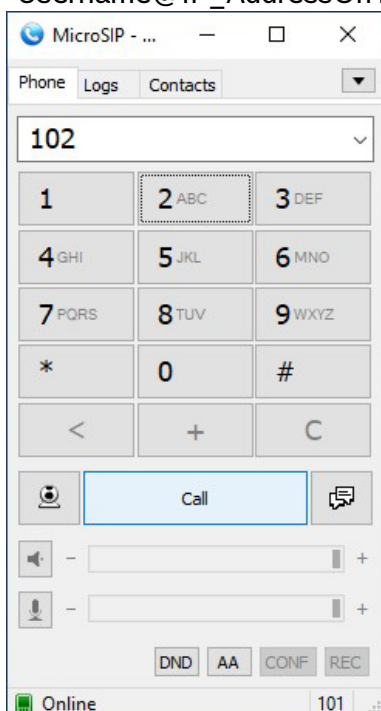
Click on the arrow in the top right corner to open the dropdown menu and click “Add Account...”.



11. Enter the following and click Save.

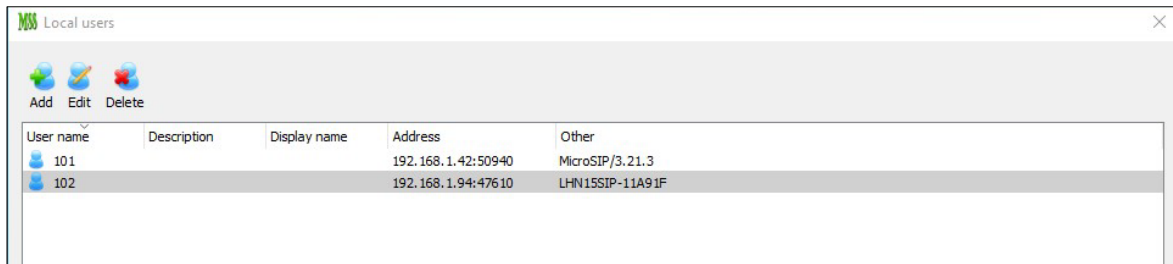
- Account Name
- SIP Server: IP address of the SIP server
- Username: 101 (Username of the SIP phone configured in the SIP server)
- Password: 101 (Password of the SIP phone configured in the SIP server)

12. You can use now the SIP phone (in this example MicroSIP) to start a call. Dial “Username” or “Username@IP\_AddressOfHorn” and press the Call button. Press End Call to stop the call.



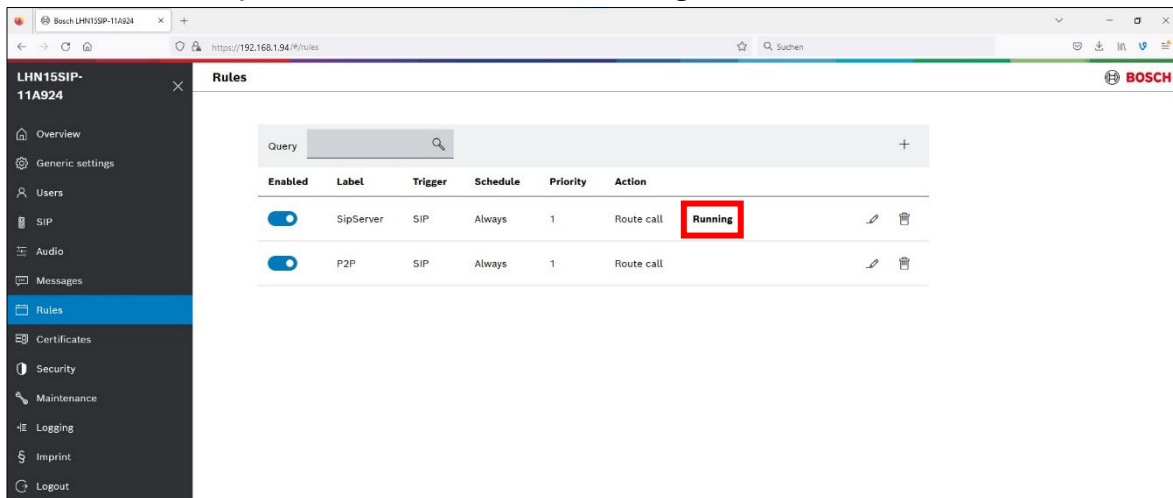
13. Very connectivity and rule activity:

On the *Local users* page of the miniSIPServer you can check if both users are registered.



User name	Description	Display name	Address	Other
101			192.168.1.42:50940	MicroSIP/3.21.3
102			192.168.1.94:47610	LHN15SIP-11A91F

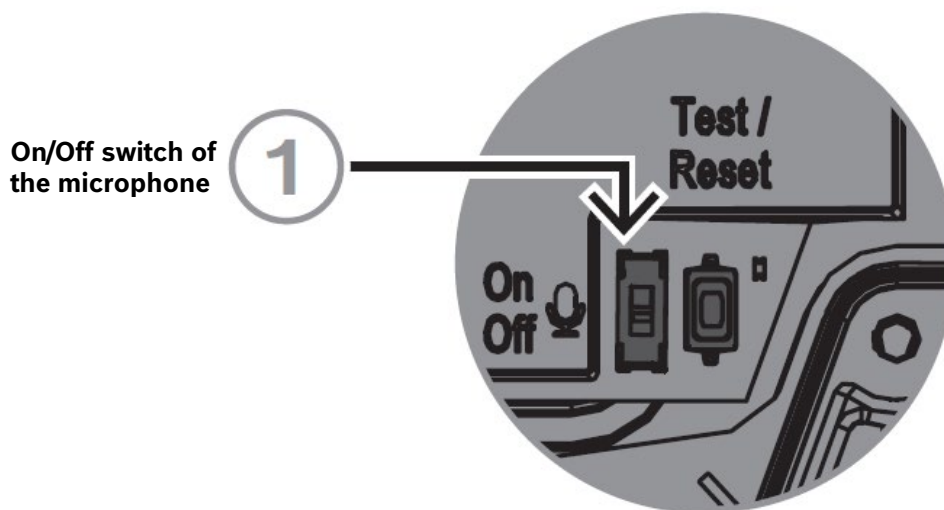
In the rules menu you can check if the rule is running.



Enabled	Label	Trigger	Schedule	Priority	Action	Running
<input checked="" type="checkbox"/>	SipServer	SIP	Always	1	Route call	Running
<input checked="" type="checkbox"/>	P2P	SIP	Always	1	Route call	

**Notice!**

If you want to use two-way SIP communication, make sure that the microphone of the IP horn is activated.

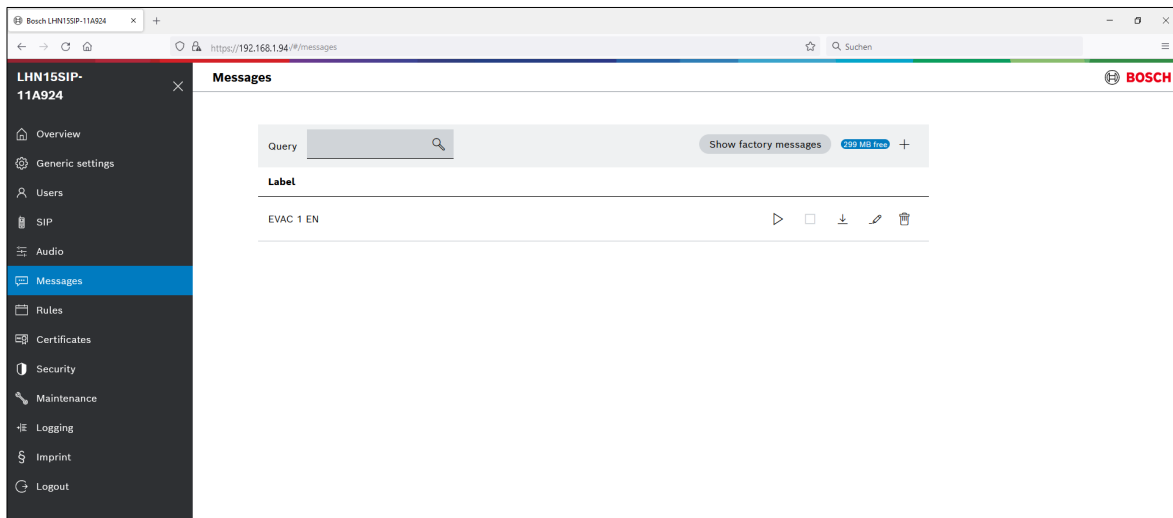


### 4.3. Trigger message via noise (horn loudspeaker only)

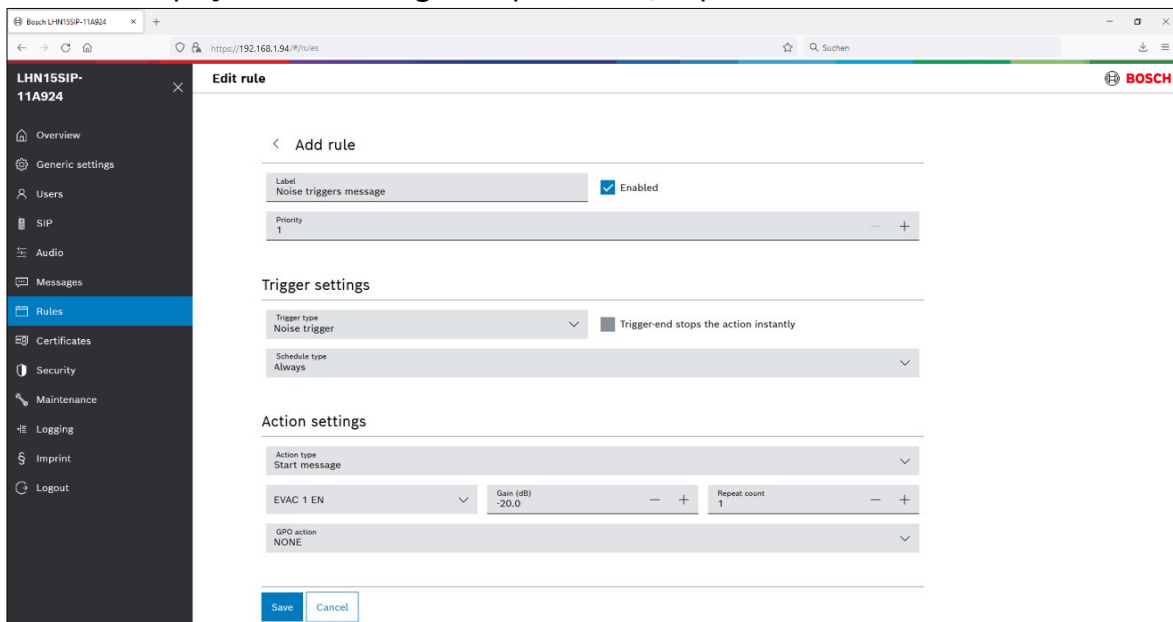
Use the Noise trigger type when an action starts after an ambient noise reaches a specific level or the noise level exceeds a specified limit. You can combine this trigger type with a schedule via Schedule type, if applicable. Otherwise, keep the default setting of Always.

#### Configuration:

1. You can upload your own messages by using the + or you can use a factory message. Supported file formats are listed in the data sheet.



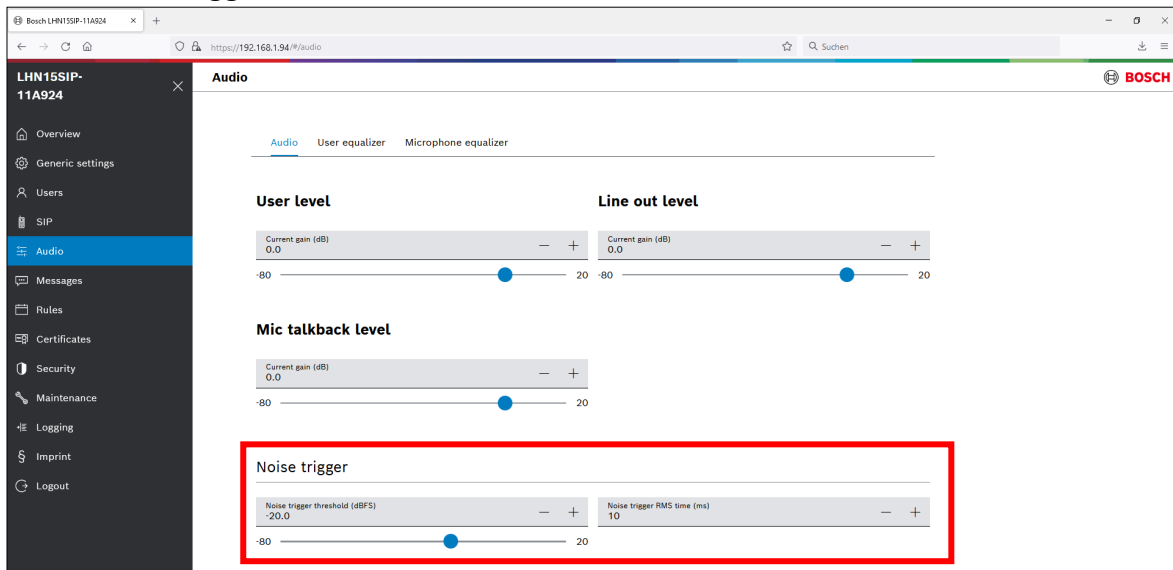
2. Create a Rule that leads Noise to start the action “Start message” and select the message you would like to play with the settings of repeat, abort/stop behavior.



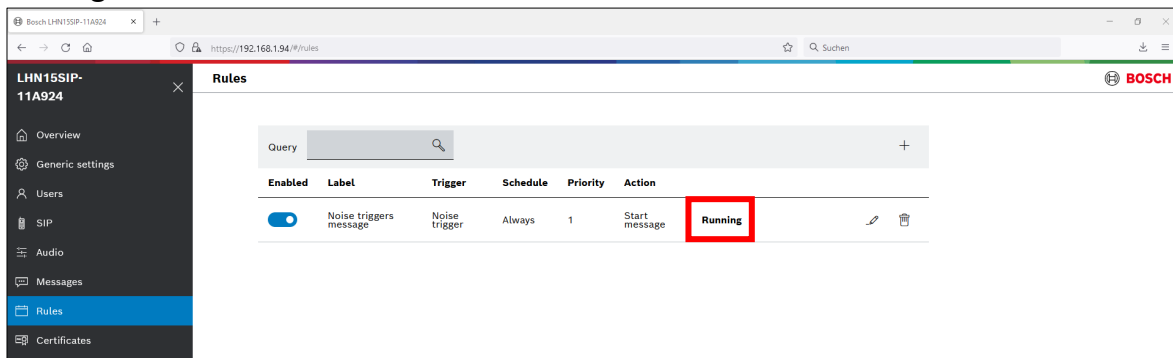
#### Notice!

If the checkbox **"Trigger-end stops the action instantly"** is enabled, the action will stop immediately the trigger finishes. If disabled, it allows an action to run its course completely depending on the settings, even when the trigger is no longer present. For instance, a message plays to the end or for a specified number of times as determined by the repeat count setting.

3. There are two noise parameters necessary for operation. You can find these parameters on the Audio page:
  - Noise trigger threshold
  - Noise trigger RMS time

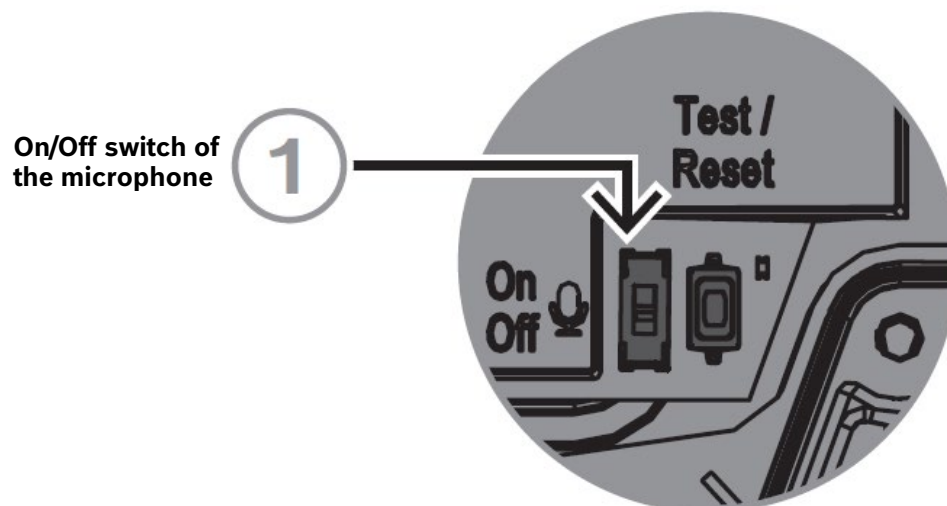


4. To test the rule, make some noise and check if the rule shows the state Running and if the message is audible.



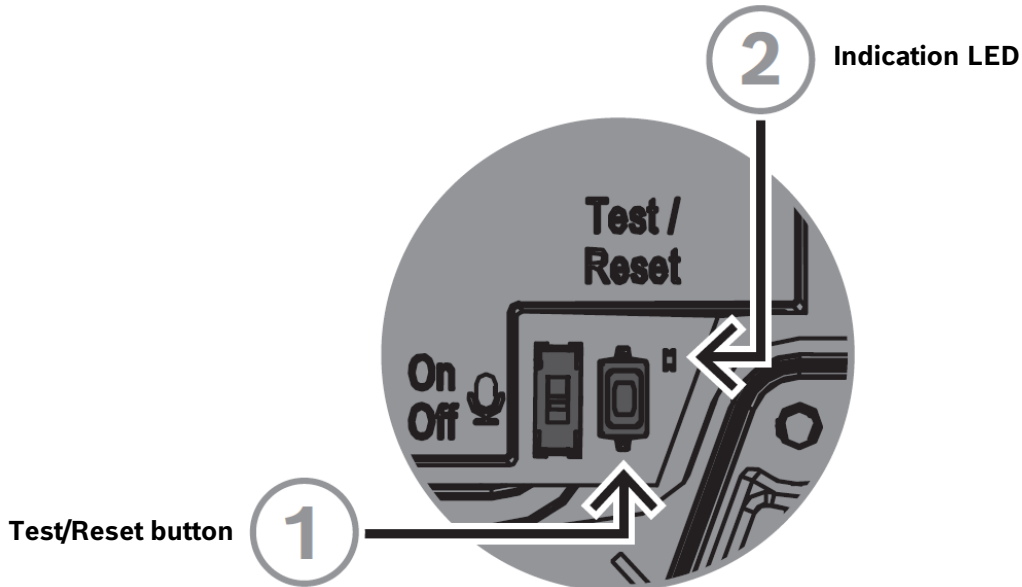
**Notice!**

The integrated microphone is used for the ambient noise level trigger. So, make sure that the microphone of the IP horn is activated.



## 5. Test/Reset button

### IP Horn loudspeaker



#### Test/Reset button

There is a physical button for test and reset purposes. This button will perform different actions depending on how long you press it:

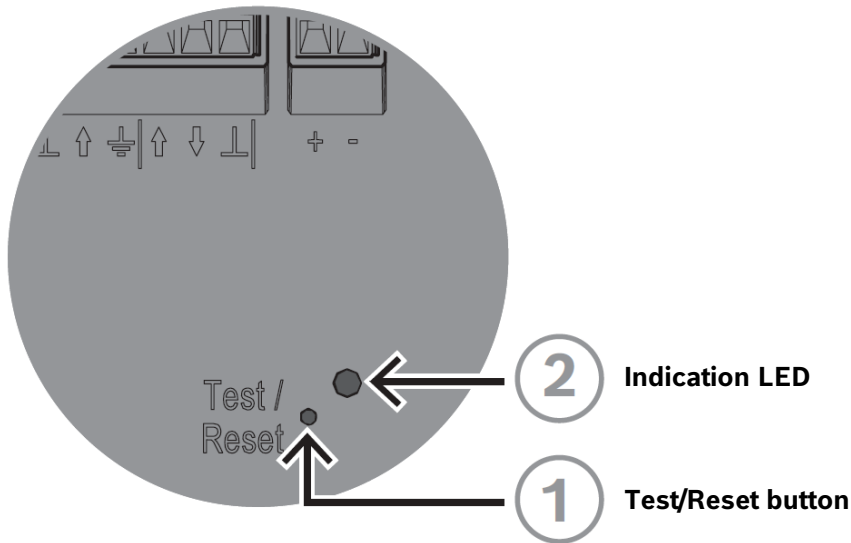
1. Press and hold for 1 - 5 seconds: the IP Horn loudspeaker will play a default message to test the loop between the speaker and the microphone. The IP Horn loudspeaker performs a check that the speaker is operating and therefore the microphone is used. When the microphone physical switch is On, the tone lasts around 2 seconds; when it is turned Off, you hear a brief beep (approximately ½ second).
2. Press and hold for 6 - 10 seconds: the IP address of the horn will reset to factory default (DHCP);
3. Press and hold for 11 - 20 seconds: the horn will reset to factory default.

#### Indication LED

The LED (2) next to the Test/Reset button serves as a time indicator of how long the Test/Reset button is pressed. Once you click the Test/Reset button once, the LED lights up every five seconds for as long as you keep the button pressed, and once more when you let go of the button to indicate the reset is applied.

The LED next to the test button flashes slowly (1 Hz) if the test is successful and quickly (4 Hz) when it is unsuccessful.

## IP Amplifier module



### Test/Reset button

There is a physical button for test and reset purposes (1). Use a paper clip or similar object to press and hold the Test/Reset button. This button will perform different actions depending on how long you press it:

1. Press and hold for 6 - 10 seconds: the IP address of the amplifier module will reset to factory default;
2. Press and hold for 11 - 20 seconds: the amplifier module will reset to factory default.

### Indication LED

The LED (2) next to the Test/Reset button serves as a time indicator of how long the Test/Reset button is pressed. Once you click the Test/Reset button once, the LED lights up every five seconds for as long as you keep the button pressed, and once more when you let go of the button to indicate the reset is applied.

## 6. Document history

Release date	Documentation version	Reason
2023-02	v1.0	1 <sup>st</sup> edition
2023-05	v1.1	Layout updated
2024-05	v1.2	Some parts have been updated to be compatible with IP horn/amp FW v2.1

## 7. Notice of liability

While every effort has been taken to ensure the accuracy of this document, neither Bosch Security Systems nor any of its official representatives shall have any liability to any person or entity with respect to any liability, loss or damage caused or alleged to be caused directly or indirectly by the information contained in this document.

Bosch Security Systems reserves the right to make changes to features and specifications at any time without prior notification in the interest of ongoing product development and improvement.

### **Bosch Security Systems B.V.**

Torenallee 49  
5617 BA Eindhoven  
Netherlands  
[www.boschsecurity.com](http://www.boschsecurity.com)