

# DIVUS HEARTBEAT

User manual

Version 1.0

REV05-2018-04-16

---

## GENERAL INFORMATION

---

DIVUS GmbH  
 Pillhof 51  
 I-39057 Eppan (BZ) - Italy

Operating instructions, manuals and software are protected by copyright. All rights are reserved. Copying, multiplication, translation and conversion, either partially or as a whole, is not permitted. You are allowed to make a single copy for backup purposes.

We reserve the right to make changes to the manual without prior notification.

We assume no responsibility for any errors or omissions that may appear in this document.

We do not assume liability for the flawlessness and correctness of the programs and data contained on the delivered discs.

You are always welcome to inform us of errors or make suggestions for improving the program.

The present agreement also applies to special appendices to the manual.

This manual can contain terms and descriptions, which improper use by third can harm the copyrights of the author.

Please read the manual before beginning and keep the manual for later use.

The manual has been conceived and written for users who are experienced in the use of PCs and automation technology.

---

## CONVENTIONS

---

[KEYS]	Keys that are to be pressed by the user are given in square brackets, e.g. [CTRL] or [DEL]
COURIER	On-screen messages are given in the Courier font, e.g. C:\>
COURIER BOLD	Keyboard input to be made by the user are given in Courier bold, e.g. C:\>DIR).
"..."	Names of buttons to be pressed, menus or other onscreen elements and product names are given within double quotes. (e.g. "Configuration").
PICTOGRAMS	In this manual, the following symbols are used to indicate particular text blocks.
	<i>Caution!</i> A dangerous situation may arise that may cause damage to material.
	<i>Hint</i> Hints and additional notes
	<i>New</i> New features

---

 INDEX
 

---

GENERAL INFORMATION	2
CONVENTIONS	2
INDEX	3
1 INTRODUCTION	6
1.1 GENERAL INFORMATION	6
1.2 THE MANAGER	7
1.2.1 DIVUS SECURE INTRANET	7
1.2.2 RESIDENTIAL INTERCOM NETWORK	8
1.2.3 HOME LAN/WAN	8
1.3 THE MANAGED SWITCH (DMS-8P-L2+)	8
2 SYSTEM INFRASTRUCTURE	9
2.1 GRAPHS/SCHEMES	9
2.1.1 GENERAL SCHEME	9
2.1.2 ISOLATED NETWORK SCHEME	10
2.1.3 DIVUS SECURE INTRANET (DSI) SCHEME	12
2.1.4 RESIDENTIAL INTERCOM NETWORK (RIN) SCHEME	13
3 WEB INTERFACE	14
3.1 FIRST ACCESS: THE SETUP WIZARD	14
3.1.1 STEP 1 - START	14
3.1.2 STEP 2 – LICENSE AGREEMENT	15
3.1.3 STEP 3 – SYSTEM INTEGRATOR DETAILS	16
3.1.4 STEP 4 – CUSTOMER DETAILS	17
3.1.5 STEP 5 – PROJECT SETUP	18
3.1.6 STEP 6 – NETWORK CONFIGURATION - DIVUS SECURE INTRANET	18
3.1.7 STEP 7 – NETWORK CONFIGURATION - RESIDENTIAL INTERCOM	19
3.1.8 STEP 8 – SUMMARY / LAST STEP	19
3.1.9 NETWORK SCAN	20

3.2	SYSTEM STATUS PAGE _____	20
3.3	SYSTEM – UPGRADE _____	20
3.3.1	UPGRADE PROCEDURE _____	21
3.4	SYSTEM – SHUTDOWN _____	23
3.5	DIVUS NETWORK – REPORT PAGE _____	23
3.5.1	THE GRAPHICAL SCHEME _____	24
3.5.2	THE PDF FILE OF THE REPORT _____	25
3.6	DIVUS NETWORK – PERFORM SCAN PAGE _____	25
3.7	DIVUS NETWORK – ARCHIVE PAGE _____	27
3.8	SIP STATUS PAGE _____	27
3.9	LOGS – SWITCH LOGS PAGE _____	28
3.10	LOGS – VOIP/SIP LOGS PAGE _____	28
3.11	LOGS – CALL LOGS PAGE _____	28
3.12	SETTINGS – SYSTEM PAGE _____	28
3.13	SETTINGS – NETWORK SETTINGS PAGE _____	29
3.13.1	DHCP _____	29
3.13.1.1	DSI _____	29
3.13.1.2	RIN _____	29
3.14	SETTINGS – SMART DEVICES PAGE _____	30
3.15	SETTINGS – FIREWALL RULES PAGE _____	30
3.16	SETTINGS – PORT FORWARDING PAGE _____	32
3.17	SETTINGS – SIP SETTINGS PAGE _____	33
4	INTERCOM _____	34
4.1	GENERAL DEFINITIONS _____	34
4.2	GENERAL VOIP ACCOUNT SCHEME (FOR ZONE 1 AND ZONE 2) _____	35
4.2.1	BASE UNIT _____	36
4.3	VOIP ACCOUNTS FOR EXTERNAL UNITS _____	37
4.4	CONCIERGE / RECEPTION ACCOUNTS _____	38
5	CLIENT DEVICE SETUP FOR THE DSI AND THE RIN _____	39

5.1	DIVUS TOUCHZONE	39
5.2	DIVUS SUPERIO AND OTHER WINDOWS BASED DIVUS DEVICES	39
5.3	DIVUS OPENDOOR	39
5.4	KNX CONTROL DEVICES (KNX SERVER, KNX SUPERIO)	40
5.4.1	SPECIAL RULES FOR DIVUS KNX SERVER AND KNX SUPERIO	40
5.5	THIRD-PARTY IP CAMS	41
5.6	THIRD-PARTY CLIENT DEVICES (WITH ETHERNET INTERFACE)	41
5.7	ANALOGUE THIRD-PARTY DEVICES	41
6	ADVANCED TOPICS	42
6.1	HOW TO MOVE A DEVICE USING A STATIC IP ADDRESS TO YOUR HEARTBEAT'S NETWORK	42
6.2	HOW TO USE THE LOG FILTERING / SEARCHING FUNCTION	42
6.3	HOW TO EDIT VOIP ACCOUNTS ON THE DIVUS HEARTBEAT	43
6.4	HOW TO DEFINE CUSTOM VOIP GROUP CALLS ON THE DIVUS HEARTBEAT	44
6.5	HOW TO ADD/EDIT A CUSTOM FIREWALL RULE	46
6.6	HOW TO DEFINE OR EDIT A CUSTOM PORT FORWARDING RULE	47
6.7	HOW TO SETUP A DEVICE FOR REMOTE VOIP ACCESS	48
	NOTES	50

# 1 Introduction

## 1.1 GENERAL INFORMATION

Thank you for having bought a DIVUS HEARTBEAT! This manual will help you to set up your smart home's networks in the optimal way.

The main goals of your new DIVUS HEARTBEAT are:

- Making the connection of all your smart home devices as simple as *plug and play*
- Isolating and securing the most sensitive devices from undesired external attacks
- Managing, controlling and troubleshooting your network and its devices

The DIVUS HEARTBEAT was planned and built with home automation as its only focus. It's a one of a kind device allowing you to solve very complex network tasks and requirements automatically.

The DIVUS HEARTBEAT is made of two parts: the **manager** and the **managed switch**. These parts are held together with the 19-inch **rack adapters**.



It may be expanded by adding any number of additional switches if more ports are needed.



## 1.2 THE MANAGER



The manager is the heart and the brain of the system: it controls 3 separate networks:

- The DIVUS Secure Intranet (also called **DSI** later on)
- The Residential Intercom network (**RIN**)
- The Home LAN/WAN

It is the gateway between all these three networks.

Its web server gives access to all the functionalities of the DIVUS HEARTBEAT.

See chapter 3 for further details about the web interface.



**Note:** The three network ports of the *Manager* are *not* PoE ports! If e.g. you're going to connect one single device to the *Residential Intercom* port and it needs power over the network cable, you must use a so-called PoE injector or an additional *DIVUS MANAGED SWITCH*.

Let's now have a quick look at the 3 networks.

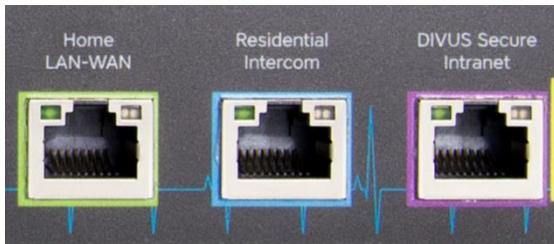
### 1.2.1 DIVUS SECURE INTRANET

The DIVUS Secure Intranet is meant to offer an isolated, secure network for your smart home devices. E.g. a DIVUS KNX SERVER, DIVUS TOUCHZONE and SUPERIO touch panels would be connected to this network. If you follow the instructions of the DIVUS HEARTBEAT Quick Start Guide or of this manual for connecting all the devices, any of the 8 main ports of the main MANAGED SWITCH can be used to connect to the DIVUS Secure Intranet.



### 1.2.2 RESIDENTIAL INTERCOM NETWORK

A safe, reliable network used for intercom communications: a firewall blocks any communication from this network to the outside world except for the VoIP communication to the VoIP server, which runs on the manager itself. Depending on the number of outdoor devices you need to connect (outdoor stations, security cams), you may need a DIVUS MANAGED SWITCH to be connected to the main RIN (Residential Intercom Network) port.



### 1.2.3 HOME LAN/WAN

Of course, there will be a home network. Depending on the customer's needs or wishes, it may or may not be desired to attach the home automation network to the internet through the home's internet router. As default, this port connects the DIVUS HEARTBEAT and the devices attached to it to the internet.

---

## 1.3 THE MANAGED SWITCH (DMS-8P-L2+)

---



The MANAGED SWITCH is an 8 ports full PoE+ switch, with two additional ports to connect to other devices in a chain. It is known to the manager, which is therefore able to not only talk directly to the devices attached to the switch, but also to log and show all the switch's activities in great detail. Any number of DMS may be attached to the main DMS using its dedicated ports 9 and 10 (*cascading*).

The other ports are currently not available for use.

## 2 System infrastructure

In this chapter, the inner workings and the tasks of the single parts of the DIVUS HEARTBEAT will be explained with easily understandable graphical schemes.

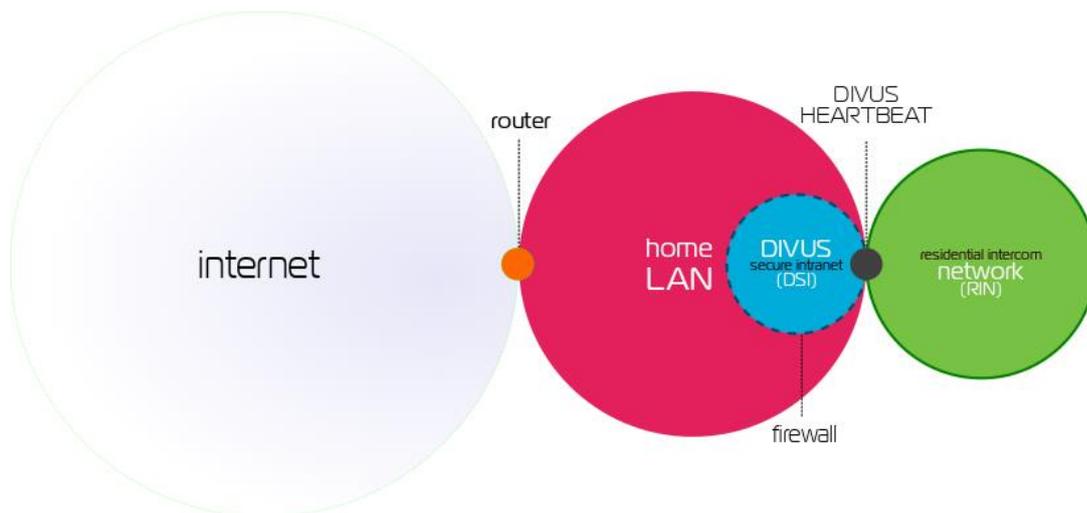
---

### 2.1 GRAPHS/SCHEMES

---

#### 2.1.1 GENERAL SCHEME

3 networks interconnected: DIVUS HEARTBEAT splits a complex system up into 3 separate, easily manageable and safe networks. How they are structured and how they relate to one another and to the internet is shown in the general scheme:

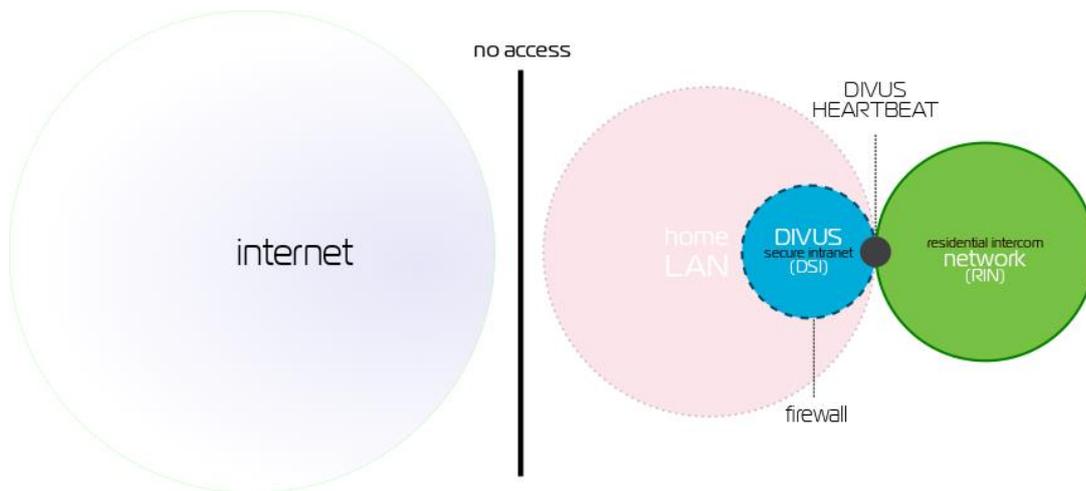


The above shows a typical network structure – probably the one most frequently adopted.

But to best understand how the DIVUS HEARTBEAT handles different setups, there are some other points to consider:

1. Usually the planned scheme is the one shown above, but when the automation devices and network are commissioned, there is no router yet – it will follow weeks or even months later.
2. Customers may prefer to have their automation system completely detached from the internet. In that case, the final scheme will be similar to the above, but without the connection to the router – and through that the internet.

## 2.1.2 ISOLATED NETWORK SCHEME



So, what happens when the network has no router in the beginning but one will be connected later on?

1. All the steps of the quick start guide should be followed. (All devices are connected, the first setup procedure on the DIVUS HEARTBEAT is completed by the network scan)
2. In this situation, the DIVUS SECURE intranet and the RESIDENTIAL INTERCOM are fully functional (except, of course, the online services).
3. Automatically detecting that there is no router active, the DIVUS HEARTBEAT will take control of the network in the router's place:
  - a. It will play the network's DHCP server role
  - b. Through DHCP and NETBIOS/WINS, it will assign IP addresses and names to the devices and make sure that special devices (e.g. a DIVUS KNX SERVER) are reachable from anywhere.
4. To open additional communication channels to/for custom devices, you can use special pre-sets or define your own new rules. See chapters 3.14, 6.5, 6.6 for details.

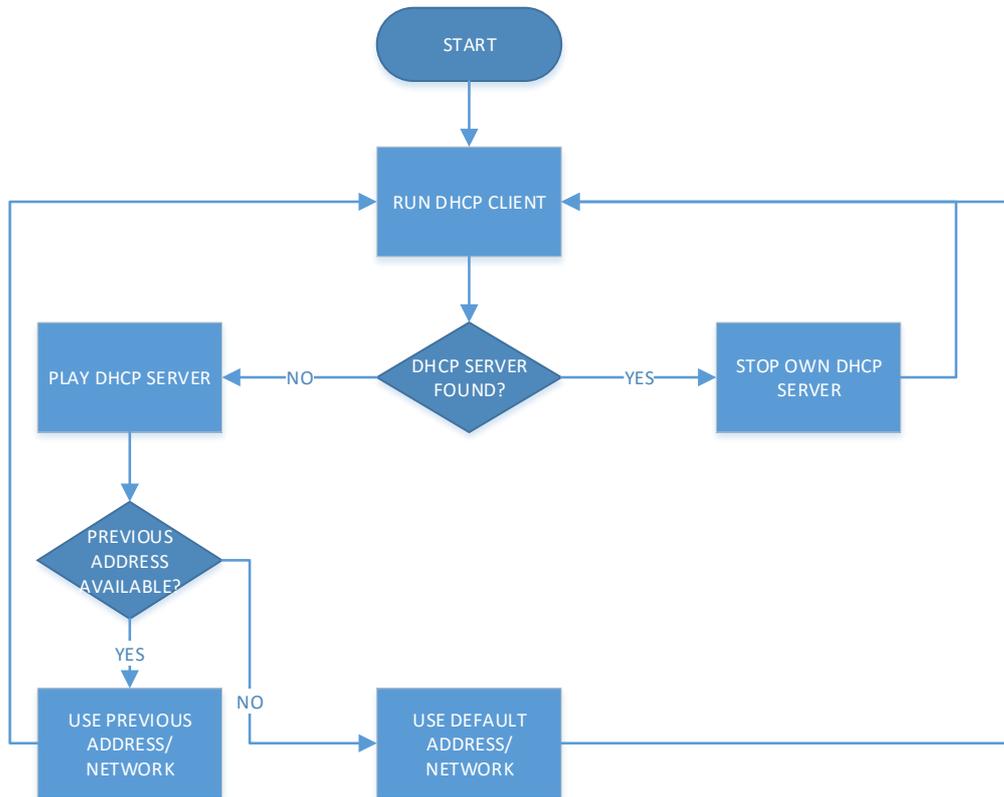
At this point, an isolated system is ready to be used. A system where a router will follow in the future can also work with this configuration without any problems.

When the router is finally installed and connected, what happens to a previously configured system with a DIVUS HEARTBEAT?

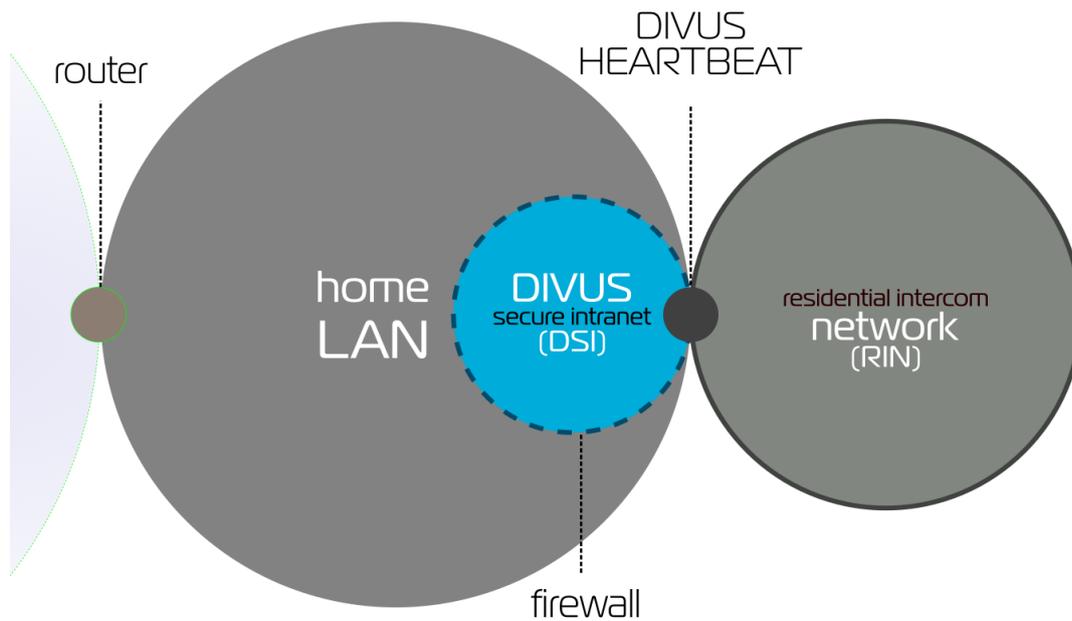
When the router is connected to the DIVUS HEARTBEAT:

- The DIVUS HEARTBEAT detects the new device and its roles
- The DIVUS HEARTBEAT will pass the general network management roles to the newcomer:
  - DHCP server role is passed to the router. This means that all the DHCP addresses leased will be renewed by another server which might also move all the devices to a completely different network.

- The DIVUS HEARTBEAT will continue to play the primary or secondary WINS server for the network. In this way, it will still be able to resolve calls to `dhb-heartbeat` to the desired underlying IP addresses.
- The DIVUS HEARTBEAT is able to switch from an isolated network (see 2.1.2) to a connected one (see 2.1.1) or vice-versa – every time it is needed:



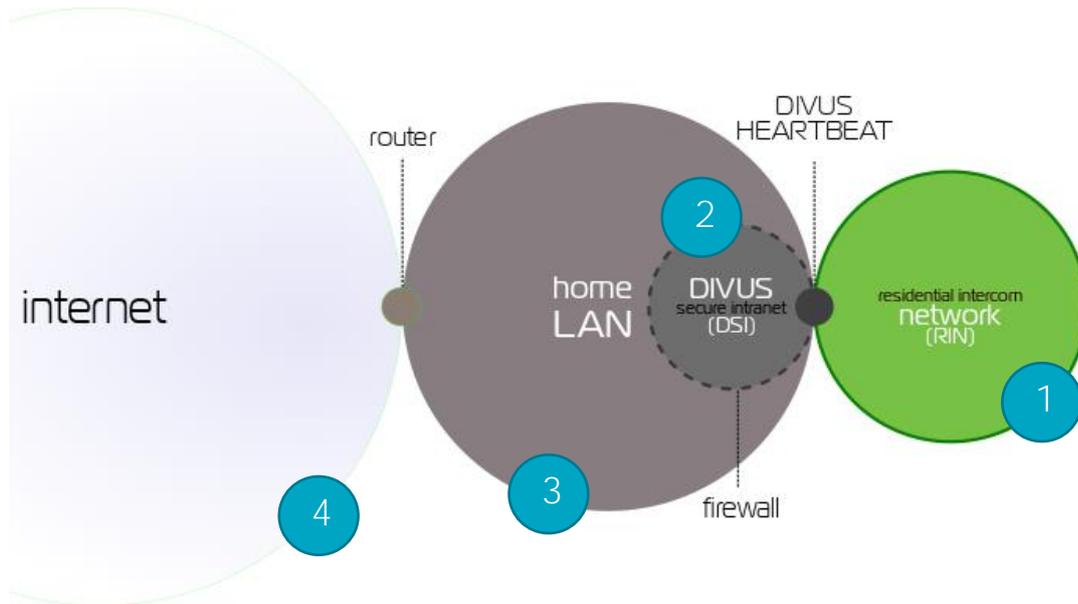
## 2.1.3 DIVUS SECURE INTRANET (DSI) SCHEME



The *DIVUS SECURE INTRANET* is the network reserved for your home automation and visualisation devices. Being a network managed by a dedicated switch and manager means having these advantages:

- A dedicated bandwidth for your home automation – it will not be influenced by the use of other networks (e.g. big downloads or streaming on a home LAN device)
- It will be safer
  - partly because it is in a separate network,
  - partly because there is a firewall between your home automation devices and your domestic LAN devices.
- Devices connected to your DSI are considered trustworthy and therefore have access to all other networks (and their devices)
- The DSI is part of the same network where your domestic LAN devices are. But the communication from the home LAN to the DSI is possible only if custom rules are defined on the DIVUS HEARTBEAT to allow it. See chapter 6.5 and 6.6.

## 2.1.4 RESIDENTIAL INTERCOM NETWORK (RIN) SCHEME



These are the relations the residential intercom network has:

- 1) *EXTERNAL UNITS* and security cams should be placed inside the **RIN** to take advantage of its special security. Devices placed in the **RIN** can't reach any other device of the other networks.<sup>1</sup> They only can reach the DIVUS HEARTBEAT on its VoIP port.
- 2) Usually the devices of the RIN will communicate with those of the **DIVUS SECURE Intranet**. The VoIP communication is managed by the DIVUS HEARTBEAT which all the devices in the network can reach. Devices placed inside the DIVUS SECURE intranet are considered trustworthy and can therefore reach all other devices. So, showing e.g. the camera stream of an EXTERNAL UNIT on a DIVUS TOUCHZONE placed in the *DSI* is not a problem, it will be accessible per default.
- 3) A device from the home LAN might want to access something inside the RIN. An example may be a mobile device to be connected to the VoIP system and therefore needing access to the HEARTBEAT and to the camera's IP address. For this to work, a firewall rule must be defined on the DIVUS HEARTBEAT. See chapter 6.5 for details.
- 4) Finally, also devices from the internet might be configured to get in touch with those from the RIN. That can happen when the user needs e.g. a mobile device to be part of the VoIP system also from outside the LAN.

See chapter 6.7 for the setup of a remote access to the intercom system.

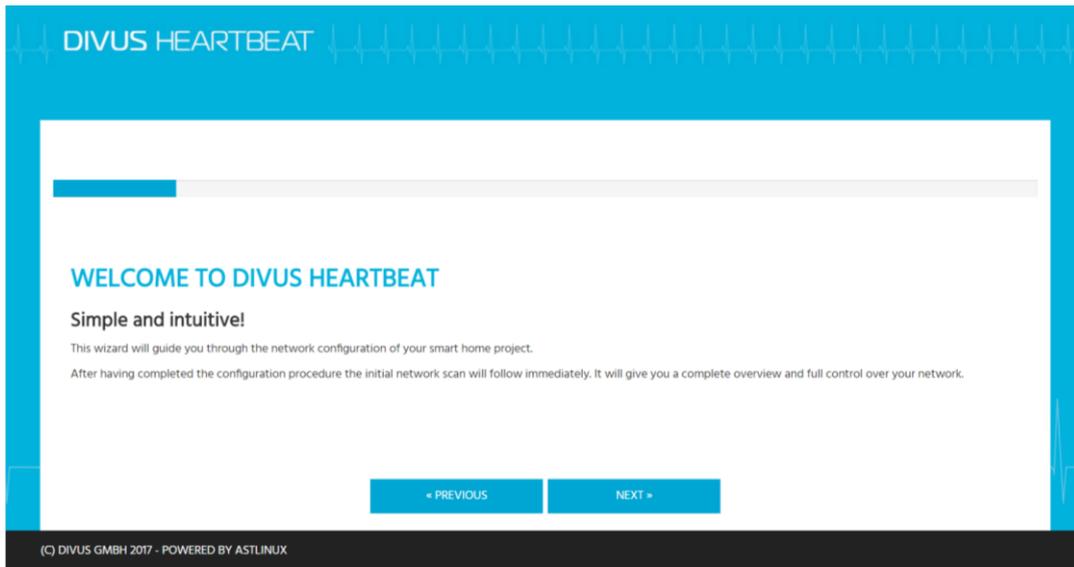
<sup>1</sup> This means they can't contact other devices in any way. They still will be able to respond to other devices if contacted by them first.

# 3 Web interface

## 3.1 FIRST ACCESS: THE SETUP WIZARD

The first time the device is started, it will show the setup wizard which is used to store the most important information about the device and the project. Choose between English (default) or German to immediately switch the GUI's language to that language.

### 3.1.1 STEP 1 - START



## 3.1.2 STEP 2 – LICENSE AGREEMENT

Read and accept the license terms checking the checkbox in step 2:

**DIVUS HEARTBEAT**

---

## DIVUS HEARTBEAT END USER LICENSE AGREEMENT

Version 1.0

terms or any purchase orders and any other communications or advertising with respect to the Software. You acknowledge that this Agreement is a complete statement of the agreement between you and DIVUS with respect to the DIVUS Product, and that there are no other prior or contemporaneous understandings, promises, representations, or descriptions with respect to the DIVUS Product.

6.2 Waiver and Modification. No failure of either party to exercise or enforce any of its rights under this Agreement will act as a waiver of those rights. This Agreement may only be modified, or any rights under it waived, by a written document executed by the party against which it is asserted.

6.3 Severability. If any provision of this Agreement is found void or unenforceable, it will be enforced to the maximum extent permissible, and the legality and enforceability of the other provisions of this Agreement will not be affected.

the DIVUS Product, and that there are no other prior or contemporaneous understandings, promises, representations, or descriptions with respect to the DIVUS Product.

6.2 Waiver and Modification. No failure of either party to exercise or enforce any of its rights under this Agreement will act as a waiver of those rights. This Agreement may only be modified, or any rights under it waived, by a written document executed by the party against which it is asserted.

6.3 Severability. If any provision of this Agreement is found void or unenforceable, it will be enforced to the maximum extent permissible, and the legality and enforceability of the other provisions of this Agreement will not be affected.

6.4 Governing Law and Jurisdiction. This Agreement and any legal matters that may arise out of or in connection with this Agreement shall be subject to,

I accept the terms of this agreement

[< PREVIOUS](#) [NEXT >](#)

(C) DIVUS GMBH 2017 - POWERED BY ASTLINUX

## 3.1.3 STEP 3 – SYSTEM INTEGRATOR DETAILS

Fill in at least the fields with a \* about the system integrator, but we recommend taking the time to fill out all the fields to have complete and clear reports thereafter.

**DIVUS HEARTBEAT**

### SYSTEM INTEGRATOR DETAILS

Name*	<input type="text" value="System Integrator Name"/>
Company*	<input type="text" value="Company Name"/>
Address	<input type="text"/>
City	<input type="text"/>
Postal code	<input type="text"/>
Country	<input type="text"/>
Phone number	<input type="text"/>
E-mail address*	<input type="text" value="integrator@system.xy"/>
Login name*	<input type="text" value="sysint"/>
Password*	<input type="password" value="*****"/>
Confirm password*	<input type="password" value="*****"/>

[← PREVIOUS](#)   [NEXT →](#)

© DIVUS GMBH 2017 - POWERED BY ASTLINUX

## 3.1.4 STEP 4 – CUSTOMER DETAILS

Again, fill in at least the fields with a \* about the customer (again we recommend to fill out all the fields)

**DIVUS HEARTBEAT**

### CUSTOMER DETAILS

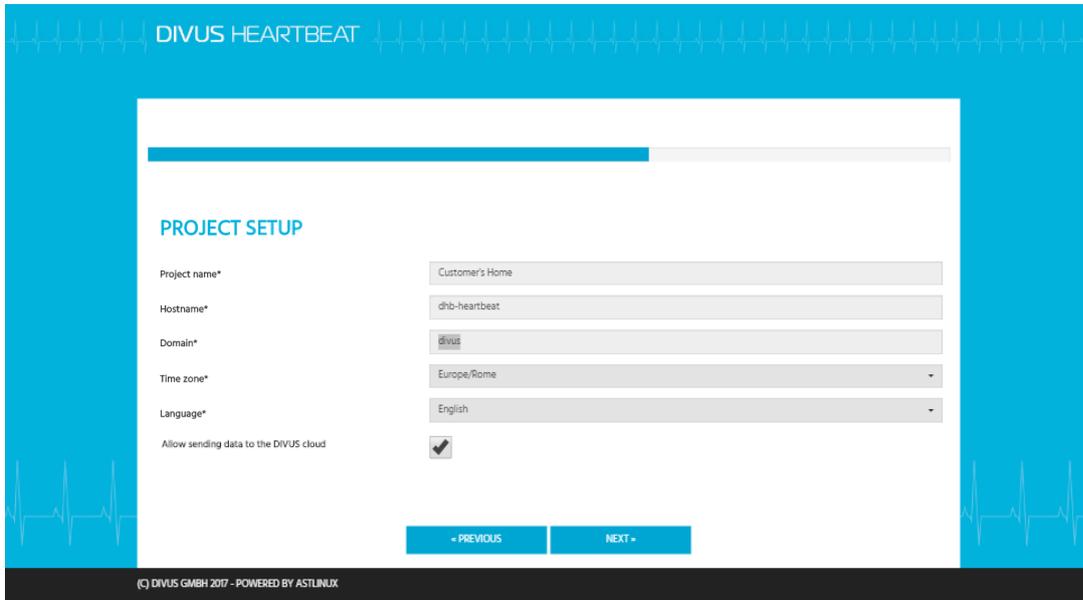
Name*	Customer Name
Company	
Address	
City	
Postal code	
Country*	Country
Phone number	
E-mail address*	customer@home.xy
Login name*	customer
Password*	*****
Confirm password*	*****

[← PREVIOUS](#) [NEXT →](#)

(C) DIVUS GMBH 2017 - POWERED BY ASTLINUX

### 3.1.5 STEP 5 – PROJECT SETUP

Choose the project's name here. The other fields have default values which may be changed if necessary. If more than one DIVUS HEARTBEAT are in the same network, their hostnames must be different to avoid issues. You may change `dhb-heartbeat` to something else, but the system will put "dhb-" in front and cut the inserted string's end if longer than 15 characters total. Alternatively, you may also use `dhb-<serial number>` (e.g. `dhb-21234`) as hostname. You can find the serial number on the status page.



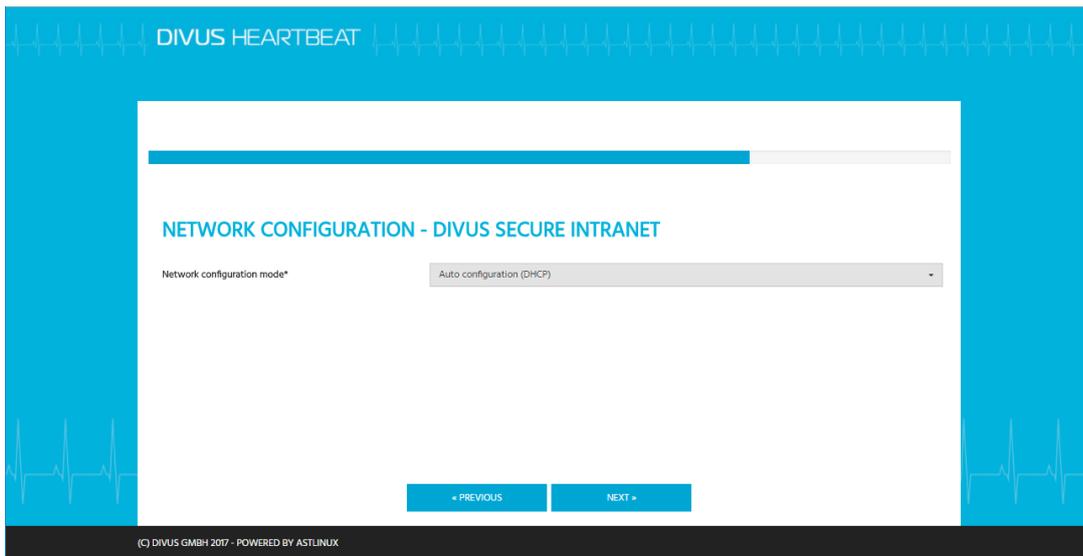
The screenshot shows the 'PROJECT SETUP' screen in the DIVUS HEARTBEAT interface. The page has a blue header with the text 'DIVUS HEARTBEAT' and a white content area. A progress bar at the top is partially filled. The form contains the following fields:

- Project name\*: Customer's Home
- Hostname\*: dhb-heartbeat
- Domain\*: divus
- Time zone\*: Europe/Rome
- Language\*: English
- Allow sending data to the DIVUS cloud:

At the bottom of the form are two buttons: '< PREVIOUS' and 'NEXT >'. The footer of the page reads '(C) DIVUS GMBH 2017 - POWERED BY ASTLINUX'.

### 3.1.6 STEP 6 – NETWORK CONFIGURATION - DIVUS SECURE INTRANET

Here you can change the network configuration. To take full advantage of DIVUS HEARTBEAT's advanced features we recommend to use the default „Auto configuration (DHCP)“ setting.



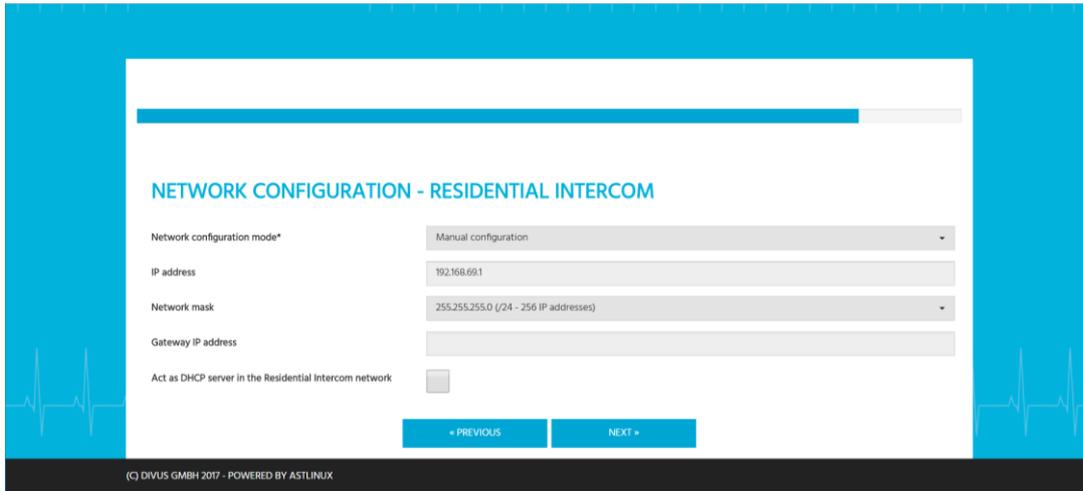
The screenshot shows the 'NETWORK CONFIGURATION - DIVUS SECURE INTRANET' screen in the DIVUS HEARTBEAT interface. The page has a blue header with the text 'DIVUS HEARTBEAT' and a white content area. A progress bar at the top is partially filled. The form contains the following field:

- Network configuration mode\*: Auto configuration (DHCP)

At the bottom of the form are two buttons: '< PREVIOUS' and 'NEXT >'. The footer of the page reads '(C) DIVUS GMBH 2017 - POWERED BY ASTLINUX'.

### 3.1.7 STEP 7 – NETWORK CONFIGURATION - RESIDENTIAL INTERCOM

Usually you may keep these default settings for the RIN and therefore use static addresses of the 192.168.69.0 network, or change them to your special needs. If needed, you may also activate a DHCP server or a DHCP client function. The recommended setting is using static IP addresses for this network.

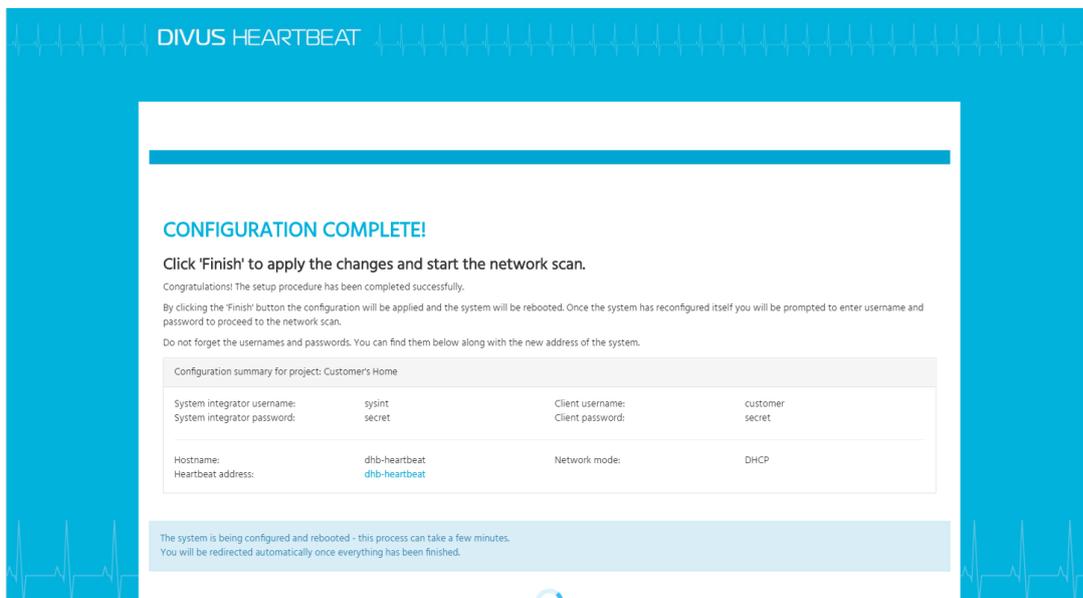


If using the DHCP server function for the RIN, please make sure that there is no other device in this network having an active DHCP service!

### 3.1.8 STEP 8 – SUMMARY / LAST STEP

This last step shows the access data and the most important settings to be confirmed pushing the FINISH button. Please note that you have to remember these settings to access the web interface from here on!

After pushing the FINISH button, the system will reboot to apply all the settings.



### 3.1.9 NETWORK SCAN

The Network scan is started automatically after the setup wizard is completed. See 3.5 and 3.6 for further details.

## 3.2 SYSTEM STATUS PAGE

The first page in the menu is also the web interface’s homepage. It gives a general overview of the system’s state, with memory and disk usage, name and IP addresses, load, uptime and the latest system’s log.

**DIVUS HEARTBEAT**

SYSTEM - DIVUS NETWORK - SIP STATUS - LOGS - SETTINGS - SUPPORT

### System status

System details

PRODUCT	DIVUS Heartbeat 110	SERIAL NUMBER	12345
HOSTNAME	dhb-heartbeat	UPTIME	8 minutes, 38 seconds
OPERATING SYSTEM	Linux	ARCHITECTURE	x64
MEMORY	1974MB total, 945MB free	CPU	4x AMD GX-412TC SOC
SYSTEM LOAD	0.71, 0.43, 0.33		
DIVUS SECURE INTRANET IP ADDRESS	192.168.0.136/21	RESIDENTIAL INTERCOM IP ADDRESS	192.168.69.1/24

Disk usage

Filesystem	Size	Used	Available	Use%	Mounted on
/dev/ada1	511.0G	165.2M	346.4M	32%	/oldroot/odcom
/dev/ada3	56.2G	1.0G	52.3G	2%	/oldroot/mnt/asturw

Latest system logs

```

Aug 22 11:15:30 dhb-FS monit[2088]: 'dnsmasq' start: '/etc/init.d/dnsmasq start'
Aug 22 11:15:30 dhb-FS dnsmasq[2739]: started, version 2.78 cache-size 4096
Aug 22 11:15:30 dhb-FS dnsmasq[2739]: compile time options: IPV6 GNU-getopt DBus no-118n no-IGMP DHCP DHCPv6 no-Lua no-IPF no-contrack ipset
Aug 22 11:15:30 dhb-FS dnsmasq-dhcp[2739]: DHCP relay from 192.168.0.136 to 192.168.5.22 via br0
Aug 22 11:15:30 dhb-FS dnsmasq[2739]: using local addresses only for domain interel.local
Aug 22 11:15:30 dhb-FS dnsmasq[2739]: reading /tmp/etc/resolv-wq.conf
Aug 22 11:15:30 dhb-FS dnsmasq[2739]: using local addresses only for domain interel.local
Aug 22 11:15:30 dhb-FS dnsmasq[2739]: using nameserver 192.168.5.22#53
Aug 22 11:15:30 dhb-FS dnsmasq[2739]: read /etc/hosts - 2 addresses
Aug 22 11:15:30 dhb-FS avahi-daemon[2744]: Found user 'avahi' (UID 70) and group 'avahi' (GID 70).
    
```

## 3.3 SYSTEM – UPGRADE

If the DIVUS HEARTBEAT has access to the internet, it will check whether there is a new firmware version available online when you open this page. If so, you will be informed and may start the upgrade procedure by pushing the button.

**DIVUS HEARTBEAT**

SYSTEM - DIVUS NETWORK - SIP STATUS - LOGS - SETTINGS - SUPPORT

### System upgrade

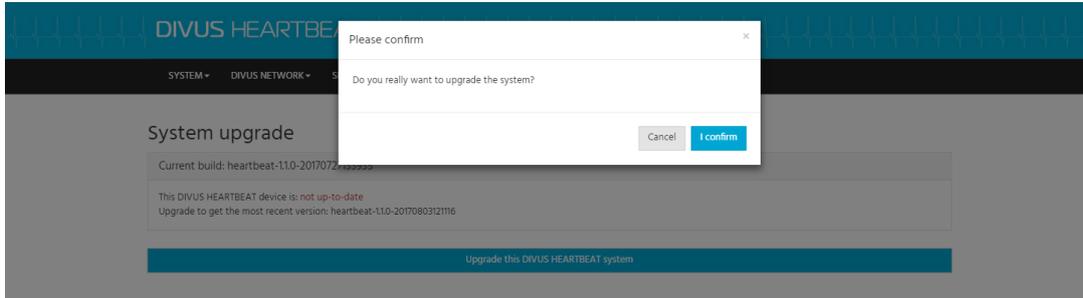
Current build: heartbeat-11.0-20170726004411

This DIVUS HEARTBEAT device is: **not up-to-date**  
 Upgrade to get the most recent version: heartbeat-11.0-20170803121116

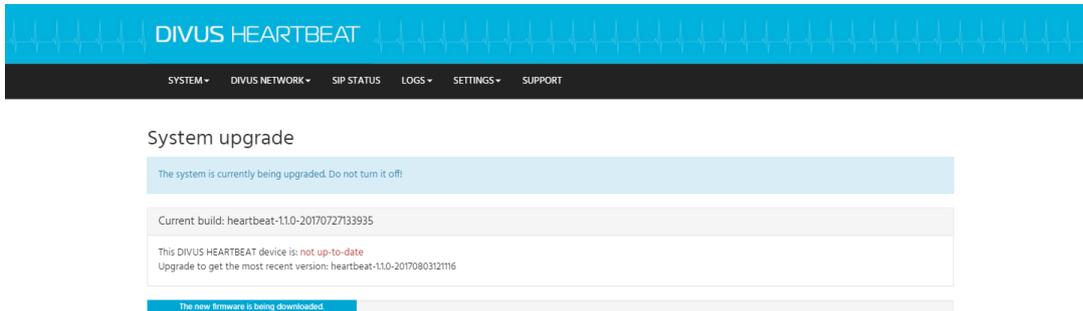
Upgrade this DIVUS HEARTBEAT system

### 3.3.1 UPGRADE PROCEDURE

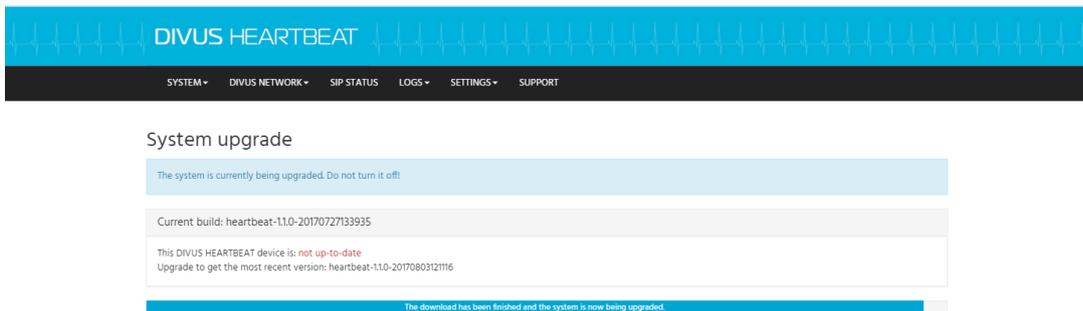
1. When you push the upgrade button, confirm the upcoming alert window with *I confirm* or interrupt the procedure choosing *CANCEL*. Note that your configuration will remain unchanged after an upgrade.



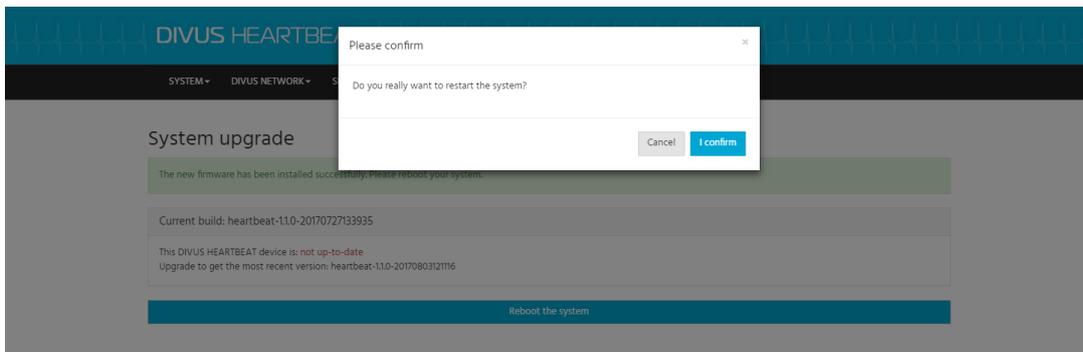
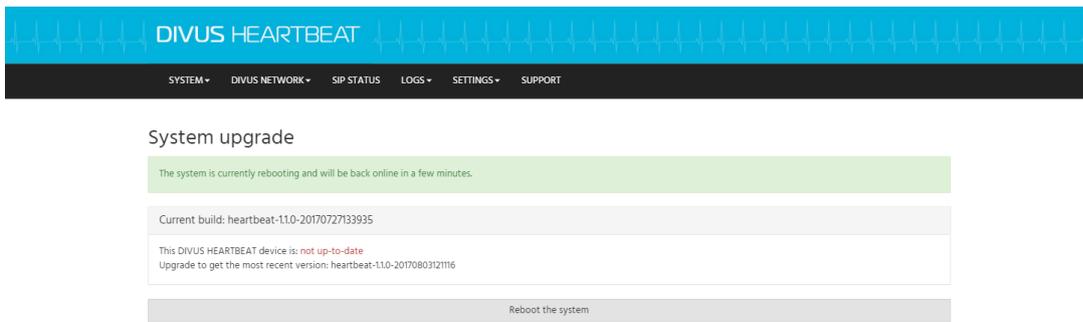
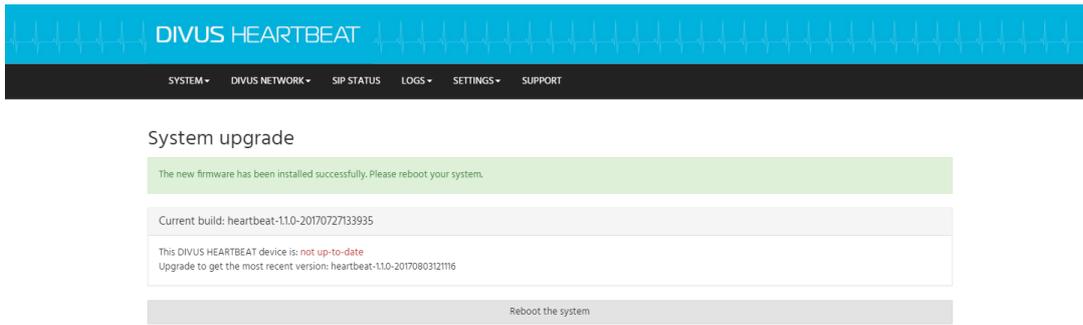
2. After confirmation, the download will start...



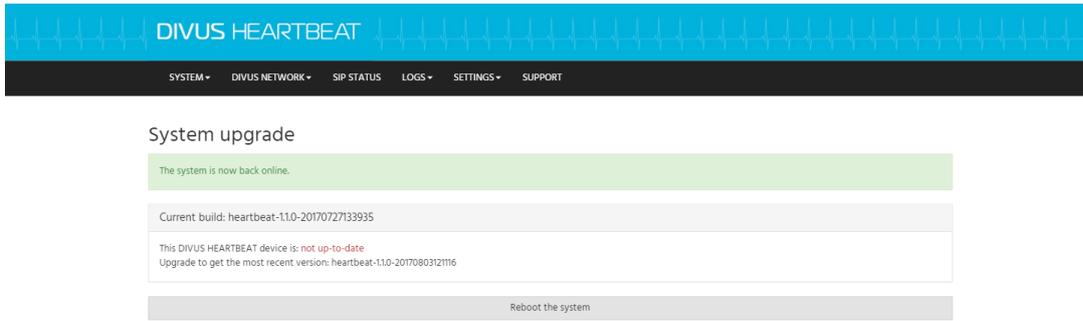
...and the upgrade will be processed.



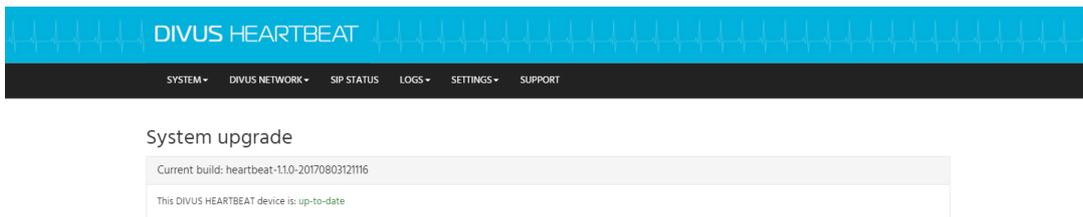
3. After the upgrade, you'll be prompted to reboot. Confirm the reboot.



4. You will be informed when the device is rebooted.

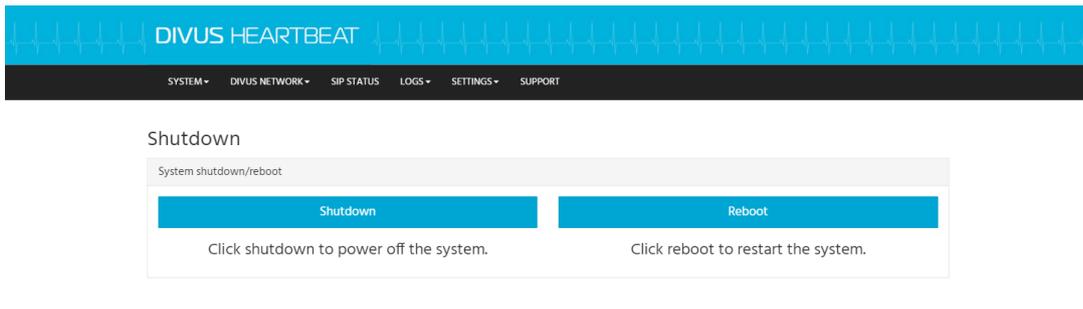


Please refresh the browser window. The reloaded page should then look like this:



### 3.4 SYSTEM – SHUTDOWN

This page has buttons to reboot or shutdown the device.



**Note:** The DIVUS HEARTBEAT uses acoustic signals when shutting down and when booted. The shutting down signal is *high-low*, the boot up signal is *medium-low-medium-high*. Please always wait for the boot up signal (if on site) to be sure the system is completely up and running – specially before a new network scan.

### 3.5 DIVUS NETWORK – REPORT PAGE

This page shows the network scan report, which is the result of the latest network scan (see 3.6). It shows a graphical representation of all the devices which were detected and the detailed information about each of them in tables.

This information contains a device's:

- Hostname

- IP address
- MAC address
- The port they are connected to (on the HEARTBEAT or on the DMS)
- Depending on the type of device, other details e.g. software/firmware version, uptime, language etc.



**Note:** During the scan, DIVUS devices use the SNMP protocol to offer more details about their status and settings than third party devices. Therefore, implementing DIVUS devices allows the DIVUS HEARTBEAT to show its full potential. Third party devices may offer basic information i.e. their IP address, name and of course the used network port.

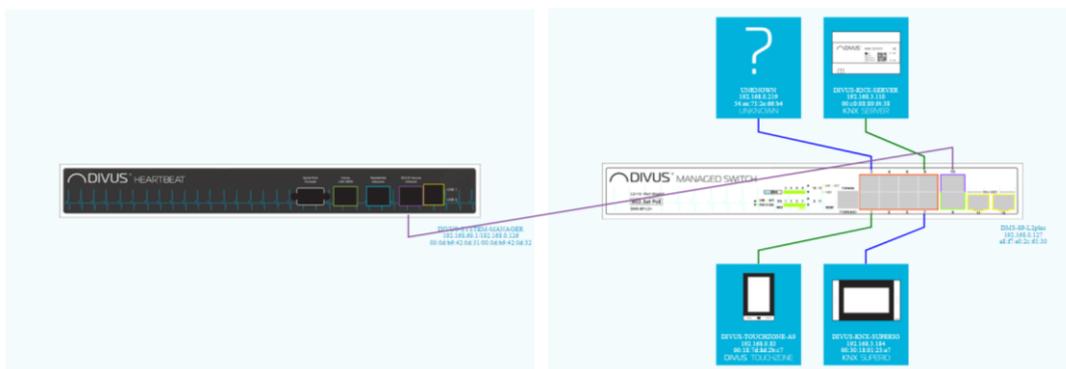
### 3.5.1 THE GRAPHICAL SCHEME

The graphical scheme shows the main device (a DIVUS HEARTBEAT or a DIVUS MANAGED SWITCH) and all the devices connected to it disposed around it. A line shows which device is connected to which port. Moreover, a colour coding is used for the lines to show the connection's bandwidth:

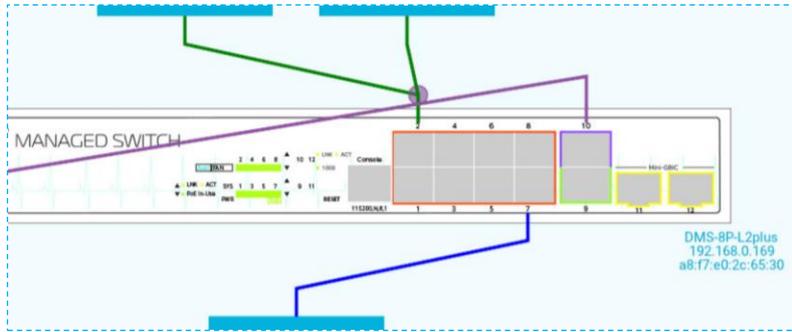
GREEN LINE	1000 Mbit/s
BLUE LINE	100 Mbit/s
PURPLE LINE	Manager-to-switch or switch-to-switch connection (1000 Mbit/s)

So usually there will be two schemes with light blue background, showing the *MANAGER* with its connected devices (the first) and the *MANAGED SWITCH* with its connected devices (the second). If other switches are attached, additional schemes will be added forming one big network scheme.

DIVUS devices will be recognized and shown with a matching image. Unrecognized devices will be shown with a default question mark symbol.



If third party switches are detected, a node (purple dot) is shown on the connection line, signalling that more than one device is connected to the shown port.



The two main devices (MANAGER and MANAGED SWITCH) are shown with their name, IP and MAC address.

Just looking at the graphical scheme, you immediately have a visual overview of the status of the network and see which device is connected to which port.



**Note:** If a device was not detected at all, please first check the physical connection: the cause might be the cable or the cable's plugs. Other possible cause: the device might be on a different network using a static IP address. See chapter 6.1 on how to deal with such a case.

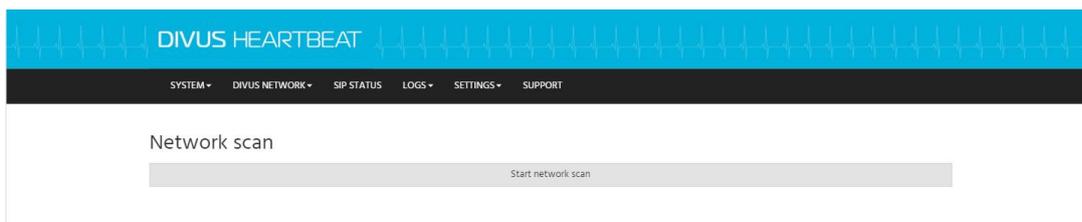
### 3.5.2 THE PDF FILE OF THE REPORT

The PDF file contains the same information as the report on the website plus some extra details: the title page shows the project name and names and addresses of system integrator and customer, and there are special pages showing the firewall and port forwarding rules which may have been added. So, the report file is almost like a paper version of a backup. Using it you will be able to

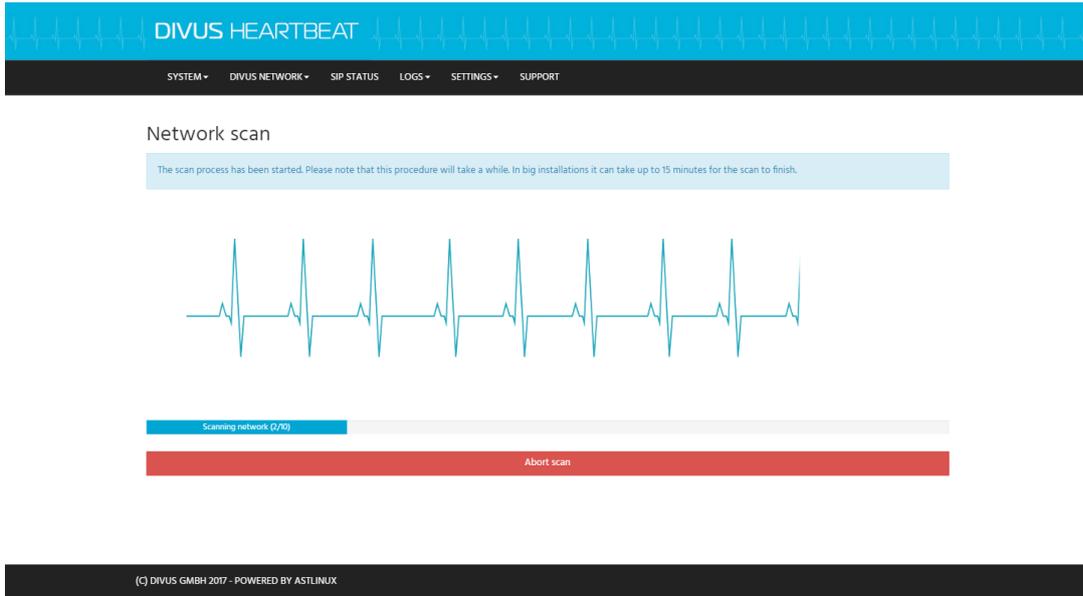
- See / remember what exactly the network state was at the time of the scan
- Proof your work on site clearly
- Check whether something was changed, is missing or isn't working compared to the time of the scan

## 3.6 DIVUS NETWORK – PERFORM SCAN PAGE

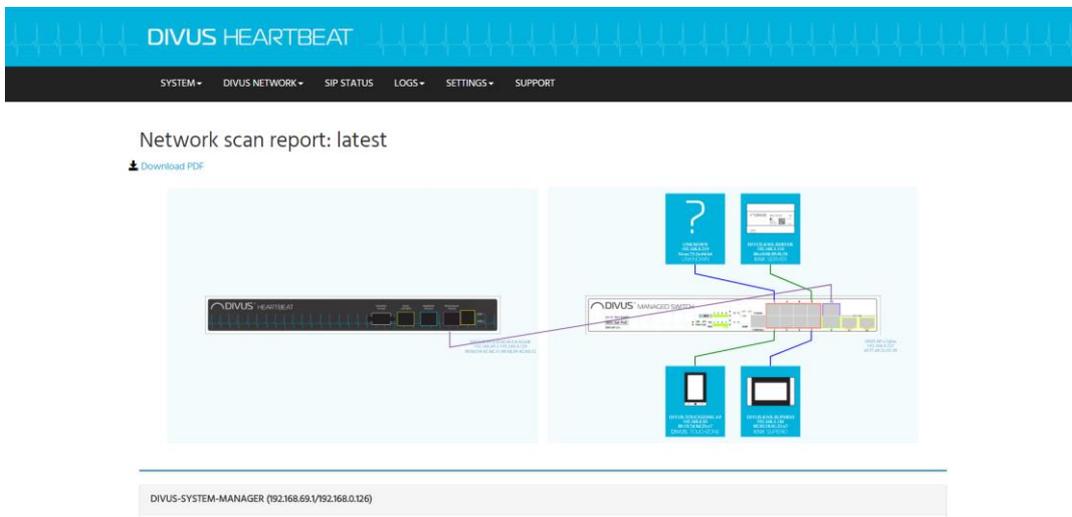
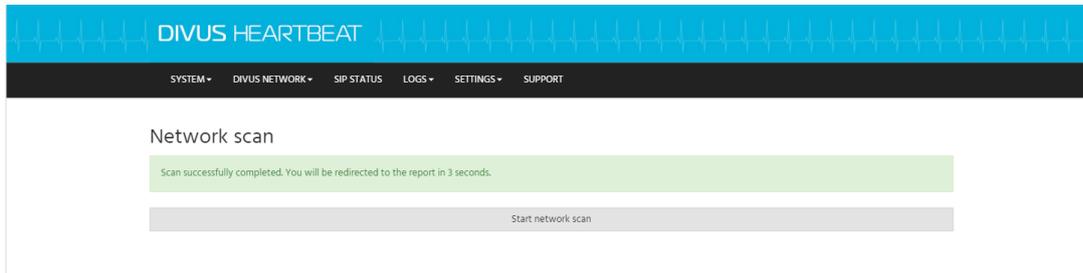
This page is used to start a new network scan.



Once you pushed the Scan button, you will see the progress of the scan graphically through a progress bar. Depending on the number of connected devices, the scan may need several minutes to complete.

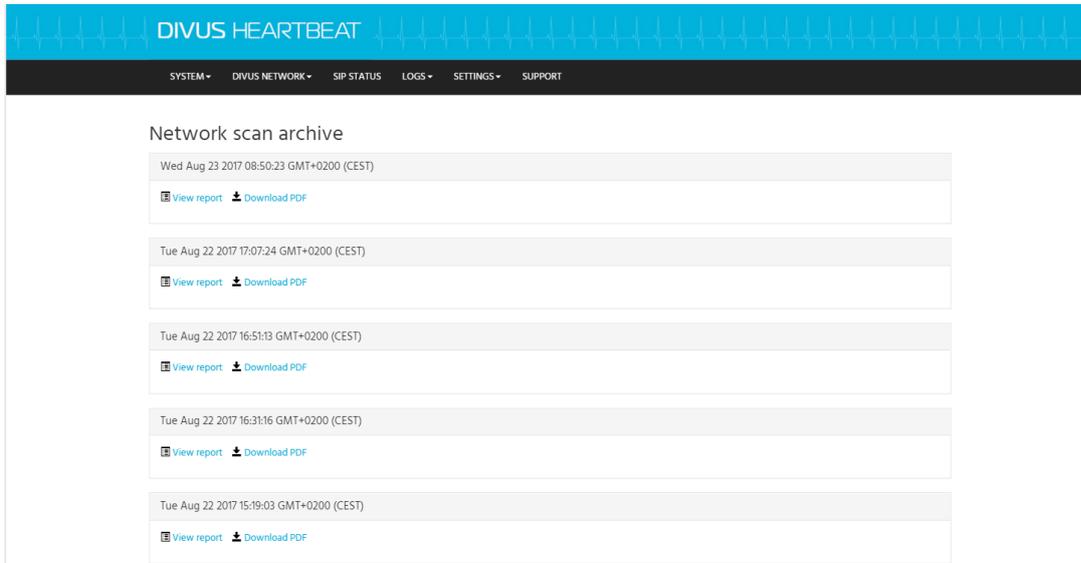


Once completed, you'll be redirected automatically to the report page.



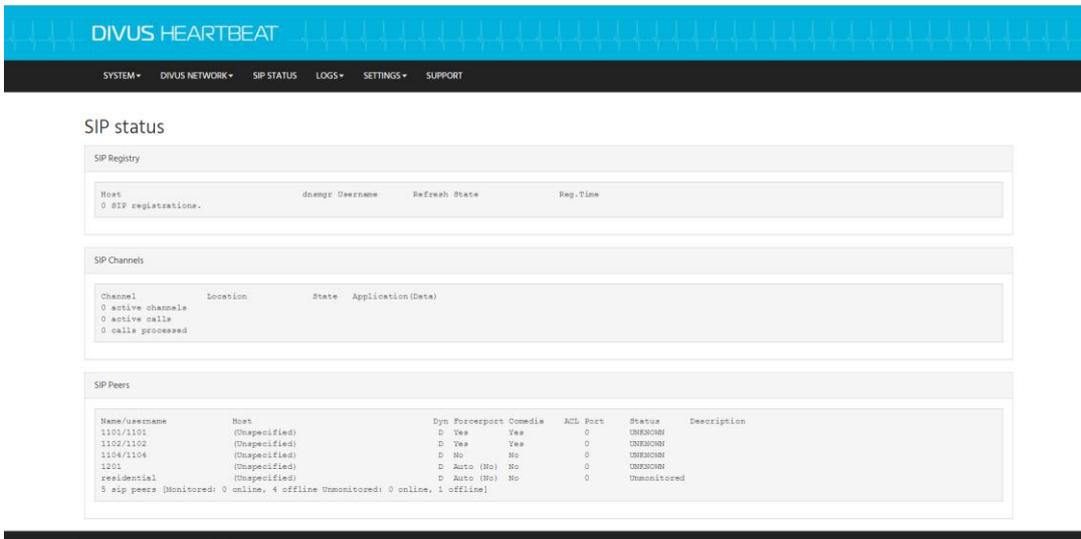
### 3.7 DIVUS NETWORK – ARCHIVE PAGE

Here you can find a list of the network scans and can open them or download them as PDF files.



### 3.8 SIP STATUS PAGE

This page shows the status of your intercom system (Registry, Channels and Peers) if you configured the DIVUS HEARTBEAT as VoIP/SIP server. Specially the *Status* column of the SIP Peers table is useful to see if all devices are registered and reachable.



---

### 3.9 LOGS – SWITCH LOGS PAGE

---

The MANAGED SWITCH logs any activity on its ports. Although these activities are limited to a port being active or not and using PoE or not, it may be very useful for troubleshooting devices. If e.g. a device reboots, it will be logged.

There is a powerful filtering / searching function which can be used to show only the interesting entries. Please refer to chapter 6.2 for details and examples about log filtering.

---

### 3.10 LOGS – VOIP/SIP LOGS PAGE

---

The SIP/VoIP server shows its log here. Also see chapter 6.2 for the filtering / searching function.

---

### 3.11 LOGS – CALL LOGS PAGE

---

All calls are logged: their time and duration can be found here. See chapter 6.2 for the filtering / searching function.

---

### 3.12 SETTINGS – SYSTEM PAGE

---

These settings (project name, hostname, domain, time zone and language) were shown during the first setup. If you have to change them later on, you can do it here.

**DIVUS HEARTBEAT**

SYSTEM ▾ DIVUS NETWORK ▾ SIP STATUS LOGS ▾ SETTINGS ▾ SUPPORT

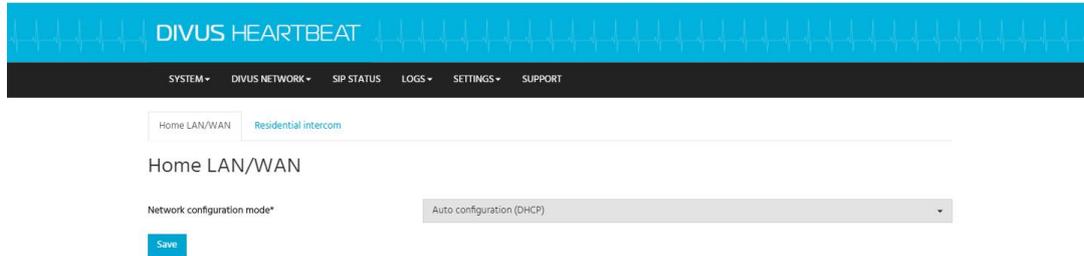
#### System settings

Project name*	Customer's Home
Hostname*	dib-8
Domain*	divus
Time zone*	Europe/Rome ▾
Language*	English ▾
Allow sending data to the DIVUS cloud	<input checked="" type="checkbox"/>

[Save](#)

### 3.13 SETTINGS – NETWORK SETTINGS PAGE

The network settings for the home LAN or the RIN can be changed here if necessary. If you already chose the correct settings during the first setup wizard, you don't have to change anything here.



r

#### 3.13.1 DHCP

##### 3.13.1.1 DSI

For the DIVUS HEARTBEAT to automatically manage a network also when changes are applied to the network structure, it is mandatory to use DHCP and to avoid using static IP addresses for the DSI network. Although it is possible to use fixed addresses, we strongly recommend not to use them. The role of DHCP server can be assigned to the DIVUS HEARTBEAT, but it will automatically pass that role to another device if such a device is detected. For this reason, the DIVUS HEARTBEAT continuously listens on the network for third-party DHCP activity – both when it is playing the DHCP server role and when it is itself a DHCP client of another device running a DHCP server. This allows the DIVUS HEARTBEAT to switch roles as required. From server to client if another server is there, from client to server if a previous server does not respond anymore.

##### 3.13.1.2 RIN

Let's see the possible scenarios and the best settings for each of them:

#### 1. One single device connected to the Residential Intercom network

In this case, the best solution is to set the RIN to "Manual configuration" and to set a static IP address on the device (e.g. 192.168.69.10)

#### 2. Two or more devices connected to a DIVUS MANAGED SWITCH on the RIN

The address of the DMS can't be set to static. Therefore, we have these possible cases:

- A. Setting the RIN to "Manual configuration" and activating the DHCP server function will make all devices reachable. Of course, all devices must be set to DHCP mode. Pre-requisite is that no other device has a running DHCP service in the RIN. After activating the DHCP server checkbox you will be required to define the range of addresses. Keep in mind that the address of the manager (IP address field), the net mask field and the DHCP range fields are all related and are checked to be correct on submission. The Gateway address field may be left empty.
- B. Another device has a running DHCP service. In this case, setting the RIN to "Auto configuration (DHCP)" will activate the DHCP client function, making all the devices reachable. Of course, all devices must be set to DHCP mode.

- C. Setting the RIN to “Manual configuration” will make the DMS invisible to the Manager. It will act as a normal, unmanaged switch. You will lose the details about the DMS in the network scans, where it will be shown as an unknown switch, and the DMS logs will also not be available. Nonetheless, the client devices, once set to a static IP address of the chosen IP network, will work normally. If you need to set this network to use static addresses, this is currently the only possibility with a DMS.

### 3. Two or more devices connected to a third-party switch on the RIN

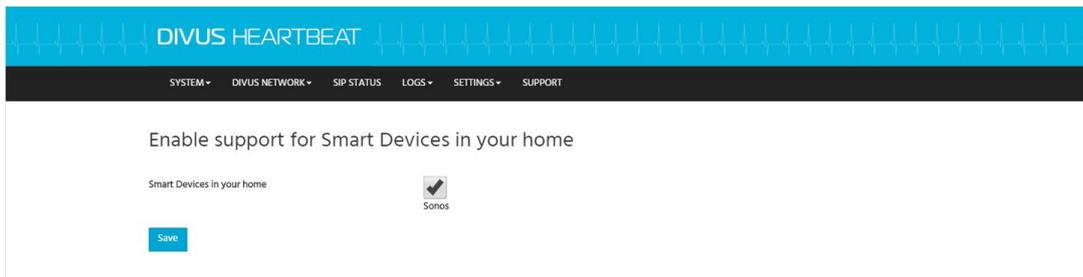
If you use a third-party switch to connect your devices to the RIN, it will be shown as an unknown switch and you will lose the functionalities described in 2-C. above. Apart from that, everything else will be the same as described above.

---

#### 3.14 SETTINGS – SMART DEVICES PAGE

---

This page allows to activate some special types of devices which are often used in smart buildings and use specific network ports and protocols. The list of supported devices will grow in time.



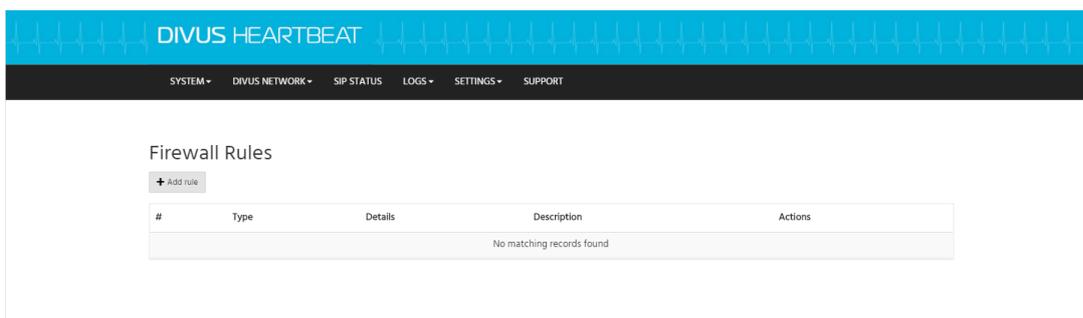
If you can't find your smart device type listed here, you still can integrate it knowing its communication channels and protocols and creating corresponding firewall and / or port forwarding rules. See chapters 6.5, 6.6

---

#### 3.15 SETTINGS – FIREWALL RULES PAGE

---

This page is used to manage the firewall rules of the DIVUS HEARTBEAT.



When you push the “+ Add rule” button, the form to define a new rule appears. For detailed instructions on the creation of firewall rules, please see chapter 6.5.



Firewall rule editor

Firewall rule type*	Home Network to DIVUS Secure Intranet
Source IP address/range	
Destination IP address/range	
Protocol*	All
Source port(s)	
Destination port(s)	
Policy*	Allow
Description	
Enabled	<input type="checkbox"/>

Save

## 3.16 SETTINGS – PORT FORWARDING PAGE

In a way similar to the FIREWALL RULES Page, you may add new port forwardings using the “Add rule” button.

### Port Forwarding Rules

[+ Add rule](#)

#	Interface	Details	Description	Actions
No matching records found				

(C) DIVUS GMBH 2017 - POWERED BY ASTLINUX

Given the special name resolution strategy adopted for the DIVUS HEARTBEAT and its networks, port forwarding plays an important role. If you use a port forwarding on the DIVUS HEARTBEAT, it means you can use the `dhb-heartbeat` name and a chosen port instead of using an IP address which might change due to network changes (e.g. a new router) in the future. So, if a device in the DSI has IP address `192.168.0.5` and some service on TCP port `81`, you may want to reach it calling `dhb-heartbeat:9000` after having added this rule:

*Incoming interface:* `All` (or one specific network)

*Protocol:* `TCP`

*Incoming port:* `9000`

*Source IP address/range:* e.g. `192.168.0.0/24` which means all `192.168.0.x` devices

*Destination IP address:* `192.168.0.5`

*Destination Port:* `81`

**Note:** If you use a DIVUS KNX SERVER, the DIVUS HEARTBEAT will recognize it during the network scan and will automatically add some special rules, so you don't have to add them manually.

---

### 3.17 SETTINGS – SIP SETTINGS PAGE

---

Here you get access to the two main configuration files for the SIP / VoIP server function.

To understand the predefined numbering scheme, see chapter 4.2. To see how to edit accounts or create group calls, see chapter 6.3 and 6.4

# 4 Intercom

Intercom allows to have voice and video communication; mainly for door opening but also for room to room communication. The following descriptions and explanations are limited to devices supporting the SIP standard for audio and IP cameras for video – all using a TCP/IP network for interconnections. A typical setup could look like this:



For most common cases, the DIVUS HEARTBEAT may be used as a plug and play VoIP server, meaning that just setting the clients' configurations using our default configuration scheme will cause them to just connect and work – without any intervention on the DIVUS HEARTBEAT's configuration itself.

The DIVUS HEARTBEAT uses a very flexible scheme to allow any complexity of intercom systems. Please read the following part carefully to understand and use the scheme for all the devices you are going to setup.

---

## 4.1 GENERAL DEFINITIONS

---

1. Even the most complex intercom structure builds up from a default base unit (see 4.2.1). This default unit (usually an apartment) has internal devices

connected to the unit's DIVUS HEARTBEAT. For simplicity and reference, we'll call this **ZONE 1**.

2. Moreover, this unit may have an external unit for calls from the floor's door or from the house's door – but still a device for the specific unit/apartment. We define this device as belonging to **ZONE 2**. (So, each unit certainly has ZONE 1 devices and may also have ZONE 2 devices)
3. There usually will be one or more outdoor devices e.g. at the entry gate. We call these the **EXTERNAL UNITS**
4. In houses with a reception/concierge, there will also be custom devices allowed to call and be called by everyone.

---

## 4.2 GENERAL VOIP ACCOUNT SCHEME (FOR ZONE 1 AND ZONE 2)

---

The default configuration of the DIVUS HEARTBEAT's intercom system uses these schemes

Name	VoIP number / SIP Account	Default password
AABCC	AABCC	AABCC
Where A: unit number, starting from 1 e.g. 1, 24, 99 B: zone number, 1 or 2, where 1 means internal devices, 2 external devices C: device number, from 01 to 99		
13101 A: 13, B: 1, C: 01	13101	13101
14201 A: 14, B: 2, C: 01	14201	14201
1101 A: 1, B: 2, C: 01	1101	1101

So, 13101 defines device 01 of the internal devices of unit 13, while 1101 will call device 01 among the internal devices of unit 1. A unit will usually correspond to an apartment. For larger systems, this scheme might be changed slightly to e.g. AABCCC or AAABCC.

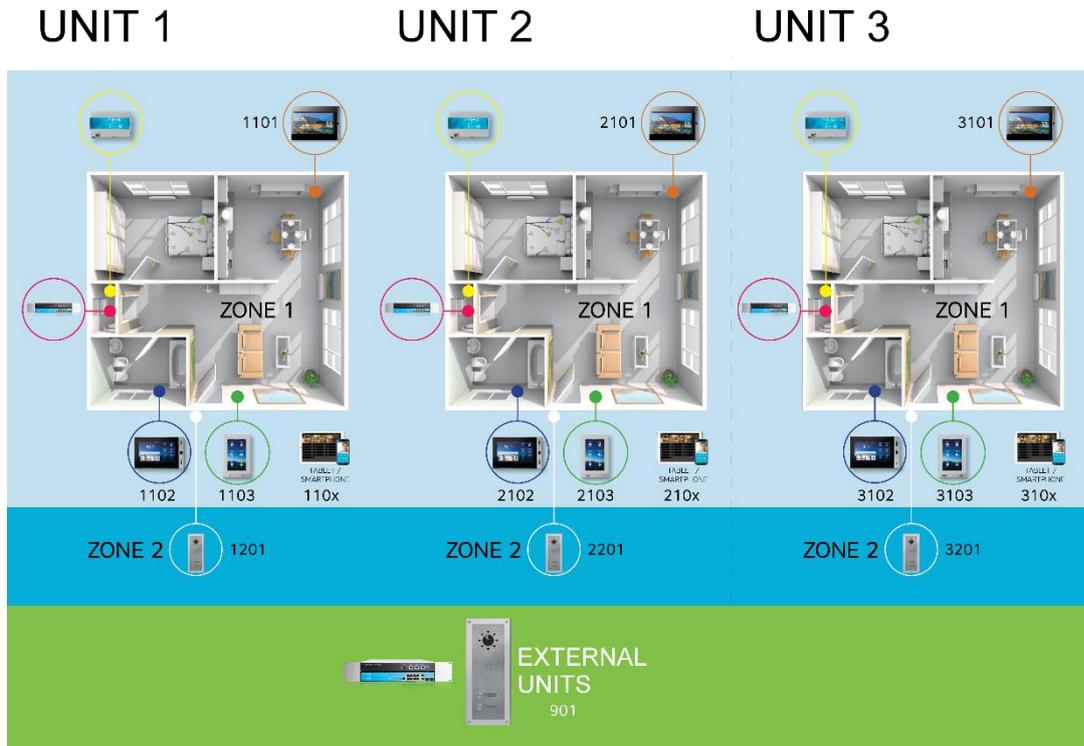
4.2.1 BASE UNIT

All systems will have a base unit with a set of predefined settings.

# UNIT 1



This base unit is then repeated like a building block for all the remaining units:



#### 4.3 VOIP ACCOUNTS FOR EXTERNAL UNITS

EXTERNAL UNITS use the same scheme used in DIVUS systems before the introduction of the DIVUS HEARTBEAT. So, the first EXTERNAL UNIT will have account 901 and password 901, the second 902 with password 902 and so on.

Name	VoIP number / SIP Account	Default password
901 External unit 1	901	901
902 External unit 2	902	902

---

#### 4.4 CONCIERGE / RECEPTION ACCOUNTS

---

If one or more concierge/reception posts are part of the intercom system, they will be numbered starting from 801 onwards.

Name	VoIP number / SIP Account	Default password
801 Concierge/reception unit 1	801	801
802 Concierge/reception unit 2	802	802



**Warning!** These default accounts are present to allow the first setup and testing to be quick and easy. Once the system is tested successfully, **you must change all the accounts' passwords** to guarantee that it is not accessed by external offenders. See chapter XX for details on editing your VoIP accounts.

For details on how to add, edit or delete single SIP accounts or group calls to your intercom system, go to chapter 6.3 and 6.4 respectively.

# 5 CLIENT Device setup for the DSI and the RIN

The following are recommended settings to fully take advantage of the DIVUS HEARTBEAT's potential. They are not mandatory though. If you prefer or if you are obliged, you may use IP addresses as usual. The advantage you would lose is the ability of the DIVUS HEARTBEAT to adapt to network changes without the need for your intervention – except very rare cases.

In all the settings below, the DIVUS HEARTBEAT's hostname is supposed to be the default `dhb-heartbeat`. If you changed the hostname, make sure to use that new name wherever `dhb-heartbeat` is shown here. The HEARTBEAT is also supposed to play the VoIP server role for intercom.

---

## 5.1 DIVUS TOUCHZONE

---

The DIVUS TOUCHZONE is supposed to be connected to the DSI (DIVUS Secure Intranet), like the KNX SERVER/KNX SUPERIO.

### OPTIMA App

From the DSI, use `dhb-heartbeat` as *IP address* and 3000 or 3001 as *Port*. If using 3001, check *SSL Protection* also. All other settings may be chosen as usual.

### VIDEOPHONE 4 App

Use `dhb-heartbeat` as *VoIP server IP*. All other settings remain the usual ones.

---

## 5.2 DIVUS SUPERIO AND OTHER WINDOWS BASED DIVUS DEVICES

---

As URL for the OPTIMA visualisation, use `http://dhb-heartbeat:3000` or `https://dhb-heartbeat:3001`.

As VoIP server in the VIDEOPHONE application, use `dhb-heartbeat` also.

---

## 5.3 DIVUS OPENDOOR

---

The default network for outdoor stations is the 192.168.69.0/24 network (i.e. the RIN). If you did not change it to something different, you should use:

192.168.69.1 as the VoIP server – using `dhb-heartbeat` is not supported currently!

As IP addresses for the single devices (OD-SIP and OD-Cam) you also must choose one of the IP addresses of this network e.g. 192.168.69.120 and 192.168.69.121 respectively.

All other settings remain the usual ones. Consider that the RIN network is generally accessible only from the DSN. If you need to access the OPENDOOR from elsewhere, you'd need to open a port for that.

---

## 5.4 KNX CONTROL DEVICES (KNX SERVER, KNX SUPERIO)

---

Nothing changes on the device's settings directly. To be able to communicate with the DIVUS HEARTBEAT and thus providing a set of information during the network scan, you need a device running OPTIMA version 2 in its newest release.

Also note that the VoIP server role, if previously held by this device, should be passed to the DIVUS HEARTBEAT.

If you necessarily need to run an embedded intercom client directly from the browser, in OPTIMA (on a Windows based panel or on the KNX SUPERIO), you may forward the VoIP server role to the HEARTBEAT from the OPTIMA intercom settings. Use 192.168.69.1 as VoIP server IP address in that case – using the hostname is not possible there.

### 5.4.1 SPECIAL RULES FOR DIVUS KNX SERVER AND KNX SUPERIO

The network scan is not only important for generating a report. It's also important because for these special devices (KNX SERVER and KNX SUPERIO) some rules are added automatically to facilitate the interaction with them. Here they are, each with a small explanation:

Destination	How to reach	Explanation
KNX SERVER/KNX SUPERIO on HTTP	<code>http://&lt;ip address&gt;</code>	Allow devices from the home network to access the KNX SERVER/KNX SUPERIO web interface on its ports 80 and 443 in the DSI.
KNX SERVER/KNX SUPERIO on HTTPS	<code>https://&lt;ip address&gt;</code>	
KNX SERVER/KNX SUPERIO on HTTP	<code>http://dhb-heartbeat:3000</code>	Allow to access the KNX SERVER/KNX SUPERIO using the DIVUS HEARTBEAT's name and these special ports: 3000 forwarding to 80, 3001 forwarding to 443. If there was a second KNX SERVER/KNX SUPERIO, it would use ports 3002 and 3003 respectively, and so on.
KNX SERVER/KNX SUPERIO on HTTPS	<code>https://dhb-heartbeat:3001</code>	

*So, which one should you use?*

Generally speaking, use https for higher security. Between using the IP address directly or using the forwarding over the DIVUS HEARTBEAT we recommend to use the latter for the best flexibility and for having a system as unattended as possible also after network changes. If this choice is not available/possible for you, choose the alternative.

---

## 5.5 THIRD-PARTY IP CAMS

---

You should set them to use a RIN IP address. Also see 5.2.3.

---

## 5.6 THIRD-PARTY CLIENT DEVICES (WITH ETHERNET INTERFACE)

---

Use the general rules detailed in the other sections: if the device supports it, use `dhb-heartbeat` as the server address/name. Otherwise, use an IP address of the appropriate network: DSI or RIN depending on the device type.

See chapter 5.1 for details about the possible ways to connect to a DIVUS KNX SERVER/KNX SUPERIO.

---

## 5.7 ANALOGUE THIRD-PARTY DEVICES

---

You may use the DIVUS Videophone-Box, a special device which can make an analogue door opening device with video and audio capable of making SIP calls to the inside and streaming video over a URL. You may check the manual [here](#) for further details. When configuring the parts about the VoIP server, see the recommendations in 5.2.6.

# 6 Advanced topics

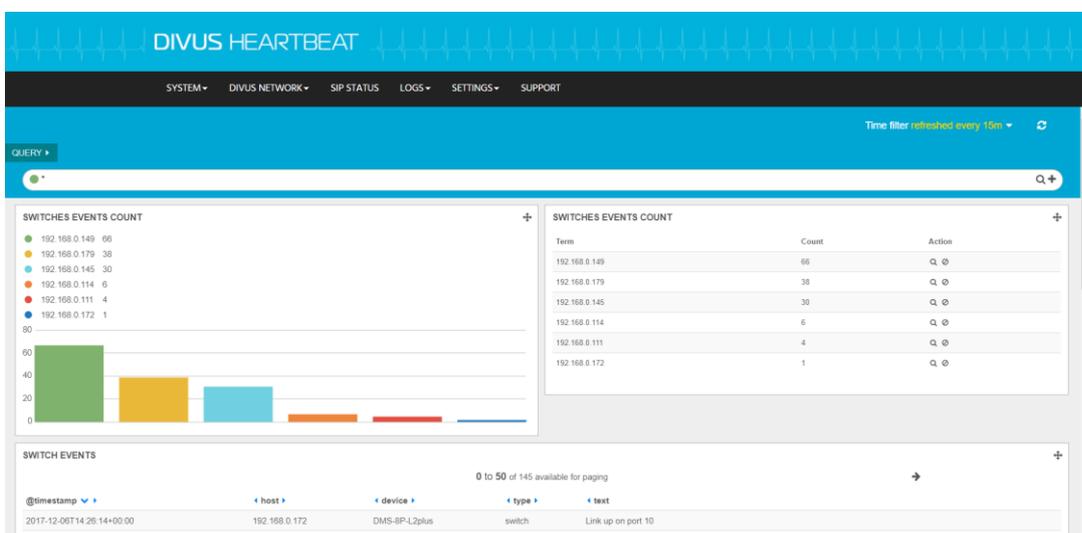
## 6.1 HOW TO MOVE A DEVICE USING A STATIC IP ADDRESS TO YOUR HEARTBEAT'S NETWORK

These are the steps to follow:

1. Make sure your laptop and the device are in the same physical network: e.g. the DSL.
2. Set your laptop's IP address to the same network as the device to be changed.  
  
E.g. the device is on network 192.168.178.x: set your laptop's address to 192.68.178.250.
3. Now you can communicate with the device: change its network settings to the new network. Ideally this means setting it to use DHCP. If the device should not support DHCP, set its static IP address to the same network as the DIVUS HEARTBEAT. Make sure the IP address you assign is currently free.  
  
E.g. the Heartbeat is on 192.168.0.11: set the device's IP to 192.168.0.210.
4. Save the changes on the device, reboot it if necessary.
5. Change the laptop's settings back to the previous.
6. Now start a new network scan on the DIVUS HEARTBEAT to see it appear with its properties in the scan report.

## 6.2 HOW TO USE THE LOG FILTERING / SEARCHING FUNCTION

The log pages have a structure like this:



The bottom table may contain a huge list of entries. How can we efficiently use this page to show us only the relevant information? The upper part contains a *Query bar* we can use for this purpose



The \* symbol means anything, therefore there is no filtering active by default.

If we change the entry to *Link* and press the lens icon, only entries having that keyword (anywhere) will be shown and all the others will be hidden.



If we use e.g. *Link up*, the response will not be the desired one, probably. That's because entering multiple words / strings is equivalent to saying "search for entries containing *Link* or entries containing *up*". Most probably, what we want instead is obtained by inserting "*Link up*".



You may also use the logical operators using uppercase characters e.g. *Link AND up* or more complex forms like ("*Link up*" OR "*Link down*") AND "*port 4*".

Another possibility is to add queries using the "+" icon on the right.




---

## 6.3 HOW TO EDIT VOIP ACCOUNTS ON THE DIVUS HEARTBEAT

---

To add a new VoIP account:

1. Go to SETTINGS – SIP SETTINGS. Scroll down to one of the entries like this:

The screenshot shows the 'SIP base configuration' page in the DIVUS HEARTBEAT interface. The configuration parameters for extension [1101] are as follows:

```
context=phones
;-----
; PRIVATE INTERNAL DEVICE
;-----
; domestic 10' touchzone
[1101]
username=1101
type=friend
secret=1101
qualify=10000
port=5060
nat=yes
host=dynamic
dtmfmode=rfc2833
context=phones
canreinvite=no
callerid=1101<1101>
call-limit=1
; domestic 7' touchzone
[1102]
```

2. Copy the whole section from [1101] to `call-limit=1` (all included)
3. Paste the block at the bottom of the file. Then edit it changing all the occurrences of the account number (1101 in this example) to the new account's number (e.g. 1115).

```
[1101]
username=1101
type=friend
secret=1101
qualify=10000
port=5060
nat=yes
host=dynamic
dtmfmode=rfc2833
context=phones
canreinvite=no
callerid=1101<1101>
call-limit=1
```

4. Change the password (*secret*) to a longer, more secure sequence. (You should do this for all the VoIP accounts you use!)
5. Finally save. Then wait a few seconds for the new settings to be effective.

---

## 6.4 HOW TO DEFINE CUSTOM VOIP GROUP CALLS ON THE DIVUS HEARTBEAT

---

A group call allows to call multiple devices at once. Then, the communication will be established between the caller and the first callee to answer. If no one answers, the ringing will continue until it reaches a timeout which may be configured on the HEARTBEAT or on the outdoor station.

A new group call just needs 2 lines to be added to the extensions configuration file which you can see and edit on the SETTINGS – SIP SETTINGS page (notice the extensions tab):

The screenshot shows the DIVUS HEARTBEAT web interface. At the top, there is a blue header with the logo and a navigation menu with items: SYSTEM, DIVUS NETWORK, SIP STATUS, LOGS, SETTINGS, and SUPPORT. Below the header, there are two tabs: 'SIP base configuration' and 'SIP extension configuration'. The 'SIP extension configuration' tab is active, showing a text area with configuration code for 'PUBLIC INTERNAL DEVICE', 'PUBLIC SHARED OPENDOOR', and 'residential\_incoming'. A 'Save' button is visible below the text area.

```

; PUBLIC INTERNAL DEVICE
;-----
[residential_internal]
exten => _8XX,1,NoOp()
exten => _8XX,n,Dial(SIP/residential/${EXTEN},30)
exten => _8XX,n,Hangup()

;-----
; PUBLIC SHARED OPENDOOR
;-----
[residential_external]
exten => _9XX,1,NoOp()
exten => _9XX,n,Dial(SIP/residential/${EXTEN},30)
exten => _9XX,n,Hangup()

[residential_incoming]
include => internal
include => external

```

The lines look like this:

```
exten => 12345,1,Dial(SIP/1101&SIP/1102,30)
```

```
exten => 12345,2,Hangup()
```

Explanation:

The first line defines what number should be used for the group call, and what accounts shall be part of the group. The number 12345 will call two devices: 1101 and 1102. Adding an additional number (e.g. 3405) is simple: just add "SIP/3405" to the existing accounts chain using the "&" symbol, so the line above would become.

```
exten => 12345,1,Dial(SIP/1101&SIP/1102&SIP/3405,30)
```

30 is the number of seconds it should ring i.e. the timeout. In the second line, the same number 12345 is repeated.

Once your 2 lines are ready, insert them at the bottom of the section starting with [internal]:

The screenshot shows the 'SIP extension configuration' page in the DIVUS HEARTBEAT interface. The page title is 'SIP extension configuration'. Below the title, there is a section labeled 'SIP Extensions\*'. A text editor displays the following configuration code:

```

;-----
; PRIVATE INTERNAL DEVICE
;-----
[internal]
exten => _11XX,1,NoOp()
exten => _11XX,n,Dial(SIP/${EXTEN},30)
exten => _11XX,n,Hangup()

exten => 12345,1,Dial(SIP/1101&SIP/1102,30)
exten => 12345,2,Hangup()

;-----
; PRIVATE EXTERNAL DEVICE
;-----
[external]
exten => _12XX,1,NoOp()
exten => _12XX,n,Dial(SIP/${EXTEN},30)
exten => _12XX,n,Hangup()

```

A blue 'Save' button is located at the bottom left of the configuration area. The footer of the page reads '(C) DIVUS GMBH 2017 - POWERED BY ASTLINUX'.

Then save and you are ready to test the new call number.

## 6.5 HOW TO ADD/EDIT A CUSTOM FIREWALL RULE

Before starting, remember that:

- The DSI is open to access everything on the other networks.
- Home Network and DSI are separated by a firewall
- The RIN is protected by a firewall and is also physically a separate network
- Firewall rules may be used to open but also to close ports, if necessary.
- When a field is left empty, that is equivalent to defining „any of that field“ e.g. an empty SOURCE PORT field means the rule will apply to any source port. In other words, the source port will not act as a filter.

Follow this procedure:

Field	Values or example	Explanation
Firewall rule type	Home to DSI, Home to RIN, RIN to DSI, RIN to Home, DSI to Home, DSI to RIN	Choose the firewall and the communication direction which should be allowed or denied.
Source IP address/range	192.168.0.0/24 (meaning any IP starting with 192.168.0. – using CIDR notation)	Choose the single source IP address or range of source addresses to which the rule shall be applied.
Destination IP address/range	192.168.69.7	Choose the single destination IP address or range of destination addresses for which the rule shall be defined.
Protocol	All, TCP, UDP, ICMP	Choose the protocol the rule should be applied to.
Source port(s)	80,81,82,83	Usually left empty meaning for any source port
Destination port(s)	8080	A port or set of ports (separated by commas without empty spaces) to which the firewall should give (or deny) access.
Policy	Allow, Block, Reject	What action the rule should cause.
Description		Use this to make it easier to recognize the rule if you plan to make multiple custom rules
Enabled	checked/unchecked	Use the checkbox to apply or disable the rule temporarily.

---

## 6.6 HOW TO DEFINE OR EDIT A CUSTOM PORT FORWARDING RULE

---

A forwarding rule allows to reach a device using another device's name. In this case, we can use the name `dhb-heartbeat` with a custom port and reach another device used as server in the same network. The advantage, like explained previously, is that we don't need to know the device's IP address and we don't need to worry if that IP address should one day change completely. We will use the DIVUS HEARTBEAT's name and its smart name resolution mechanism to always be able to reach our devices.

Field	Values or example	Explanation
Incoming interface	All, DIVUS Secure Intranet, Residential Intercom, Home Network	Choose which of the three network ports of the MANAGER is targeted
Protocol	TCP UDP	Choose the protocol
Incoming port	50000 (port of the HEARTBEAT)	Choose a free port
Source IP address/range	192.168.1.0/24	Choose a single address or a range, or allow all the devices on the network (see incoming interface)
Destination IP address	192.168.1.110	Insert the address of the target device
Destination port	80	If it is the web interface, use 80. Otherwise, refer to the device's manual.
Enabled	checked/unchecked	Use the checkbox to apply or disable the rule temporarily.

---

## 6.7 HOW TO SETUP A DEVICE FOR REMOTE VOIP ACCESS

---

Please note that allowing remote access to your system means weakening your system's security. If you need this functionality anyway, please follow these steps:

1. Add a port forwarding rule to your internet router: use any external port - don't use 5060 and of course never use the ones where known services run like 80, 443 etc. This should be forwarded to port 5060 of your DIVUS HEARTBEAT. In this case use the IP address 192.168.69.1 - or if you changed that, the new one - as destination. Use the chosen port in your client configuration(s).
2. Make sure the devices used for the remote access use the correct settings for the sip parameters
  - `nat=force_rport,comedia`
  - `qualify=20000`
  - `directmedia=no`
  - `localnet=192.168.69.0/24,192.168.0.0/24`
  - `externip/externhost=(public IP address/domain name)`

If these settings are all correct, the voice will travel over the SIP channel. Therefore, no additional port forwardings for RTP are needed. If you should still have issues, try adding a port forwarding for RTP on a range of 100 ports

eg. 10000 – 10100. These can go straight (external range being equal to internal range) from router to HEARTBEAT.

For viewing also VIDEO from an IP cam during a SIP call, you may need an additional port forwarding (usually) to port 80 of the cam. The DIVUS Videophone 4 App has a special place for this: use the public IP or domain name, the chosen external port number and also video will be shown during an intercom call.



