

# DIVUS HEARTBEAT

**Benutzerhandbuch**

Version 1.0

REV05-2018-04-16

---

## ALLGEMEINE INFORMATIONEN

---

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

Betriebsanleitungen, Handbücher und Software sind urheberrechtlich geschützt. Alle Rechte bleiben vorbehalten. Das Kopieren, Vervielfältigen, Übersetzen, Umsetzen im Ganzen oder in Teilen ist nicht gestattet. Eine Ausnahme gilt für die Anfertigung einer Sicherungskopie der Software für den eigenen Gebrauch.

Änderungen des Handbuchs behalten wir uns ohne Vorankündigung vor. Die Fehlerfreiheit und Richtigkeit der in diesem Dokument und auf den mitgelieferten Speichermedien enthaltenen Daten können wir nicht garantieren. Anregungen zu Verbesserungen sowie Hinweise auf Fehler sind uns jederzeit willkommen. Die Vereinbarungen gelten auch für die speziellen Anhänge zu diesem Handbuch.

Die Bezeichnungen in diesem Dokument können Marken sein, deren Benutzung durch Dritte für eigene Zwecke die Rechte der Inhaber verletzen können.

**Benutzerhinweise:** Bitte lesen Sie das Handbuch vor dem ersten Einsatz und bewahren Sie es zur späteren Verwendung sorgfältig auf.

**Zielgruppe:** Das Handbuch ist für Anwender mit Vorkenntnissen in der PC- und Automatisierungstechnik geschrieben.

---

## DARSTELLUNGSKONVENTIONEN

---

[TASTE]	Tasteneingaben des Benutzers werden in eckigen Klammern dargestellt, z.B. [STRG] oder [ENTF]
COURIER	Bildschirmausgaben werden in der Schriftart Courier beschrieben, z.B. c:\>
<b>COURIER FETT</b>	Tastatureingaben durch den Benutzer sind in Schriftart Courier fett beschrieben, z.B. c:\> <b>DIR</b>
„...“	Namen von auszuwählenden Schaltflächen, Menüs oder anderen Bildelementen werden in „Gänsefüßchen“ wiedergegeben.
PIKTOGRAMME	Im Handbuch sind folgende Piktogramme zur Kennzeichnung bestimmter Textabschnitte verwendet:
	<i>Achtung!</i> Möglicherweise gefährliche Situation. Sachschäden können die Folge sein.
	<i>Notizen</i> Tipps und ergänzende Hinweise
	<i>Neu</i> Kennzeichnet Änderungen und neue Features

---

## INHALTSVERZEICHNIS

---

ALLGEMEINE INFORMATIONEN	2
DARSTELLUNGSKONVENTIONEN	2
INHALTSVERZEICHNIS	3
1 EINLEITUNG	6
1.1 ALLGEMEINE INFORMATIONEN	6
1.2 DER MANAGER	7
1.2.1 DIVUS SECURE INTRANET	7
1.2.2 RESIDENTIAL INTERCOM NETZWERK	8
1.2.3 HOME LAN/WAN	8
1.3 DER DIVUS MANAGED SWITCH (DMS-8P-L2+)	8
2 SYSTEMSTRUKTUR	9
2.1 GRAFIKEN	9
2.1.1 ALLGEMEINES SCHEMA	9
2.1.2 ISOLIERTES NETZWERK	10
2.1.3 DIVUS SECURE INTRANET (DSI)	12
2.1.4 RESIDENTIAL INTERCOM NETZWERK (RIN)	13
3 WEBOBERFLÄCHE	14
3.1 ERSTER ZUGRIFF: DER SETUP-WIZARD	14
3.1.1 SCHRITT 1 – START	14
3.1.2 SCHRITT 2 – ENDBENUTZER-LIZENZVEREINBARUNG	15
3.1.3 SCHRITT 3 – DETAILS ÜBER DEN SYSTEMINTEGRATOR	16
3.1.4 SCHRITT 4 – DETAILS ÜBER DEN BAUHERRN	17
3.1.5 SCHRITT 5 – PROJEKT SETUP	18
3.1.6 SCHRITT 6 – NETZWERKKONFIGURATION - DIVUS SECURE INTRANET	18
3.1.7 SCHRITT 7 – NETZWERKKONFIGURATION - RESIDENTIAL INTERCOM	19
3.1.8 SCHRITT 8 – ZUSAMMENFASSUNG / LETZTER SCHRITT	19
3.1.9 NETZWERKSCAN	20

3.2	SYSTEM-STATUS-SEITE _____	20
3.3	SYSTEM – UPGRADE-SEITE _____	20
3.3.1	UPGRADE-PROZEDUR _____	21
3.4	SYSTEM – HERUNTERFAHREN-SEITE _____	23
3.5	DIVUS NETZWERK – BERICHT-SEITE _____	23
3.5.1	DAS GRAFISCHE SCHEMA _____	24
3.5.2	DIE PDF-DATEI DES BERICHTS _____	25
3.6	DIVUS NETZWERK – FÜHRE SCAN DURCH _____	25
3.7	DIVUS NETZWERK – ARCHIV-SEITE _____	26
3.8	SIP STATUS-SEITE _____	27
3.9	PROTOKOLL – SWITCH LOGS-SEITE _____	27
3.10	PROTOKOLL – VOIP/SIP LOGS-SEITE _____	28
3.11	PROTOKOLL – GESPRÄCHSPROTOKOLL-SEITE _____	28
3.12	EINSTELLUNGEN – SYSTEM-SEITE _____	28
3.13	EINSTELLUNGEN – NETZWERK _____	29
3.13.1	DHCP _____	29
3.14	EINSTELLUNGEN – SMART DEVICES-SEITE _____	30
3.15	EINSTELLUNGEN – FIREWALL REGELN-SEITE _____	31
3.16	EINSTELLUNGEN – PORT-FORWARDING-REGELN-SEITE _____	31
3.17	EINSTELLUNGEN – SIP EINSTELLUNGEN-SEITE _____	33
4	INTERCOM _____	34
4.1	ALLGEMEINE DEFINITIONEN _____	34
4.2	ALLGEMEINES VOIP-ACCOUNT-SCHEMA (FÜR ZONE 1 UND ZONE 2) _____	35
4.2.1	BASISEINHEIT _____	36
4.3	VOIP ACCOUNTS FÜR EXTERNE EINHEITEN _____	37
4.4	CONCIERGE / RECEPTION ACCOUNTS _____	37
5	CLIENT-GERÄTEEINRICHTUNG FÜR DSI UND RIN _____	39
5.1	DIVUS TOUCHZONE _____	39
5.2	DIVUS SUPERIO UND ANDERE WINDOWS-BASIERTE DIVUS-GERÄTE _____	39

5.3	DIVUS OPENDOOR	39
5.4	KNX CONTROL GERÄTE (KNX SERVER, KNX SUPERIO)	40
5.4.1	SONDERREGELN FÜR DIVUS KNX SERVER UND KNX SUPERIO	40
5.5	IP-KAMERAS VON DRITTANBIETERN	41
5.6	DRITTANBIETER-CLIENT-GERÄTE (MIT ETHERNET-SCHNITTSTELLE)	41
5.7	ANALOGUE DRITTHERSTELLERGERÄTE	41
6	ERWEITERTE THEMEN	42
6.1	EIN GERÄT MIT EINER STATISCHEN IP-ADRESSE IN DAS HEARTBEAT-NETZWERK HOLEN	42
6.2	VERWENDUNG DER LOG-FILTER- / SUCH-FUNKTION	43
6.3	VOIP-ACCOUNTS AUF DEM DIVUS HEARTBEAT BEARBEITEN	44
6.4	VOIP-GRUPPENRUFEN AUF DEM DIVUS HEARTBEAT DEFINIEREN	45
6.5	SO ERSTELLEN/BEARBEITEN SIE EINE BENUTZERDEFINIERTER FIREWALL-REGEL	46
6.6	BENUTZERDEFINIERTER PORTWEITERLEITUNGSREGELN ERSTELLEN	47
6.7	EIN GERÄT FÜR DEN REMOTEZUGRIFF AUF DAS INTERCOM-SYSTEM EINRICHTEN	48
	NOTES	50

# 1 Einleitung

## 1.1 ALLGEMEINE INFORMATIONEN

Danke, dass Sie sich für DIVUS HEARTBEAT entschlossen haben! Dieses Handbuch wird Ihnen dienen, das Netzwerk Ihres Smart Home's optimal einzurichten.

Die Hauptziele Ihres neuen DIVUS HEARTBEAT sind:

- Die Vernetzung aller Ihrer Smart Home-Geräte simpel wie *plug and play* zu machen
- Die sensiblesten Geräte zu isolieren und vor unerwünschten Zugriffen zu schützen
- Ihr Netzwerk und dessen Geräte zu verwalten, zu kontrollieren und beim Troubleshooting zu unterstützen

Der DIVUS HEARTBEAT wurde rund um Gebäudeautomation geplant und entwickelt. Es ist ein einzigartiges Gerät, das komplexe Netzwerkeinstellungen und sichere Voraussetzungen automatisch schafft.

Der DIVUS HEARTBEAT besteht aus zwei Teilen: den **Manager** und den **Managed Switch**. Die zwei werden durch 19-Zoll **Rack-Adapter** zusammengehalten.



Er kann durch das Hinzufügen von beliebig vielen zusätzlichen Switches erweitert werden, falls mehrere Ports benötigt werden.



## 1.2 DER MANAGER



Der Manager ist das Herz und das Hirn des Systems: er kontrolliert 3 getrennte Netzwerke:

- Das DIVUS Secure Intranet (später auch **DSI** genannt)
- Das Residential Intercom-Netzwerk (**RIN**)
- Das Home LAN/WAN

Er ist das Gateway zwischen all diesen drei Netzwerken.

Sein Web-Server gewährt den Zugriff zu all den Funktionalitäten des DIVUS HEARTBEAT.

Siehe Kapitel 3 für weitere Details über die Web-Oberfläche.



**Hinweis:** Die drei Netzwerkports des *Managers* sind nicht PoE-Ports! Falls Sie z.B. ein einziges Gerät zum *Residential Intercom*-Port verbinden möchten und es Strom über das Netzkabel benötigt, müssen Sie einen sogenannten PoE-Injector einsetzen oder einen zusätzlichen *DIVUS MANAGED SWITCH*.

Werfen wir nun einen Blick auf die 3 Netzwerke!

### 1.2.1 DIVUS SECURE INTRANET

Das DIVUS Secure Intranet ist konzipiert, um ein isoliertes, sicheres Netzwerk für Ihre Smart Home-Geräte zu liefern. Z.B. ein DIVUS KNX SERVER, DIVUS TOUCHZONE- und SUPERIO-Panels würden mit diesem Netzwerk verbunden werden. Wenn Sie den Anweisungen des DIVUS HEARTBEAT Quick Start Guide oder dieses Handbuchs folgen, um alle Ihre Geräte zu verbinden, können sie einen der 8 Ports des MANAGED SWITCH nutzen, um sie mit dem DIVUS Secure Intranet zu verbinden.





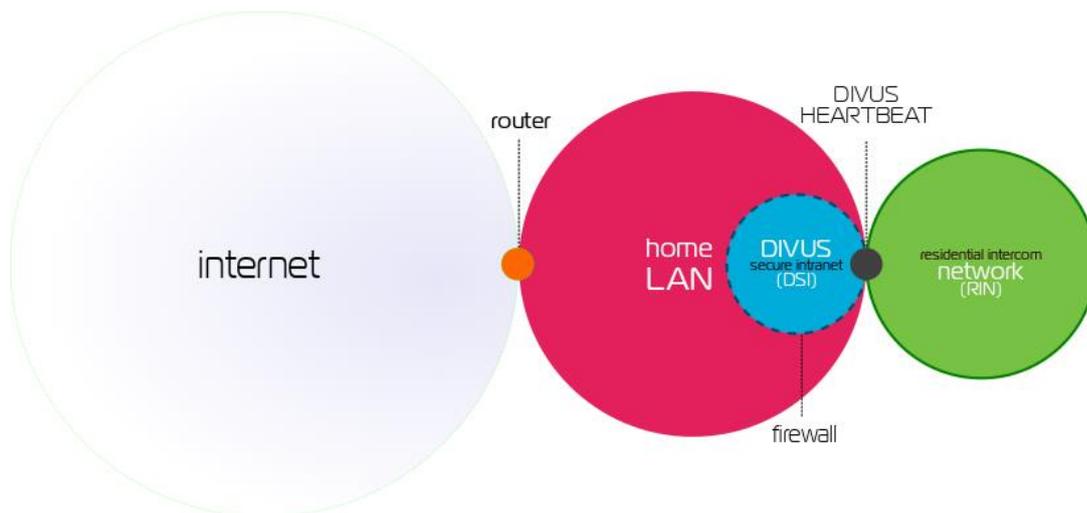
## 2 Systemstruktur

In diesem Kapitel werden die Aufgaben der einzelnen Bestandteile des DIVUS HEARTBEAT durch einfach verständliche Grafiken erläutert.

### 2.1 GRAFIKEN

#### 2.1.1 ALLGEMEINES SCHEMA

3 verbundene Netzwerke: der DIVUS HEARTBEAT teilt ein komplexes System in 3 separate, einfach verwaltbare und sichere Netzwerke auf. Wie diese strukturiert sind und in welcher Beziehung zueinander und zum Internet sie stehen, entnehmen Sie diesem allgemeinen Schema:

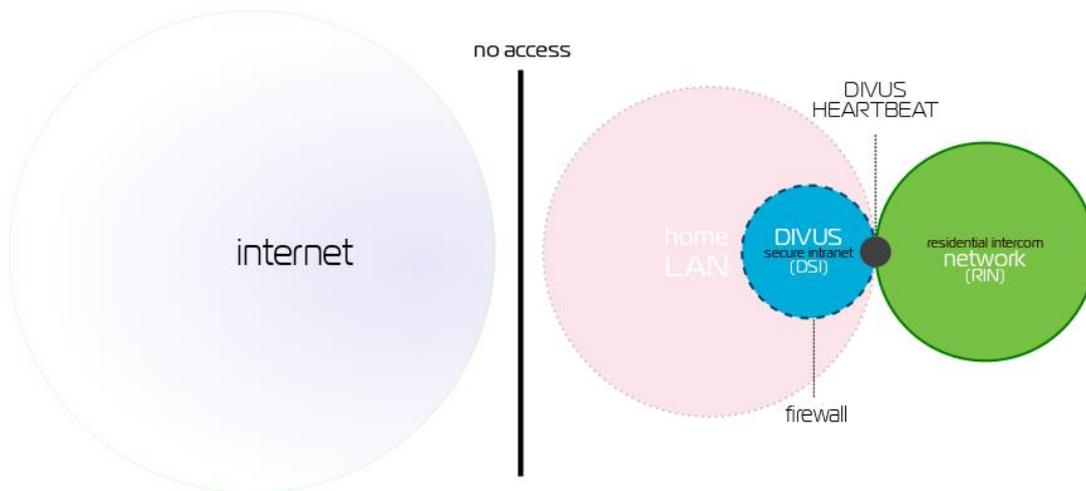


Dieses Schema zeigt eine typische Netzwerkstruktur – wahrscheinlich die meist vorkommende.

Um aber besser zu verstehen, wie der DIVUS HEARTBEAT verschiedene Setups verwalten kann, müssen wir etwas genauer hinschauen:

1. Üblicherweise ist zwar das obere das geplante Schema, doch wenn die Gebäudeautomationsgeräte und dessen Netzwerk eingerichtet werden, ist noch kein Internetrouter vorhanden – dieser wird erst Wochen oder Monate später folgen.
2. Kunden bevorzugen manchmal (und zurecht), die Gebäudeautomation netzwerkmäßig vom Internet getrennt zu halten. In dem Fall wird das Schema ähnlich wie das obige aussehen, aber ohne Verbindung mit dem Router – und über diesen mit dem Internet.

## 2.1.2 ISOLIERTES NETZWERK



Was passiert also, wenn das Netzwerk anfangs ohne Router ist aber dann einer hinzugefügt wird?

1. Alle in der Quickstart Guide beschriebenen Schritte sollten durchgeführt werden. (Alle Geräte werden verbunden, die erste Setup-Prozedur auf dem DIVUS HEARTBEAT wird durchgeführt und durch den ersten Netzwerkschscan vervollständigt)
2. In dieser Situation sind das DIVUS SECURE Intranet und das RESIDENTIAL INTERCOM voll funktionstüchtig (bis natürlich auf eventuelle Online-Dienste).
3. Durch die automatische Erkennung, dass kein Router im Netzwerk aktiv ist, wird der DIVUS HEARTBEAT die Kontrolle des Netzwerks an dessen Stelle übernehmen:
  - a. Er wird die DHCP-Server-Rolle für das Netzwerk übernehmen
  - b. Durch DHCP und NETBIOS/WINS, wird er IP-Adressen und Namen an die Geräte vergeben und sicherstellen, dass besondere Geräte (z.B. ein DIVUS KNX SERVER) von überall aus erreichbar sind.
4. Um zusätzliche Kommunikationskanäle für oder zu besonderen Geräten zu öffnen, können besondere vordefinierte Regeln aktiviert werden oder manuell neue hinzugefügt werden. Siehe Kapitel , 6.5, **Fehler! Verweisquelle konnte nicht gefunden werden.** für Details.

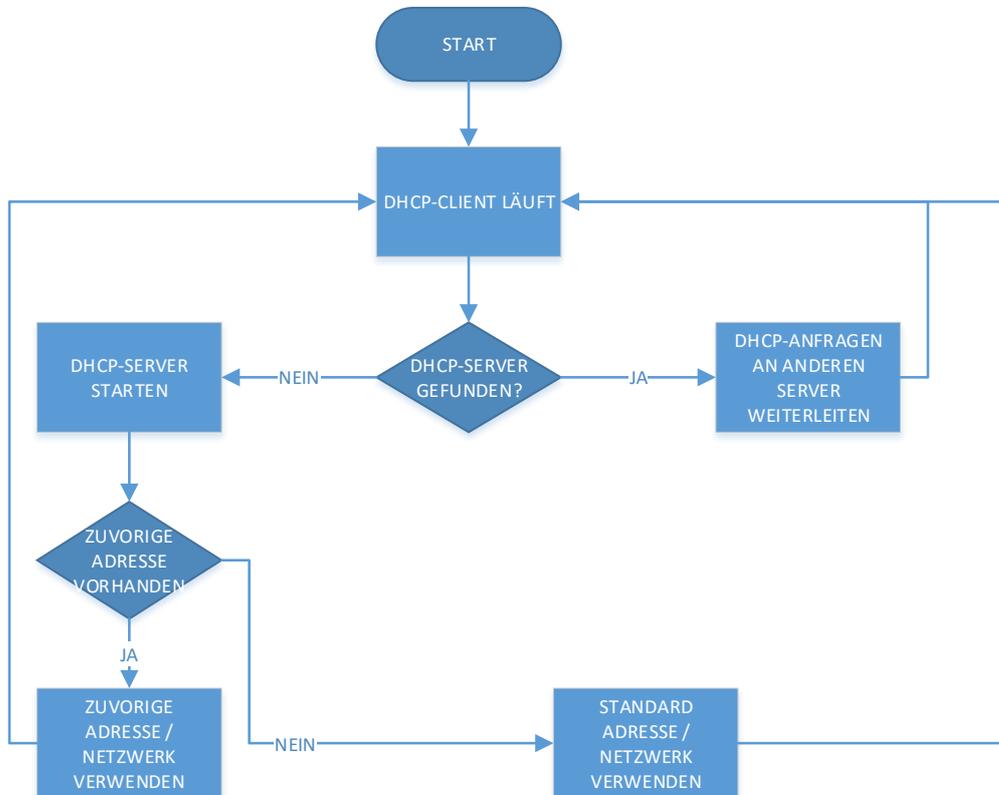
Zu diesem Zeitpunkt kann ein isoliertes System benutzt werden. Ein System, wo ein Router zukünftig folgen wird, kann auch mit dieser Konfiguration normal laufen.

Was passiert dem zuerst mit einem DIVUS HEARTBEAT konfigurierten System, sobald der Router dann installiert und verbunden wird?

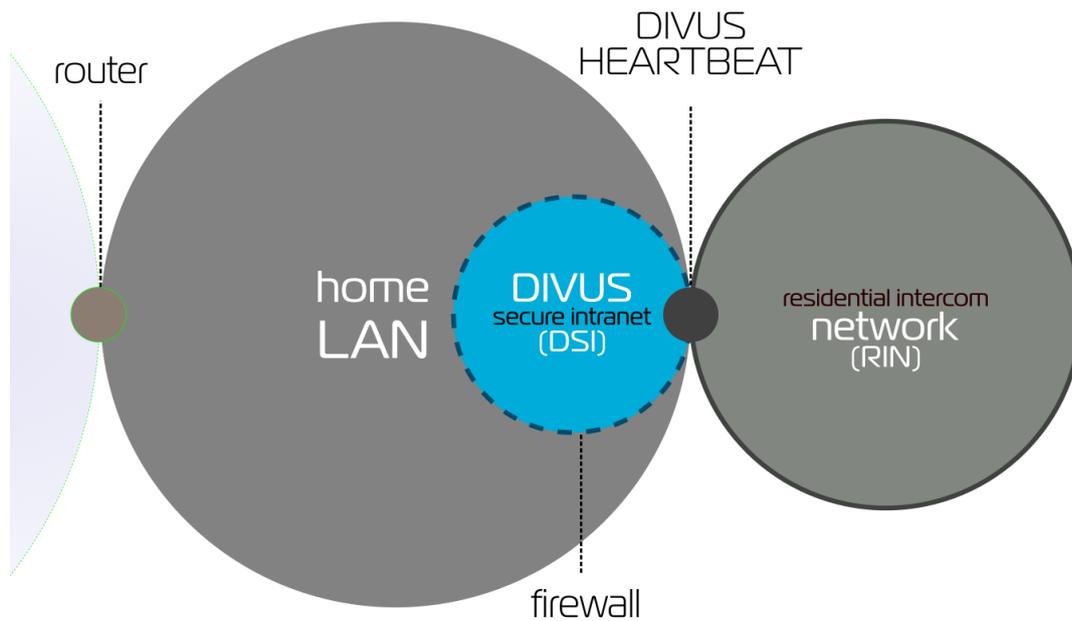
Wenn der Router mit dem DIVUS HEARTBEAT verbunden wird:

- bemerkt DIVUS HEARTBEAT das neue Gerät und dessen Rolle
- übergibt DIVUS HEARTBEAT dem Neuling die Netzwerkverwaltungsrolle:

- die DHCP-Serverrolle wird dem Router überlassen. Das bedeutet, dass alle vergebenen DHCP-Adressen von einem anderen Server erneuert werden werden, was die Geräte auch in ein total anderes Netzwerk bringen könnte.
- Der DIVUS HEARTBEAT wird weiterhin die Rolle des primären oder sekundären WINS-Server für das Netzwerk spielen. Dadurch wird er weiterhin im Stande sein, jegliche Abfrage nach `dhb-heartbeat` mit der darunterliegenden IP-Adresse aufzulösen.
- Der DIVUS HEARTBEAT kann von einem isolierten Netzwerk (siehe 2.1.2) zu einem verbundenen schalten (siehe 2.1.1) oder umgekehrt – wann immer das nötig ist:



## 2.1.3 DIVUS SECURE INTRANET (DSI)

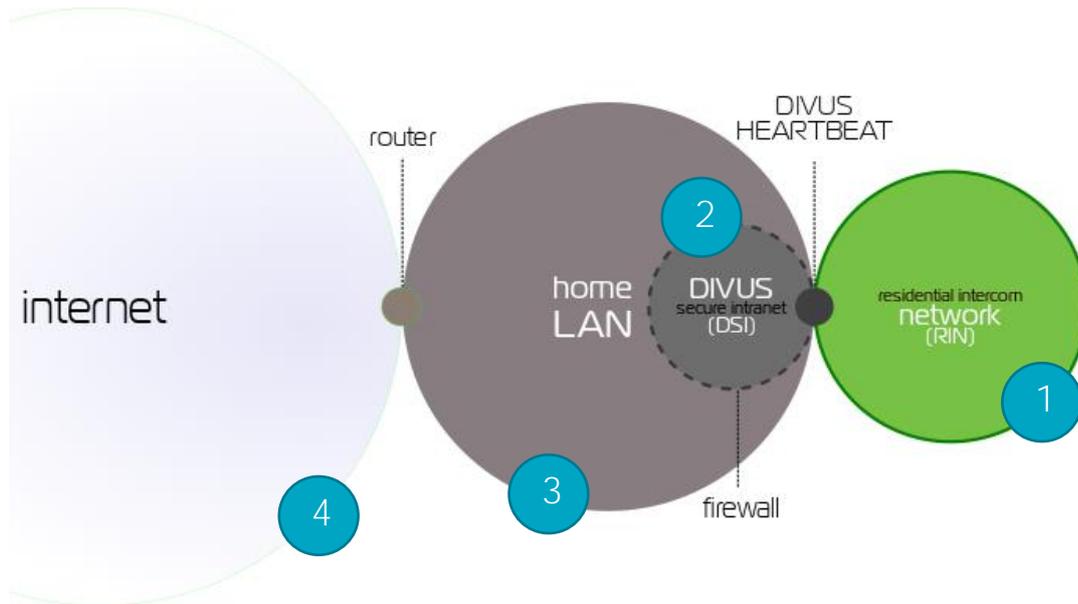


Das *DIVUS SECURE INTRANET* ist das Netzwerk, das für Ihre Home Automation- und Visualisierungsgeräte reserviert ist.

Von einem Manager und einem dedizierten Switch verwaltet zu werden bringt mehrere Vorteile mit sich:

- Dedizierte Bandbreite für Ihre Home Automation – sie wird durch den Gebrauch auf anderen Netzwerken nicht beeinträchtigt (z.B. große Downloads oder Streaming auf einem Gerät im Home LAN)
- Größere Sicherheit
  - Teils durch das separate Netzwerk gegeben,
  - Teils durch die Firewall zwischen den Home Automation-Geräten und Ihren herkömmlichen LAN-Geräten.
- Geräte, die an Ihrem DSI verbunden sind, werden als vertrauenswürdig betrachtet und haben dadurch uneingeschränkten Zugriff auf alle Netzwerke (und dessen Geräte)
- Das DSI ist ein Teil desselben Netzwerks, wo sich auch Ihre netzwerktauglichen Haushaltsgeräte (Laptops, Smartphones, Smart-TV usw.) befinden. Doch die Kommunikation vom Home LAN zum DSI ist nur möglich, wenn besondere Regeln dafür auf dem DIVUS HEARTBEAT eingerichtet werden. Siehe dazu Kapitel 6.5 und 6.6.

## 2.1.4 RESIDENTIAL INTERCOM NETZWERK (RIN)



Dies sind die Beziehungen, die das RIN mit den anderen Netzwerken hat:

- 1) *EXTERNE EINHEITEN (Aussensprechstellen)* und Kameras sollten im **RIN** untergebracht werden, um dessen besondere Sicherheitsmaßnahmen nutzen zu können. Geräte innerhalb des *RIN* können keine anderen Geräte oder andere Netzwerke erreichen.<sup>1</sup> Sie können ausschließlich den DIVUS HEARTBEAT auf dessen VoIP-Port ansprechen.
- 2) Im Normalfall werden die Geräte des RIN mit denen des **DIVUS SECURE Intranet** kommunizieren. Die VoIP-Kommunikation ist vom DIVUS HEARTBEAT verwaltet, den alle Geräte im Netzwerk erreichen können. Geräte im DSI sind vertrauenswürdig und können deshalb alle anderen Geräte erreichen. Also ist es kein Problem, z.B. den Stream einer Ausseneinheit auf einem DIVUS TOUCHZONE zu zeigen, der mit dem *DSI* verbunden ist; standardmäßig wird diese Verbindung immer möglich sein.
- 3) Ein Gerät vom Home-LAN könnte auf etwas im RIN zugreifen wollen. Ein Beispiel ist ein Smartphone, das am VoIP-System teilnehmen soll und deshalb Zugriff zum HEARTBEAT sowie zur IP-Adresse der Kamera benötigt. Für solche Fälle ist eine eigene Firewallregel auf dem DIVUS HEARTBEAT nötig – standardmäßig sind solche Zugriffe nämlich gesperrt. Siehe Kapitel 6.5 für Details.
- 4) Und zuletzt könnten auch Geräte aus dem Internet konfiguriert werden, um auf solche im RIN zugreifen zu können. Das könnte zum Beispiel der Fall sein, wenn der Benutzer von seinem Smartphone aus dem Intercom-System teilnehmen will, auch wenn er sich ausserhalb seines Heimnetzwerks befindet.

Siehe Kapitel 6.7 für die Konfiguration des Remotezugriffs auf das Intercom-System.

<sup>1</sup> Das bedeutet, dass sie keine anderen Geräte erreichen können. Trotzdem sind sie natürlich im Stande, Abfragen vonseiten anderer Geräte zu beantworten, falls aufgefordert. Die Richtung des Kommunikationsaufbaus macht es aus.

# 3 Weboberfläche

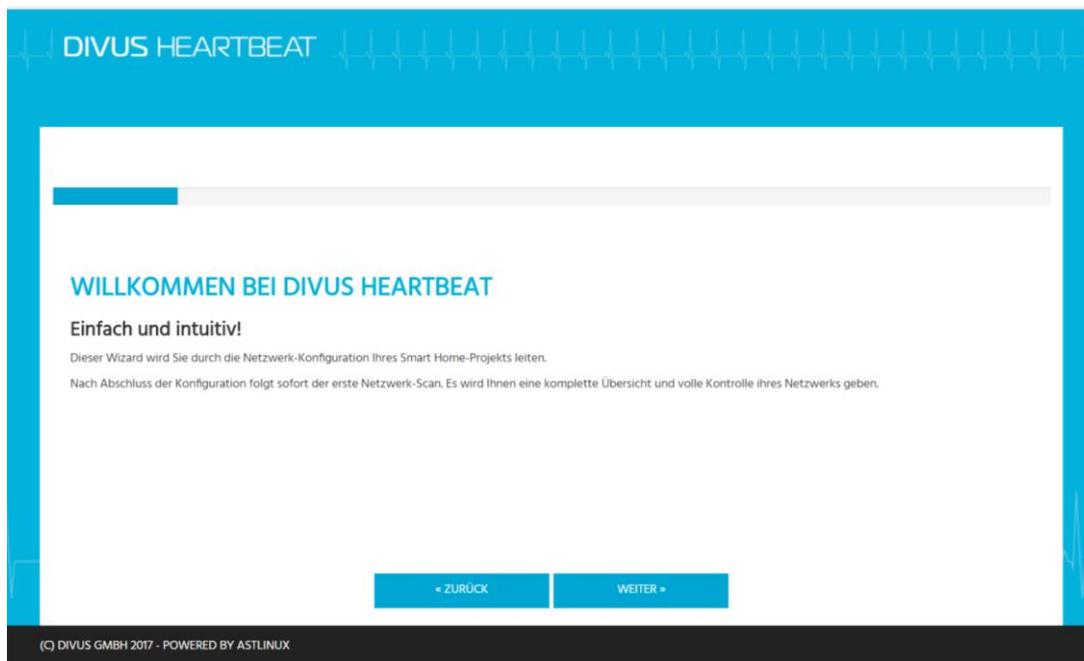
## 3.1 ERSTER ZUGRIFF: DER SETUP-WIZARD

Beim ersten Zugriff auf die Weboberfläche über

```
https://dhb-heartbeat
```

wird der Setup-Assistent gestartet, der die wesentlichsten Einstellungen bezüglich Gerät und Projekt speichern wird. Wählen Sie als erstes die Sprache English (Standard) oder Deutsch, um sofort die Weboberfläche dementsprechend umzuschalten.

### 3.1.1 SCHRITT 1 – START



## 3.1.2 SCHRITT 2 – ENDBENUTZER-LIZENZVEREINBARUNG

Lesen Sie und akzeptieren Sie die Lizenzvereinbarung durch die Checkbox in Schritt 2:

DIVUS HEARTBEAT

## DIVUS HEARTBEAT ENDBENUTZER-LIZENZVEREINBARUNG

Version 1.0

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.

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, and construed exclusively in accordance with the Law of Italy. The courts of Bologna, Italy, shall have exclusive jurisdiction. In addition, DIVUS

Ich akzeptiere die Nutzungsbedingungen

- ZURÜCK WEITER -

(C) DIVUS GMBH 2007 - POWERED BY ASTLREUX

## 3.1.3 SCHRITT 3 – DETAILS ÜBER DEN SYSTEMINTEGRATOR

Füllen Sie mindestens die durch einen \* gekennzeichneten Felder aus; wir empfehlen allerdings, möglichst alle Felder auszufüllen, damit die Berichte später vollständig und klar erstellt werden können.

**DETAILS ÜBER DEN SYSTEMINTEGRATOR**

Name*	System Integrator Name
Unternehmen*	Unternehmen Name
Adresse	Integratorstraße 1
Ortschaft	München
Postleitzahl	12345
Land	Deutschland
Telefonnummer	123456789
E-Mail-Adresse*	integrator@system.de
Login-Name*	sysint
Kennwort*	*****
Kennwort bestätigen*	*****

[← ZURÜCK](#) [WEITER →](#)

© DIVUS GMBH 2017 - POWERED BY ASTLINUX

## 3.1.4 SCHRITT 4 – DETAILS ÜBER DEN BAUHERRN

Hier wiederum füllen sie mindestens die mit einem \* gekennzeichneten Felder aus – wiederum empfehlen wir aber, alle Felder auszufüllen.

**DETAILS ÜBER DEN BAUHERRN**

Name*	Bauherr Name
Unternehmen	-
Adresse	Bauheradresse 1
Ortschaft	Ortschaft X
Postleitzahl	12345
Land*	Deutschland
Telefonnummer	98765432
E-Mail-Adresse*	bauherr@home.de
Login-Name*	bauherr
Kennwort*	
Kennwort bestätigen*	

← ZURÜCK      WEITER →

(C) DIVUS GMBH 2017 - POWERED BY ASTLINUX

### 3.1.5 SCHRITT 5 – PROJEKT SETUP

Geben Sie hier einen Namen für das Projekt / Bauvorhaben ein. Die anderen Felder sind auf Standardwerte gesetzt, die Sie bei Bedarf ändern können. Wenn mehr als ein DIVUS HEARTBEAT im selben Netzwerk stehen werden, sollten sich dessen Hostnamen unterscheiden, um Probleme zu vermeiden. Sie können `dhb-heartbeat` zu etwas anderem ändern, doch das System wird jedenfalls `dhb-` am Anfang hinzufügen und am Ende das wegschneiden, was die Gesamtlänge von 15 Zeichen überschreitet.

Als Alternative kann man auch `dhb-<Seriennummer>` (z.B. `https://dhb-21234`) verwenden, um ein Gerät aufzurufen. Die Seriennummer finden Sie u.A. auf der Statusseite.

**DIVUS HEARTBEAT**

**PROJEKT-SETUP**

Projektname\*

Hostname\*

Domäne\*

Zeitzone\*

Sprache\*

Ich erlaube das Senden der Daten auf die DIVUS-Cloud

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

(C) DIVUS GMBH 2017 - POWERED BY ASTLINUX

### 3.1.6 SCHRITT 6 – NETZWERKKONFIGURATION - DIVUS SECURE INTRANET

Hier kann die Netzwerkkonfiguration des DSI geändert werden. Um die erweiterten Eigenschaften des DIVUS HEARTBEAT's voll zu nutzen, empfiehlt es sich, die Standardeinstellung „Auto-Konfiguration (DHCP)“ zu bestätigen.

**DIVUS HEARTBEAT**

**NETZWERKKONFIGURATION - DIVUS SECURE INTRANET**

Netzwerk-Konfigurationsmodus\*

[< ZURÜCK](#) [WEITER >](#)

(C) DIVUS GMBH 2017 - POWERED BY ASTLINUX

### 3.1.7 SCHRITT 7 – NETZWERKKONFIGURATION - RESIDENTIAL INTERCOM

Als Standardeinstellung für das RIN wird die Benutzung statischer IP-Adressen des 192.168.69.0-Netzwerks angeboten. Falls notwendig kann auch eine DHCP-Server- oder eine DHCP-Client-Funktion aktiviert werden. Genaueres finden Sie in Kapitel 3.13.1.

The screenshot shows the 'NETZWERKKONFIGURATION - RESIDENTIAL INTERCOM' screen. It features a progress bar at the top, followed by the title. Below the title are several input fields: 'Netzwerk-Konfigurationsmodus\*' (set to 'Manuelle Konfiguration'), 'IP-Adresse' (192.168.69.1), 'Netzwerkmaske' (255.255.255.0), and 'Gateway-IP-Adresse'. There is also a checkbox for 'Als DHCP-Server im Residential Intercom Netzwerk agieren'. At the bottom, there are two buttons: '← PREVIOUS' and 'NEXT →'. The footer contains the text '(C) DIVUS GMBH 2017 - POWERED BY ASTINUX'.



Wenn die DHCP-Server-Funktion für das RIN eingesetzt wird, muss im Vorfeld sichergestellt werden, dass kein anderes Gerät in diesem Netzwerk einen aktiven DHCP-Dienst hat!

### 3.1.8 SCHRITT 8 – ZUSAMMENFASSUNG / LETZTER SCHRITT

Dieser letzte Schritt zeigt nochmal die Zugangsdaten und die wesentlichen Einstellungen, die samt allen zuvorigen Einstellungen erst durch die NEUSTART-Taste bestätigt und gespeichert werden. Merken Sie sich die Zugangsdaten – ab jetzt brauchen Sie sie, um auf die Weboberfläche zuzugreifen!

The screenshot shows the 'KONFIGURATION ABGESCHLOSSEN!' screen. It features a progress bar at the top, followed by the title. Below the title is a bold instruction: 'Klicken Sie auf 'Neustart', um die Änderungen zu übernehmen und den Netzwerkskan zu starten.' This is followed by a success message: 'Glückwunsch! Die Setup-Prozedur wurde erfolgreich abgeschlossen.' and a note: 'Durch Drücken des 'Neustart'-Buttons wird die Konfiguration gespeichert und das System neu gestartet. Sobald das System sich neu konfiguriert hat, werden Sie aufgefordert werden sich mit Benutzername und Kennwort anzumelden um mit dem Netzwerkskan fortzufahren.' Below this is a warning: 'Vergessen Sie nicht die Benutzernamen und Passwörter. Sie finden sie unten mit der neuen Adresse des Systems.' A table titled 'Konfigurationsübersicht für das Projekt: BV Zuhause' contains the following data:

Benutzername Systemintegrator:	fl	Benutzername des Bauherrn:	bauherr
Kennwort Systemintegrator:	23262r	Passwort des Bauherrn:	bauherr
Hostname:	dhb-fl	Netzwerk-Modus:	DHCP
HEARTBEAT Adresse:	dhb-fl		

At the bottom, there are two buttons: '← ZURÜCK' and 'NEUSTART'. The footer contains the text '(C) DIVUS GMBH 2017 - POWERED BY ASTINUX'.

Nachdem Sie die NEUSTART-Taste gedrückt haben, startet das System neu mit den neuen Einstellungen.

### 3.1.9 NETZWERKSCAN

Der Netzwerkscan wird automatisch nach dem Neustart gestartet. Siehe Kapitel 3.5 und 3.6 für genauere Details.

## 3.2 SYSTEM-STATUS-SEITE

Die erste Seite im Menu ist auch die Homepage der Weboberfläche. Sie zeigt eine Zusammenfassung über den aktuellen Status des Systems mit Speichernutzung, Name und IP-Adressen, Last, Uptime und die letzten Log-Einträge.

DIVUS HEARTBEAT

SYSTEM ▾ DIVUS NETZWERK ▾ SIP STATUS PROTOKOLL ▾ EINSTELLUNGEN ▾ SUPPORT

### System-Status

System-Details

<b>PRODUKT</b>	DIVUS Heartbeat 110	<b>SERIENNUMMER</b>	21024
<b>HOSTNAME</b>	dhb-fl	<b>UPTIME (LAUFZEIT)</b>	37 Minuten, 5 Sekunden
<b>BETRIEBSSYSTEM</b>	Linux	<b>ARCHITEKTUR</b>	x64
<b>SPEICHER</b>	1974MB total, 1119MB free	<b>CPU</b>	4x AMD GX-412TC SOC
<b>SYSTEM-LAST</b>	103, 0.93, 0.56		
<b>DIVUS SECURE INTRANET IP-ADRESSE</b>	192.168.0.132/21	<b>IP-ADRESSE RESIDENTIAL INTERCOM</b>	192.168.69.1/24

Festplattennutzung

Filesystem	Size	Used	Available	Use%	Mounted on
/dev/sda1	511.6M	165.6M	346.1M	32%	/oldroot/odrom
/dev/sda3	56.2G	355.5M	53.0G	1%	/oldroot/mnt/asturw

Aktuellste System-Log-Einträge

```

Apr 9 14:29:39 dhb-fl openvpn[3043]: Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
Apr 9 14:29:39 dhb-fl openvpn[3043]: Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
Apr 9 14:29:39 dhb-fl openvpn[3043]: RESOLVE: Cannot resolve host address: hb-cloud.divus.eu:1194 (Name or service not known)
Apr 9 14:29:39 dhb-fl openvpn[3043]: RESOLVE: Cannot resolve host address: hb-cloud.divus.eu:1194 (Name or service not known)
Apr 9 14:29:39 dhb-fl openvpn[3043]: Could not determine IPv4/IPv6 protocol
Apr 9 14:29:39 dhb-fl openvpn[3043]: SIGUSR1[soft,init_instance] received, process restarting
Apr 9 14:30:19 dhb-fl openvpn[3043]: Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
Apr 9 14:30:19 dhb-fl openvpn[3043]: Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
Apr 9 14:30:19 dhb-fl openvpn[3043]: RESOLVE: Cannot resolve host address: hb-cloud.divus.eu:1194 (Name or service not known)
Apr 9 14:30:19 dhb-fl openvpn[3043]: RESOLVE: Cannot resolve host address: hb-cloud.divus.eu:1194 (Name or service not known)
Apr 9 14:30:19 dhb-fl openvpn[3043]: RESOLVE: Cannot resolve host address: hb-cloud.divus.eu:1194 (Name or service not known)

```

## 3.3 SYSTEM – UPGRADE-SEITE

Falls Ihr DIVUS HEARTBEAT Internetzugriff hat, wird er auf den Aktualisierungsserver nach einer neuen Firmwareversion suchen, wenn Sie diese Seite aufrufen. Sollte Ihr Gerät nicht die aktuellste Version haben, werden Sie darüber informiert und können direkt die Upgradeprozedur starten.

DIVUS HEARTBEAT

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

### System upgrade

Current build: heartbeat-110-20170726004411

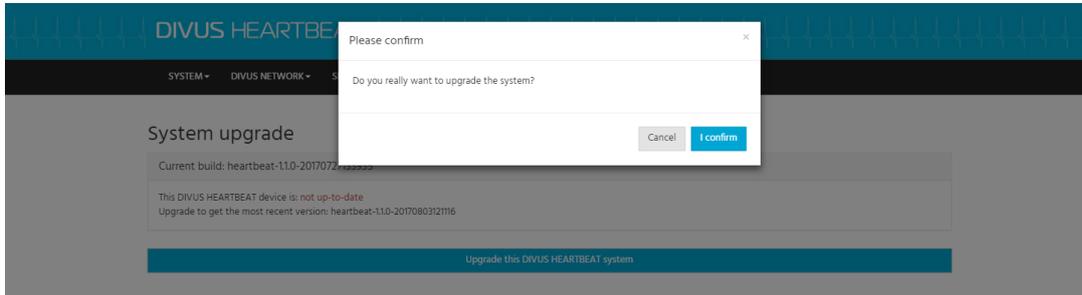
This DIVUS HEARTBEAT device is: not up-to-date

Upgrade to get the most recent version: heartbeat-110-20170803121116

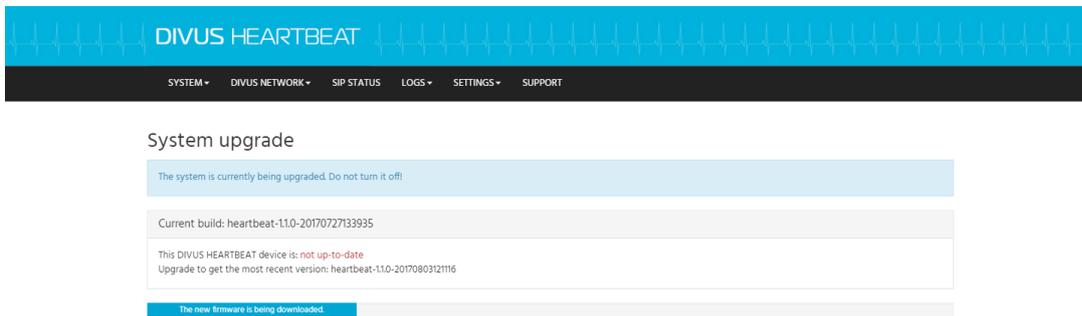
Upgrade this DIVUS HEARTBEAT system

## 3.3.1 UPGRADE-PROZEDUR

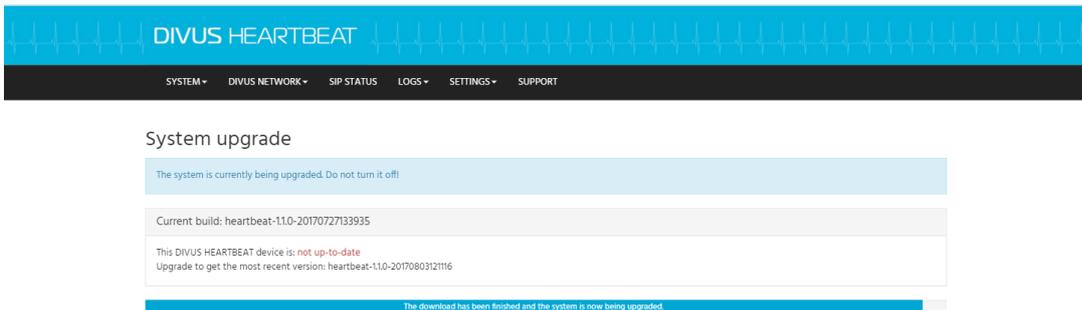
1. Wenn Sie den Upgrade-Button drücken, können Sie in der aufscheinenden Meldung den Start des Vorgangs bestätigen oder unterbrechen. Die Konfiguration des Geräts wird von einer Aktualisierung nicht geändert und bleibt also nach dem Upgrade problemlos erhalten.



2. Nach der Bestätigung startet das Herunterladen der Firmwaredatei...



...und die Aktualisierung wird durchgeführt.



- 
- 
3. Nach der Aktualisierung werden Sie aufgefordert, das Gerät neuzustarten. Bestätigen Sie!

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, the page title is "System upgrade". A green message box states: "The new firmware has been installed successfully. Please reboot your system." Below this, a white box displays: "Current build: heartbeat-11.0-20170727133935" and "This DIVUS HEARTBEAT device is: not up-to-date" (with "not up-to-date" in red). Underneath, it says: "Upgrade to get the most recent version: heartbeat-11.0-2017080312116". At the bottom, there is a grey button labeled "Reboot the system".

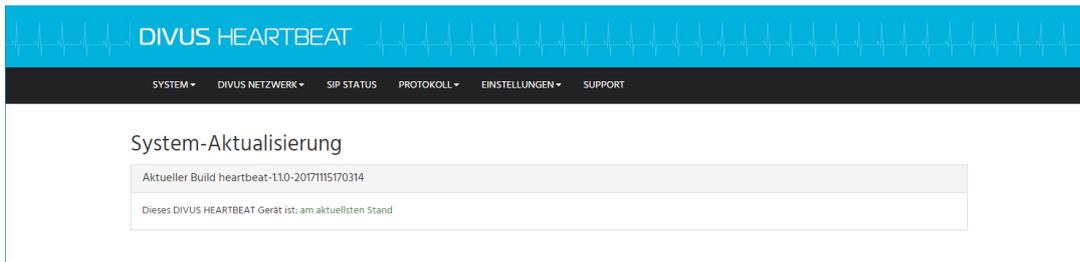
The screenshot shows the DIVUS HEARTBEAT web interface. At the top, there is a blue header with the logo and a navigation menu with items: SYSTEM, DIVUS NETWORK, SIP STATUS, LOGS, SETTINGS, and SUPPORT. Below the header, the page title is "System upgrade". A green message box states: "The system is currently rebooting and will be back online in a few minutes." Below this, a white box displays: "Current build: heartbeat-11.0-20170727133935" and "This DIVUS HEARTBEAT device is: not up-to-date" (with "not up-to-date" in red). Underneath, it says: "Upgrade to get the most recent version: heartbeat-11.0-2017080312116". At the bottom, there is a grey button labeled "Reboot the system".

The screenshot shows the DIVUS HEARTBEAT web interface. A modal dialog box titled "Please confirm" is centered on the screen. The dialog contains the text: "Do you really want to restart the system?". There are two buttons at the bottom of the dialog: "Cancel" and "I confirm". The background of the web interface is dimmed, showing the same "System upgrade" page as in the previous screenshots.

- 
- 
- 
4. Sie erhalten eine entsprechende Meldung, sobald das Gerät den Neustart vervollständigt hat.

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, the page title is "System upgrade". A green message box states: "The system is now back online." Below this, a white box displays: "Current build: heartbeat-11.0-20170727133935" and "This DIVUS HEARTBEAT device is: not up-to-date" (with "not up-to-date" in red). Underneath, it says: "Upgrade to get the most recent version: heartbeat-11.0-2017080312116". At the bottom, there is a grey button labeled "Reboot the system".

Aktualisieren Sie nun das Browserfenster. Die neugeladene Seite sollte dann so aussehen:



### 3.4 SYSTEM – HERUNTERFAHREN-SEITE

Diese Seite hat Buttons zum Herunterfahren und Neustarten des Geräts.



Hinweis: Der DIVUS HEARTBEAT verwendet akustische Signale beim Herunterfahren und nach dem Neustart. Das Herunterfahren-Signal ist *hoch-tief*, das Neustart-Signal ist *mittel-tief-mittel-hoch*. Bitte warten Sie immer auf das Neustartsignal (wenn vor Ort) um sicher zu sein, dass das Gerät vollständig gebootet hat und läuft – besonders vor einem neuen Netzwerksan.

### 3.5 DIVUS NETZWERK – BERICHT-SEITE

Diese Seite zeigt den Bericht, welcher das Ergebnis des letzten durchgeführten Netzwerksans ist (siehe 3.6). Er zeigt ein grafisches Schema aller entdeckten Geräte und detaillierte Infos über jedes einzelne in tabellarischer Form.

Unter Anderem findet man hier von jedem Gerät:

- Hostname (wenn verfügbar)
- IP-Adresse
- MAC-Adresse
- Port an dem sie verbunden sind (am HEARTBEAT oder am DMS)
- Abhängig vom Gerätetyp, andere Details z.B. Software/Firmware-Version, Uptime, Sprache usw.



Hinweis: Während dem Scan liefern DIVUS-Geräte durch das SNMP-Protokoll mehr Details über ihren Status und ihre Einstellungen als Drittherstellengeräte. Darum ermöglicht der Einsatz von DIVUS-Geräten,

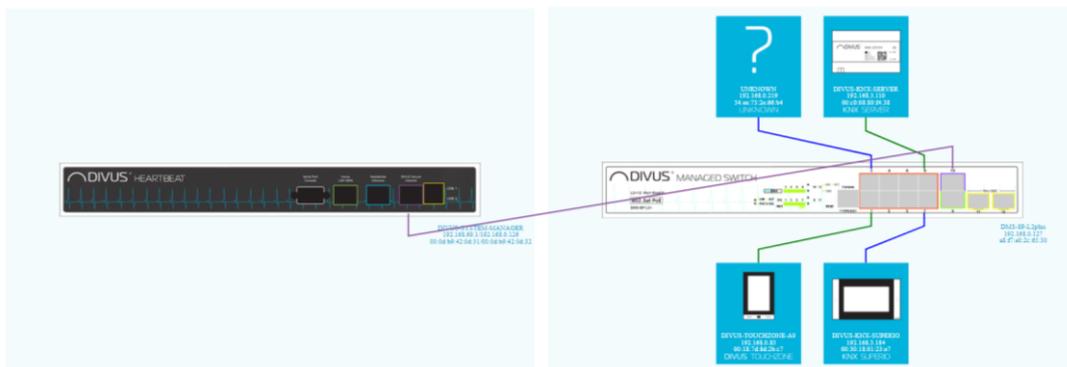
das volle Potential Ihres DIVUS HEARTBEAT auszureizen. Drittherstellergeräte können jedenfalls Basisinformationen liefern wie ihre IP-Adresse, ihren Namen und natürlich den Netzwerkport, an dem sie angeschlossen sind.

### 3.5.1 DAS GRAFISCHE SCHEMA

Das grafische Schema zeigt das Hauptgerät (ein MANAGER oder ein MANAGED SWITCH) und alle damit verbundenen Geräte rundherum. Linien zeigen, welches Gerät an welchem Port verbunden ist. Zusätzlich wird eine Farbkodierung gebraucht, die über die verfügbare Bandbreite deutet:

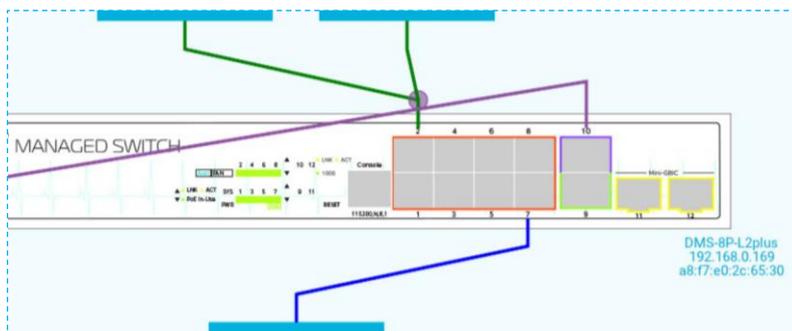
GRÜNE LINIE	1000 Mbit/s
BLAUE LINIE	100 Mbit/s
VIOLETTE LINIE	Manager-zu-Switch oderr Switch-zo-Switch-Verbindung (1000 Mbit/s)

In der Regel gibt es also zwei Schemata mit hellblauem Hintergrund, auf denen der MANAGER mit seinen angeschlossenen Geräten (erstes Schema) und der MANAGED SWITCH mit seinen angeschlossenen Geräten (zweites) zu sehen sind. Wenn andere Switches angeschlossen sind, werden zusätzliche Schemata hinzugefügt, die ein großes Netzwerkschema bilden.



DIVUS-Geräte werden erkannt und mit einem passenden Bild angezeigt. Nicht erkannte Geräte werden mit einem Standard-Fragezeichen angezeigt.

Wenn Drittanbieter-Switches erkannt werden, wird ein Knoten (violetter Punkt) auf der Verbindungslinie angezeigt, der signalisiert, dass mehr als ein Gerät an den angezeigten Port angeschlossen ist.



Die beiden Hauptgeräte (MANAGER und MANAGED SWITCH) werden mit ihrem Namen und ihrer IP- und MAC-Adresse angezeigt.

Schon beim ersten Blick auf das grafische Schema haben Sie sofort einen visuellen Überblick über den Status des Netzwerks und sehen, welches Gerät an welchem Port angeschlossen ist.



Hinweis: Wurde ein Gerät überhaupt nicht erkannt, prüfen Sie bitte zuerst die physikalische Verbindung: Ursache könnte das Kabel oder die Stecker des Kabels sein. Andere mögliche Ursache: Das Gerät befindet sich möglicherweise in einem anderen Netzwerk mit einer statischen IP-Adresse. In Kapitel 6.1 wird gezeigt, wie man mit einem solchen Fall umgeht.

### 3.5.2 DIE PDF-DATEI DES BERICHTS

Die PDF-Datei enthält die gleichen Informationen wie der Bericht auf der Website und einige zusätzliche Details: Die Titelseite zeigt den Projektnamen und die Namen und Adressen von Systemintegrator und Kunde und es gibt spezielle Seiten, die die Firewall- und Portweiterleitungsregeln zeigen. So ist die Berichtsdatei fast wie eine Papierversion eines Backups. Mit ihr werden Sie in der Lage sein

- zu sehen / sich zu merken, was genau der Netzwerkstatus zum Zeitpunkt des Scans war
- ihre Arbeit vor Ort deutlich zu beweisen
- zu überprüfen, ob etwas geändert wurde, nicht mehr vorhanden ist oder im Vergleich zum Scanzeitpunkt nicht mehr funktioniert.

---

## 3.6 DIVUS NETZWERK – FÜHRE SCAN DURCH

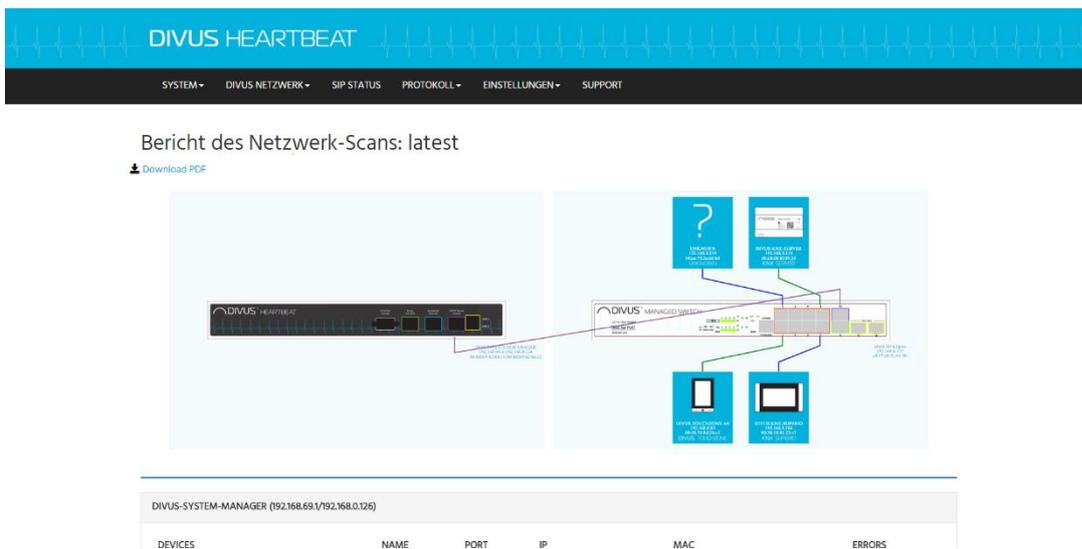
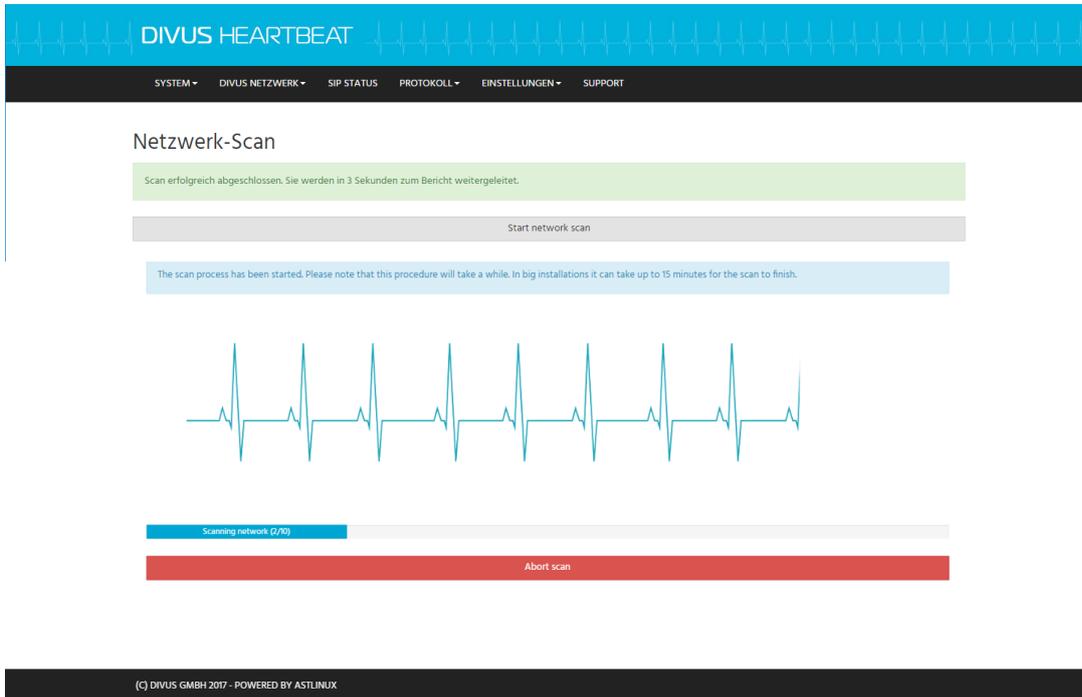
---

Von dieser Seite aus wird ein neuer Netzwerkskan gestartet oder der Status eines laufenden Scans abgefragt.



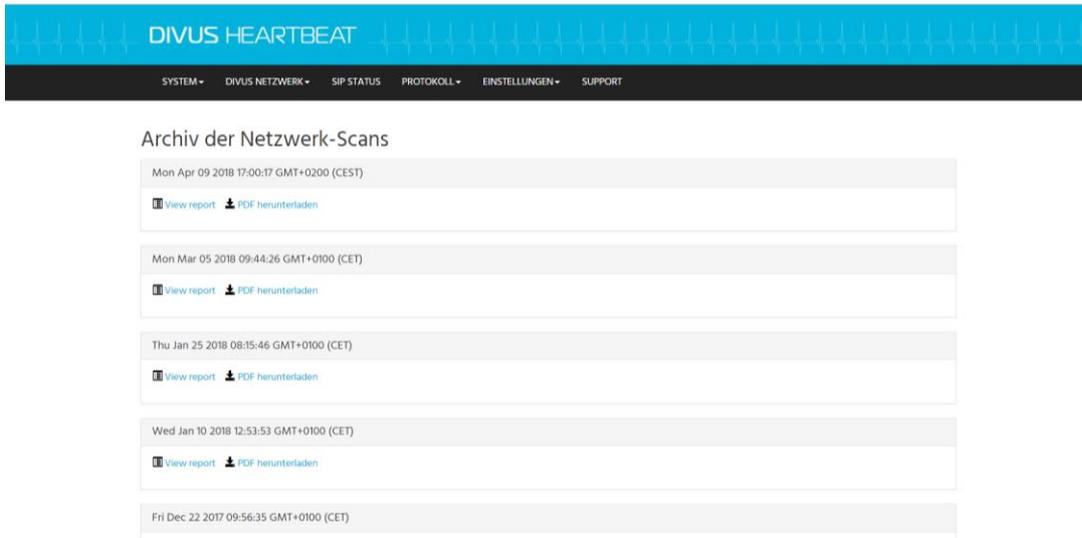
Sobald Sie die Scan-Taste gedrückt haben, sehen Sie den Fortschritt des Scans grafisch über einen Fortschrittsbalken. Abhängig von der Anzahl der angeschlossenen Geräte kann der Scan mehrere Minuten dauern.

Sobald er fertig ist, werden Sie automatisch auf die Berichtsseite weitergeleitet. (Siehe 3.5)



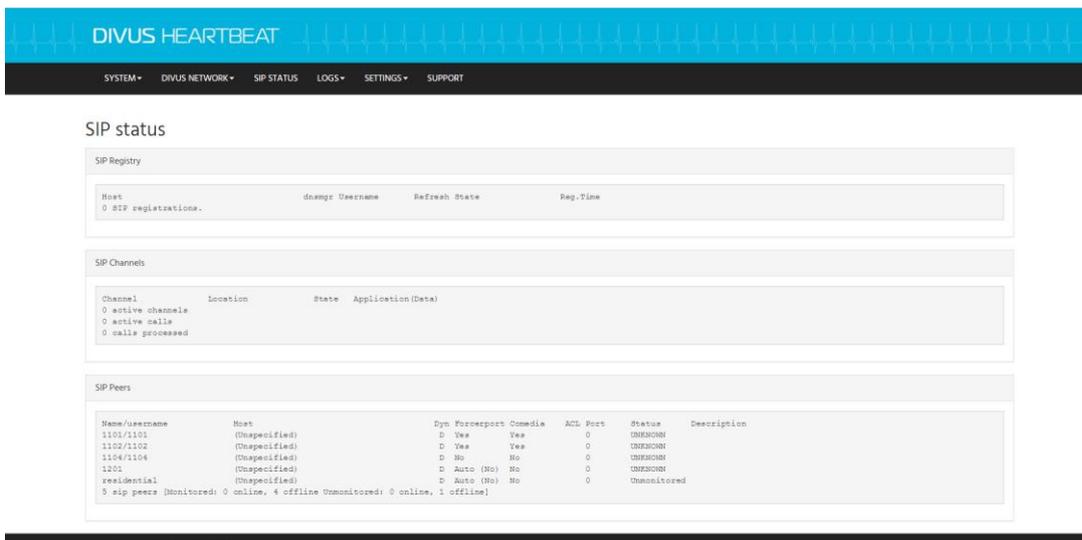
### 3.7 DIVUS NETZWERK – ARCHIV-SEITE

Hier finden Sie eine Liste der Netzwerkscans und können diese im Browser öffnen oder als PDF herunterladen.



### 3.8 SIP STATUS-SEITE

Diese Seite zeigt den Status Ihres Intercom-Systems (Registry, Channels und Peers) an, wenn Sie den DIVUS HEARTBEAT als VoIP / SIP-Server konfiguriert haben. Besonders die Status-Spalte der SIP-Peers-Tabelle ist nützlich, um zu sehen, ob alle Geräte registriert und erreichbar sind.



### 3.9 PROTOKOLL – SWITCH LOGS-SEITE

Der MANAGED SWITCH protokolliert alle Aktivitäten an seinen Ports. Obwohl diese Aktivitäten bloss zeigen, ob ein Port aktiv ist oder nicht und PoE verwendet oder nicht, kann dies beim Troubleshooting von Geräten sehr nützlich sein. Wenn z.B. Ein Gerät neu gestartet wird, wird es protokolliert.

Es gibt eine mächtige Filter- / Suchfunktion, mit der nur die interessanten Einträge angezeigt werden können. Details und Beispiele zur Protokollfilterung finden Sie in Kapitel 6.2

---

### 3.10 PROTOKOLL – VOIP/SIP LOGS-SEITE

---

Der SIP / VoIP-Server zeigt hier sein Protokoll an. Siehe Kapitel 6.2 für die Filter- / Suchfunktion.

---

### 3.11 PROTOKOLL – GESPRÄCHSPROTOKOLL-SEITE

---

Alle Anrufe werden protokolliert: Ihre Zeit und Dauer finden Sie hier. Siehe Kapitel 6.2 für die Filter- / Suchfunktion.

---

### 3.12 EINSTELLUNGEN – SYSTEM-SEITE

---

Diese Einstellungen (Projektname, Hostname, Domäne, Zeitzone und Sprache) wurden während des ersten Setups angezeigt. Wenn Sie sie später ändern müssen, können Sie dies hier tun.

The screenshot shows the 'Systemeinstellungen' (System Settings) page in the DIVUS HEARTBEAT interface. The page has a blue header with the 'DIVUS HEARTBEAT' logo and a black navigation bar with menu items: SYSTEM, DIVUS NETZWERK, SIP STATUS, PROTOKOLL, EINSTELLUNGEN, and SUPPORT. The main content area is titled 'Systemeinstellungen' and contains several input fields and a checkbox. The fields are: 'Projektname\*' with the value 'BV DIVUS', 'Hostname\*' with 'dnh-heartbeat', 'Domäne\*' with 'divus', 'Zeitzone\*' with 'Europe/Berlin', and 'Sprache\*' with 'Deutsch'. Below these is a checkbox labeled 'Ich erlaube das Senden der Daten auf die DIVUS-Cloud' which is checked. A blue 'Speichern' (Save) button is located at the bottom left of the form.

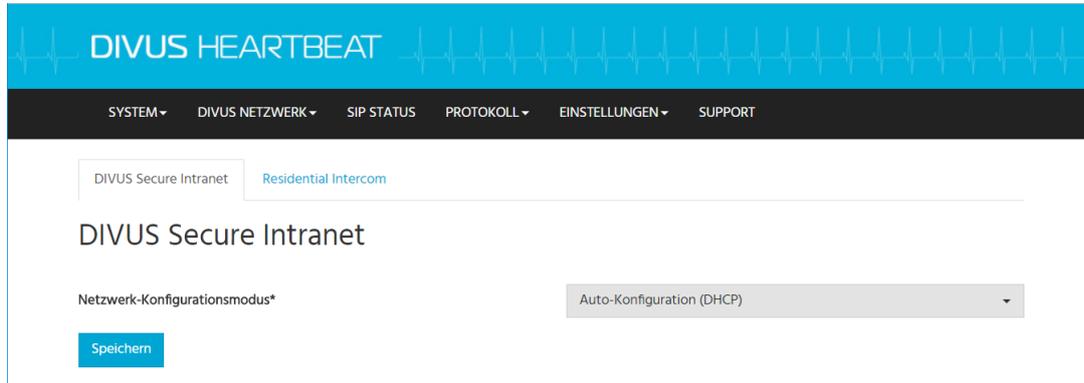
Projektname*	BV DIVUS
Hostname*	dnh-heartbeat
Domäne*	divus
Zeitzone*	Europe/Berlin
Sprache*	Deutsch

Ich erlaube das Senden der Daten auf die DIVUS-Cloud

[Speichern](#)

### 3.13 EINSTELLUNGEN – NETZWERK

Die Netzwerkeinstellungen für das Home LAN oder das RIN können hier bei Bedarf geändert werden. Wenn Sie bereits beim ersten Setup-Assistenten die richtigen Einstellungen gewählt haben, müssen Sie hier nichts ändern.



#### 3.13.1 DHCP

##### 3.13.1.1 DSI

Damit der DIVUS HEARTBEAT ein Netzwerk auch dann automatisch verwaltet, wenn Änderungen an der Netzwerkstruktur vorgenommen werden, ist es zwingend erforderlich, DHCP zu verwenden und statische IP-Adressen für das DSI-Netzwerk zu vermeiden. Obwohl es möglich ist, feste Adressen zu verwenden, empfehlen wir dringend, dies zu vermeiden. Die Rolle des DHCP-Servers kann dem DIVUS HEARTBEAT zugewiesen werden, aber diese Rolle wird automatisch an ein anderes Gerät weitergegeben, wenn ein solches Gerät erkannt wird. Aus diesem Grund überwacht der DIVUS HEARTBEAT ständig das Netzwerk für DHCP-Aktivitäten von Drittanbietern - sowohl wenn er die DHCP-Server-Rolle spielt als auch wenn er selbst ein DHCP-Client eines anderen Geräts ist, auf dem ein DHCP-Server läuft. Dies ermöglicht dem DIVUS HEARTBEAT, die Rollen nach Bedarf zu wechseln. Von Server zu Client, wenn ein anderer Server vorhanden ist, von Client zu Server, wenn ein vorheriger Server nicht mehr antwortet.

##### 3.13.1.2 RIN



Wenn die DHCP-Server-Funktion für das RIN eingesetzt wird, muss im Vorfeld sichergestellt werden, dass kein anderes Gerät in diesem Netzwerk einen aktiven DHCP-Dienst anbietet!

Schauen wir uns die möglichen Szenarien an und die besten Einstellungen für jedes von diesen:

1. Ein einziges Gerät, das an das Residential Intercom-Netzwerk angeschlossen ist. In diesem Fall ist es die beste Lösung, das RIN auf "Manuelle Konfiguration" zu setzen und eine statische IP-Adresse auf dem Gerät festzulegen (z. B. 192.168.69.10).
2. Zwei oder mehrere Geräte, die an einen DIVUS MANAGED SWITCH am RIN angeschlossen sind. Die Adresse des DMS kann nicht auf statisch gesetzt werden. Daher haben wir diese möglichen Fälle:
  - A. Wenn Sie das RIN auf "Manuelle Konfiguration" einstellen und die DHCP-Serverfunktion aktivieren, werden alle Geräte erreichbar. **Voraussetzung ist, dass kein anderes Gerät im RIN über einen laufenden DHCP-Dienst verfügt.** Natürlich müssen alle Geräte auf den DHCP-Modus eingestellt sein. Nachdem Sie das Kontrollkästchen *DHCP-Server* aktiviert haben, müssen Sie den

entsprechenden Adressbereich definieren. Beachten Sie, dass die Adresse des Managers (IP-Adressfeld), das Feld für die Netzmaske und die Felder für den DHCP-Bereich alle miteinander verknüpft sind und bei der Übermittlung auf Richtigkeit überprüft werden. Das Feld für die Gateway-Adresse kann leer bleiben.

- B. Ein anderes Gerät hat einen laufenden DHCP-Dienst. In diesem Fall wird durch Setzen des RIN auf "Auto-Konfiguration (DHCP)" die DHCP-Client-Funktion aktiviert, wodurch alle Geräte erreichbar werden. Natürlich müssen alle Geräte auf den DHCP-Modus eingestellt sein.
  - C. Wenn Sie das RIN auf "Manuelle Konfiguration" einstellen, wird der DMS für den Manager unsichtbar. Er wird ein normaler Switch (nicht „managed“). Sie werden die Details über den DMS in den Netzwerk-Scans verlieren, wo er als ein unbekannter Switch angezeigt wird, und die DMS-Protokolle werden auch nicht verfügbar sein. Nichtsdestotrotz funktionieren die Client-Geräte, sobald sie auf eine statische IP-Adresse des gewählten IP-Netzwerks eingestellt sind, normal. Wenn Sie dieses Netzwerk auf statische Adressen einstellen müssen, ist dies derzeit die einzige Möglichkeit mit einem DMS.
3. Zwei oder mehrere Geräte, die mit einem Drittanbieter-Switch im RIN verbunden sind. Wenn Sie einen Switch eines Drittanbieters verwenden, um Ihre Geräte mit dem RIN zu verbinden, wird dieser als unbekannter Switch angezeigt und Sie verlieren die in 2-C beschriebenen Funktionen. Abgesehen davon wird auch alles andere wie oben beschrieben sein.

---

### 3.14 EINSTELLUNGEN – SMART DEVICES-SEITE

---

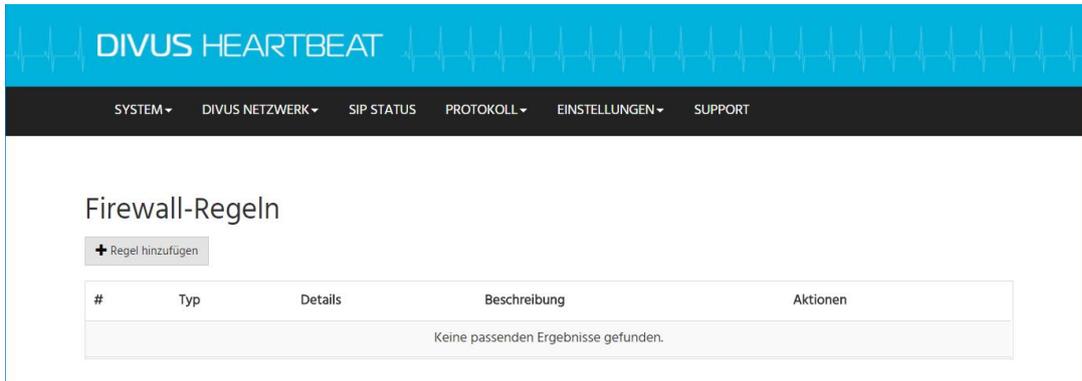
Auf dieser Seite können einige spezielle Gerätetypen aktiviert werden, die häufig in intelligenten Gebäuden verwendet werden und spezifische Netzwerkports und Protokolle verwenden. Die Liste der unterstützten Geräte wird mit der Zeit wachsen.



Wenn Sie Ihren Smart Device-Typ hier nicht finden können, können Sie ihn dennoch in Kenntnis seiner Kommunikationskanäle und Protokolle integrieren und entsprechende Firewall- und / oder Port-Forwarding-Regeln erstellen. Siehe Kapitel 6.5 und 6.56.6.

### 3.15 EINSTELLUNGEN – FIREWALL REGELN-SEITE

Auf dieser Seite werden die Firewall-Regeln des DIVUS HEARTBEAT verwaltet.



**DIVUS HEARTBEAT**

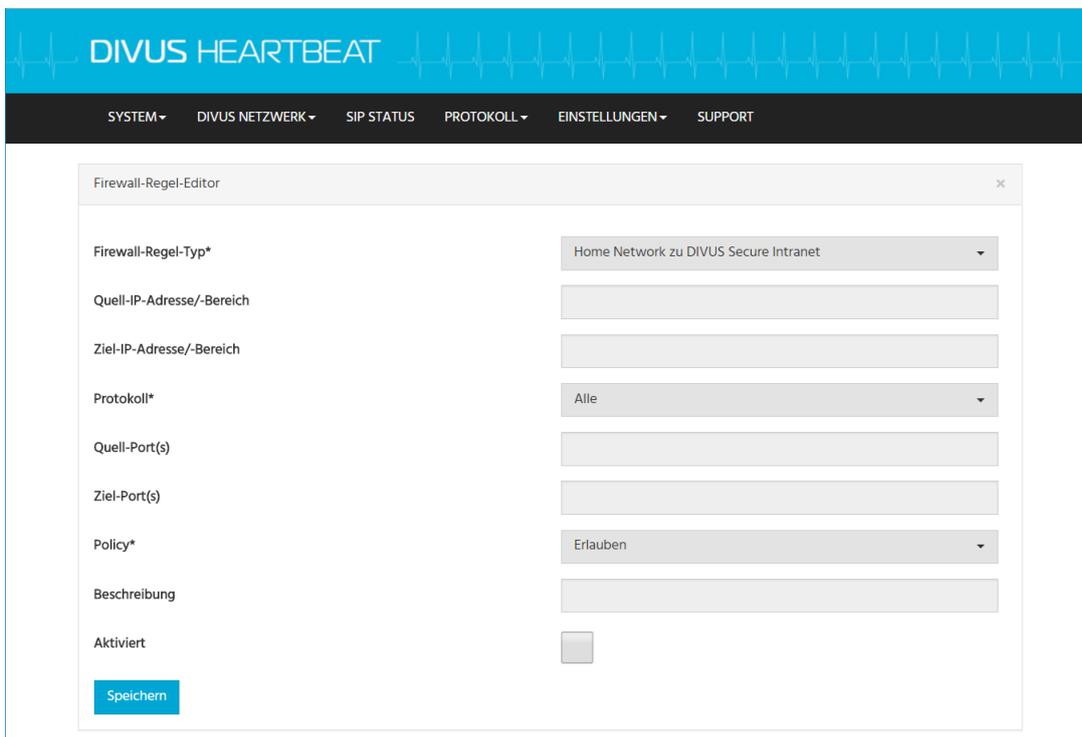
SYSTEM ▾ DIVUS NETZWERK ▾ SIP STATUS PROTOKOLL ▾ EINSTELLUNGEN ▾ SUPPORT

## Firewall-Regeln

[+ Regel hinzufügen](#)

#	Typ	Details	Beschreibung	Aktionen
Keine passenden Ergebnisse gefunden.				

Wenn Sie die Schaltfläche "+ Regel hinzufügen" drücken, wird das Formular zum Definieren einer neuen Regel angezeigt. Detaillierte Anweisungen zum Erstellen von Firewall-Regeln finden Sie in Kapitel 6.5.



**DIVUS HEARTBEAT**

SYSTEM ▾ DIVUS NETZWERK ▾ SIP STATUS PROTOKOLL ▾ EINSTELLUNGEN ▾ SUPPORT

Firewall-Regel-Editor ×

Firewall-Regel-Typ\* Home Network zu DIVUS Secure Intranet ▾

Quell-IP-Adresse/-Bereich

Ziel-IP-Adresse/-Bereich

Protokoll\* Alle ▾

Quell-Port(s)

Ziel-Port(s)

Policy\* Erlauben ▾

Beschreibung

Aktiviert

[Speichern](#)

### 3.16 EINSTELLUNGEN – PORT-FORWARDING-REGELN-SEITE

Ähnlich wie auf der Seite FIREWALL-REGELN können Sie mit der Schaltfläche "+ Regel hinzufügen" neue Portweiterleitungsregeln hinzufügen.

Angesichts der speziellen Namensauflösungsstrategie, die für den DIVUS HEARTBEAT und seine Netzwerke angewendet wird, spielt die Portweiterleitung eine wichtige Rolle. Wenn Sie eine Portweiterleitung auf dem DIVUS HEARTBEAT verwenden, bedeutet dies, dass Sie den

`dhb-heartbeat`

-Namen und einen gewählten Port nutzen können, anstelle einer IP-Adresse, die sich in Zukunft durch Netzwerkänderungen (z. B. einen neuen Router) ändern könnte. Wenn z.B. ein Gerät in der DSI die IP-Adresse 192.168.0.5 und einen Dienst auf dem TCP-Port 81 hat, können Sie ihn nach dem Hinzufügen dieser Regel mit

`dhb-heartbeat:9000`

aufrufen:

<i>Schnittstelle einkommend:</i>	Alle (oder ein spezifisches Netzwerk)
<i>Protokoll:</i>	TCP
<i>Port einkommend:</i>	9000
<i>Quell-IP-Adresse/-Bereich<sup>2</sup>:</i> z.B.	192.168.0.0/24 (was alle 192.168.0.x-Geräte von 1 bis 254 bedeutet)
<i>Ziel-IP-Adresse:</i>	192.168.0.5
<i>Ziel-Port:</i>	81



Hinweis: Wenn Sie einen DIVUS KNX SERVER verwenden, wird der DIVUS HEARTBEAT diesen während des Netzwerkscan erkennen und automatisch einige spezielle Regeln hinzufügen, so dass Sie diese nicht manuell hinzufügen müssen. Siehe Kapitel 5.4.1

<sup>2</sup> IP-Adressbereiche werden mit der sogenannten CIDR-Notation angegeben. Siehe [hier](#) für eine Erläuterung.

---

### 3.17 EINSTELLUNGEN – SIP EINSTELLUNGEN-SEITE

---

Hier erhalten Sie Zugriff auf die beiden Hauptkonfigurationsdateien für die SIP / VoIP-Serverfunktion.

Siehe Kapitel 4.2. um das vordefinierte Nummerierungsschema zu verstehen. Informationen zum Bearbeiten von SIP-Accounts oder zum Erstellen von Gruppenrufen finden Sie in Kapitel 6.3 und **Fehler! Verweisquelle konnte nicht gefunden werden.**

# 4 Intercom

Intercom ermöglicht Sprach- und Videokommunikation - hauptsächlich für die Türkommunikation, aber auch für die Raum-zu-Raum-Kommunikation. Die folgenden Beschreibungen und Erläuterungen beschränken sich auf Geräte, die den SIP-Standard für Audio- und IP-Kameras für Video unterstützen - alle verwenden ein TCP/IP-Netzwerk zur Verbindung. Ein typisches Setup könnte folgendermaßen aussehen:



In den meisten Fällen kann der DIVUS HEARTBEAT als Plug-and-Play-VoIP-Server verwendet werden. Wenn Sie also nur die Konfigurationen der Clients mit unserem Standardkonfigurationsschema einstellen, werden diese sich verbinden und laufen - ohne Eingriff in die Konfiguration des DIVUS HEARTBEAT.

Der DIVUS HEARTBEAT verwendet ein sehr flexibles Schema, um jede Komplexität von Intercom-Systemen zu ermöglichen. Bitte lesen Sie den folgenden Teil sorgfältig, um das Schema für alle Geräte, die Sie einrichten möchten, zu verstehen und zu verwenden.

## 4.1 ALLGEMEINE DEFINITIONEN

1. Selbst die komplexeste Intercom-Struktur baut auf einer Standard-Basiseinheit auf (siehe 4.2.1). Diese Standardeinheit (normalerweise eine Wohnung) verfügt über interne Geräte, die an den DIVUS HEARTBEAT der Einheit

angeschlossen sind. Zur Vereinfachung und Bezugnahme nennen wir diese **ZONE 1**.

2. Außerdem kann diese Einheit eine externe Einheit für Anrufe von der Tür des Flurs oder von der Haustür haben - aber jedenfalls ein Gerät für die spezifische Einheit / Wohnung. Wir definieren dieses Gerät als zu **ZONE 2** gehörend. (Also hat jede Einheit ZONE 1-Geräte und kann zusätzlich auch ZONE 2-Geräte haben)
3. In der Regel wird es im Außenbereich ein oder mehrere Geräte geben - z.B. am Eingangstor. Wir nennen diese die **EXTERNEN EINHEITEN**.
4. In Häusern mit einer Rezeption / einem Concierge können auch besondere Geräte vorhanden sein, mit der Möglichkeit, alle anzurufen und von allen angerufen zu werden.

---

## 4.2 ALLGEMEINES VOIP-ACCOUNT-SCHEMA (FÜR ZONE 1 UND ZONE 2)

---

Die Standardkonfiguration des Intercom-Systems des DIVUS HEARTBEAT verwendet dieses Schema

Name	VoIP number / SIP Account	Default password
AABCC	AABCC	AABCC
Wo A: der Einheitsnummer entspricht, von 1 anfangend z.B. 1, 24, 99 B: der Zone entspricht, 1 or 2 (1 interne Geräte, 2 externe Geräte) C: der Gerätenummer entspricht, von 01 bis 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 definiert 13101 das Gerät 01 der internen Geräte der Einheit 13, während 1101 das Gerät 01 unter den internen Geräten der Einheit 1 anruft. Eine Einheit entspricht normalerweise einer Wohnung. Bei größeren Systemen könnte dieses Schema leicht geändert werden in z.B. AABCCC oder AAABCC.

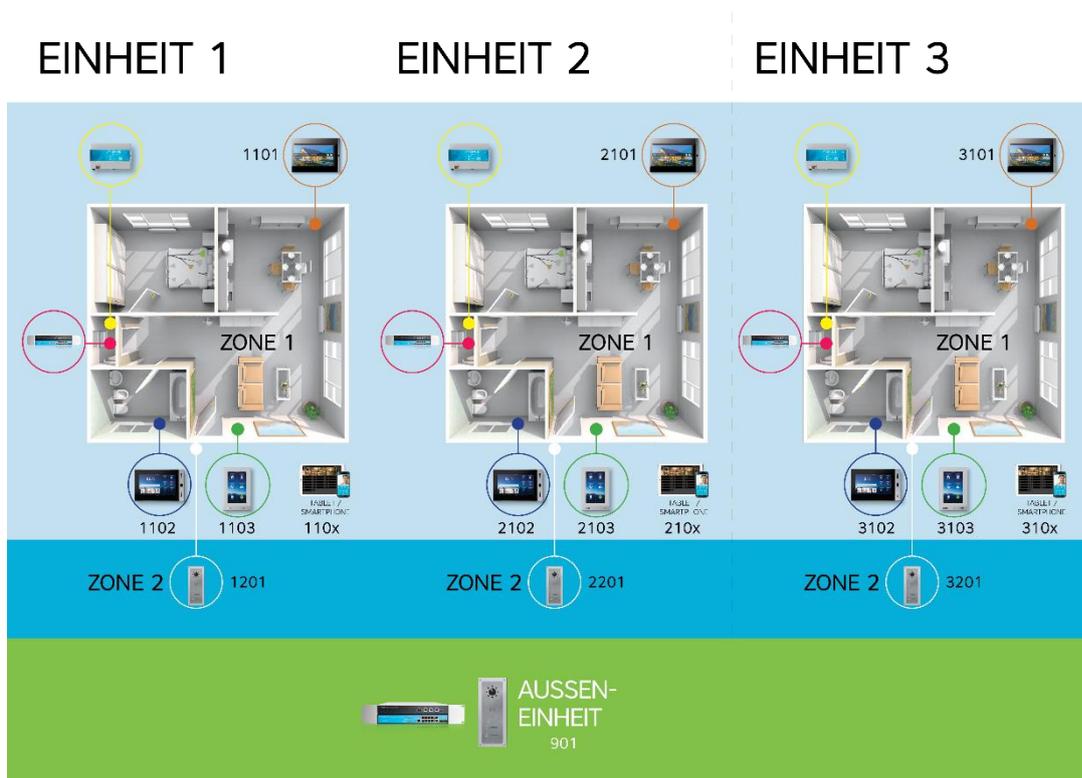
4.2.1 BASISEINHEIT

Alle Systeme haben eine Basiseinheit mit einer Reihe vordefinierter Einstellungen

# EINHEIT 1



Diese Basiseinheit wird dann wie ein Baustein für alle übrigen Einheiten wiederholt:



#### 4.3 VOIP ACCOUNTS FÜR EXTERNE EINHEITEN

EXTERNE EINHEITEN verwenden das gleiche Schema, das in DIVUS-Systemen vor der Einführung des DIVUS HEARTBEAT verwendet wurde. Also, die erste externe Einheit wird Account 901 und Passwort 901 haben, die zweite 902 mit Passwort 902 und so weiter.

Name	VoIP-Nummer / SIP-Account	Standard-Kennwort
901 Externe Einheit 1	901	901
902 Externe Einheit 2	902	902

#### 4.4 CONCIERGE / RECEPTION ACCOUNTS

Wenn ein oder mehrere Concierge- / Receptionposten Teil der Intercomanlage sind, werden diese ab 801 nummeriert.

Name	VoIP-Nummer / SIP-Account	Standard-Kennwort
801 Concierge/Reception Einheit 1	801	801
802 Concierge/Reception Einheit 2	802	802



Achtung! Diese Standardaccounts sind vorhanden, damit das erste Setup und Testen schnell und einfach durchgeführt werden können. Sobald das System erfolgreich getestet wurde, müssen Sie alle Passwörter der Accounts ändern, um sicherzustellen, dass externe Zugriffe nicht auf sie zugreifen. Einzelheiten zur Bearbeitung Ihrer VoIP-Accounts finden Sie in Kapitel 6.3.

Einzelheiten zum Hinzufügen, Bearbeiten oder Löschen einzelner SIP-Konten oder Gruppenanrufe zu Ihrem Intercom-System finden Sie in den Kapiteln 6.3 und 6.4 **Fehler! Verweisquelle konnte nicht gefunden werden.**

# 5 Client-Geräteeinrichtung für DSI und RIN

Die folgenden Einstellungen werden empfohlen, um das Potenzial des DIVUS HEARTBEAT vollständig zu nützen. Sie sind jedoch nicht obligatorisch. Wenn Sie es vorziehen oder wenn Sie dazu verpflichtet sind, können Sie wie gewohnt IP-Adressen verwenden. Der Vorteil, den Sie verlieren würden, ist die Fähigkeit des DIVUS HEARTBEAT, sich an Netzwerkänderungen anzupassen, ohne dass Sie eingreifen müssen - außer in sehr seltenen Fällen.

In allen folgenden Einstellungen wird als Hostname des DIVUS HEARTBEATS der Standardwert `dhb-heartbeat` vorausgesetzt. Wenn Sie den Hostnamen geändert haben, müssen Sie diesen neuen Namen immer dort verwenden, wo `dhb-heartbeat` angezeigt wird. Der HEARTBEAT spielt ausserdem standardmäßig die VoIP-Serverrolle für Intercom.

---

## 5.1 DIVUS TOUCHZONE

---

Der DIVUS TOUCHZONE soll, wie der DIVUS KNX SERVER / KNX SUPERIO, mit dem DSI (DIVUS Secure Intranet) verbunden sein.

### OPTIMA-App

Verwenden Sie vom DSI aus `dhb-heartbeat` anstelle der IP-Adresse und 3000 oder 3001 als Port. Wenn Sie 3001 verwenden, überprüfen Sie auch den SSL-Schutz. Alle anderen Einstellungen können wie gewohnt gewählt werden.

### VIDEOPHONE 4-App

Verwenden Sie `dhb-heartbeat` als VoIP-Server-Adresse. Alle anderen Einstellungen bleiben die üblichen.

---

## 5.2 DIVUS SUPERIO UND ANDERE WINDOWS-BASIERTE DIVUS-GERÄTE

---

Als URL für die OPTIMA-Visualisierung verwenden Sie  
`https://dhb-heartbeat:3000` oder `https://dhb-heartbeat:3001`.

Verwenden Sie als VoIP-Server in der Anwendung VIDEOPHONE auch `dhb-heartbeat`.

---

## 5.3 DIVUS OPENDOOR

---

Das Standard-Netzwerk für Außenstationen ist das Netzwerk 192.168.69.0/24 (d.h. das RIN). Wenn Sie es nicht in etwas anderes geändert haben, sollten Sie Folgendes verwenden: 192.168.69.1 als VoIP server – die Verwendung von `dhb-heartbeat` wird zurzeit nicht unterstützt!

Als IP-Adressen für die einzelnen Geräte (OD-SIP und OD-Cam) müssen Sie auch IP-Adressen dieses Netzwerks auswählen z.B 192.168.69.120 bzw. 192.168.69.121.

Alle anderen Einstellungen bleiben die üblichen. Bedenken Sie, dass das RIN-Netzwerk generell nur vom DSI aus erreichbar ist. Wenn Sie von woanders aus auf die OPENDOOR zugreifen müssen, müssen Sie dafür einen Port öffnen.

---

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

---

An den Geräteeinstellungen ändert sich nichts direkt. Um mit dem DIVUS HEARTBEAT kommunizieren zu können und somit während des Netzwerkscan Informationen zur Verfügung zu stellen, benötigen Sie ein Gerät mit OPTIMA Version 2 in der neuesten Version.

Beachten Sie auch, dass die VoIP-Serverrolle, wenn sie zuvor von diesem Gerät gehalten wurde, an den DIVUS HEARTBEAT übergeben werden sollte.

Wenn Sie einen integrierten Intercom-Client direkt über den Browser ausführen müssen, können Sie in OPTIMA (auf einem Windows-basierten Panel oder auf dem KNX SUPERIO) die VoIP-Serverrolle aus den OPTIMA Intercom-Einstellungen an den HEARTBEAT weiterleiten. Verwenden Sie in diesem Fall 192.168.69.1 als IP-Adresse des VoIP-Servers - dort ist der stellvertretende Hostname als Eintrag nicht möglich.

### 5.4.1 SONDERREGELN FÜR DIVUS KNX SERVER UND KNX SUPERIO

Der Netzwerkscan ist nicht nur wichtig für die Erstellung eines Berichts. Er ist auch wichtig, weil für diese speziellen Geräte (KNX SERVER und KNX SUPERIO), sobald sie im Scan erkannt werden, einige Regeln automatisch hinzugefügt werden, um die Interaktion mit ihnen zu erleichtern. Hier sind sie, jeweils mit einer kurzen Erklärung:

Ziel	Wie erreichbar	Erklärung
KNX SERVER/KNX SUPERIO über HTTP	<code>http://&lt;ip address&gt;</code>	Erlaubt den Geräten des Home-Netzwerks, über die Ports 80 und 443 auf das Webinterface von KNX SERVER / KNX SUPERIO im DSI zuzugreifen. Die Firewall Regel öffnet also automatisch Port 80 und 443 des KNX SERVER / KNX SUPERIO für das Home Lan.
KNX SERVER/KNX SUPERIO über HTTPS	<code>https://&lt;ip address&gt;</code>	
KNX SERVER/KNX SUPERIO über HTTP	<code>https://dnh-heartbeat:3000</code>	Ermöglicht den Zugriff auf den KNX SERVER / KNX SUPERIO über den Namen des DIVUS HEARTBEAT und diese speziellen Ports: 3000
KNX SERVER/KNX SUPERIO über HTTPS	<code>https://dnh-heartbeat:3001</code>	Weiterleitung auf 80, 3001 Weiterleitung auf 443. Wenn es einen zweiten KNX SERVER / KNX SUPERIO gäbe, würde er die Ports 3002 bzw. 3003 verwenden und so weiter.

*Also, welchen sollte ich benutzen?*

Im Allgemeinen verwenden Sie `https` für höhere Sicherheit. Zwischen der direkten Verwendung der IP-Adresse oder der Weiterleitung über den DIVUS HEARTBEAT empfehlen wir letztere für die größtmögliche Flexibilität und für ein möglichst unbeaufsichtigtes System auch nach Netzwerkänderungen. Wenn diese Auswahl für Sie nicht verfügbar oder möglich ist, wählen Sie die Alternative.

---

## 5.5 IP-KAMERAS VON DRITTANBIETERN

---

Sie sollten sie so einstellen, dass sie eine IP-Adresse des RIN erhalten.

---

## 5.6 DRITTANBIETER-CLIENT-GERÄTE (MIT ETHERNET-SCHNITTSTELLE)

---

Verwenden Sie die allgemeinen Regeln der anderen Abschnitte: Wenn das Gerät dies unterstützt, verwenden Sie `dhb-heartbeat` als Serveradresse / -name. Verwenden Sie andernfalls eine IP-Adresse des entsprechenden Netzwerks: DSI oder RIN, abhängig vom Gerätetyp und vom Installationsort.

Einzelheiten zu den möglichen Verbindungsmöglichkeiten zu einem DIVUS KNX SERVER / KNX SUPERIO finden Sie in Kapitel 5.4.1.

---

## 5.7 ANALOGE DRITTHERSTELLERGERÄTE

---

Sie können die DIVUS Videophone-Box verwenden, ein spezielles Gerät, das ein analoges Türöffnergerät mit Video- und Audioquellen in eines umwandeln kann, das SIP-Anrufe ins Innere tätigen und Videos über eine URL streamen kann. Sie können [hier](#) das Handbuch für weitere Details finden.

# 6 Erweiterte Themen

---

## 6.1 EIN GERÄT MIT EINER STATISCHEN IP-ADRESSE IN DAS HEARTBEAT-NETZWERK HOLEN

---

Folgen Sie diesen Schritten:

1. Stellen Sie sicher, dass sich Ihr Laptop und das Gerät im selben physischen Netzwerk befinden: z.B. das DSI.
2. Stellen Sie die IP-Adresse Ihres Laptops auf das gleiche Netzwerk als das zu ändernde Gerät ein.  
z.B.:

Das Gerät ist im Netzwerk 192.168.178.x: Stellen Sie die Adresse Ihres Laptops auf 192.168.178.250 – wenn diese Adresse derzeit frei ist.

3. Jetzt können Sie mit dem Gerät kommunizieren: Ändern Sie seine Netzwerkeinstellungen in die des neuen Netzwerks. Im Idealfall bedeutet dies, dass DHCP eingestellt wird. Sollte das Gerät DHCP nicht unterstützen, setzen Sie seine statische IP-Adresse auf das gleiche Netzwerk wie den DIVUS HEARTBEAT. Stellen Sie sicher, dass die zugewiesene IP-Adresse derzeit frei ist.

z.B. Der Heartbeat ist auf 192.168.0.11: Setzen Sie die IP-Adresse des Geräts auf 192.168.0.210.

4. Speichern Sie die Änderungen auf dem Gerät, starten Sie es gegebenenfalls neu.
5. Machen Sie die geänderten Netzwerkeinstellungen des Laptops rückgängig.
6. Starten Sie nun einen neuen Netzwerksan auf dem DIVUS HEARTBEAT und das Gerät mit seinen Eigenschaften sollte im Scanbericht aufscheinen.

## 6.2 VERWENDUNG DER LOG-FILTER- / SUCH-FUNKTION

Die Protokollseiten haben eine solche Struktur:

The screenshot shows the DIVUS HEARTBEAT interface. At the top, there is a navigation bar with menu items: SYSTEM, DIVUS NETWORK, SIP STATUS, LOGS, SETTINGS, and SUPPORT. Below this is a search bar labeled 'QUERY' with a search icon and a 'Time filter refreshes every 15m' indicator. The main content area is divided into three sections:

- SWITCHES EVENTS COUNT:** A bar chart showing event counts for various IP addresses. The data is as follows:
 

IP Address	Count
192.168.0.149	66
192.168.0.179	38
192.168.0.145	30
192.168.0.114	6
192.168.0.111	4
192.168.0.172	1
- SWITCHES EVENTS COUNT:** A table showing event counts for various terms. The data is as follows:
 

Term	Count	Action
192.168.0.149	66	Q
192.168.0.179	38	Q
192.168.0.145	30	Q
192.168.0.114	6	Q
192.168.0.111	4	Q
192.168.0.172	1	Q
- SWITCH EVENTS:** A table showing event details. The data is as follows:
 

timestamp	host	device	type	text
2017-12-05T14:26:14+00:00	192.168.0.172	DMS-8P-L2plus	switch	Link up on port 10

Die untere Tabelle kann eine lange Liste von Einträgen enthalten. Wie können wir diese Seite effizient nutzen, um uns nur die relevanten Informationen zu zeigen? Der obere Teil enthält eine Abfrageleiste, die wir für diesen Zweck verwenden können

The screenshot shows the search bar with the query "\*" entered. The search icon is on the right.

Das \*-Symbol bedeutet *alles*, daher ist standardmäßig keine Filterung aktiv.

Wenn wir den Eintrag zu *Link* ändern und das Linsensymbol drücken, werden nur Einträge mit diesem Schlüsselwort angezeigt und alle anderen werden versteckt.

The screenshot shows the search bar with the query "Link" entered. The search icon is on the right.

Wenn wir z.B. *Link up* verwenden, wird die Antwort wahrscheinlich nicht die gewünschte sein. Der Grund dafür ist, dass die Eingabe mehrerer Wörter / Strings gleichbedeutend ist mit "Suche nach Einträgen, die *Link* enthalten oder Einträge, die *up* enthalten". Höchstwahrscheinlich wird das, was wir stattdessen wollen, durch Einfügen von "*Link up*" erhalten.

The screenshot shows the search bar with the query "Link up" entered. The search icon is on the right.

Sie können auch die logischen Operatoren mit Großbuchstaben z.B. *Link AND up* oder komplexere Formen wie ("*Link up*" ODER "*Link down*") UND "*Port 4*".

Eine weitere Möglichkeit ist das Hinzufügen von Abfragen mit dem "+" - Symbol auf der rechten Seite..

The screenshot shows the search bar with multiple queries: "Link up", "Link down", and "\*". The search icon is on the right.

## 6.3 VOIP-ACCOUNTS AUF DEM DIVUS HEARTBEAT BEARBEITEN

So fügen Sie einen neuen VoIP-Account hinzu:

1. Gehen Sie zu EINSTELLUNGEN - SIP-EINSTELLUNGEN. Scrollen Sie nach unten zu einem der folgenden Einträge:

2. Kopieren Sie den gesamten Abschnitt von [1101] nach call-limit = 1 (alles inklusive)
3. Fügen Sie den Block am Ende der Datei ein. Dann bearbeiten Sie ihn, indem Sie alle Vorkommen der Accountnummer (in diesem Beispiel 1101) auf die Nummer des neuen Kontos (z. B. 1115) ändern.

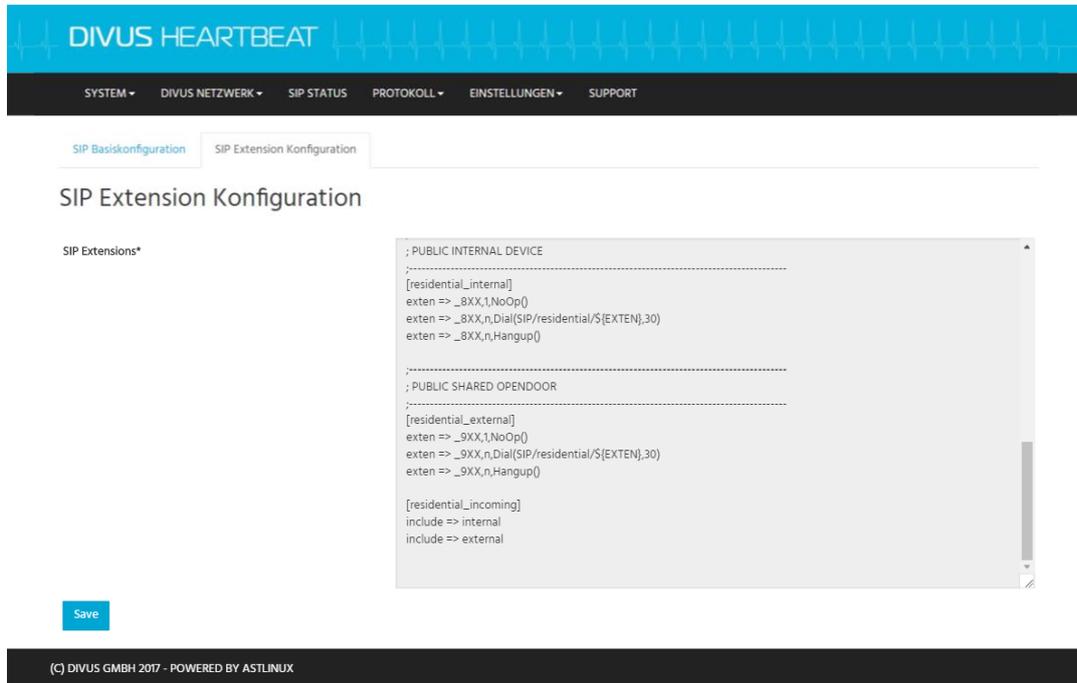
```
[1101]
username=1101
type=friend
secret=1101
qualify=10000
port=5060
nat=yes
host=dynamic
dtmfmode=rfc2833
context=phones
canreinvite=no
callerid=1101<1101>
call-limit=1
```

4. Ändern Sie das Passwort (secret) in eine längere, sicherere Reihenfolge. (Sie sollten dies für alle von Ihnen verwendeten VoIP-Accounts tun!)
5. Zuletzt speichern! Warten Sie dann ein paar Sekunden, bis die neuen Einstellungen wirksam sind.

## 6.4 VOIP-GRUPPENRUFE AUF DEM DIVUS HEARTBEAT DEFINIEREN

Ein Gruppenruf ermöglicht es, mehrere Geräte gleichzeitig anzurufen. Dann wird die Kommunikation zwischen dem Anrufer und dem ersten Angerufenen hergestellt, der antwortet – die anderen Geräte hören gleichzeitig auf zu klingeln. Wenn niemand antwortet, wird das Klingeln fortgesetzt, bis eine Zeitüberschreitung erreicht wird, die am HEARTBEAT oder an der Außenstation konfiguriert werden kann.

Ein neuer Gruppenruf benötigt nur zwei Zeilen, die der SIP Extensions-Konfigurationsdatei hinzugefügt werden müssen, die Sie auf der Seite EINSTELLUNGEN - SIP-EINSTELLUNGEN sehen und bearbeiten können (beachten Sie die Registerkarte *SIP Extension Konfiguration*):



Die Zeilen sehen so aus:

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

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

Erklärung:

Die erste Zeile legt fest, welche Nummer für den Gruppenruf verwendet werden soll und welche Accounts Teil der Gruppe sein sollen. Die Nummer 12345 ruft zwei SIP-Accounts an: 1101 und 1102. Das Hinzufügen einer zusätzlichen Nummer (z.B. 3405) ist einfach: Fügen Sie einfach "SIP / 3405" zur bestehenden Accountskette hinzu, indem Sie das "&" Symbol verwenden.

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

30 ist die Anzahl der Sekunden, die geklingelt werden sollte bzw. die Timeout-Zeit. In der zweiten Zeile wird dieselbe Nummer 12345 wiederholt.

Sobald Ihre 2 Zeilen fertig sind, fügen Sie sie am Ende des Abschnitts ein, der mit [internal] beginnt:

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

```

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

exten => 12345,1,Dial($SIP/11018.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 yellow highlight is placed over the lines: `exten => 12345,1,Dial($SIP/11018.SIP/1102,30)` and `exten => 12345,2,Hangup()`. A blue 'Save' button is located at the bottom left of the editor area. The footer of the page reads '(C) DIVUS GMBH 2017 - POWERED BY ASTLINUX'.

Dann speichern Sie und Sie sind bereit, die neue Rufnummer zu testen.

## 6.5 SO ERSTELLEN/BEARBEITEN SIE EINE BENUTZERDEFINIERTER FIREWALL-REGEL

Bedenken Sie vor dem Start Folgendes:

- Das DSI ist für den freien Zugriff auf alle anderen Netzwerke konfiguriert.
- Home-Netzwerk und DSI sind durch eine Firewall getrennt d.h. vom Home-Netzwerk in Richtung DSI besteht standardmäßig eine Sperre.
- Das RIN ist durch eine Firewall geschützt und auch physisch ein separates Netzwerk
- Firewall-Regeln können zum Öffnen, aber auch zum Schließen von Ports verwendet werden, falls erforderlich.
- Wenn ein Feld leer gelassen wird, entspricht das der Definition "irgendeines" z.B. ein leeres Quell-Port(s)-Feld bedeutet, dass die Regel für jeden Quellport gilt. Mit anderen Worten, der Quellport fungiert nicht als Filter.

Befolgen Sie dieses Verfahren:

Feld	Wert oder Beispiel	Erklärung
Firewall-Regel-Typ	Home zu DSI, Home zu RIN, RIN zu DSI, RIN zu Home, DSI zu Home, DSI zu RIN	Wählen Sie die Firewall und die Kommunikationsrichtung aus, die zugelassen oder gesperrt werden soll.
Quell-IP-Adresse/-Bereich	192.168.0.0/24 (bedeutet alle IP-Adressen die mit 192.168.0. anfangen)	Wählen Sie die Quell-IP-Adresse oder den Quelladressenbereich, auf den die Regel angewendet werden soll. Angaben mit CIDR-Notation.
Ziel-IP-Adresse/-Bereich	192.168.69.7	Wählen Sie die einzelne Ziel-IP-Adresse oder den Bereich der Zieladressen aus, für die die Regel definiert werden soll.
Protokoll	Alle, TCP, UDP, ICMP	Wählen Sie das Protokoll, auf das die Regel angewendet werden soll.
Quell-Port(s)	80,81,82,83	In der Regel leer gelassen – also für jeden Quellport.
Ziel-Port(s)	8080	Ein Port oder eine Gruppe von Ports (getrennt durch Kommata ohne Leerzeichen), denen die Firewall den Zugriff gewähren (oder verweigern) soll.
Policy	Erlauben, Blockieren, Abweisen	Welche Aktion die Regel verursachen soll. A
Beschreibung		Verwenden Sie dieses Feld, um die Regel leichter zu erkennen, wenn Sie mehrere benutzerdefinierte Regeln erstellen möchten.
Aktiviert	aktiviert / deaktiviert	Verwenden Sie das Kontrollkästchen, um die Regel vorübergehend anzuwenden oder zu deaktivieren.

## 6.6 BENUTZERDEFINIERTER PORTWEITERLEITUNGSREGELN ERSTELLEN

Eine Portweiterleitungsregel ermöglicht es, ein Gerät unter Verwendung des Namens eines anderen Geräts zu erreichen. In diesem Fall können wir den Namen `ahb-heartbeat` mit einem benutzerdefinierten Port verwenden und ein anderes Gerät erreichen, das als Server im selben Netzwerk verwendet wird. Wie zuvor erläutert, ist der Vorteil, dass wir die IP-Adresse des Geräts nicht kennen müssen und wir uns keine Sorgen machen müssen, falls sich diese IP-Adresse eines Tages vollständig ändern sollte. Wir werden den Namen des DIVUS HEARTBEAT und seinen intelligenten Namensauflösungsmechanismus verwenden, um immer in der Lage zu sein, unsere Zielgeräte zu erreichen.

Feld	Wert oder Beispiel	Erklärung
Schnittstelle einkommend	Alle, DIVUS Secure Intranet, Residential Intercom, Home Network	Wählen Sie, auf welchen der drei Netzwerkports des MANAGERS gezielt zugegriffen wird
Protokoll	TCP UDP	Wählen Sie das Protokoll
Port einkommend	z.B. 50000 (Port des HEARTBEAT)	Wählen Sie einen freien Port
Quell-IP Adresse/-Bereich	192.168.1.0/24	Wählen Sie eine einzelne Adresse oder einen Bereich oder erlauben Sie alle Geräte im Netzwerk (siehe Eingangsschnittstelle)
Ziel-IP-Adresse	192.168.1.110	Fügen Sie die Adresse des Zielgeräts ein. Dieses Feld kann nicht leer gelassen werden.
Ziel-Port	80	Wenn es sich um die Weboberfläche handelt, verwenden Sie 80. Beachten Sie andernfalls das Handbuch des Geräts. Dieses Feld kann nicht leer gelassen werden.
Beschreibung		Verwenden Sie dieses Feld, um die Regel später leichter zu erkennen, wenn Sie mehrere benutzerdefinierte Regeln erstellen möchten.
Aktiviert	aktiviert / deaktiviert	Verwenden Sie das Kontrollkästchen, um die Regel vorübergehend anzuwenden oder zu deaktivieren.

## 6.7 EIN GERÄT FÜR DEN REMOTEZUGRIFF AUF DAS INTERCOM-SYSTEM EINRICHTEN

Bitte beachten Sie, dass der Remote-Zugriff auf Ihr System bedeutet, dass **die Sicherheit Ihres Systems durch das Öffnen eines Zugriffskanals vom Internet aus beeinträchtigt wird**. Wenn Sie diese Funktionalität trotzdem benötigen, führen Sie die folgenden Schritte aus:

1. Fügen Sie Ihrem Internet-Router eine Port-Weiterleitungsregel hinzu: Verwenden Sie einen beliebigen externen Port - verwenden Sie nicht 5060 und natürlich niemals die, bei denen bekannte Dienste wie 80, 443 usw. laufen. Diese sollten an Port 5060 Ihres DIVUS HEARTBEAT weitergeleitet werden. Verwenden Sie in diesem Fall die IP-Adresse 192.168.69.1 - oder, falls Sie diese geändert haben, die neue - als Ziel. Verwenden Sie den ausgewählten Port in Ihren Client-Konfigurationen.
2. Stellen Sie sicher, dass die für den Fernzugriff verwendeten Geräte die korrekten Einstellungen der SIP-Parameter verwenden:
  - `nat=force_rport,comedia`

- `qualify=20000`
- `directmedia=no`
- `localnet=192.168.69.0/24,192.168.0.0/24`
- `externip` Od. `externhost=[öffentliche IP-Adresse od. Domainname]`

Wenn diese Einstellungen korrekt sind, wird die Stimme über den SIP-Kanal übertragen. Daher sind keine zusätzlichen Portweiterleitungen für RTP erforderlich.

Zum Anzeigen von VIDEO von einer IP-Kamera während eines SIP-Anrufs benötigen Sie möglicherweise eine zusätzliche Portweiterleitung zum Port 80 (normalerweise) der Kamera. Die DIVUS Videophone 4 App hat dafür einen besonderen Platz: Verwenden Sie die öffentliche IP oder den Domainnamen, die gewählte externe Portnummer und so wird nun während eines Intercom-Anrufs auch das Video angezeigt.



