



CERTIFICATION DOCUMENTATION SHEET

AutoPilot™ User Interface

Company :	A.I.Pilot GmbH	Issue :	Revision R1
Location :	Hohenstein-Ernstthal, Germany	Date :	20-01-2020
Project Name :	-	Pages :	60
Product Name:	AutoPilot™ User Interface	Doc No:	AIP-CDS-009-ZIP_GWA.docx

© 2019 A.I.Pilot GmbH. All rights reserved. Under copyright laws, this document may not be copied, in whole or in part, without the written consent of A.I.Pilot GmbH.

Other company and product names mentioned herein are trademarks of their respective companies. Mention of third-party products is for informational purposes only.

Table of Contents

1	Change Control History	3
2	Introduction	4
2.1	Readership	4
2.2	Applications	4
3	Product Range and Description.....	5
4	AutoPilot™ – User Interface (UI).....	6
4.1	What is AEOTEC ID™	7
4.2	Setup AutoPilot™ with AEOTEC ID™	7
4.3	Initial Landing Page Explained	11
4.4	Views Explained	13
4.4.1	Login	13
4.4.2	Dashboard.....	14
4.4.3	Rooms.....	16
4.4.4	Elements	18
4.4.5	Moments	23
4.4.6	Automation	24
4.4.7	Analytics.....	25
4.4.8	Menu	26
4.5	Apps	27
4.6	Devices	29
4.6.1	Manage Z-Wave Devices	30
4.6.2	Manage Z-Wave Network.....	43
4.6.3	Z-Wave SmartStart	46
4.7	Customize	47
4.7.1	Create Your own Icons.....	47
4.7.2	Create an Icon Pack.....	47
4.7.3	Upload your Icon Set.....	47
4.8	My Settings	49
4.9	Management	50
4.9.1	User Management.....	50
4.9.2	Remote Access	51
4.9.3	Time Zone	51
4.9.4	Backup & Restore	51
4.9.5	Factory Default.....	53
4.9.6	Firmware Update.....	53
4.9.7	App Store Access.....	54
4.9.8	Report Problem	54
4.9.9	Info	54
4.10	News	54
5	Association – Supported Lifeline Reports	55
6	Command Class Reference	56
7	Documentation Attachments	58
8	Contents	59
9	References.....	60

1 Change Control History

Issue	Date	Change Description	Author
R1	02-05-2019	First Release, Management / Control API Documentation	NR
R2	20-06-2019	First Revision for Certification	NR
R3	26-07-2019	Assoc Lifeline Reports and CC Reference added	NR
R4	06-09-2019	Old Setup with new AEOTEC Id setup replaced (WIP)	NR
R5	25-10-2019	Ad Hoc Certification Release	NR
R6	30-10-2019	Ad Hoc Certification Release - Fixes	NR
R7	04-11-2019	Ad Hoc Certification Done - Minor Fixes	NR
R8	20-01-2020	Add Information about DSK placement on the box (Market Cert)	NR
R9	31.01.2020	Do more adjustments for Market Cert	NR

2 Introduction

2.1 Readership

The audience of this document is considered to be Marketing Managers, Product Managers, Design Engineers and 3rd party partners who may be involved in the design / development / production of the product detailed herein.

It is necessary that the reader is familiar with the complete, proposed product range.

It is necessary that the reader is familiar with Z-Wave Technology and its terminologies.

2.2 Applications

Application detailed in this document must be used for:

- Residential Home Automation
- Commercial Building Automation inclusive of public and private spaces in hotels.

3 Product Range and Description

The product detailed in this document forms part of the AEOTEC Z-Wave product range.

The product is intended for residential applications.

The product is designed for the following target groups:

- expert smart home user like installers etc.

4 AutoPilot™ – User Interface (UI)

The graphical user interface of the AutoPilot™ is considered as a main control interface based on the ZWare™ library of Sigma Designs. It can be operated in any Z-Wave network with other Z-Wave certified devices from other manufacturers. All mains operated nodes within the network will act as repeaters regardless of vendor to increase reliability of the network.

The interface is designed and developed by A.I.Pilot GmbH, a 100% daughter company of the AEOTEC™ group and was influenced and inspired by Z-Way™ from Z-Wave.Me.

Similar to the Z-Way™ Smart Home interface, the AutoPilot™ user interface follows some very clear logic which was developed by Prof. Christian Paetz and presented the first time on the Smart Home Summit 2014 in Munich/Germany.

Based on the Z-Way™ Smart Home interface, the following basic rules apply:

1. **Elements:**

Every function of any physical device (endpoint) is shown as one single element (widget). In case it has multiple functions, like switching and metering, it will be rendered as multiple elements. All elements are listed in an elements view and can be filtered by their function type (switch, dimmer, sensor, ...) or other filtering criteria.

2. **Elements Configuration:**

Every element offers a configuration interface for changing names, removing it from the screens, etc. Important elements can be placed in the Dashboard. To avoid overhead, not necessary elements can be disabled for view and logics. Besides, elements can be assigned to different rooms.

3. **Moments (formerly “Event”):**

Every change in a sensor value, a switching status or system notification is called a “Moment” and is shown in a timeline called “Moments”. Filtering allows monitoring the changes of a specific source or device.

4. **Apps:**

All non-Z-Wave specific functions such as time-triggered actions, automation rules, the use of information from the internet, scenes, plugins of other third-party technologies and services are realized in apps accessible in the setup menu.

4.1 What is AEOTEC ID™

AutoPilot™ uses the AEOTEC Single-Sign-On Service **AEOTEC ID™** to make your login experience as much safe and easy as possible.

You simply create one account to use all services available under AEOTEC ID™:

- Remote Access to your AutoPilot(s)™
- Remote Control Center
- Developer Center

During setting up your AutoPilot™ you will be asked to connect it to your AEOTEC ID™. Just follow the steps in the next section 4.2 to get your AutoPilot™ work with AEOTEC ID™.

4.2 Setup AutoPilot™ with AEOTEC ID™

1. Connect the AutoPilot™ to your local network using the ethernet slot
2. Connect the 5V power supply and put the AutoPilot™ into operation
3. Navigate in your browser (Chrome, Firefox, Safari) to the following homepage:
<https://setup.aeotec.com> (Fig. 1)

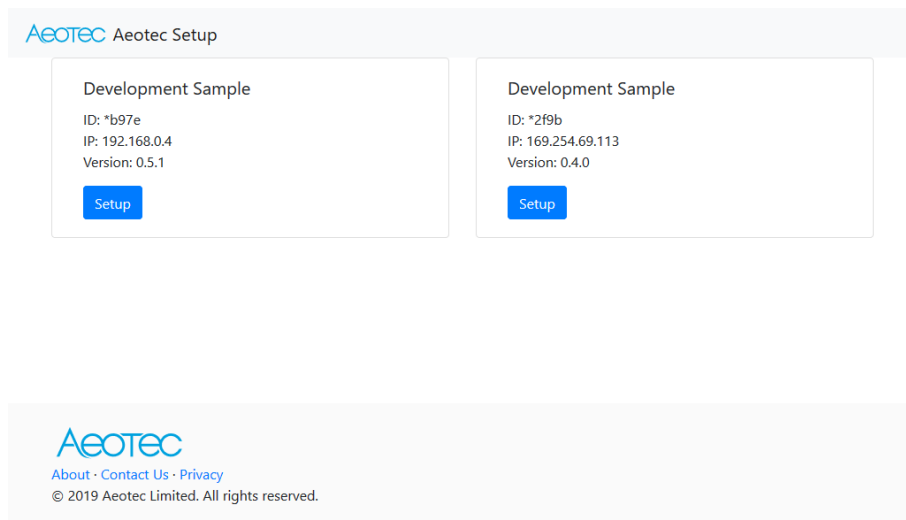


Fig. 1: Homepage: <https://setup.aeotec.com>

4. There you will find one of the following two possible variants. Continue with the corresponding instructions:
 - a. Only one AutoPilot™ was found in your local network:
→ You will be redirected to <https://id.aeotec.com> (Figs. 2 and 3)
 - b. Several AutoPilot™ Gateways were found in your local network:
→ From the list of available AutoPilot™ gateways,

select the one you want to set up.
→ Click on **Setup** (Fig. 1)

If your AutoPilot™ is not yet visible, reload the page. If necessary, check the ethernet connection and restart the device by disconnecting it from the power supply for a short time and retry the first steps.

To register your AutoPilot™ via the AEOTEC ID™, the address <https://home.aeotec.com> can also be used as an alternative to <https://id.aeotec.com>.

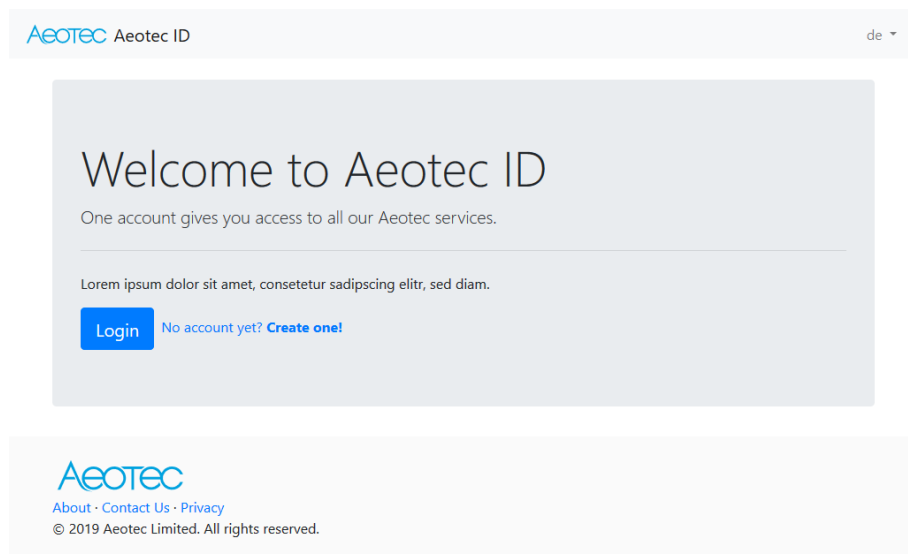


Fig. 2: Homepage: <https://id.aeotec.com>

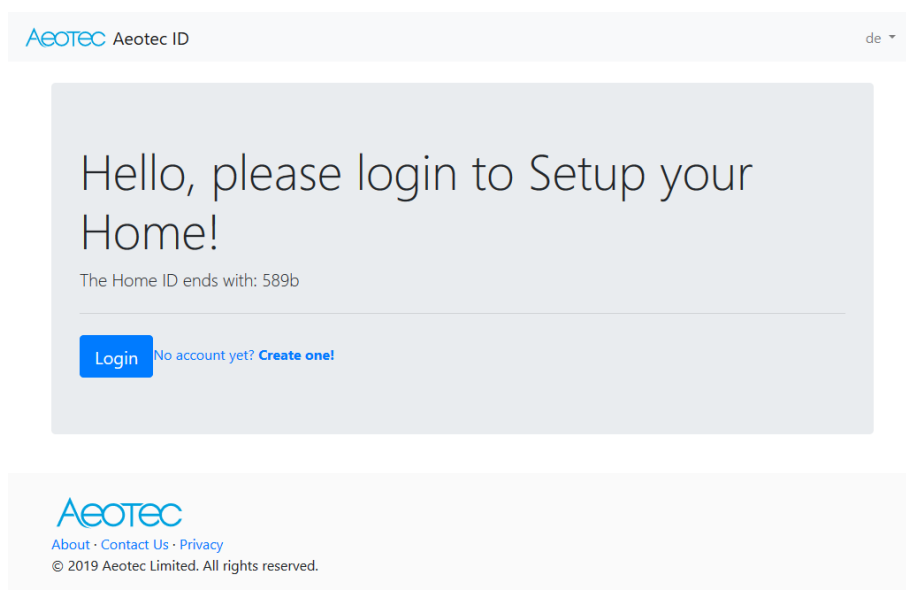
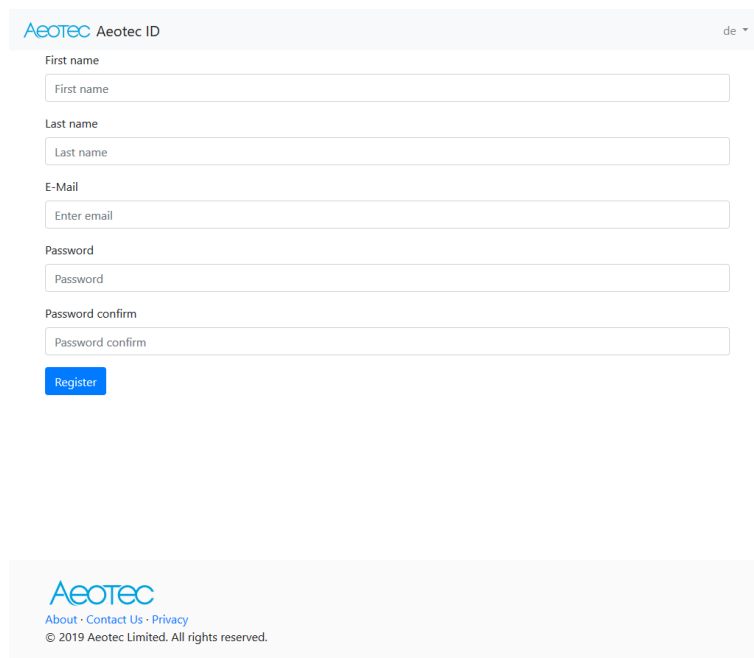


Fig. 3: Forwarding AutoPilot setup

5. Login with your credentials to AEOTEC ID™ (Fig. 2) to connect the AutoPilot™ to your account
 - a. You already have an AEOTEC ID™ Account?
 - Just log in (Fig. 6)
 - You will be forwarded to the **Setup/Connect Dialog** (Fig. 7)
 - b. You don't have an account yet?
 - Click on **No account yet? Create one!** (Fig. 2 and 3)
 - After the successful creation of a new AEOTEC ID™ account (Fig. 4), an e-mail verification is performed (Fig. 5).
 - You will be forwarded to the **Setup/Connect Dialog** (Fig. 7)



Aeotec ID de ▼

First name
First name

Last name
Last name

E-Mail
Enter email

Password
Password

Password confirm
Password confirm

[Register](#)

Aeotec
[About](#) · [Contact Us](#) · [Privacy](#)
 © 2019 Aeotec Limited. All rights reserved.

Fig.4: AEOTEC ID – create new account

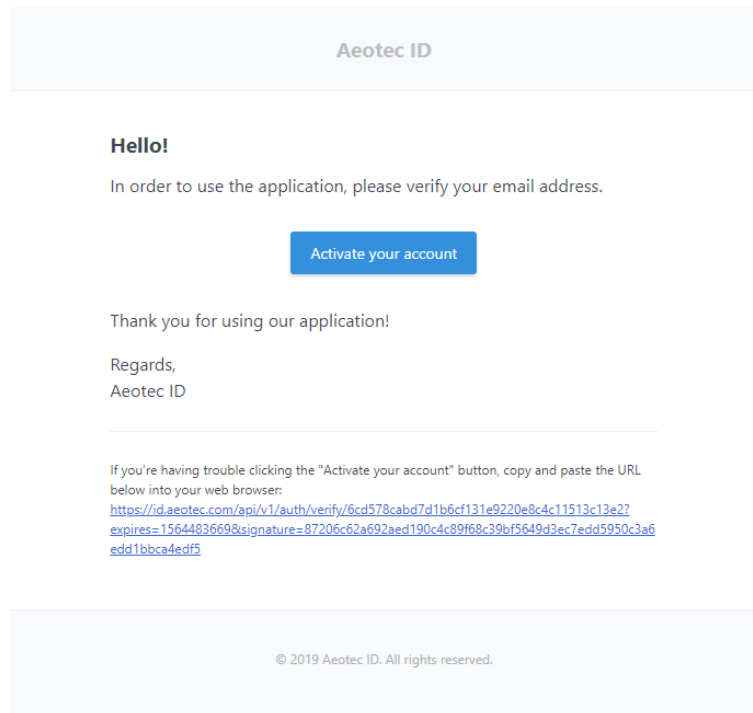


Fig. 5: E-mail validation

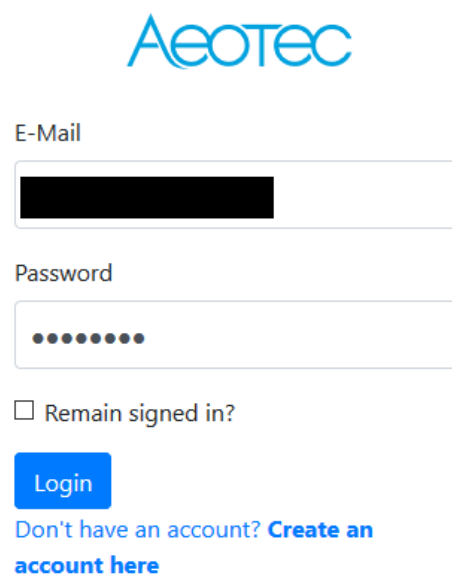


Fig. 6: AEOTEC ID login

6. Click Connect to connect AutoPilot™ to your AEOTEC ID™ account (Fig. 7)

→ You will then be redirected directly to the initial setup interface of the AutoPilot™

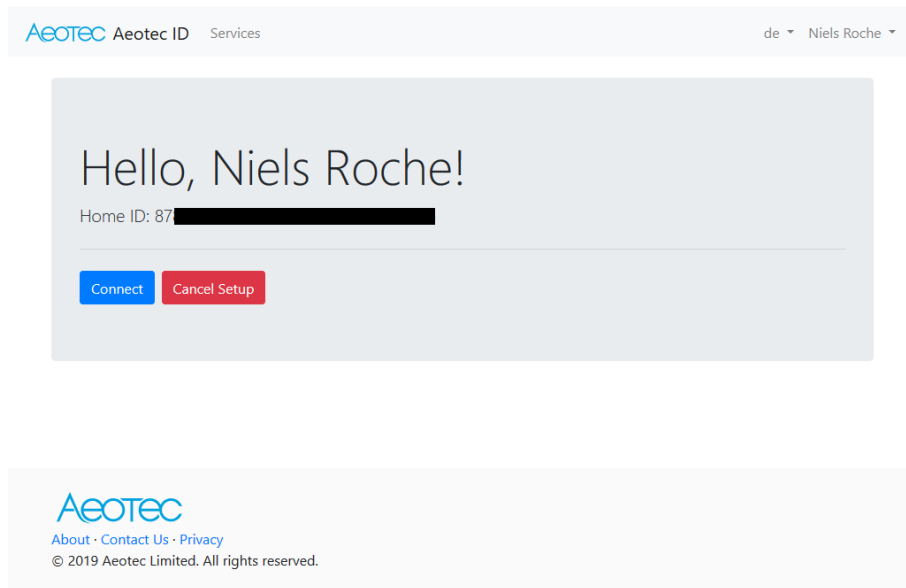


Fig. 7: Connect Dialog

7. Do further readings on section *4.3 Initial Landing Page Explained*

4.3 Initial Landing Page Explained

If the AutoPilot™ is accessed first time you will see the Initial Setup page (Figure 4.2). Here you can define the:

- Default administrator password (MANDATORY)
 - MUST at least 8 characters long
 - MUST contain one number (0-9)
 - MUST contain one character (a-z, A-Z)
 - MUST contain one special character (@\$_-!\$+.,;:~\{}()[]~<>|!=%*#?`'^^o"')&)
- UI language (EN, DE, RU, ...)
- The email address, which is used for password reset, notifications and cloud backups
- Enable support of speech assistants like Amazons Alexa.

After submitting the initial setup configuration, you will be forwarded to the Dashboard, which is the main landing page of your AutoPilot™. This view collects all important information at a glance and give you quick access to your favorite widgets. More information you will get in section [4.3.2](#).



Welcome to your AutoPilot

! You need to set the password for the admin user. (minimum 8 characters long and should contain at least one number (0-9), one character (a-z,A-Z) and one special character(@\$_-\$+.,,:/{}()~<>|!=%*#?'`"~&))

Gateway ip address: 192.168.0.7

Select language: 

Login: **admin**

***Insert new password:**

***Retype password to confirm:**

Email:

! Please provide the email address in case you loose your password. Also get access to additional features e.g. CloudBackup.

✓ Submit

Figure 4.2: Initial Setup

On first access the *Welcome to your Smart Home* slideshow on the dashboard (Figure 4.3) will give you a quick introduction to familiarize yourself with the AutoPilot™ interface. Press **Next >** to start the slideshow or **Skip** to jump over.

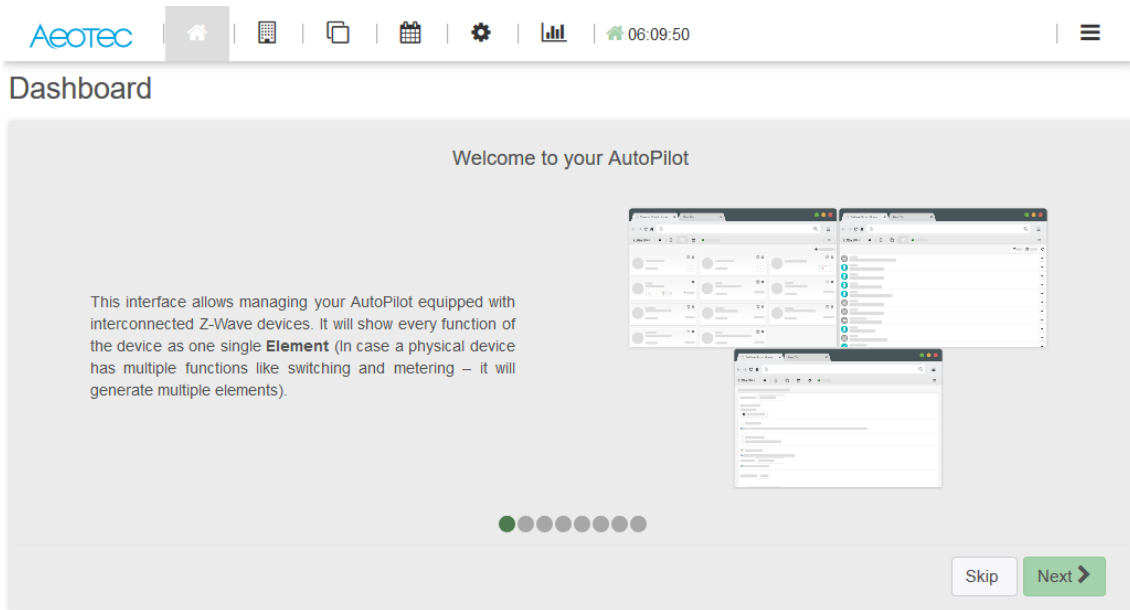


Fig. 9: AutoPilot - Introduction

4.4 Views Explained

The following headlines explain all main views of the AutoPilot™ interface which can be accessed, excluding the login page, by navigating on the top through the icon bar next to the AEOTEC™ logo:

- Dashboard
- Rooms
- Elements
- Moments
- Automation
- Analytics
- Menu
- 08:35:15 – the house symbol indicates the connectivity (green: OK, red: interrupted) and a click on it or the time will refresh the page

4.4.1 Login

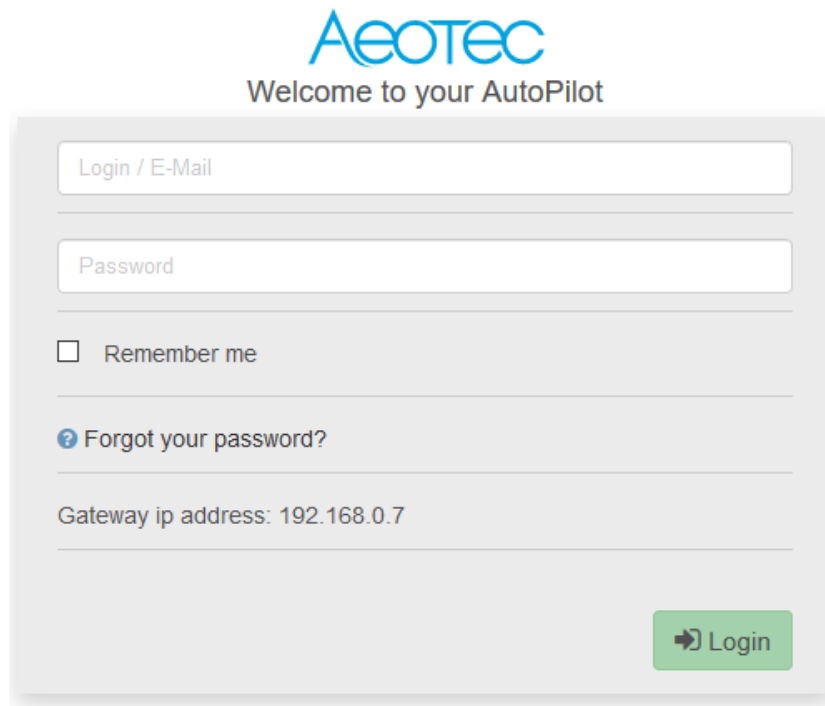
To get access to the AutoPilot™ you need to enter a valid user login and password on the login page (Figure: 4.4) first. This will give you a role specific access to the hub (see [4.7.1](#) to get more information about user roles).

If you want to access your hub remotely which means from the outside of your local network e.g. via mobile app, from your office, during your holiday, etc. you can use the AEOTEC ID™ service to get access to your AutoPilot™ or you call its referenced Home ID address directly in a browser e.g. https://*****589b.home.aeotec.com

This allows you to access your AutoPilot™ from all over the world.

Independent from the kind of access the login page of the AutoPilot™ will look the same as in Figure 4.4.

Use the *Remember me* checkbox to save your login credentials into the browser to access each time automatically (deleting cookies will reset it).



The image shows the Aeotec AutoPilot login interface. At the top, the Aeotec logo is displayed in blue, followed by the text 'Welcome to your AutoPilot' in a smaller, dark font. Below this, there is a light gray rectangular box containing the login form. The form has two input fields: the first is labeled 'Login / E-Mail' and the second is labeled 'Password'. Below the password field is a checkbox labeled 'Remember me'. Underneath the checkbox is a link that says '? Forgot your password?'. Further down, the text 'Gateway ip address: 192.168.0.7' is displayed. At the bottom right of the form box is a green button with a white right-pointing arrow and the word 'Login' in white text.

Figure 4.4: Login Page

Forgot your password? enables you to change the password of a profile by sending a verification code to an entered email address. To make it work, this email address needs to be stored in the profile which can be done e.g. during the Initial Setup, by activating the Cloud Backup or adding it on My Settings.

4.4.2 Dashboard

The Dashboard (Figure 4.5) is the main landing page of the AutoPilot™.

It provides you with all important data at a glance:

- Network health (Figure: 4.6)
- List of latest Moments
- List of current Problems
- Most important Elements which are defined by the user e.g. security, heating, presence widgets

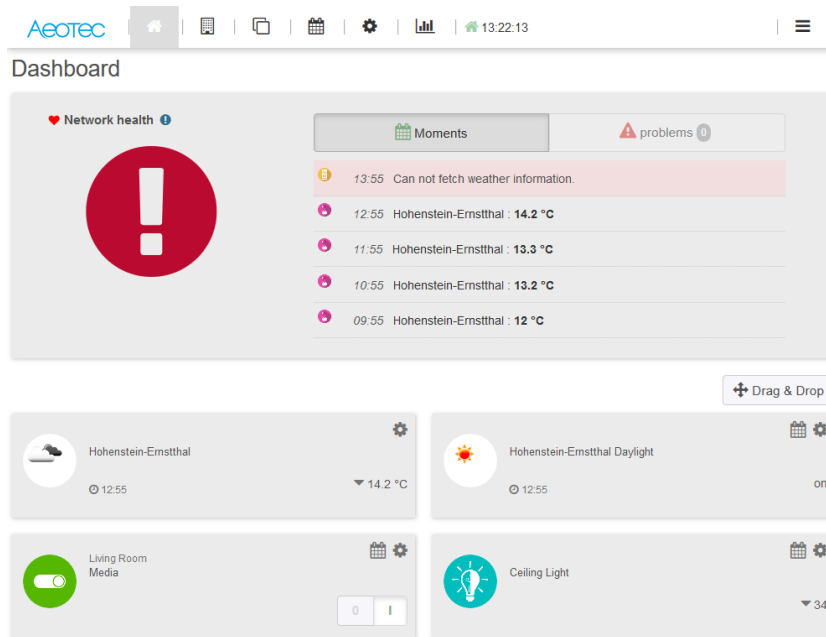


Figure 4.5: Dashboard

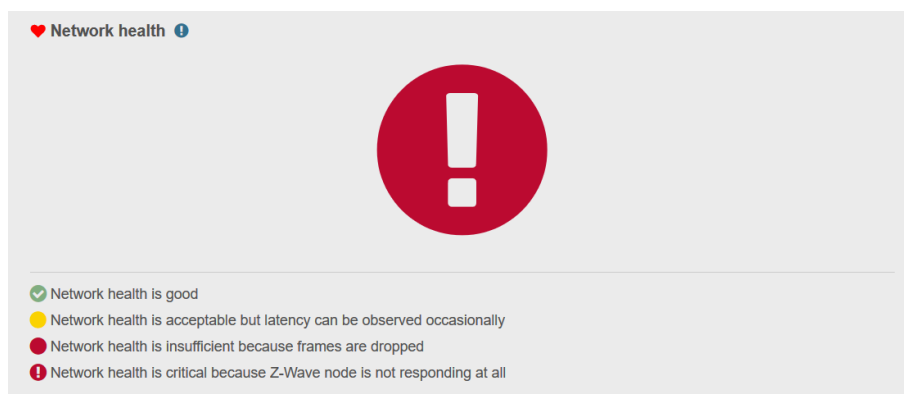


Figure 4.6: Network Health

If no Elements are assigned to the dashboard, two possibilities are described how to add devices (Figure 4.7):

- Using Apps
- Add Z-Wave devices to your AutoPilot™

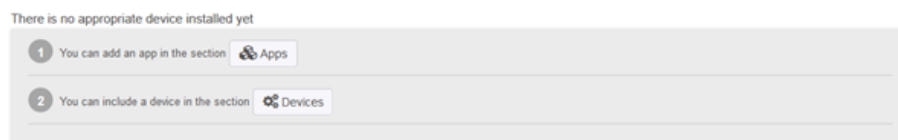


Figure 4.7: Blank Dashboard

Use the **+ Drag & Drop** button to arrange assigned elements on your own. Adjust the element configuration ([4.3.4](#)) to add or remove assigned elements on the dashboard. The dashboard information is stored in each profile which allows you to configure user specific dashboards for each user on the hub.

4.4.3 Rooms

The AutoPilot™ interface allows managing and assigning certain elements to different rooms.

Each element can be placed in one room only. Clicking on the room symbol on the top menu  opens the room view with a list of room widgets, as shown in Figure 4.8. By default, this view is empty, except there are already elements available which are automatically assigned in a room called **Not assigned to a room**.

To add new rooms, use the button labelled **+ Add new room** which leads you in a configuration view that is similar to the room configuration.

In a bigger list of rooms, the search bar in the top right corner helps to find and select rooms quickly.

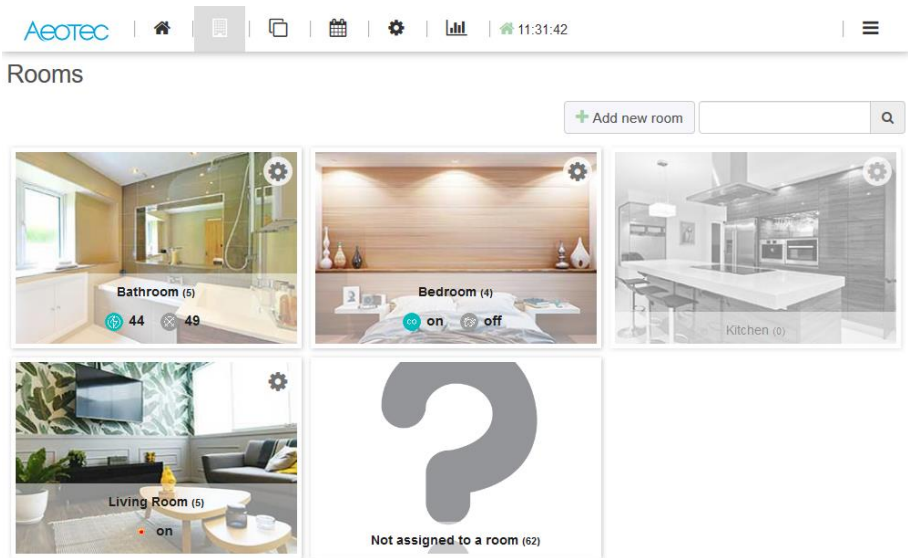


Figure 4.8: Rooms overview

The view of a room widget can be configured in its configuration menu  at the widgets top right corner. By default, the room name, the count of assigned devices and a system background image is shown. If a room has no elements assigned it is greyed out. If **Main Sensors** are selected, they will be shown right below the room name and in the top menu in the individual room view.

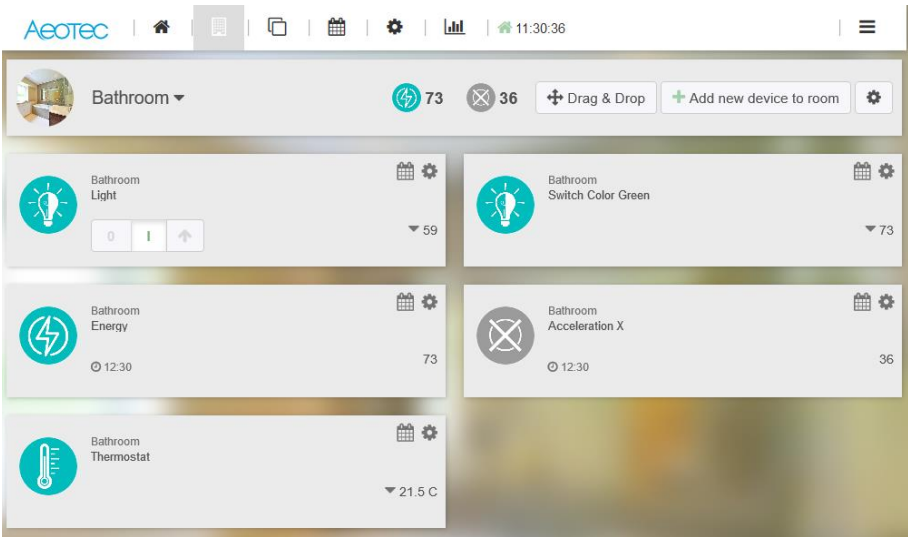


Figure 4.9: Single room view

Clicking on the room element leads you to the room view (Figure 4.9). The room view lists all the elements in the room. The top line shows up to three **Main Sensors** and allows quick change of the room using the dropdown list on the left. If your browser supports gestures, you can change the rooms by swiping left or right. As in the element view, the **✚ Drag & Drop** button can be used to re-arrange the single elements. With the **+ Add new device to room** button you can quickly add new Z-Wave devices to the network.

Room Configuration

Clicking on the gear wheel symbol **⚙** of the room element or inside the room view in the top line opens the room configuration dialog, as shown in Figure 4.10. There you can define the name of the room which must be different from the others, assign or unassign elements, customize your room with its own background image, set main sensors or remove the room completely.

Besides some pre-installed images, it is possible to upload images for the room. A checkbox enables that the selected room image is also used as a background image in the room view. The dialog allows assigning elements to this room which were not assigned to any room yet. Just click on the element name in the list of **Available devices**. The little checkbox on the right-hand side allows selecting up to three main sensors which will be shown in the single room view head bar and on the room widgets in the room view.

The screenshot shows the 'Room: (#2) Bathroom' configuration window. At the top, there's a header bar with the Aeotec logo and navigation icons. The main content area is divided into several sections:

- Name:** A text input field containing 'Bathroom'.
- Select an image:** A section with 'Sample Images' (four small thumbnails) and 'Custom images' (a message stating 'No custom images have been uploaded yet.').
- Display selected image as background:** A checkbox that is currently checked.
- Upload image:** A button with a green plus icon and a file upload icon.
- File upload instructions:** Two lines of text: 'The uploaded file must be smaller than 5.0 MB and in one of the following formats: .jpg, .jpeg, .gif, .png, .svg, .tif, .tiff.' and 'The recommended dimension of the images is 1920 x 1080 px.'
- Delete room:** A red button with a white 'X' icon.
- Devices in this room:** A section with a message 'You can max. 3 sensors add to the room header (2/3).', a 'Clear sensors' button, and a row of device cards: 'Acceleration X' (with a red 'X' and a checked checkbox), 'Energy' (with a red 'X' and a checked checkbox), 'Light' (with a red 'X' and an unchecked checkbox), 'Switch Color Green' (with a red 'X' and an unchecked checkbox), and 'Thermostat' (with a red 'X' and an unchecked checkbox).
- Available devices:** A section with a grid of device cards, each with a green plus icon: 'alarm ...', 'alarm ...', 'alarm ...', 'alarm ...', 'alarm ...', 'alarm ...', 'alarm ...', 'sensor multilevel ...', 'binary switch', 'multilevel switch ...', 'multilevel switch ...', 'multilevel switch ...', 'multilevel switch ...', 'multilevel switch ...', 'switchRGBW (rgb)', 'multilevel switch ...', and 'thermostat *F ...'.
- Buttons:** At the bottom right, there are 'Cancel' and 'Save' buttons.

Figure 4.10: Room configuration view

4.4.4 Elements

Figure 4.11 shows the standard element view of the AutoPilot™ Smart Home Interface. Figure 4.12 the default view with the same options as mentioned on the blank Dashboard in Figure 4.7. Elements with an icon, buttons, or variables are placed side by side. Depending on the screen size, they are grouped in one (mobile phone), two (pad), or three (PC screen) columns. The very same display is also available on the Dashboard and the Room View.

The element view shows all elements available while the dashboard shows elements that were manually selected for display on the dashboard. The clock on the topline menu shows the actual time in the time zone of the gateway (not the actual position of the browser), which is UTC per default. A click on the clock will do a complete data reload of all elements.

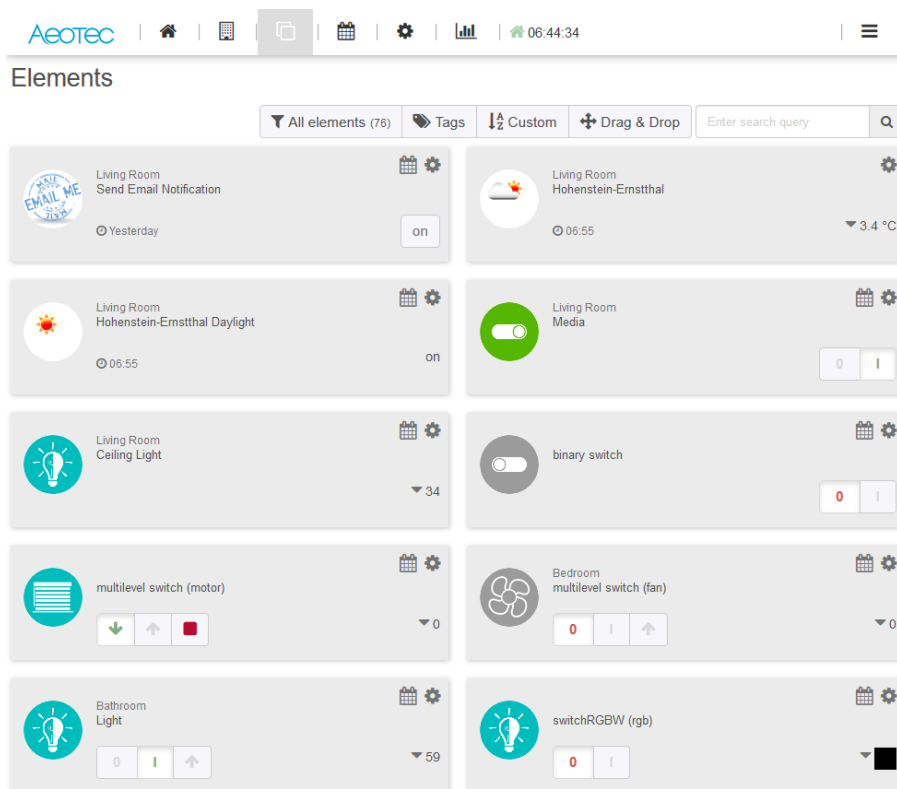


Figure 4.11: Element View

The elements can be filtered by element type and tags or can be ordered by

- Time of creation (ascending or descending)
- Given name in alphabetical order (ascending or descending)
- Last update
- Custom

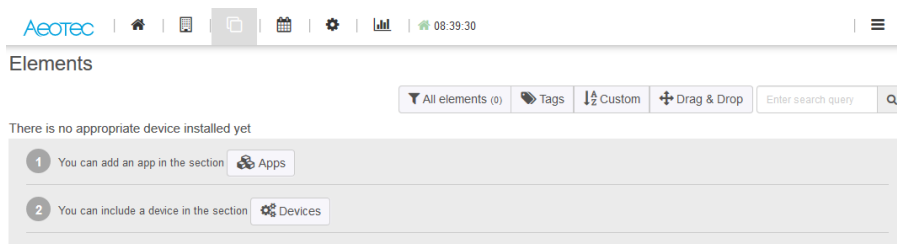


Figure 4.12: Blank Element View

The button  *Drag & Drop* turns the user interface in a reordering mode (Figure 4.13). Just drag and drop elements to reorder them.

After the new order is saved, it is available as custom in the sort by menu . The same logic can be applied to all view showing elements (Element View, Dashboard, and Room View).

A search field  allows searching for given names of the elements.

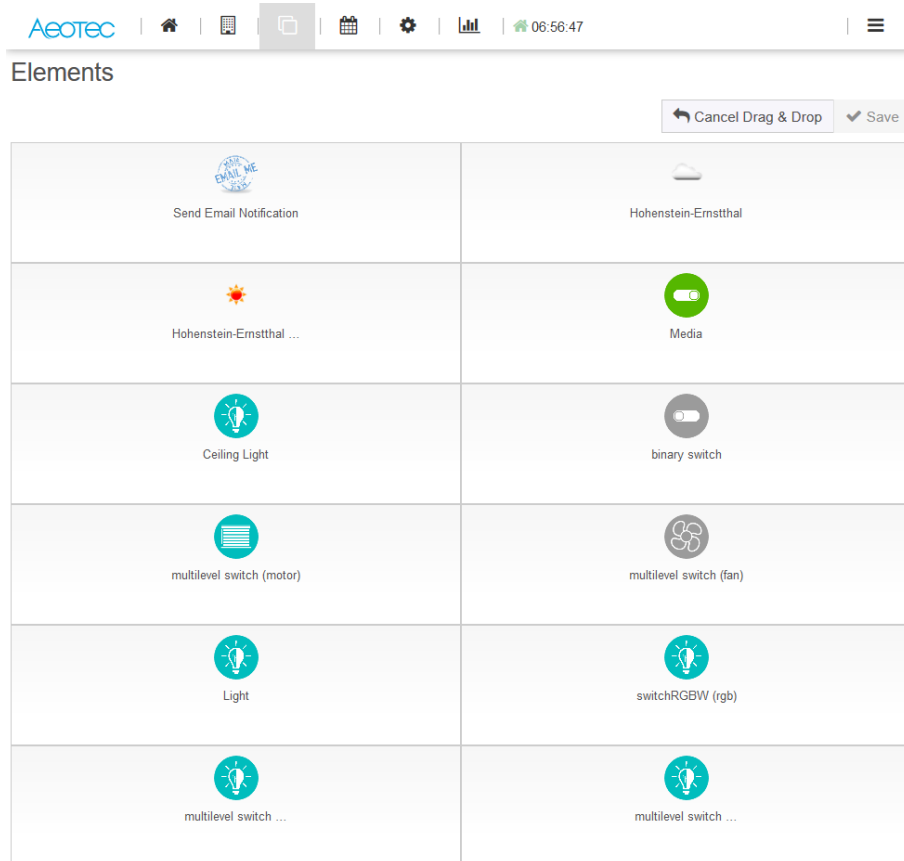


Figure 4.13: Drag & Drop reordering mode

All elements can be assigned to tags: Tags are text blocks that can be arbitrarily chosen. Typical tags are for example *Temperature*, *Energy* and *Outdoor*. Multiple elements can have the same tag and one element can have several tags. By selecting a tag, only elements are shown that are tagged with this name. Tags are managed on the element configurations described below.

Figure 4.14 shows two typical elements: Each element has a given name. This name may refer to the function or the position. Please make sure to keep the name short enough so that no display problem is created. Each element also has one or several icons. In case the element represents an actor function, the icon usually refers to the switching state of the actor (on or off, up or down). Changing icons also indicate the status of binary sensors such as motions detectors. Analog sensors typically only have one icon. The upper right element is a binary actor allowing to be switched on and off.

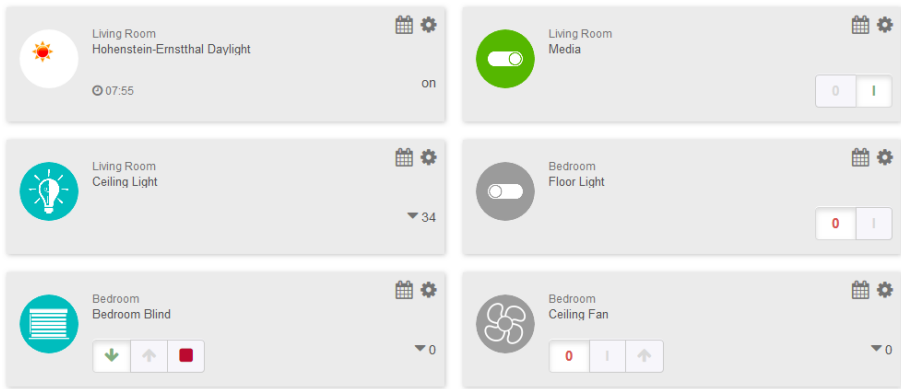


Figure 4.14: Types of elements

The ⚙️ on the right-hand side of each element's widget (Figure 4.14) opens the element configuration dialog. The symbol left to the configuration wheel depends on the type of device. For devices with analog values such as rain sensors, temperatures, etc., the icon 🕒 will open a 24-hour history of the sensor value.

Elements of the type binary or multi sensor also show a time stamp when the last value update was received. Clicking on the large widget icon itself or on the sensor update time icon 🕒 7:33 will call for a value update, but please keep in mind that battery-operated devices will only send updated values after the next wakeup. For event-driven devices such as actuators or binary sensors, an icon 📅 will show a list of the last 10 events with the time stamp. One click away is then the full list of events, as described in Section [4.3.5](#), but filtered for this element.

Element Configuration

Every element has its own configuration dialog (Figure 4.15). Clicking on the gearwheel symbol ⚙️ on the upper right-hand side opens this dialog. Figure 4.15 shows the upper part of the element configuration dialog.

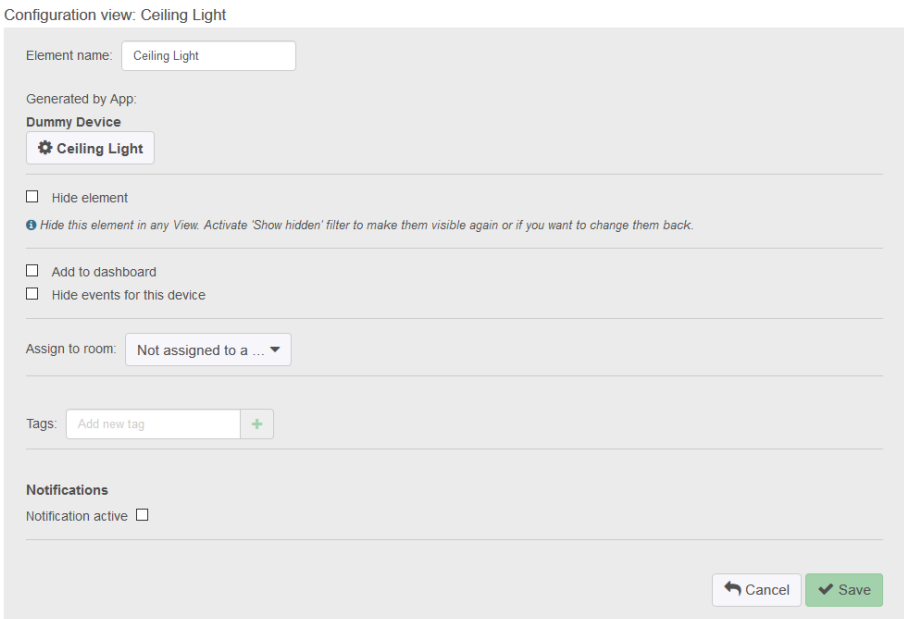


Figure 4.15: Element configuration

- **Element name:**

This is the given name of the element. AutoPilot™ tries to automatically find a reasonable name based on the device information, but for a better handling the user should change this name according to the specific setup of his home.

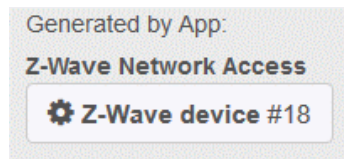


Figure 4.16: Generated by Z-Wave device

- **Generated By:**

Above the button the name of the source (system) app is shown. The button shows the labeled reference and can have one of these properties:

- If the element is an endpoint of a Z-Wave device (sensor, switch, etc.), its node ID is shown as reference (e.g. node #18, Figure 4.16). A click on the button then will forward you to its Z-Wave node configuration ([4.5](#)).
- If this element is created by an app (e.g. Dummy Device, Figure 4.15), a click on the button will forward you to its referred app configuration ([4.4](#)).

- **Hide element:**

As explained in the dialog, this checkbox will hide the element. Enabling the filter *Show hidden* will make them visible in the different views again. Use this setting to avoid element mess in your views.

- **Delete Element:**

This checkbox allows removing the element. It will not only disappear from the element view but also from any dropdown list to setup device relationships, etc. for information on how to re-activate such an element, refer to the info below the button or to the description in Z-Wave node configuration ([4.5](#)).

- **Add to Dashboard:**

This place the element on the dashboard.

- **Hide moments from this device:**

This is a filter configuration which allows you to ignore all moments of this device. If enabled, moments of the device won't appear in the moments view.

- **Assign to room:**

This allows assigning this element to a certain room or changing this assignment.

- **Tags:**

The tag option allows to create +, assign + and remove ✖ tags. When a tag name is inserted into the text field, it autocompletes known tag names (Figure 4.17).

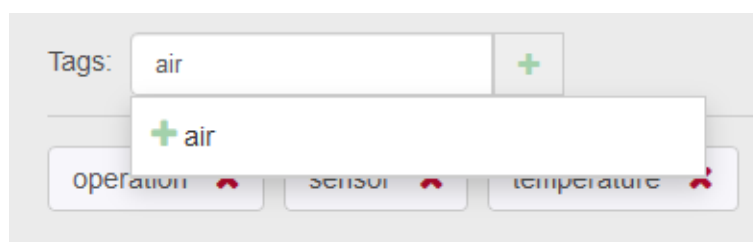


Figure 4.17: Tags

- **Notifications:**

Enabling **Notifications active** allows you to create element specific push notifications (Figure 4.18). If a predefined state becomes true, the user-defined message is sent to all mobile devices assigned to the hub.

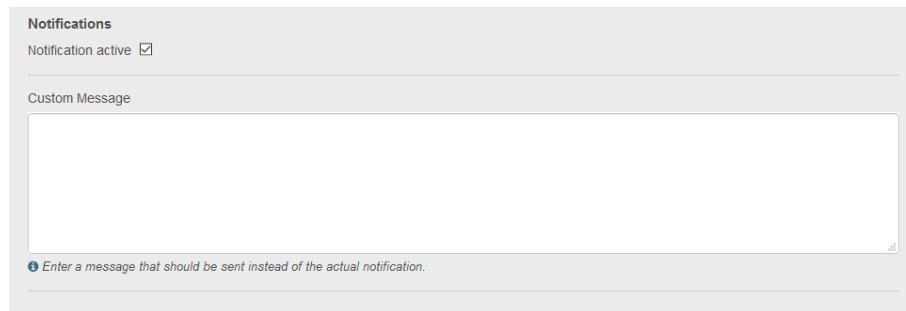


Figure 4.18: Element notifications

The conditions are depending on the element type. Because a scene has only the condition **trigger** there is no configuration possibility – if it is triggered, the push message is sent.

For binary actors/sensors you can choose between **All**, **On**, **Off** and multilevel actors allow in addition **Level** as trigger (Figure 4.19). Multilevel sensor conditions will be realized by logical parameters: **=**, **!=**, **>**, **<**, **>=**, **<=** and its level (Figure 4.20).

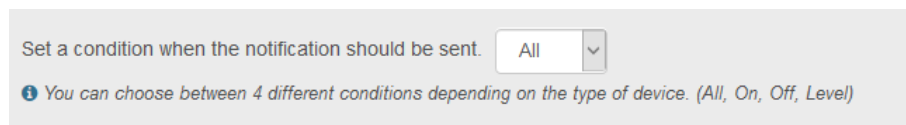


Figure 4.19: Element notifications – level condition

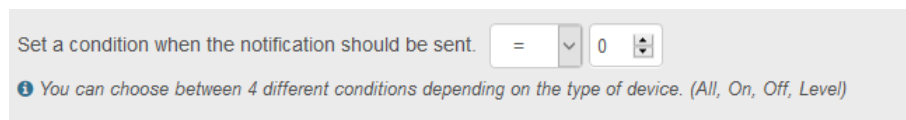


Figure 4.20: Element notifications – logical condition

Custom Icons

This sub-dialog (Figure 4.21) allows changing the icons of the element. Each element has at least one or more icons depending on the status indicated. Each of the icons can be replaced by an own individual icon. Just click on the pencil button to change the icon. To download more icons, refer to the customization section ([4.6](#)) in the configuration menu.



Figure 4.21: Element – Custom icons

4.4.5 Moments

Moments  is the fourth menu item in the top menu. This timeline dialog offers a chronological view (Figure 4.22) of all events in the Smart Home up to 7 days. The events are:

- Status change of actuators (dimmers, blind controls, switches, etc.)
- Tripping of binary sensors (motion, door, etc.)
- Change of measured value of sensors (temperature, air pressure, voltage, etc.)
- Z-Wave network status changes (device lost, device back, etc.)
- Critical system notifications

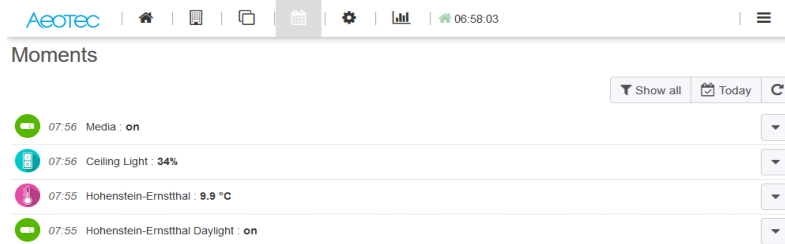


Figure 4.22: Moments

The standard view of a Moment, as shown from left to right in Figure 4.23, consists of:

1. the level and element specific status icon
2. the timestamp
3. the name of the element or source name
4. the status or message info
5. optional the room name

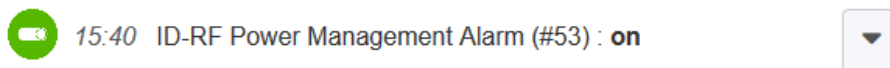


Figure 4.23: Moments – Single moment view

Additional every line item has a context menu ▼ on the right-hand side. This context menu (Figure 4.24) allows:

-  Show all - Show all Moments
-  Events of this Source - showing Moments of this source element only (element, app, ...)
-  Events of this Type - showing Moments of this event type only (on/off, multilevel, ...)
-  Events of this Type and Source - showing Moments of this event and source type only
-  Source configuration - directly forwarding to the element configuration
-  Hide events of this Source - hide Moments of this sources by adding them to the list ***Hidden events of devices in My Settings.***
-  Delete this event - remove Moment from Moments list

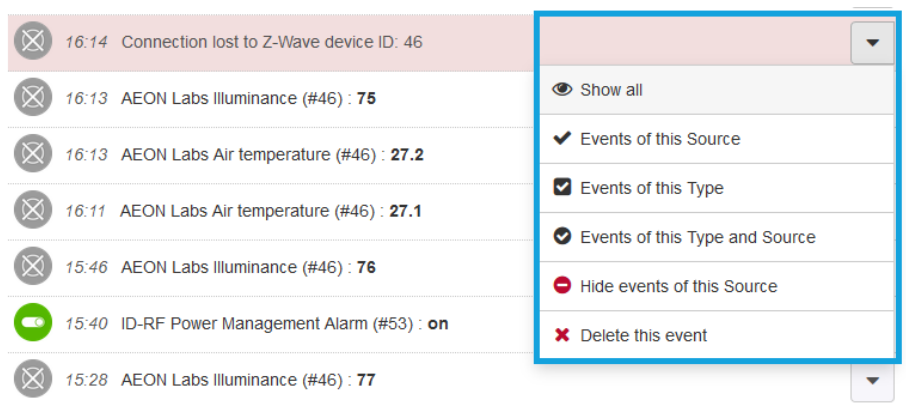
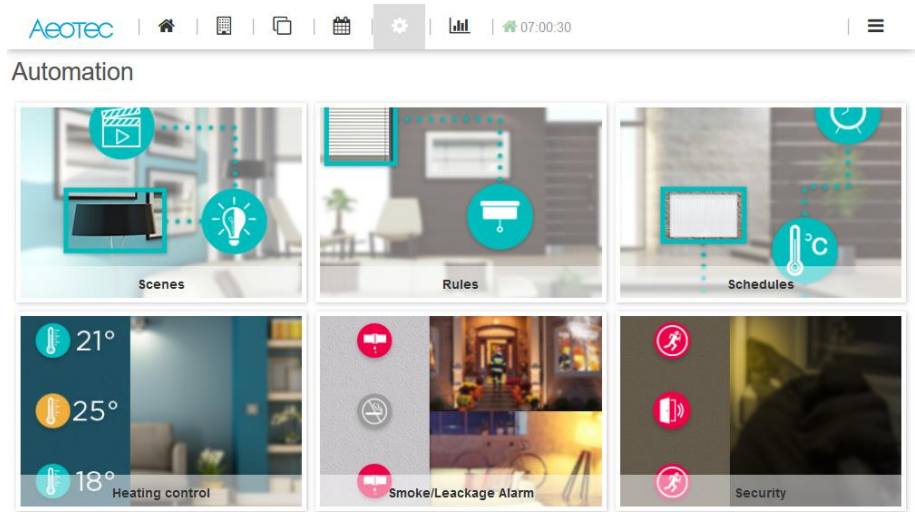
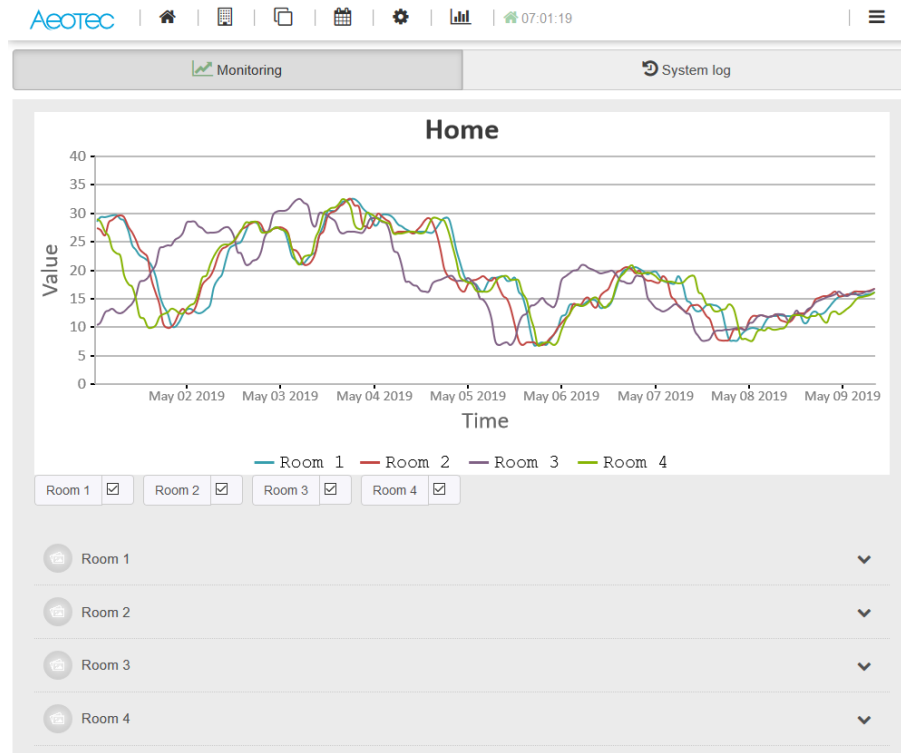


Figure 4.24: Moments - Actions

4.4.6 Automation



4.4.7 Analytics



Aeotec | Home | Monitoring | System log | 07:01:51

Monitoring

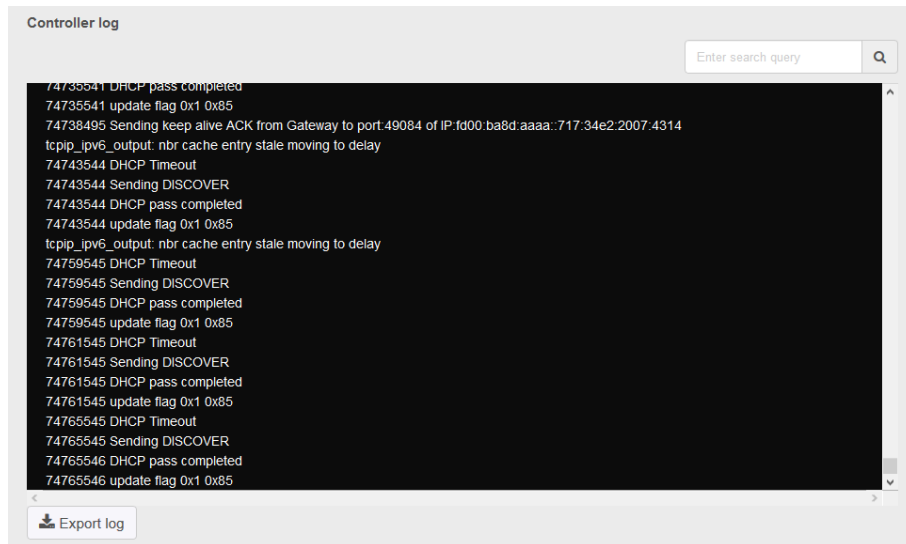
System log

Software log

Enter search query

```
[2019-05-09 06:55:34.720] [core] Instantiating module 8 from class OpenWeather
[2019-05-09 06:55:34.722] [core] -- Starting module Local Weather
[2019-05-09 06:55:34.738] [core] Creating device sensorMultiline OpenWeather_8
[2019-05-09 06:55:34.777] [core] Creating device sensorBinary OpenWeatherDaylight_8
[2019-05-09 06:55:35.144] [core] Notification: device-info (device-OnOff): {"dev":"Hohenstein-Ernstthal Daylight","T":"on","location":""}
[2019-05-09 06:55:35.178] [core] Notification: device-info (device-temperature): {"dev":"Hohenstein-Ernstthal","T":"9.9 °C","location":""}
[2019-05-09 06:55:48.865] [core] Instantiating module 9 from class DummyDevice
[2019-05-09 06:55:48.867] [core] -- Starting module Dummy Device
[2019-05-09 06:55:48.878] [core] Creating device switchBinary DummyDevice_9
[2019-05-09 06:56:03.979] [core] Instantiating module 10 from class DummyDevice
[2019-05-09 06:56:03.981] [core] -- Starting module Dummy Device
[2019-05-09 06:56:03.996] [core] Creating device switchMultilevel DummyDevice_10
[2019-05-09 06:56:52.174] [core] -- DummyDevice_10 performCommand processing: {"0":"exact","1":{"level":"34"}}
[2019-05-09 06:56:52.194] [core] Notification: device-info (device-status): {"dev":"Ceiling Light","T":"34%","location":""}
[2019-05-09 06:56:56.843] [core] -- DummyDevice_9 performCommand processing: {"0":"on","1":{}}
[2019-05-09 06:56:56.848] [core] Notification: device-info (device-OnOff): {"dev":"Media","T":"on","location":""}
[2019-05-09 06:56:56.843] [core] -- DummyDevice_9 performCommand processing: {"0":"on","1":{}}
[2019-05-09 06:56:56.848] [core] Notification: device-info (device-OnOff): {"dev":"Media","T":"on","location":""}
```

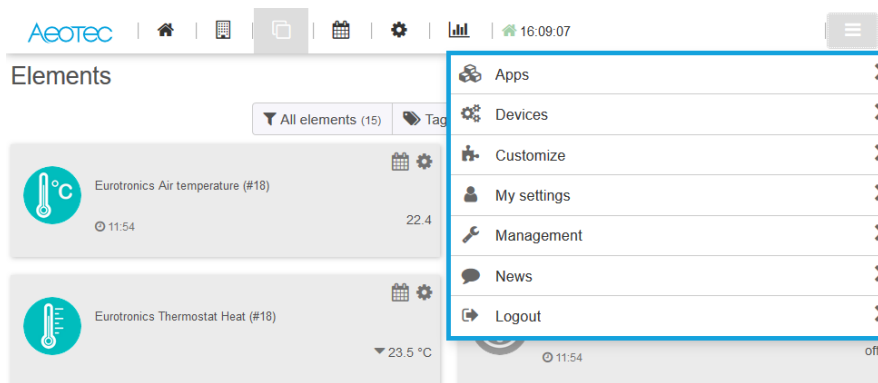
Export log



4.4.8 Menu

Clicking on the menu item on the top right corner opens the configuration menu. The configuration menu offers various functions to enhance and configure the smart home system as such and the user interface. Available functions are:

- Apps ([section 4.3](#)) – Application menu
- Devices ([section 4.4](#)) – Device Configuration (radio networks: Z-Wave, Wi-Fi, etc.; mobile phone access, camera ...)
- Customize ([section 4.5](#)) – Skin and Icon Configuration
- My Settings ([section 4.6](#)) – Profile settings
- Management ([section 4.7](#)) – Administrative system management
- News ([section 4.8](#)) – As shown in Figure 4.35, this dialog lists all news entries received from the RSS feed.
- Logout – The logout button cancels the user sessions of the AutoPilot™ Smart Home Interface. In case of a login from find.zwave.me



4.5 Apps

This menu option allows managing the home automation applications and interfaces of Internet or IP-based services or devices.

AutoPilot™ apps are like software applications that use the infrastructure of the Z-Wave network to provide application solutions and dependencies. These software applications also extend the capabilities of the network and implement automation functions.

Like any other application software such as those for PCs, some AutoPilot™ apps are preinstalled on the device, and others can be downloaded and installed by the user. Like application software, some software solutions can only run once while others can be started multiple times.

The app menu has three parts:

- List of apps locally available for use.
- List of apps available on the central server and ready for download.
- List of apps that are active and running.

The list of local apps, as displayed in Figure XXX, shows a small subset of apps that are already on the local devices.

The top part shows some of the apps that are most frequently used (featured apps). A filter allows filtering for certain app types; ordering and direct search in the search box also help to find the right app. If there are active instances of the app (software running x times with different parameters), this is indicated right below the name of the app.

Clicking on the name will open a dialog with further information about the app. Clicking on the + button will lead right to the configuration page of the app.

The online app list, as shown in Figure XXX, offers the same functions. However, apps need to be downloaded first before they can be configured and started. Clicking on the download button will copy the app to the local repository and start the configuration dialog, as shown in Figure XXX.

Each app has its own name that can be changed. Depending on the function of the app, there are several different setup parameters.

Please note again that some apps can be started multiple times while other apps are “singletons.” They must only run once on the system. Once they run, they will disappear from the repository since they cannot be started again. Configuration of such a singleton is still possible using the menu of running apps. If such an app stops, the app entry will reappear in the local repository.

The tab for active app management is shown in Figure XXX. It lists all active apps by app type. If there are more than one app of the same type (e.g. 'IF->THEN' is usually needed multiple times), the view is collapsed for this type of application but can be expanded. It is possible to expand all sections of multiple app types using the checkbox on the top. It is also possible to search for certain app names.

Every app line has a submenu with the following functions:

- ✕ Stop this app
- 📄 Allows cloning an app. This will open a dialog for a new instance of the same app with the same settings.

After saving these settings, the new app becomes active and is shown in the list too.

- 🔴 Stop the App. It remains configured but is inactive. Once inactive, the green flame changes into a red ON button to restart the app.
- ⚙️ Opens the configuration dialog. This is the very dialog to be completed during the initial start of the app.

Please refer to Chapter 6 for more information on different apps.

07:06:50

Active
Local Apps
Online Apps

☐ Expand all

	Battery Polling	⚙️ ⏸️ ✖️
	System Clock (CRON)	⚙️ ⏸️ ✖️
	Dummy Device (2)	⏸️ ✖️
	Inband Notifier	⚙️ ⏸️ ✖️
	Send Email Notification	⚙️ ⏸️ 📄 ✖️
	Local Weather	⚙️ ⏸️ 📄 ✖️
	Remote Access	⚙️ ⏸️ ✖️
	Periodical Sensor Polling	⚙️ ⏸️ ✖️
	Z-Wave Network Access	⚙️ ⏸️ 📄 ✖️

07:09:10

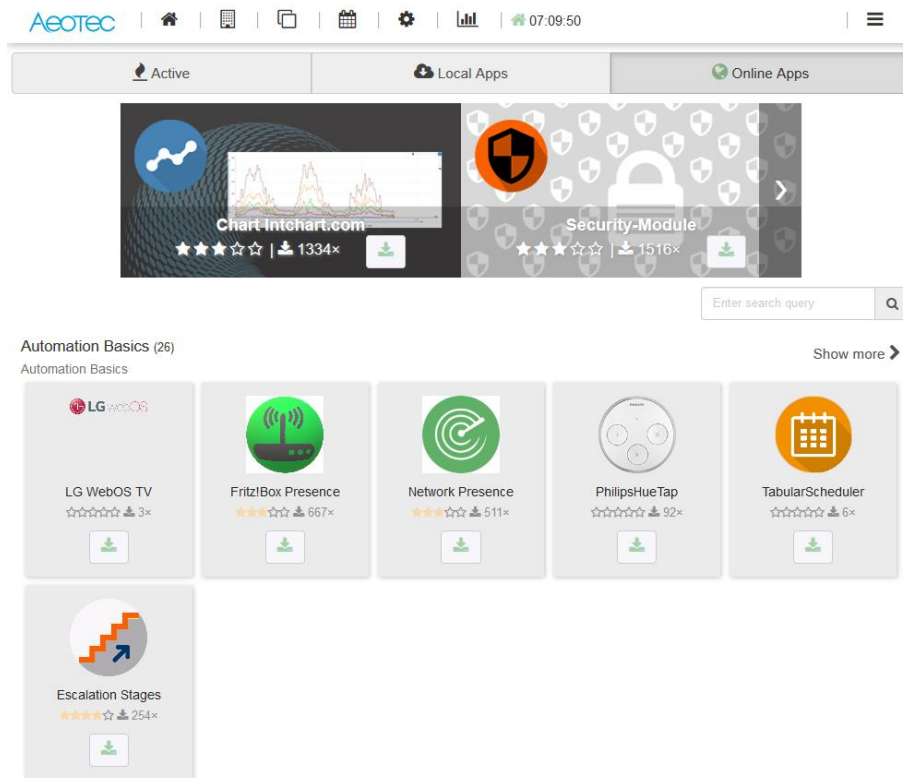
Active
Local Apps
Online Apps

Featured Apps

 24 Hours Device History +	 If -> Then +	 Local Weather +	 Schedule +
---	--	---	--

All Apps

 Alexa +	 Association +	 Automated Locking of ... +	 Automated Switch Off +	 Battery Polling +
 CloudBackup +	 Correct sensor value +	 Counter triggering bin... +	 Delayed Action +	 Dummy Device +



4.6 Devices

The device menu allows managing physical devices. By default, it offers the following physical device types:

- Z-Wave
- Mobile phone
- Camera
- Speech Assistant
- Wi-Fi

Optional if the controlling app is activated:

- RF 433 MHz
- EnOcean

Please refer to Section [4.10](#) for more information on how to integrate further wireless technologies. This section will explain how to add/remove and manage these devices and IP cameras. Figure 4.5.1 shows the default device list. Each option offers you the possibility to **+** Add new or **✎** Manage physical devices. Therefore, let us focus here on managing Z-Wave devices.

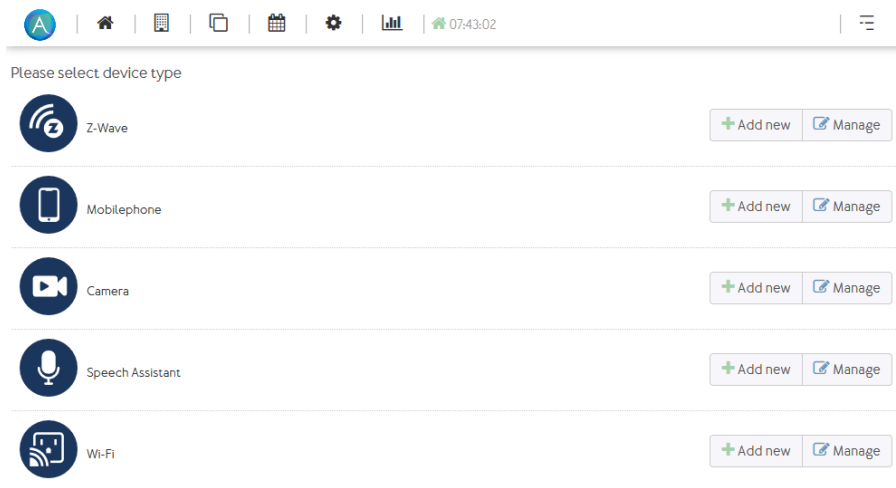


Figure 4.5.1: Devices view

4.6.1 Manage Z-Wave Devices

Next to the usual way to add Z-Wave devices by enabling the Learn Mode, the Z-Wave **+ Add new** menu (Figure 4.5.2) also offers you to use the new SmartStart feature of Z-Wave.

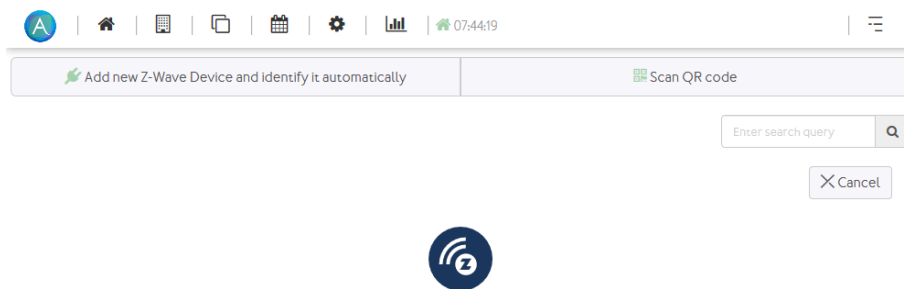


Figure 4.5.2: Add new Z-Wave device view

SmartStart is a new way to add devices into Z-Wave using a QR Code provided with S2 authentication. The user scans the QR code whose information goes directly in a provisioning list. When powered up, the SmartStart Device will announce to be ready to be added. In case the S2 key is in the provisioning list the controller will automatically add this new device without any further user interaction.

Clicking on the tab *Scan QR code* will open a form (Figure 4.5.3) where you can manually add a 40-digit Z-Wave device DSK or download the mobile APP instead to Scan Z-Wave SmartStart QR-Codes directly.

Manage your device information added by its Z-Wave DSK or SmartStart QR under *Manage*. More information how to do this you will find in section [4.5.2](#).

Please note that a standard web browser running on a standard PC may not provide the capability to scan QR Codes via the AutoPilot™ interface.

A click on the Z-Wave logo at the button will forward you back to the Devices view.

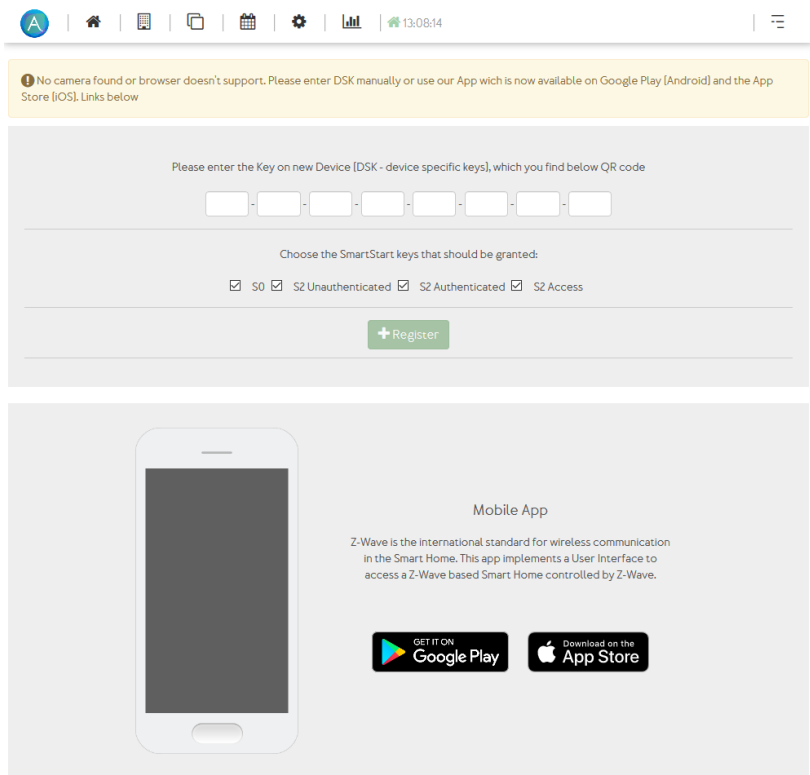


Figure 4.5.3: Scan QR Code view

Clicking on the tab:  *Add new Z-Wave Device and identify automatically* (Figure 4.5.2) will directly guide you to the Z-Wave Add / Remove section (Figure 4.5.4) but offers you no user guidance how to add or remove the device. For that way it is recommended to have a look at the device manual too.

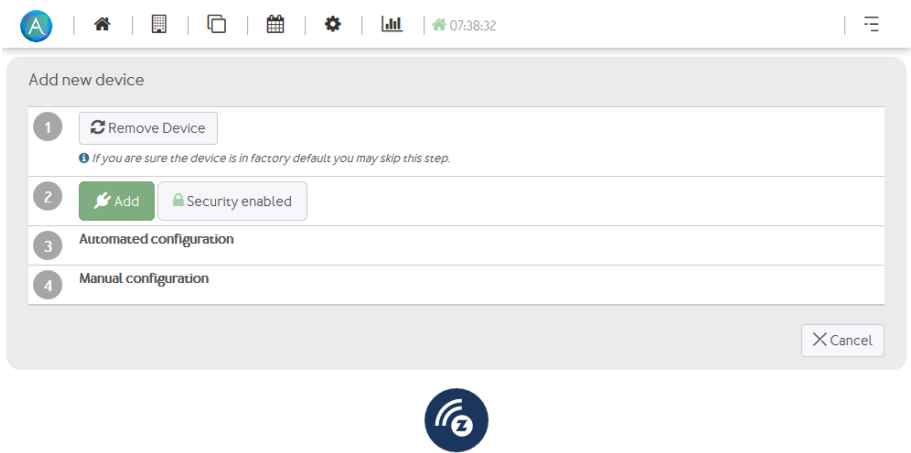


Figure 4.5.4: Z-Wave device Add / Remove view

Add Mode

Since most Z-Wave devices have one Z-Wave action button where a single or triple click will do the add process, the additional information shown in the Z-Wave device specific Add / Remove view (Figure 4.5.6) is only needed for some devices with exotic add mode options. Whether you decide to choose this way or to add a device by automatically identification (Figure 4.5.4), the procedure will be the same. Please refer to the devices manual on how to do an add process.

In the case the device cannot be added as expected, please remove the device first. More than 90 % of all add process problems are caused by devices which still belong to a network. In that case they cannot being added again.

Skip this step, if you are sure that the device is new and in factory default state.

To start the Add process click on the green  Start button (Figure 4.5.7).

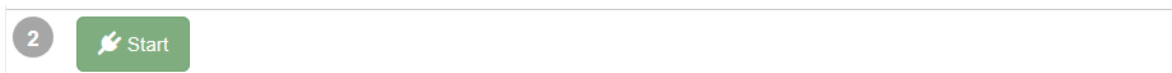


Figure 4.5.7: Add Start button

If the process is started, the controller signals its readiness. Unless no device is found you can stop the Add process by pressing on the red  Stop button (Figure 4.5.8). Furthermore, the controller will cancel it automatically if no device is added.

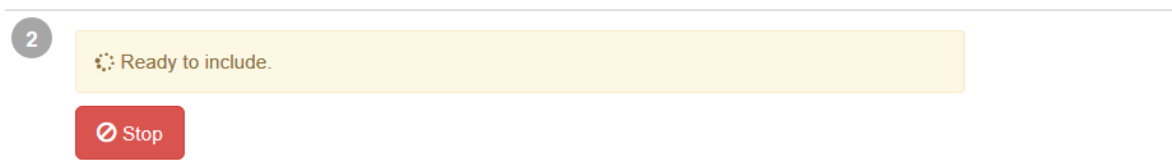


Figure 4.5.8: Add Stop button

First, after adding to the network any newly added Z-Wave device will be interviewed. In this process, all functions announced by the device itself will be verified the status. Incomplete interviews can influence the device functionality, so it is recommended to retry the add-process or manually complete the interview (please read further below).

A progress bar (0 – 100%) in the third row which is called Automated Configuration (Figure 4.5.4) will show you the progress of the Z-Wave interviews. You can also find the node number assigned to the new device and all further configuration which are pending after the device was successfully added to the controller (Figure 4.5.9). A click on this progress bar will list you all available command classes and their interview status (Figure 4.5.10).

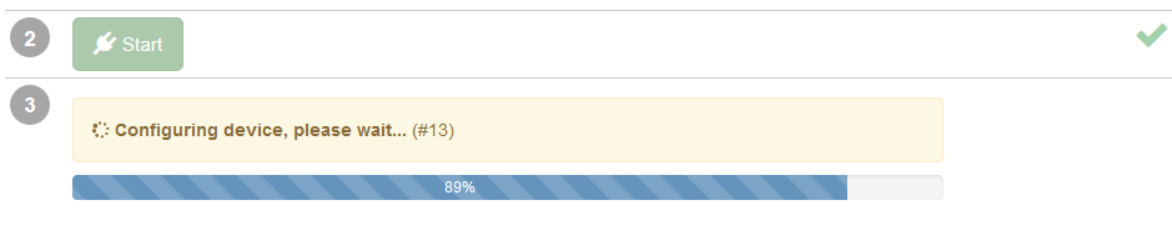


Figure 4.5.9: Automated Configuration progress

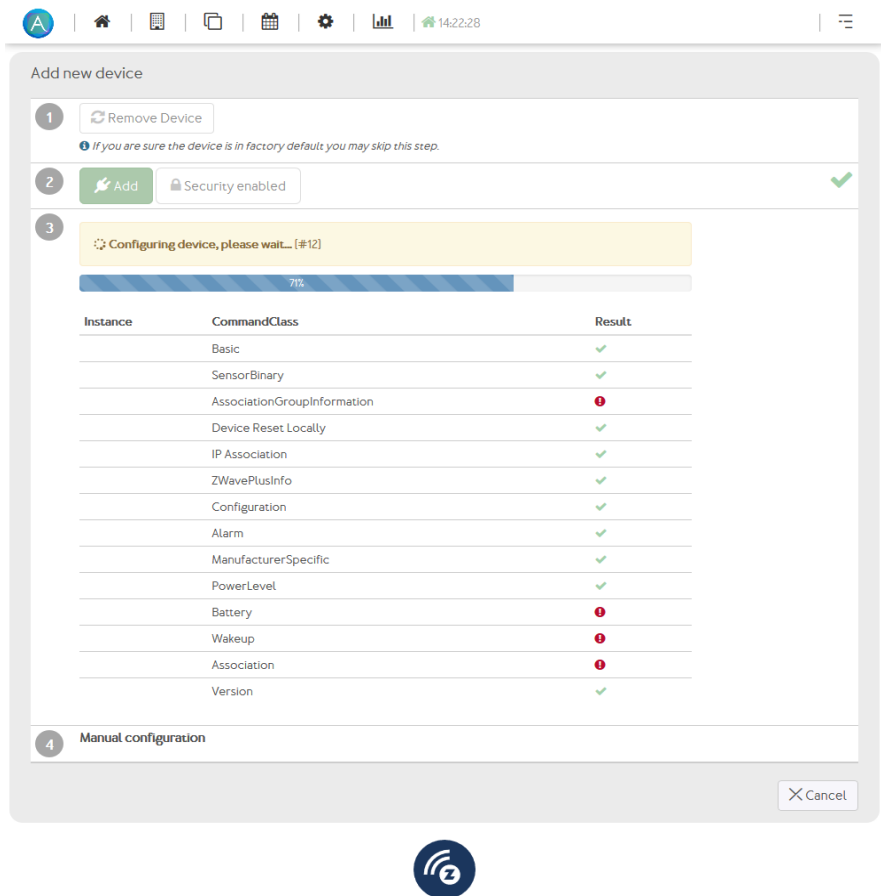


Figure 4.5.10: List interviewed Command Classes

A short message with the new node ID and a green fade-in message on the top right corner will indicate that the device was successfully added.

If there is a problem or the configuration process isn't complete (Figure 4.5.11), an input popup will be shown (Figure 4.5.12) where the user is prompted to repeat or continue the add process.

To see what happens after a Z-Wave device was successful added please do further reading on headline [Manual Configuration](#) otherwise continue with the next headline.

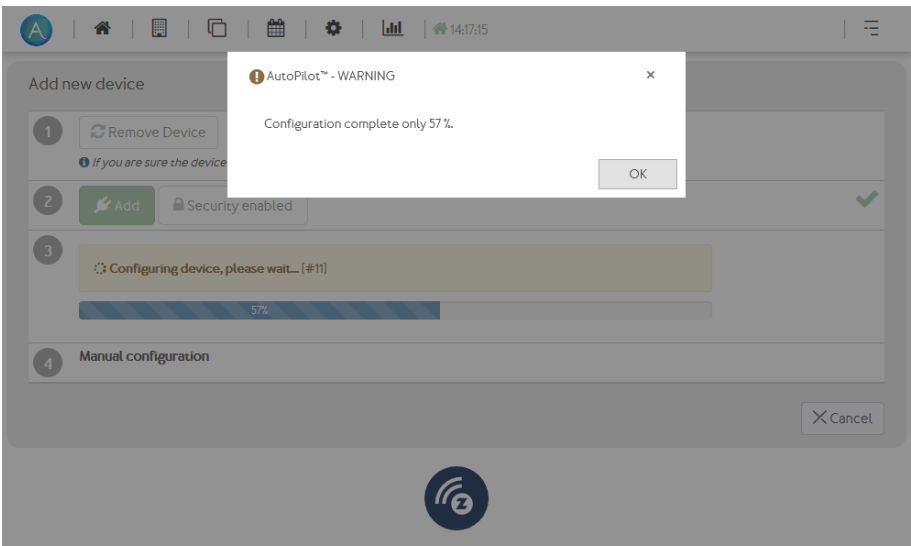


Figure 4.5.11: Interview progress incomplete

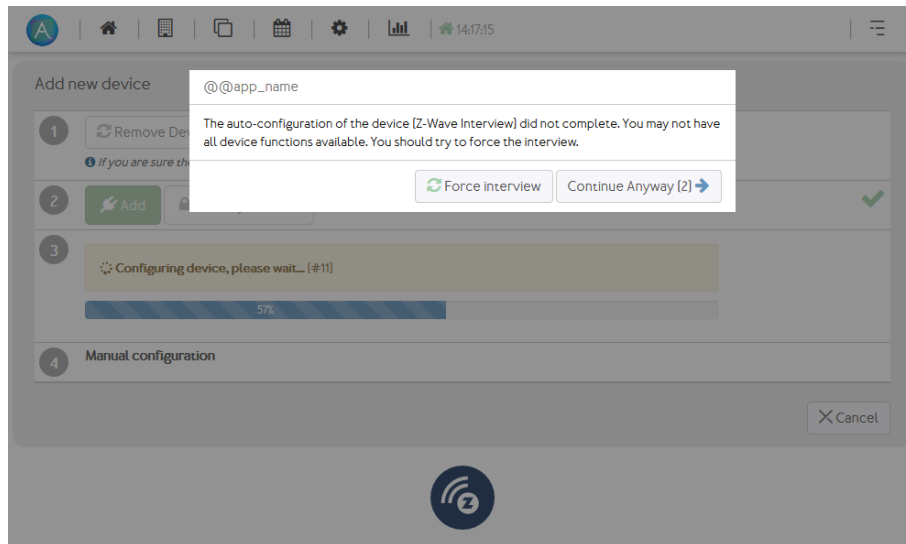


Figure 4.5.12: Interview progress retry prompt

Add Z-Wave devices with S2

If the new device supports the new S2 Z-Wave security standard, it could be possible that it will require an authorization which needs to be done right after the add process. The authorization ensures that the device that appears on the user interface is the device in your hand. For that case the device offers either a device individual QR Code or a PIN number. Both types of information need to be provided to the user interface manually. The controller will then match the information provided by the user with the information provided by the device. Only in case they match, the device can be used.

The QR Code is mainly made for the Z-Wave SmartStart (Section [4.5.3](#)) feature which is a kind of Z-Wave

“plug and play”. Is the QR-code registered in the controller (Figure 4.5.2 – Scan QR Code), the device will automatically be added to the network.

Authentication is only required for certain devices. In the case you’re adding an access control device which supports S2 like a door lock or keypad, temporarily a window pops up (Figure 4.5.13) asking for the authentication information.

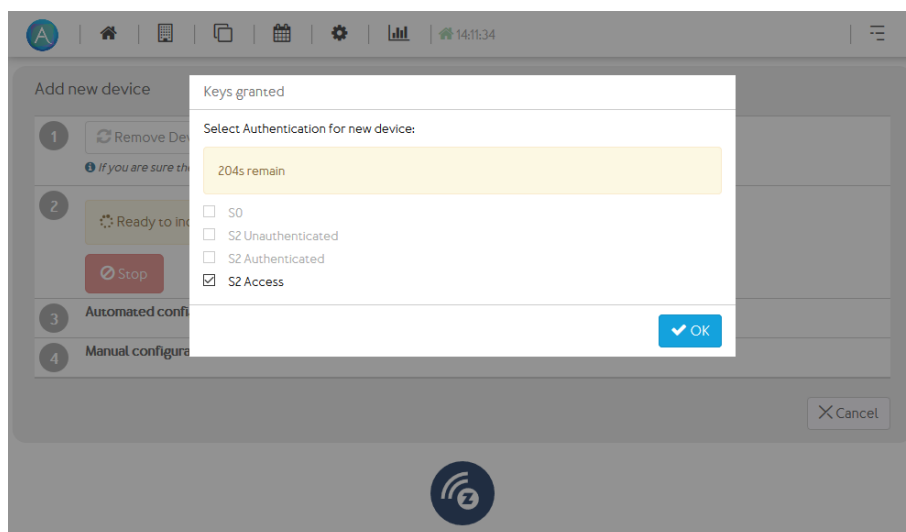


Figure 4.5.13: S2 – Choose authentication

The overview below (Table 4.1) gives you a short description about the listed authentication options:

Authentication Type	Description	User Input
S0	Backward compatibility with older Z-Wave devices (previous Z-Wave security standard, unsecure)	no
S2 Unauthenticated	S2 Z-Wave security standard without authentication	no
S2 Authenticated	S2 Z-Wave security standard with authentication	enter 5-digit PIN
S2 Access	S2 Z-Wave security standard with authentication	1. confirm S2 Access 2. enter 5-digit PIN

Table 4.1

Once the PIN is transmitted (Figure 4.5.14), it is verified against the information requested from the device itself during the add process. If the authentication fails, a warning is displayed. In that case it is not possible to just repeat the authentication. The device must be removed and re-added again.

Both authentication prompts will be canceled automatically after 20 seconds with the message “add-process failed due timeout” if no input is made. A count down in the yellow information field displays you the pending seconds (Figure 4.5.14).

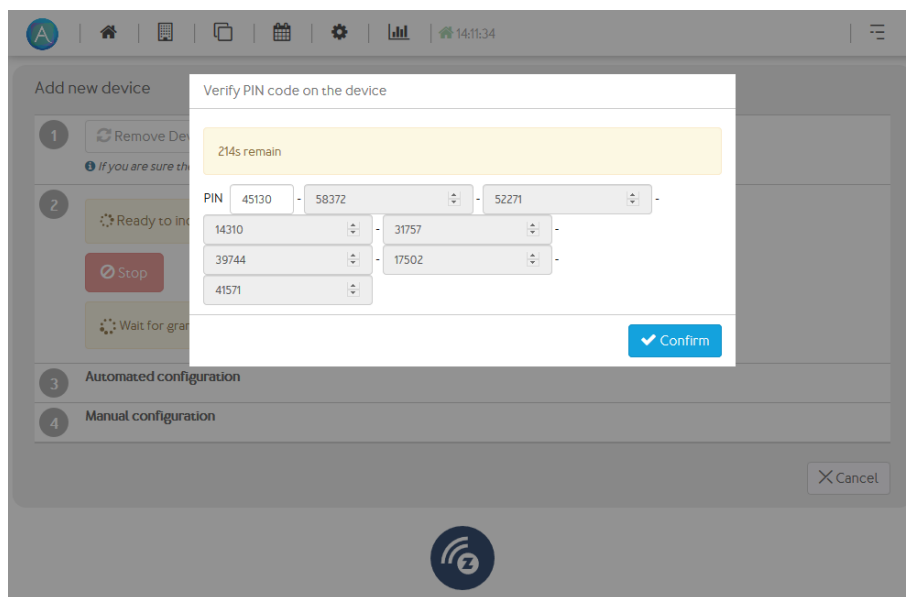


Figure 4.5.14: S2 – Authenticated / Access

A green info box (Figure 4.5.15) will inform you if the authentication was successful. After that the controller will start the interview progress (similar to the Add Mode description above – Figure 4.5.9). If the interview was successful, the user is redirected to the Manual Configuration overview of the newly added device (Figure 4.5.16).

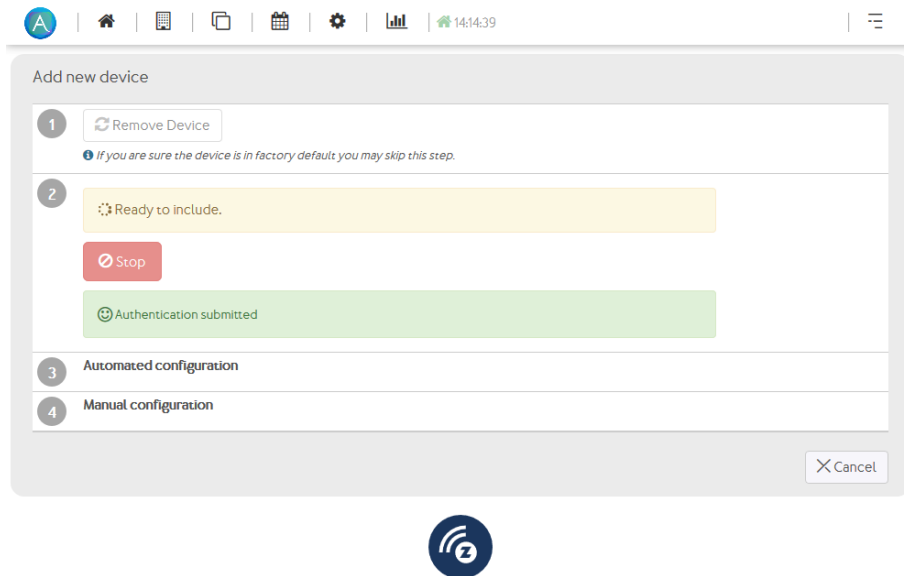


Figure 4.5.15: S2 - Authentication successful

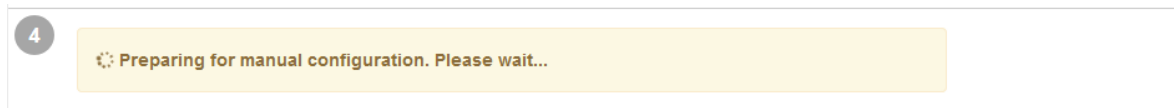


Figure 4.5.16: Device configuration redirect

To see what happens after a Z-Wave device was successful added please do further reading on headline [Manual Configuration](#) otherwise continue with the next headline.

Remove Mode

This function is used to remove an available and functioning device from the network. After removing the device, it can be added in another Z-Wave network again. To remove a device, it is not necessary that the device is part of the network.

Start Remove process

It doesn't matter if you navigate through the tab Add new Z-Wave Device and identify it automatically Menu (Figure 4.5.2) or the vendor-device-specific way (Figure 4.5.6), in both cases a press on the button Remove Device will start the remove process (Figure 4.5.17).

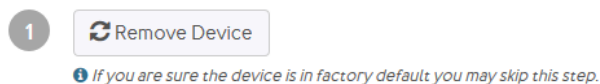


Figure 4.5.17: Remove Device

Stop Remove process (after Remove Device was triggered)

A click on Stop will simply stop the remove process (Figure 4.5.18).

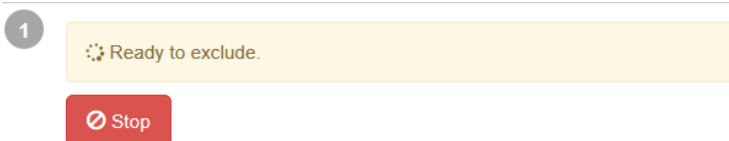


Figure 4.5.18: Remove device - stop

The remove mode also stops when a device was successfully removed or times out after a while if no device was found. A short message including the node ID (if known) or the simple message that the device was successfully removed, will be shown in the remove row. A green fade-in message on the top right corner will indicate that the process was successful, too.

Manual Configuration

If the Automated Configuration was successful, the user is redirected to the Manual Configuration view of the newly added device. Outside the Add process, this view is also reachable under **Menu > ⚙️ Devices > Z-Wave - Manage > Tab - 📶 Z-Wave Devices > Node - ⚙️ Configuration**. Use this view to configure the following properties:

- **Custom Node Settings** (Figure 4.5.19) like node title, create a room, assign node to room, choose type of device group

Figure 4.5.19: Custom node settings

- **Virtual endpoint** (element) naming and their view abilities (Figure 4.5.20) – *Deactivate* means: disable this endpoint completely so it is not visible and cannot be used within logics and other apps

Figure 4.5.20: Virtual endpoint settings

• Node Info

A view (Figure 4.5.21) that shows you all relevant Z-Wave information of the node like:

- *Device Id* - the assigned Z-Wave node ID
- *Brand* - vendor or brand name
- *Device Type* - Z-Wave device type description
- *Wireless Activity* - wireless activity status
(battery devices: 🌿 active, 🌙 sleeping; powered devices: ✅ operating, ❌ dead)
- *Application Version* - application (firmware) version of the device
- *SDK Version* - SDK version of the Z-Wave chip on the device
- *Command Classes* – list of interview status of the Command Classes
- *Security Interview* - Security Interview status
- *Interview* - complete Interview Status

The [🔧 Force Interview](#) button below allows you to reset incomplete device interviews. The controller will then try to repeat the whole interview. This action only makes sense if the device was already added with successful interviewed security command class (it doesn't matter if S0 or S2). If not, it is recommended to remove and add the device again.

The [🔊 Call for NIF](#) button gives you the possibility to send a Note Information Frame to the device which is similar to a simple status request. Note that battery driven devices need to be woken up manually if a quick response is desired. Otherwise the device will react on this NIF on its next wakeup (depending on the controller configuration 1h - 24h).

The screenshot shows the 'Node Info' window for a device with ID 13, brand Fibaro, and device type Notification Sensor. The 'Wireless Activity' is 'deep sleep'. The 'Application version' is 3.2 and the 'SDK version' is 6.51.06. Below this, a table lists the 'Command Classes' and their interview status. All listed command classes have a 'Result' of '✅'. At the bottom, the 'Security interview' status is '✅' and the 'Interview' progress bar is at 100%. Two buttons are visible: '🔧 Force Interview' and '🔊 config_ui_request_node_info'.

Instance	CommandClass	Result
0	Basic	✅
0	ApplicationStatus	✅
0	SensorBinary	✅
0	SensorMultilevel	✅
0	AssociationGroupInformation	✅
0	ZWavePlusInfo	✅
0	Configuration	✅
0	Alarm	✅
0	ManufacturerSpecific	✅
0	PowerLevel	✅
0	FirmwareUpdate	✅
0	Battery	✅
0	Wakeup	✅
0	Association	✅
0	Version	✅
0	MultiChannelAssociation	✅
0	Security	✅
0	AlarmSensor	✅

Figure 4.5.21: Node Info

• Node Association (Needs to be supported by the device)

Associations allow switching a Z-Wave Device B (target) as a result of an event in Z-Wave Device A (source). Z-Wave Device A manages a list of devices to be controlled for each event supported. The device list associated to a specific event - also called association groups - and the devices that are associated with it are shown in the association form in Figure 4.5.22.

In case the information is provided either by the device or by the device record stored in the software, the meaning of the events is written. Otherwise, the event group is shown unnamed as number only. In this case, refer to the device's manual for more information about the association group meaning. The stored devices can be called from the actual device using the button  Update from Device. The buttons  and  are used to add and remove device from the group. Clicking on the add button  will open a dialog with dropdown list, where the target device can be picked.

Within the association group row, the color of the device widget indicates the status of the association entry:

- **Yellow:** Selected in user interface but not stored in device.
- **Grey:** Active in device but not selected in user interface.
- **Blue:** Selected in user interface and stored in device.
- **Grey and Crossed out:** Device is removed

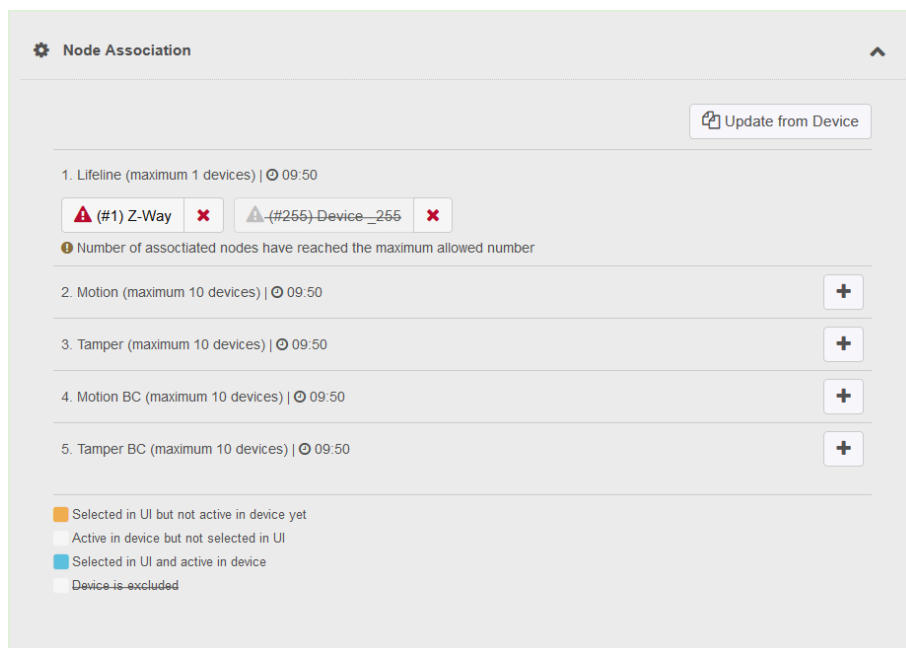


Figure 4.5.22: Node Associations

• Expert Configurations

This section allows you to make some deeper configurations like device adjustments, tests and maintenance. You will find the following three buttons below the node sections:

-  [Hardware Configuration](#)
-  [Expert Commands](#)
-  [Firmware Update](#)

Hardware Configuration

Instead to the view configuration this view allows you to adjust your device hardware properties more in dept e.g. changing the sensitivity or request intervals of a sensor endpoint of the device. If the device was recognized correctly, the different configuration parameters are translated into human-readable dialogs (Figure 4.5.24).

If the device is not known which means there is no Device Description File assigned to it, it is still possible to set configuration values. Figure 4.5.23 shows the generic configuration dialog used in this case. The specific configuration parameters and its values need to be read from the device manual.

Both configurations come with the following standard dialog options:

- **Time Stamp** - when the configuration value was last updated
- **Set Value** - configured value as integer
- **Default value** - information about the default value of this parameter
- **Save this parameter** - button to save the parameter into the device
- **Set to default** - button to reset to default value given by the device itself

There are four more command classes that may need additional configuration and are displayed in the same dialog if the device supports them.

- **Wakeup**
Defines the wakeup interval in which the device wakes up regularly. The controller will set a standard wakeup time of 3600 seconds (1 hour) unless the devices sets a different minimal or maximal wakeup time. In most cases the node ID of the controller is the correct setting for the target node ID and should not be changed. In case this controller is only a secondary controller, this value may change. A tool tip on the input field shows the allowed minimum and maximum wakeup time as reported by the device.
- **Protection**
In case the device supports local protection, meaning suppressing local use of the device, the behaviour of this function can be defined. The protection command class offers more options than displayed here. Refer to the [Expert Commands](#) section for a complete set of controls.
- **Switch All configuration**
Z-Wave supports the so-called switch all function as a broadcast to all switches and dimmers. This setup defines the reaction of the device to such a Switch All command.

Note: For **mains powered** and **FLIRS** devices, the button **Save this parameter** or **Save into Device** will activate the changes within few seconds. For battery-operated devices, the commands are stored to the next wakeup. It is possible and recommended to wake up the device manually to speed up the change of configuration values.

Aeotec | Home | Documents | Calendar | Settings | Status | 10:45:09

(#14) Fibaro PIR G5 (Magic Eye)

Configuration

Parameter: 0

SetDefault

Parameter: 0

Value: 0

Size

☒ auto_detect

☐ 1 byte

☐ 2 byte

☐ 4 byte

Set

Parameter: 0

Get

Param	Date	Size	Value
1	10/27	2	15
2	10/27	1	15
3	10/27	1	1
4	10/27	1	2
6	10/27	2	30
8	10/27	1	-
9	10/27	2	200
12	10/27	1	-
14	10/27	2	255
16	10/27	2	-
20	10/27	1	20
22	10/27	2	30
24	10/27	1	-
25	10/27	1	1
28	10/27	1	-
29	10/27	1	-
40	10/27	2	200
42	10/27	2	3600
60	10/27	2	10
62	10/27	2	900
64	10/27	2	-
66	10/27	2	-
80	10/27	1	10
81	10/27	1	50
82	10/27	2	100
83	10/27	2	1000
86	10/27	2	18
87	10/27	2	28
89	10/27	1	1

Wakeup Settings

Figure 4.5.23: Hardware configuration fallback dialog

Aeotec | Home | Documents | Calendar | Settings | Status | 10:27:45

(#14) Fibaro PIR G5 (Magic Eye)

Configuration Settings

N° 1 - SENSITIVITY

15

Updated at: 10:27 | Default value is: 10 | ⓘ

Save this parameter

N° 2 - BLIND TIME (INSENSITIVITY)

15

Updated at: 10:27 | Default value is: 15 | ⓘ

Save this parameter

N° 3 - PULSE COUNTER

☐ Define amount of pulses. Formula to calculate the number of pulses: pulses = (value + 1)

☐ null

☐ null

Updated at: 10:27 | Default value is: 1 | ⓘ

Save this parameter

Figure 4.5.24: Hardware configuration beautified

Expert Commands

Expert Commands as shown in Figure 4.5.25 display the status values and possible commands in a very generic way. On the left-hand side, the different instances (channels) of the device are listed in a column. In case there is only one channel (that’s the case for most devices), only channel 0 is shown. Clicking on the number opens a dialog showing all internal variables for the channel. The next column shows all the command classes exposed by the device. Again, clicking on the name opens a dialog with more internal status variable information for this command class. On the right-hand side, there is a list of commands. This dialog form is auto generated from the information provided by the command class itself and not optimized for daily usage, so a basic knowledge of how to interact with Z-Wave command classes is essential.

If the command class offers a list of different properties, they will be shown as a table below the command class button. If this table is empty it is recommended to send a Get request and wakeup the device if necessary.

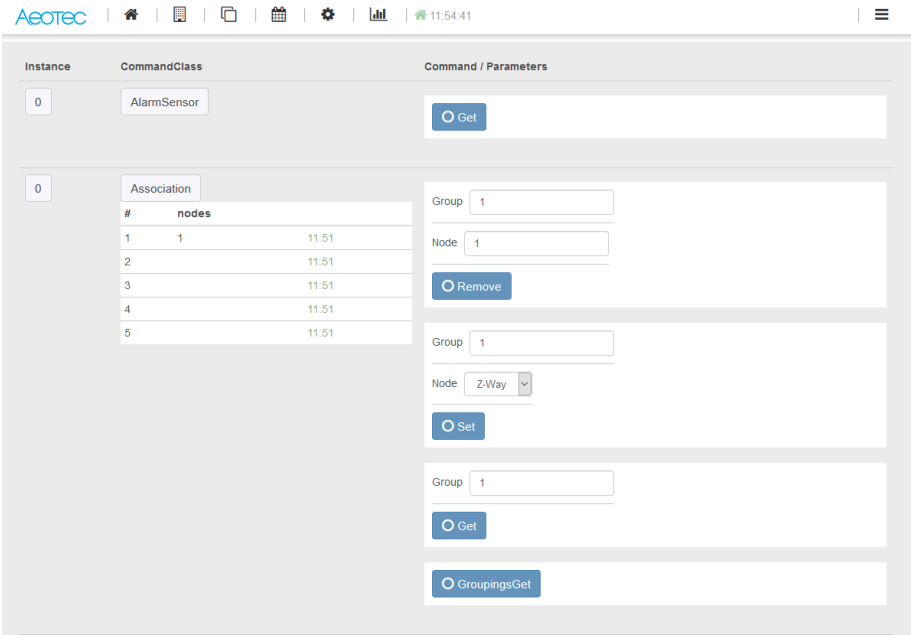


Figure 4.5.25: Expert Commandos

Firmware Update

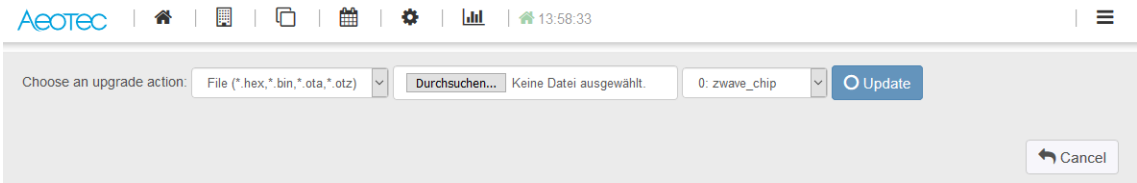


Figure 4.5.26: Firmware update

This button is active if the device supports “Over the Air” firmware update (OTA). The view called up (Figure 4.5.26) will then allow you to upload a firmware in different formats. The uploaded firmware file must be from type *.bin, *.hex, *.ota or *.otz. Furthermore, it is possible to enter an URI to the download target of the firmware file with the same restrictions.

The target field allows to specify the target memory or processor for the update process. For updating the Z-Wave firmware the target 0 must be set. The target 1 is reserved for bootloader updates.

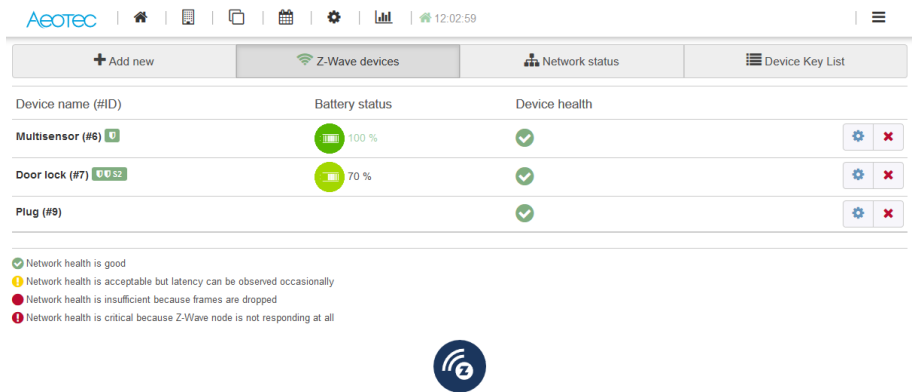
The firmware updating process will take up to 10 minutes. Please do not do any other operation during this time. It may be required to activate the firmware update mode on the device to be updated. Please refer to the manual for further information about activation.

4.6.2 Manage Z-Wave Network

The second option for the menu Z-Wave devices besides adding new devices is the device management menu. Clicking on the  Manage button in the devices view (Figure 4.5.1) opens a menu with four tabs:

-  **Add new** - forwarding to the **Add new Z-Wave device** view (Figure 4.5.2)
-  **Z-Wave devices**
-  **Network status**
-  **Device Key List**

Z-Wave Devices



Device name (#ID)	Battery status	Device health
Multisensor (#6) 	 100 %	
Door lock (#7) 	 70 %	
Plug (#9)		

 Network health is good
 Network health is acceptable but latency can be observed occasionally
 Network health is insufficient because frames are dropped
 Network health is critical because Z-Wave node is not responding at all

Figure 4.5.27: Z-Wave devices view

This is the main overview of all Z-Wave nodes belonging to the network. Figure 4.5.27 shows a list of the physical Z-Wave devices. The column **Device name (#ID)** includes all given node names plus their node id. Clicking on the name, forwards you to the manual node configuration (4.5.1). If the device supports any Z-Wave security standard, it is labelled next to the node name:  for the (old) simple Z-Wave security standard,  **S2** for the new Z-Wave S2 standard and nothing if no security standard is supported. Presumed the device has a battery, the **Battery status** column shows you an icon with the latest battery status in percent.

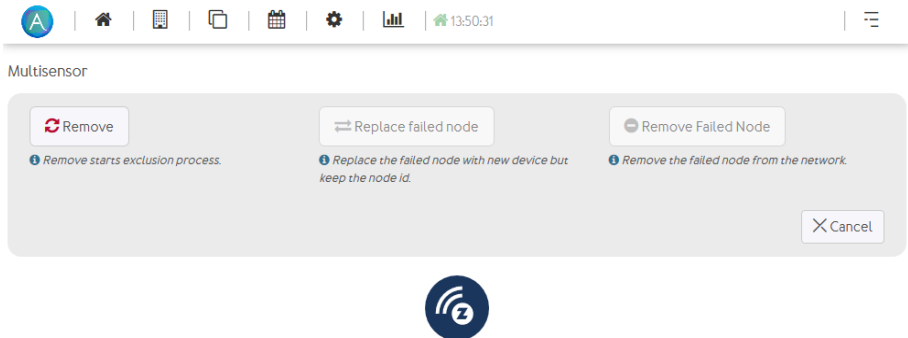


Figure 4.5.28: Remove dialog

In the third column the **Device health** is displayed which is categorized similar as the network health on the dashboard. The small legend at the bottom shows you descriptions of each single health state.

On the right side in each row there are two more buttons:

The  button will open same device management dialog as described during manual post-add-process configuration in Section 4.5.1. The  button opens a dialog to remove the device. As shown in Figure 4.5.28 there are three options:

-  **Remove**
This button will start the Z-Wave Remove Process. The Remove process requires that the device which should be removed is still functioning and accessible.
-  **Replace Failed Node**
Replace a failed node with a new one. Be aware that a failed node can be replaced by a node of another type. Always request device NIF and force re-interview after successful replace process. (gets active if node is failed)
-  **Remove Failed Node**
Only in case the device is defect nor not existent anymore this option shall be used. It will use the Z-Wave function 'Remove Failed Node' without any involvement of the device to be removed. (gets active if node is failed)

Network Status

Figure 4.5.29 shows the  **Network status** overview which collect all important controller data at a glance. It is structured in:

- **Network Health**
Shows you the status of network health (legend below the page) and its quality. The button  **Start network health check** allows you to run a full controller network health check which also often helps to solve problems within the network (Figure 4.5.30).
- **Role in Network**
Gives you information about the role of the controller, its Home ID and the assigned node ID. Usually a controller has the **Primary** role as master device in the Z-Wave network. But it is possible to add it to another Z-Wave network by activating the Learn Mode button  **Start Network Learn Mode**. After the controller was successfully added to the other network, the controller role will become **Secondary**. Note a controller with secondary role has limited configuration possibilities in the network.

Copy Network Information:

In order to initiate a Z-Wave controller replication (copy Z-Wave network information and transfer them from the main controller to a secondary controller), start the Add Mode on your main controller and then initiate the Learn Mode of the already included secondary controller. This will transfer the network relevant information manually.

If a DSK needs to be verified or a DSK pin input is prompted, please check out the label of AutoPilot™'s rear side.

- **Software Information**
Information about the installed version number and compile data.

- **UI**
Information about the UI version and its build date.

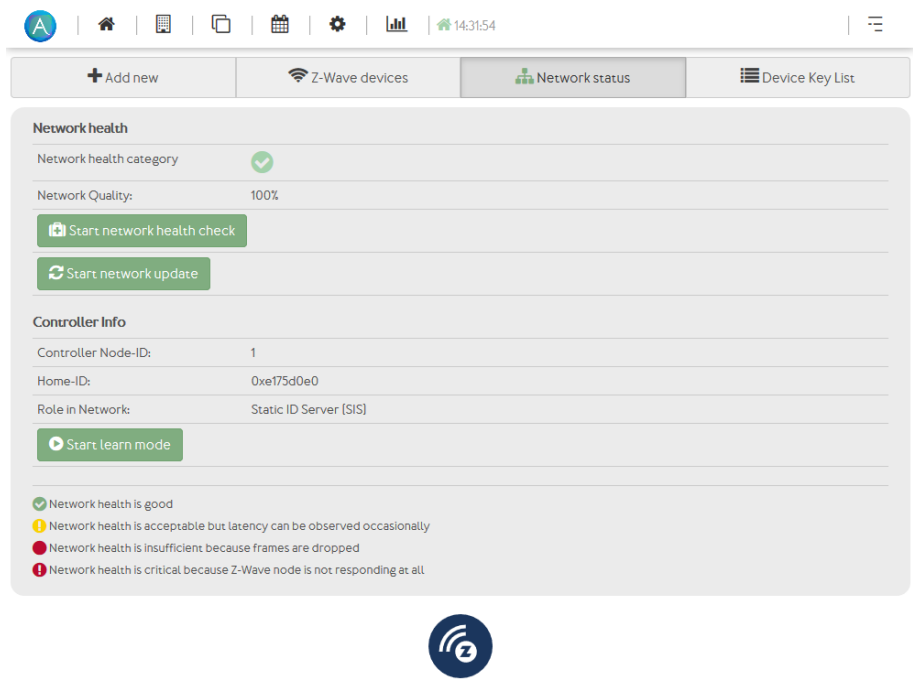


Figure 4.5.29: Network status

Device Key List

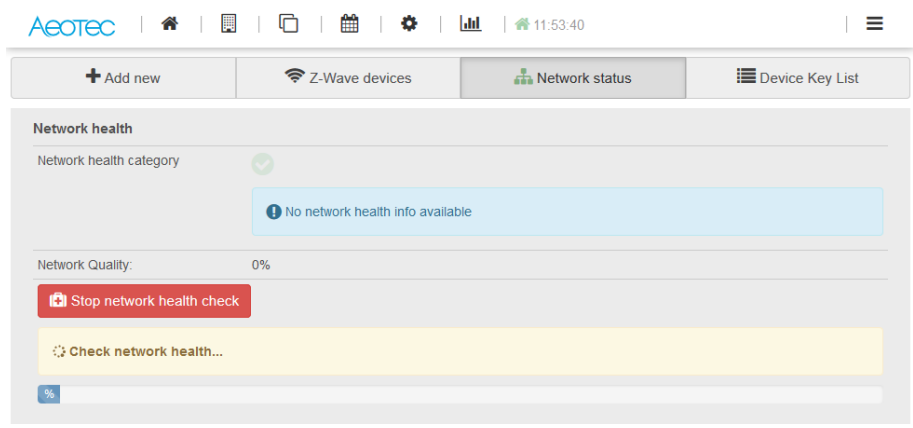


Figure 4.5.30: Learn mode progress

If a device was registered by the SmartStart functionality e.g. **Scan QR Code** (Section [4.5.1](#)), it is listed in this view. The **Reload** button can be used to refresh the list manually. Figure 4.5.31 for example shows the list of device keys which are already registered in the system. One of them is only registered and the other one is registered and in use (**added**). Used means in this context that the corresponding device was added by scanning its QR Code or entering its DSK and then powered up in proximity of the controller and got added automatically. Or in other words: It was added via Z-Wave SmartStart.

A click on opens a popup (Figure 4.5.32) that gives you more information about the device. Furthermore, you can change the device name and assign it to a room although it is not added to

the network yet. Some information will only be available after the device was successfully added. ⚙ will forward you to the manual node configuration (Section 4.5.1). Clicking on 🗑 will remove the registration entry of the device but will not automatically remove it from the network. Therefore, the

Device name	Room	Brand name	Device type	Product name	State
Popp & Co - Binary Switch	Not assigned to a room	Popp	-	Smart Outdoor Plug	
Popp & Co - Binary Switch	Not assigned to a room	Popp	-	Smart Outdoor Plug	included

Figure 4.5.31: Device Key List

device also needs to be removed from the network directly via the Devices menu (Section 4.5.1).

AutoPilot

Device name Popp & Co - Binary Switch

Room Not assigned to a ...

Brand name Popp

Product name Smart Outdoor Plug

Device type -

State included

DSK
09499-59651-30514-48606-45116-49266-55388-00694

Cancel Save

Figure 4.5.32: Device Key List - Information

4.6.3 Z-Wave SmartStart

The Z-Wave SmartStart technology is promoted with:

Simple, Speedy, Trouble-free Installations - Every Time

SmartStart simplifies the installation and setup of smart home systems and devices. Device recognition and add process can now be automatic through the gateway, or through a quick scan of a QR code, for efficient and consistent installation success. It also reduces the susceptibility to errors to a minimum near zero.

There are no complicated add process sequences or keystroke combinations. You can simply mount the devices and provide them with power; setups can be done without even using an instruction manual. In addition to this it comes also with S2 security framework which gives you the highest security level. ([1] Silabs)

To be conform with the Z-Wave Security S2 standard, the AutoPilot™ has a label with DSK code, DSK pin and QR code printed on the rear side.

4.7 Customize

It is possible to add individual icon sets to the AutoPilot™ and share it with others.

4.7.1 Create Your own Icons

First to the icon as such. They must have a size of 64x64 pixel and must be encoded in PNG image file format. You are free to make every icon you can imagine. Please note that there is a list of typical devices where standard icons are applied:

- battery
- heating
- motion
- energy
- water
- gas
- switch
- smoke
- door
- window
- light
- media
- blinds
- cooling
- co
- fan
- flood
- thermostat
- luminosity
- humidity
- temperature

Please note as well that certain elements need two or even three icons to indicate different status of their operation.

4.7.2 Create an Icon Pack

It is certainly possible to just replace the icons right in the User interface exchanging the file in the filesystem on /opt/aeotec-server but there is a much better way. Icons should be grouped into icon sets and should be placed on the server to be available for all AutoPilot™ users. The grouped icons are called icon packs.

An icon pack is essentially a *.gz or *.zip archive file containing different icons. All icons need to be stored in a subfolder with the name of the icon set. The archive must then have the very same name. Only store the icons in the archive and not the subfolder itself!

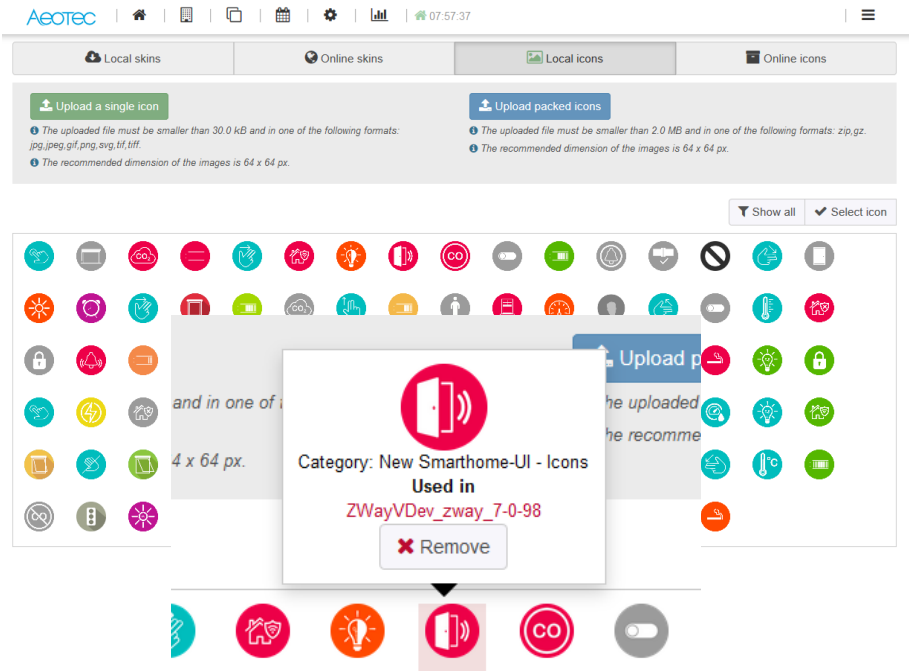
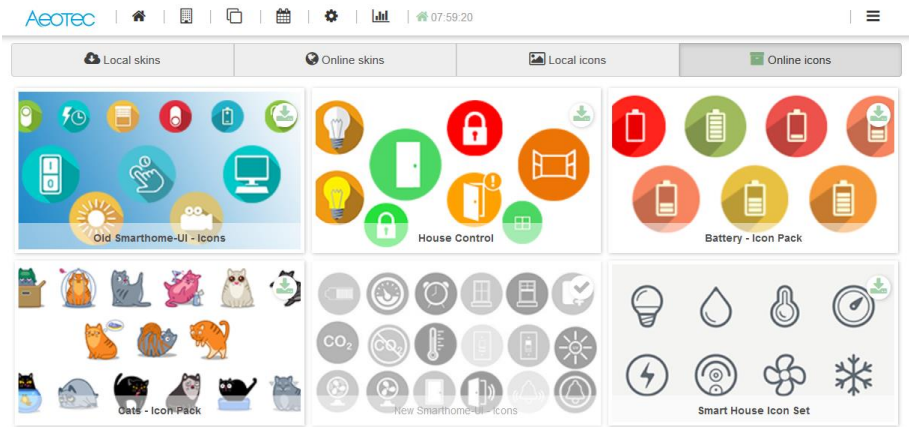
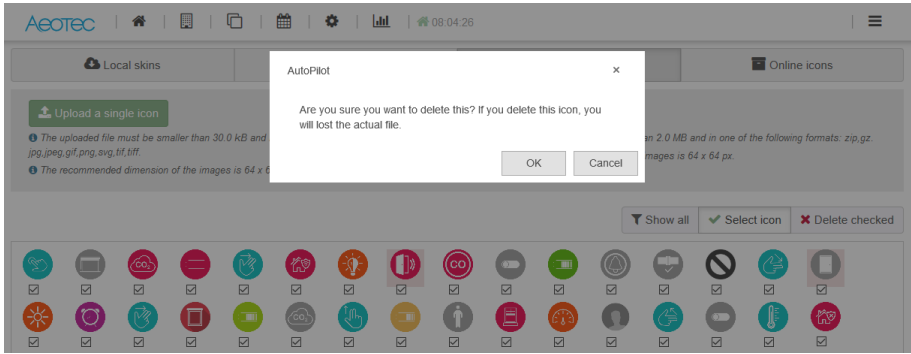
The total size of the archive must not exceed 2 MB.

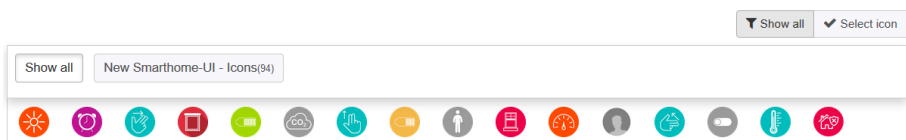
4.7.3 Upload your Icon Set

For this please register at <http://developer.z-wave.me/>.

Once logged in, the right-hand side menu icon allows opening the icon set management dialog. Here you can create a new Icon pack record and manage you existing ones:

Please choose the title of your icon pack and provide a screenshot. This is the image shown in the icon set preview.

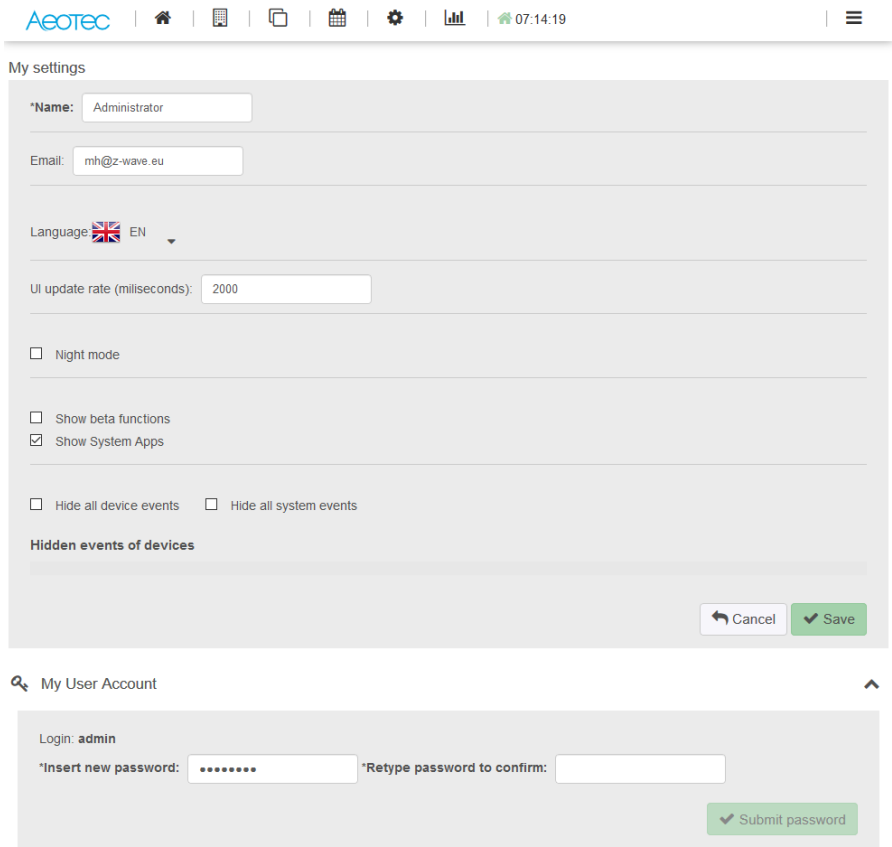




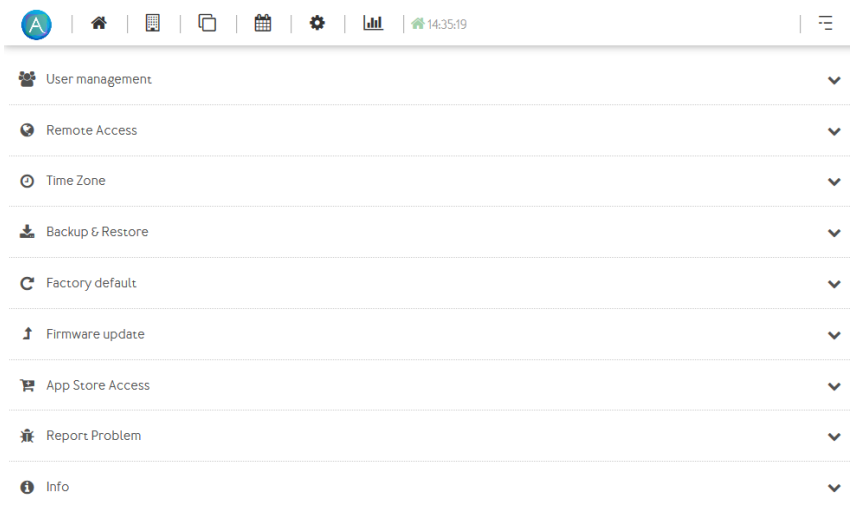
4.8 My Settings

In this dialog the local user interface settings for the logged in user can be changed.

- **Name**
This is the name of the account. Even if this name is changed, the login name is NOT changed.
- **Email**
This email is used for certain email notifications, for password recovery and for the recovery of cloud backups.
- **Language**
Click on the flags to change the user interface language.
- **UI update rate**
This is the refresh rate for the user interface web pages.
- **Expert View**
Having the checkbox marked shows some system apps in the overview of running apps that are not shown by default. For more information on apps, please refer to Chapter 6.
- **Moments**
The two checkboxes allow suppressing certain events. They are then removed from the timeline and will not create any out-of-band alert.
- **Hidden events of devices**
This is a list of the devices where events are deactivated in the element configuration overview. This is the only way to reactivate them if needed.
- **My User Account**
In My User Account also the individual password can be changed.



4.9 Management

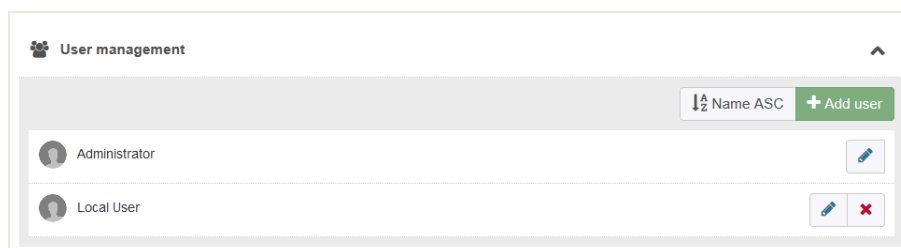


The menu item Management opens a new menu with options to technically manage the platform. Please note that this menu is available for users with administrator privileges only.

The following settings are available:

-  User Management ([4.7.1](#))
-  Remote Access ([4.7.2](#))
-  Time Zone ([4.7.3](#))
-  Backup & Restore ([4.7.4](#))
-  Factory Default ([4.7.5](#))
-  Firmware Update ([4.7.6](#))
-  App Store Access ([4.7.7](#))
-  Report Problem ([4.7.8](#))
-  Info ([4.7.9](#))

4.9.1 User Management



This menu shows the list of users. It is possible to add more users, change their settings, and remove them. Clicking on the setup button opens the user setup dialog. It allows managing:

- **Name**
- **Email**

- **Role types**

This defines the access rights of the user account. Admin allows accessing the management submenu. Standard users will be role-type “users.” It is possible to further restrict a user account to real local access or to make it an anonymous user.

- **Language**

Change language of the user interface.

- **Password**

Change individual password settings.

4.9.2 Remote Access

The dialog allows managing the remote access functions of the controller. By default, the remote access function is activated. This enables accessing the controller from any end device in the Internet, e.g. a mobile phone.

The remote support function is deactivated by default. This function allows support starts with access rights to the remote access server to remotely access your controller using remote shell (SSH). For complicated support issues, the support staff may ask to activate this function. Please make sure to deactivate it after the session. The remote SSH is only accessible to support staff with support infrastructure rights. Nevertheless, there is no good reason to keep a port open if not needed.

4.9.3 Time Zone

This dialog allows managing the time zone of the controller. This ensures that all time stamps and the time clock on the top menu bar refer correctly to the local time at the location of the server. Please note that the time remains unchanged if you access the device from a browser from a different time zone.

4.9.4 Backup & Restore

Under this menu option the AutoPilot™ offers you the possibility to create backups of your whole network information and configurations and also to restore them. A backup allows you to restore your AutoPilot™ in case of broken controller hardware or any other software dysfunctionalities. In addition, the backup is like a copy of the whole system including the Z-Wave controller because it stores all network information. This gives you the possibility to restore or copy it completely on a brand-new AutoPilot™ with a different controller for example.

Local Backup (make a copy of a controller)

The local backup option will generate a local backup file that needs to be stored on the local hard drive of the PC. It includes all important settings and information that currently exist on your AutoPilot™ plus all Z-Wave network information.

Local backup

The backup saves all device names, icons, apps, settings, etc. Informations about Z-Wave nodes present in the network are determined automatically on boot up and can not be changed using a backup. Hence, after a Factory reset all information about the network are gone regardless of any backup. Restoring a Z-wave network with all its Node Ids and its topology from a backup file is possible but requires special caution and knowledge. A dedicated backup/restore function - [available in the Z-Wave expert User Interface](#) - is required for such an operation.

[Download backup to your computer](#)

Restore a Backup (restore a copy of a controller)

If already available on the hard drive, the backup file can now be used to restore or copy the network on a controller as follows:

- tick the checkbox
Are you sure you want to overwrite your current configuration? Have you created a backup?
to enable the upload form
- choose your backup *.zab file within the upload form
- to overwrite the existing network information completely tick the checkbox
Restore Z-Wave Network (read the information carefully!)
Use this also if you want to restore a copy of a foreign network.
- click on  **Upload the file** to start the restore process

After the restore was successful use  **Start network health check** under **≡ Menu > ⚙️ Devices > Z-Wave -  Manage >  Network status** to finish the process. The controller will then complete all missing Z-Wave network information and request all nodes again. Wake up battery driven devices manually to get their response immediately.

Hint to copy a controller:

*A backup of a foreign AutoPilot™ gateway can also be used to copy its Z-Wave network information on another box. Tick **Restore Z-Wave Network** during the restore process to let the controller completely overwrite the existing network configuration. If successful, the gateway will then have the same network configuration as the gateway from which the copy was made from and can also interact with its added Z-Wave devices.*

Restore

☒ Are you sure you want to overwrite your current configuration? Have you created a backup?

ⓘ This function allows you to restore your AutoPilot settings (my settings, spaces, users, apps, Z-Wave network...) that were previously saved in a .zab backup file. The usual restore restores all AutoPilot settings and compares the current state of the Z-Wave network data with the stored ones and tries to heal failed nodes or incomplete interviews. The restored backup does NOT overwrite the existing Z-Wave network configuration. If you want to restore a fully resetted controller or restore your Z-Wave network to an older configuration, select the 'Restore Z-Wave Network' checkbox.

☒ Restore Z-Wave Network

⚠ Attention! Make sure that this option overwrites your entire Z-Wave network information with that of the backup file! Use this option only if you want to restore a previous Z-Wave network backup, i.e. migration of a gateway due to defective hardware or software. Please read the user manual first.

[Durchsuchen...](#) Keine Datei ausgewählt.

[Upload the file](#)

4.9.5 Factory Default

This menu under **Menu > Management > Factory Default** offers you two different ways to reset your AutoPilot™:

- **Controller Factory Default**

This turns just the controller back into factory reset. All connections to added devices, their configurations and all Z-Wave specific settings are lost. This function must be handled with extreme care. An additional dialog requires to explicitly confirm the function. All other settings which are not depending on the Controller or its Z-Wave configuration are not influenced.

If this controller is the primary controller for your network, resetting it will result in the nodes in your network being orphaned and it will be necessary after the reset to exclude and re-include all of the nodes in the network. If this controller is being used as a secondary controller in the network, use this procedure to reset this controller only in the event that the network primary controller is missing or otherwise inoperable.

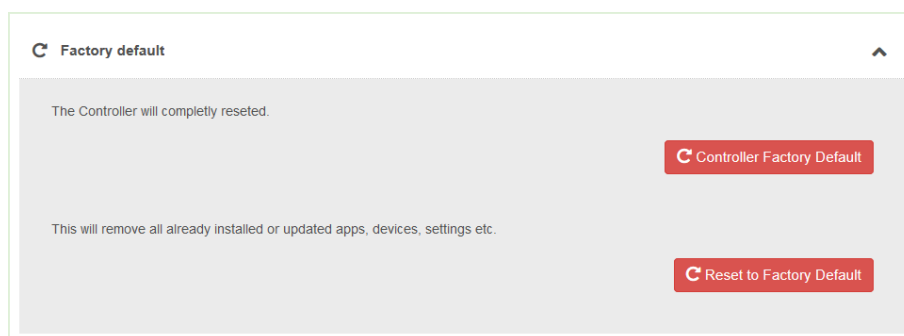
- **Reset to Factory Default**

This function resets the AutoPilot™ back to its factory state, which means:

- Controller will be reset to its factory default → All connections to added devices, their configurations and all Z-Wave specific settings are lost.
- All uploaded images/icons will be deleted
- All custom installed apps and all other app configurations will be removed
- All other settings will be set back to default

Note:

After the controller of the AutoPilot™ was reset in both cases the Z-Wave devices which were added to this controller before will NOT be removed automatically. They still try to communicate with the known controller. To make them ready for a new network insertion just remove them before the add process first or do a manually factory reset of the device (please refer to its manual).



4.9.6 Firmware Update

The firmware update menu refers to two different processes:

- **Update device database**

This button can be triggered to update the Z-Wave device database used for the add process. This update is not critical and new firmware updates will update this device database anyway. However, for debugging purposes, it is sometimes beneficial to force a database update.

- **Firmware Update**

This option will update the whole firmware including the dialog offering this update.

Hitting the button **Open Updater** will open a popup with your unique box ID in the upper left corner, a list of update options, your current installed version on the left and the changelog of the last published version.

After the successful you will, depending on the changes made during the update, stay logged in or be automatically logged out – e.g. after a box or automation server reboot.

4.9.7 App Store Access

The app store allows downloading new apps provided either by AutoPilot™ or other independent developers. Some of these developers may want to limit the use of their apps to a certain group of people, either because this is related to their business model, or because the apps are beta stage or for trial only.

The token concept is a simple and efficient method to limit access. Apps that are uploaded to the app server can be marked with one or more tags. These tags are simple strings and the developer can choose whatever token he wants. He can also have more than one tag for different purposes.

In order to access apps that are tagged, the various tags need to be added to the controller using the form. Tags can be added and removed. Once a tag is added, all the apps with this tag will be shown in the app store.

4.9.8 Report Problem

This menu item demonstrates a quick and simple way to report bugs and problems related to this User Interface. Providing an email is optional, but please be aware that the form will transmit some meta data such as version number of the User Interfaces or version number of the firmware. If you don't like to share such information, please use your personal email. Also, please don't expect an individual answer to the bug reports. This is not a support tool.

4.9.9 Info

The info menu item provides some version information for the user interface and the backend. This information is usually needed for support and troubleshooting purposes only.

4.10 News

Each AutoPilot™ is connected to an RSS feed. This feed contains news and alerts about the platform. Whenever there is a new feed entry, the top menu bar will indicate this with a sign. Clicking on this opens the full list of news. This full list can also be accessed using the 'News' menu item in the configuration section.

5 Association – Supported Lifeline Reports

The controller supports one association group, so called "lifeline" and one node ID can be assigned to this group. A node assigned to this group will be informed upon the device reset of the AutoPilot™ controller.

6 Command Class Reference

Command Classes are groups of wireless commands that allow using certain functions of a Z-Wave device. In the AutoPilot™ ZWave module each Z-Wave device has a data holder entry for each Command Class supported. During the add process and interview of the device the Command Class structure is instantiated in the data holder and filled with certain data.

Command Class commands change values of the corresponding data holder structure. The follow list shows the public commands of the Command Classes supported with their parameters and the data holder objects changed.

In the AutoPilot™ User Interface navigate to **Menu > Devices > Z-Wave - Manage > Select a node > Expert Commands** to execute commands of the supported Command Classes and visualizes all data holder elements in as tree in a simplified user interface.

Command Class (support)	Version	Security Level
ZWAVEPLUS_INFO	2	non-secure
TRANSPORT_SERVICE	2	non-secure
CRC_16_ENCAP	1	non-secure
APPLICATION_STATUS	1	non-secure
SECURITY_2	1	non-secure
SECURITY	1	non-secure
INCLUSION_CONTROLLER	1	non-secure
POWERLEVEL	1	non-secure
MANUFACTURER_SPECIFIC	2	non-secure
VERSION	3	non-secure
SUPERVISION	1	non-secure
INDICATOR	3	non-secure
TIME	1	non-secure
MULTI_CMD	1	non-secure
ASSOCIATION	3	non-secure
MULTI_CHANNEL_ASSOCIATION	4	non-secure
ASSOCIATION_GRP_INFO	3	non-secure
DEVICE_RESET_LOCALLY	1	non-secure
SECURITY	1	secure (S0)

NETWORK_MANAGEMENT_INCLUSION	3	secure (S2)
NETWORK_MANAGEMENT_BASIC	2	secure (S2)
NETWORK_MANAGEMENT_PROXY	2	secure (S2)
ASSOCIATION_GRP_INFO	3	secure (S2)
DEVICE_RESET_LOCALLY	1	secure (S2)
NETWORK_MANAGEMENT_INSTALLATION_MAINTENANCE	2	secure (S2)
MANUFACTURER_SPECIFIC	2	secure (S2)
POWERLEVEL	1	secure (S2)
PROVISIONING_LIST	1	secure (S2)
FIRMWARE_UPDATE_MD	5	secure (S2)
ASSOCIATION	3	secure (S2)
VERSION	3	secure (S2)
INDICATOR	3	secure (S2)
MULTI_CHANNEL_ASSOCIATION	4	secure (S2)
Z/IP	4	secure (S2)

7 Documentation Attachments

Item	Description	Link
DA.1	SDS14222-Association-Command-Class	https://www.silabs.com/documents/login/miscellaneous/SDS14222-Association-Command-Class.xlsx

8 Contents

Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.

9 References

[1] Silicon Labs, Z-Wave SmartStart (n.y.),
URL: <https://www.silabs.com/products/wireless/mesh-networking/z-wave/benefits/smartstart>
(05.07.2019)