Est. USA 1981

www.AKCP.com

SP2+ Introduction Manual

Table of Contents

Introduction

In this manual, we'll cover the main features and basic configuration of the SP2+ and the setup of notifications and the explanation of events will be in the "Notifications" manual.

What is the SP2+?

The SP2+ is a high speed, accurate, intelligent monitoring device, featuring a completely embedded host and operating system. The SP2+ is a complete redesign of the world's best-selling environmental monitoring platform, 3 years in the making with all new hardware and software. We've combined the low cost and simplicity of use of the SP2, along with many advanced features of our securityProbe platform.

The SP+ units support a maximum of 150 sensors per unit. This unit supports up to 4 (physical) sensors.

SP2 + Features:

- IP based, including SNMPv3, HTTPS, VPN
- Send encrypted SNMP Trap and Email Notifications
- Supports 4 Intelligent Sensors or up to 20 Dry Contacts
- Optional cellular modem with external antenna
- Notification Wizards
- Front and Rear Thermal Mapping for any server cabinet
- Low Cost Daisy Chained Temperature sensors
- Optional Expansion Module connectivity
- Virtual Sensors
- Patented Fire Suppression feature
- AKCP Swing Handle Lock support

Important notes:

A) Some of the pictures shown in this manual might not represent the actual Web UI of the unit; this is because we are constantly working on improving the firmware. Please provide us with feedback if you have any issues configuring your unit.

B) All units are shipped with the **default web interface fixed IP address of 192.168.0.100**. We strongly recommend you change this to avoid problems with duplicate IP addresses on your network. Please see the section in this manual on how to setup a new IP address on the unit.

C) AKCP also always highly recommends using a **dedicated 3rd party UPS on the units**. Any damage caused by unstable power or power outages *will void the warranty* on our units.

What’s the difference between the SP2+ and SPX+?

The SP2+ has 4 sensor ports for connecting any compatible AKCP sensor. With the Expansion option it has 3 sensor ports and 1 expansion port.
The SPX+ also supports expansion modules and has modular design allowing you to choose your own configuration.
We have several standard configurations, but with the AKCP Configuration Tool you are able to custom design a unit to your own specifications. See below for available modules to choose from.

What’s the difference between F4 (older) and F7 (newer) processor versions?

The F4 SP+ & the F7 SP+ processors - or as we will refer to them as platforms are different.
The new F7 processor or platform supports more memory on the SP+ (SP2+ and SPX+) units, thus more features. Future firmware development will concentrate on the F7 units and F4 units won’t get new features.

The most notable difference between the platforms is the supported number of sensors when the VPN feature is enabled: the total sensor count is reduced to 36 on F4 units, but it is still 150 on F7 units.

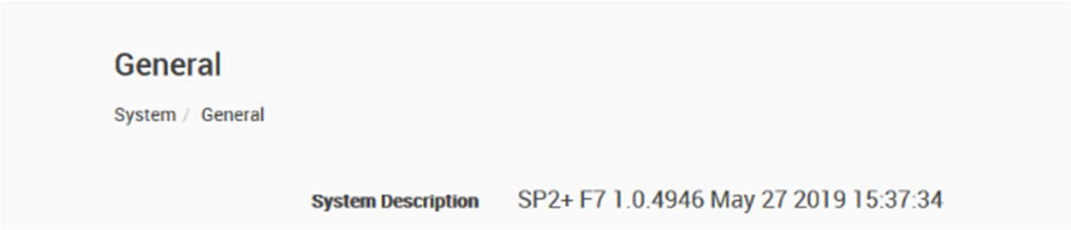
When upgrading the firmware, there are two separate .bin files included in the firmware update package. One for the F4 units and one for the F7 units.

If you try to upgrade your unit with the wrong .bin file, the firmware upgrade will fail. So please make sure you use the correct file for your unit type following the firmware upgrade instructions in the text file that is included in the compressed firmware package.

Also very important to note that any backup configuration created on the F4 platform cannot be uploaded to the F7 platform unit and vice versa.

In the SP+ units web UI you will be able to view which platform the unit is using.

This can be checked in the Settings >> General page >> System Description:

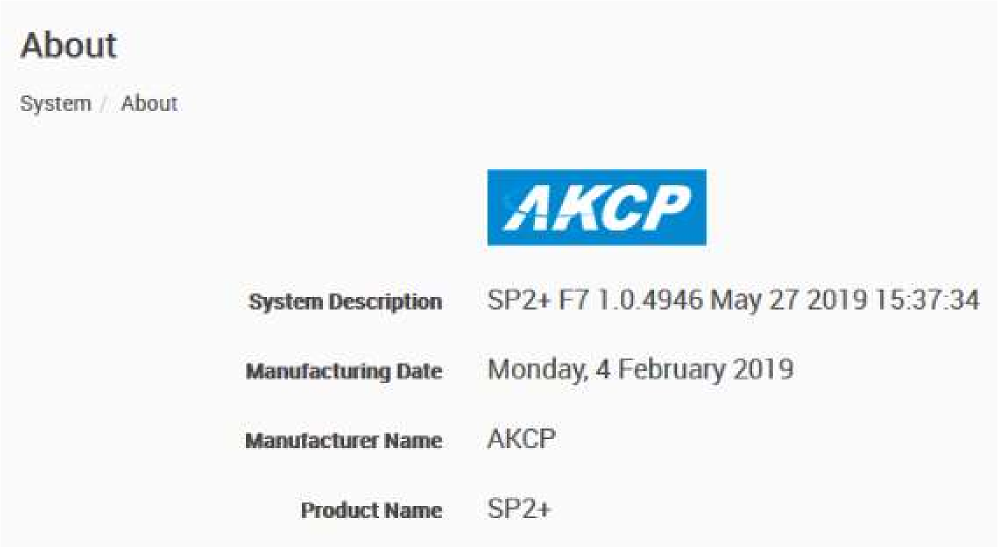


General

System / General

System Description SP2+ F7 1.0.4946 May 27 2019 15:37:34

And in the Settings >> About page >> System Description:



About

System / About

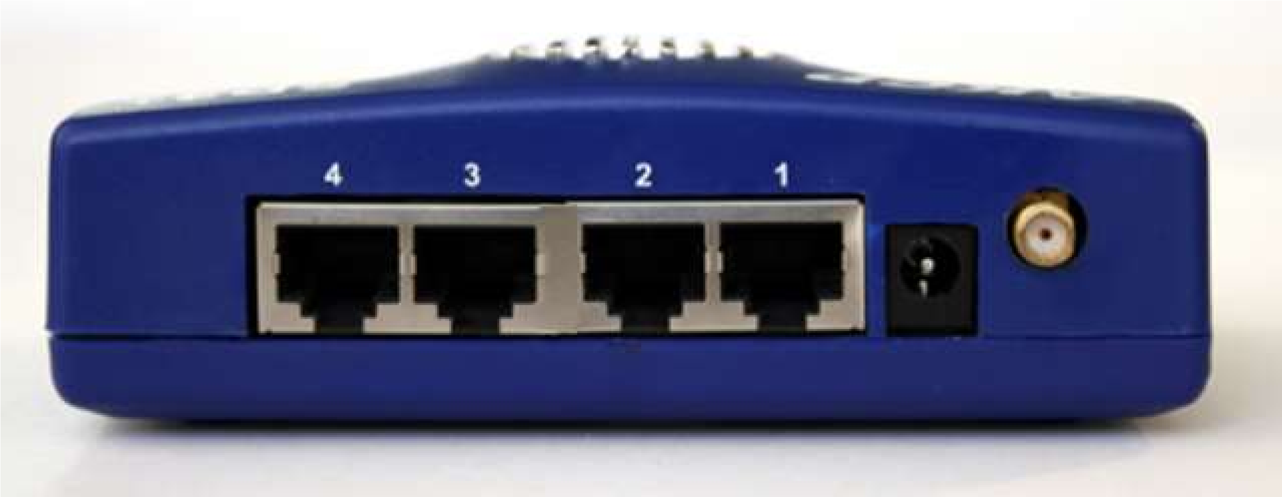
System Description SP2+ F7 1.0.4946 May 27 2019 15:37:34

Manufacturing Date Monday, 4 February 2019

Manufacturer Name AKCP

Product Name SP2+

Port assignment information for SP2+ units

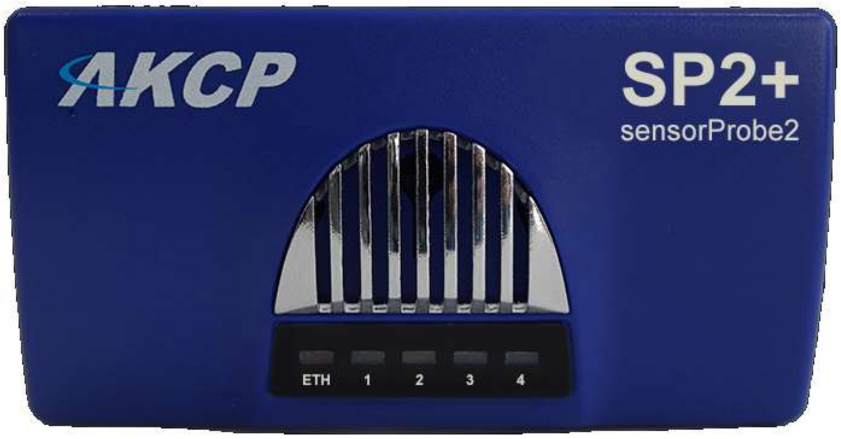


Port numbering starts from the power connector on the unit: the closest port to the power connector is Port 1 and closest to the Ethernet interface is Port 4.
You may connect AKCP intelligent sensors to any available ports.

Important notes:

- The power adapters that are used on sensorProbe+ units **shipped after August 2017** are now **5 Volts**. Please verify the voltage of your sensorProbe+ before ordering replacement power supplies.
- If you're using analog pins on the sensor ports (with manually on-lined DCV sensors, and pin 7 of the RJ45 connector) make sure that the **voltage doesn't exceed 3 Volts**. Otherwise you can damage the unit!

LED information for SP2+ units



Power/Ethernet Link - Sensor 1 - Sensor 2 - Sensor 3 - Sensor 4

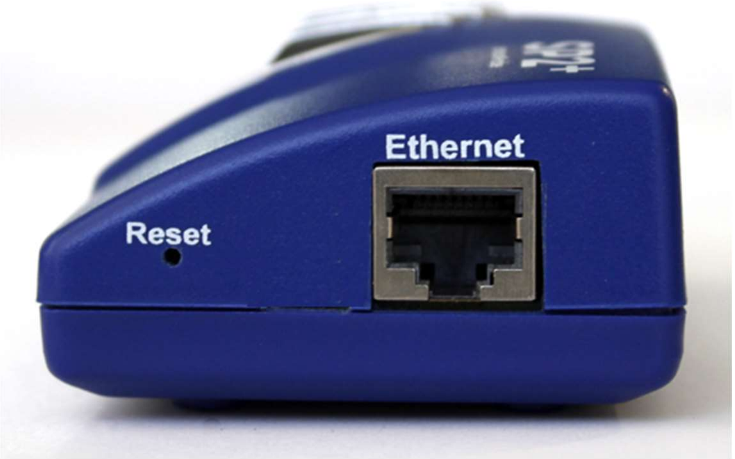
The **Power/Ethernet LED** will become red if there's no network connection, and blinking green (according to LAN activity) when the connection is normal.

For **Sensor LEDs** (green):
Off = offline
On = online and normal
Slow blinking = Warning status
Fast blinking = Critical and Error status

The internal **Buzzer** can provide audible notifications for sensor statuses. Please check our separate SP+ Buzzer manual for using this feature.

Reset button functions for SP2+ units

There are specific commands you can send to the unit by holding the Reset button for a specified amount of time.
You'll have to use something sharp, such as a straightened paperclip to be able to press Reset.



Commands:

Time to hold	Action
< 3 sec	Speak/show IP and broadcast its info (display on LCD sensor too, if connected)
3..7 sec	Reboot (reset CPU)
7..12 sec	Web UI password reset
12..17 sec	Clear the sensor, notification and access DBs, logs Serial flash erase (DB erase without factory reset, the system configuration is kept)
17..25 sec	Reset to factory defaults (serial flash erase + config erase)
> 25 sec	No action (useful when the button was pressed by mistake)

Notes:

- When the Reset button is held for longer than 12 seconds (DB erase) and then released, the Sensor Port 1 and 2 LEDs will give a visual indication of the state of database erase (the reboot and password reset doesn't have visual indication).
- When the button is held longer than 17 seconds (factory reset) and then released, these sensor port LEDs will be blinking fast and alternate during the factory reset mode.

Setting up the unit's IP address

<u>Very Important Note:</u> The unit's ship with the passwords **<u>enabled</u>**. The default log in for the web interface is Username: *admin* Password: *public*

Every unit is shipped with the default IP address of **192.168.0.100**
First we will go through the process of changing this IP address to fit your own network configuration.

Note: In some cases your computer might not be able to connect to this default IP address. In this situation you either need to:
a) add this IP your computers routing table or
b) add a secondary IP address to the LAN card to allow access to the unit.
See below how to setup these.

Ensure the following items are available to you before starting:
- RJ45 CAT5 crossover cable with RJ45 male connection
- A PC with Ethernet card or LAN socket, logged in with Administrator rights

1) Connect the unit via the Ethernet port of the unit to your computers LAN or Ethernet port with a CAT5 crossover cable.
2) Open a web browser and type the default IP address, hit enter.

You'll be presented by the **Summary** page.
Go to the **System/Network** page to change the network settings (see below in this manual).

Once you have assigned the new IP address use the "ping" command to test the unit's reply.

How to add a manual route to the computer’s routing table?

Open an Administrator Command Prompt (CMD) window and type:

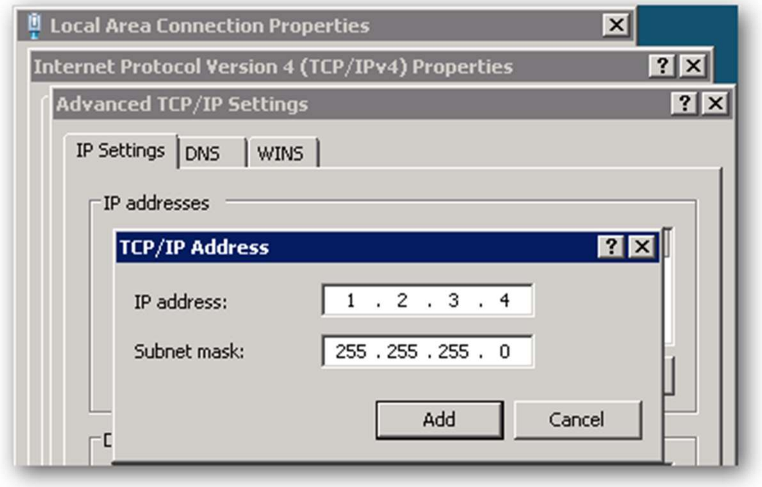
```
route add 192.168.0.100 10.1.1.20
```

Where 10.1.1.20 is the IP address of the Ethernet interface on the PC that the unit is plugged into with the crossover cable.

Note: If you do not receive an 'OK!' message then a parameter was wrong or missing.
The route is not persistent (removed upon rebooting), but you can also delete it with the `route delete 192.168.0.100` command.

How to add a secondary IP address to the computer’s LAN card?

You can do this via the GUI by opening the LAN connection’s properties:


Local Area Connection Properties
Internet Protocol Version 4 (TCP/IPv4) Properties
Advanced TCP/IP Settings
IP Settings
DNS
WINS
IP addresses
TCP/IP Address
Add
Cancel

IP address: 1 . 2 . 3 . 4

Subnet mask: 255 . 255 . 255 . 0

Or open an Administrator Command Prompt (CMD) window and type:

```
netsh interface ipv4 add address “Local Area Connection” 192.168.0.2
255.255.255.0
```

The above command adds the IP Address 192.168.0.2 (with Subnet Mask 255.255.255.0) to the connection titled “Local Area Connection”.
You will then be able to connect to the unit with its default IP.

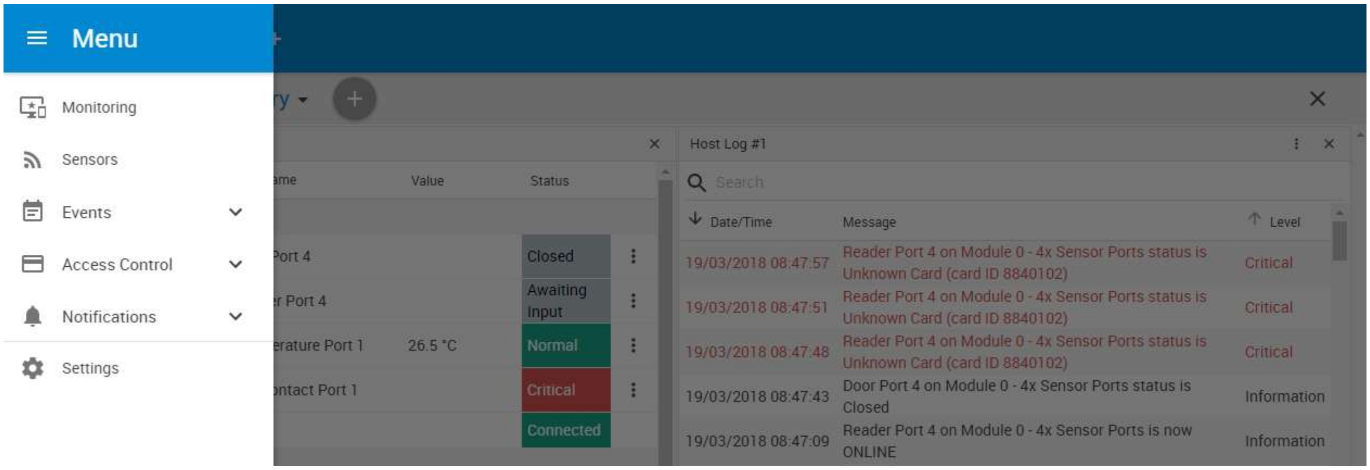
Note: The secondary IP address is permanent for the LAN connection; don’t use it if you only need it once. Instead use the routing table method above.

SP2+ Web UI Walkthrough

Menu navigation

With newer firmware (after 1.0.3074), the Web UI and the menu structure has been changed on all SP+ family devices.

To open the menu, click on the three horizontal lines in the upper left corner: ☰



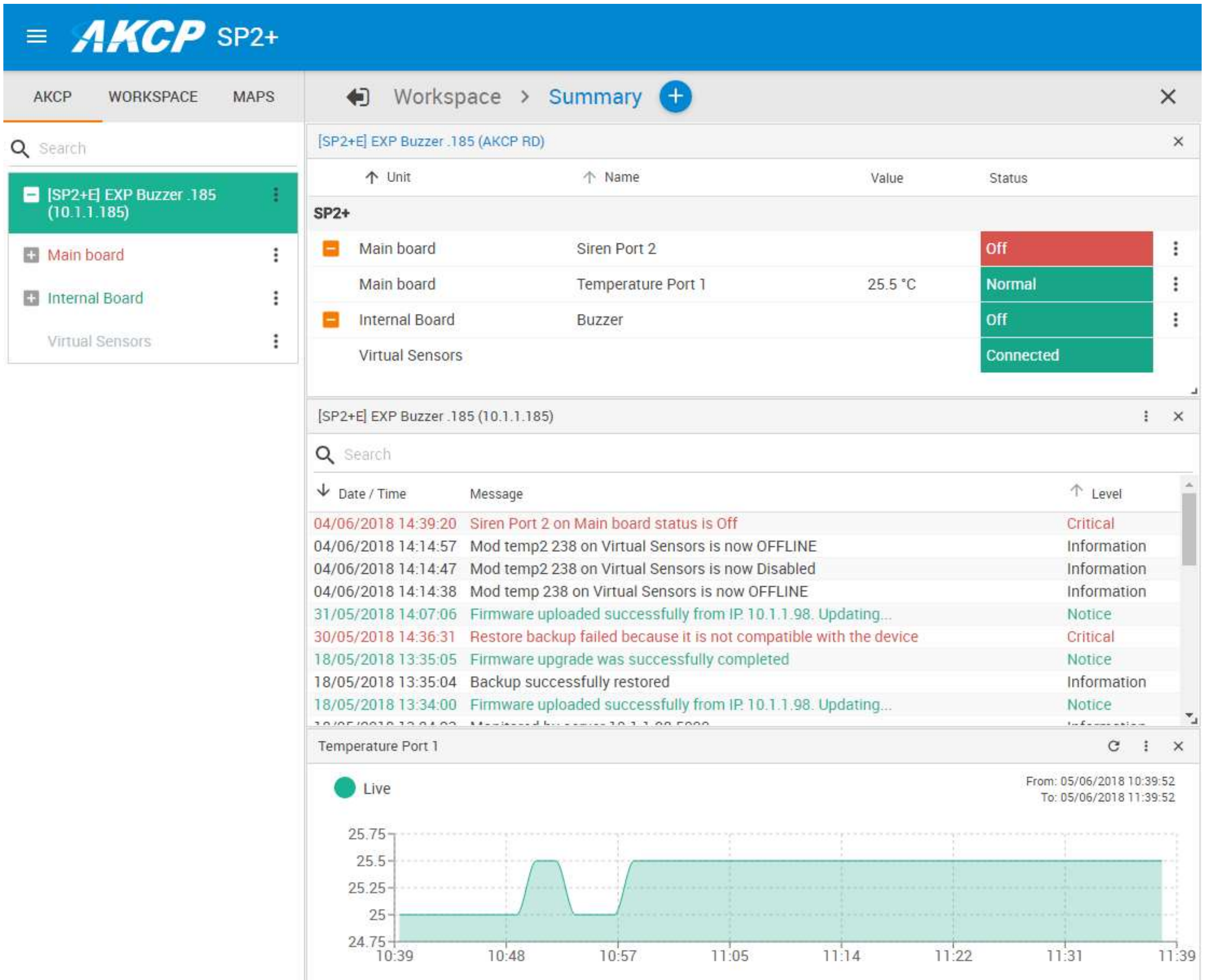
ame	Value	Status
Port 4		Closed
r Port 4		Awaiting Input
erature Port 1	26.5 °C	Normal
ntact Port 1		Critical
		Connected

Date/Time	Message	Level
19/03/2018 08:47:57	Reader Port 4 on Module 0 - 4x Sensor Ports status is Unknown Card (card ID 8840102)	Critical
19/03/2018 08:47:51	Reader Port 4 on Module 0 - 4x Sensor Ports status is Unknown Card (card ID 8840102)	Critical
19/03/2018 08:47:48	Reader Port 4 on Module 0 - 4x Sensor Ports status is Unknown Card (card ID 8840102)	Critical
19/03/2018 08:47:43	Door Port 4 on Module 0 - 4x Sensor Ports status is Closed	Information
19/03/2018 08:47:09	Reader Port 4 on Module 0 - 4x Sensor Ports is now ONLINE	Information

This will bring up the full menu for navigation.
Depending on the device, you might see additional menu items, such as Power.

Important Note:- As Microsoft no longer supports the Internet Explorer web browser, we also do not support any version of IE when viewing our web interface on all AKCP base units. Please use the Chrome or Firefox browsers when viewing the base units web UI.

Monitoring Summary page



[SP2+E] EXP Buzzer .185 (AKCP RD)

Unit	Name	Value	Status
SP2+			
Main board	Siren Port 2		Off
Main board	Temperature Port 1	25.5 °C	Normal
Internal Board	Buzzer		Off
Virtual Sensors			Connected

[SP2+E] EXP Buzzer .185 (10.1.1.185)

Date / Time	Message	Level
04/06/2018 14:39:20	Siren Port 2 on Main board status is Off	Critical
04/06/2018 14:14:57	Mod temp2 238 on Virtual Sensors is now OFFLINE	Information
04/06/2018 14:14:47	Mod temp2 238 on Virtual Sensors is now Disabled	Information
04/06/2018 14:14:38	Mod temp 238 on Virtual Sensors is now OFFLINE	Information
31/05/2018 14:07:06	Firmware uploaded successfully from IP. 10.1.1.98. Updating...	Notice
30/05/2018 14:36:31	Restore backup failed because it is not compatible with the device	Critical
18/05/2018 13:35:05	Firmware upgrade was successfully completed	Notice
18/05/2018 13:35:04	Backup successfully restored	Information
18/05/2018 13:34:00	Firmware uploaded successfully from IP. 10.1.1.98. Updating...	Notice

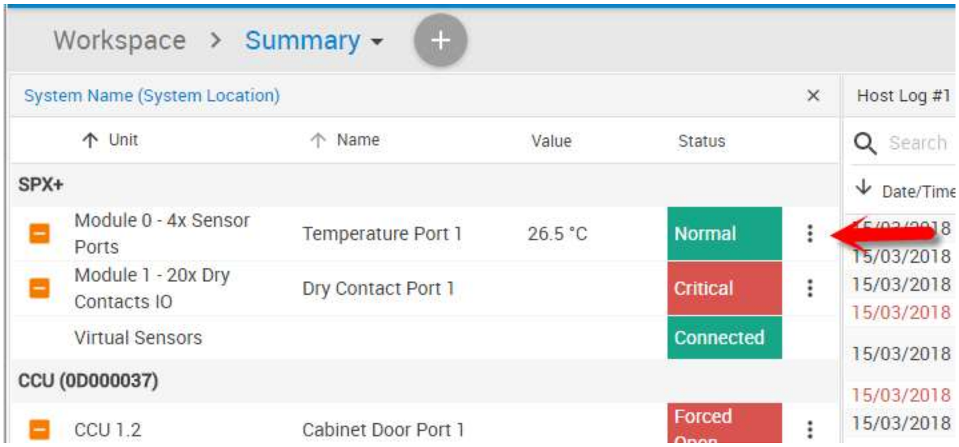
Temperature Port 1

This is the Summary page with Sensor Status and the Event Log, with the Temperature Sensor Graph enabled.

Host Log

The Host Log contains all entries from the “All Events” category. We’ll explain the different categories in the Notifications manual.
The last 30 entries are shown, but if you’re scrolling down the list, more events (30 more) will be loaded automatically. You can view the full log if you keep scrolling down.

In the Summary page's Sensors Information window you can do the following:

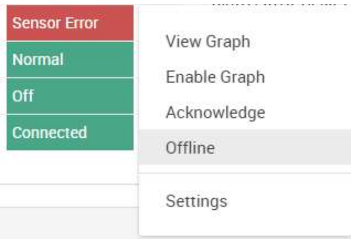


System Name (System Location)

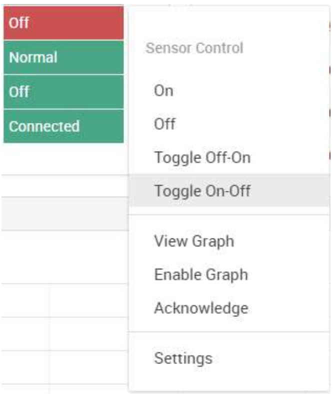
Unit	Name	Value	Status
SPX+			
Module 0 - 4x Sensor Ports	Temperature Port 1	26.5 °C	Normal
Module 1 - 20x Dry Contacts IO	Dry Contact Port 1		Critical
Virtual Sensors			Connected
CCU (0D000037)			
CCU 1.2	Cabinet Door Port 1		Forced Open

Date/Time
15/03/2018
15/03/2018
15/03/2018
15/03/2018
15/03/2018
15/03/2018
15/03/2018

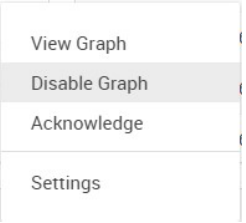
Click on the configuration menu button ⋮ directly next to the right of a sensor to access its popup menu.



Directly acknowledge a sensor's status, and put the sensor offline



Control the relay-type sensors

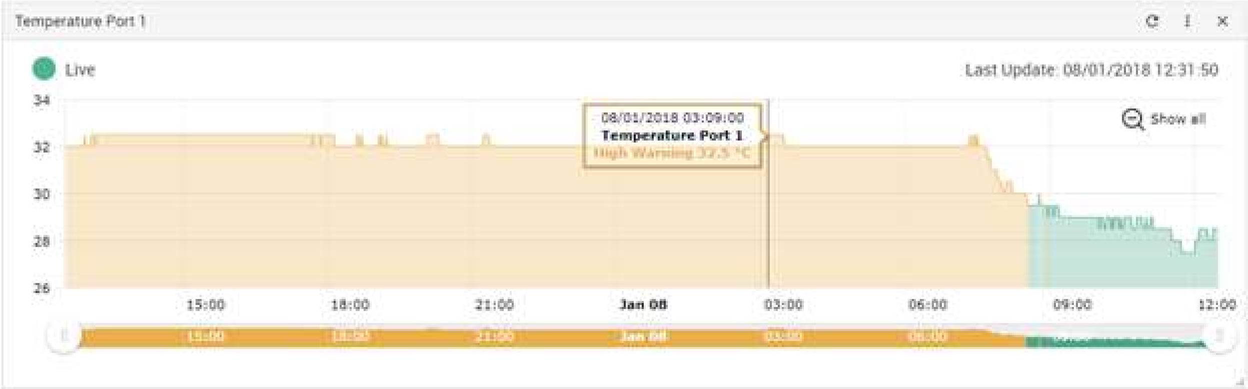


Enable/disable graph data collection per sensor (if they support it), and display the graph display window for the Summary page
We'll explain the Graph feature in more detail below.

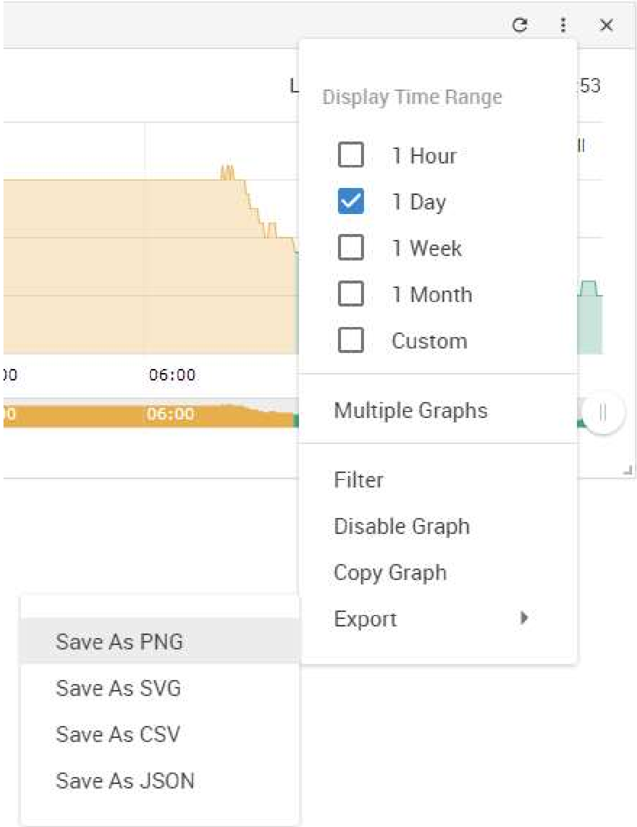
Graph feature

After you've enabled the data collection for a sensor, you can choose to display specific time intervals of the stored data: hourly/daily/weekly/monthly and custom display interval.
You can also export the recorded data in multiple formats.

Important: The maximum number of enabled graphs per unit is 14.

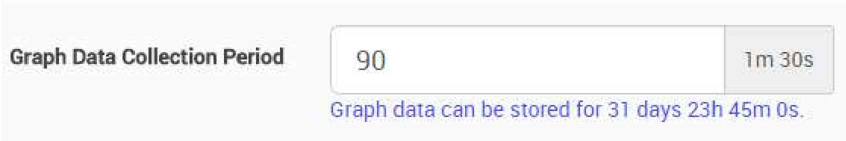


In this example picture, we've chosen to display the temperature sensor's daily maximum.
You could also resize the graph window (including full screen) and move the scale to display more or less data.



You can choose to export the graph data in selected formats by clicking on the graph's menu on the right, then by choosing the desired format from the popup menu.
The file will be downloaded automatically and assigned a file name that will contain the sensor's name, IP address of the unit, and the date and time.

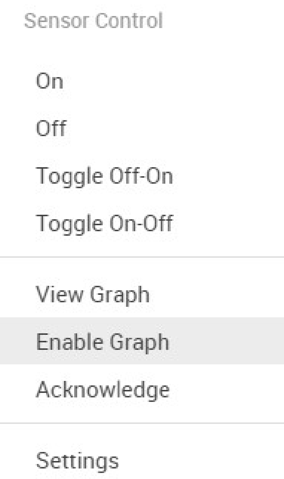
The graph is always a **Live Graph**; you can set the data collection period in the General Settings page (see below for more information).
You may also refresh the graph data manually with the refresh button on the right.



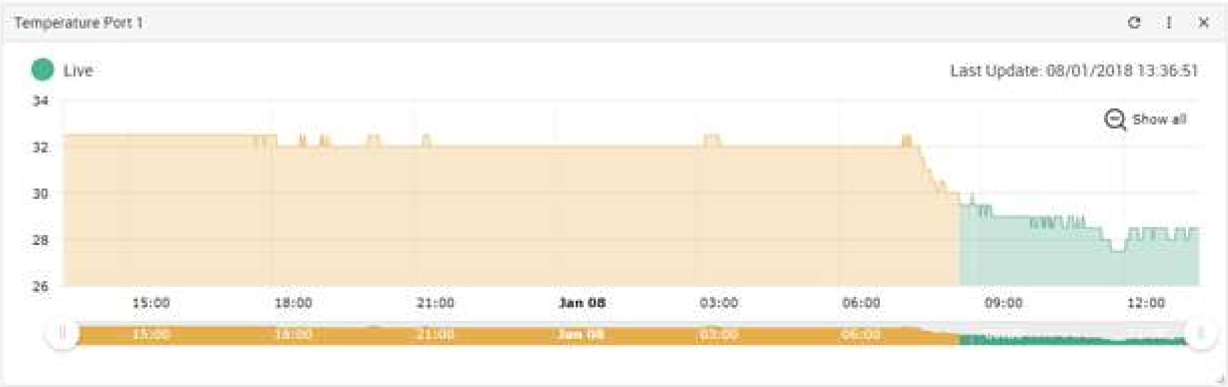
Graph Data Collection Period 90 1m 30s

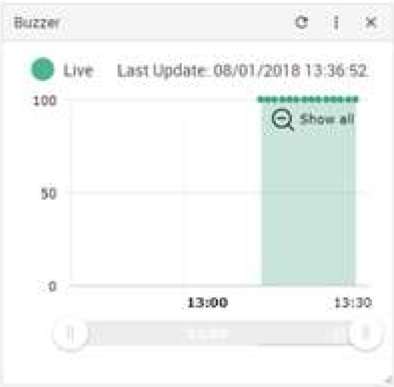
Graph data can be stored for 31 days 23h 45m 0s.

If you want to view multiple sensor graphs, first you need to **Enable Graph** for a sensor that supports graphing from the sensor's menu. Then select **View Graph** to display it. The data collection will run in the background even if you don't display the graph.



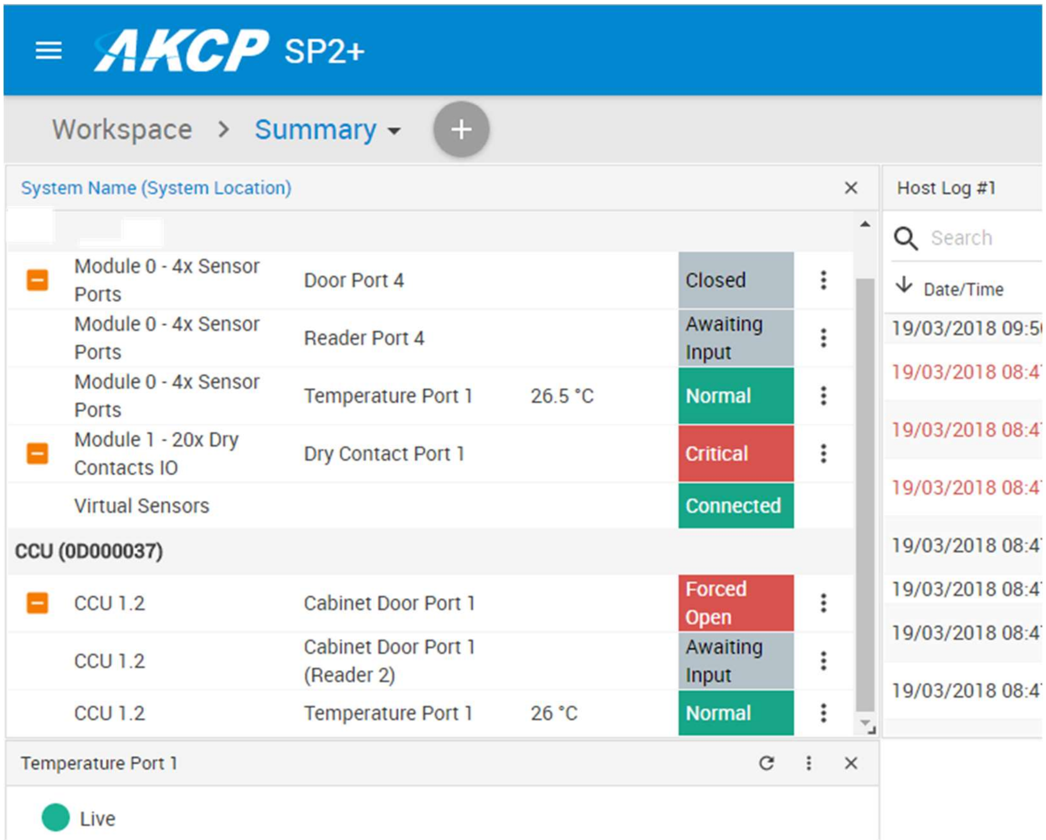
The second graph will appear below the first graph (you can freely rearrange it).





Expansion Units

If you have an expansion unit connected and sensors on the expansion board, they will be also listed in the System Name Information window as shown below. If you have a BEB unit, please refer to that separate manual titled SPX+ BEB Units. BEB units are NOT supported on the SP2+, only on the SPX+ units. E-sensor8 & E-opto16 expansion units are supported on the SP2+.



System Name (System Location)

Module 0 - 4x Sensor Ports	Door Port 4		Closed
Module 0 - 4x Sensor Ports	Reader Port 4		Awaiting Input
Module 0 - 4x Sensor Ports	Temperature Port 1	26.5 °C	Normal
Module 1 - 20x Dry Contacts IO	Dry Contact Port 1		Critical
Virtual Sensors			Connected
CCU (0D000037)			
CCU 1.2	Cabinet Door Port 1		Forced Open
CCU 1.2	Cabinet Door Port 1 (Reader 2)		Awaiting Input
CCU 1.2	Temperature Port 1	26 °C	Normal

Host Log #1

Search

Date/Time

19/03/2018 09:5
19/03/2018 08:4
19/03/2018 08:4
19/03/2018 08:4
19/03/2018 08:4
19/03/2018 08:4
19/03/2018 08:4
19/03/2018 08:4

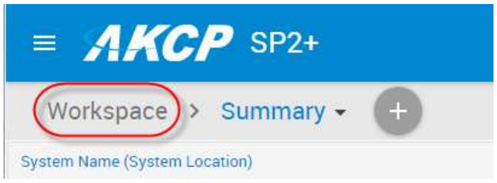
Temperature Port 1

● Live

In the picture above we have a CCU (Cabinet Control Unit) connected as an expansion board, with an additional Temperature Sensor connected to one of its ports.
The base unit (listed as System Name) can be changed by clicking on the link also has a Temperature Sensor connected to Port 1.

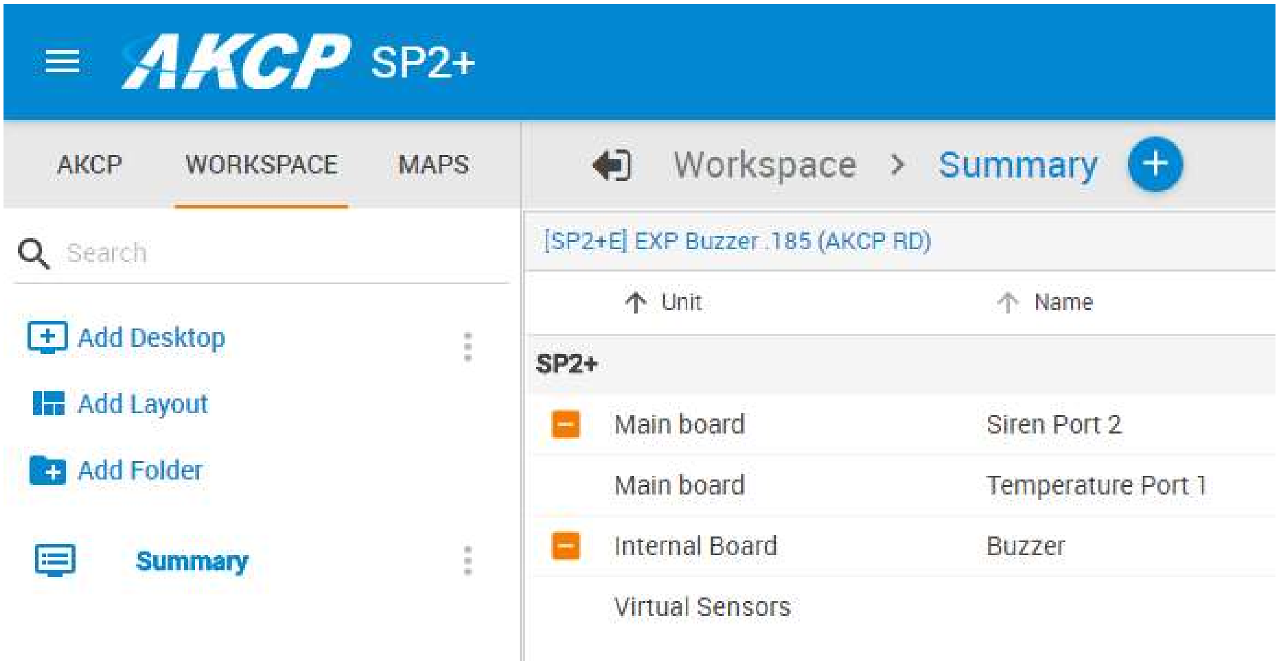
Managing Desktops and Maps

The updated SP+ Web UI has the Workspaces feature from the AKCPro Server's HTML5 UI.
With this you can manage and view different Desktop layouts in a quick and easy way, create multiple custom Desktops as well as select from pre-defined layouts with placeholders for displaying your sensor gauges, logs etc.



To enter into the Workspace mode, click on the Workspace link circled in red as shown above.

The default Desktop is the Summary page on all devices.



[SP2+E] EXP Buzzer .185 (AKCP RD)

Unit	Name
SP2+	
Main board	Siren Port 2
Main board	Temperature Port 1
Internal Board	Buzzer
Virtual Sensors	

Important Notes on custom desktops

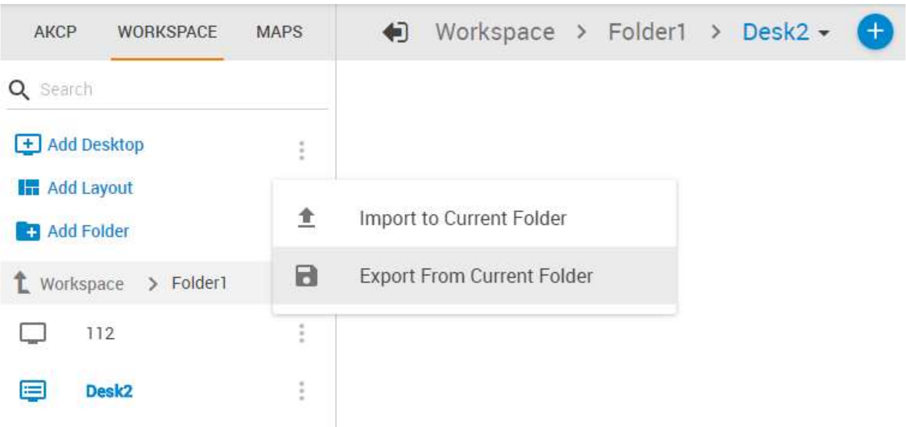
Please note the custom Desktops that are created **ARE NOT** stored in the SP+ units memory. These are HTML based, so they are stored in the browser cache, or local data on the Chrome & Firefox browsers. In other words, the Workspaces are not portable.

So, if you factory reset the unit or clear the cache on your internet browser the folders and custom desktops will be lost.

Generating a backup file from the Maintenance menu will also contain the custom desktops (added after firmware version 1.0.4209).

Without generating a full backup file, you could to export and then import the desktop configuration before you change browser, change your device or before you clear your browser cache. The configuration files will be saved as JSON files.

You can click the Export / Import command on a Desktop to save/reload it individually:



Viewing custom desktops different users & PC’s

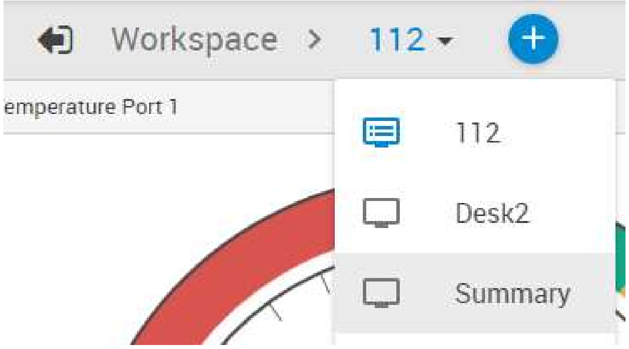
Regarding the viewing of your custom desktops via other users. Because multiple users can log into the SP+ unit from the same PC or different PC’s on the network, the following applies:-

If two different users (different usernames) log in to the same SP+ unit they will not be able to view the other users custom desktops.

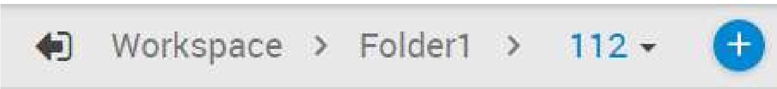
If the same user logs into the SP+ from two different PC’s they will not be able to view the custom desktops (they do not synchronize), so the custom desktops will only be viewable on the original PC that they were created on as again these are stored on the PC’s browser local data.

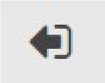
Managing Desktops

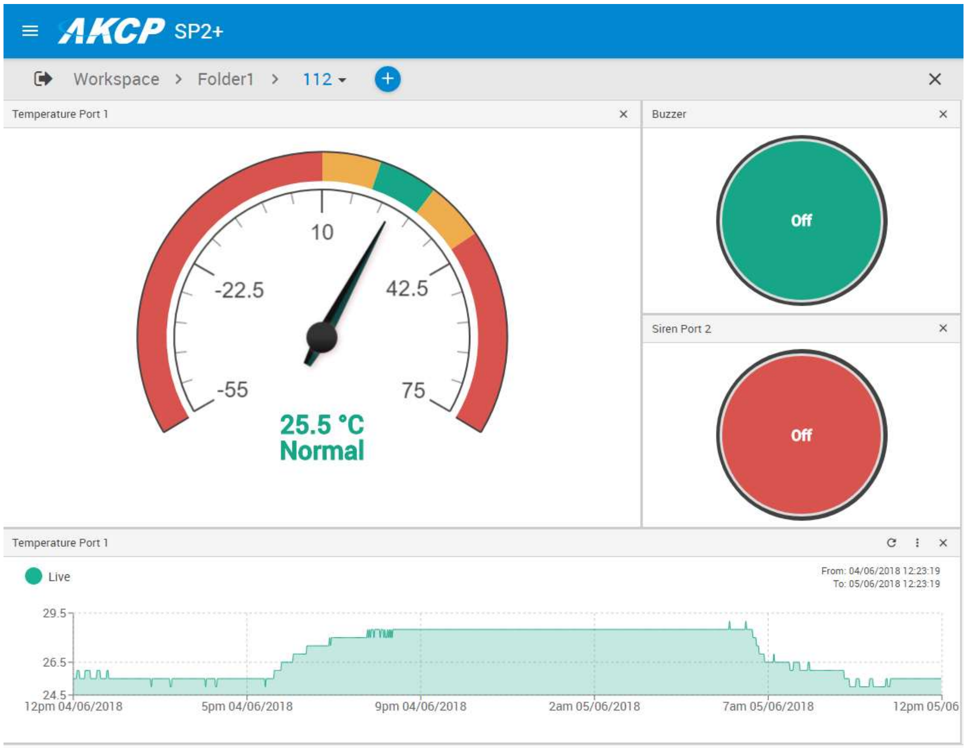
Navigation



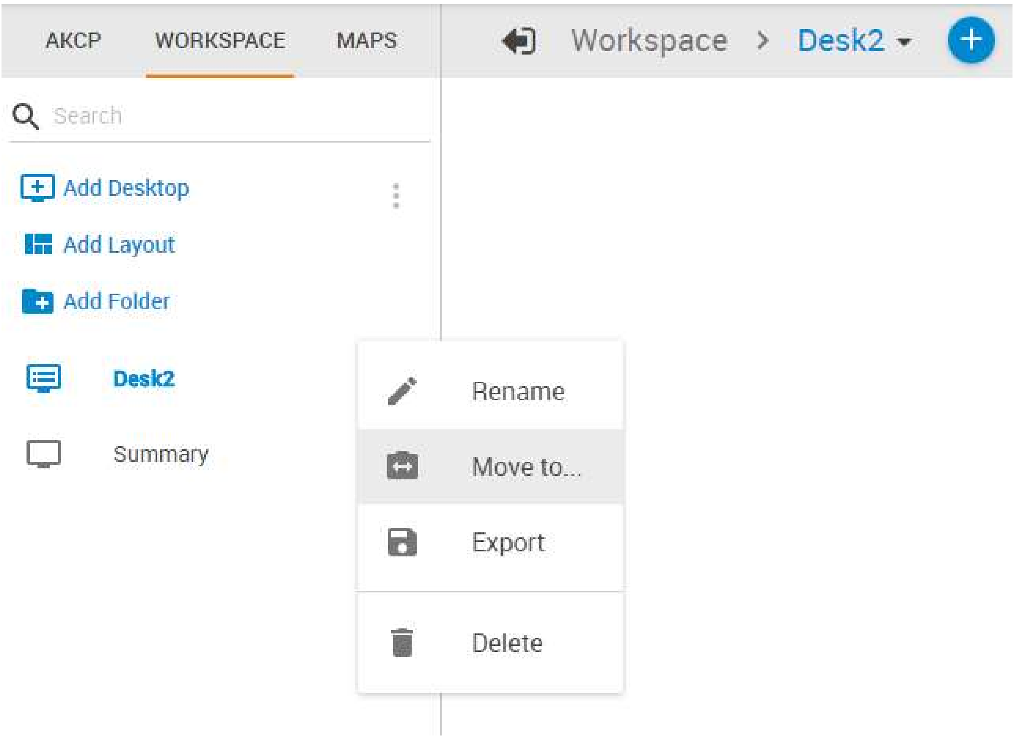
You can manually change between Desktops using the arrow menu, or by directly clicking on the desired Desktop if they are stacked under a folder.



 With this button, your current Desktop will expand to the browser's screen width as shown on the screenshot below:

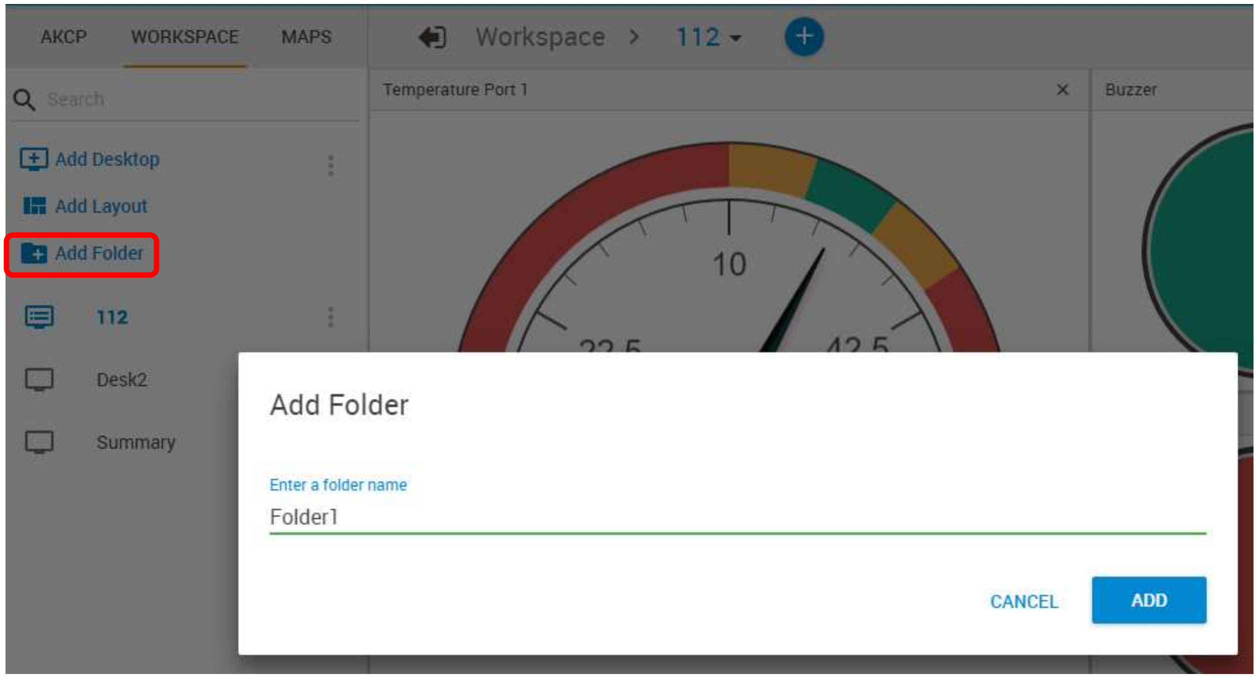


Click it again to go back to the full view.



On each Desktop and Folder item, you have the option to Rename, Move, Export or Delete them.
Move is useful if you’ve created multiple folders (see below).
As noted earlier, don’t forget to export your Workspace items to save them permanently.

Folders

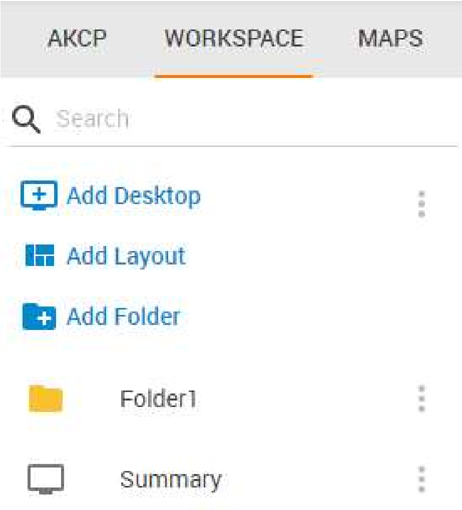


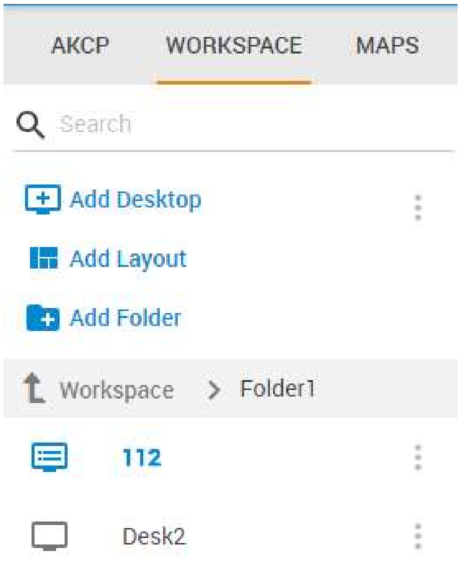
Add Folder

Enter a folder name

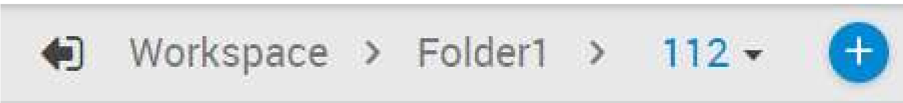
Folder1

You can add Folders to arrange your desktops into a hierarchical view.



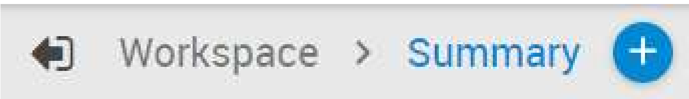


After created, you can simply drag and drop your Desktops under the folder, or use the Move menu. The folder structure will also display on the Desktop selector menu on top:

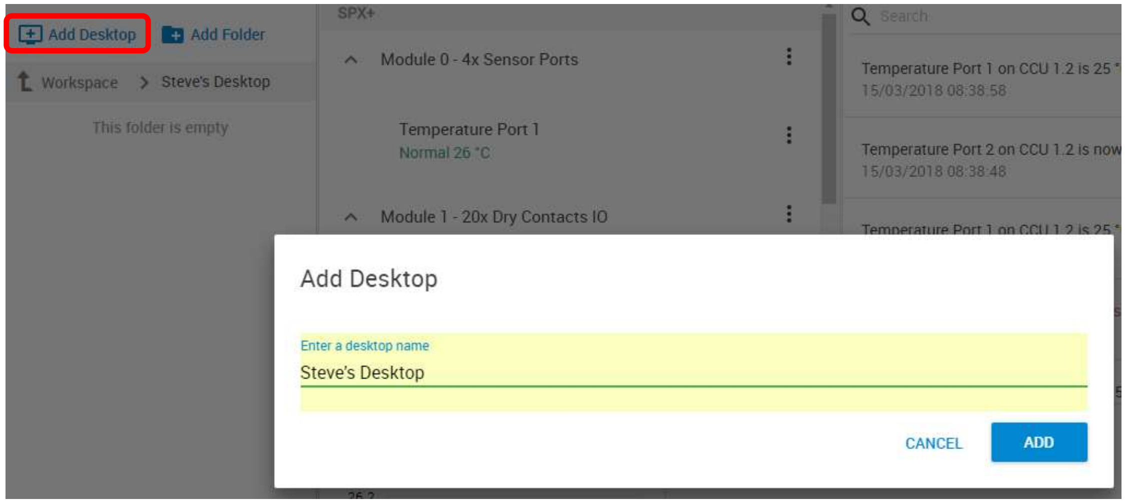


Desktops

You can add new Desktops where you can customize the layout to place any sensor gadget, logs, graphs etc. on the screen.



There are two ways to add a new desktop. The first is by creating a blank desktop using the **Add Desktop** link under the Workspace tab:



This folder is empty

Module 0 - 4x Sensor Ports

Temperature Port 1
Normal 26 °C

Module 1 - 20x Dry Contacts IO

Temperature Port 1 on CCU 1.2 is 25 °
15/03/2018 08:38:58

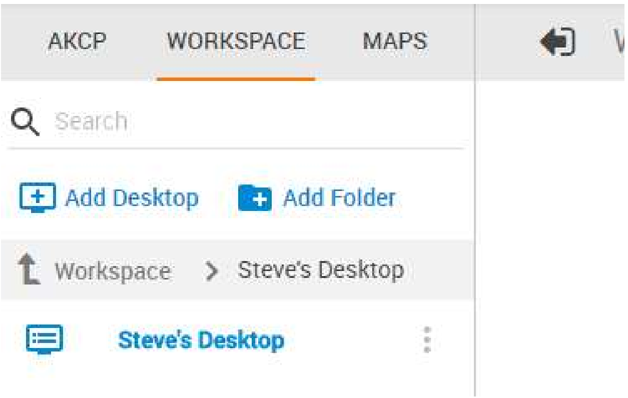
Temperature Port 2 on CCU 1.2 is now
15/03/2018 08:38:48

Temperature Port 1 on CCU 1.2 is 25 °

Add Desktop

Enter a desktop name: Steve's Desktop

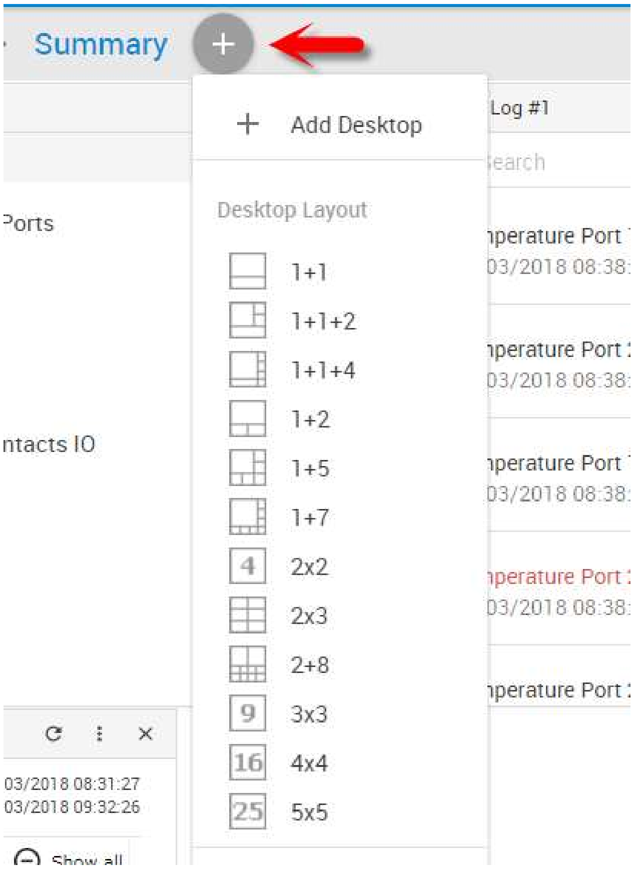
Name the new desktop and click the **Add** button.



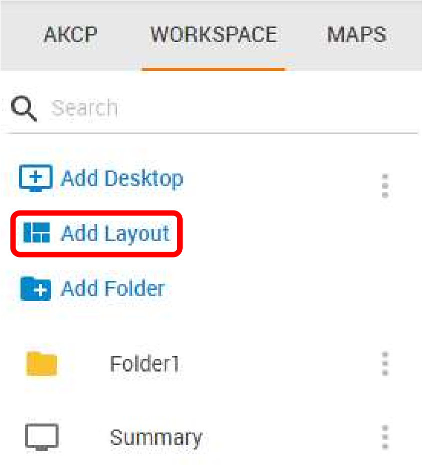
It will appear in the Workspace menu list.

In addition to the simple blank desktop, the second way to add a new desktop is via pre-defined Desktop Layouts. You could choose one that best suits your monitoring needs to drag and drop your sensor gadgets.

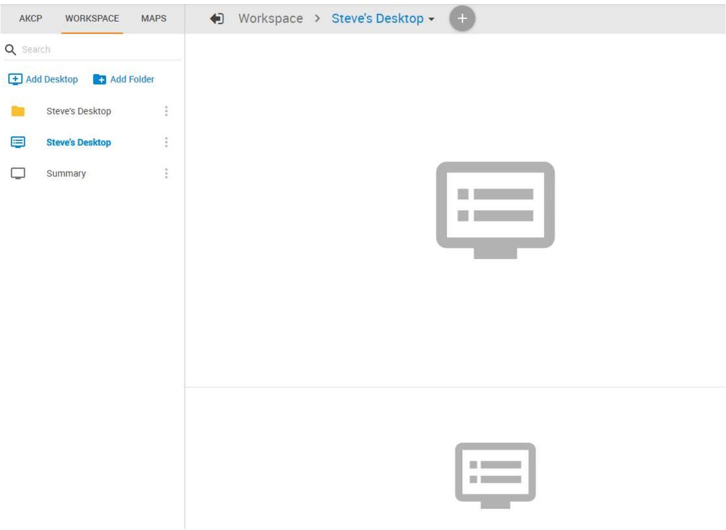
Use the plus button at the top of the page and select the layout for your new desktop:



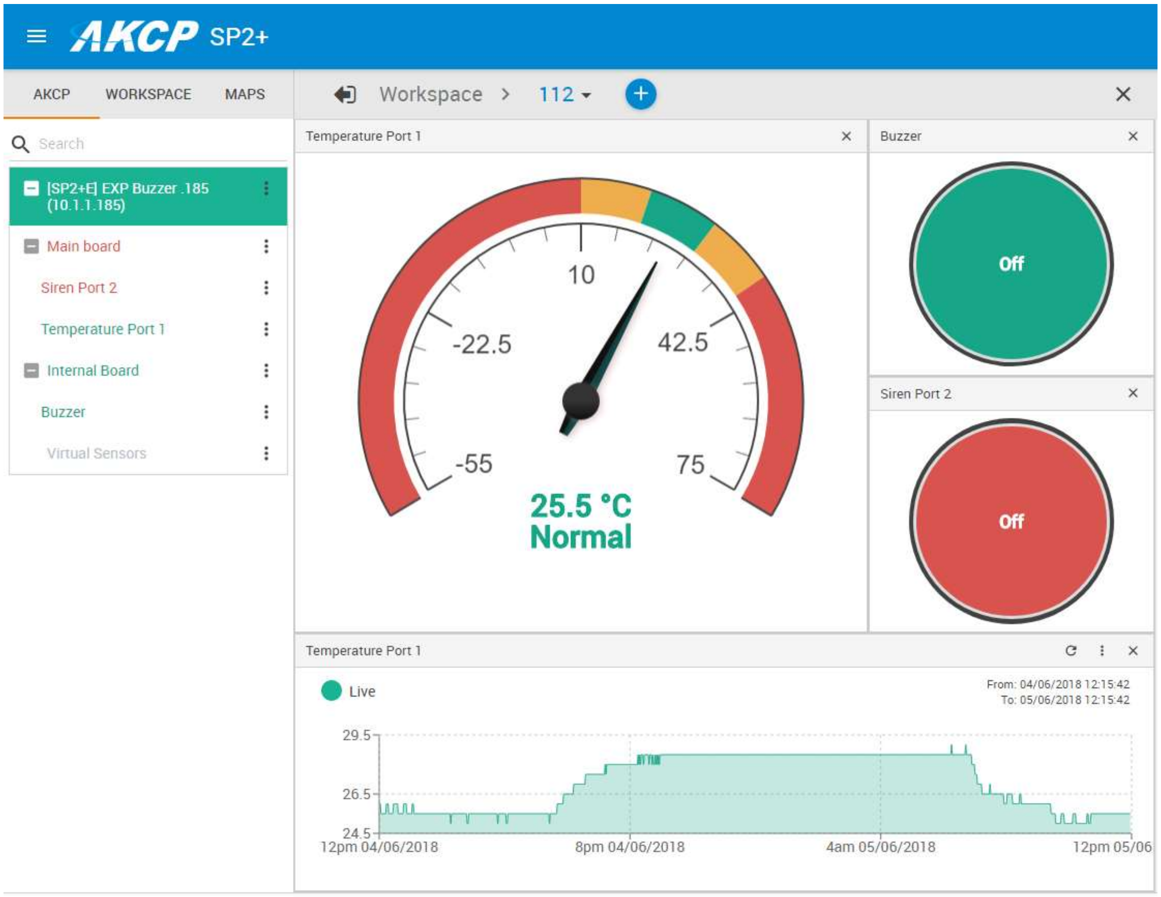
Alternatively you can click on the Add Layout link to select from layouts:



The empty desktop will have placeholders similar to this:

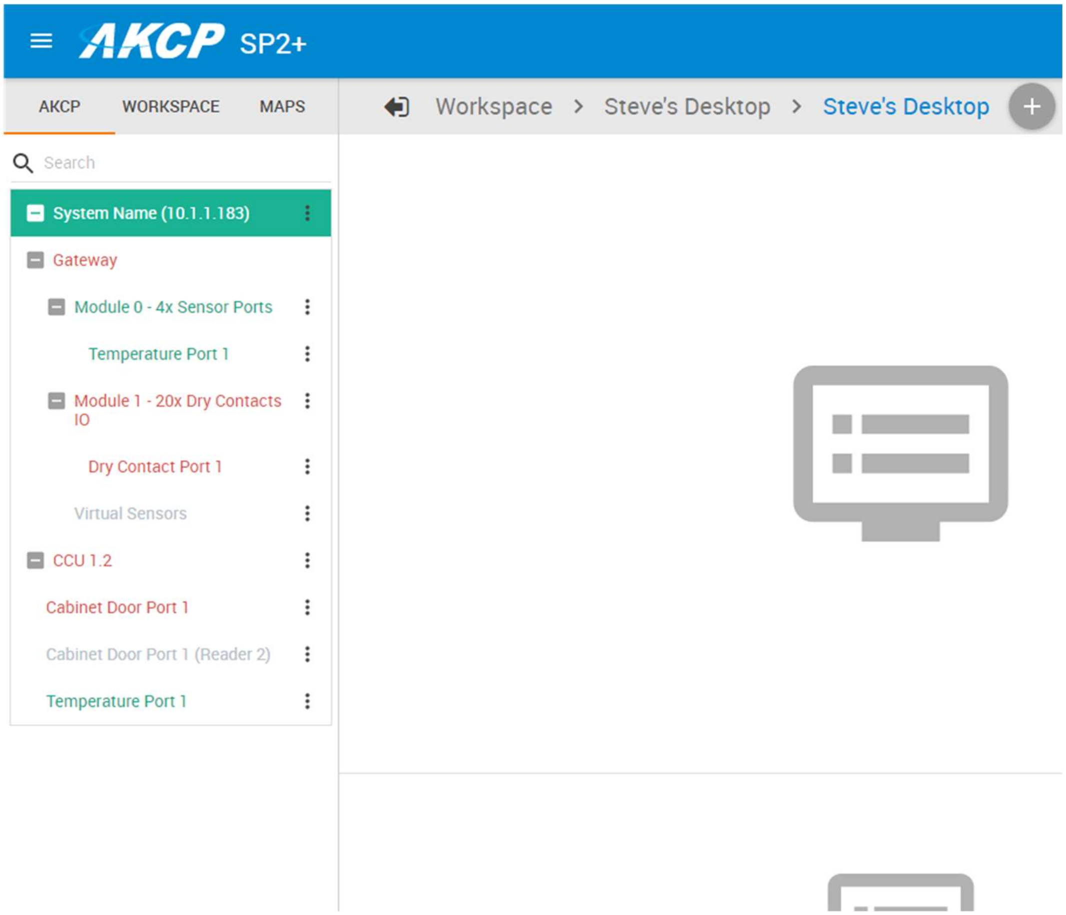


As an example below, we've selected the 1+1+2 layout.
Then you can drag and drop sensors, logs and graphs on the layout:



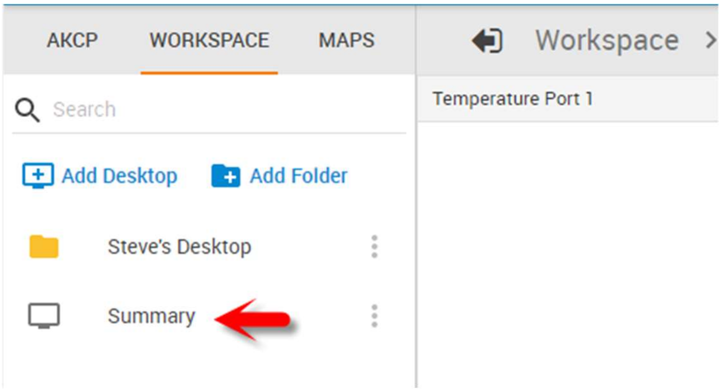
Below we'll show you how you can add sensors to the desktops.

Adding items to your custom desktop

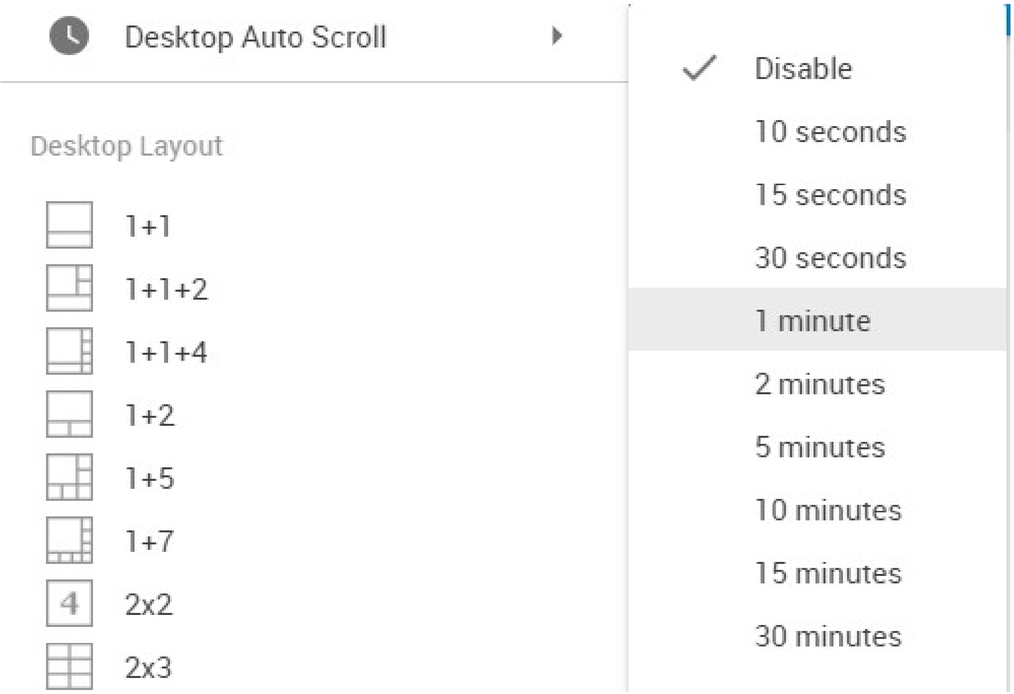


To add items from the units that are connected to the SP+ unit, you will first need to click on the AKCP link in the Navigation Tree as shown above.

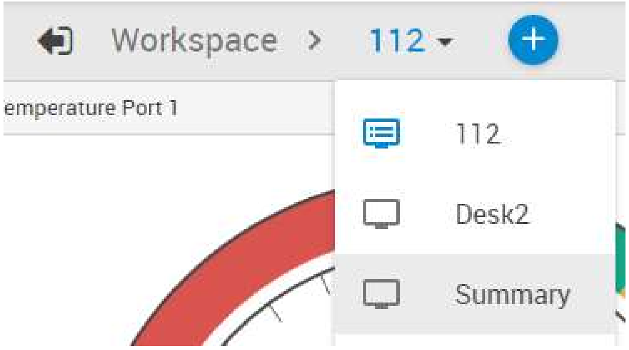
Next simply drag and drop the items you wish to add to your new desktop. This is also how you can add items to the Summary page. To navigate back to the Summary or Main Monitoring page click on the Summary link shown below.



Desktop Auto Scroll feature

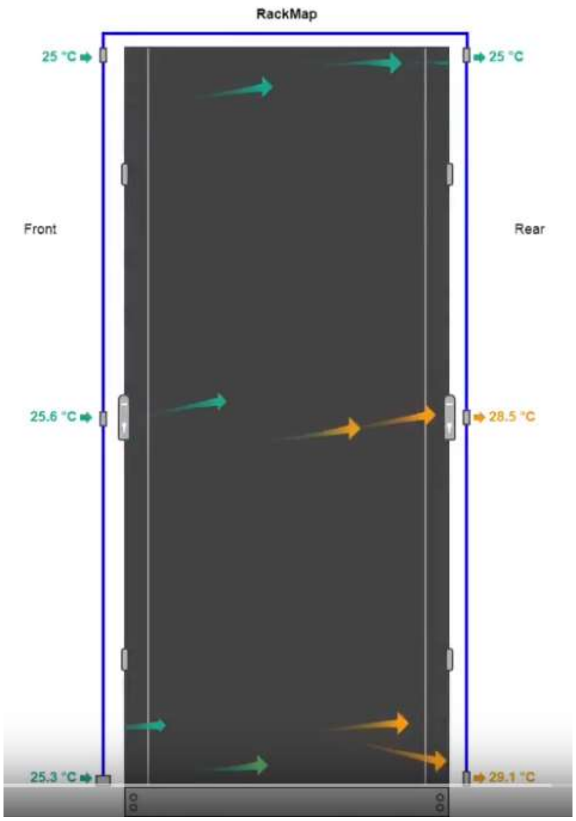


With this feature enabled, your desktop view will automatically switch between the created additional desktops within the specified time interval.



You can also manually change between Desktops using the menu.

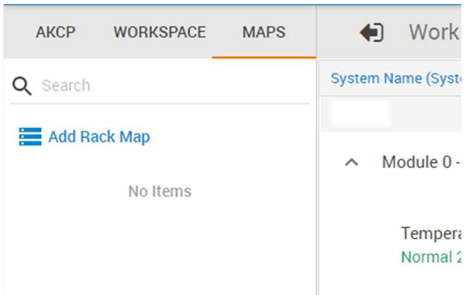
Managing Rack Maps

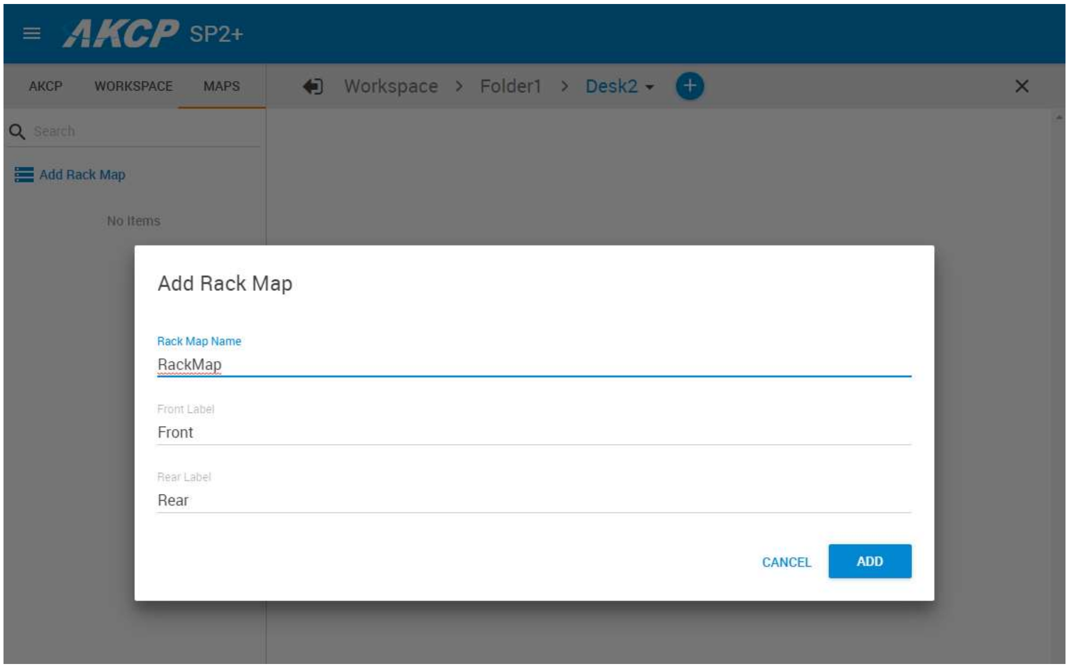


The Rack Map feature was originally (and still is) included in the AKCess Pro Server / AKCPro Server (HTML5) and has also been added to the SP+ units. You can add a Rack Map as a graphical representation of your server rack, and to display and record the temperature of the airflow within your server cabinets.

Note that on SP+ family Web UI only limited options are available for the Rack Map; for example you cannot add devices or assets.

Click on the Maps tab and Add Rack Map link to add a Rack Map:





Add Rack Map

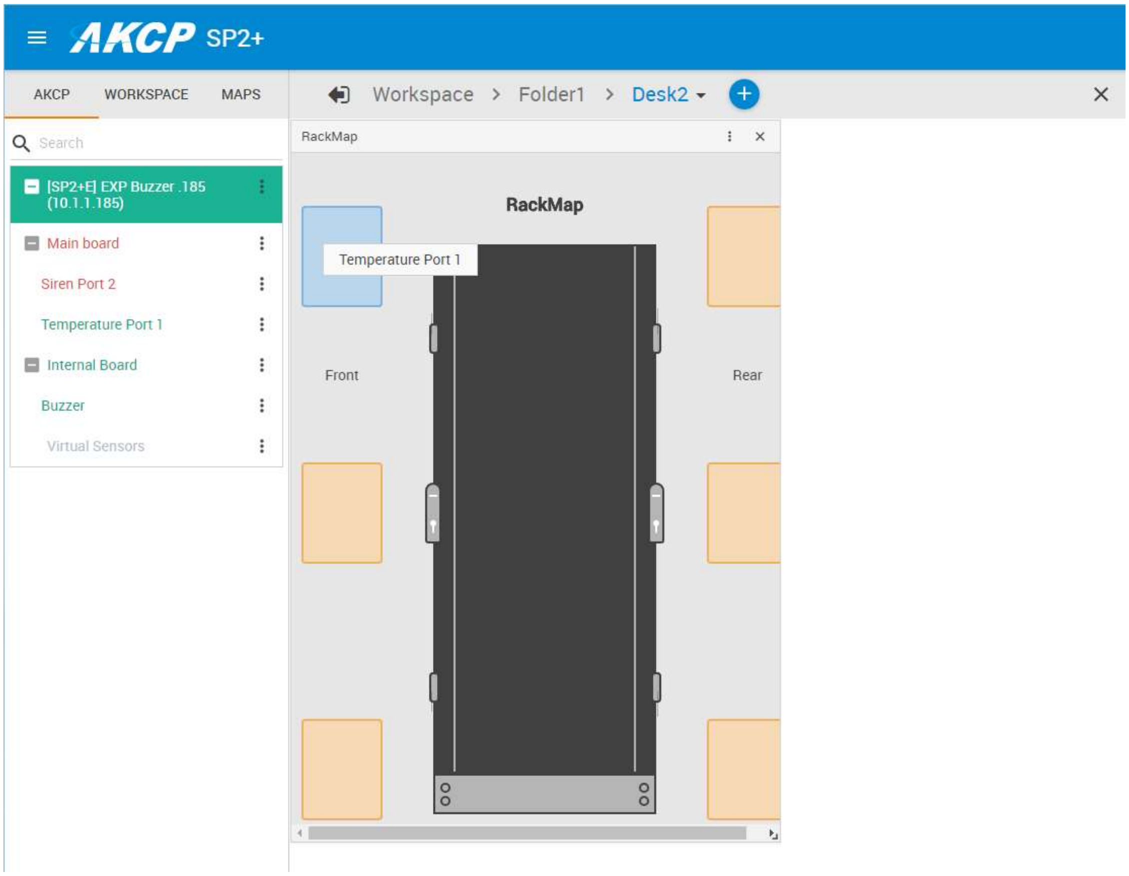
Rack Map Name
RackMap

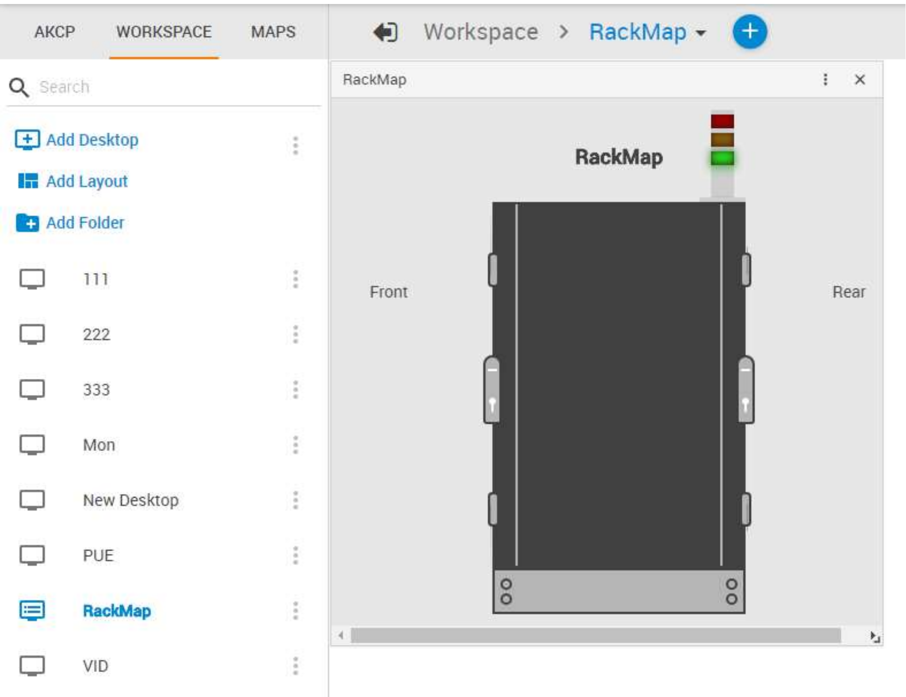
Front Label
Front

Rear Label
Rear

After created, you can drag and drop the Rack Map to a desktop.

You can add Temperature sensors, the Swing Handle Lock and the Sensor Status Light gadget on a Rack Map. Simply drag and drop the desired sensor from your unit's sensor list, as shown below.

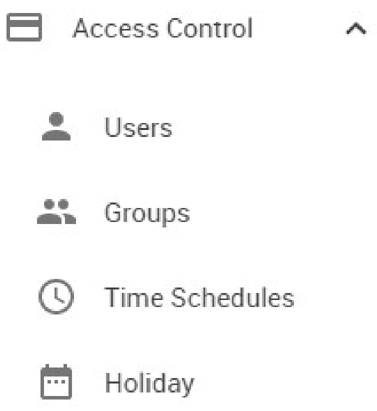




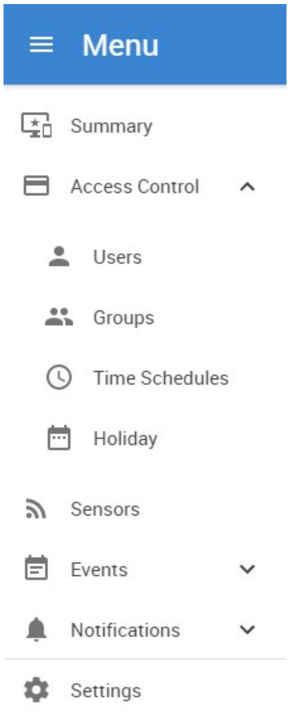
This example picture shows a Sensor Status Light added to a Rack Map.

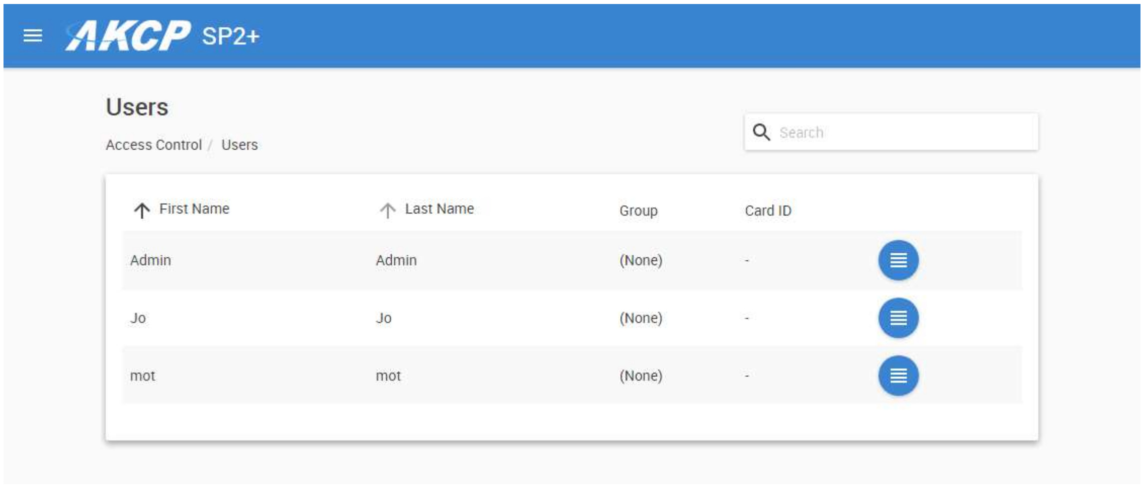
Please see the Thermal Map sensor manual for complete installation & setup instructions for the Thermal Map sensors.

Access Control Users and Groups



The Access Control Users and Groups are managed from the AKCPro Server and are used for accessing doors with the Swing Handle Lock. You can only view the existing users and groups from the unit's Web UI and modify only a few parameters on them.





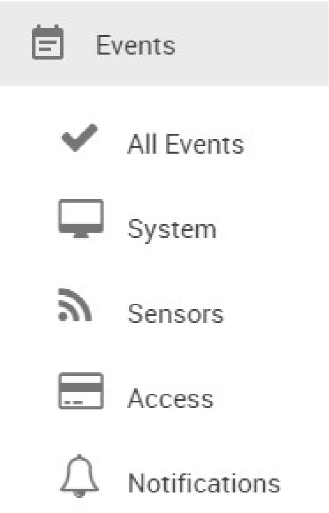
Users

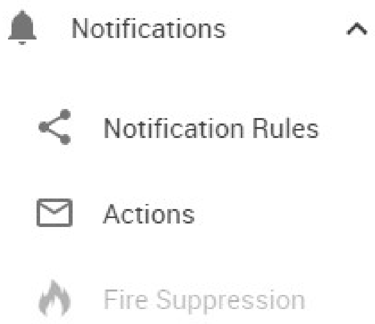
Access Control / Users

First Name	Last Name	Group	Card ID
Admin	Admin	(None)	-
Jo	Jo	(None)	-
mot	mot	(None)	-

This feature has its own manual, refer to the SP+ Swing Handle Lock Manual for more information.

Notifications and Events





You can view all of the SP+ unit’s events and filter them by each of the categories’ listed above in the Events drop down menu.

Please refer to the SP+ units “Notifications Manual” for setting up the alerts and the Event log on the units.

The Sensors menu

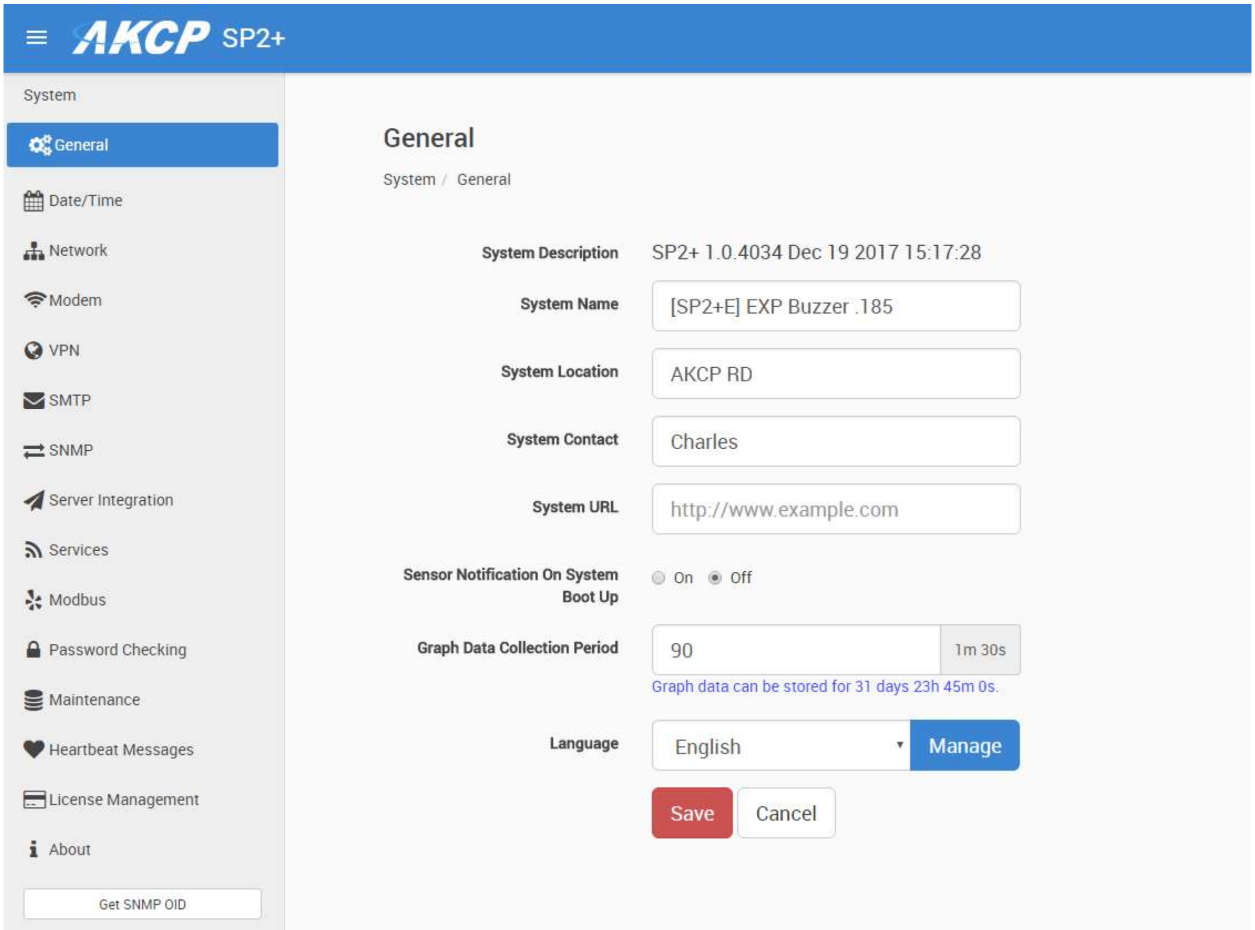
The “Sensors” shortcut will allow you navigate directly to the sensors setting page where you can setup the sensors connected to the unit. This is covered in the Sensors section in this manual.

The Settings menu

This shortcut will take you to the unit’s system settings pages. Each page will be described below in detail.

System page

General



General

System / General

System Description: SP2+ 1.0.4034 Dec 19 2017 15:17:28

System Name: [SP2+E] EXP Buzzer .185

System Location: AKCP RD

System Contact: Charles

System URL: http://www.example.com

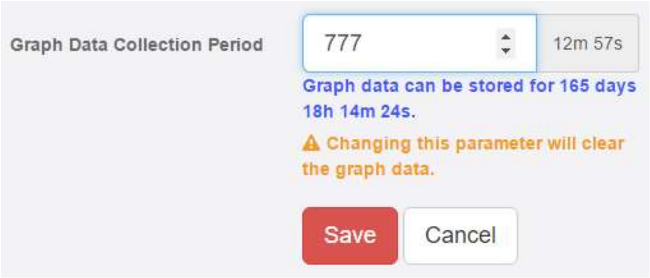
Sensor Notification On System Boot Up: ○ On ● Off

Graph Data Collection Period: 90 | 1m 30s

Graph data can be stored for 31 days 23h 45m 0s.

Language: English

Here you can change general settings for the device.
The unit’s firmware version is shown in the Description field, and the System Name/Location/Contact options are user configurable. You could also specify the System URL option, for quick access of a custom part of the Web UI for example, but you can specify any URL.
With newer firmware you can also specify GPS coordinates.


Graph Data Collection Period: 777 | 12m 57s

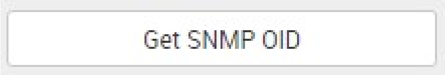
Graph data can be stored for 165 days 18h 14m 24s.

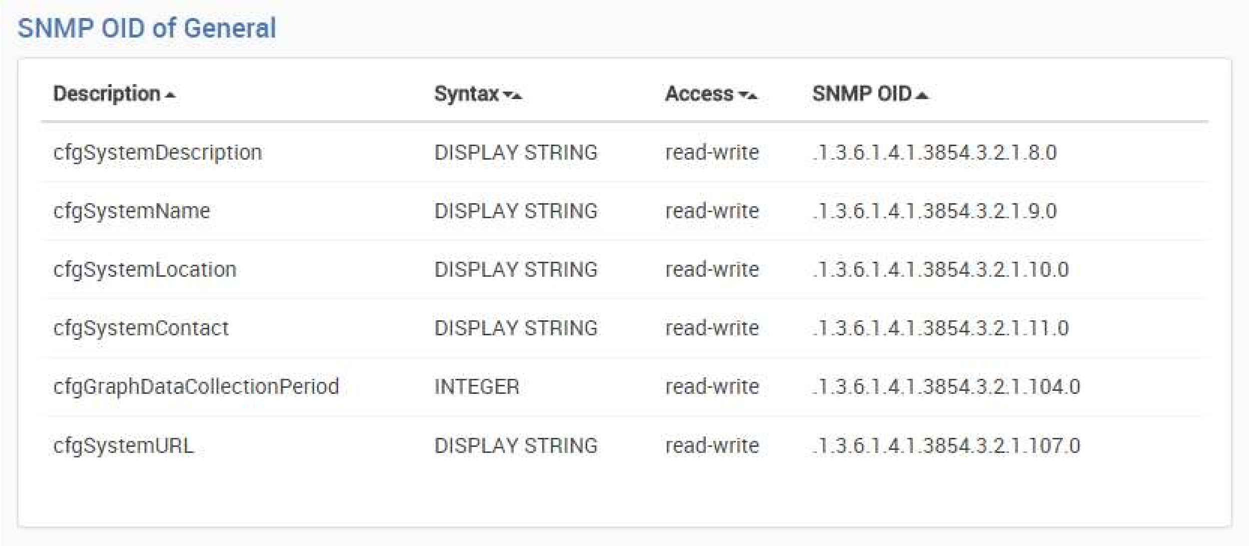
⚠ Changing this parameter will clear the graph data.

By changing the **Graph Data Collection Period**, you can choose how frequently the data is sampled. Note that if you had stored graph data previously, changing this setting will clear the data.

With the option **Sensor Notification On System Boot Up**, you can choose to allow/disallow running the notifications with sensor values read at system boot up. In some cases, invalid values are read while the unit is starting up, and you could get false alarm notifications. You can enable/disable the notification processing at startup with this option.

On each System subpage you can see a **Get SNMP OID** button (where applicable):





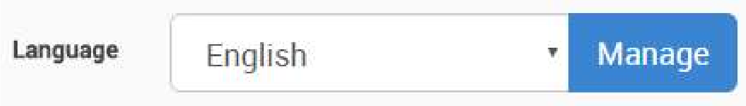
SNMP OID of General

Description ▴	Syntax ▾▴	Access ▾▴	SNMP OID ▴
cfgSystemDescription	DISPLAY STRING	read-write	.1.3.6.1.4.1.3854.3.2.1.8.0
cfgSystemName	DISPLAY STRING	read-write	.1.3.6.1.4.1.3854.3.2.1.9.0
cfgSystemLocation	DISPLAY STRING	read-write	.1.3.6.1.4.1.3854.3.2.1.10.0
cfgSystemContact	DISPLAY STRING	read-write	.1.3.6.1.4.1.3854.3.2.1.11.0
cfgGraphDataCollectionPeriod	INTEGER	read-write	.1.3.6.1.4.1.3854.3.2.1.104.0
cfgSystemURL	DISPLAY STRING	read-write	.1.3.6.1.4.1.3854.3.2.1.107.0

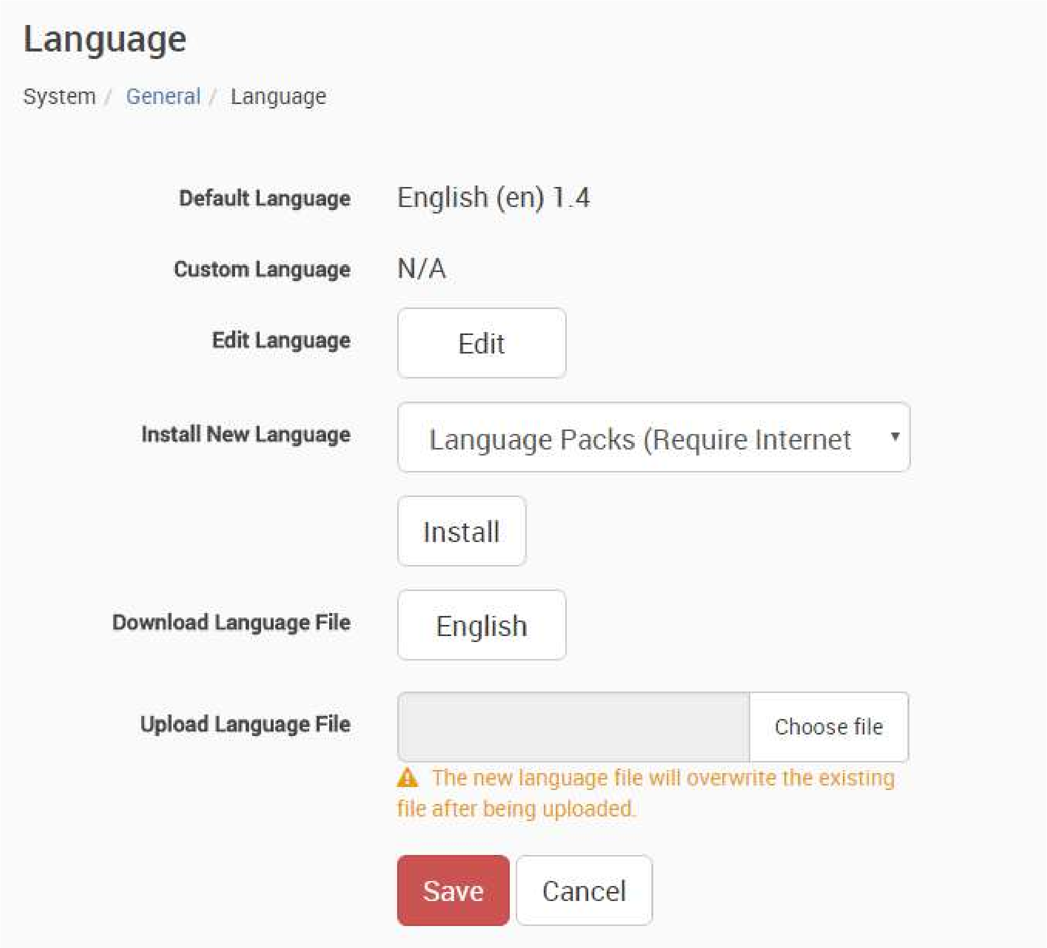
This will give you a popup window with all relevant OIDs for the actual page (here the General page is shown).
You can use OIDs for SNMP calls and in custom scripts, or for setting up the unit for monitoring by a third party NMS software such as WhatsUpGold or Paessler.

This button is also accessible on the *Sensors page* for each sensor.

Language management



You can change the display language of the Web UI with this option. Only one additional language is supported, together with the default (and fallback if there's an error) English.



Language

System / General / Language

Default Language: English (en) 1.4

Custom Language: N/A

Edit Language: Edit

Install New Language: Language Packs (Require Internet

Install

Download Language File: English

Upload Language File: Choose file

⚠ The new language file will overwrite the existing file after being uploaded.

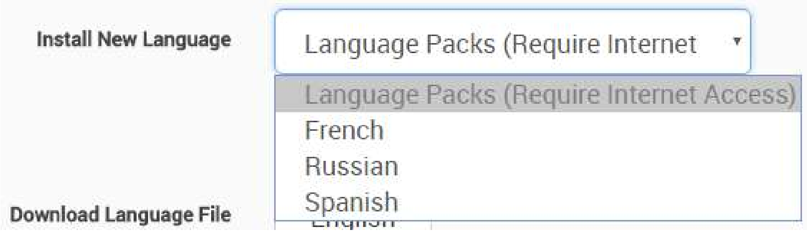
Save Cancel

In **Manage**, you can choose to **Download Language File** if you'd like to edit the language file offline (you can also download the custom language's file if it's already present). Then upload the completed file, and it will be selectable as the Custom Language. For official translation files, the language code and version will show the correct values.

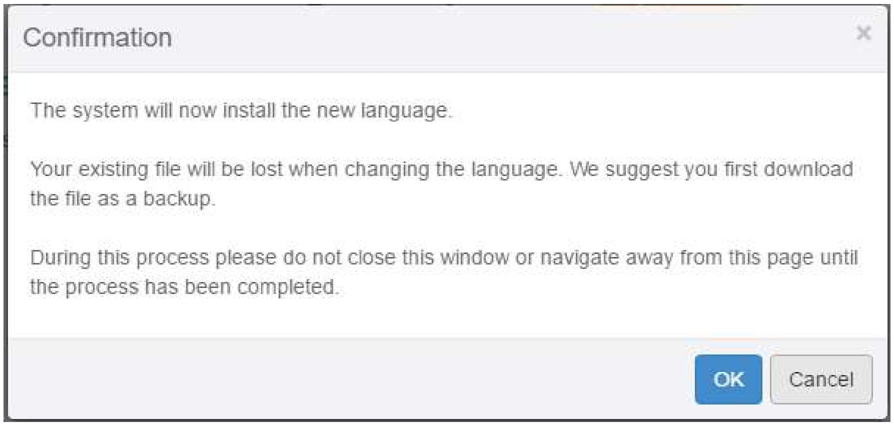
Note: Whenever you upload or install a custom language file, it will overwrite the old file. Only one additional language is supported.

You can get separately downloadable language files from our website in the Support section.

If you have active internet connection, the unit supports installing the official language files directly from our server.
Select a language from the drop-down menu **Install New Language**:


Install New Language
Language Packs (Require Internet
Language Packs (Require Internet Access)
French
Russian
Spanish
Download Language File
English

Then press the **Install** button. It will ask you to confirm the action in a popup window:

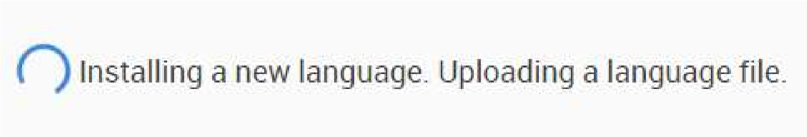

Confirmation

The system will now install the new language.

Your existing file will be lost when changing the language. We suggest you first download the file as a backup.

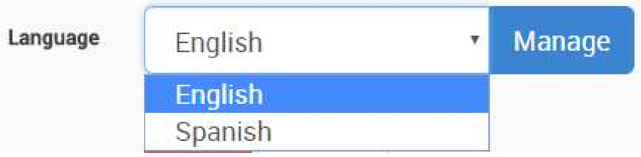
During this process please do not close this window or navigate away from this page until the process has been completed.

Wait until the language is downloaded and installed:

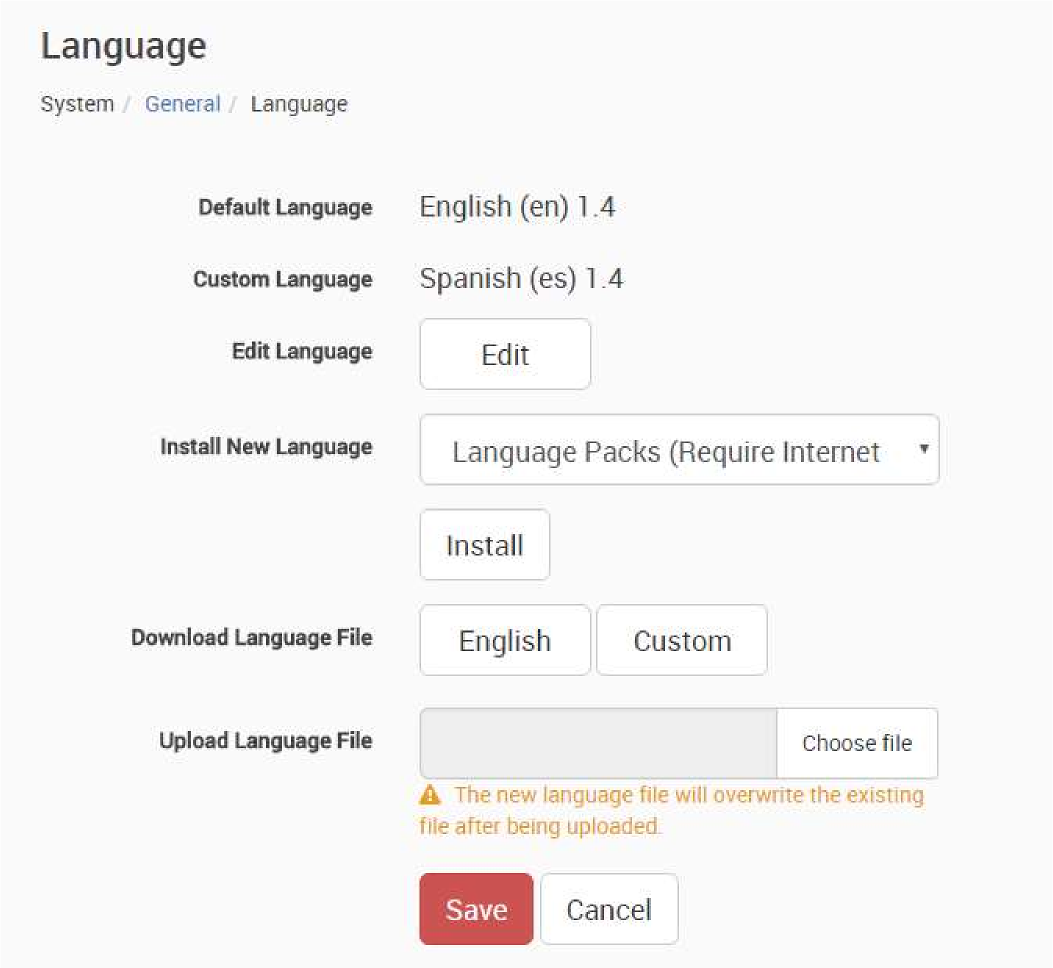

Installing a new language. Uploading a language file.

The unit will notify you about the successful language installation. If you installed it from the list, it won't change the language of the Web UI automatically.

Now you can switch display languages by selecting from the drop-down list on the **General** page, then pressing **Save**:



After you've added the custom language, you can manage it from the same menu:


Language

System / General / Language

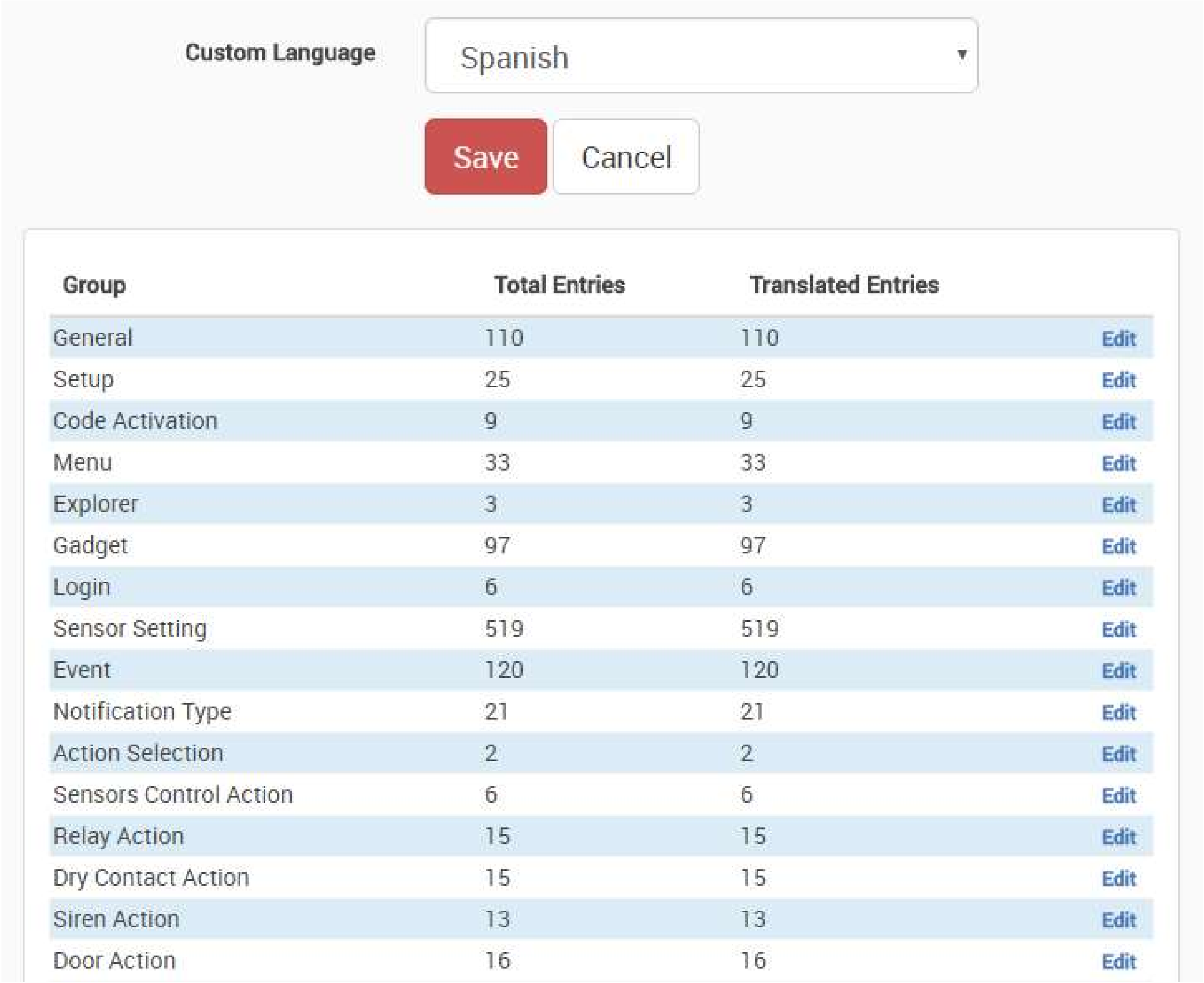
Default Language: English (en) 1.4

Custom Language: Spanish (es) 1.4

⚠ The new language file will overwrite the existing file after being uploaded.

Note: The official language files are also included in the firmware update packages.

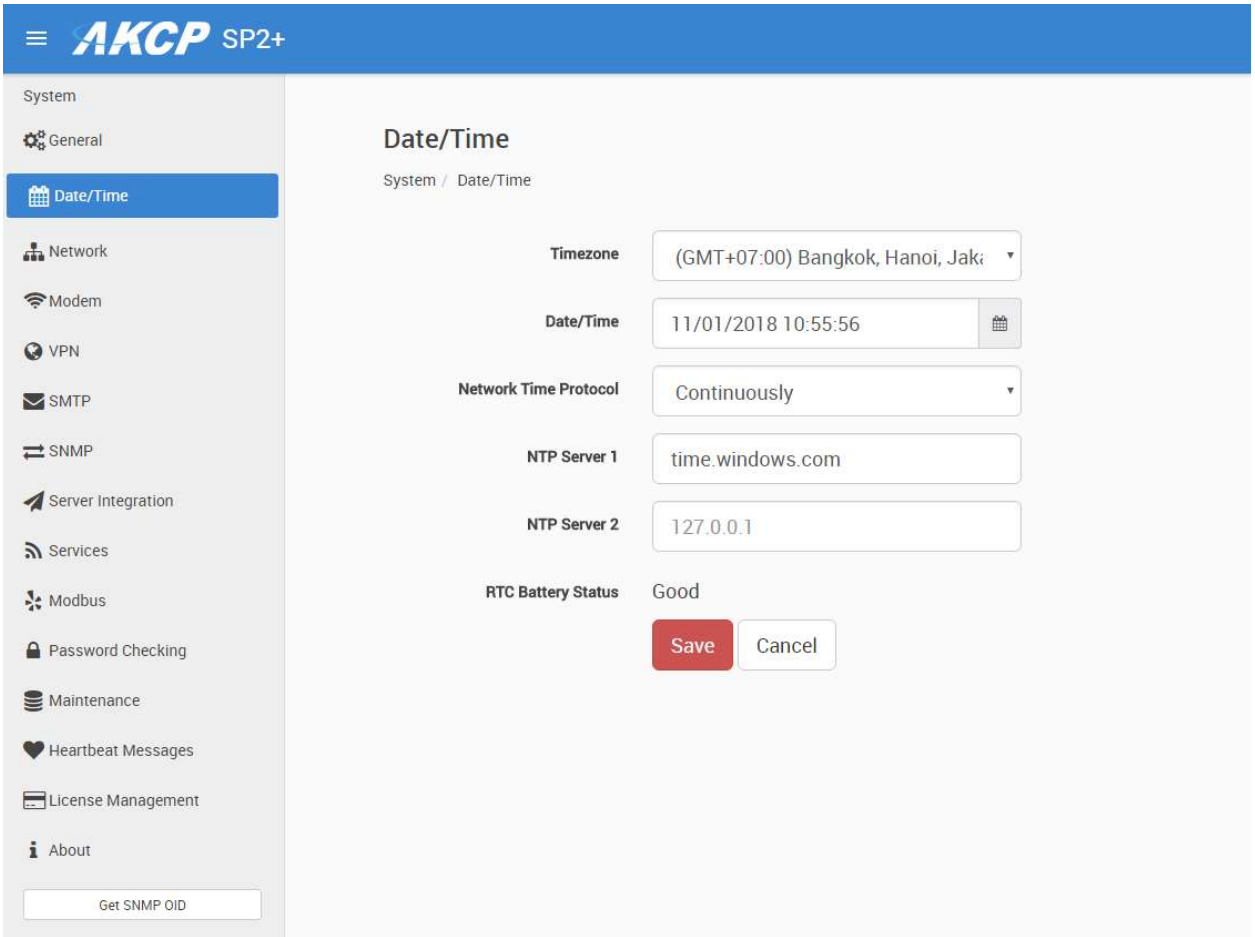
You can also edit the chosen language directly in the Web UI, if you choose **Edit Language**:



Custom Language: Spanish

Group	Total Entries	Translated Entries	
General	110	110	Edit
Setup	25	25	Edit
Code Activation	9	9	Edit
Menu	33	33	Edit
Explorer	3	3	Edit
Gadget	97	97	Edit
Login	6	6	Edit
Sensor Setting	519	519	Edit
Event	120	120	Edit
Notification Type	21	21	Edit
Action Selection	2	2	Edit
Sensors Control Action	6	6	Edit
Relay Action	15	15	Edit
Dry Contact Action	15	15	Edit
Siren Action	13	13	Edit
Door Action	16	16	Edit

Date/Time



Date/Time

System / Date/Time

Timezone: (GMT+07:00) Bangkok, Hanoi, Jak‹

Date/Time: 11/01/2018 10:55:56

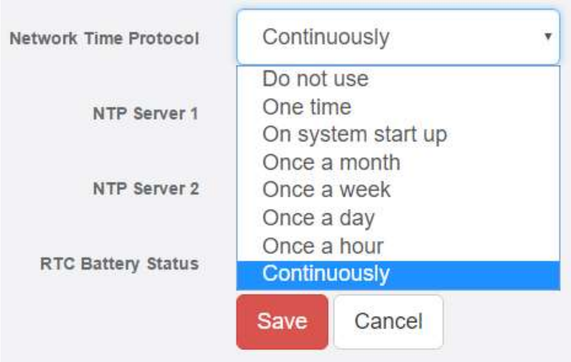
Network Time Protocol: Continuously

NTP Server 1: time.windows.com

NTP Server 2: 127.0.0.1

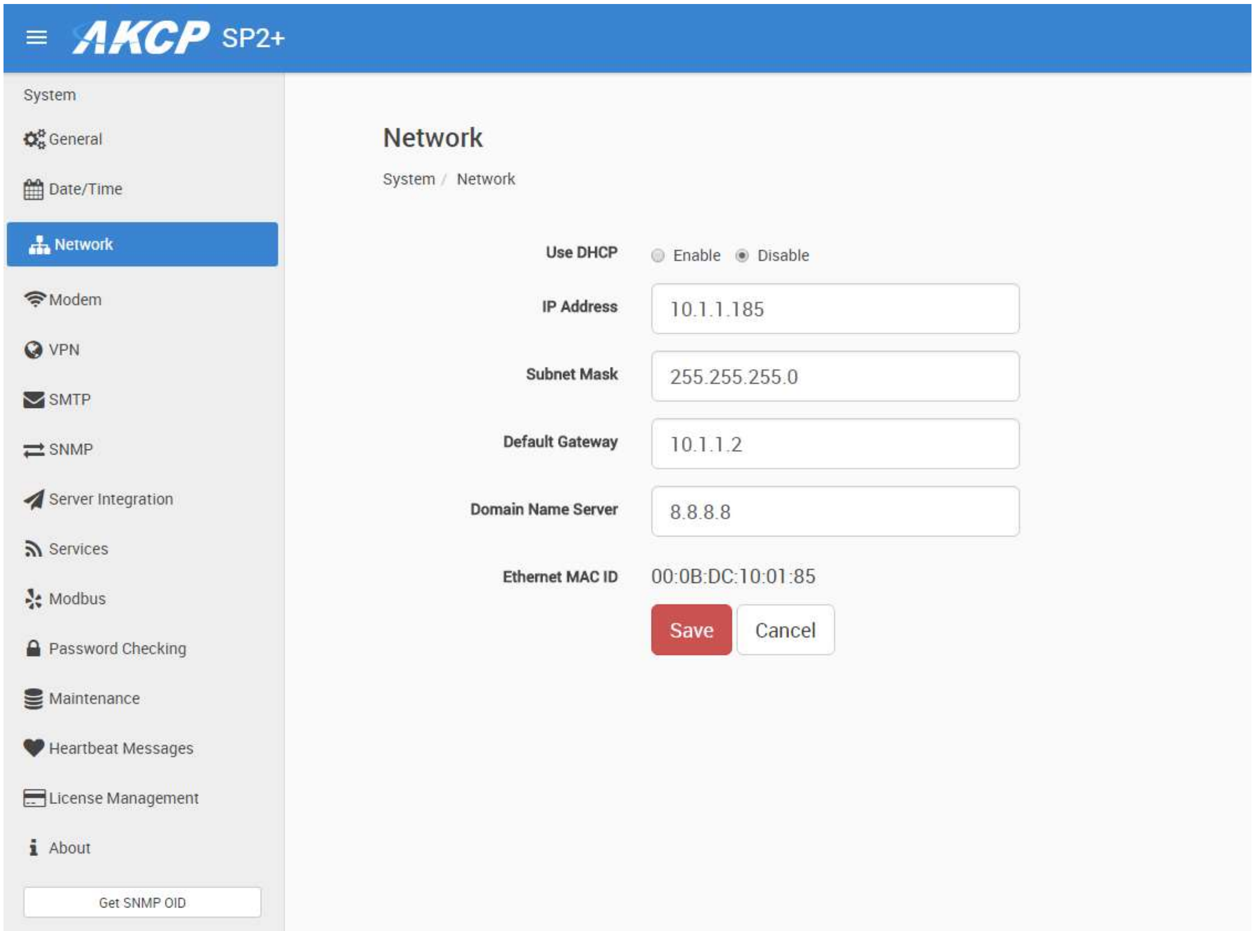
RTC Battery Status: Good

The system date and time with time zone is user configurable, with NTP server synchronization. If the unit is connected to APS (AKCPro Server), then it will sync with the APS NTP service. Also displayed is the status of the RTC battery (good/bad).
F7 units will also let you specify secondary NTP, and secured NTP servers.



You can also select the frequency of NTP synchronization with the drop-down menu.

Network



Network

System / Network

Use DHCP ○ Enable ● Disable

IP Address 10.1.1.185

Subnet Mask 255.255.255.0

Default Gateway 10.1.1.2

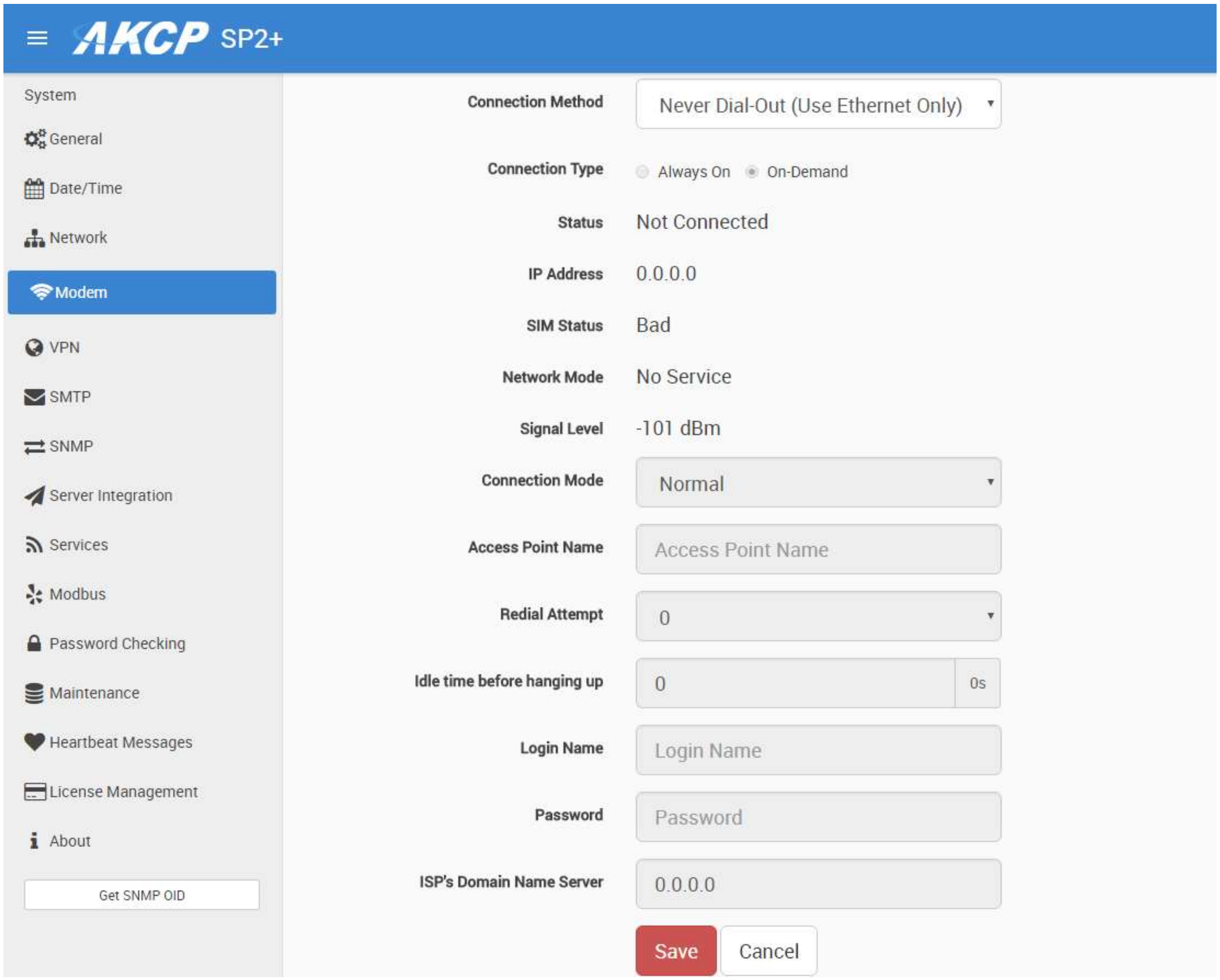
Domain Name Server 8.8.8.8

Ethernet MAC ID 00:0B:DC:10:01:85

The unit’s MAC ID is displayed here, and all user configurable options for IPv4 with fixed IP or DHCP client mode.

F7 units also have IPv6 settings (separately licensed feature), we have a separate manual about this feature.

Modem



Connection Method: Never Dial-Out (Use Ethernet Only)

Connection Type: ○ Always On ● On-Demand

Status: Not Connected

IP Address: 0.0.0.0

SIM Status: Bad

Network Mode: No Service

Signal Level: -101 dBm

Connection Mode: Normal

Access Point Name: Access Point Name

Redial Attempt: 0

Idle time before hanging up: 0 0s

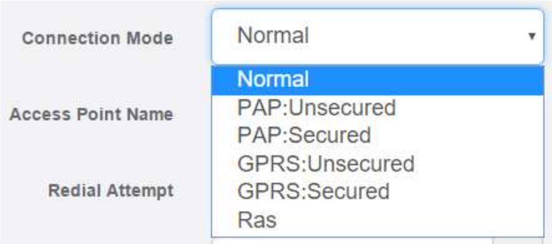
Login Name: Login Name

Password: Password

ISP's Domain Name Server: 0.0.0.0

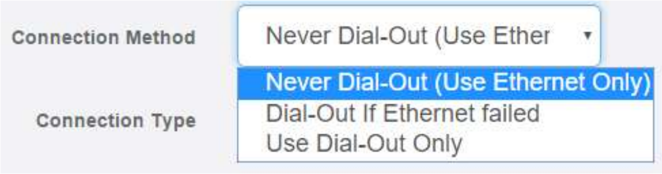
If the unit is equipped with the internal modem module, then the modem's **Dial-Out configuration** can be set up here for data connections. Contact your service provider for the correct settings.

You can also see on this page the state of the connection, the **Network Mode** and the assigned IP address when connected, if the SIM card is detected properly by the modem (**SIM Status**), and the **Signal Level**.



Connection Mode: Normal

You may select a different *Connection Mode* (PAP/GPRS/RAS).
The most commonly used is *GPRS Unsecured*.

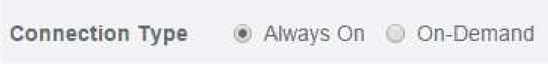


Connection Method: Never Dial-Out (Use Ether

Connection Type
Never Dial-Out (Use Ethernet Only)
Dial-Out If Ethernet failed
Use Dial-Out Only

You may change the *Connection Method* as follows:

- *Never Dial Out (Use Ethernet only):* the unit will never try to use the modem for sending out notifications. If you don't have Ethernet connection, you should change this setting; otherwise you won't get any notifications.
- *Dial-Out if Ethernet failed:* the unit will only use the modem for sending out notifications, if the Ethernet connection fails.
- *Use Dial-Out Only:* the unit will only use the modem to send out the notifications, regardless of the state of the Ethernet connection.



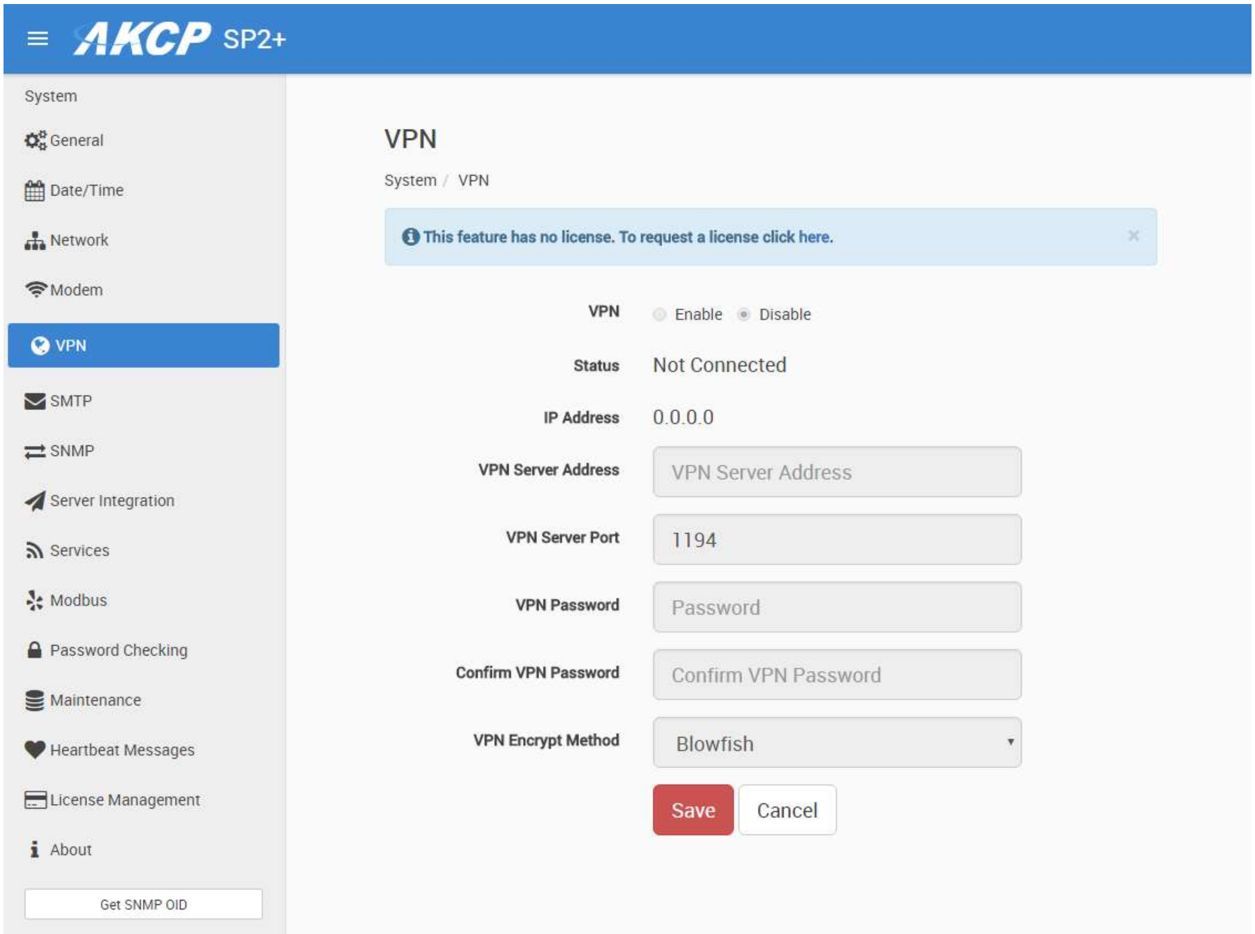
Connection Type ● Always On ○ On-Demand

Also you may change the *Connection Type*:

- *On-Demand:* the unit will initiate a connection only when it's necessary for sending out the notifications.
- *Always On:* the unit will keep the connection up, even when there is nothing to send.

Note 1: There's no auto-detection feature for the internal modem module, the configuration is always shown even if your unit is not equipped with the module.
Note 2: Only insert and remove the SIM card when the unit is turned off. Otherwise you can damage the SIM and the modem.
Note 3: The PIN code for the SIM card needs to be removed; otherwise the modem can't use it.

VPN



VPN

System / VPN

This feature has no license. To request a license click here.

VPN ○ Enable ● Disable

Status Not Connected

IP Address 0.0.0.0

VPN Server Address: VPN Server Address

VPN Server Port: 1194

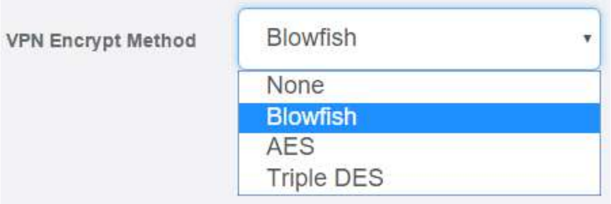
VPN Password: Password

Confirm VPN Password: Confirm VPN Password

VPN Encrypt Method: Blowfish

This feature requires a separate license. You can read more details about the licensing later in this manual.

This feature is used by connecting the SP2+ with the APS VPN server. After the license has been activated and the APS VPN server is set up, you'll need to fill out the same options here to be able to use the VPN connection (see below).

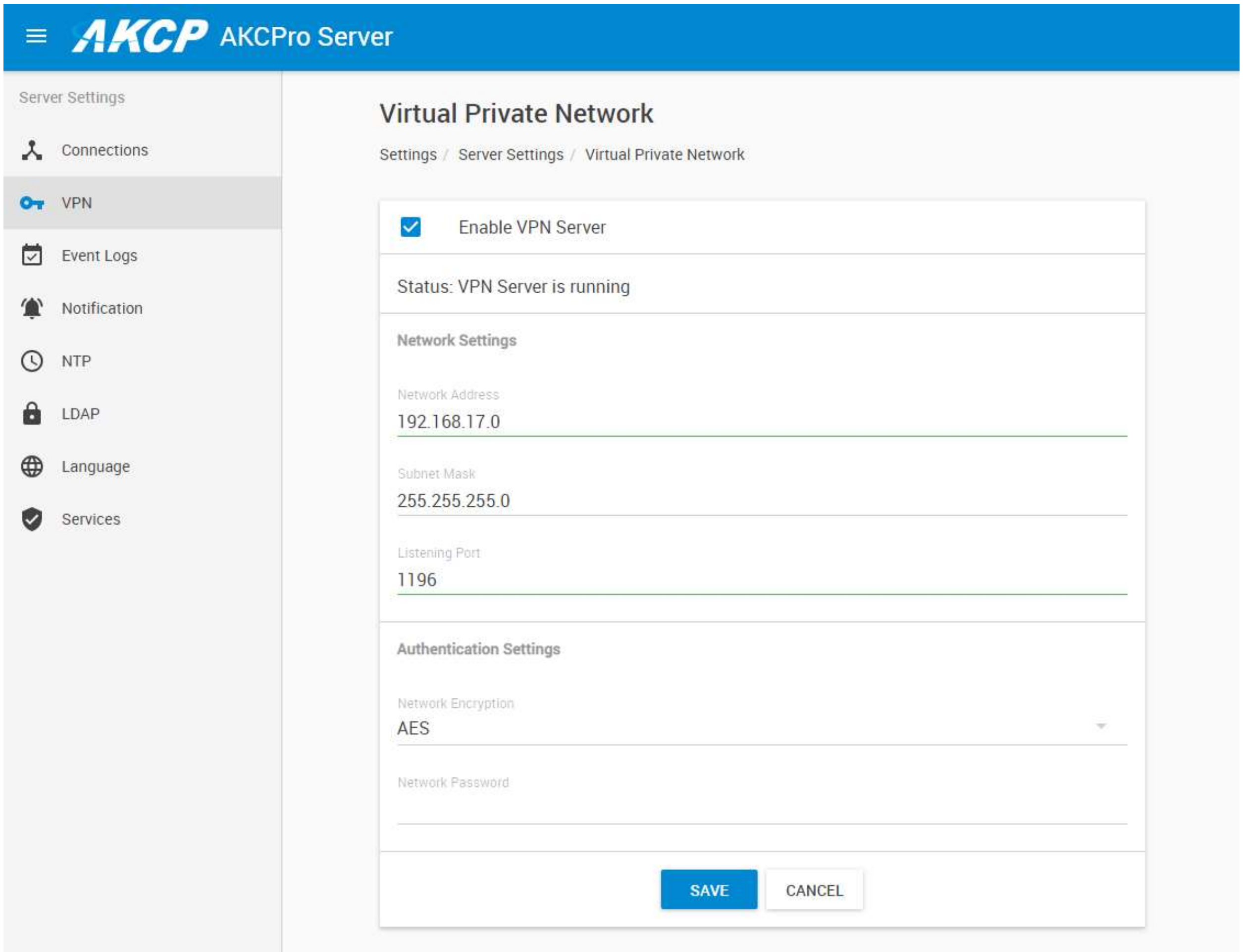

VPN Encrypt Method: Blowfish

Note 1: You can also configure these settings from the APS console for the unit.
Note 2: If you use the VPN option, the maximum number of sensors that can be used by the unit will be reduced to 36 on F4 units (no limit on F7).

Set up VPN connection to APS

In the following pages, we'll describe how to set up the VPN connection to APS.

1. On APS HTML, Go to **Settings>Server Settings>Virtual Private Network**



Virtual Private Network

Settings / Server Settings / Virtual Private Network

☑ Enable VPN Server

Status: VPN Server is running

Network Settings

Network Address: 192.168.17.0

Subnet Mask: 255.255.255.0

Listening Port: 1196

Authentication Settings

Network Encryption: AES

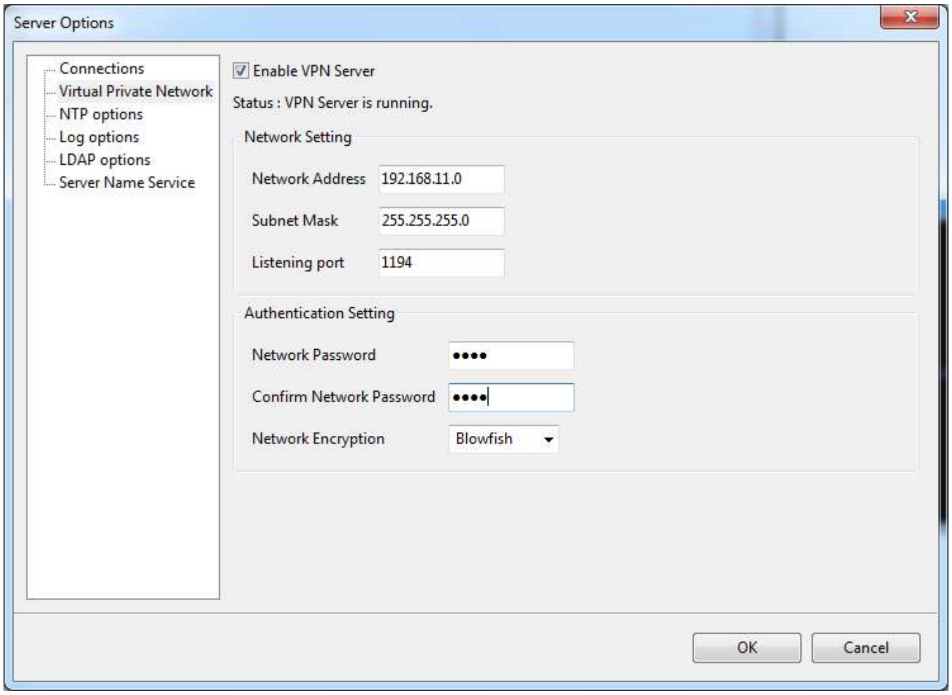
Network Password:

Enable the VPN Server by clicking on the checkbox, and then change the **Network Password** in Authentication Setting. Remember the **Network Encrytion Mode** that you have chosen; you'll need to provide the same setting on the SP+. See more details in the APS HTML manual.

You can also make changes to the network settings, but you'll have to use the same port on both sides of the VPN.

Note: The VPN virtual network has to be an entirely different subnet from the one you're currently using, otherwise it won't work!
Ex. if you're using 192.168.1.x network subnet on your LAN, use 192.168.11.x (or any other that's different from 192.168.1.x) for the VPN link.

You could also configure the VPN settings using the deprecated APS Windows Client interface: **Settings>Server Option>Virtual Private Network**



Server Options

☑ Enable VPN Server

Status : VPN Server is running.

Network Setting

Network Address 192.168.11.0

Subnet Mask 255.255.255.0

Listening port 1194

Authentication Setting

Network Password ••••

Confirm Network Password ••••

Network Encryption Blowfish

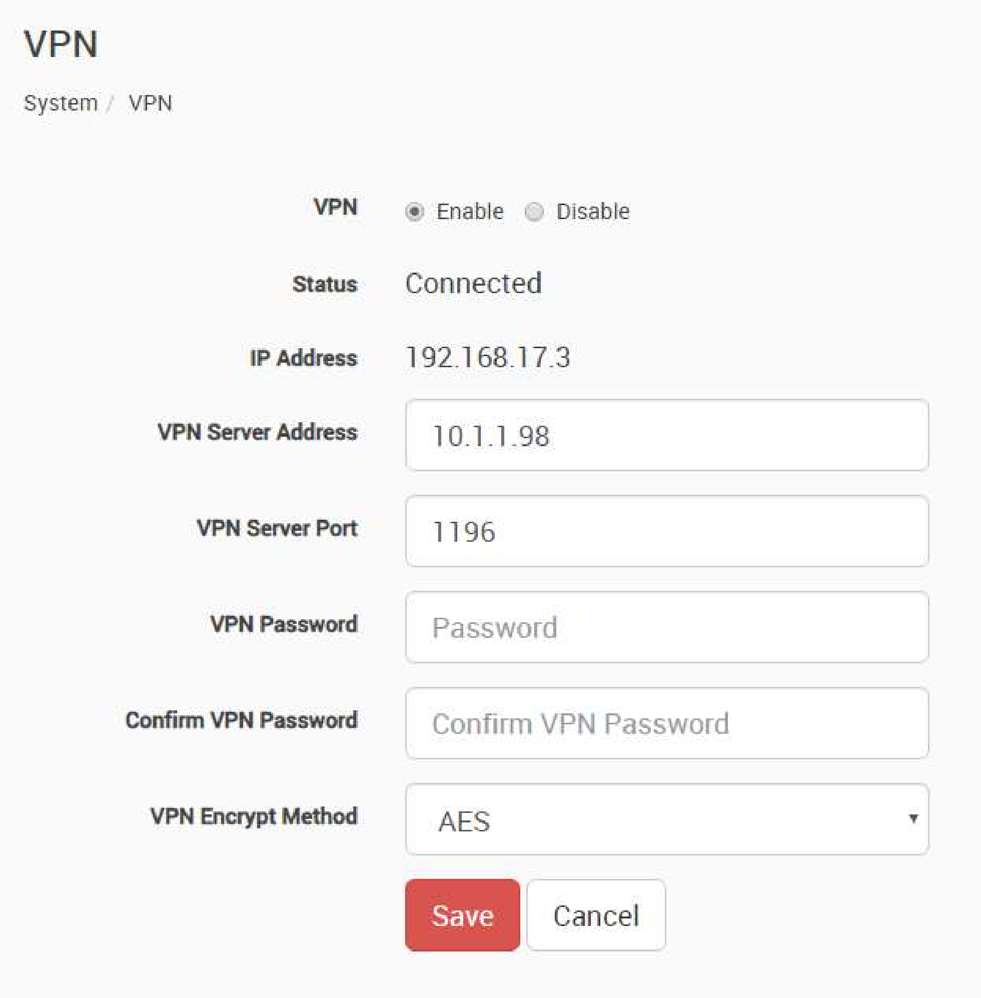
2. On the SP+ Web UI, enable the VPN

First change the VPN Client on the top to "Enabled" and configure the VPN Settings on the form:

- Specify the AKCPro Server's IP or DNS name in VPN Server Address
- Use the VPN Network Password that you have specified on APS
- Set up the the VPN Encrypt Method on the Encryption tab; use the same setting that you have specified on APS.

After clicking the "Save" button, the unit will ask you to reboot.

After the unit has rebooted and shows "Connected", it will show the VPN client’s IP Address.



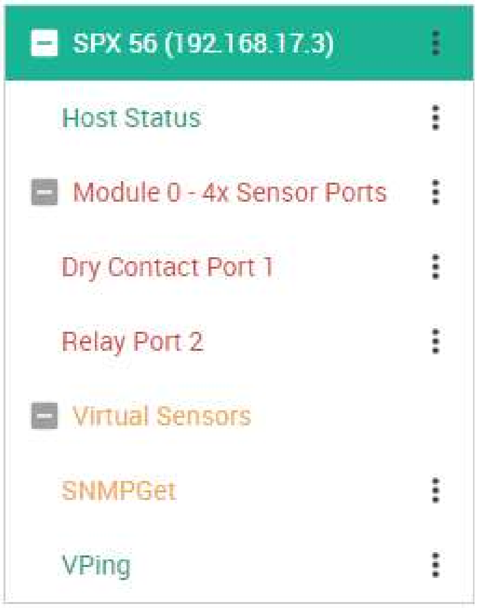
VPN

System / VPN

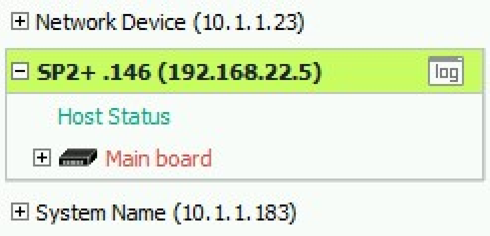
VPN	● Enable ○ Disable
Status	Connected
IP Address	192.168.17.3
VPN Server Address	10.1.1.98
VPN Server Port	1196
VPN Password	Password
Confirm VPN Password	Confirm VPN Password
VPN Encrypt Method	AES

You can review the unit’s syslog to see if there were any errors with connecting to the VPN server.

3. On your APS console, the SP+ unit will be added to the **Server Explorer** automatically, with an IP address automatically assigned from the range you specified.



SPX 56 (192.168.17.3)
Host Status
Module 0 - 4x Sensor Ports
Dry Contact Port 1
Relay Port 2
Virtual Sensors
SNMPGet
VPing



Network Device (10.1.1.23)
SP2+ .146 (192.168.22.5)
Host Status
Main board
System Name (10.1.1.183)

Important notes:

A) If the SP+ was previously added to the APS using a LAN IP, it has to be removed (delete host). Connecting by VPN will use a different IP address for SP+ but the unit's MAC address is the same, and they'll be in conflict. This is not an issue if the unit has never been added to APS before.

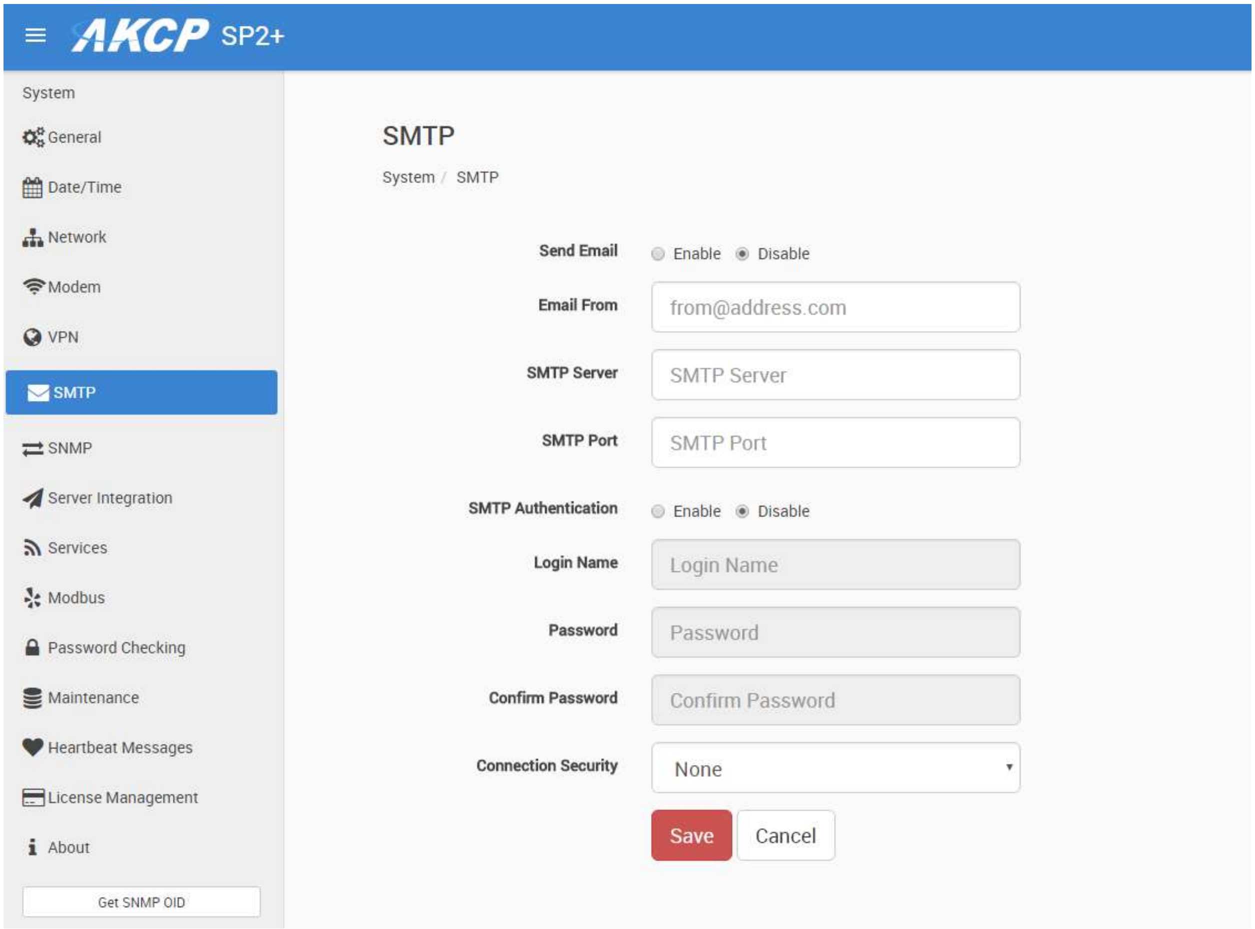
B) If the SP+ unit was previously monitored by APS, you should do a "reset to factory defaults" from the Maintenance menu to fully remove the APS integration from the unit (the existing IP configuration can be kept).

C) The Virtual Sensor Ping cannot ping an IP address on the VPN network.

Important notes for VPN setup with modem connection:

- Port Forwarding to the APS is needed to be set up on your router (allow incoming VPN connection on your selected port)
- The Internal Modem on the unit has to be configured first with the correct APN settings

SMTP



SMTP

System / SMTP

Send Email ○ Enable ● Disable

Email From: from@address.com

SMTP Server: SMTP Server

SMTP Port: SMTP Port

SMTP Authentication ○ Enable ● Disable

Login Name: Login Name

Password: Password

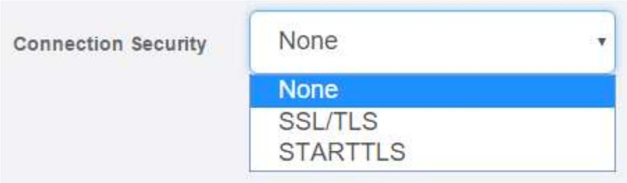
Confirm Password: Confirm Password

Connection Security: None

Save Cancel

The SMTP server configuration options are shown here, it’s required to be set up for the Email actions.

Fill out all parameters; the address in the *Email From* parameter will be used by the Email actions by default, but you could change it if your mail server supports it (when it’s not required to match the SMTP user for example).

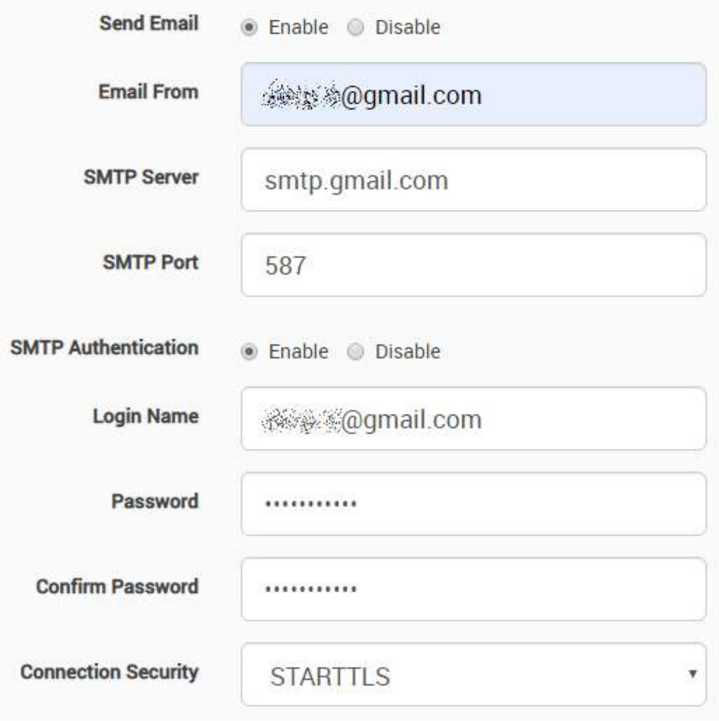


Connection Security: None

SSL/TLS and STARTTLS are supported for the connection security.

You could also turn off any email sending from the unit by disabling the *Send Email* option.

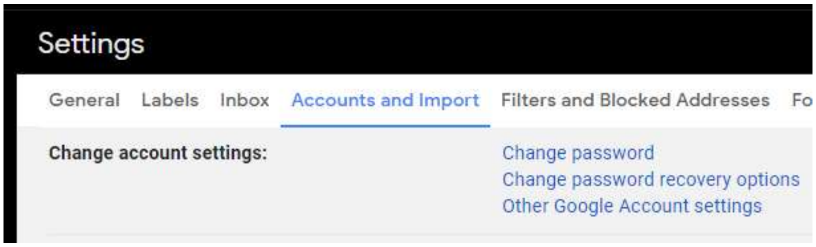
Settings for Gmail



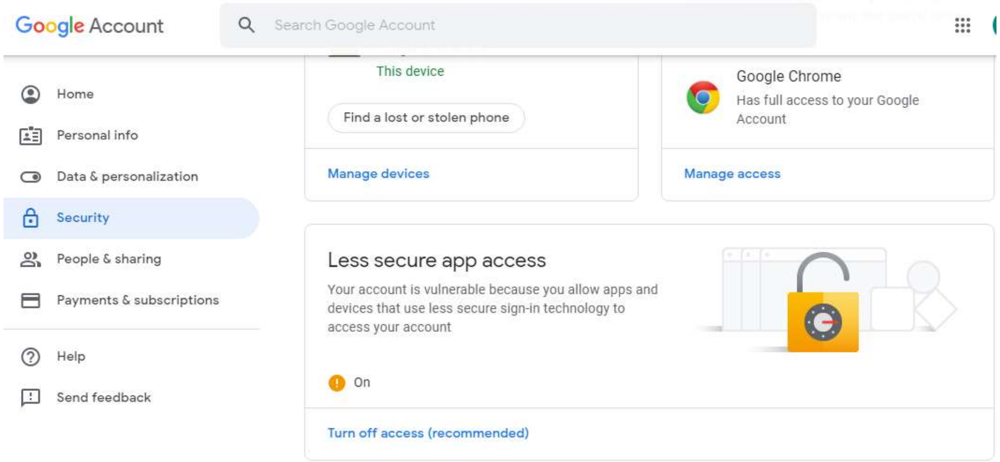
Send Email	● Enable ○ Disable
Email From	[redacted]@gmail.com
SMTP Server	smtp.gmail.com
SMTP Port	587
SMTP Authentication	● Enable ○ Disable
Login Name	[redacted]@gmail.com
Password	•••••••••••
Confirm Password	•••••••••••
Connection Security	STARTTLS ▾

You can use Gmail account to send Email alerts with the settings shown on this screenshot on the left.

Important: before this can work, you'll need to set up an additional setting in your Google account.


Settings
General
Labels
Inbox
Accounts and Import
Filters and Blocked Addresses
Fo
Change account settings:
Change password
Change password recovery options
Other Google Account settings

Open Gmail in a web browser and go to Settings / Accounts and Import / Other Google Account settings



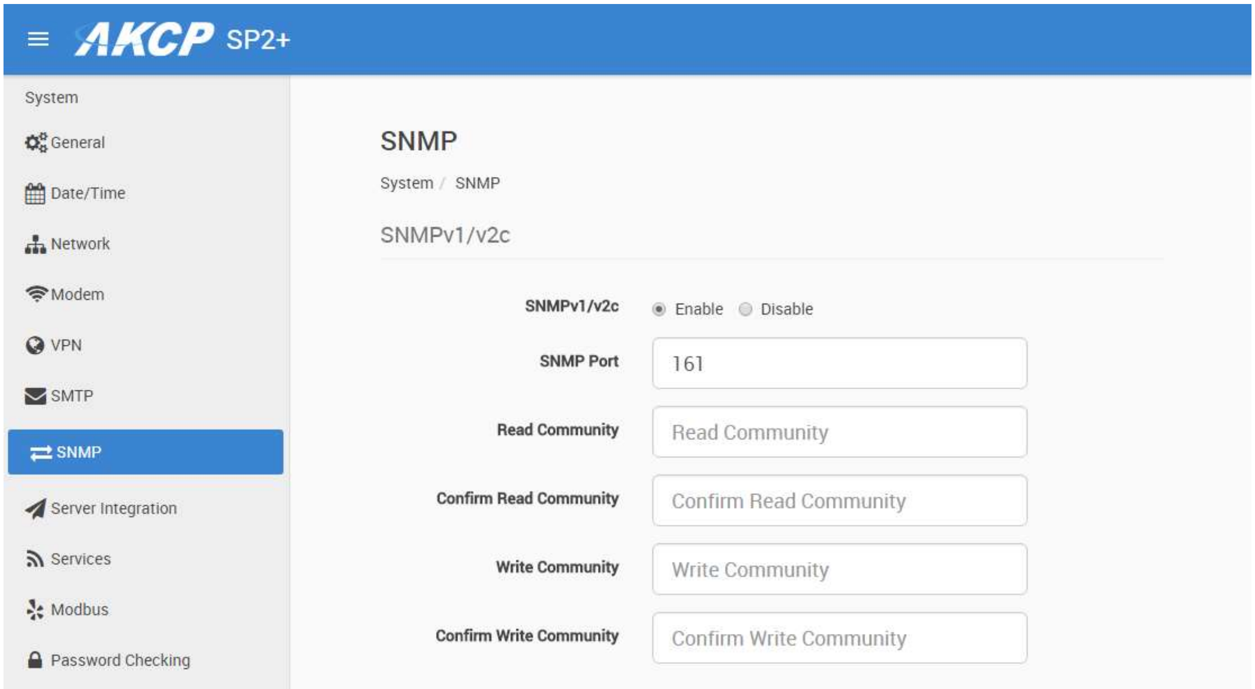
Less secure app access

Your account is vulnerable because you allow apps and devices that use less secure sign-in technology to access your account

On

Then from the Account settings open Security tab / **Enable Less Secure Apps**

SNMP



SNMP

System / SNMP

SNMPv1/v2c

SNMPv1/v2c ● Enable ○ Disable

SNMP Port: 161

Read Community: Read Community

Confirm Read Community: Confirm Read Community

Write Community: Write Community

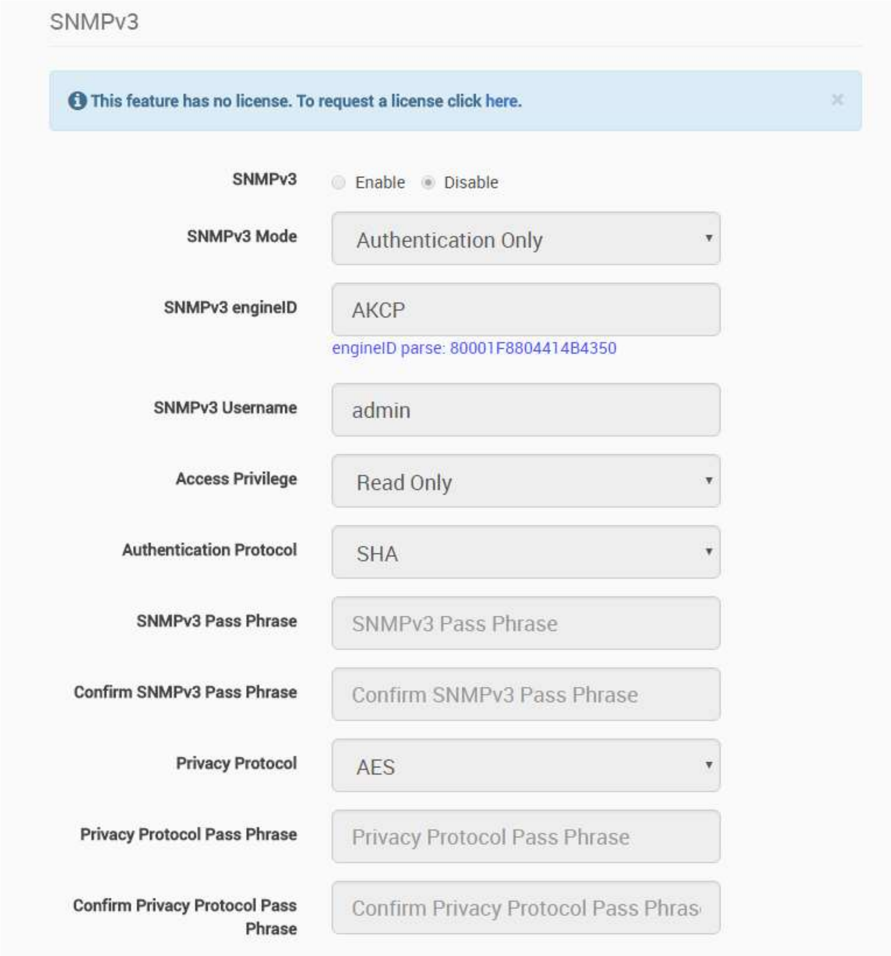
Confirm Write Community: Confirm Write Community

The SNMP service configuration options are shown here, it is required for SNMP operations.

SNMPv1 is enabled by default, with community password “**public**”.
This is provided for the easiest integration with third party SNMP tools.
For enhanced security, it is recommended that you change the default SNMP password.

Scroll down for SNMPv3 options.

SNMPv3



SNMPv3

ℹ This feature has no license. To request a license click here. ×

SNMPv3: ○ Enable ● Disable

SNMPv3 Mode: Authentication Only

SNMPv3 engineID: AKCP

engineID parse: 80001F8804414B4350

SNMPv3 Username: admin

Access Privilege: Read Only

Authentication Protocol: SHA

SNMPv3 Pass Phrase: SNMPv3 Pass Phrase

Confirm SNMPv3 Pass Phrase: Confirm SNMPv3 Pass Phrase

Privacy Protocol: AES

Privacy Protocol Pass Phrase: Privacy Protocol Pass Phrase

Confirm Privacy Protocol Pass Phrase: Confirm Privacy Protocol Pass Phras

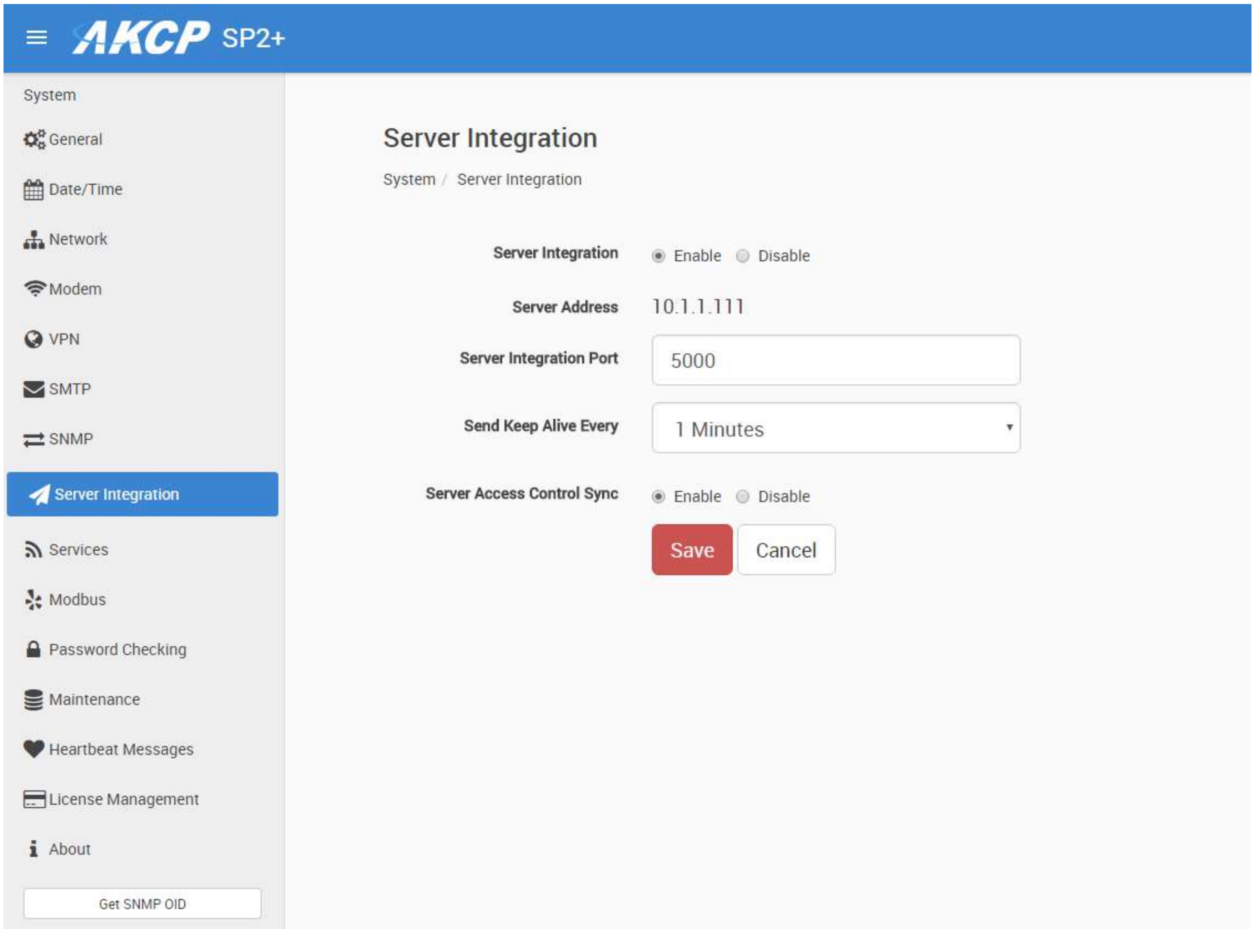
The SNMPv3 options can be found by scrolling down on the SNMP page.
This feature requires a separate license. You can read more details about the licensing below in this manual.

Below we'll give a quick description of each setting:

<u>Level</u>	<u>Authentication</u>	<u>Encryption</u>	<u>Description</u>
No Authentication	Username	No	Match Username (same as SNMP v1/v2c)
Authentication Only	MD5 or SHA	No	Auth Based on Algorithms (check password)
Auth&Privacy	MD5 or SHA	Yes - DES	Auth Algorithms and Encryption

Basically if you select **No Authentication** then the setup will be the same as with SNMP v1 and v2c versions: authentication is only checked by unencrypted username.
Authentication Only will provide password protection but no encryption.
Authentication&Privacy provides encrypted username and password protection.

Server Integration



Server Integration

System / Server Integration

Server Integration ● Enable ○ Disable

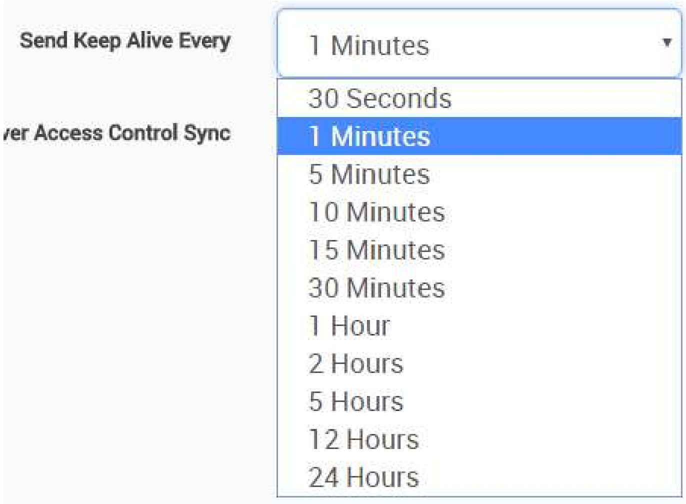
Server Address 10.1.1.111

Server Integration Port 5000

Send Keep Alive Every 1 Minutes

Server Access Control Sync ● Enable ○ Disable

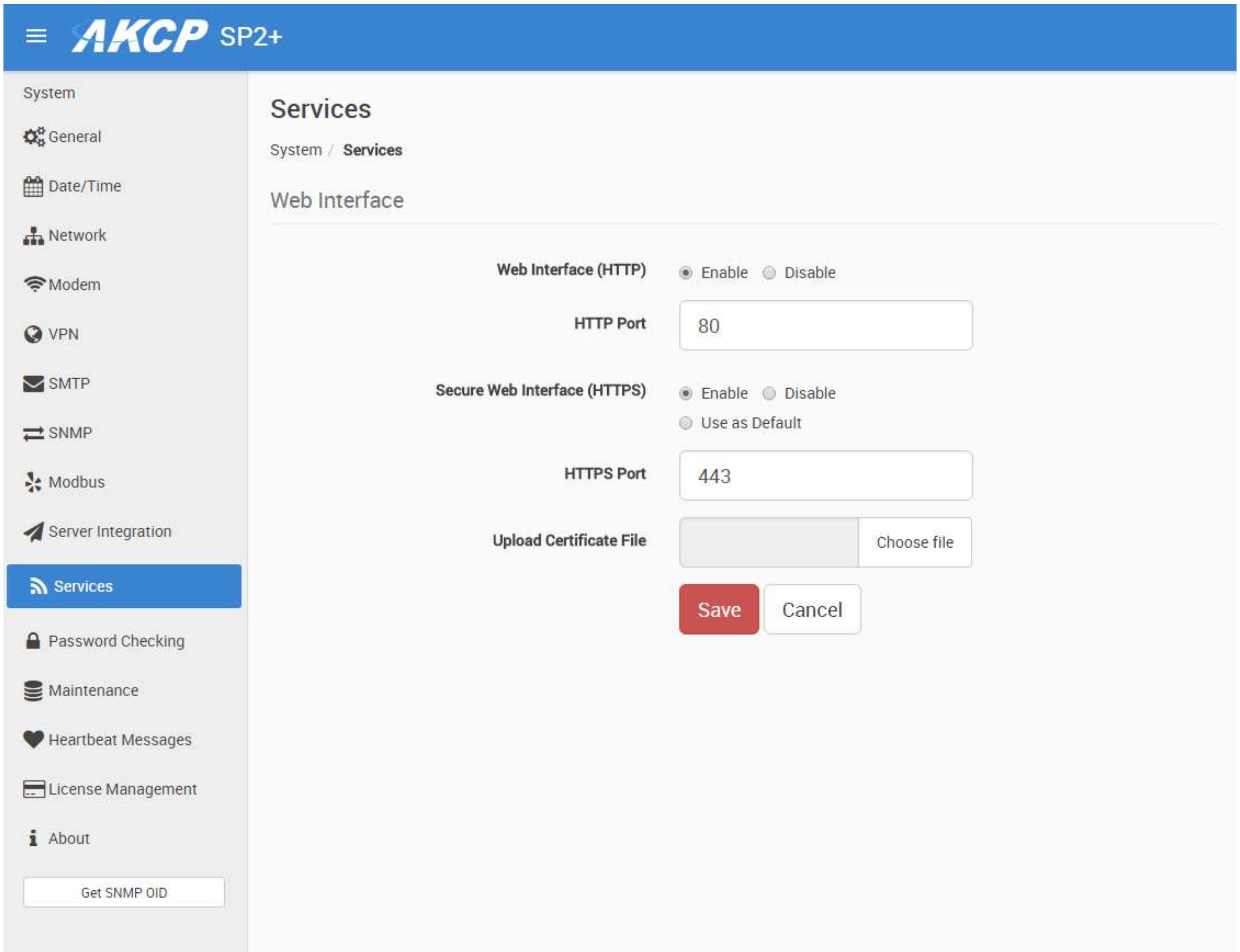
If the unit has been added to the AKCPro Server console, the server's IP address will be displayed here. User configurable options are the APS port and keep-alive period.



You can change the APS port when the server's port changes, and the keep-alive period (heartbeat sync to APS).
Alternatively you can re-initialize your unit from the APS console to re-establish communication.

You may disable the **Access Control Sync** on this device. This will disable importing the Access Control users and groups that are set up in APS. This feature is used by the Swing Handle Lock.

Services



Services

System / Services

Web Interface

Web Interface (HTTP) ● Enable ○ Disable

HTTP Port: 80

Secure Web Interface (HTTPS) ● Enable ○ Disable ○ Use as Default

HTTPS Port: 443

Upload Certificate File: Choose file

Save Cancel

You can close or change the ports used to access the unit's web interface, disable HTTP and enable HTTPS only, which can also be set to be used as default.

On the SP+ family, the HTTPS supports TLS v1.1 and v1.2.
The HTTPS cypher suites are not customizable.

Using the "Upload Certificate File" option you can upload an SSL certificate that will be used by the unit's Web UI for HTTPS connection (see below).

Important: the default, built-in self-signed SSL certificate is only provided for user convenience so that the HTTPS WebUI would work on the units out of the box. It WILL raise browser SSL security warnings and is not meant to be used in production environments where higher security is mandatory. To use SSL without warnings, you need to either add the units IP address to the exceptions, or replace the certificate using the method described below.

SSL Certificate

SSL certificates are generated for DNS host names and not IP addresses. You should set a host name for the SP+ unit in your local DNS server or DHCP server, and then generate the SSL certificate for that host name.

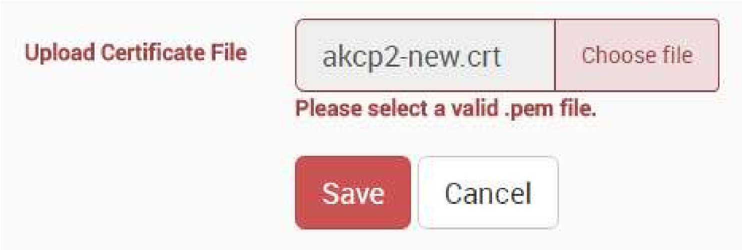
Example: spplus.mycompany.org

The unit's DNS host name is "spplus". Wildcard SSL certificates should also work, but this hasn't been tested.
If the name doesn't match with the one in the certificate, the browser will still show a security warning.

You can purchase a certificate from a trusted, verified Certificate Authority such as GoDaddy or use your company's own CA if you have one.

Please note that only non-password protected certificate files are supported.

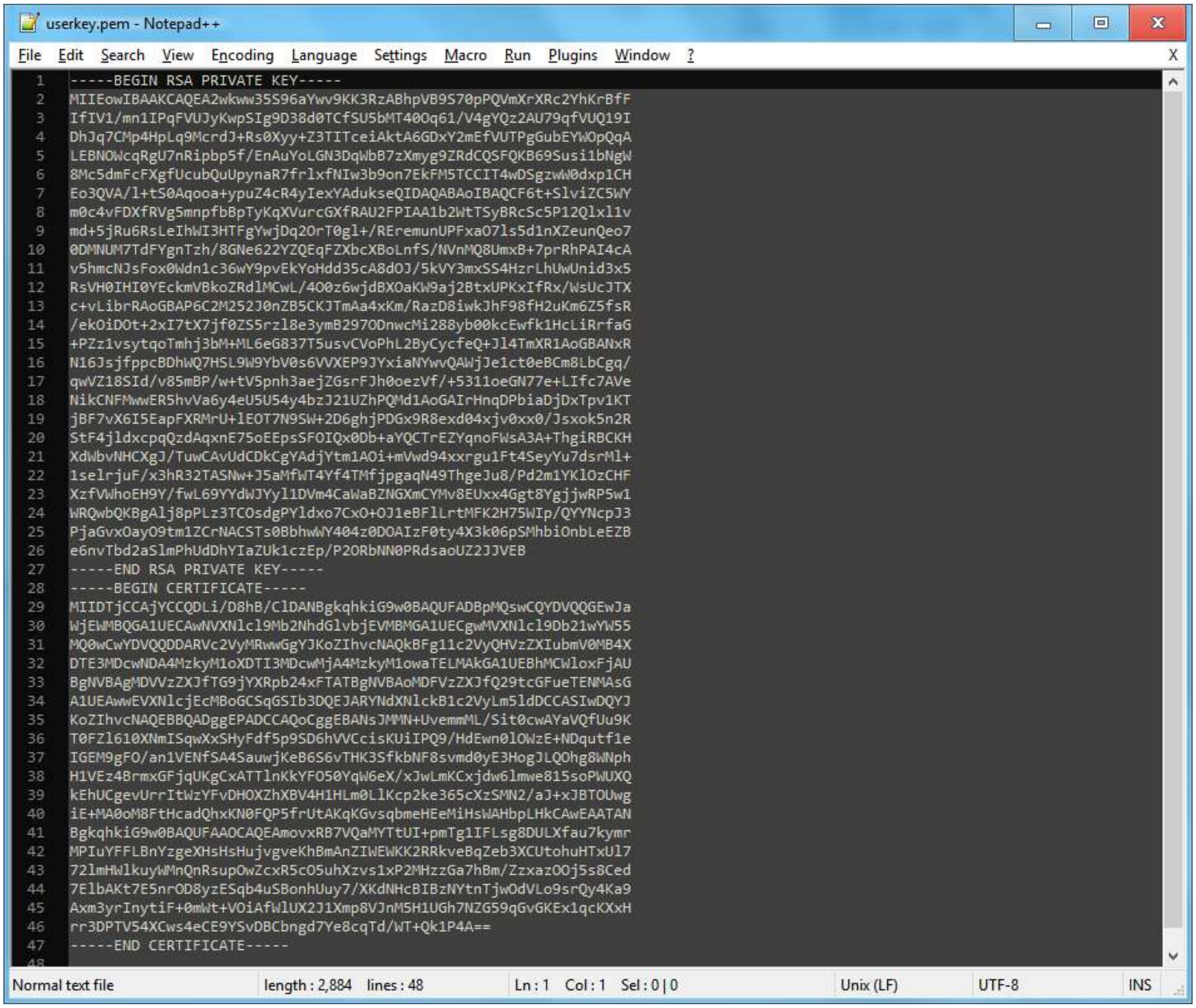
When you select the file for uploading, you'll get a warning if the file is not in .PEM format:



Upload Certificate File: akcp2-new.crt

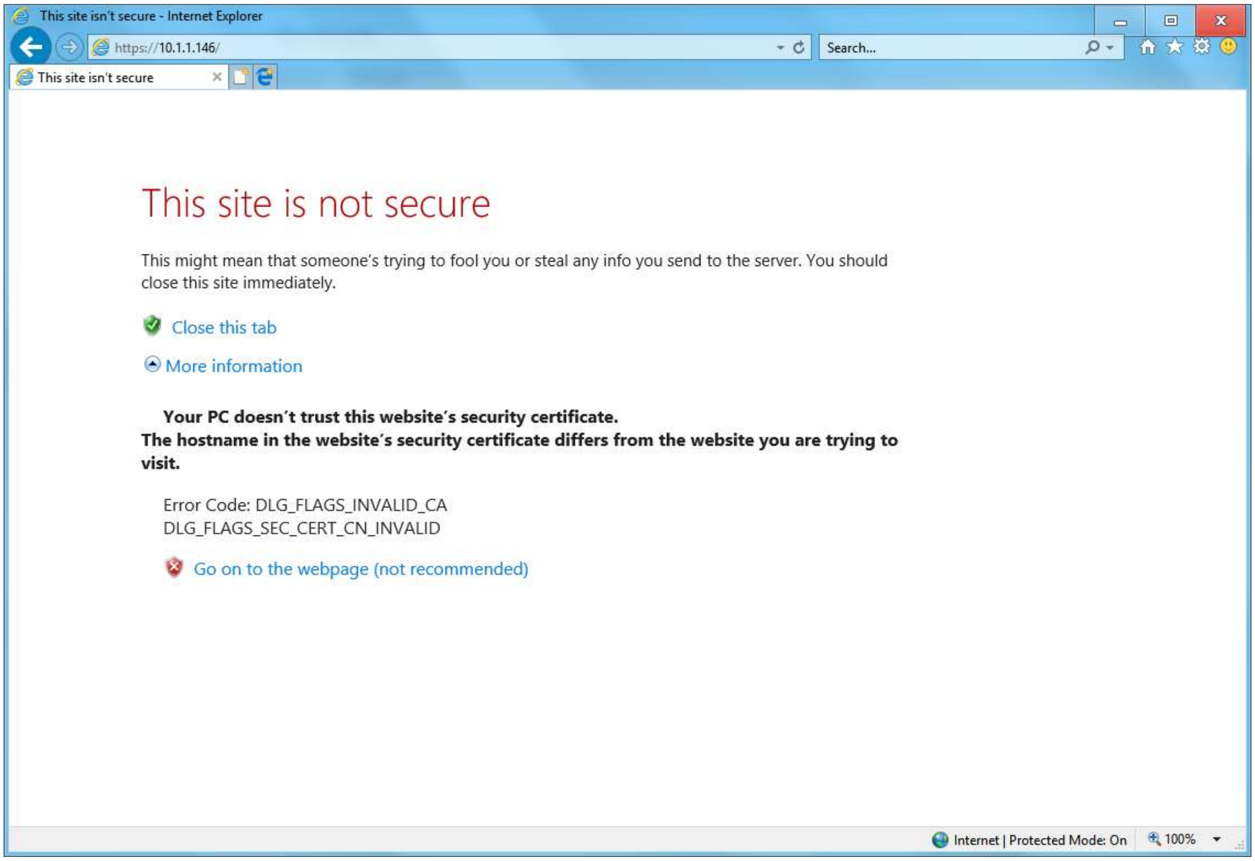
Please select a valid .pem file.

The .PEM file is the private key + certificate combined. You can copy them to one file using Notepad++ if you have 2 separate files, as shown below (it has to be in Unix Line Format and not Windows):



```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA2wkww35S96aYwv9KK3RzABhpVB9S70pPQVmXrXRc2YhKrBfF
IfIV1/mn1IPqFVUJyKwpSIg9D38d0TCfSU5bMT40Oq61/V4gYQz2AU79qfVUQ19I
DhJq7CMp4HpLq9McrdJ+Rs0Xyy+Z3TITceiAktA6GDxY2mEfVUTPgGubEYWOpQqA
LEBNOWcqRgU7nRipbp5f/EnAuYoLGN3DqWbB7zXmyg9ZRdCQSFQKB69Susi1bNgW
8Mc5dmFcFXgfUcubQuUpynaR7frlxfNIw3b9on7EkFM5TCCIT4wDSgzwW0dxp1CH
Eo3QVA/l+tS0Aqooa+ypuZ4cR4yIexYAdukseQIDAQABAoIBAQCF6t+SlviZC5WY
m0c4vFDXfRVg5mnpfbBpTyKqXVurcGXfRAU2FPIAA1b2WtTSyBRcSc5P12Qlxl1v
md+5jRu6RsLeIhWI3HTFgYwjDq2OrT0gl+/REremunUPFxaO7ls5d1nXZeunQeo7
0DMNUM7TdFYgnTzh/8GNe622YZQEqFZXbcXBoLnfS/NVnMQ8UmxB+7prRhPAI4cA
v5hmcNJsFox0Wdn1c36wY9pvEkYoHdd35cA8dOJ/5kVY3mxSS4HzrLhUwUnid3x5
RsVH0IHI0YEckmVBkoZRdlMCwL/4O0z6wjdBXOaKW9aj2BtxUPKxIfRx/WsUcJTX
c+vLibrRAoGBAP6C2M252J0nZB5CKJTmAa4xKm/RazD8iwkJhF98fH2uKm6Z5fsR
/ekOiDOt+2xI7tX7jf0ZS5rzl8e3ymB297ODnwcMi288yb00kcEwfk1HcLiRrfaG
+PZz1vsytqoTmhj3bM+ML6eG837T5usvCVoPhL2ByCycfeQ+Jl4TmXR1AoGBANxR
N16JsjfppcBDhWQ7HSL9W9YbV0s6VVXEP9JYxiaNYwvQAWjJe1ct0eBCm8LbCgq/
qwVZ18SId/v85mBP/w+tV5pnh3aejZGsrFJh0oezVf/+5311oeGN77e+LIfc7AVe
NikCNFMwwER5hvVa6y4eU5U54y4bzJ21UZhPQMd1AoGAIrHnqDPbiaDjDxTpv1KT
jBF7vX6I5EapFXRMrU+lEOT7N9SW+2D6ghjPDGx9R8exd04xjv0xx0/Jsxok5n2R
StF4jldxcpqQzdAqxnE75oEEpsSFOIQx0Db+aYQCTrEZYqnoFWsA3A+ThgiRBCKH
XdWbvNHCXgJ/TuwCAvUdCDkCgYAdjYtm1AOi+mVwd94xxrgu1Ft4SeyYu7dsrMl+
1selrjuF/x3hR32TASNw+J5aMfWT4Yf4TMfjpgaqN49ThgeJu8/Pd2m1YKlOzCHF
XzfVWhoEH9Y/fwL69YYdWJYyl1DVm4CaWaBZNGXmCYMv8EUxx4Ggt8YgjjwRP5w1
WRQwbQKBgAlj8pPLz3TCOsdgPYldxo7CxO+OJ1eBFlLrtMFK2H75WIp/QYYNcpJ3
PjaGvxOayO9tm1ZCrNACSTs0BbhwWY404z0DOAIzF0ty4X3k06pSMhbiOnbLeEZB
e6nvTbd2aSlmPhUdDhYIaZUk1czEp/P2ORbNN0PRdsaoUZ2JJVEB
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDTjCCAjYCCQDLi/D8hB/ClDANBgkqhkiG9w0BAQUFADBpMQswCQYDVQQGEwJa
WjEWMBQGA1UECAwNVXNlcl9Mb2NhdGlvbjEVMBMGA1UECgwMVXNlcl9Db21wYW55
MQ0wCwYDVQQDDARVc2VyMRwwGgYJKoZIhvcNAQkBFg11c2VyQHVzZXIubmV0MB4X
DTE3MDcwNDA4MzkyM1oXDTI3MDcwMjA4MzkyM1owaTELMAkGA1UEBhMCWloxFjAU
BgNVBAgMDVVzZXJfTG9jYXRpb24xFTATBgNVBAoMDFVzZXJfQ29tcGFueTENMAsG
A1UEAwwEVXNlcjEcMBoGCSqGSIb3DQEJARYNdXNlckB1c2VyLm5ldDCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBANsJMMN+UvemmML/Sit0cwAYaVQfUu9K
T0FZl610XNmISqwXxSHyFdf5p9SD6hVVCcisKUiIPQ9/HdEwn0lOWzE+NDqutf1e
IGEM9gFO/an1VENfSA4SauwjKeB6S6vTHK3SfkbNF8svmd0yE3HogJLQOhg8WNph
H1VEz4BrmxGFjqUKgCxATTlnKkYFO50YqW6eX/xJwLmKCxjdw6lmwe815soPWUXQ
kEhUCgevUrrItWzYFvDHOXZhXBV4H1HLm0LlKcp2ke365cXzSMN2/aJ+xJBTOUwg
iE+MA0oM8FtHcadQhxKN0FQP5frUtAKqKGvsqbmeHEeMiHsWAHbpLHkCAwEAATAN
BgkqhkiG9w0BAQUFAAOCAQEAmovxRB7VQaMYTtUI+pmTg1IFLsg8DULXfau7kymr
MPIuYFFLBnYzgeXHsHsHujvgveKhBmAnZIWEWKK2RRkveBqZeb3XCUtohuHTxUl7
72lmHWlkuyWMnQnRsupOwZcxR5cO5uhXzvs1xP2MHzzGa7hBm/ZzxazOOj5s8Ced
7ElbAKt7E5nrOD8yzESqb4uSBonhUuy7/XKdNHcBIBzNYtnTjwOdVLo9srQy4Ka9
Axm3yrInytiF+0mWt+VOiAfWlUX2J1Xmp8VJnM5H1UGh7NZG59qGvGKEx1qcKXxH
rr3DPTV54XCws4eCE9YSvDBCbngd7Ye8cqTd/WT+Qk1P4A==
-----END CERTIFICATE-----
```

If you don't upload a certificate but enable HTTPS, a built-in certificate will be used. You'll get a browser warning upon opening the Web UI about an incorrect certificate. This is normal and you should add it as an exception or proceed, depending on your browser:


This site isn't secure - Internet Explorer
https://10.1.1.146/
Search...
This site isn't secure
Internet | Protected Mode: On
100%

This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

Close this tab

More information

Your PC doesn't trust this website's security certificate.
The hostname in the website's security certificate differs from the website you are trying to visit.

Error Code: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

Go on to the webpage (not recommended)

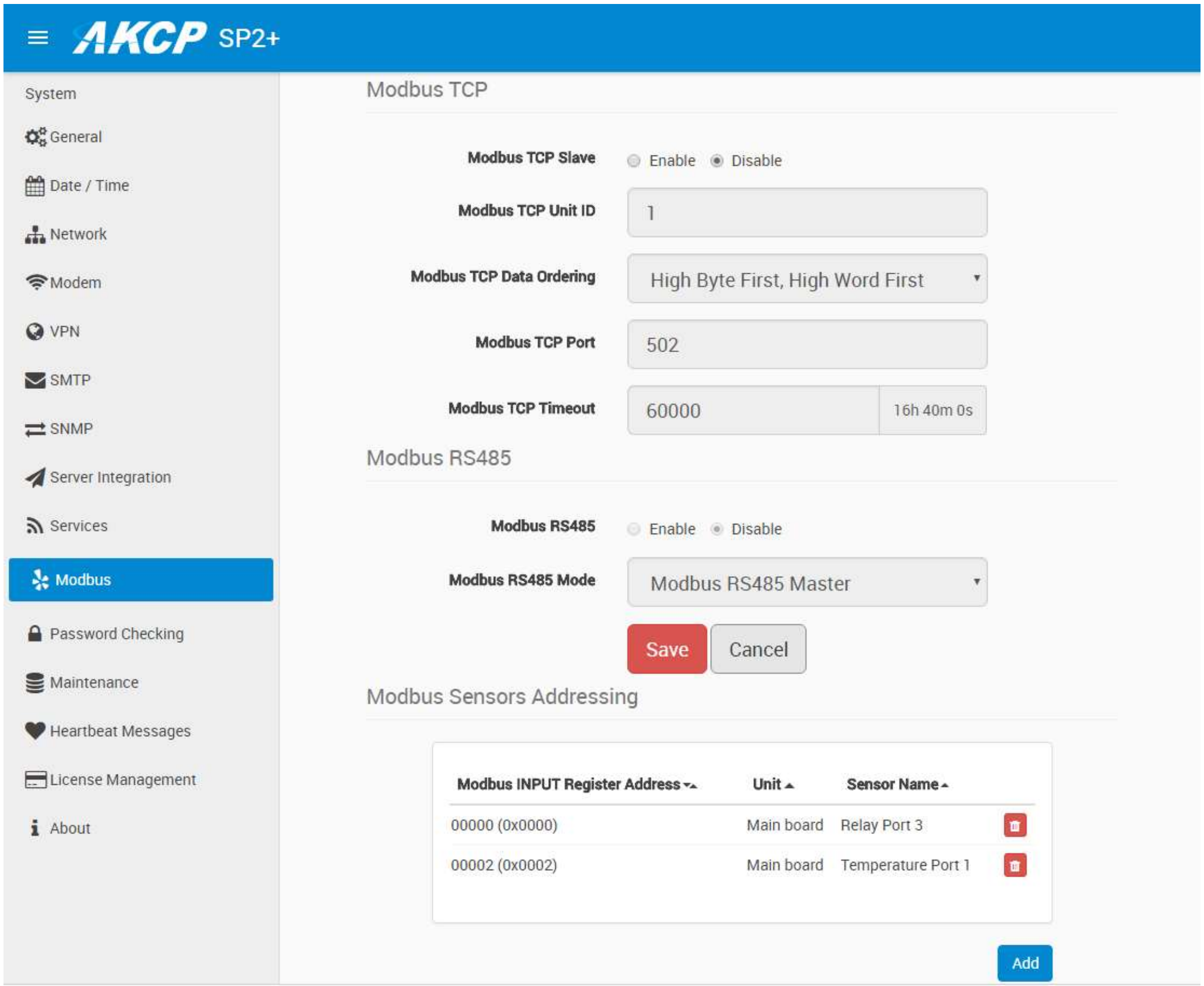
Important: the default, built-in self-signed SSL certificate is only provided for user convenience so that the HTTPS WebUI would work on the units out of the box. It WILL raise browser SSL security warnings and is not meant to be used in production environments where higher security is mandatory. To use SSL without warnings, you need to either add the units IP address to the exceptions, or replace the certificate.

Modbus

MODBUS RTU is a non-proprietary serial communications protocol that is widely used in the process control industry actuation. The sensorProbe+ can represent both “master” and “slave” devices and supports both Modbus RTU (RS-485) and Modbus TCP protocols.

SP2+ Expansion and SPX+ currently only supports Modbus with RJ45 connector (RTU and TCP) on its Expansion port. For just Modbus, only the pin 1 and 2 are used, being respectively, Modbus A/+ and Modbus B/-. You cannot use other sensor ports for Modbus other than the Expansion port. *Important: When you use Modbus, you can’t connect expansion boards to the unit!*

SP2+ Standard can only use the Modbus Virtual Sensors.
Note: Modbus queries are slow (up to 3 seconds). This is per Modbus protocol definition, it’s not an AKCP limitation. The more sensors you have, the bigger the polling interval must be.



Modbus TCP

Modbus TCP Slave: ○ Enable ● Disable
Modbus TCP Unit ID: 1
Modbus TCP Data Ordering: High Byte First, High Word First
Modbus TCP Port: 502
Modbus TCP Timeout: 60000 16h 40m 0s

Modbus RS485

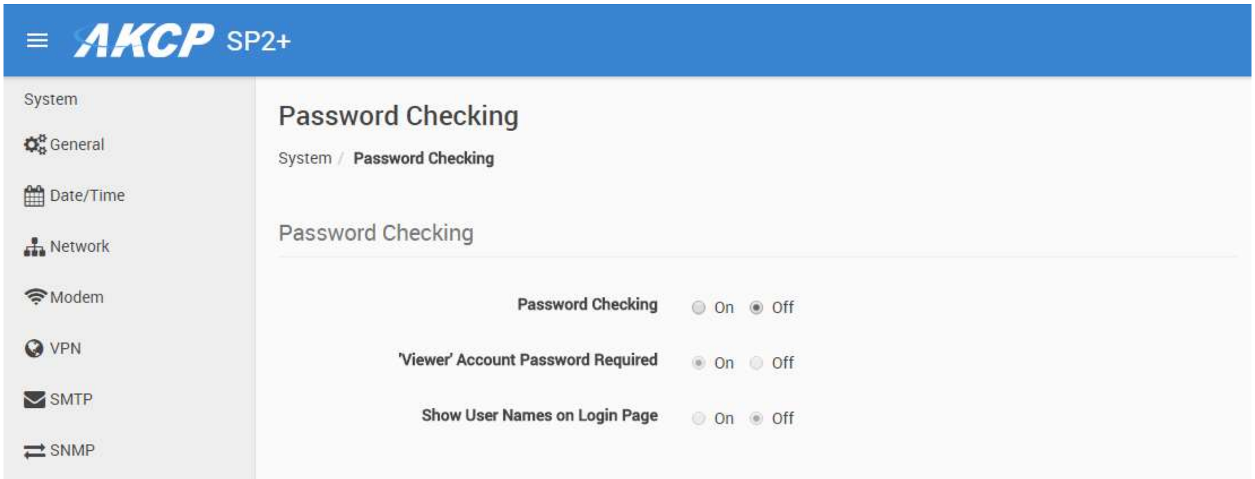
Modbus RS485: ○ Enable ● Disable
Modbus RS485 Mode: Modbus RS485 Master

Modbus Sensors Addressing

Modbus INPUT Register Address	Unit	Sensor Name
00000 (0x0000)	Main board	Relay Port 3
00002 (0x0002)	Main board	Temperature Port 1

Configuring the Modbus options and more information about this feature is explained in the separate **SP+ Modbus manual**.

Password Checking and Security



Password Checking

Password Checking

Password Checking ○ On ● Off

'Viewer' Account Password Required ● On ○ Off

Show User Names on Login Page ○ On ● Off

You can turn on the password checking for the Web UI to ensure only authenticated users have access to the unit. You can also specify to show all user names on the login page, or keep them confidential.
After you enable the password checking, you'll need to re-login.
If you don't remember the Admin password, you can hold the unit's reset button for 7-12 seconds to be able to log in to the Web UI without a password.

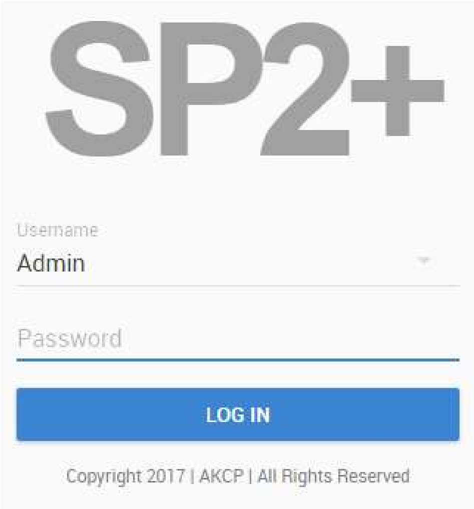
Note 1: The passwords can only be set from the unit's Web UI; this option is not available from APS.
Note 2: The default password is "public" for all access levels.

Web UI user access levels and permissions

Admin - full access to all settings, system and notification configurations
Viewer - read-only guest access for every page
User - full access to most settings except for those which are the system-related such as network

In detail, the User access level provides these permissions in addition to the Viewer level:

Allow modifying board/sensor settings
Allow add/modify/remove notifications
Allow add/modify/remove heartbeats
Allow open/close the door on the Handle Lock
Allow send configuration to Support
Allow change Graph settings
Allow change the Web UI language

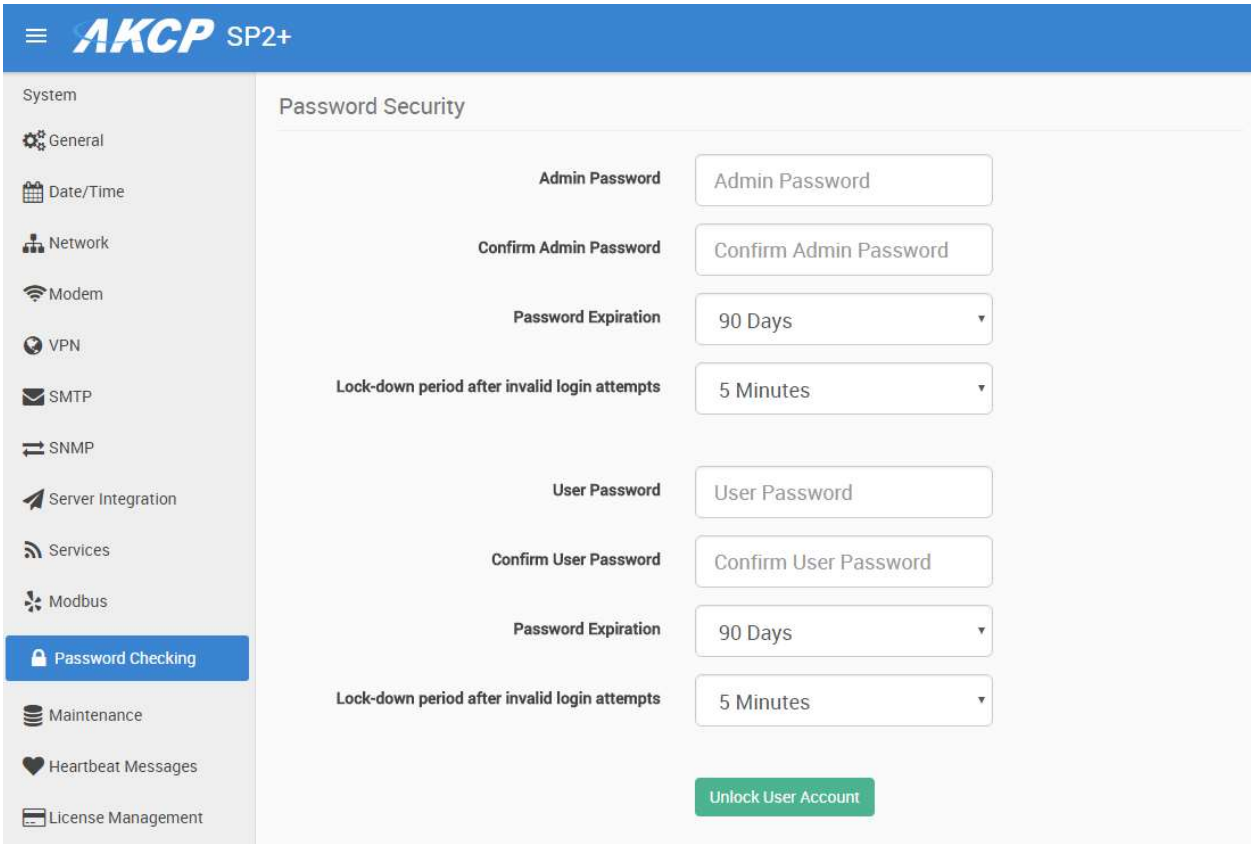


Username
Admin

Password

Copyright 2017 | AKCP | All Rights Reserved

Password Security options



Password Security

Admin Password: Admin Password

Confirm Admin Password: Confirm Admin Password

Password Expiration: 90 Days

Lock-down period after invalid login attempts: 5 Minutes

User Password: User Password

Confirm User Password: Confirm User Password

Password Expiration: 90 Days

Lock-down period after invalid login attempts: 5 Minutes

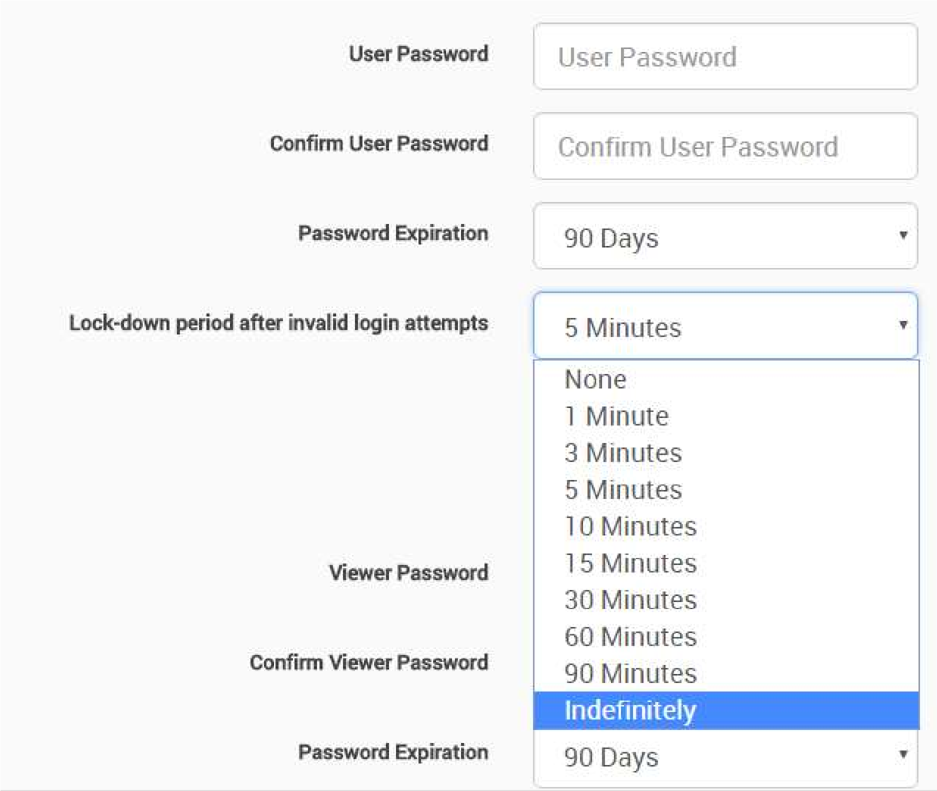
All user account types (Admin, User, Viewer) have adjustable password expiration and lockdown periods.

The password can be up to 15 characters (a-z, A-Z, 0-9 and special characters).

The IP address of the remote user’s computer will be logged in the syslog so you can trace back each login session to its origin.

F7 units also support Radius password checking (licensed separately), we have a separate manual about this feature.

Lockdown



User Password: User Password

Confirm User Password: Confirm User Password

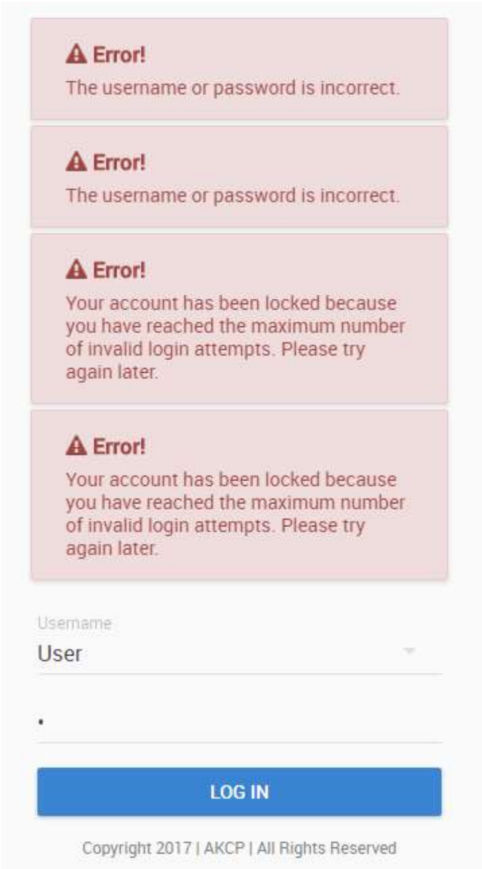
Password Expiration: 90 Days

Lock-down period after invalid login attempts: 5 Minutes

Viewer Password

Confirm Viewer Password

Password Expiration: 90 Days



⚠ Error!
The username or password is incorrect.

⚠ Error!
The username or password is incorrect.

⚠ Error!
Your account has been locked because you have reached the maximum number of invalid login attempts. Please try again later.

⚠ Error!
Your account has been locked because you have reached the maximum number of invalid login attempts. Please try again later.

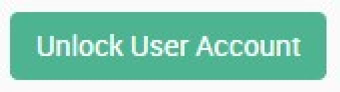
Username: User

Copyright 2017 | AKCP | All Rights Reserved

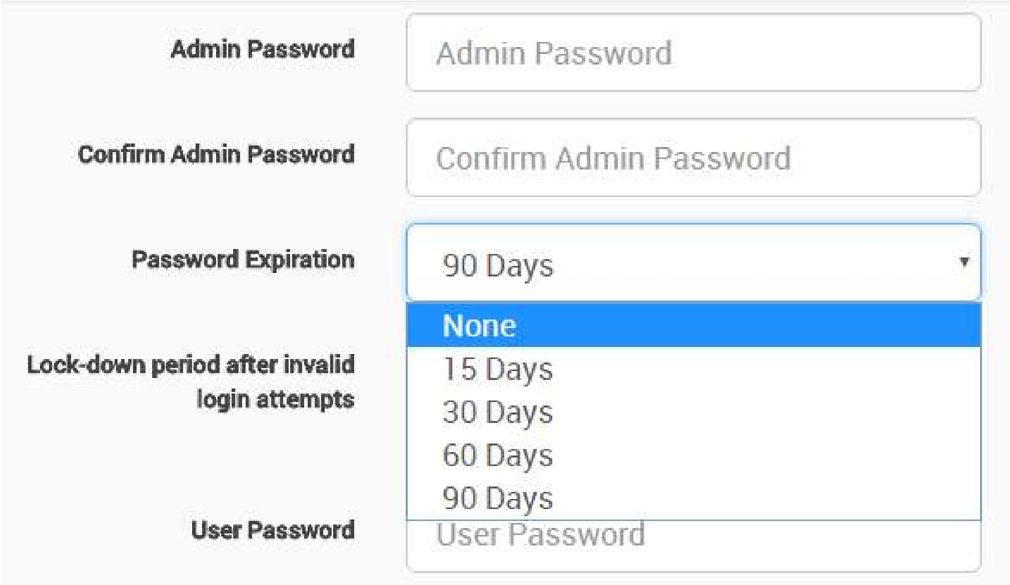
The accounts can be set to lock down the account after 3 invalid login attempts, to prevent brute-force hacking attempts.
You can specify how long the account will automatically unlock itself.

Note that for the Admin user, you can’t select “indefinitely” as this would prevent you from logging in to the Web UI if it has locked itself.

If an account has been locked, you can unlock it immediately by logging in with the Admin user, and by using the green unlock button:



Password Expiration



Admin Password: Admin Password

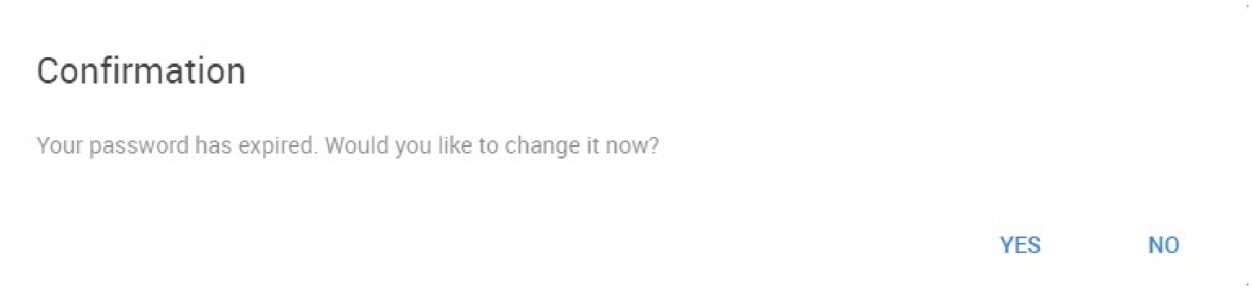
Confirm Admin Password: Confirm Admin Password

Password Expiration: 90 Days

Lock-down period after invalid login attempts

User Password: User Password

You can specify password expiration between every 15 and 90 days for all account types. You could also set “none” to disable expiration.

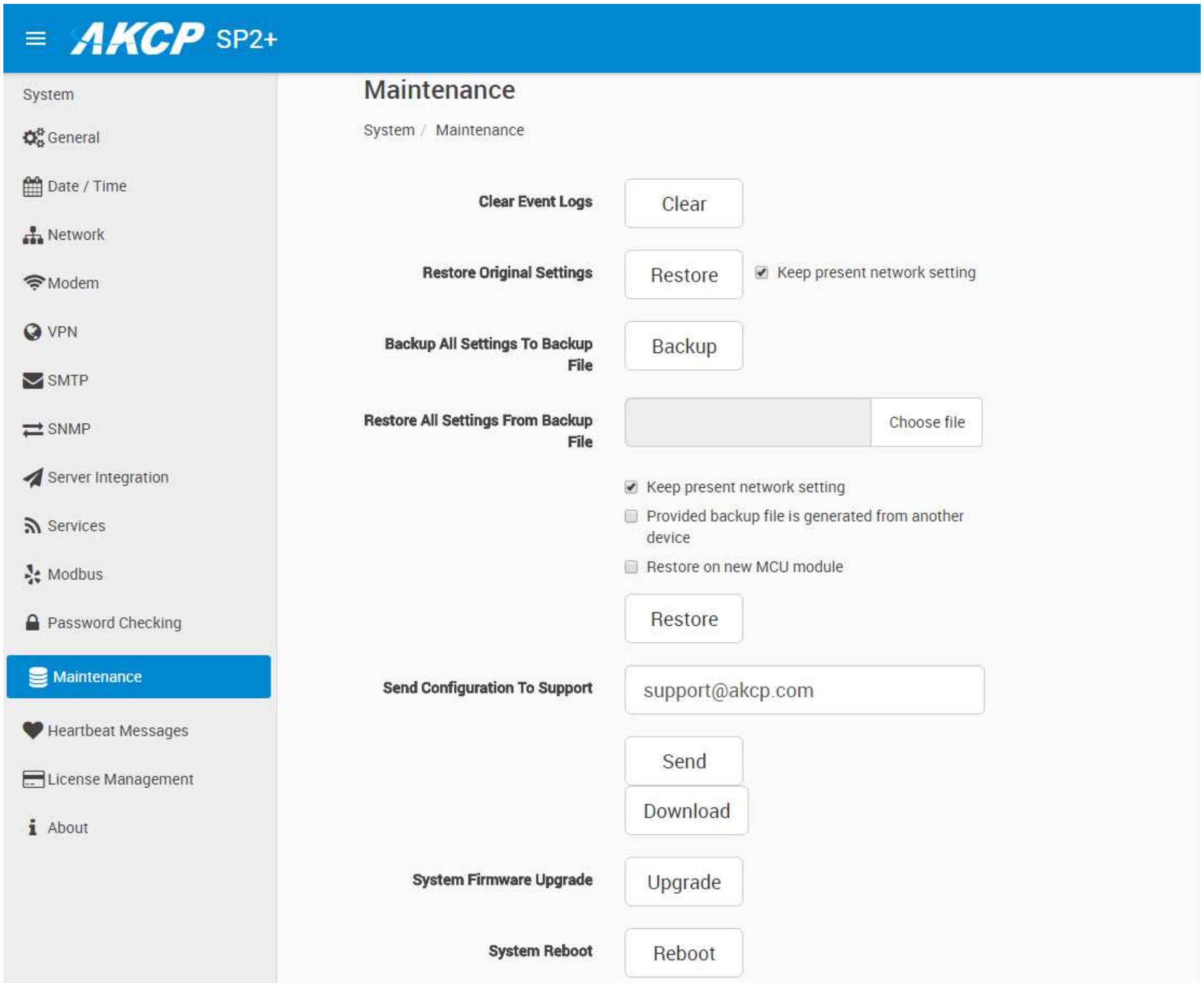


Confirmation

Your password has expired. Would you like to change it now?

You’ll get a notification upon login when the password has expired, and will be asked to change it. It’s advised to change it when asked, but you can still proceed without changing.

Maintenance



Clear Event Logs

Restore Original Settings ☑ Keep present network setting

Backup All Settings To Backup File

Restore All Settings From Backup File

☑ Keep present network setting

☐ Provided backup file is generated from another device

☐ Restore on new MCU module

Send Configuration To Support: support@akcp.com

System Firmware Upgrade

System Reboot

On this page the following options are available:

Clear Event Logs: clears all logged events.

Restore Original Settings: removes all customized settings and returns the unit to factory defaults - you can also choose to keep the network configuration intact.

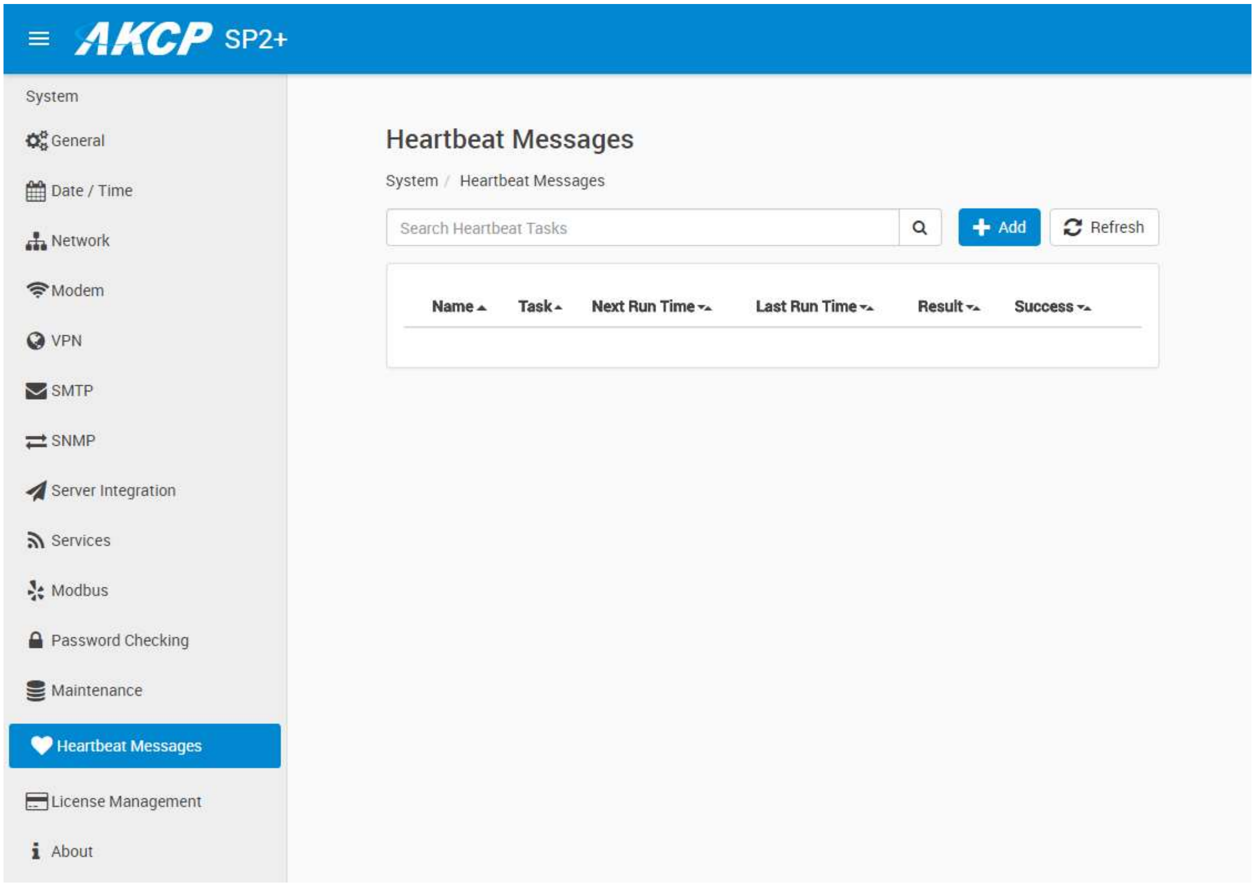
Backup/Restore All Settings: the unit’s configuration can be backed up to a file and restored quickly and easily. You can choose to keep the present network settings, if the backup file is from another unit. The backup file contains all settings and notifications for the unit.

Send Configuration To Support: when asked by Support, this sends the unit’s backup file to us. This also contains the device’s internal logs which are useful for troubleshooting.

System Firmware Upgrade: allows you to upgrade to the latest firmware of the unit - alternatively you could upgrade from APS. We'll show you the process of the Web UI firmware upgrade below in another section.

System Reboot: this will initiate a software reboot of the unit, useful when you only have remote access. You'll need to specify the Admin user's password again.

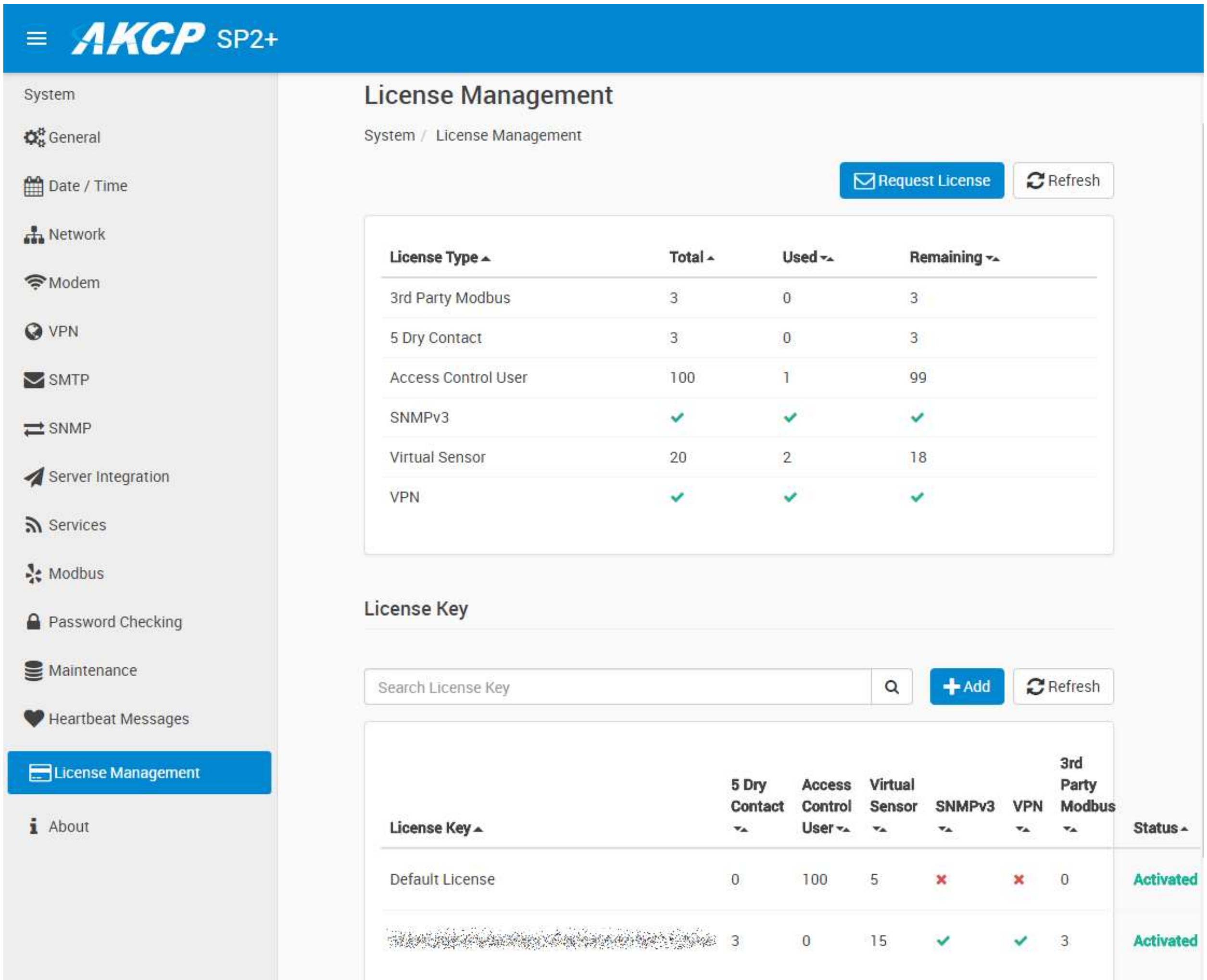
Heartbeat Messages



This feature allows you to set up periodical “keep alive” notifications task by email, SMS or SNMP Trap to indicate the unit is still working properly.

We’ll show you how to set up these in another manual with the other notifications and actions.

License Management



License Type	Total	Used	Remaining
3rd Party Modbus	3	0	3
5 Dry Contact	3	0	3
Access Control User	100	1	99
SNMPv3	✓	✓	✓
Virtual Sensor	20	2	18
VPN	✓	✓	✓

License Key

License Key	5 Dry Contact	Access Control User	Virtual Sensor	SNMPv3	VPN	3rd Party Modbus	Status
Default License	0	100	5	✗	✗	0	Activated
[redacted]	3	0	15	✓	✓	3	Activated

Here you can manage the purchased licenses for specific features on the unit.

For example you can request SNMPv3 license by clicking on the **Request License** button.
This will send an email to our Sales team with your unit’s MAC ID. You can then add the purchased license key with the **Add** button and activate this feature on the unit.

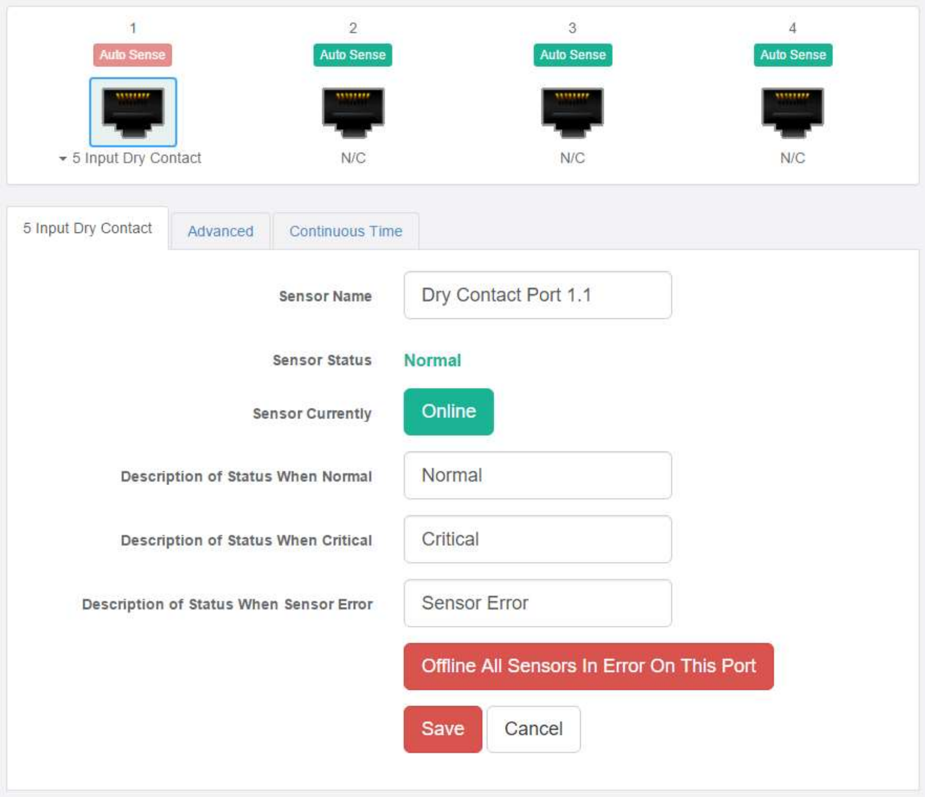
License keys can be backed up/restored with the backup file.
All keys are unique per device and per feature.

Features that needs separate licensing:

- *5 Dry Contact option:* Allows you to connect 5 dry contacts (input only) per sensor ports. See below for more information.
- *Access Control User licenses over 100:* The first 100 user licenses are free (1 is always used for the Admin user), and you can get more licensed users in blocks of 100; the limit is 1000.
- *SNMPv3 feature:* Allows you to use and configure secure, authenticated SNMP trap messages.
- *Virtual Sensors:* Allows you to use and configure virtual sensors. The first 5 sensors are free, you can get more license in blocks of 5.
- *VPN feature:* Currently the APS VPN integration is supported, to use a secure VPN channel between the unit and APS. Please note that when using this option, the number of maximum sensors that can be used by the unit will be reduced to 34 on the older F4 units.
- *3rd Party Modbus Device:* Allows you to easily integrate your Modbus devices with the SP+ units using configuration template files. This is only available on units with expansion ports.
- *F7 units:* IPv6 and Radius features (see separate manuals about these).

About Dry Contact Inputs

The dry contact inputs can be configured as ***inputs only* up to 5 Volts**.



Sensor Name: Dry Contact Port 1.1

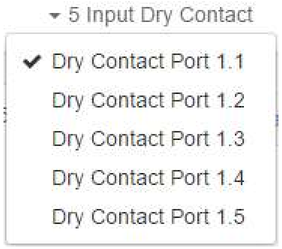
Sensor Status: Normal

Sensor Currently: Online

Description of Status When Normal: Normal

Description of Status When Critical: Critical

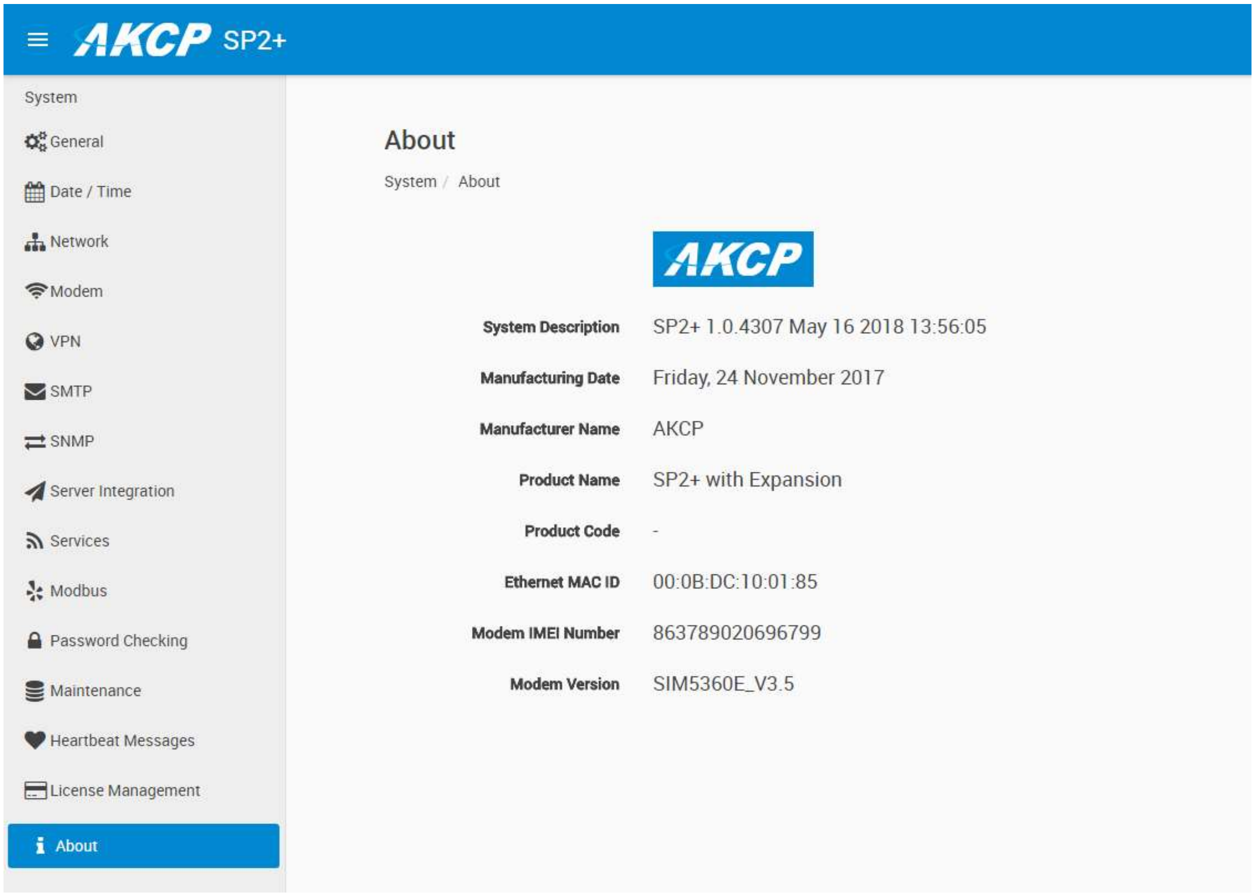
Description of Status When Sensor Error: Sensor Error



Practical applications:

The dry contact inputs can be used to monitor many types of equipment, for example, you can run the connection from warning lights on alarm panels to the dry contact inputs, so that when the warning light on the alarm panel is activated, the dry contact is triggered, thus allowing you to send notifications via emails or SNMP traps.

About

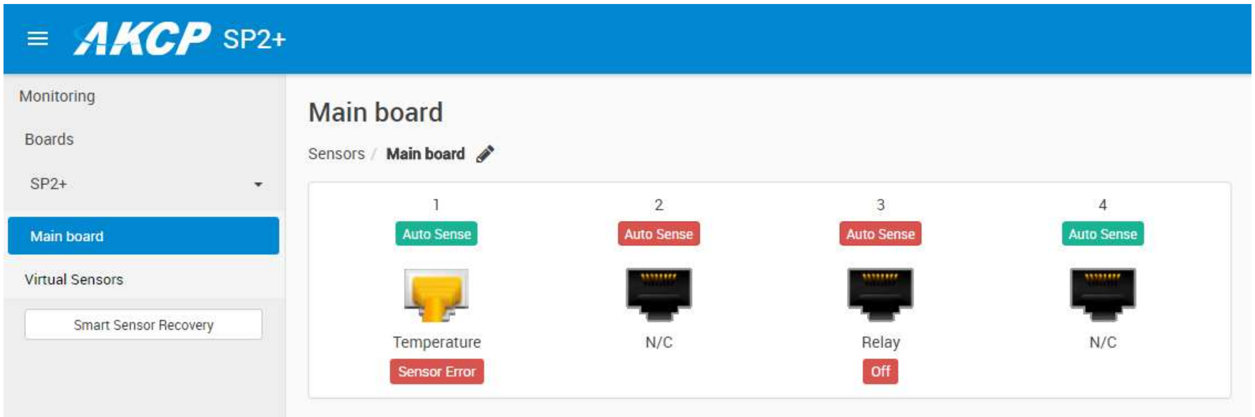


System Description	SP2+ 1.0.4307 May 16 2018 13:56:05
Manufacturing Date	Friday, 24 November 2017
Manufacturer Name	AKCP
Product Name	SP2+ with Expansion
Product Code	-
Ethernet MAC ID	00:0B:DC:10:01:85
Modem IMEI Number	863789020696799
Modem Version	SIM5360E_V3.5

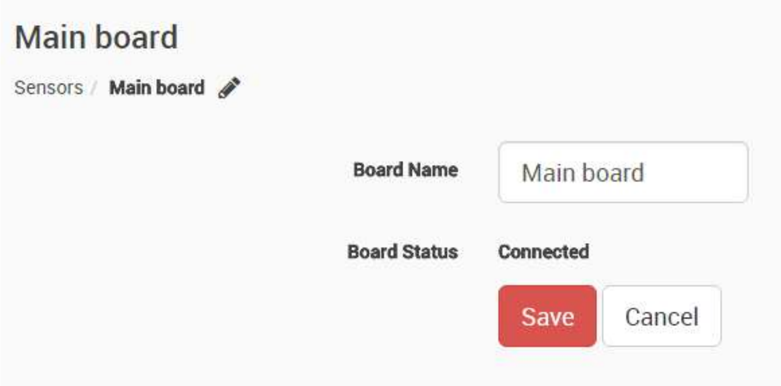
This page shows information about the **Manufacturing Date**, **Ethernet MAC ID**, **System Description** and **unit type (F4/F7)** which are important when you request support.
If equipped, the internal modem's details will be also listed here.

You could make a similar screenshot when you need help with your unit, as this information can help us diagnose the problem.

Sensors page



On this page you can view all sensors connected to the unit per port.
Non-connected sensors will be also displayed, until you re-attach or manually remove them from the configuration.


Main board

Sensors / Main board

Board Name: Main board

Board Status: Connected

You could also rename the unit's Main board by clicking on the pencil icon: ✎

Please note the **maximum supported cable length to use with Thermal Map Sensors**:
Maximum extension cable length from the SP2+ sensor port to the TMS using CAT5 = 28 Feet
Maximum extension cable length from the SP2+ sensor port to the TMS using CAT5e & CAT6 = 60 Feet

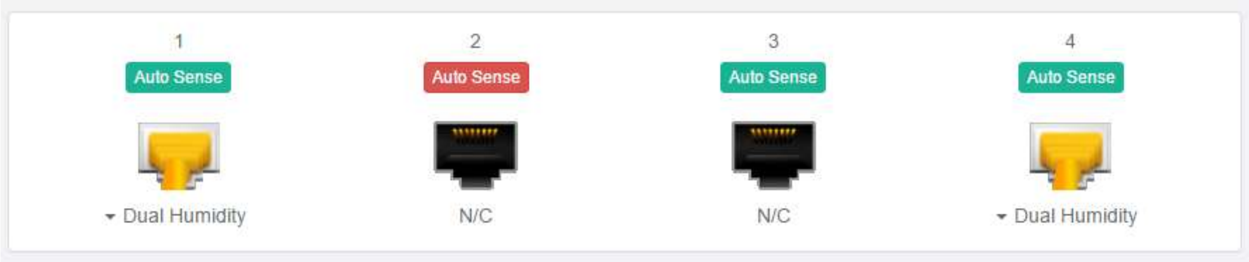
Important note: If you're using analog pins on the sensor ports (with manually on-lined DCV sensors, and pin 7 of the RJ45 connector) make sure that the **voltage doesn't exceed 3 Volts**. Otherwise you can damage the unit!

General options for all sensors

You can change the following general options for all sensors:

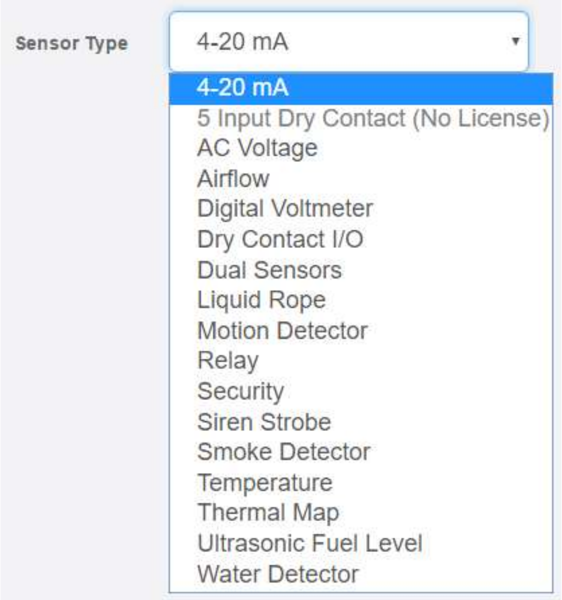
Disable Auto Sense

Click on the **Auto Sense** button to turn off the automatic sensor detection for a port.



This feature is useful if you want to simulate a sensor (this works for Relay type sensors) or to prevent a sensor from going offline state. Note however that the sensor will be in “sensor error” state if the unit can’t get any reading from the sensor.

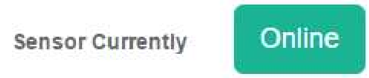
Choose Sensor Type



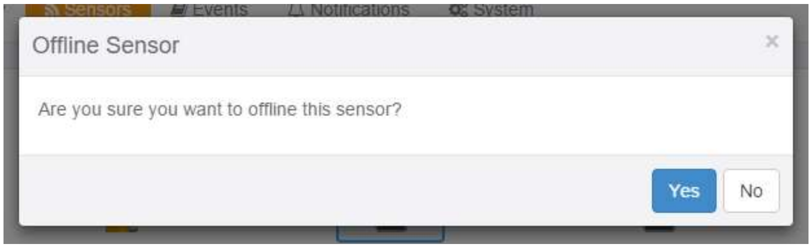
Sensor Type: 4-20 mA

You can pre-configure a specific sensor type if needed, for example if you put the sensor offline before.

Offline a sensor


Sensor Currently

You can manually offline any sensor by clicking on the green **Online** button on the sensor’s configuration page.



Offline Sensor

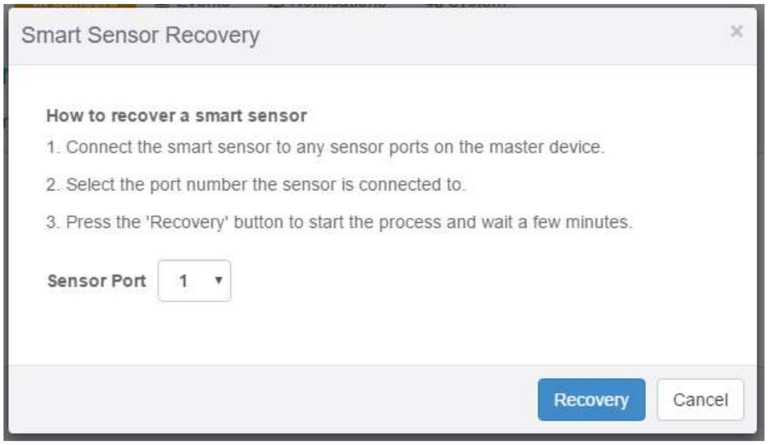
Are you sure you want to offline this sensor?

You’ll be asked for confirmation in a popup window.

Note: if you change a sensor to “offline” it will no longer be displayed on the web interface. In order to reactivate it, you have to toggle it back to “online”.

Smart Sensor Recovery

This feature will be used **only** for the new **Smart Sensor** type. The firmware can be updated on these sensors automatically, and if the upgrade has failed for some reason and the sensor becomes unresponsive, with this option you can recover them to the default firmware. It’s not used by other sensor types.


Smart Sensor Recovery

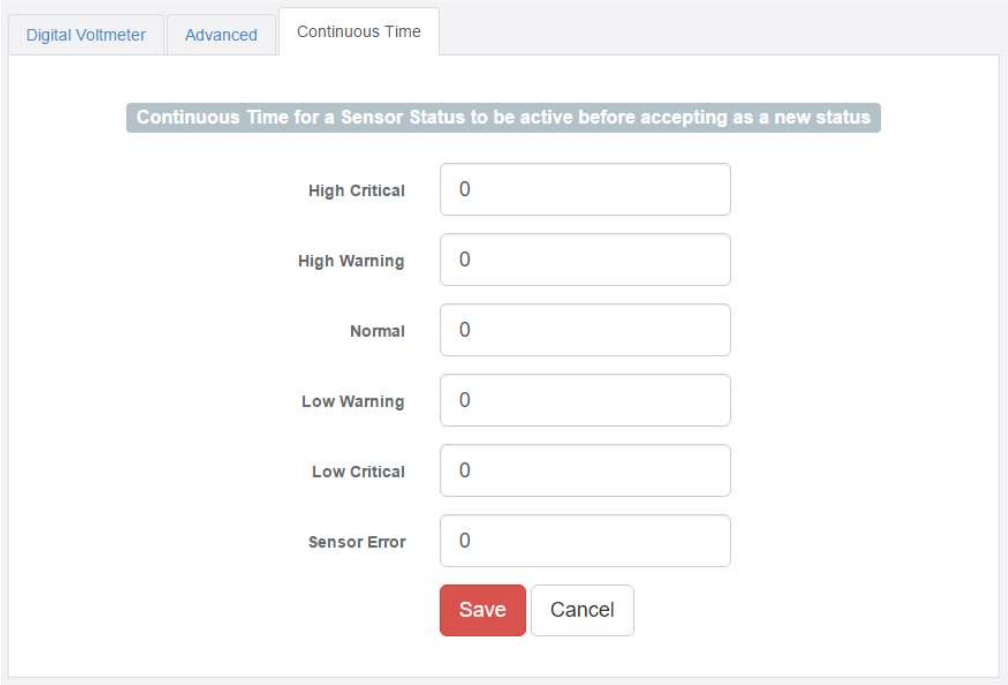
How to recover a smart sensor

1. Connect the smart sensor to any sensor ports on the master device.
2. Select the port number the sensor is connected to.
3. Press the 'Recovery' button to start the process and wait a few minutes.

Sensor Port: 1

Note:
If there's a difference between the version stored in the unit's firmware and the sensor’s firmware, it will upgrade/downgrade the sensor’s firmware upon powering up/reboot of the unit, or on sensor reconnection.
If you need to downgrade the smart sensor firmware, you can only do so together with the unit’s firmware.

Change Continuous Time



Continuous Time for a Sensor Status to be active before accepting as a new status

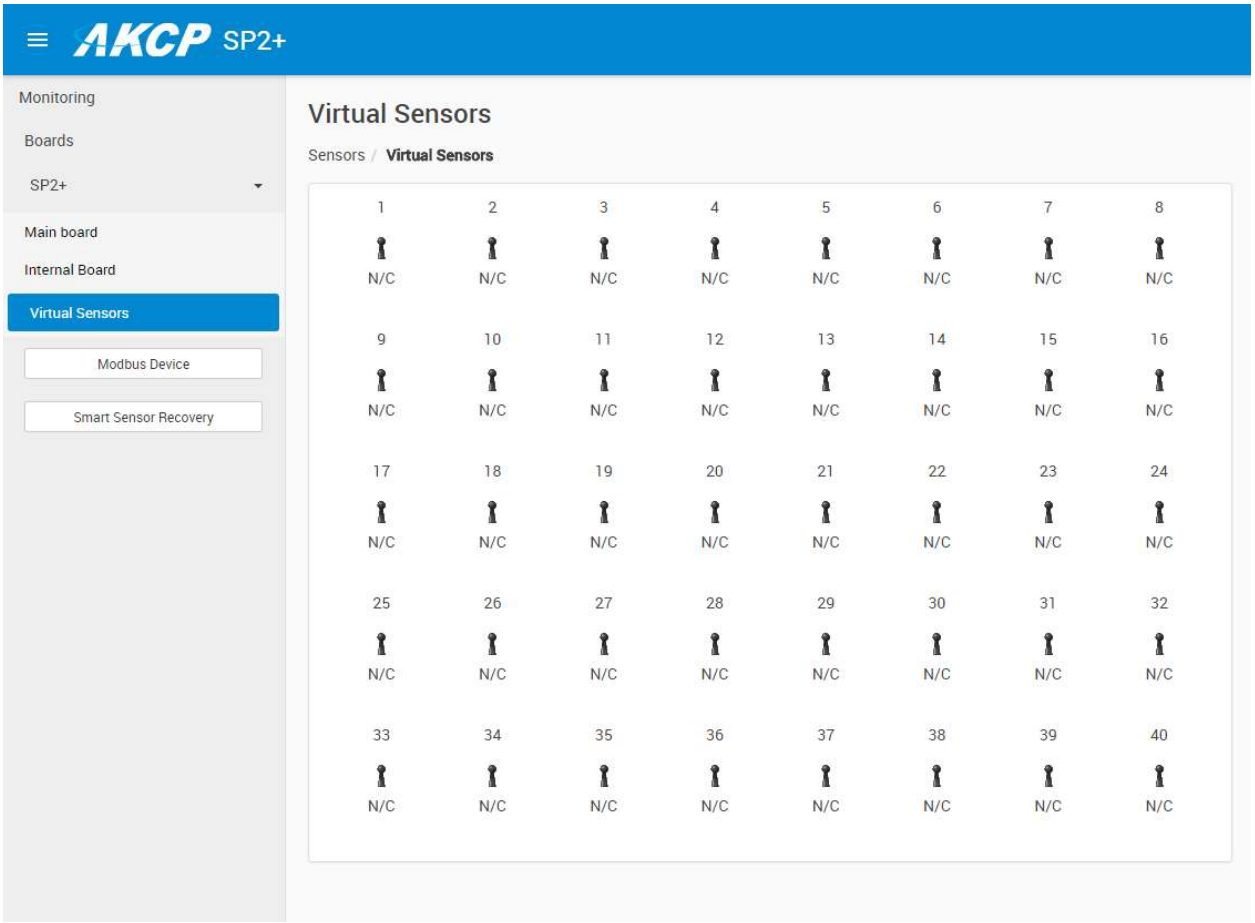
High Critical	0
High Warning	0
Normal	0
Low Warning	0
Low Critical	0
Sensor Error	0

The following advanced functions are for setting the time frame in which the system should delay a notification being triggered when a sensor gives a reading that exceeds the thresholds (high warning, normal, etc).

Continuous Time to Report High Critical: This helps to eliminate unnecessary messages during minor fluctuations. You can set the amount of time to delay a notification of a status change from high warning to high critical. Enter the time in seconds and press the “Save” button. The amount of time that can be entered is between 0 and 65535 seconds which equals approximately 18 hours.
Continuous Time to Report High Warning: As above but delays notification for “High Warning”.
Continuous Time to Report for Normal: As above but delays notification for return to “Normal” state.
Continuous Time to Report for Low Warning: As above, but delays notification for “Low Warning” state.
Continuous Time to Report for Low Critical: As above but delays notification for “Low Critical” state.
Continuous Time to Report for Sensor Error: As above, but delays notification being sent for sensor going into an error state.

Example: An airflow sensor or humidity sensor may have temporary drops in readings which are normal operating characteristics; a logical time limit is set to show abnormal conditions.

Virtual Sensors

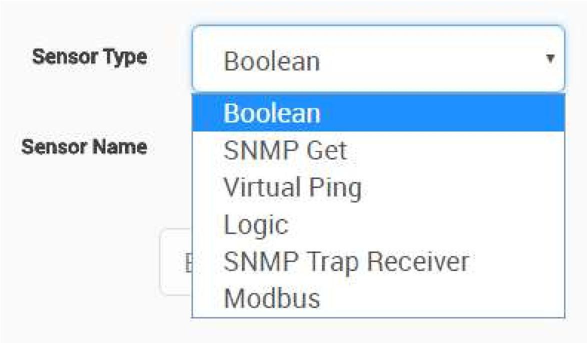


Virtual Sensors

Sensors / **Virtual Sensors**

1	2	3	4	5	6	7	8
N/C	N/C	N/C	N/C	N/C	N/C	N/C	N/C
9	10	11	12	13	14	15	16
N/C	N/C	N/C	N/C	N/C	N/C	N/C	N/C
17	18	19	20	21	22	23	24
N/C	N/C	N/C	N/C	N/C	N/C	N/C	N/C
25	26	27	28	29	30	31	32
N/C	N/C	N/C	N/C	N/C	N/C	N/C	N/C
33	34	35	36	37	38	39	40
N/C	N/C	N/C	N/C	N/C	N/C	N/C	N/C

On this page you can configure the Virtual Sensors. The first 5 sensors are free; if you need to use more you can purchase additional licenses (see the Licensing section in this manual).


Sensor Type: Boolean

Sensor Name

Virtual Sensors can be a very powerful tool in your monitoring system. On the SP2+ you can have up to 32 of these virtual sensors and they allow for a multitude of applications.

SNMP Get, sensor logic evaluation and ping commands among others are all possible from the virtual sensors. An example use of this could be to use the SP2+ as a probe manager. If you had a SP2+ and multiple sensorProbe devices they could all be monitored, mapped and alerted via the SP2+. You can perform SNMP Get commands on a server to monitor memory or CPU load, or you can ping network enabled devices and be alerted if they go offline.

Please note:
The Virtual Sensor Ping cannot ping an IP address on the VPN network.

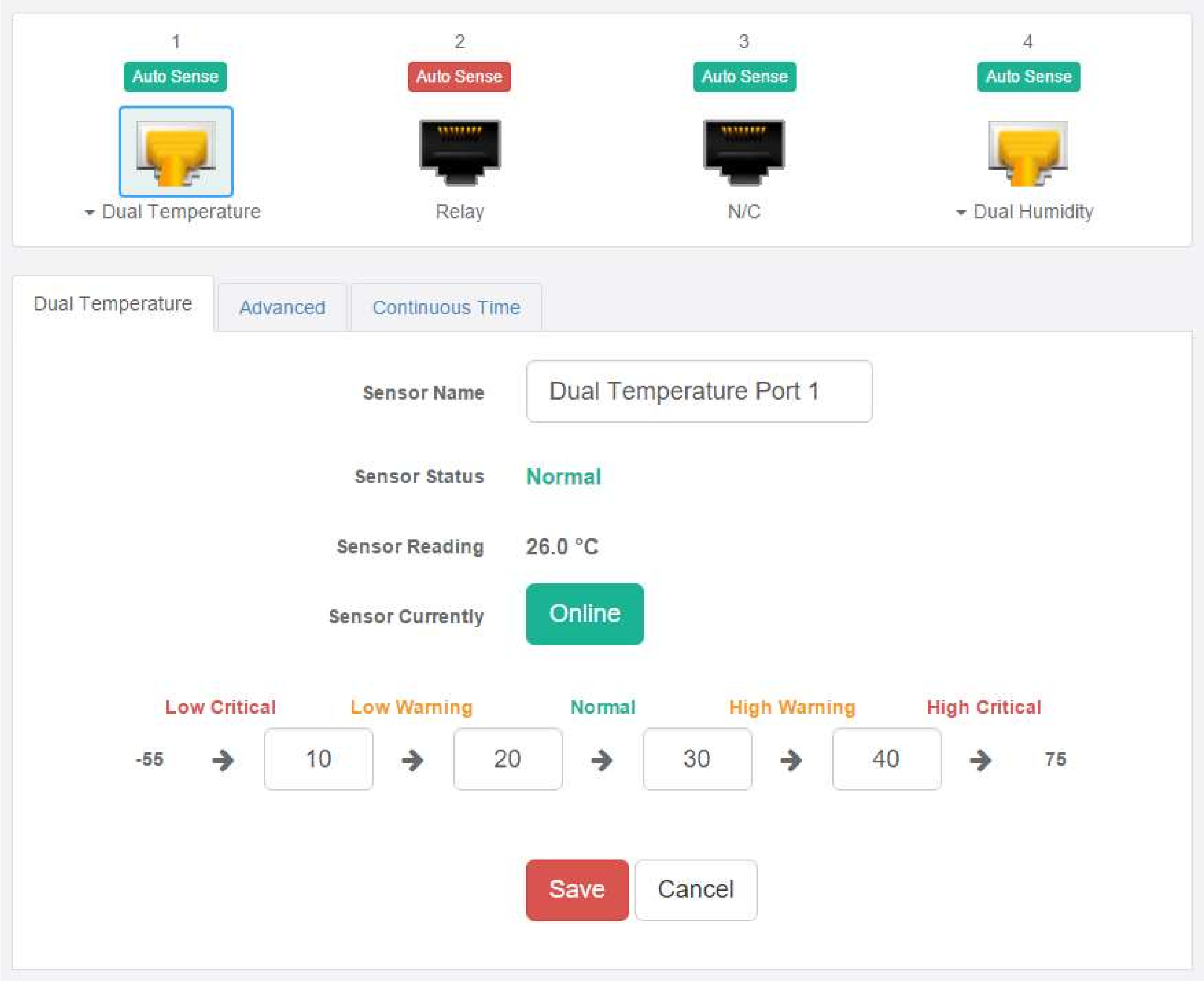
We'll explain more about the Virtual Sensors and how to configure them in the **Notifications manual**.

Example sensor configuration

Below we’ll show the configuration of 2 sensor types: the Temperature/Humidity and a Relay sensor. The configuration of these 2 types of sensors covers most settings that can be configured for other sensor types.

Temperature/Humidity Sensor

Click on the sensor port where the sensor is connected to open the sensor’s configuration.
Note: another way of accessing this page is to click on the sensor from the Summary page.



Sensor Name: Dual Temperature Port 1

Sensor Status: Normal

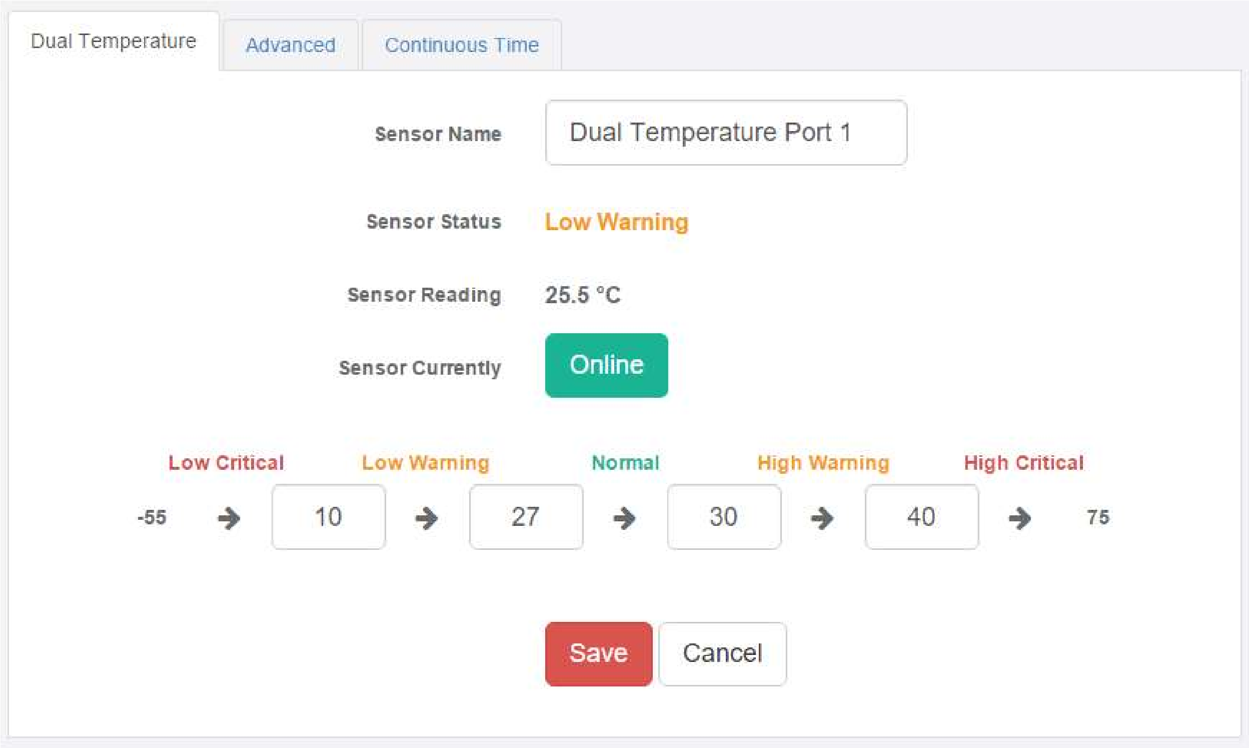
Sensor Reading: 26.0 °C

Sensor Currently: Online

Low Critical		Low Warning		Normal		High Warning		High Critical	
-55	→	10	→	20	→	30	→	40	→ 75

From this page you can carry out various operations. You can view the current status (normal, low critical, high critical etc), rename the sensor, put it offline and change the thresholds. In the screen shot above you can see the sensor is indicating a temperature of 26 degrees °C, and a status of Normal.

You can re-configure the thresholds for each sensor state. After changing a threshold value, click “**Save**”. In the next screen shot you can see that a threshold has been changed to 27 make a new “low warning” state, and along with it the sensor status has changed:



Sensor Name: Dual Temperature Port 1

Sensor Status: Low Warning

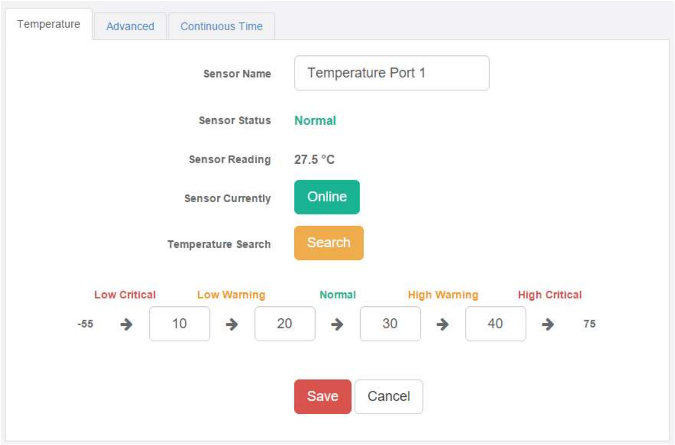
Sensor Reading: 25.5 °C

Sensor Currently: Online

Low Critical		Low Warning		Normal		High Warning		High Critical
-55 →	10	→	27	→	30	→	40	→ 75

Note: the Humidity sensor has the same configuration options as the Temperature sensor.

You might see a **Temperature Search** option for the connected Temperature sensors:



Sensor Name: Temperature Port 1

Sensor Status: Normal

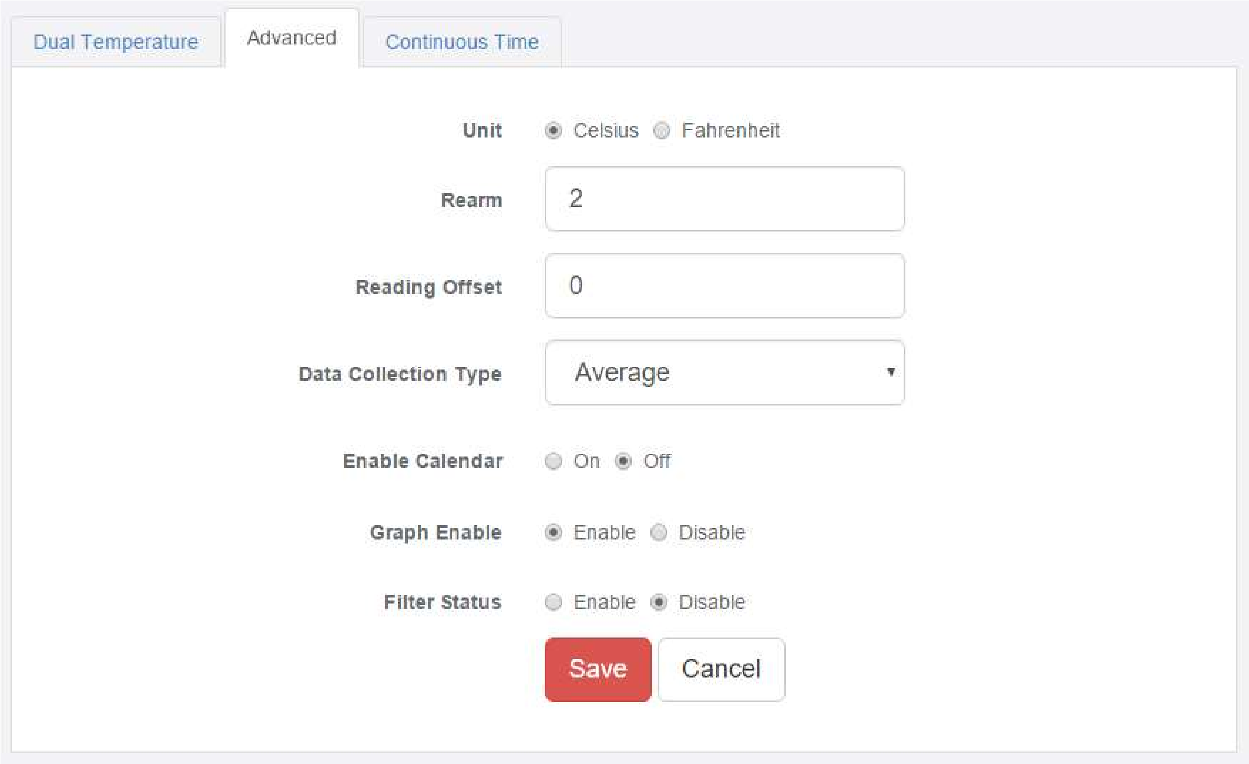
Sensor Reading: 27.5 °C

Sensor Currently: Online

Low Critical		Low Warning		Normal		High Warning		High Critical
-55 →	10	→	20	→	30	→	40	→ 75

What this button does is to search for new temperature sensors in a chain, if you’ve connected more than 1 sensor in a Daisy-Chain Temperature (DCT) sensor chain.
It is **not** available for Thermal Map Sensors (TMS).

Advanced sensor configuration for Temperature/Humidity sensors



Unit ● Celsius ○ Fahrenheit

Rearm 2

Reading Offset 0

Data Collection Type Average

Enable Calendar ○ On ● Off

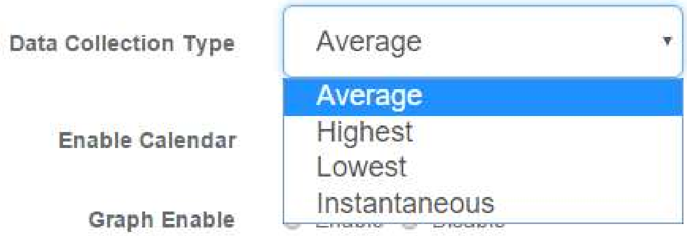
Graph Enable ● Enable ○ Disable

Filter Status ○ Enable ● Disable

Units: changes units from °C to °F or vice versa.

Rearm: The Rearm parameter is useful for sensors whose values can vary such as the temperature and humidity sensors.
It is used to prevent the sensor from rapidly changing between two states. For example if the **Warning High** threshold for the temperature sensor is set to 80 degrees and the sensor were to vary between 79 and 80 you could be faced with a very large number of emails, traps, and events logged. The Rearm parameter prevents this by forcing the temperature to drop by the Rearm value before changing the state back to normal. In this example, if Rearm is set to 2 then the sensor would have to drop from 80 down to 77 before the status would change from **Warning High** back to normal.

Reading Offset: The Reading Offset feature is a calibration tool. If you wish to calibrate the temperature sensor, for example, you could enter an offset value of 5. This would mean if the sensor reads 20 degrees then it would record as 25 degrees. This figure can also be a minus figure (e.g. -5 would show 15 degrees instead of 20).



Data Collection Type: This refers to the data collection from the sensor and how the data is then displayed on the graphs.
There are four options for the collection of data: Average, Highest, Lowest and Instantaneous. The default setting is “Average”.
When the data collection type is set to “Average” the averaged value between 2 graph intervals is stored and output graphs for the daily, monthly, and yearly all have the same size on the screen. For the daily graph, each data point on the graph is one data point collected from the sensor. But for the monthly and yearly graph, in order to display more data into the same size as the daily graph, some consolidation on the data is needed. One data point on the monthly and yearly graph is an average of the sensor data in a range.
The maximum and minimum values showing on the monthly and yearly graphs are the value of this consolidated data and not the raw data over that period of that time.
The When the Data Collection Type is set to the Highest setting then you will get the graphing output displaying the sensors highest average readings during sampling. This is the same for the Lowest setting (lowest average).
With the Instantaneous setting you can store the actual value of the sensor at the sampling interval without averaging.

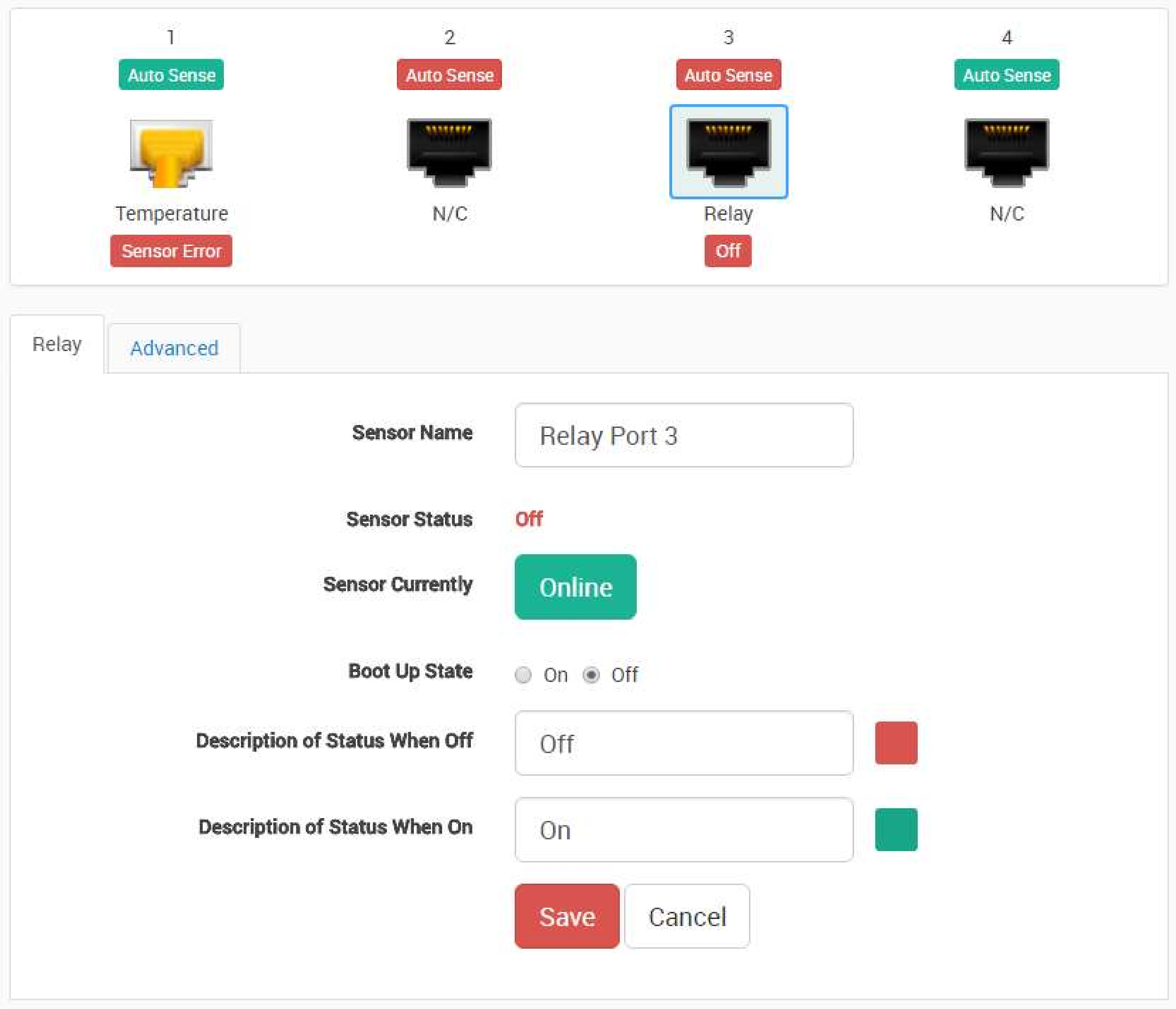
Graph Enable: In order to save the data from the sensors on the unit you will need to enable the Graphing feature on the unit. You need to change the Enable Graph to the On position and click on the Save button to enable the graphing. Note that you could also enable the graphing from the Summary page.

Filter Status: The Sensor Filter Status is a feature that you can Enable or Disable and when enabled will check the sensor status. If the status of the sensor changes very rapidly, then it will report how many times the sensor status changed, instead of having multiple separate entries in the syslog. When enabled, this will report the changes and status of a sensor only once.

Relay Sensor

Click on the sensor port where the sensor is connected to open the sensor's configuration. *Note:* another way of accessing this page is to click on the sensor from the Summary page.

You can directly see the Relay's current status below the sensor port.



Sensor Name: Relay Port 3

Sensor Status: Off

Sensor Currently: Online

Boot Up State: ○ On ● Off

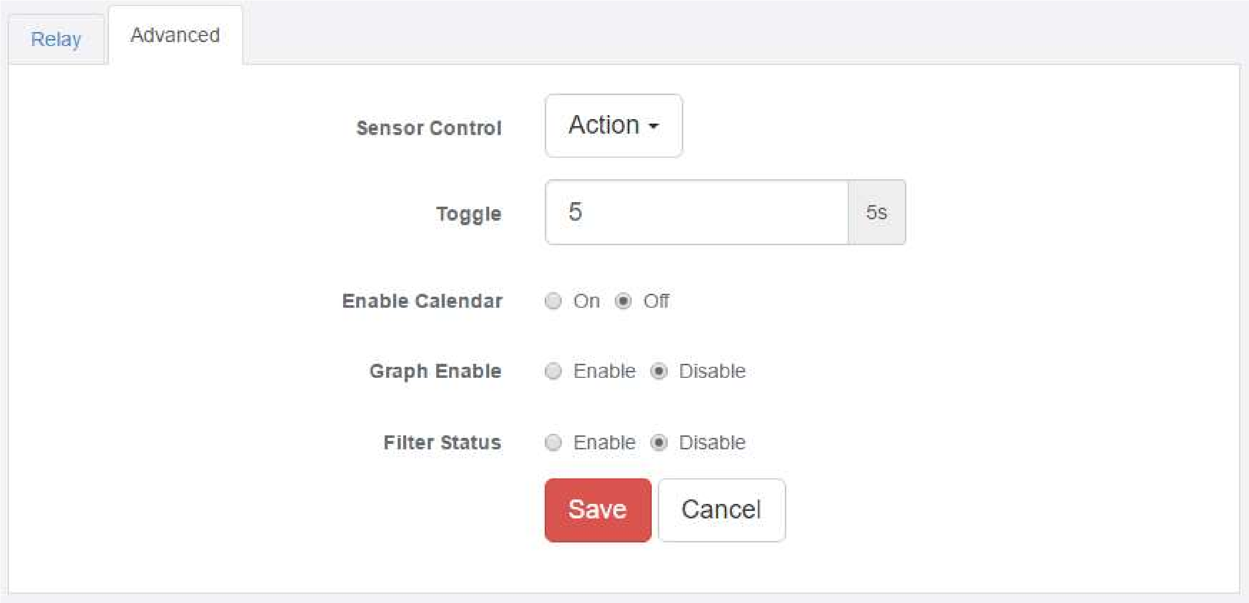
Description of Status When Off: Off 🟥

Description of Status When On: On 🟩

Boot Up State: You can change the state of the relay when the unit starts. The default is Off.

Description of Status When Relay Off/On: These fields are the custom description, which will be displayed in the Relay Status field when the relay state is off/on. The same text is listed as one of the relay actions used to turn off/on the relay. Examples for this field are Close/Open Door, Turn Pump Off/On, Turn Light Off/On, etc.
Color: You could assign a custom color for the Off/On status: click on the color and the color picker will be shown.

Advanced sensor configuration for Relay sensors



Sensor Control: Action ▾

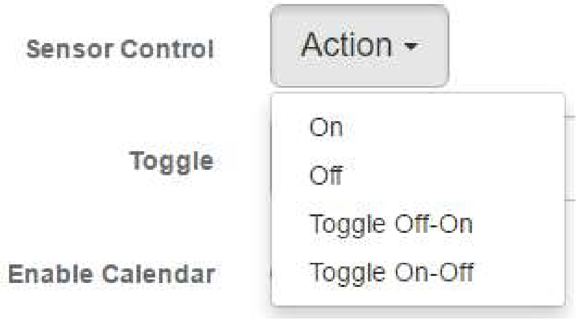
Toggle: 5 5s

Enable Calendar: ○ On ● Off

Graph Enable: ○ Enable ● Disable

Filter Status: ○ Enable ● Disable

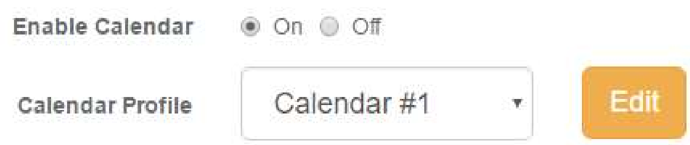
Sensor Control:



This button allows you to manually control the relay by controlling the cycle of the relay in an on-off-on or an off-on-off cycle. You can also set the “Toggle” (Cycle Time) here in seconds.

You don’t need to change an option to be able to link the relay to an action.
The following actions can be chosen in an action: Turn on until sensor normal, turn off until sensor normal, cycle the relay, turn on until acknowledged, and turn off until acknowledged.
We’ll explain more about these options in the Notifications manual.

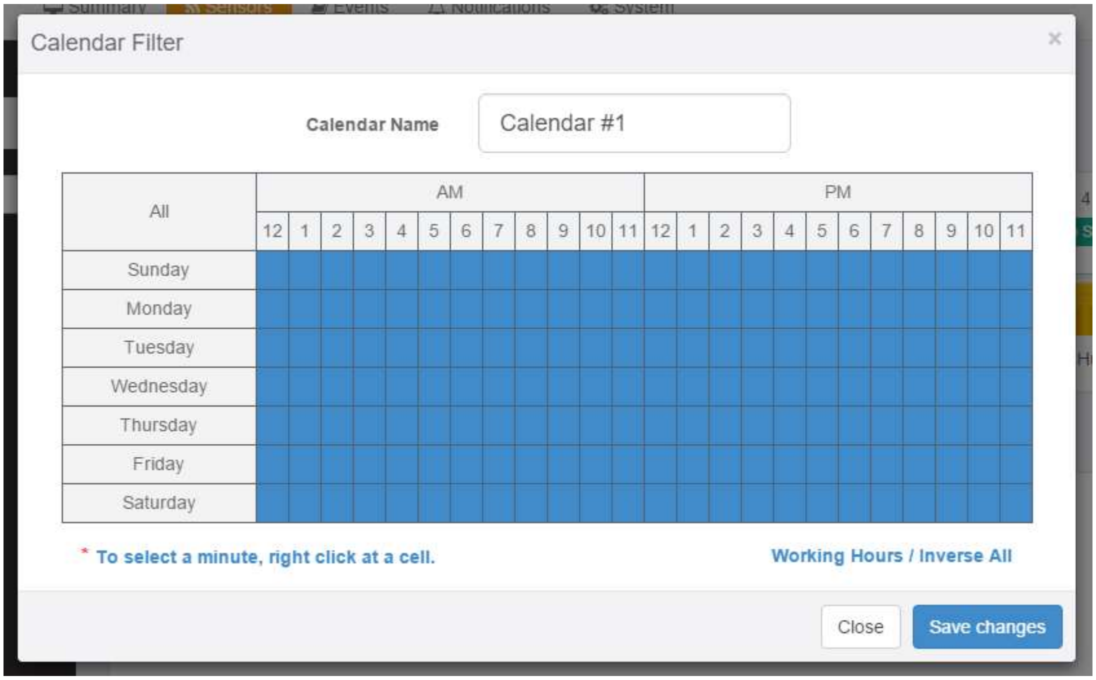
Enable Calendar: Allows you to setup a *Calendar Profile* for what days and times you want or do not want the relay to be active.



Enable Calendar ● On ○ Off

Calendar Profile: Calendar #1

Click on the **Edit** button next to a selected calendar to modify it.

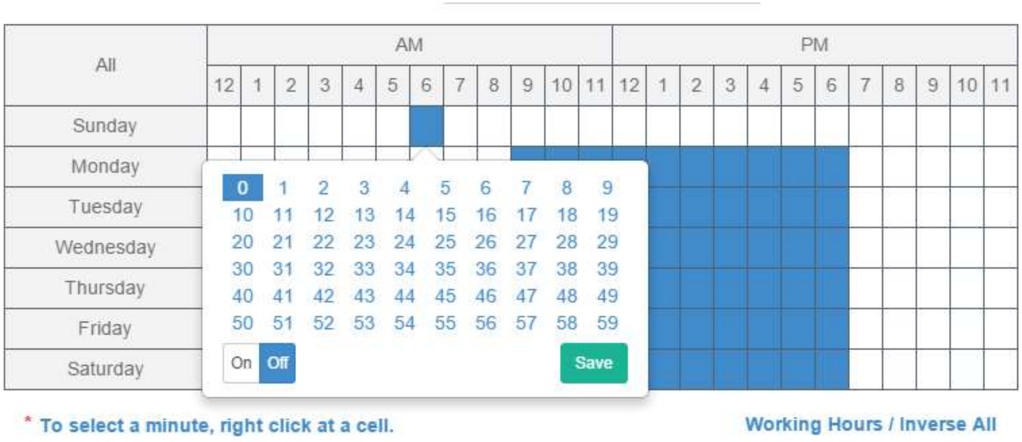


Calendar Name: Calendar #1

All	AM												PM											
	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Sunday	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
Monday	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
Tuesday	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
Wednesday	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
Thursday	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
Friday	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
Saturday	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦

* To select a minute, right click at a cell.

Blue cells means that the notification is on, white cells means it's off.

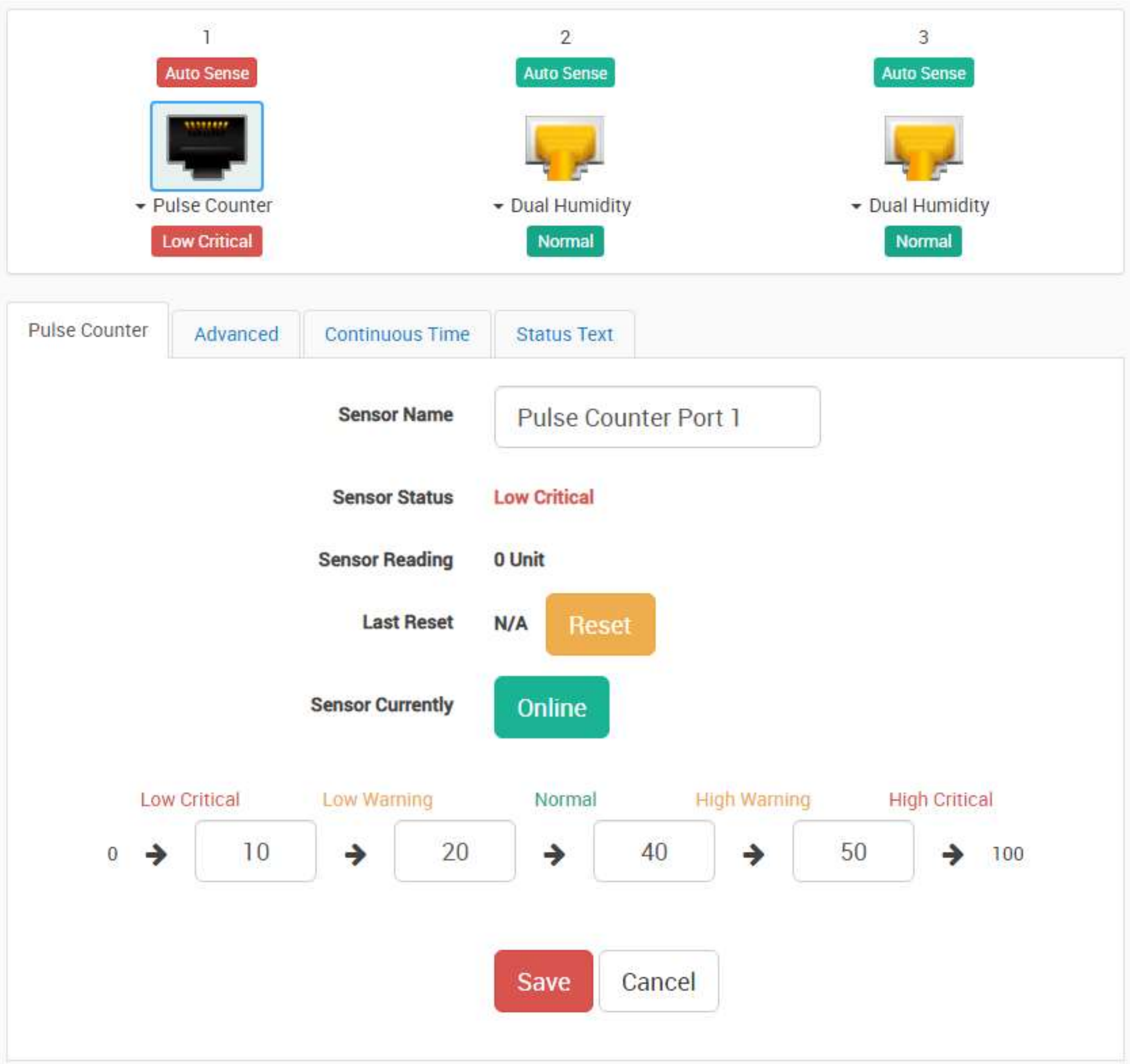


* To select a minute, right click at a cell.

Working Hours / Inverse All

You can quickly select the Working Hours only, and specify a custom schedule down to minutes by right clicking on a cell.

Pulse Counter sensor



Sensor Name: Pulse Counter Port 1

Sensor Status: Low Critical

Sensor Reading: 0 Unit

Last Reset: N/A

Sensor Currently: Online

Low Critical	Low Warning	Normal	High Warning	High Critical
0 → 10	→ 20	→ 40	→ 50	→ 100

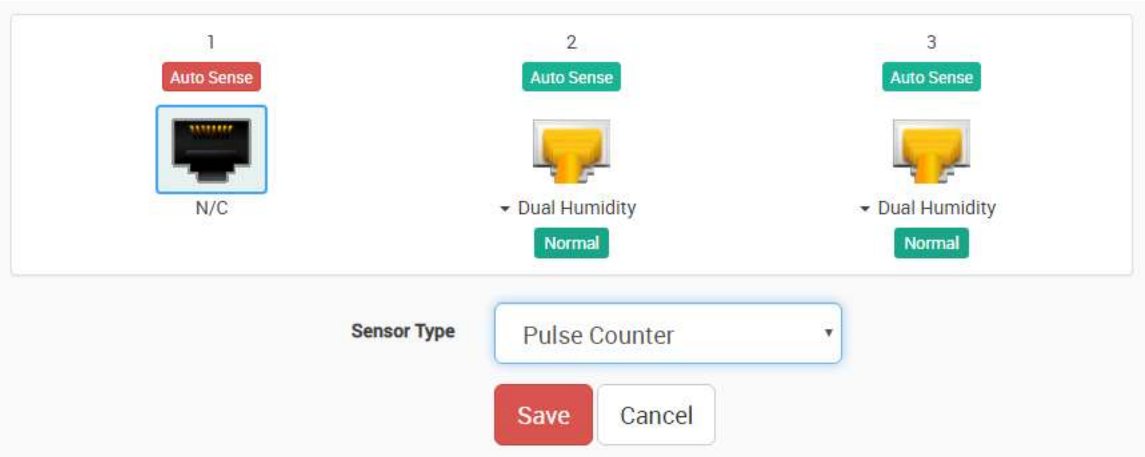
The pulse counter is available on the SP+ platform, as of firmware version 1.0.4967. It provides:
- accumulated pulse count
- flow conversion of the pulse count

It can measure up to 1000 pulses / sec (1 Kilohertz).
Normally this sensor should be used with some external sensor which outputs pulses.

Sensors that could work: basically any switch type sensor, and any custom sensor that could generate a pulse signal. For example Wind speed sensor, Electricity meter etc.

For example, you can connect the output of a third-party water flow sensor in the market to our sensor port.
The specs of those sensors will indicate how many pulses equal to, for example 1 liter: 100 pulses = 1 Liter.
Then you can set the "Number of Pulses per Unit" to 100, and change the unit to L.
Then the sensor value will be changed according to the output of the water flow sensor which is connected to the sensor port.

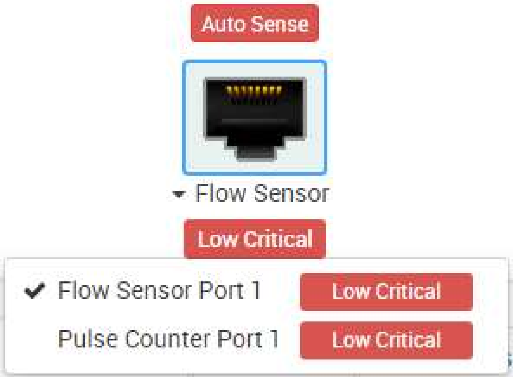
How to use the pulse counter?



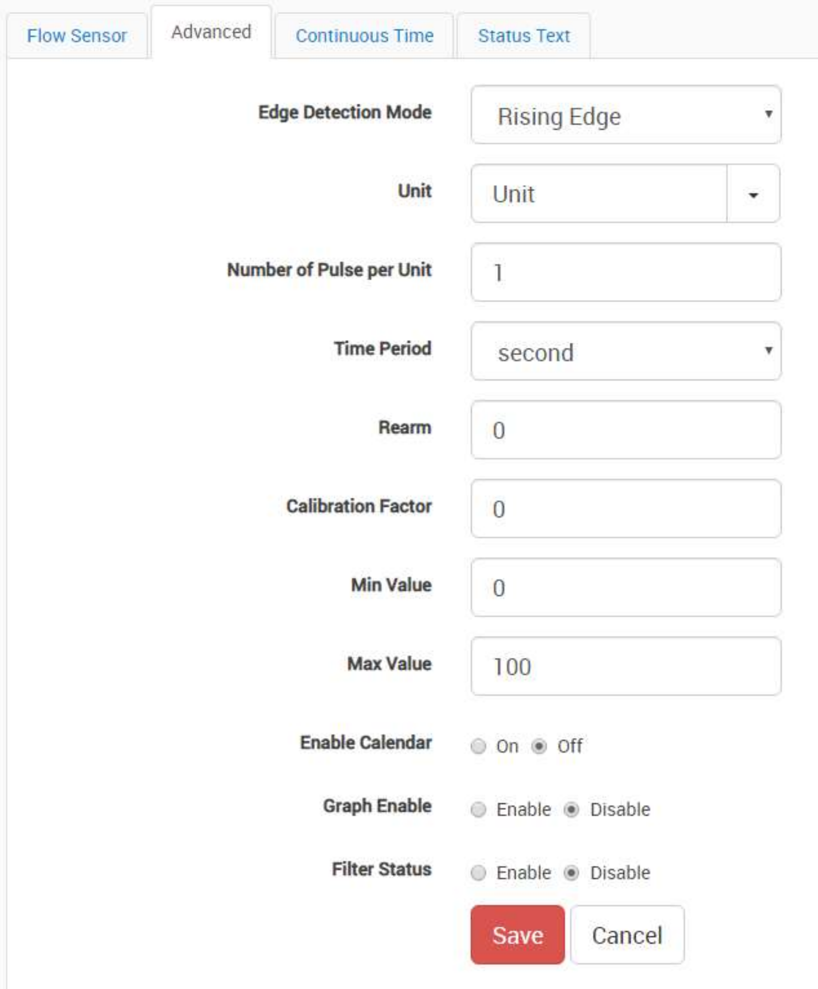
Sensor Type: Pulse Counter

The sensor is designed to be used by disabling the Autosense and connecting an external sensor to the sensor port. This sensor will detect changes on the Data pin (Pin 1 of Sensor Port).

If there's changes:
- Flow Sensor value will show rate of the change in Unit / Second
- Pulse Counter will accumulate the pulses since the sensor is set to online



To set it up, disable Auto Sense on a sensor port and select the Pulse Counter sensor type from the list. This will give a dual sensor with Flow Sensor and Pulse Counter.



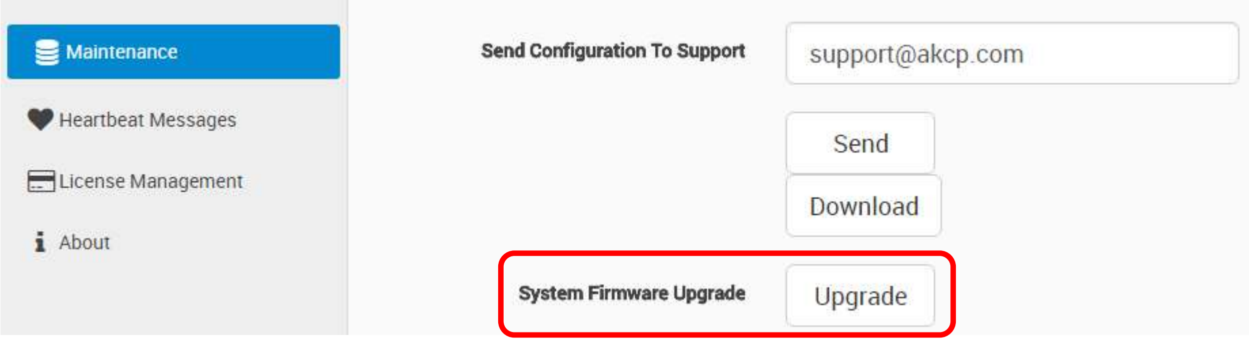
Edge Detection Mode	Rising Edge
Unit	Unit
Number of Pulse per Unit	1
Time Period	second
Rearm	0
Calibration Factor	0
Min Value	0
Max Value	100
Enable Calendar	○ On ● Off
Graph Enable	○ Enable ● Disable
Filter Status	○ Enable ● Disable

In the Flow Sensor there is "Number of Pulse per Unit" in the config.
You can use this value to adjust the sensor reading to match the real-world value.

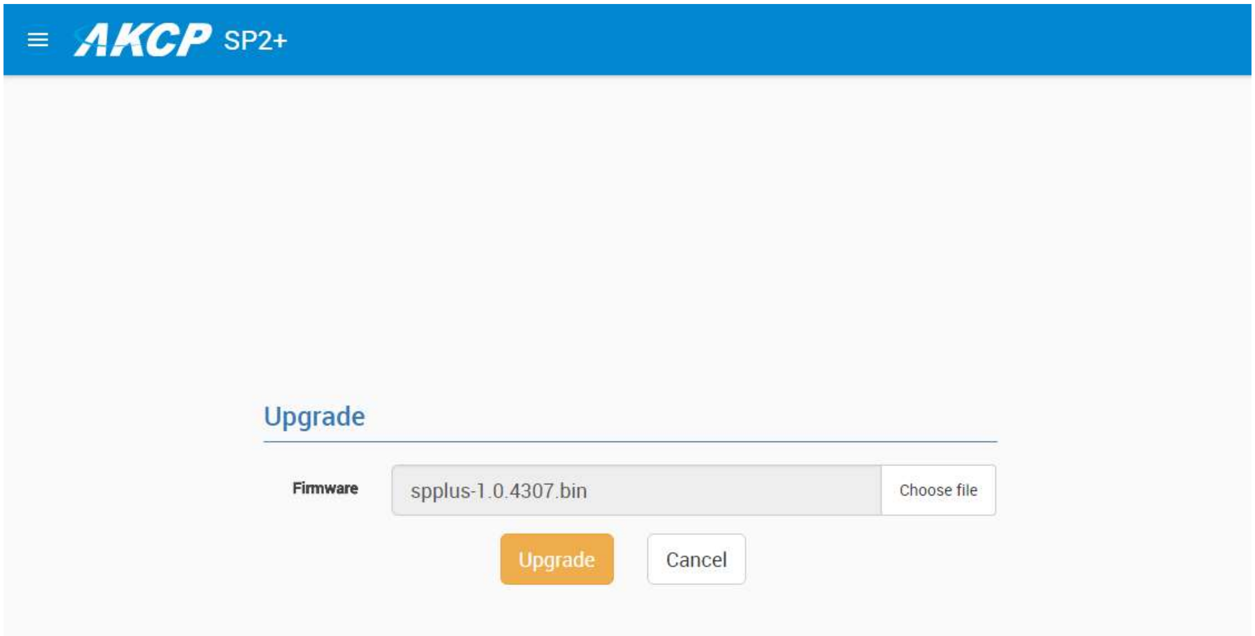
Dry contact will also work but only to count the pulses. If you want to test for the rate accuracy, you'd have to test with something that can generate a wave signal, like using an oscilloscope to generate wave form and plug it to the sensor port.
But the general idea of this sensor is that it will show the rate of received pulses and also count it.

Firmware upgrade through the Web UI

The firmware upgrade process is very simple and straight-forward.

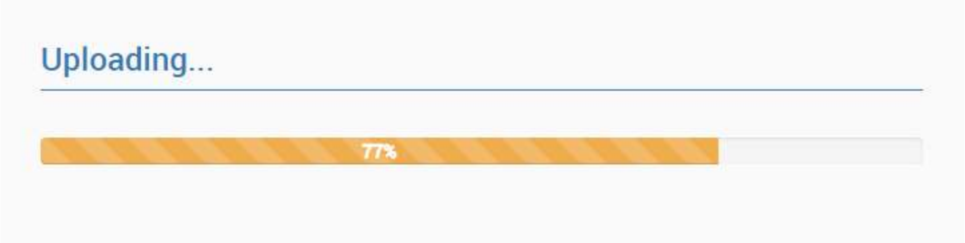


Open the **System/Maintenance** page and click on the **Upgrade** button at the System Firmware Upgrade section.

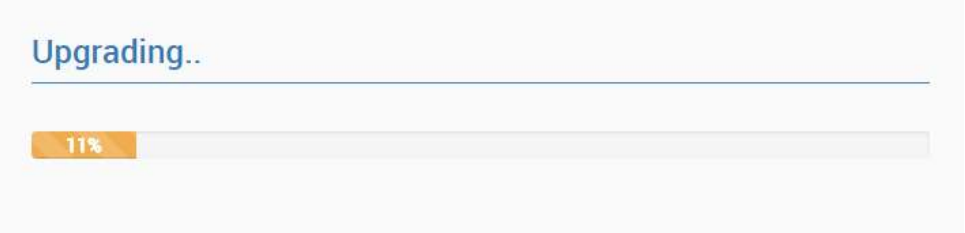


This will load the Upgrade page. Choose the firmware file from your PC and click on **Upgrade** to start the process.

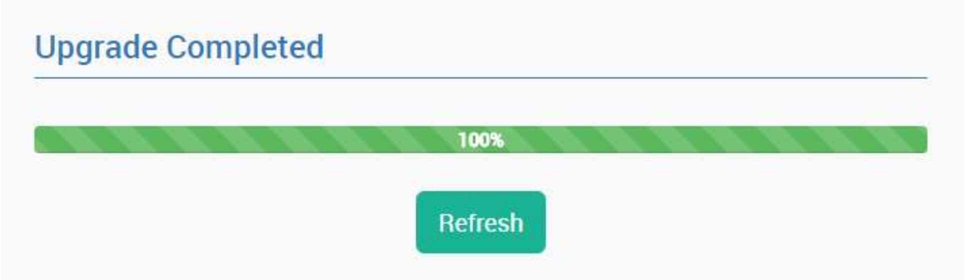
Important: There are two separate .bin files included in a firmware update package. One for the F4 units and one for the F7 units. The .bin file for the F4 units is named spplus-1.0.xxxx.bin and the .bin file for the F7 units is named spplus_f7-1.0.xxxx.bin. If you try to upgrade your unit with the wrong .bin file, the firmware upgrade will fail, so please make sure you use the correct file for your unit type.



First the file will be uploaded to the unit…



…then the upgrade process will run. The whole process can be done in a few minutes.
The Power/Ethernet LED will be red during the upgrade.



The unit will reboot at the end of the upgrade. Click on the **Refresh** button to reload the Web UI.

Network ports used by SP+ units

Below we list the ports used by our SP+ units. Most of them are needed for external communications with APS, and to use network features.
Most ports are user configurable, these are the default ports.

Main ports:

- 5000 TCP for RPC with APS - note: not fully user configurable
- 161 TCP/UDP for SNMP
- 80 TCP for HTTP of Web UI

Other ports:

- 123 TCP for NTP (Network Time Protocol) - note: port is not user configurable
- 162 TCP/UDP for SNMP Trap
- 25 TCP for Email SMTP (if used)
- 1194 TCP/UDP for VPN (if used)
- 443 TCP for HTTPS of Web UI
- 502 TCP for Modbus TCP (if used)

FCC Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

Please contact support@akcp.com if you have any further technical questions or problems.

Thanks for Choosing AKCP!