www.AKCP.com

AKCPro Server HTML Manual

Table of Contents

1. Introduction

AKCPro Server (APS) is our world class central monitoring and mangement software, suitable for a wide range of monitoring applications. It is free to use with all AKCP devices. You can monitor your infrastructure, whether it be a single building, or remote sites over a wide geographic area. Integrate third party devices with Modbus, SNMP and ONVIF compatible IP cameras.

This manual is dedicated to the new HTML5 interface of APS.
Most APS features (98%) are also on the HMTL5 UI, and configuring them matches the Windows client (wx). You may check our earlier APS manuals if you need more help with the Windows client.

Differences and advantages over v12 series

- APS is now AKCPro Server and not AKCess Pro Server. This change will also result in the installation- and user data paths being different, so make sure to review and change your custom scripts if you hard-coded the APS paths in it.

- The biggest difference is that now there's a built-in web server (HTML UI) in v13 which provides access to APS management without installing a separate APS client program. You just need a HTML5 compatible web browser running on any device to be able to manage your APS installation (more on this feature later).

- Only APS v13 supports new sensors such as ILPM, Thermal Map.

- APS v13 code has been rewritten on a more modern compiler so it has better performance on modern OS's.

- APS now has a memory dump feature (which can be sent to Support and the engineers) that will help us to better troubleshoot and fix issues.

- Further development and new features will only be added to the HTML5 interface. *Note:* some existing features are missing from the HTML UI but the feature coverage is ove 98% compared to the Windows client.

- APS is now fully Unicode aware; you can specify and use Unicode characters (for example for path names, action names)

- Backup & Restore feature has been rewritten and should produce smaller backups when video recording is used (it doesn't include the Reserved folder in the backup).

- The graph library is new in APS v13 and the feature has been rewritten.

- When you uninstall APS v13, the default option is to keep your user data and settings (but you can choose to remove them).

- New licensing features for APS v13:

- The product still requires activation for using more than one sensor of each type, but the demo usage now doesn't requre online registration with email. APS will use an offline Default license.

- If you already have a paid Active license and online access, APS will automatically activate itself after installation. No need to run the Activation Wizard on first use.

- Now you can also activate using a license file that has been sent over email and no need to copy-paste the long activation key (but this method is also still supported).

AKCPro Server Online Demo

If you need to study the graphical user interface and features of the v13 AKCPro Server you can log in directly to our online demo server.
The demo includes a step by step walkthrough of the user interface and introduces many of the new features you can find in our latest HTML5 version of the software.
This is not only a good training tool we highly recommend you and your staff review along with the manuals, but also a nice option if you need to provide a demonstration to your customers on the server software.

https://akcpcloud.ddns.net:208

uName : demo
pWord : yCkVeHdz

2. Installation and upgrade

In this section of the manual, we'll show you the steps necessary for installing AKCPro Server (APS) Windows version on a computer.
We will also provide the system requirements, and a comparison between the internal and external databases, to help you choose the best option for your organization.

Note: some of the pictures shown are from earlier versions but the process hasn't been changed since; it's the same for the current version.

System Requirements

AKCPro Server - Minimum Specifications

CPU	Dual-Core CPU is recommended Intel Xeon 3050 2.1 GHz or higher AMD Opteron 1218 2.6 GHz or higher
RAM	1 GB (2 GB or more and dual-channel recommended)
Network	Ethernet 100/1000baseT (1 Gbit recommended)
Graphics Card	Onboard or external, minimum 1024x768 resolution, 16 bit colors
Hard Disk	Minimum 100 Gbyte free (depends on the number of servers, cameras, rules and logging settings), NTFS file system (on Windows) Recommended: 7200 RPM or faster SATA/SAS HDDs and RAID1/RAID5
Operating System	Minimum: Windows 7 64 bit or Windows Server 2008 R2 Recommended: Windows 10 64 bit or Windows Server 2016 Note: Windows Server Core versions are not supported AKCPro Server also supports running on Linux

Please note: Camera recording and playback performance depends on your CPU speed, Memory, Network Bandwidth and the frames per second (FPS) selected.

Please also note: The AKCPro Server can support up to a maximum of 1,000 data points before you need to upgrade to the full SQL database as indicated on our price list. You need to consider the data points and not just total sensors. For exmaple our dual temperature humidity sensor would count as two data points.

Network Specifications

The communication between the AKCPro Server and the client units is based on standard TCP/IP protocol. As long as they can connect to each other, you can add your units to the AKCPro Server. This depends on your network administrator to design the network topology. Here is the communication protocol used in our system:

> ➢ Communication from the AKCPro Server to the client units:
> **SNMP (Default Port 161 UDP)**

> ➢ Communication from the client units to the AKCPro Server:
> **RPC (Default Port 5000 UDP/TCP)**

The APS installer will automatically add firewall rules to the Windows Firewall upon installation, and also a VPN rule after you enable the VPN feature. However if you use a third party firewall software (or hardware) you must make sure that the required ports are open on your firewall.

If the client unit is behind a NAT firewall, you will have to set up port-forward to your unit to Port 161. For the AKCPro Server, you will have to do port-forwarding to the Server's Port 5000.
If the client unit and the AKCPro Server are on a different LAN, you can set up Virtual LAN to make these nodes able to talk to each other over the switch.

Step-by-step Installation

The installation process in short:

- ➢ Create directories and shortcuts
- ➢ Copy program files to the disk
- ➢ Install NTP server and WinPcap programs (third party software)
- ➢ Set up and populate the database (internal or external)
- ➢ Stop (if running) and restart the APS service
- ➢ Add firewall exceptions automatically to the Windows Firewall

Step-by-step installation procedure:
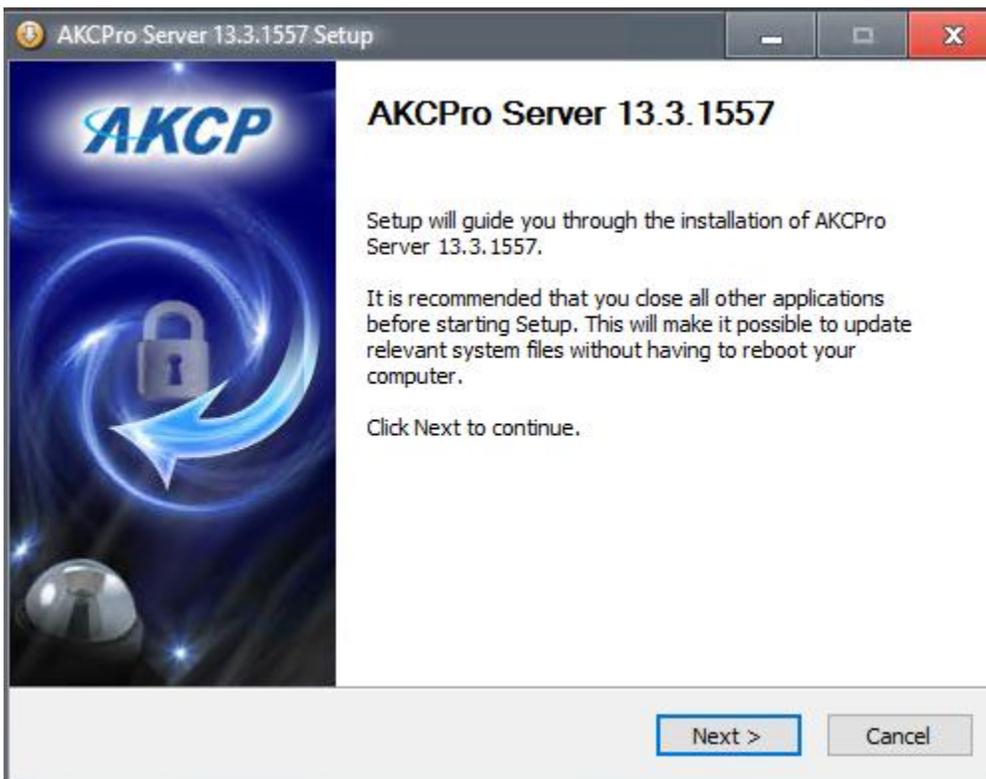
Start the installer. After its contents has been verified, click **Next** to continue.
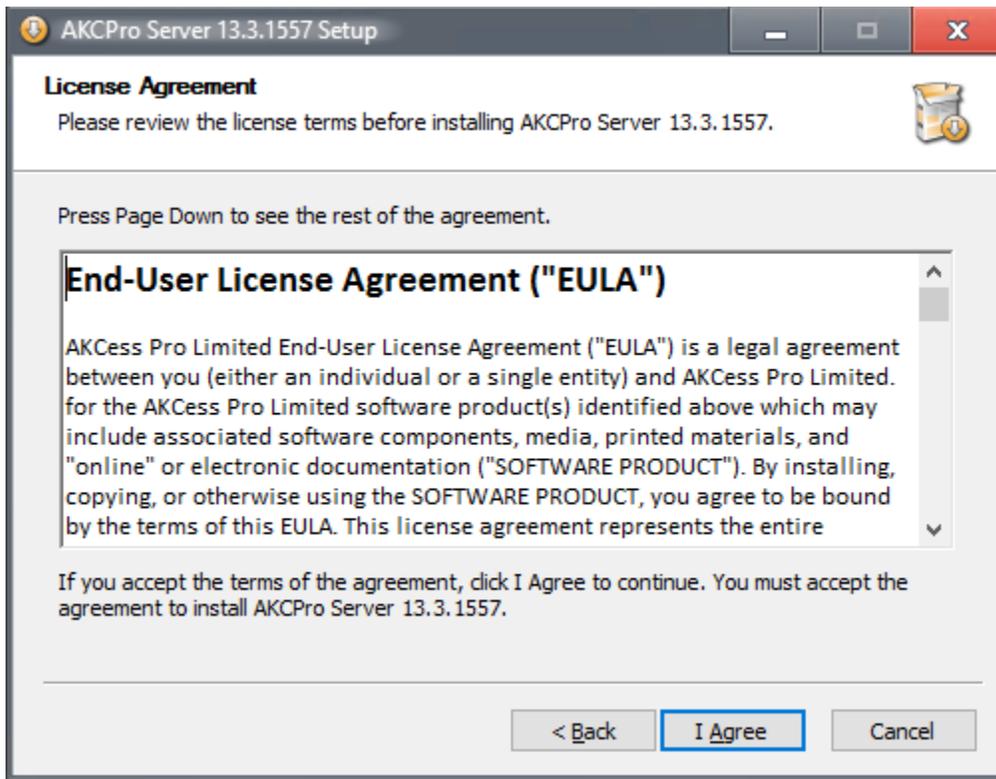
Read the EULA carefully, and accept it by clicking "**I Agree**".
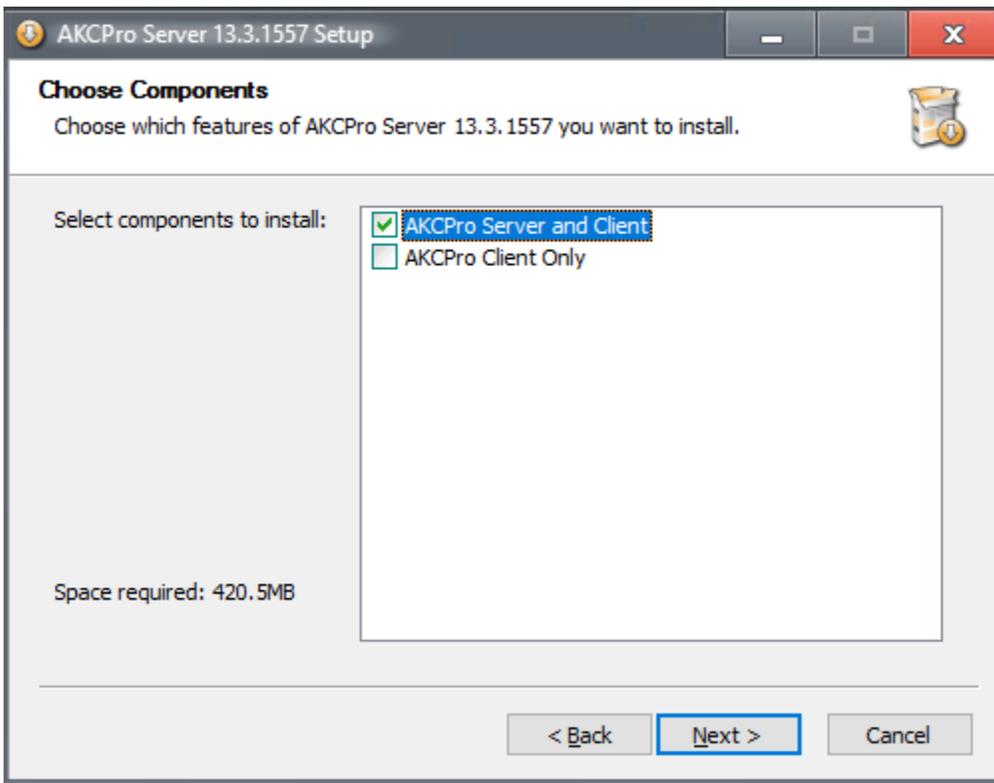
Choose which APS components you would like to install on this computer:

- ➢ *Server and Client:* all services and databases will be installed, in addition to the local Windows AKCPro Client
- ➢ *Client only:* only the Windows AKCPro Client components will be installed
  Normally you don't need to install this client as the HTML interface can be accessed remotely from a web browser, but this is still provided for compatibility (see below for more details).
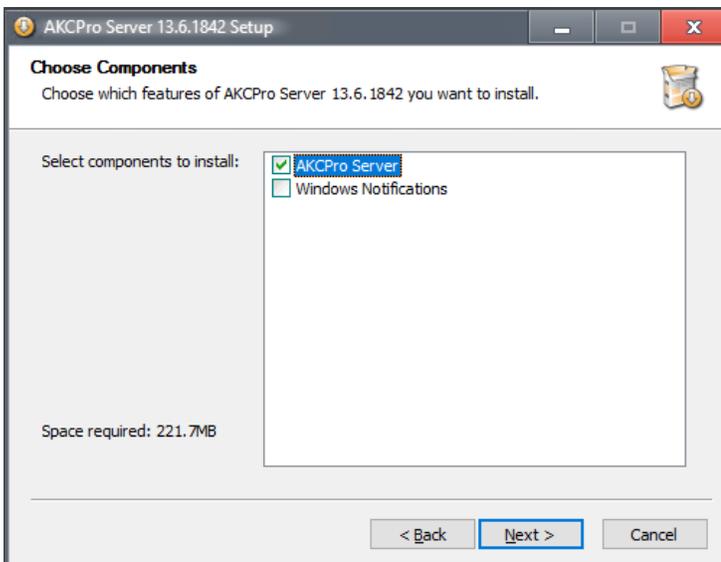
Important Note: on newer APS installations (after the 13.4.1634 release) the **Windows Client (wx) is removed** from the installation package and **only the HTML server** components are installed. During upgrade if a previous Windows Client installation is found, it will be removed and you need to manually reinstall this Client component from a separate installation package.

We'll show you some installation examples below.

1. Install Server with Client - same as in earlier APS versions, and you can manage APS locally with both the Windows client and the HTML5 UI (available until 13.4.1634 release)
After the 13.4.1634 release, the AKCPro Server only installs the HTML5 components.

2. Install Windows Client only - same as in earlier APS versions, and you can manage APS locally with both the Windows client and the HTML5 UI

3. Access the Server from web browser from another device (mobile or desktop) - you don't need to install anything on your device, just open the Server's URL and log in to manage it

1. Install the AKCP Pro Server with Client - same as in earlier APS versions, and you can manage APS locally with both the Windows client and the HTML5 UI.

Server Computer

PC

Laptop

Smart Phone
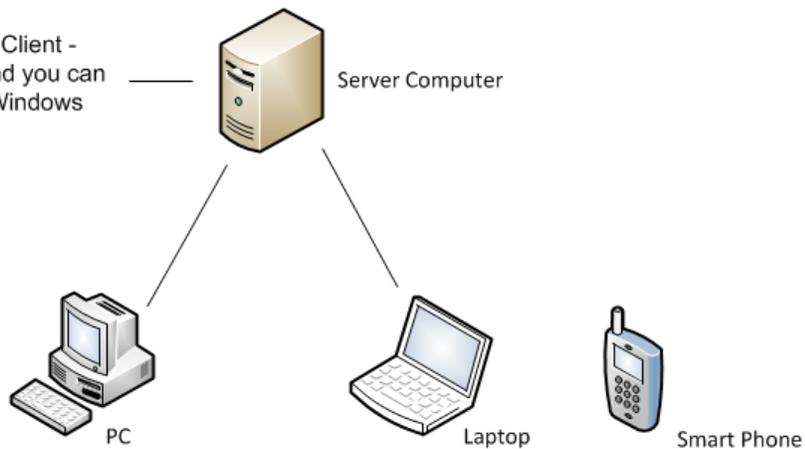
2. Install Windows Client only - same as in earlier APS versions, and you can manage APS locally with both the Windows client and the HTML5 UI.

3. Access the Server from web browser from another device (mobile or desktop) - you don't need to install anything on your device, just open the Server's URL and log in to manage it.

Click on **Next** to continue.
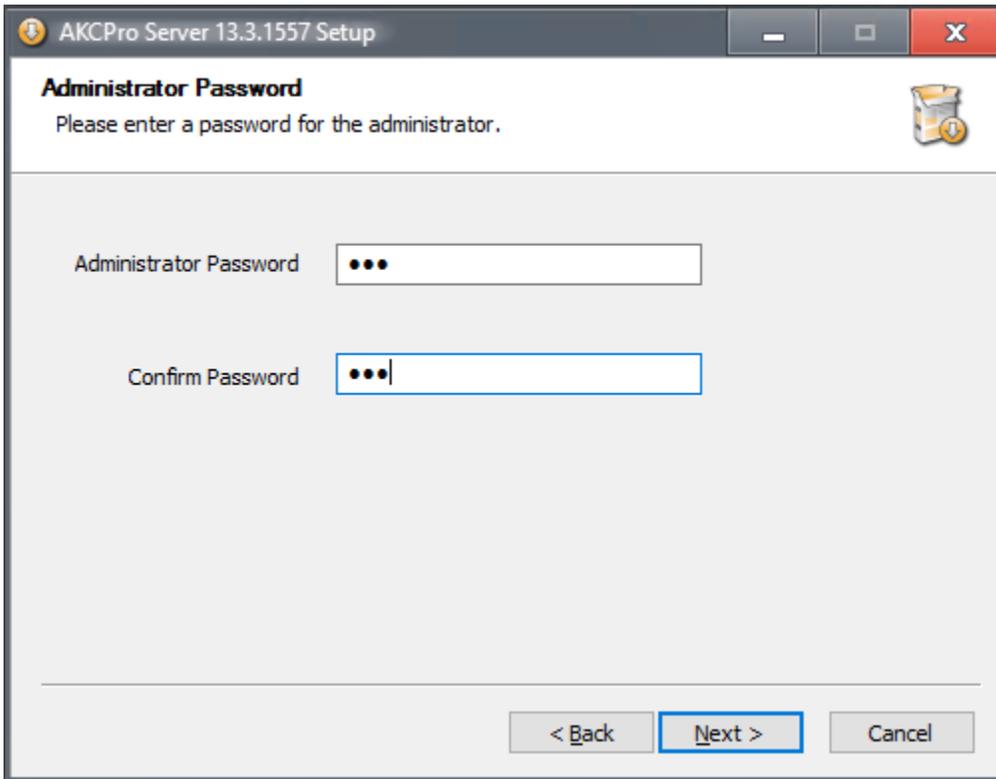
Provide an administrator password for the main APS user (admin). Be sure to keep it in a secure place.

You'll need to specify the admin password upon each version upgrade; the *admin user password will be reset*, so you should be using the same password if you intend to keep it.

In case you forgot this password, you could still gain access to the server:

➤ By using the Windows AKCPro Client that's installed on the server's console, and using the "local machine" option (more about this below)
➤ By reinstalling/upgrading APS; you'll be prompted for the admin password again, as shown here

Click on **Next** to continue.
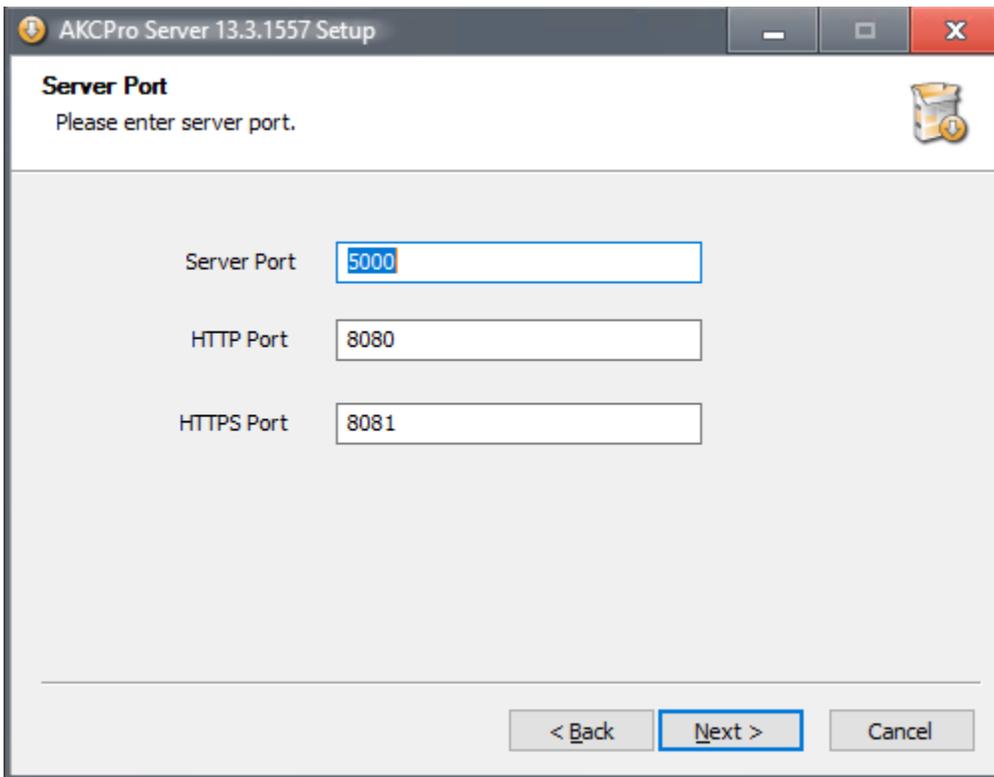
If you're installing the full server, then the installer will ask you for server ports.
The Windows client installation doesn't need the ports set up because it's a server component.

Ports configuration required for:

➢ APS HTML Web UI (HTTP, HTTPS): you can access by https://127.0.0.1:8081
➢ APS RPC server port (which is used by the monitored devices to communicate with APS)

Click on **Next** to continue.

If there are no port conflicts, the installer will proceed to the next step.

However, if some ports are in use, the installer will notify you about the port conflict and you cannot proceed until you resolve the issue by changing the problematic port or ports (see below).

You will need to change the port numbers if the ports are in use by other applications eg. Oracle database server Web UI. The installer will check and notify you if some ports are in use:
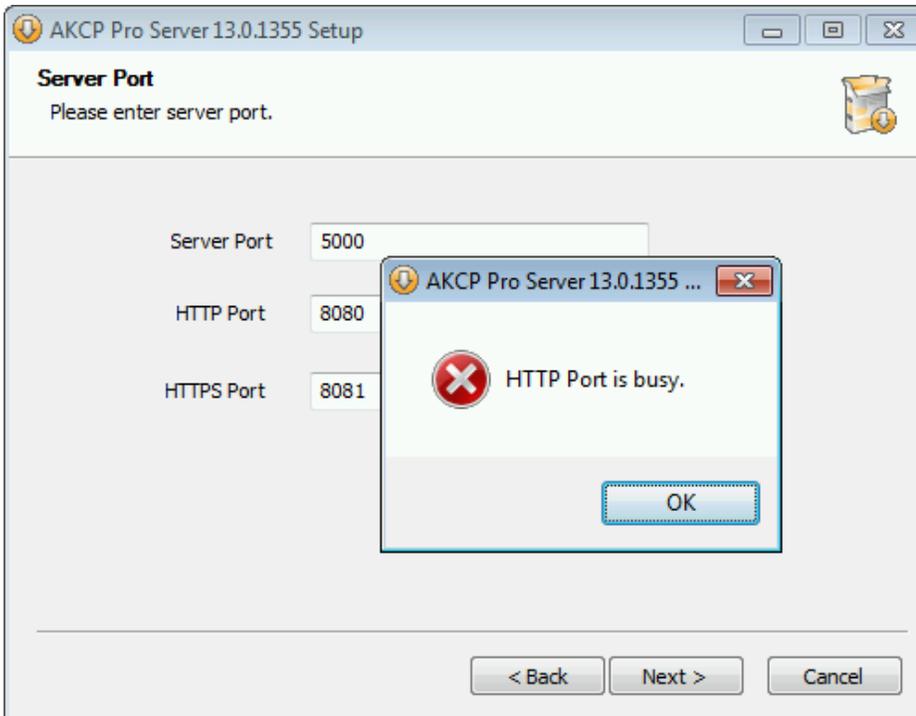
This message indicates that another application is using this port.

You can either manually change this port for the APS-HTML interface or either stop that 3rd party application to use this port.
A way to figure out which application are using a specific port is to open CMD prompt terminal (as administrator) and run the following command:

```
netstat -abno | findstr 8081
```

Where you should replace 8081 by the problematic port number.
In the results, the last row is the process ID (PID) of the program that's using this port - you can then open the Windows Task Manager and search for this PID to find the executable's name.

On Linux based APS run the following: `netstat -abno | grep -e ':8081' -A1`

Important Note: You wil need to ensure that your firewall, security, or antivirus software is not blocking these ports noted above, or again that any other application running on the computer is not using these ports, for example Skype which can run on port 8080, etc.

Proceed with the installation when all port conflicts are resolved.
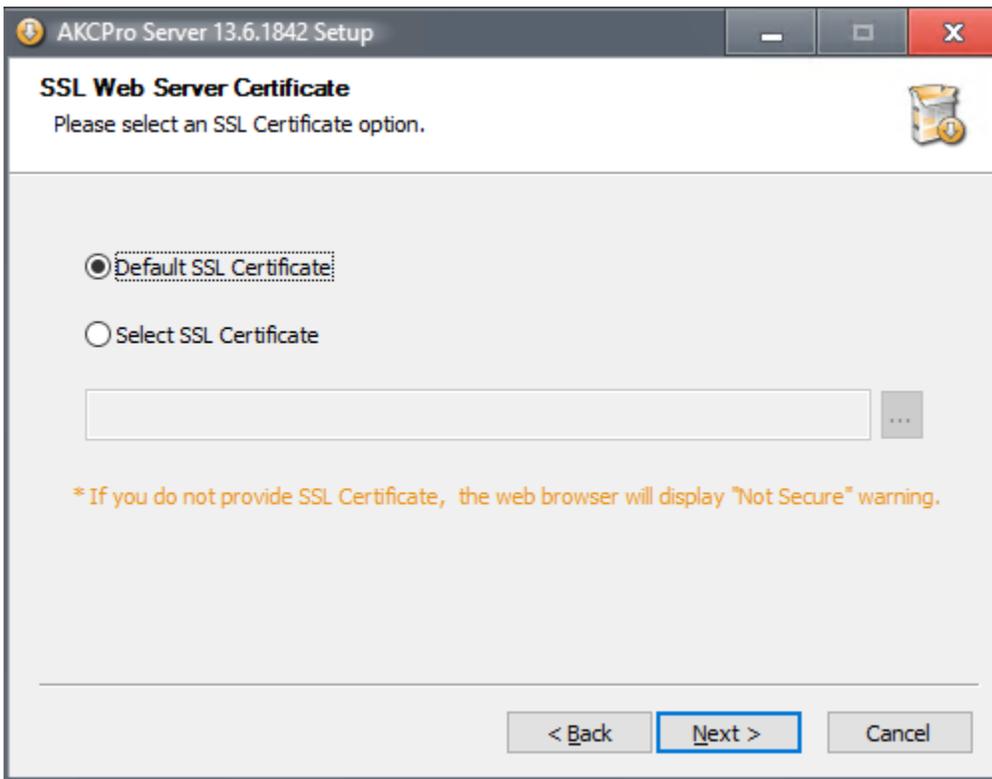
On newer APS versions, the installer also includes a step to select the SSL certificate for the APS HTML WebUI.

The default certificate is self-signed, so it will produce security warnings in all web browsers.
Note: the SSL connection is still safe and secure with the self-signed certificate, only the web browser is not trusting it. Alternatively you can select to upload a custom certificate. The file has to be in PEM format; see the SSL section in this manual for more information.

Browser Connections & Log in Issues

Please note that currently the only supported browsers are Google Chrome and Mozilla Firefox. With other unsupported browsers, the Web UI might not load correctly.

Impoartant Note: All of the newer versions (from 2020 on) of the third party web browsers, including Chrome will evetually include new security restrictions that will affect your connections to all of our units and also our AKCPro Server web interface.

You have two options to avoid the browser connection issues when connecting to our web interfaces.

The first is to simply use HTTP and not HTTPS.

The second is to replace or upload your own HTTPS certificate and adding this certificate to your trusted certificate lists within the browser. You should consult with your network administrator or

sytem adminitrator for further assistance with this second option. Please also see the manual in the All Manuals section labeled "Adding Security Certificates to AKCP products."

Select between the internal or an external database for APS.

The internal database is a SQLite type database, suitable for smaller organizations.

These hard limits are defined for the database:

- Maximum number of users: 20000
- Maximum number of groups: 1024
- Max. number of different access schedules (time schedules when a user or group of users are allowed to access a door, by default 6 schedules are defined): 256

The internal SQLite database is the default. If you don't have external database server, choose this.

Click on **Next** to continue.
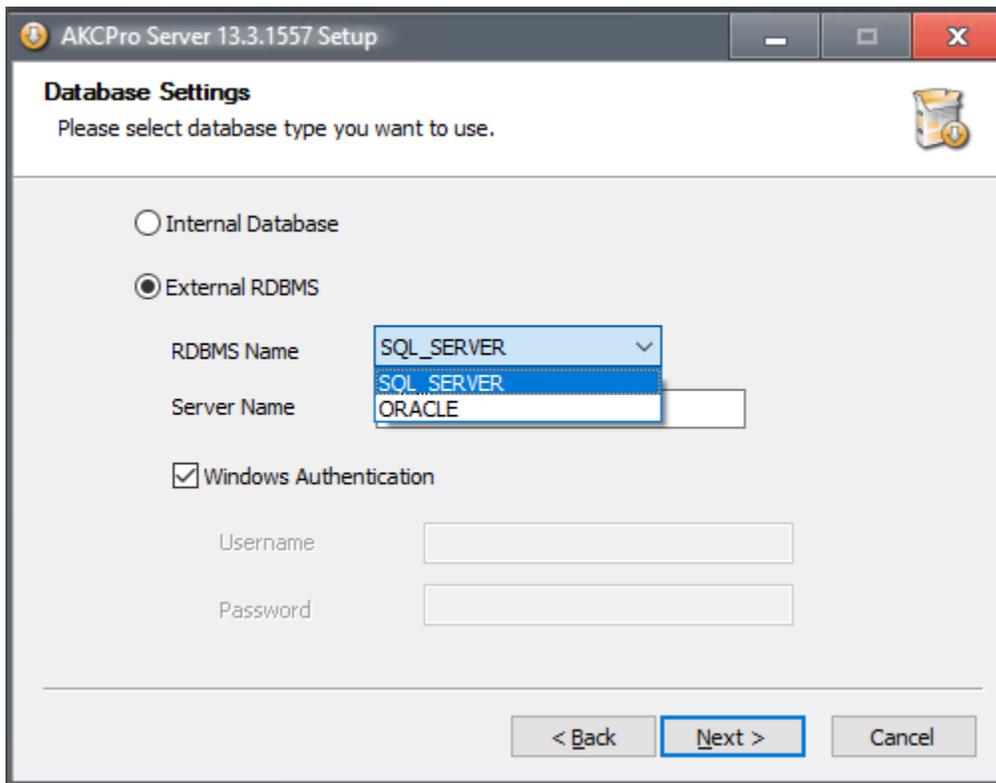
External dabases offer better performance and flexibility, when the database would hold lots of records.
If you intend to use up to or exceed the limitations of the internal database, you have to use an external database.

If you choose to use external database, it has to be installed and configured prior installing APS. The external database communicator uses standard ODBC connectors.

You can get more information about using MS SQL Server as an external database in its own separate manual.

Depending on the features of your database server, you could use Windows Authentication (same username and password as the user running APS), or specify alternate credentials.

Note: Migration / porting from the internal (SQLite) database format to an external database format is possible. We have a separate manual describing this process; please contact support.

Click on **Next** to continue.
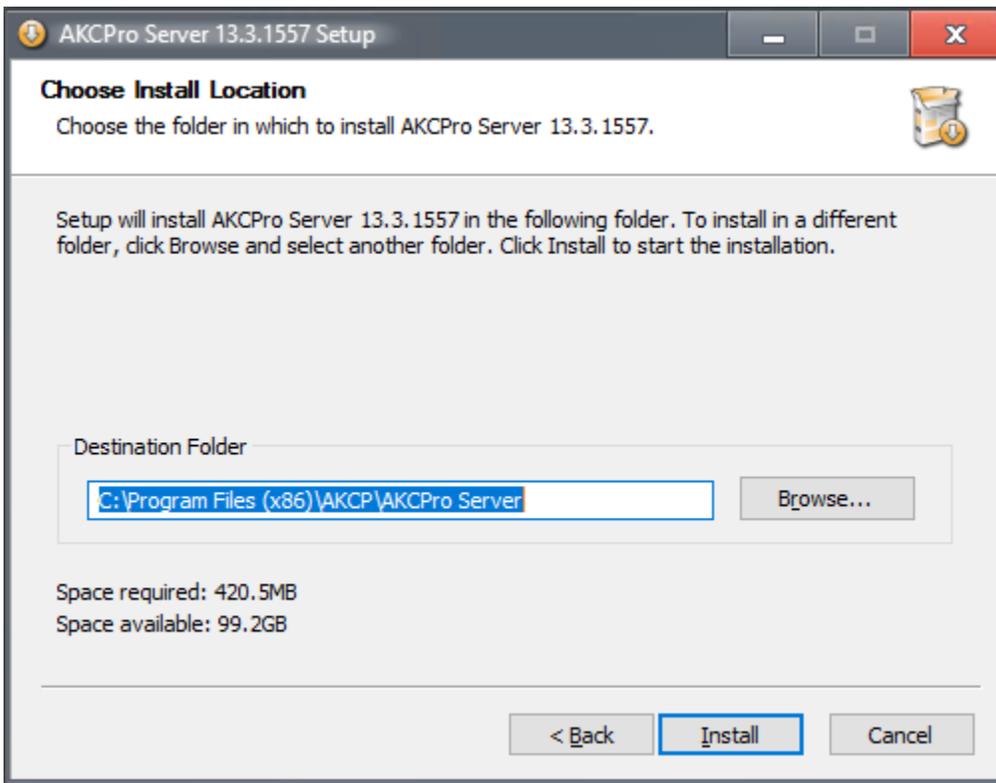
Choose the installation directory.

That's all the information required for installing APS; press the **Install** button to begin copying the files and creating the database.
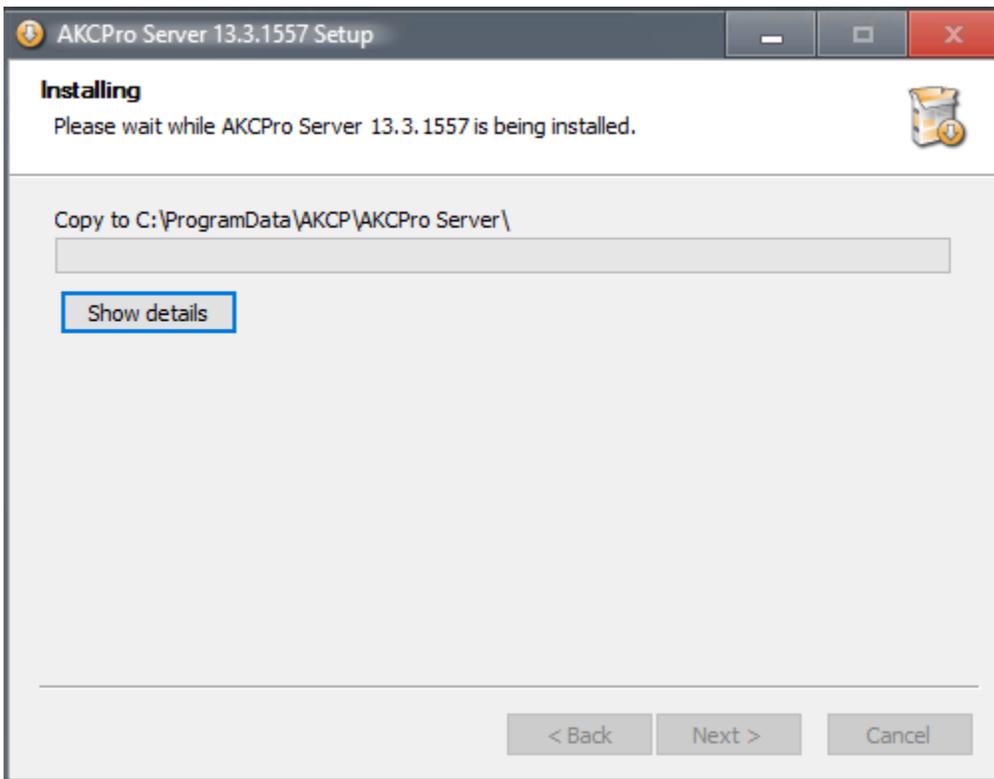
The installer will stop any previously running APS services upon an upgrade, and begin copying the files to the server.

You may press the **Show details** button for a detailed view of the installation process:
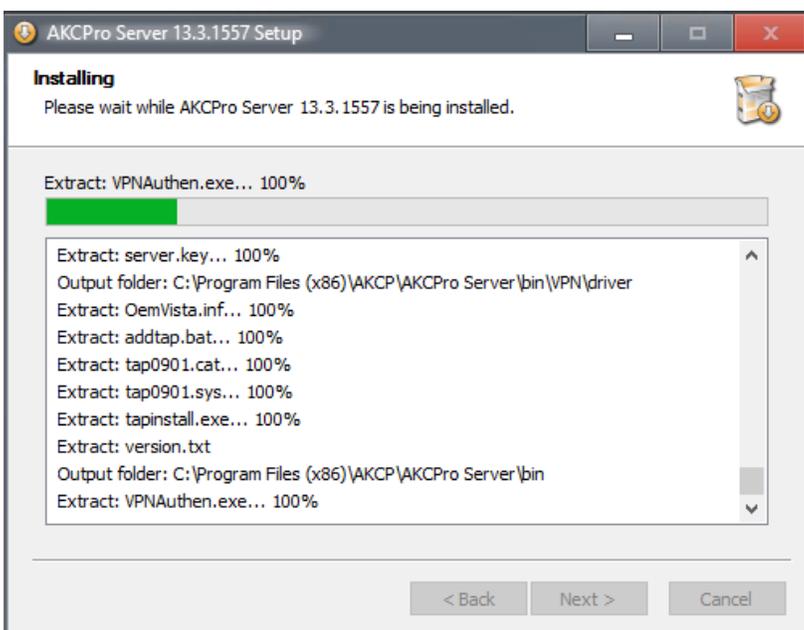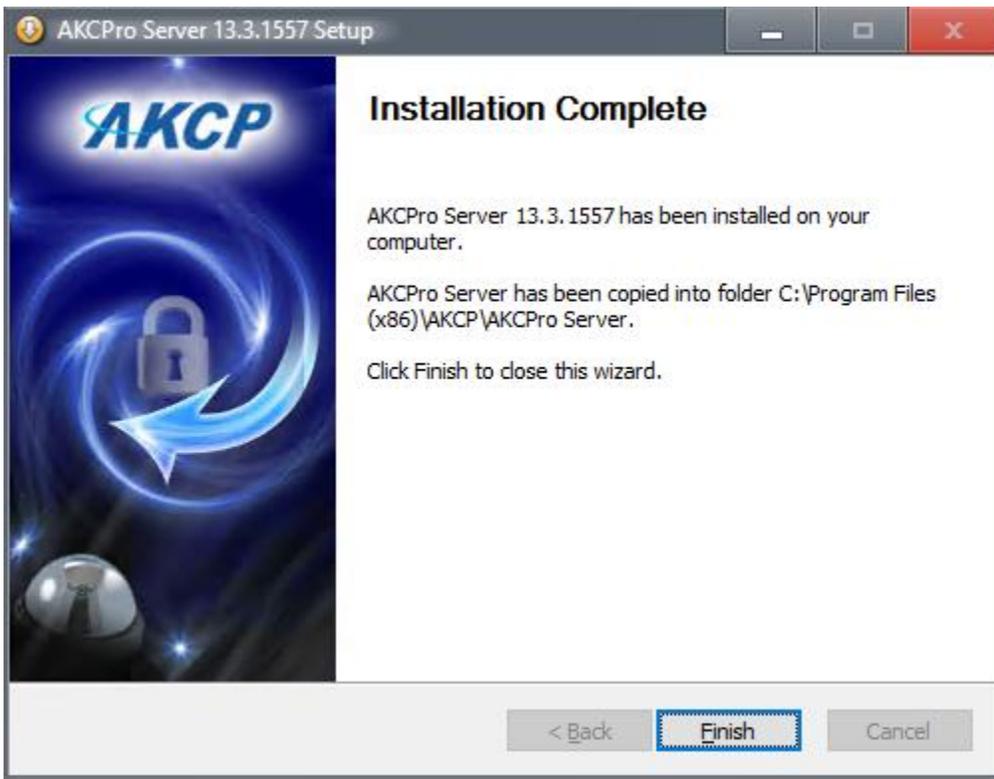
When the installation has been finished, press the **Finish** button.

Now you can start the HTML interface with a web browser to log in to the newly installed server (see below).
If the Windows Client is installed, use the icon either on the Desktop, or in the Start menu (AKCPro).

Logging in to the local server with Windows Client (deprecated)

To log in to the locally installed server, you can just click the option **Local machine** and press OK; it will log you in without any password requirements.
To ensure security, you'd have to make sure that access to your server's console is restricted.

Upgrading previous versions

Upgrading over APS v12 or the first v13 release is designed to be simple and easy.
The installer will automatically migrate all your existing settings and data and remove the v12 installation. Just run the installer and follow the wizard.

A standard upgrade should follow the same steps like a fresh install, so you may check the Install section again in this manual if you need more information.

Future version upgrades should work the same way (upgrading from APS v13) just ensure you always have up to date backups.

Note 1: if you intend to reinstall v12 for some reason, make sure to back up your system using the Backup & Restore feature before the upgrade, and store this backup separately.
APS v13 will change the database schema and the installation location, so it's not possible to downgrade without uninstalling v13 and then restoring a v12 backup on a fresh v12 installation!

Note 2: on newer APS installations (after the 13.4.1634 release) the **Windows Client (wx) is removed** from the installation package and **only the HTML server components** are installed. During upgrade if a previous Windows Client installation is found, it will be removed and you need to manually reinstall this Client component from a separate installation package.

3. HTML5 interface

There is a built-in web server (HTML UI) in APS v13 which provides access to the APS management without installing a separate APS Windows client program.
You just need an HTML5 compatible web browser running on any device (mobile or desktop) to be able to manage your APS installation, just open the Server's URL and log in (see in the next page).

Very important note: the HTML UI is designed for Google Chrome and Firefox only (no Safari, Edge or MS IE browsers), and we only support these. You'll get a warning popup message if you log in with an unsupported browser. Some features might not work correctly with an unsupported HTML5 compatible browser, such as MS Edge.

Features

Most APS features (98%) are also on the HMTL5 UI, and configuring them matches the Windows client (wx). Changing a setting, adding an action or sensor etc. will also appear in the Windows client (and vice versa).
You can view the changes made in the Event Logs which will list the user and the device's IP address who made the change.
There are some HTML UI-only settings that are only accessible from the HTML5 UI, such as Language (for HTML display language) and Services (where you can change web server ports).

Workspaces & Desktops

All your workspaces, desktops, user settings and configurations are stored on the APS server and changing your device or browser will have no effect on your configured settings, they will "follow you" anywhere (provided that you log in with the same user) using either the Windows client or HTML UI.

When first upgrading from the APS v12 to the v13 and then using the HTML5 browser to log into the APS server the devices, access control, users and notifications will be present, however the workspaces and desktops will be blank or empty and you will need to create these again.

Please note: a desktop or workspace configured in the Windows (wx) client is not compatible with the HTML5 interface (and vice versa), you'll need to recreate your environment for the different clients!

See below in this manual for more information on the Workspaces and Desktops features.

Login to HTML5 UI

After setup completes, you can log in to the server by using the HTML UI with a web browser.
To log in, point your browser to the server's IP address and port. The default ports are 8080 (HTTP) and 8081 (HTTPS).
If it's the local machine, you can use this link: https://127.0.0.1:8081

You need to change the IP address if you're accessing APS remotely. For example to access APS on 10.1.1.121 IP address open: http://10.1.1.121:8080
Note: By default the HTTP is disabled on the HTML5 log in so it will be re-directed to the HTTPS link: https://10.1.1.121:8081 This can be changed in the Server Settings >> Services page.

⚠ Not secure | ~~https~~://127.0.0.1:8081/app.html#/event/all

⚠

Your connection is not private

Attackers might be trying to steal your information from **127.0.0.1** (for example, passwords, messages, or credit cards). Learn more
NET::ERR_CERT_AUTHORITY_INVALID

☐ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

HIDE ADVANCED   **Back to safety**

This server could not prove that it is **127.0.0.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 127.0.0.1 (unsafe)

Confirm the SSL warning or add the site as a security exception, as it's using the built-in self-signed certificate by default.
You can change this certificate during setup, or in the settings after logging in (see below at the Server Settings / Services section in this manual).

Wait until the logon prompt appears. This could take some time on slow connections to a remote server.

You'll need to sign in first with the Admin account, as the database doesn't have additional user accounts yet.

The password for Admin user is the one you specified during setup at this step:

Tutorial and Demo

After logging in successfully, the HTML UI loads and you'll be presented with a short demo about the main APS features:
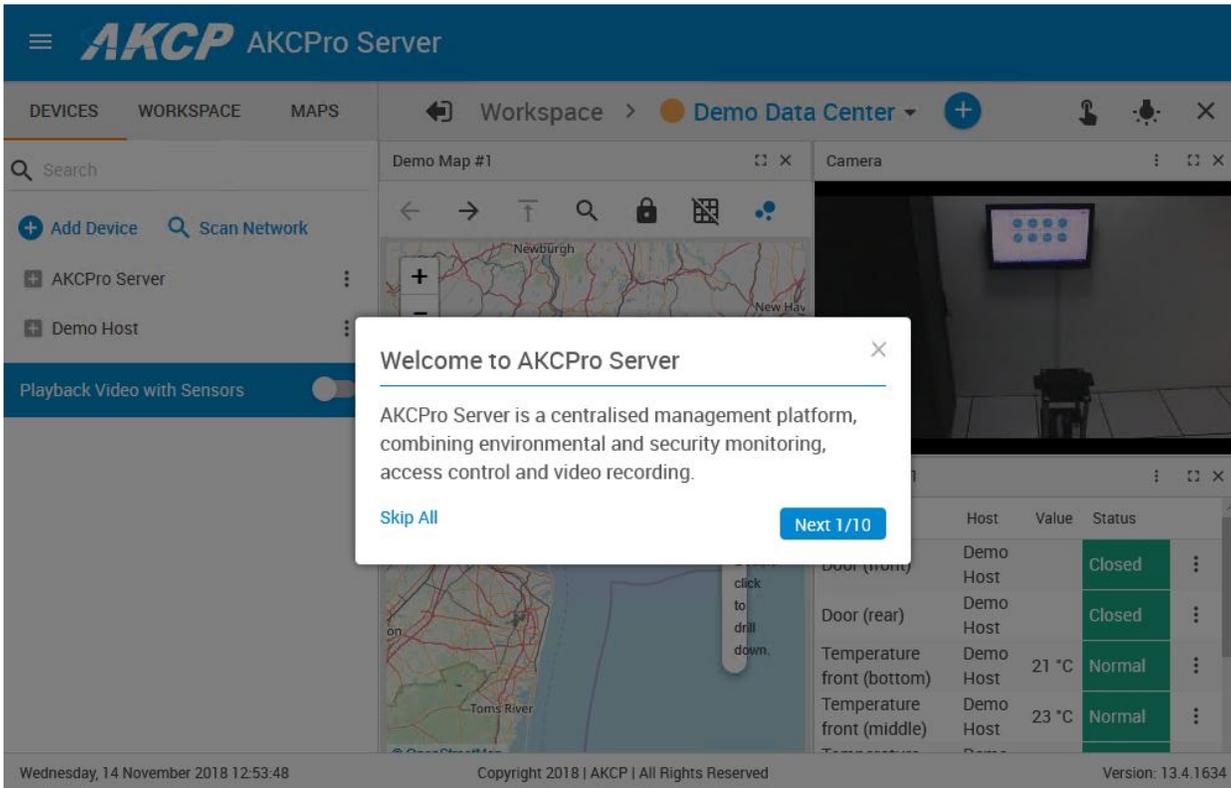
You can dismiss the demo by clicking on **Skip All** or continue to preview the features with **Next**.

Demo Hosts: One host with a virtual camera and the Demo Data Center desktop with a Demo Map and Rack Map, and a Demo Generator is added for this demonstration purpose.
You can manually remove all demo devices when you start using APS, but you may keep them for checking specific settings described in this manual.
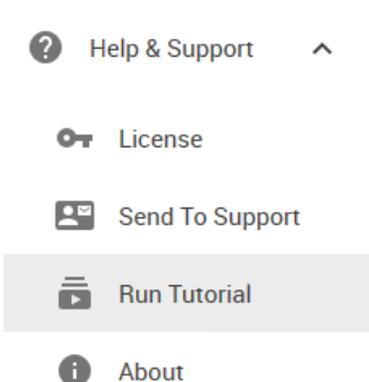
The **Tutorial** can be re-run from the Help & Support menu again if you've dismissed it.

In addition, the Tutorial will run again for different APS features when you start using them the first time, ex. it will run when you first click on the Actions menu.

Unit and sensors management
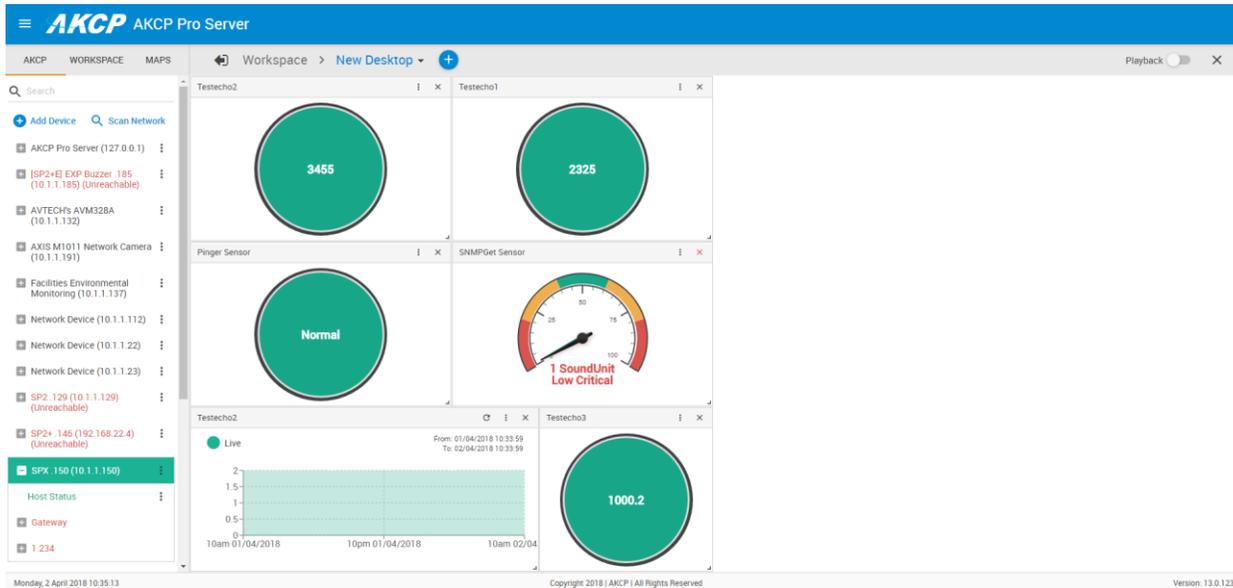
Below we'll give a quick overview of the unit- and sensor management tasks. See below in this manual for information about how to add your units to the console.

Note: by default the standard workspace (New Desktop) is empty and you need to drag and drop sensors on it to display them.
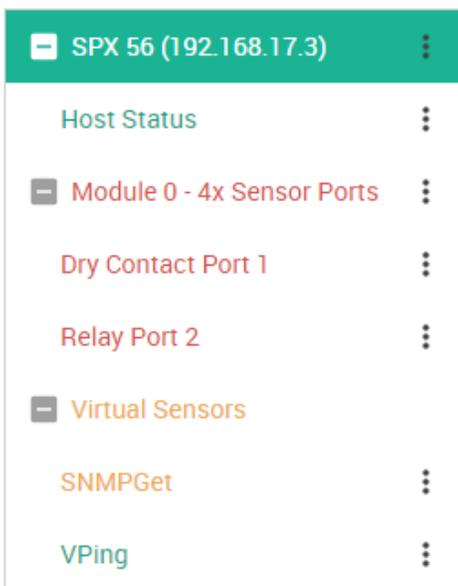
To manage a connected unit's sensor ports, click on it to expand and show the sensors. The available sensors and options will vary depending on the unit type.
The Host Status is always available for every connected unit or camera.

Click on the configuration menu button ⋮ directly next to the right of a sensor or host name to access its popup menu (see below for more information).

Important note: the SP+ and SEC5E virtual sensors cannot be managed using the APS HTML interface. You'll be redirected to the specific unit to set them up or manage them. You can still view the readings and statuses, place gadgets on Desktops etc. just the management needs to be done on the unit itself where the sensor is used.

When you drag and drop a unit on the Desktop, a Sensors Information window will be shown with its sensors. From here you can do the following:

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**. Open the sensor's own **gauge** (gadget) and the sensor's **log** window.

Switch To menu: with this option you can quickly change the displayed gadget to another type and then back. For example, if you have a log view open but you quickly need to check the graph of the sensor.

Get SNMP OID: you can directly display the OID table of the sensor (if it supports SNMP addressing).

Control the relay-type sensors with the Sensor Control menu.

Enable/disable graph data collection per sensor (if they support it), and display the graph display window on the current Desktop.
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, and display multiple graphs in one view.
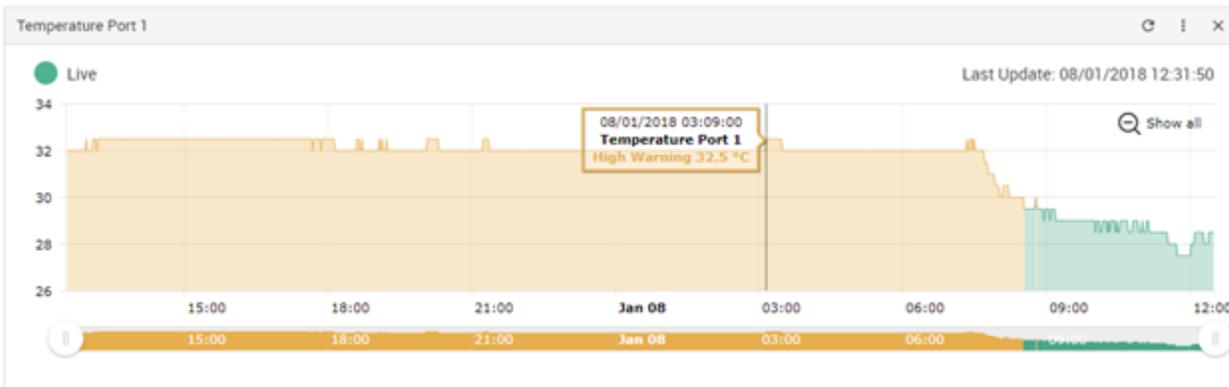
In this example picture, we've chosen to display the temperature sensor's daily maximum.
You could also resize the graph window (including full screen) and move the scale to display more or less data.
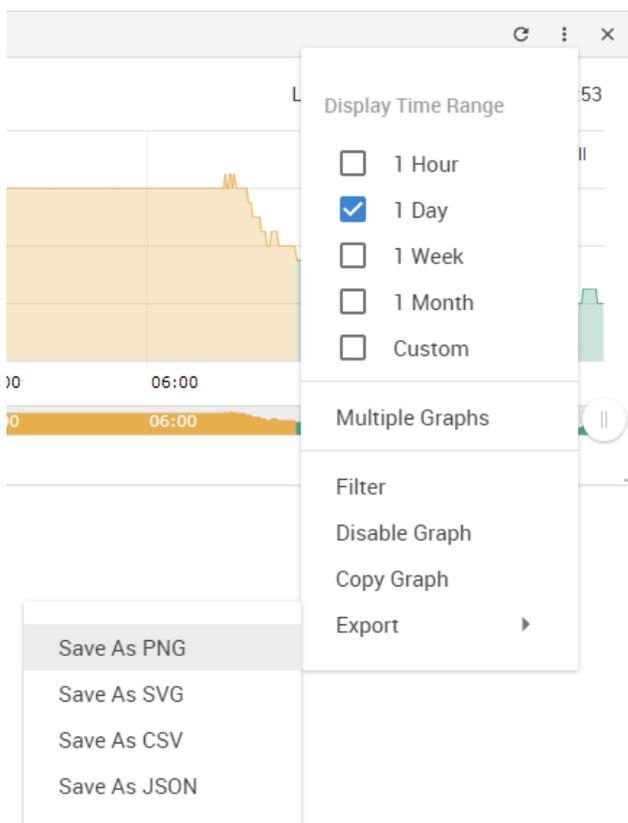
You can choose to export the graph data in selected formats by clicking on the graph's menu on the right, then by choosing the desired format from the popup menu.
The file will be downloaded automatically and assigned a file name that will contain the sensor's name, IP address of the unit, and the date and time.

The graph is always a **Live Graph** and the data collection period is nearly infinite (approximately 1 year) as it is stored in the APS database.
You may also refresh the graph data manually with the refresh button on the right.

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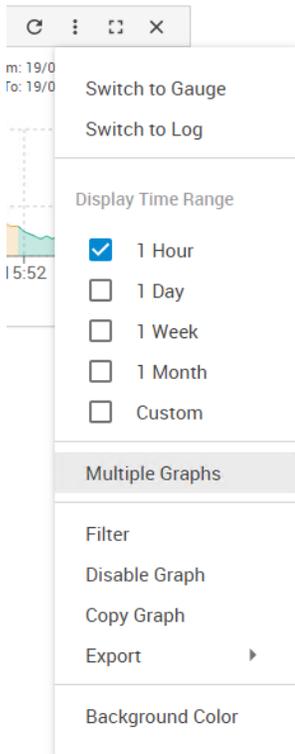
If you want to view multiple sensor graphs, first you need to **Enable Graph** for a sensor that supports graphing from the sensor's menu. Then select **View Graph** to display the first graph. The data collection will run in the background even if you don't display the graph.

After the graph has been opened, choose **Multiple Graphs** from the popup menu as shown.
You'll then be asked to select the other graph(s) that you wish to display in one view.
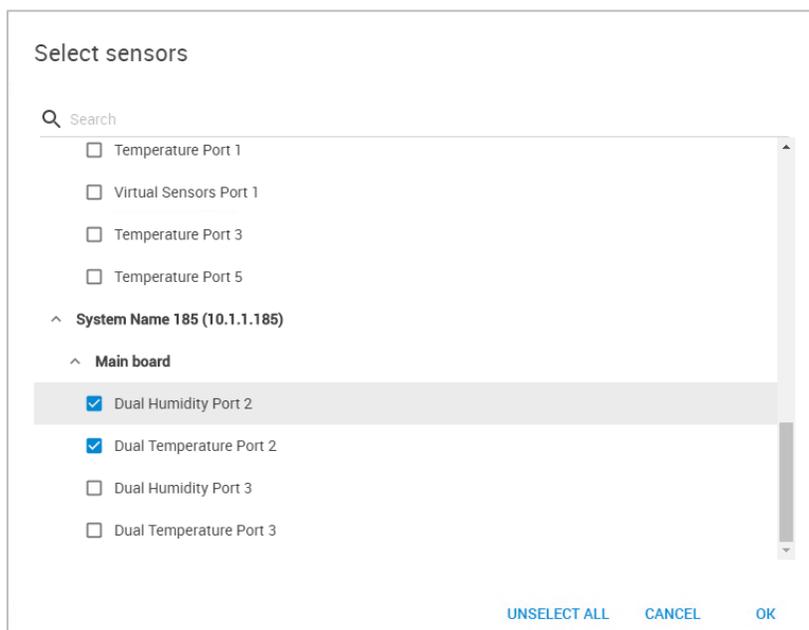
For example we'll choose to display the temperature and humidity in one view from this list.

The second graph will be shown together with the first graph:
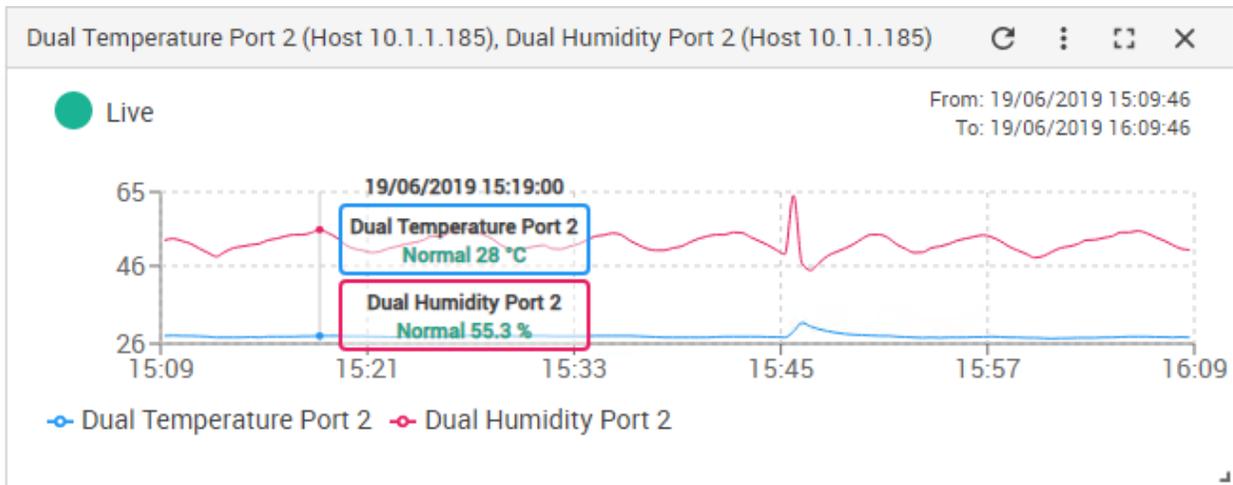
Unlike a single graph, the multiple views won't have a solid color fill for indicating the sensor status. This is required to be able to see multiple graph lines.

Expansion Units

If you have a device with an expansion unit connected and sensors on the expansion board, they will be also listed under the Sensors list.

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+ and SEC+ units. E-sensor8 & E-opto16 expansion units are supported on all SP+ family devices.

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 unit's name (listed as System Name) can be changed by clicking on the link.

4. Adding client units and devices to APS

Adding AKCP device

Before adding a unit to the APS console, ensure that the **Server Integration** option is **enabled** in the client unit's Web UI on the **System page**.

If you don't enable this option, the unit cannot be added to APS as an AKCP device.

Click on the **Add Device** button to begin:
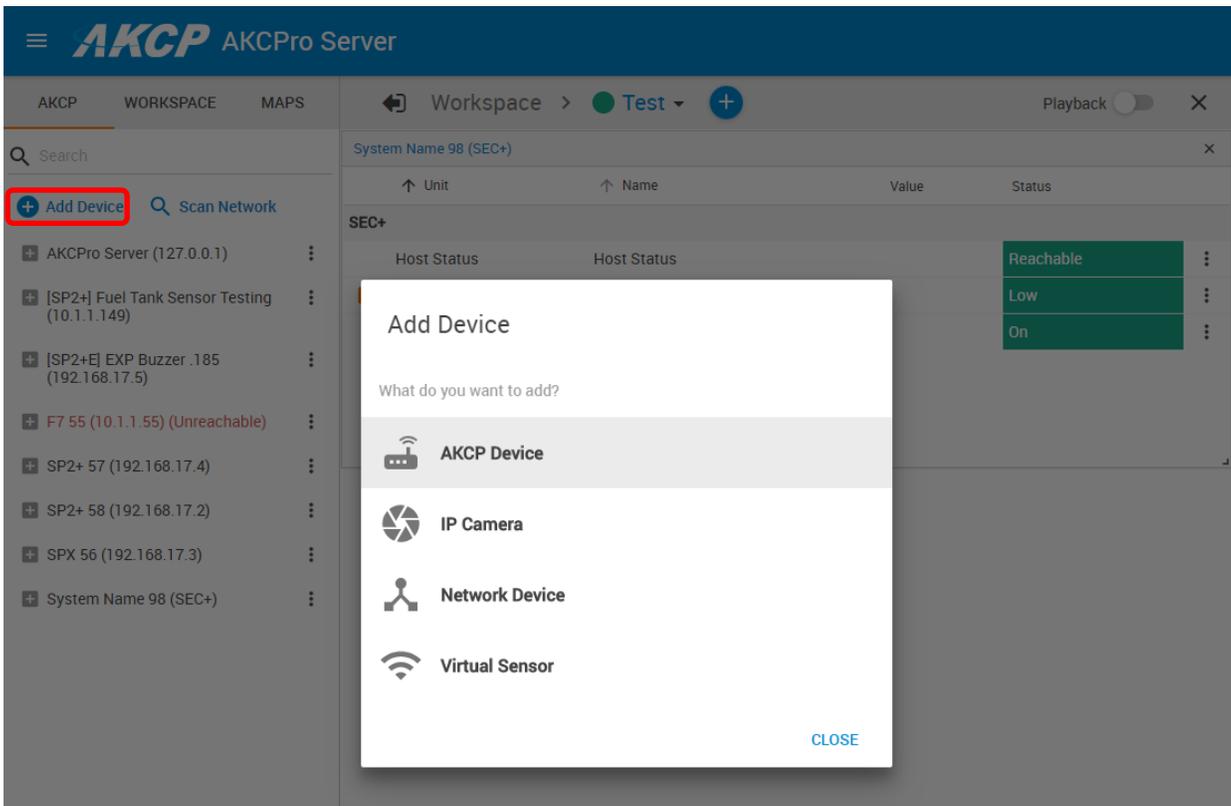
This step will be the same for all device types.

For AKCP client units choose **AKCP Device** from the list.

To add an AKCP unit to the APS console:

- Type in the unit's IP or host name
- User name: administrator
- SNMP Write Community: if you haven't changed it in the Web UI, the default is "public".

Then click on the **Add** button. If there were no errors, the unit will be added to the APS console.

In case the SNMP and RPC ports are changed on the unit, you can also adjust them under the Advanced Options during adding.

Important note: if your AKCP device was already added to another APS, a confirmation popup will appear asking if you still wish to proceed to add the given host. If you do so, the unit will become disabled on the previous APS that it was added to, and become active on this APS.

Confirmation

This host is currently connected to another server. Do you still wish to add this host?

CANCEL   OK

If you enable the option "**Configure automated Rack Map setup**", then the Rack Map wizard will start after the unit has been added (see below for Rack Map settings).

With the "**Configure automated Desktop setup**" option, when you're adding a unit with sensors, APS will create a new Desktop for the unit with relevant gadgets and graphs already pre-selected for you (you will have the choice to select the desktop layout from a list):

After the unit's initialization has finished, you can see the its connected sensors, similar to the view of the Summary page on the unit's Web UI.

You can click on the 3 dots menu on the unit and select **Settings** for configuring the sensors on it. Depending on the sensor type, you'll get different options in this popup menu. You may review an earlier section of this manual for more details about unit and sensors management in general.

Add IP camera

Add the camera to the APS console this way:
- Type in the camera's IP or host name
- User name: this will depend on the brand and model, usually "admin"
- Choose your camera's brand and model from the drop-down lists (see below)

If necessary, you can change the connection's port under the Advanced options:

IMPORTANT NOTICE: Please take note the following information regarding the 3rd party IP camera support policy on our AKCPro Server Software.

Unless the IP camera was purchased from AKCP, or the make and model of the IP camera is listed below, then they will not be supported and cannot be added to the server software.

Moreover, AKCP highly suggests you or your end customer first test any IP camera(s) to insure they can be successfully added to our server software before purchase, or committing them to an installation project. A maximum of 25 x IP cameras are supported per APS installation.

The following IP cameras have been tested and confirmed to be supported on the AKCPro Server Software:

IPCAM (AKCP product code) - ONVIF IP Camera with WiFi (includes 1x IP camera license)
Axis - M3044-V
HIKvision - DS-2CD2125FWD-I
AVTech - AVM328A

When adding the Axis or the HIKvision IP cameras to the APS software there are specific instructions for these, so please contact AKCP support for these manuals.
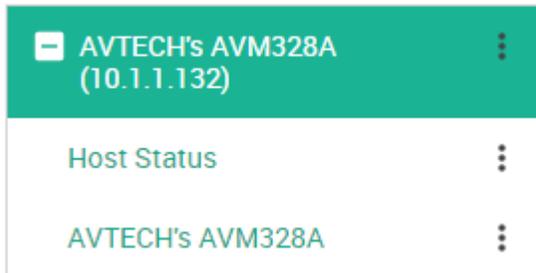
After clicking on the Add button, your camera will be then added to the APS console and you can view its status. Some cameras have adjustable options, which could be reached from their options popup menu.

You can then drag and drop the camera to a Desktop to view the live feed of the camera (adjust the gadget window if necessary), and start to configure *Recording Policies* (see below in this manual):
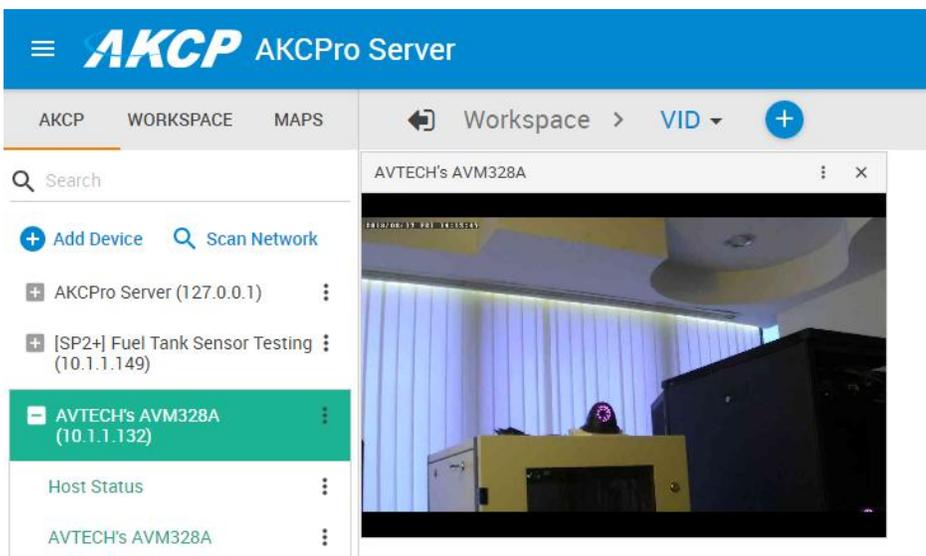
Add Network Device

Add new network device

Hostname or IP

SNMP Read Community

••••••

SNMP Port

161

CANCEL   ADD

Any device connected to your network with an IP address could be added to APS as a network device.

If your device supports SNMP monitoring (for example managed network switches) you could optionally create SNMP Virtual Sensors to monitor its status.
This feature is optional, and your Network Device unit will still be added to APS if you don't specify SNMP options.

Network Device (10.1.1.23)   ⋮

Host Status   ⋮

The host status is monitored by ping requests.

Add Virtual Sensor

Add new Virtual Sensor

Select Host
AKCPro Server

Select Virtual Sensor Type
SNMP Get

CANCEL   NEXT

SNMP Get

Custom Script

Modbus TCP

Virtual Ping

Multiple Sensors

Logic

Energy Cost

PUE Sensor

APS supports many different types of Virtual Sensors.
These doesn't need to be unit specific as they'll run on the APS computer itself; you only need to choose the client unit which you'd like the VS to be attached to, from the "Select Host" drop-down list.

Important: This feature is licensed separately, so if you need to use more than 1 VS you'll need to purchase additional licenses.

Each VS supports a wide range of configuration options.

The Virtual Sensors feature is more detailed below in this manual.

Scan Network
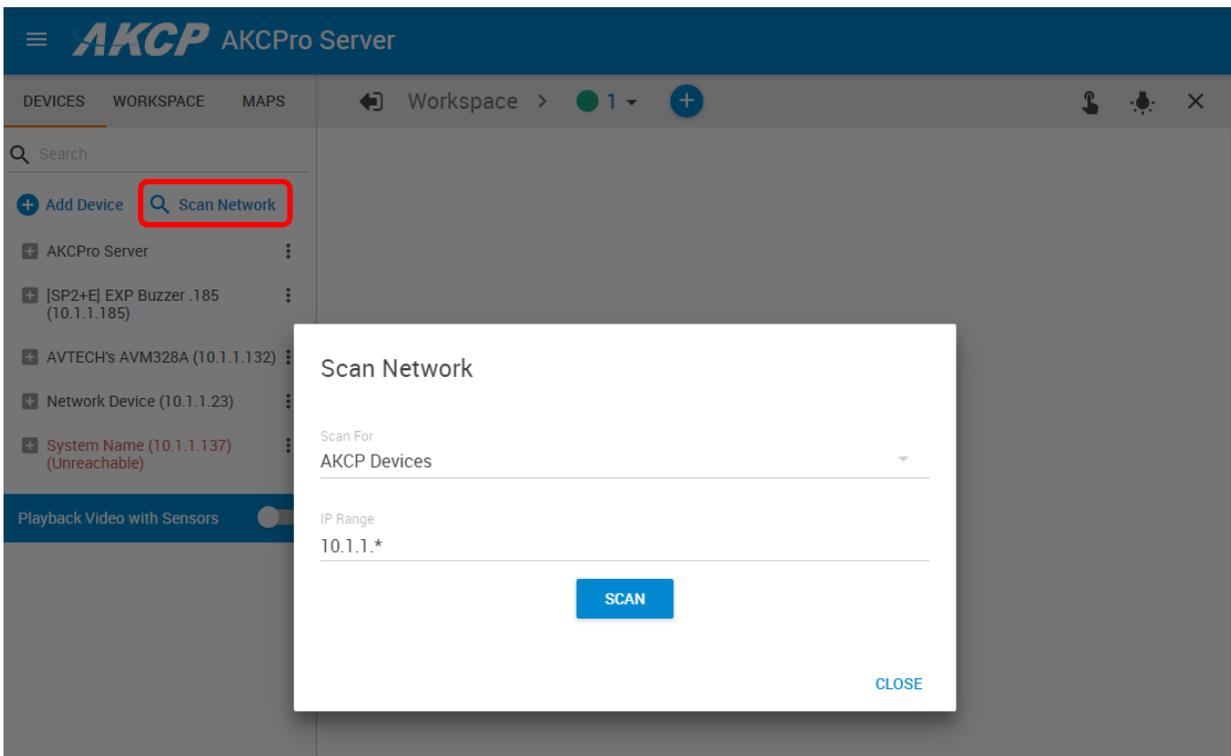
You can also scan the network for devices that you wish to add to APS.
Click on the **Scan Network** link on the Monitoring page to begin.

Select the **Device Type** from the drop-down menu that you wish to scan for, and the **IP range**.

The Network Scan will automatically find the device types you select, from the IP address specified.
The currently used IP range will be auto-detected but you can define a custom range if necessary
(note however that the APS machine must be able to reach this network).

Scan Network

Scan For

AKCP Devices

IP Range

10.1.1.*

Scanning. 8 devices found. (50%)

+   10.1.1.50

+   10.1.1.55
SPX+ (SPX F7 Gabor)

+   10.1.1.57
SP2+ (SP2+ 57)

+   10.1.1.58
SP2+ (SP2+ 58)

CLOSE   STOP

During scanning it's possible to stop the scan if the correct device has already been discovered. APS will list all found devices in a list, and you can add a device by clicking on the blue + icon.

From here it will ask for the unit's username and password, the same way as you would add it manually.

5. Managing Desktops and Maps

The new AKCPro Server's HTML5 UI has the Workspaces feature.
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 tab** while on the Monitoring page:
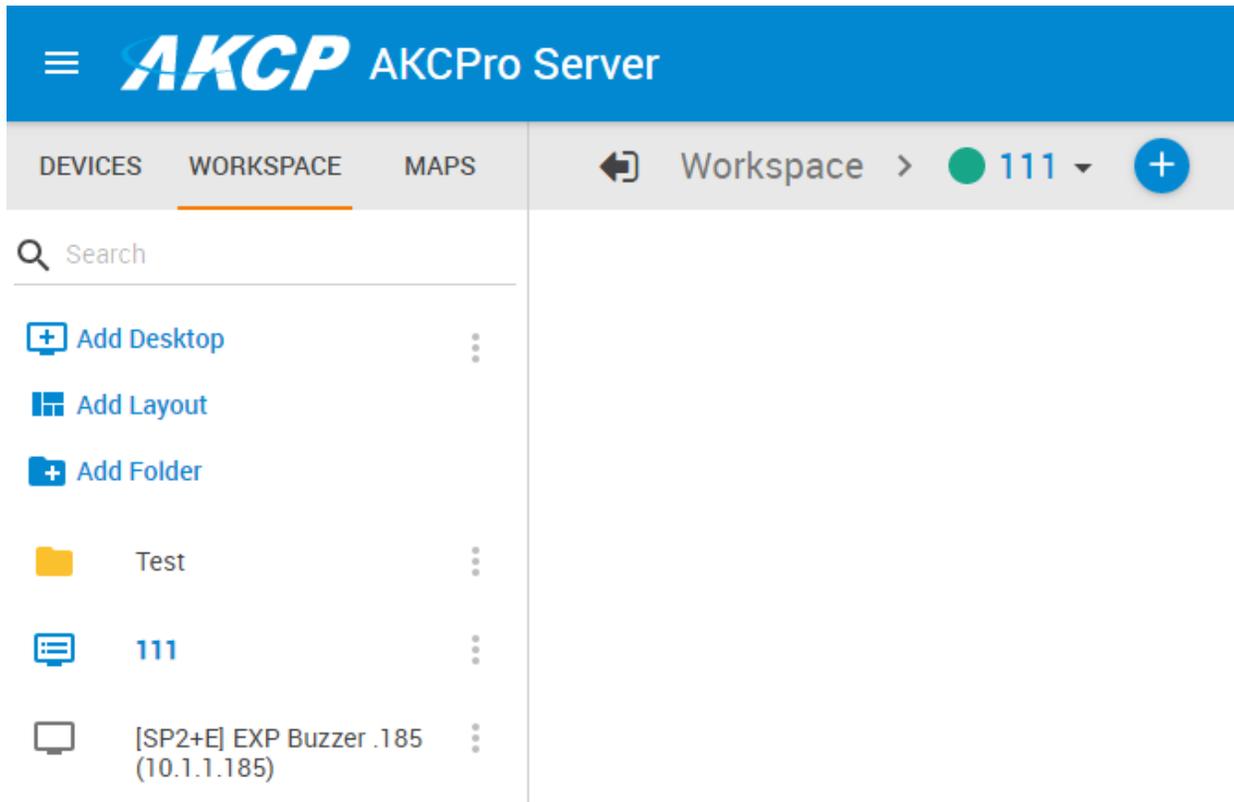
Important Notes on custom desktops

On APS the custom Desktops that are created are stored in the APS data folders on the server computer. Each user can have their own layout and preferences, which will appear the same if logged in from another device or even a different browser. In other words, the Workspaces are fully portable (per user).
Note: the Desktops and any changes made to them are saved when the user logs out.

Generating a backup file from the Backup & Restore menu will also contain the custom desktops.

Without generating a full backup file, you could also export and then import the desktop configuration. The configuration files will be saved as JSON files.

You can click the **Export / Import** command on a Desktop to save/reload it individually:
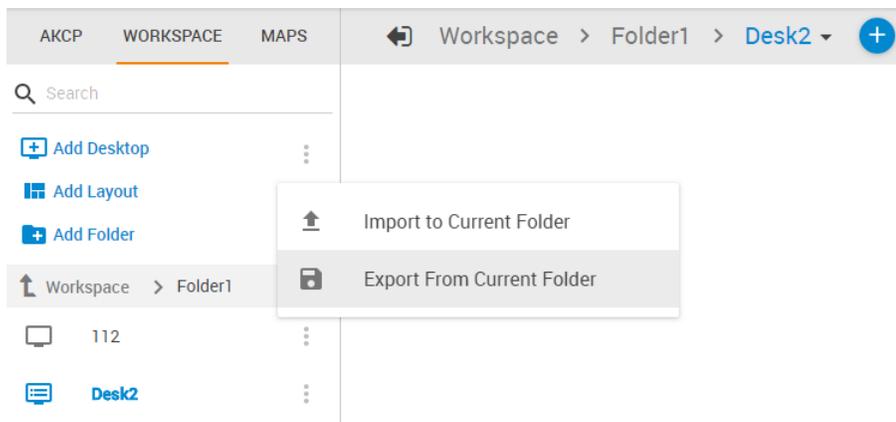
If necessary, you could also make manual backups.
On the server computer, the Workspaces and Desktops are stored under this (hidden) folder:

C:\ProgramData\AKCP\AKCPro Server\Workspaces

Managing Desktops

Navigation
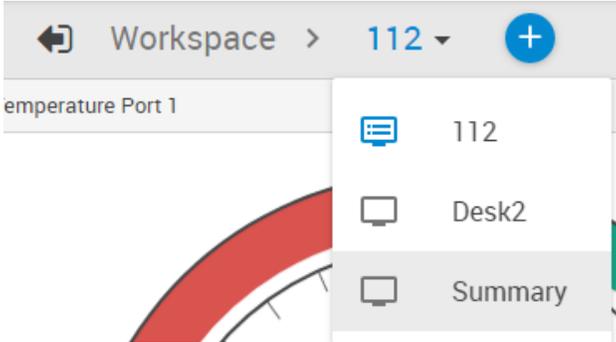
You can manually change between Desktops using the arrow menu, or by directly clicking on the desired Desktop if they are stacked under a folder.
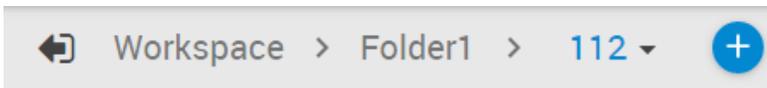
   With this button, your current Desktop will expand to the browser's screen width as shown on the screenshot below:
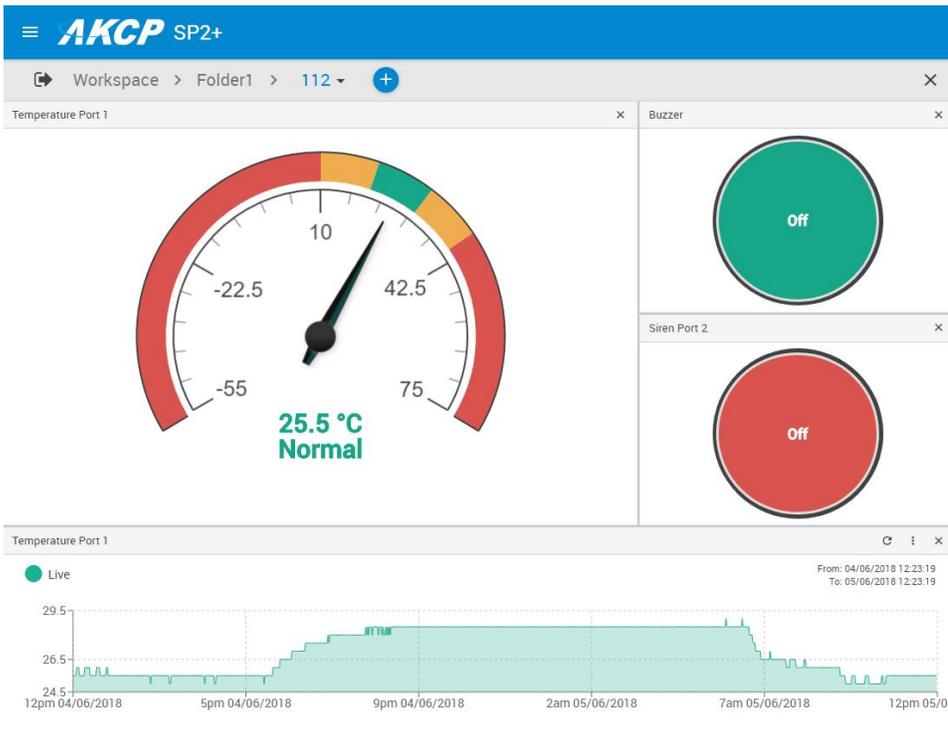
Click it again to go back to the full view.

Common options
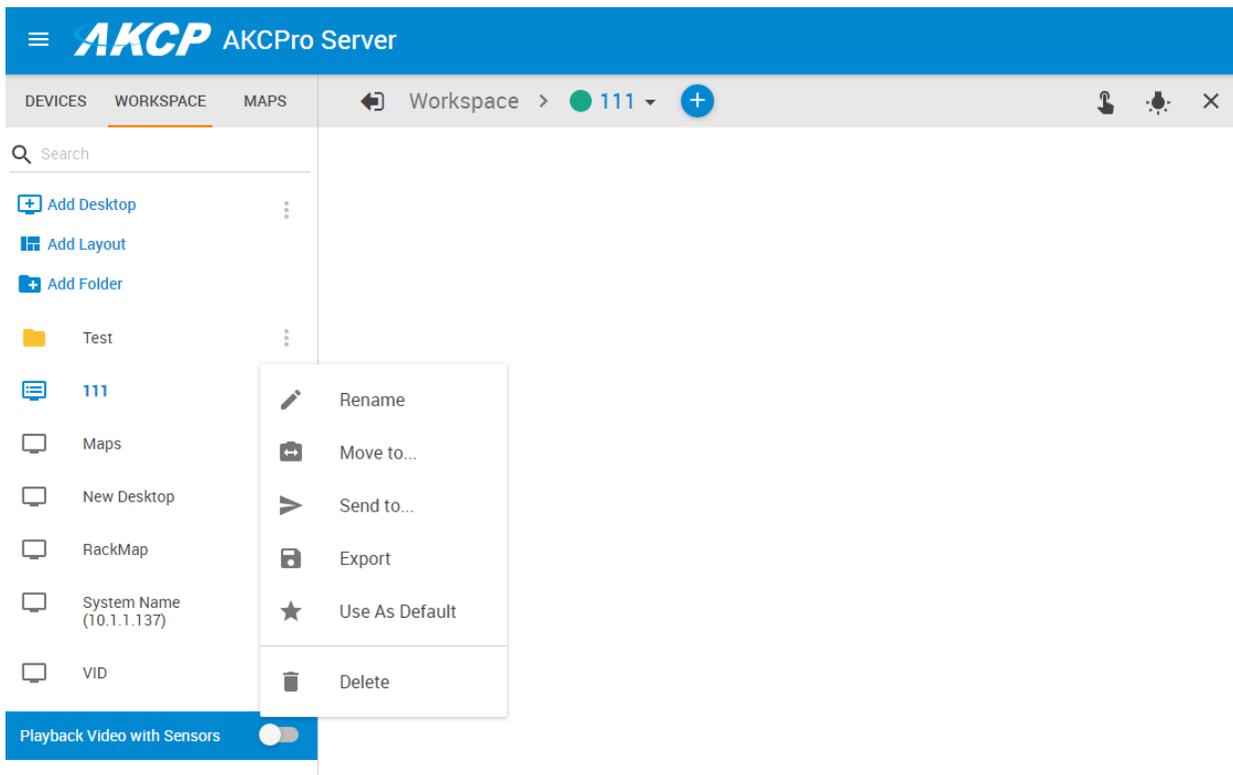
On each Desktop and Folder item, you have these common options:

Rename, **Move**, **Export** and **Delete.**
Move is useful if you've created multiple folders (see below).

With the **Send to** option, you can distribute your workspaces to other users. This is particularly useful when you pre-create a desktop with gadgets, then send this desktop to any other (possibly more restricted) users who should get a pre-configured desktop.

On Desktops you also get an option to **Use as Default**, so that it will be open by default after you log in.

For each Workspace there is a status icon before their name:

With this status icon it's easy to see if the given workspace has a critical status sensor or host placed on it. It will be green if all sensors are in normal state and red if a status reading became critical.

Folders
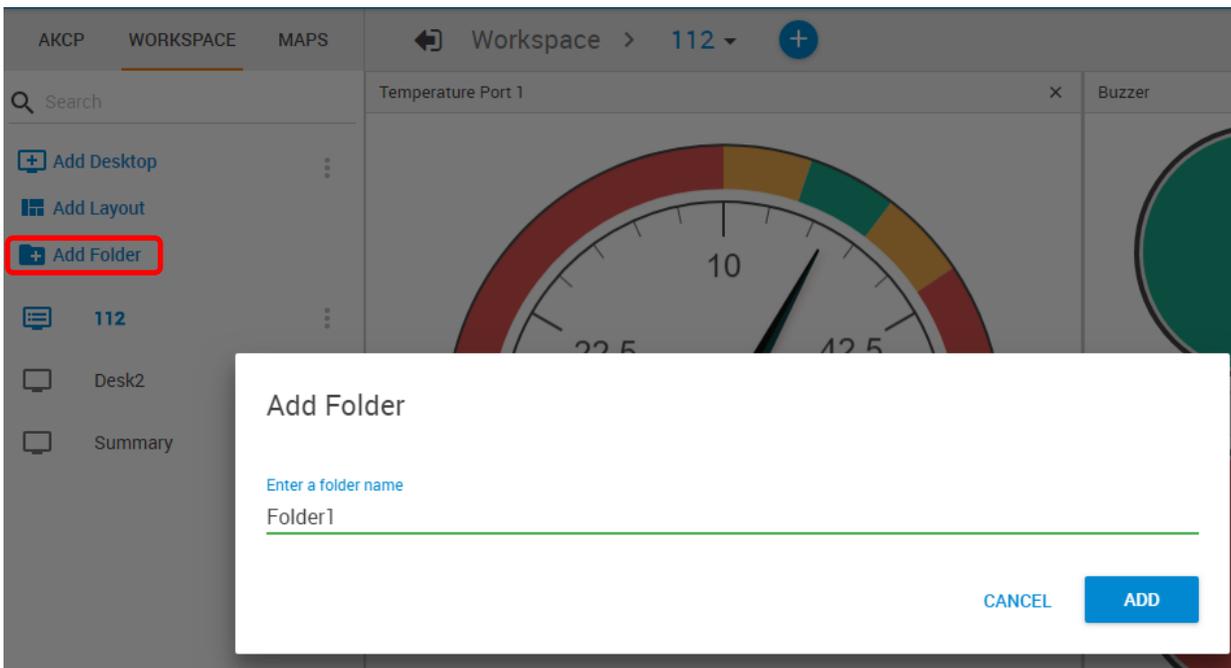
You can add Folders to arrange your desktops into a hierarchical view.
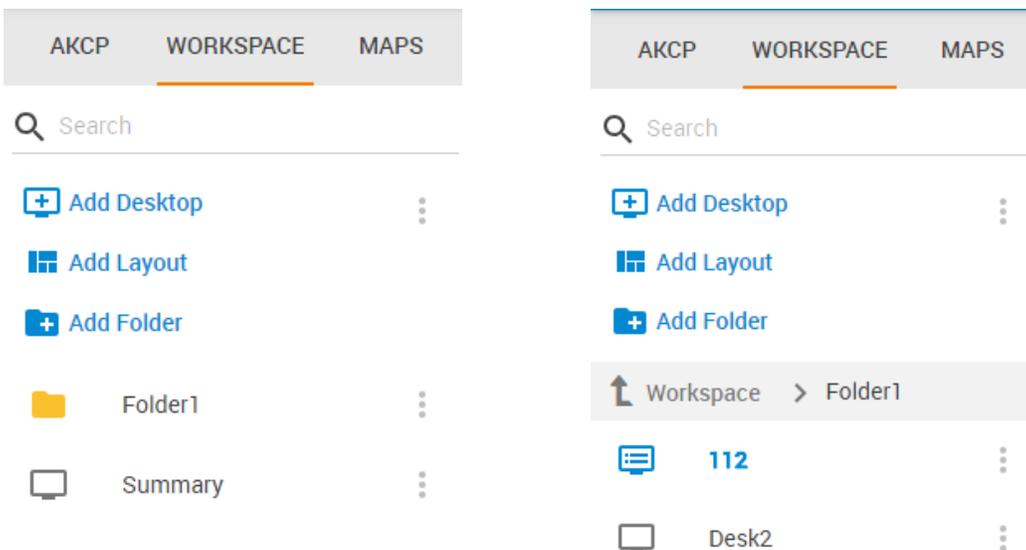
After created, you can simply drag and drop your Desktops under the folder, or use the Move menu. The folder structure will also display on the Desktop selector menu on top:
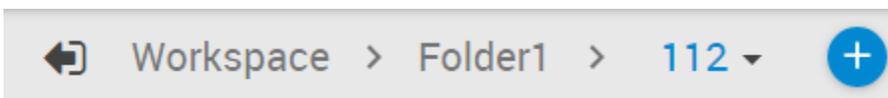
Desktops

You can add new Desktops where you can customize the layout to place any sensor gadget, logs, graphs etc. on the screen.
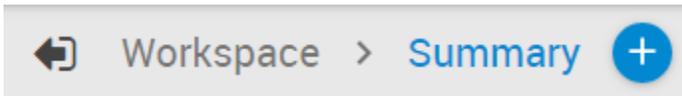
There are two ways to add a new desktop. The first is by creating a blank desktop using the **Add Desktop** link under the Workspace tab:
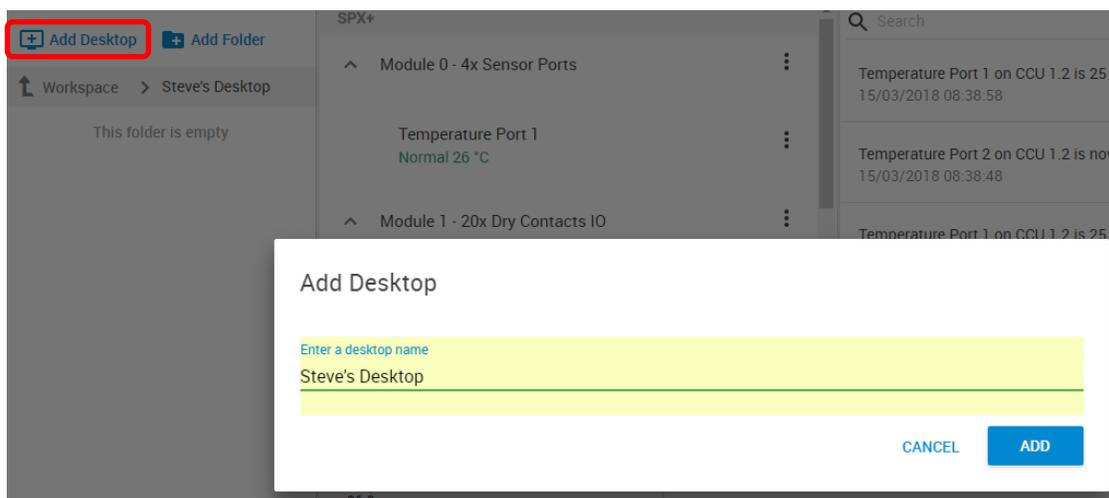
Name the new desktop and click the **Add** button.
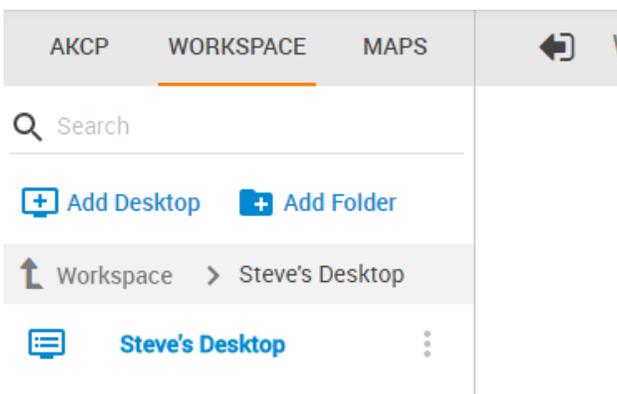
It will appear in the Workspace menu list.

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:
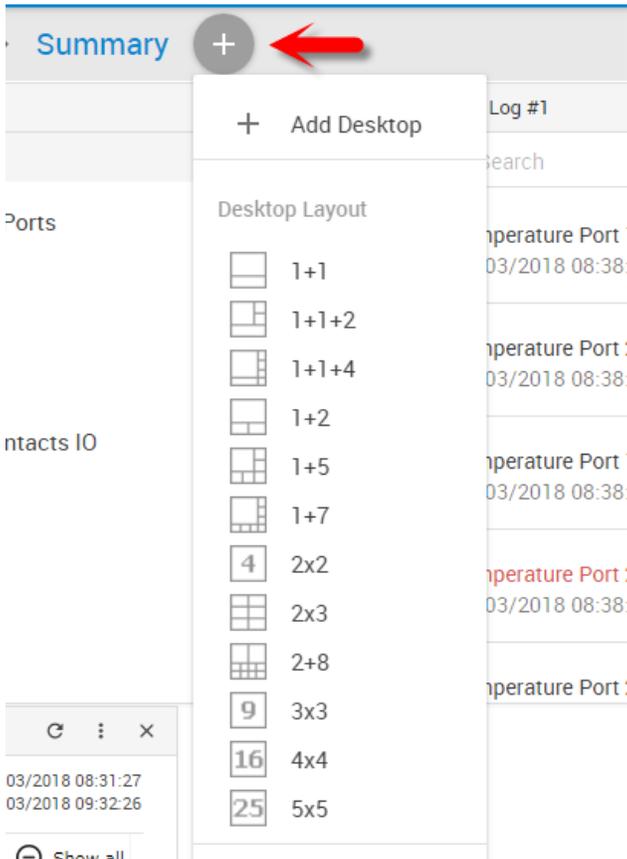
Note: on Windows APS versions, you can also get a small preview picture of each layout if you hover the mouse over them (without clicking).
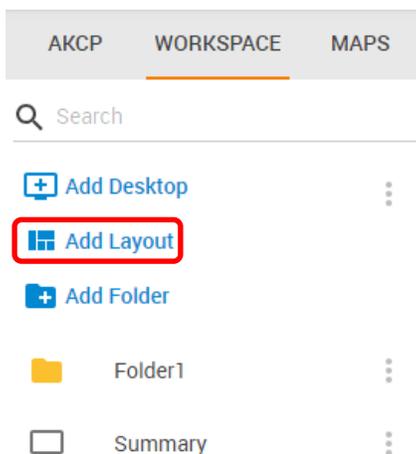
Alternatively you can click on the **Add Layout** link to select from layouts

Depending on the selected type, the empty desktop will usually have placeholders similar to this:
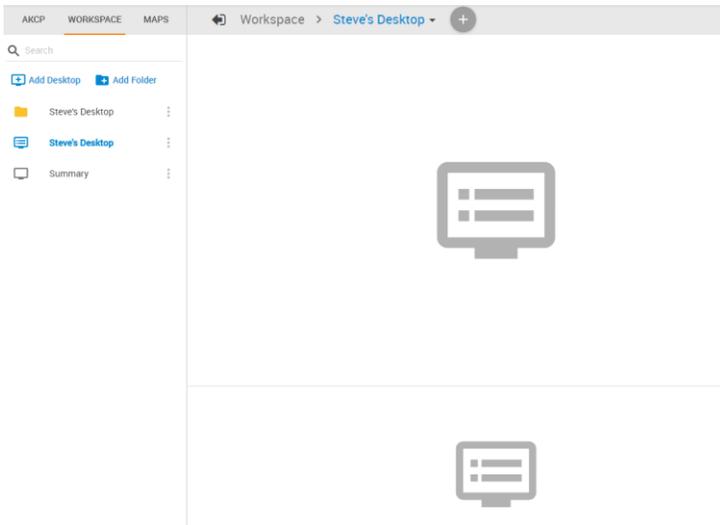
As an example below, we've selected the 1+1+2 layout.
Then you can drag and drop sensors, logs and graphs on the layout:
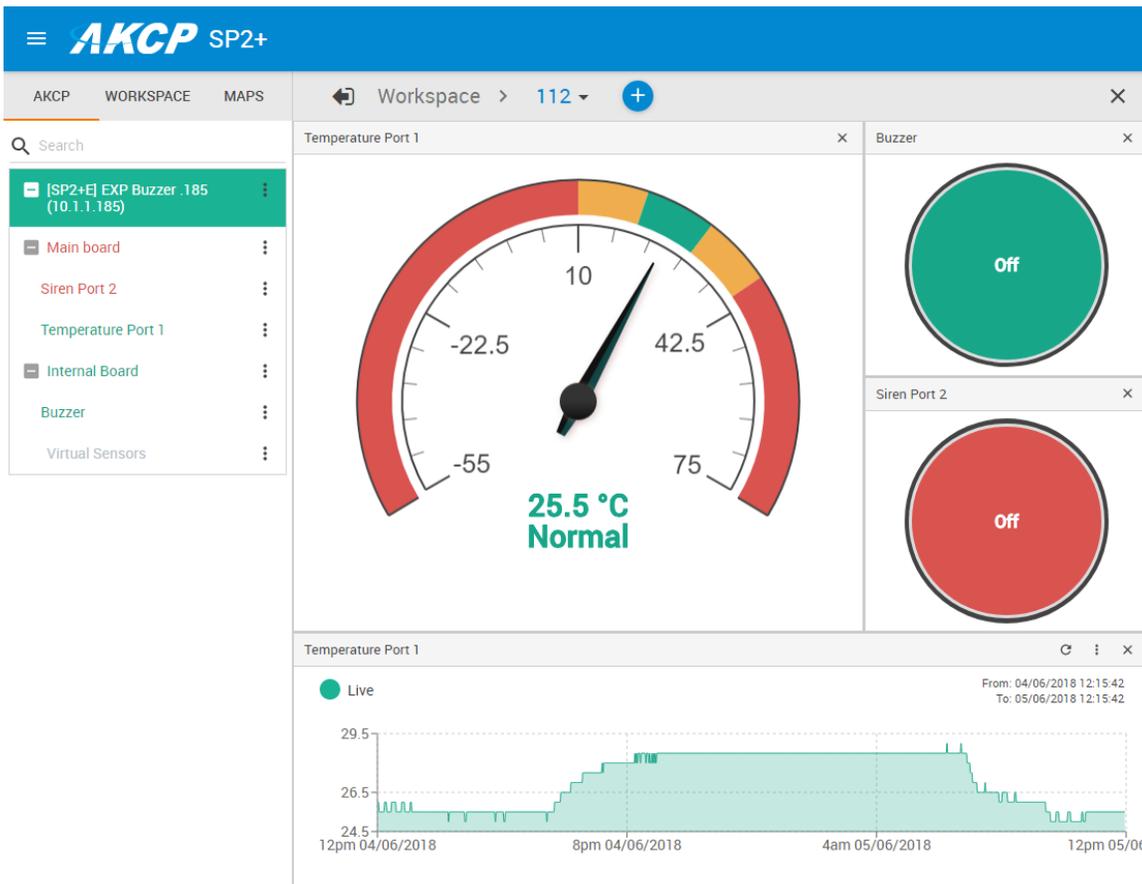
Below we'll show you how you can add sensors to the desktops.

Adding items to your custom desktop
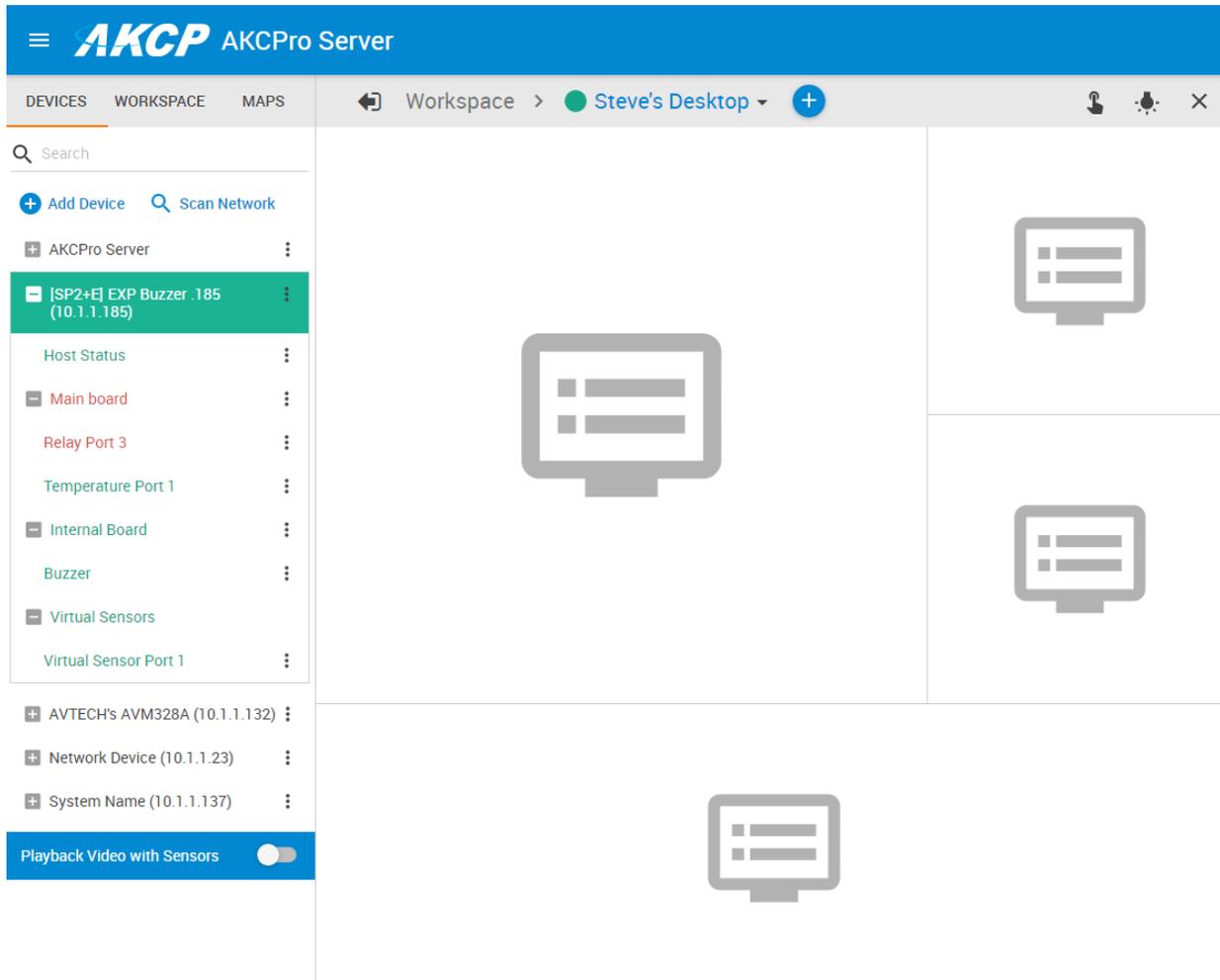
To add items from the units that are connected to APS, you will first need to click on the Devices tab in the Navigation Tree as shown above, to show all added hosts with sensors.

Next expand your chosen host with the + button before its name, and simply drag and drop the items you wish to add to your new desktop. This is also how you can add items to any other desktops.

For example we'll add the Temperature Sensor on the SP2+ Port 1:

Gadgets

On each sensor gadget window you'll see a small button on the top right corner:

Temperature Port 1 (Host 10.1.1.185)   ⋮ [ ] ✕
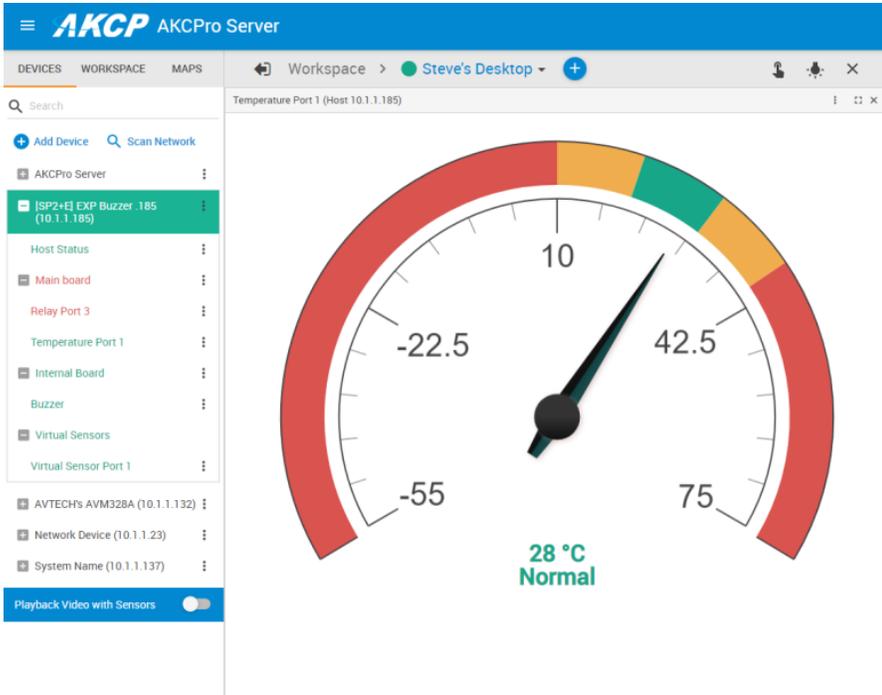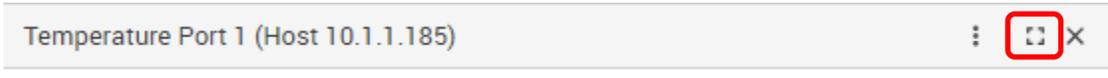
With this, you can maximize the gadget to fill the Workspace screen. Click it again to go back to the previous size.

The gadget's own 3-dot menu could provide specific commands (see below) in addition to standard menus.
You can close any gadget with the X button.
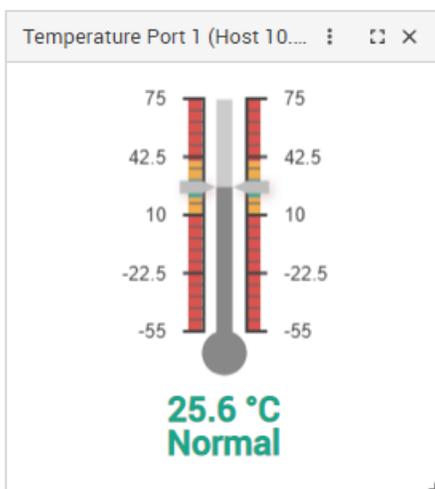
On the newer APS releases the default Temperature Sensor gauge is a new Thermometer type.
If you prefer, it's possible to use the standard gauge type again by using the Switch Gauge menu (see below).
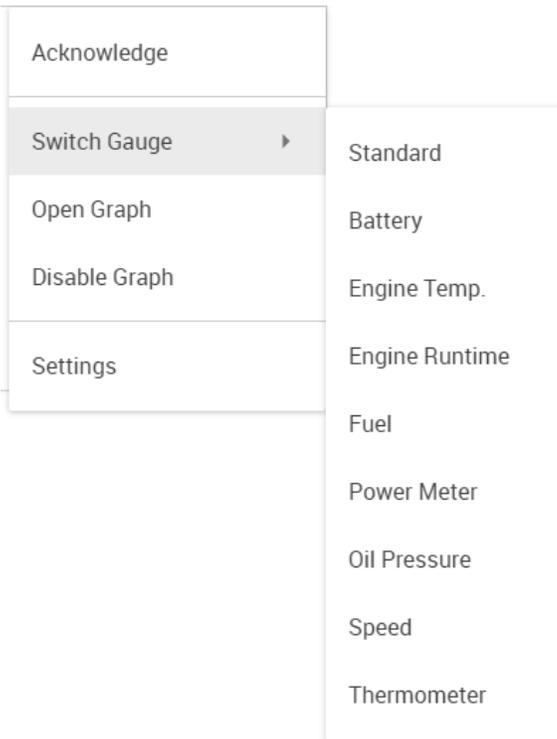
For any Gadget you'll have these common options in the popup menu (to open, single click on the Gadget itself):

- Acknowledge sensor status
- Open Graph
- Disable Graph - when you add a sensor that can be graphed, the graph is enabled by default
- Settings - opens the sensor settings
- Switch Gauge - with this option you can change the gauge style between multiple formats, as seen on the example screenshot on the left
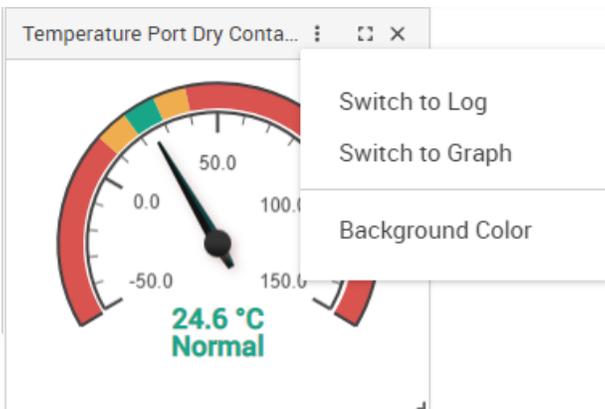
Opening a gadget's 3-dot popup menu will let you:

- Switch to Graph view
- View sensor log
- Change the gadget's background color (on newer APS versions)

If you change the gadget, you can switch back to gauge view again the same way using the menu.
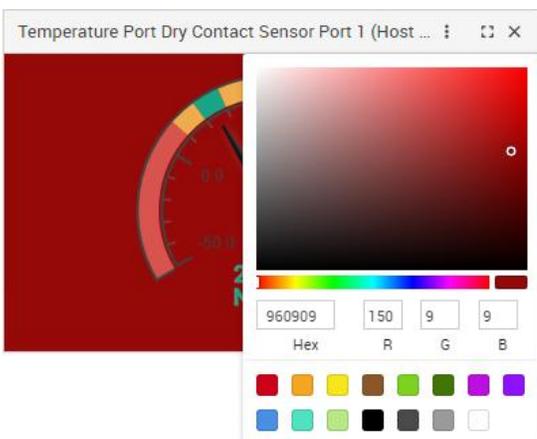
Choosing to change the background color will show the color picker. Change to the desired color and click on the gadget again to close the color picker.

If you wish to return to the default white background, just open the color picker again and select the white predefined color from the list on the bottom.

Button Action and Light Status gadgets
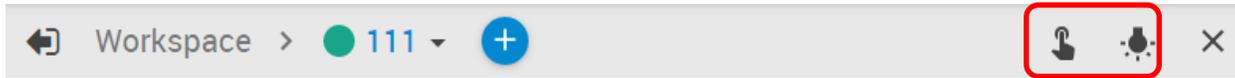
On the top right corner of any Workspace you can find buttons to create Button Action and Light Status gadgets.

Light Status
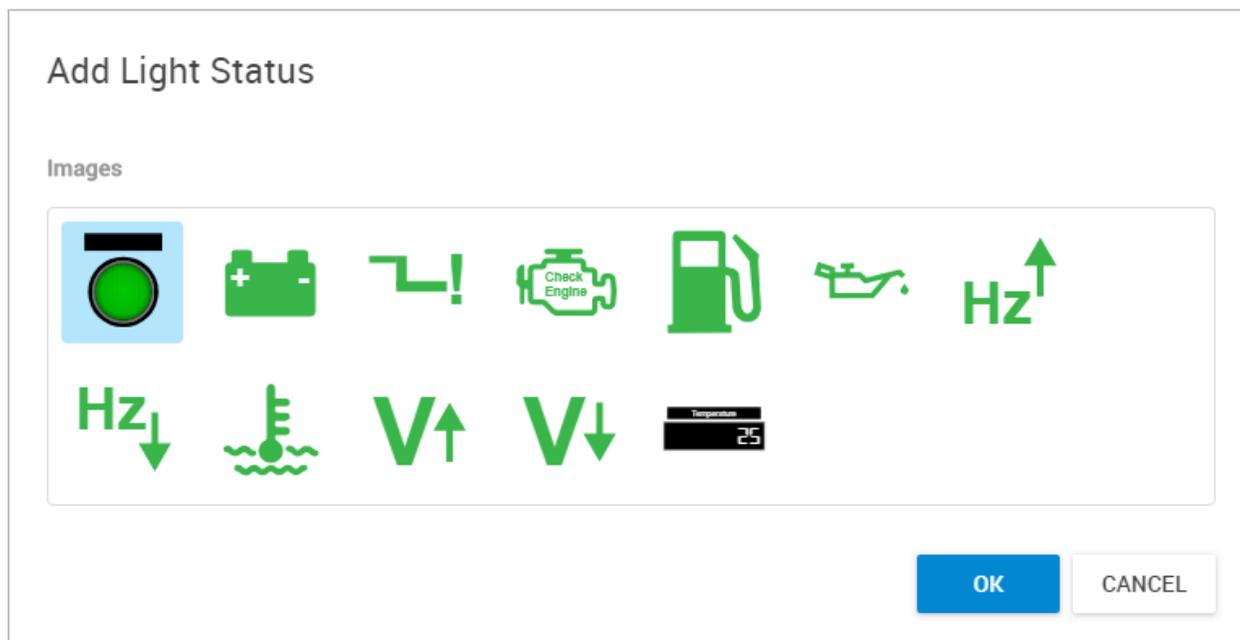
You can add a simple status LED icon with this gadget type.

By default the gadget will be empty and there are no configuration options for this gadget type. To use it, you'll need to drag and drop your sensor which you wish to monitor the status for.

For example, drag and drop the Temperature Sensor on this gadget and it will show the sensor status. You can only close this gadget; there are no configuration options.

Button Action
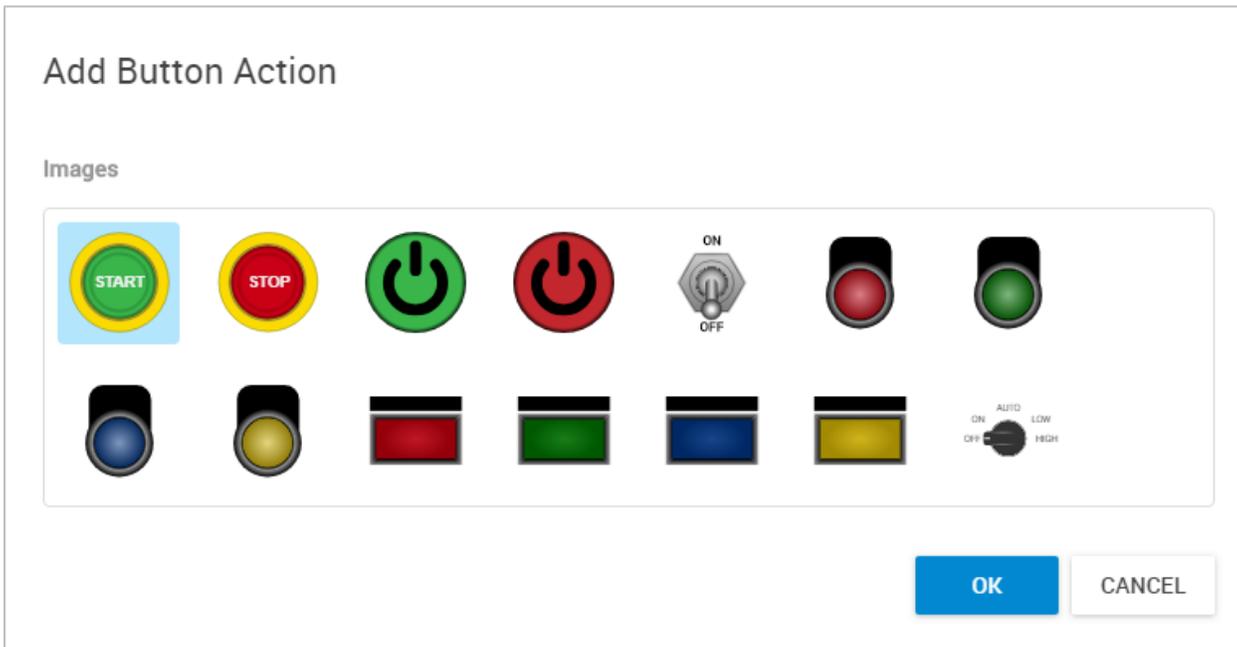
With the Button Action gadgets you can place a button gadget on any Workspace and directly execute the selected action(s) with it.

There are various button styles available, and the number of actions you can execute with them differ between the button style. Usually you can toggle 1 or 2 actions in the on/off state of the button.

Choose your style and click OK. These buttons will appear on the currently opened Workspace.

As an example, we use this button gadget with on/off states. Click on it once to bring up the Button Action configuration window.

Button Action

Select actions

Button Label	Off
Off	Disable ▾

Button Label	On
On	Disable ▾

CREATE ACTION   CANCEL   OK

Here you can configure the button gadget.

You can modify the **Button Label** to display any text for the 2 states the button can control (this could be more or less states depending on the button style).

Disable
Windows Alert 1
Custom Script
SMS Action 1
FTP Upload 1
Modbus Action 1

Then choose from the drop-down menu and select the **Action** that you wish to execute with each button state.
If you don't have any Actions yet, only the "Disable" will be selectable. Click on **Create Action** to create new Actions. This will take you to the Actions page where you can create your action.
More about configuring the actions can be found below in this manual.

AKCP AKCPro Server

Actions
Notifications / Actions

🔍 Search   + ADD

Enable	↑ Action Type	↑ Action Name		
🔵	🔌 Relay	Relay Action 1	✏️ 🗑️	TEST ACTION

After the first configuration, you can always reconfigure the gadget by right-clicking on it and selecting **Edit**.

Desktop Auto Scroll feature
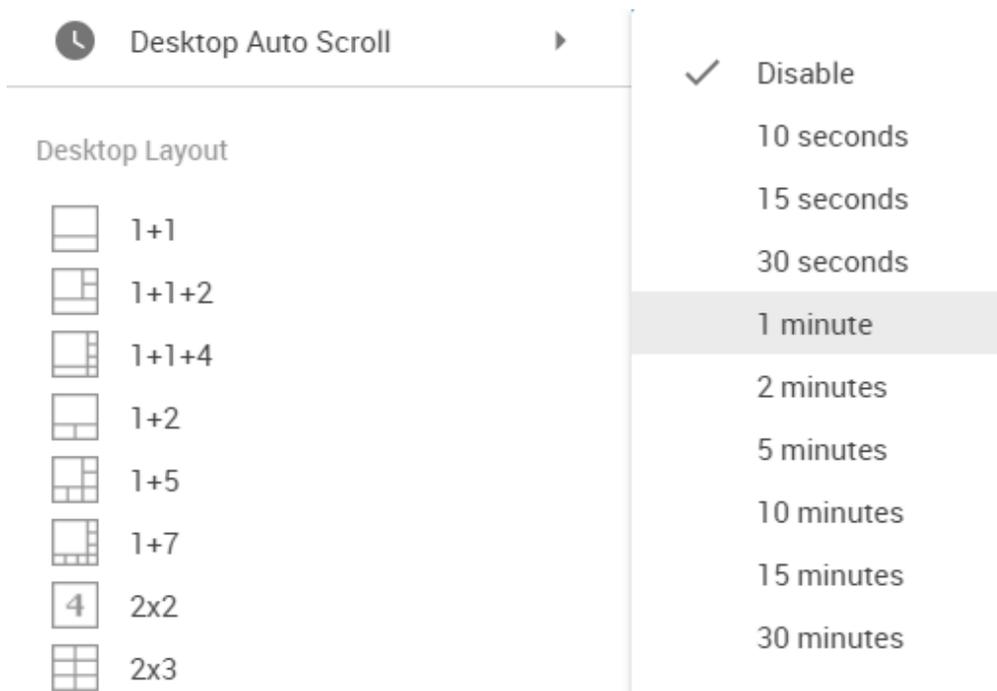
With this feature enabled, your desktop view will automatically switch between the created additional desktops within the specified time interval.
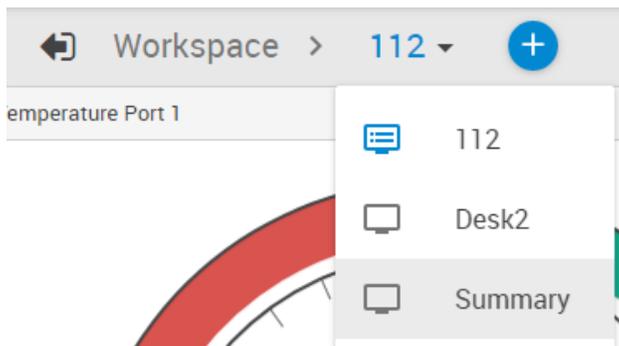
You can also manually change between Desktops using the menu.

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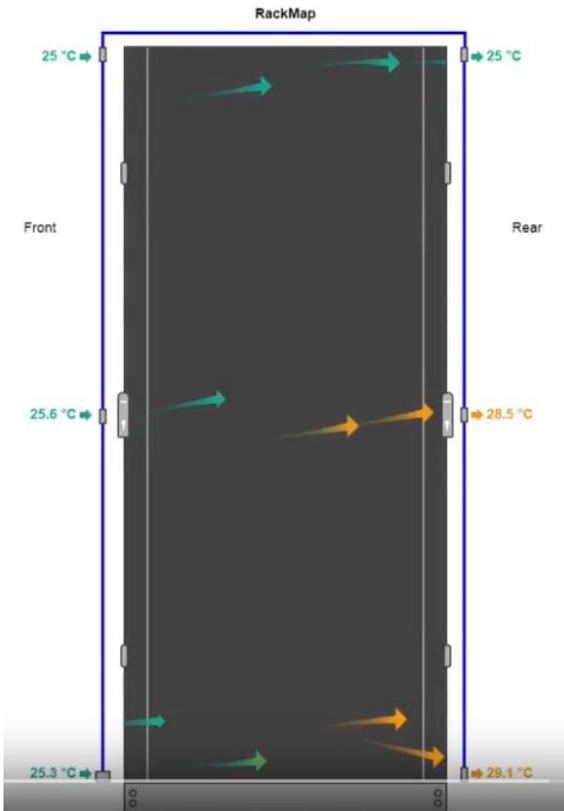
The Rack Map feature is included in the AKCess Pro Server / AKCPro Server (HTML5) and has also been added to the SP+ units. You can add a Rack Map as a graphical representation of your server rack, and to display and record the temperature of the airflow within your server cabinets.

On APS you can use the full features that are available for the Rack Map; for example you can add devices and assets.
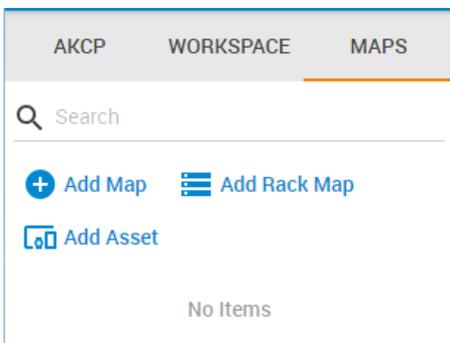
Click on the Maps tab and the **Add Rack Map** link to add a Rack Map.
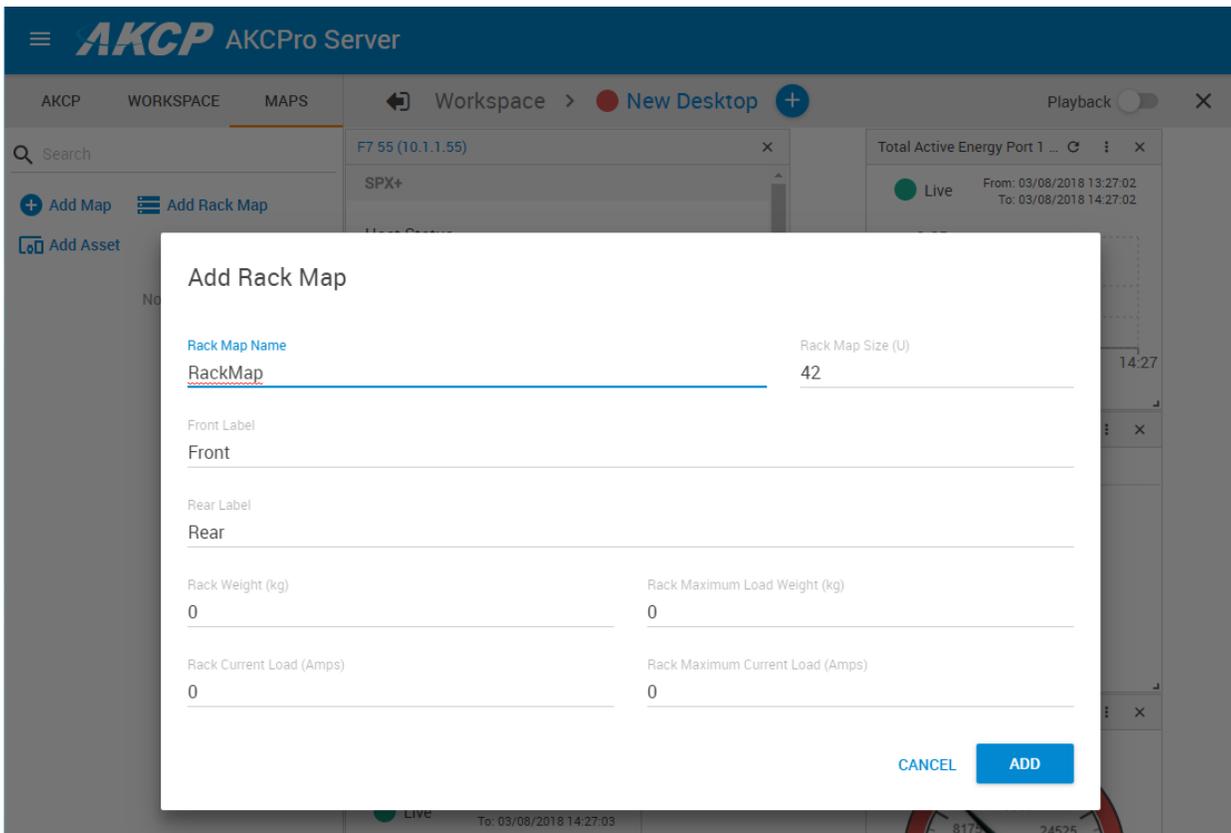
The Rack Map supports some new optional features:

- Rack weight, maximum weight limit settings
- Rack power consumption and maximum consumption limit settings (current)

With these options, you can set weight and power consumption for the rack itself, and a maximum for any added devices and assets.
The current values will be computed automatically and display on top of the rack.

After created, you can drag and drop the Rack Map to a desktop or to an existing map (see at the maps management section in this manual).

E-learning videos:

Live PUE calculations
https://youtu.be/iLxnaZD-8VE

PUE virtual sensor setup
https://youtu.be/Thvz7iTDiCk

You can add the following sensors as a gadget on a Rack Map:
- Rack Assets
- Temperature sensors
- Swing Handle Lock
- Sensor Status Light
- Power Meter
- Dry Contact
- Security Sensor

Simply drag and drop the desired sensor from your unit's sensor list, as shown below.
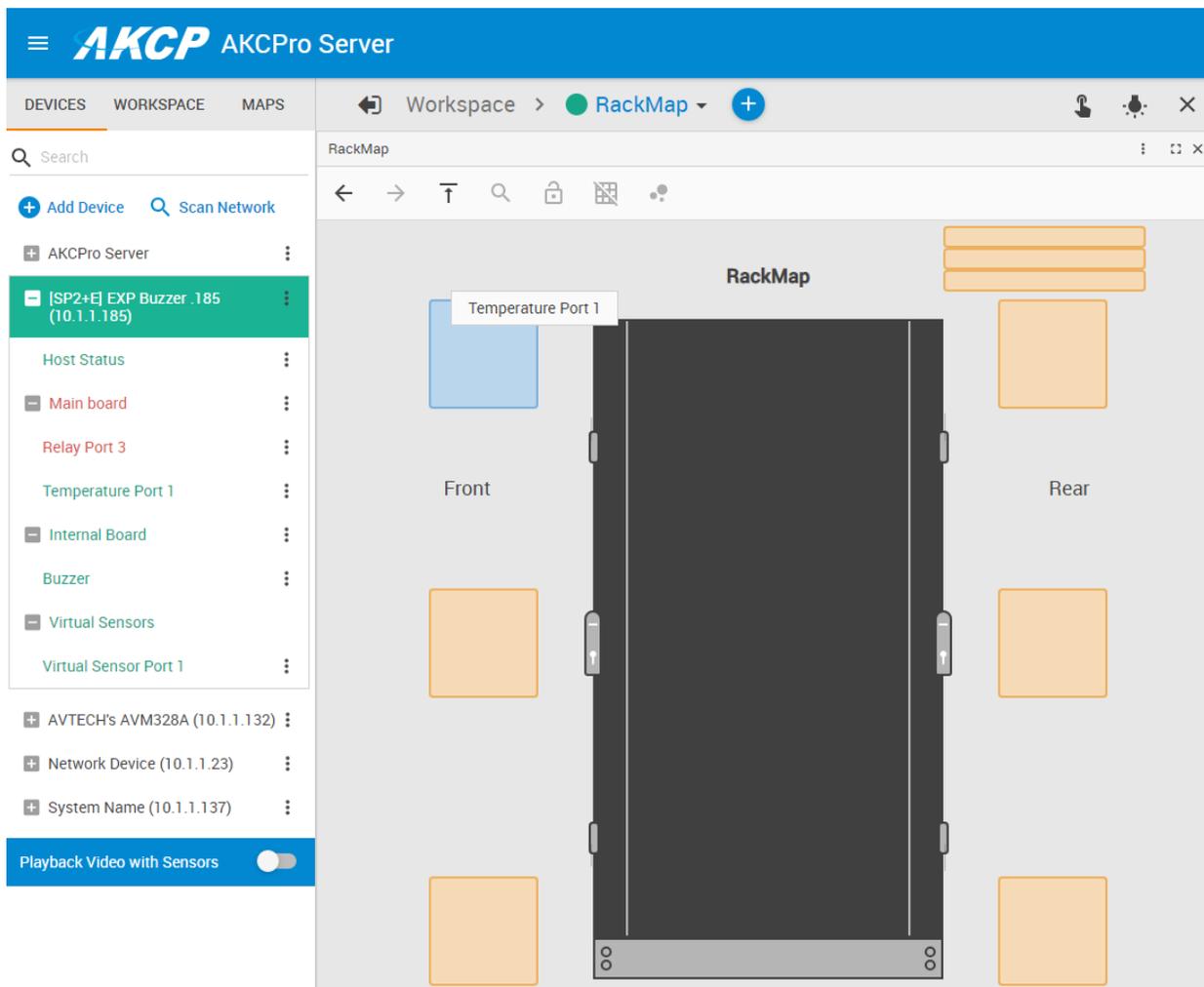
Additional 3 sensors can be dragged & dropped in the top right corner (only supported types):
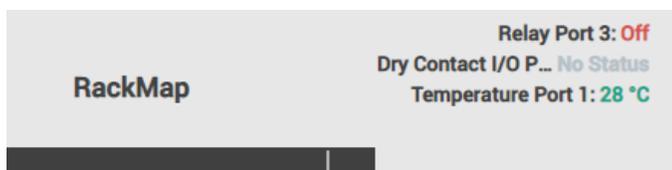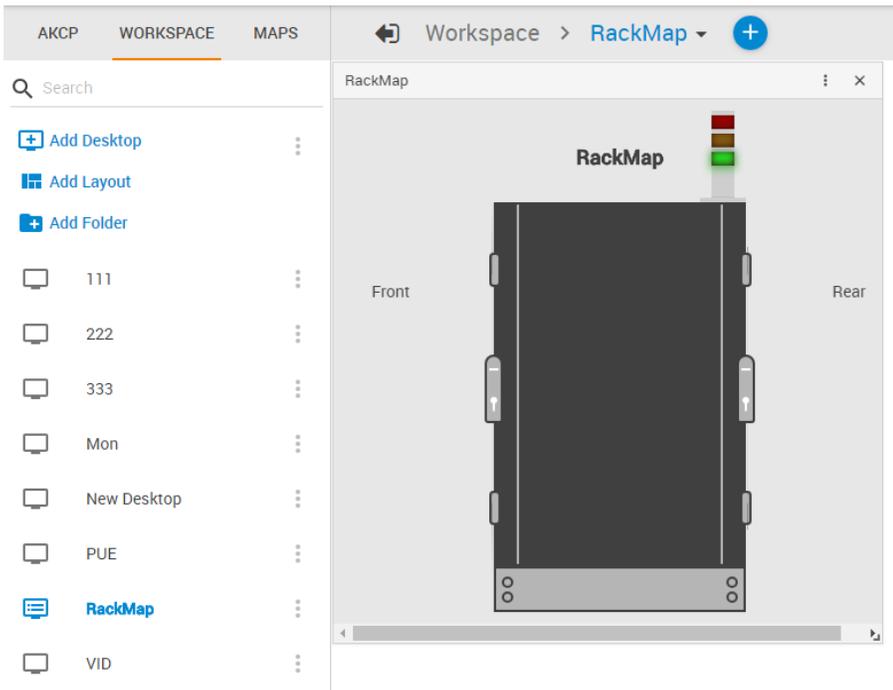
This example picture shows a Sensor Status Light added to a Rack Map.

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

E-learning video:
Thermal Maps in APS
https://youtu.be/zDr3TwydBWU
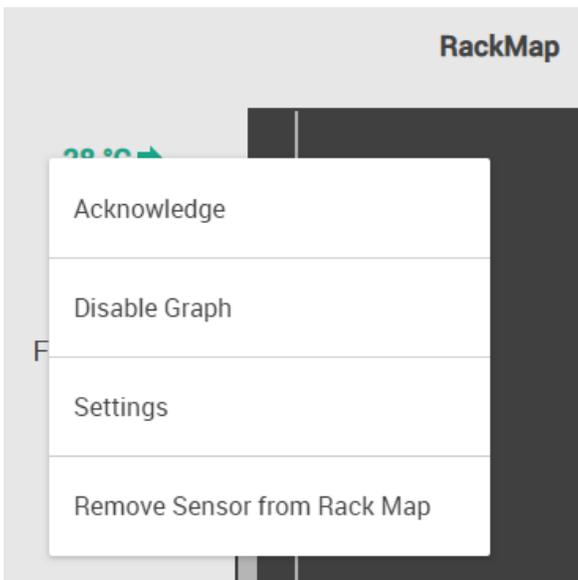
After you've added a sensor to the Rack Map, you can access its sensor menu. The contents will vary depending on the sensor type, for example you can directly control Relay type sensors.

Common options are to manage graphing, sensor settings, acknowledge status and to remove the sensor from the Rack Map.

Assets

Assets represent any other devices and equipment you have installed in the rack.
You can add any number of assets to your Rack Map.
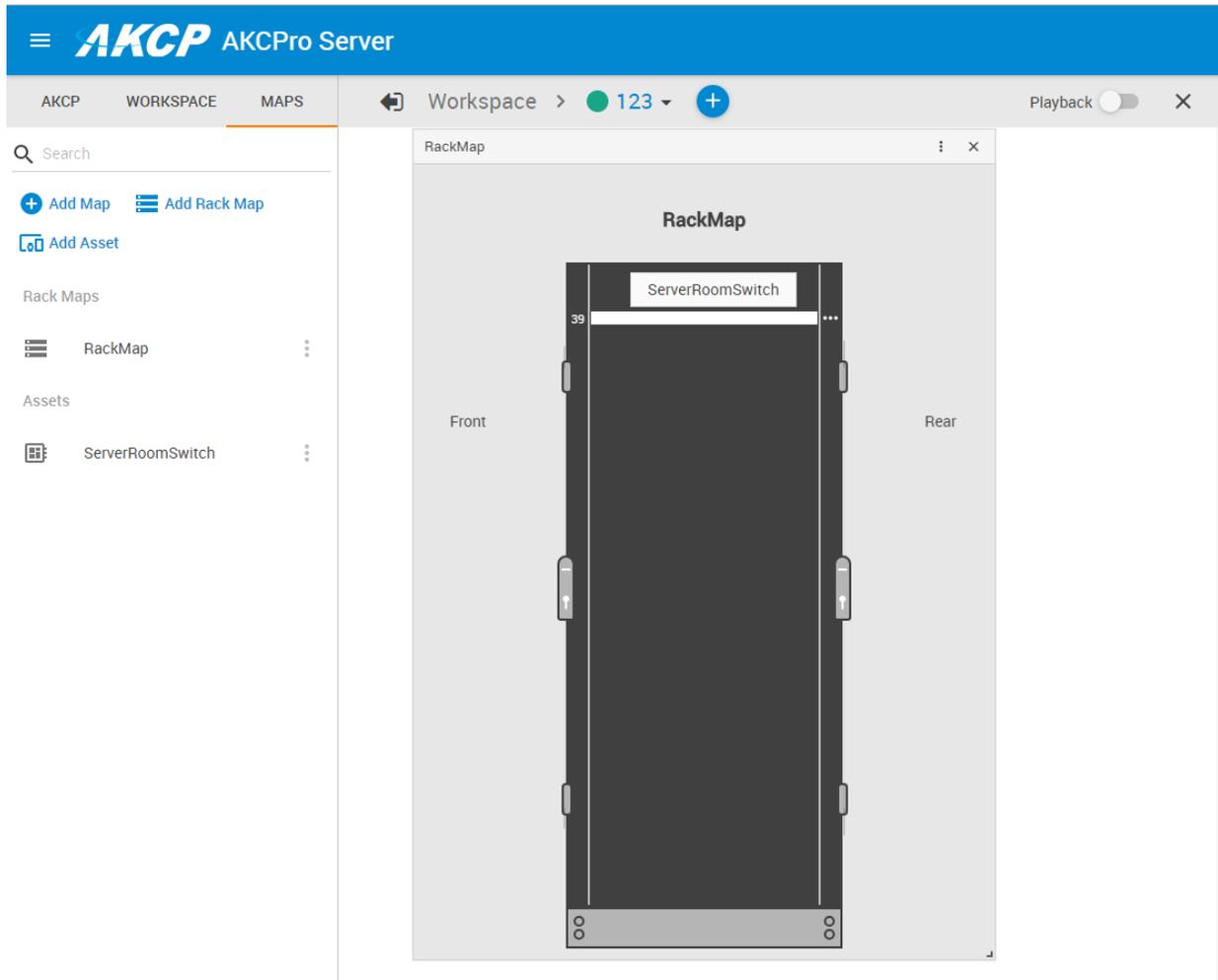
Click on the **Add Asset** button under the Maps tab to add an asset.

Another way to add an asset is by right-clicking on the Rack Map, and on the popup menu click "Add Asset". This way you don't need to drag and drop the created asset, it will appear in the Rack Map where you created it.

E-learning videos: Asset Management overview and advanced Rack Map features
https://youtu.be/ptPK9L94Q4o
https://youtu.be/cqPVhelS1Zg
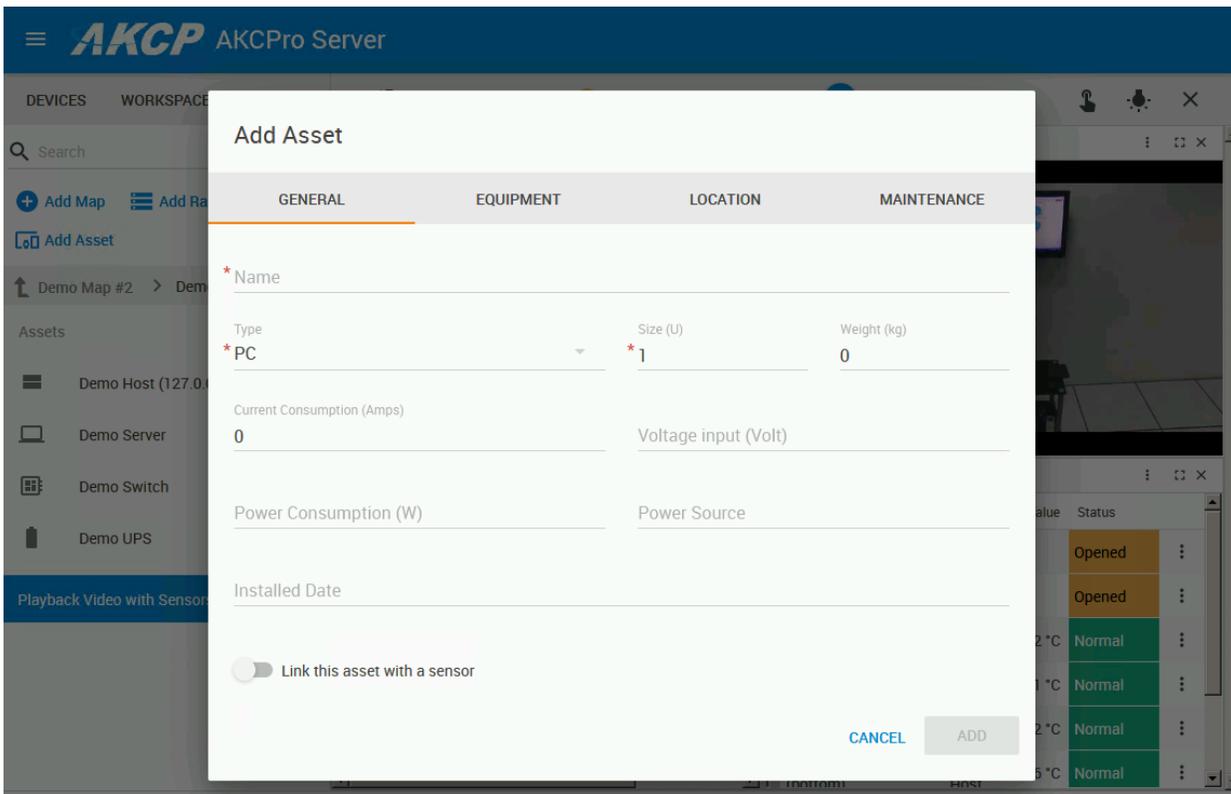
You can choose from many types of assets that would best describe the kind of equipment you have (not all options are shown on the picture).

The required fields are marked with a star * the other fields are optional (see below).

As an example, we'll show a server room switch's asset configuration.

The asset name, type and size are mandatory options, but the rest are optional.

You can define the size (in rack units), weight and current consumption of the device (if any).
As the power source, you can usually describe the PDU or connector socket.
You can also set an installation date and time when it was installed in the rack.

On newer APS versions, additional detailed information can be added in the other tabs (Equipment, Location, Maintenance), but these fields are also optional.

You can also link the asset with a sensor, then you'll be able to see the sensor's status and readings directly on the RackMap.

After you created the asset, it will appear under the Maps tab.
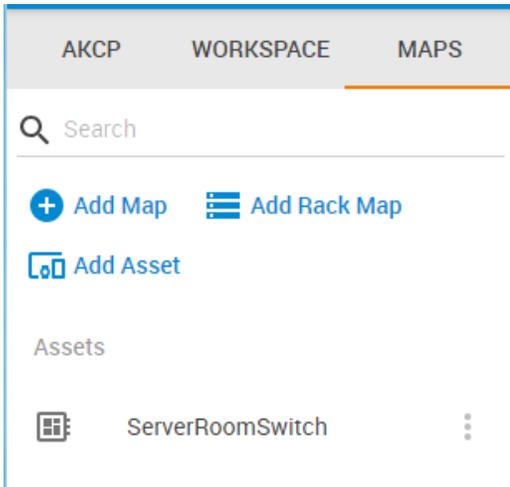
Now you can freely drag and drop it on a Rack Map.
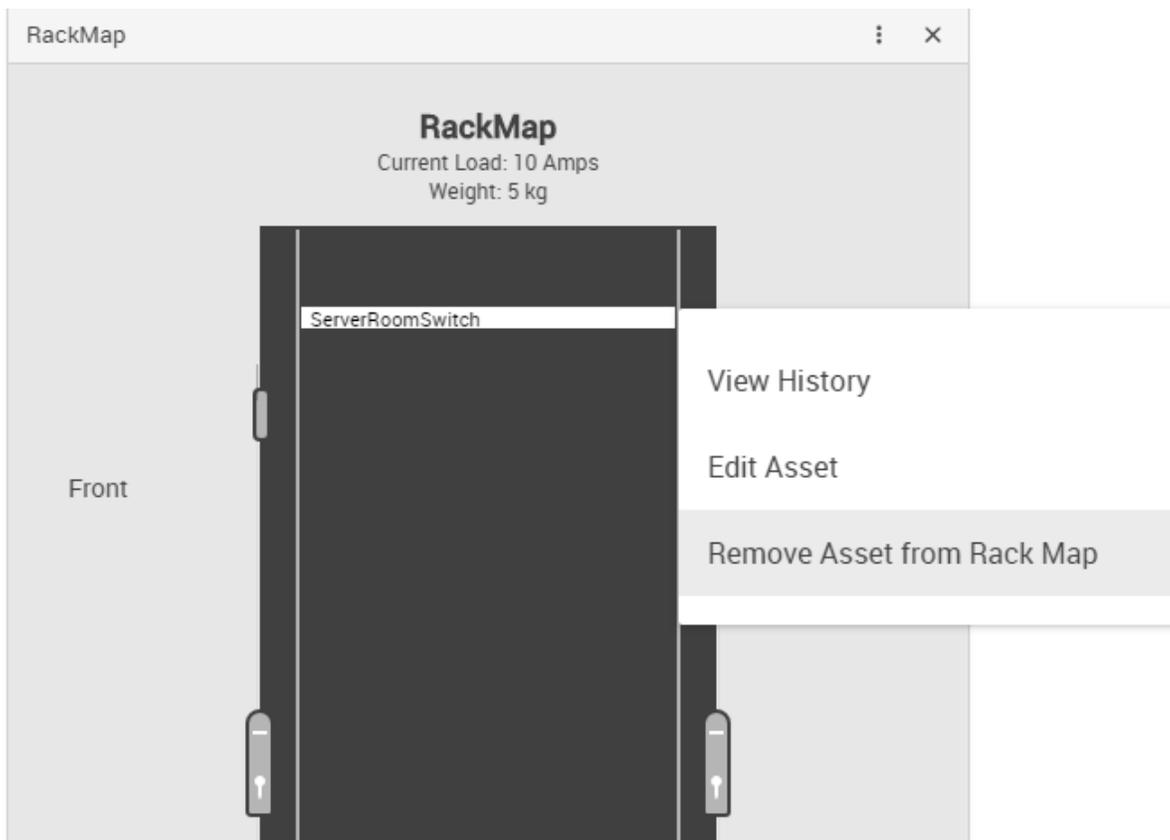
You can remove an asset from the Rack Map by using its popup menu.
This won't delete the asset from your list, only removes it from the Rack Map.
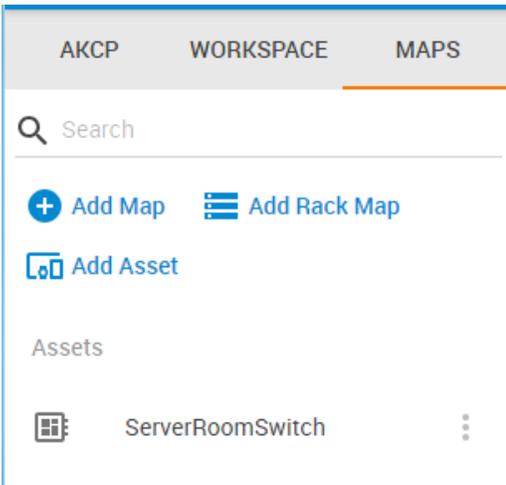
With every asset's menu you can edit, delete and export them, and view the change tracking (see below).

Asset change tracking
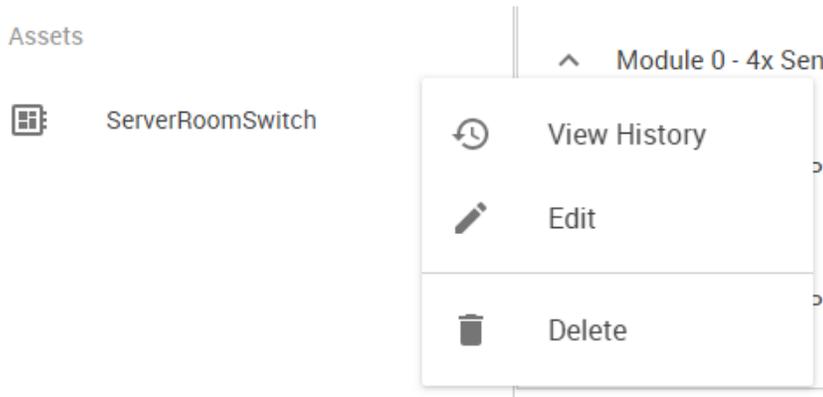
There's also a change tracking feature for each asset.
You can access it by clicking **View History** under its popup menu.

ServerRoomSwitch

Q Search

↓ Date	Asset Comments/Notes	↑ User

No Items

CANCEL   ADD

By default the list is empty. You can add an entry with the **Add** button.

ServerRoomSwitch

Asset Comments/Notes
Installation

CANCEL   ADD

Then you can make your notes with your currently logged in user name.

ServerRoomSwitch

Q Search

↓ Date	Asset Comments/Notes	↑ User	
03/08/2018 14:53:05	Installation	Admin	🗑

CANCEL   ADD

The date and time will be fixed to the time when you added the notes, it cannot be changed.
You can delete any notes selectively, and add new ones.

Close the window with the **Cancel** button; your notes are already saved.

Managing maps

You could visually monitor sensors placed on a map where you can view their details. You can easily spot in a glance which sensor needs attention and at the same time tells you where it's located. Below we'll show how to add a map and place some sensors on it.
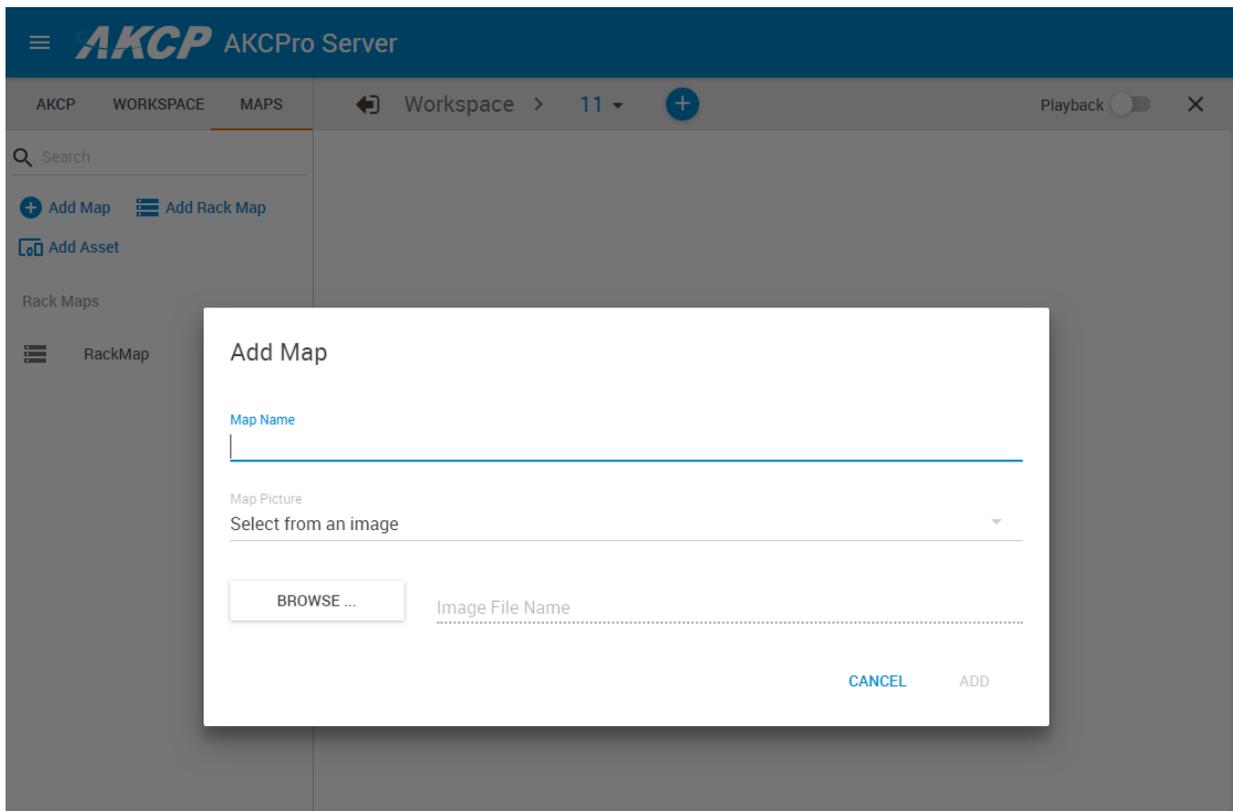
To add a map, click on the **Maps tab** and click on the '**Add Map**' link.

The Map Adding Wizard will then guide you through in adding an image as your map.
Enter a meaningful map name that will appear under the Maps tab.
Next choose the **Map Picture**. There are 3 options to choose from; the default is to select from an image file.

Map from an image

Click the '**Browse'** button to browse for a map image and a preview of the map will appear.
Only JPEG, GIF and BMP formats with a maximum size of 512kB are supported for upload.

Click the '**Add'** button to close the wizard and add the map.

Generate blank map

If you don't have a map image ready for upload, you can alternatively generate a new blank map. Set its height and width, and choose the background color.

As an example we'll create both map types.

In addition, a third Geographical Map type is available in APS. See below for details.
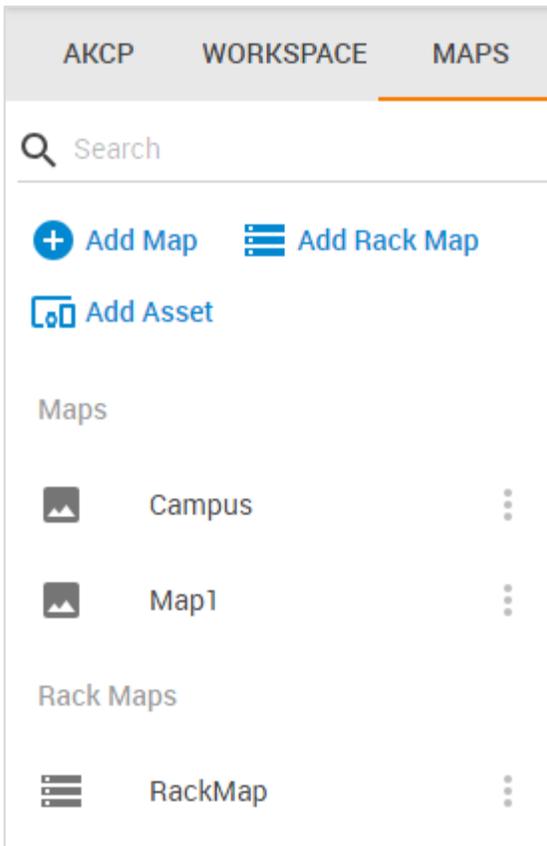
In this screenshot you can see under the **Maps tab** the added 'Campus' map with the image, and the 'Map1' which was created as a blank map.

AKCP   WORKSPACE   MAPS

Search

⊕ Add Map   ☰ Add Rack Map

⌷ Add Asset

Maps

🖾   Campus   ⋮

🖾   Map1   ⋮

Rack Maps

☰   RackMap   ⋮

Maps

🖾   Map1

Rack Maps

☰   RackMap

🖾   Open Map

✎   Edit
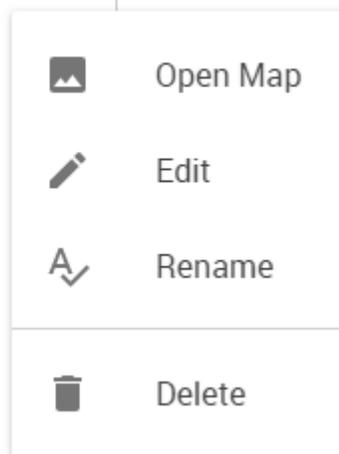
A✓   Rename

🗑   Delete

Every map has its own menu where you can Edit/Rename/Delete them.
If you click **Open Map** it will open the map on the currently viewed Desktop.

- 72 -
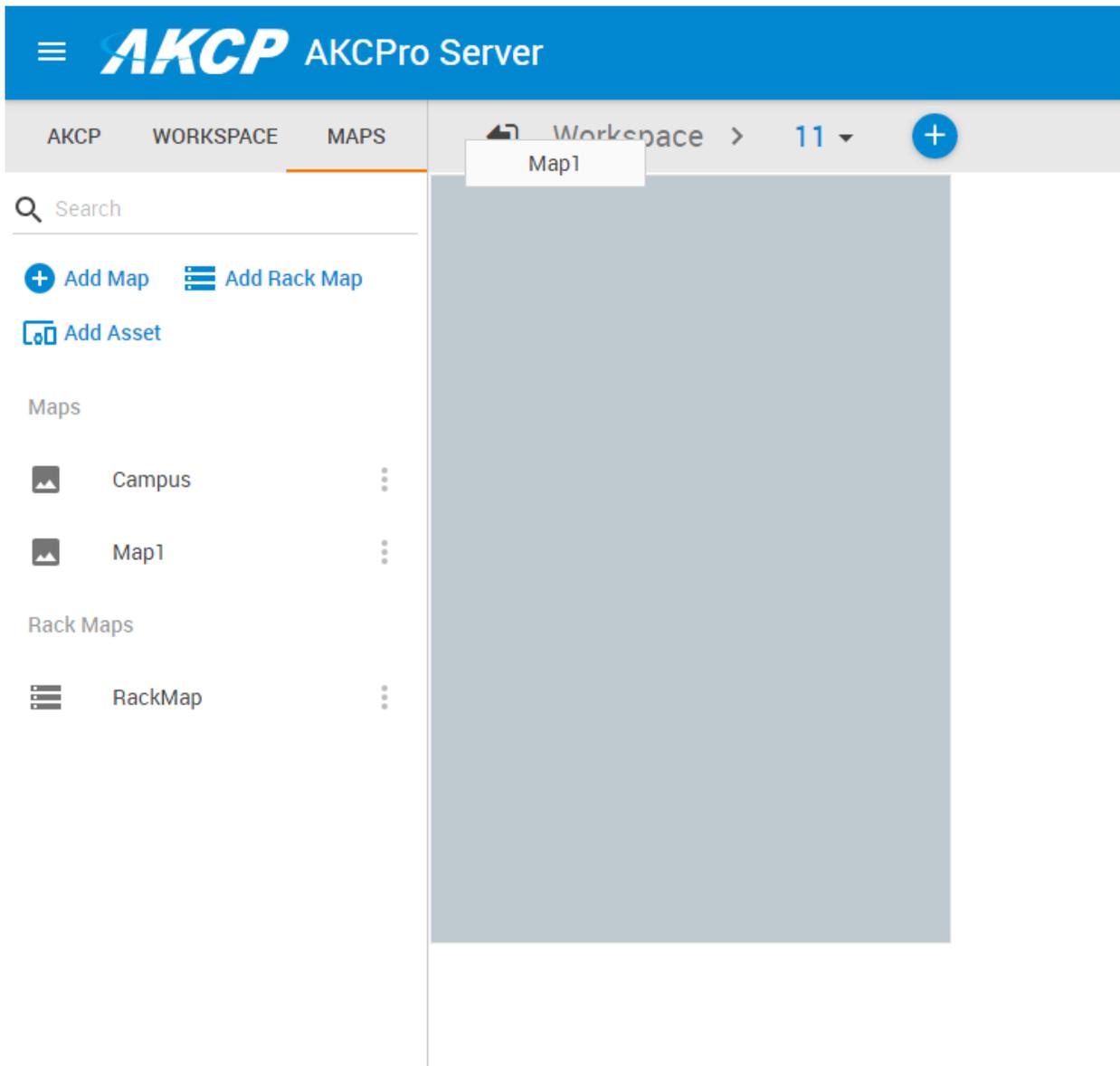
Now you can drag and drop the maps on any Desktop.
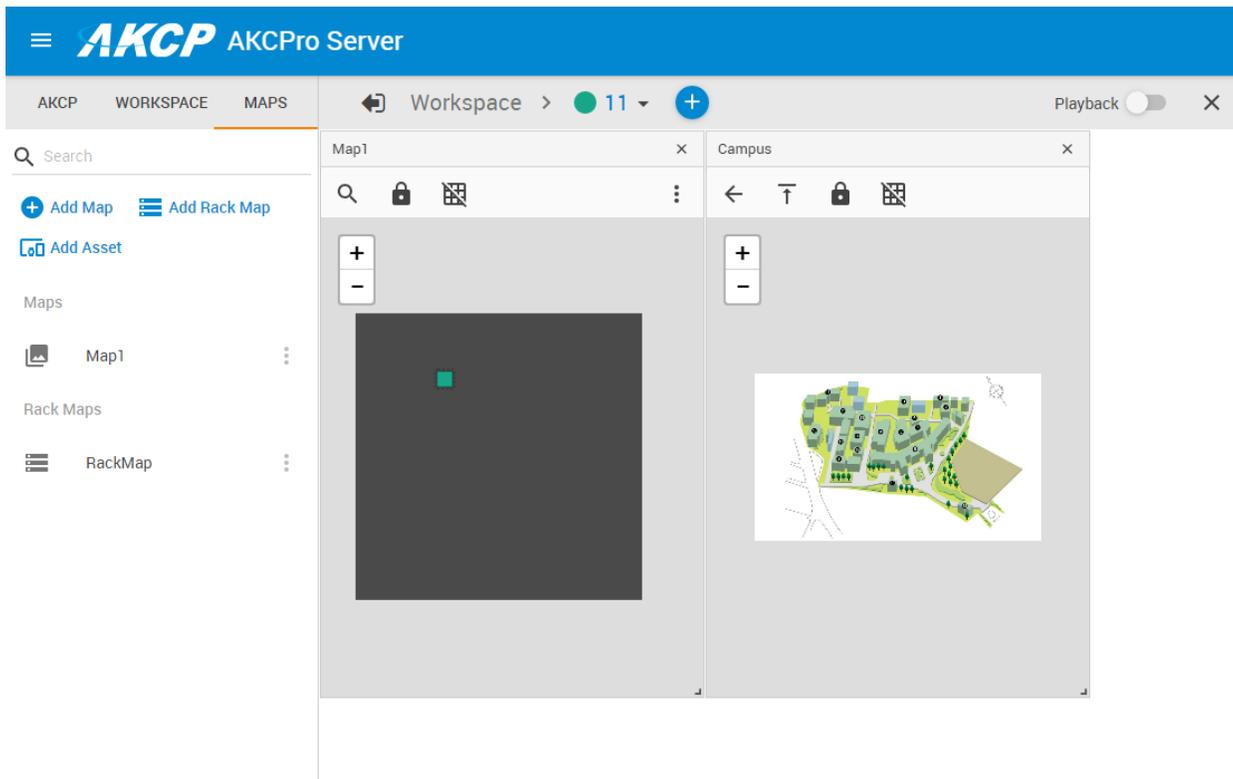
You can also drag other maps onto a map as sub maps; this is called drill down mapping. As an example we've made the 'Campus' map a child map of 'Map1' by dragging and dropping it on the other map.

You can also place Rack Maps and Desktops/Workspaces on other maps:
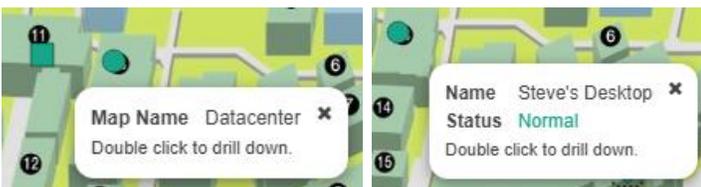
Then you can double click to open the Rack Map or Desktop that was placed on the map.

E-learning video: Drill down mapping
https://youtu.be/3MLqM3cdWkw

Drill down mapping with Geographical Map
https://youtu.be/mAYteMwmZYM

Map navigation

These buttons will help you to go back and forward in the map hierarchy.

This button will automatically search the maps for the closest critical device or sensor. We'll detail this feature below.

With this button you can turn on/off the map marker clustering when you're using Geographical Map (see below). If there are many map markers around the same location, they'll be shown as a single marker until you zoom in.
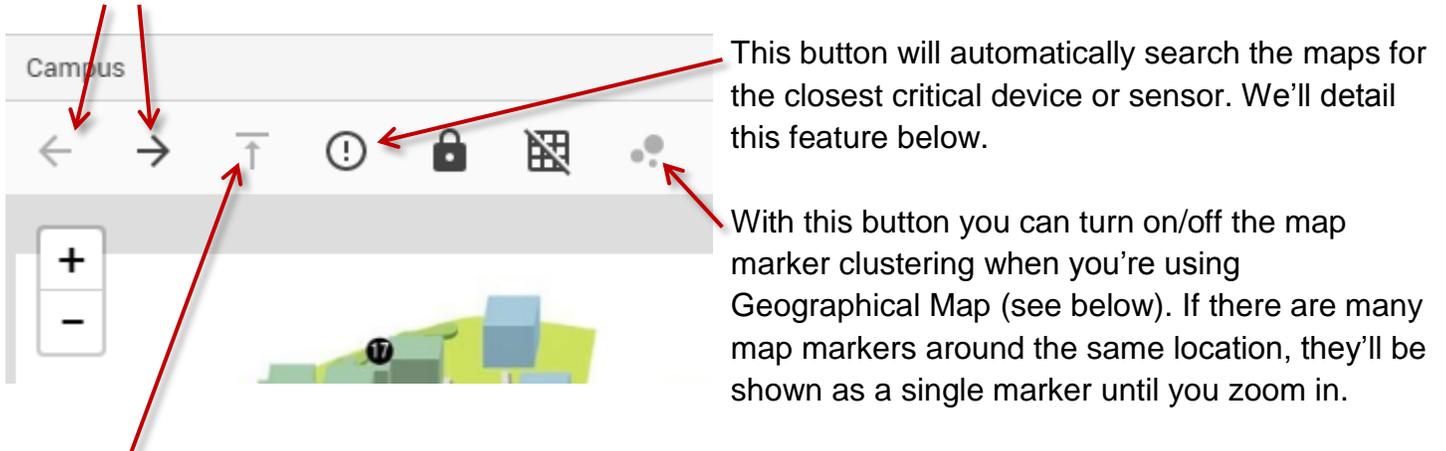
This button will help you to move to the top in the map hierarchy.

There's also zoom in/out, show grid lines and lock/unlock map buttons.
With the lock on, you cannot move the sensor markers on the map, so you'll first need to unlock it.

Drawing program

On newer APS versions, you'll find an additional pencil icon for the maps:
Clicking this icon will pop up a menu with these options:
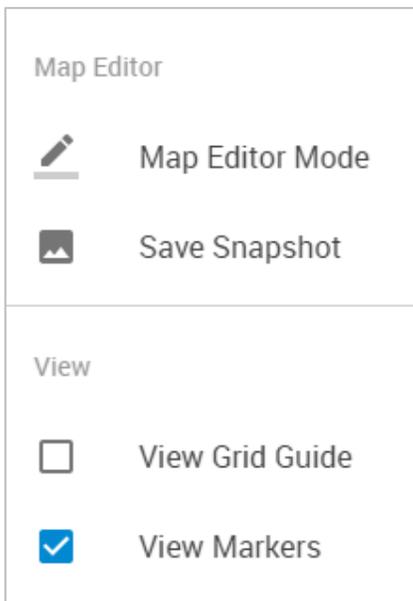
With the **Save Snapshot** you can save the current display as an image.
In **Map Editor Mode** you can load a web-based editor program (see below).

Note: it is recommended to enable the "View Grid Guide" option so that drawing horizontal or vertical lines will be easier.
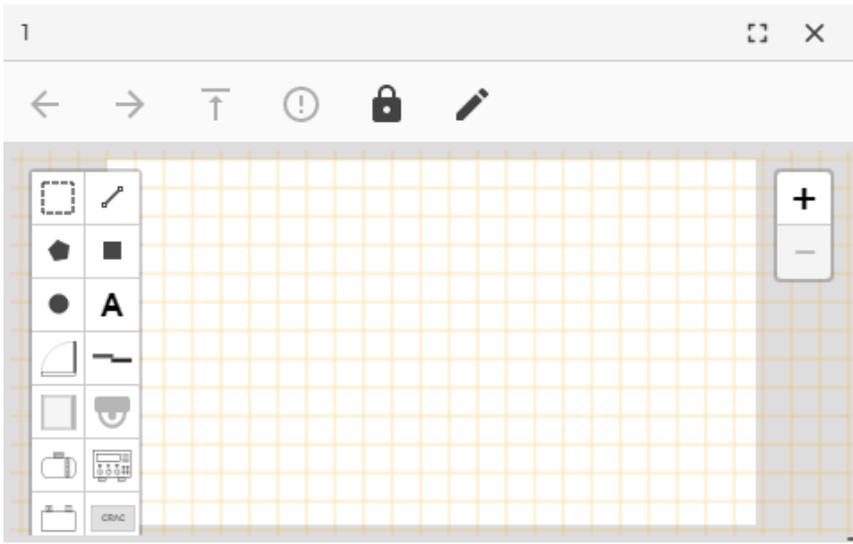
The drawing program has a toolbar where you can select the shapes, objects or text that you wish to place on the map.

Helpful text messages will be shown as you start drawing with the mouse:
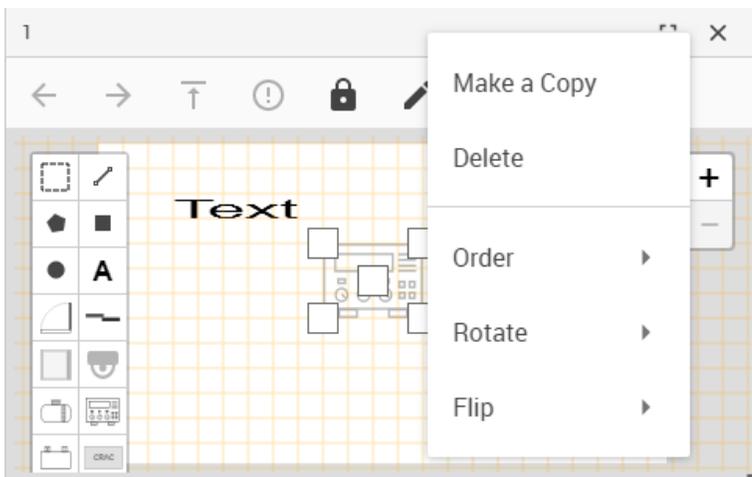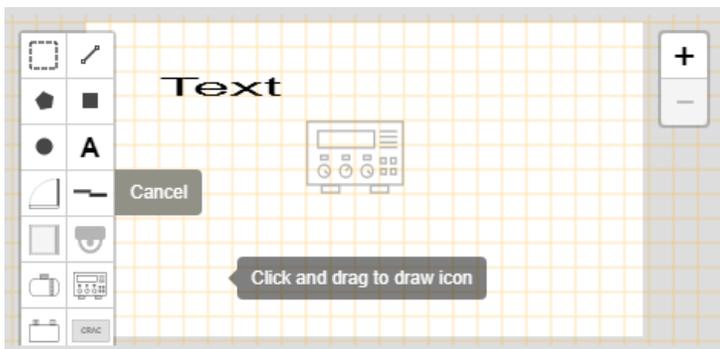
To modify an object, click or right-click on it:
To **delete**, you can press the 'delete' button on the keyboard or right click the object to access its popup menu.
Each object has a popup menu to **delete**, **make copy** and **rotate** them.
For **moving** objects, you just need to click and drag them from their middle point.
To **resize** objects, use the side points.

Geographical Map type
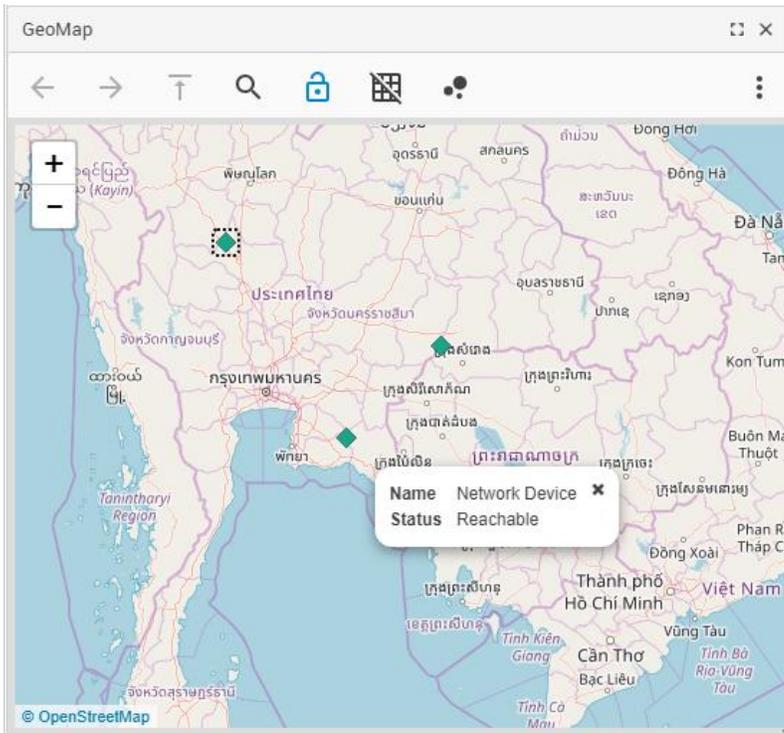
This is a new type of map and uses the OpenStreetMap as the source.
You can drag and drop any units, sensors or cameras anywhere on the world map as you would on other map types.
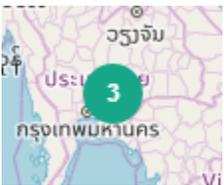
Map markers can cluster together when you zoom out of the map - this clustering can be optionally turned off.

The GPS coordinates will be saved in the unit's System tab if supported (see below) - currently SP+ devices with newer firmware (2018 September) support this feature.

This screenshot shows the GPS latitude/longitude coordinates which are saved into a SP+ unit's settings in the General Settings Tab.

Adding Sensors to the map

Now we have added maps, we will add some sensor data to these maps.
To add sensors to a map the process is exactly the same as adding sensors to any desktop. Simply drag and drop your chosen sensor to a specific place within your map.
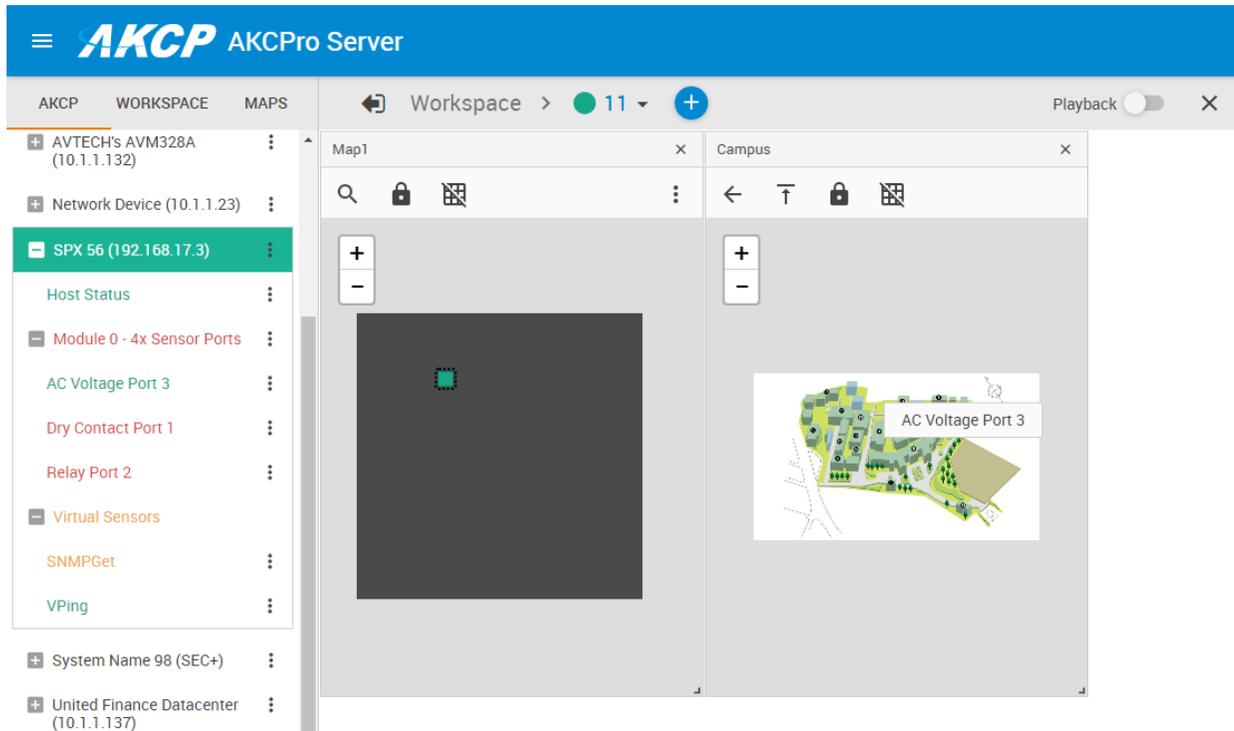
In the example below you can see we have added an AC Voltage sensor from a connected SPX+ to the map by dragging and dropping it on the 'Campus' map.

By hovering your mouse over, or right clicking on the sensor icon and selecting 'Show Marker Info' you will see the sensor information displayed, as shown below:
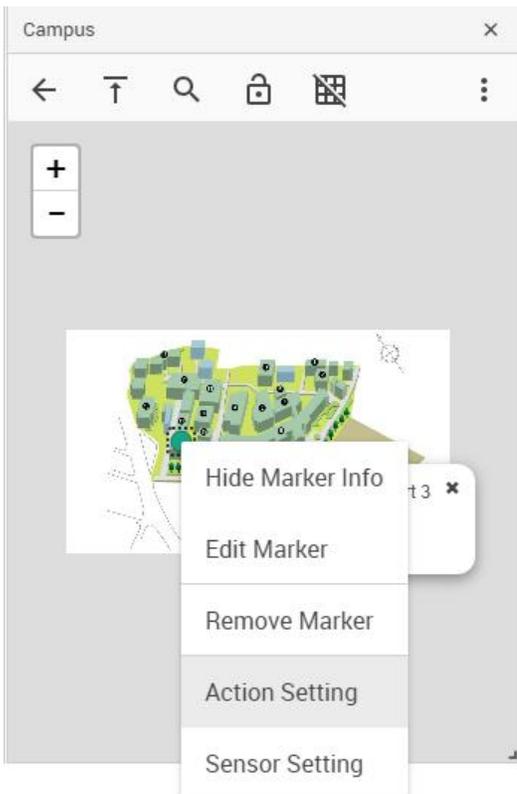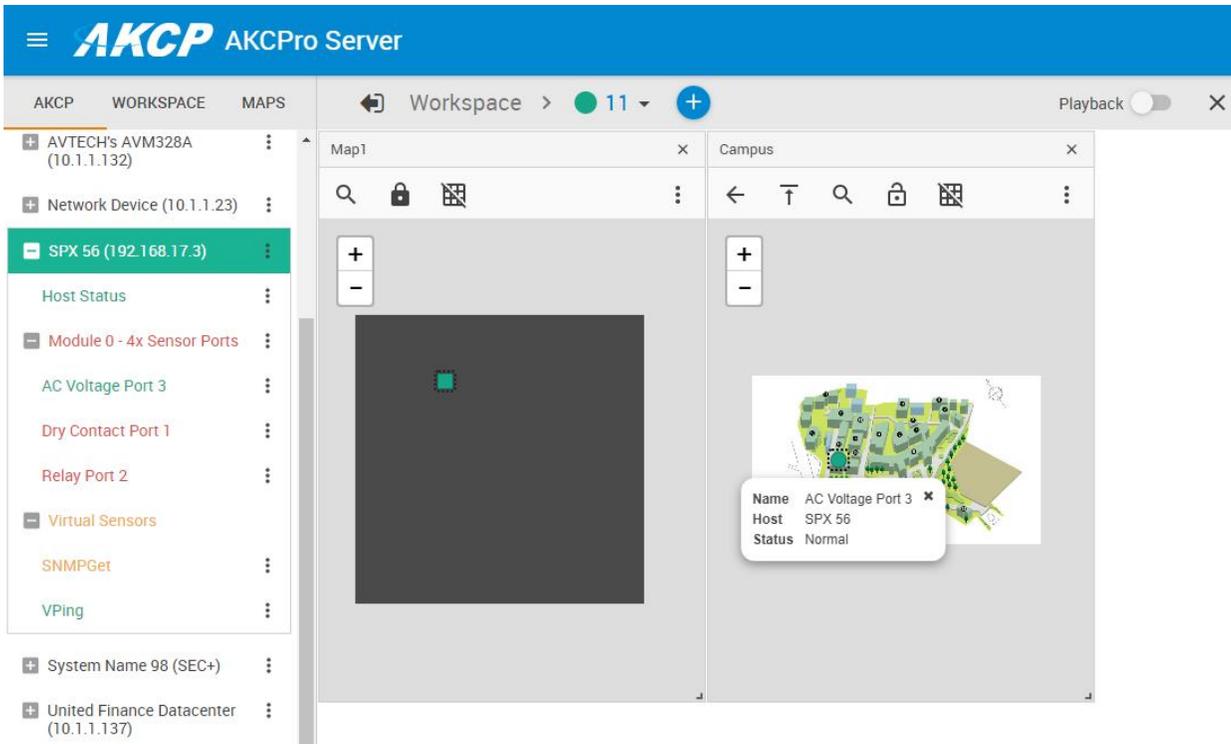
From the sensors right click menu you can show/hide the marker info, remove it from the map, change the sensor's settings and add a custom action that you can perform directly from the map (more on this feature later).

Note: the icon's color will show the current status of the sensor it's monitoring, and it cannot be changed. You can only add a colored additional text to it (see below).

Now that we can see our sensor data within the map window we will add a custom text to the icon. To do this we need to open the '**Edit Marker**' option from the sensor's right click menu.

After selecting this option a new window will be presented.

In this window you can select which type of icon you would like to use.

As an example, we'll change its icon to diamond shape and flashing, and add custom text with another color.

Choose diamond shape and click **Next**.

Here you can make changes to the icon.

As an example we'll change the size, add some extra text with color and set it flashing (click on the **Color** button to pick a color):

Marker Icon Setting

✓ Icon ———————————— ✓ Option ———————————— ③ Apply Default

Make this setting to be a default for the following types

☐ Temperature	SELECT ALL
☐ Humidity	UNSELECT ALL
☐ 4-20 mA	
☐ Digital Voltmeter	
☐ AC Voltage	
☐ RMS Voltage 7763	
☐ RMS Current 7763	
☐ Energy Meter 7763	
☐ Watt-Hour Meter 7763	

☐ Overwrite all existing icon settings to default for selected types

BACK   FINISH   CANCEL

Campus   ×

← T̄ 🔍 🔒 ▦   ⋮

+
−
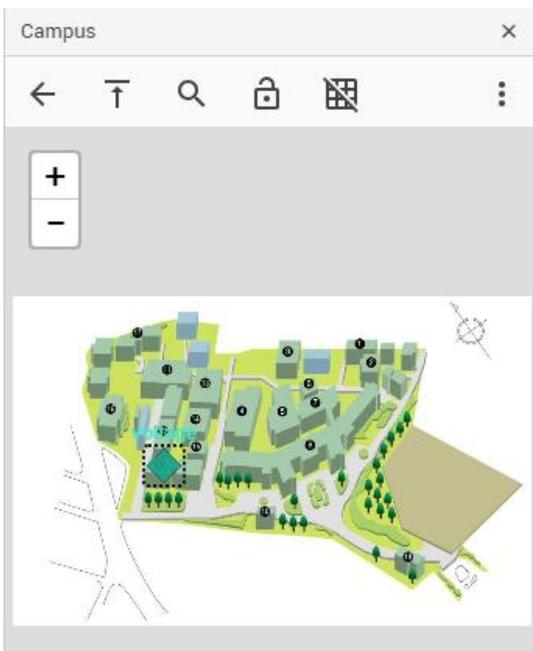
If you wish, you could make this style default for other sensor types.
To change only this icon, click on **Finish**.

Now as you can see on the picture on the left, the sensor marker has changed, and the additional text is displayed on it.

Marker Icon Setting

✓ Icon ——— ✓ Option ——— ③ Select Image ——— ④ Apply Default

Select an image for each status

Normal	∨
High Warning	∨
High Critical	∨
Low Warning	∨
Low Critical	∨

* Please select an image for all status

BACK   NEXT   CANCEL

If you choose the '**Image**' type icon setting, you'll have to choose an image for each sensor status:

Map Icon Image

Images

Please enter 1 item.

ADD   REMOVE   OK   CANCEL

Map Action Setting

On the maps you can place custom actions to directly execute them.
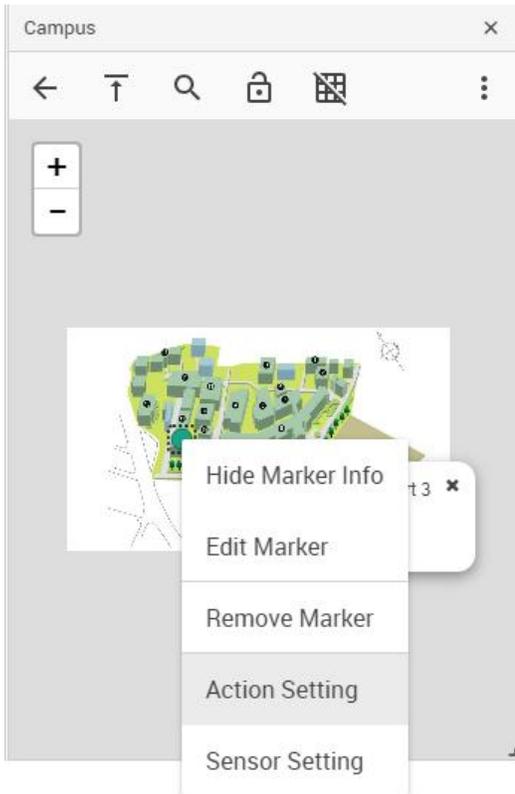
Right click on a sensor and select **'Action Setting'** from the popup menu.

This will show a selection dialog (see below) where you can assign any existing action to this map marker.
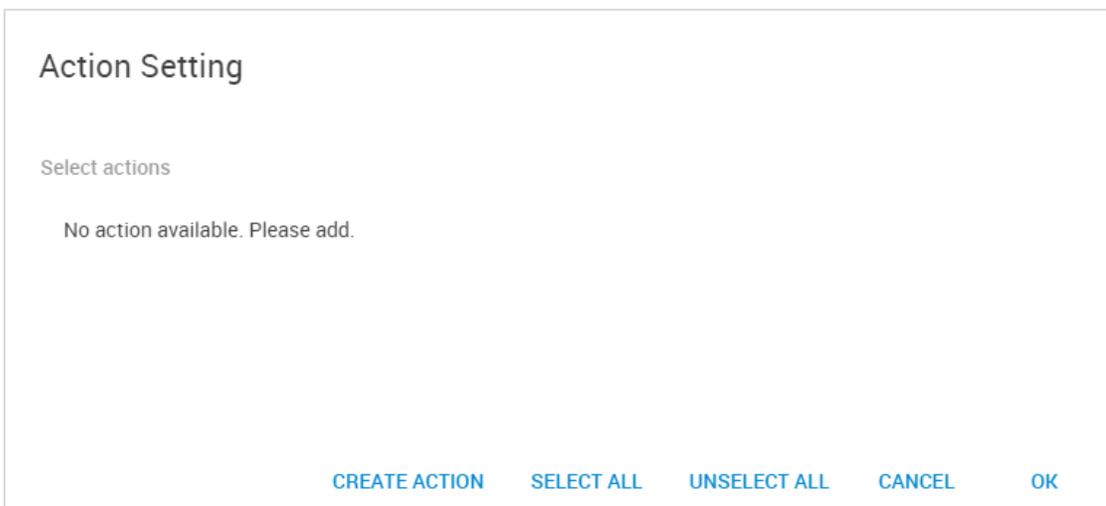
By default no action is assigned. If you haven't created any actions before, click on **Create Action** to add at least one action.

This will open the Actions page on a new browser tab, where you can create your action. More about configuring the actions can be found below in this manual.
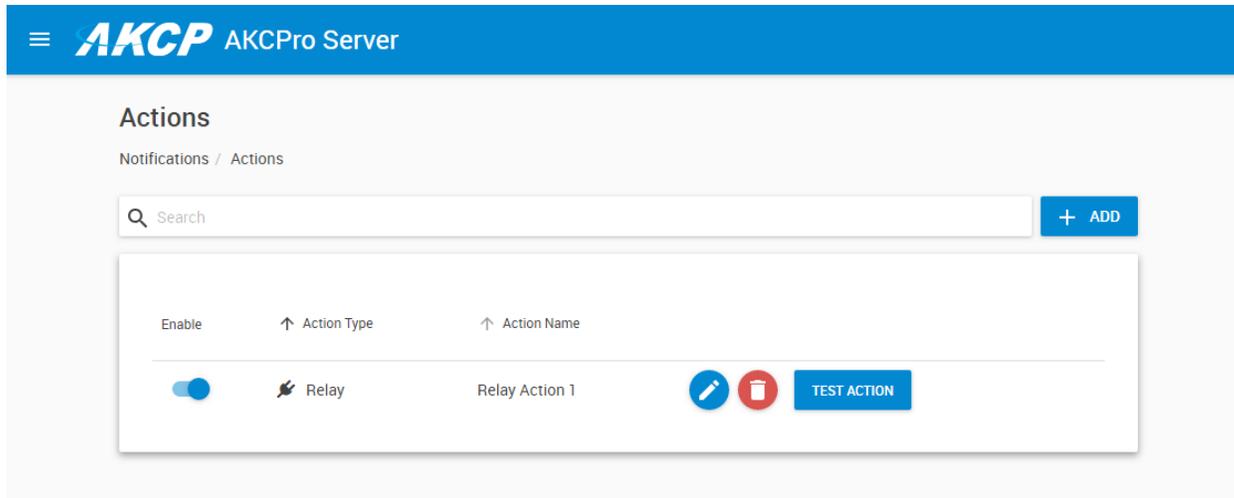
Here we've added a Relay action for demonstrating this feature. You can close the Actions page after your action is created.
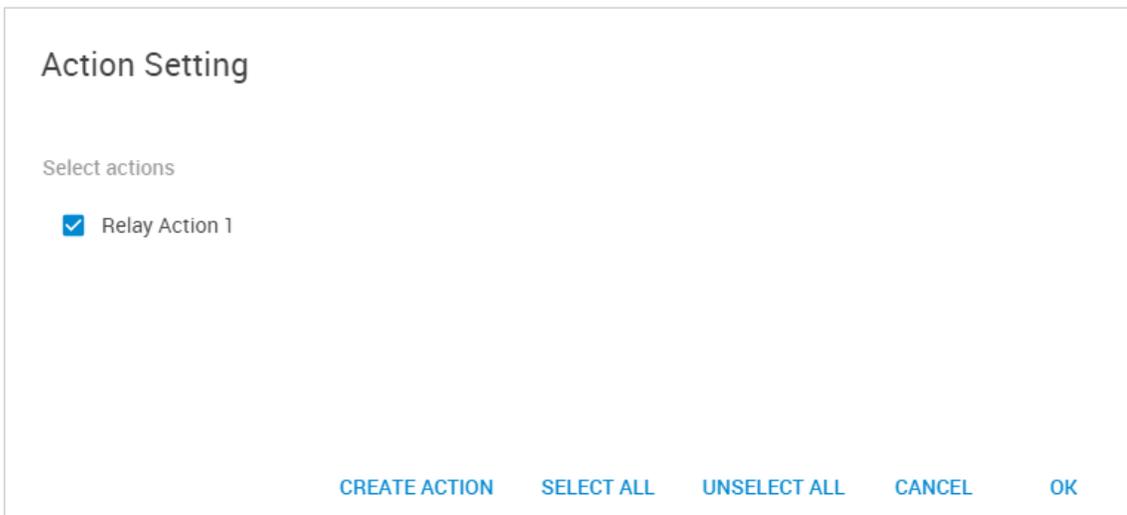
The new action will appear in the list; place a checkmark to it to select it, and then press OK.

If you already created some actions before, they'll be shown here.
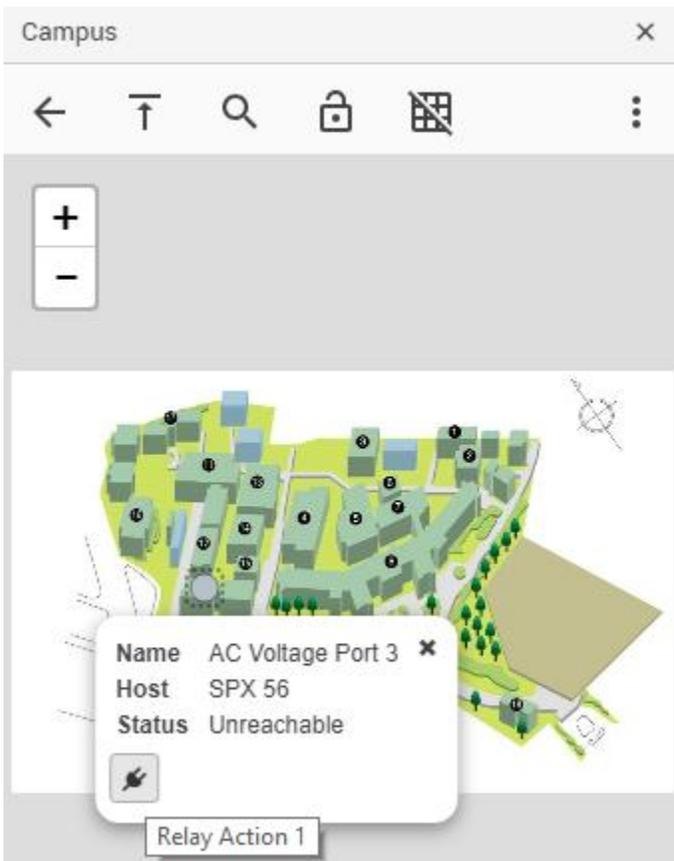
The new action will appear under the Sensor Marker Info popup.
You can click on the button to directly execute the action from the map.
The displayed icon will reflect the action type.

Locating critical sensors on a map

Every map has an exclamation icon (or magnifier icon in older versions) that will let you quickly find a sensor or device with critical status on a map, or sub-map.
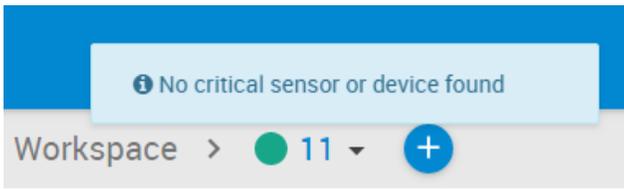
If there are no critical sensors or devices found, you'll get a popup like this.
Note the green marker next to the Desktop name; it also reflects the sensor statuses on the given desktop.
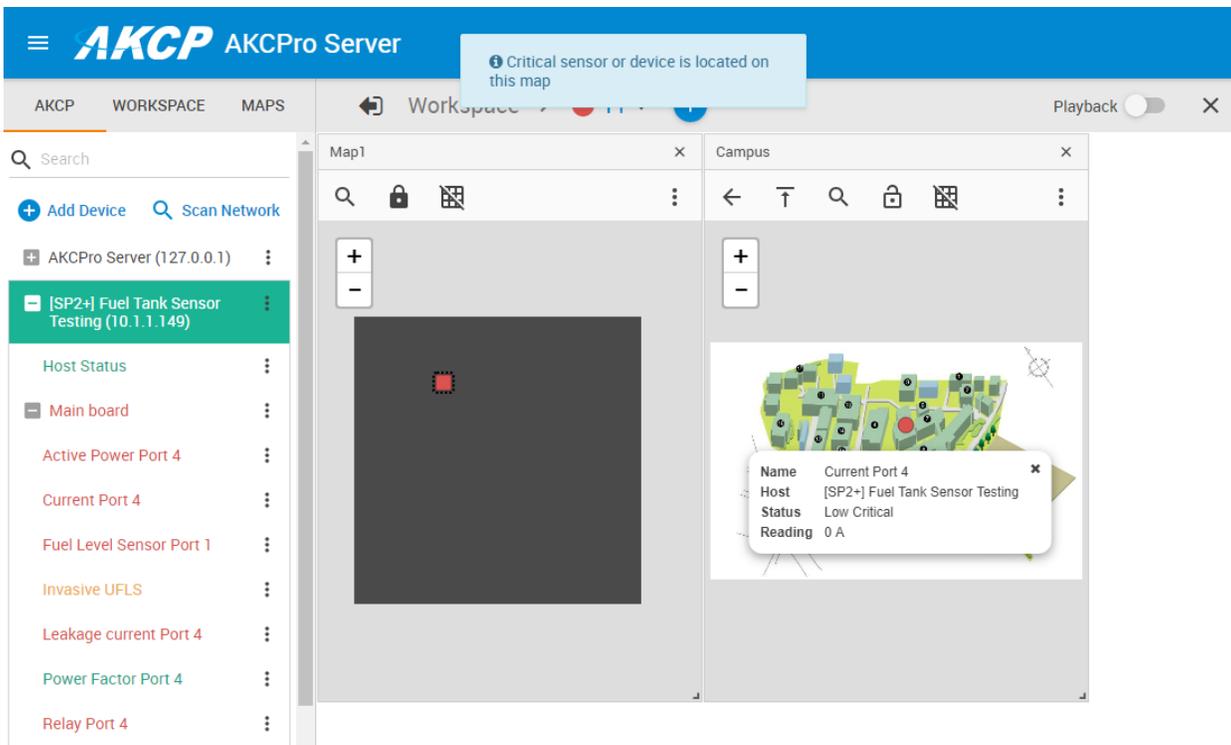
In case a sensor is in critical status and you press the locate icon, the system will show the map with the critical sensor and says in the popup that a critical sensor was found. Also note the Desktop's marker which turned red.

6. Playback feature

The playback function will let you replay the recorded video, along with any monitored sensor's status changes and logs. The Playback mode will sync all video and sensor statuses on the marker time in all opened windows.

Playback Video with Sensors ⬤

Click on the Playback slider to go into Playback mode.

Note: the camera's live video feed needs to be dragged to a desktop, and Recording Policies has to be configured to be able to use video playback, but sensor status playback always works.

Very Important Note: If you close a gadget, host or camera window on a desktop, it will not reappear in Playback or normal mode!
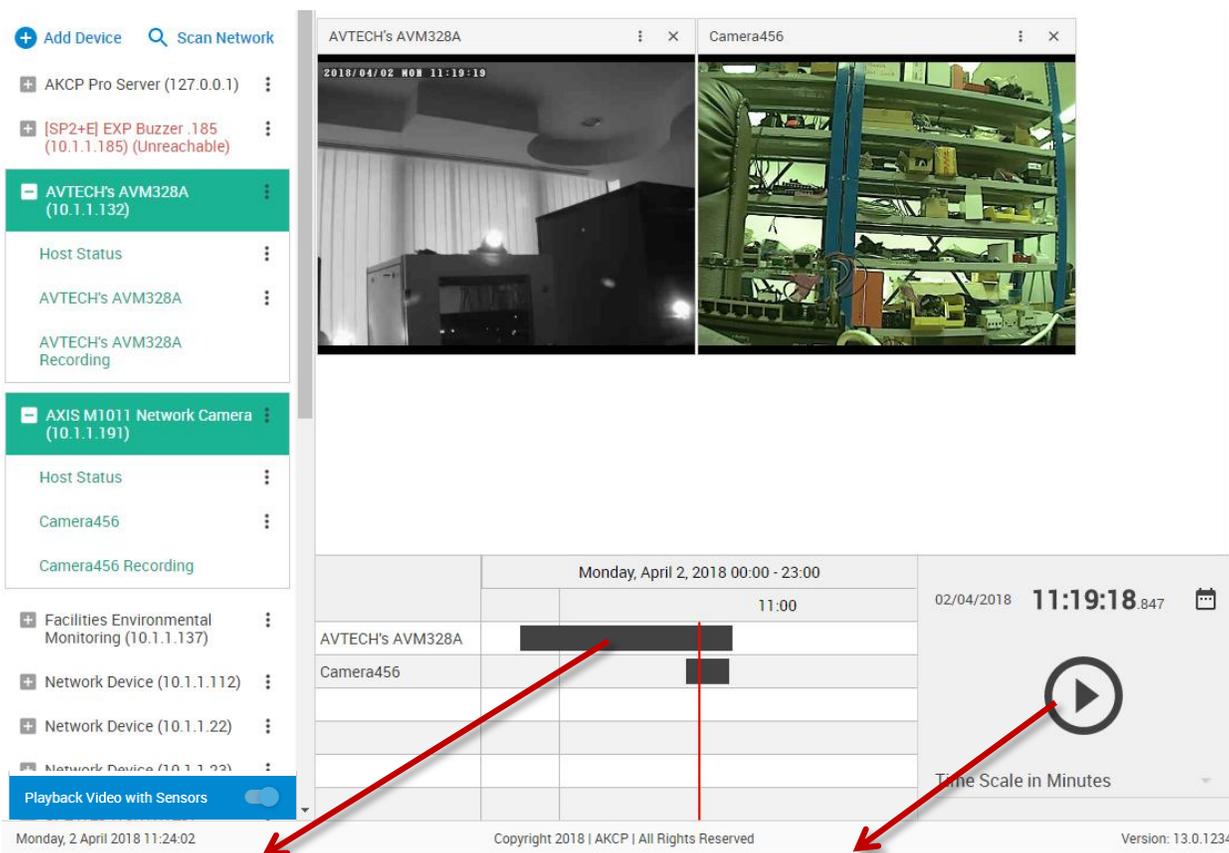
Timeline
Easily view what events take place at that time. You can drag the timeline with the mouse when seeking each critical event. There's a timeline per sensor and per camera.

Video Controller
The Controller will let you quickly choose a given date and time. You can also move the timescale with the mouse, and change the display between minutes/hours/days etc.

7. Menu and options walkthrough

Menu navigation

The Web UI and the menu structure is similar to the one on the SP+ family devices.

To open the menu, click on the three horizontal lines in the upper left corner: ☰
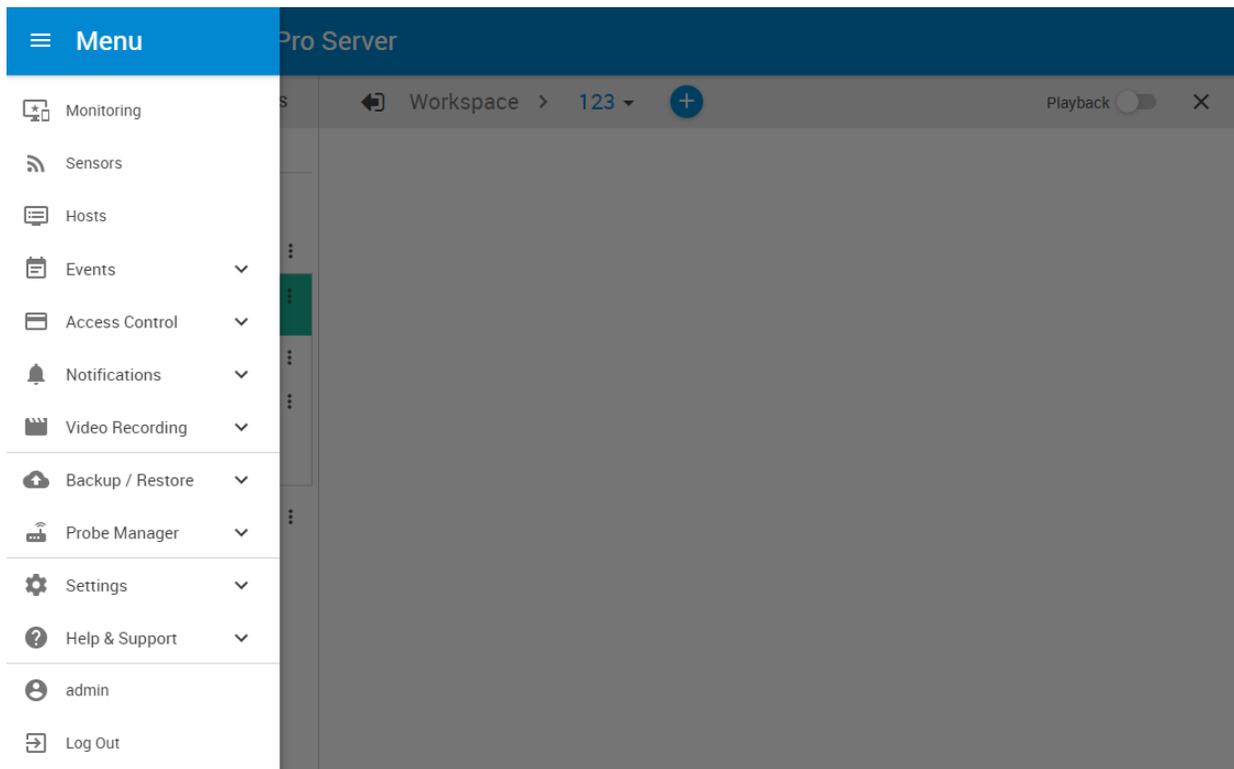
This will bring up the full menu for navigation.

You can always see the currently logged in user's name (and picture) at the bottom of the menu. Clicking on it will take you to the User Settings menu (see below in this manual).

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 APS Web UI.

7.1. Hosts menu

The contents of this page will vary depending on the selected unit type that has been added to the APS console, and is available for configuring.

Options from the SP+ and SEC5 product family can be configured with this menu.

You can select a host to configure from the drop-down menu at the upper right corner:

If there are no available hosts added yet to APS, it will just display a message "No hosts available":

7.2. Sensors menu

The contents of this page will vary depending on the selected unit type that has been added to the APS console, and has available sensors for configuring.
Sensor configuration options are nearly identical to the SP+ family's.
As with the Hosts menu, you can choose the host to configure with the drop-down menu at the top.

If there are no units added with sensors, you won't see any configurable sensors here:

7.3. Events menu
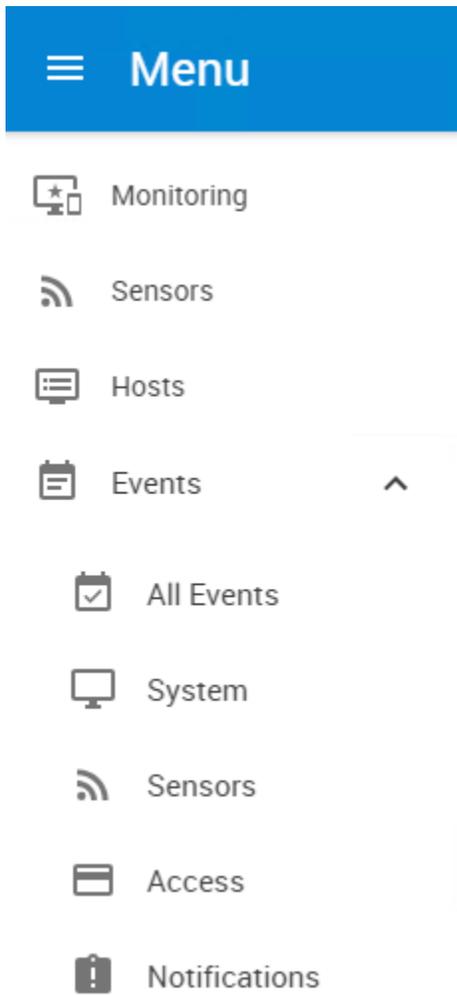
All Events

Events / All Events

Q Search

FILTER   **EXPORT**

Date/Time	Message	Host	Level
02/04/2018 10:50:01	'Increase' is now 1.00 Unit, status is now Low Critical	AKCP Pro Server (127.0.0.1)	Critical
02/04/2018 10:49:41	'Increase' is now 81.00 Unit, status is now High Critical	AKCP Pro Server (127.0.0.1)	Critical
02/04/2018 10:49:20	'Increase' is now 60.00 Unit, status is now High Warning	AKCP Pro Server (127.0.0.1)	Warning
02/04/2018 10:49:05	'Increase' is now 45.00 Unit, status is now Normal	AKCP Pro Server (127.0.0.1)	Information
02/04/2018 10:48:50	'Increase' is now 30.00 Unit, status is now Low Warning	AKCP Pro Server (127.0.0.1)	Warning
02/04/2018 10:48:22	'Increase' is now 2.00 Unit, status is now Low Critical	AKCP Pro Server (127.0.0.1)	Critical
02/04/2018 10:48:01	'Increase' is now 81.00 Unit, status is now High Critical	AKCP Pro Server (127.0.0.1)	Critical
02/04/2018 10:47:41	'Increase' is now 61.00 Unit, status is now High Warning	AKCP Pro Server (127.0.0.1)	Warning
02/04/2018 10:47:26	'Increase' is now 46.00 Unit, status is now Normal	AKCP Pro Server (127.0.0.1)	Information
02/04/2018 10:47:06	'Increase' is now 25.00 Unit, status is now Low Warning	AKCP Pro Server (127.0.0.1)	Warning
02/04/2018 10:46:43	'Increase' is now 3.00 Unit, status is now Low Critical	AKCP Pro Server (127.0.0.1)	Critical
02/04/2018 10:46:23	'Increase' is now 83.00 Unit, status is now High Critical	AKCP Pro Server (127.0.0.1)	Critical
02/04/2018 10:46:18	'V4' status is now Unreachable	TestDCU .72 (192.168.22.3)	Information
02/04/2018 10:46:18	'V3' status is now Unreachable	TestDCU .72 (192.168.22.3)	Information
02/04/2018 10:46:18	'V2' status is now Unreachable	TestDCU .72 (192.168.22.3)	Information
02/04/2018 10:46:18	'V1' status is now Unreachable	TestDCU .72 (192.168.22.3)	Information
02/04/2018 10:46:18	Door Control Unit(192.168.22.3) is now offline	TestDCU .72 (192.168.22.3)	Information
02/04/2018 10:46:18	'Airflow Port 652' status is now Unreachable	TestDCU .72 (192.168.22.3)	Information
02/04/2018 10:46:18	'Temperature Port 2' is now 0.00 °C, status is now Unreachable	TestDCU .72 (192.168.22.3)	Information
02/04/2018 10:46:18	'Door Port 1 (Tamper Detector)' status is now Unreachable	TestDCU .72 (192.168.22.3)	Information

|< 1 2 3 4 5 6 7 8 9 10 >| Display 20

Event logging is an important part of APS and is very helpful for troubleshooting. It allows you to review what events happened on the system, and when.

Events by category:

All Events - contains all logs sorted by date and time; you can filter the logs for example by specifying the start- and end dates to narrow the list, or by choosing a specific log category.

System - contains the logs for the APS system events, such as reboot, user logins, system update etc.

Sensors - contains logs for all sensor related events, such as status changes, online/offline etc. and the port number where the sensor is attached.

Access - contains logs for all user authentication-related events, such as access granted/denied.

Notifications - contains logs for the notifications and actions, for example the result of an email notification, heartbeat message or an SNMP Trap.

You can change the number of log entries displayed per page. The default is 20, it's possible to specify up to 50. Also you can filter the events further in the **Filter** options (see below).

Log Filtering

The easiest way to filter the logs is to start to type in the search field:

For example to find all logged events that contain the string 'camera'.

If you need more advanced filter options, click on the **Filter** button.
A popup window will be shown with all the filtering options.

You can define a custom filter to find the important logs easier.
It's possible to filter by:

- Date/time
- Log level
- Action type
- Sensor type and sensor status
- Door status
- Video recording status

For example, this log level filtering will only show Critical, Error and Warning statuses.

You can find additional examples for log filtering at the Access Control section of this manual.

Event Log Export
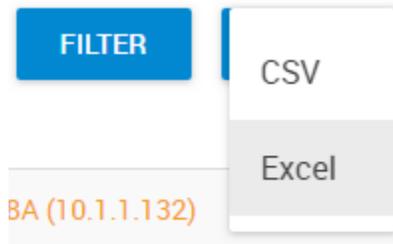
If you click on the **Export** button, a confirmation popup menu will appear, asking for the file format to export the log entries.

You can export the records as CSV file or Excel (XLS) file formats.

7.4. Access Control

Access Control Users and Groups overview

In this section we'll show how to use the Access Control Users and Groups feature of APS. This is mostly used for managing door access with the Swing Handle Lock or a Door Control Unit.

Please refer to the SP+ Swing Handle Lock Manual if you need more specific information about using the Handle Lock.

Access Logs overview

Under **Events menu / Access**, you can also view the **Access Logs** which will show events related to the door status changes and user authentication.

You can find more information about this feature in the section **Card and User management** below.

Access Control management

Access Control Menu Overview

This menu is where the new Groups, Users, Schedules and Reports are entered and stored into the database of the AKCPro Server software.

To add a new Group, click on the Group menu and complete the wizard. To add a new User click on the User menu and complete the wizard and finally to add a new Schedule click on the Time Schedules menu and complete that wizard.

You can define your optional Departments and Holidays in separate menus.

Sync the Access Control database with your client devices in the Sync Devices menu.

We will go through each of these in detail in the following sections. Make sure that a unit has been added to the APS console already with a configurable door.
Although you could define users and groups even without a door to control, you won't be able to complete all setup steps.

Access Control – Groups Overview

The AKCPro Server software allows you to setup Groups of users. This feature is used for allowing or denying access to specific doors, specific times and also to set security and access levels for our groups of users. Creating new groups will be covered in another section.

We will cover the Users and Schedules before covering the "Manage Permissions" for each of our groups as we need to add our users and schedules before adding our permissions to each group.
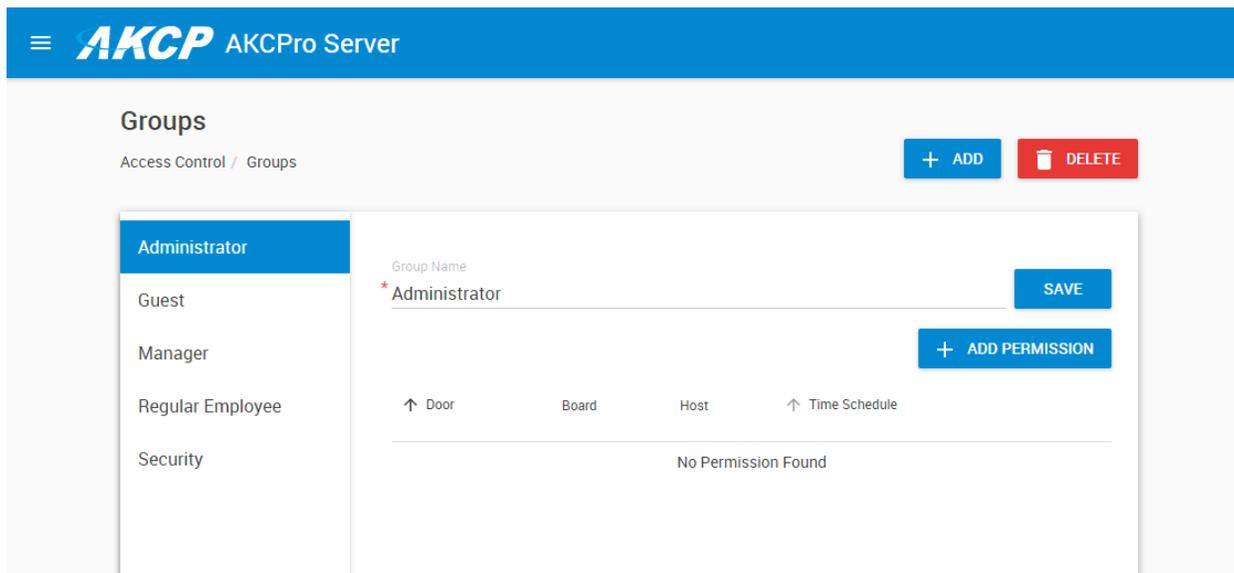
If we click on the **Groups menu** as we can see in the screen shot above, we have a list of the existing groups that by default are already setup in the system. We can use these pre-set groups or we can create our own groups using the **New Group wizard**.

As mentioned above the new group wizard will be covered in another section of this manual after we have added our users and schedules to the system.

After our groups have been created or chosen, then the Users, Schedules and Permissions can be assigned to each of the groups.

Access Control – Users

The AKCPro Server software allows you to setup individual system users. You can enter your users name and details, assign each user to departments, holidays for each department and other personal information such as the users picture, email, telephone number etc.
The users database will also hold each users' system log in and out times and from which door they used.

To add a new user to the AKCPro Server software you will first click on the Users menu as shown above, then click on the **Add** button which will launch the new user wizard.
If you don't see the **Add** button it means your user doesn't have the necessary privileges to add or modify users.

Important Note: *In order for each user that has been added to the software to clock in or out using their EM cards or to open doors in the system, the Users must be first added to a Group and that Group must be given permission to open that door and also have that access time schedule added. This is all covered in the Groups and Permissions in the following sections of this manual.*

As you can see on the first screen of the new user wizard above is where you will begin to enter the new user details such as the users first and last name.

Choose a Group from the drop-down list. You can select an existing group first, if you haven't created your own groups yet. The user can be reassigned.

The validity date will start from the day you create this user account.

Optionally you can choose a department from the drop down list. If you do not have any department created already, you can click on he "Add" button under the separate "Departments" menu and add your own. Refer to the Departments section below.

You can now enter the remaining user information, and optionally upload a photo.

Only the fields marked with a star * are mandatory, the other fields are optional.

Now you can scan in your EM card with the card reader that is on the Handle Lock.
Simply click in the Card ID field and scan your card in the reader. The card number will be filled in automatically. Depending on the reader, you may still need to enter it manually.

Important: For the Handle Lock don't specify a PIN code as there's no keypad to type it in, but this feature is supported by other card readers.

Optionally you can scan an unused card on the reader, and its ID will be logged in the Event Log:

You can then click on the card number from the log to create a new user with this card:

You will need to choose your group that this new user will belong to from the "Group" drop down list. The group membership will define which doors the user has access to. This can be edited per user. We'll show how to manage the groups below in this manual.

You can specify the validity dates per user account.

After all this information is entered you can press the **Add** button to complete the wizard.

After finishing the wizard we can now see our new user has been added to our access control list.

You will need to sync you devices in order for your changes to take effect.

Clicking the **Sync Now** link will take you to the **Sync Devices menu**:

Sync Devices menu

Extremely Important Note: *In order to activate the new access DB in the system YOU MUST RUN THE SYNCRONISE from the Sync Devices menu as shown in the screen shot below.*
You will need to sync you devices in order for your changes to take effect:

Click on the **Sync Now** button and confirm that you want to sync the access control database on all connected units.

Having Trouble Opening the Doors?

If all the door locks and readers are wired up, you should be able to scan and open the doors. If you're having trouble or you receive two beeps when scanning your card, proceed to the Users menu and check the Group to which the user you're having problems with is assigned in the correct group that you have added permissions for.

In the next section beginning on the following page, we will cover the AKCPro Server Access Control Schedules.

Access Control – Schedules

The AKCPro Server software allows you to add scheduling to either allow access or deny access to specific users, groups and doors during these custom pre-set time zones.

When you first click on the **Schedules menu** as shown above you can either edit any of the existing schedules that are in your schedules list, or you can create a new schedule.

Click on the **Add** button which will launch the new schedule wizard:

Give your new schedule a descriptive name.
Now choose the times when this schedule will be active.

You can allow or deny access just by clicking on each of the individual time zone squares or click on the times or days to all or deny access to that entire row.
If you right mouse click on an individual time zone square you can adjust the Time Offset in minutes for each of the zones as shown in the screen shot above.

Your new time schedule will be added to the list.
You may edit the schedule directly from this list again.

As with any changes, you'll need to sync the database to the client devices.

Holiday menu

Note: This feature is optional.
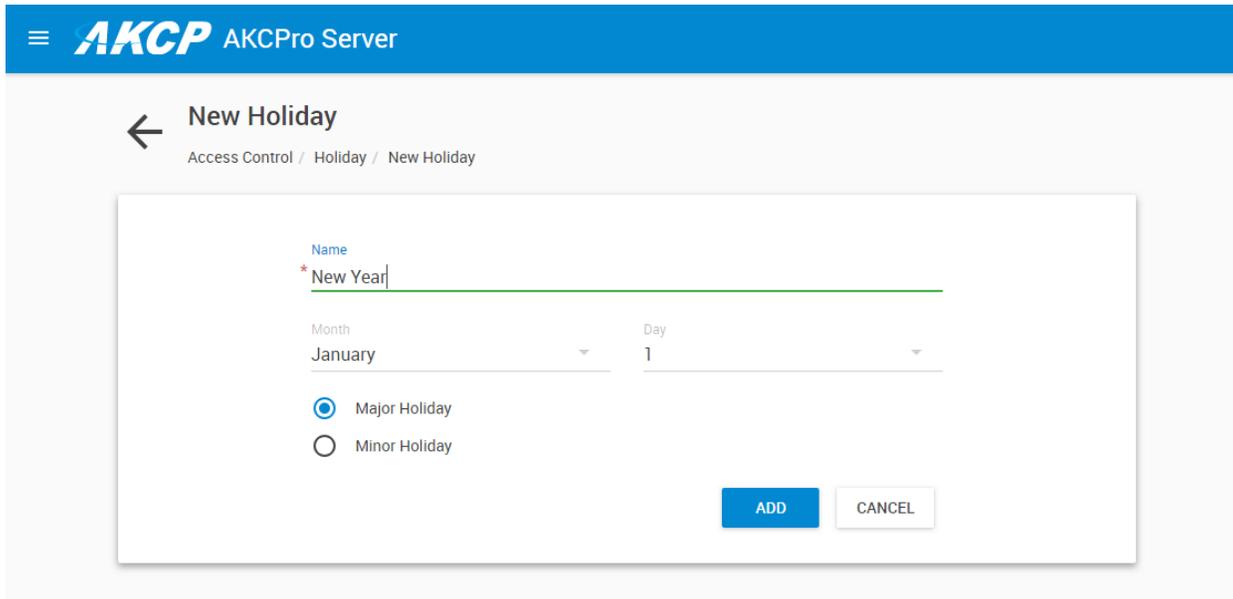
You can define your Holidays under the Holiday menu, as shown in the screen shot above.

Type in a name and select the date, then specify major or minor holiday type.

Departments menu

Note: This feature is optional.
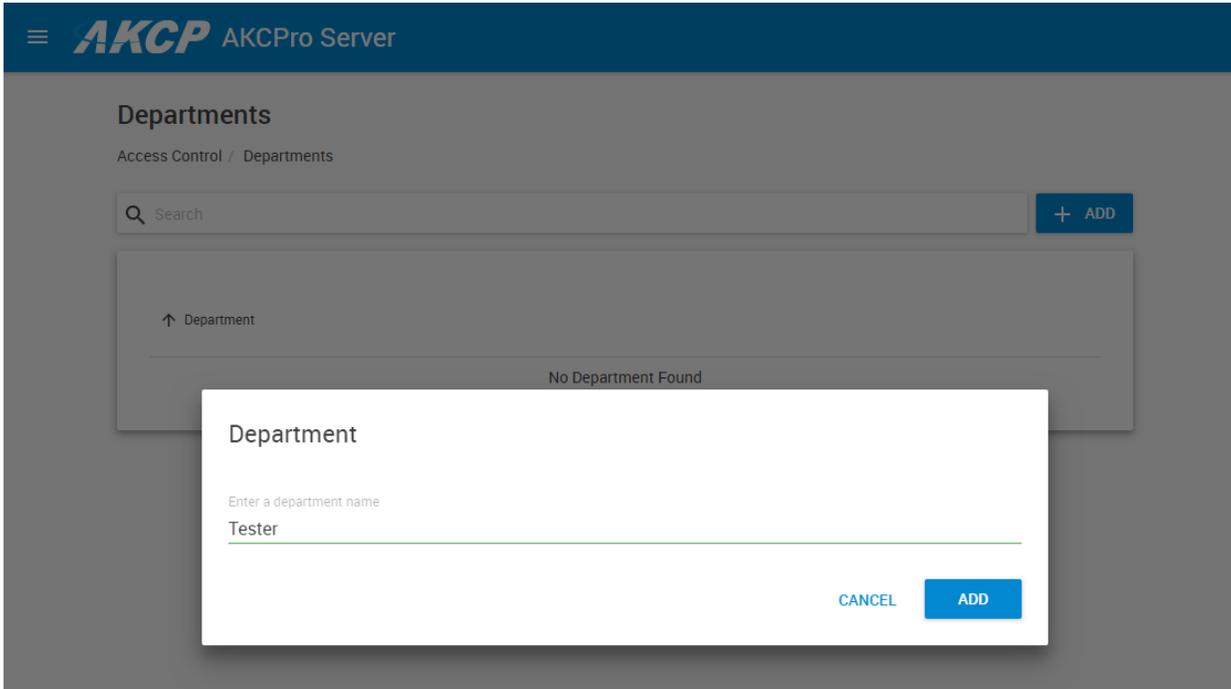
You can add or remove any department in this menu.

The APS departments help you to better categorize your organization's structure in APS, but they are just labels without any specific feature.

Access Control – New Groups

The New Group function of the Access Control section allows you to assign groups of users access permissions to each of the doors that are controlled by the sensorProbe+ Handle Locks that you have added to the system.
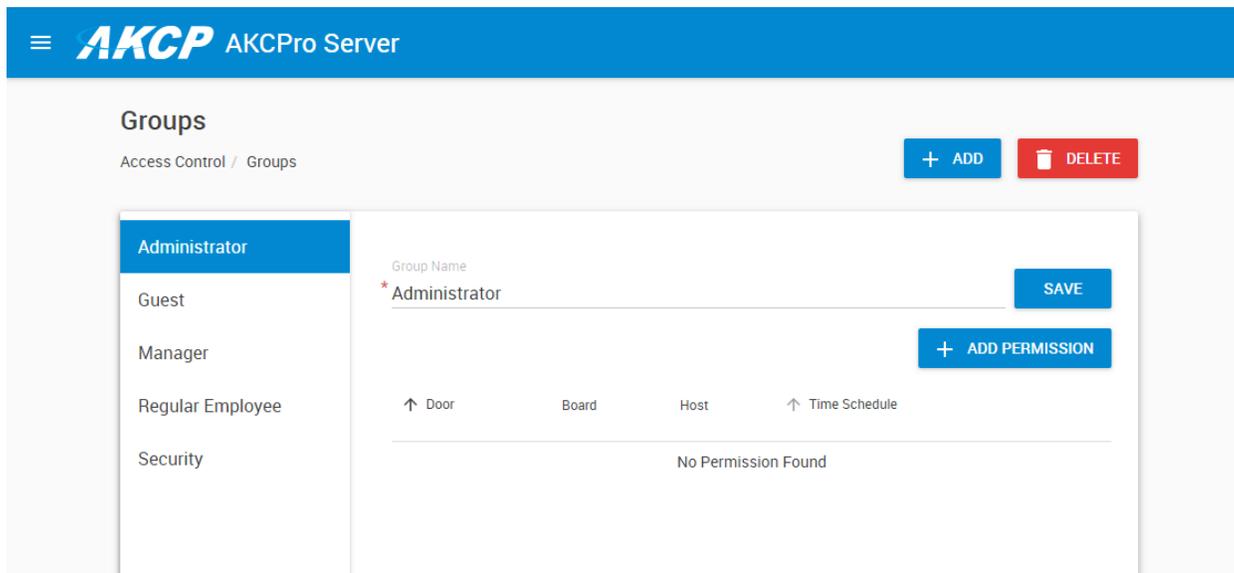
Now that you have completed adding your user and a new schedule, you can now create a new Group and also assign a user and a schedule to an existing group.
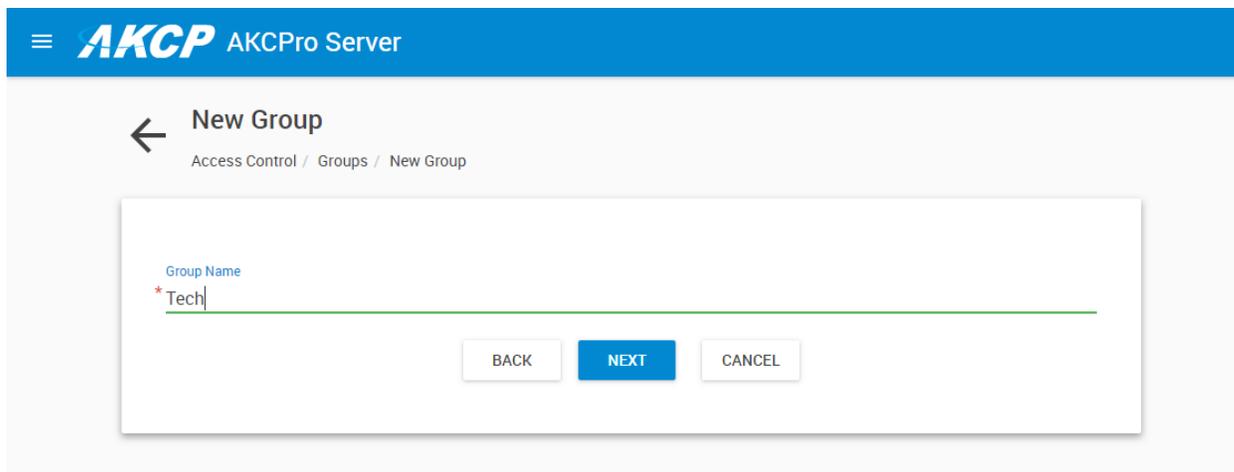
After clicking on the **Groups menu**, click on the **Add** button. This will launch your New Group Wizard as shown in the screen shot above.

You first enter your new group name in the Group Name field then click on the **Next** button to continue.

Now you need to assign the group access permissions to each of the doors that are controlled by the sensorProbe+ Handle Locks that you have added to the system. These permissions include the doors the groups can access and the schedules too.

As the screen shot shows, you need to add permissions to your groups before each of our users in the system will be able to open each of the doors using the card reader.

Choose your door(s) from the list and place a checkmark next to each door that you want to assign to this group of users.

Click **Next** to continue.
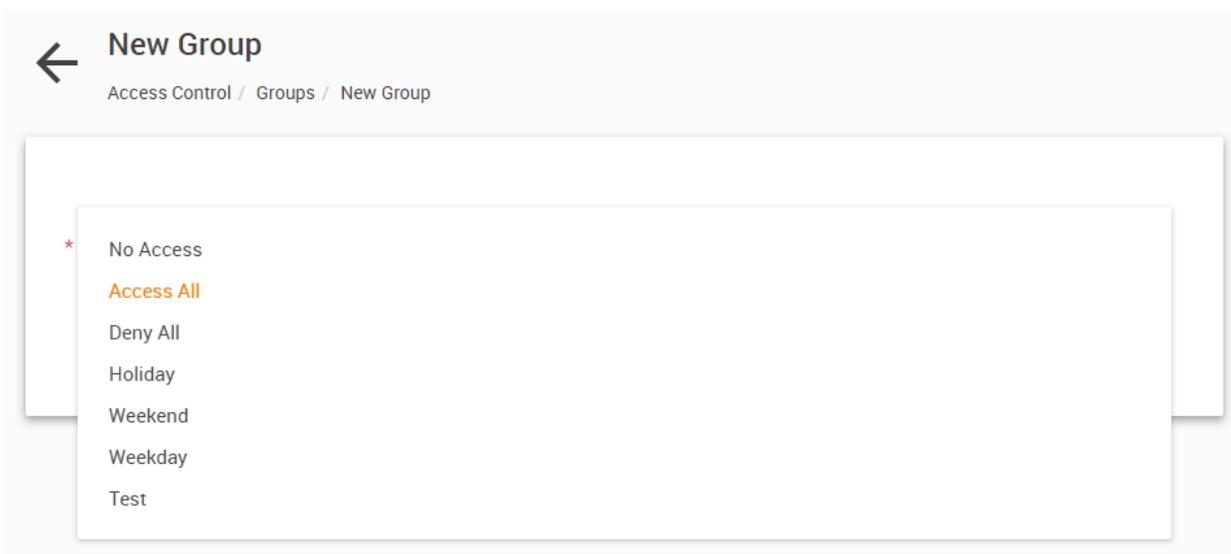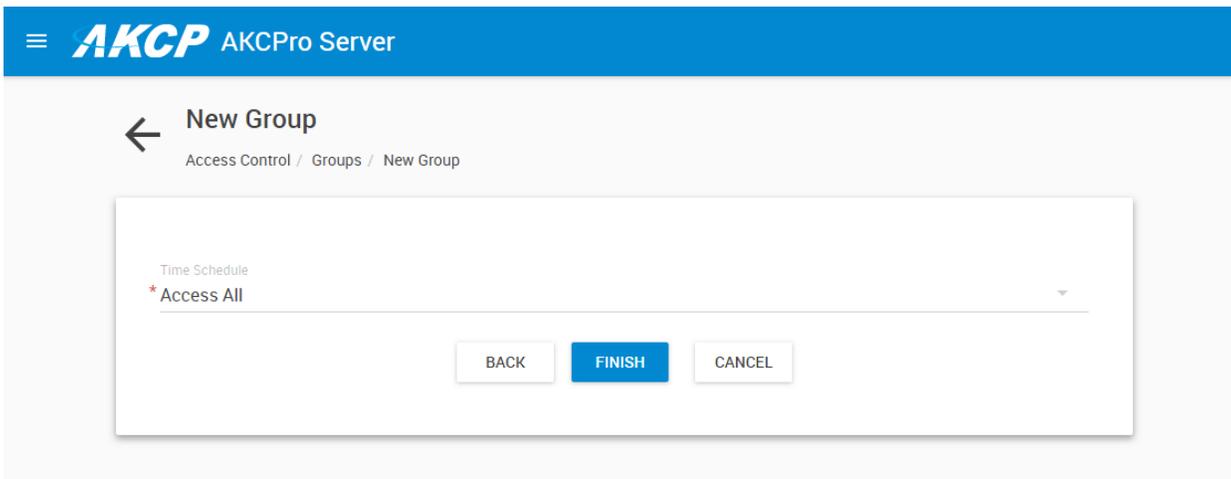
You will now choose the Schedule for the access from the drop down menu as shown in the screen shot above. And to finish the New Group wizard you click on the **Finish** button.

Now as you can see in the screen shot above that our new group has been added.
With the **Add Permission** button you can add more doors to access to this group.
You can directly edit or remove existing door permissions, then click **Save** to save your changes.
You will need to **sync your devices** in order for your changes to take effect.

Important: If you attempt to open a door with a user who has no door permissions assigned, the access will be denied. After we've added a schedule ("access all") to the user's group, the user can open the door as seen on this screenshot:

Access Control – Access Logs

The Access Logs hold all of the information the users who accessed the system which includes the date and time, the user, the door name, the host or unit name, and the event which occurred. The access logs can be accessed by clicking on the **Events menu** and selecting **Access** as shown in the screen shot below.

You can directly access a user's profile and card ID from the logs by clicking on them.

There are several filters that can be applied to the logs for viewing specific information such as the Custom Filter, sorting by Today, Yesterday, This week or This Month by choosing any one of these from the drop down list as shown it the screen shot below.
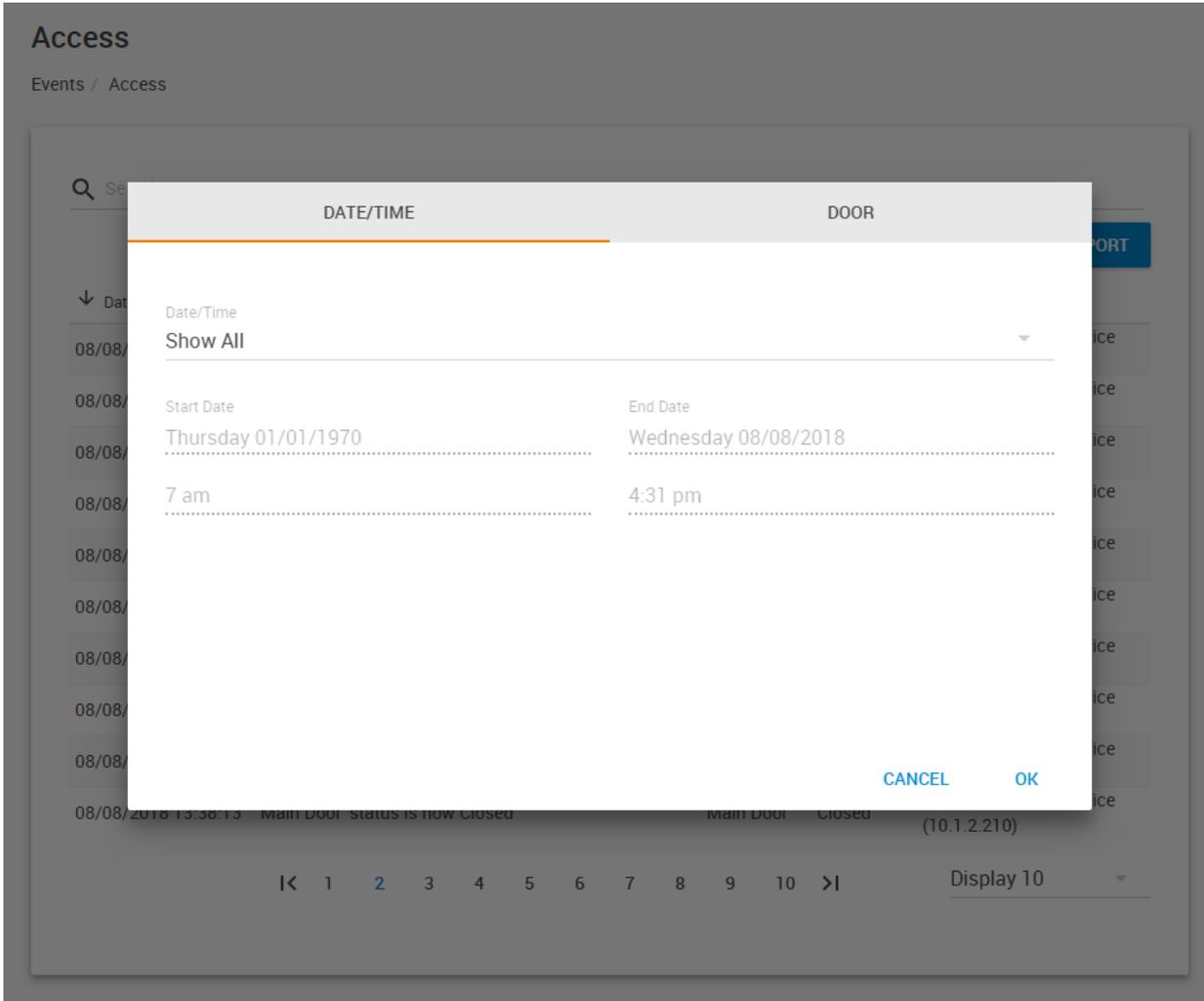
If you choose the **Custom Filter** you can enter any custom date and time for your report.

DATE/TIME	DOOR

Date/Time
Custom

Start Date
Thursday 01/01/1970

End Date
Wednesday 08/08/2018

7 am

4:31 pm

CANCEL   OK

DATE/TIME	DOOR

☑ Tampered
☑ Held Open
☑ Opened with Key
☑ Lock Jammed
☑ Awaiting Input
☑ Access Denied: Wrong Card/PIN Combination
☑ Access Denied: Wrong Door Code

☑ Forced Open
☑ Opened
☑ Closed
☑ Access Granted
☑ Access Denied: No Permission
☑ Access Denied: Input Entry Timeout
☑ Access Denied: Unknown User

SELECT ALL   UNSELECT ALL   CANCEL   OK

You can also chose the Filter as shown above which will give you many more options for generating reports based on Events or Status.

Access

Events / Access

After generating your report, you can Export this data into a CSV type file which can then be imported into an Excel file or other types of file. To export your report just click on the **Export** button as shown in the screen shot above.

Blocking a User

To block a user, move them to the No Access Group.
You can also set a fixed account validity length, and and remove the user from the DB.
After any modifications you have to run the Synchronize with the unit(s).

Re-Using or Re-Assigning Access Cards

You can also delete the card number from one person and make a new UserProfile with that Card. The past Access Details for the first card owner is retained in the system.

If you update the User Profile of the First person with the Second Persons name for example changing Mary to Matt. Then all of the system log's would show Matt and Mary would cease to exist. So the best thing to do, for an example is if an employee works for you temporarily is to keep that user profile and remove their card number, save and synchronize. Then make a new employee with that card that way you can still search for Mary.

7.5. Notifications
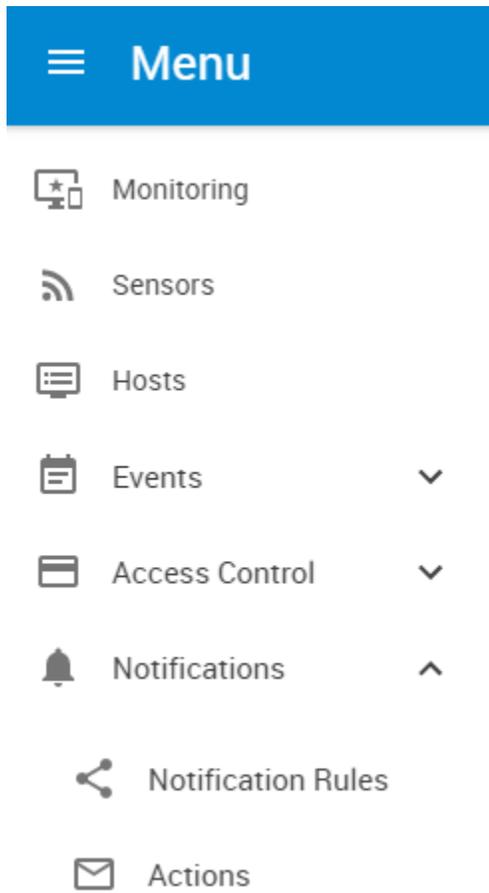
External GSM Modems

Important Note: Our AKCP policy regarding support for 3rd party (non-AKCP branded) external modems is as follows:

AKCP no longer supports any 3rd party external GSM modems for sending out the SMS or voice call alerts from our AKCPro Server software, or from the embedded server software running on our L-DCIM units. Nor will there be any engineering provided to add 3rd party external GSM modems to our software.

Both the SMS and the voice call alerts will ONLY be supported using our AKCP branded external GSM modem, which is listed on our MSRP price list.

Please contact our support team if you have any questions on this policy and also our sales team if you require the cost or a quote for the AKCP external GSM modem we offer.

When you setup a notification you can define the action to take when a sensor gives a reading beyond your previously set thresholds. This allows you to determine how you will be notified that a sensors reading has reached the specified thresholds (high warning, critical etc).

There are many different types of notifications that AKCPro Server is capable of. We will discuss each one of them in this chapter of the manual.

After setting a notification, you should be able to receive an alert message from APS informing you about your unit or sensor's status. You are then able to take immediate action. With notifications, you can then be able to monitor your sensors anytime and anywhere.

What function do the different types of notifications provide?

The notifications are used to notify you when a sensor reading has hit a certain preset "critical" threshold. There are many ways you can be notified. A few examples:

SNMP Trap: This form of notification sends out a signal to your SNMP trap receiver server.
E-Mail: This sends a notification via e-mail.
SMS: This sends an SMS message to your mobile phone.
Relay: The relay is used as a switch, for example it could switch on an air con unit if the temperature reading of a temperature sensor reaches a certain threshold.
Telephone call: Will call you and play a customizable text to speech message.
Door: Controls the door with the Handle Lock sensor.
Dry Contact: You can control the Dry Contact ports with the notification, similar to the Relay action.

First we'll list all possible Action types.
Then as an example notification rule, we will show you how to set up a SMS notification when a 'host status' virtual sensor goes unreachable using a modem.

Actions

APS supports many different types of Actions. We'll describe each of them in detail, you can see some of them on this screenshot below:

After listing all Actions configuration we'll show the process of creating a notification and a new action together in the Notifications menu.

Below we'll list all supported APS actions and the steps required to configure them.

Click on the **Add** button to begin the Action Wizard.

Every Action configuration begins with the Action Wizard selection screen:
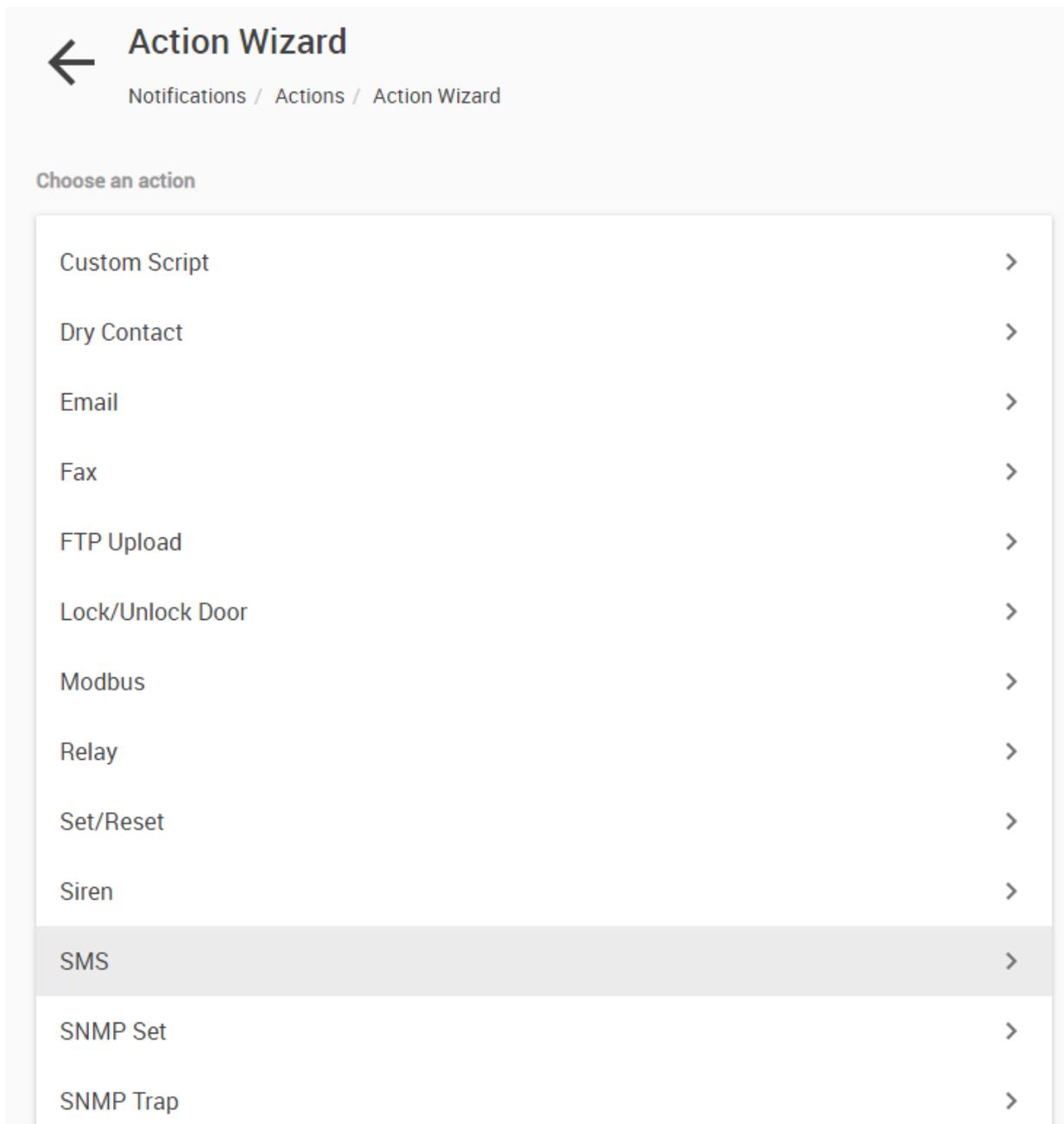
You will see a list of possible notification actions.
Select the Action you wish to configure and click '**Next**'.
The Action configuration steps will differ slightly depending on the chosen type, below we'll show each one.

Note: some actions are not supported on the HTML5 UI such as Skype notification.

Custom script action

You can execute custom scripts or programs with this action.
The script language supported will depend on the OS platform (Windows or Unix) and you cannot execute scripts that cannot run on the OS (for example .BAT won't run under Linux).

Click on the **Add** button to upload your script, or you can select it from the drop-down list in case if you've already uploaded it earlier.
Optionally, parameters and APS macros to the script can be passed in the **Arguments** field.

Important: your script file must have an exit code when it finishes execution. APS will check the exit code when the script finishes, and report error if the code is different than the normal value you give here.
Example: to have a return code 0 when your script finishes regardless of the execution outcome, type "exit 0" or "echo 0" as the last line in the script. This will ensure your action to be logged as a success.

Custom Script

Notifications / Actions / Custom Script
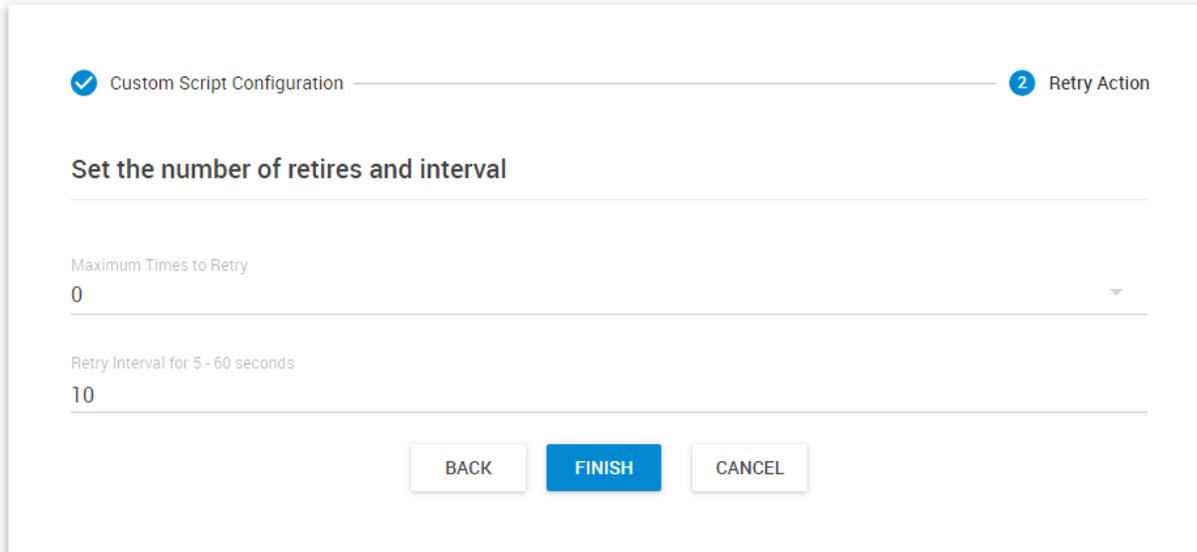
✓ Custom Script Configuration ———————————————— ② Retry Action

Set the number of retires and interval

Maximum Times to Retry

0

Retry Interval for 5 - 60 seconds

10

BACK   FINISH   CANCEL

If required, specify the action retry parameters (up to 5 times to retry) and the interval of the retries, then press **Finish**.

Important note for running Linux scripts (only for non-Windows APS platforms such as SEC+):
If you're using Bash specific syntax in your script, you must explicitly use the Bash interpreter:
`#!/bin/bash`
Using `#!/bin/sh` might not work correctly, if the syntax of your script is not fully POSIX compliant.

Dry Contact action

Dry Contact Action

Notifications / Actions / Dry Contact Action

① Dry Contact Configuration   ② Sensor   ③ Retry Action

Name your action and configure the dry contact

Action Name
Dry Contact Action 1

Action Mode
Turn Low Until Sensor Status ▾

Status
Normal ▾

Turn back to this state after above action is finished

◉ Closed/GND
◯ Open/+5 Volts

BACK   NEXT   CANCEL

Dry Contact sensors 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.

With this action you can set up the parameters for the Dry Contact sensor that will be set when the action is triggered.

First choose the Action Mode. When the Action runs, this will set the Dry Contact to a state defined here:

Turn Low

Turn High

Turn Low Until Sensor Status

Turn High Until Sensor Status

Turn Low Until Acknowledge

Turn High Until Acknowledge

Cycle Dry Contact

Choose the status for the Dry Contact to be set:

No Status

Normal

High Warning

High Critical

Low Warning

Low Critical

Sensor Error

Unreachable

Low Out

High Out

After the action runs, you can choose to set the Dry Contact to be in Open or Closed state.

Press **Next** to continue.

Choose your Dry Contact sensor from the sensors list and press **Next**.

Note: if you don't see the sensor(s) listed here, check that your unit with the sensor(s) connected has been already added to the APS console.

Dry Contact Action

Notifications / Actions / Dry Contact Action

✓ Dry Contact Configuration ──────── ✓ Sensor ──────── ③ Retry Action

Set the number of retires and interval

Maximum Times to Retry
0

Retry Interval for 5 - 60 seconds
10

BACK   FINISH   CANCEL

If required, specify the action retry parameters (up to 5 times to retry) and the interval of the retries, then press **Finish**.

Email action

You can use the Email Action to send a notification by email when a sensor reaches a certain threshold.

Fill out the basic email settings:

From / To / CC addresses (the Mail To and From fields are mandatory).
Multiple recipients may be entered by separating addresses by a comma (,) or semicolon (;).

Click **Next** for the message content settings.

Email Action

Notifications / Actions / Email Action

✓ Email Configuration ——— ② Email Message ——— ③ Media Attachment ——— ④ Email Server ——— ⑤ Retry Action

Define the content of the message

Subject

$[DESCRIPTION] is now $[VALUE], status is now $[STATUS]

Body

From: $[SYSNAME]($[IP])
Time: $[TIME]
$[DESCRIPTION] is now $[VALUE], status is now $[STATUS]

PREVIEW   RESTORE DEFAULT   ADD MACRO

BACK   NEXT   CANCEL

Here you can input the e-mail subject and message. By default the message has macros that is useful to send an automated e-mail which will display sensor and status information.
Press the *"Preview"* button to see the message sample:

Define the content of the message

Subject

Testing Sensor Port 1 is now 80, status is now Normal

Body

From: System Name(127.0.0.1)
Time: 14:07:50
Testing Sensor Port 1 is now 80, status is now Normal

EDIT   RESTORE DEFAULT   ADD MACRO

You can add/remove macros (dynamic fields) and any custom text to the email. We'll show you more details about macros at the SMS action description. Go back to editing mode by clicking the **Edit** button again.

Email Action

Notifications / Actions / Email Action

Email Configuration ——— Email Message ——— **3** Media Attachment ——— **4** Email Server ——— **5** Retry Action

Select media content that will attach to the email

Attach Media Content

Camera	Host	Picture	Video	Before	After	FPS

ADD

BACK   NEXT   CANCEL

Optionally, you can attach video or pictures to the email as attachments.
Click on Attach Media Content if you want to add media then click **Add** and select a camera from the list:

Select Cameras

Cameras

Q Search

∧ **AVTECH's AVM328A (10.1.1.132)**

☑ AVTECH's AVM328A

∧ **System Name (10.1.1.137)**

☐ V1

☐ V2

☐ V3

☐ V4

Media

☑ Current Picture
☑ Video Clip

Video Clip Option

Before Event
3

After Event
3

Framerate
30

SELECT ALL   UNSELECT ALL   CANCEL   OK

Choose the camera first.

Then click on the attached media type:

- Current Picture
- Video Clip

For the video, you can also specify how many seconds before and after the sensor event should be recorded, and in what frame rate. Please keep in mind the size of the email when attaching video files.

Email Action

Notifications / Actions / Email Action

✓ Email Configuration —— ✓ Email Message —— ③ Media Attachment —— ④ Email Server —— ⑤ Retry Action

Select media content that will attach to the email

🔵 Attach Media Content

Camera	Host	Picture	Video	Before	After	FPS	
AVTECH's AVM328A	AVTECH's AVM328A (10.1.1.132)	✓	✓	3	3	30	🗑
V1	System Name (10.1.1.137)	✓	—	—	—	—	🗑

ADD

BACK   NEXT   CANCEL

On this example picture, we've added 2 cameras with picture attachments, and one of the cameras will also attach a short video.

You can remove cameras from the action and re-add them with different options, but cannot edit the media option once they're added.

Click **Next** for the SMTP server settings for the action.

✓ Email Configuration —— ✓ Email Message —— ✓ Media Attachment —— **4** Email Server —— **5** Retry Action

Setup the alert type and the destination of the alert

SMTP Server

SMTP Port
25

SMTP Connection Security
None

SMTP Authentication Method
No Authentication

SMTP Server Login Name

SMTP Server Password

BACK   NEXT   CANCEL

Specify the SMTP server parameters. APS supports SSL/TLS and STARTTLS modes:

None
SSL/TLS
STARTTLS

The connection security defines the security mode - if it's set to "none" or "no authentication" then there won't be any encryption to the server and no user login. This usually only works with servers in the LAN.

No Authentication
DEFAULT
PLAIN
LOGIN
CRAM-MD5

If authentication is required, type in the login details and choose the authentication method for the server.
The authentication method is the way the password is sent to the server (if password is used), and usually it should be on the DEFAULT setting.

Email Action

Notifications / Actions / Email Action

✓ Email Configuration ——— ✓ Email Message ——— ✓ Media Attachment ——— ✓ Email Server ——— 5 Retry Action

Set the number of retires and interval

Maximum Times to Retry
0

Retry Interval for 5 - 60 seconds
10

BACK   FINISH   CANCEL

If required, specify the action retry parameters (up to 5 times to retry) and the interval of the retries, then press **Finish**.

Settings for Gmail

Email From
※※※※@gmail.com

Email To

SMTP Server
smtp.gmail.com

SMTP Port
587

SMTP Connection Security
STARTTLS

SMTP Authentication Method
DEFAULT

SMTP Server Login Name
※※※※@gmail.com

SMTP Server Password
············

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

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

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

Fax action

Fax Action

Notifications / Actions / Fax Action

① **Fax Numbers** ─────── ② Fax Message ─────── ③ Fax Settings ─────── ④ Retry Action

Name the action and enter phone number of the recipients

Action Name
Fax 1

Fax Number

BACK   NEXT   CANCEL

This action will send a Fax to you with a notification message.

Fill out the fax number first.
The message content is similar to what you can receive by email. Click **Next** to continue.

Note: The fax needs to be connected and configured on the server already before configuring the action.

Fax Action

Notifications / Actions / Fax Action

Customize your fax message.

Similar to the email action you can add/remove macros and preview the content.
We'll show you more details about macros at the SMS action description.

Press **Next** to continue.

Fax Action

Notifications / Actions / Fax Action

✔ Fax Numbers ——————— ✔ Fax Message ——————— ③ Fax Settings ——————— ④ Retry Action

Enter modem port

Fax Modem Port
COM2

Device Name: Communications Port (COM2)

Process Timeout for 180 - 600 seconds
180

BACK   NEXT   CANCEL

Choose the correct port for the fax, and set the process timeout.

Fax Action

Notifications / Actions / Fax Action

✔ Fax Numbers ——————— ✔ Fax Message ——————— ✔ Fax Settings ——————— ④ Retry Action

Set the number of retires and interval

Maximum Times to Retry
0

Retry Interval for 5 - 60 seconds
10

BACK   FINISH   CANCEL

If required, specify the action retry parameters (up to 5 times to retry) and the interval of the retries, then press **Finish**.

FTP Upload action

With this action you can upload camera images and videos along with a status message text file to an FTP server.

Keep in mind that FTP is an unsecure protocol and the usernames, passwords and files will be sent in clear text form over the network.

Important: First you must have cameras added to APS (or to a client unit that is added to APS) and specify the cameras to attach media from (see below) before you can continue.

The options and the dialog is the same as in the Email action.

Choose the camera first.

Then click on the media type:

- Current Picture
- Video Clip

For the video, you can also specify how many seconds before and after the sensor event should be recorded, and in what frame rate.

Note: the uploaded files will stay on the FTP server and are not removed automatically. Keep this in mind when you're uploading a lot of video files, your FTP server's storage could get full.

FTP Upload

Notifications / Actions / FTP Upload

① FTP Upload Configuration —— ② FTP Attached Message —— ③ FTP Server Information —— ④ FTP Upload Settings

Name the action and select the media content you wish to upload.

Action Name
FTP Upload 1

| Camera	Host	Picture	Video	Before	After	FPS	
AVTECH's AVM328A	AVTECH's AVM328A (10.1.1.132)	✓	✓	3	3	30	🗑
V1	System Name (10.1.1.137)	✓	—	—	—	—	🗑

ADD

BACK   NEXT   CANCEL

On this example picture, we've added 2 cameras with picture attachments, and one of the cameras will also upload a short video.

You can remove cameras from the action and re-add them with different options, but cannot edit the media option once they're added.

Click **Next** to continue.

FTP Upload

Notifications / Actions / FTP Upload
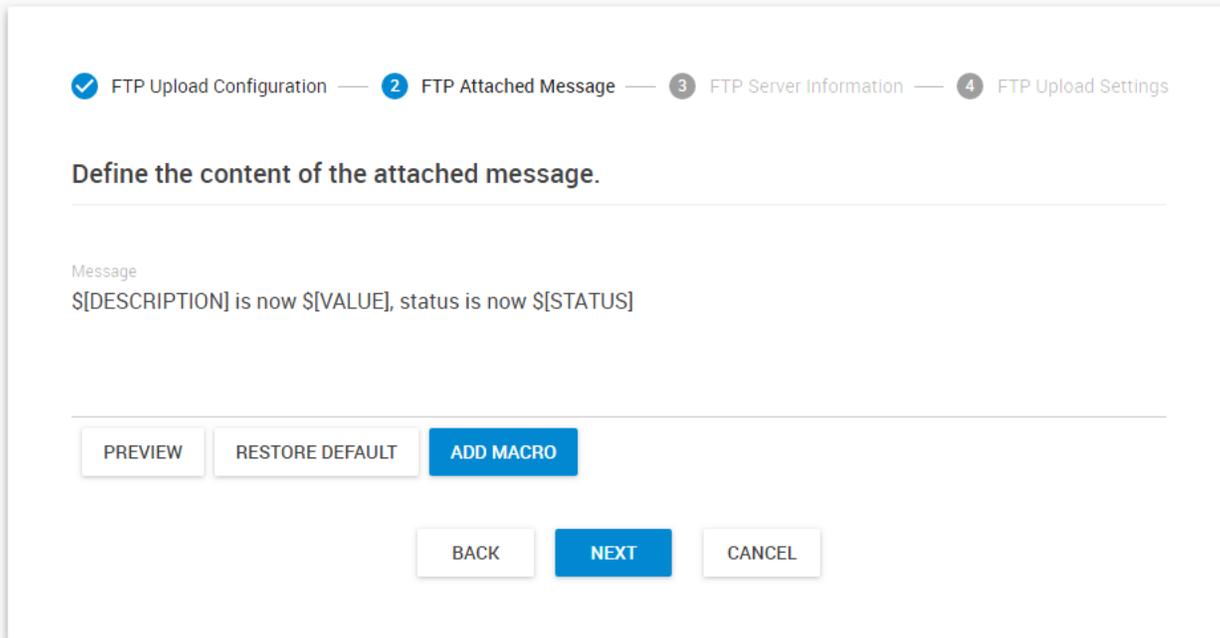
✓ FTP Upload Configuration —— ② FTP Attached Message —— ③ FTP Server Information —— ④ FTP Upload Settings

Define the content of the attached message.

Message
$[DESCRIPTION] is now $[VALUE], status is now $[STATUS]

[PREVIEW] [RESTORE DEFAULT] [ADD MACRO]

[BACK] [NEXT] [CANCEL]

Here you can change the content of the uploaded status text message.
This .TXT file will be always uploaded together with any media content you selected.

The editing, preview and macro usage are similar to the Email action.
We'll show you more details about macros at the SMS action description.

Click **Next** for the FTP server options.

Enter the FTP server's details here.

For the **Destination Path** you generally don't need to modify it, since it's usually restricted per-user on the FTP server. Just leave it empty, or enter a dot (.) to upload to the root folder.

If required, you can change the **FTP Mode** between Active/Passive.

For troubleshooting and diagnosis you can turn on the **FTP Log**. This log can be viewed using the APS Server Manager application and by clicking View Logs menu.
Important: the FTP username and password will be stored in clear text in the log! Therefore don't use the logging unless necessary.

FTP Upload

Notifications / Actions / FTP Upload

✓ FTP Upload Configuration ── ✓ FTP Attached Message ── ✓ FTP Server Information ── 4 FTP Upload Settings

Select the upload option.

Upload Option
Single

Upload Attempt (Times)
0

Upload Attempt Interval (Seconds)
10

BACK   **FINISH**   CANCEL

Finally choose the **Upload Option**: Single/Continuous.
Single will only upload when the action runs, while continuous will always upload once the action has started:

Select the upload option.

Upload Option
Continuous

After action disabled, upload (Times)
30

After action disabled, upload (Times)
0

After action disabled, upload every (Seconds)
30

If required, specify the action retry parameters (upload attempts) and the interval of the retries, then press **Finish**.

Door action

You can use the Door Action to open/close a door when a sensor reaches a certain threshold.

Note: a Handle Lock or other door sensor needs to be connected to a client unit, and this unit added to APS console before the action is configured.

You can control the door with the action for **Lock / Unlock**.

The door will automatically lock by default with the "After a period of time" setting. You can specify the time in seconds for how long the door should be opened before closing it again.
Otherwise you can set it to "When acknowledged" then it won't be locked until it's acknowledged.

Click **Next** to choose the door sensor.

Choose the door or doors that will be controlled by this action, and click **Next**.

Door Action

Notifications / Actions / Door Action

If required, specify the action retry parameters (up to 5 times to retry) and the interval of the retries, then press **Finish**.

Modbus action

Modbus Action

Notifications / Actions / Modbus Action

① Modbus Configuration ────── ② Modbus Data ────── ③ Retry Action

Name the action and enter Modbus details

Action Name
Modbus Action 1

Modbus IP Address

Modbus TCP Port (Default is 502)
502

Modbus Slave ID
255

BACK   NEXT   CANCEL

With the Modbus Action you can send Modbus Write commands to a Modbus TCP compatible device.

Type in the **Modbus IP** address of the target device.
If necessary change the **Modbus TCP Port** but the default is already selected.
Type in the device's **Modbus Slave ID** then press **Next**.

If the target device doesn't respond or you configure the action incorrectly, APS will display an error popup message.

Note: this action doesn't work with SP+ devices since on SP+ Modbus Slave is used only for getting data from SP+ to another device and it can't be used to control or write data into.

Modbus Action

Notifications / Actions / Modbus Action

✓ Modbus Configuration ——————— ② Modbus Data ——————— ③ Retry Action

Enter Modbus command and data

Modbus Command
(0x05) Write Single Coil ▼

Modbus Coil Address (0x0000)
0

Data #1 (0x0000)
0

BACK   NEXT   CANCEL

(0x05) Write Single Coil

(0x06) Write Single Register

(0x0F) Write Multiple Coils

(0x10) Write Multiple Registers

Choose the **Modbus Command** that you wish to send with this action. The configuration will slightly vary depending on you select single- or multiple coils/registers.

Example: set a single register with data value 11.

Modbus Command
(0x06) Write Single Register

Modbus Register Address (0x0008)
8

Data #1 (0x000B)
11

Mbslave1
ID = 22: F = 03

	00000
0	
1	
2	0
3	0
4	0
5	0
6	0
7	0
8	11
9	100

Using a Modbus Slave tester program (Holding Register function) we can see the specified register was modified by this action successfully.

Modbus Action

Notifications / Actions / Modbus Action

✓ Modbus Configuration ———— ✓ Modbus Data ———— ③ Retry Action

Set the number of retires and interval

Maximum Times to Retry
0

Retry Interval for 5 - 60 seconds
10

BACK   FINISH   CANCEL

If required, specify the action retry parameters (up to 5 times to retry) and the interval of the retries, then press **Finish**.

Relay action

Relay Action

Notifications / Actions / Relay Action

1 Relay Configuration ———————— 2 Sensor ———————— 3 Retry Action

Name the action and configure the relay action

Action Name
Relay Action 1

Relay Action
Turn On

BACK   NEXT   CANCEL

With this action you can set up the parameters for the Relay sensor on a connected unit that will be set when the action is triggered.

First choose the **Relay Action**. When the Action runs, this will set the Relay to a state defined here:

Turn On

Turn Off

Turn On Until Acknowledge

Turn Off Until Acknowledge

Cycle Off-On-Off

Cycle On-Off-On

Press **Next** to continue.

Choose the Relay or multiple Relays which you'd like to control with this action and click **Next**.

Relay Action

Notifications / Actions / Relay Action

- Relay Configuration ———————————— Sensor ———————————— **3** Retry Action

Set the number of retires and interval

Maximum Times to Retry

0

Retry Interval for 5 - 60 seconds

10

BACK   FINISH   CANCEL

If required, specify the action retry parameters (up to 5 times to retry) and the interval of the retries, then press **Finish**.

SET/RESET action

SET/RESET Action

Notifications / Actions / SET/RESET Action

① SET/RESET Configuration ────── ② Sensor ────── ③ Retry Action

Name the action and configure the SET/RESET action

Action Name

SET/RESET Action 1

Action

⦿ RESET

○ SET

BACK   NEXT   CANCEL

With this action you can control the **Logic Virtual Sensor** that is running on APS, to be in SET or RESET state.

Therefore, before configuring this action you'll need to add and set up your Logic Virtual Sensor first:

Add new Virtual Sensor

Select Host

AKCPro Server

Select Virtual Sensor Type

Logic

CANCEL   NEXT

Logic

Logic ─── ② Select Sensor ─── ③ Sensor Description ─── ④ Interval

SET Source Sensors

Select Host	Select Sensor	Status
10.1.1.23	Host Status	Unreachable
None	None	None
None	None	None
None	None	None

RESET Source Sensors

Select Host	Select Sensor	Status
10.1.1.23	Host Status	Reachable
None	None	None
None	None	None
None	None	None

BACK   NEXT   CANCEL

As an example, you can see this Virtual Sensor setup.
It is in SET state when the network device is unreachable, and in RESET state when it is reachable.

Please check the Virtual Sensor section at the end of this manual for more information about this Logic Virtual Sensor.

SET/RESET Configuration —————— ② Sensor —————— ③ Retry Action

Choose Logic Virtual Sensor

Sensor

🔍 Search

⌄ **AKCPro Server**

☑ Logic Sensor

BACK   **NEXT**   CANCEL

Choose the Logic Sensor from the list which you'd like to control with this Action and click **Next**.

SET/RESET Action

Notifications / Actions / SET/RESET Action

SET/RESET Configuration ——————— Sensor ——————— 3 Retry Action

Set the number of retires and interval

Maximum Times to Retry

0

Retry Interval for 5 - 60 seconds

10

BACK   FINISH   CANCEL

If required, specify the action retry parameters (up to 5 times to retry) and the interval of the retries, then press **Finish**.

Siren action

You can use the Siren Action to turn on the siren and strobe light (connected to a client unit) or a supported unit's Buzzer sensor when a sensor reaches a certain threshold.

You'll have the following options for controlling the siren or buzzer with the action:

The siren/buzzer can be turned on until acknowledged, until a sensor status is changed to a specified state, or it can turn off after a defined time.
If you select Defined Time, also enter the Delay before Turn On and the Length of Time the light is on.

Press **Next** to select the sensor from a connected unit.

Choose your sensor from the connected client units list and press **Next**.

Siren and Buzzer sensors can be controlled by this action. On this example picture we've selected a SP+ unit's buzzer.

Siren Configuration ————— ✓ Sensor ————— ③ Retry Action

Set the number of retires and interval

Maximum Times to Retry

0

Retry Interval for 5 - 60 seconds

10

BACK   FINISH   CANCEL

If required, specify the action retry parameters (up to 5 times to retry) and the interval of the retries, then press **Finish**.

SMS action

SMS Action

Notifications / Actions / SMS Action

1 Phone Numbers ——— 2 SMS Message ——— 3 Modem ——— 4 Retry Action

Name the action and enter the phone number of the recipients

Action Name
SMS Action 1

Phone Number

BACK   NEXT   CANCEL

With the SMS Action you can send short text messages to telephones with a modem.

Note: this action requires a supported modem to be connected to the APS computer.

Enter an action name and enter at least one phone number in the Phone Number List.

Click '**Next**' to continue.

You can preview and customize the SMS message to be sent here.

The IP address can be seen in the From field as an example of a macro description named $[IP]. In the actual SMS message, the value of $[IP] will depend on the IP address of the host sending the notification.

Use the **Preview** button to check the message contents.

To customize your message, enter your custom text in the Message box - however keep in mind the maximum character limit of an SMS.

We'll describe the APS action macro usage below, before proceeding with the SMS action setup.

Macros

You can modify the macros (dynamic values) by clicking on the 'Add Macro' button and add/remove the fields as desired. After you select a macro, you can get help about it in the Description field below:

These macro values will be replaced by the actual sensor and host data during action execution. All APS actions use the same macro format.

When you're testing an action, usually the macros will just expand to 0 values instead of a real sensor reading.

See an example macro usage below.

Macro examples

You could modify the default email message content as follows:

Subject:

```
Status: $[SYSNAME] $[STATUS] $[VALUE]
```

Body:

```
From: $[SYSNAME]($[IP])
Time: $[TIME]

Sensor Status:
$[DESCRIPTION]
$[STATUS] $[VALUE] $[UNIT]

Device Detail:
$[SYSNAME]
$[SYSLOCATION]
$[SYSCONTACT]
$[SYSURL]
$[IP]
$[IP_ETH]
```

Email Configuration

Define the content of the me

Subject
Status: System Name Normal 80

Body
From: System Name(127.0.0.1)
Time: 11:07:23

Sensor Status:
Testing Sensor Port 1
Normal 80 Unit

Device Detail:
System Name
System Location
System Contact
http://www.address.com
127.0.0.1
127.0.0.1

Then check with the „**Preview**" button to see how the message will look like. In the actual mail the current, correct values will be used for IP, status and value.

The same macro settings can be used for sending SMS or Email, there's no difference.
Only for SMS the message length must be shorter than 160 characters, so some parts should be left out. For example:

```
$[SYSNAME]($[IP])
$[TIME]

$[DESCRIPTION]
$[STATUS] $[VALUE] $[UNIT]

$[SYSNAME]
$[SYSLOCATION]
$[SYSCONTACT]
```

Continuing the SMS action setup, now choose the settings for the connected modem.
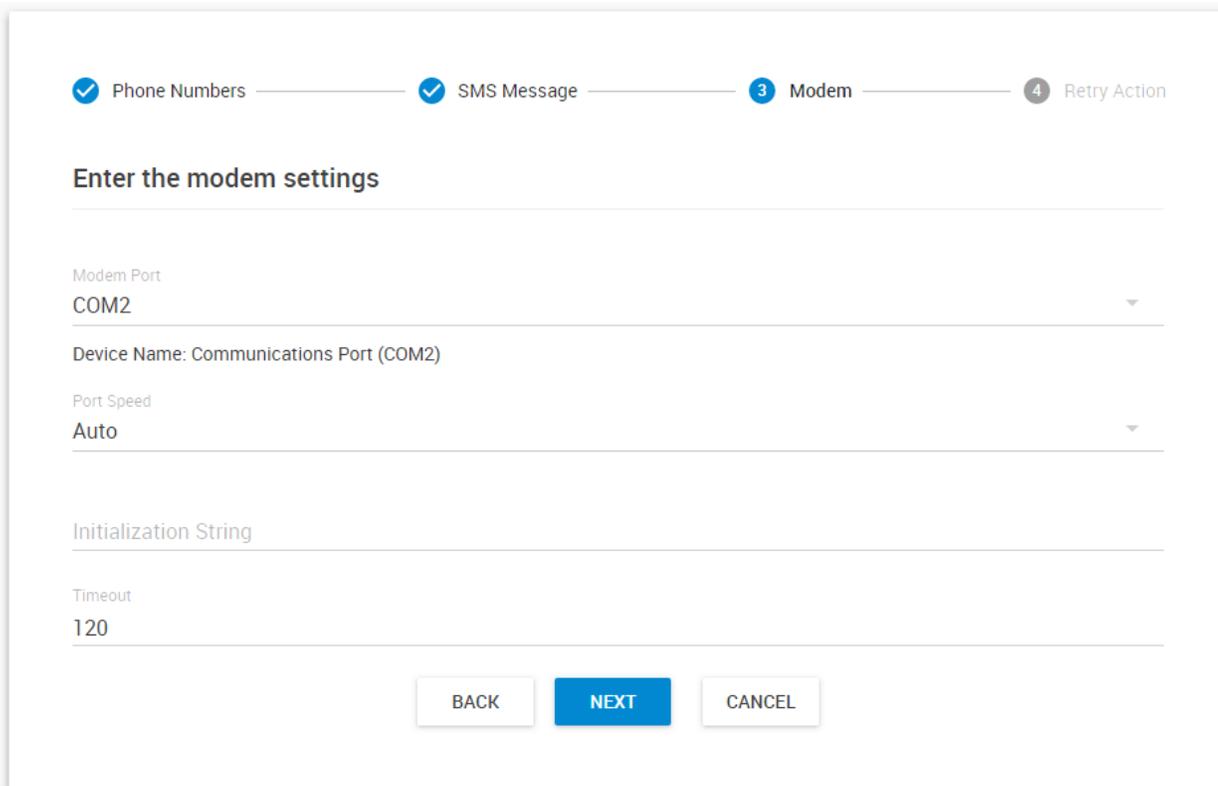
Select the serial port where the modem is connected to, for example COM2 as the **Modem Port**. Usually the connected device name will be also displayed.
If you are unsure what Port your modem is connected to, use the Windows Device Manager and find it under Modems. Right click on your device and click on Properties. There you can see the Port and maximum port speed.

| |
| Auto |
| 2400 |
| 4800 |
| 9600 |
| 19200 |
| 38400 |
| 57600 |
| 115200 |

Usually you can leave the **Port Speed** at 'Auto' but you can specify lower speeds if required.

Some modems require custom **Initialization String** specified. Usually this is not needed and you can leave this field empty.

"**Timeout**" is the time lapsed in seconds that the system has no response from the modem device.

Click '**Next**' to continue.

Phone Numbers ───── SMS Message ───── Modem ───── 4 Retry Action

Set the number of retires and interval

Maximum Times to Retry

0

Retry Interval for 5 - 60 seconds

10

BACK   FINISH   CANCEL

If required, specify the action retry parameters (up to 5 times to retry) and the interval of the retries, then press **Finish**.

SNMP Set action

With the SNMP Set Action you can set a value to any OID on a remote device.

Choose the **SNMP Version** between v1/v2/v3, the available options will vary slightly depending on the trap version selected.
The default **SNMP Port** is automatically selected, but you can modify if required.

You can specify multiple SNMP Set targets in one action, see below.

Destination IP Address

10.1.1.24

Community

••••••

ADD   DELETE

	Address	Community
☐	10.1.1.23	••••••

BACK   NEXT   CANCEL

Enter your **Destination IP Address** and **Community**, then press **Add**.

If you need to add further computers to the list, add them the same way.

When done, select the computers you'd wish to send the SNMP Set to and click **Next**.

Set the SNMP OID and the value which will be set by this action (the specified OID must be writable on the target machine).

APS supports **String** and **Signed Integer** values to be set by this action, choose one **Value Type**:

Then type in the **Value** that you wish to set.

Press **Next** to continue.
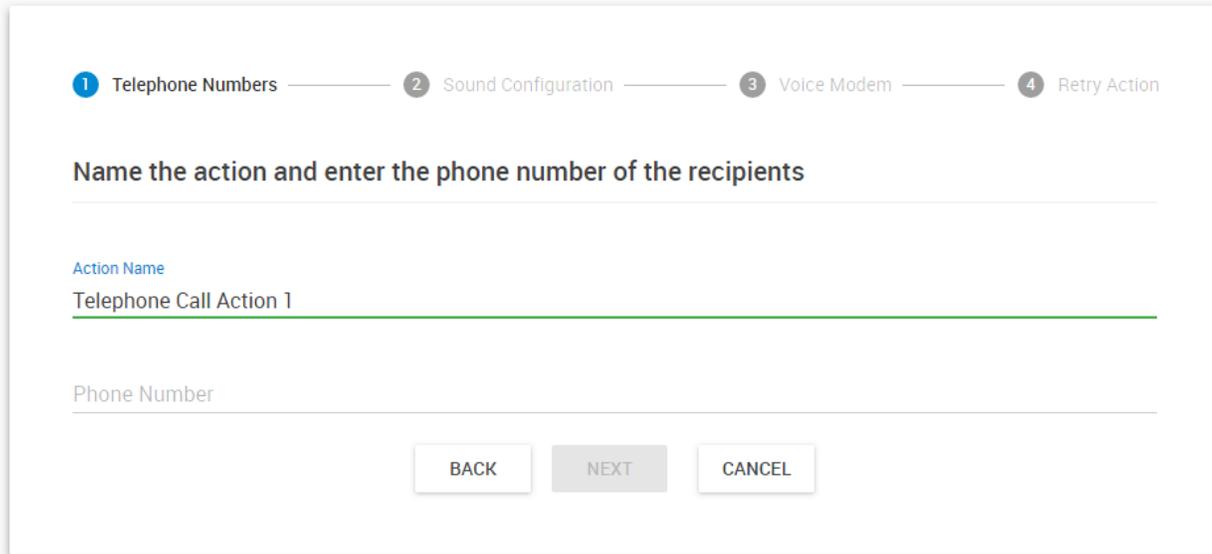
If required, specify the action retry parameters (up to 5 times to retry) and the interval of the retries, then press **Finish**.

SNMP Trap action

You can use the SNMP Trap Action to send a notification (Trap message) to your SNMP Trap Receiver server when a sensor reaches a certain threshold.

Choose the **SNMP Trap Version** between v1/v2/v3, the available options will vary slightly depending on the trap version selected.
The default **SNMP Port** is automatically selected, but you can modify if required.

You can specify multiple trap targets in one action, see below.

Destination IP Address

10.1.1.24

Community

••••••

| | ADD | DELETE |

	Address	Community
☐	10.1.1.23	••••••

| BACK | NEXT | CANCEL |

Enter your **Destination IP Address** and **Community**, then press **Add**.

If you need to add further computers to the list, add them the same way.

When done, select the computers you'd wish to send the trap message to and click **Next**.

A different trap message is sent for each sensor type such as temperature, humidity, and switch. The trap messages include *VarBind* fields that include the current sensor status (Normal, Critical High, Warning High, Critical Low, Warning Low, and sensorError), the current sensor value, the level exceeded, the sensor index, the sensor name, and the sensor description.

You can enable or disable specific fields if you choose the *customTypeTraps* from the drop-down list.

If required, specify the action retry parameters (up to 5 times to retry) and the interval of the retries, then press **Finish**.

Sound action

With the Sound Action, you can play an audio file when the notification runs.

Set the speaker volume and the play time. You can also choose to play the sound until it's acknowledged.

Important: the sound will only play locally on the server machine, where APS is installed.

You can select from the built-in alarm sounds to play from the list, or add your own .WAV file.

If required, specify the action retry parameters (up to 5 times to retry) and the interval of the retries, then press **Finish**.

Speech action

With the Speech Action, you can hear an audio report with your predefined message using text-to-speech.
You can customize the message with your own text, and add/remove macros as required.
We'll show you more details about macros at the SMS action description.

Set the speaker volume and speech speed, then preview the message.

Important: the sound will only play locally on the server machine, where APS is installed.

If required, specify the action retry parameters (up to 5 times to retry) and the interval of the retries, then press **Finish**.

Telephone call action

With the Telephone Call Action and a voice modem, you can directly call telephones and play an audio message.

Specify the telephone number first that you want to call to, then press **Next** for more options.

Select your **Call Type**:

With the **WAV file** method, you can play a predefined alert sound (in .WAV format). You can also add your own file to the list, not just the default ring sounds.

If you choose **Text to Speech**, then it will behave similarly to the Speech Action.

Define your custom message (with macros) and set the volume and speed parameters.
We'll show you more details about macros at the SMS action description.

Press **Next** for the modem settings.

Telephone Numbers ———— Sound Configuration ———— **3** Voice Modem ———— **4** Retry Action

Enter the modem settings

Voice Modem Port
COM2

Device Name: Communications Port (COM2)

Voice Modem Port Speed
Auto

Voice Modem Chipset
Custom Setup

ATD Command
ATD

Initialize String

AT Command After Answer Call

BACK   NEXT   CANCEL

This action needs a supported voice modem to function properly. Not all modems support analog voice input; you may contact Support for help on selection.

Custom Setup

Conexant

Rockwell

Wavecome

Cinterion MC55i

Teltonika G10

Edge-180M

Choose the connected modem from the serial ports list, and choose its chipset. If it's not listed in the selection, you can also specify a custom setup with custom initialization string.

The port speed could be left at Auto but if your modem has connection problems, try a fixed lower speed.

If required, specify the action retry parameters (up to 5 times to retry) and the interval of the retries, then press **Finish**.

Wake Up / Shutdown action

With this action, you can remotely shut down or wake up computers.
Windows and Unix/Linux systems are supported.

First choose the action type between **Shutdown** or **Wake Up**.
We'll show the settings for each type.

Wake on LAN (Wake Up)
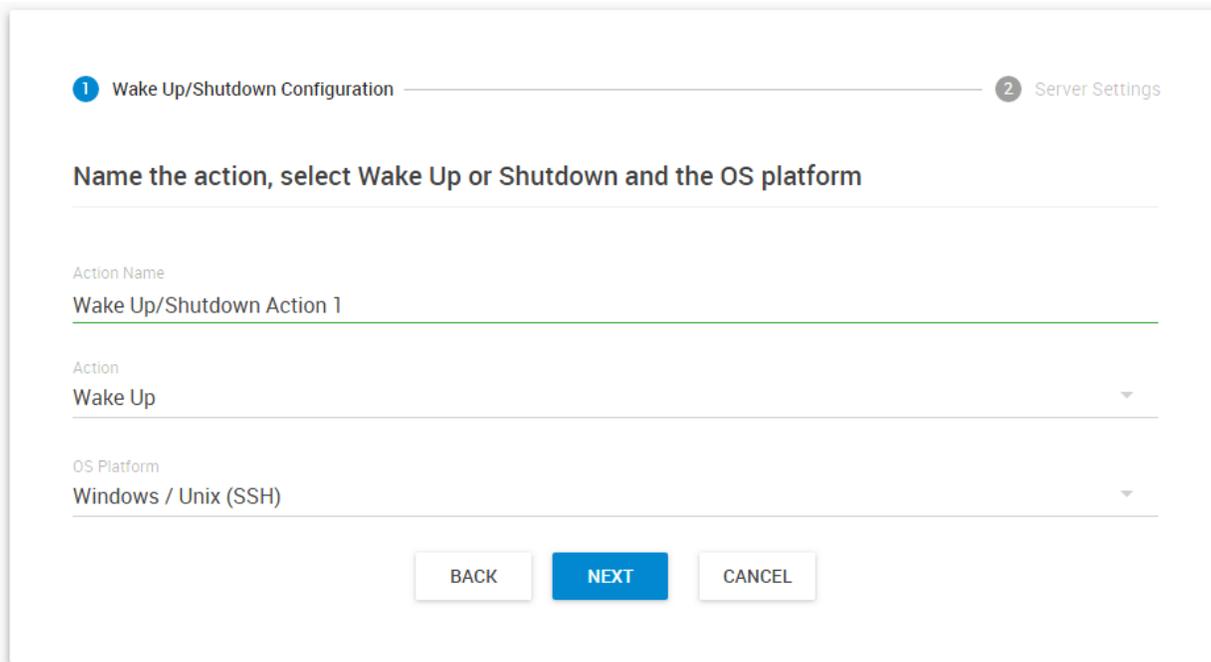
Choose the "Wake Up" action from the drop-down menu.
There's only one option needed for both Windows and Unix platforms, as the Wake-On-LAN function is OS-independent.
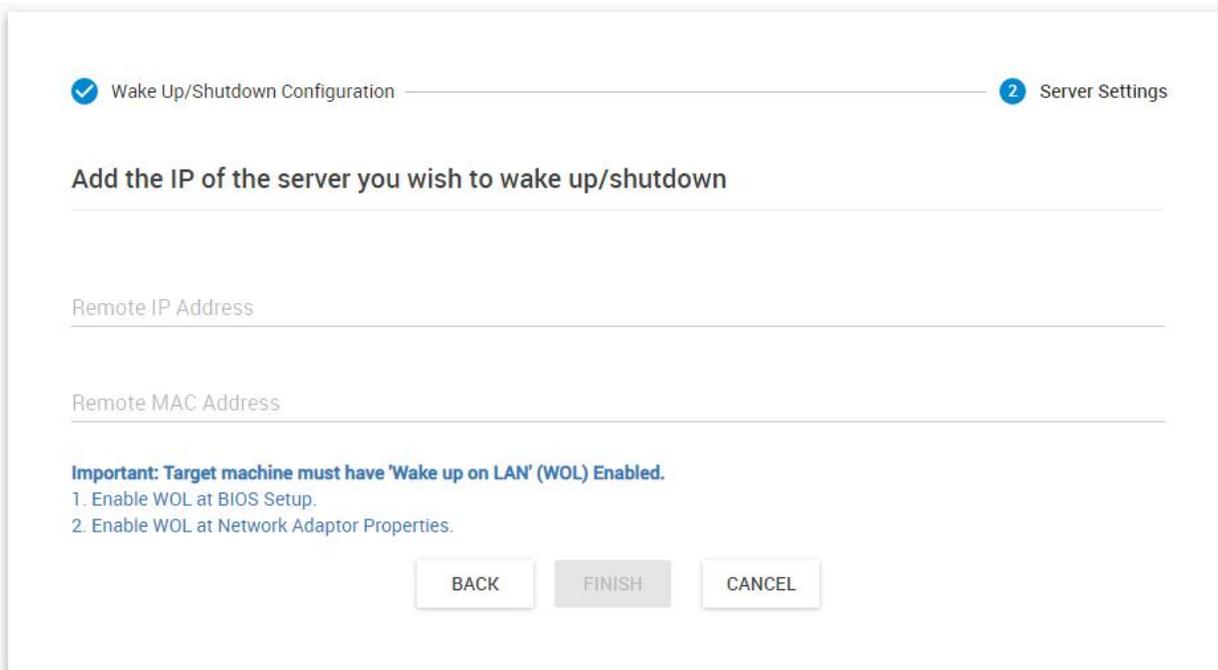
WOL needs the MAC address of the machine to function and you only need to enter this.
If you don't know your remote server's MAC ID then input the IP or hostname. APS can usually resolve these to a MAC ID automatically.

In case the remote machine doesn't support WOL, an error message will appear.

Note: The hardware must support *Wake On LAN*, and it has to be enabled in the system BIOS to be able to use this function. Consult your system's or mainboard's user manual on how to configure this setting. As a general rule, if you still see the LAN card showing network link and traffic LEDs when the computer is turned off, Wake On LAN could work.

Windows Shutdown

For the Shutdown action, first you'll need to select the OS platform.

Input your servers IP address into the "Remote IP Address" field.

Then input your log in username (who has rights to shut down the system) into the "Login" field, and the password.

Note: the host needs to be online to be able to verify the login credentials.

You may select additional options such as force-closing the running programs (recommended) and adding a timeout before shutdown. Click "**Next**" to continue.

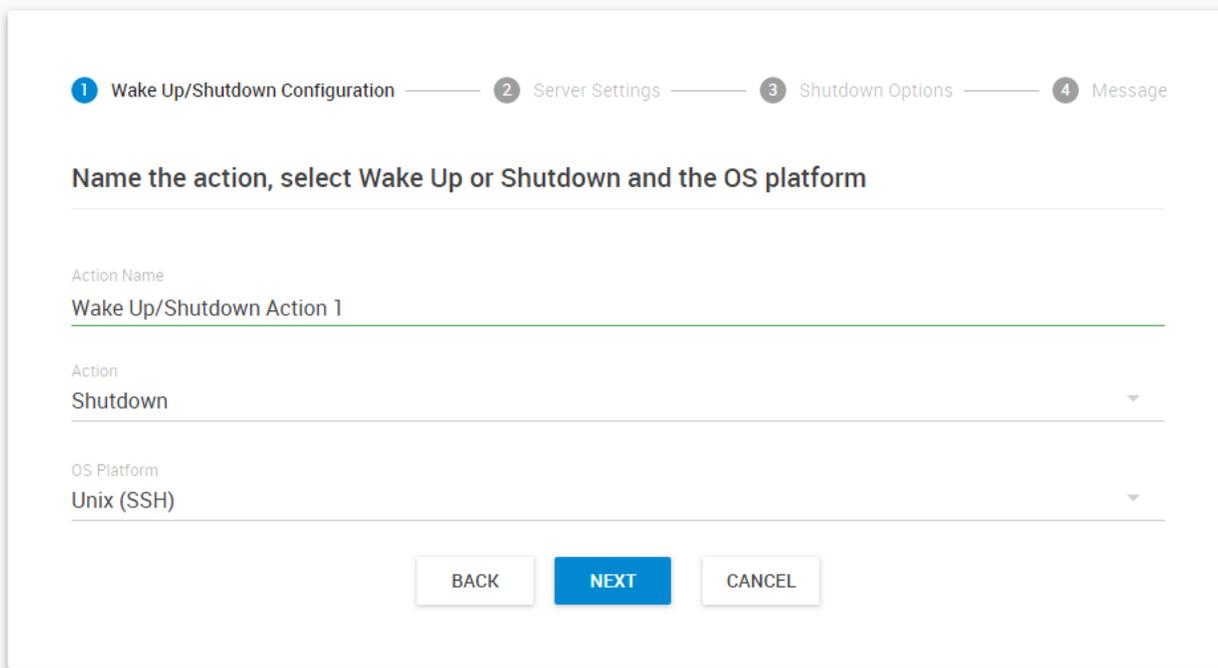*Note:* the timeout value must be between 30 and 86400 seconds.

You can also enable a shutdown message to be sent by first choosing "Show shutdown message", then entering your message in the "Message text" box (it also supports macros, see the SMS action for more details on macros), then click "**Finish**".

The message will be sent to the server log. The sent message will include the details relevant to your sensor.
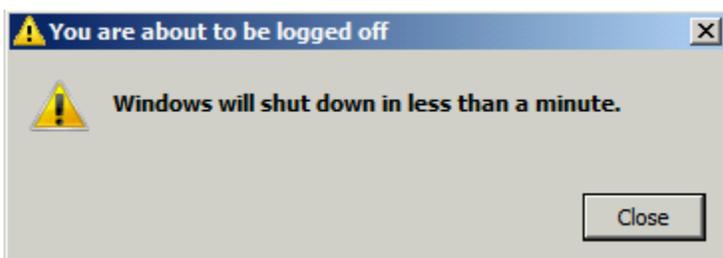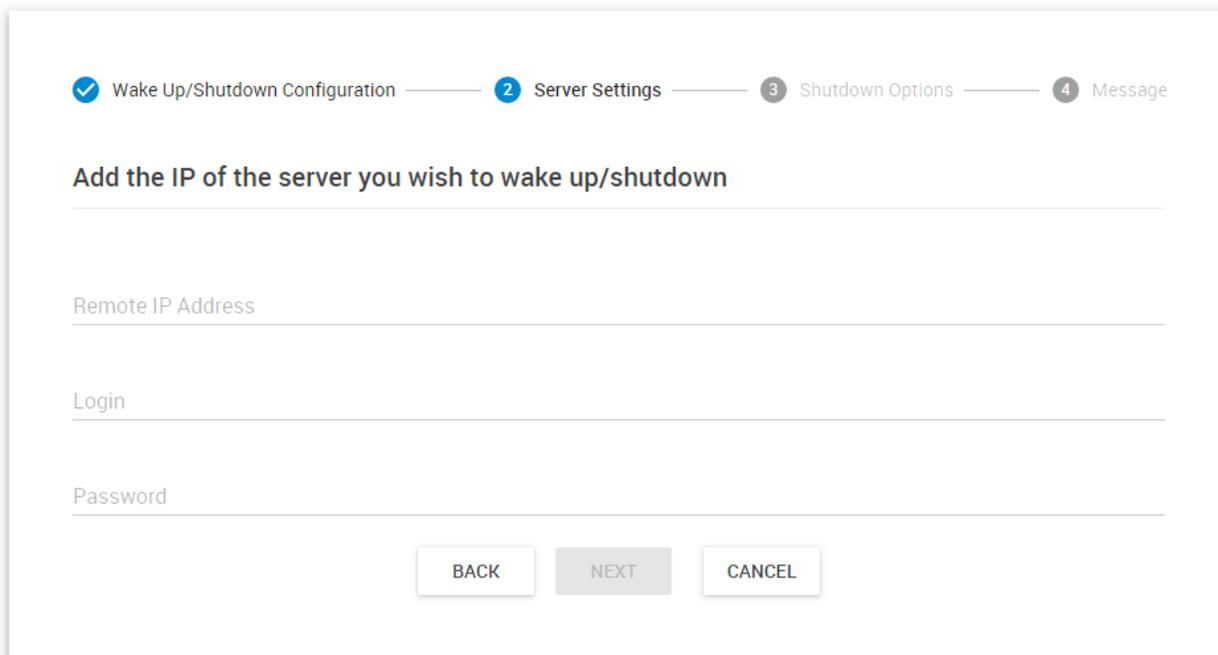

During shutdown on the remote machine, Windows will display a similar message before closing all programs.

Unix shutdown

For the Shutdown action, first you'll need to select the OS platform.
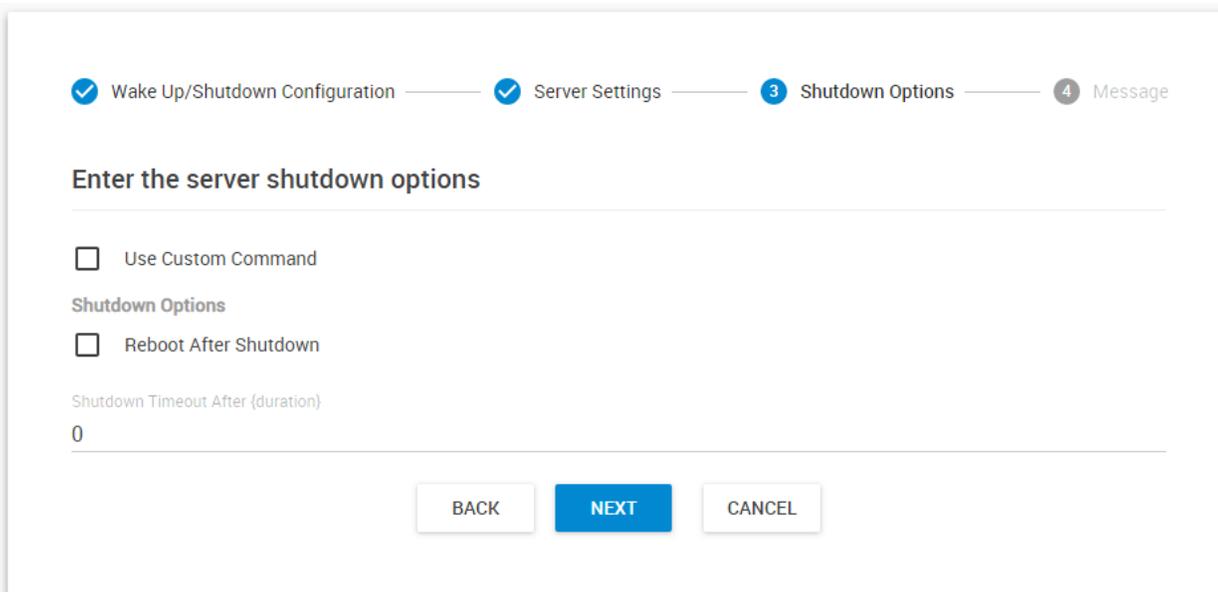
Input your servers IP address into the "Remote IP Address" field.
Then input your log in username (who has rights to shut down the system) into the "Login" field, and the password.

Note: the host needs to be online to be able to verify the login credentials.

You can set some other settings for the Shutdown action:

Reboot after Shutdown will perform a reboot instead of a poweroff command.
By clicking Use Custom Command you can specify your own shutdown command (see below).

Click "**Next**" to continue.

Normally you don't need to change the Shutdown Command. However you should change this for example for VMware ESXi servers where the shutdown binary is actually another script. We have a manual about shutting down ESXi servers with SEC units, the same workaround can be used here.

You can also enable a shutdown message to be sent by first choosing "Show shutdown message", then entering your message in the "Shutdown Message" box, then click "**Finish**".

The message will be sent to the server log. The sent message will include the details relevant to your sensor.

Windows alert action

Windows Alert

Notifications / Actions / Windows Alert

① Windows Alert Configuration ——————— ② Alert Message ——————— ③ Retry Action

Setup the alert type and the destination of the alert

Action Name
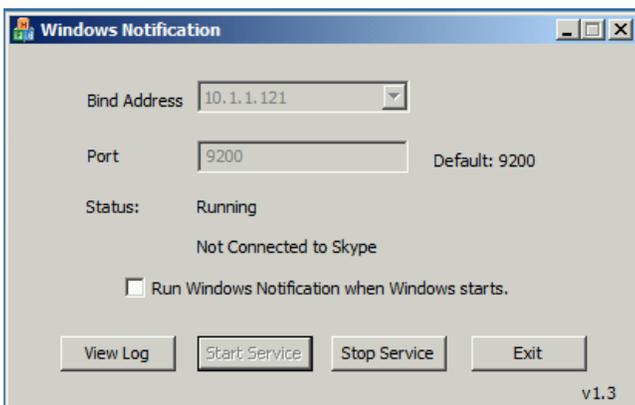Windows Alert 1

Windows Host Address

Windows Host Port (default: 9200)
9200

Windows Alert Type
Tray notification

Sound Alert
None

BACK   NEXT   CANCEL

With the Windows Alert Action, you can display a visual alert message on the remote computer. For this action to work, you need to install and start the **Windows Notification service** (selectable part of APS installation) on the target PC:

Windows Notification

Bind Address 10.1.1.121

Port 9200   Default: 9200

Status: Running

Not Connected to Skype

☐ Run Windows Notification when Windows starts.

View Log   Start Service   Stop Service   Exit

v1.3

You can choose to display the alert message as a tray notification or in a popup window:

Tray notification

Pop-up window

Optionally you can also add the default Windows alert sound when the popup is shown:

None

Windows alert sound

✔ Windows Alert Configuration ——— ② Alert Message ——— ③ Retry Action

Define the content of the message

From
$[IP]

Message
$[DESCRIPTION] is now $[VALUE], status is now $[STATUS]

PREVIEW   RESTORE DEFAULT   **ADD MACRO**

BACK   **NEXT**   CANCEL

Customize the message contents here (macros are supported).
We'll show you more details about macros at the SMS action description.

Note that you cannot display a lot of information due to the small size of the popup.

Windows Alert Configuration ——————— Alert Message ——————— 3 Retry Action

Set the number of retires and interval
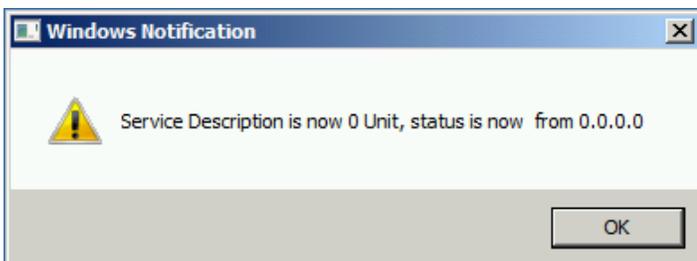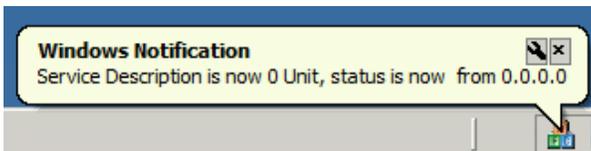
Maximum Times to Retry
0

Retry Interval for 5 - 60 seconds
10

BACK   FINISH   CANCEL

If required, specify the action retry parameters (up to 5 times to retry) and the interval of the retries, then press **Finish**.

Test your action. If the notification doesn't show on the target machine, check the firewall settings and that the notification program is running and bind to the correct IP address.

The test action will show only 0 values.

Windows Notification
Service Description is now 0 Unit, status is now from 0.0.0.0

Windows Notification
Service Description is now 0 Unit, status is now from 0.0.0.0
OK

Notifications

This is the **Notification Rules** page. If you have notifications set up, they will appear in the list and you can edit or remove them.
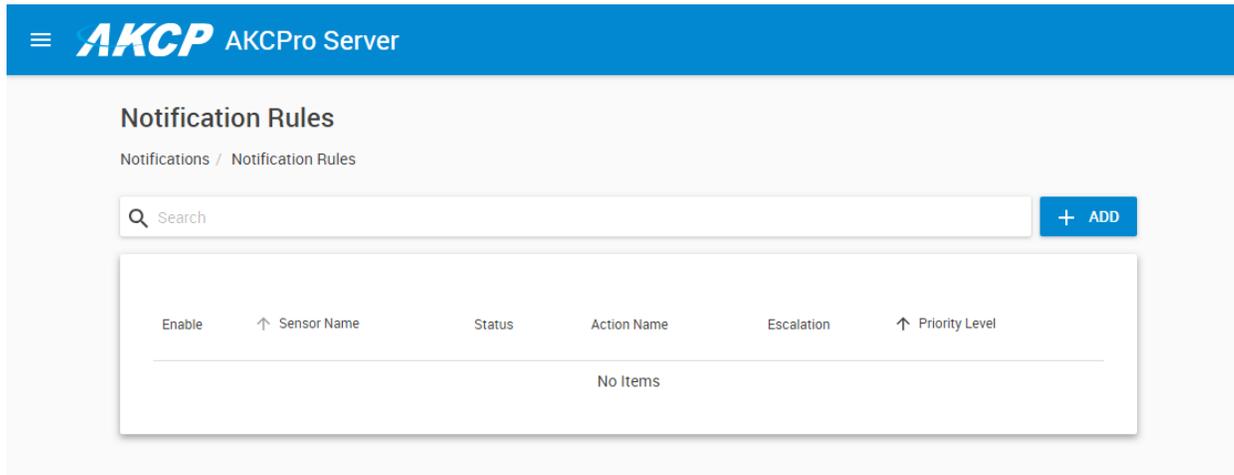
With Notification Rules you can define which Actions to take when certain sensor statuses happen. Therefore first you need to create **Actions** and then create a **Notification Rule** to link the Action to sensor- and status conditions.

You could create an action under the Actions menu beforehand, or create it during the Notification wizard.

Notifications usage are best described through an example; we'll show you one on the following pages. We'll set up an example rule for SMS notification, and we'll use the second method of creating actions during the Notification wizard.

Example Notification rule

On this picture you can see 3 notification rules already created. As an example we'll create the SMS notification, which will alert you when a network device's status become unreachable.

Click on the **Add** button to begin the Notification wizard.

First the wizard will ask about the notification priority level.
If you have many notifications, you can adjust their priority with this setting.
The notification(s) with the highest priority will execute first, if there are multiple conditions occurring at the same time.

This priority level can be adjusted at a later time, so usually you can leave it as Normal.

Click **Next** to continue.

Notification Rule Wizard

Notifications / Notification Rule Wizard

✓ Priority Level ——— ② Sensors ——— ③ Actions ——— ④ Duration ——— ⑤ Scheduler ——— ⑥ Escalation

Choose sensor and status that will trigger the notification

Sensor

🔍 Search

∨ **AKCPro Server**

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

∨ **AVTECH's AVM328A (10.1.1.132)**

∧ **Network Device (10.1.1.23)**

  ☑ Host Status

∨ **System Name (10.1.1.137)**

Status

☐ Reachable

☑ Unreachable

☐ Sensor Error

➡

BACK   NEXT   CANCEL

Select a sensor and the status requirements which will trigger this notification. The statuses that you can select from will vary depending on the device or sensor.

As our example, we'll select the Network Device Host Status that we want to monitor, and the Unreachable status.

Click **Next** to continue.

Select an action to execute with this notification by placing a mark in the checkbox before the action name.

If the desired action does not exist yet, you can create an action from here by clicking the '**Create Action**' button.

In the example below, we'll set up a notification rule where an SMS notification to the administrator will be sent out when the 'Host Status' of a connected Network Device becomes 'Unreachable' status.

Since the SMS action doesn't exist in our list yet, we'll be creating this action in the following steps.

After you click on the '**Create Action**' button, it will open another browser tab with the Actions menu. The Notification Rule wizard will continue to run in the background and you can return to it when the Action configuration has finished.

Click on the **Add** button here to add the new action. This will begin the Action Wizard.
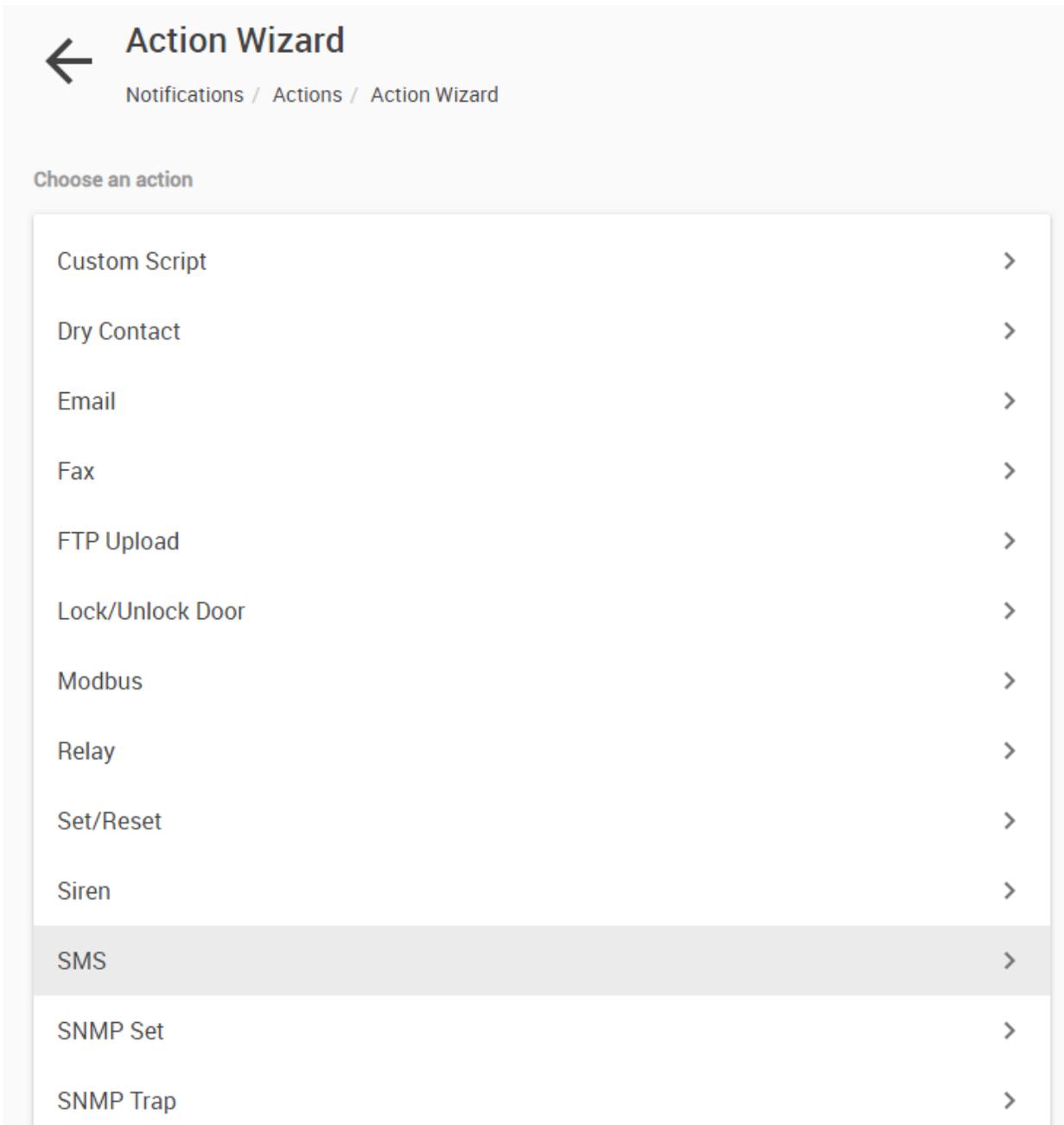
Action Wizard

Notifications / Actions / Action Wizard

Choose an action

Custom Script	>
Dry Contact	>
Email	>
Fax	>
FTP Upload	>
Lock/Unlock Door	>
Modbus	>
Relay	>
Set/Reset	>
Siren	>
SMS	>
SNMP Set	>
SNMP Trap	>

In the Action Wizard, you will see a list of notification actions.
Select the SMS action and click '**Next**'.

Enter the action name and enter at least one phone number in the Phone Number List.

Click '**Next**' to continue.

SMS Action

Notifications / Actions / SMS Action

✓ Phone Numbers ──── **2** SMS Message ──── **3** Modem ──── **4** Retry Action

Define the content of the message

From
$[IP]

Message
$[DESCRIPTION] is now $[VALUE], status is now $[STATUS]

[PREVIEW] [RESTORE DEFAULT] [**ADD MACRO**]

[BACK] [**NEXT**] [CANCEL]

You can preview and customize the SMS message to be sent here.

The IP address can be seen in the From field as an example of a macro description named $[IP]. In the actual SMS message, the value of $[IP] will depend on the IP address of the host sending the notification.

Define the content of the message

From
127.0.0.1

Message
Testing Sensor Port 1 is now 80, status is now Normal

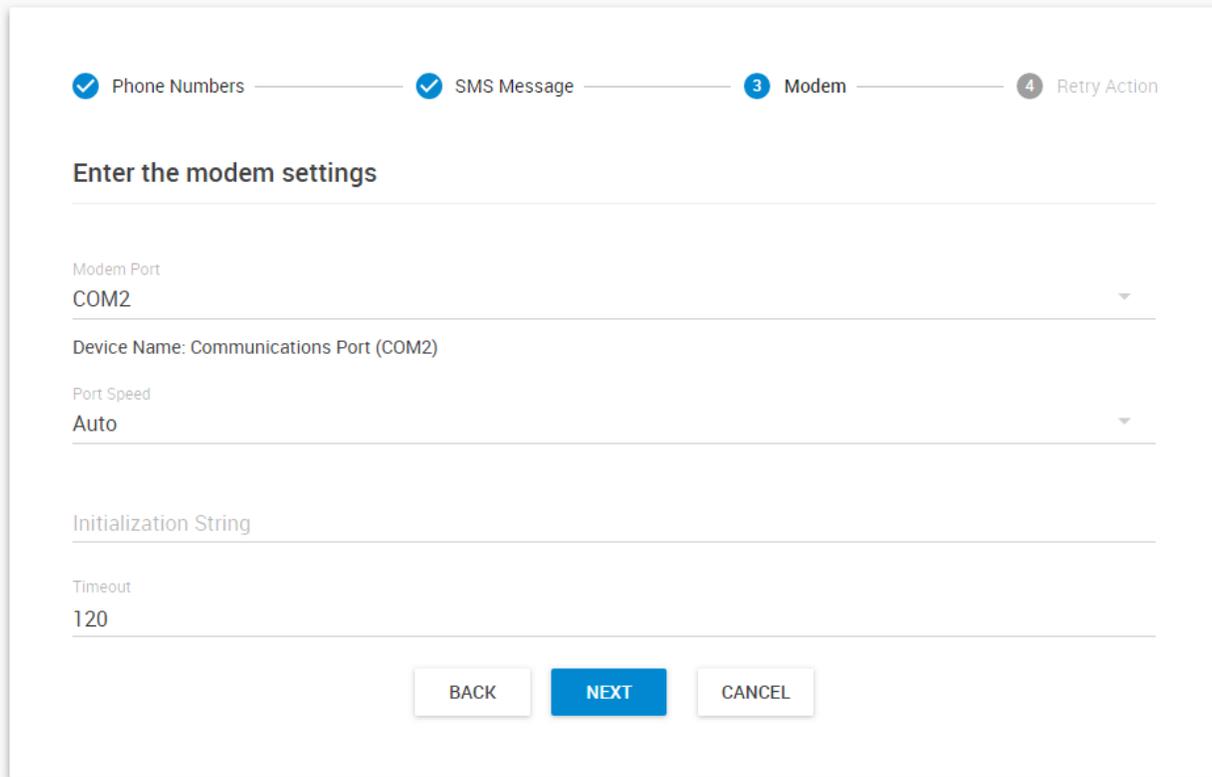[EDIT] [RESTORE DEFAULT] [ADD MACRO]

Use the **Preview** button to check the message contents.
You can get more details about macros at the SMS action description.

To customize your message, enter your custom text in the Message box - however keep in mind the maximum character limit of an SMS.

SMS Action

Notifications / Actions / SMS Action

✓ Phone Numbers ——— ✓ SMS Message ——— ③ Modem ——— ④ Retry Action

Enter the modem settings

Modem Port
COM2 ▾
Device Name: Communications Port (COM2)

Port Speed
Auto ▾

Initialization String

Timeout
120

BACK **NEXT** CANCEL

We select COM2 as the **Modem Port**. Usually the connected device name will be also displayed.

We will the leave the **Port Speed** at 'Auto' (default setting).

Some modems require custom **Initialization String** specified. Usually this is not needed and you can leave this field empty.

"**Timeout**" is the time lapsed in seconds that the system has no response from the modem device.

Click '**Next**' to continue.

SMS Action

Notifications / Actions / SMS Action

"**Maximum Times to Retry**" is the number of times the SMS message will be resent, if unsuccesful. "**Retry Interval**" is the time interval in seconds between the resent SMS messages.

In this example, we only want to receive one SMS message so we will set the "Maximum Times to Retry" to 0.

You can click the '**Back**' button to change any previous configuration.
Click the '**Finish**' button to create the SMS Notification Action.

Actions

Notifications / Actions

Enable	↑ Action Type	↑ Action Name			
🔵	📄 Custom Script	Custom Script	✏️	🗑️	TEST ACTION
🔵	🗔 SMS	SMS Action 1	✏️	🗑️	TEST ACTION
🔵	≡ Windows Alert	Windows Alert 1	✏️	🗑️	TEST ACTION

Our new SMS action named 'SMS' is created and displayed in the Actions list.

You can test your newly created notification action by clicking on the '**Test Action**' button to make sure it does what you need it to do. You can click the 'Edit' button if you need to reconfigure the action.
You can also disable an Action selectively with the slide button before its name.

Now you can close this browser tab with the Actions, and resume the Notifications setup.

The newly created SMS action will appear in the Actions list.

Place a checkmark in front of it to select this action, then click '**Next**' to continue.

Notification Rule Wizard

Notifications / Notification Rule Wizard
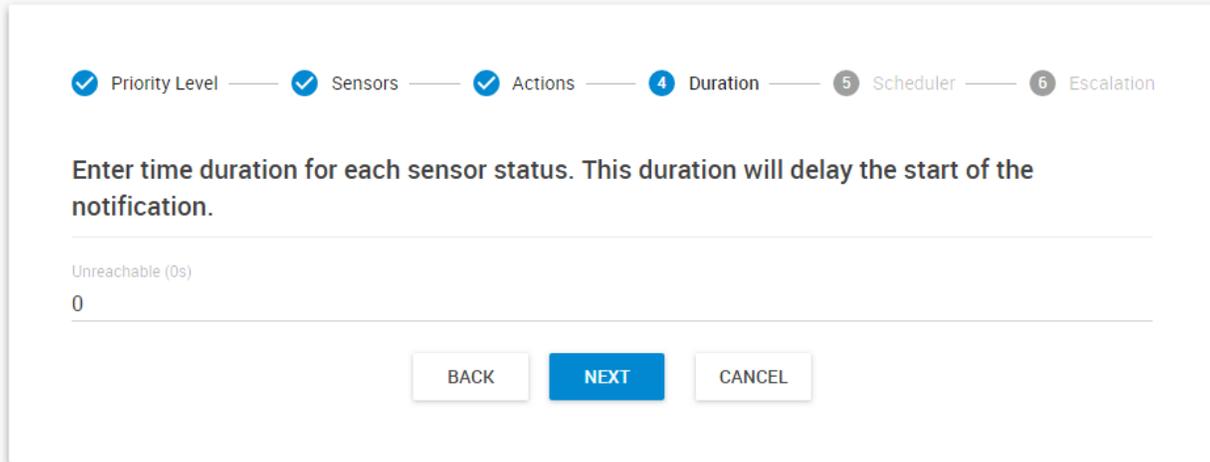
✓ Priority Level ——— ✓ Sensors ——— ✓ Actions ——— **4** Duration ——— **5** Scheduler ——— **6** Escalation

Enter time duration for each sensor status. This duration will delay the start of the notification.

Unreachable (0s)

0

BACK   NEXT   CANCEL

You can set up the notification rule wherein it will only execute when a certain status will persist in the specified continuous time (in seconds). This feature allows us to filter the real threats from false alarms because of possible fluctuations that can occur in the sensor values but poses no real threat.

This step may vary slightly depending on the source sensor type you selected.

Click '**Next**' to schedule when the notification will only be active.

You have the option to enable the calendar option, else the notification will always be active.

You have the option to include an escalation that will trigger after a given time after the initial notification. If you wish, you may add it later from the Notification Rules list page.

Click '**Finish**' to create the notification rule.

You now have created the notification rule, it will appear in the Notification Rules list.

You have the option to Edit, Remove and add an Escalation to the rule.
You can also disable a Notification rule selectively with the slide button before its name.

7.6. Video Recording

Recording Policies
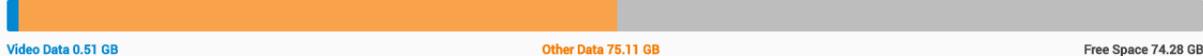
In order to setup the recording policies on the server software, you need to first make sure that your cameras are online, are operating properly and are mounted in the correct position.

IP cameras should be accessible on the network and with ONVIF protocol enabled.
In case of USB cameras, you should have them already connected to the securityProbe 5E base units' USB ports or to the SEC+ base units.

We'll show you the recording steps using an IP camera. The setup steps are identical when using a USB camera connected to a client securityProbe 5E base unit, or an IP camera.

First, add the IP camera (or your client unit SEC5 with USB camera) to the AKCPro Server. You can review the section "Adding your client unit" in this manual.
After this, the camera will be visible as a client unit (USB cameras will be shown under the unit they're connected to):
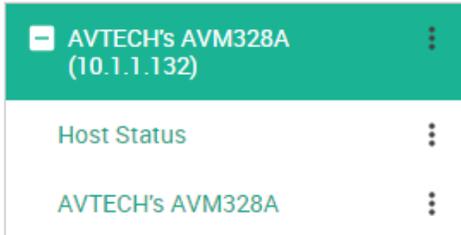
In case your camera doesn't get recognized immediately, try to refresh the HTML page.
If it's still not visible, it could be that the particular model is not supported. Although many types of ONVIF cameras might work, sometimes you need to configure ONVIF users manually to make them work with APS. We have guide manuals for specific IP camera models and manufacturers; you may ask help from Support if you cannot configure the camera yourself.

Next, click on the **Recording Policies** menu.
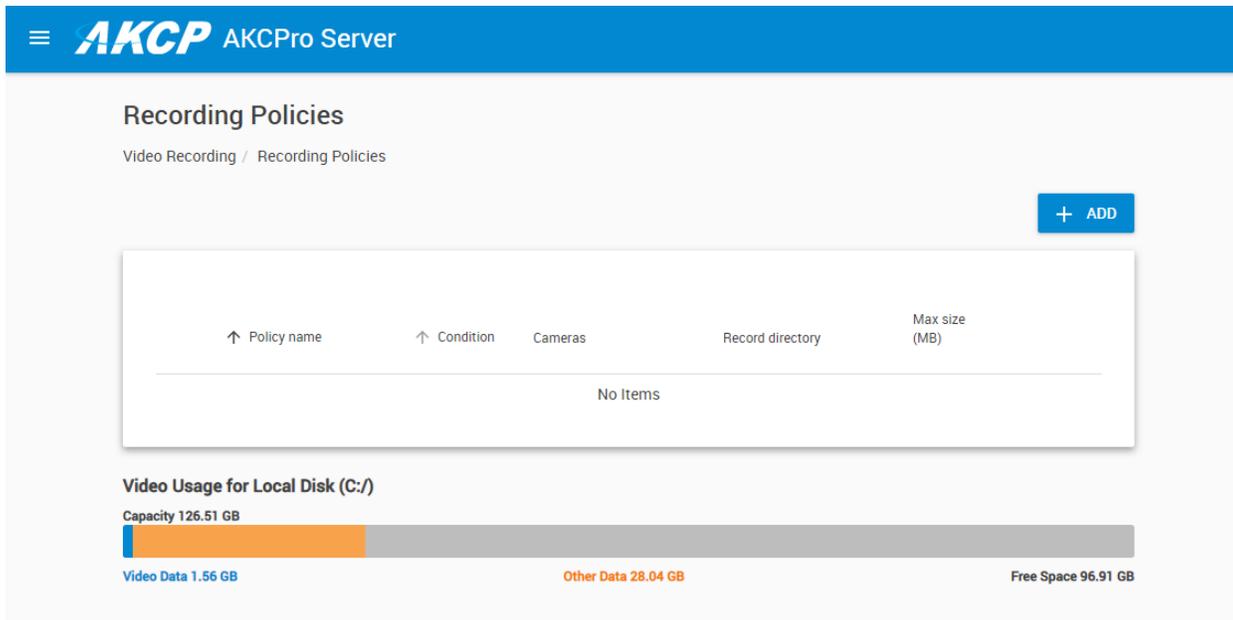
Here you can add/remove/edit policies.
Click **Add** for a new policy.

Also you can see the storage usage of your disks with the video data and other data, and the free space.
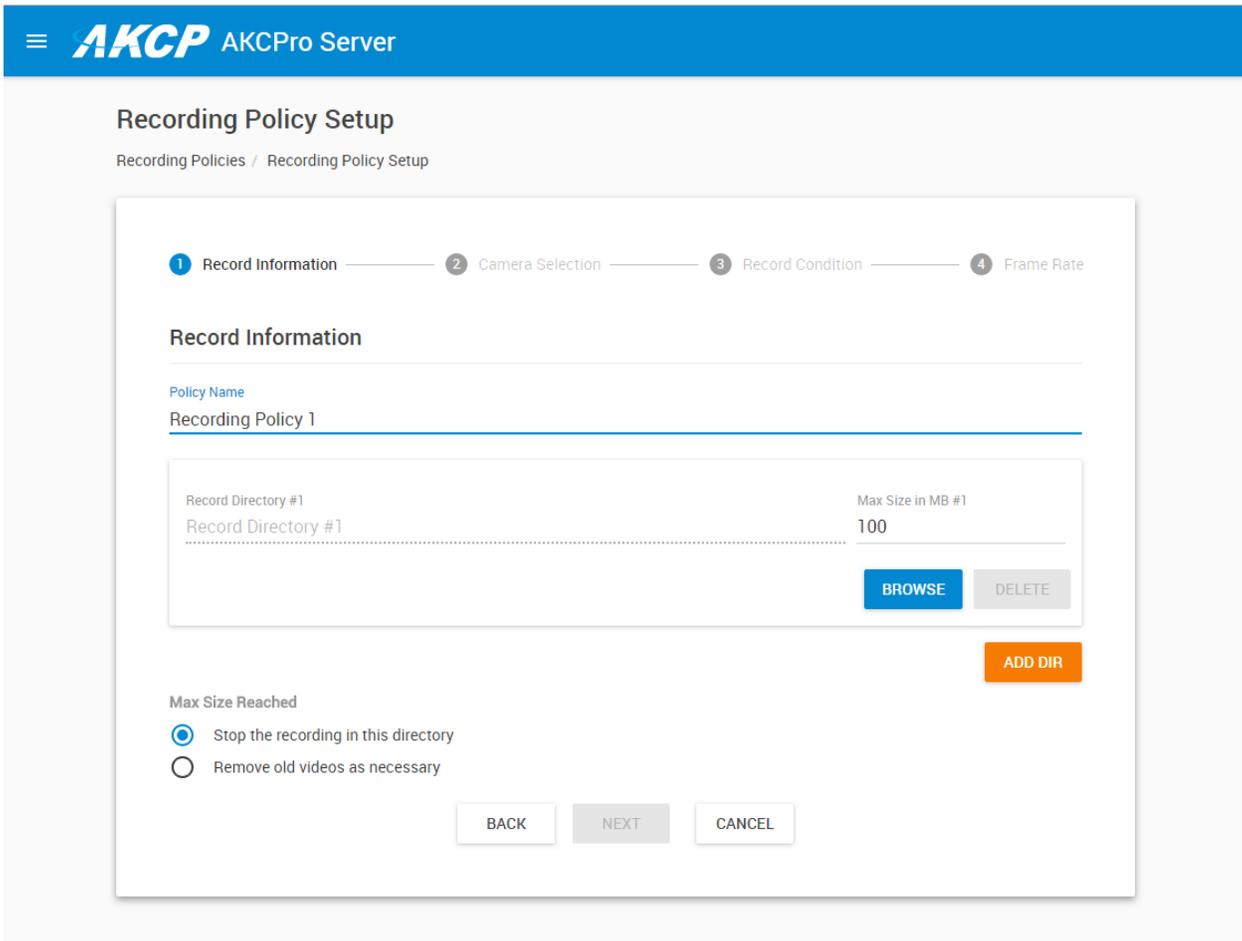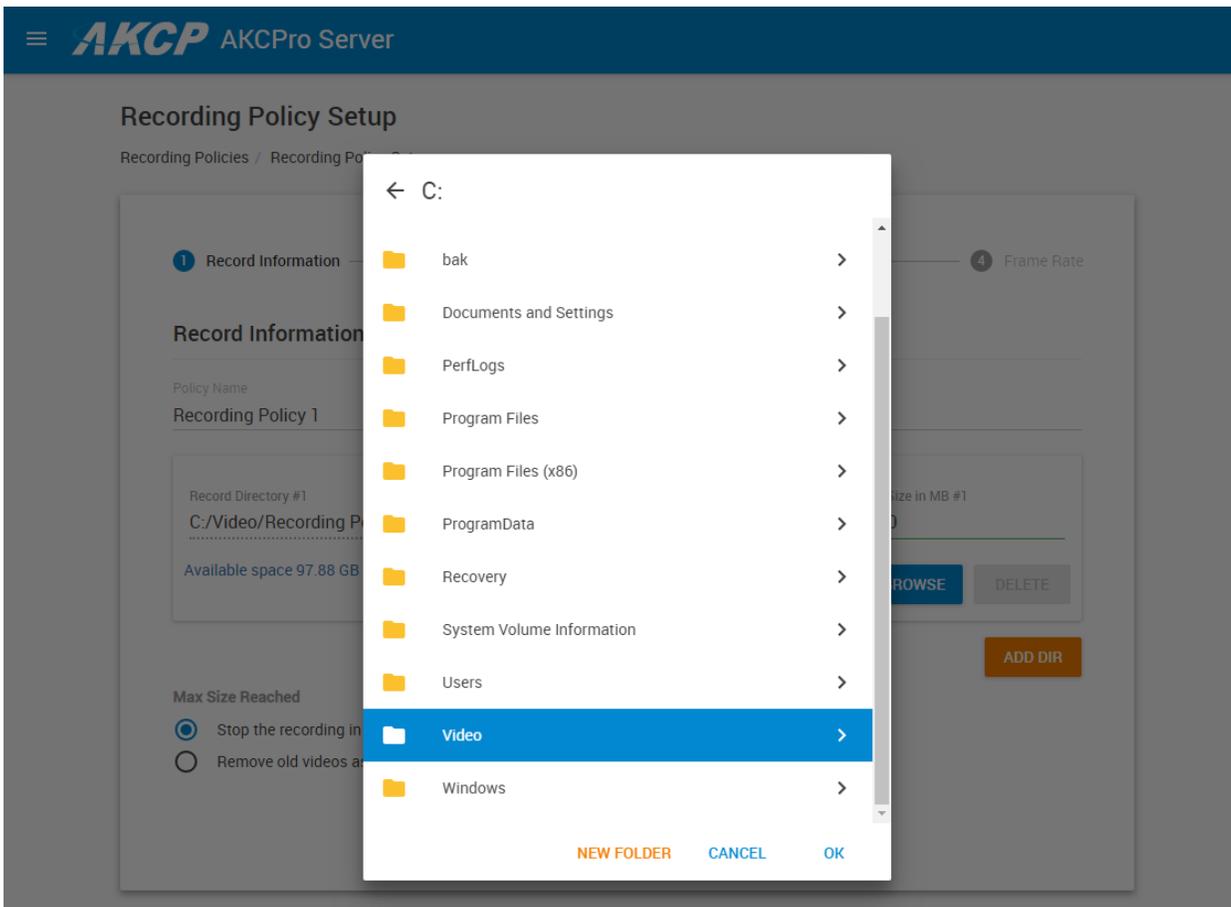
The Recording Policy setup wizard will be launched.

1: Give the new policy a name.
Next, select the maximum size of the video recording storage.
Choose a folder on the server to store the video with the **Browse** button.
Decide if you want to record over the oldest video, or stop recording when the storage limit is reached.

You can select an existing directory, or make a new one to store your videos.

Any new recording policies will be created under here.
Very important: you only need to select the folder itself and don't browse into it.
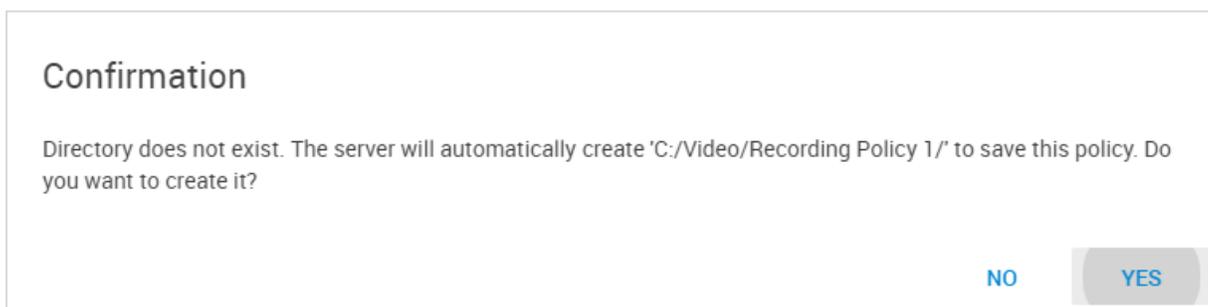
If the directory where you want to record the video has not yet been created, you will be prompted to create it.

Note: The software will create another sub-folder with the policy's name under the specified directory.

2: Choose which camera you would like to be recording the video from the **Available Cameras list** and click **Next**.
For this example we've selected the single AVTECH IP camera.

USB cameras on a client SEC5 unit would show as V1, V2, V3, V4 cameras (unless they have been renamed on the unit). You can tell which camera is on which unit by their IP addresses, as seen here:

Important note: If a camera has been already assigned to a recording policy, you cannot add it to a new policy without first disabling that policy or removing the camera from it.

Recording Policy Setup

Recording Policies / Recording Policy Setup

✓ Record Information ———— ✓ Camera Selection ———— ③ Record Condition ———— ④ Frame Rate

Record Condition

Choose when to record videos

⦿ Always
   A video is always recorded

○ Time Event
   A video is recorded according to a scheduled time

○ Sensor Event
   A video is recorded when a sensor status changes

○ Time-Sensor Event
   A video is recorded when both events occur

[BACK] [NEXT] [CANCEL]

3: Choose the recording condition.

Recording with the "Always" option is the simplest and require no extra options except the framerate.

In our example we'll use the **Sensor Event** option so that the camera will record when a sensor's status is changed.

Recording Policy Setup

Recording Policies / Recording Policy Setup

✓ – ✓ – ✓ Record Condition – ④ Frame Rate – ⑤ Sensor Selection – ⑥ Sensor Status – ⑦ Sensor Schedule

Frame Rate Setup

☐ Enable video recording when no event occurs

Enter sensor event frame rate (fps)

30

Enter pre/post recording time on sensor event

Pre Recording Time in seconds

3

Post Recording Time in seconds

3

[BACK] [NEXT] [CANCEL]

4: If you wish so, you can enable video recording when no event occurs and set the frame rate. This will allow the camera to still record video if there is no special event.

Here you can also set the frame rate for the video, and set the camera's pre- and post-recording time in seconds.

Recording Policy Setup

Recording Policies / Recording Policy Setup

✓ – ✓ – ✓ Record Condition – ✓ Frame Rate – **5** Sensor Selection – 6 Sensor Status – 7 Sensor Schedule

Choose sensors and status that will trigger the sensor event

Sensor

🔍 Search

☐ Virtual Sensor Port 11

⌃ SPX 56 (192.168.17.3)

☐ Host Status

⌃ Module 0 - 4x Sensor Ports

☑ Dry Contact Port 1

☐ Relay Port 2

⌃ Virtual Sensors

☐ SNMPGet

☐ VPing

⌃ System Name 98 (SEC+)

Status

☐ Sensor Error

☐ Low

☑ High

BACK   NEXT   CANCEL

5: Choose the sensor that will trigger the sensor event for the recording.
In this example, we choose the Dry Contact on a connected SPX unit's Port 1.

Recording Policy Setup

Recording Policies / Recording Policy Setup

✓ – ✓ – ✓ Record Condition – ✓ Frame Rate – ✓ Sensor Selection – ⑥ Sensor Status – ⑦ Sensor Schedule

The sensor event setup helps you to filter false sensor notifications. By setting the duration for each chosen sensor status, you can offset the start of a recording policy

High status delay in seconds

0

BACK   NEXT   CANCEL

6: Specify the sensor duration times for the sensor that will trigger an event.

Recording Policy Setup

Recording Policies / Recording Policy Setup

✓ – ✓ – ✓ Record Condition – ✓ Frame Rate – ✓ Sensor Selection – ✓ Sensor Status – 7 Sensor Schedule

The scheduler provides the facility to have the sensor event active for selected period

☑ Enable Event Scheduler

Select the time that sensor event will be active

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.   Working Hours / Inverse All

BACK   FINISH   CANCEL

7: If you need to add a schedule to the recording policy, you can add it here. Otherwise the recording policy will be always active.

8: Finish the wizard, and verify your new recording policy.

If you need to modify the policy, just click on the **Edit** button to return to the wizard to make the changes.

Your camera will show the recording state when it's capturing video. If the configured disk limit has been reached, then the recording will stop:
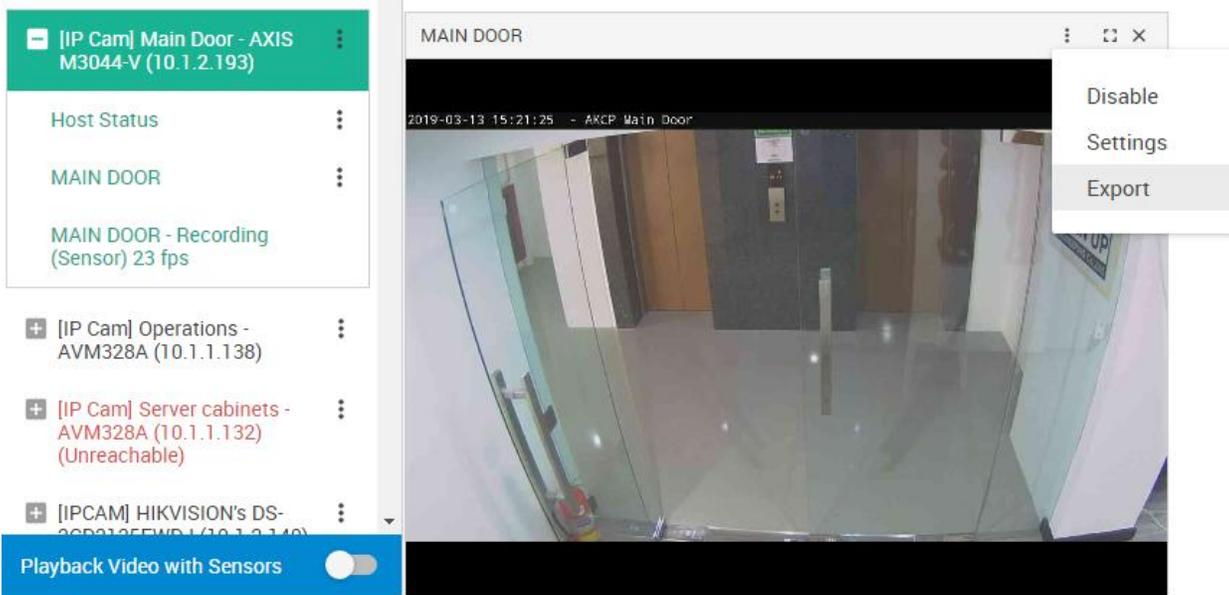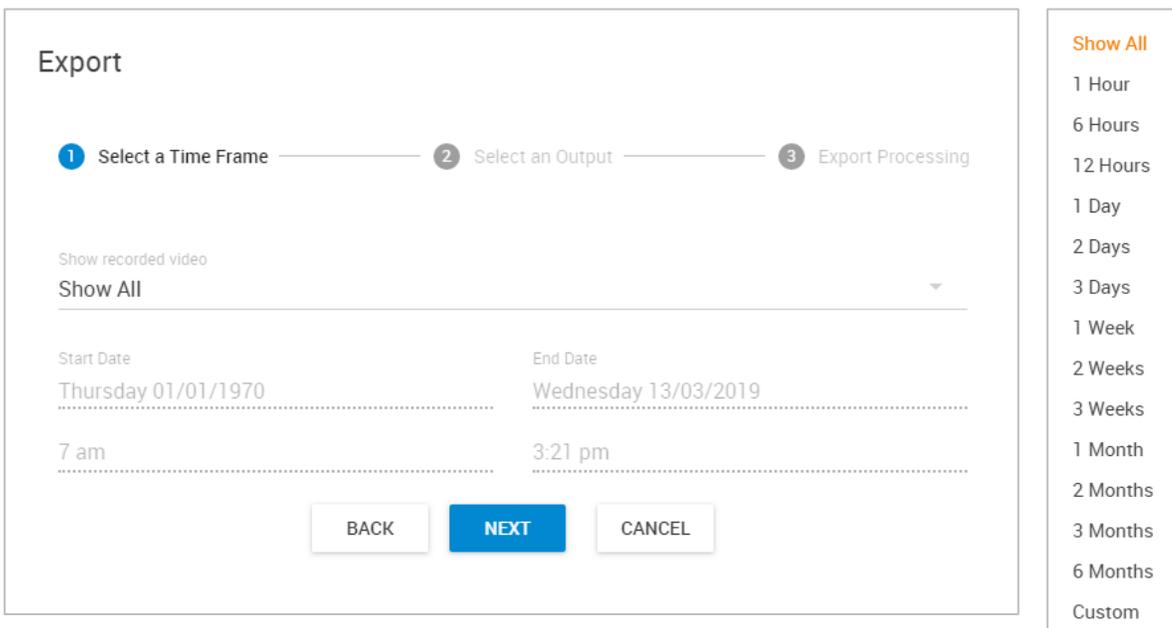

You can also disable a policy so that its settings will be kept, but the recording will be turned off:
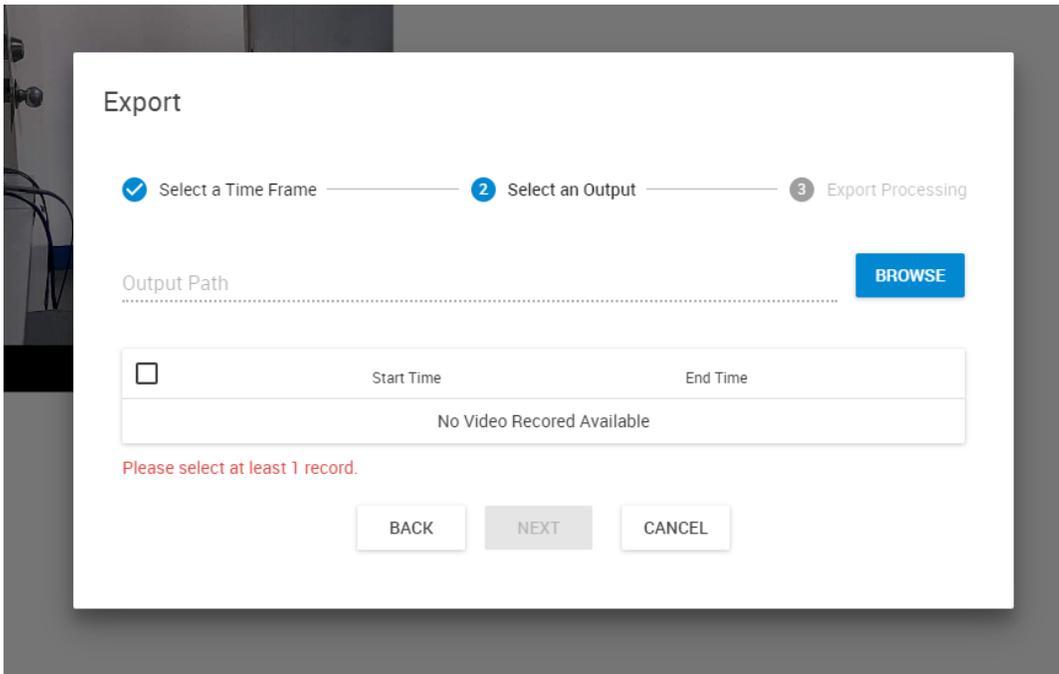
Exporting recorded videos

Once you have set up Recording Policies to record video files, you can export them within a chosen time frame. Click on the camera's popup menu and select **Export**.

The Video Export wizard will run. First you have to select the time frame of the recorded videos.
The default option is to show all recorded files.
Click **Next** to continue.

Important:

APS needs time to record and split the video files. Until the first file is still being opened and data written to it, you won't see any video files to appear under the Export window.
The duration for beginning a new video file is depending on the camera type and its video stream.
APS can only export the file if it's released and no longer being written to. While APS is still writing to the current video file, it can't offer it for exporting.

Under Windows you can open the Recording Policy's directory to see when APS begins to record to a new file:

If there are AMC files, they will split frequently with smaller sizes. But if it's MJPEG, then the file split may take a long time until it reaches 2-4 or more Gigabytes.
To force APS to stop recording video, you can disable the Recording Policy.

Export

Select a Time Frame ———— ② Select an Output ———— ③ Export Processing

C:/Marketing/   **BROWSE**

Available space 152.35 GB of 465.66 GB

	Start Time	End Time
☐	26/02/2019 19:00:00	26/02/2019 19:59:59
☑	26/02/2019 20:00:00	26/02/2019 20:22:07
☑	26/02/2019 20:22:16	26/02/2019 20:23:21
☑	26/02/2019 20:23:29	26/02/2019 20:33:45
☐	26/02/2019 20:34:00	26/02/2019 20:35:05
☐	26/02/2019 20:35:14	26/02/2019 20:58:03
☐	26/02/2019 20:58:18	26/02/2019 20:59:22
☐	26/02/2019 20:59:32	26/02/2019 20:59:59
☐	26/02/2019 21:00:00	26/02/2019 21:23:35

Total File Size: 2132.03 MB

BACK   **NEXT**   CANCEL

Next choose a directory where you'll export the video files to, with the **Browse** button.
In our example we've chosen the *C:\Marketing* directory.

Important: this export directory will be local to the server computer, not the PC or device where you're using the Web UI. On SEC+ you'll only be able to select a fixed directory.

Choose the video files from the list that you wish to export, and click **Next**.
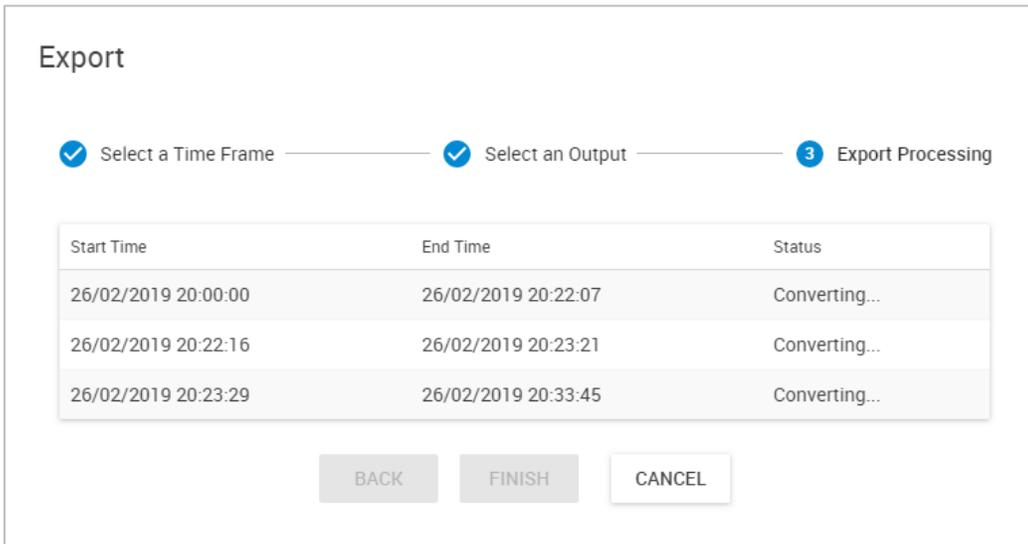
APS will proceed with converting the files to MP4 format.
Please keep in mind that it can take a long time for the conversion to process, especially with the huge MPEG files.
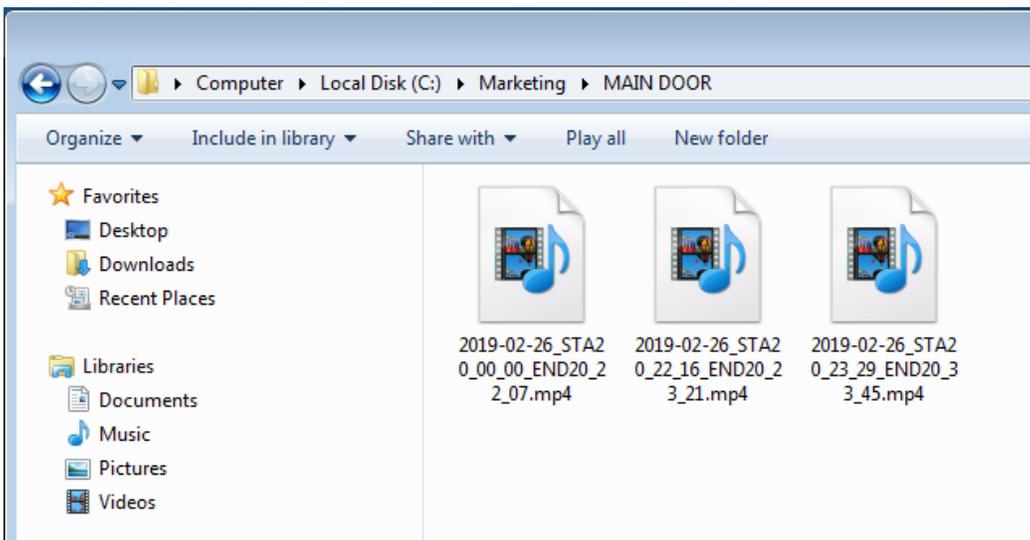
You can access the converted files in the chosen directory, under a directory with the camera's name.
To be able to play these files you would need VLC, Media Player Classic or a codec pack.

On SEC+ units you can use the Export to USB function to copy these video files to a USB drive.

Archive policies

Click on the **Archive Policies** menu to configure the automatic video archiving.
During video playback, the video files which have already moved to the archive directories should still be able to play back normally (provided that the archive directory and the required video file is still accessible).

Here you can add/remove/edit policies. Click **Add** for a new policy.
As with the Video Recording policies, you can see the storage usage of your disks with the video data and other data, and the free space.

The Archive Policy setup wizard will be launched.
You must change the Archive Directory's location to be different from the recording directory.

1: Choose a folder on the server to store the archived videos with the **Browse** button.

Important Note: there is no maximum size limit for the video archive. You'll have to manually delete old video files if your storage is getting full. Keep this in mind when you choose the archive options.
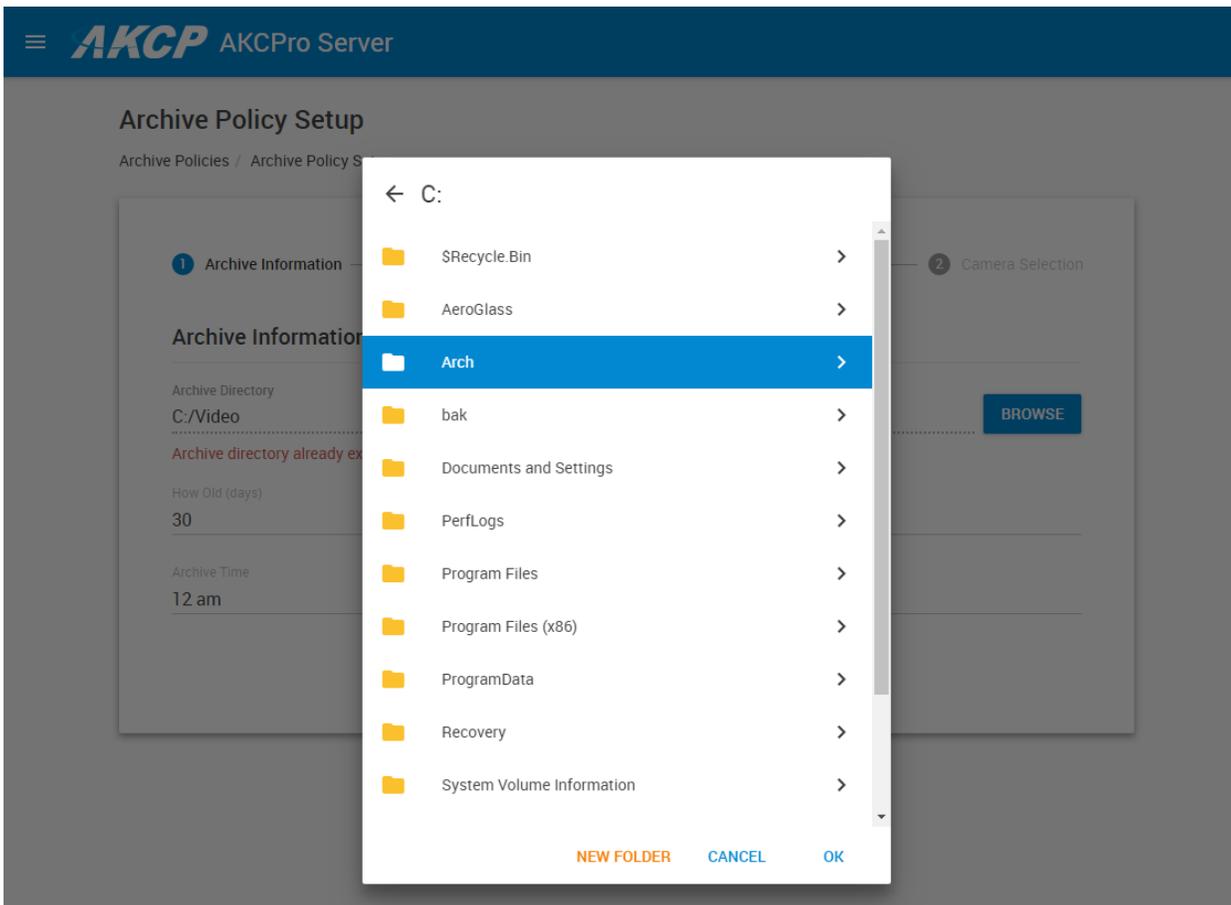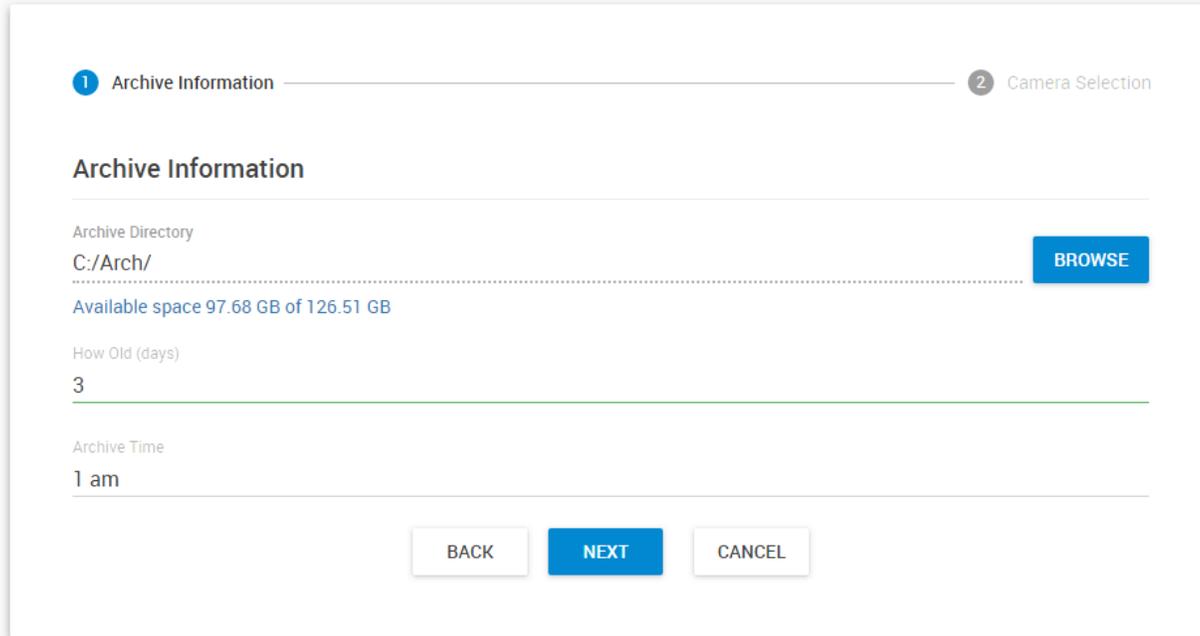
You can select an existing directory from local drives, or make a new one to store your videos. In later APS versions it is possible to create an Archive directory on a USB drive.

Note: The software will create another sub-folder with the camera's name under the specified directory.

2: Choose all other parameters for the archiving:

How frequently to make the archiving: specify in number of days. Any recorded video that are older than the specified X days will be moved to the archiving directory.

Archiving time: when to run the archiving operation. It is recommended to run it during the night because it is a time consuming and resource intensive operation.

Click **Next** to continue.

3: Choose the cameras for this policy and click **Finish**.

Review the policy and modify/delete if necessary. As with the Recording Policies, you can also disable a policy without deleting it.

7.7. Reports
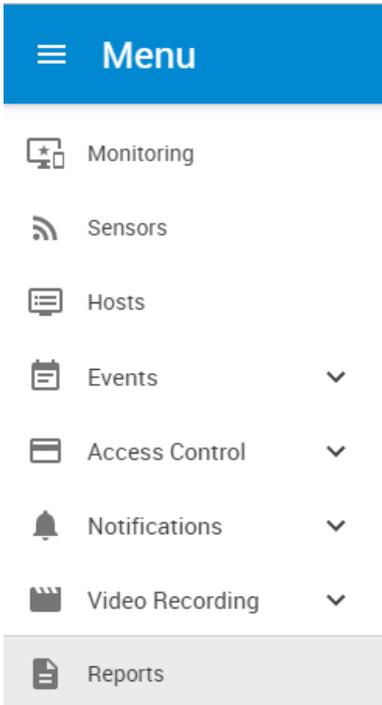
Using the Reports feature you can schedule automated reports for sensors, hosts and racks.
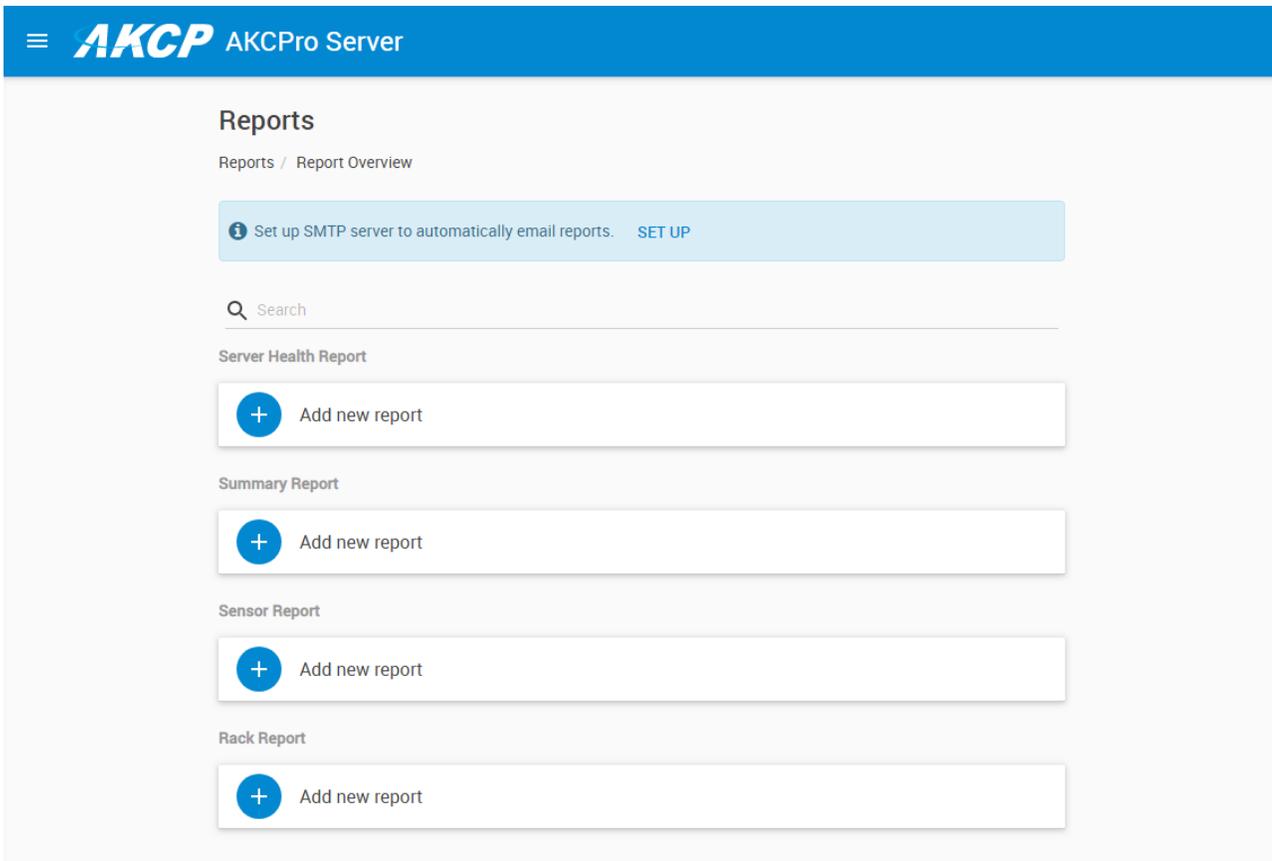With analog type sensors, a graph will be also generated and included in the report.

The reports can be set to automatically send in email to selected recipients, or could be manually downloaded in PDF and CSV formats.

Below we'll show how to configure each report type.

First you'll need to set up the SMTP server settings to be able to send the automated reports in email. Fill out the required parameters; for detailed explanation of the settings, see the Email Action section in this manual. Since there's no Test button here, you should test the SMTP parameters with the Email action. Then you can enter the same parameters for the Reports and it should work. **Important:** There's no notification popup message in the Reports SMTP menu saying "settings saved", it just saves the settings silently.

Note 1: if you plan to only manually run the reports and download them as PDF or CSV format, the email configuration is not necessary.

Note 2: the notification banner with the SETUP button is always displayed, so you could go back to edit the SMTP settings again if necessary:

Note 3: the WebUI saves your password properly. But when you go back to edit it, then it won't show the ****** field but you can retype the password if it needs to be modified.

Summary report

Summary Report

Reports / Summary Report

Enter report name

Report Name

Automated email

How often do you want to email your report?

Hourly   ▾

Email Recipients

[PREVIEW]   [SAVE]   [CANCEL]

[ADD LOGO]   Summary Report

Date: 13/06/2019 11:01:09
User: Admin Admin

[FILTER]

Location	Host	Sensor	
Enter location	Select a host ▾ This field is required.	Select a sensor ▾ This field is required.	➕ 🗑 ↑ ↓

With this report type, you can send a sensor state per host summary report.
Depending on your needs, you can include multiple hosts and sensors, or just a selected few.

First enter a **report name** to identify this report.

Never
Hourly
Daily
Weekly
Monthly

Then select the **frequency** of the automated report sending from the drop-down list.
You'll also need to define the time or day when it will be sent.

Enter the **email recipients** of the report. You can separate them with commas, for example:
joe@company.com,bill@company.com,jane@company.com

Optionally you can add your own **company logo** to the report's header. A popup window will be shown to select the image for uploading.

The date, time and the user account that was used to set up the report will be always included in the report's header.

Next you'll need to **choose the hosts and sensors** that will be included in this report:

Location	Host	Sensor	
Enter location	Select a host ▾ This field is required.	Select a sensor ▾ This field is required.	➕ 🗑 ⬆ ⬇

Use the drop-down menus, for sensors on a host you can also select "All Sensors" to include all of them in the report.
You can optionally enter a location ex. "Server Room" or "Exit Door".
To add multiple hosts or sensors per line, use the blue + button. You can also rearrange the list of hosts and sensors using the arrow buttons.

You can use the **Filter** button to show only selected sensor statuses for easier selection:

SENSOR	DOOR	RECORD
☑ Acknowledged	☑ High Critical	
☑ High Out	☑ High Warning	
☑ Low Critical	☑ Low Out	
☑ Low Warning	☑ No Status	
☑ No Volt Present	☑ Normal	
☑ Offline	☑ Sensor Error	
☑ Switch Timed to On	☑ Unknown Status	
☑ Unreachable	☑ Volt Present	

SELECT ALL   UNSELECT ALL   CANCEL   OK

See an example report report below with a custom logo and 2 hosts with multiple sensors:

Enter report name
Test

Automated email

How often do you want to email your report?
Daily

Email Recipients

Start Time
12 am

PREVIEW   SAVE   CANCEL

Change Logo
Remove

Summary Report

Date: 13/06/2019 11:04:34
User: Admin Admin

FILTER

Location	Host	Sensor	
Server room	AKCPro Server	Pinger	
Enter location	SP2+ .146 (192.168.22.5)	All Sensors	

Using the **Preview** button you can see how your report will look like:

After configuring your report, save it with the **Save** button. It will be added to the reports list:

With the popup menu you can also **export the report** as PDF or CSV file. This will take a few minutes to prepare based on the number of sensors and data included in the report:

Export as PDF

Export as CSV

Delete

ⓘ Export is in progress. It may take up to 10 minutes depends on number of logs.

Important: the file export might only work when you use the HTTP protocol, or a custom SSL certificate. In Chrome browser with the self-signed SSL certificate the file download is blocked.

To edit the report again, just click on its name. Use the popup menu to delete it.

Sensor report

Sensor Report

Reports / Sensor Report

Enter report name

Report Name

Automated email

How often do you want to email your report?

Hourly

Email Recipients

[PREVIEW] [SAVE] [CANCEL]

[ADD LOGO]   Sensor Report

Date: 13/06/2019 16:17:59
User: Admin Admin

Host

Select a host

This field is required.

Sensor

Select a sensor

This field is required.

With the sensor report type, you can send automated reports about a **single selected sensor**.

As shown earlier in the Summary report type, you'll need to fill out the report name, frequency and email recipients. You can also add a custom logo in the header.

Using this report you'll need to choose a **host** and a **sensor** that you wish to get a report about. As an example we've chosen a temperature sensor on a SP2+ unit.

You'll need to choose the **time period** for the sensor report.

All sensor readings and statuses will be included in the selected timespan, which could be a lot of data. For this reason we recommend setting a shorter timespan first.

After you've selected the sensor from the drop-down list, click on the **Preview** button to see how your report will look like. For analog type sensors, a graph will be also generated and included:

Date: 13/06/2019 16:53:11
User: Gabor Gabor

Sensor: Room 113 Temperature
Location:
Host: [SP2+] Room 113 (192.168.11.4)

Time Period: Wednesday 12/06/2019 04:52 pm
            Thursday 13/06/2019 04:52 pm

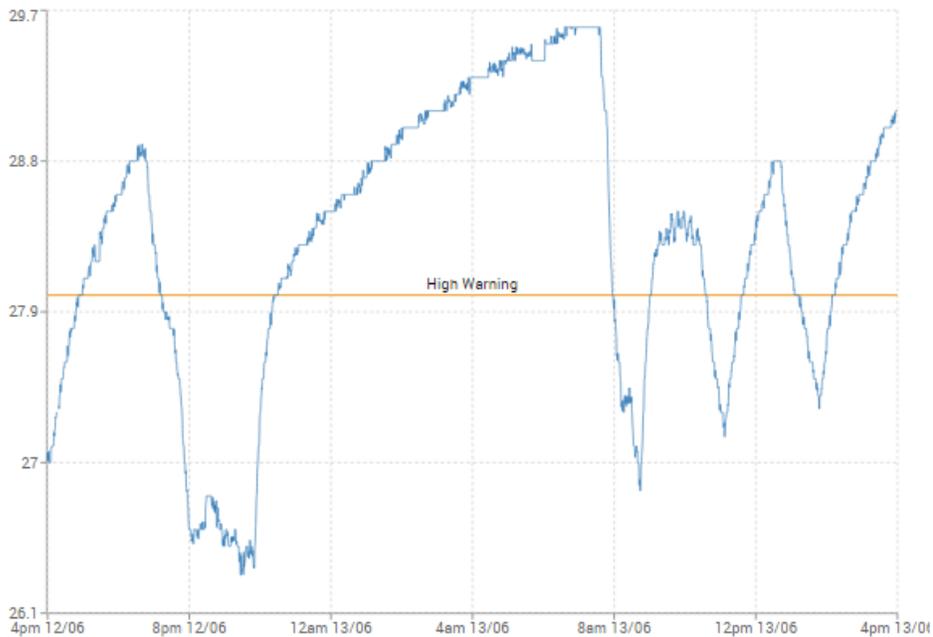High Critical Threshold: 30 °C
No. of times high critical threshold exceeded: 0

High Warning Threshold: 28 °C
No. of times high warning threshold exceeded: 5

Low Warning Threshold: 24 °C
No. of times low warning threshold exceeded: 0

Low Critical Threshold: 22 °C
No. of times low critical threshold exceeded: 0

Switch style sensors will produce a different report format, as shown in the example below:

After you've saved your report, you'll have the same options as the Summary type to edit/delete and download as PDF or CSV file.

Rack report

With this report type you can get status and sensor report for the door, user and card usage per RackMap you've added to the server.

As shown in the Summary report type, you'll need to fill out the report name, frequency and email recipients. You can also add a custom logo in the header.

First **select the RackMap(s)** that you wish to get the report about, and the **time period** (same time period settings as the Sensor report type). Note that you can select multiple racks at once:

Click on the **Preview** button to see your report sample.

If you haven't added Handle Lock or other sensors to your RackMaps, this report will just generate an empty report as shown above.

After you've saved your report, you'll have the same options as the Summary type to edit/delete and download as PDF or CSV file.

Server Health Report

With this report type you can get a periodic "heartbeat" server status report. The live preview will show the data that will be sent; it can't be customized further.

As shown in the Summary report type, you'll need to fill out the report name, frequency and email recipients. You can also add a custom logo in the header.

After you've saved your report, you'll have the same options as the Summary type to edit/delete and download as PDF or CSV file.

7.8. Documents
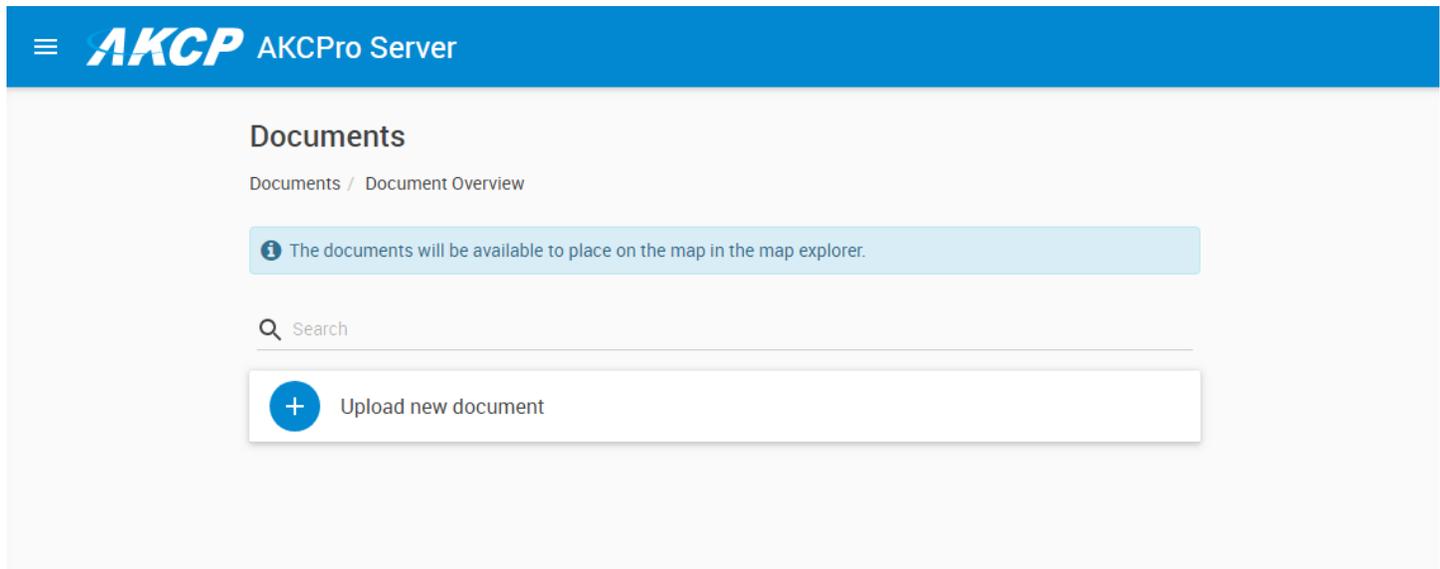
The Documents feature lets you upload any kind of document files to the APS computer, and display them on a map (not on RackMaps).

First click on the **Upload new document** button.

Select your file from your local computer by clicking **Browse**. It could be any text document, image, spreadsheet etc.

The **Document Label** will be shown on the map and is customizable. By default it's set to the uploaded file's name.

As an example we've uploaded the "List Of Units.docx" file.
You can upload further files, and there's a search window to find your file in the list.
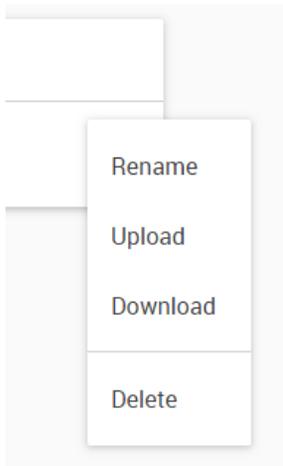
After uploading you can manage the files with these options:

- Rename – you can change the Document Label
- Upload – you can re-upload or replace the file
- Download – download the file from APS
  Note: in Chrome browser this will only work with HTTPS protocol if you have replaced the SSL certificate – otherwise you need to enable HTTP protocol
- Delete – remove the file from APS

The Documents feature is closely related to the Maps feature. You can place the uploaded files on maps from the Maps tab:
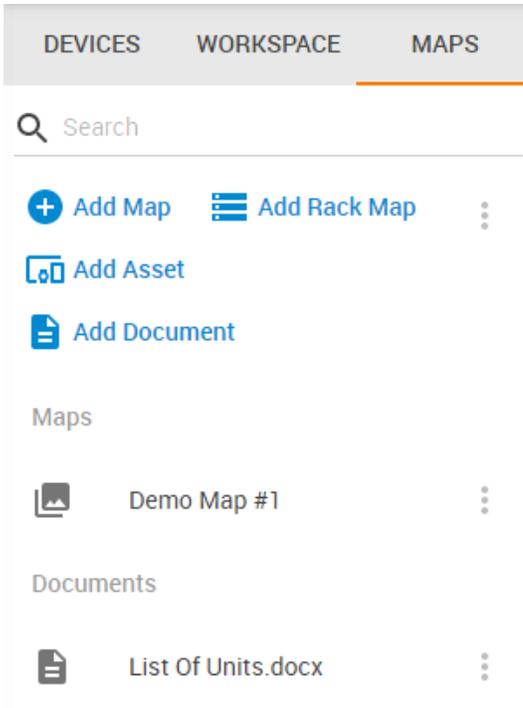
To add a Document to an existing map, just drag and drop the file on the map. It will behave like any other sensor, unit etc. that you could place on a map.

To remove a Document from a map, just right-click and select "Remove Marker" option (you may need to unlock the map first). This doesn't remove the file from APS, just removes it from the map and you can re-add it to another map.

See the "Managing Maps" section in this manual for more details.

As an example, we've added the "List Of Units.docx" file to the Demo Map #2 as seen on the screenshot below:
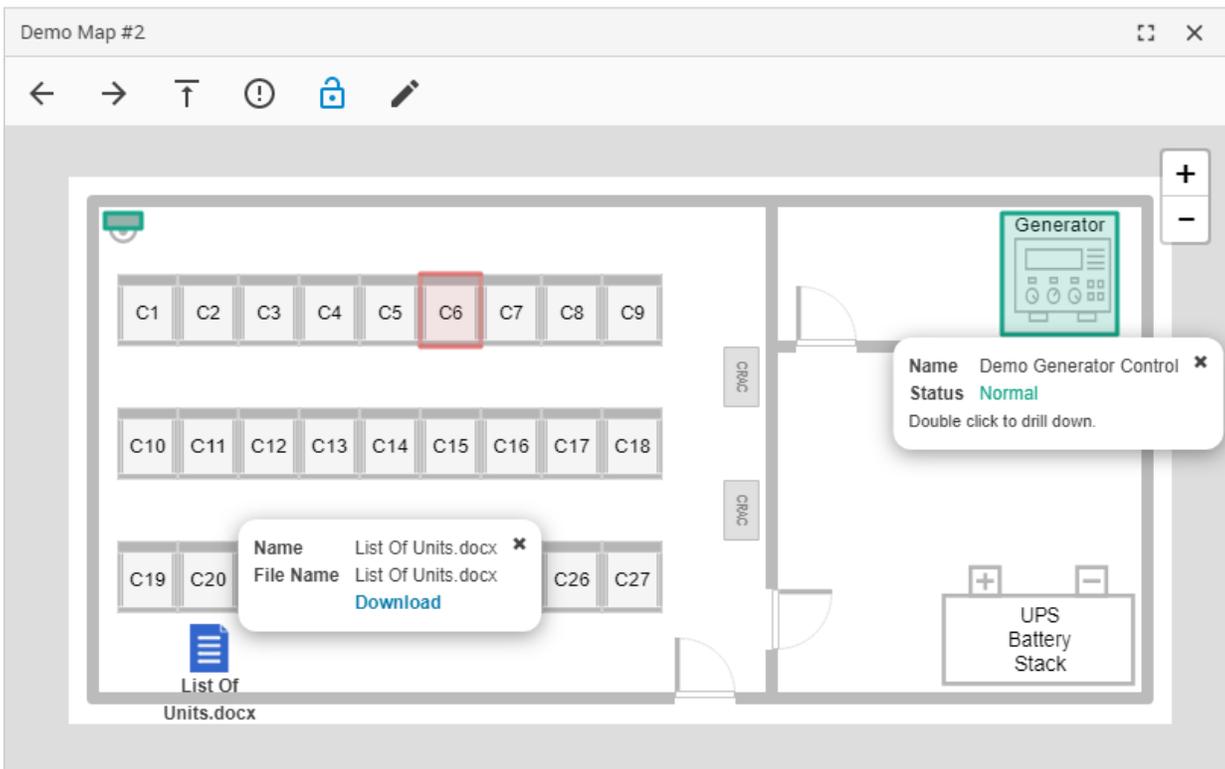
7.9. Settings

Account Settings

With the Account Settings menu you can specify the security users and groups which can access the HTML UI and log in to APS.
The added Access Control users are also shown here, but by default they are disabled. You can manually set a username and password for these users to enable their login access (see below).

Account users

As you can see on the screenshot, we've created Bob Hope's Access Control user earlier, so his account is shown as disabled. Click on the pencil icon next to it to edit the account.

To add a new account user just click on the **Add** button.

You'll need to enable the account, assign a unique user name and password to it, and make it part of a security group (more on the groups later):

You'll see that this new account can log in now, with the group permissions you assigned to it.

Account Settings

Settings / Account Settings

User Name	First Name	Last Name	Group	
admin	Admin	Admin	Administrator	
bob	Bob	Hope	ViewAll	

We'll detail the account groups below.
On the example screenshot below, you can see some users with enabled LDAP authentication:

Account Settings

Settings / Account Settings

User Name	First Name	Last Name	Group	Use LDAP	
	New	Test		✓	
	Prefix	Test		✓	
admin	Admin	Admin	Administrator		
aps2	user_aps2	user_aps2	Administrator	✓	
gabor	Gabor	Test	Administrator		
joe	joe	joe	test, ConfigAll		
mmm	user_apsuser	user_apsuser	test		
mot	mot	mot	Administrator, test		
test	test	test	ConfigAll		
testlang	test	language	ViewAll		
viewer	view	view	ViewAll	✓	

Account groups

Click on the **Groups tab** to view and edit the security groups on the unit.

By default there are 3 groups available: Administrator, ConfigAll and ViewAll.

ViewAll only has read-only access to everything except the users.
ConfigAll could edit and manage most of the settings, except the user account settings.

On the example screenshot below, you can see we've added a "test" group:

Click on the **Add** button to add a new security group, where you can fine-tune the access levels.

You can define read and write access to each item (not all of them are shown on the screenshot). When you give write/configure access to an item, the read permission will be also added to it automatically.

Some items allow host-by-host specific access, so you could show/hide selected hosts for this group:

User settings

On this page you can make changes to your own user account, which doesn't affect any other accounts.

To change the Web UI display language, choose another available language from the drop-down list and click **Save**:

Everyone has rights to change the following settings in their account (even with the ViewAll group):

You could rename your own account's First- and Last Name:

And here you can change your own password.

You can also customize the display colors for each sensor status and other events by category:
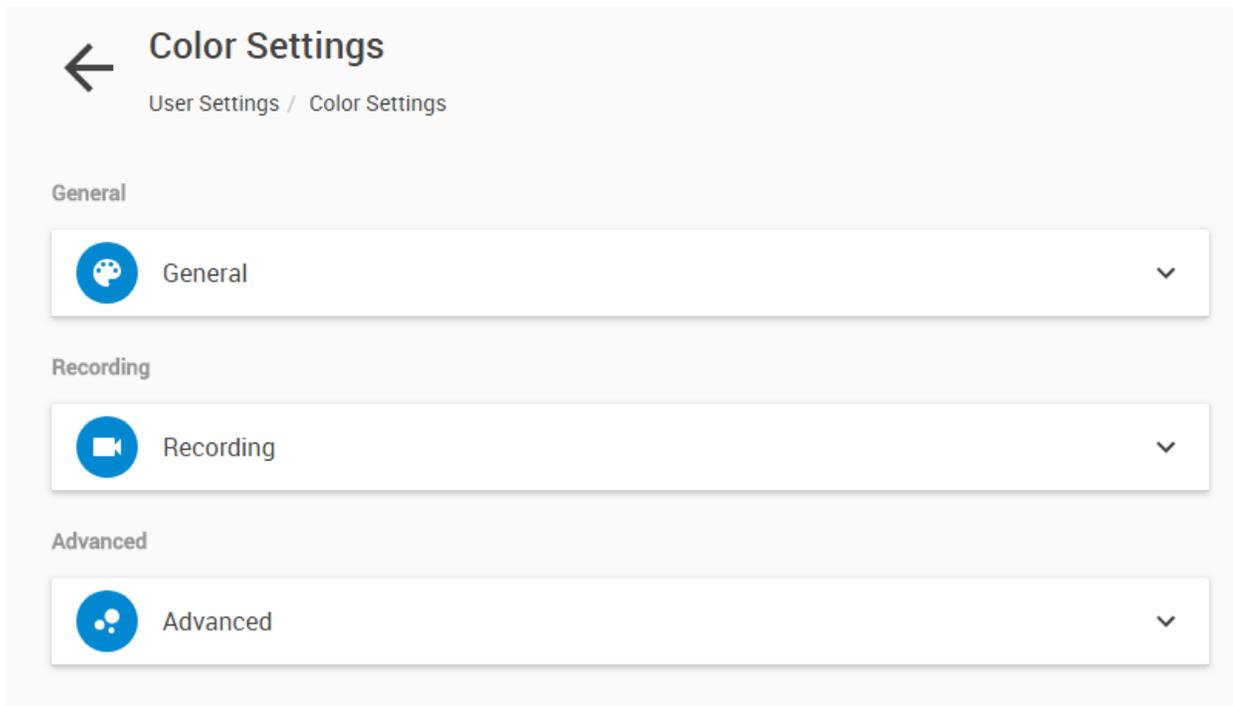
Click on a selected category, which will then expand and show the available color choices.

For example, under the General category you can customize these colors:

(the picture does not show all possible choices)

Server settings

In Server settings you can configure the generic APS settings. Most of these options can be also found in the Windows (wx) Client, but there are some additional settings.

Connections

Under Connections, you can specify the following:

Listen for connections on port: the RPC communication port that needs to match with the client units' configuration. Defaults to TCP 5000.

UPnP port mapping: this will try to dynamically negotiate ports with the connected units. It's recommended to keep it enabled to avoid communication errors.

Add Windows Firewall exception: this option will automatically add the required ports for APS automatically to the Windows Firewall, including the VPN port if used.

VPN

You can configure the built-in VPN server here. Its configuration is identical to that of the Windows APS versions.

This feature is used to connect your SEC5E and SP+ units remotely with the APS VPN server. After the APS VPN server is set up, you'll need to fill out the same options on both ends to be able to use the VPN connection (see below).

Note: This feature requires a separate license on SP+ units. When you use the VPN option on the SP+ units, the maximum number of sensors that can be used by the unit will be reduced to 36 (on older SP+ units with F4 CPU). This limitation only applies to the SP+ unit and not to APS.

Set up VPN connection to APS

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

E-learning video: VPN connection between SP+ and APS
https://youtu.be/s9MPxvO-p24

1. On APS, Go to **Settings>Server Settings>Virtual Private Network** as shown in the picture on the previous page.

Enable the VPN Server by clicking on the checkbox, and then change the **Network Password** in Authentication Setting.

None

Blowfish

AES

Triple DES
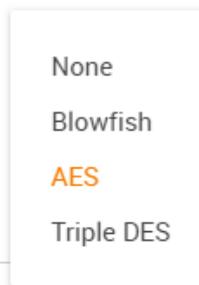
Remember the **Network Encrytion Mode** that you have chosen; you'll need to provide the same setting on the client units.

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

Click **Save** and the VPN server status should show that it is running.

Important: It might be necessary to disable and re-enable the APS VPN server if your clients cannot connect. Your settings will be still saved if you disable the VPN server, so you don't need to re-enter them when you re-enable it.

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 192.168.17.x (or any other that's different from 192.168.1.x) for the VPN link.

2. On the SP+ Web UI, enable the VPN (your license needs to be enabled first)

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

- Specify the APS 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.
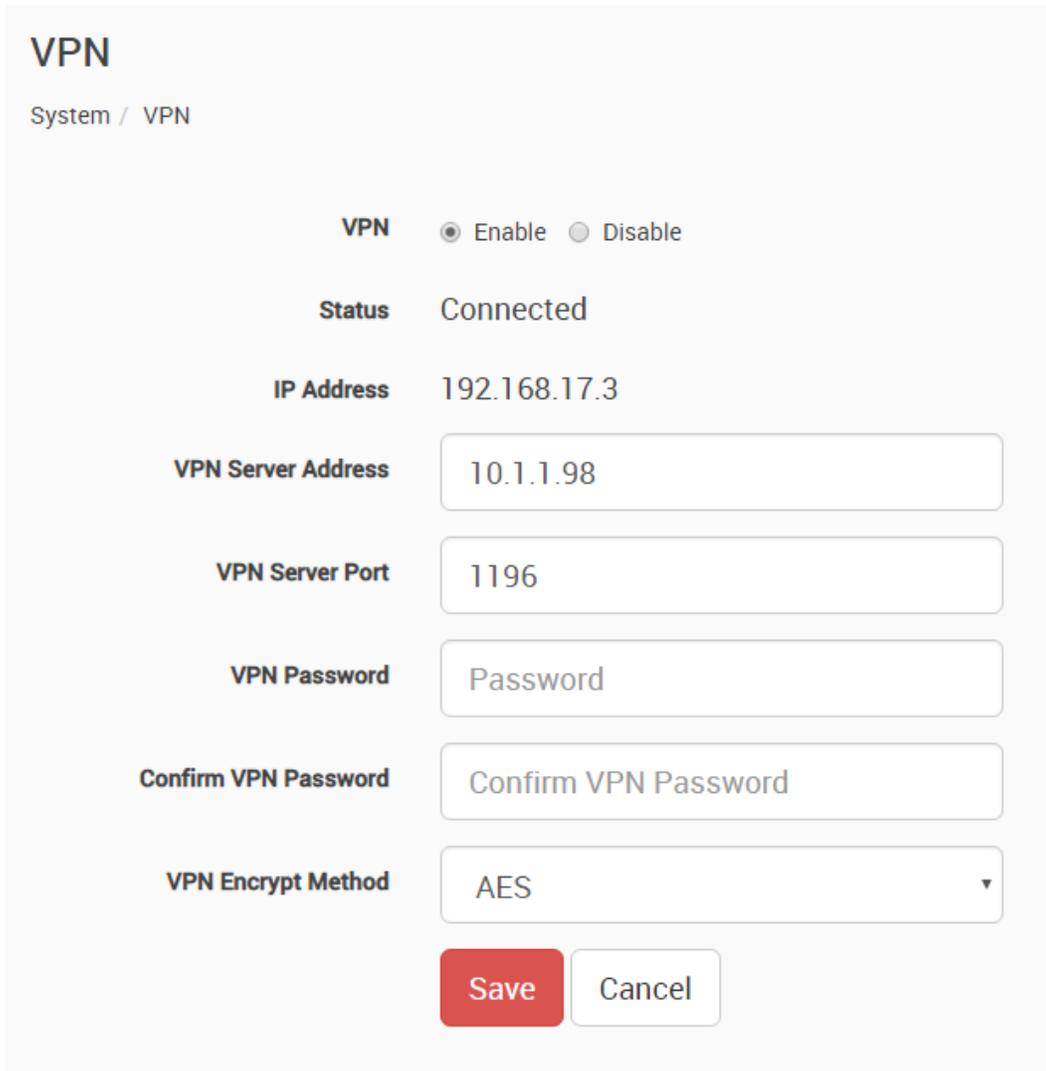
VPN

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 ▾

Save   Cancel

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 **Monitoring page** automatically, with an IP address automatically assigned from the range you specified.

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 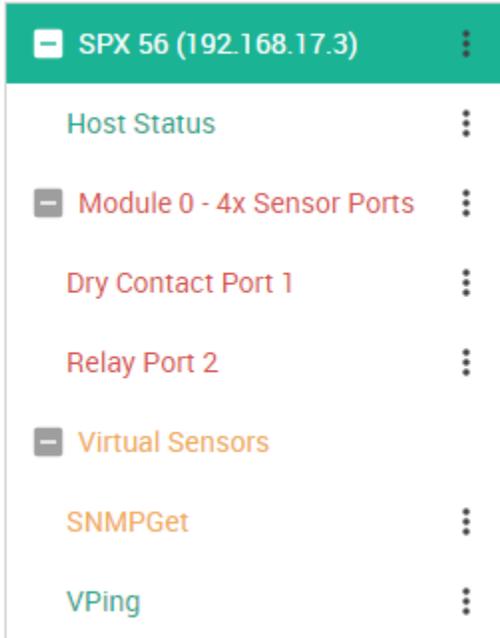IP address for SP+ but the unit's MAC address is the same, and they'll be in conflict. This is not an issue if the unit has never been added to your APS before.

B) If the SP+ unit was previously monitored by any APS, it is recommended that 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.

D) You cannot configure SP+ virtual sensors and the Buzzer on the VPN client units from APS. APS will instead try to redirect you to the unit's Web UI but in some cases this will not work correctly.

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 client unit has to be configured first with the correct APN settings

Event logs configuration

You can configure the maximum number of log entries with this setting.
The size is unit of thousands, so the default 100 means 100,000 log entries.

Also you can specify to either stop logging further events (not recommended) or remove the oldest entries when the maximum size is reached.

With the **Clear** button you can erase all existing logs.

On newer APS versions you will also have the option **Enable logging Server Service events to the Windows Event Log**. This will send specific service events and their reason to the Windows Application Log, for example if NotificationServer service has stopped responding, or the main APS service has exceeded the configured RAM/CPU limits and have been auto-restarted. You can then collect events directly from the Windows log for analysis and remote management.

The logs contain important information with date and time, so you should always refer to the logs when troubleshooting. See the "Events" and "Access Control" sections in this manual for more information.

Notification
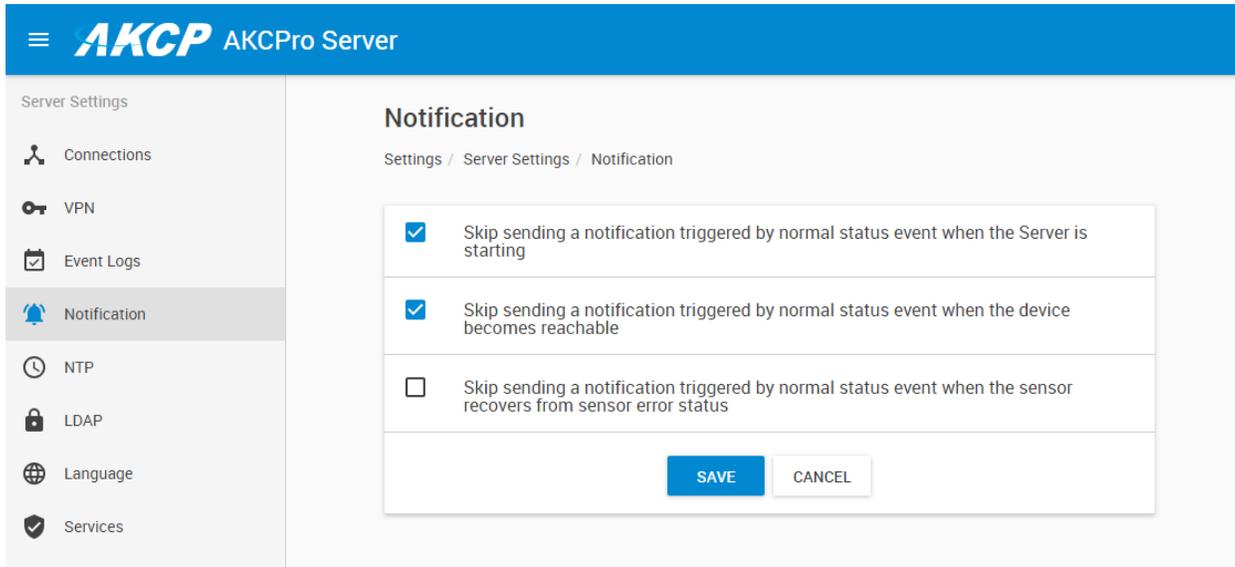
With these settings you can control to skip sending notifications in these conditions:

- "Normal status" notifications during APS startup (if a sensor is in normal state), default enabled
- When a device becomes "reachable" again after an "unreachable" state, default enabled
- Turn off alerts if a sensor recovers from "sensor error" status

NTP

APS has a built-in network time server (NTP).

This is necessary to synchronize the date and time on all connected client units, to have the log entries and the Access Control features to work properly.

You could de-select to force the time sync with client units, but this is not recommended.

You can specify custom third-party NTP time servers for a reliable time source. Use the **Ping** button to check if they are reachable.

The list of specified NTP servers will be sent to the connected client units - on most units only the first 2 servers will be used.

Note: if there are no servers specified (default setting), then the built-in APS NTP server will be used and the client units will sync with APS only.

LDAP

LDAP authentication can be turned on, so that any user account from the LDAP directory could be used to log into APS, even if the account is not present in the APS database.

Currently this feature is used for authentication checking only and no security settings are read from LDAP - all LDAP users will have a read-only account.

For existing APS accounts, you can configure it per user account from the Access Control database, then these accounts will use LDAP password checking instead of APS.

This feature has its own manual, please refer to the separate APS LDAP manual.

Note: not all available options are shown on this screenshot

Language

In Language, you can change the display language of the HTML UI, change translations or create new language files.
The default (and fallback if there's an error) is English.

With the **Default Language** option you can pre-define a language for new users, so they don't need to change it themselves (but they still can, of course - see at the User settings in this manual).

To edit the existing languages, or create your own, just click on the arrow next to it: **>**

There is a built-in language editor (similar to the one on SP+) that you can use to translate the interface to your language.
You can also download the language file for future reference (at this time you cannot upload it back to the server yet).

Click on **Edit** next to each section of the language file to edit its contents:

When done, save your changes and change the UI display language from the drop-down list.

Services

In Services you can choose the web interface's ports, enable/disable HTTP and change the SSL certificate. Since changing settings from here won't verify if the selected port is available (unlike during APS setup), you have to make sure the port is free before changing the existing port.

HTTP

Clear-text HTTP is disabled by default for security reasons, but you can re-enable it from here and change its listening port, if necessary.

HTTPS

The HTTPS port is always enabled. You can change its listening port, if necessary.
HTTPS supports TLS v1.1 and v1.2.
The HTTPS cypher suites are not customizable.

To eliminate browser warnings about the self-signed SSL certificate, you'll need to replace it.
Using the "Upload Certificate File" option you can upload an SSL certificate that will be used by the APS Web UI for HTTPS connection (see below).

SSL Certificate

SSL certificates are generated for DNS host names and not IP addresses. Ensure that the host name of the APS computer is registered in your local DNS server or DHCP server, and then generate the SSL certificate for that host name.

Example: akcpro.mycompany.org

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, LetsEncrypt or use your company's own CA if you have one.
Please note that only non-password protected certificate files are supported.

Choose your file (PEM format) with the **Browse** button and press **Upload**:

Upload Certificate File

userkey.pem   BROWSE   UPLOAD

Then you'll be asked to restart the APS service in order to proceed with the new certificate:
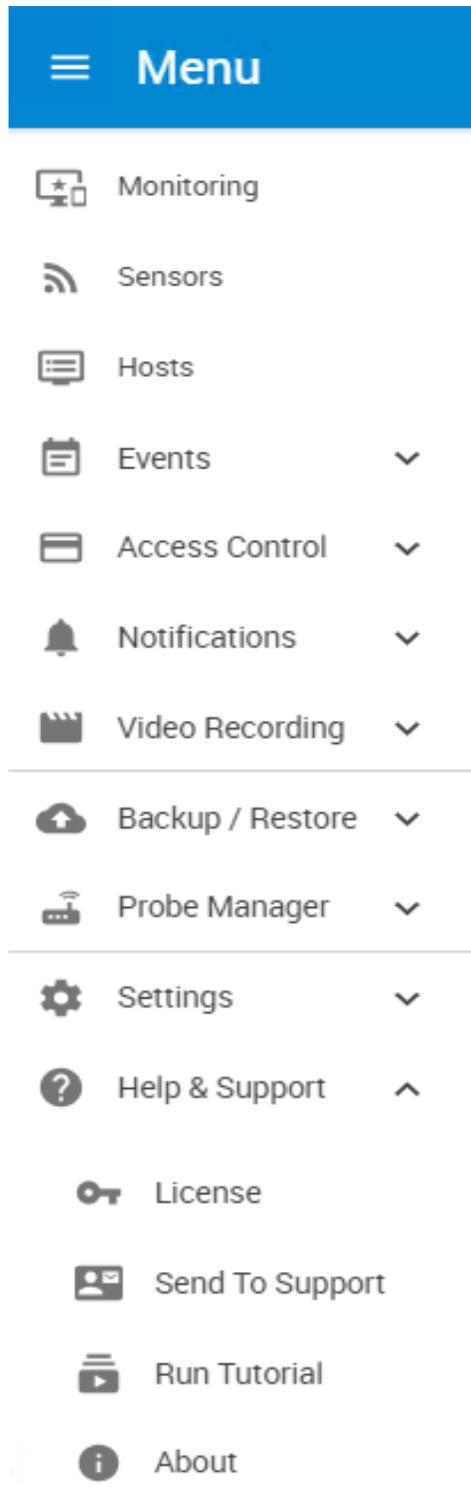
Server Restarting

For the changes to take effect, the Server must be restarted. Do you want to continue? The system will automatically redirect to login page.

NO   YES

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

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):

If you don't upload a certificate, the 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.
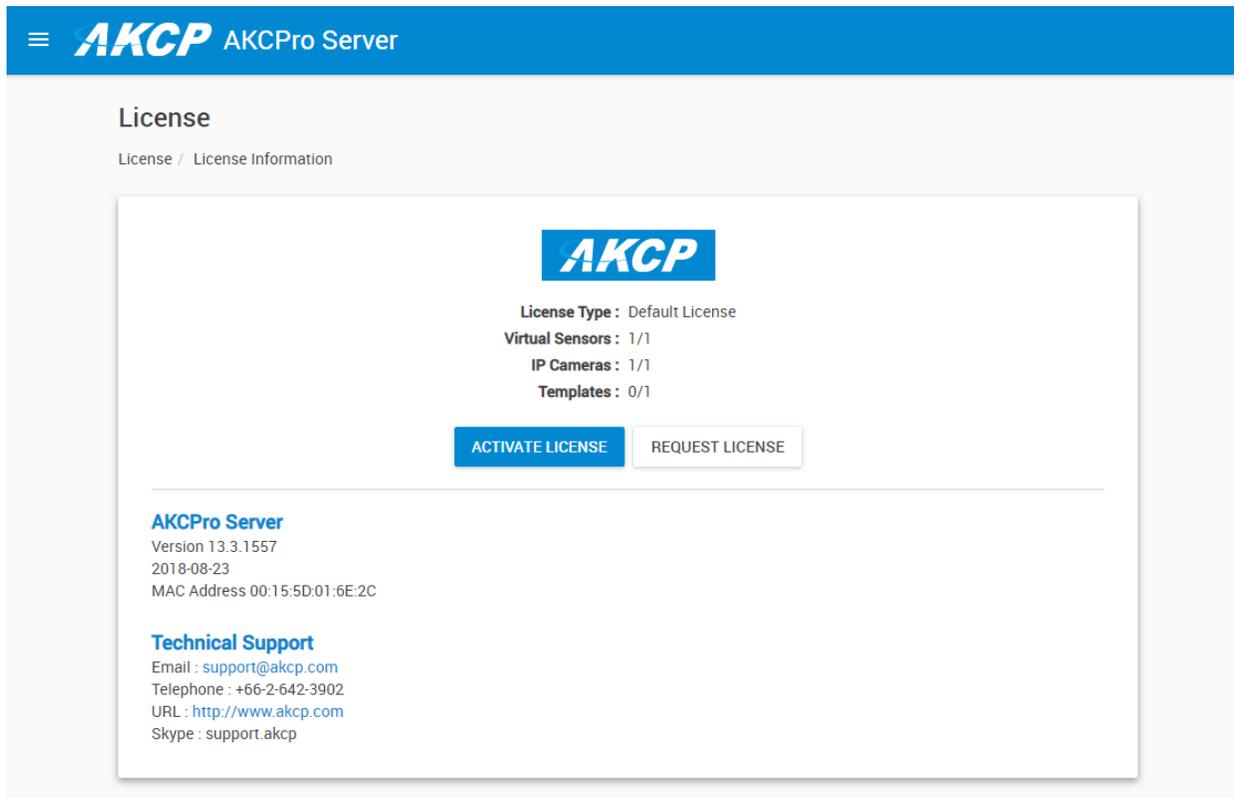
7.10. Help & Support

From this menu you can manage your licenses, send the unit's configuration to Support, re-run the tutorial and view the unit's information at the About screen.

License

APS v13 has a Default License, which allows basic usage (1 licensed Virtual Sensor, IP camera and Template).

You are required to purchase a number of licenses for each component that you need.
Click on the Request License button, which will compose an email automatically with your default Email application.

After our Support team has responded that you can now activate your unit's license, click on the **Activate License** button to begin the activation wizard.

Important note:
If you use virtual machines, ensure that the VM has a fixed MAC address assigned. With a dynamic MAC the APS license cannot be activated. All licenses are tied to the unit's MAC address - the used MAC ID is displayed here.

License

License / License Activation

1 Activation Process — 2 Activation Complete

Activation Process

- ⦿ Activate Purchased License via Internet
- ○ Enter License Key

BACK NEXT CANCEL

The easiest way of activation is if you have internet access. APS should automatically activate itself if it finds an online license at startup, but you can also do this manually.

License

License / License Activation

✓ Activation Process — 2 Activation Complete

Activating...

BACK FINISH CANCEL

APS will need to restart the services when the license has applied successfully, then you'll be taken back to the login page.

The server is restarting. The browser will automatically redirect to login page when the server is ready.

REFRESH

If there was some problem with online activation, we'll show you the manual activation steps below.

License

License / License Activation

Manual activation supports 2 methods: select a license file, or enter the license key.

License

License / License Activation

Click on the blue box or drag and drop the license file to select it.
The box will turn to green if it detects a correct license file.

License

License / License Activation

Activation Process ——— 2 Enter License Key ——— 3 Activation Complete

Enter License Key

To activate your application, simply paste the license key or select the license file that has been sent to you into the box below and press 'Next'.
If you do not have a key, please contact sales@akcp.com

○ Select License File

⦿ Enter License Key

Enter License Key

BACK   NEXT   CANCEL

You can also enter the key manually (copy-paste) as it was supported by earlier APS versions.

APS will need to restart the services when the license has applied successfully, then you'll be taken back to the login page.

If there were any errors during activation, please contact Support.

License

License / License Information

AKCP

License Type : Active License
Expiration Date : 31 July 2019
Virtual Sensors : 0/300
IP Cameras : 0/5
Templates : 0/2
5 Input Dry Contacts : 0/10

ACTIVATE LICENSE   REQUEST LICENSE

AKCPro Server
Version 13.2.463
2018-08-07
MAC Address B8:27:EB:3F:8E:5D

Technical Support
Email : support@akcp.com
Telephone : +66-2-642-3902
URL : http://www.akcp.com
Skype : support.akcp

After logging in again, please check the License page again to see if your license has been applied correctly, with the correct number of sensors as you purchased.

If it still shows the Default License, it could be a problem with your network interface MAC address.

About

On this screen you can see our Support contact information, and some diagnostic information of your APS.

On newer APS versions the Total Number of Sensors and Hosts are also displayed for your reference. This is the total count of online sensors in your system, including all hosts.

When troubleshooting license issues or other software problems, make sure you check this page and note:
- the APS Server Version
- the unit's MAC ID

Send to Support

With this option you can send diagnostic data from the unit to our Support team (internet connection is required) or directly download the support package. If you send online, by default the configuration and logs will be also attached to the message.

You can also select to directly download the support file instead of sending it online:
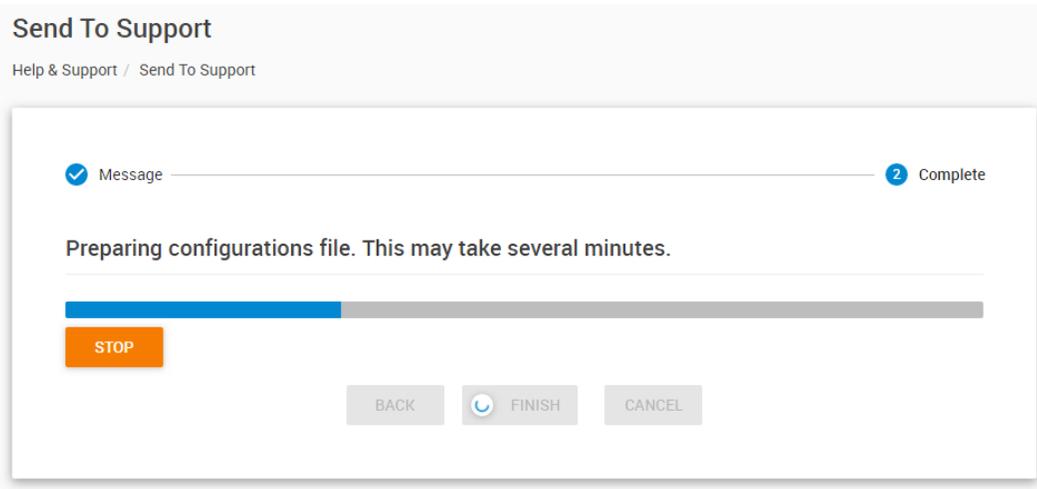
This option is useful when you don't have internet access, or you wish to directly send the file to Support by email.

You don't need to specify email address and the support message if you choose to download the files.

7.11. Probe Manager
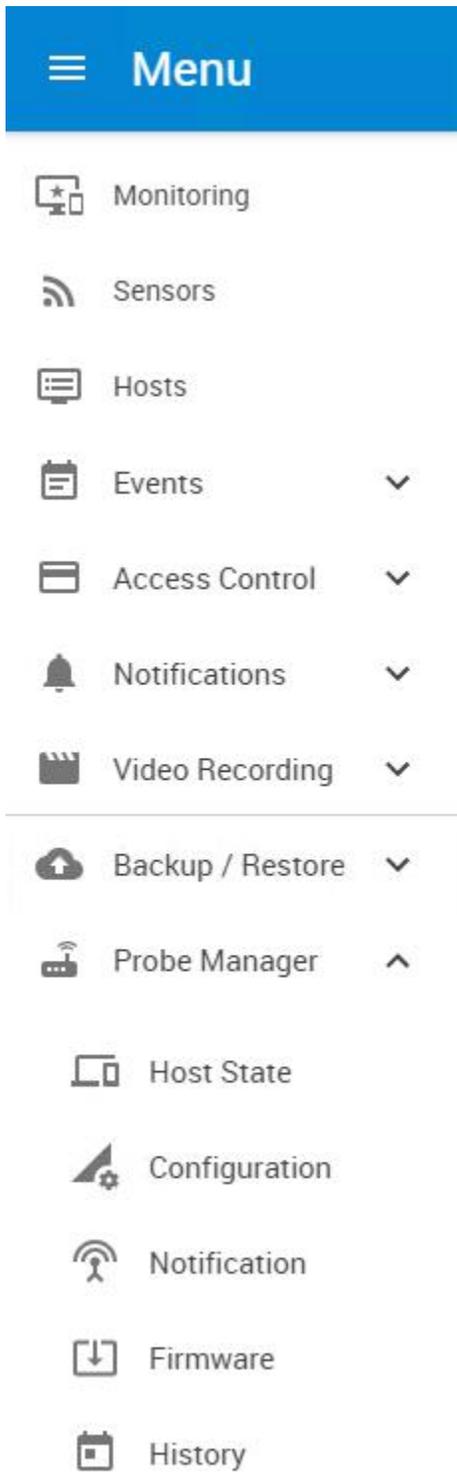
Probe Manager   ^

Host State

Configuration

Notification

Firmware

History

Using the Probe Manager, you can:

- Update your client devices' firmware
- Get- and set device configurations and notifications (backup and restore) on supported units
- View the history of previous Probe Manager tasks
- Overview the connection state of all of your client units (Host State)

We'll show you how to use each of these options.

Host state

This is a simple page to overview the connection state of all of your client units, as well as their firmware versions and IP addresses.

You can only perform Probe Manager actions on units with the Ready state.

Configuration management

You can save and reload the configuration of supported units, or restore their default configuration:

- sensorProbe units (SP)
- securityProbe 5E units (SEC) and Door Control Units (DCU)
- sensorProbe+ units (SP+)

If you attempt to save/reload configuration from an unsupported unit, you'll get a warning prompt and the action will fail.

Get configuration

To get a unit's configuration (or multiple units) first you'll need to add them to the hosts list.
Click on the **Add Hosts** button and select your host(s).

Choose at least one and click OK. Only units with Ready state are shown.

Now your unit is added and you can click the **Get Now** button.

Configuration

Probe Manager / Configuration

Select Operation

○ Send Configuration to Host

● Get Configuration from Host

Selected Hosts

ADD HOSTS

↑ Host	↑ Status	Progress		
SPX 56 (192.168.17.3)	Ready	Completed	**HTTP**	🗑

GET NOW   CANCEL

The configuration is collected from the unit (it's shown at the Progress state, until Completed) then it will be saved as a downloadable .CNF file on your PC with the unit's IP address and the current date. You may cancel the operation while it's still in progress.

Send configuration

This option works similarly as the Get Configuration:
To set a unit's configuration (or multiple units) first you'll need to add them to the hosts list.
Click on the **Add Hosts** button and select your host(s).

Choose at least one and click OK. Only units with Ready state are shown.

Now your unit is added and you can select the saved configuration file (.CNF) from your PC using the **Browse** button.

If the configuration file is incompatible with the device (eg. trying to restore a SEC configuration to an SPX+) then the operation will fail with error.

You can use this Probe Manager option to restore a client unit's default configuration; when using this option you don't need to select an existing .CNF file.

Click **Send Now** to send the configuration data to the unit.
It will be uploaded and then applied on the client unit, which will then reboot to make the changes.

You may cancel the operation while it's still in progress, but only during the first upload stage.

Get / Send Notification

These functions work the same way for saving or restoring notifications, so we'll only show the Send process in the screenshots.

Currently this function only supports the SEC5 and DCU units.

First, select your unit with the **Add Hosts** button.

Then choose the saved configuration file from your PC (.DNF) that you saved, and click **Send Now**.

If you attempt to select a unit which doesn't support this feature, you'll get an error popup:
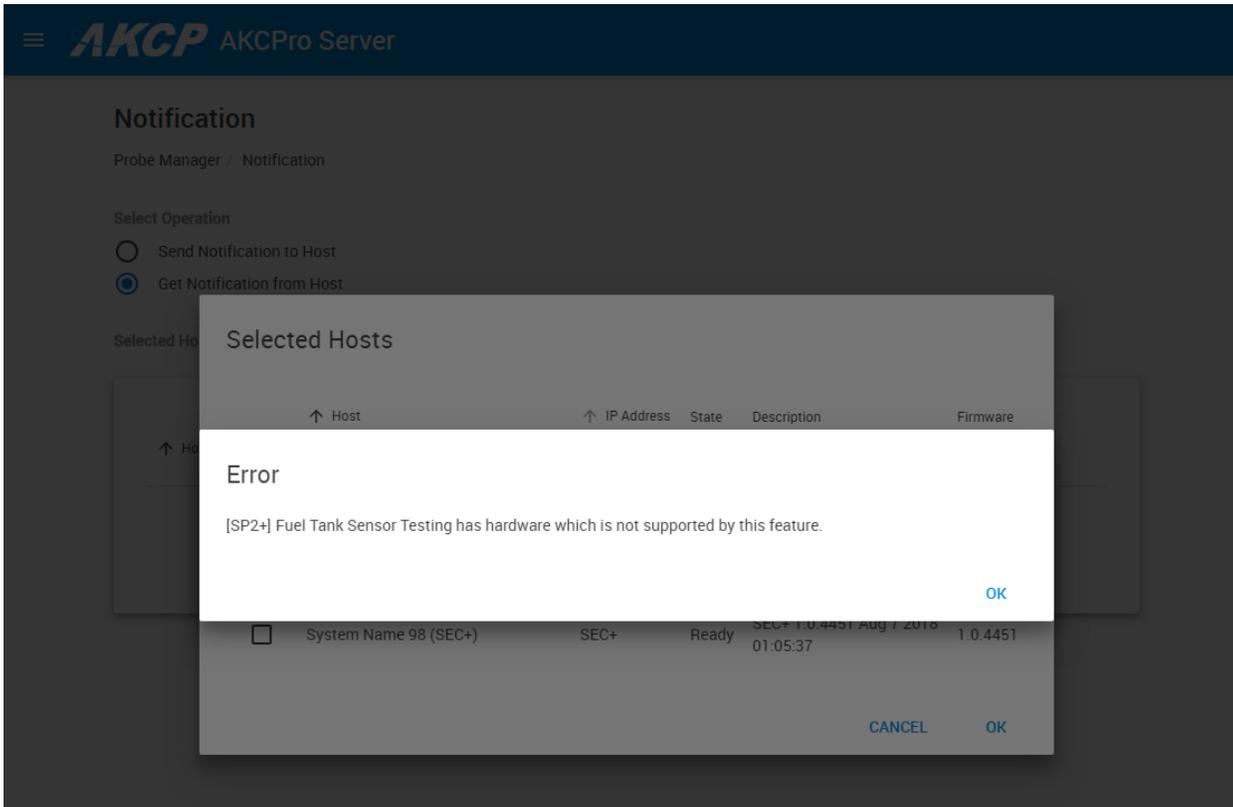
Firmware update
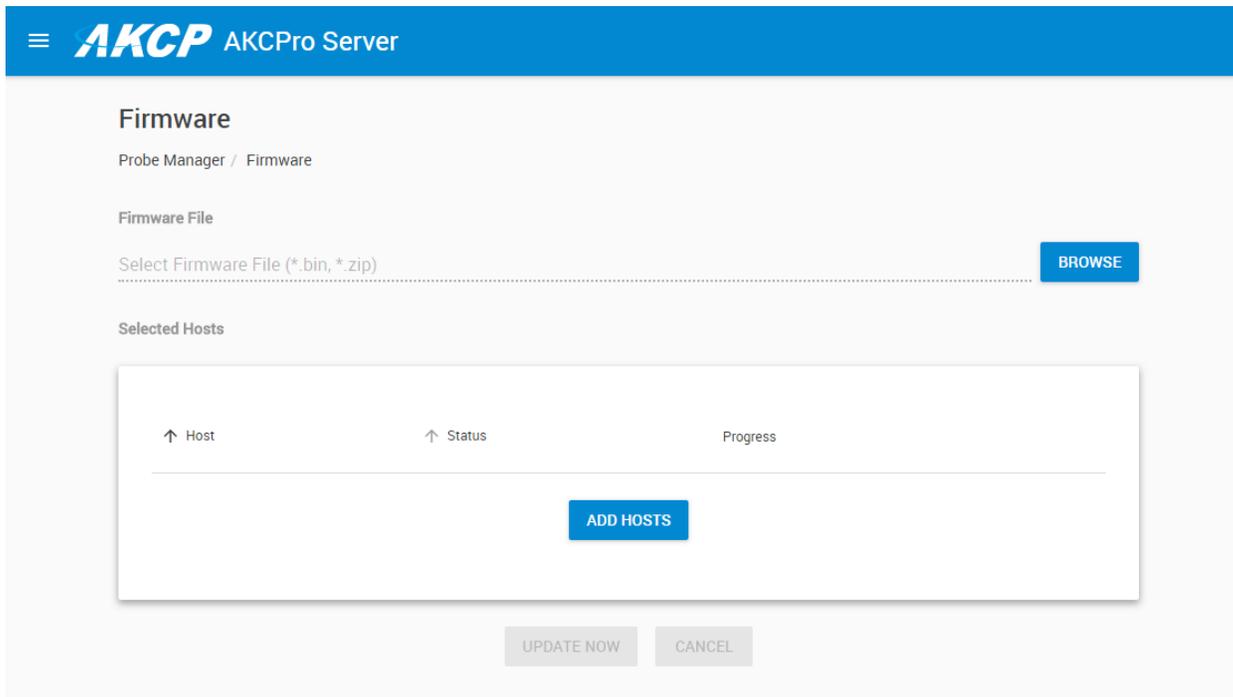
Firmware

Probe Manager / Firmware

Firmware File

Select Firmware File (*.bin, *.zip)   BROWSE

Selected Hosts

↑ Host	↑ Status	Progress

ADD HOSTS

UPDATE NOW   CANCEL

You can update the firmware of any AKCP client unit with this option.

Choose the firmware update file from your PC with the **Browse** button.

Then click **Add Hosts** to select your units for updating. Multiple units can be added at once, as long as they're belonging to the same product family, and could use the same firmware update file.

If they don't match, you'll get an error popup:

Click on the **Update Now** button to begin the upgrade.

You can cancel the upgrade while the firmware file is still being uploaded, but not in a later stage.

In case you attempt to update a unit with an incompatible firmware (eg. using SEC5 firmware trying to update SPX+), you'll get an error popup and the operation will fail, as shown below:

Probe Manager History

On this page you can view the history of previous Probe Manager tasks.
Similar to the Event Log, you can filter the different events for easier viewing.

7.12. Backup & Restore

Backing up your APS system's configuration is essential. The Backup and Restore feature is built-in to the program, and is an integral part of saving your APS environment and its data.
It is capable of saving and restoring all of your APS environment (monitored units, notifications, time attendance settings, other user accounts, etc.) and optionally the recorded video data.
Important: APS backups are "snapshots" of your configuration and will only contain data and graphs up until the time of the backup was made - keep this in mind when restoring an older backup.

Note: you must log in with the Admin account to APS, otherwise you won't be able to see or use the Backup and Restore feature.

Backup

The Backup menu will show the backup state and the configuration.
If you have performed a backup before, the date and time with result of the backup will be shown, as on the picture above.
By default the backup is not configured, so you'll need to click on the **Configuration** button first.

First, choose your backup directory where you want to store the backups with the **Browse** button.
Currently *only local disks are supported* for selecting the backup target.

Make sure there's enough free space on the target. You can also create a new folder using the browsing dialog, if you haven't made one before.

Maximum Size (Gigabytes)

1

* Reducing your backup size may remove your old backup.

Maximum Size Reach

○ Stop Backup

● Remove Old Backup

Do you want to backup the video?

☐ Yes, I want to backup the video.

Next choose the **maximum allowed size for all backup files** in Gigabytes.
If you plan to back up the recorded video files as well, then plan your backup size accordingly.
For making configuration backups only, 1-2 GB is typically enough.

Note: all of the chosen disk space will be pre-allocated immediately, when you select the directory. It is to ensure there will be enough disk space for the backups and also to reduce file fragmentation (thus improve the backup and restore speed).

Choose what happens when the maximum backup size is reached: stop the backup process or remove the oldest backup files first.
It is recommended to select "Remove Old Backup upon Maximum Size Reach" option, as it will ensure you'll still have a recent backup.

You can choose to include the recorded video files in your backup, but this is not recommended due to the backup export to USB drive will take a very long time (more on this later).
Instead, we recommend you to use the Video Archiving policies for automated video backup.

Click **Next** for further options.

You could schedule your backup to run automatically, but it's not necessary if you plan to manually run the backup.
If you decide to set up scheduled backups, choose the frequency, and the time when it will be performed:

Also you can specify a backup password for security reasons. You'll be asked for the password upon restoring.

Click on **Finish** to finish the backup configuration.

You'll be taken back to the main Backup page, where you can start the backup process.
Click on the **Backup Now** button and let it finish. A percentage counter will show the state of the backup process, as shown below:

Backup

Backup / Backup Information

Backup Status

Backing up the system 0%

Last successful backup
Monday, 9 April 2018 12:51 PM

Next backup
N/A

Backup location
C:/bak/

Available space
1.00 Gigabytes (Overwrite old backup file)

Backup Options

☐　Remind me to backup every week

BACKUP NOW　　EXPORT BACKUP　　　　　　　　CONFIGURATION

When the backup has finished (whether it was success or failure) you can review the backup log on your PC with the **Download Log** option on the upper right corner:

Download Log

Copying the backup export files to other media

After the backup export file is generated, you can just copy it to another backup media from Windows, or by using any conventional backup software.
If you need to find the latest backup, the files always have a date and time stamp in their file names, so you can find the most recent one easily.

There is a **Reserved** directory under the chosen backup directory; it doesn't need to be backed up, as it contains only "placeholder" files, to reserve the disk space for the growing number of backup archives.

In this folder, the **backupLog.txt** file stores the information about the previous backups, with their respective folder names.
See below for information about the full backup log's location.

The log files are:

backupLog.txt
restoreLog.txt

Their location in the file system is:

C:\ProgramData\AKCP
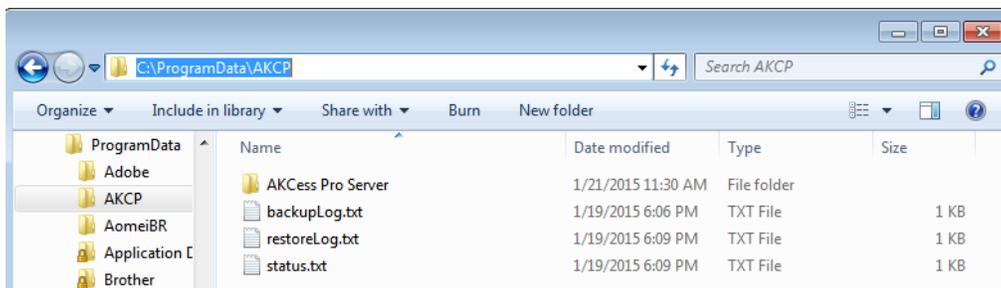
ProgramData is a hidden directory, so if you haven't enabled the "show hidden files and folders" in Folder Options, just copy-paste the directory name to Explorer and press Enter to go there, as shown on the picture.

Export backup to USB

Click on the **Export Backup** option from the main Backup page to run the export wizard.
Plug in your USB drive before starting this wizard.

On the first screen **you only need to select the backup file you want to export**.
The backup file source path should be automatically selected.
In case you have backups in other directories that you want to export, you can still browse to them with the **Browse** button.

Click **Next** to choose the folder where you want to copy the backup file to on your USB drive (or download it via the web browser).

Here you can either **download the backup file** (important: usually this only works with HTTP protocol enabled) or **choose the export folder** where you want to copy the backup file to on your USB drive with the **Browse** button:
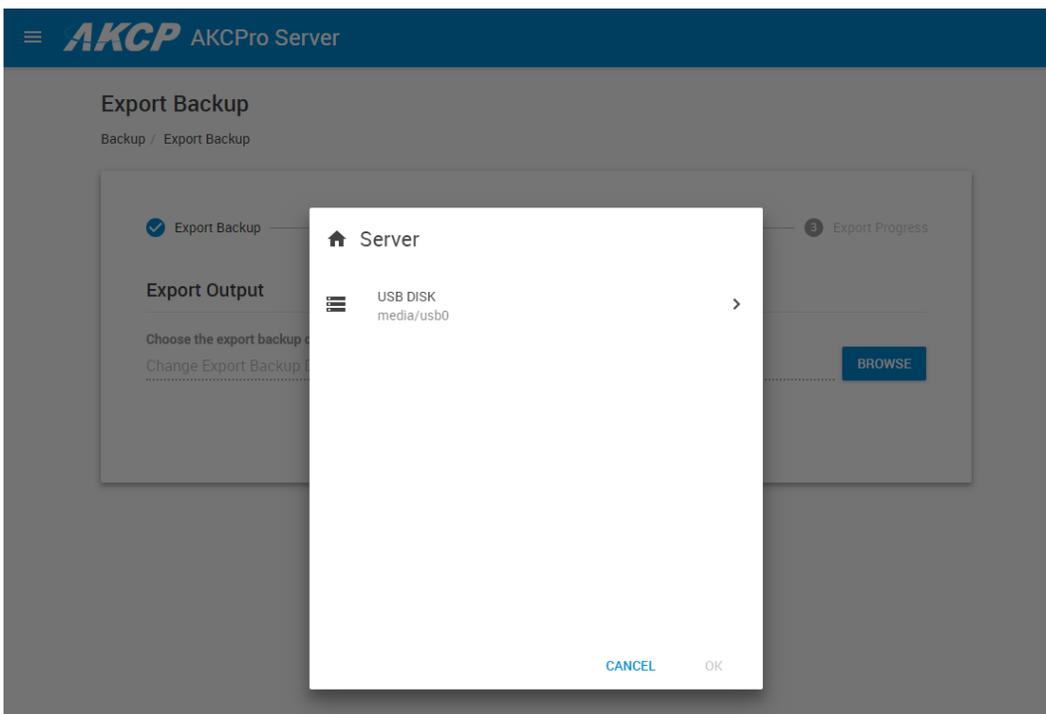
Open the USB drive's folders with the **>** button.
Note: on Windows, other fixed drives will be also shown in the list.
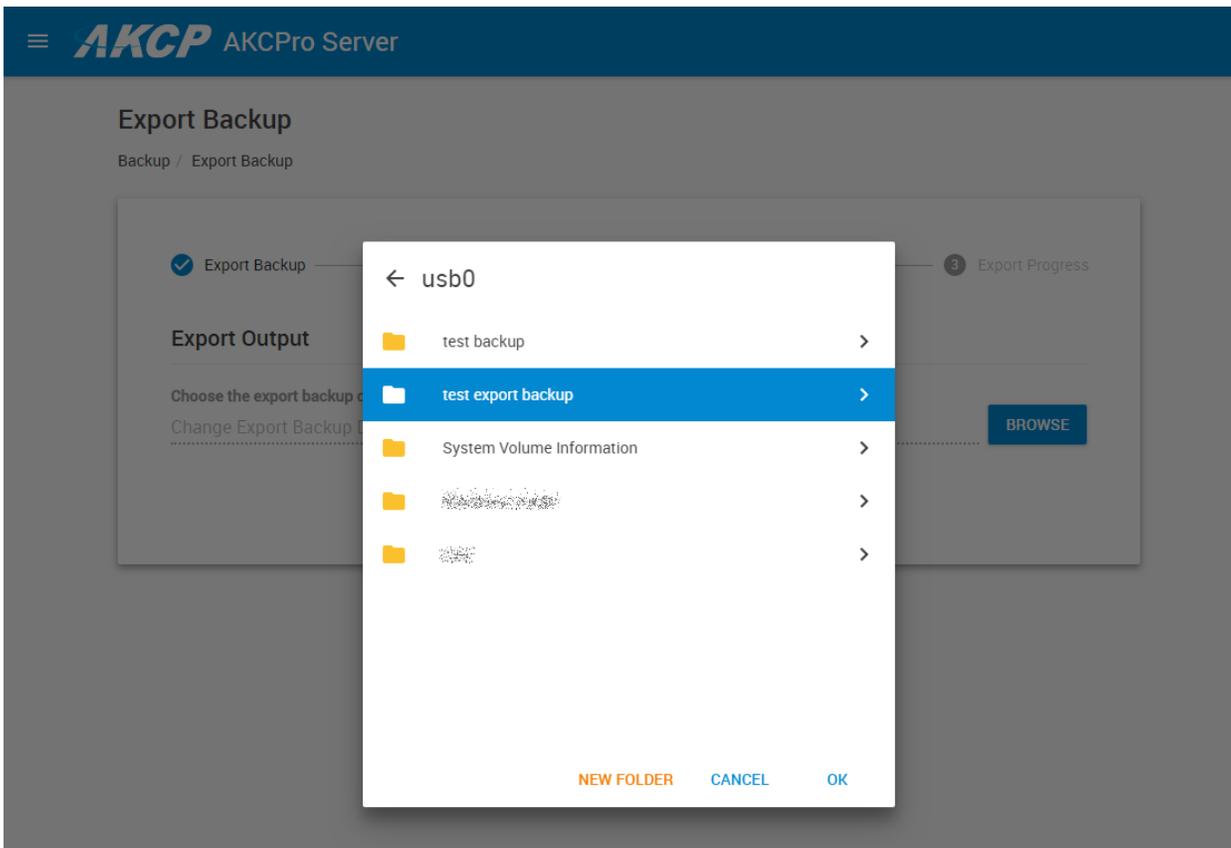
Highlight only the folder where you want to place your backup into; don't go inside the folder itself. You could also create a new folder if necessary. Click **OK** when done.
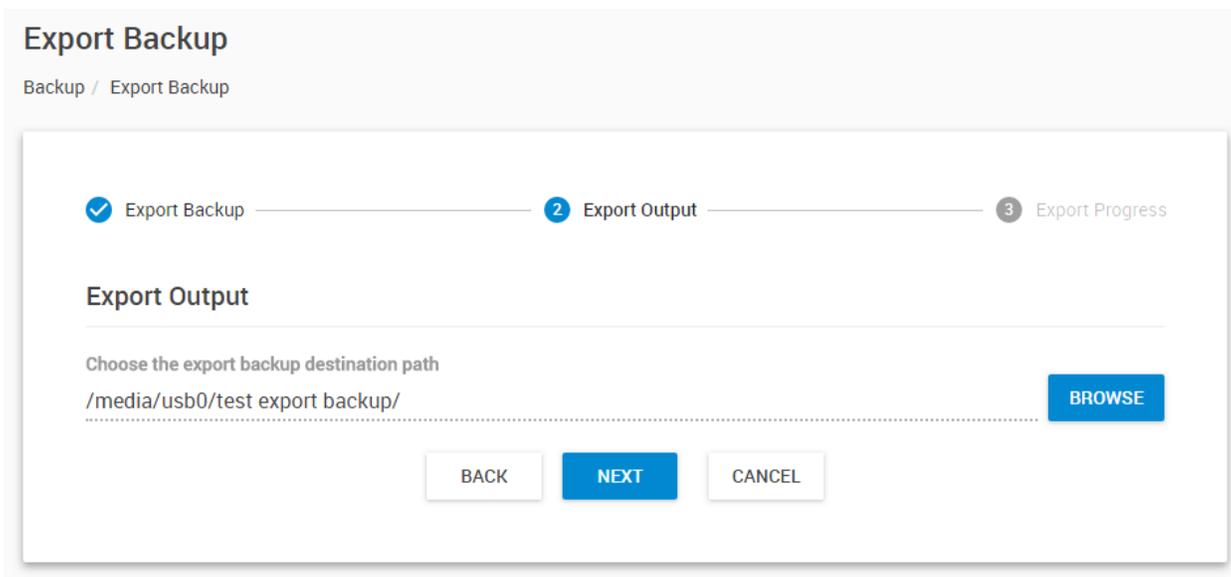
Your Export Output path will show the destination folder on your USB drive. Click **Next** to begin.

Now the backup export has started.

You'll see the progress indicator. This process can take a significant amount of time if you have chosen to include videos in your backup (even hours!) so please be patient. Its duration is also depending on the write speed of your USB drive.

During the export you can still use the APS Web UI for other tasks, but don't close the export page. You can still open another browser tab or window with the Monitoring page for example.

When the export has finished, click on **Finish**.

Restore

You can restore the full APS configuration from a backup file created earlier.
The backup contains all of your settings, users, Desktops and any connected units.
Optionally it can also contain recorded videos, but this is not recommended.
Important note: because backups are "snapshots" you'll lose any configuration changes and any graph data that was recorded <u>after the backup was made</u>.

Click on the **Restore Now** button to begin the restore process.
If you have performed a restore before, the date and time with result of the restore will be shown, as on the picture below:

The first important step is to choose the location of your backup files.

You can restore backups from internal backup files, or upload a backup file from local computer or USB drive. If you already have local backup files already, just press **Next** here.

If you haven't made local backups yet, you can upload an external backup file. After uploading, the restoration process of an external file or internal file is the same.

First choose the backup directory on the server where the file will be uploaded.

Then choose your backup file to upload.

Finally press the **Upload** button and wait until the upload finishes.

Click the **Next** button for further recovery steps.

If you have configured and made backups before, then the default path will be auto-selected.

Now you'll need to select the **backup archive file** (.bak) you wish to restore (which is named after the date and time it was made).
The server's MAC ID and IP address are listed in the details, and whether the backup contains video data or not.

Provide the backup file password, if it's necessary. We can recover your password for your backup file in case you have lost it. Please send us an e-mail to Support.

Click **Next** to continue.

If your system was reinstalled, or the backup is on an external USB drive, see the below steps how to access it.

Note: the screenshots for the USB restore process was taken from a Linux environment, but the Windows folder selection is functionally the same.
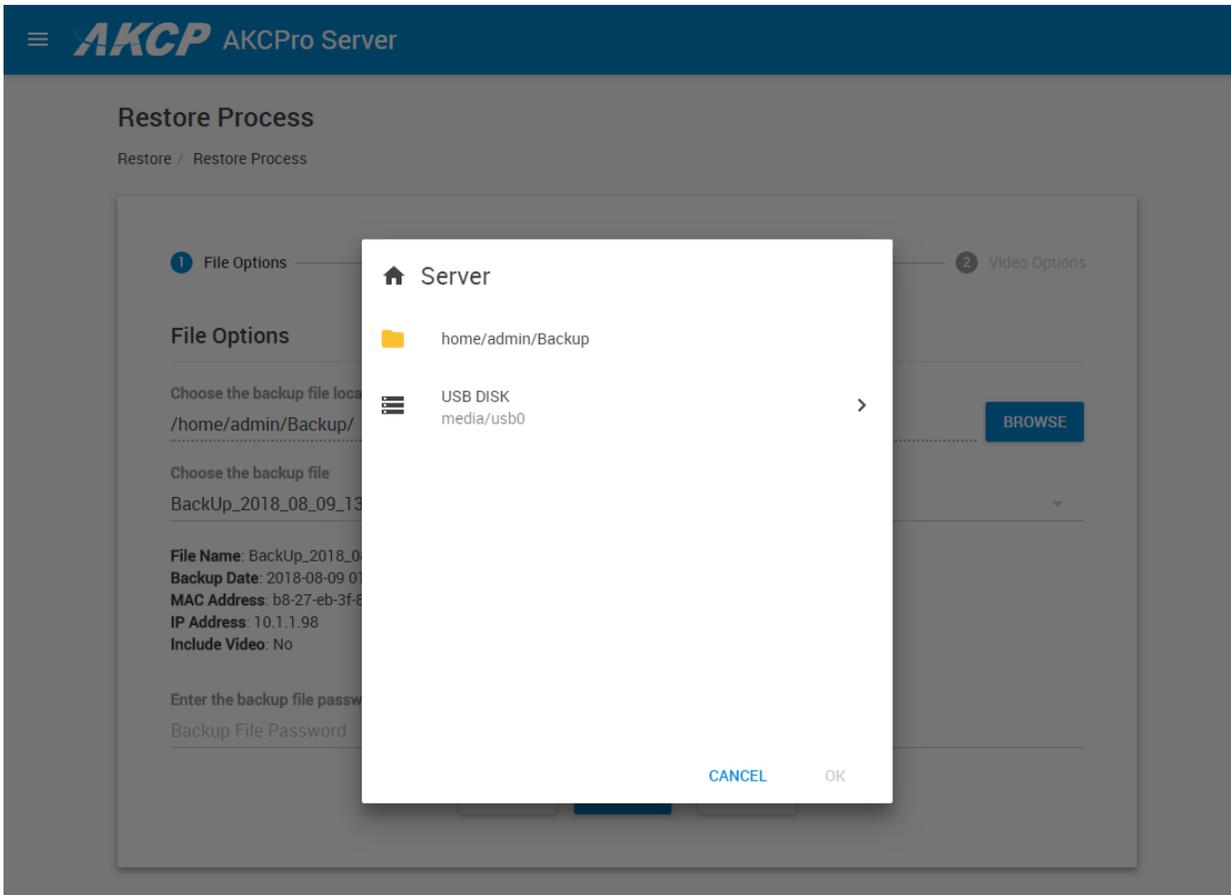
When you click the **Browse** button to search for the backup files location, you'll be able to browse local disks for files, and your USB drive.
Note: you need to plug in the USB drive before this step, otherwise it won't be shown.

Click on the **>** arrow to open your USB disk.
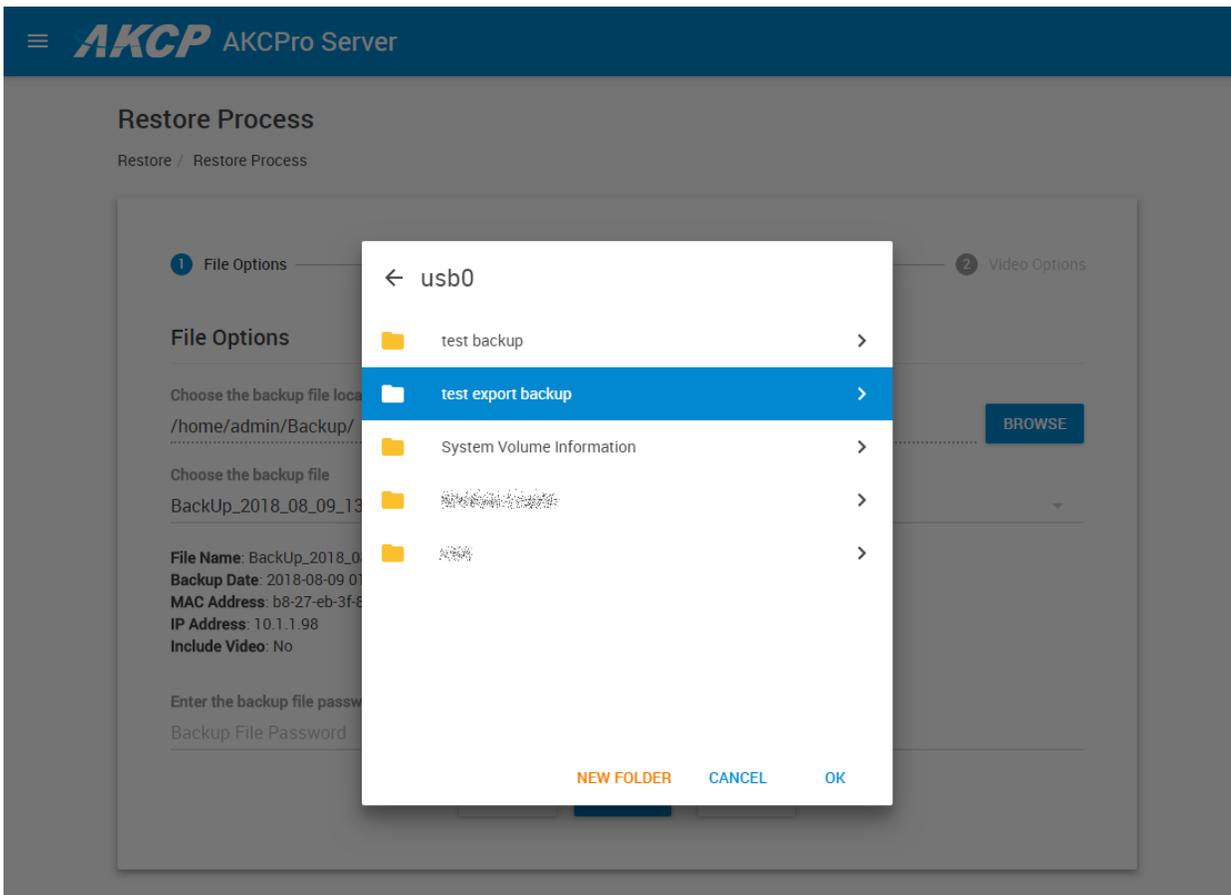
Now choose the folder where your backups are stored.
Don't go inside the folder, **you just need to highlight the folder** and press **OK**.

If you open the folder and go inside, a message will be shown to only select the folder itself.

Restore Process

Restore / Restore Process

1 File Options   **2** Video Options

File Options

Choose the backup file location

/media/usb0/test export backup/   **BROWSE**

Choose the backup file

> BackUp_2018_08_09_13_20_13.bak
>
> BackUp_2018_08_08_10_51_53.bak
>
> BackUp_2018_07_19_12_07_48.bak
>
> BackUp_2018_07_18_09_32_57.bak
>
> BackUp_2018_07_16_12_13_12.bak
>
> BackUp_2018_07_11_16_57_54.bak

Backup File Password

BACK   **NEXT**   **CANCEL**

As you can see on the screenshot, this folder on the USB drive has many backup files to choose from.

Select the one you wish to restore and provide the password if needed, then press **Next**.

If recorded video data is included in the backup archive, choose whether to restore them to their original path, or to another location.

Press **Finish** to start the restore process.

Be patient while the restore process is running.

It can take a very long time if your backup file is on a USB drive and contains videos.
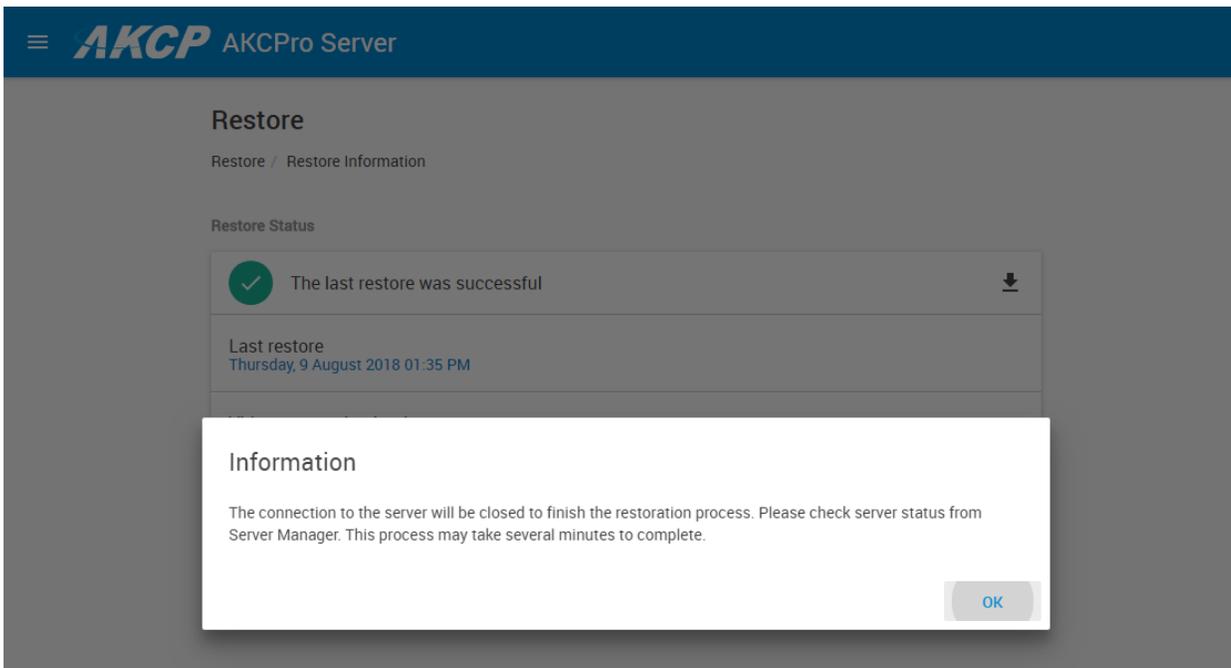
You'll be notified by a popup window when the restore is almost complete. The APS service needs to be restarted to finish restoring.
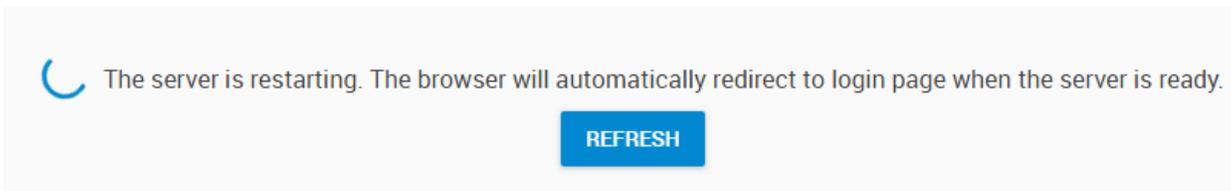
When the server is ready, you'll be redirected back to the login page:
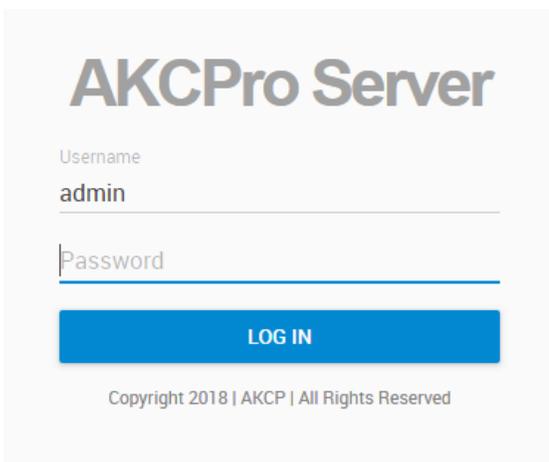
After logging in, you should see all your units, Desktops and settings have been correctly restored.

As with the Backup option, you can download and view the Restore log to see if it has finished properly.

Complete server reinstallation steps

Assuming a database backup has been made before, follow these steps to restore the APS environment:

1. Install the program (the admin password should be the same as on the previous install)
2. Re-activate the license (this should happen automatically if you have internet connection)
3. Start APS, log in with Admin then go to the Backup and Restore menu
4. Select Restore from file, and select the backup export file
5. Follow the instructions about the restore process (provide the backup password when prompted and if required)

Note: These instructions are for using the internal database. If you use a third-party database software to store APS data (such as MS SQL, Oracle), then you will have to first reinstall that database system, and restore the APS database file prior to installing APS.

We can recover your password for your backup file in case you have lost it. Please send us an e-mail to Support and include the backup log files.

8. Virtual Sensors

Virtual Sensors can be a very powerful tool in your monitoring system. On APS you can have virtually unlimited number of these Virtual Sensors (depending on your license count) 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 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.

Aside from a client unit's auto detected sensors, we can monitor a device by creating Virtual Sensors in APS.

You can create Virtual Sensors on any device that has been added to the APS console, not just AKCP units.

During configuration you could also set an External URL value for the Virtual Sensor, which will be visible and clickable when you place the VS on a map or on a Workspace.

All VS types support graphing and this can be already enabled for them during the configuration.
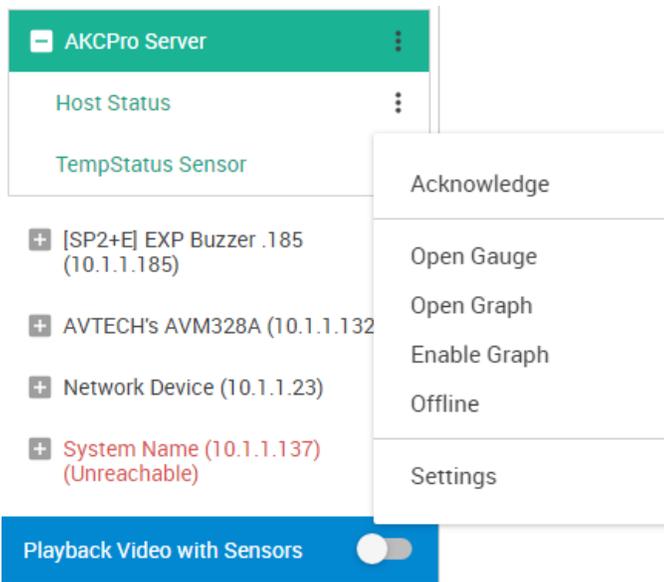
After a VS is created, you'll have the following choices in the popup menu, as seen on the example picture:

- Acknowledge status or warnings
- Open Gauge on the current Desktop
- Open Graph on the current Desktop
- Enable or Disable Graph
- Offline the sensor
- Reconfigure the VS under Settings

Very Important Note:

The APS Virtual Sensors will always run on the APS server machine locally. They are not to be confused with the SP+ or SEC5 Virtual Sensors which run on the units and cannot be managed with APS.

You can add a Virtual Sensor in two ways:
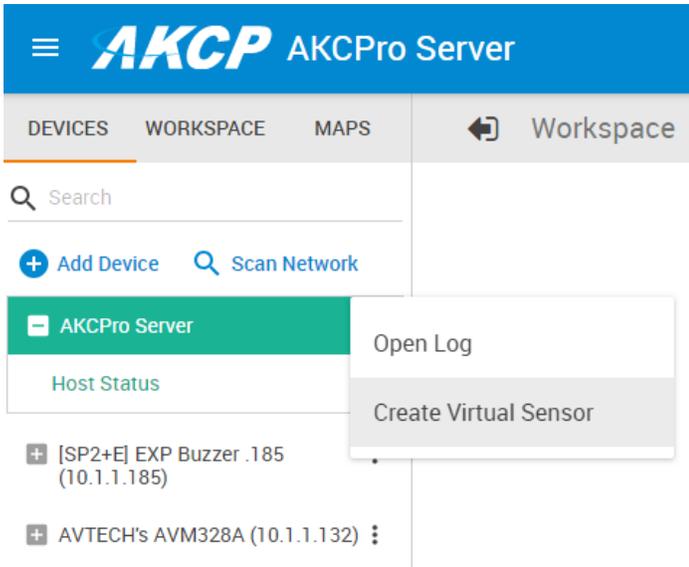
A) By clicking on the AKCPro Server's (or on any other connected device's) **popup menu** from the Devices tab on the Monitoring page and selecting **Create Virtual Sensor** from the popup menu, as shown on this picture.

B) By clicking **Add Device** from the Devices tab on the Monitoring page, and selecting **Virtual Sensor** device type:
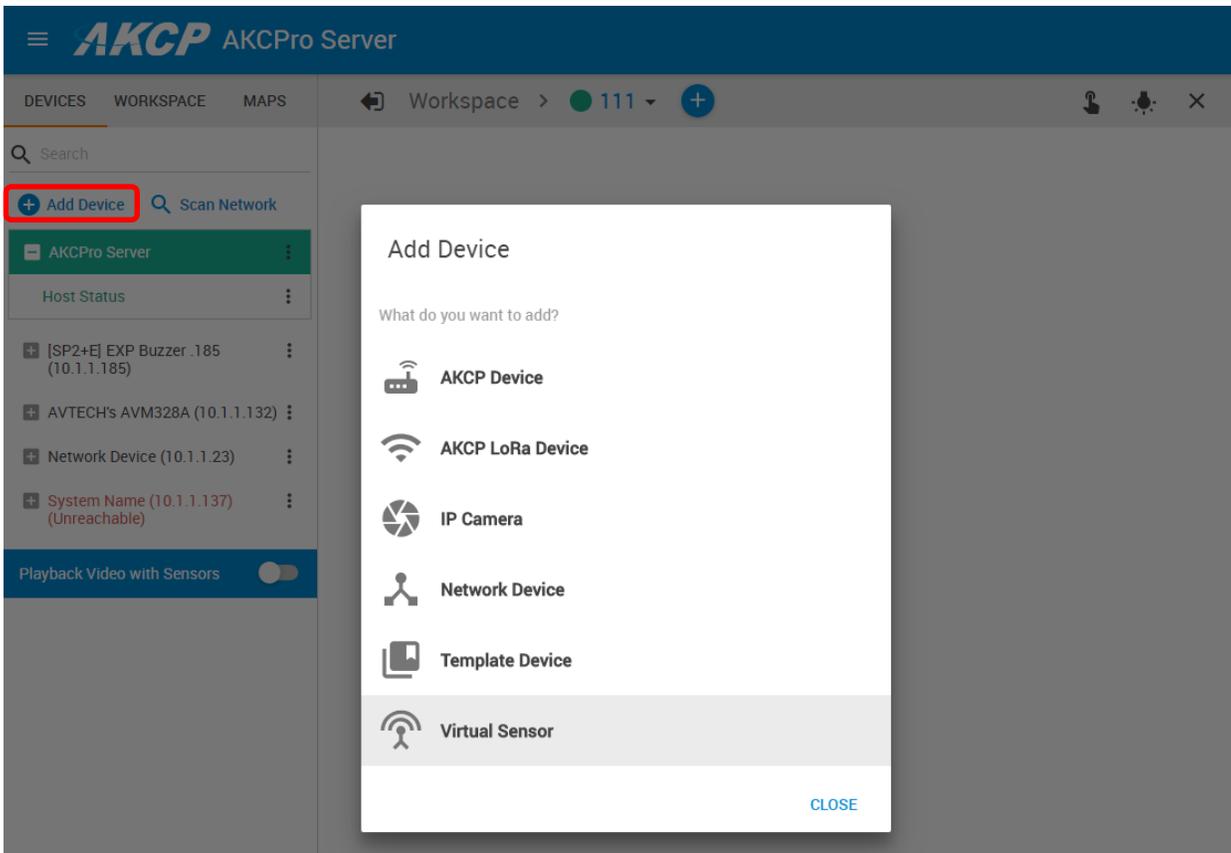
The **Virtual Sensor Wizard** will then run and lists the types of Virtual Sensors you can add:

Add new Virtual Sensor

Select Host
AKCPro Server

Select Virtual Sensor Type
SNMP Get

CANCEL   NEXT
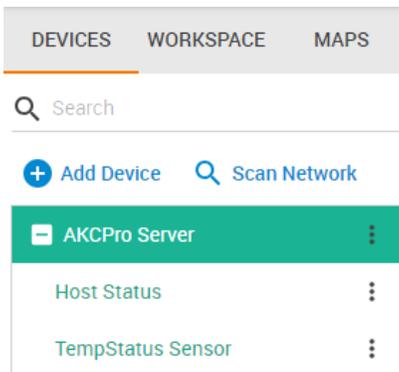
Choose the **Host** from the drop-down menu where you'd like to attach the new sensor to. If you clicked on a device's own popup menu, this will be already selected for you. If you don't want to attach the VS to a specific device, just leave the default AKCPro Server host. Your new VS will be created and configurable from the AKCPro Server host in the Monitoring page.

Regardless of the Host setting, all APS VS will still run on the APS computer itself.

As an example we've added an SNMP Get VS under the AKCPro Server host on this picture on the left.

DEVICES   WORKSPACE   MAPS

Q Search

⊕ Add Device   Q Scan Network

■ AKCPro Server   ⋮

Host Status   ⋮

TempStatus Sensor   ⋮

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

SNMP Get

Custom Script

Modbus TCP

Virtual Ping

Multiple Sensors

Logic

Energy Cost
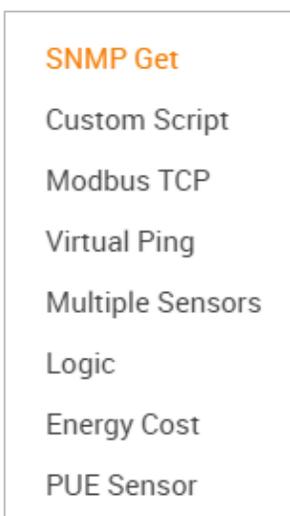
PUE Sensor

Secondly choose the **Virtual Sensor Type** from the second drop-down menu, and click **Next** for further configuration of the sensor.

Below we will go through the steps of creating each one of these Virtual Sensor types.

SNMP Get

The SNMP Get Virtual Sensor can poll any SNMP enabled device for monitoring.

First give the sensor a name and select the **Hostname or IP** of the unit which you like to monitor.

Specify the **SNMP Community**, and set the **SNMP Port** - the default is already added.

You could also set an External URL for the Virtual Sensor, which will be visible when you place the VS on a map or on a Workspace.

Click **Next** to continue.

SNMP Get

Set the **OID value** from which you wish to poll from.

Click **Next** to continue.

In this important step you have to choose the **Virtual Sensor's Data Type** between **Number / String**. This will define the further configuration options depending on the type you selected. We'll show you the configuration for each type below.

You can optionally enable the sensor's graph and click **Next** to continue.

Number Type / Switch Style

This style is used to get integer values and compare value readings.

Choose the **State Value**: if the SNMP value reading will be any other number different than the number you set here, then the VS state will be Critical.
Or if you toggle the State to be Critical, then the VS will become Critical state only when the SNMP value reading is exactly the same number you set in the State Value.

For example, the AKCP Temperature Sensor's normal status value is 2 so you should set the State Value to 2 for monitoring AKCP sensor status OIDs.

Click **Next** to continue.

SNMP Get

✓ SNMP Get — ✓ OID — ✓ Sensor — ✓ Sensor Detail — **5** Sensor Description — **6** Interval

Description of Normal Status
Normal

Description of Critical Status
Critical

[BACK] [**NEXT**] [CANCEL]

Set the Sensor Status Description values and click **Next**.

SNMP Get

✓ SNMP Get — ✓ OID — ✓ Sensor — ✓ Sensor Detail — ✓ Sensor Description — **6** Interval

Polling Interval
15

[BACK] [**FINISH**] [CANCEL]

Choose the **Polling Interval** and click **Finish**.

Number Type / Analog Style

SNMP Get

✓ SNMP Get — ✓ OID — ✓ Sensor — 4 Sensor Detail — 5 Sensor Description — 6 Interval

Sensor Style
Analog

Min	Unit
0	Unit

Low Critical	Value Factor
20	x1

Low Warning	Rearm
40	0

High Warning
60

High Critical
80

Max
100

BACK   NEXT   CANCEL

This style is used to get integer values and display a gauge with the value readings.
For analog style sensor, you can set custom thresholds and even turn off the unnecessary statuses, for example if you don't want to include the High Warning / Low Warning readings in the VS.
Choose the displayed **Unit** and the **Value Factor**. With Value Factor you can modify the reading range of the VS (Example: if raw value is 1234 and needs to show a value to 12.34, then this should be set to x0.01. Default is x1).
With the **Rearm** value you can control how sensitive your VS is to changes. For example if you set the Rearm to 2, then the VS status won't change unless the read values are bigger than 2.

Set the Sensor Status Description values and click **Next**. Set the **Polling Interval** and **Finish**.

String Type

SNMP Get

SNMP Get — OID — **3** Sensor — **4** Sensor Detail — **5** Sensor Description — **6** Interval

Data Type
String

Separator
Comma

Separate Index
1

Enable Graph

BACK   NEXT   CANCEL

Select the String Data Type if the SNMP Get reading will return multiple data as String type.

Choose the **Separator** type between Comma or Semicolon, and set the **Separate Index**.

You can also optionally enable graphing, and click **Next** to continue.

SNMP Get

✓ SNMP Get — ✓ OID — ✓ Sensor — **4** Sensor Detail — **5** Sensor Description — **6** Interval

Sensor Style
Analog

Min	Unit
0	Unit

Low Critical	Value Factor
20	x1

Low Warning	Rearm
40	0

High Warning
60

High Critical
80

Max
100

BACK   NEXT   CANCEL

For analog style sensor, you can set custom thresholds and even turn off the unnecessary statuses, for example if you don't want to include the High Warning / Low Warning readings in the VS.

Choose the displayed **Unit** and the **Value Factor**. With Value Factor you can modify the reading range of the VS (Example: if raw value is 1234 and needs to show a value to 12.34, then this should be set to x0.01. Default is x1).

With the **Rearm** value you can control how sensitive your VS is to changes. For example if you set the Rearm to 2, then the VS status won't change unless the read values are bigger than 2.

Set the Sensor Status Description values and click **Next**. Set the **Polling Interval** and **Finish**.

SNMP Get Examples

A) SNMP Get Temperature Sensor Status setup

This is a simple SNMP GET type Virtual Sensor, for checking the status of the given sensor (SNMP OID). It's a switch style SNMP sensor, State Value 2. Like the ping sensor, it runs on the APS machine.

Tip: Get the actual OID values from the Web UI of the unit if available, or use a MIB browser.

B) SNMP Get Temperature Sensor Value setup
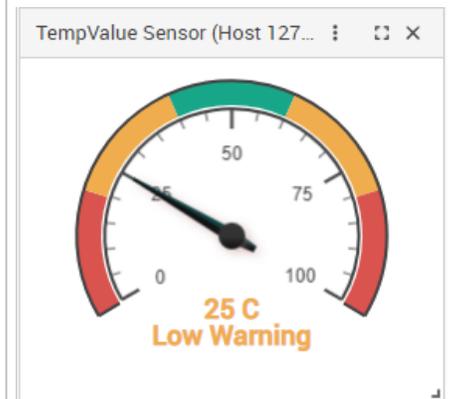
This is a simple SNMP GET type Virtual Sensor, for checking the decimal reading value of the given sensor (SNMP OID). It's an analog style SNMP sensor. Like the ping sensor, it runs on the APS machine.

Tip: Get the actual OID values from the Web UI of the unit if available, or use a MIB browser.

Custom Script

You can execute custom scripts or programs with this Virtual Sensor.
The script language supported will depend on the OS platform (Windows or Unix) and you cannot execute scripts that cannot run on the OS (for example .BAT won't run under Linux).

Give the Virtual Sensor a name and click **Next** to continue.

Optionally you can specify the External URL.

Very Important Note:
The script itself will run on the server machine where APS is installed.
Also, you'll have to use Windows script commands and programs in the script.

Script files physical location for troubleshooting and backup:
C:\ProgramData\AKCP\AKCPro Server\VirtualSensor\Custom

Click on the **Add** button to upload your script, or you can select it from the list in case if you've already uploaded it earlier.

Optionally, parameters to the script can be passed in the **Arguments** field.

See a simple example below.

Example Ping sensor setup with custom script

Create a .BAT file with this content:

```
@echo off
ping %1 | findstr unreachable >NUL
if %errorlevel% EQU 0 echo 1
if %errorlevel% NEQ 0 echo 0
```

This script file will ping the host specified as a parameter (%1, in our case 10.1.1.225), and will set the end result of the script depending on the ping result. If the host is reachable, it will return 0; if it's unreachable, returns 1. This script needs a switch style sensor since it has 2 values (see below).

Click **Next** to select the sensor style.

For virtual script sensor, there are 3 sensor types to choose from:

Switch
Analog
Static

1. Analog
2. Switch
3. Static

For each type:
1. Analog, script returns Integer (user configurable for each high warning/low warning etc. state)
2. Switch, script returns Integer (user configurable for normal/critical state)
3. Static script returns String (any string output that is returned will be the sensor state displayed)

We'll detail each type below.

Important: your script file must have an exit code when it finishes execution. APS will check the exit code when the script finishes, and report error if the code is different than the normal value you give here.
Example: to have a return code 0 when your script finishes regardless of the execution outcome, type "exit 0" or "echo 0" as the last line in the script. This will ensure your sensor doesn't show "Sensor Error" status.

Important note for running Linux scripts (only on non-Windows APS platforms):
If you use Bash specific syntax in your script, you must explicitly use `#!/bin/bash`
Using `#!/bin/sh` might not work correctly, if the syntax of your script is not fully POSIX compliant.

Switch style

Custom Script

Host —— Custom Script —— ③ Sensor —— ④ Sensor Description —— ⑤ Interval

Sensor Style
Switch

State Value
0

State
◉ Normal
○ Critical

⬤ Enable Graph

BACK   NEXT   CANCEL

For Switch style you just need to select the **Default State** between Normal or Critical.

Then set the **State Value**: if the script output's value reading will be any other number different than the number you set here, then the VS state will be Critical.
Or if you toggle the State to be Critical, then the VS will become Critical state only when the script end result value reading is exactly the same number you set in the State Value.

Optionally you can enable the graph here.

Click **Next** to continue.

Custom Script

Host —— Custom Script —— Sensor —— ④ Sensor Description —— ⑤ Interval

Description of Normal Status
Normal

Description of Critical Status
Critical

BACK   NEXT   CANCEL

Set the Sensor Status Description values and click **Next**.

Custom Script

Host —— Custom Script —— Sensor —— Sensor Description —— ⑤ Interval

Polling Interval
15

Execute timeout
10

Retry
3

BACK   FINISH   CANCEL

Set the **Polling Interval**, **Execute Timeout** and **Retry** values then click **Finish**.

Analog style

Custom Script

✓ Host ———— ✓ Custom Script ———— ③ Sensor ———— ④ Sensor Description ———— ⑤ Interval

Sensor Style
Analog

Min
0

Unit
Unit

Low Critical
20

Value Factor
x1

Low Warning
40

Rearm
0

High Warning
60

Enable Graph

High Critical
80

Max
100

BACK   **NEXT**   CANCEL

This style is used to get integer values and display a gauge with the value readings.
For analog style sensor, you can set custom thresholds and even turn off the unnecessary statuses, for example if you don't want to include the High Warning / Low Warning readings in the VS.
Choose the displayed **Unit** and the **Value Factor**. With Value Factor you can modify the reading range of the VS (Example: if raw value is 1234 and needs to show a value to 12.34, then this should be set to x0.01. Default is x1).
With the **Rearm** value you can control how sensitive your VS is to changes. For example if you set the Rearm to 2, then the VS status won't change unless the read values are bigger than 2.

Custom Script

Host ✓ —— Custom Script ✓ —— Sensor ✓ —— **4** Sensor Description —— **5** Interval

Description of Low Critical Status
Low Critical

Description of Low Warning Status
Low Warning

Description of Normal Status
Normal

Description of High Warning Status
High Warning

Description of High Critical Status
High Critical

BACK   NEXT   CANCEL

Set the Sensor Status Description values and click **Next**.

Custom Script

Host ✓ —— Custom Script ✓ —— Sensor ✓ —— Sensor Description ✓ —— **5** Interval

Polling Interval
15

Execute timeout
10

Retry
3

BACK   FINISH   CANCEL

Set the **Polling Interval**, **Execute Timeout** and **Retry** values then click **Finish**.

Static style

This sensor style doesn't have any additional settings.
The script output will be displayed "as is" in string format and you cannot use a gauge style gadget for this style.

Set the **Polling Interval**, **Execute Timeout** and **Retry** values then click **Finish**.

Modbus TCP

With the Modbus TCP Virtual Sensor you can monitor any Modbus device (read values) that supports the Modbus TCP protocol.

First type in the **Modbus Hostname or IP** of the device you wish to monitor.

The default **Modbus TCP Port** is already defined but you can modify it if needed.

Optionally you can give the VS an External URL then click **Next** to continue.

First choose the Modbus command that you wish to execute with this Virtual Sensor.

This example picture shows the configuration for Read Coil Status and Read Input Status.
Reading registers will have more options available (see on next page).

Type in the **Modbus Register Address** and the **Slave ID**.

Modbus TCP

✓ Modbus TCP — ② Modbus TCP detail — ③ Sensor — ④ Sensor Description — ⑤ Interval

Data Ordering
(0x03) Read Holding Registers

Data Ordering
Low Byte First, Low Word First

Data Type
16 bits unsigned int

Value Factor in Command
1

Modbus Register Address
0

Modbus Slave ID
255

* The slave ID is required if the message must reach a device on a serial network. (Default is 255)

BACK   NEXT   CANCEL

Reading Holding- and Input registers will have some more options available.

You can also specify the **Data Ordering** options:

Low Byte First, Low Word First

Low Byte First, High Word First

High Byte First, High Word First

High Byte First, Low Word First

And also you can select the **Data Type**:

16 bits unsigned int

16 bits signed int

16 bits two characters ASCII

32 bits unsigned int

32 bits signed int

32 bits IEEE floating point

***Important note for Data Type:** if you wish to monitor negative values, you'll have to use the Signed Integer type. With Unsigned Integer, you can only get positive values.*

With **Value Factor** you can multiply or divide the actual value reading.
For example setting 10 will multiply the reading by 10, or setting it to 0.1 will divide by 10.
(Example: if raw value is 1234 and needs to show a value to 12.34, then this should be set to x0.01. Default is x1)

When you use Modbus TCP VS on AKCP units:

- 0x03 Read Holding Registers is usually used for getting the sensor status
- 0x04 Read Input Registers is usually used for getting the sensor value

Note for Sensor Error state with AKCP sensors: Modbus just gives values but no extra information if the monitored sensor is in error state. If you see a VS reading with 65535 value that usually indicates the sensor has error. As on this example picture we monitor a Temperature sensor with both SNMP Get and Modbus TCP VS, while it goes to Sensor Error state:

Click **Next** to continue.

Choose the sensor's display style between Switch or Analog.

Switch style

For Switch style you just need to select the **Default State** between Normal or Critical.

Then set the **State Value**: if the SNMP value reading will be any other number different than the number you set here, then the VS state will be Critical.
Or if you toggle the State to be Critical, then the VS will become Critical state only when the Modbus value reading is exactly the same number you set in the State Value.

Optionally you can enable the graph here.

Click **Next** to continue.

Set the Sensor Status Description values and click **Next**.

Set the **Polling Interval**, **Execute Timeout** and **Retry** values then click **Finish**.

Analog style

This style is used to get integer values and display a gauge with the value readings.

For analog style sensor, you can set custom thresholds and even turn off the unnecessary statuses, for example if you don't want to include the High Warning / Low Warning readings in the VS.

Choose the displayed **Unit** and the **Value Factor**. With Value Factor you can modify the reading range of the VS (Example: if raw value is 1234 and needs to show a value to 12.34, then this should be set to x0.01. Default is x1).

With the **Rearm** value you can control how sensitive your VS is to changes. For example if you set the Rearm to 2, then the VS status won't change unless the read values are bigger than 2.

Modbus TCP

✓ Modbus TCP — ✓ Modbus TCP detail — ✓ Sensor — ④ Sensor Description — ⑤ Interval

Description of Low Critical Status
Low Critical

Description of Low Warning Status
Low Warning

Description of Normal Status
Normal

Description of High Warning Status
High Warning

Description of High Critical Status
High Critical

BACK   NEXT   CANCEL

Set the Sensor Status Description values and click **Next**.

Modbus TCP

✓ Modbus TCP — ✓ Modbus TCP detail — ✓ Sensor — ✓ Sensor Description — ⑤ Interval

Polling Interval
15

Execute timeout
10

Retry
3

BACK   FINISH   CANCEL

Set the **Polling Interval**, **Execute Timeout** and **Retry** values then click **Finish**.

Example Modbus TCP Virtual Sensor

In the following example, we'll show you how to set up a Virtual Sensor to monitor the Temperature Sensor on a SP+ unit via Modbus TCP.

First you'll need to configure Modbus on the SP+ unit with the sensor which you'd like to monitor.
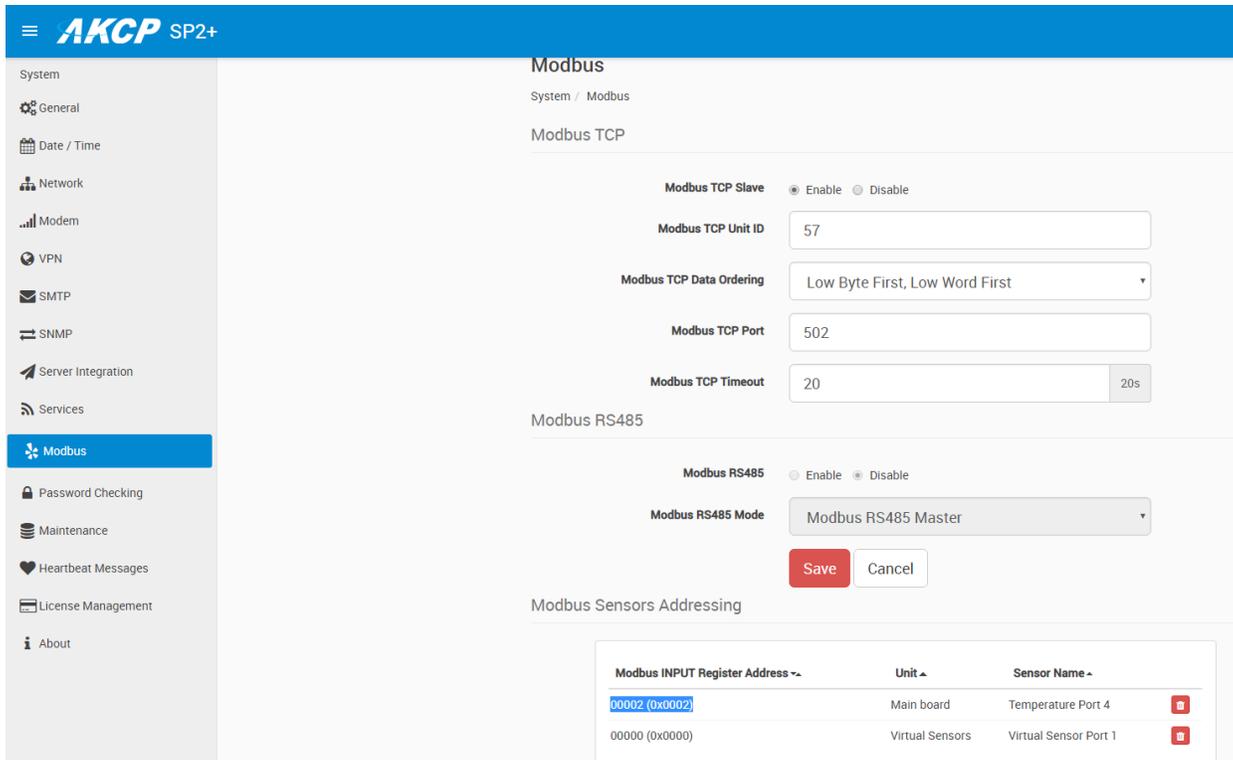
Go to the **unit's Web UI -> Settings menu -> System -> Modbus** as shown on the screenshot above.

Enable the **Modbus TCP Slave** option and set the **Unit ID**. This needs to be unique on your network. Set the **Modbus TCP port** (default 502) and a **timeout**. It's recommended to set the timeout to a low value on a local network (minimum is 20 seconds).

To monitor the Temperature Sensor via analog style VS, we'll need to set the **Data Ordering** to be **Low Byte First, Low Word First**.

Make a note of the **Modbus Input Register Address** for your **Temperature Sensor**. On our screenshot it's shown as 0x0002.

Now click on **Save** and reboot the SP+ unit. You can perform software reboot under the **Maintenance** menu.

Secondly, set up the Modbus VS on APS as follows.

Modbus TCP

1 **Modbus TCP** — 2 Modbus TCP detail — 3 Sensor — 4 Sensor Description — 5 Interval

Sensor Name
ModbusTemp Sensor

Modbus Hostname or IP
10.1.1.57

Modbus TCP Port
502

External URL

BACK   NEXT   CANCEL

Type in the unit's IP address and the Modbus port.

Modbus TCP

✓ Modbus TCP — ② Modbus TCP detail — ③ Sensor — ④ Sensor Description — ⑤ Interval

Data Ordering
(0x04) Read Input Registers

Data Ordering
Low Byte First, Low Word First

Data Type
16 bits signed int

Value Factor in Command
1

Modbus Register Address **(0x2)**
2

Modbus Slave ID
57

* The slave ID is required if the message must reach a device on a serial network. (Default is 255)

BACK   NEXT   CANCEL

Set up the sensor as follows:

- Use the **Read Input Registers (0x04)** function
- Data ordering: **Low Byte First, Low Word First** (as on the source unit)
- Data type: **16 bit signed integer** (allows negative values)
- Value factor in command: 1
- **Modbus Register Address**: use the correct number from your source unit; ours is 2
- **Modbus Slave ID**: use the correct number from your source unit; ours is 57

Modbus TCP

✓ Modbus TCP — ✓ Modbus TCP detail — **3** Sensor — **4** Sensor Description — **5** Interval

Sensor Style
Analog

Min
0

Unit
°C

Low Critical
20

Value Factor
x0.1

Low Warning
40

Rearm
0

High Warning
60

Enable Graph

High Critical
80

Max
100

BACK   NEXT   CANCEL

Specify **Analog style** and set the value ranges to your specific needs.
The **Value Factor** should be **x0.1** when using Modbus reading.

Modbus TCP

✓ Modbus TCP — ✓ Modbus TCP detail — ✓ Sensor — ④ Sensor Description — ⑤ Interval

Description of Low Critical Status

Low Critical

Description of Low Warning Status

Low Warning

Description of Normal Status

Normal

Description of High Warning Status

High Warning

Description of High Critical Status

High Critical

BACK   NEXT   CANCEL

Set the sensor state descriptions according to your needs.

Modbus TCP

✓ Modbus TCP — ✓ Modbus TCP detail — ✓ Sensor — ✓ Sensor Description — ⑤ Interval

**Polling Interval**

15

Execute timeout

10

Retry

3

BACK   **FINISH**   CANCEL

Set the sensor polling intervals and timeouts according to your needs.

Modbus VS

26 °C
Low Warning

Modbus VS

🕐 Display Time Range

2pm 04/12/2018   7pm 04/12/2018   12am 05/12/2018   4am 05/12/2018   9am 05/12/2018
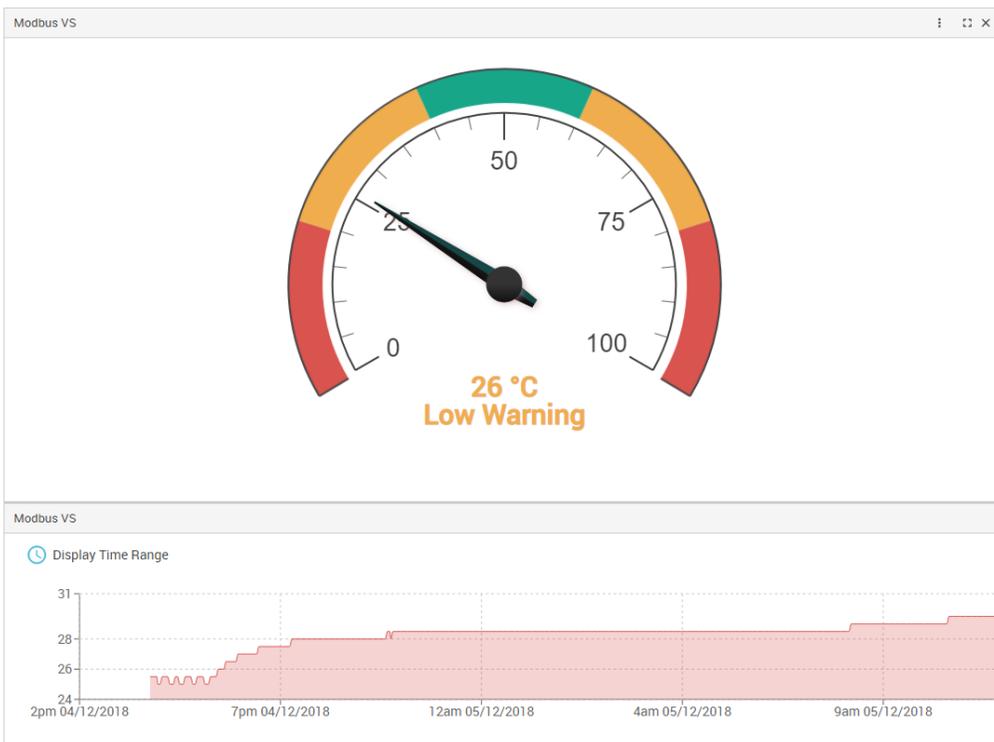
After setting up the sensor, you can place the gauge on a Desktop and enable graphing for it (for VS the graph needs to be enabled separately).

Virtual Ping

With the Virtual Ping sensor you can monitor any network device by ping or HTTP requests.

Select the **Hostname or IP** that you wish to monitor by this sensor.

Choose the **Method to monitor**: Ping or HTTP

You can also enable Graph and specify External URL.

Click **Next** to continue.

Choose the **Status Description** for each status and click **Next**.

Finally choose the **Polling Interval**, **Execution timeout** and **Retry** values and click **Finish**.

Multiple Sensors

The Multiple Sensors is a special Virtual Sensor type. It allows for a very wide selection and configuration options, with which you can monitor sensor statuses.

Compare and calculation options include:

AND / OR / ALL FALSE
ADD / DIVIDE / MULTIPLY / AVERAGE
(on newer APS you'll also be able to use SUBTRACT)

The available options will depend on the sensor style and source sensors.

First give the new Virtual Sensor a name, and you can specify External URL and enable graphing (these could be also configured later).

Click **Next** to select the sensors that you want to work with.

Switch style

The switch style sensor's configuration is relatively simple:

Select your source sensors and their statuses, and choose when the Virtual Sensor will become Critical status.

For example if you set the condition to be AND, and select 2 Temperature Sensors from the list, then the Virtual Sensor will become critical only when both of them are critical.

Click **Next** to continue.

The switch style VS has only 2 sensor status descriptions. Click **Next** to continue.

Select the **Polling Interval** and click **Finish**.

Analog style

Multiple Sensors

✔ Multiple Sensors – ② Select Sensor – ③ Sensor Detail – ④ Sensor Description – ⑤ Interval

Sensor Style
Analog ▾

Calculation
Add ▾

	Select Host	Select Sensor
A	None ▾	None ▾
B	None ▾	None ▾
C	None ▾	None ▾
D	None ▾	None ▾
E	None ▾	None ▾
F	None ▾	None ▾
G	None ▾	None ▾
H	None ▾	None ▾

Please select at least one sensor.

BACK   NEXT   CANCEL

Add
Subtract
Multiply
Divide
Average

The analog style VS is a little more complex, and allows advanced calculations to perform on the sensor readings (on newer APS you'll also be able to use Subtract). Because it is performing calculations on numerical readings, you could only select sensors that have integer values.

Click **Next** to continue.

Multiple Sensors

✓ Multiple Sensors – ✓ Select Sensor – ③ Sensor Detail – ④ Sensor Description – ⑤ Interval

Min
0

Unit
Unit

Low Critical
20

Value Factor
1

Low Warning
40

Rearm
0

High Warning
60

High Critical
80

Max
100

BACK   NEXT   CANCEL

For analog style sensor, you can set custom thresholds and even turn off the unnecessary statuses, for example if you don't want to include the High Warning / Low Warning readings in the VS.

Choose the displayed **Unit** and the **Value Factor**. With Value Factor you can modify the reading range of the VS (Example: if raw value is 1234 and needs to show a value to 12.34, then this should be set to x0.01. Default is x1).

With the **Rearm** value you can control how sensitive your VS is to changes. For example if you set the Rearm to 2, then the VS status won't change unless the read values are bigger than 2.

Click **Next** and set your **Polling Interval**, then **Finish**.

Multiple State style

This is the most complex sensor style.

First you'll have to select the source sensors and their statuses, from which you wish to perform comparing or calculations on.

Click **Next** to continue.

Multiple Sensors

Multiple Sensors – Select Sensor – **3** Sensor Detail – **4** Sensor Description – **5** Interval

Low Critical
B ⬤ **False**

Low Warning
◯ Disabled

Normal
A **False**

High Warning
◯ Disabled

High Critical
◯ Disabled

EVALUATE

BACK | NEXT | CANCEL

Here you can configure the evaluation of the Virtual Sensor. This would be a short- or a long list, depending on how many source sensors you selected (for simplicity, here we've only chosen 2 source sensors).
As with the Analog style, you can select to disable some unused states.

APS will automatically calculate a result from your source sensors. If you changed some options, click on the **Evaluate** button again to see the calculation result.

Click **Next** to continue.

The Sensor Status Description values will depend on the number of sensors you selected.

Click **Next** and set your **Polling Interval**, then **Finish**.

Logic

Logic

① Logic ———— ② Select Sensor ———— ③ Sensor Description ———— ④ Interval

Sensor Name
Logic Sensor

Trigger Logic
FlipFlop

Default Status
No Status

Normal State
False

External URL

◯ Enable Graph

BACK   NEXT   CANCEL

The Logic is a special sensor type on APS which uses FlipFlop logic. You can monitor any host's any sensor's statuses with it, and change the Logic virtual sensor's state with the pre-set values for the status of another sensor (SET Source Sensor).
The Logic will ignore all other intermediate sensor statuses and only changes the virtual sensor's state back if it **exactly** matches the specified physical sensor status (RESET Source Sensor).
We'll show some examples below.

First configure the Logic sensor's **Normal State** between True or False.
With this setting you can easily reverse the monitoring logic that you'll configure in the next step.

Choose the Virtual Sensor's **Default Status**:

Normal or Critical default status will be depending on your monitored sensors.
No Status is useful if you'll monitor sensors which by default don't report any status, only if there's an error.

No Status

Normal

Critical

You can also enable Graphing and specify an External URL.

Click **Next** to configure your monitored sensors.

Choose your **Host** (where your sensor is connected), the **Sensor to Monitor**, and the **Status** you'd like the logic to monitor.

See an example below.

For example, you can set the logic to change the virtual sensor to *Critical* if the *Temperature sensor's status* becomes *High Critical* on one of your SP+ units, and only change the virtual sensor back to *Normal* when the *Temperature sensor's status* also becomes *Normal*.

It will ignore a status change if the Temperature sensor becomes *Sensor Error* or *Low Critical* etc.

There's also support for **Multiple Sensors FlipFlop** logic as you can see on this example below:

In this mode you can choose from multiple sensors for monitoring (up to 4).

It has AND relation between them, and only changes the virtual sensor's state if there's an **exact match** for these statuses.

For example we set up a server room monitoring as follows:
The Logic virtual sensor will be *Normal* state until *both* the Host Status and Temperature sensors show *Normal* state, and only become *Critical* if *both* of these monitored sensors report critical statuses. The virtual sensor will only change back to *Normal* state if both the Host Status and Temperature sensors show *Normal* state.

Logic

Choose the sensor status descriptions for this Virtual Sensor and click **Next**.

Choose the Polling Interval for this Virtual Sensor and click **Finish**.

Energy Cost

With the Energy Cost Virtual Sensor you can easily monitor the consumption reading from your PMS, and calculate the energy costs.

Specify your **Currency** and the **Cost Rate** then click **Next**.

Choose the source sensor from a connected client unit.
Usually this would be a Power Meter (PMS) unit reading with the Active Power value, but Virtual Sensors are also supported for example to get the power reading from a PMS through Modbus VS.

Also, you can select multiple PMS sensors from the list, if required. Their readings will be added together for the calculation.

Click **Next** to continue.

Energy Cost

Energy Cost ——————— Select Sensor ——————— ③ Threshold ——————— ④ Interval

Min

0

Low Critical

2000

Low Warning

4000

High Warning

6000

High Critical

8000

Max

10000

BACK   NEXT   CANCEL

Set the threshold values that will be used for this sensor and click **Next**.

Energy Cost

Finally set the **Polling Interval** and click **Finish**.

PUE

You can create your own live, dynamic PUE calculation display with this virtual sensor type. Power usage effectiveness (PUE) is a ratio that describes how efficiently a computer data center uses energy; specifically, how much energy is used by the computing equipment (in contrast to cooling and other overhead). An ideal PUE is 1.0.

Anything that isn't considered a computing device in a data center (i.e. lighting, cooling, etc.) falls into the category of facility energy consumption (Non-IT).

$$PUE = \frac{\text{Total Facility Energy}}{\text{IT Equipment Energy}}$$

To calculate PUE, a division is performed between IT Energy and Non-IT Energy consuming values. Therefore **you must specify 2 different source sensors to do the calculation** (in the next steps).

E-learning videos

Live PUE calculations
https://youtu.be/iLxnaZD-8VE
PUE virtual sensor setup
https://youtu.be/Thvz7iTDiCk

First give the sensor a descriptive name and set the **Polling Interval**, then click **Next**.

PUE Sensor

PUE ——— ② Select IT Power Sensor ——— ③ Select Non-IT Power Sensor ——— ④ Threshold

Select IT Power Sensor

🔍 Search

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

　　⌃ **Virtual Sensors**

　　　☑ Virtual Sensor Port 1

　　　☐ Virtual Sensor Port 2

BACK　　NEXT　　CANCEL

First choose the source of the **IT power sensor** from a connected client unit.
Usually this would be a Power Meter (PMS) unit reading with the Active Power value, but Virtual Sensors are also supported for example to get the power reading from a PMS through Modbus VS.

Click **Next** to continue.

PUE Sensor

✓ PUE ——— ✓ Select IT Power Sensor ——— **3** Select Non-IT Power Sensor ——— **4** Threshold

Select Non-IT Power Sensor

🔍 Search

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

   ∧ **Virtual Sensors**

      ☐ Virtual Sensor Port 1

      ☑ Virtual Sensor Port 2

[BACK] [**NEXT**] [CANCEL]

Now choose the source of the **Non-IT power sensor** from a connected client unit.
Usually this would be a Power Meter (PMS) unit reading with the Active Power value, but Virtual Sensors are also supported for example to get the power reading from a PMS through Modbus VS.

Click **Next** to continue.

PUE Sensor

✓ PUE ——— ✓ Select IT Power Sensor ——— ✓ Select Non-IT Power Sensor ——— ④ Threshold

Min

1

Very Efficient

1.2

Efficient

1.5

Inefficient

2.5

Very Inefficient

3.0

Max

5

BACK   FINISH   CANCEL

As the final steps, set the thresholds for the PUE calculation.
The default values are already set but you can specify your own if you wish, then click on **Finish**.

After the wizard completes, you'll actually get a series of PUE VS which you could modify further to your needs. Therefore you'll need to have at least 4 APS VS licenses to calculate the PUE:

- PUE
- PUE (IT)
- PUE (Non-IT)
- PUE (Total)

9. Troubleshooting

Steps to manually replace the HTTPS certificate of APS HTML UI on Windows

1. Make the correct PEM file (see the SSL section in this manual)
2. Stop all APS services using Server Manager: Service menu / Stop service
3. Navigate to *C:\ProgramData\AKCP\AKCPro Server\SSL*
4. Make a backup of the existing **http_cert.pem** file
5. Copy your custom .pem file there (in the screenshot it's akcp2-new.pem)
6. Delete the old **http_cert.pem** file (don't touch **server.pem**!)
7. Rename your custom .pem to **http_cert.pem**
8. Start all APS services again using Server Manager
9. Open APS HTML UI and verify your SSL certificate has been replaced
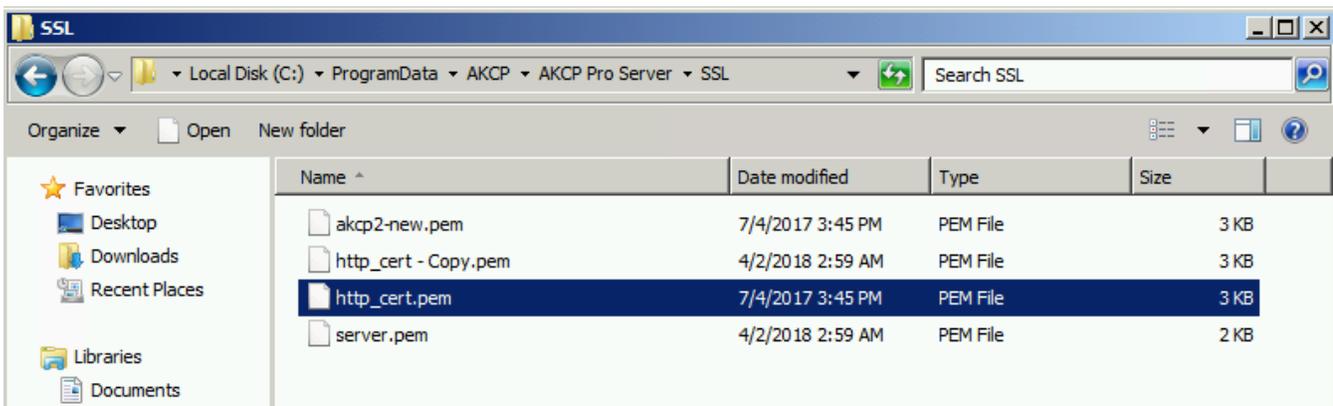

About 3rd party IP cameras. Cannot add the IP camera to the APS software or view the video from the added camera.

#1. Check the port setting on the IP camera and try changing it. Make sure that this port is not blocked by your firewall or antivirus software. If the IP camera uses a non-standard port, it should be specified in the Advanced options, then make sure this matches when adding the IP camera.

#2. Check the HiK Vision and Axis IP camera manuals (contact Support) and make sure the token is disabled.

#3. Make sure the 3rd party IP camera conforms to ONVIF profile S specification. In particular, GetProfiles operation is not supported. This means the APS cannot receive the video streaming URI from the camera.

#4. Check the APS Server Manager to ensure the video service is running. Try stopping and restarting the videoServer.exe service. If this doesn't help, try also restarting the APS service or even the computer.
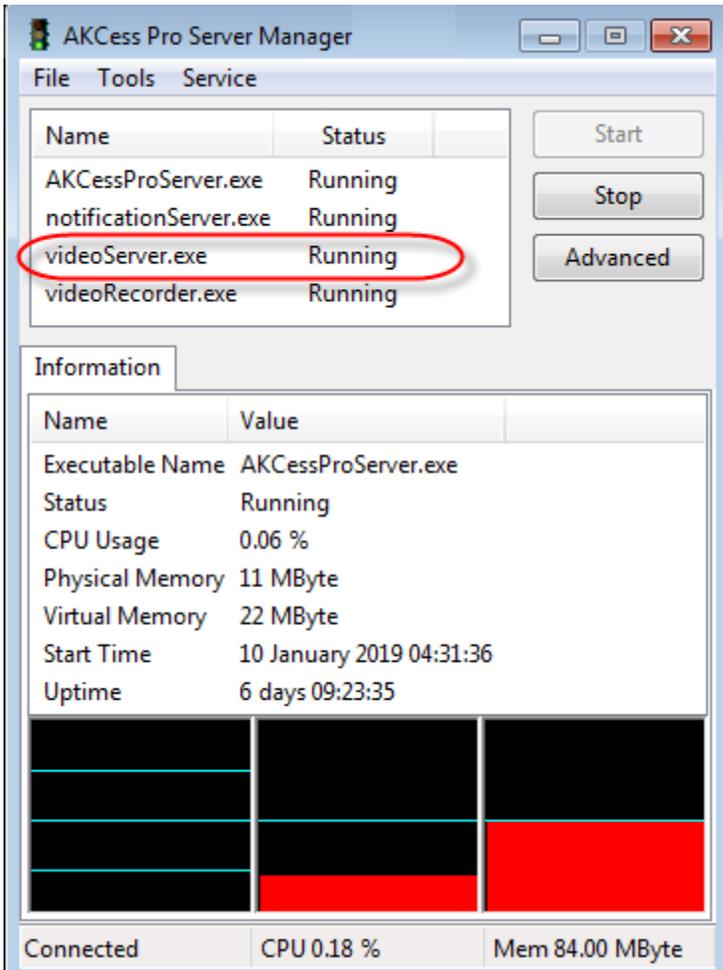
#5. Check the IP camera settings to be sure the IPv6 is NOT enabled on the IP camera.

#6. Make sure you are entering the correct ONVIF username and password for the IP camera.

#7. Make sure your license supports the amount of IP cameras you are trying to add.

Important Note: We do not recommend adding more than 25 3rd party IP cameras to a single server installation and this would be on a high quality server computer with good network bandwidth and fast hard drives or SSDs.

Troubleshoot service restarts, WebUI force-logoff

The likely cause is that APS is reaching the memory threshold limits. When the APS service restarts, WebUI will force-logoff your user.
Try to increase the memory thresholds for increased stability. You should update the values to 500MB in the APS Server Manager utility as follows:
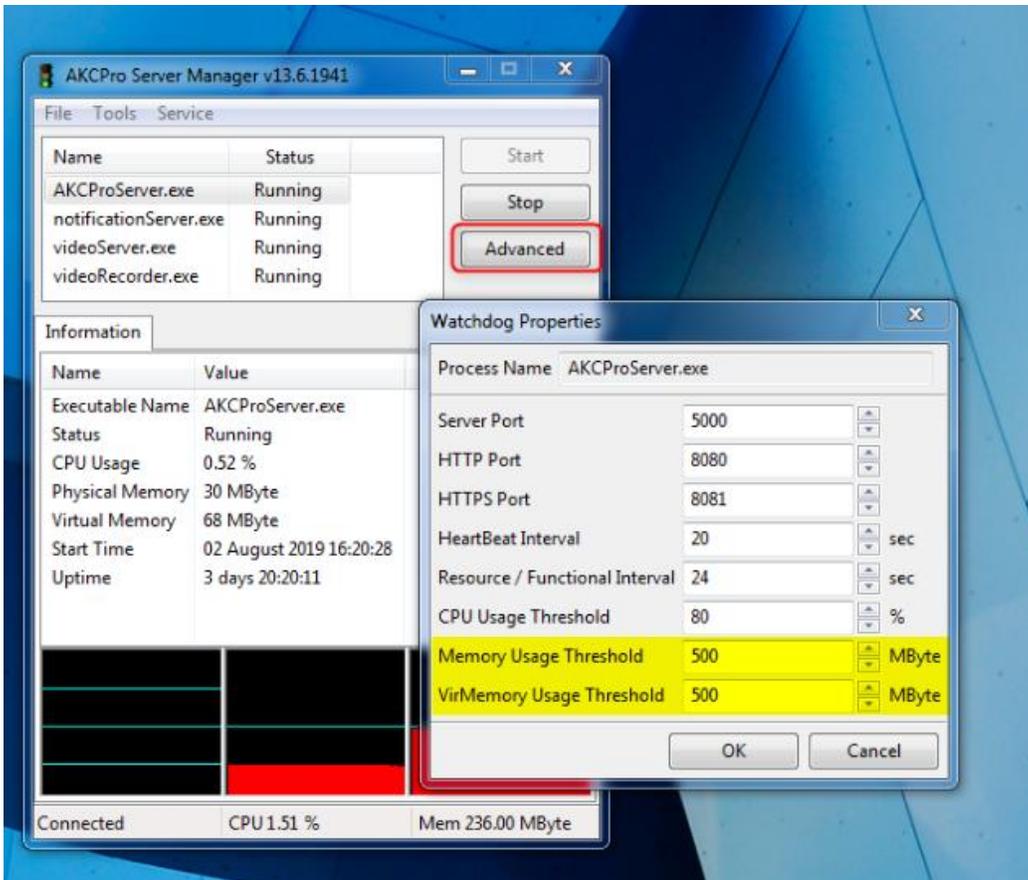
The new values will take effect when the service restarts.

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

Thanks for Choosing AKCP!