



Est. USA 1981

www.AKCP.com

L-DCIM & BOS

Product Manual



DIN rail / Desktop L-DCIM

Table of Contents

| | |
|---|----|
| Introduction | 4 |
| Reset button functions for L-DCIM units..... | 8 |
| Connecting to the unit for the first time | 9 |
| Initial out-of-box configuration | 11 |
| Initial setup steps | 12 |
| Setting up the unit's IP address | 12 |
| Recovery information | 23 |
| Information about software updates | 24 |
| Backup & Restore | 25 |
| Backup | 26 |
| Export backup to external USB | 31 |
| Restore | 35 |
| Server settings | 43 |
| General | 44 |
| Connections | 45 |
| Local Network..... | 46 |
| LoRa Wireless | 47 |
| Wi-Fi..... | 49 |
| Station mode | 50 |
| Access Point mode | 53 |
| Modem..... | 54 |
| SNMP..... | 56 |
| VPN | 58 |
| SMTP Email Alert | 62 |
| Event logs configuration | 64 |
| Notification | 65 |
| NTP - Network Time Protocol | 66 |
| Language | 68 |
| Maintenance | 70 |
| Services | 72 |

| | |
|--|-----|
| Software update | 75 |
| Safe Mode | 76 |
| Firmware Upgrade process..... | 78 |
| Safe Mode Troubleshooting..... | 80 |
| Wireless Sensors | 81 |
| Installation examples | 83 |
| Adding wireless sensors..... | 85 |
| Wireless sensor synchronization | 90 |
| Sync troubleshooting | 94 |
| Wireless sensor parameter setup | 96 |
| Overview | 96 |
| Device..... | 98 |
| Sensors | 101 |
| Network | 111 |
| Incoming packets logger feature..... | 113 |
| Wireless sensor firmware update..... | 118 |
| Firmware Update Over The Air (FOTA) | 118 |
| Firmware update with direct USB connection | 122 |

Introduction

In this manual, we'll only cover the basic configuration of the L-DCIM units and their unique features, such as the wireless sensor support. Please refer to the APS HTML manual for configuring the unexplained parts of the system and for the setup of notifications, as they're identical with the AKCPro Server WebUI.

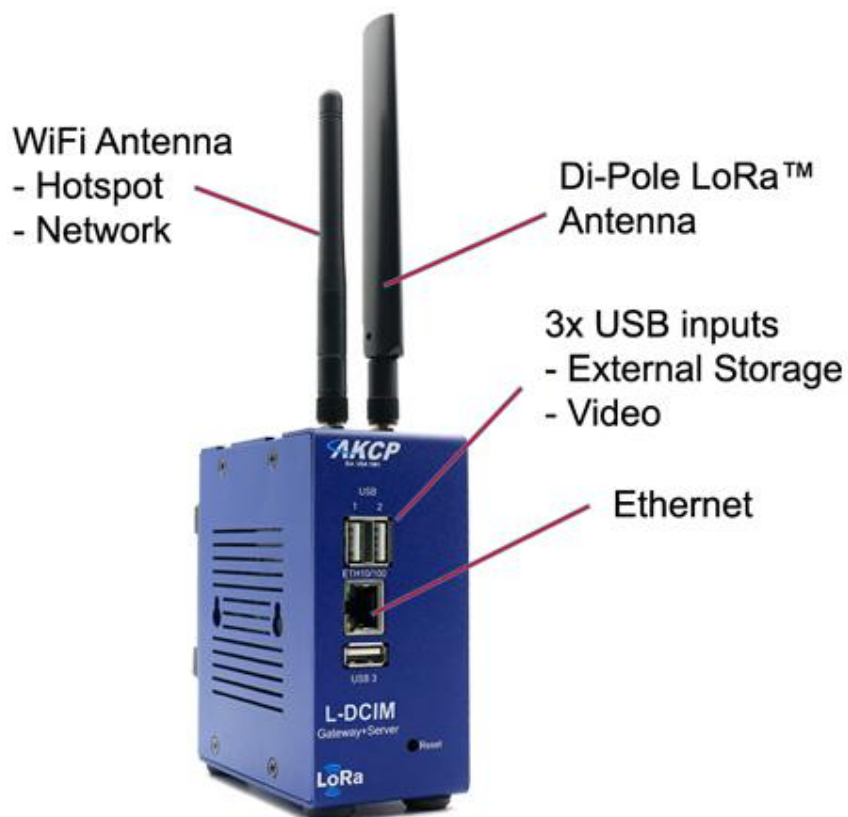
Very important note:

All units come with a **system storage USB flash drive** plugged in to USB port 3.

DO NOT REMOVE THIS USB DRIVE! It contains the AKCPro Server installation and all your user settings and data.

If you remove the USB drive, the unit will stop working until you re-insert the same drive. If the drive gets corrupted and you insert another drive (or reformat the original), the unit will perform a factory reset and all your settings will be lost!

Always perform backups and export your backups to external drive to avoid losing your data (see below about backup & restore features in this manual). The drive is formatted with Linux Ext4 file system partitions and is unreadable under Windows OS, you cannot recover data from it this way.



Important note:

AKCP always highly recommends using a dedicated 3rd party UPS on the units. Any damage caused by unstable power or power outages will void the warranty on our units. The image on the left shows the L-DCIM unit.

What is the L-DCIM?

The AKCP L-DCIM is a “DCIM in a box” solution with embedded AKCPro Server. You can monitor all your network enabled devices such as intelligent PDU’s, UPS’s rectifiers and CRAC units. It supports SNMP, Ping and Modbus TCP/IP virtual sensors. Add sensors connected to AKCP base units for a complete end to end data center monitoring solution.

LoRa™ Radio

L-DCIM is equipped with a LoRa™ wireless radio for connecting AKCP wireless sensors. Easily deploy environmental and security monitoring solutions in hard to reach areas, no cabling, no IP addresses, no power needed.

Tablet View

The L-DCIM has a dedicated tablet view user interface, allowing you to monitor your data center stats with drill down mapping from custom desktops over WiFi while roaming your data center. This allows technicians on the ground to be updated real time and respond to critical alerts immediately.

Important notes:

- Some of the pictures shown in this manual might not represent the actual Web UI of the unit and may refer to the SP+ units or APS; this is because the L-DCIM is a new family of units and its Web UI is basically all the same as for SP+. We are constantly working on improving the firmware; please provide us with feedback if you have any issues configuring your unit.
- All units are shipped with DHCP disabled and the default web interface IP address will be 192.168.0.100. We strongly recommend you change this to avoid problems with duplicate IP addresses on your network. Please see the section in this manual on how to setup a new IP address on the unit.
- The L-DCIM unit is designed for smaller installations with a few devices, and APS on a PC should be used for larger installations (more IP cameras, lot of devices and sensors to monitor etc.)
- You can add any AKCP units to the L-DCIM including SP+, SEC & sensorProbe units but you cannot add a L-DCIM to HTML5 APS on a PC. This might be possible in future releases.
- You cannot have an AKCP unit connected to a L-DCIM and to APS on a PC simultaneously. A warning popup will be shown if you attempt to do so. IP cameras and other network devices however could be connected to multiple APS.
- All AKCP sensors are supported on L-DCIM, except probeSwitch. The 5 Dry Contact Sensors are supported as a licensed feature.

Hardware installation remark: It is recommended to connect the power supply's cable prior to mounting the unit in the rack; otherwise it might be hard for you to connect it while it's mounted. AKCP also always highly recommends using a dedicated 3rd party UPS on the units.

What is the difference between the previous securityProbe (SEC5E, SEC5ES, SEC5ESV etc.) units and the L-DCIM (securityProbe+)?

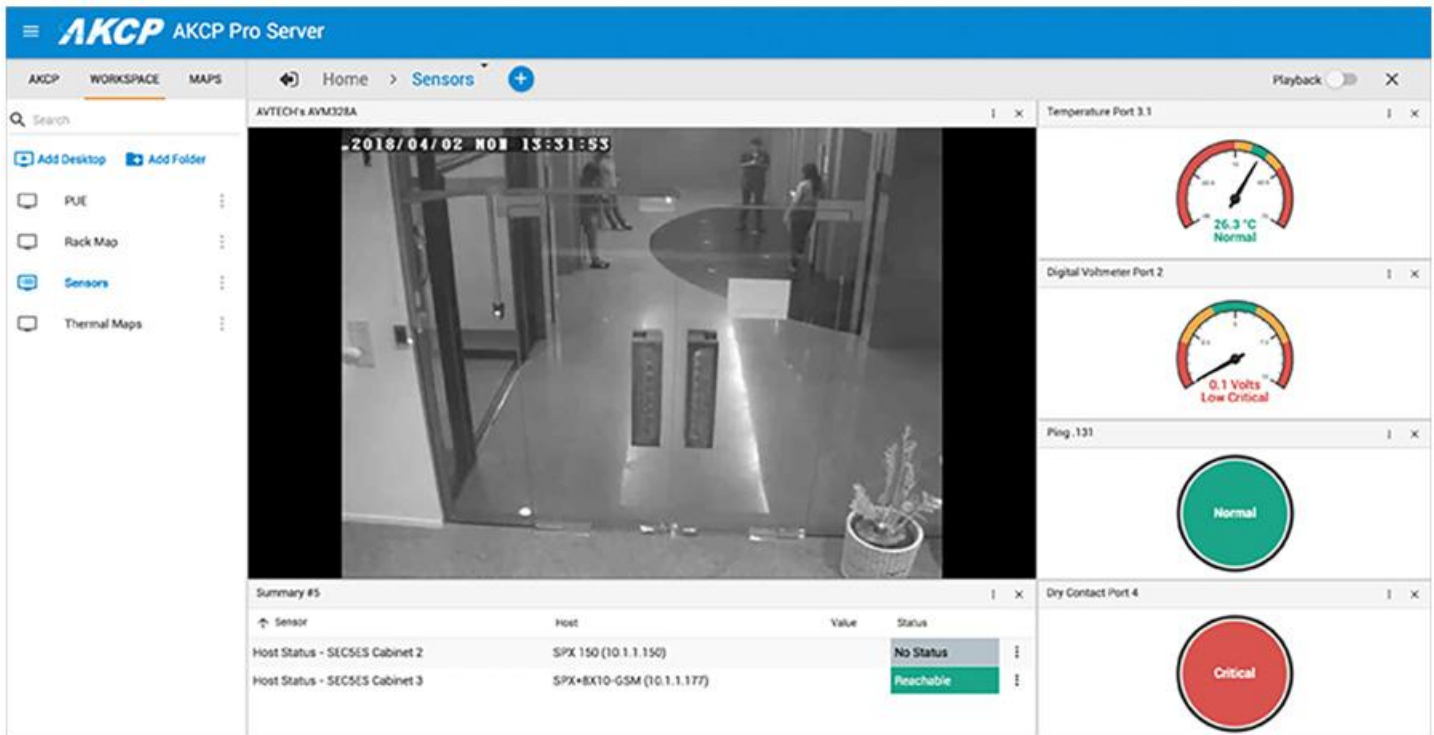
The main difference is that the L-DCIM is running the ported (embedded) AKCPro Server software instead of the previous securityProbe built in web interface. You can think of it as the AKCPro software running on the L-DCIM unit instead of a separate computer server machine.

This not only frees up resources not having to use expensive server computers, but allows you to have the power of the server software running in your server cabinet or rack in a 1U unit.

And like the AKCPro Server you can add and monitor all of your other AKCP units into the L-DCIM units APS application for centralized monitoring from a single L-DCIM unit in your cabinet or server rack.

AKCPro Server Embedded on the L-DCIM

AKCPro Server is our central monitoring and mangement software comes embedded, or ported on the L-DCIM units. **Note:** When upgrading the units image to a new version it is not nessasary to upgrade the Windows AKCPro Server software application that you might have running separatly on your PC. Also, we do not support the IE browser, only Chrom and FF.



Reset button functions for the L-DCIM units



There are specific commands you can send to the unit by holding the Reset button for a specified amount of time.

The Normal Mode and Safe Mode commands are different (see below).

You'll have to use something sharp, such as a straightened paperclip to be able to press Reset.

Commands:

Normal Mode

| Function | Button hold time, sec | LED blink frequency, blinks per sec |
|---|-----------------------|-------------------------------------|
| Show IP (display on LCD sensor too, if connected) | from 0.05 up to 3 | 4 |
| Reboot | from 3 up to 7 | 2 |
| Reset Admin password | from 7 up to 12 | 1 |
| Reboot to Recovery mode | from 12 up to 17 | 0.5 |
| Factory Reset | from 17 up to 25 | 0.25 |

Safe Mode

| Function | Button hold time, sec | LED blink frequency, blinks per sec |
|---|-----------------------|-------------------------------------|
| Show IP (display on LCD sensor too, if connected) | from 0.05 up to 3 | 4 |
| Reboot to Regular mode | from 3 up to 7 | 2 |
| Factory Reset | from 7 up to 12 | 1 |

Connecting to the unit for the first time

Very Important Note: The units **require** you to enter passwords to access the web interface every time. Unlike other SP+ units, this cannot be disabled.

The default log in is Username: *admin* Password: *admin*

Every unit is shipped with the default IP address of **192.168.0.100 and DHCP disabled.**

In the next section in this manual we will go through the process of changing this IP address to fit your own network configuration.

Note: In some cases your computer might not be able to connect to this default IP address. In this situation you either need to:

- a) check your DHCP server (or router, if any) for the automatically assigned IP address
- b) add the default IP your computers routing table or
- c) add a secondary IP address to the LAN card to allow access to the unit.

See below how to setup these.

Ensure the following items are available to you before starting:

- RJ45 CAT5 crossover cable with RJ45 male connection (straight cable should also work, depending on your LAN card)
- A PC with Ethernet card or LAN socket, logged in with Administrator rights
- Stable power source for the unit (UPS)

1) Connect the unit via the Ethernet port of the unit to your computers LAN or Ethernet port with a CAT5 crossover cable.

2) Proceed to the next section in this manual: Initial out-of-box configuration

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

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

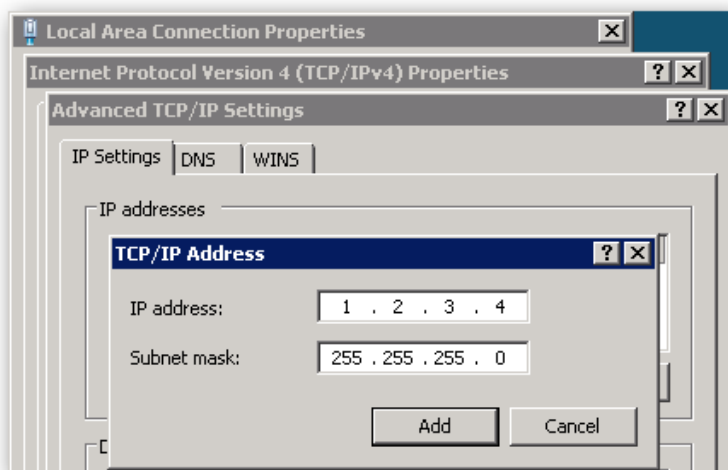
```
route add 192.168.0.100 10.1.1.20
```

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

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

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

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



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

```
netsh interface ipv4 add address "Local Area Connection" 192.168.0.2  
255.255.255.0
```

The above command adds the IP Address 192.168.0.2 (with Subnet Mask 255.255.255.0) to the connection titled "Local Area Connection".

You will then be able to connect to the unit with its default IP.

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

Initial out-of-box configuration

L-DCIM Initial setup steps

Connect all cables to L-DCIM, arrange the antennas and power it on. It can take a few minutes before the system gets ready for the first time.

During startup, L-DCIM will check the system USB drive, and format it again if necessary - this will also add to the boot time, please be patient.

You can already point your browser to the unit's default IP address, and it will open when the system is ready.

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.

Important Note: All of the newer versions (from 2020 on) of the third party web browsers, including Chrome will eventually 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.

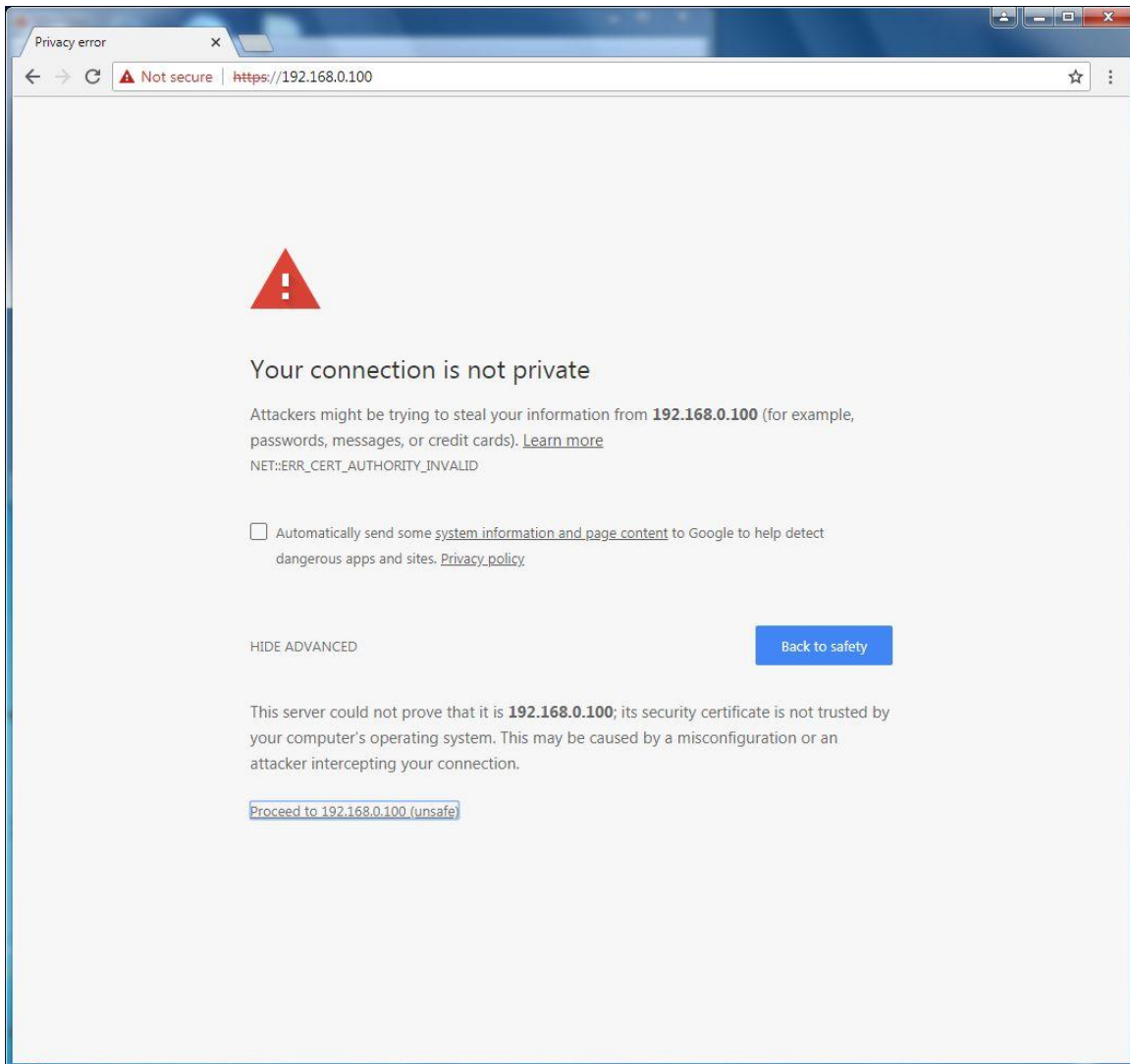
The first is to simply use HTTP and not HTTPS.

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

Note: The following steps are also required after you perform a factory reset using the Maintenance menu on the unit.

If you have the unit directly connected to your PC via a LAN cable: Open the Web UI with default IP 192.168.0.100

In this example we're using direct cable connection, so we'll open the default IP:
192.168.0.100



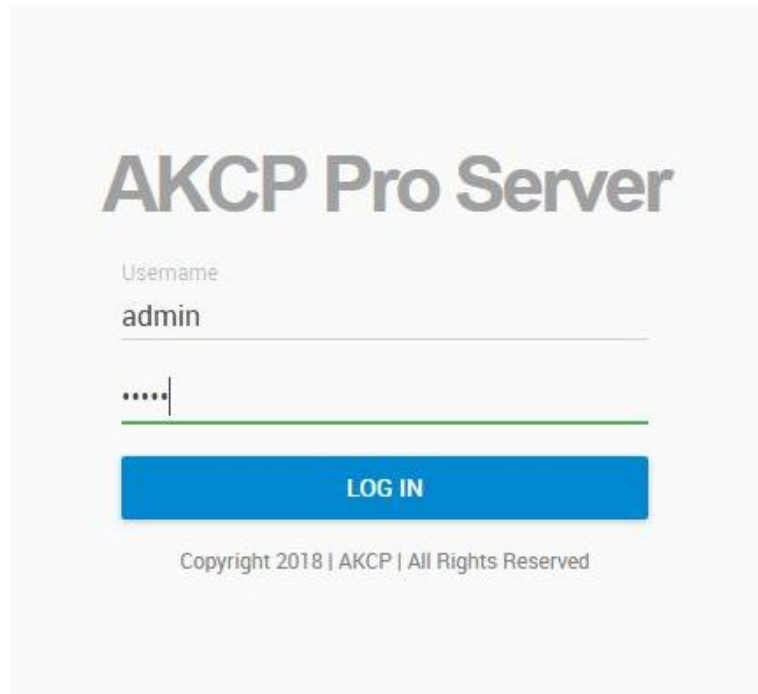
The unit's login page defaults to HTTPS protocol. It's using a self-signed certificate and you'll need to accept that to continue. This is depending on your browser, Chrome is shown as an example.

Advanced

Back to safety

Click the **Advanced** button and then **Proceed to 192.168.0.100 (unsafe)**.

You can replace the SSL certificate to eliminate the browser warnings, or enable the HTTP port. Please see page #11 above if you are having problems with the browser connection or log in errors.



The login page will load. It is necessary to log into the system every time the Web UI is accessed. The default login name and password is:
admin / admin.

Important Notes: If you are having trouble connecting for the first time to the L-DCIM from your laptop or PC when the unit is directly connected using the yellow cross over cable.

First, you must allow at least 20 to 30 minutes for the USB stick drive connected to port #3 to be formatted and the other system files to be installed to complete the initial setup (done automatically).

Secondly, make sure that the LAN extension cable from your PC or laptop is not faulty. You can use either the cross over, or straight through LAN cable as the Ethernet port on the L-DCIM will detect and handshake (connect) accordingly.

Third, check to make sure you have configured your PC or laptop's LAN adapter IP address correctly, for example 192.168.0.101. Four, temporally disable the Windows firewall and antivirus on your PC.

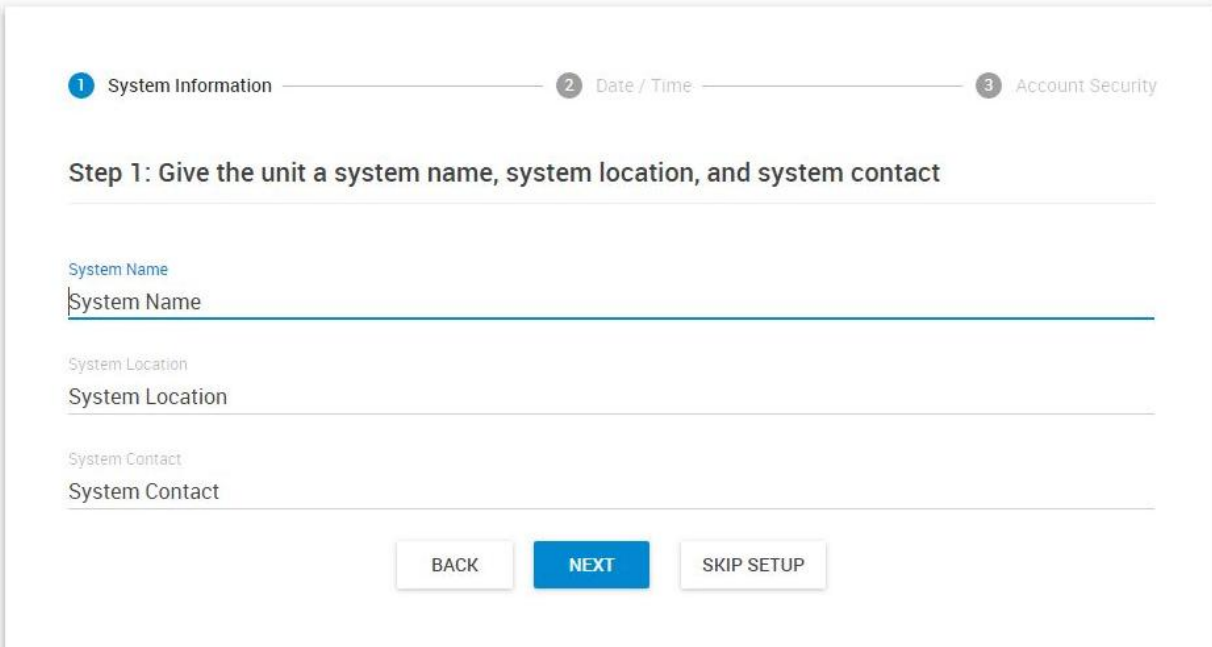
LinuxIPSet

You can also check to make sure the unit has been assigned the default IP address by using the LinuxIPSet version 6.0.0. Run the LinuxIPSet (firewall & antivirus disabled) then push the reset button once on the L-DCIM. This will display the IP address assigned to the L-DCIM in the LinuxIPSet.

The LinuxIPSet utility ver. 6.0.0 can be downloaded from our website via the support portal. Here is the direct link: <http://www.akcp.in.th/downloads/Firmwares/lnuxIPSet6.0.0.zip>

Welcome to AKCP Pro Server Setup

In the next few screens, we will help you set up your system information, date/time, and account security. This simple process takes only a few moments to get your unit fully functional and ready to go.



The screenshot shows the first step of the setup wizard. At the top, there are three numbered steps: 1. System Information (active), 2. Date / Time, and 3. Account Security. Below the steps, the title "Step 1: Give the unit a system name, system location, and system contact" is displayed. There are three input fields: "System Name", "System Location", and "System Contact". Each field has a label above it and a text input area below it. At the bottom, there are three buttons: "BACK", "NEXT" (highlighted in blue), and "SKIP SETUP".

Now the initial setup wizard will load.
Here you can set the basic parameters for the device.

Note: If you skip the setup with the “Skip Setup” button, the default values will be used. These can be later modified using the system menus.

You can also skip the setup if you plan to restore a backup from USB drive, since the backup will contain these parameters.

How to run the setup wizard again?

If you wish, you can run the initial setup wizard again by going this URL: /app.html/setup
For example, with the default IP the full link will be: <https://192.168.0.100/app.html/setup>

Welcome to AKCP Pro Server Setup


In the next few screens, we will help you set up your system information, date/time, and account security. This simple process takes only a few moments to get your unit fully functional and ready to go.

✓ System Information

2 Date / Time

3 Account Security

Step 2: Choose the appropriate date/time and time zone



Date

Friday 22/06/2018

Time

1:29 pm

Timezone

(GMT+07:00) Bangkok, Hanoi, Jakarta

BACK

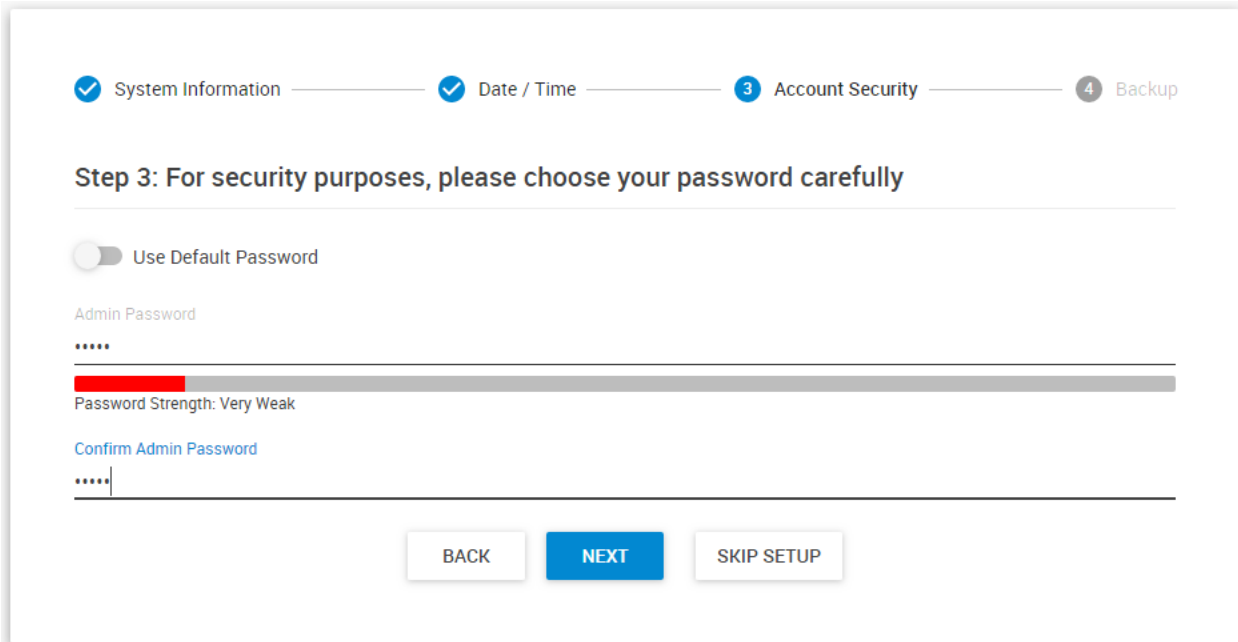
NEXT

SKIP SETUP

The timezone should be auto-detected from the browser. It can slightly differ from the actual zone but the time should display correctly.

Correct it if necessary.

Note: system upgrades might reset your timezone back to UTC time. It is recommended to re-check and correct your timezone after doing any updates.



☒ System Information
 ☒ Date / Time
 ☒ 3 Account Security
 ☐ 4 Backup

Step 3: For security purposes, please choose your password carefully

☐ Use Default Password

Admin Password

.....

Password Strength: Very Weak

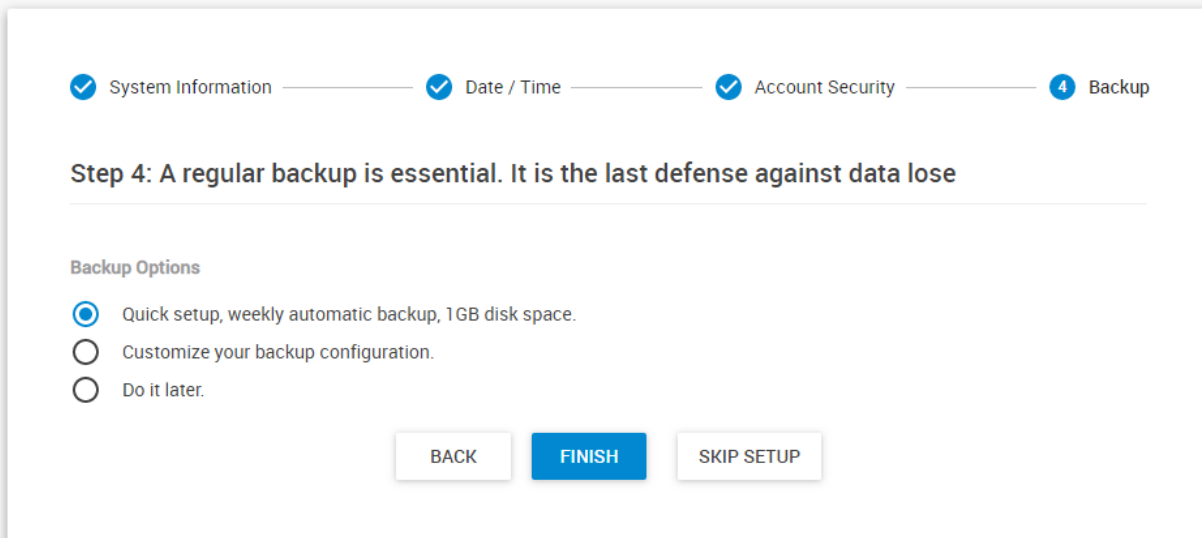
Confirm Admin Password

.....

BACK
 NEXT
 SKIP SETUP

Next specify a different password for the default admin user.

A password strength meter helps to choose a strong password, but it's not enforced - you can use weak password at your own risk.



☒ System Information
 ☒ Date / Time
 ☒ Account Security
 ☒ 4 Backup

Step 4: A regular backup is essential. It is the last defense against data lose

Backup Options

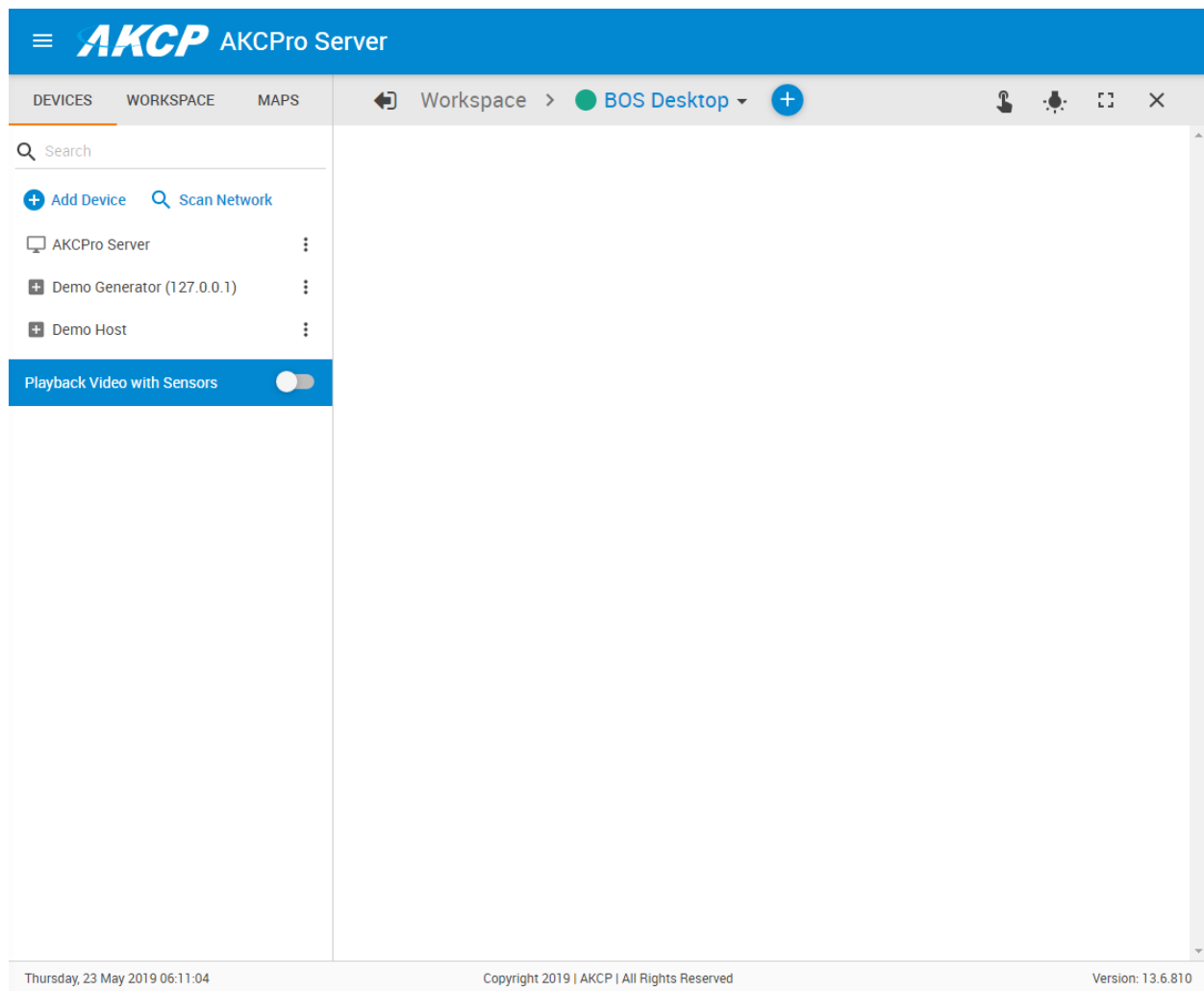
☒ Quick setup, weekly automatic backup, 1GB disk space.
 ☐ Customize your backup configuration.
 ☐ Do it later.

BACK
 FINISH
 SKIP SETUP

As the final step, the unit will ask you to set up the backup options.

As noted earlier, the backups are essential to safeguard against losing your data - don't forget to also regularly export the backup files to external media!

You could accept the default quick setup setting or customize the backup options, or skip it altogether at your own risk.



The default empty Web UI will load, which is very similar to a Windows HTML5 APS desktop.

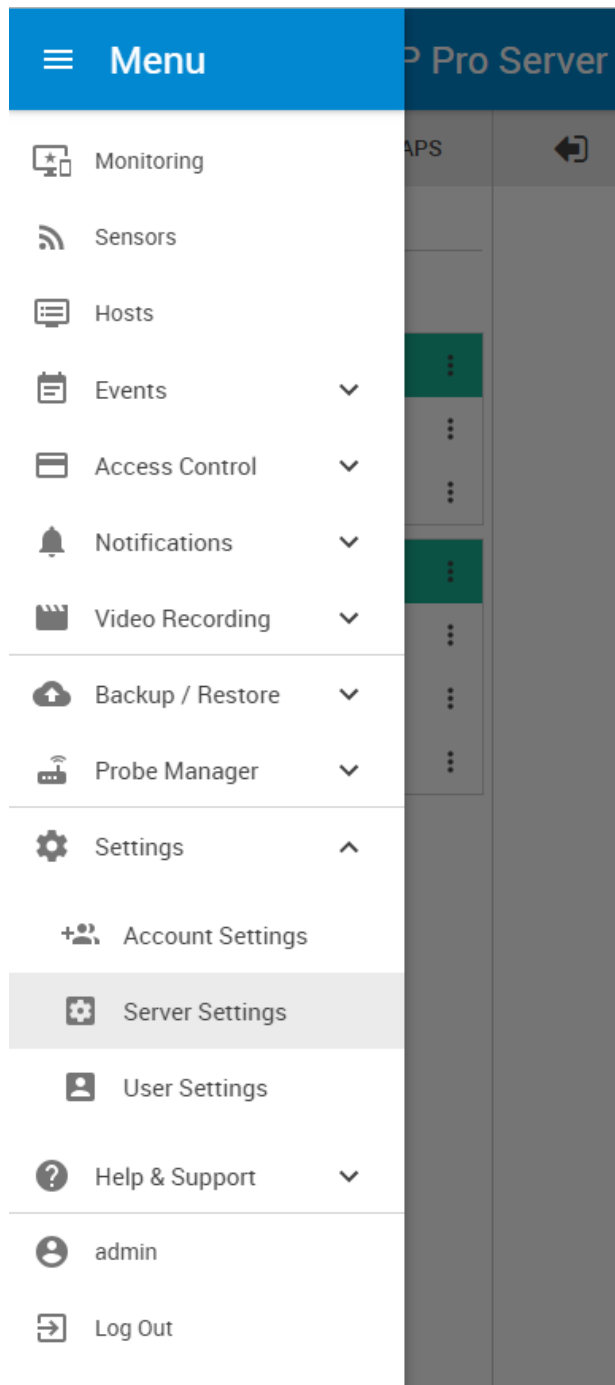
A tutorial will run to show you the basics of UI navigation. You may either proceed with the tutorial or skip it. Similar tutorials will be shown for various menu options as you navigate the UI.


Demo hosts

You'll see two hosts for demonstration purposes: a demo host and a demo generator. You can use them for trying out various features, setting up notifications and actions etc. They even have dedicated Desktops which serve as additional tutorials.

Important: before adding real devices and sensors to L-DCIM, after you've checked the demo host and generator, it is recommended to remove them because the system logs will be full of demo events logged from these hosts.

Setting up the unit's IP address



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

Important: We'll only describe the unique L-DCIM WebUI elements in details in this manual. All other menus and UI elements can be found in our separate APS HTML manual.

Please refer to that manual if you need help navigating the menu.

Go to the **Settings menu / Server Settings / Local Network page** to configure a different IP address for the unit.

☰

AKCP Pro Server

Server Settings

General

Connections

Local Network

Wi-Fi

SNMP

VPN

Event Logs

Notification

NTP

Language

Maintenance

Services

Software Update

Local Network

Settings / Server Settings / Local Network

☒

Enable DHCP

↻

IP Address

192.168.0.100

Subnet Mask

255.255.255.0

Gateway

SET THIS GATEWAY AS DEFAULT

Default Gateway

PING

MAC Address : B8:27:EB:3F:8E:5D

SAVE

CANCEL

Friday, 22 June 2018 13:30:14

Copyright 2018 | AKCP | All Rights Reserved

Version: 13.0.408

Settings menu / Server Settings / Local Network page

Here you can configure a different IP address for your unit. The default settings are as follows:

1. If a DHCP server is used on the network, the auto-assigned IP settings should display (see below).
2. If a direct connection to the PC was used, the default IP 192.168.0.100 should display (as on this screenshot above).

Note that L-DCIM currently only supports IPv4 addressing.

Dynamic IP (DHCP)

Local Network

Settings / Server Settings / Local Network

☒ Enable DHCP ↻

IP Address

10.1.6.37

Subnet Mask

255.255.255.0

Gateway

10.1.6.2

SET THIS GATEWAY AS DEFAULT

Default Gateway

10.1.1.2

PING

MAC Address : 02:81:7A:D2:5F:E1

SAVE

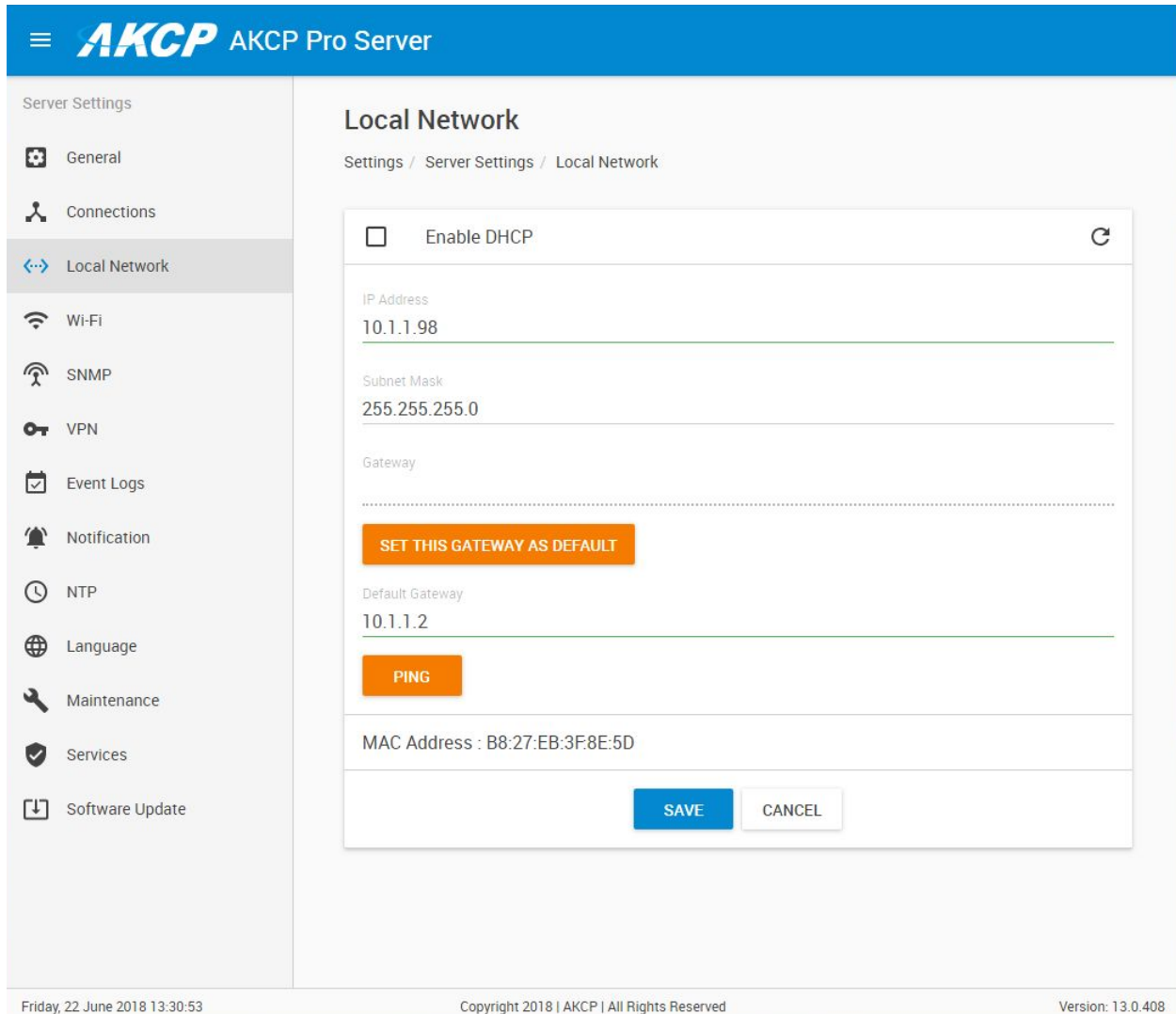
CANCEL

This is the default setting; the unit should display the dynamically assigned IP address, subnet and gateway settings from the DHCP server.

These are displayed for your reference for connecting to the unit by its DHCP IP address.

You may want to set up IP address reservation for L-DCIM (so that it always gets the same IP from DHCP), or assign a DNS hostname for it. Contact your network administrator for setting these up.

Static IP



AKCP Pro Server

Server Settings

- General
- Connections
- Local Network**
- Wi-Fi
- SNMP
- VPN
- Event Logs
- Notification
- NTP
- Language
- Maintenance
- Services
- Software Update

Local Network

Settings / Server Settings / Local Network

☐ Enable DHCP

IP Address
10.1.1.98

Subnet Mask
255.255.255.0

Gateway

SET THIS GATEWAY AS DEFAULT

Default Gateway
10.1.1.2

PING

MAC Address : B8:27:EB:3F:8E:5D

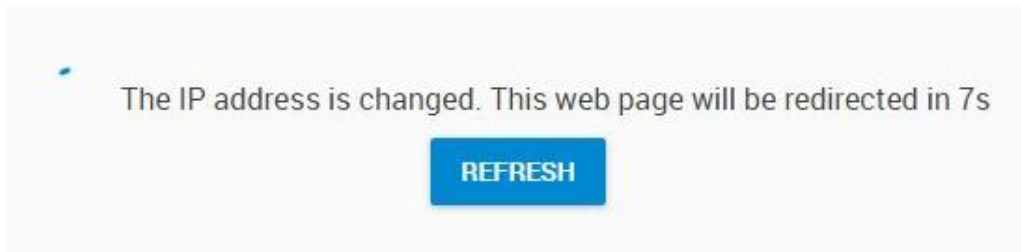
SAVE CANCEL

Friday, 22 June 2018 13:30:53 Copyright 2018 | AKCP | All Rights Reserved Version: 13.0.408

You can change the LAN IP to static on the Local Network page this way:

1. Clear the checkbox from the option "Enable DHCP"
2. Enter the static IP, netmask and Gateway IPs
3. Click Save

Note: you can only enter the new gateway as Default Gateway



After you click **Save**, the unit will save the new IP address and redirect the browser there. You'll need to re-login again because of the IP change.

Very Important Note: do not unplug the network cable until at least 60 seconds! If you remove the cable too early, the new IP settings won't be saved correctly and you cannot access your unit.

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

Important information: after setting up the new IP, the unit *has to be left turned on for at least 10-15 minutes without rebooting*. The changes you made are just saved to a temporary database, and it takes at least 10 minutes for these changes to be written to the DB stored on the flash storage. The Safe Mode's IP settings are programmed to EEPROM storage during this time. If you don't keep the system running for at least 10 minutes, the Safe Mode's IP address will still be on the default DHCP setting.

The same rule applies when you do a *Factory Reset from a working system with a fixed IP*: first the IP address will be the previous fixed IP, as used in Safe Mode and read from EEPROM. But if you reboot back to Normal mode you'll see the IP address setting is changed back to DHCP mode in the system settings. If you don't change this back to the correct fixed IP value, then after 10 minutes the unit will set the DHCP setting to the EEPROM and to Normal mode, and upon reboot you might have a problem accessing the Web UI. So always be sure to check and re-set your fixed IP when doing a Factory Reset.

Recovery information

There is a “**Restore factory defaults**” option under the Maintenance menu (and by using the Reset button) which will restore all settings to default (including the IP address) and removes any applied APS updates. You’ll need to set up the unit again from the start and reapply any software updates.

The units have a special boot mode: **Safe Mode**. You can perform factory reset and system firmware update with Safe Mode. We’ll describe using it below in this manual.

Backup & Restore works the same way as in the APS PC version, except that backups can be only made on the unit’s internal USB drive. You can then import/export the backup files using additional USB drives. We’ll explain the backups in more detail in this manual.

Important: always export your backups to external drives too.

If the unit’s **system storage USB drive** gets corrupted and not readable, you can usually recover your configuration by inserting a known good drive while the system is still running and not rebooted. Restoring an exported backup configuration might still be necessary.

If you remove the USB drive, the system will display a warning message that the USB drive is removed. You’ll need to insert the same drive or a new drive to the same USB port before the system can resume normal operation. If the SMTP notification is set up (see below) you’ll get a warning about the removed system USB drive.

LinuxIPSet can be used only for getting the unit’s IP address. There is no recovery feature using this utility.

WebUI password recovery should work the same way as on SP+ units, by pressing the Reset button for no more than 3 seconds.

To enter Safe Mode using the Reset button:

Power on the unit and then press and hold Reset button for about 8-10 seconds. This will boot the unit to Safe Mode directly.

Important: don’t press Reset before you apply power, as this might cause the unit to not be able to turn on properly.

Information about software updates

System update

Any system updates are done via an *aps-installer.deb* file that can be either uploaded via HTML or via USB drive. This package contains updates to the APS software, and also contains any firmware updates necessary for the device.

The Linux OS can be updated from Safe Mode (see below) via a special image file. Your configuration and settings will be kept intact.

Always make backups and export them to another USB drive before you attempt any updates!

Wireless sensor firmware updates

Wireless sensor firmware can be updated in 2 ways:

- Firmware Update Over The Air (FOTA)
- Firmware update with direct USB connection to the L-DCIM unit (faster)

We'll describe the steps below in this manual.

Important Note: Also see our separate manual titled "L-DCIM Upgrade How To" in the All Manuals >> L-DCIM Manuals section on our support website page.

Backup & Restore

Backing up your system's configuration is essential. The Backup and Restore feature is built-in to the unit, 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.

After setting up the unit's IP address, we recommend you to configure the backup immediately.

It is the end user's responsibility to always make backups and export them to external media to avoid possible data loss! Your data and settings will be lost if the system USB drive has any problems and you did not make backups and export them!

Review this section carefully and set up your backup configuration!

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.

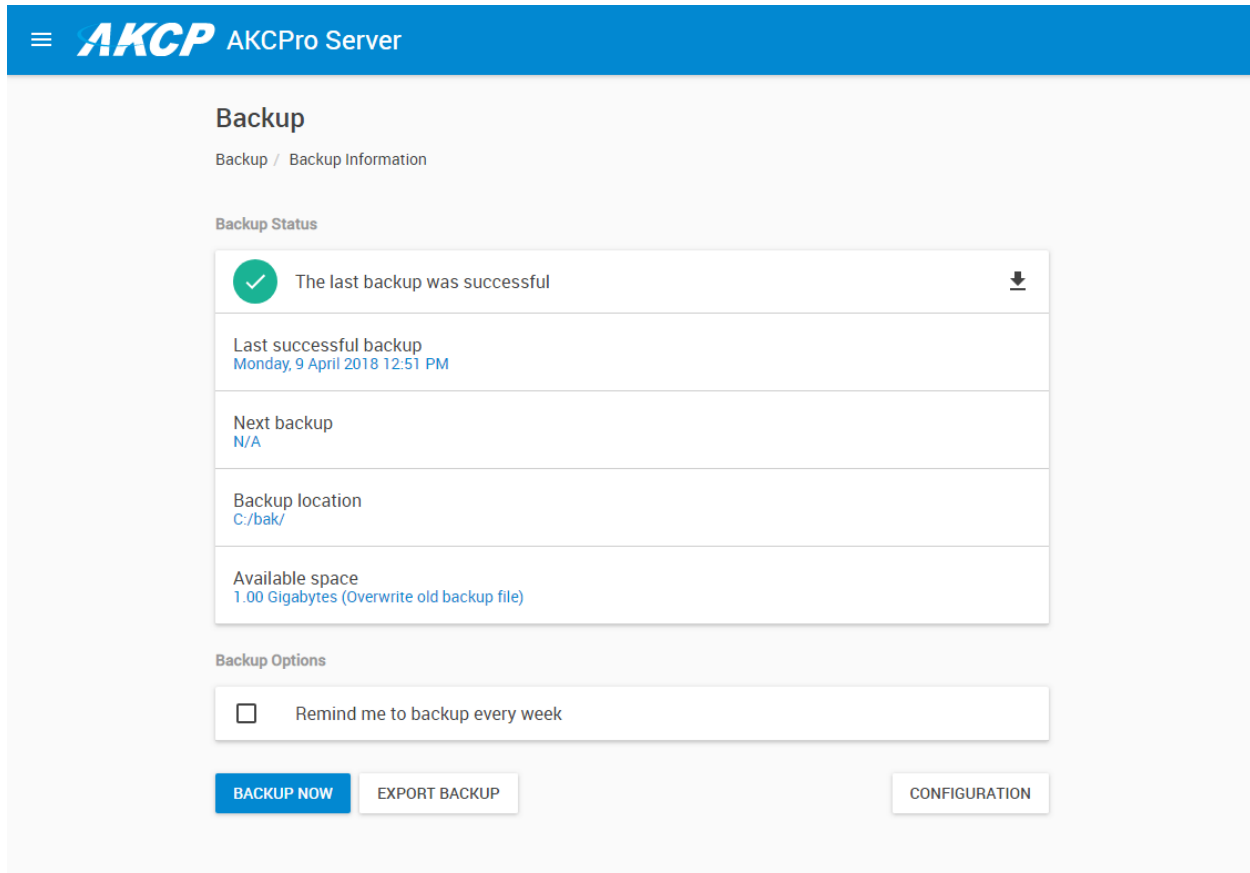
Note: you must log in with the Admin account to APS, otherwise you won't be able to see or use the Backup and Restore feature.

Note for wireless sensors:

When you restore a backup, the connected wireless sensors might display as "unreachable". This is expected because for the system, the last received radio packet timestamp has been sent a long time ago.

The sensors will return to normal state and display correctly again, when their pre-set packet sending interval has been reached (normally 15 minutes) or if you manually press the Mode button on the sensor to force-send a data packet immediately.

Backup



The screenshot shows the 'Backup' page of the AKCPPro Server interface. At the top is a blue header with the AKCP logo and 'AKCPro Server'. Below the header, the page title 'Backup' is followed by a breadcrumb 'Backup / Backup Information'. The main content area is titled 'Backup Status' and contains a white box with a green checkmark icon and the text 'The last backup was successful'. Below this, there are four rows of backup information: 'Last successful backup' (Monday, 9 April 2018 12:51 PM), 'Next backup' (N/A), 'Backup location' (C:/bak/), and 'Available space' (1.00 Gigabytes (Overwrite old backup file)). Below the status box is a 'Backup Options' section with a checkbox labeled 'Remind me to backup every week'. At the bottom, there are three buttons: 'BACKUP NOW' (blue), 'EXPORT BACKUP' (white), and 'CONFIGURATION' (white).

Backup

Backup / Backup Information

Backup Status

✓ The last backup was successful

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

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 (Note that some images will show the Windows APS Web UI).

By default the backup is not configured, so you'll need to click on the **Configuration** button first.

AKCP

AKCPro Server

Backup Configuration

Backup / Backup Configuration

1 Backup Options

2 Backup Schedule and Password

Backup Options

Where do you want to store the backup?

C:/bak/

BROWSE

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.

BACK

NEXT

CANCEL

AKCP

AKCPro Server

Backup Configuration

Backup / Backup Configuration

1 Backup Options

2 Backup Schedule and Password

Backup Options

Where do you want to store the backup?

/var/opt/aps-home/Backup

BROWSE

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.

BACK

NEXT

CANCEL

Server

var/opt/aps-home/Backup

CANCEL OK

First, choose your backup directory where you want to store the backups with the **Browse** button.

On the L-DCIM units currently *only one location is supported* for selecting the backup target.

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.
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.

Backup Configuration

Backup / Backup Configuration

✓ Backup Options

2 Backup Schedule and Password

Backup Schedule and Password

How often do you want to create a backup?

How Often

Never

Backup password protection (Optional)

* Please remember your password, you will require this to restore the system.

BACK

FINISH

CANCEL

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:

How often do you want to create a backup?

Never

Yearly

Monthly

Weekly

Daily

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

Export backup to external USB

Export Backup

Backup / Export Backup

1 Backup Selection

2 Export Output

3 Export Progress

Backup Selection

Choose the directory of the backup file

C:/bak/ BROWSE

Choose the backup file

BackUp_2018_09_11_13_24_15.bak

File Name: BackUp_2018_09_11_13_24_15.bak
Backup Date: 2018-09-11 1:24:15 PM
MAC Address: 00-15-5d-01-6e-2c
IP Address: 192.168.16.1
Include Video: No

BACK
NEXT
CANCEL

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.

Choose the backup file

BackUp_2018_09_11_13_24_15.bak
BackUp_2018_04_09_12_51_00.bak

MAC Address: 00-15-5d-01-6e-2c

On the first screen **you only need to select the backup file you want to export.**

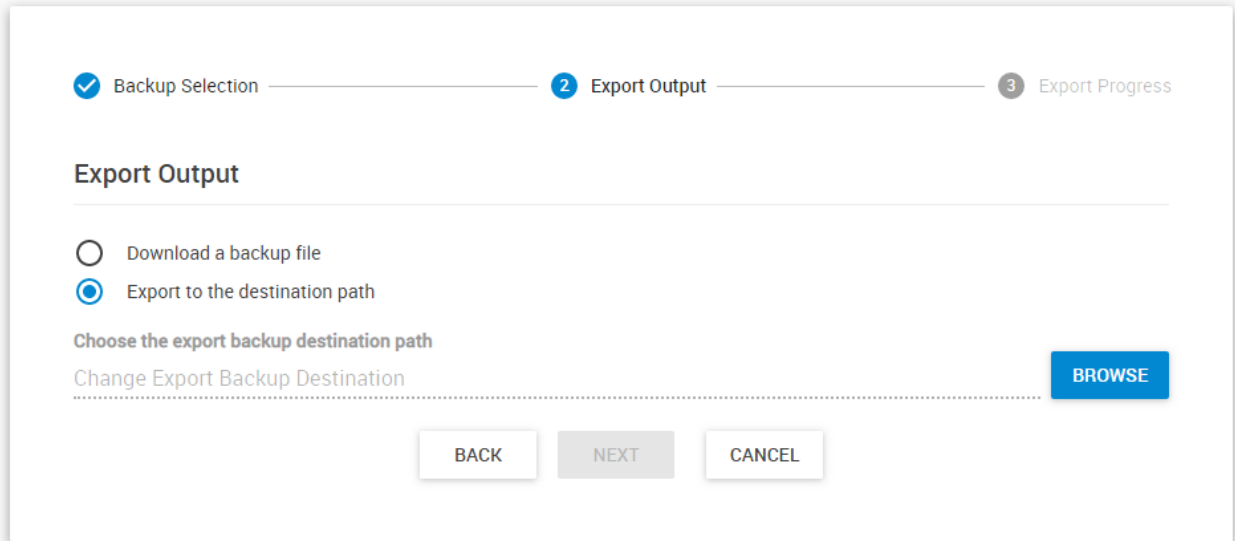
The backup file source path should be automatically selected.

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).

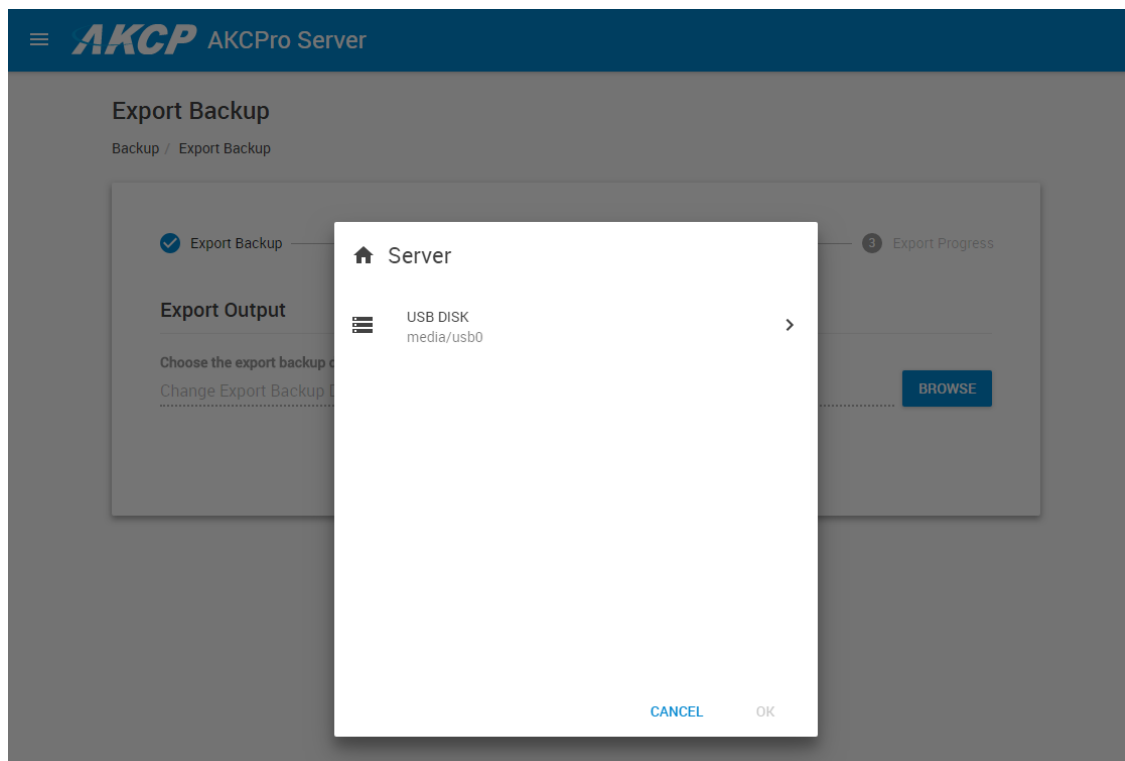
Export Backup

Backup / Export Backup

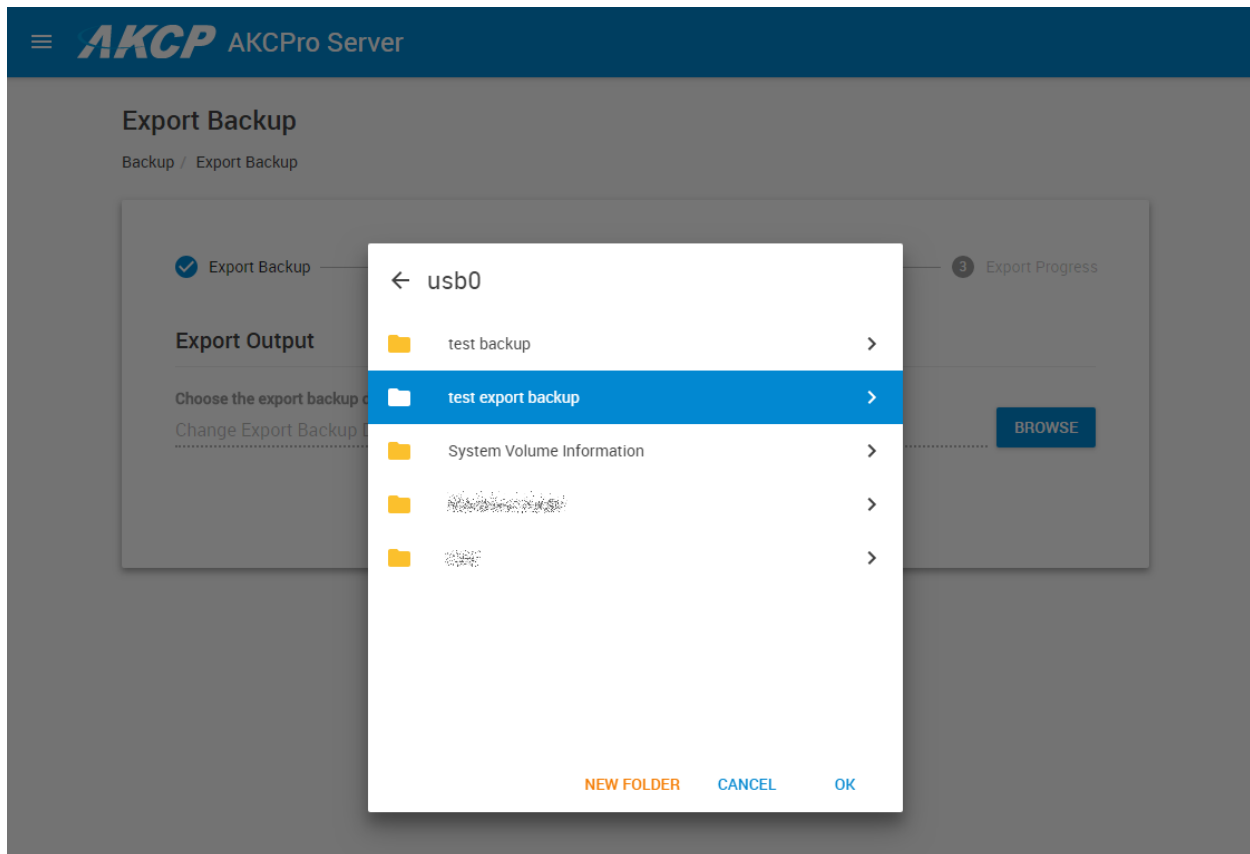


The dialog box shows a progress bar with three steps: 1. Backup Selection (checked), 2. Export Output (active), and 3. Export Progress. Under the 'Export Output' section, there are two radio buttons: 'Download a backup file' and 'Export to the destination path' (selected). Below these, there is a text input field labeled 'Choose the export backup destination path' with a 'BROWSE' button to its right. At the bottom, there are three buttons: 'BACK', 'NEXT', and 'CANCEL'.

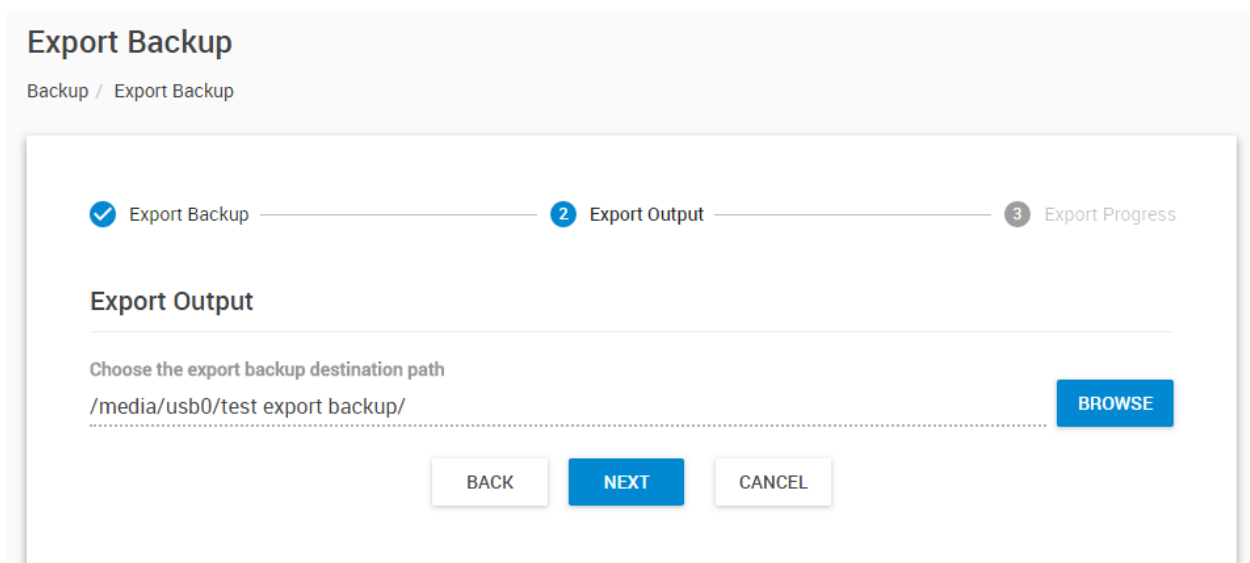
Here you can either **download the backup file** (important: usually this only works with HTTP protocol enabled) or **choose the export folder** where you want to copy the backup file to on your USB drive with the **Browse** button:



Open the USB drive's folders with the > button.



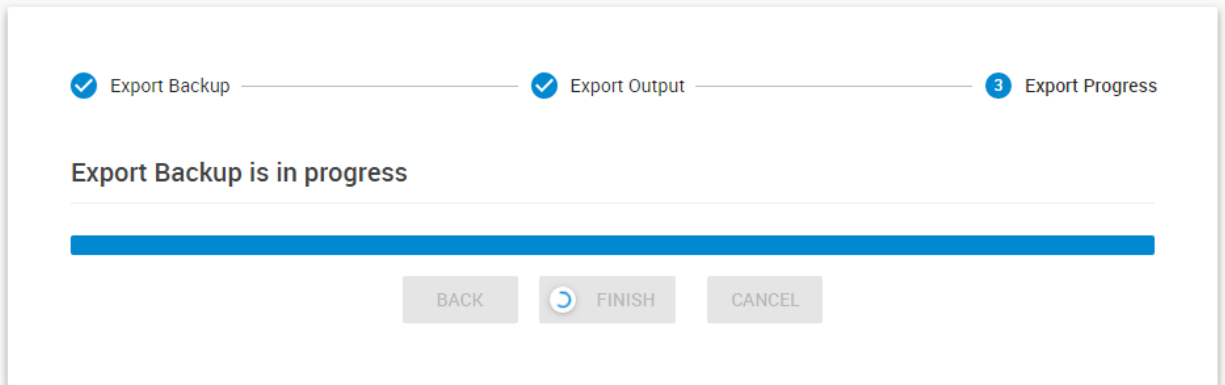
Highlight only the folder where you want to place your backup into; don't go inside the folder itself. You could also create a new folder if necessary. Click **OK** when done.



Your Export Output path will show the destination folder on your USB drive. Click **Next** to begin.

Export Backup

Backup / Export Backup



The screen shows a progress bar that is almost full. Above the progress bar, the text "Export Backup is in progress" is displayed. At the top, there are three steps: "Export Backup" (checked), "Export Output" (checked), and "Export Progress" (active, indicated by a blue circle with the number 3). At the bottom, there are three buttons: "BACK", "FINISH" (with a circular arrow icon), and "CANCEL".

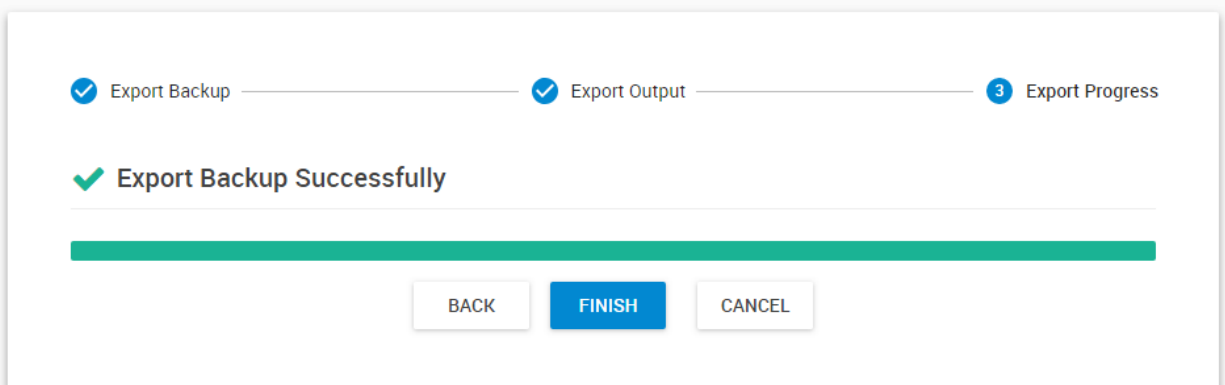
Now the backup export has started.

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.

Export Backup

Backup / Export Backup



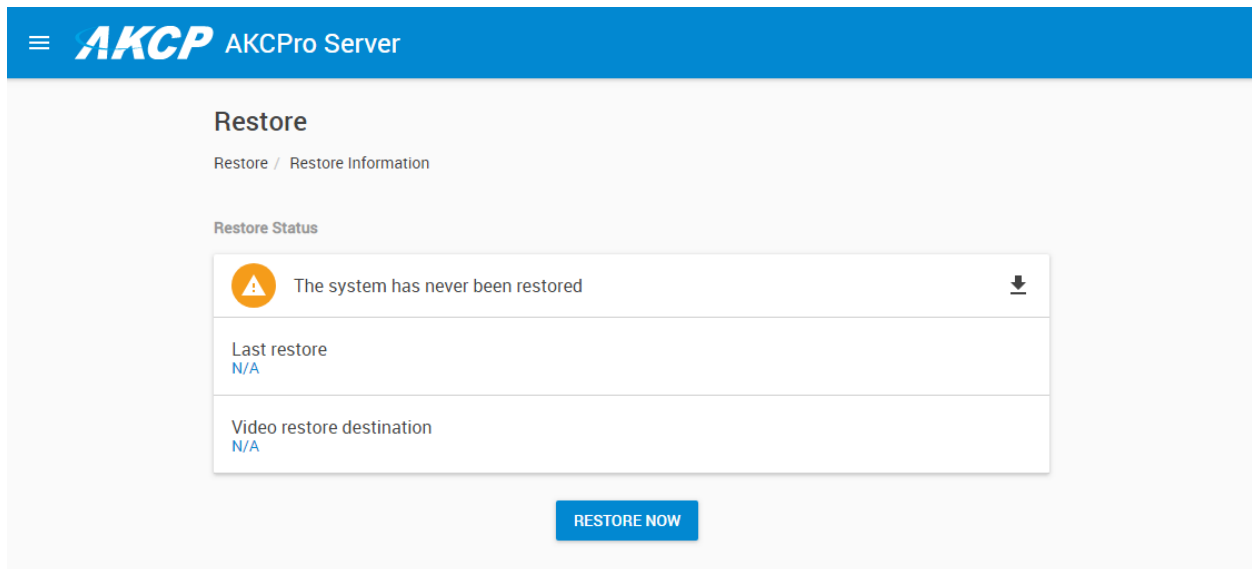
The screen shows a progress bar that is completely full and green. Above the progress bar, the text "Export Backup Successfully" is displayed with a green checkmark icon. At the top, there are three steps: "Export Backup" (checked), "Export Output" (checked), and "Export Progress" (active, indicated by a blue circle with the number 3). At the bottom, there are three buttons: "BACK", "FINISH" (highlighted in blue), and "CANCEL".

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.

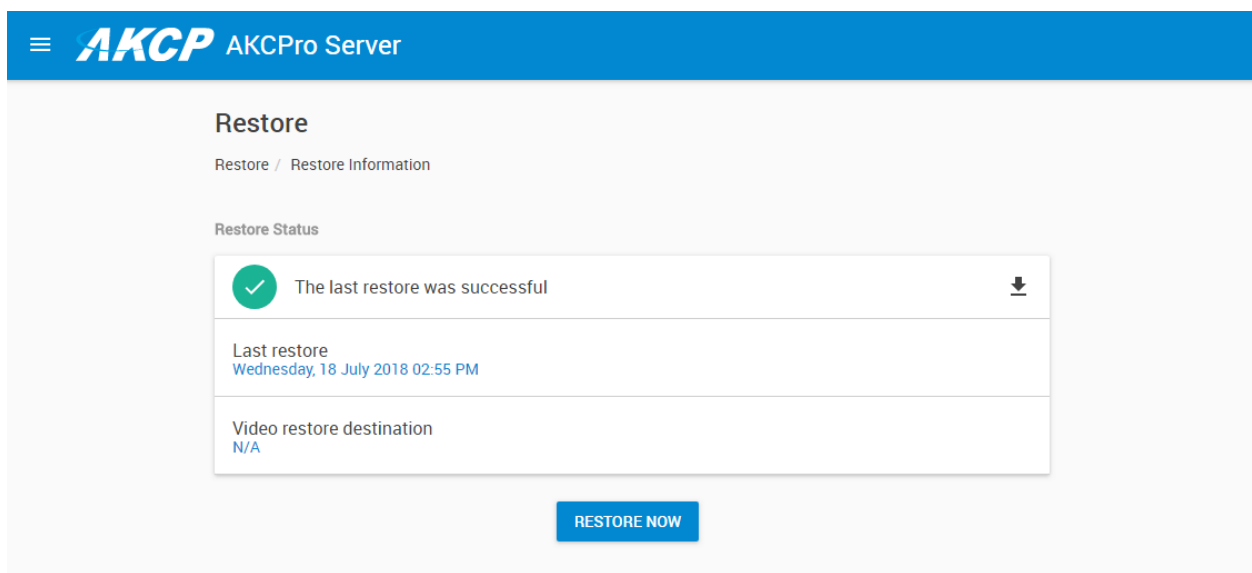
Important note: because backups are “snapshots” you’ll lose any configuration changes and any graph data that was recorded after the backup was made.



The screenshot shows the AKCPPro Server interface. The header is blue with the AKCP logo and 'AKCPro Server'. The main content area is titled 'Restore' with a breadcrumb 'Restore / Restore Information'. Under 'Restore Status', there is a white box with a yellow warning icon and the text 'The system has never been restored'. Below this, there are two rows: 'Last restore' with 'N/A' and 'Video restore destination' with 'N/A'. At the bottom, there is a blue button labeled 'RESTORE NOW'.

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 screenshot shows the AKCPPro Server interface after a successful restore. The header is blue with the AKCP logo and 'AKCPro Server'. The main content area is titled 'Restore' with a breadcrumb 'Restore / Restore Information'. Under 'Restore Status', there is a white box with a green checkmark icon and the text 'The last restore was successful'. Below this, there are two rows: 'Last restore' with 'Wednesday, 18 July 2018 02:55 PM' and 'Video restore destination' with 'N/A'. At the bottom, there is a blue button labeled 'RESTORE NOW'.

Restore Process

Restore / Restore Process

1 File Options

2 Video Options

File Options

Choose the backup file location

C:/bak/ BROWSE

Choose the backup file

BackUp_2018_09_11_13_24_15.bak

File Name: BackUp_2018_09_11_13_24_15.bak
Backup Date: 2018-09-11 1:24:15 PM
MAC Address: 00-15-5d-01-6e-2c
IP Address: 192.168.16.1
Include Video: No

Enter the backup file password (Optional)

Backup File Password

BACK
NEXT
CANCEL

The first important step is to choose the location of your backup files.

If you have configured and made backups before, then the default path will be auto-selected.

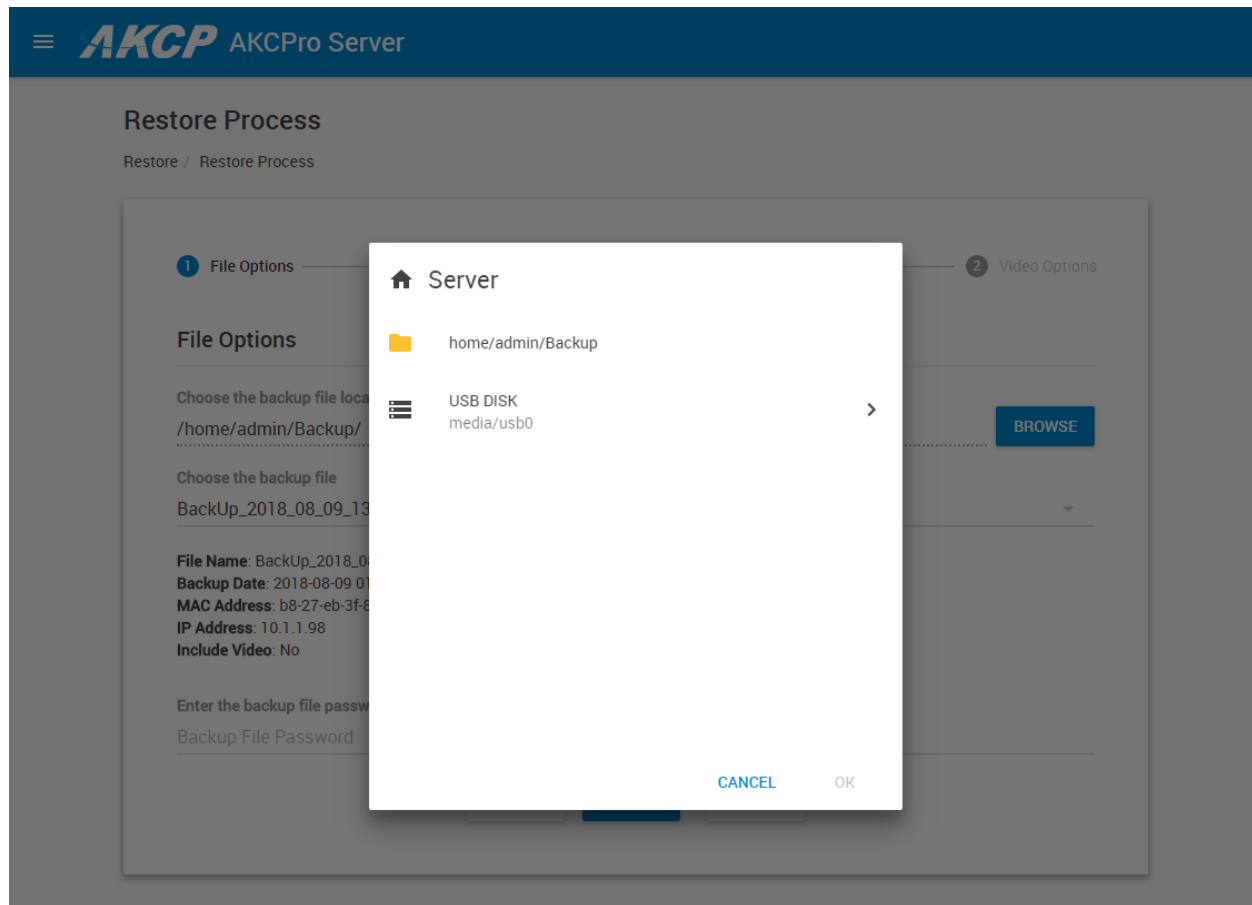
Then you'll need to select the **backup archive file** (.bak) you wish to restore (which is named after the date and time it was made).

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.

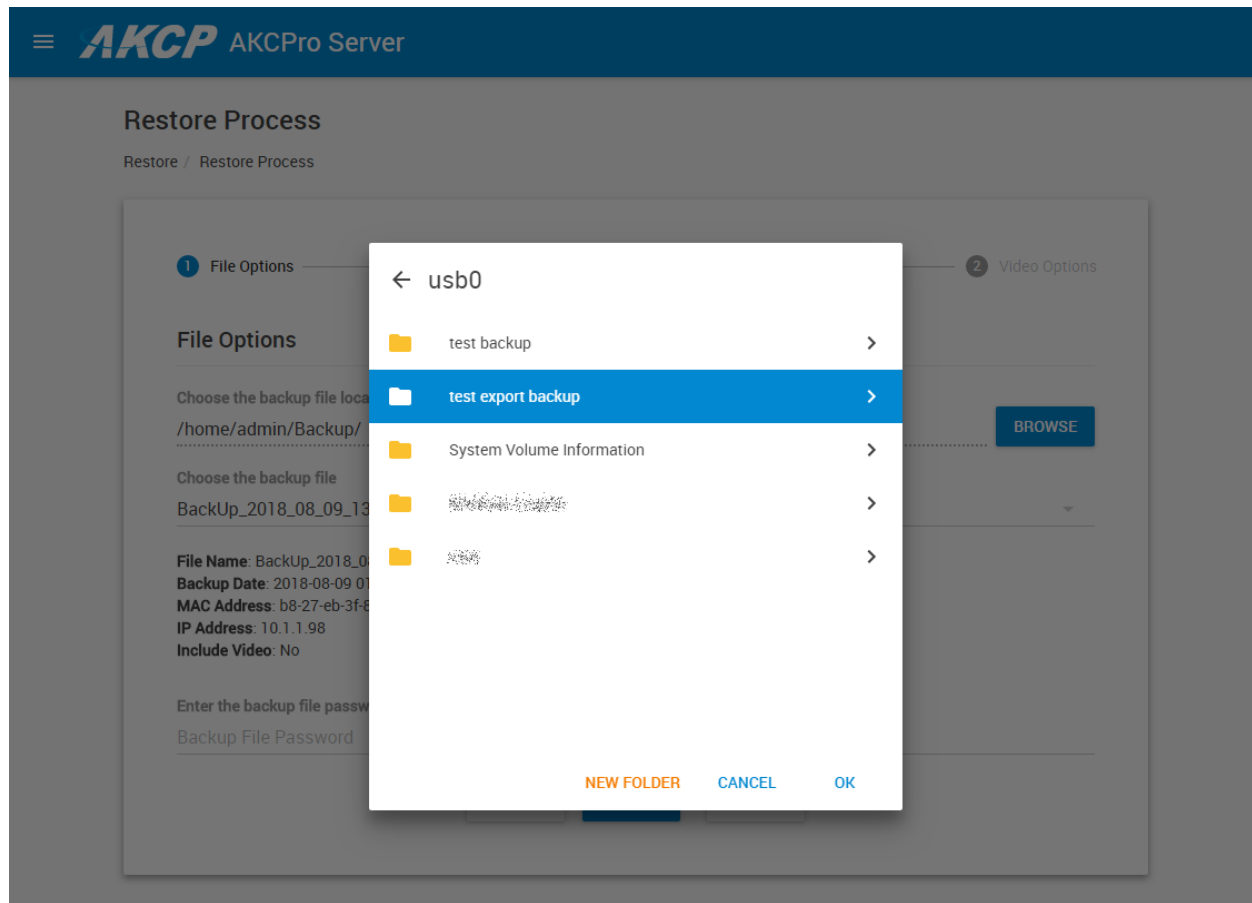
If your system was reinstalled, or the backup is on an external USB drive, see the below steps how to access it.



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**.

Restore Process

Restore / Restore Process

✓

File Options

2

Video Options

Video Options

Video Recording Path Options

☒ Keep the original video recording path

BACK

FINISH

CANCEL

On the L-DCIM units the video storage path is not configurable. Press **Finish** to start the restore process.

Restore

Restore / Restore Information

Restore Status

⌚

Restoring the system 0%

⌵

Last restore

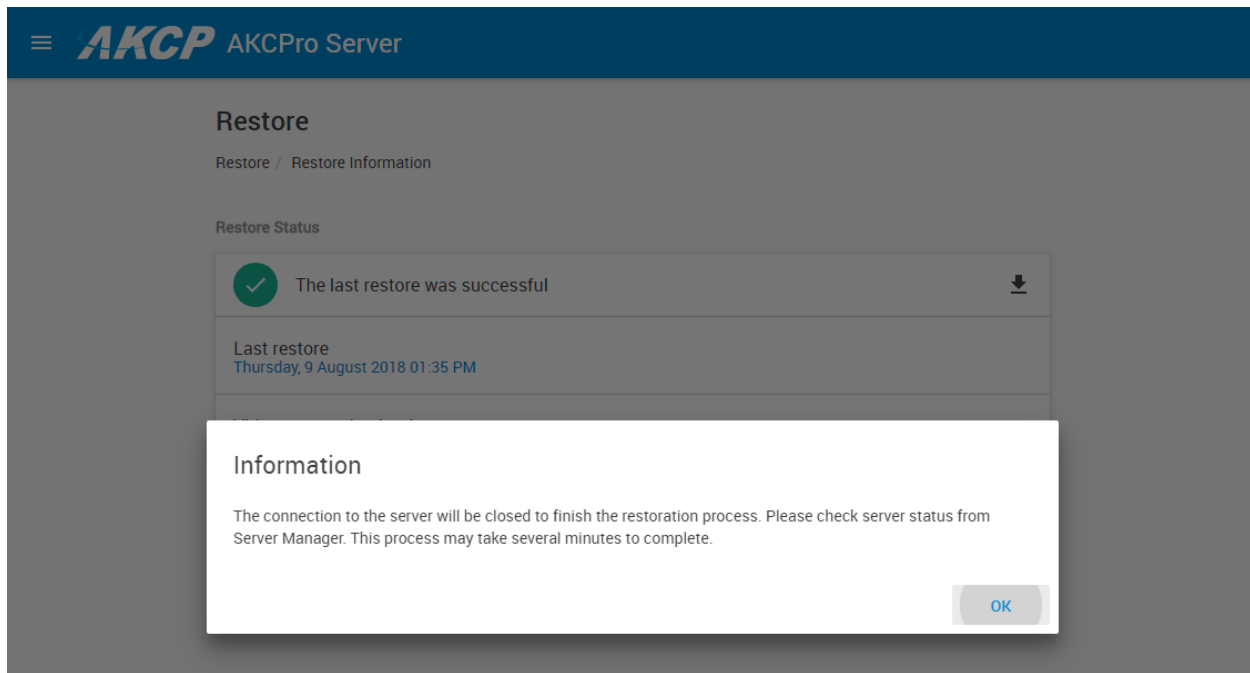
Thursday, 9 August 2018 01:35 PM

Video restore destination

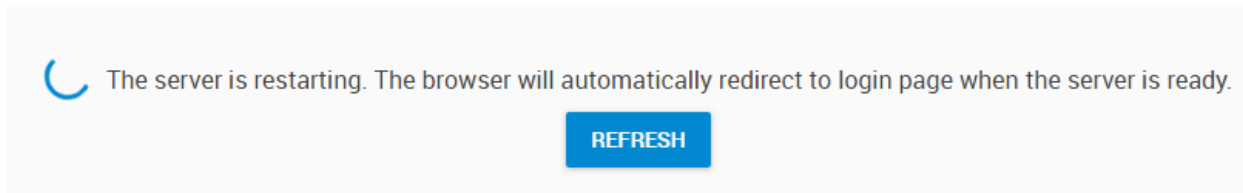
N/A

RESTORE NOW

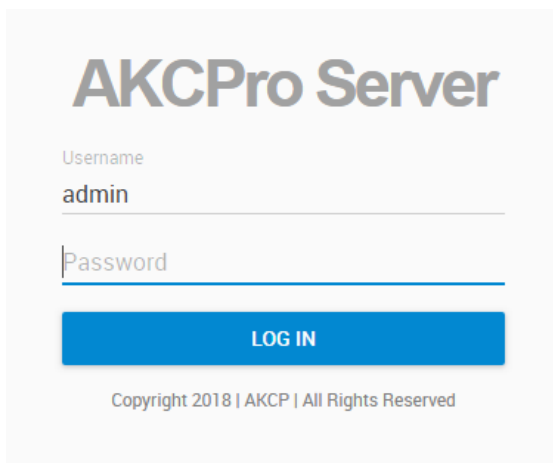
Be patient while the restore process is running. It can take a very long time if your backup file is on a USB drive and contains videos.



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.

Restore

Restore / Restore Information

Restore Status

 The last restore was successful 

Last restore
Wednesday, 18 July 2018 02:55 PM

Download Log

Video restore destination
N/A

RESTORE NOW

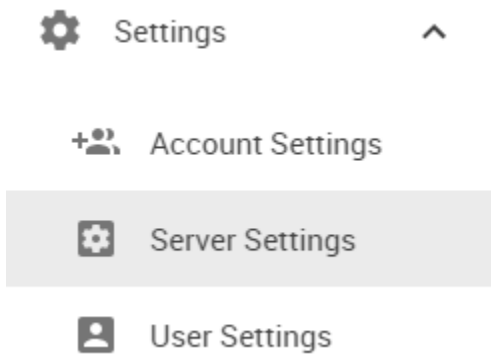
As with the Backup option, you can download and view the Restore log to see if it has finished properly.

Note for wireless sensors:

When you restore a backup, the connected wireless sensors might display as “unreachable”. This is expected because for the system, the last received radio packet timestamp has been sent a long time ago.

The sensors will return to normal state and display correctly again, when their pre-set packet sending interval has been reached (normally 15 minutes) or if you manually press the Mode button on the sensor to force-send a data packet immediately.

Server settings



You can make changes to the unit's settings in this menu.

Very important note:

After you made changes to any of the options, let your unit sit idle for at least 10-15 minutes or longer before removing the power or rebooting. If you remove power or reboot before this timeout, you might notice that your settings were not saved.

This is because the unit first saves the settings to a temporary database and only writes the changes to the flash storage later.

General

≡

AKCP

AKCPro Server

Server Settings

General

Connections

Local Network

Wireless

Wi-Fi

Modem

SNMP

VPN

SMTP Email Alert

Event Logs

Notification

NTP

Language

Maintenance

Services

Software Update

General

Settings / Server Settings / General

System Name

AKCPro Server

System Location

System Location

System Contact

System Contact

System URL

http://www.example.com

GPS Latitude

GPS Longitude

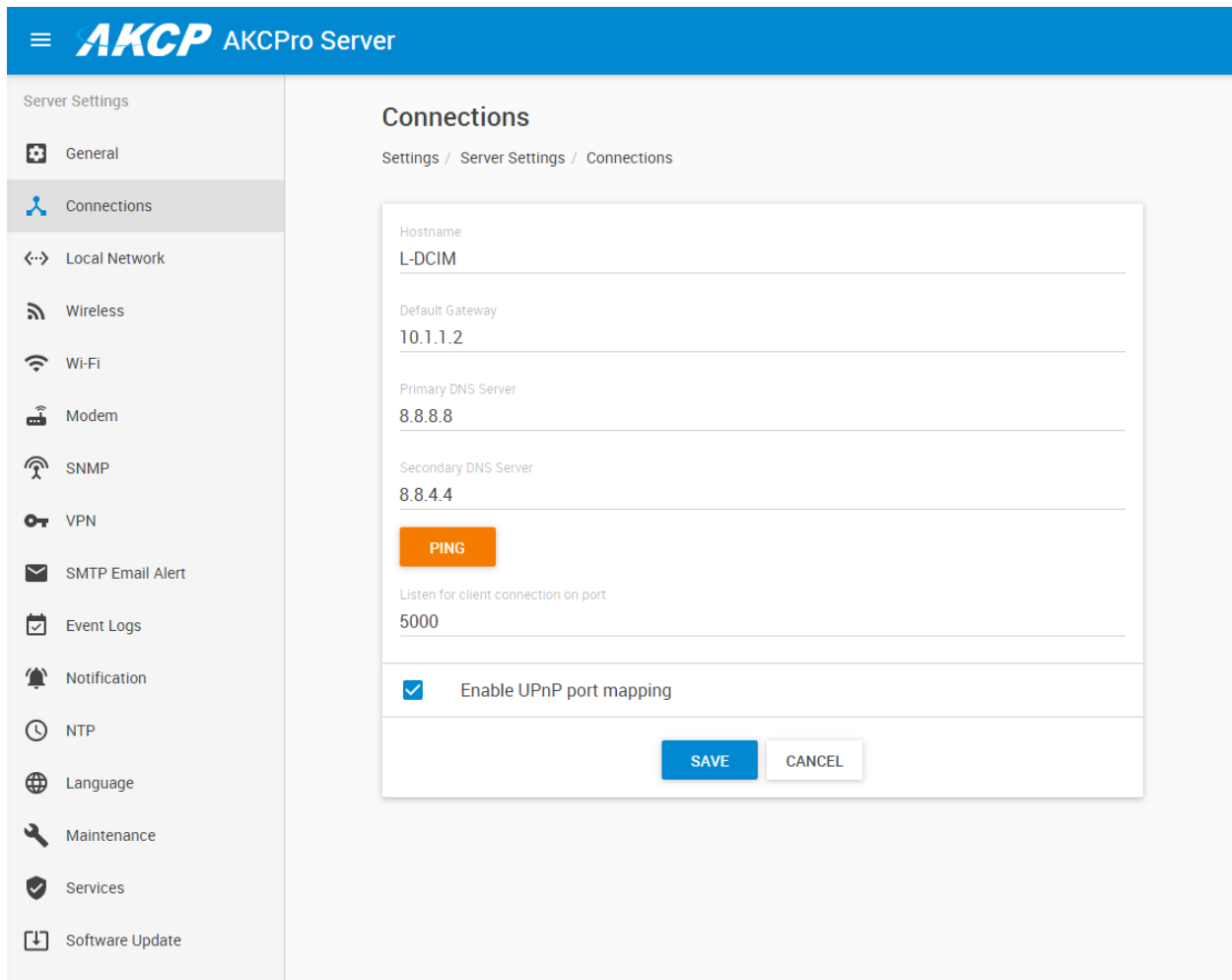
SAVE

CANCEL

You can set your unit's name, location, contact and System URL. Normally you can specify these during the setup.

If you enter the GPS coordinates for your unit here, and then place it on a GeoMap type, the map will offer the automatic placement on the world map based on the coordinates you entered - see details of this feature in the APS HTML manual.

Connections



AKCP AKCPro Server

Server Settings

- General
- Connections**
- Local Network
- Wireless
- Wi-Fi
- Modem
- SNMP
- VPN
- SMTP Email Alert
- Event Logs
- Notification
- NTP
- Language
- Maintenance
- Services
- Software Update

Connections

Settings / Server Settings / Connections

Hostname
L-DCIM

Default Gateway
10.1.1.2

Primary DNS Server
8.8.8.8

Secondary DNS Server
8.8.4.4

PING

Listen for client connection on port
5000

☒ Enable UPnP port mapping

SAVE **CANCEL**

Under Connections, you can specify the following:

Default gateway: this shows the default gateway (default route) for the unit. It can be set on either the Local Network or Wi-Fi pages, you shouldn't modify it from this page.

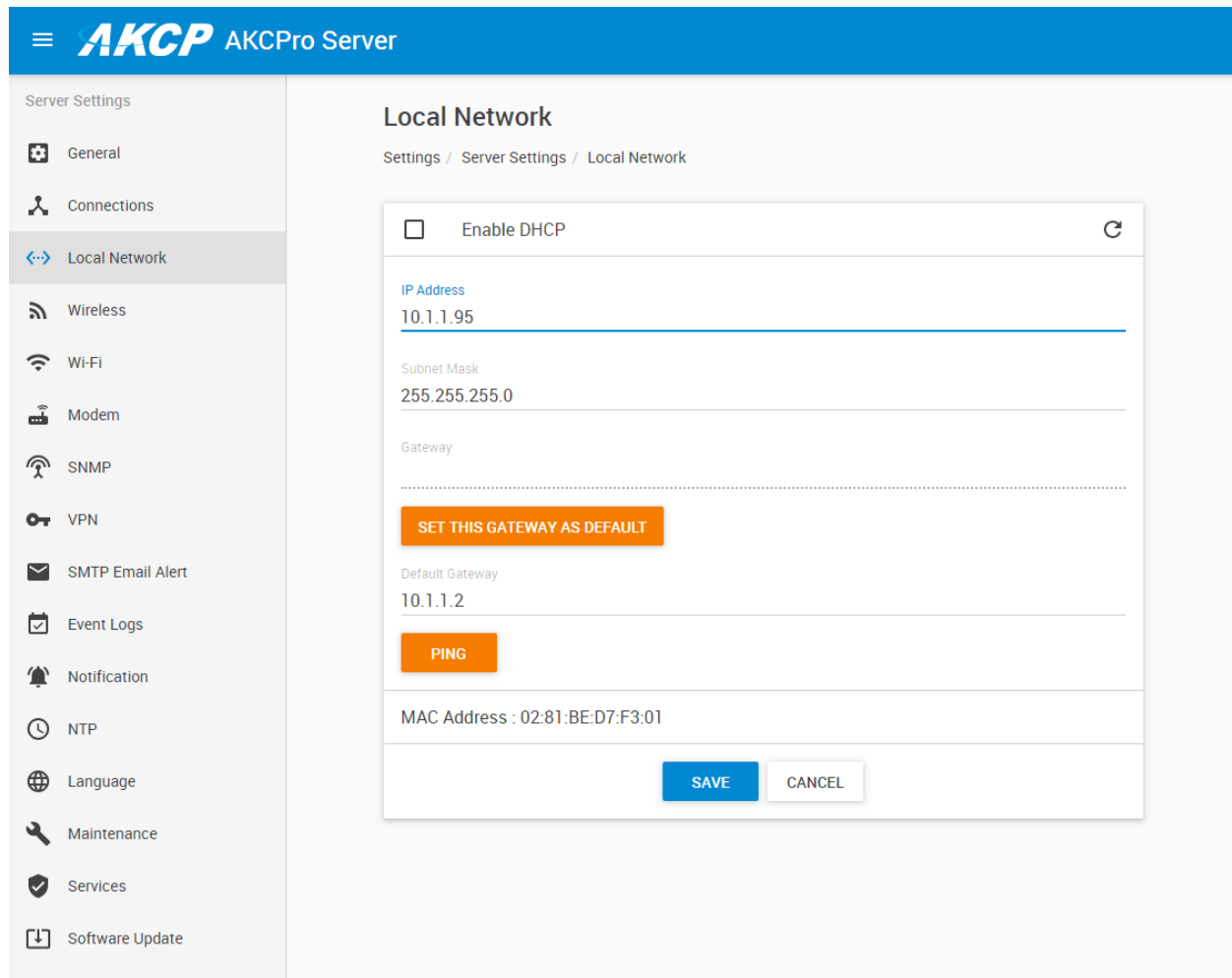
Hostname: the DNS and DHCP hostname for the unit change it if you have multiple units.

DNS servers: these are required for name resolution (eg. to find the www.akcp.com address). The defaults are set to Google's public DNS. You can ping them to verify you have a working connection.

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.

Local Network



AKCP AKCPPro Server

Server Settings

- General
- Connections
- Local Network**
- Wireless
- Wi-Fi
- Modem
- SNMP
- VPN
- SMTP Email Alert
- Event Logs
- Notification
- NTP
- Language
- Maintenance
- Services
- Software Update

Local Network

Settings / Server Settings / Local Network

☐ Enable DHCP

IP Address
10.1.1.95

Subnet Mask
255.255.255.0

Gateway
.....

SET THIS GATEWAY AS DEFAULT

Default Gateway
10.1.1.2

PING

MAC Address : 02:81:BE:D7:F3:01

SAVE **CANCEL**

You can manage the unit's Ethernet interface from this page.

Normally this should have already been configured during the first time setup (review that section in this manual for more information).

Make sure your **Default Gateway** is correct and reachable, if your unit has to connect to external servers on the internet.

Your Ethernet MAC ID will be also displayed here.

Important:

Since all licenses are tied to the unit's MAC ID, it's important to choose the interface which you'll be using to access the unit. If you use another interface than what you used before, your licenses won't work and the unit goes back to the default license.

Wireless

≡

AKCP

AKCPro Server

Server Settings

General

Connections

Local Network

Wireless

Wi-Fi

Modem

SNMP

VPN

SMTP Email Alert

Event Logs

Notification

NTP

Language

Maintenance

Services

Software Update

Wireless

Settings / Server Settings / Wireless

☐ Enable Wireless

RF Channel

Region: EU863-870MHz ISM Band

Channel to Use

Channel #0 (868.10 MHz DR5)

SAVE

CANCEL

Last received Wireless packets

No Logs

You can manage the unit's LoRa Wireless Sensor interface from this page.

You'll need to enable it before you can add any wireless sensors (the unit will ask you to do so if you haven't enabled it yet).

Channel #0 (868.10 MHz DR5)

Channel #1 (868.30 MHz DR5)

Channel #2 (868.50 MHz DR5)

Channel #3 (867.10 MHz DR5)

Channel #4 (867.30 MHz DR5)

Channel #5 (867.50 MHz DR5)

Channel #6 (867.70 MHz DR5)

Channel #7 (867.90 MHz DR5)

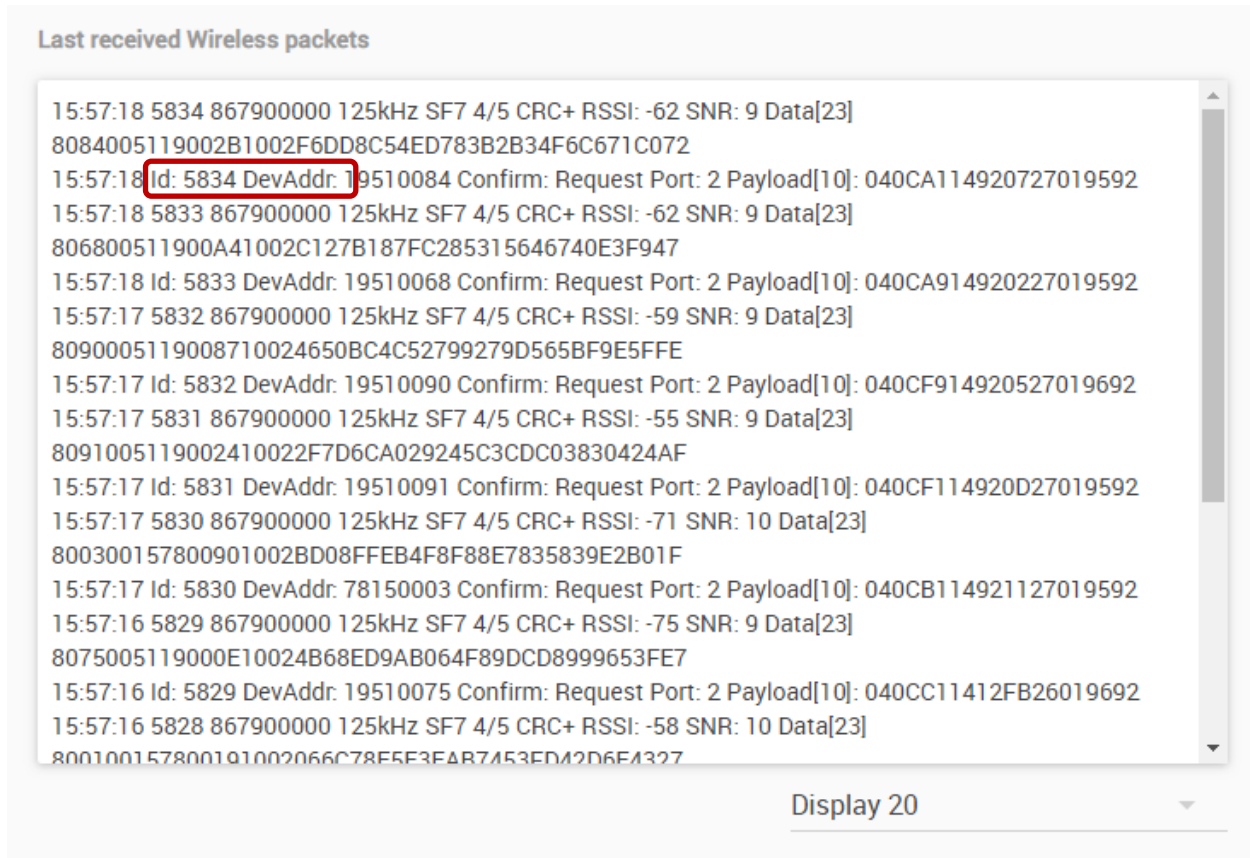
First you'll have to choose a Wireless Channel for operation. After this, click on "Enable Wireless" option and then **Save**.

Note: the RF Channel Region is defined by the hardware and cannot be changed!

For best performance, check each channel for wireless communication and see which has the lowest traffic - the ideal channel is if it is “empty” and you don’t see any packets received while your unit doesn’t have any sensors added yet.

After you've enabled the radio, the Wireless Packet monitor window becomes active. If there's radio traffic on the selected channel, you'll already see some packets received.

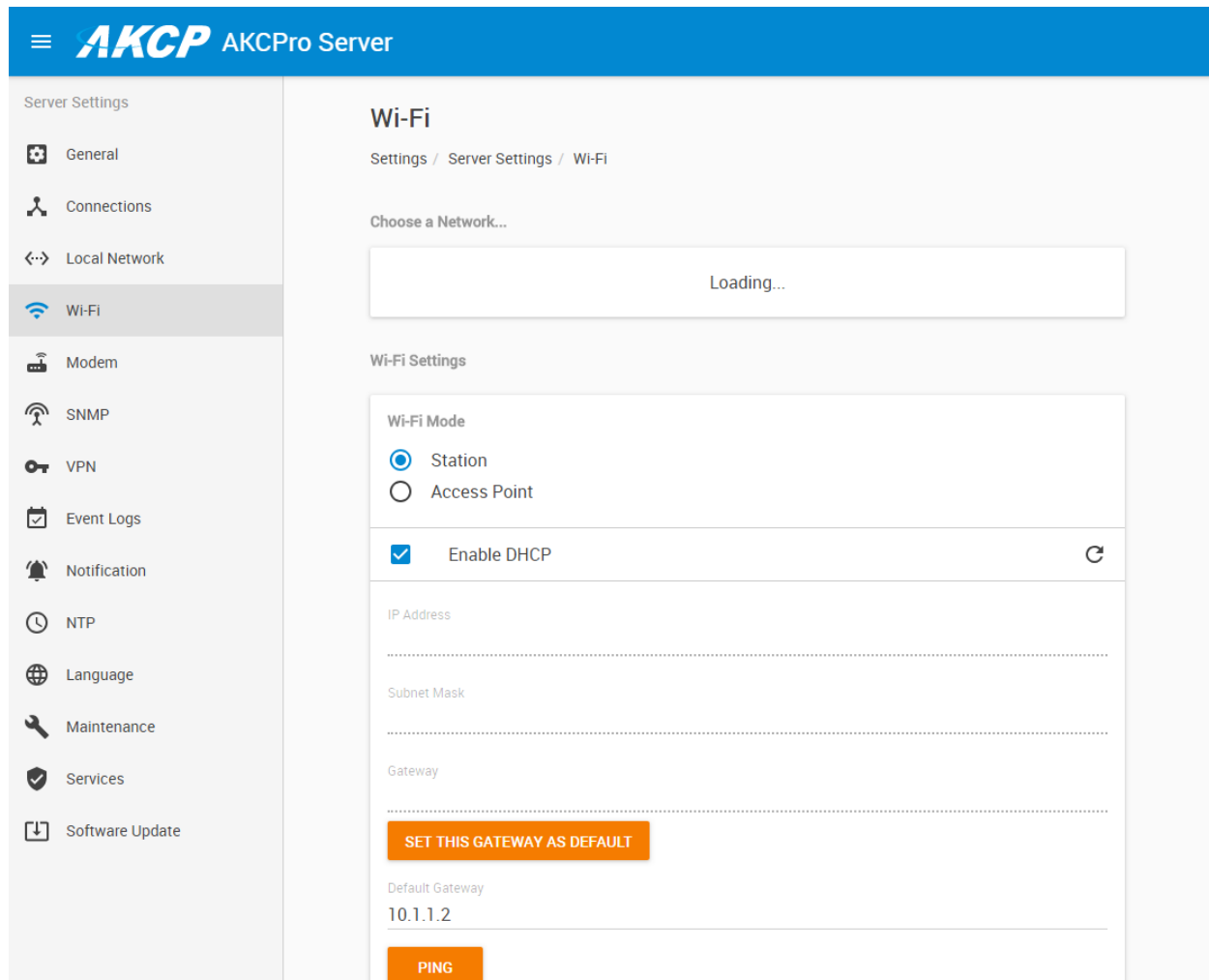
After you add wireless sensors, you'll see their sent and received packets in the window. You can find each sensor by their Device Network Address, for example 19510084 on the screenshot below.



You can also choose to display more or less log lines at once. This window is a live log view and cannot be paused/stopped.

For troubleshooting, newer firmware (after image 186) has additional packet logging feature per sensor. See the wireless packet logger section in this manual for more information.

Wi-Fi



You can manage the unit's built-in Wi-Fi interface from this page.

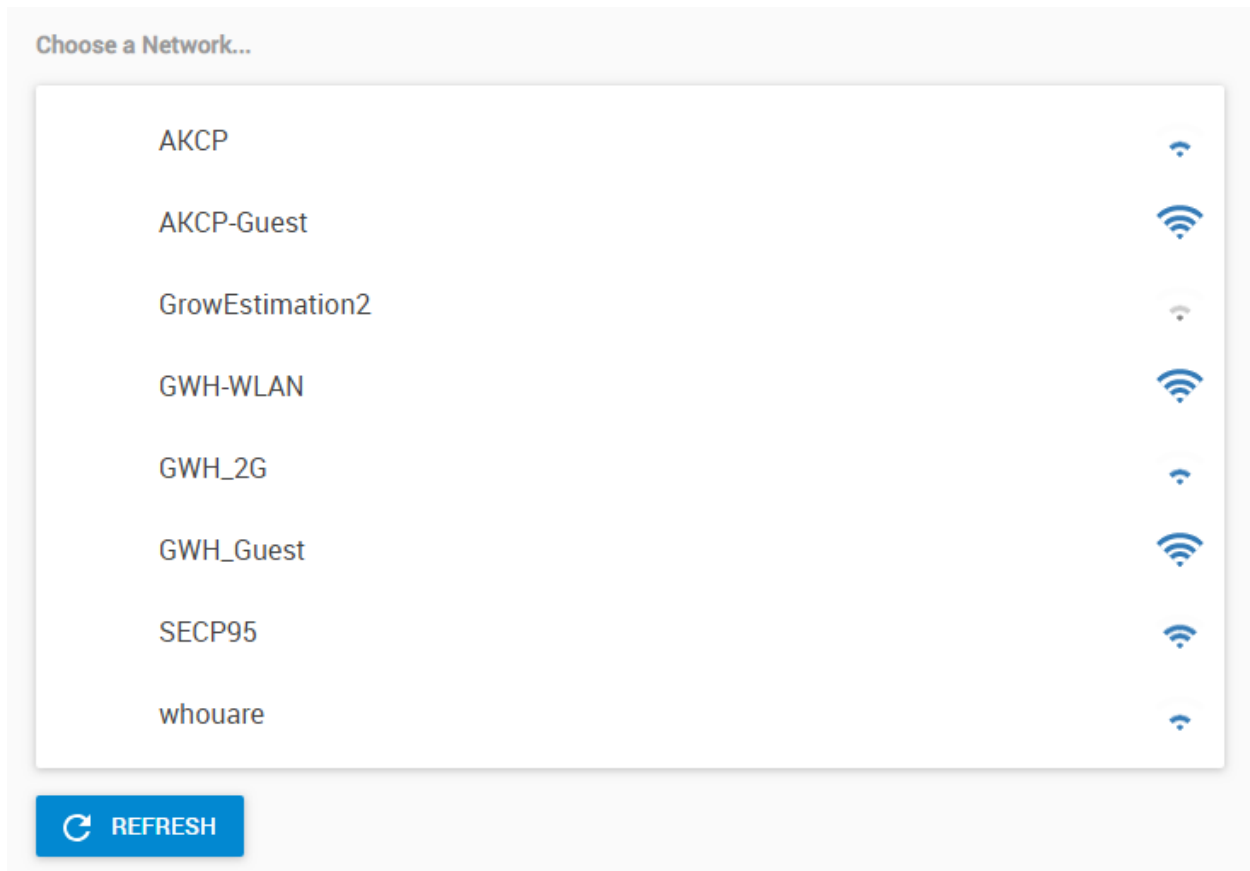
It supports 2 modes:

- Access Point - act as a router for other wireless devices to connect
- Station - act as a wireless client to connect to another router (most common scenario)









We'll describe the 2 modes below.


Station mode

An automatic network search will run to let you easily connect to an existing network:

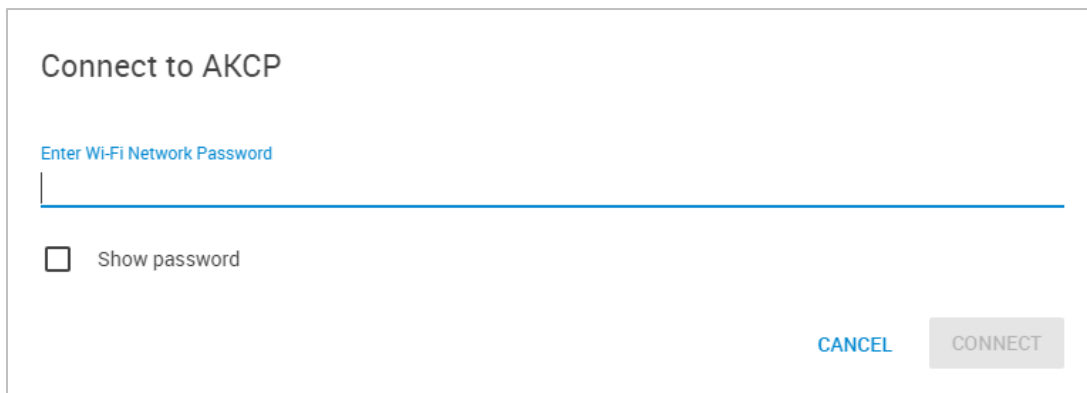


Choose a Network...

| | |
|-----------------|---|
| AKCP |  |
| AKCP-Guest |  |
| GrowEstimation2 |  |
| GWH-WLAN |  |
| GWH_2G |  |
| GWH_Guest |  |
| SECP95 |  |
| whouare |  |

 REFRESH

A network list is shown with their signal levels. The list is updated automatically.



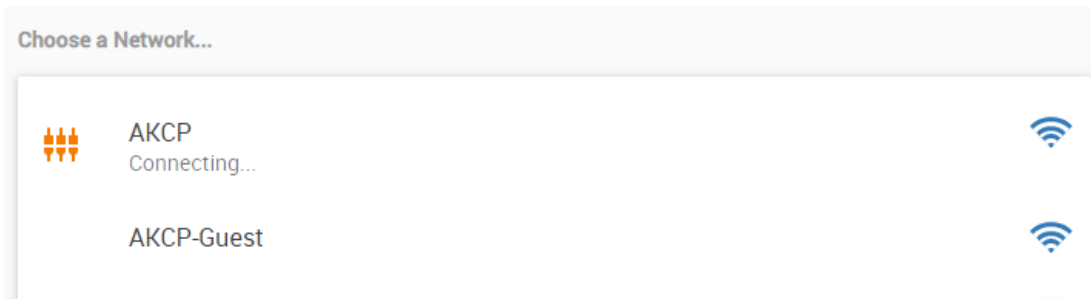
Connect to AKCP

Enter Wi-Fi Network Password

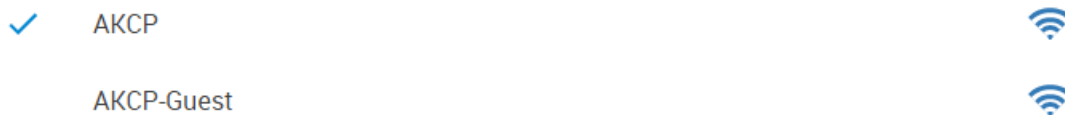
☐ Show password

[CANCEL](#) [CONNECT](#)

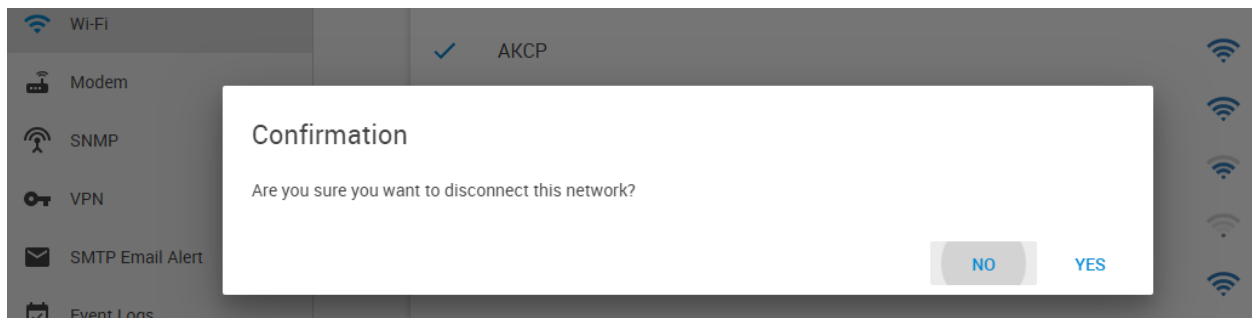
Click on your Wi-Fi network's name and enter your password to connect. The network security type is auto-detected.



First the unit will try connecting and get IP address automatically from the access point. If there were any errors, you'll get a notification popup.



If there were no errors while connecting, the network will be marked as connected. The unit will remember the connection's password and the IP setting you used (see below).



To disconnect from a network, you'll need to click on the network's name again in the list and the unit will ask you to confirm the disconnection.

Note: the unit won't remember the password you used to connect if you choose to disconnect from a network. If you have to reconnect, you'll need to re-enter the password again.

Important note: currently the unit supports only a WiFi SSID (network name) which contains ASCII-8 printable characters, excluding the double-quote sign "

For example, this SSID would work: ~! @\$%^&*()_ |-=\ []';:<>,.?/

But if your SSID contains the " character, the unit won't be able to connect to your network.

Wi-Fi Settings

Wi-Fi Mode

☒ Station
 ☐ Access Point

☒ Enable DHCP

IP Address

10.1.6.38

Subnet Mask

255.255.255.0

Gateway

SET THIS GATEWAY AS DEFAULT

Default Gateway

10.1.1.2

PING

MAC Address : 12:81:7A:D2:5FE1

SAVE

CANCEL

In most cases you need keep the interface in DHCP mode, but if necessary, you can enter a fixed IP. The default gateway could be modified to use the Wi-Fi interface if you plan to use this interface as the primary to access the unit.

After you've successfully connected to an access point, the assigned DHCP IP address and gateway will be displayed here.

Important:

Since all licenses are tied to the unit's MAC ID, it's important to choose the interface which you'll be using to access the unit. If you use another interface than what you used before, your licenses won't work and the unit goes back to the default license.

Access Point mode

Wi-Fi Mode
☐ Station
☒ Access Point

Access Point Name (SSID)
SECP95

Password
.....

Password Strength: Good

Channel
6

Status : Active

IP Address
192.168.128.1

Subnet Mask
255.255.255.0

☒ Enable DHCP

MAC Address : 12:81:BE:D7:F3:01

SAVE

CANCEL

Specify your SSID (network name) and connection password. The security is dynamic; it will use the strongest method that the client supports.

Set your network channel (between 1 to 11) to one that is not over-crowded with other neighboring devices. If you have problems connecting with other devices, channel 6 is recommended.

L-DCIM provides a basic DHCP server for the clients.

The IP range is 192.168.128.x

Modem

AKCP

AKCPro Server

Server Settings

General

Connections

Local Network

Wireless

Wi-Fi

Modem

SNMP

VPN

SMTP Email Alert

Event Logs

Notification

NTP

Language

Maintenance

Services

Software Update

Modem

Settings / Server Settings / Modem

☐ Enable Modem

Status: Not Connected

Remote IP Address:

Signal Strength: -113 dBm

Modem Device

Device Name:

Connection Method

Never Dial-Out (Use Ethernet Only)

Connection Type

Always On

Connection Mode

NORMAL

Access Point Name

internet

Redial Attempt (Enter 0 for No Limit)

0

Login Name

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

You can also see on this page the state of the connection: the **Status** and the assigned IP address when connected, as well as the **Signal Strength**.

Never Dial-Out (Use Ethernet Only)

Dial-Out If Ethernet Failed

Use Dial-Out Only

Connection Method:

As with other SP+ devices, you can set the Connection Method and Connection Type to be always on, or on-demand depending on the Ethernet state.

You may change the *Connection Method* as follows:

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

NORMAL

CHAP

MS-CHAP

MS-CHAPv2

EAP

PAP

Connection Mode:

You may select a different *Connection Mode* (PAP/EAP/CHAP).

The most commonly used is *NORMAL* which is GPRS Unsecured.

Always On

On-Demand

Also you may change the *Connection Type*:

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

Note 1: There's no auto-detection feature for the internal modem module, the configuration is always shown even if your unit is not equipped with the module.

Note 2: Only insert and remove the SIM card when the unit is turned off. Otherwise you can damage the SIM and the modem.

Note 3: The PIN code for the SIM card needs to be removed; otherwise the modem can't use it.

SNMP

≡

AKCP

AKCPro Server

Server Settings

General

Connections

Local Network

Wi-Fi

Modem

SNMP

VPN

Event Logs

Notification

NTP

Language

Maintenance

Services

SNMP

Settings / Server Settings / SNMP

SNMP Settings

SNMP Port

161

SAVE

CANCEL

SNMPv1/v2c

☒ Enable SNMPv1/V2c

Read Community

Write Community

SAVE

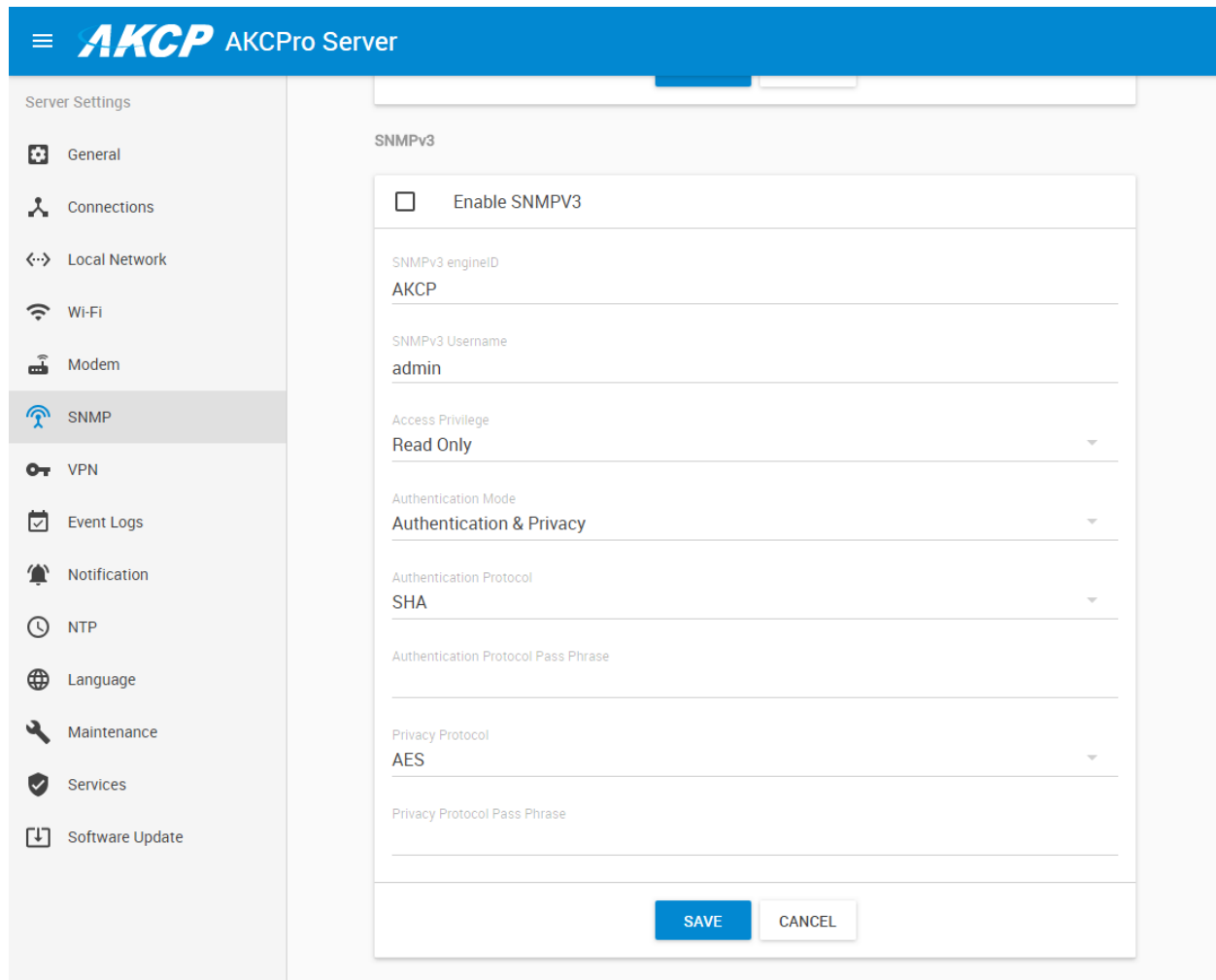
CANCEL

The SNMP service configuration options are shown here, it is required for SNMP operations. SNMPv1/v2 is enabled by default, with community password “public”.

You can customize the SNMP port if required, but in most cases you should leave it at default to avoid connection problems with other client units.

Scroll down for SNMPv3 options.

SNMPv3



The SNMPv3 options can be found by scrolling down on the SNMP page.

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

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

Basically if you select **No Authentication** then the setup will be the same as with SNMP v1 and v2c versions: authentication is only checked by unencrypted username.

Authentication Only will provide password protection but no encryption.

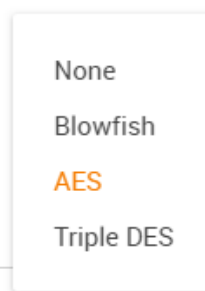
Authentication&Privacy provides encrypted username and password protection.

Set up VPN connection to the L-DCIM

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

1. On the L-DCIM, 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.



Remember the **Network Encryption 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 L-DCIM 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 L-DCIM IP or DNS name in VPN Server Address
- Use the VPN Network Password that you have specified on the L-DCIM
- Set up the the VPN Encrypt Method on the Encryption tab; use the same setting that you have specified on the L-DCIM

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

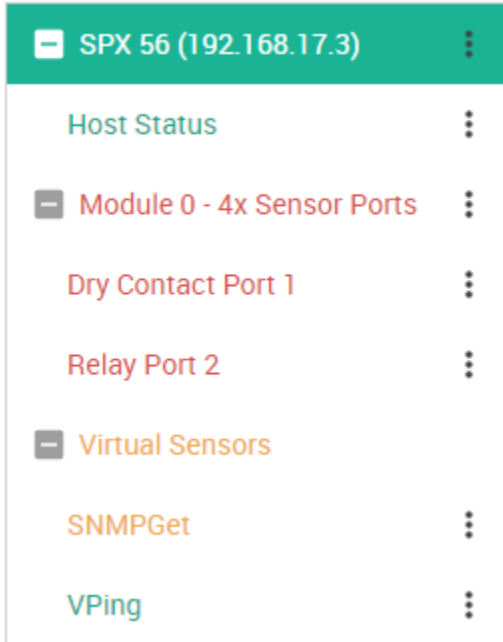
Confirm VPN Password Confirm VPN Password

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 L-DCIM console, the SP+ unit will be added to the **Monitoring page** automatically, with an IP address automatically assigned from the range you specified.



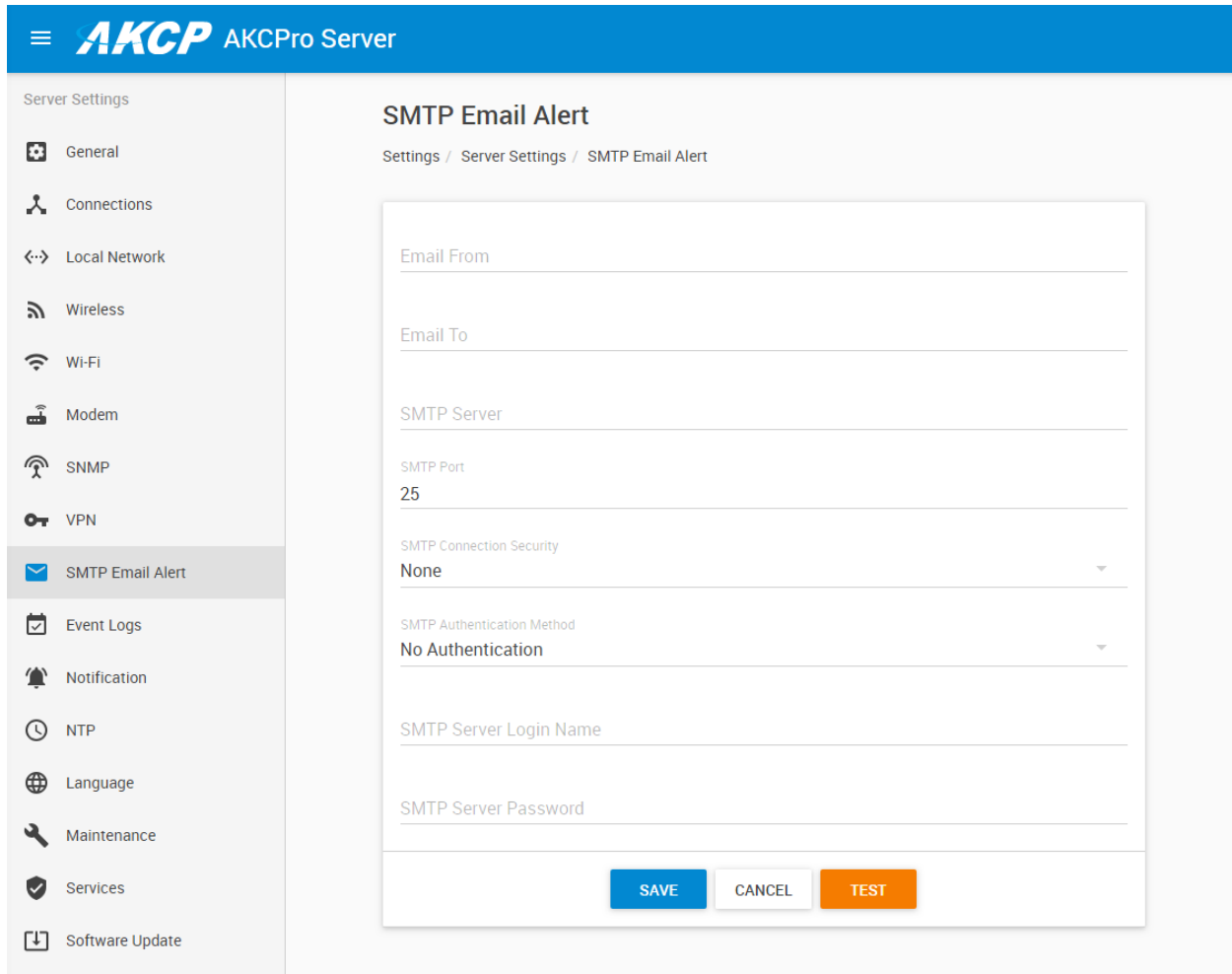
Important notes:

- If the SP+ was previously added to the L-DCIM 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 L-DCIM before.
- If the SP+ unit was previously monitored by any APS or L-DCIM, 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).
- The Virtual Sensor Ping cannot ping an IP address on the VPN network.
- You cannot ping or open a unit's Web UI if it's connected through VPN to the L-DCIM; these units are **ONLY** accessible via the L-DCIM interface. Therefore you cannot configure SP+ virtual sensors and the Buzzer on these client units.

Important notes for VPN setup with modem connection:

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

SMTP Email Alert



AKCP AKCPPro Server

Server Settings

- General
- Connections
- Local Network
- Wireless
- Wi-Fi
- Modem
- SNMP
- VPN
- SMTP Email Alert**
- Event Logs
- Notification
- NTP
- Language
- Maintenance
- Services
- Software Update

SMTP Email Alert

Settings / Server Settings / SMTP Email Alert

Email From

Email To

SMTP Server

SMTP Port
25

SMTP Connection Security
None

SMTP Authentication Method
No Authentication

SMTP Server Login Name

SMTP Server Password

SAVE CANCEL TEST

You can define a custom SMTP server for sending email for the following features:

- Send configuration to AKCP Support
- Get notified by a failed or unplugged system USB drive

The Connection Security and Authentication Method parameters are similar as with other SMTP settings on SP+ units, such as SSL/TLS/STARTTLS.

Note: you can only test the entered email settings after they've been saved.

Important: make sure that your Network Gateway setting is correct (see at the Local Network parameter). If there's no Gateway defined or it's unreachable, then the unit won't be able to connect to external servers on the internet.

Example setup using a Gmail account

SMTP Email Alert

Settings / Server Settings / SMTP Email Alert

| | |
|--|-----------------|
| Email From | xxxxx@gmail.com |
| Email To | xxxxx@gmail.com |
| SMTP Server | smtp.gmail.com |
| SMTP Port | 587 |
| SMTP Connection Security | STARTTLS |
| SMTP Authentication Method | DEFAULT |
| SMTP Server Login Name | xxxxx@gmail.com |
| SMTP Server Password | ***** |
| <div> <div>SAVE</div> <div>CANCEL</div> <div>TEST</div> </div> | |

Enter your Gmail account and use the SMTP parameters as shown on this screenshot above.

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

| Settings | |
|-------------------------------|----------------------------------|
| General | Labels |
| Inbox | Accounts and Import |
| Filters and Blocked Addresses | Forwarding and POP/IMAP |
| Change account settings: | |
| | Change password |
| | Change password recovery options |
| | Other Google Account settings |

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

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

Event logs configuration

The screenshot shows the AKCP Pro Server web interface. On the left is a sidebar with 'Server Settings' and a list of menu items: General, Connections, Local Network, Wi-Fi, Modem, SNMP, VPN, Event Logs (highlighted), and Notification. The main content area is titled 'Event Logs' and shows the breadcrumb 'Settings / Server Settings / Event Logs'. It contains two sections: 'When limit is reached' with radio buttons for 'Stop adding new logs' and 'Remove the oldest logs' (which is selected), and 'Maximum log entry in database (unit of thousands)' with a text input field containing '100'. At the bottom right are 'SAVE' and 'CANCEL' buttons.

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.

The logs contain important information with date and time, so you should always refer to the logs when troubleshooting.


Notification

≡


AKCP

AKCPro Server


Server Settings




General




Connections




Local Network




Wireless




Wi-Fi




Modem




SNMP




VPN




SMTP Email Alert




Event Logs




Notification




NTP




Language



Maintenance



Services



Software Update

Notification

Settings / Server Settings / Notification

☒

Skip sending a notification triggered by normal status event when the Server is starting

☒

Skip sending a notification triggered by normal status event when the device becomes reachable

☐

Skip sending a notification triggered by normal status event when the sensor recovers from sensor error status

SAVE

CANCEL

With these settings you can control to filter sending “normal status” notifications during the L-DCIM startup, and if a device becomes “reachable” again after an “unreachable” state.

In addition you can skip the notification for the “sensor error” to “normal” status change of sensors.

NTP - Network Time Protocol

≡

AKCP

AKCPro Server

Server Settings

General

Connections

Local Network

Wi-Fi

Modem

SNMP

VPN

Event Logs

Notification

NTP

Language

Maintenance

Services

Software Update

Network Time Protocol

Settings / Server Settings / Network Time Protocol

Date / Time

Date

Thursday 09/08/2018

Time

10:31 am

Timezone

(GMT+07:00) Bangkok, Hanoi, Jakarta

SAVE

CANCEL

☒ Force AKCP devices to use AKCPro Server clock

Network Time Protocol

Auto

NTP Server #1

0.debian.pool.ntp.org

NTP Server #2

1.debian.pool.ntp.org

L-DCIM has a built-in network time server.

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.

Here you can also manually set the date and time, plus the time zone.

If you have a working internet connection, you should sync with a trusted online NTP time source (more on this below).

You could de-select to force the time sync with client units, but this is not recommended.

Important: Check your time zone setting after applying L-DCIM updates. It might be necessary to adjust the time zone again for your region.

Online NTP sync

☒ Force AKCP devices to use AKCPro Server clock

Network Time Protocol
 Auto

NTP Server #1
 0.debian.pool.ntp.org

NTP Server #2
 1.debian.pool.ntp.org

NTP Server #3
 2.debian.pool.ntp.org

NTP Server #4
 3.debian.pool.ntp.org

SYNC NTP NOW

PING

SAVE

CANCEL

You can specify your custom NTP time servers for a reliable time source.

Use the **Ping** button to check if they are reachable.

To force-sync your unit's time with these servers, use the **Sync NTP Now** button.

Disabled

Auto

Once an hour

Once a day

Once a week

Once a month

You can also customize the frequency how often your unit's clock will get synchronized with the trusted online NTP servers.

Language

The screenshot displays the AKCP Pro Server web interface. The top navigation bar is blue with the AKCP logo and 'AKCPro Server' text. A left sidebar lists various settings categories: General, Connections, Local Network, Wi-Fi, Modem, SNMP, VPN, Event Logs, Notification, NTP, Language (highlighted), Maintenance, Services, and Software Update. The main content area is titled 'Language' and shows the breadcrumb 'Settings / Server Settings / Language'. It includes a section 'Choose Default Language For New Users' with a dropdown menu set to 'English' and 'SAVE'/'CANCEL' buttons. Below this is a 'Choose Language To Translate' section with a list of languages: Français (French), русский (Russian), and Español (Spanish), each with a right-pointing arrow. The final section is 'Create Your Own Language' with a list of languages: Afrikaans, Shqip (Albanian), العربية (Arabic), and Հայերեն (Armenian), each with a right-pointing arrow.

You can change the display language of the Web UI with this option. 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 unit).

←

Edit Language

Settings / Server Settings / Language / Edit Language

Español v1.7

Download

| Section | Total Entries | Translated Entries | |
|-----------------|---------------|--------------------|----------------------|
| General | 127 | 127 | Edit |
| Setup | 26 | 26 | Edit |
| Code Activation | 9 | 9 | Edit |
| Menu | 55 | 55 | Edit |
| Explorer | 17 | 17 | Edit |
| Gadget | 131 | 130 | Edit |
| Map | 96 | 96 | Edit |

Click on Edit next to each section of the language file to edit its contents:

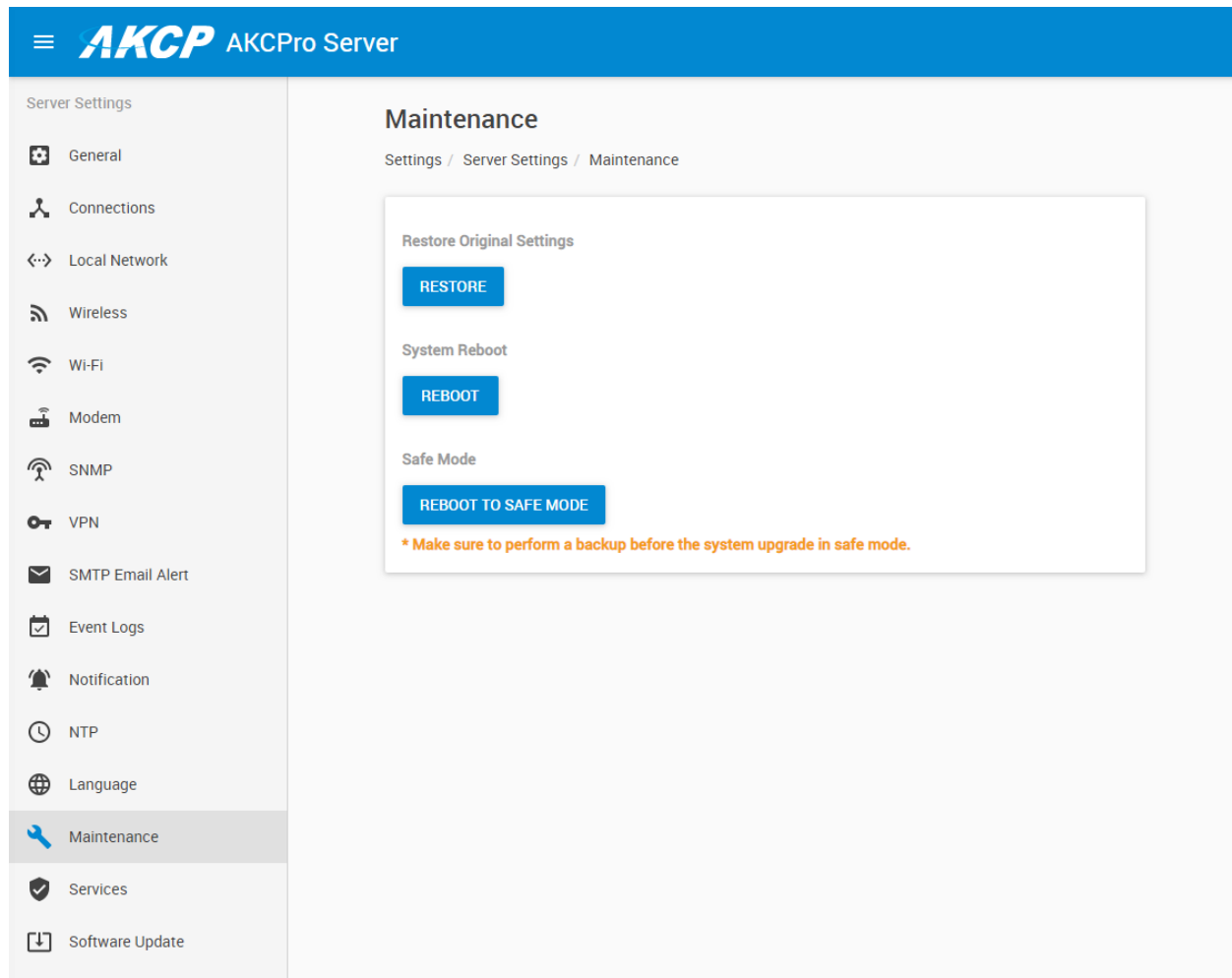
Español v1.7 / General

☐ Show Only Non-Translated

| Key | English | Español |
|--------|---------|----------|
| ERROR | Error | Error |
| OK | OK | OK |
| CANCEL | Cancel | Cancelar |
| BACK | Back | Back |

When done, save your changes and change the UI display language.

Maintenance



You can perform some maintenance tasks from this page:

Restore original settings

This will perform a Factory Reset: it will **reset all unit settings to their defaults, including the IP address**. Using this option will also remove any applied APS updates, so you'll need to reapply them. **Important:** You'll need to freshly set up the unit again from the start; see the "Initial setup steps" section in this manual. You can then restore a backup if necessary.

System reboot

This will reboot your unit. Unlike on SP+ devices, to reboot the L-DCIM you don't need to enter a password, as you are already authenticated.

Reboot to Safe Mode

This will reboot the unit into Safe Mode, to perform recovery and updates. It is recommended to perform a backup prior to using Safe Mode to make sure your data is safe if the upgrade fails for some reason. For more details see the Safe Mode section in this manual.

Services

≡

AKCP

AKCPro Server

Server Settings

General

Connections

Local Network

Wireless

Wi-Fi

Modem

SNMP

VPN

SMTP Email Alert

Event Logs

Notification

NTP

Language

Maintenance

Services

Software Update

Services

Settings / Server Settings / Services

Active Services

☒ Secure Shell (SSH)

User

admin

Password

☐ Web Interface (HTTP)

HTTP Port

80

Secure Web Interface (HTTPS)

HTTPS Port

443

Upload Certificate File

Select Certificate File

BROWSE

UPLOAD

☒ Enable Hardware Watchdog

SAVE

CANCEL

You can manage the unit's service features from this page.

Hardware Watchdog

If there's a software issue that makes the unit to stop responding, the watchdog will automatically reboot the unit.

SSH

L-DCIM runs Linux OS, and provides SSH terminal access, which is useful for troubleshooting and running special custom scripts. You can customize the SSH username and password, or disable SSH access.

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.

On the SP+ family, the 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 unit's Web UI for HTTPS connection (see below).

SSL Certificate

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

Example: secplus.mycompany.org

The unit's default DNS host name is "secplus" but you can customize this.

Wildcard SSL certificates should also work, but this hasn't been tested.

If the name doesn't match with the one in the certificate, the browser will still show a security warning.

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

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

Choose your file 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:

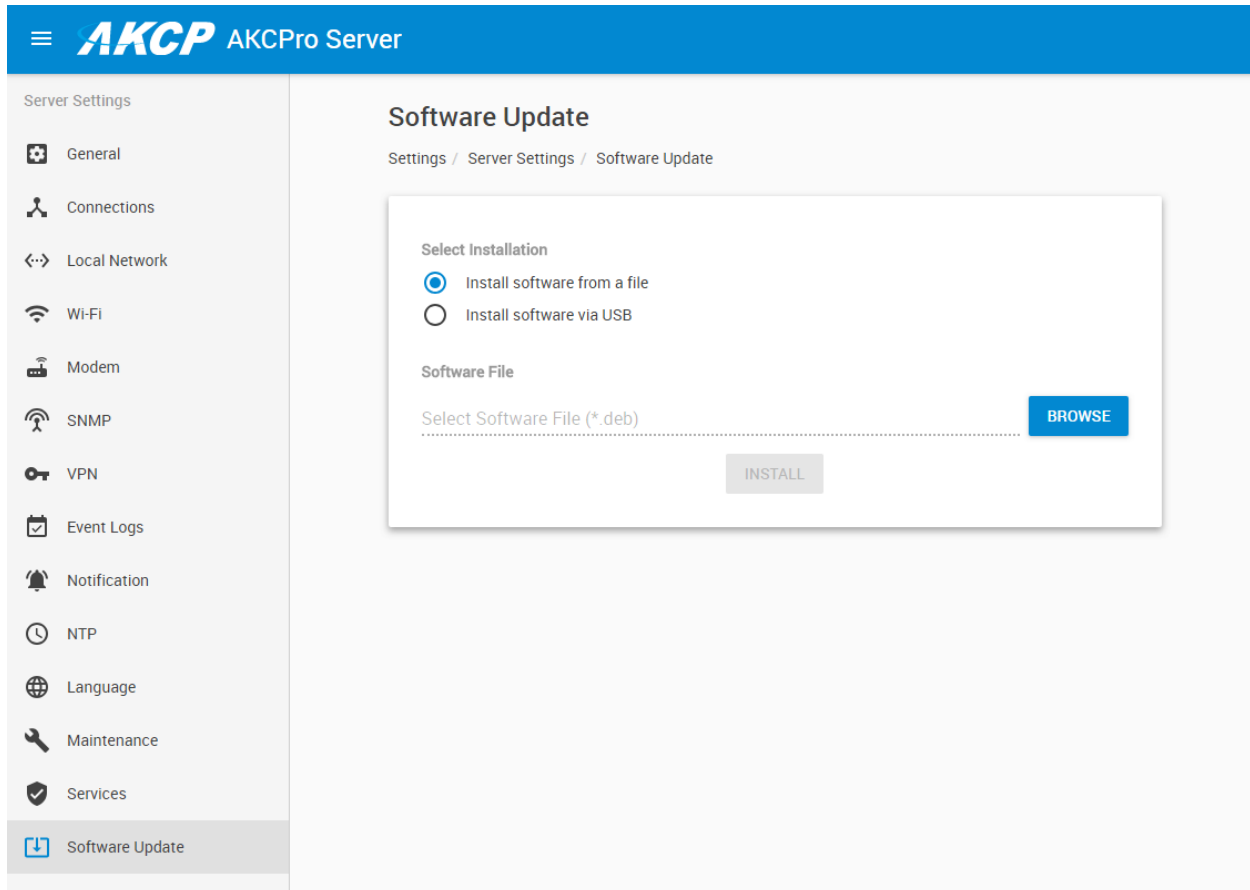
Server Restarting

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

Software update



AKCP AKCPPro Server

Server Settings

- General
- Connections
- Local Network
- Wi-Fi
- Modem
- SNMP
- VPN
- Event Logs
- Notification
- NTP
- Language
- Maintenance
- Services
- Software Update

Software Update

Settings / Server Settings / Software Update

Select Installation

☒ Install software from a file

☐ Install software via USB

Software File

Select Software File (*.deb) **BROWSE**

INSTALL

You can install updates to L-DCIM APS using this option.

You'll need to select a .deb package from your local PC with the **Browse** button, which will be uploaded and installed.

Optionally, if you place the .deb file on the root directory of a USB flash drive (don't put it to subfolders) then L-DCIM can find it and install the update from there. If the .deb file is not found in the root directory, you'll get a prompt that the update package cannot be found.

Important: when you use the "Reset to defaults" option under Maintenance menu, any updates you installed previously will be also removed.

Important: check your time zone setting after applying L-DCIM updates. It might be necessary to adjust the time zone again for your region.

Safe Mode

Safe Mode is a special boot mode of the unit. You can perform firmware update (Linux OS update) and recovery functions even if the unit cannot boot in normal mode any longer. Safe Mode is accessible even if the system USB drive is corrupt or removed.

Important: when the unit is booted into Safe Mode, **the WebUI is run only on the default HTTP port 80 - there's no SSL support in Safe Mode**. Therefore the HTTPS link won't work, you need to use HTTP protocol only.

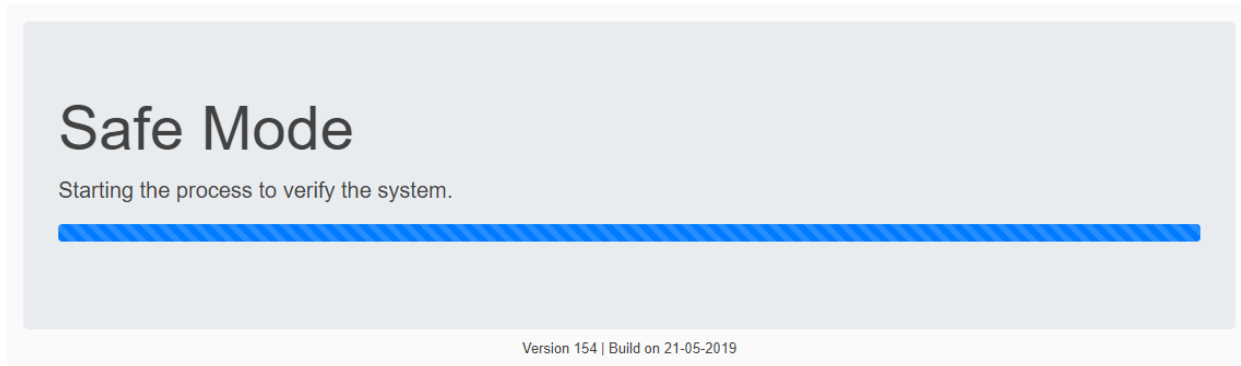
In order to access the unit in Safe Mode, use URL:

HTTP://{unit_ip_address}/index.php

For example: <http://192.168.0.100/index.php>

You can boot to Safe Mode in 3 ways:

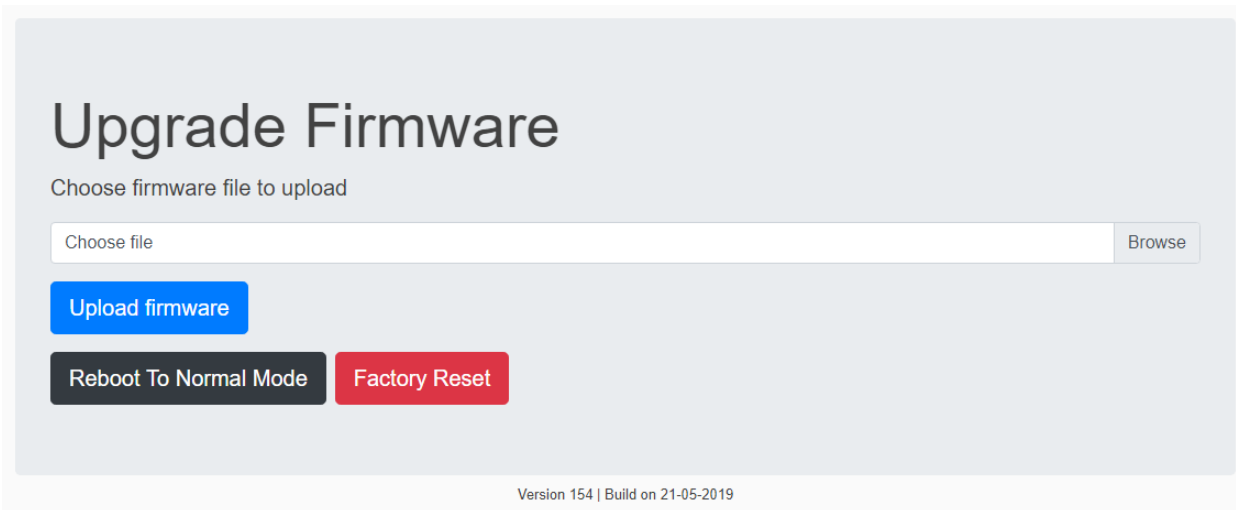
- A) by quickly pressing the Reset button on for at least 8 seconds as soon as the unit is powered on
- B) by selecting "Reboot to Safe Mode" from the Maintenance menu in normal mode
- C) using SSH commands (recommended only for advanced users or troubleshooting)



As the browser establishes connection to the unit, the Safe Mode verification script is run, which takes a few seconds. After this it will reserve disk space for proper file operations.

If the verification ends with an error, the following options available:

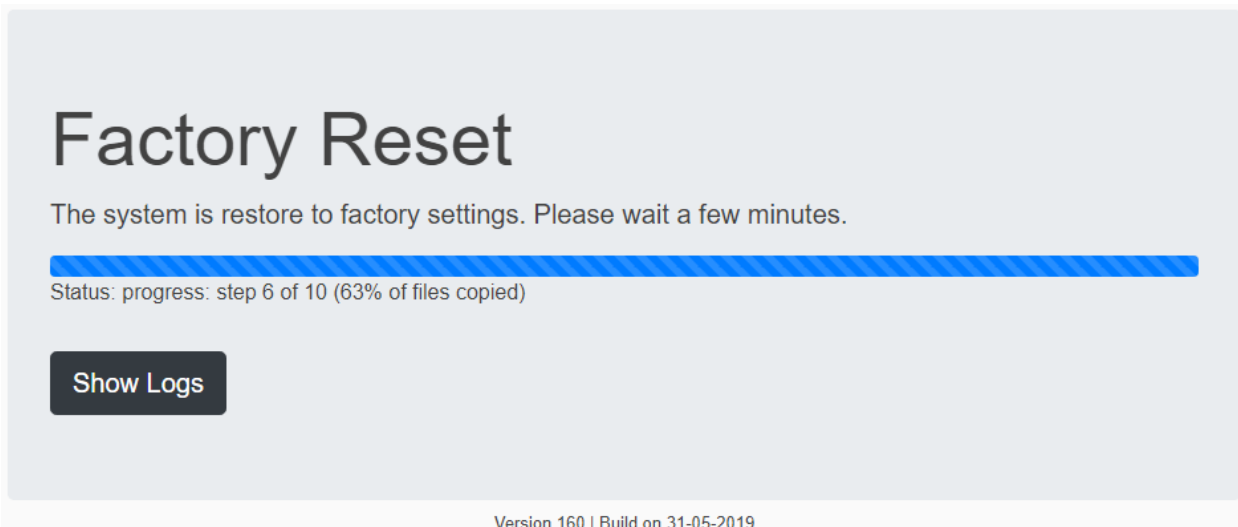
- 1) Perform 'Factory Reset'
- 2) Reboot to Normal Mode



If there were no errors during the verification step, then the available Safe Mode options are:

- 1) Specify filename for firmware upgrade (7zip archive)
- 2) Perform firmware upgrade (to upgrade the Linux OS)
- 3) Perform 'Factory Reset'
- 4) Reboot to Normal Mode

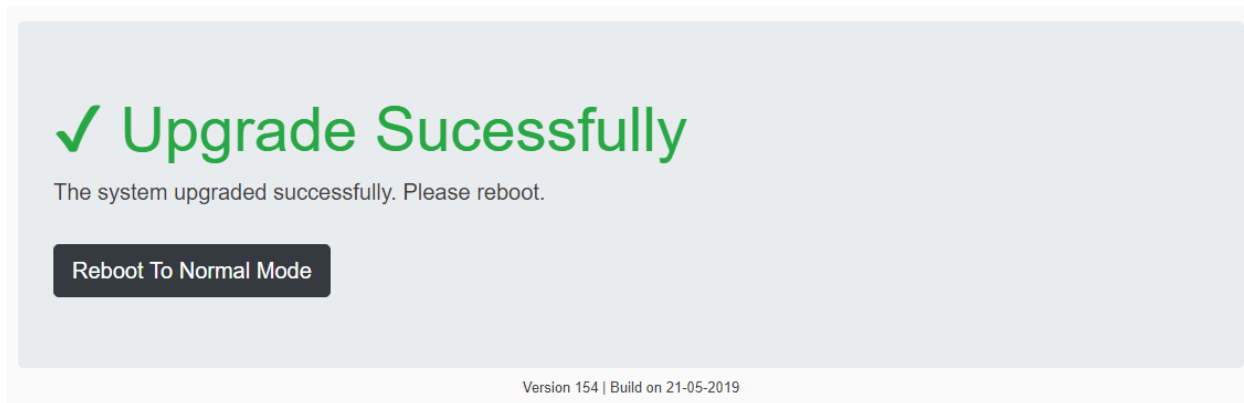
Factory Reset information



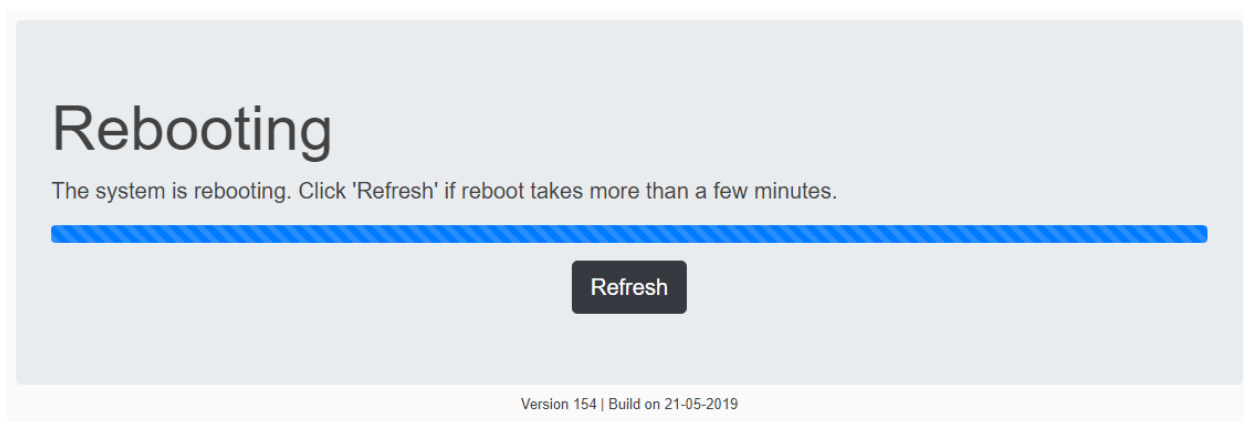
Using this option will erase all user data and settings, removes any APS upgrades applied and returns the unit to the default IP address (192.168.0.100).

Warning: the reset will start without confirmation once you press the “Factory Reset” button!

Very Important Note: If the unit's power is lost during upgrade, the Normal Mode won't start anymore. As a recovery feature, the unit should reboot back to Safe Mode and wait for either another attempt of Firmware Update or Factory Reset. If the automatic reboot to Safe Mode doesn't work, you'll need to manually boot the unit to Safe Mode by pressing Reset button for about 8 seconds during startup, or switch to Safe Mode boot by SSH commands (see below).



As the procedure completes, the 'Reboot to Normal Mode' button will be shown.



After clicking this button, the unit starts in Normal Mode again with the full APS-Server listening on the default HTTPS port (443).

Normally the WebUI should automatically redirect and you don't need to press the '**Refresh**' button.

Safe Mode Troubleshooting

Important note: SSH/SFTP access is also active in Safe Mode, there are special cases when you can use them. SSH is useful to manually check error logs and copy files to USB, with SFTP you can copy files in/out of the unit easily.

What to do if power is lost during upgrade and Normal Mode doesn't start: As a recovery feature, the unit should reboot back to Safe Mode and wait for either another attempt of Firmware Update or Factory Reset. If the automatic reboot to Safe Mode doesn't work, you'll need to manually boot the unit to Safe Mode by pressing Reset button for about 8 seconds during startup, or switch to Safe Mode boot by SSH commands (if Linux can boot up, see below).

How to manually switch to Safe Mode from Normal Mode SSH: Log in as Admin user and enter the following commands, followed by pressing the Enter key after each line:

```
sudo /sbin/akcp/switch_recovery.sh  
sudo reboot
```

Note: You'll be prompted for the Admin user password again when using commands with the "sudo" prefix.

Wireless Sensors

Wireless sensors enable you to monitor your environment without the need of sensor cables. After setting them up and adding them to the L-DCIM unit, you can use them as conventional sensors.

The setup procedure is more complex than with standard sensors; we'll describe the necessary steps and the wireless sensor properties in detail below.

Temperature and Humidity Monitoring

You can monitor temperature and humidity in cabinets, refrigerators, and rooms. With the integrated door contact sensor on LBTHD you are also able to keep track of your security condition or ignore temperature fluctuations when the door is opened. IP54 rated enclosure provides waterproofing for use in outdoor environments. Mounting with DIN rail, magnetic, wall hang, cable tie or pipe clamp.

Sensor Options

- Battery powered, with 10 year guaranteed battery life*
- USB powered
- USB powered with backup internal battery**
- Custom sensor cable length to position sensor and antenna in optimal position

*10 year battery life based on data broadcast once every 15 minutes at an ambient temperature of 25°C

The most common sensor types are the LBTH and LBTHD (both types supports temperature and humidity monitoring), and we'll use these sensors as examples.

Important Note: Due to airlines & FAA restrictions it is not possible for us to include the internal batteries for the **LBCAS and LSSI** wireless sensors, so they are not included.

You will need to purchase the re-chargeable AA batteries for each of the two sensors at your local retail store (4 for each sensor). You **MUST USE** the NiMh rechargeable batteries. If you try and use other types of batteries there is a risk of them exploding. Please refer to the separate LBCAS/LSSI manual for more specific details.

This will void the warranty and AKCP will not be responsible for any loss due to damage, injury or otherwise if the correct batteries are not used.

This **ONLY** applies to the LBCAS and the LSSI sensors. This does **NOT** apply to **ALL** other BOS or the AKCP wireless sensors with the internal batteries that are guaranteed for 10 years.

LBTD

External LoRa™ antenna for superior broadcast strength

IP54 enclosure



Sensor on custom cable lengths

LBTHD

External LoRa™ antenna for superior broadcast strength

IP54 enclosure

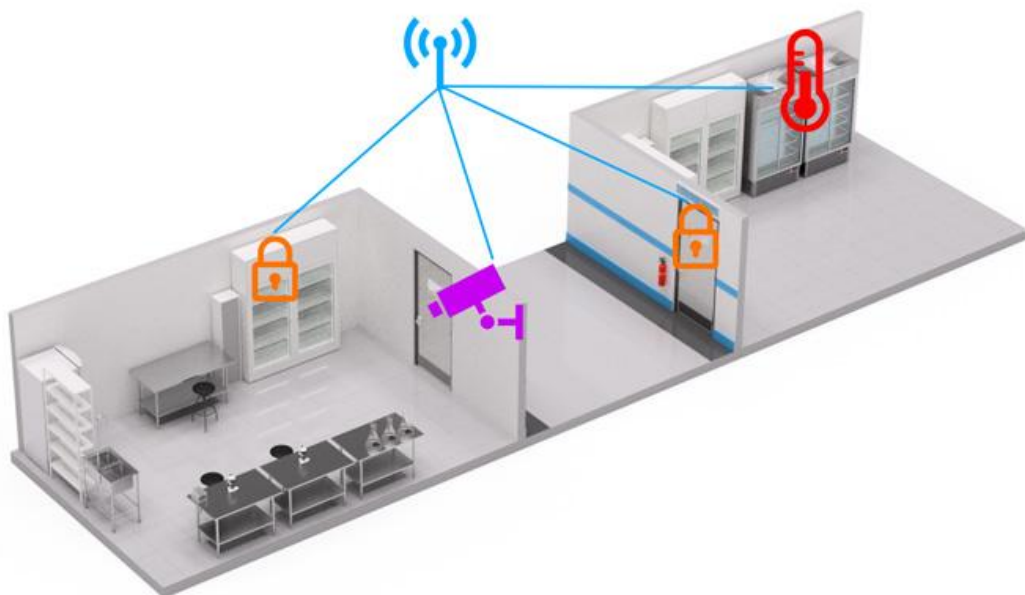


Dual Temp/Hum Sensor on custom cable length

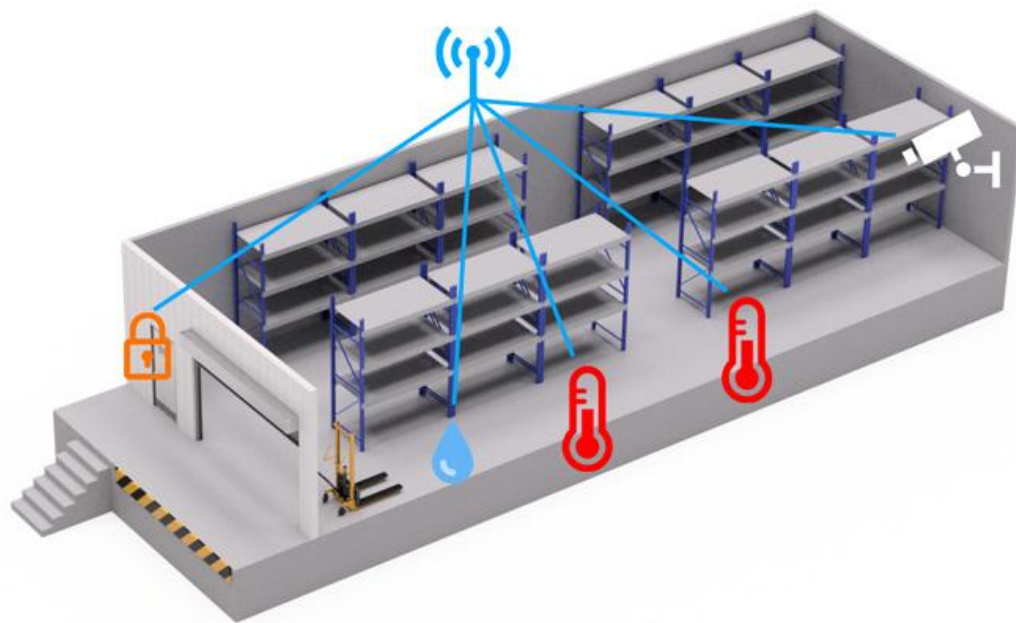
Door Contact Sensor on custom cable length

The difference is that the LBTHD wireless sensor has an additional Dry Contact sensor.

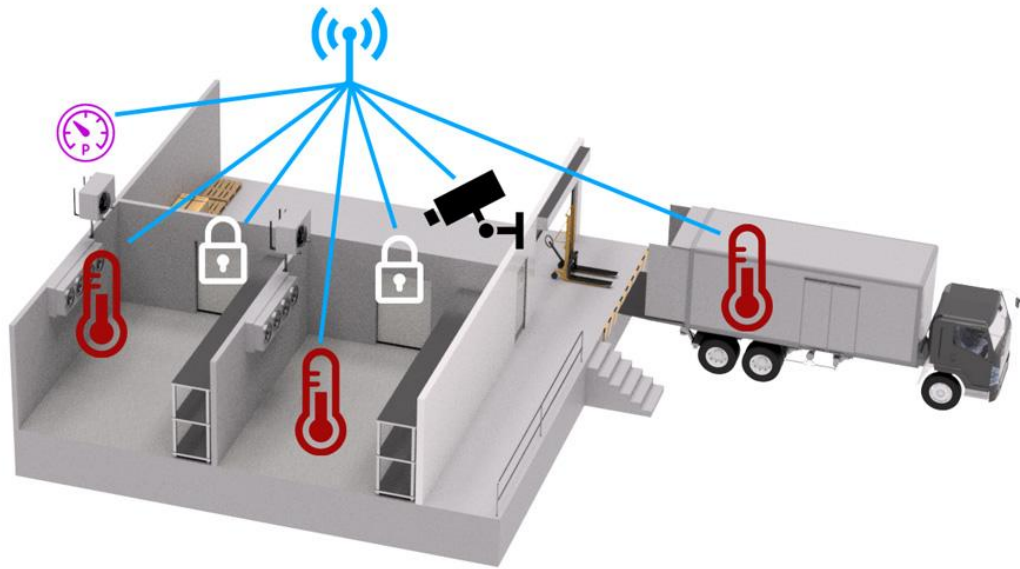
Installation examples



Pharmaceutical

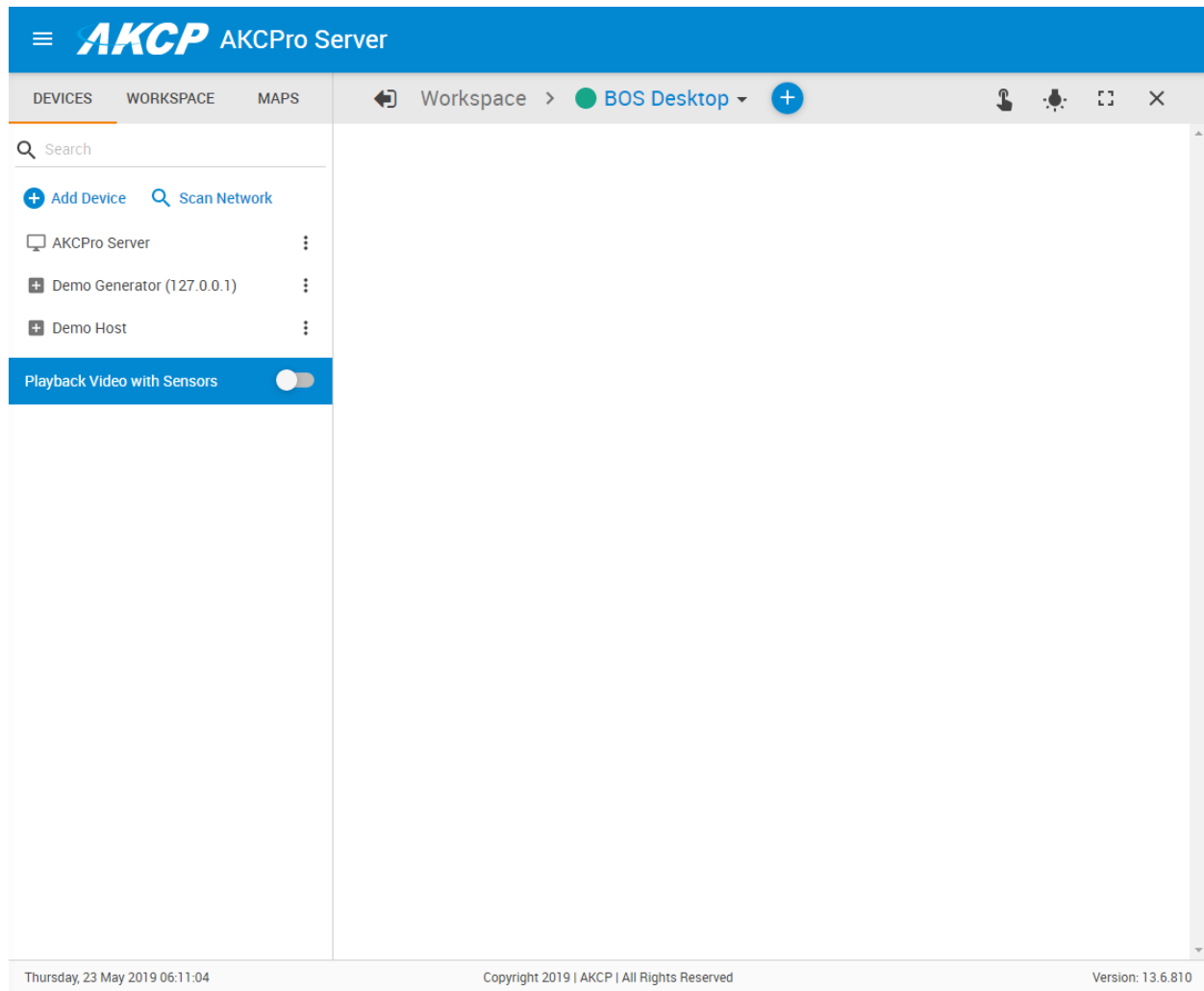


Warehouse



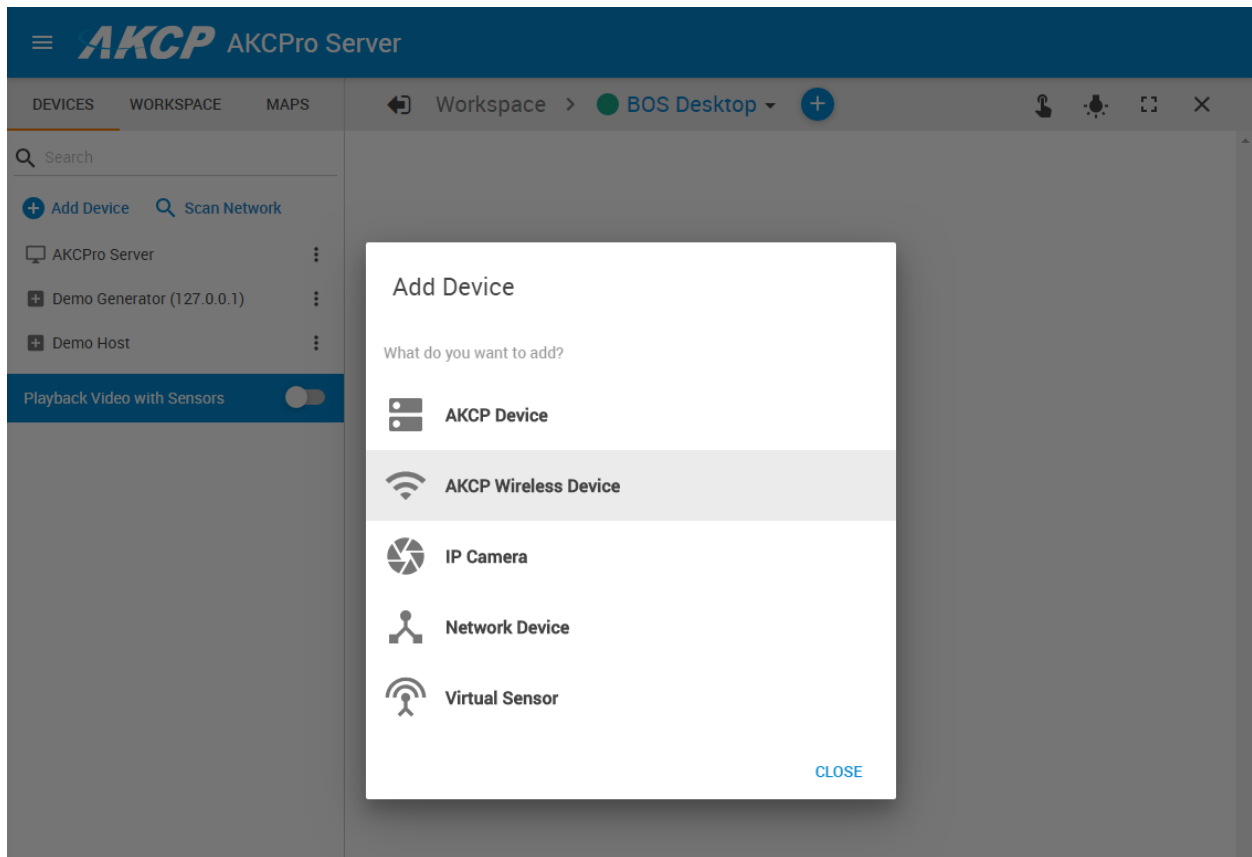
Cold storage

Adding wireless sensors



The wireless sensors are needed to be added to L-DCIM then paired (data sync) before they can work together.

Click on the **Add Device** link to begin adding your wireless sensor.



Choose **AKCP Wireless Device** from the list.

Add new wireless device

Device Type

AKCP Sensor

System Name

Device Network Address (Hex)

Network Session Key (Hex)

Application Session Key (Hex)

CANCEL

ADD

In the popup window, make sure the **Device Type** is set to **AKCP Sensor**.

For the **System Name** parameter give it a meaningful value, such as the sensor type (ex. LBTH). You can modify it later.

Now you'll need to fill out the **sensor's network parameters carefully**.

To avoid mistakes, it is highly recommended to copy-paste the long HEX keys from a text file rather than typing them in. If you mistype a character or number, the sensor won't be able to be synced with the unit!

In future software releases, there will be an easier way to add the network parameters.

See below for an example of correct sensor parameters.

Add new wireless device

Device Type

AKCP Sensor

System Name

LBTH-BATT #14

Device Network Address (Hex)

19510092

Network Session Key (Hex)

ABC61586AE8943CF077060E5F533B39E

Application Session Key (Hex)

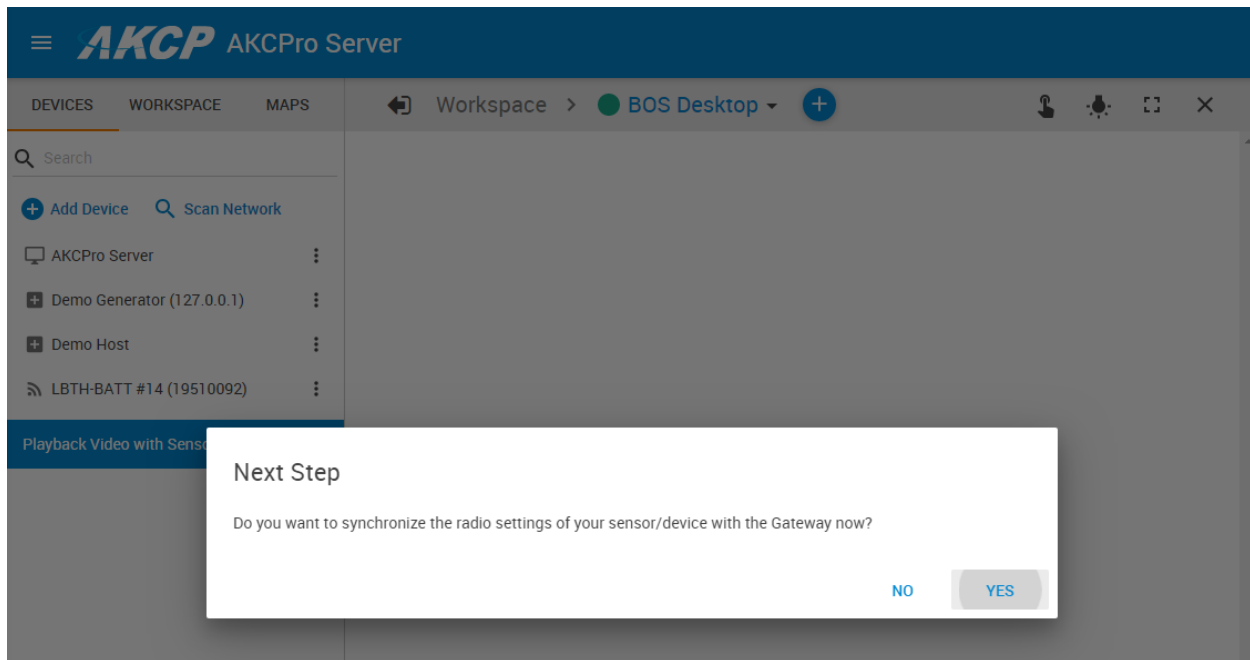
A93DE599569D7B720A4670982CEC35A1

CANCEL

ADD

On this sample picture, we'll add a LBTH wireless sensor to L-DCIM.
The network keys for the sensor are copied and pasted from a text file.

Click on the **Add** button when all the parameters are set.



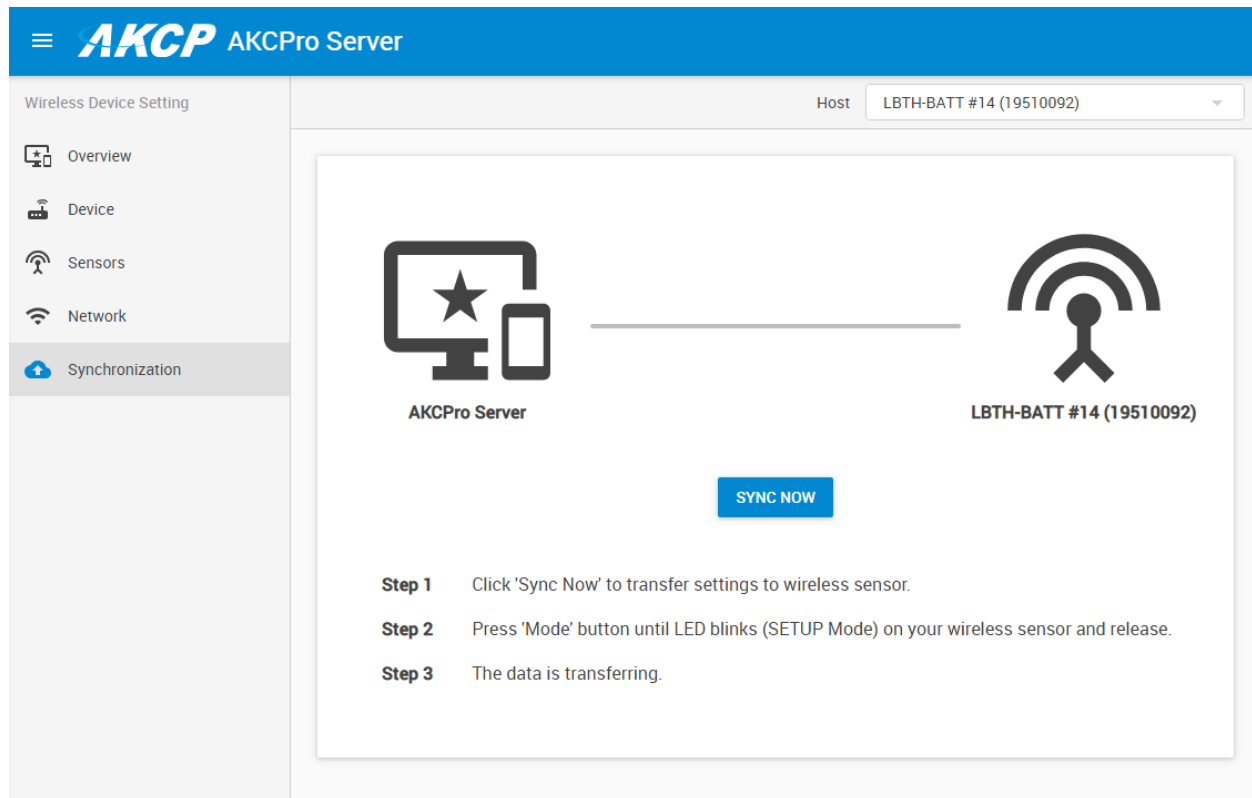
After you click **Add**, the sensor will be added to the APS console but couldn't receive any data yet. The system will ask if you'd like to immediately sync the sensor, so that it can get the sensor's data readings.

Sync is required for each sensor; otherwise they won't be paired and couldn't be used. We'll describe the sync process below.

Note: if you haven't yet enabled the unit's LoRa radio interface and chosen a wireless channel, the unit will first ask you to enable this interface. See details for configuring the wireless channels in this manual's Server Settings section.

Important: you might have to sync the sensor twice. The first is to initialize the network parameters, and the second is for setting the sensor thresholds. With only one sync the sensor parameters might not be correct.

Wireless sensor synchronization

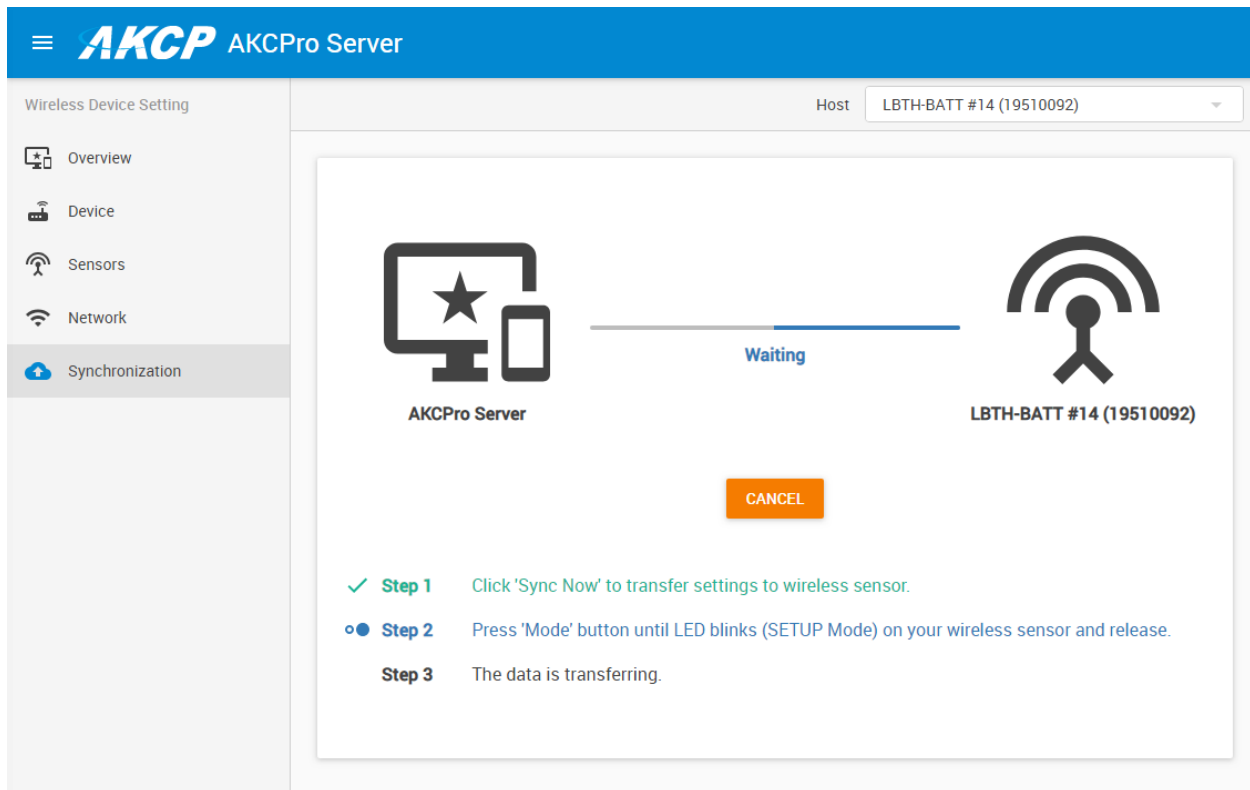


The sync wizard needs to be run every time when you change a wireless sensor specific setting, such as the sensor thresholds for a LBTH temperature sensor. You'll be notified to re-sync the sensor if you change a setting that requires it.

The wizard has 3 steps to follow; we'll describe each step below in detail.

Important: you'll need to have physical access to the wireless sensor in order to be able to press the Mode button on it. You cannot sync the sensor if you cannot press the button.

Press the **Sync Now** button to start the sync wizard (first step).

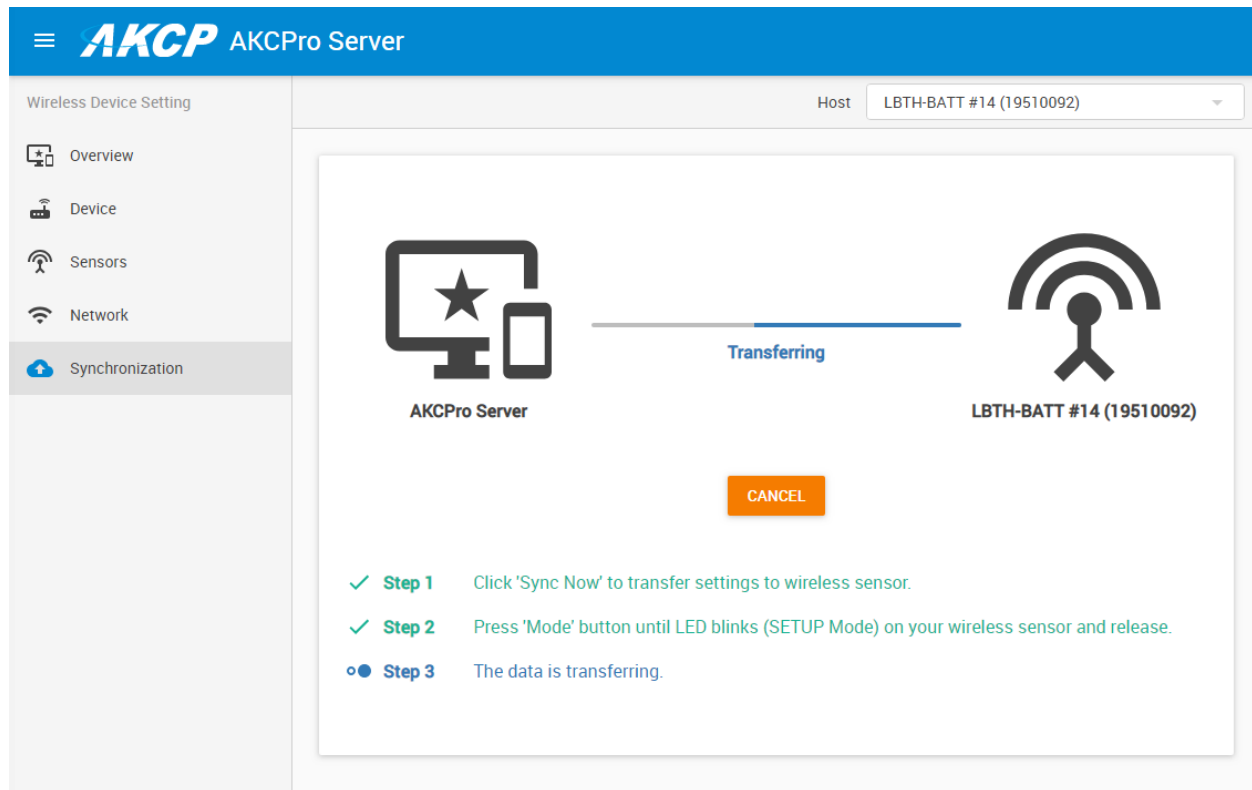


In the second step, APS will prepare the parameters for the sensor, switch to the sync radio frequency (channel #6) and wait for a reply from the sensor with the network key values specified.

Now you need to press and hold the Mode button on your wireless sensor until its LED starts to blink fast (after approx. 3-4 seconds) then release. The fast LED blinking is an identification that the sensor is now in SETUP mode and can receive the new parameters by radio packets from L-DCIM.

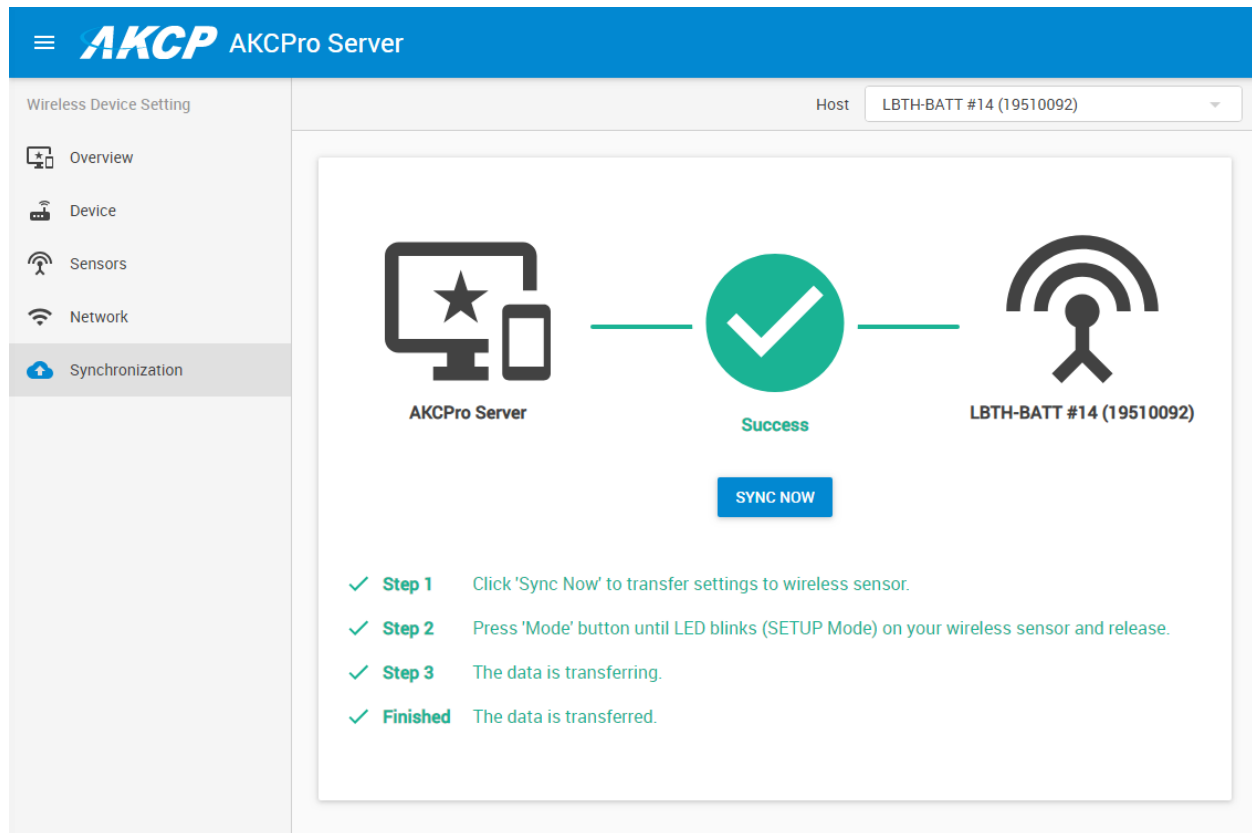
The second step will timeout after 60 seconds; if there was no reply from the wireless sensor during this period, the sync process will cancel and the system will return to the normal radio frequency again.

Check below at the troubleshooting section if your sensor cannot sync.



The wizard will proceed to step 3 only if it receives acknowledgement packet from the wireless sensor that it has entered SETUP mode and can receive the new parameters.

Then the unit will transfer the configuration parameters to the sensor, and set up the system to receive data from the sensor.



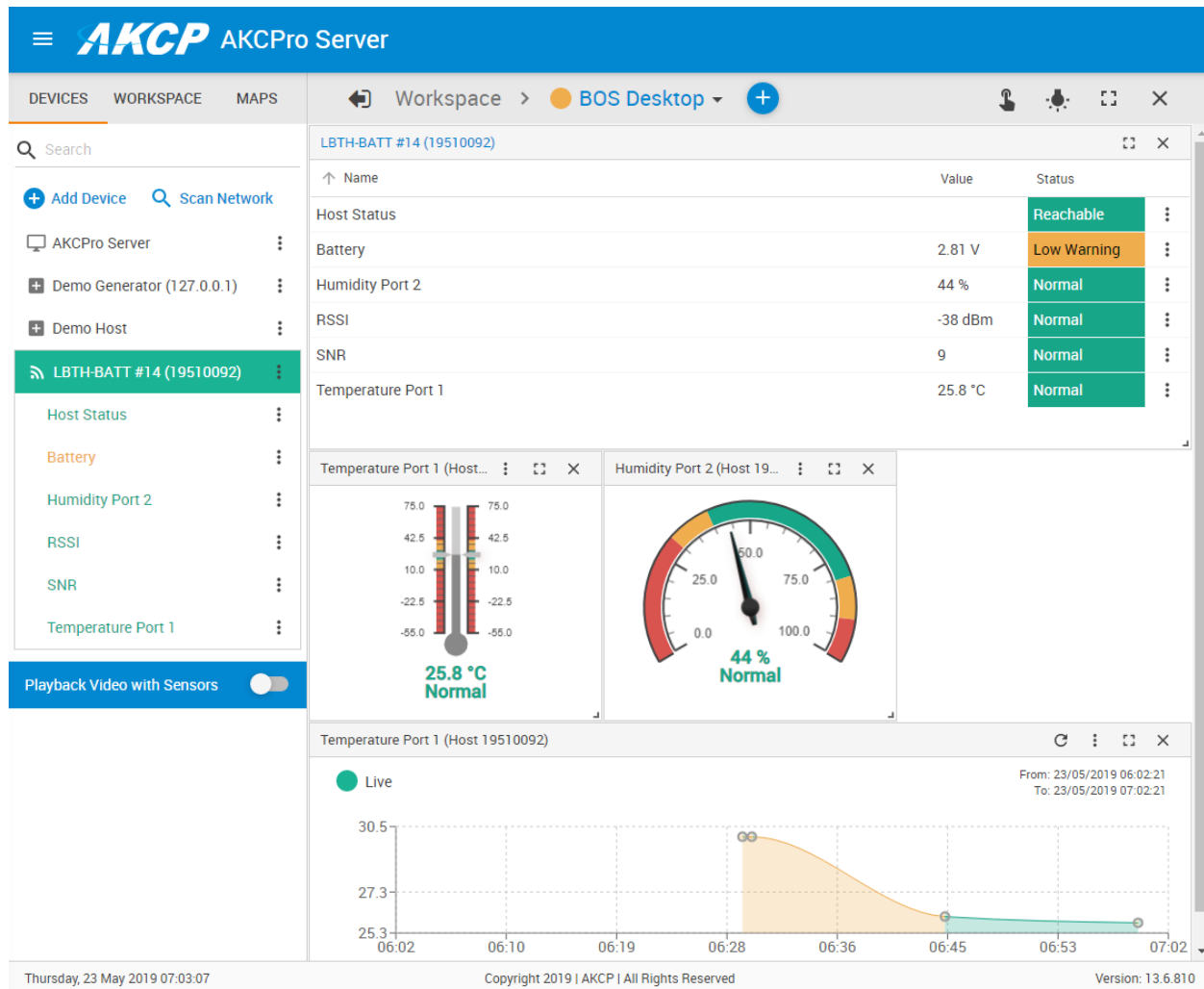
After the sync has been completed, your sensor will periodically transmit radio data packets and basically behave like any other non-wireless sensor.

Sync troubleshooting

If your sensor cannot be synced, check the following:

- Double-check the wireless sensor network parameters. Even one character mistake can make the sync fail. You can remove and re-add the sensor or edit its parameters.
- Check the antennas on both the L-DCIM and wireless sensor side. Antennas are required to be used at all times even if the sensor and the unit are in close range.
- Ensure there is no other strong radio or magnetic interference in the area that could disrupt the communication between wireless sensor and L-DCIM.
- Check that the wireless sensor is powered on and in Run mode. Press and hold the Mode button on it and watch the status LED. If it doesn't blink, the sensor could have a damaged firmware, or failed internal battery. The firmware can be re-flashed again (see in this manual's firmware update section for the steps). The batteries are not user replaceable.
- Check the battery voltage on the sensor (if it has been added to your unit before). Low voltages will prevent the sync to successfully finish and the process will be stuck at step #2. If possible, connect your sensor to USB power source then the sync should work.
- If you have another L-DCIM unit, you could set it to wireless radio channel #6 and watch the network packets. Channel #6 is the wireless sensor sync frequency and there should be packets sent/received during sync mode with a wireless sensor (even if the other unit is not the sender).

Important: you might have to sync the sensor twice. The first is to initialize the network parameters, and the second is for setting the sensor thresholds. With only one sync the sensor parameters might not be correct.



After your sensor has been synced, you can add gauges and enable graph for the sensor the same way like with any other supported sensor type.

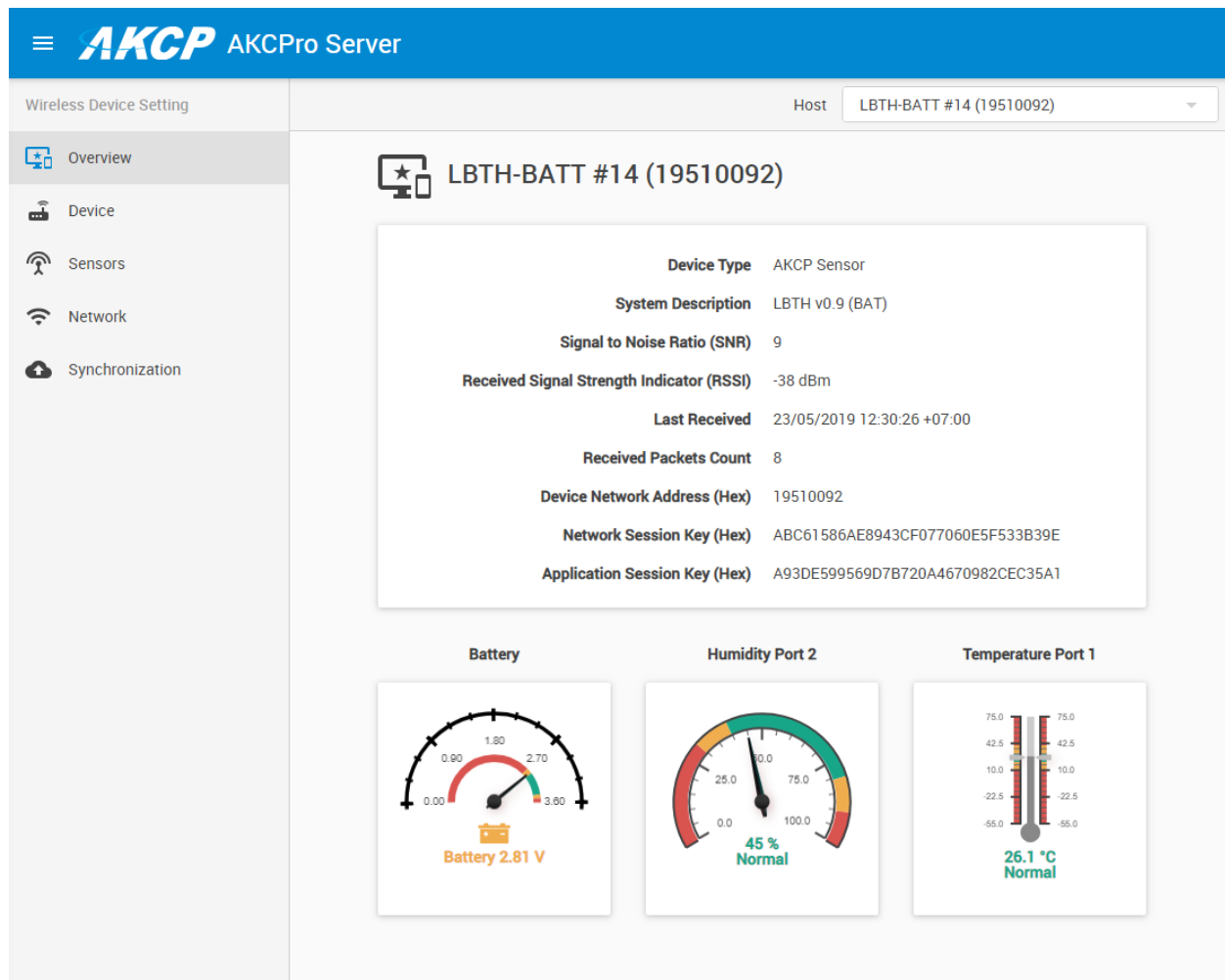
Note: since the wireless sensor is not permanently connected to the unit but only by radio data packets, there can be some cases when they become “unreachable” state. This state means that the L-DCIM unit hasn’t received a data packet from the sensor over the specified timeout value.

This can also happen when a backup file was restored on the unit - you can force-send a packet from the sensor by pressing its Mode button once, then the sensor will became reachable again. Otherwise it will be reachable state again when the pre-defined sensor packet interval occurs (see below).

Wireless sensor parameter setup

On the following pages we'll describe the specific wireless sensor property pages.

Overview



After you've synced the sensor, it will display a quick summary of the wireless sensor, such as:

The network key values, radio signal quality, packet received count and the list of the internal sensors on the wireless sensor.

If you haven't yet synced the sensor with L-DCIM and just added it to the console, this page will just display the entered network values and no packet received count:

AKCP AKCPro Server

Wireless Device Setting

Overview

Device

Sensors

Network

Synchronization

Host

LBTH-BATT #14 (19510092)

LBTH-BATT #14 (19510092)

| | |
|---|----------------------------------|
| Device Type | AKCP Sensor |
| System Description | |
| Signal to Noise Ratio (SNR) | 0 |
| Received Signal Strength Indicator (RSSI) | 0 dBm |
| Last Received | 01/01/1970 07:00:00 +07:00 |
| Received Packets Count | 0 |
| Device Network Address (Hex) | 19510092 |
| Network Session Key (Hex) | ABC61586AE8943CF077060E5F533B39E |
| Application Session Key (Hex) | A93DE599569D7B720A4670982CEC35A1 |

Device

☰

AKCP

AKCPro Server

Wireless Device Setting

HostLBTH-BATT #14 (19510092)

Overview

Device

Sensors

Network

Synchronization

Device

Settings / Device

Device

Device TypeAKCP Sensor

System DescriptionLBTH v0.9 (BAT)

Signal to Noise Ratio (SNR)9

Received Signal Strength Indicator (RSSI)-26 dBm

Last Received24/05/2019 12:44:25 +07:00

Received Packets Count202

Settings

System Name

LBTH-BATT #14

System Location

System Contact

System URL

http://www.example.com

After you've synced the sensor, this page will display the network key values, packet received count and radio signal quality.

Here you can edit the sensor's network parameters and system name as well (see below).

Scroll down for the Settings part where you can edit the network key parameters, System Name, Contact, GPS coordinates etc:

Settings

System Name

LBTH-BATT #14

System Location

System Contact

System URL

http://www.example.com

GPS Latitude

GPS Longitude

Device Network Address (Hex)

19510092

Network Session Key (Hex)

ABC61586AE8943CF077060E5F533B39E

Application Session Key (Hex)

A93DE599569D7B720A4670982CEC35A1

SAVE

CANCEL

If you haven't yet synced the sensor with L-DCIM, this page will just display the entered network values (where you can edit them if necessary) and the received packet count will be 0:

AKCP

AKCPro Server

Wireless Device Setting

Overview

Device

Sensors

Network

Synchronization

Host

LBTH-BATT #14 (19510092)

Device

Settings / Device

Device

Device Type

AKCP Sensor

System Description

Signal to Noise Ratio (SNR)

0

Received Signal Strength Indicator (RSSI)

0 dBm

Last Received

01/01/1970 07:00:00 +07:00

Received Packets Count

0

Settings

System Name

LBTH-BATT #14

System Location

System Contact

System URL

http://www.example.com

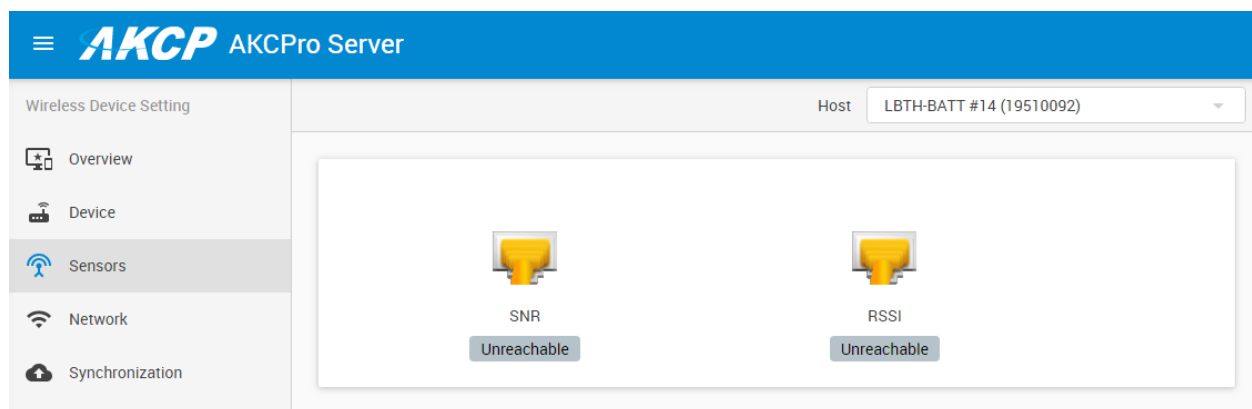
Sensors

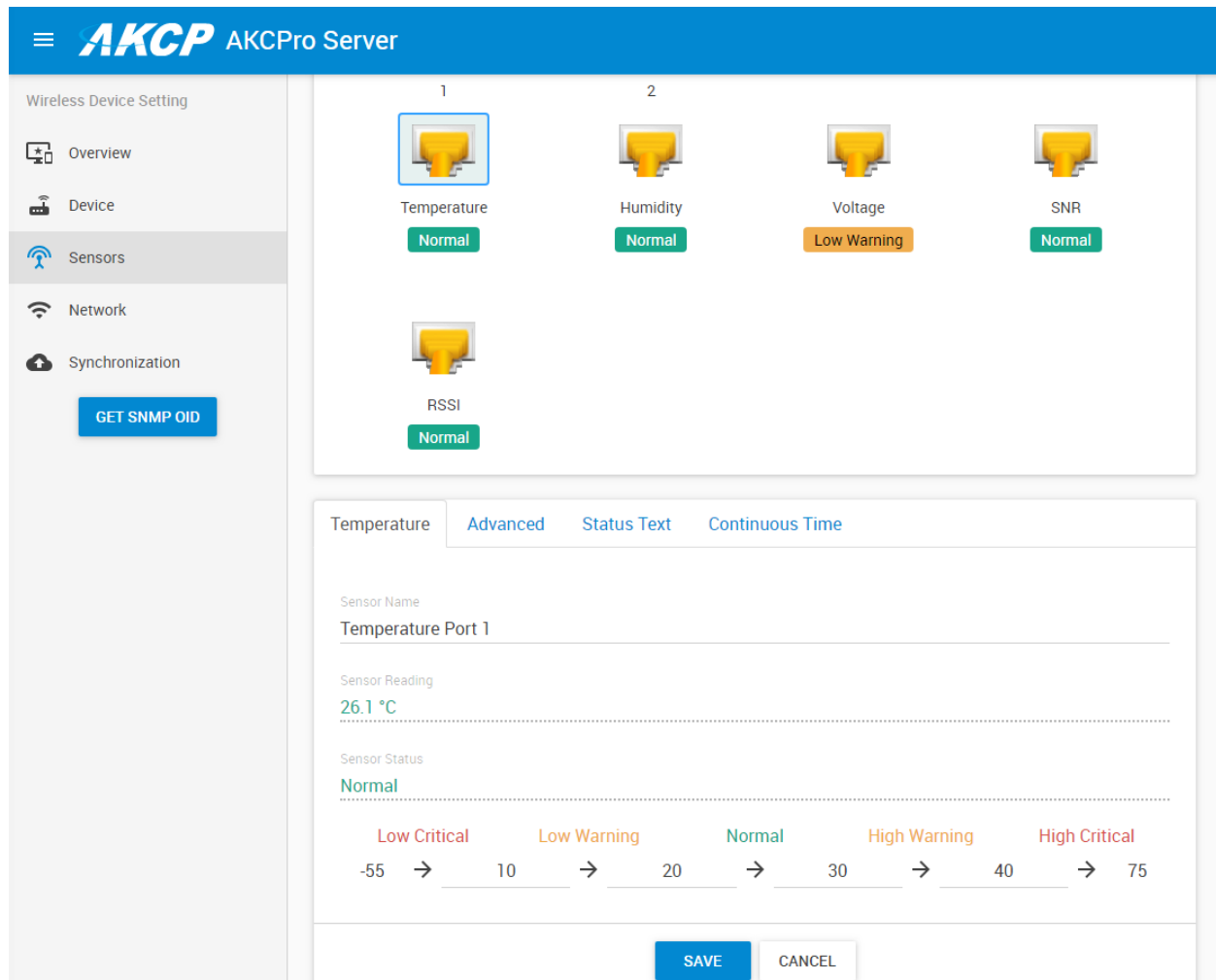


This page will display the wireless sensor's internal sensors. Click on each sensor for details and configuration. See below for examples.

If you haven't yet synced the sensor with L-DCIM, this page will just display the 2 predefined radio signal sensors that each wireless sensor has: the SNR (signal to noise ratio) and the RSSI (received signal strength indication).

These sensors are present for each wireless sensor, regardless of their type.





The screenshot displays the AKCP Pro Server interface. On the left, a sidebar lists navigation options: Overview, Device, Sensors (selected), Network, and Synchronization. Below these is a 'GET SNMP OID' button. The main area shows a grid of sensor status cards for Temperature, Humidity, Voltage, SNR, and RSSI. The Temperature card is highlighted with a blue border. Below the grid, a detailed configuration panel for the Temperature sensor is shown, including tabs for Temperature, Advanced, Status Text, and Continuous Time. The configuration includes fields for Sensor Name (Temperature Port 1), Sensor Reading (26.1 °C), and Sensor Status (Normal). A threshold scale is visible at the bottom of the panel, ranging from -55 to 75, with markers for Low Critical, Low Warning, Normal, High Warning, and High Critical. The panel concludes with SAVE and CANCEL buttons.

For example, on the LBTH type sensors you would have a Temperature and a Humidity sensor. You can configure them the same way as you would with any other Temperature or Humidity sensor:

You can change threshold values, sensor name, status description, continuous time etc. see below for details.

For each sensor that supports SNMP addressing, you'll find the **Get SNMP OID** button on the left.

SNMP OID of Temperature Port 1 - Google Chrome

Not secure | <https://10.1.6.37/app.html#/oid?id=44&type=512&name=Temperature%20Port%201&system=0>

SNMP OID of Temperature Port 1

| Description ▲ | Syntax ▼▲ | Access ▼▲ | SNMP OID ▲ |
|-------------------------------|----------------|------------|-----------------------------------|
| commonIndex | DISPLAY STRING | read-only | .1.3.6.1.4.1.3854.2.3.1.1.1.44 |
| commonId | INTEGER | read-only | .1.3.6.1.4.1.3854.2.3.1.1.1000.44 |
| commonDescription | DISPLAY STRING | read-write | .1.3.6.1.4.1.3854.2.3.1.1.2.44 |
| commonType | INTEGER | read-only | .1.3.6.1.4.1.3854.2.3.1.1.3.44 |
| commonValue | INTEGER | read-only | .1.3.6.1.4.1.3854.2.3.1.1.4.44 |
| commonUnit | DISPLAY STRING | read-only | .1.3.6.1.4.1.3854.2.3.1.1.5.44 |
| commonStatus | INTEGER | read-only | .1.3.6.1.4.1.3854.2.3.1.1.6.44 |
| commonGoOffline | INTEGER | write-only | .1.3.6.1.4.1.3854.2.3.1.1.8.44 |
| commonRaw | INTEGER | read-only | .1.3.6.1.4.1.3854.2.3.1.1.20.44 |
| commonPort | INTEGER | read-only | .1.3.6.1.4.1.3854.2.3.1.1.35.44 |
| commonSubPort | INTEGER | read-only | .1.3.6.1.4.1.3854.2.3.1.1.36.44 |
| commonDisplayStyle | INTEGER | read-write | .1.3.6.1.4.1.3854.2.3.1.1.45.44 |
| commonHighCriticalDescription | DISPLAY STRING | read-write | .1.3.6.1.4.1.3854.2.3.1.1.46.44 |
| commonLowCriticalDescription | DISPLAY STRING | read-write | .1.3.6.1.4.1.3854.2.3.1.1.47.44 |
| commonSensorNormalDescription | DISPLAY STRING | read-write | .1.3.6.1.4.1.3854.2.3.1.1.48.44 |
| commonLowWarningDescription | DISPLAY STRING | read-write | .1.3.6.1.4.1.3854.2.3.1.1.49.44 |

You can open the SNMP OID list in a popup window that will list the OIDs that you can query/set from any other SNMP enabled network device.

Temperature

Advanced

Status Text

Continuous Time

Rearm

1

Graph Enable

Disable

Data Collection Type

Instantaneous

SAVE

CANCEL

In the **Advanced** tab you can change the sensor's rearm value, enable/disable the graph and change the data collection type.

On newer versions (13.6.892 and up) you'll be also able to change between Celsius/Fahrenheit units. For details of these parameters, please refer to other AKCP sensor manuals.

| Temperature | Advanced | Status Text | Continuous Time |
|---------------|---------------|-------------|-----------------|
| High Critical | High Critical | | |
| High Warning | High Warning | | |
| Normal | Normal | | |
| Low Warning | Low Warning | | |
| Low Critical | Low Critical | | |
| Sensor Error | Sensor Error | | |

In the **status text** tab you can change the displayed text for each sensor status.

Please note: wireless sensors could usually just display “unreachable” state and not “sensor error” if there’s any error with the received packets. This is because of the sensor’s nature: you can either receive radio packets or cannot, and the sensor is not permanently connected to the unit as the conventional wired sensors.

| | | | |
|-------------|----------|-------------|-----------------|
| Temperature | Advanced | Status Text | Continuous Time |
|-------------|----------|-------------|-----------------|

High Critical (second)

0

High Warning (second)

0

Normal (second)

0

Low Warning (second)

0

Low Critical (second)

0

Sensor Error (second)


0

SAVE

CANCEL


You can also edit the **continuous time** settings; for details of these parameters, please refer to other AKCP sensor manuals.

Common sensors




Temperature

Normal




Humidity

Normal




Voltage

Low Warning



SNR

Normal



RSSI

Normal

Voltage

Advanced

Status Text

Sensor Name

Battery

Sensor Reading

2.81 V

Sensor Status

Low Warning

Low Critical Low Warning Normal High Warning High Critical

0 → 2.7 → 2.85 → 3.4 → 3.5 → 3.6

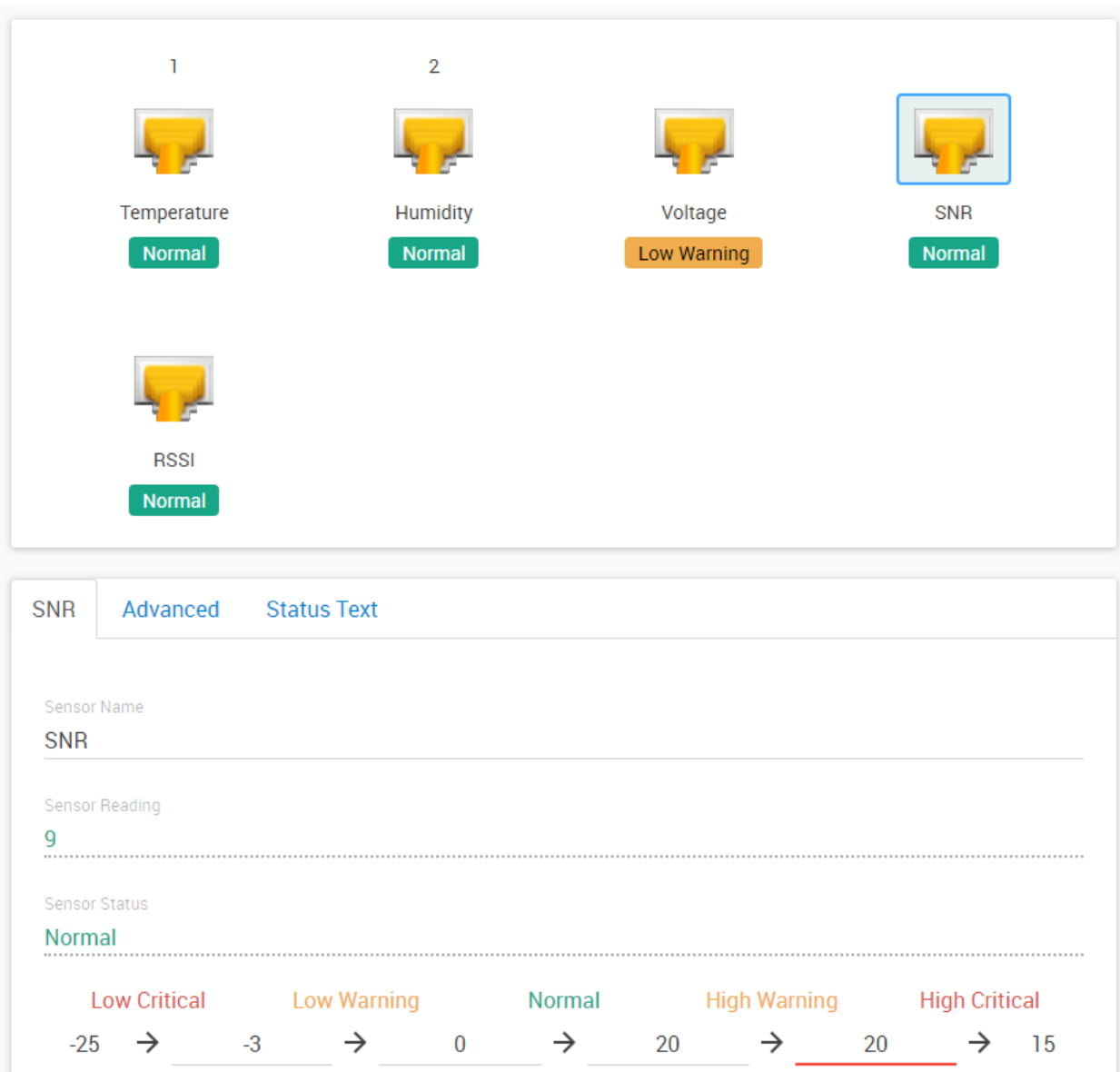
SAVE

CANCEL

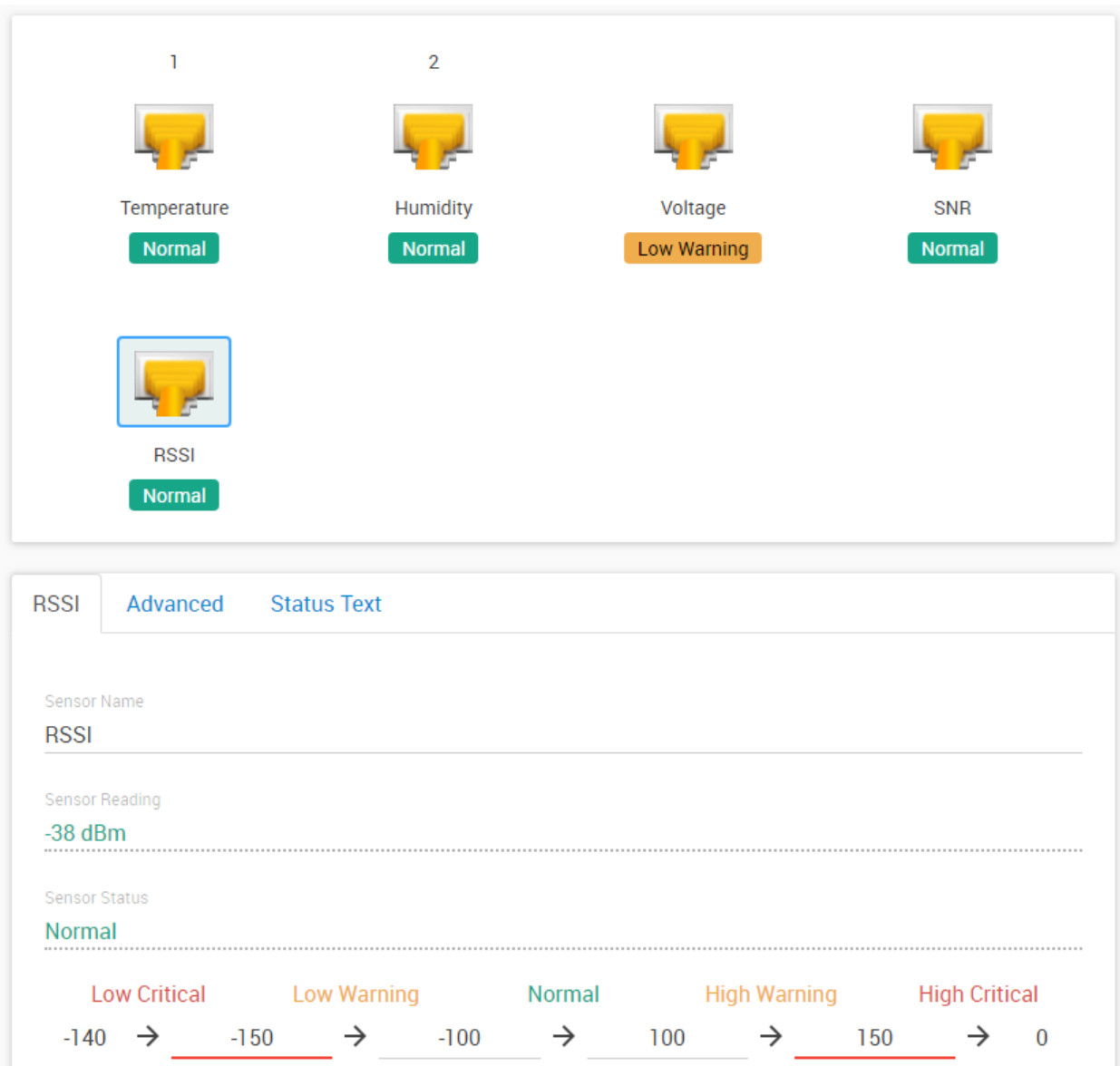
Every wireless sensor has a **Voltage sensor**, even if it's a USB type. You shouldn't need to modify the displayed thresholds.

For battery-only type sensors, the displayed reading will show the status of the sensor's internal batteries. If the voltage drops below the critical level, your sensor will stop working. With longer data transmission settings (see below) the battery would be good for approx. 10 years, but their life can be considerably shortened if you specify very short packet transmission times.

For USB type sensors, the displayed voltage is what the sensor's integrated MCU receives through the USB port.

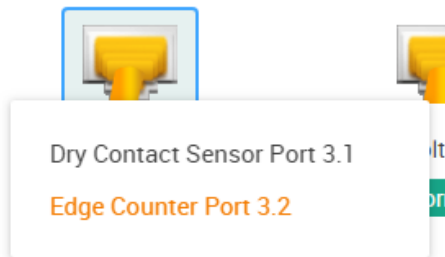


This informational sensor indicates the radio signal's SNR value (signal to noise ratio). In high noise ratio environments the sensor might not work correctly (there will be many lost packets).



This informational sensor indicates the radio signal's RSSI value (received signal strength indication). With poor RSSI values the sensor might not work correctly (there will be many lost packets).

Edge Counter sensor



All dry contact/switch type sensors on the wireless sensors have an edge counter sensor, which is an indication on how many times the input has changed state. It increments every time the dry contact changes state.

However if it changes too often or too fast, the wireless sensor cannot transmit a packet for each changes instantly due to duty cycle regulation and also to reduce packet loss or collisions. This counter value is transmitted at each minimum broadcasting interval (aka keep-alive) depending on customer setting (see the following pages at Network settings).

Edge Counter
Advanced

Sensor Name
Edge Counter Port 3.2

Sensor Reading
55

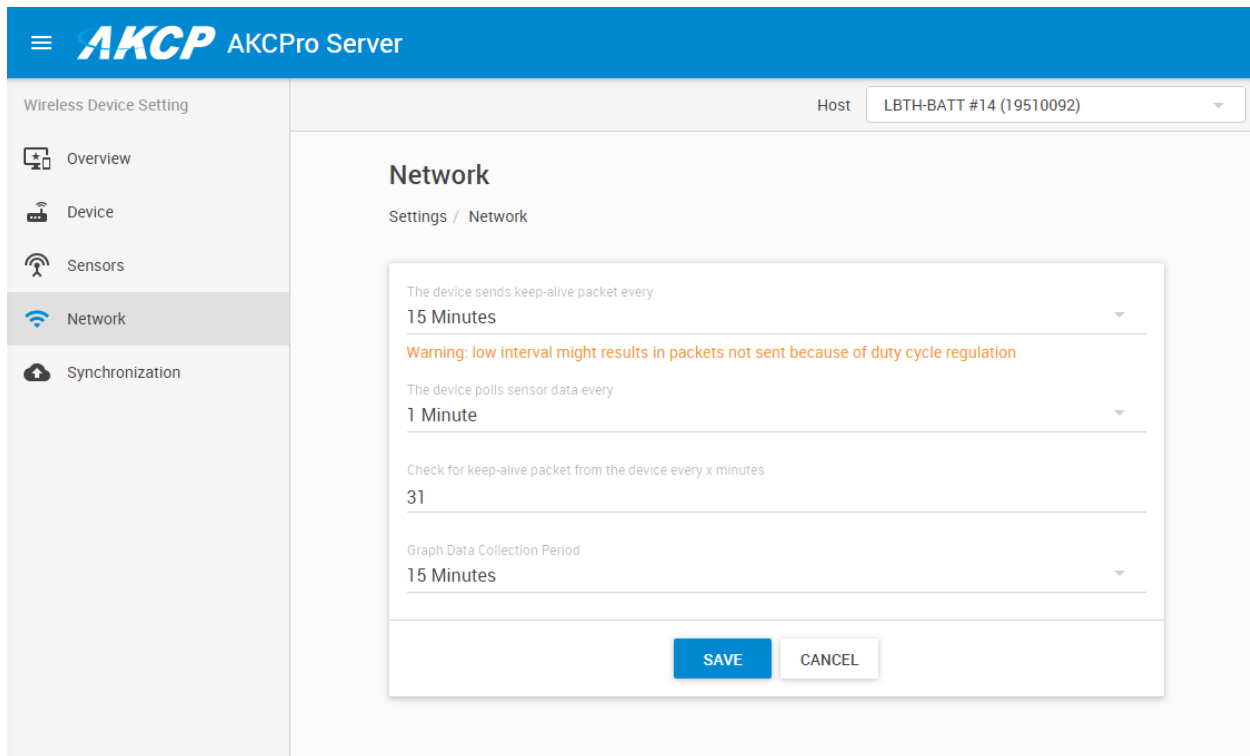
Sensor Status
Normal

Last Reset
N/A

RESET

Optionally the counter can be reset, then the date/time of the last reset will be shown.

Network



AKCP AKCPro Server

Wireless Device Setting

Host LBTH-BATT #14 (19510092)

Network

Settings / Network

The device sends keep-alive packet every
15 Minutes

Warning: low interval might results in packets not sent because of duty cycle regulation

The device polls sensor data every
1 Minute

Check for keep-alive packet from the device every x minutes
31

Graph Data Collection Period
15 Minutes

SAVE CANCEL

This is an important part of the wireless sensor configuration: here you can specify the sensor's packet sending, keep-alive and data collection periods.

For battery-only type sensors, you should use longer intervals to keep the sensor's internal batteries working for longer. If the voltage drops below the critical level, your sensor will stop working. Also with a low battery voltage the sensor couldn't sync its settings anymore. Using longer data transmission settings, the battery would be good for approx. 10 years, but their life can be considerably shortened if you specify very short packet transmission times.

Device keep-alive packet:

This parameter defines how often the wireless sensor will send a notification data packet to the L-DCIM indicating it's still online and working, along with non-critical sensor and graph data. The more wireless sensors you have, the longer the keep-alive parameter should be to avoid packet collisions. This parameter has big effect on battery life, therefore it's recommended to use USB type sensors if quick data polling and fast graphing is required.

You may also force-send a keep-alive packet by pressing the Mode button on the sensor.

Note: the wireless sensor's edge counter value is only sent with the keep-alive packet.

Sensor data polling:

This parameter defines how often the wireless sensor will collect data from its integrated sensors. This parameter also has a big effect on battery life.

Important note: if the sensor registers a status change on its internal sensor, ex. from “normal” to “high warning” on the temperature, it will immediately send a notification packet to L-DCIM regardless of the polling parameter. The polling parameter is just the periodic sensor data check parameter; if the value usually stays the same then there’s no need to decrease the poll period.

Check for keep-alive packet:

This parameter is used on the L-DCIM side, to check if the wireless sensor is still online and transmitting packets. It has to be equal to or greater than the keep-alive packet send parameter of the wireless sensor (the first parameter on the list).

Graph data collection period:

This parameter defines how often the wireless sensor should store the graph data internally. The sensor will continue to record graphing data in its own flash memory even if the L-DCIM is unreachable. A wireless sensor can store about a month’s graph data internally. When the L-DCIM unit becomes reachable again, the graph data will be gradually sent back to the unit from the sensor.

Note: graph data for the non-critical internal sensors (SNR, RSSI, Voltage) won’t be stored on the wireless sensor, and their values only update with the keep-alive packet.

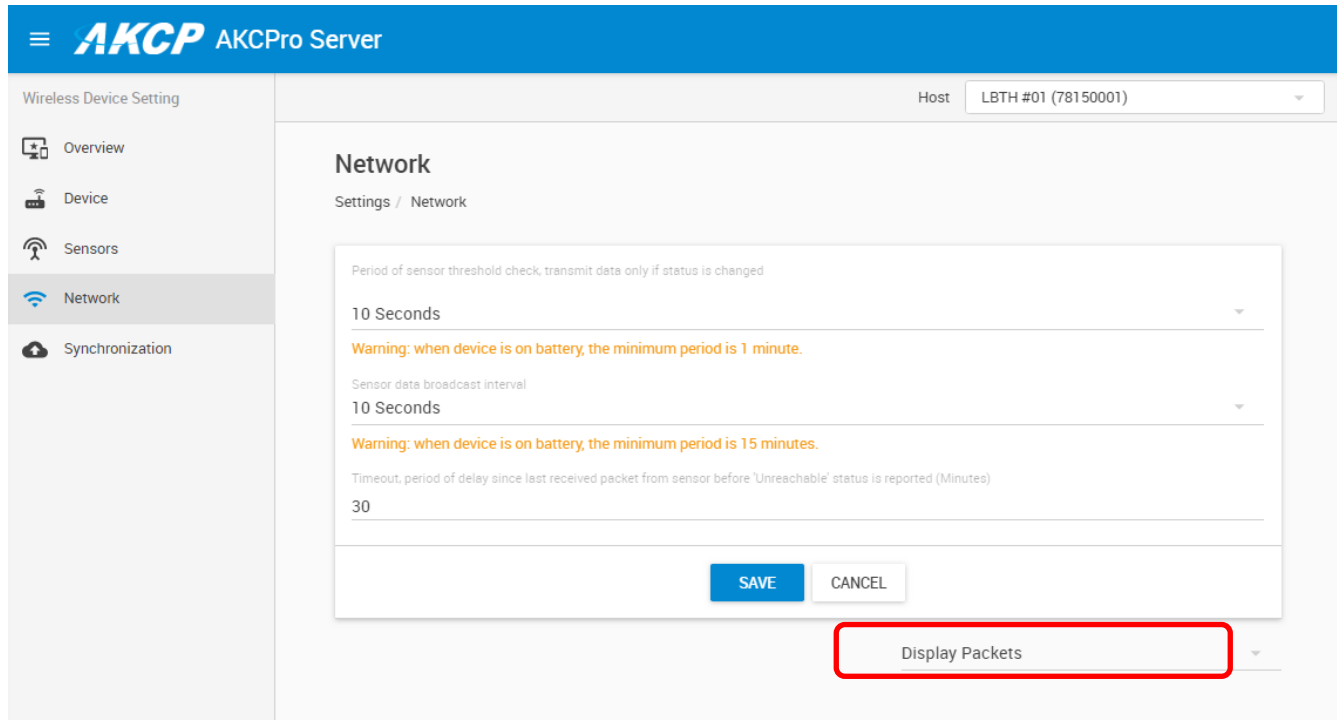
Important note: the stored graph values are only for the internal sensors such as temperature and humidity, but not the radio signal sensors that are counted on the L-DCIM such as SNR and RSSI. If the sensor becomes unreachable, it is normal to see gaps in the graphs for the non-integrated sensors. The wireless sensors shouldn’t have missing gaps in the graph for their own internal sensors.

On newer firmware (after image 186) you’ll also see a packet logger feature on this Network tab, which can help troubleshooting your sensor. See below about how to use this feature.

Incoming packets logger feature

This feature is added in newer firmware (after L-DCIM image 186). It helps to diagnose and troubleshoot wireless sensor problems.

Each received packet (except setup packets) will be logged under Hosts menu, on the Network tab for each wireless sensor host.



AKCPPro Server

Host: LBTH #01 (78150001)

Wireless Device Setting

- Overview
- Device
- Sensors
- Network**
- Synchronization

Network

Settings / Network

Period of sensor threshold check, transmit data only if status is changed

10 Seconds

Warning: when device is on battery, the minimum period is 1 minute.

Sensor data broadcast interval

10 Seconds

Warning: when device is on battery, the minimum period is 15 minutes.

Timeout, period of delay since last received packet from sensor before 'Unreachable' status is reported (Minutes)

30

SAVE CANCEL

Display Packets

None

Short

Detailed

By default, the packet logging is turned off.

You can choose to display Short or Detailed packet information.

Normally the Short style is enough to easily see the transmitted and received packets. See below for examples.

Each packet has:

- state (which is used for icon, success/failure)
- short description (one line short packet description)
- long description (multiline packet description)
- error description (which is required for support engineer)

Display Packets - Short ▼

Incoming Packet Queue

🔍 Search

| |
|--|
| ✓ 26/09/2019 04:51:17: Graph data packet |
| ✓ 26/09/2019 04:51:30: Graph data packet |
| ✓ 26/09/2019 04:51:49: Graph data packet |
| ✓ 26/09/2019 04:51:52: Graph data packet |
| ✓ 26/09/2019 04:51:54: Graph data packet |
| ✓ 26/09/2019 04:51:57: Graph data packet |
| ✓ 26/09/2019 04:52:07: Graph data packet |
| ✓ 26/09/2019 04:52:14: Graph data packet |
| ✓ 26/09/2019 04:52:27: Graph data packet |
| ✓ 26/09/2019 04:52:37: Graph data packet |
| ✓ 26/09/2019 04:52:47: Graph data packet |
| ✓ 26/09/2019 04:52:57: Graph data packet |
| ✓ 26/09/2019 04:53:24: Graph data packet |
| ✓ 26/09/2019 04:53:30: Graph data packet |
| ✓ 26/09/2019 04:53:37: Graph data packet |
| ✓ 26/09/2019 04:53:47: Graph data packet |
| ✓ 26/09/2019 04:53:57: Graph data packet |
| ✓ 26/09/2019 04:54:07: Graph data packet |
| ✓ 26/09/2019 04:54:23: Graph data packet |
| ✓ 26/09/2019 04:54:25: Graph data packet |

Outgoing Packet Queue

🔍 Search

| |
|--|
| → 24/09/2019 10:26:19: RTC synchronization |
| → 25/09/2019 10:25:45: RTC synchronization |

On this picture with the short logging you can see normal sensor traffic: the wireless sensor transmits the collected graph data back to the unit, and receives RTC clock sync packets to keep the time in sync.

There are several packet types that are shown in the log:

Configuration packet

Configuration packet: device type: {}, firmware version: {}, power source: {}, sensors count: {}
sensor #{}: compound ID: ({}, {}, {}, {}, {}), sensor type: {}, graph data: {}
- where {} is a placeholder for appropriate value

Events data packet

Events data packet: events count: {}
event #{}: timestamp: {}, type: {} ({}): reboots count: {}, last reboot reason code: {}
event #{}: timestamp: {}, type: {} ({}): power source: {}
event #{}: timestamp: {}, type: {} ({}): sensor #{}: sensor ID: {}, timestamp: {}, sensor status: {}, sensor value: {}
- where {} is a placeholder for appropriate value

Sensors data packet

Sensors data packet: sensors count: {}
sensor #{}: sensor ID: {}, timestamp: {}, sensor status: {}, sensor value: {}
- where {} is a placeholder for appropriate value

Graph data packet

Graph data packet: graphs count: {}, graph data block timestamp: {}, graph data points count: {}
- where {} is a placeholder for appropriate value

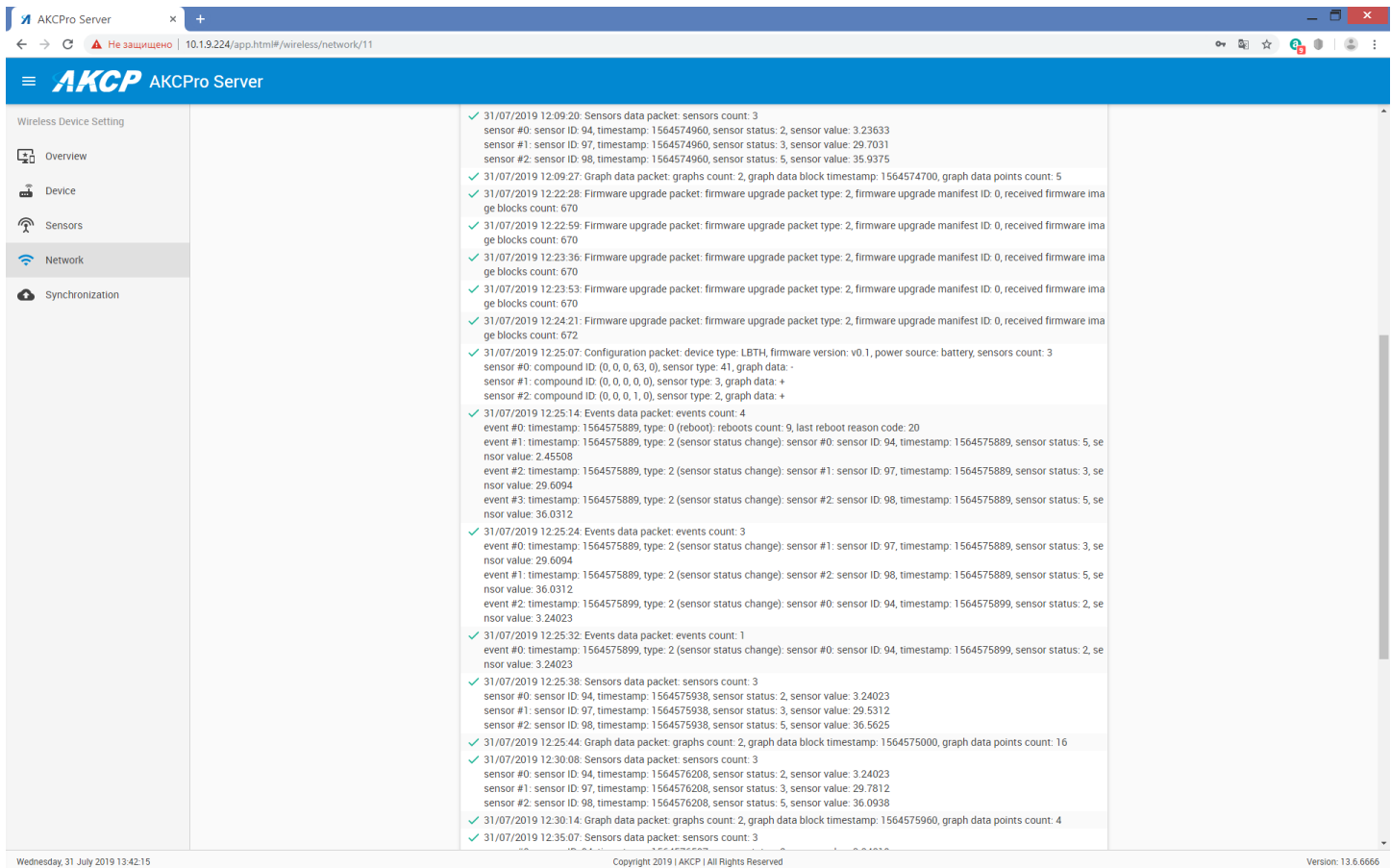
Setup packets

Firmware upgrade packet

Firmware upgrade packet: firmware upgrade packet type: {}, firmware upgrade manifest ID: {},
received firmware image blocks count: {}
- where {} is a placeholder for appropriate value

Synchronization packet

Synchronization packet: packet ID: {}
- where {} is a placeholder for appropriate value



AKCP Pro Server

Wireless Device Setting

- Overview
- Device
- Sensors
- Network
- Synchronization

31/07/2019 12:09:20: Sensors data packet: sensors count: 3
 sensor #0: sensor ID: 94, timestamp: 1564574960, sensor status: 2, sensor value: 3.23633
 sensor #1: sensor ID: 97, timestamp: 1564574960, sensor status: 3, sensor value: 29.7031
 sensor #2: sensor ID: 98, timestamp: 1564574960, sensor status: 5, sensor value: 35.9375

31/07/2019 12:09:27: Graph data packet: graphs count: 2, graph data block timestamp: 1564574700, graph data points count: 5

31/07/2019 12:22:28: Firmware upgrade packet: firmware upgrade packet type: 2, firmware upgrade manifest ID: 0, received firmware image blocks count: 670

31/07/2019 12:22:59: Firmware upgrade packet: firmware upgrade packet type: 2, firmware upgrade manifest ID: 0, received firmware image blocks count: 670

31/07/2019 12:23:36: Firmware upgrade packet: firmware upgrade packet type: 2, firmware upgrade manifest ID: 0, received firmware image blocks count: 670

31/07/2019 12:23:53: Firmware upgrade packet: firmware upgrade packet type: 2, firmware upgrade manifest ID: 0, received firmware image blocks count: 670

31/07/2019 12:24:21: Firmware upgrade packet: firmware upgrade packet type: 2, firmware upgrade manifest ID: 0, received firmware image blocks count: 672

31/07/2019 12:25:07: Configuration packet: device type: LBTH, firmware version: v0.1, power source: battery, sensors count: 3
 sensor #0: compound ID: (0, 0, 0, 63, 0), sensor type: 41, graph data: -
 sensor #1: compound ID: (0, 0, 0, 0, 0), sensor type: 3, graph data: +
 sensor #2: compound ID: (0, 0, 0, 1, 0), sensor type: 2, graph data: +

31/07/2019 12:25:14: Events data packet: events count: 4
 event #0: timestamp: 1564575889, type: 0 (reboot): reboots count: 9, last reboot reason code: 20
 event #1: timestamp: 1564575889, type: 2 (sensor status change): sensor #0: sensor ID: 94, timestamp: 1564575889, sensor status: 5, sensor value: 2.45508
 event #2: timestamp: 1564575889, type: 2 (sensor status change): sensor #1: sensor ID: 97, timestamp: 1564575889, sensor status: 3, sensor value: 29.6094
 event #3: timestamp: 1564575889, type: 2 (sensor status change): sensor #2: sensor ID: 98, timestamp: 1564575889, sensor status: 5, sensor value: 36.0312

31/07/2019 12:25:24: Events data packet: events count: 3
 event #0: timestamp: 1564575889, type: 2 (sensor status change): sensor #1: sensor ID: 97, timestamp: 1564575889, sensor status: 3, sensor value: 29.6094
 event #1: timestamp: 1564575889, type: 2 (sensor status change): sensor #2: sensor ID: 98, timestamp: 1564575889, sensor status: 5, sensor value: 36.0312
 event #2: timestamp: 1564575899, type: 2 (sensor status change): sensor #0: sensor ID: 94, timestamp: 1564575899, sensor status: 2, sensor value: 3.24023

31/07/2019 12:25:32: Events data packet: events count: 1
 event #0: timestamp: 1564575899, type: 2 (sensor status change): sensor #0: sensor ID: 94, timestamp: 1564575899, sensor status: 2, sensor value: 3.24023

31/07/2019 12:25:38: Sensors data packet: sensors count: 3
 sensor #0: sensor ID: 94, timestamp: 1564575938, sensor status: 2, sensor value: 3.24023
 sensor #1: sensor ID: 97, timestamp: 1564575938, sensor status: 3, sensor value: 29.5312
 sensor #2: sensor ID: 98, timestamp: 1564575938, sensor status: 5, sensor value: 36.5625

31/07/2019 12:25:44: Graph data packet: graphs count: 2, graph data block timestamp: 1564575000, graph data points count: 16

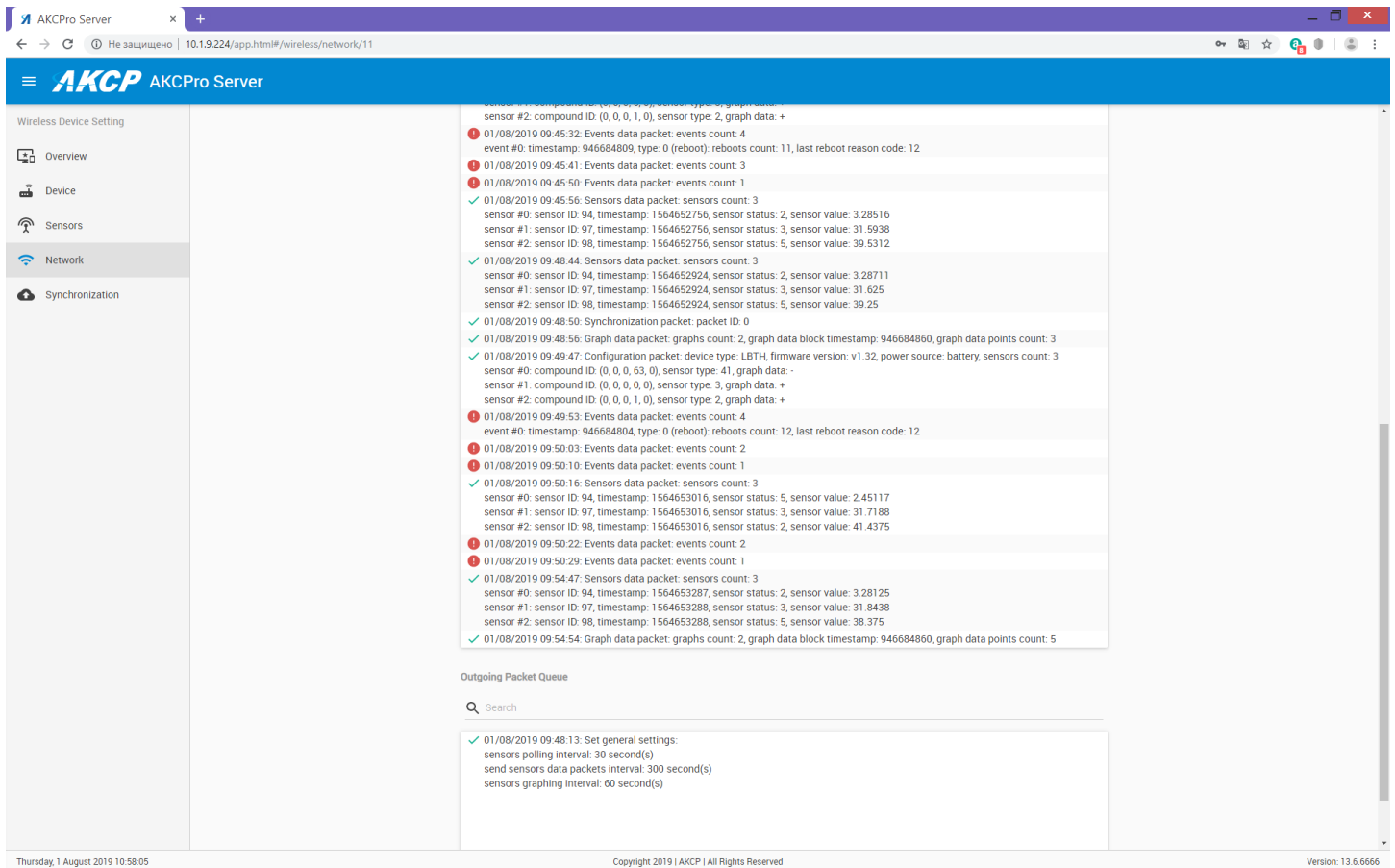
31/07/2019 12:30:08: Sensors data packet: sensors count: 3
 sensor #0: sensor ID: 94, timestamp: 1564576208, sensor status: 2, sensor value: 3.24023
 sensor #1: sensor ID: 97, timestamp: 1564576208, sensor status: 3, sensor value: 29.7812
 sensor #2: sensor ID: 98, timestamp: 1564576208, sensor status: 5, sensor value: 36.0938

31/07/2019 12:30:14: Graph data packet: graphs count: 2, graph data block timestamp: 1564575960, graph data points count: 4

31/07/2019 12:35:07: Sensors data packet: sensors count: 3

Wednesday, 31 July 2019 13:42:15 Copyright 2019 | AKCP | All Rights Reserved Version: 13.6.6666

On this example picture with detailed logs you can see firmware upgrade, graph data, configuration- and sensor value packets logged.



The screenshot displays the AKCPPro Server web interface. The left sidebar contains navigation links: Overview, Device, Sensors, Network (selected), and Synchronization. The main content area shows a detailed log of events and sensor data. The log entries include timestamps, event counts, sensor IDs, timestamps, sensor status, sensor value, and graph data. The log is organized into sections, with some entries marked with a red 'X' icon indicating errors or warnings. The bottom section of the log shows the 'Outgoing Packet Queue' with a search bar and a list of configuration settings.

Wireless Device Setting

- Overview
- Device
- Sensors
- Network
- Synchronization

01/08/2019 09:45:32: Events data packet: events count: 4
event #0: timestamp: 946684809, type: 0 (reboot): reboots count: 11, last reboot reason code: 12
01/08/2019 09:45:41: Events data packet: events count: 3
01/08/2019 09:45:50: Events data packet: events count: 1
01/08/2019 09:45:56: Sensors data packet: sensors count: 3
sensor #0: sensor ID: 94, timestamp: 1564652756, sensor status: 2, sensor value: 3.28516
sensor #1: sensor ID: 97, timestamp: 1564652756, sensor status: 3, sensor value: 31.5938
sensor #2: sensor ID: 98, timestamp: 1564652756, sensor status: 5, sensor value: 39.5312
01/08/2019 09:48:44: Sensors data packet: sensors count: 3
sensor #0: sensor ID: 94, timestamp: 1564652924, sensor status: 2, sensor value: 3.28711
sensor #1: sensor ID: 97, timestamp: 1564652924, sensor status: 3, sensor value: 31.625
sensor #2: sensor ID: 98, timestamp: 1564652924, sensor status: 5, sensor value: 39.25
01/08/2019 09:48:50: Synchronization packet: packet ID: 0
01/08/2019 09:48:56: Graph data packet: graphs count: 2, graph data block timestamp: 946684860, graph data points count: 3
01/08/2019 09:49:47: Configuration packet: device type: LBTH, firmware version: v1.32, power source: battery, sensors count: 3
sensor #0: compound ID (0, 0, 0, 63, 0), sensor type: 41, graph data: -
sensor #1: compound ID (0, 0, 0, 0, 0), sensor type: 3, graph data: +
sensor #2: compound ID (0, 0, 0, 1, 0), sensor type: 2, graph data: +
01/08/2019 09:49:53: Events data packet: events count: 4
event #0: timestamp: 946684804, type: 0 (reboot): reboots count: 12, last reboot reason code: 12
01/08/2019 09:50:03: Events data packet: events count: 2
01/08/2019 09:50:10: Events data packet: events count: 1
01/08/2019 09:50:16: Sensors data packet: sensors count: 3
sensor #0: sensor ID: 94, timestamp: 1564653016, sensor status: 5, sensor value: 2.45117
sensor #1: sensor ID: 97, timestamp: 1564653016, sensor status: 3, sensor value: 31.7188
sensor #2: sensor ID: 98, timestamp: 1564653016, sensor status: 2, sensor value: 41.4375
01/08/2019 09:50:22: Events data packet: events count: 2
01/08/2019 09:50:29: Events data packet: events count: 1
01/08/2019 09:54:47: Sensors data packet: sensors count: 3
sensor #0: sensor ID: 94, timestamp: 1564653287, sensor status: 2, sensor value: 3.28125
sensor #1: sensor ID: 97, timestamp: 1564653288, sensor status: 3, sensor value: 31.8438
sensor #2: sensor ID: 98, timestamp: 1564653288, sensor status: 5, sensor value: 38.375
01/08/2019 09:54:54: Graph data packet: graphs count: 2, graph data block timestamp: 946684860, graph data points count: 5

Outgoing Packet Queue

Search

01/08/2019 09:48:13: Set general settings:
sensors polling interval: 30 second(s)
send sensors data packets interval: 300 second(s)
sensors graphing interval: 60 second(s)

Thursday, 1 August 2019 10:58:05 Copyright 2019 | AKCP | All Rights Reserved Version: 13.6.6666

Another example picture with detailed logs, which has some error events as well as a configuration packet for setting sensor polling intervals.

Wireless sensor firmware update

Wireless sensor firmware can be updated in 2 ways:

- Firmware Update Over The Air (FOTA)
- Firmware update with direct USB connection to L-DCIM unit (faster)

Below we'll describe the steps, but the WebUI might look different on your unit.

In both cases, the unit will update all sensors of the same type (based on the firmware binary file), therefore you'll need to re-run the update for different sensor types.

If the firmware you attempt to upgrade to is lower version than what is already on the unit, then the upgrade will fail.

Very important: on older system firmware the upgrade can only run if the sensor is powered by USB! Even the battery-only sensors have a USB port for this purpose. On newer firmware (after image 180) the battery-only sensors can now do FOTA upgrade without USB connection.

FOTA update


 Probe Manager ^

 Host State

 Configuration

 Notification

 Firmware

 Wireless Device Firmware

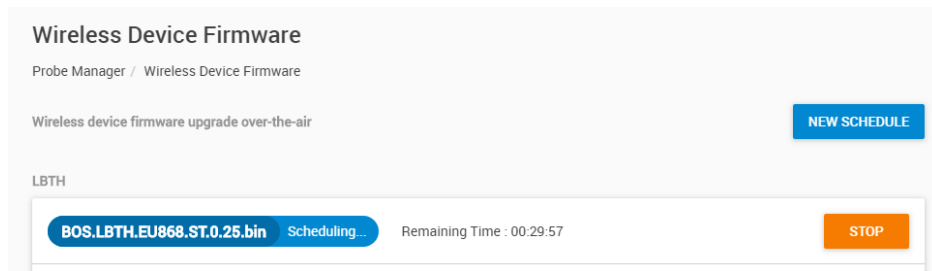
 History

This is a method of updating the wireless sensor firmware over the air, with radio packets only.

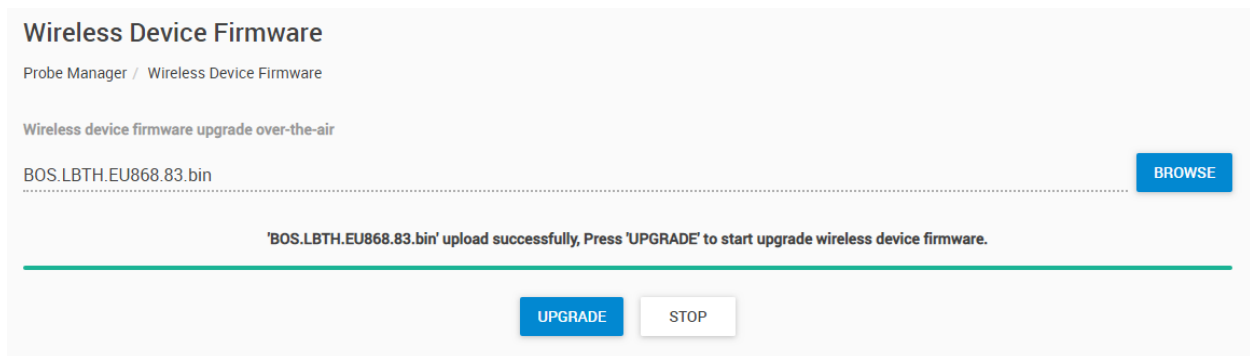
It takes a long time due to the packet send, receive and verify mechanism.

Open the main menu, and expand the **ProbeManager** menu.

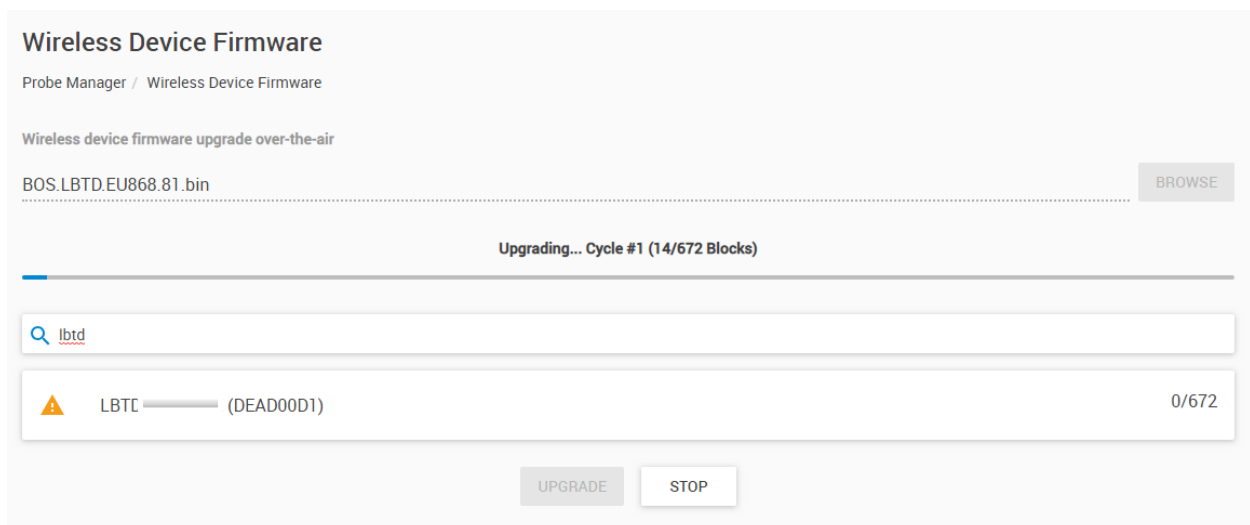
Click on the **Wireless Device Firmware** option.



Note: on newer firmware (after image 180) the FOTA update process has been changed slightly. You will still need to proceed the steps mentioned below, but first you will have to make a schedule for the upgrade (between 30 minutes and 1 day) instead of immediately upgrading. This has been done to improve the efficiency of the upgrade, and let each sensor have time to prepare for the upgrade.



First you'll need to select your firmware binary file. It will define which sensor types it can update. It needs to be uploaded to the L-DCIM unit first with the **Upload** button. Then press the **Upgrade** button to start.



First cycle: the unit sends the update packets, and asks the wireless sensors if they received all correctly.

Note: the wireless sensor will stop transmitting packets and enter pause mode during the upgrade (if it doesn't receive further packets it will return to normal mode after a few minutes).

The sensors which have already started receiving update packets will change their status to pending (blue icon):

Wireless Device Firmware

Probe Manager / Wireless Device Firmware

Wireless device firmware upgrade over-the-air

BOS.LBTD.EU868.81.bin BROWSE

Getting upgrade status...

| | |
|--|---------|
| <div> ● </div> <div>LBTD (DEAD00D1)</div> | 669/672 |
|--|---------|

UPGRADE
STOP

Those which didn't respond will remain in yellow warning state (no answer) and they won't be updated.

Wireless Device Firmware

Probe Manager / Wireless Device Firmware

Wireless device firmware upgrade over-the-air

BOS.LBTD.EU868.81.bin BROWSE

Upgrading... Cycle #2 (236/672 Blocks)

| | |
|--|---------|
| <div> ● </div> <div>LBTD (DEAD00D1)</div> | 669/672 |
|--|---------|

UPGRADE
STOP

Second cycle: the unit asks the sensors for the missing packets and it will resend them, until no wireless sensor asks for further packets.

Wireless Device Firmware

Probe Manager / Wireless Device Firmware

Wireless device firmware upgrade over-the-air

BOS.LBTD.EU868.81.bin
BROWSE

Getting upgrade status...

| | | |
|---|-------------------------------|---------|
| ✓ | LBTI <div></div> : (DEAD00D1) | 672/672 |
|---|-------------------------------|---------|

UPGRADE
STOP

Third cycle: the unit will wait until it doesn't receive any packet queries from the wireless sensors, then display "upgrade successful" on the WebUI.

In this case the "upgrade successful" message means that the firmware was sent to the air and each wireless sensor has responded that they got the new firmware successfully.

After this step, the wireless sensors will begin the upgrade by themselves.

Note: the graphing will still run on the sensors while in upgrade mode, the sensor will store graph data inside of its flash and send to L-DCIM later.


After the wireless sensor has finished the upgrade, it will return to normal running mode by itself, and start to send data packets again.

Usually the upgrade has finished when the wireless sensor reports its new firmware version number.


In case the upgrade fails for some reason, you can recover the sensor by flashing the firmware with the USB method (see below).


USB upgrade

 Probe Manager ^

 Host State

 Configuration

 Notification

 Firmware

 Wireless Device Firmware

 History

Using the **ProbeManager's Firmware** option, you can upgrade the wireless sensor's firmware in a conventional way.

Important: the sensor needs to be directly connected to one of the L-DCIM unit's free USB ports via a USB data cable. If the cable doesn't provide USB data signaling, the upgrade will fail.

The ProbeManager might display an unknown error code if you attempt the upgrade without connecting the sensor via USB data cable, or if you attempt to downgrade the firmware version.

Note: with this method you can recover sensors that had earlier failed the upgrade, even if they're in "unreachable" state - but their network parameters have to be correct, and the sensor should not be removed from the APS console.

Firmware

Probe Manager / Firmware

Firmware File

BOS.LBTH.EU868.83.bin

BROWSE

Selected Hosts

↑ Host

↑ Status

Progress

ADD HOSTS

UPDATE NOW

CANCEL

First you need to select the firmware binary file with the **Browse** button.

| Selected Hosts | | | | | |
|-------------------------------------|--------------------------|----------|-------------|-----------------|-----------|
| ↑ Host | ↑ IP Address | State | Description | Firmware | |
| <input checked="" type="checkbox"/> | LBTH-BATT #14 (19510092) | 19510092 | Ready | LBTH v0.9 (BAT) | v0.9 |
| <input type="checkbox"/> | Test (1) | 1 | Unreachable | | |
| | | | | | CANCEL OK |

Next choose the sensor(s) you'd like to update with the **Add Host** button.


Firmware

Probe Manager / Firmware

Firmware File

BOS.LBTH.EU868.83.bin BROWSE

Selected Hosts ADD HOSTS

| ↑ Host | ↑ Status | Progress | |
|--------------------------|----------|----------|--|
| LBTH-BATT #14 (19510092) | Ready | - | HTTP  |

UPDATE NOW CANCEL

Click on the **Update Now** button to begin.

After this the upgrade will proceed like with other AKCP units: the firmware is uploaded to the sensor and then applied. The sensor will return to normal running mode after the upgrade.



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

Thanks for Choosing AKCP!