Date	22/01/2009 10:35
Last saved on	25/08/2021 15:40:00
Filename	ENG Manual DAS, S&G Pro, Master, v1

WRITTEN BY	VERIFIED BY	APPROVED BY
Full Name	**Full Name**	**Full Name**
Mario Elia	date + signature	date + signature

Purpose of the document

English manual for DAS, Scan&Go Pro CU5v2 controllers
Firmware version 2.1.4.
Commissioning via barcode cards and ProConfig Embeded

Document Management

DATE	AUTHOR(S)	VERSION	COMMENTS

Contents

1 Introduction

Dear customer. First of all, we'd like to thank you for choosing DAS Access&Revenue Control.

The DAS Scan&Go PRO range consists of **access control and payment solutions for vehicles and pedestrians**. We have a strong **focus on effective and efficient management of both regular and temporary users** (so to avoid unwanted users) and on **converting even relatively small parking facilities into profitable revenue car parks**.

That's why we develop and manufacture:

- A range of **access control products** in order to control both the periphery of your site and the exterior doors of your premises.
- **Pay stations and a manual cash register**, all compatible with our access control range, enabling even relatively small car parks to be converted into profitable car parks.

Our access control products are usually connected to different types of physical accesses such as automatic barriers, fences, tripods, etc. Our payment solutions allow you to run your sites for profit. All this without the need for a wired or wireless network by default. Electrical power is enough.

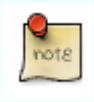
The entire range has been **developed on the basis of the principle of virtual communication**, whereby information transfer occurs **by default** via a carrier. This carrier can be, for example, a barcode or an RFID card. As a result, we have been able to productize (= making our products extremely plug&play as we do not need a central database) and democratize the business of parking systems, so that this market can now be approached perfectly via an indirect sales model.

In order to find the right balance between ease and cost of installation, performance, and low cost of ownership over the whole lifecycle of your purchase, we have developed a scalable and modular product range whose controllers operate by default in offline mode but also in online mode when more advanced features are required such as for example anti-passback, anti-passtime, counting, compatibility with a cloud application, VOIP intercom, etc...

To help you see connections between the different chapters in this manual, we have created cross-references. If you click on these blue coloured numbers you will be immediately taken to additional information about the topic you are reading.

2 The RC152cnbx.x/6.2 pay-in-lane station

This manual describes a pay-in-lane column which is the most complete variant of all DAS products as it combines both access & revenue control features. It includes: a CU5v2 controller with integrated graphic LCD display, a CCD barcode scanner, a thermal kiosk printer, a coin recycler with cash box, a bill recycler, a bank card terminal, a power supply, a heater, an RFID/NFC reader, a USB 4G modem/router and an embedded VOIP intercom. The last three features are always optional. Even if your DAS column is not equipped with all these devices/options, we do invite you to read the manual entirely as it will also help you to commission the configuration you've bought. Who can do more can do less.



The three possible payment methods are: coins, bills (banknotes) and bank cards. The available combinations are: coins, coins-bills, coins-bank cards, bank cards, coins-notes-bank cards.
Please note that an electronic payment cycle usually takes less time than a cash-payment cycle. In the case of a pay-in-lane column, cash payments can therefore lead to longer queues during peak times.

2.1 Description

The RC152cnbx.x pay-in-lane station is delivered fully assembled. It consists of:

- Aluminium column with dimensions: 633*340*1180mm, by default powder-coated in RAL 7016, other colours are optional.
- CU5v2 controller with integrated graphic LCD display
- 1D/2D CCD scanner
- Thermal paper kiosk printer
- Coins recycler
- Secured/lockable cash box
- Autofill bill (banknotes) recycler
- Worldline bank card terminal
- Power supply kit including a heater
- S&G Pro Identity card
- The RFID/NFC reader, embedded VOIP intercom, 4G modem/router, thermal paper roll and aluminium pedestal are optional.
- The aluminium pedestal is available in different heights to be compatible with use cases ranging from: pay-in-lane, disabled to pay-on-foot.

All Scan&Go Pro Access products (Vehicles & Pedestrians) are compatible with all Scan&Go Revenue products (manual cash desk, pay-on-foot and pay-in-lane column).

2.2 Good to know

DAS revenue columns allow you to charge your customers a variable rate (based on their parking duration) by simply scanning a barcode ticket printed by one of our printers (entry columns and/or desktop printers and/or virtual printers).
However, our revenue columns can also be configured for fixed-amount use cases (entrance of public toilets, public parks, fixed-rate car parks, etc.). In this configuration, the user pays the requested fixed amount without having to scan any ticket first, provided that the payment cycle was triggered by a presence detection.
Our payment columns can also be configured for a tokenization use case, whereby one just needs to present their same bank card to the entry and exit terminals, after which a payment transaction takes place automatically at the predetermined rate (variable or fixed).

The RC152cnbx.x pay station also accepts discount tickets (printed by a DAS Discount Printer, a DAS Barcode Updater, a POS cash register, a DAS entry column, a DAS desktop or virtual printer …) and credit barcode tickets. A credit ticket is a specific barcode that represents the value corresponding to a shortage of change that would occur after a cash payment.
In order to be taken into account, these credit and discount tickets can be scanned both before or after **a cash payment** but **always prior to an electronic payment** and always after having initialized the payment cycle by scanning an entry ticket or triggering a presence detection. When paying with a bank card, the system will always process the full amount shown on the display.

All DAS pay stations are compatible with DAS Scan&Go Pro access products. A basic commissioning can therefore be done only by using DAS command cards (offline mode). The free-of-charge configuration applications ProConfig Offline and ProConfig Embedded and the optional ProConfig Cloud allow advanced configuration.

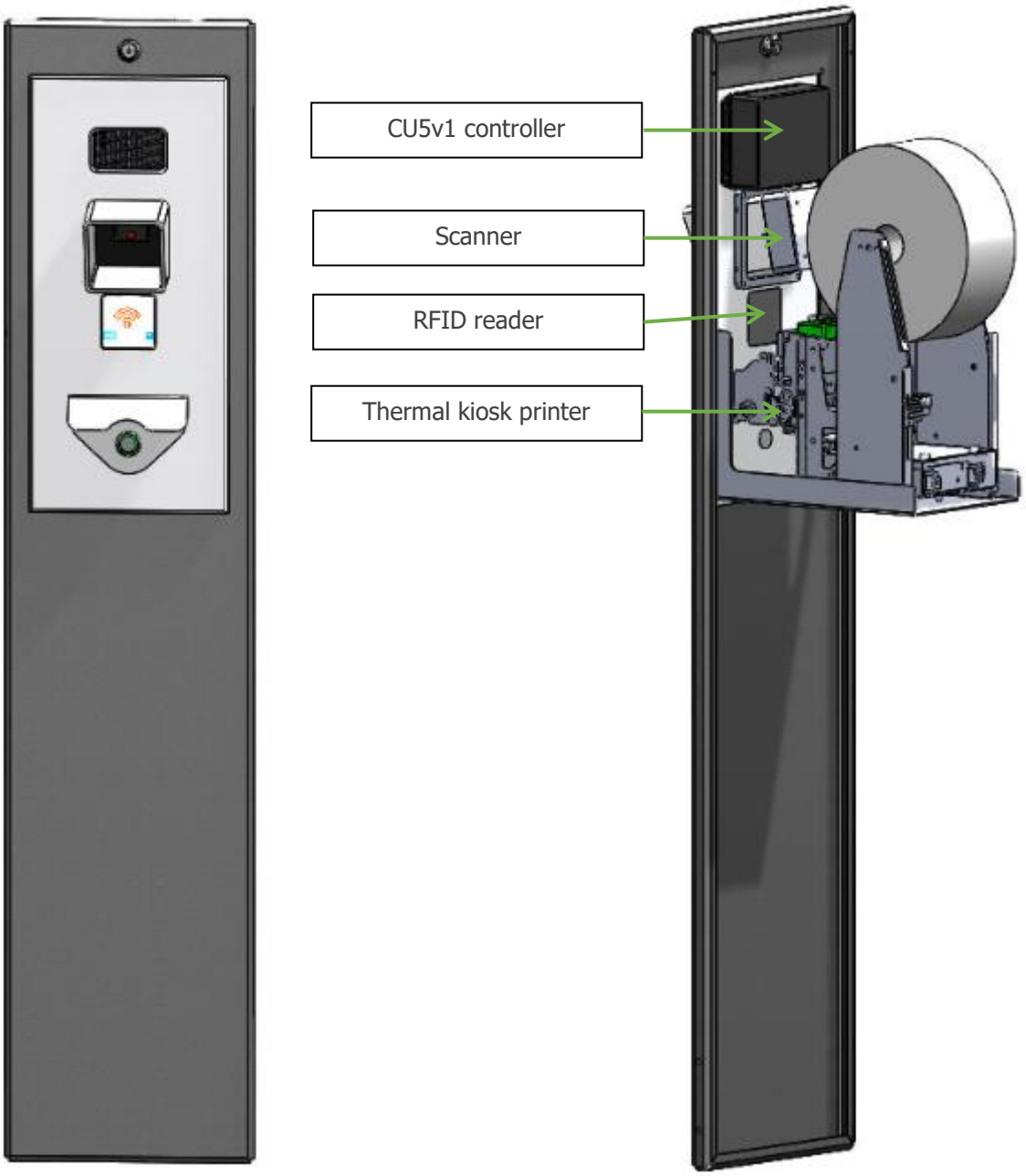
In this manual we'll help you with the first two commissioning principles (barcode command cards and ProConfig Embedded). For the other two applications ProConfig Embedded and ProConfig Cloud we refer to their respective manuals.

When installed outdoors, we recommend protecting the pay station column against direct weather conditions. Please contact your installer to inquire about our optional awnings.

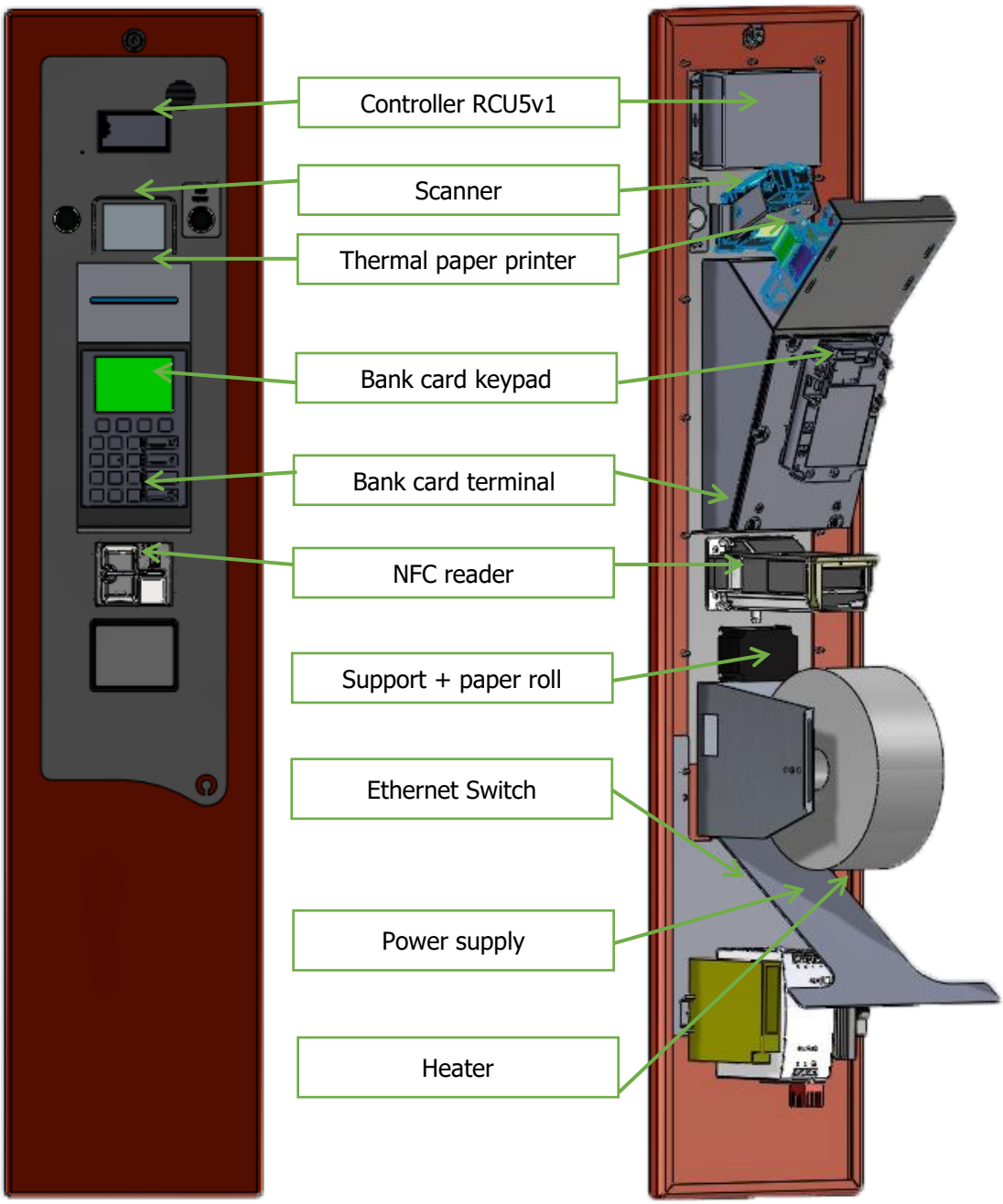
2.3 Column parts

2.3.1 Left door: scanner/printer access columns and cash only columns.

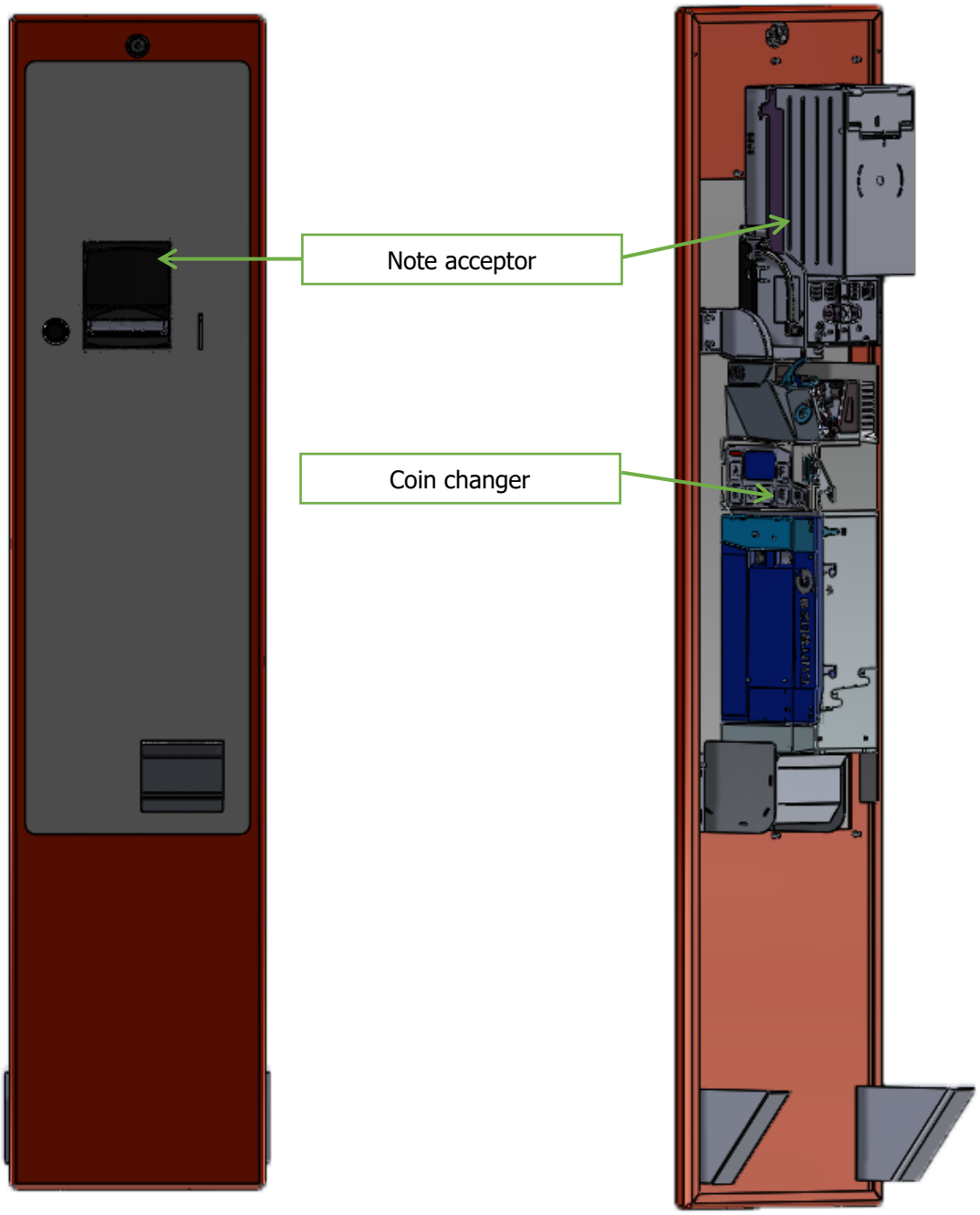
(put here the new rendering)



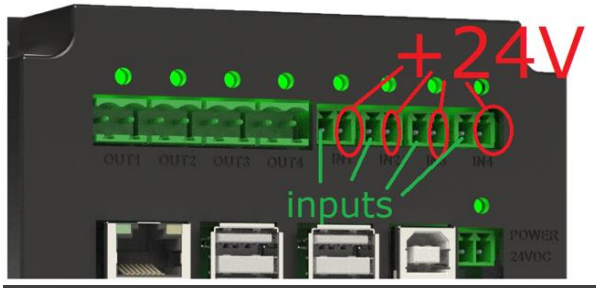
2.3.2 Left door of a cash + bank-card-columns or the only door for bank-card-only columns.



2.3.3 Right side door of revenue columns including cash payment devices



2.3.4 The CU5v2 controller

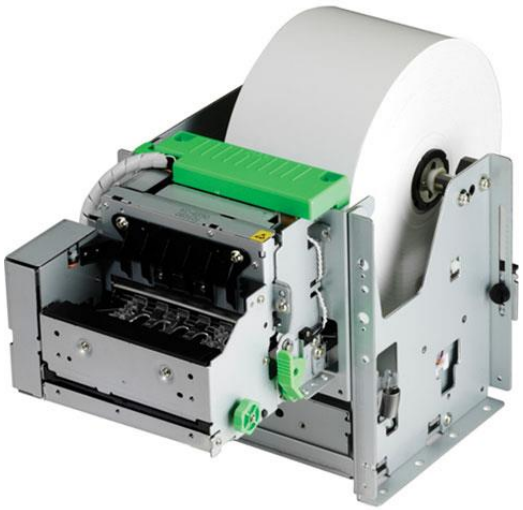


Housing:	Steel housing, powder-coated in RAL 7016.
Display :	TFT colour graphic display, transmissive, 320x240 pixels, 70x52mm
IN 1-4:	4 inputs. The right pin on each connector is +24V. The left pin on each connector is the actual input of which the minimum high voltage is 18V. So it can be controlled by a switch/relays by controlling both pins or a digital input by only using the left pin (and share the same gnd). Go to Error! Reference source not found. for more info.
OUT 1-4:	4 outputs. Solid state relays, 24V AC/DC, max 1A. Go to Error! Reference source not found. for more info.
Ethernet:	RJ45 connector.
USB1-4:	USB Host port used for the scanner, kiosk printer, RFID reader or slave controller.
USB:	USB device port.
POWER :	24VDC.
RS232:	Serial port.
Switch 1-2:	LED push buttons.
MDB:	MDB connector (only used in case of a revenue column).
LED 1-2-3:	Not used.
SPEAK:	The speaker is used for both the buzzer and intercom function.

2.3.5 Kiosk printer

Thermal kiosk printer TUP500. This printer has been chosen for its reliability and for its ease of use and maintenance.

Depending on the column configuration, the stainless steel printer support may vary.



Voltage supply:	24VDC
Consumption:	2.5A during printing – 0.07A standby
Printing technology:	Direct thermal printing
Resolution:	203dpi (8dot/mm)
Print speed:	200mm/s
Print width:	80mm
Paper width:	80mm
Cutter mechanism:	Guillotine

Every ten rolls of paper, we recommend performing preventive maintenance on the print head. Please take a look at the following videos:

- http://clouddrive.dasaccess.com/f/f79cc34008/?dl=1
- http://clouddrive.dasaccess.com/f/baca166dd2/?dl=1
- http://clouddrive.dasaccess.com/f/1efcf651a4/?dl=1

2.3.6 Scanner

Specifications:

Scanner:	CCD 2D
Input voltage:	5VDC +/- 0.25V
Operating power:	1.4W (275mA @ 5V)
Power in standby mode:	1.2W (230mA @ 5V)
Laser class:	Class 1: IEC60825-1, EN60825-1
EMC:	FCC Part 15, ICES-003, EN55022 Class B
Operating temperature:	-20°C to 40°C
Light source:	Laser 650nm +/- 10nm
Communication :	USB

In order to guarantee proper barcode reading performances, it is recommended to regularly clean the window with a soft, dry cloth.

2.3.7 Coins recycler

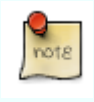
Input voltage:	24VDC
Consumption:	1A Max.
Coins accepted:	0.10€, 0.20€, 0.50€, 1€ and 2€
Default coin tube configuration:	EUR39 2x0.10€, 2x0.20€ and 2x0.50€
Operating temperature:	0°C to 55°C
Capacity:	More or less 80 coins per tube

For the configuration of the coin changer, we refer to the Currenza C2 manual.
http://www.nri.de/download/PDF_Englisch/KA_c2_SA_EN.pdf

2.3.8 Notes recycler

- Banknotes recycler gives change with one type of predefined notes.
- This recycler has change autonomy/stock box of 30 notes.
- This recycler can autofill the stock box with a predefined type of banknotes.

Input voltage:	12-24VDC
Consumption:	2A Max.
Size of accepted notes:	62 to 74mm
Operating temperature:	-20°C to 65°C
Validation time:	2.5 seconds
Capacity:	+/-250 notes



For the configuration of the note recycler, please refer to the ICT X7P manual.
http://www.ictgroup.com.tw/download/Installation%20Guide/X7P%20Installation%20Guide%20(EN)%20H6651A-R.pdf

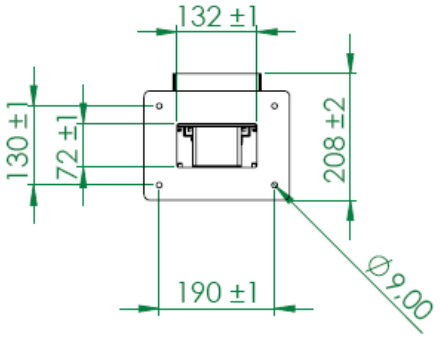
2.3.9 Power supply kit

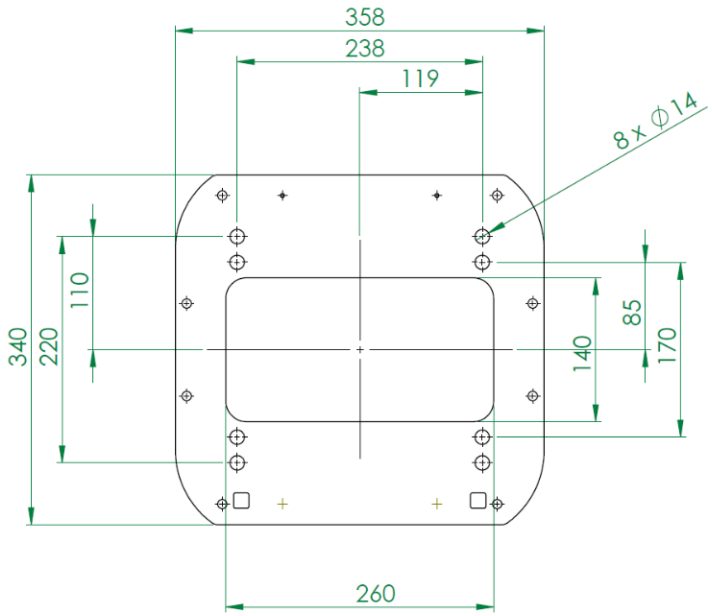
Input voltage:	90-264VAC
Output voltage:	24VDC +/-1%
Output current:	4.2A
Thermostatic heater:	+15°C to +25°C

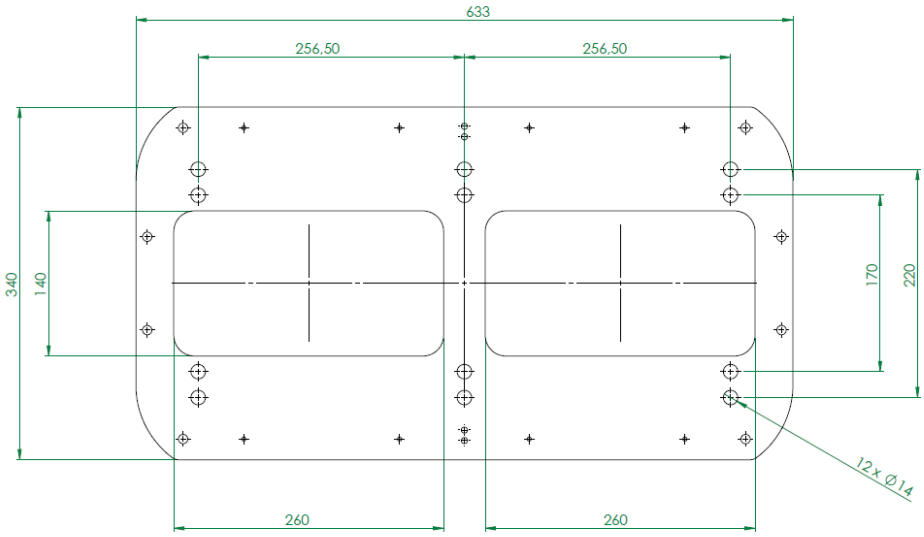
2.4 Installing a DAS column

2.4.1 Floor plans

Our products are available in three different column types. See below the floor plans of respectively type2, type 6 and type 6+.



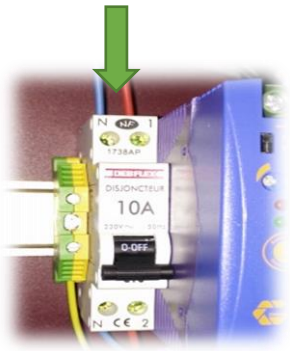




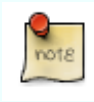
2.4.2 Connections

Route the cables under the column through the base and fix the column to the floor.

1. Connect the power supply to the circuit breaker



2. Connect the vehicle detection system* to the IN1 input using the supplied green connector.
3. Connect the OUT1 output to the physical access (gate, automatic barrier ...) using one of the green connectors provided.
4. Connect your LAN cable to the Ethernet switch.



* The controller only handles dry contacts on its I/O. In the case where there is no vehicle detection system (= presence detection loop), the IN1 input must be disabled using our configuration software or by scanning the appropriate DAS barcode command cards. We'll come back to this later in this manual.

2.4.3 Thermal paper specifications

Many competitors are still using thermal fanfold cards, which for a long time was the best solution. DAS was one of the first, if not the first, to switch to thermal paper rolls for the following reasons:

Greener and less expensive than cards. To ensure a good balance between reading performance and cost, we use rolls of 80g/m2 and 135g/m2. Either way, you use less paper per ticket than with cards.

High autonomy. We use rolls with a diameter of 200 mm. Depending on the gsm (grams per m²) and the length of the ticket inherent to the ticket layout customization chosen (logos, specific text, etc.), you can print up to +/- 4250 tickets with a roll.

More compact: If you stack 4250 thermal cards in your column, you get a much larger volume than one DAS thermal paper roll. Also, the storage of the rolls in your warehouse therefore takes up less space and the transport is cheaper.

Quick replacement: Changing a roll is faster and easier than a fanfold card cassette.

Ticket layout customization options are almost unlimited: Cards have a predefined printable surface, limited in width and length. However, our thermal paper roll kiosk printers can print tickets of almost unlimited length and of which only the width is predefined (in our case 8cm). You therefore have the free choice to add logos and specific texts to your tickets.

We use direct thermal paper rolls for kiosk printers:

- Direct thermal paper 80mm width (+/- 0.5mm)
- Waterproof
- Diameter: +/- 200mm
- Diameter axis: 25 ~ 26mm
- Paper thickness:
    - 80grs / m² (product code TPtc80KPa/1)
    - 135grs / m² (product code TPtc135KP/1)

The user experience with 135 g/m2 cards is comparable to that of thermal cards but without the drawbacks mentioned above, inherent in the use of cards.

The use of paper rolls other than DAS paper rolls may cause malfunctions (paper jams, print quality deterioration ...) that DAS cannot be held responsible for.

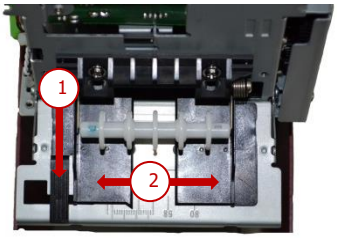
In cases where the column is installed outdoors, we strongly recommend to use 135 gsm paper and to make sure the "Enable paper loop" box is unchecked in the settings (which is the default).

2.4.4 Setting up a paper roll

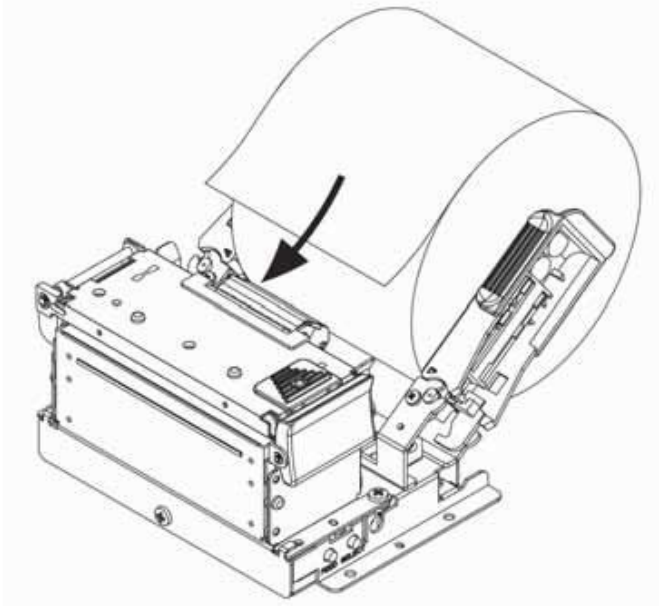
- Turn on the power (make sure both the printer and controller are powered ON)
- Take the paper axis and remove one roll holder by pulling on the green part.

- Insert the paper roll on the axis.
- Put back the roll holder whilst pushing on the green part until the paper roll is properly secured.
- Make sure the paper edge is clean and straight.

- Make sure the printer cover is closed before inserting the paper



- Insert the paper between the paper guide until the printer starts pulling the paper.



- Remove the blank ticket that has come out of the "printer mouth".

3 Commissioning

Commissioning a CU5 controller or updating its default configuration can be done in multiple ways:

- **Using barcode command cards (BC cards)**. BC cards allow basic configuration updates simply by scanning specific barcode cards to the scanner. In the case of a printer controller, you scan these BC cards via a portable USB scanner that you connect to one of the CU5 USB ports.
- **Using the PC application ProConfig Offline** so to allow advanced configuration of **unconnected** CU5 controllers applying **offline** update procedures (without being connected with the CU5).
- **Using the web pages of ProConfig Embedded** that run on the CU5's embedded web server so to allow advanced configuration of **connected** CU5 controllers and regular users applying **online** update procedures (while being connected with controllers, either directly via a UTP cable or via your LAN).
- **Using the PC application ProConfig Users** so to allow management of your regular and temporary users by applying **offline** update procedures (without being connected with the CU5).
- **Using the web-hosted application ProConfig Cloud** so to allow advanced configuration of CU5 controllers and regular users applying both **offline** and **online** procedures.

Now let's update the configuration of your controller using BC cards.

If your project includes the optional 4G/Wifi modem/route (WLINTx) or an Ethernet switch (SwEthx), please refer to their respective manuals for the configuration of these devices.

...

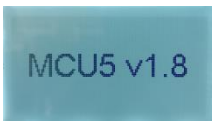
3.1 Good to know

If your order includes the product codes AcPar and/or RcPar, we will email you a questionnaire. Based on your answers, you will then receive preconfigured controllers (with access control and/or revenue features respectively).

If the pay station you ordered contains a bank card terminal, you will receive a preconfigured and fully operational terminal linked to an already activated transaction contract upon delivery. That is why the order of the product code CpPar is also mandatory at every bank card terminal.

As soon as the power is turned on a CU5 starts showing for a few seconds: its hardware number, its firmware version and its DAS ID number (= configuration file number) on its display. The hardware number is necessary when connecting remotely with a controller. A CU5 configuration file contains information such as access rules, print layout, push button presets, controller input/output configuration, etc… (Show here updated display pictures).

Hardware nr



Firmware version

ID DAS

In the unlikely event of having to swap a controller (for example due to a technical fault), DAS offers you the option of ordering a new controller (with a new hardware number, of course) with the same DAS ID as that of the controller that needs to be replaced. This has the advantage that the physical swap can take place without having to use one of our ProConfig applications/software. All you need to do is import the backup configuration file of the original controller into the new controller (using for instance a USB stick or via the applications ProConfig Offline, ProConfig Embedded, ProConfig Cloud).

A CU5 controller is by default configured as follows:

- Language is English
- No virtual links with printers
- The paper loop feature is disabled (mandatory when using 135gsm paper – see **2.4.3**)
- Inputs:
  - IN1: Presence detection input (dry contact)
  - IN2: Push button input (when kiosk printer is needed)
  - IN3: Abort / lost ticket button (in case of a revenue column)
  - IN4: Free/available input.
- Outputs:
  - S1: Output for physical access (automatic barrier, gate …)
  - S2: Printer error output (dry contact)
  - S3: Free/available output
  - S4: Free/available output

If you look at the logs of the CU5v2 or generate a report with one of our software programs, you will see that the controller does an automatic reboot every Sunday around 3AM. This is normal. Every CU5v2 has this as the factory setting.

3.2 Configuring a CU5 using barcode command cards

To a limited extent the CU5 controller can be configured without using any of the DAS software available. For this we've created barcode command cards that allow a basic yet quick commissioning.

Each controller comes with a unique barcode card called "S&G Pro Identity". This card is required for a "software-less", basic commissioning of the controller.

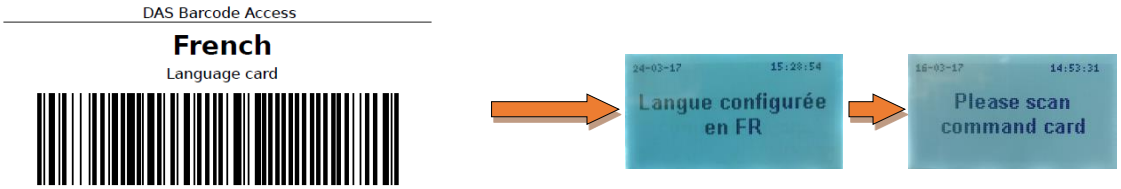
Since the controllers are by default configured in English, the first thing you might want to do is to modify the language.

3.2.1 Change the default language

In this example, we want messages to appear in French.

1. Scan the card "S&G Pro Identity" until the message 'Please scan command card' is displayed. You now are in Admin Mode.
2. Scan the command card « Set language » until you see the message 'Please scan language card'.

3. Scan the command card « French ». You now see the message 'FR'.



4. Scan "Set Language", your column will be configured for one language only.

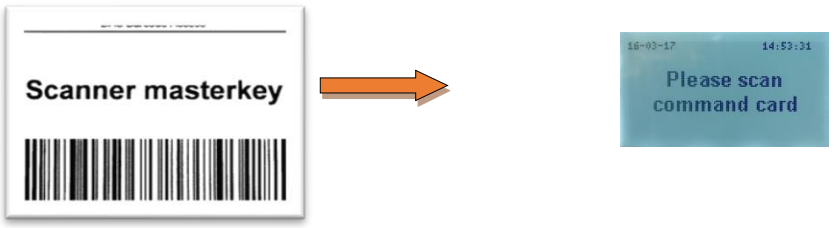
The LCD display can show each message in up to 3 languages alternately. To do so, scan during step 3 the language cards you would like to add.

After step 4 all user messages on the display will appear in the same order in which the language cards were scanned.

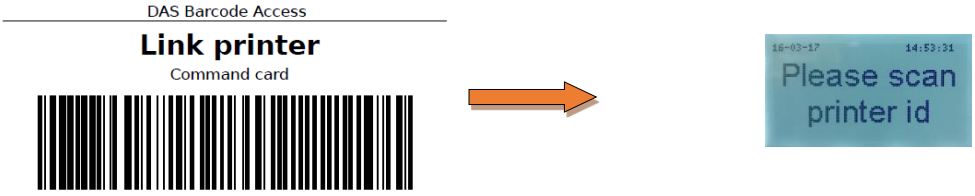
3.2.2 Link a printer

Barcode tickets will not be interpreted by the scanner until a virtual link between the DAS printer(s) and the scanner has been activated. By printer is meant any DAS hardware or software capable of printing a barcode ticket.

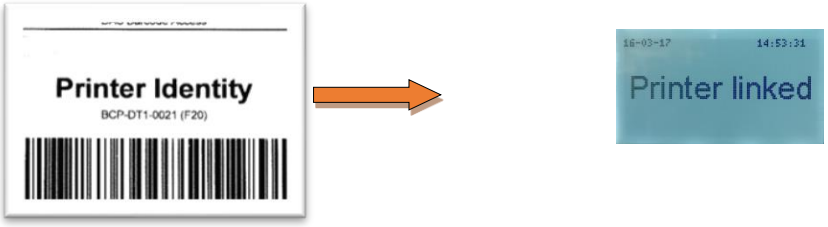
- Scan the card "S&G Pro Identity" until the message 'Please scan command card' is displayed. You now are in Admin Mode.



- Scan the command card "Link printer" until the message 'Please scan printer ID' is displayed.



- Scan all the "Printer identity" cards of the DAS printers (hardware or software) that you want to virtually link to the column. Each time you scan a "Printer identity" you'll see the message 'Printer linked'.



- Scan "Link Printer" to end the procedure.

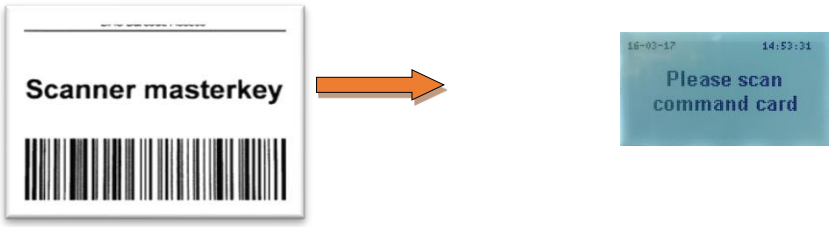
To undo a virtual link, follow the same procedure, replacing the "Link printer" card with the "Unlink printer" card.

If you want to link multiple printers to this scanner, scan the Printer Identities of all these printers during step 3 and end with the command card "Link Printer".

The message "Printed by another system" appears when your visitor scans a ticket printed by a printer that was not yet virtually linked.

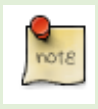
3.2.3 Configure the column in Free Access

- Scan the card "S&G Pro Identity" until the message 'Please scan command card' is displayed. You now are in Admin Mode.



- Scan the command card "Free access" until the message 'Free access' is displayed.

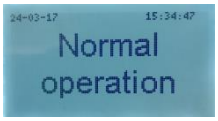
- You now configured your column in Free Access mode.



If you combine this feature with presence detection, the physical access will open as soon as a vehicle is detected. If you combine it WITHOUT presence detection, output 1 will permanently be activated and the physical access will remain permanently open.

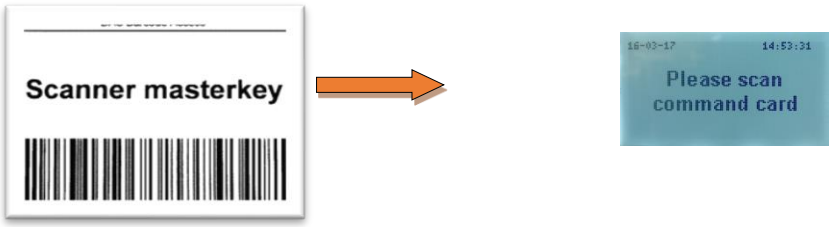
Please check the compatibility of your physical access with the latter configuration. For example, an automatic barrier could be configured to close automatically after a while even with our permanent open command.

To re-enable the access control mode, renew the same procedure. After scanning the command card 'Free access' the display will show the following message:



3.2.4 Configure the column in Closed Access

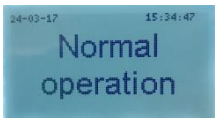
- Scan the card "S&G Pro Identity" until the message 'Please scan command card' is displayed. You now are in Admin Mode.

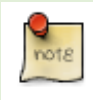


- Scan the command card « Permanent Closed » until the message « Closed» is displayed.

- You now configured your column in Closed Access mode.

To re-enable the Access Control Mode, renew the procedure. After scanning the 'Closed Access' command card the display will show the following message before returning to normal operation.





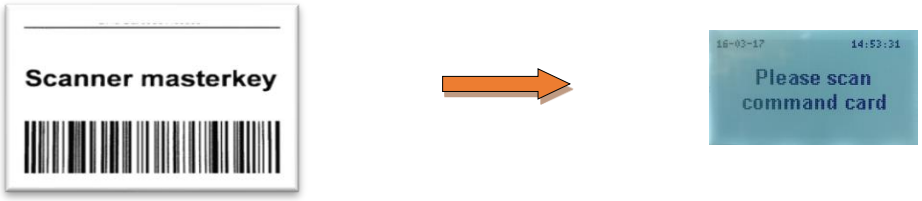
You can configure opening and closing hours (= operating modes) for the controller using the configuration software ProConfig Offline. See points Error! Reference source not found. and Error! Reference source not found..

3.2.5 Add/Remove barcode and RFID cards for regular users

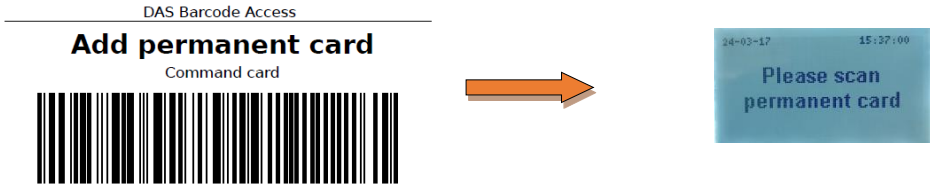
Let's start with adding/activating barcode cards for regular users.

> Permanent barcode cards are PVC cards on which a barcode is printed. Once activated, these cards are permanently valid 24/7 until they are deactivated again. Permanent cards are numbered and are always supplied in duplicate. Make sure not to lose the duplicates. You'll need them later to be able to deactivate "lost" cards.

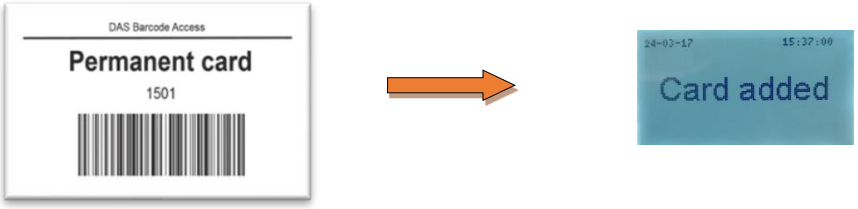
1. Scan the card "S&G Pro Identity" until the message 'Please scan command card' is displayed. You now are in Admin Mode.



2. Scan the command card « Add permanent card » until the message 'Please scan permanent card' is displayed.



3. Scan all the permanent cards one by one.

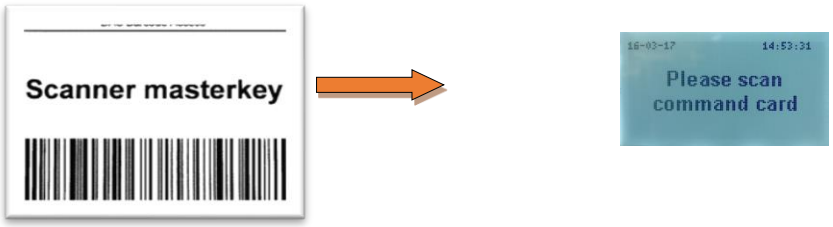


4. Once all permanent cards have been scanned, scan the 'Add permanent' card again to end this procedure.

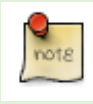
> To activate RFID cards, apply this same procedure using, during step 3, RFID cards instead of permanent barcode cards. Attention, this procedure only works with RFID cards that do not have access rules in the card memory.
>
> To deactivate permanent barcode cards, repeat the procedure above but this time, during step 2, use the command card 'Remove permanent card' instead of 'Add permanent card' and then, during step 3, scan the duplicate(s).
>
> Deactivating lost RFID cards by applying the procedure described above, is not possible as RFID cards, for obvious security reasons, do not come with duplicates. Deactivating lost RFID cards is only possible using the applications ProConfig Users or ProConfig Embedded.

3.2.6 Restore factory defaults

- Scan the card "Scanner S&G Pro" until the message 'Please scan command card' is displayed. You now are in Admin Mode.



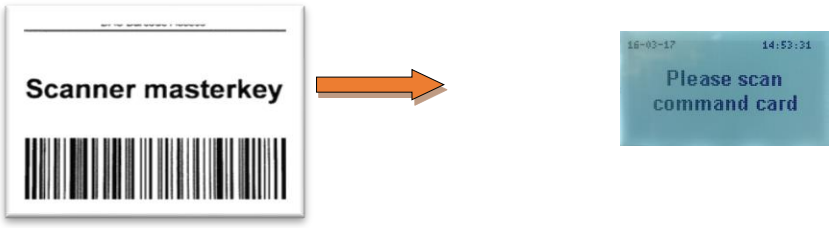
- Scan the card « Restore factory defaults» until the message 'Restoring factory defaults' is displayed. The controller will automatically reboot to take into account the new settings.



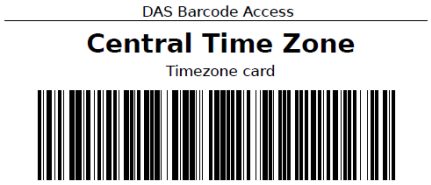
After restoring factory defaults, all data will be deleted except for the controller identity and features/licenses.

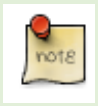
3.2.7 Determine the time zone

- Scan the card "S&G Pro Identity" until the message 'Please scan command card' is displayed. You now are in Admin Mode.

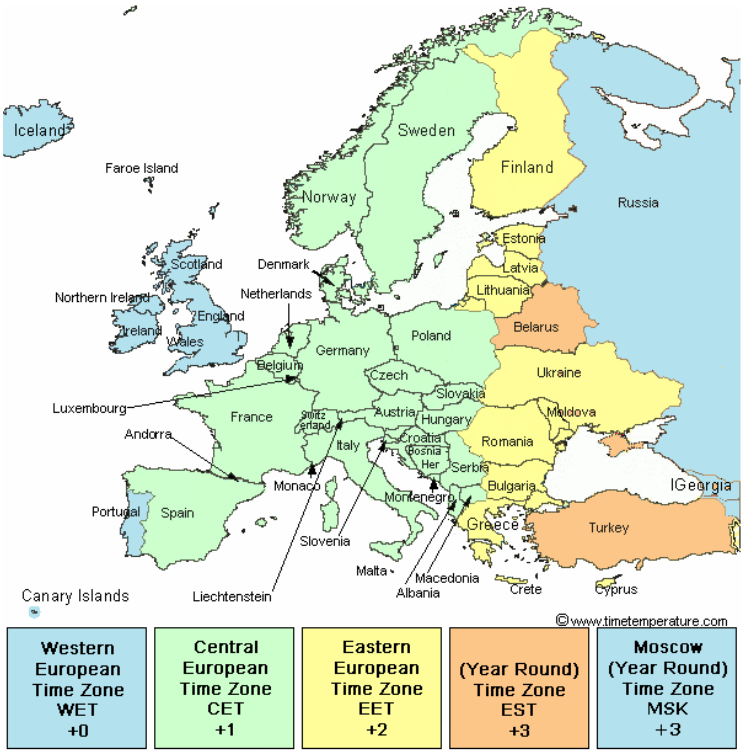


- Scan the command card representing the time zone you would like to activate.





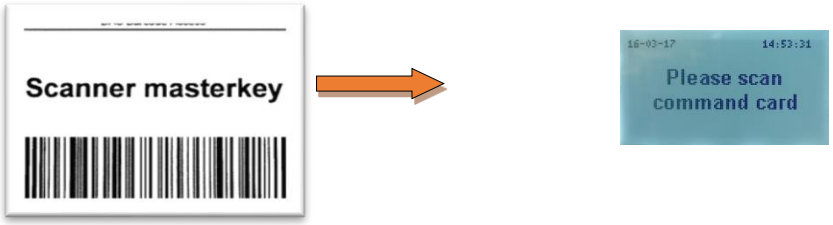
You can choose between CET (UTC+1/+2), EET (UTC+2/+3), WET (UTC+0/+1) and EAT/MSK (UTC+3). time zones. Winter daylight saving time will automatically be applied where and when necessary. Please contact your supplier if you need other time zones.



3.2.8 Enable / disable presence detection

A presence detection loop is not mandatory yet recommended. Especially in the case of a printer column.

- Scan the card "S&G Pro Identity" until the message 'Please scan command card' is displayed. You now are in Admin Mode.

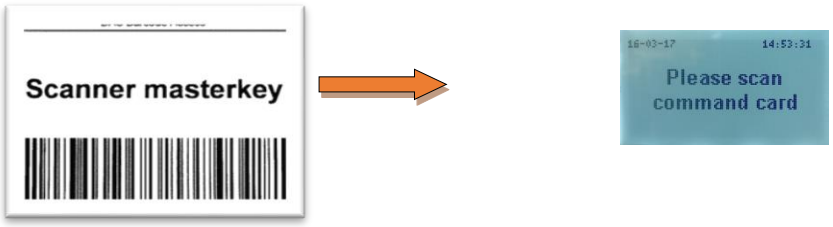


- Scan the command card « Detection loop » until the message 'Detect car off' is displayed.

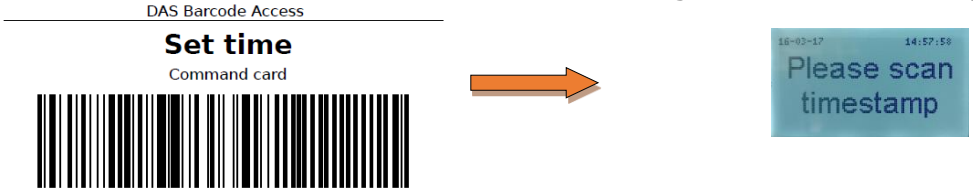
- To reactivate vehicle detection, repeat the same procedure until the message 'Detect car ON' appears.

3.2.9 Synchronize the time of a printer controller with a scanner controller

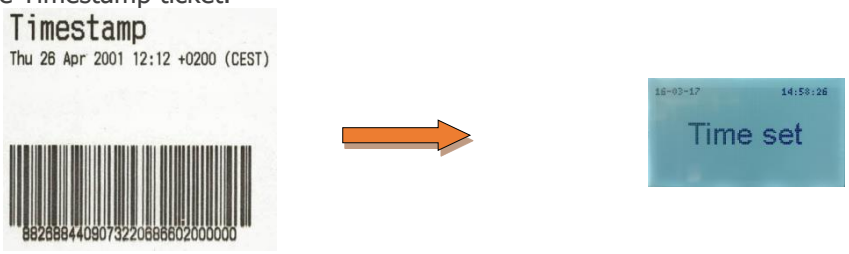
- Make sure you have the Timestamp of the desktop or kiosk printer you want to synchronize the time with. For this we refer to their manuals or suggest you contact your supplier.
- Scan the card "S&G Pro Identity" until the message 'Please scan command card' is displayed. You now are in Admin Mode.



- Scan the command card « Set time » until the message 'Please scan timestamp' is displayed.



- Scan the Timestamp ticket.



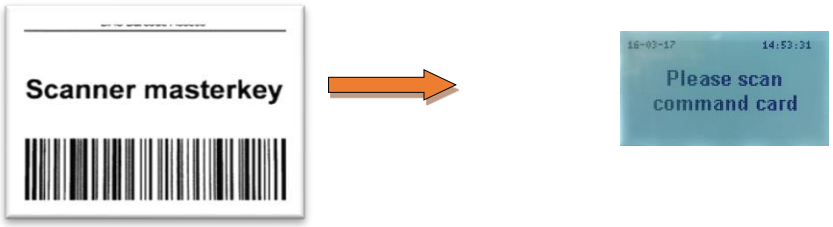
Attention, the time spent between the moment when the timestamp ticket was printed and then scanned to the scanner will not be taken into account. Thus, if it took you 10 minutes to scan the timestamp ticket, there will be a 10-minute time gap between the internal clock of the printer and scanner controller.

If you want a precise time configuration for your controllers, you have four options. 1) using ProConfig Offline: go to Error! Reference source not found., 2) via the web server of the controller: read the manual "ProConfig Embedded", 3) via the internet: internet-connected controllers will synchronize their Real Time Clock values automatically with a cloud-hosted time server and 4) using a USB GPS receiver (see below).

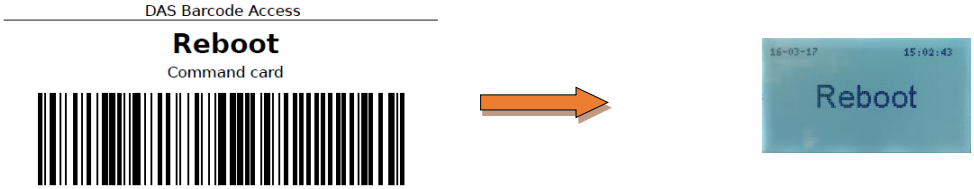
Real Time Clock values (= internal clock) of standalone CU5v2 controllers may deviate over time. If you want precise time values for these controllers without having to update them regularly manually, you can choose to provide the controller with our USB GPS receiver. When ordering the product code GPSTS1 you will not only receive the aforementioned product but also a license code that you can enter on the feature/options page (see Error! Reference source not found.). Attention, this GPS receiver may only work effectively when the column is installed outside.

3.2.10 Reboot

- Scan the card "S&G Pro Identity" until the message 'Please scan command card' is displayed. You now are in Admin Mode.



- Scan the command card « Reboot».



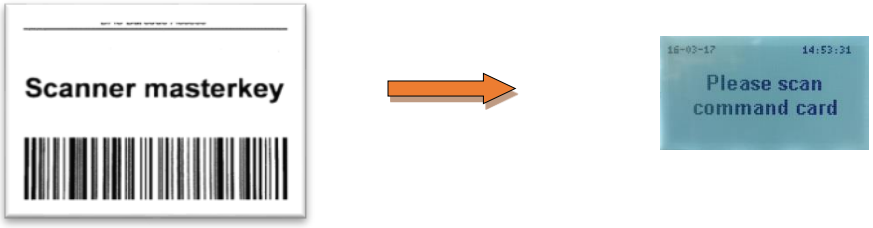
After scanning the "Reboot" command card, the column turns off temporarily.

3.2.11 Coins filling procedure

By default the coins recycler accepts all coins from 0.10 € to 2 € and the language is English. The 1, 2 and 5c coins automatically fall into the cash box. We invite you to read the coins recycler manual to learn how to change the language.

> **It is not allowed to fill the tubes by following the coin filling procedure described in the coin changer manual**! Doing so will result in erroneous sales reports as the CU5 will thus not receive the necessary information. Instead you must follow the specific coin filling procedure described below.

- Scan the card "S&G Pro Identity" until the message 'Please scan command card' is displayed. You now are in Admin Mode.



- Scan the "Start coin filling" command card. You now can see the level of each tube on the display. You can start filling.

- Once the filling is complete, scan the "Start coin filling" card again. A ticket will then be printed with the summary of the operations carried out.

DAS Identity
Hardware serial number
Filling date

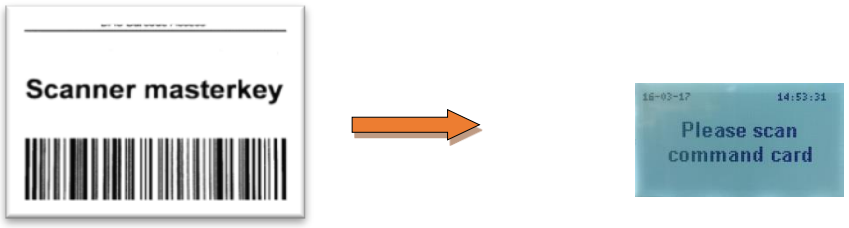
Amounts inserted

Amounts in the tubes

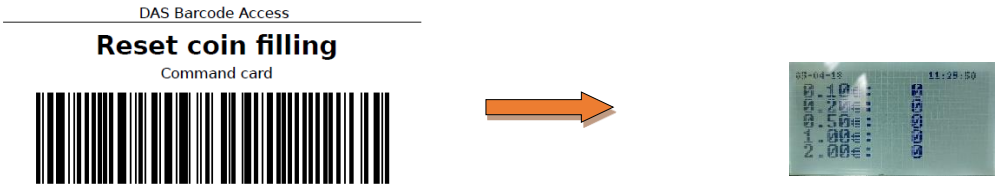
Please note that coins that are not recognized (dirty, deteriorated, or other ...) or that are configured to be refused by the coin changer will immediately be returned to the user and will therefore not be counted. They will not appear on the report.

3.2.12 Resetting the coins recycler tubes to zero

- Scan the card "S&G Pro Identity" until the message 'Please scan command card' is displayed. You now are in Admin Mode.



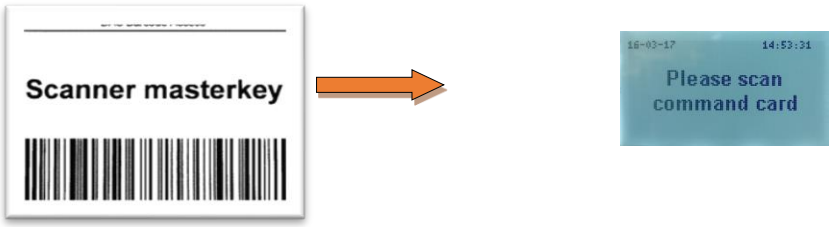
- Scan the command card « Reset coin filling ». Counters have now been reset to zero and the display shows "please empty tubes".



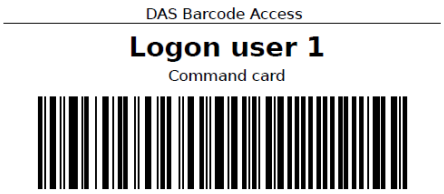
ATTENTION: Resetting (zeroing) the coin tubes using this command card implicates that you now MUST empty the tubes as the CU5 controller will be waiting for the coins recycler to report an "empty tubes message" before being operational again. Only empty the coin tubes by pressing on Menu>Service<Empty tubes on the coin recycler keypad or scan a barcode to cancel the operation. Never empty the tubes by removing and emptying the tube cassette by removing and emptying it manually.

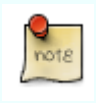
3.2.13 Offline sales reports

- Scan the card "S&G Pro Identity" until the message 'Please scan command card' is displayed. You now are in Admin Mode.



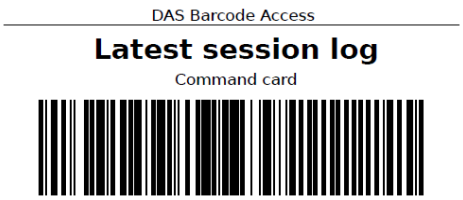
- Scan the command card « Logon user 1 », the controller will print a summary of the current session and then start a new session. The printout will mention the logon user number (number "1" in this case). Up to five logon user cards are available so you can delegate the sales report printout (and thus money collection) to five different people.



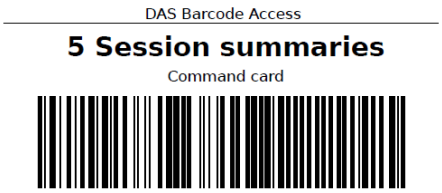


When you generate an offline sales report the system assumes you emptied at that moment the cash box as well as the banknote recycler and therefore resets these counters. Do never empty the coin tubes of the coins recycler (also called the cassette) or the bank notes cassette without using the adequate command card as this will result in erroneous sales statistics.

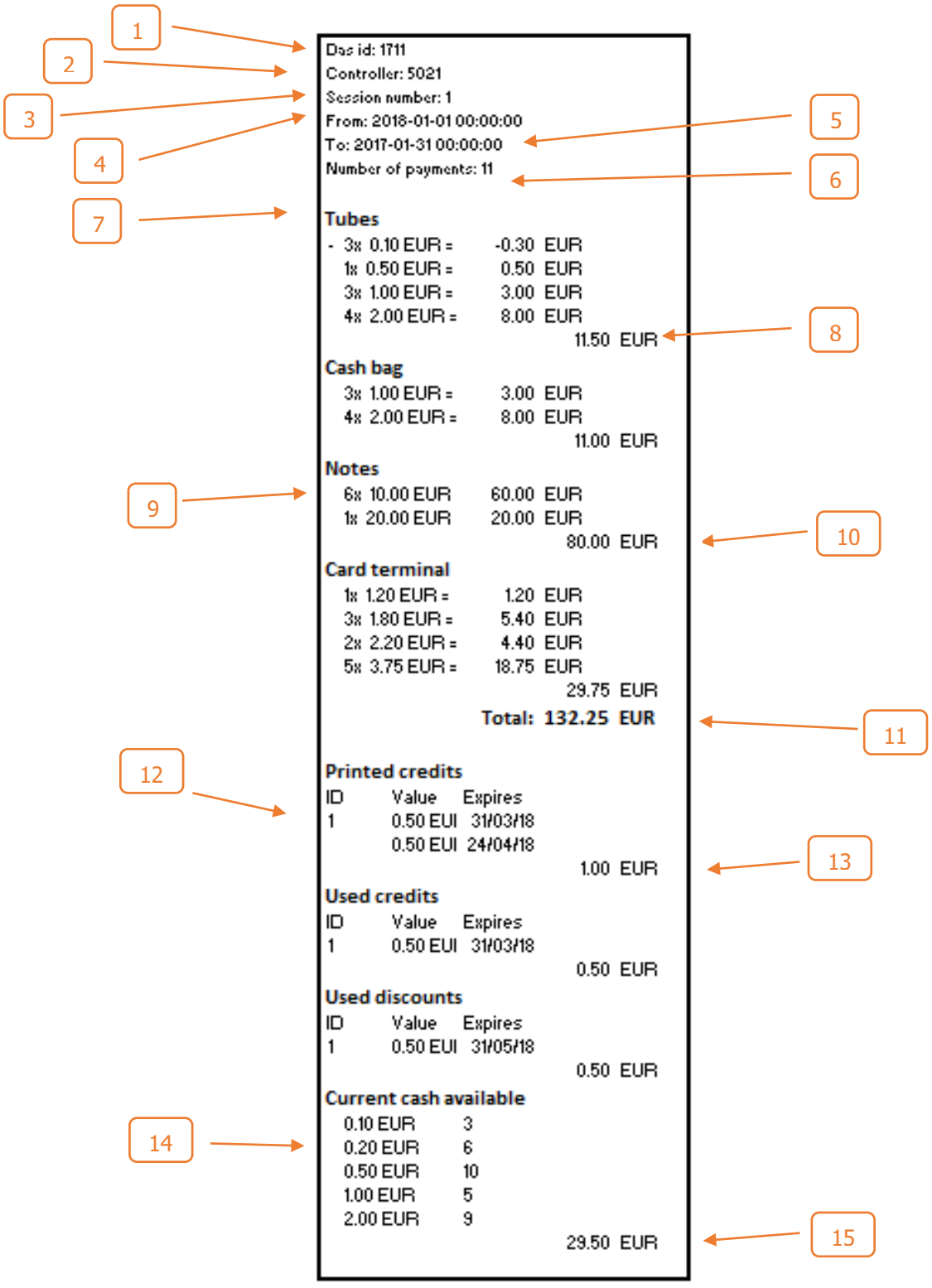
- Scanning the "S&G Pro Identity" followed by the card "Latest session log" allows the system to print details of the current session without closing the current session.



- Scanning the "S&G Pro Identity" followed by the card "5 session summaries" allows the system to print a summary of the current session + the previous four sessions without closing the current session.



Below is an example of an offline report printout



1 The Das Id corresponds to the DAS identifier of the controller. This is the number that will be requested during the configuration processes (virtual link, ...) but also when requesting support and remote intervention.

2 Hardware serial number of the controller. This number can also be requested during the system configurations.

3 Session number. This number is incremented automatically with each new session (= when a logon card was scanned).

4 Indicates the start time and date of the sequence.

5 Indicates the time and date of the end of the sequence, which also corresponds to the time and date when the sales report ticket was edited.

6 This number indicates the number of payments (= transactions) that have been recorded.

7 The controller keeps track of all inserted coins and shows here the difference in the amount of coins in the tubes since the start of the sequence (=end of previous session). So if for instance 10x 2€ coins have been used to pay change and 10x2€ coins have been routed to the tubes during payment transactions, no value will be shown at all (value will be "0" for each tube).

8 Represents the total of all values in number 7 or in other words: the difference in amount of money in the tubes since the start of the session.

9 Represents the list and the number of notes inserted in the note acceptor during the session.

10 Represents the total value stored in the note acceptor during the session including deposits.

11 Represents the total turnover during the current session (including cash bag and bank card revenue).

12 Represents the list of credit tickets that have been printed by the pay station. We can see for each ticket the value and the expiry date. When the pay station cannot return all or part of the money, it will issue a credit ticket on which appears the amount due (= unreturned value).

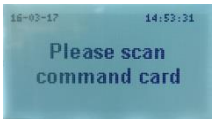
13 Indicates total value of credits (= unreturned money because of cash shortage).

14 Represents a detail of the coins available in the tubes.

15 Represents the total value of coins available in the tubes.

3.2.15 Printing a Credit Report

- Scan the card "S&G Pro Identity" until the message 'Please scan command card' is displayed. You now are in Admin Mode.



- Scan the command card « Create credit report ». A ticket will then be printed.

On this report it is possible to see the number of credit tickets printed, their expiry date, their value and whether they were used or not.

Credit report

DAS Id: 1968
Controller: 5111
Date: 09/04/18 11:22

Id	Value	Expires	Used
1	4.20 EUR	08/06/2018	
2	9.90 EUR	08/06/2018	
3	0.10 EUR	08/06/2018	
4	0.90 EUR	08/06/2018	

Total valid credits 15.10 EUR

3.3 Configuring connected CU5 controllers and regular users using ProConfig Embedded

DAS CU5 controllers are compatible with up to four applications, each running on a different platform:

- AdminTool (ATool) is a **PC application** that allows **management of unconnected controllers**, by **applying offline update procedures** (for example using a USB Update stick). While using PCOffline, you are not connected to controllers.
- ProConfig Embedded (PCEmbedded) is a **web application**, accessible via Google Chrome, that runs on the **embedded web server of a CU5 controller** and therefore allows the **management of both your regular users and connected/networked controllers** by **applying online update procedures,** either via your LAN or by connecting your computer directly to a controller.
- ProConfig Users (PCUsers) is a **PC web application**, accessible via Google Chrome, that can be installed as a standalone application on a PC or as a client/server on a server, allowing **management of both regular users and visitors** by applying **offline controller update procedures for your regular users** (for example using a USB Update stick) and by **e-mailing electronic barcodes for your visitors**. While using PCUsers you are not connected to controllers.
- ProConfig Cloud (PCCloud) is a **cloud-hosted web application** that allows **management of online controllers** as well as **regular users and visitors** by applying both **online update procedures**.

In this chapter we'll take a closer look at the application **ProConfig Embedded**.

3.3.1 Introduction

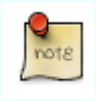
Whatever the controller configuration (access and/or revenue control), the CU5 remains physically always the same. It is the list of activated features/options that defines whether it becomes an access and/or revenue controller (both in the case of a pay-in-lane controller). In this manual the controller is defined as a pay-in-lane controller as this is the most complete variant available (see chapter **2**).

We assume here that your CU5 controller has all available commercial firmware options (= full option) and that you've ordered all available peripheral products that go along with it (such as an RFID reader, a slave ANPR camera, etc…). That's why, depending on the firmware options and peripheral products you've bought, some options described below may not be available in your ProConfig Embedded.

3.3.2 Launching ProConfig Embedded (PCEmbedded)

PCEmbedded is an application that runs on the embedded web server of CU5 controllers. These web pages allow you to configure both **connected/networked** CU5 controllers and your regular users. As the management of regular users is optional, make sure to have the necessary license code activated for your controller (see **3.3.6**).
You can access PCEmbedded via Google Chrome, either directly connected to the controller(s) (with a UTP cable) or via your LAN.

If you know the IP address of your controller, enter this address in Google Chrome and go to chapter **3.3.3**. If you don't know the IP address, install AdminTool and then go to **3.3.2.1**.

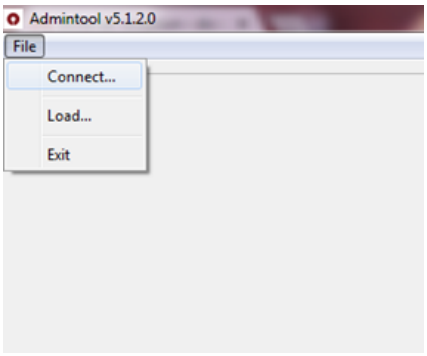


Pro Config Embedded is only compatible with Google Chrome.

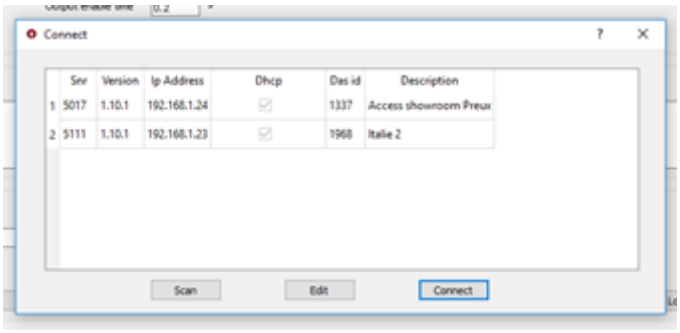
3.3.2.1 Finding your CU5- IP address(es).

We assume here that you've already installed AdminTool and that your controller is **networked/connected** with your computer.

When you start AdminTool and click on File you will see the following page.



Click on File>Connect. A window will pop up indicating, amongst other things, the IP address of all connected controllers. If you are on a local network, it is possible that more than one DAS controller will appear. In this case select the one of your interest, then click on "Connect" on the bottom right of this popup window.



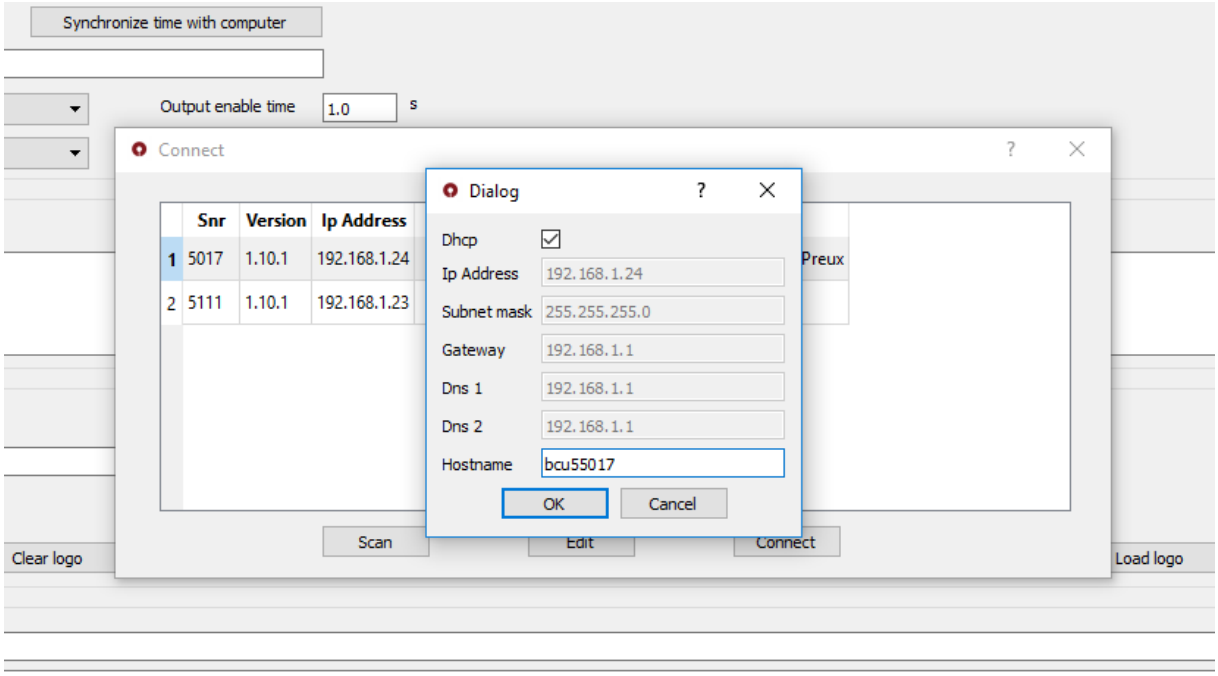
AdminTool will now automatically redirect you to the Settings page. On that page, click on the tab Regular Users and ATool will then redirect you to Google Chrome and open the ProConfig Embedded login page for this controller (see **3.3.3**).

WARNING, when the controller is configured in DHCP (=default) the LAN port of the computer must be in DHCP too (= default). If the controller was configured with a fixed IP address, the computer must have an IP address in the same range.

If you want to access your controllers via the internet, please use our web application DAS ProConfig Cloud. Contact your supplier for more information or go to www.dasaccess.com.

3.3.2.2 Modifying network settings

Before accessing ProConfig Embedded, you might want to modify your controller network settings. If so, go to File>Connect, select the controller and then click on Edit. You will then see its network information:



By unchecking the "DHCP" field you can choose your own values for: IP address, Subnet Mask, Gateway, Dns1 and Dns2.

Click on "Connect" on the bottom right of this popup window. AdminTool will now automatically redirect you to the Settings page. On that page, click on the tab Regular Users and ATool will then redirect you to Google Chrome and open the ProConfig Embedded login page for this controller (see **3.3.3**).

Please do not confuse the field Hostname with the controller name that you fill in the field Description that you find under Settings>System info (see **3.3.5.1.1**).

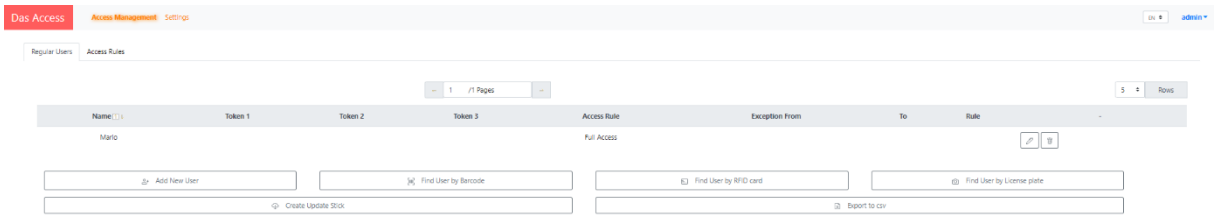
3.3.3 ProConfig Embedded (PCEmbedded) login page

This is the homepage that you see when you've entered the correct CU5-IP address in Google Chrome (see **3.3.2.1**) The default login and password are admin/admin. You will be given the option to change it later on.

Please notice that for security reasons any update of a CU5 controller via PCEmbedded must be done within 5 minutes after reboot or a scan of the S&G Pro Identity. After this time period the S&G Pro Identity must be scanned again or the controller rebooted before being able to perform a new configuration upload (by clicking on the blue button Save). This is to prevent easy access to unauthorized people.

3.3.4 ProConfig Embedded (PCEmbedded) home page

When you log into PCEmbedded, you see at first the page Regular Users. Before you start configuring your users, we recommend that you start by first choosing the language in which you want to use PCEmbedded and then check your password and your CU5 features/licenses/options. Let's start with Language.



3.3.4.1 Language

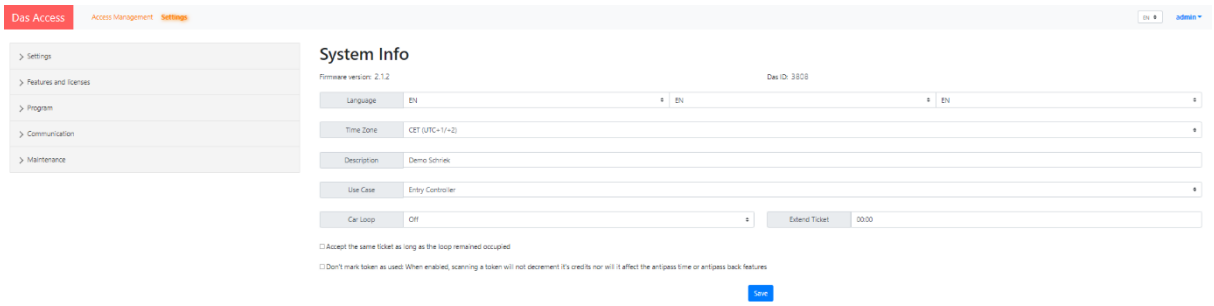
Select the language at the top right of your screen. You can choose from four languages.

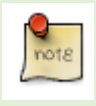
3.3.4.2 Your account name

By clicking on your account name at the top right you can leave your session or change the password your account is associated with.

3.3.5 Settings

Click on Settings at the top of your screen. This is the page you will see:





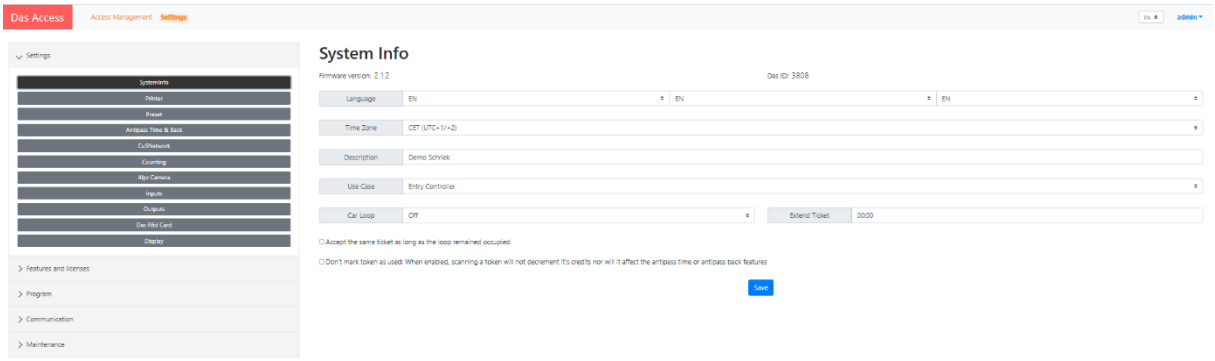
If you click Save after changing controller-specific settings like virtual links, ticket layout, controller input and output configurations, etc… **ONLY** the controller you are connected to will be automatically updated.
If you click Save after changing the settings for Counting, Anti-passback, Anti-passtime, Networked Controllers and/or Regular Users (with their respective access rights), **ALL** affected/involved networked controllers will be automatically synchronized/updated.

3.3.5.1 Settings

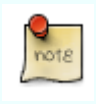
Click on Settings on your left. Depending on the configuration of the controller you've bought, you now can see up to eleven settings windows. Below is a brief description of each menu. You will find a detailed description later on in this manual.

- System Info: General controller configuration information including: firmware version, DAS ID number, controller display message languages, time zone, description, controller use case (entry, exit or validation), car loop (= presence detection loop), extend ticket, etc… .
- Printer: Resumes options and actions related to the kiosk printer.
- Preset 1, 2 & 3: Define here the ticket layouts and their validity.
- Anti-passback & anti-passtime: Determine here how you want to apply the features "Anti-passback" and "Anti-passtime".
- CU5 network: List here controllers that, once they'll be networked, need to communicate with each other for functions such as: anti-passback, anti-passtime, anti-passtime, counting, 1-ticket and database replication. This is also the place where you define the virtual connections between scanners and printers.
- Counting: Determine here if and how you want to apply the feature "Counting".
- ANPR camera: Configure here license plate recognition cameras.
- Inputs & outputs: Determine here how you want to configure up to four controller inputs, two input switches & four outputs.
- DAS RFID card:
    - Read user and access rule data from card: We assume here that the computer used for RFID card enrolment is not connected to CU5 controllers. The access rights are therefore first written on Mifare cards and with the first scan the controllers then copy these rights into their own database.
    - Enable copy protection: Determine here if you want to activate the card copy protection feature and thus limit the risk of copied cards.
- Display: Determine here whether and for how long the LCD backlight should be turned off, after the system has been idle for some time.

3.3.5.1.1 System info



- Firmware version: Find here the firmware version that runs on your controller. Always state this version number together with the DAS ID in the case of an after sales request.
- DAS ID: This is the number of the controller configuration file. It contains data such as: ticket layout, push buttons presets, regular users access rules, etc.



In the unlikely event that a controller needs to be replaced (for example due to a technical failure), DAS offers you the option of ordering a new controller (with a new hardware number, of course) with the same DAS ID as that of the controller that needs to be replaced. This has the advantage that the physical swap can take place without having to reconfigure the virtual and/or physical network connections for the swapped controller, using one of our configuration software. All you then need to do is to import the backup configuration file of the original controller in the new controller.

- Language : The controller display can show messages in up to 3 languages one after the other. In the case where only one language is necessary, only the first box is to be completed. Make your choice of languages by clicking on the drop-down menu of each position. In the case of a printer controller, only the first language box will be considered for ticket printing.
- Time Zone:

Please use the correct time zone so that daylight saving times can automatically be applied: WET (UTC+0/+1), CET (UTC+1/+2), EET (UTC+2/+3) and EAT/MSK (UTC+3).

When connected to the internet, CU5 controllers automatically synchronize their time values with a "time cloud server".

When directly connected to your computer via ProConfig Offline, CU5 controllers can synchronize their time values with your computer by clicking on "*Synchronize time with computer"* (see above).

Offline/standalone/disconnected CU5 controllers rely on their RTC (Real Time Clock) to determine the time. Their time values may therefore vary over time. If you still want accurate time values for these controllers without updating them manually, you can choose to provide them with our USB GPS receiver. When ordering the product code GPSTS1 you will receive not only the aforementioned GPS receiver but also a license code that you can enter on the feature/options page. See **3.3.6**. Attention, this GPS receiver may only work effectively when the column is installed outside.

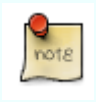
- Description: Add here a controller description/name. For example: "Entry Lane 1". This way the controller will be recognizable when it appears in one of the DAS software.
- Use case: Specify the use of the controller:
    a. Entry controller:
        i. In the case of a printer controller, the default message is: "Please, press the button and take your ticket." In the case of a scanner controller, the default message is: "Please scan your ticket". In the case of a scanner/printer controller, the default message is: "Please take or scan your ticket".
        ii. The default message after a valid identification is "Welcome"
        iii. When the "anti-passback" function is activated and you have completed a successful identification, your identifier will be marked as "in".
        iv. When the feature "counting" is activated, the presence counter increments with every valid identification.
        v. In the case of an entry pay-in-lane revenue controller (fixed amount per visit), that fixed amount will be the default message on the LCD display.
    b. Exit Column:
        i. In the case of a scanner controller, the default message is: "Please scan your ticket".
        ii. The default message after a valid identification is "Goodbye"
        iii. When the "anti-passback" function is activated and you have completed a successful identification, your identifier will be marked as "out".
        iv. When the feature "counting" is activated, the presence counter decrements with every valid identification.
        v. In the case of an exit pay-in-lane revenue controller with a fixed amount per visit, that fixed amount will be the default message on the LCD display.
    c. Ticket validator controller: Choose 'Ticket Validator' when neither of the two use cases above applies. For instance:
        i. A scanner column or scanner/printer column that operates respectively as an online or offline Barcode Updater.
        ii. A Pay-on-foot revenue column.
        iii. All use cases where you don't want a controller output to be triggered and where the feature Counting (see **0**) is not needed.

- Car loop (vehicle presence detection):
  « OFF »: No presence detection is taken into account. Select "off" in case there's no presence detection device available (for instance in the case of pedestrian access control).

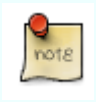
  « ON »: As long as the controller's presence-loop input is triggered, users can take or scan their tokens/identifiers (= barcode, RFID, license plate). This implies that the controller does not take tailgating into account (= two cars that follow each other so close that the loop thinks it still is detecting the first car). The loop must therefore not necessarily have been interrupted before interpreting a new valid identifier. However, in the case of (for instance) a Single-Use identifier that did not leave the loop in time and as a result of which the barrier is closed again, that same identifier will only be accepted again at the same controller if you checked for this controller the box "Accept the same identifier as long as the detection loop remains occupied".

  « Anti-tailgating » (A-TG): During their presence detection cycle, users can take or scan only one same valid identifier. The loop must become free before the controller can interpret or generate another (different) token/identifier, sanctioning this way people that would try tailgating. When two cars tailgate on a controller with A-TG enabled, the second one is refused even if it scans a different valid identifier than the first car. The function "Accept the same ticket as…" can also be applied here, which only makes sense in the case of a scanner controller.

- Accept the same identifier as long as the loop remains occupied:
  When this box is checked, as long as they did not leave the presence detection loop, users can use their same token/identifier multiple times to (re)open the physical access, even if their identifier would for instance be a Single Use ticket and even if the second scan would happen after the identifier's validity.



With the function "Accept the same identifier…" you overrule both the credits and the time validity of identifiers.



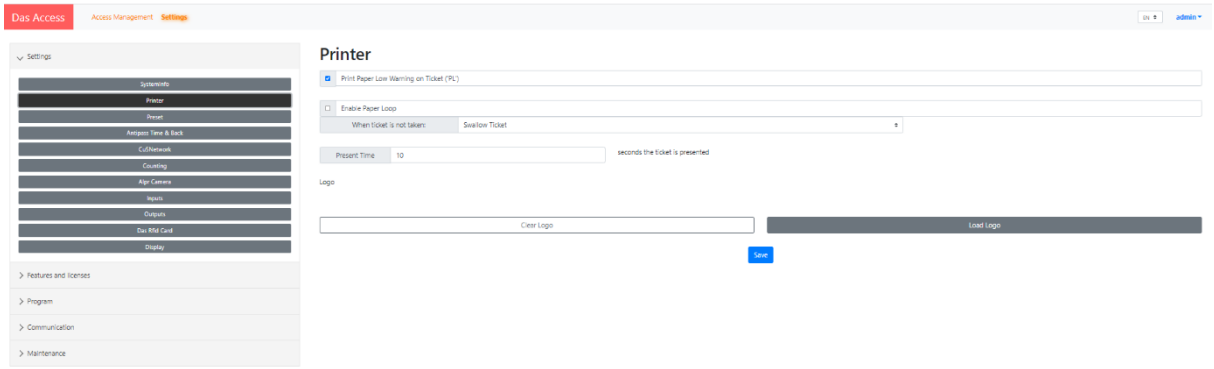
To make a printer column "coronaproof or contactless", connect your presence detection module to a push button input of the controller. The CU5 will from then on automatically print one ticket upon each new presence detection. If the ticket is then not taken, the CU5 will retract or eject that ticket after a predetermined time (depending on the configuration you've chosen, see **3.3.5.3**).

- Extend ticket: validity time added automatically to each scanned identifier.

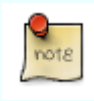
A scanner controller with a time value in the Extend Ticket field will extend the validity of scanned identifiers by this value. If you would by accident configure this feature for a printer controller, it won't be taken into account.

3.3.5.2 Printers

This window allows you to set up kiosk printer-related functions.

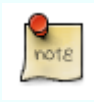


- Printer paper low warning: This option allows the printer to print "PL" (paper low) at the top right of tickets when the paper roll reaches a critical level. On the kiosk printer, move the paper sensor next to the paper roll so to determine the level you find acceptable.
- Enable paper loop: Check this box only when using 80gsm paper. Unchecking (= default) is mandatory when using paper that exceeds 80gsm.



The box "Enable paper loop" is by default unchecked which is the mandatory box status when using thermal paper thicker than 80 g / m².

- When ticket is not taken: Determine here what you want the printer to do (eject or swallow) when the ticket is not taken after the Present Time has passed.
- Present time: Represents the time during which the printer will present the ticket to the user. After this time the ticket will be swallowed or rejected.
- Logo: These buttons allow to add or remove a logo to the ticket layout. When uploading the logo file, ProConfig Embedded rescales logos that would be too large to the correct dimensions. A coloured logo will automatically be converted into black/white shades.

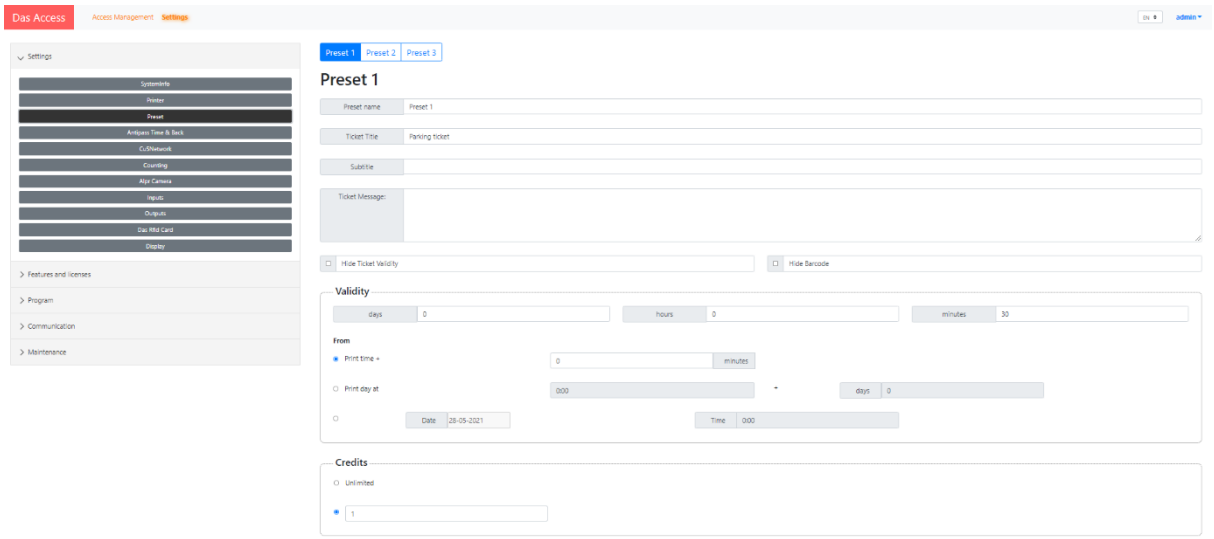


The logo file should meet the following specifications:

- Black/white (no colours)
- Resolution of 200dpi or more
- Formats: .bmp or .png

3.3.5.3 Presets 1, 2 & 3

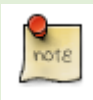
Define here the layout and validity of barcode tickets of up to three different presets. Each controller can thus have its own three preset configurations. Later in this manual, we'll show you how to link these presets to controller inputs.



- Preset name**:** Give a name the Preset.
- Ticket title**:** Title to be printed on the ticket. For example "Parking" (24 characters per line).
- Subtitle**:** Subtitle to be printed on the ticket. For example "Downtown" (48 characters per line).
- Ticket message**:** Add here a personalized text such as additional information on the operation of the car park (48 characters per line).
- Hide ticket validity**:** Check this box if you do not want the expiration time to be printed on the ticket.
- Hide barcode**:** Check this box if you do not want the barcode to be printed on the ticket.
- Ticket validity**:** This time represents the validity of the ticket. When filled in, both a start and end validity will be printed on the ticket.
- Validity**:** Determine here the ticket validity and when this validity starts
    - **Validity duration**: Determine the number of days/hours/minutes a ticket will be valid for
    - **From:** Determine when the duration starts
        - Print time + x minutes. Determine the start time of the validity period based on a number of minutes after the print time.
        - Print day at……+ days: Determine how many days in the future and at what time of that day the validity starts.
        - Date & time: Determine the start time of the validity period based on a specific date and time (HH/MM) of that day.
- Credits**:** This value represents the number of times the ticket will be accepted within the ticket validity period.
- Hide barcode**:** Check this box if you do not want the barcode to be printed on the ticket.

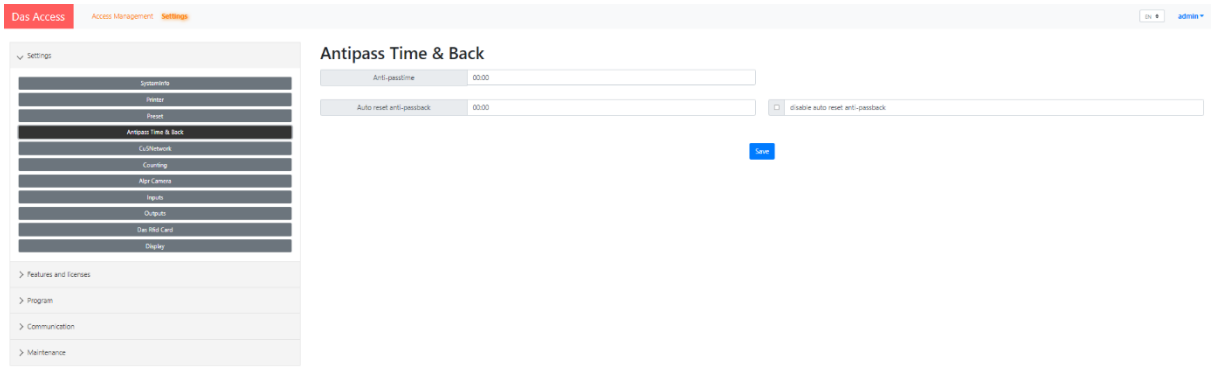
The Credits principle is applied differently in the case of networked or standalone controllers. For networked controllers, Credits is valid for the entire group of controllers. With standalone controllers, Credits is valid for each controller separately. Example:

- Two **networked** controllers, two-credits identifier:
  - One IN and one OUT controller = 2x go inside and 2x go outside (**four** passages).
  - Two OUT controllers = go twice on any of the controllers (**two** passages).
- Two **standalone** controllers, two-credits identifier:
  - One IN and one OUT controller = 2x go inside and 2x go outside (**four** passages).
  - Two OUT controllers = go twice on **both** controllers (**four** passages).

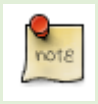


If you activate a virtual or physical link between an entry and an exit controller, the "entry preset values" determine whether and how much time a user has to leave the site.

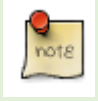
3.3.5.4 Anti-passback & Anti-pass time



- Anti-pass time: When this feature is active, it limits the number of accesses that users can do in a given time. For example if you set the anti-pass time to 30min. (00:30), users will be able to scan their ticket once every 30 min at maximum, even with a multiple use ticket that would be valid for a longer period of time. This function is therefore only applicable for tickets that were generated to allow multiple passes (= multiple use tickets).
- Anti-passback (APB): For the APB principle to work, at least one entry and one exit controller must be included in the APB network/access rule. See **3.3.11.1** for how to include the APB function on access rule level, **3.3.5.5** for how to activate the function "Network Connection" for the controllers in question and **3.3.10.1** for how to perform a punctual/manual/forced reset.
    - Auto reset anti passback: Determine here during which period an identifier, after it has been scanned or printed, is checked for its APB position and after which DAS will perform an automatic APB reset.
    - Disable "Auto reset anti passback": check this box if you do not want to enable this function.



With the anti-passback feature, users are required to use their identifiers on any access that is part of an APB network, in order not to be denied access. More specifically: a user will not be accepted at the APB exit column if she/he has not been detected at the APB entrance column first, and vice versa.

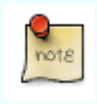


If one of the network controllers is unresponsive while an identifier is being checked for its APB position, the controller you are requesting access to will still grant access anyway after two seconds of unsuccessful polling.

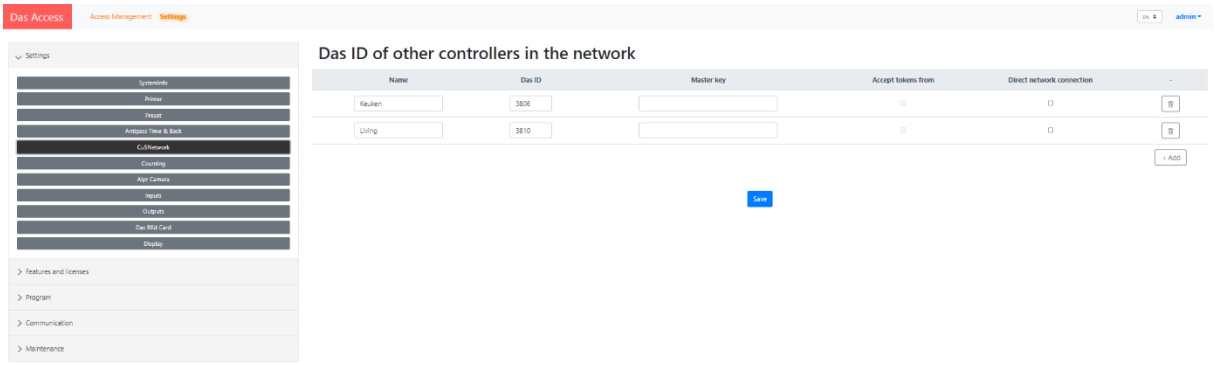
3.3.5.5 CU5 network

Enter here controllers that should be linked to each other either via a virtual link or via a data network. A data-network link is necessary for functions such as: "anti-passback & anti-passtime" (see **3.3.5.4**), "counting" (see **0**) and "one-ticket". In short, all functions/use cases for which the barcode information is insufficient. A virtual link is necessary for the function "Linked Printer" (see **3.2.2**), (see Error! Reference source not found.) so that an offline/stand-alone scanner controller would know from which printer controller(s) it is allowed to interpret identifiers.

Later in this manual we'll show you how to configure access rules for your regular users using ProConfig Embedded. The controllers you enter here will then be available to create those access rules.



By "one-ticket" we mean a function in which (usually) a barcode ticket is converted into or associated with an exit or discount ticket. For example: 1) DAS Barcode Up-Downgrader that links a discount value to a scanned entry ticket, so that the pay station automatically applies a discount when you scan that same ticket to it, 2) DAS pay station where your entry and/or discount ticket becomes an exit ticket after a valid payment, 3) DAS Barcode Up-Downgrader that upgrades your entry ticket with a 30-minutes validity on the exit column, …



- Name**:** Add here a meaningful controller description/name. For example: "Entry Lane 1". This way the controller will be recognizable when it appears in one of the DAS software.
- DAS ID**:** This is the CU5's configuration file number. The DAS ID is also shown on the CU display when powering it ON.
- Master key/Accepts tokens from**:** When this box is checked, the Masterkey field on the same row must mandatory be filled in (with 28 digits) so that the controller in question and the controller above (in System Info) are virtually linked to each other. The Masterkey consists of 28 digits (S&G Pro Identity) and is supplied with the controller on a PVC card.
- Direct network connection**:** Check this box for all the controllers (DAS ID) that need to be able to communicate (with each other and with the controller in System Info) over a local data network. This is necessary for functions such as: anti-passback, anti-passtime, counting, one-ticket, and database replication. In short, all functions/use cases for which the barcode information is insufficient.

With a revenue controller, we recommend making a virtual link with itself in "Other controllers in the same ....". Thus, a parking user who decides to stay parked longer after receiving the first receipt will only have to scan this receipt at the pay station to pay only for the additional parking time.

You can enter data here for controllers which have not yet been commissioned and/or networked. Then, if you were to perform an offline configuration update procedure on an offline/stand-alone controller (for example, by applying a USB update key procedure), the "virtual links" of that controller will be updated.

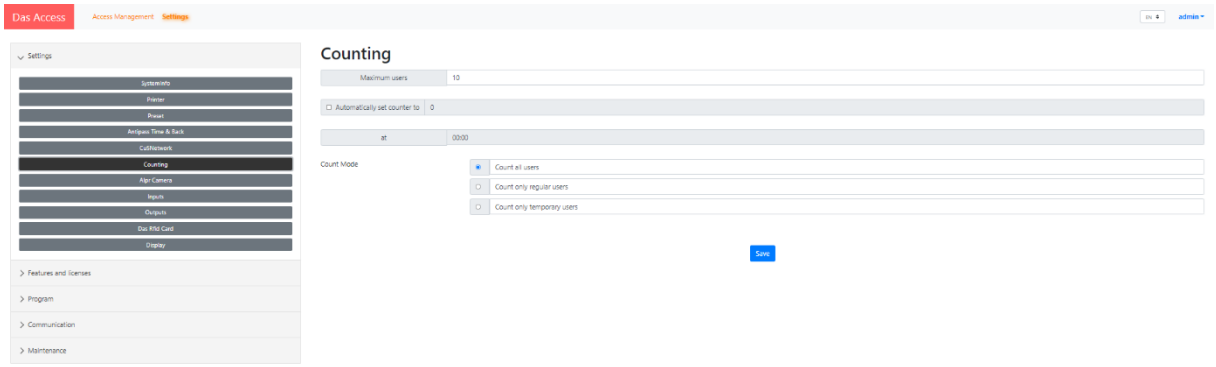
However, if you were to perform an offline configuration update procedure on a networked controller:

- The "virtual links" of that controller will be updated
- The "network links" of **ALL** networked controllers involved in the update will be updated too since CU5 controllers always automatically synchronize the list of networked controllers with each other.

The Virtual Link box can only be checked after a valid printer identity has been entered in the Masterkey/S&G PRO Identity field.

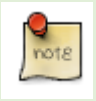
If you entered a controller (e.g. DasID 1111) in "Other controllers in the same network" with the "Network connection" box checked, and if that controller for some reason were to lose its network connection, the message "Controller 1111 offline" will appear at the bottom of the LCD screen of all other networked controllers involved in that same network.

3.3.5.6 Counting



This menu allows counting (for all the networked controllers that you listed in "CU network", see **3.3.5.5**) by taking into account the number of entered and exited identifiers so that entering becomes impossible when a predefined counter limit (= see Maximum Users below) is reached. When reaching this limit the CU5 display will show the message "Full".

- Maximum users: Determine the maximum number of users in your Counting network.
- Automatically set counter to/At : Determine if and at what time you want an automatic reset of the counter.
- Count mode: Determine here which types of users you include in the counting mode. Regular user only, temporary users only or all users.

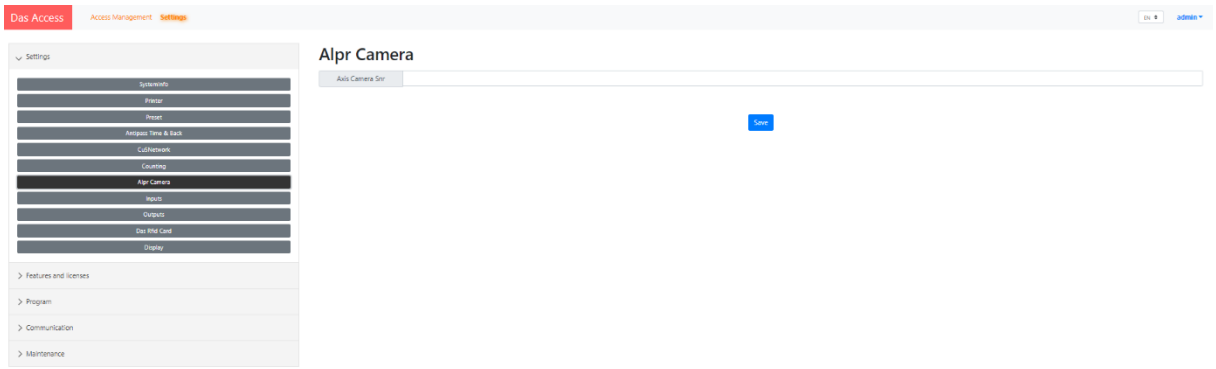


Attention, only the entrances and exits operating in airlock (= SAS) can guarantee a precise presence counter. Without an airlock it is possible to have a situation where the theoretical counter does not correspond to reality. This is why we offer you the possibility of an automatic and regular update of the counter.

3.3.5.7 ALPR camera

A DAS ANPR camera can be ordered and configured as a Master (with integrated optional CU5 firmware) or as a Slave of a CU5 controller. In both cases, enter the serial number of the ANPR camera below and choose between the two working modes:

- Verify access on plate scan: In this mode, only the license plate is used as identifier. This option therefore only makes sense if the camera involved, is a Master controller.
- Create access on plate scan (Print Preset 1): When taking a ticket, the number plate is printed on the ticket. In this mode you use the barcode ticket as a redundant solution. Namely, if the automatic license plate recognition at the exit should fail, you can still scan the barcode ticket to leave the parking lot. It makes therefore no sense to select this mode for a scanner controller.



A CU5 controller and its slave ANPR camera must be connected to the same LAN.

The CU5 will by default accept a one-character ANPR incompatibility (mismatch).

Scan & Go Pro is compatible with Vaxtor's ANPR software integrated with Axis IP dome cameras. Please contact your supplier if you want Scan&Go Pro to be compatible with other camera's and ANPR software as well.

DAS' ANPR solution is extremely plug & play. As a result, each APo60f3/3.x column is supplied with a mounted and pre-programmed ANPR camera. All that remains for you to do is fine-tuning on site. These fine-tuning adjustments can optionally be performed by DAS via Team Viewer. For this, please order product code = ReAss1 and if necessary ReAss2 too. We kindly refer to our pricelist for more information.

A DAS ANPR camera always comes with an integrated SD memory card. For privacy reasons, images are stored locally on that card and are only uploaded when requested via our cloud application ProConnect.

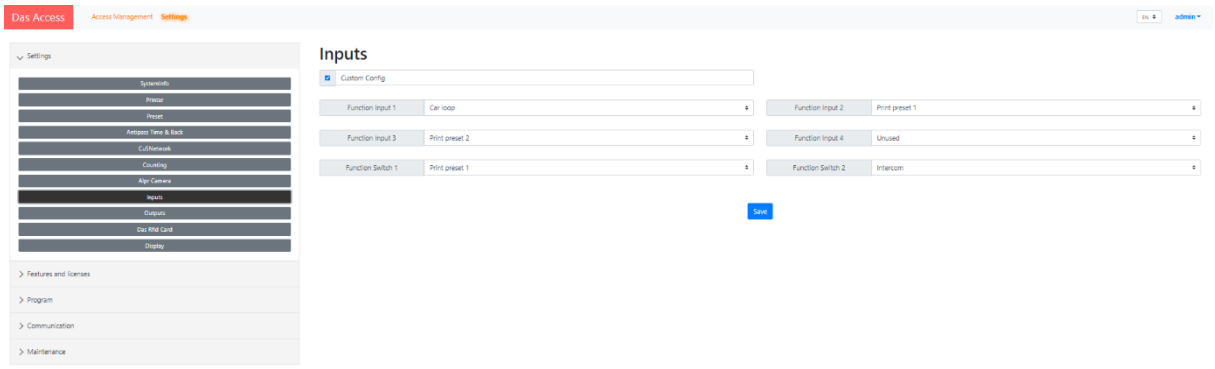
A Master DAS ANPR camera comes with integrated CU5 firmware but only has an Ethernet connector and no USB connector. As a result, a DAS Master camera can be configured via its embedded web pages (accessible via Google Chrome) but offline update procedures using a USB stick are not possible.

Depending on the configuration of your installation, it may happen that an entry ANPR camera scans the front of an entering vehicle and then, immediately afterward, an exit ANPR camera scans the rear of the same entering vehicle, causing the DAS system to conclude incorrectly that the car has exited the parking lot. This can happen, for example, with a "one barrier – one entry camera - one exit camera"-configuration. You can avoid this problem by linking to the entry camera a Preset having in the "Validity start" field the value of (for example) one minute. This way the exit camera will only start taking into account possible scans of the same license plate, one minute after the vehicle has entered. For this to work, both cameras must of course be networked.

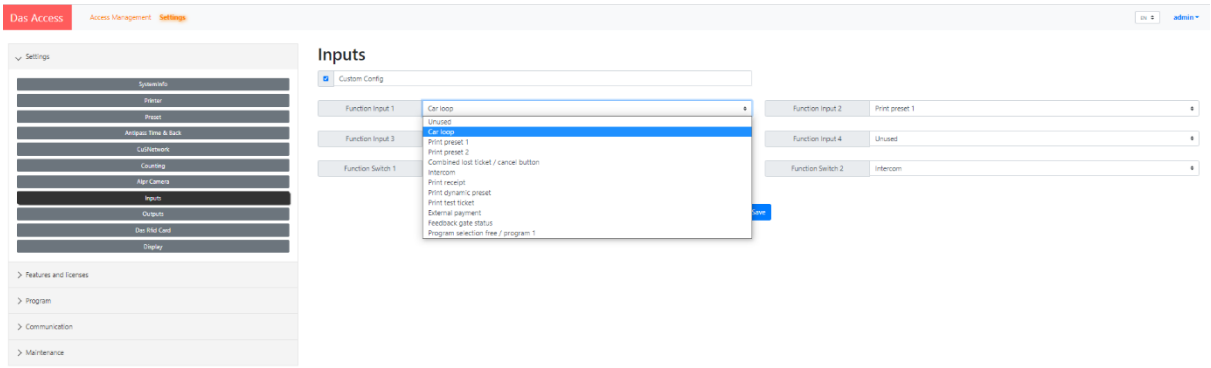
3.3.5.8 Inputs

A CU5 controller comes with the following default configuration for the inputs:

- IN1: Presence detection input (dry contact)
- IN2: Push button input (only when kiosk printer is needed)
- IN3: Abort / lost ticket button (only in case of a revenue column)
- IN4: Free/available input.



ProConfig Offline allows you to deviate from this default configuration. Determine here the custom functions for up to six inputs of which two input switches that allow to connect for instance LED push buttons.



For each input you can choose between:

- Unused
- Car loop
- Printer preset 1
- Printer preset 2
- Combined lost ticket/cancel button (only applicable for a revenue column)
- Intercom
- Print receipt (only applicable for a revenue column)
- Print dynamic preset (see Program 1 and Program 2, chapter **3.3.7**)
- Print test ticket: This command allows to print a test ticket without taking the loop detection into account. During maintenance this allows to test the printer without bridging or switching off the loop.
- External payment: When selecting External Payment for one of the controller inputs and linking an external payment method to it, the controller will interpret each contact on this input as a validated payment and will include it in the reports/statistics accordingly.
- Feedback gate status: When selecting Feedback Gate Status to one of the controller inputs, the controller will interpret each contact it receives as the status of the physical access product in

question and display this status in the DAS software. *(this option can be selected but is not yet available in the controller!!!)*

- Program selection free/program1 (allows this contact to switch between modes Free and Normal/Controlled using a key switch).

For each Input Switch you can choose between:

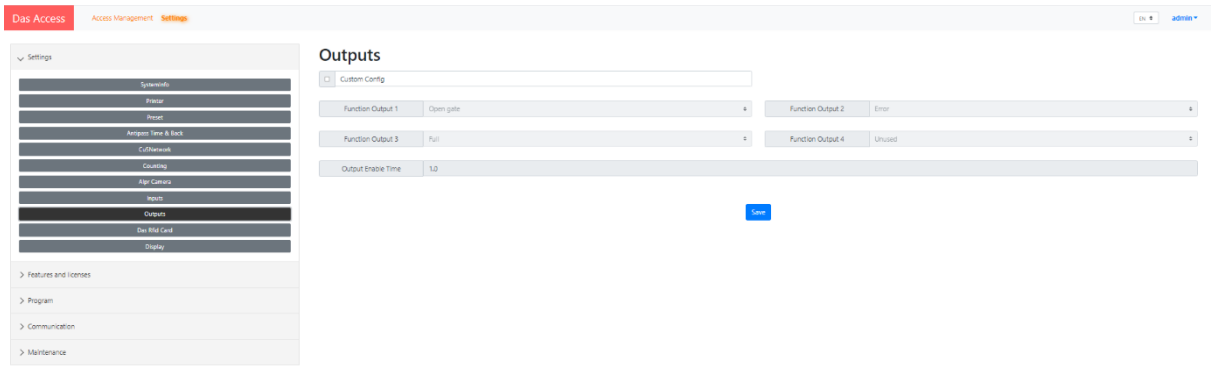
- Unused
- Printer preset 1
- Printer preset 2
- Combined lost ticket/cancel button (only applicable for a revenue column)
- Intercom
- Print receipt (only applicable for a revenue column)
- Print dynamic preset (see Program 1 and Program 2, chapter **3.3.7**)
- Print test ticket: This command allows to print a test ticket without taking the loop detection into account. During maintenance this allows to test the printer without bridging or switching off the loop.
- External payment: When selecting External Payment for one of the controller inputs and linking an external payment method to it, the controller will interpret each contact on this input as a validated payment and will include it in the reports/statistics accordingly.

Some choices are greyed out when Printer or Revenue features have not been activated on your controller. See Error! Reference source not found.. for more info on Features & Licenses.

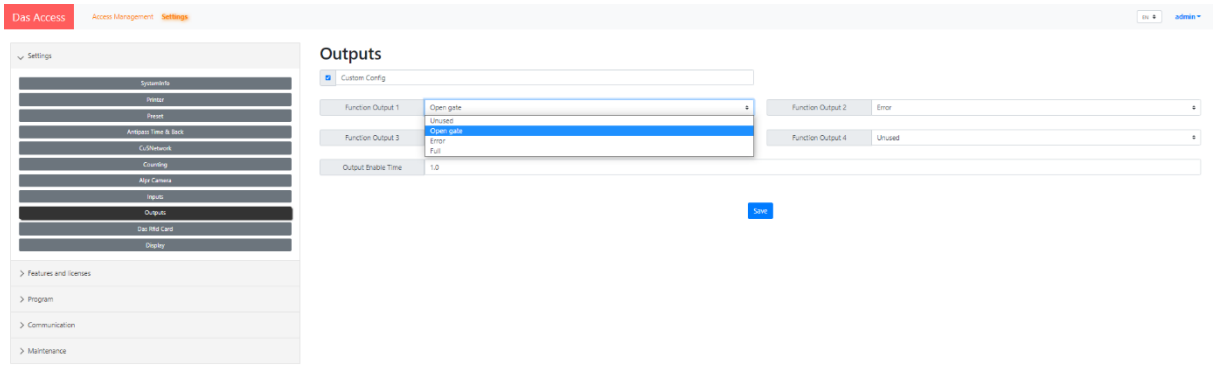
3.3.5.9 Outputs

A CU5 controller comes with the following default configuration for the outputs:

- S1: Output for physical access (automatic barrier, gate …)
- S2: Printer error output (dry contact)
- S3: Free/available output
- S4: Free/available output



ProConfig Embedded allows you to deviate from this default configuration. Determine here the custom functions for up to four output connectors.

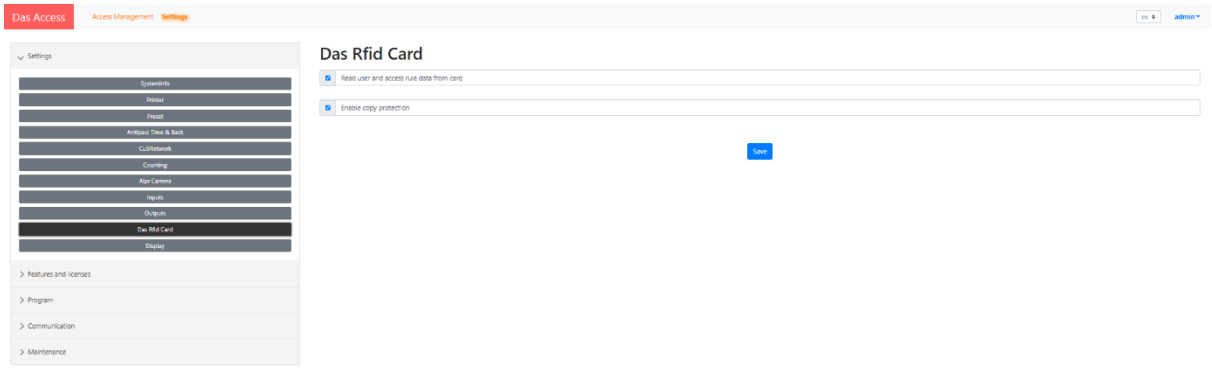


For each output you can choose between:

- Unused
- Open gate
- Error: The CU5 activates this output depending on what you have configured at **3.3.9.3**.
- Full: The CU5 activates this output when the counting limit is reached (= a number of attendees). See **0**.

With "Output enable time" you define the trigger time for the outputs of the controller you now are connected to.

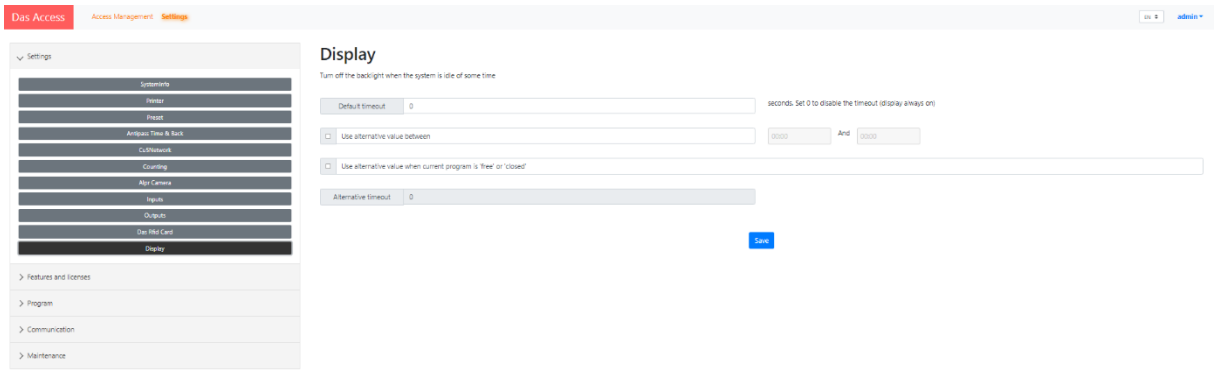
3.3.5.10 DAS RFID cards



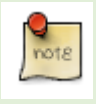
- Read user and access rule data from card: We assume here that the computer used for RFID card enrolment is not connected to CU5 controllers. The access rights are therefore first written on Mifare cards and with the first scan the controllers then copy these rights to their own database.
  When the feature "Read user and…" is enabled, on the first scan of a Mifare card, the CU5 copies the access rights stored on that card to its database. With each subsequent scan of that same card, the CU5 will only update its database again if the access rights on that card are more recent. The controller will always first complete this check and only then execute the access rights. This whole procedure is, of course, performed in a fraction of a second.
- Enable copy protection: Determine here if you want to activate the card copy protection feature and thus limit the risk of copied cards. How does the Copy Protection principle work?
  When we (= DAS) format RFID cards, we initialize a counter on the card. When you (= the customer) create RFID cards using our software in offline modus (= not connected to our CU5 controllers while you generate RFID cards), you write access rules on the Mifare card. When you scan this card for the first time to a controller, the controller increments the counter in the card and copies the access rules and that counter in its own database. From then on, each time this card is scanned to a controller, the controller will first increment the counter in the card, copy the card counter to its own database and compare this counter value to the previous counter value that the controller already had for that card. Conclusion: if for a given card, the internal counter in the card is lower than the counter in the controller, this controller will consider the card as a copy and therefore refuse it.

3.3.5.11 Display

Determine here whether and for how long after the system has been idle, the LCD backlight should be turned off.



- Default timeout = the number of seconds that the system must be idle before the display backlight can be turned off. When set to 0, the display will remain ON all the time.
- Alternative value: determine an alternate timeout value and when to apply it.
    - Start and end time
    - When the program Free or Closed is applied for this CU
    - *When both boxes above are checked their relation is "or" and not "and".*



The controller's idle state starts as soon as the LCD displays a standard message AND (in case the Car Loop input has been activated) no presence has been detected.

3.3.6 Standard and optional features and licenses

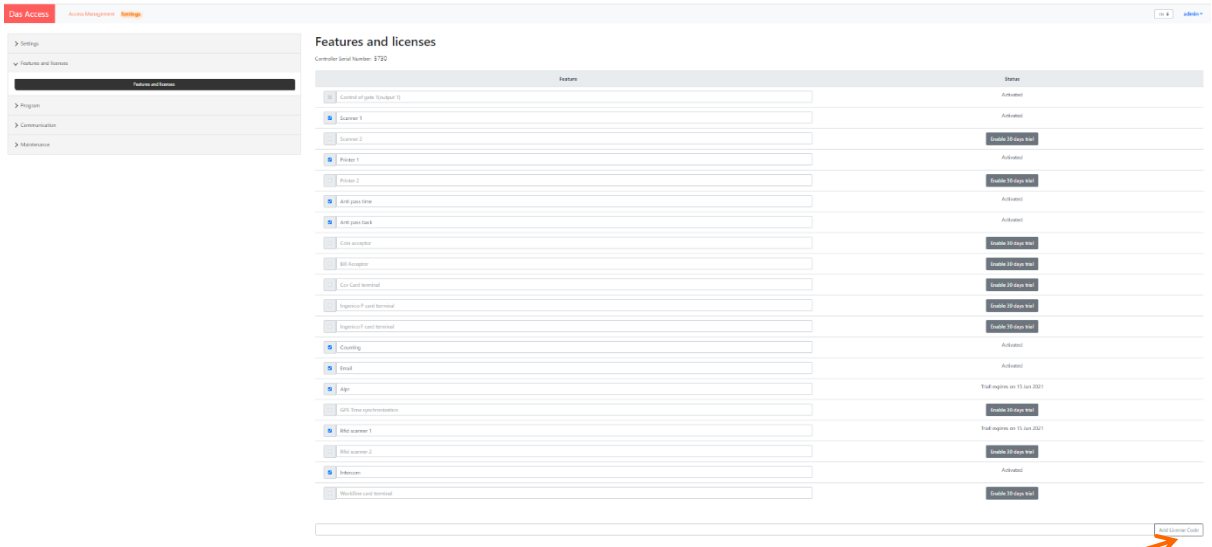
Click on Settings (in the banner on top of your screen) and then on Features&Licenses (in the treeview on the left of your screen).

A CU5v2 controller comes with activated features and licenses according to the configuration and options you've ordered (scanner controller, printer controller, revenue controller, anti-passback, etc ….).

With ProConfig Embedded you can temporarily activate, for a 30-days trial period, firmware functions that you didn't order. However, keep in mind that some of these features/options can only work if you have the according peripheral products too, such as an ANPR camera, an RFID reader, etc ... After this trial period, the activated options and devices will automatically be deactivated again.

If you wish to purchase one or more features and activate them permanently, please contact your supplier, inform them about the hardware number of the controller(s) that you'd like to upgrade (you can find it at the top of your "Features and licenses" page) and which options you want. Your supplier will provide a license code that you can enter at the bottom of this page. Then click on Save. You can also activate the license code by scanning a specific barcode to the controller. Contact your DAS supplier for more info.

Each license code is unique to each controller and cannot be used for other controllers. For example, if a license was generated to activate a printer and scanner for the controller with the serial number 5062, you will not be able to use this license code for the controller with serial number 5063.

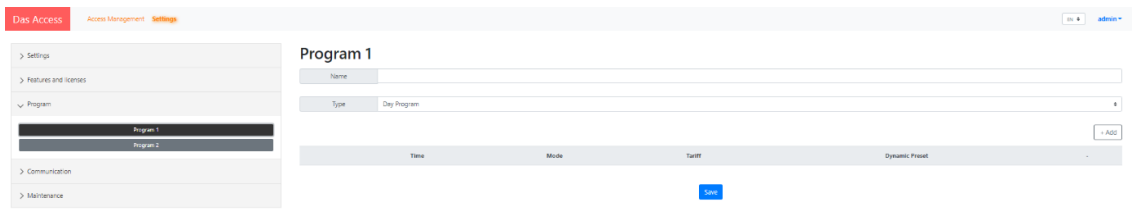


Enter your licence code and click on:

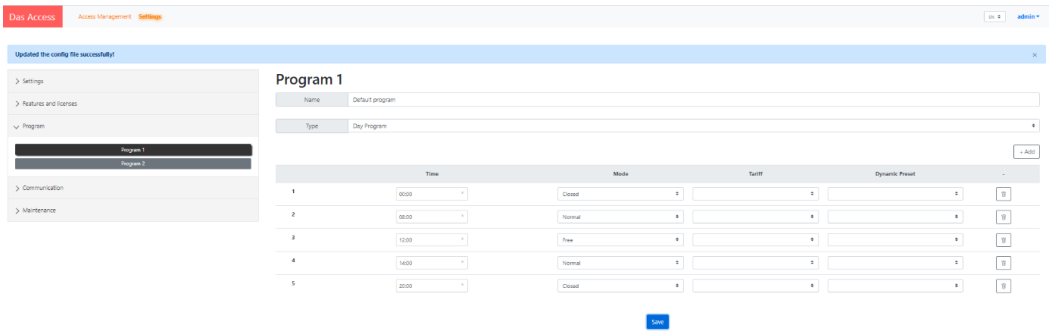
3.3.7 Program 1 and Program 2

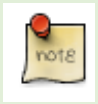
Here you can define two programs of up to 64 time lines each, with for each time line a controller operating mode, a pay tariff (in case of a revenue controller) and a dynamic preset (in case you've selected Dynamic Preset for a controller input – see **3.3.5.8**). The two programs are specific to each controller. In the worst case, one installation can therefore consist of controllers that each have a different setting for the two programs.

Start by giving your program a name and choose whether you are going to create a day program or week program.



Then set the start time of each period and the operating mode. You have 64 zones available to define a typical day or week. Example: parking lot is closed from 20:00 to 08:00, controlled from 08:00 to 12:00 and from 14:00 to 20:00. Between 12:00 and 14:00, the access is open. This is what you then get:





If you combine the modus "Free" with loop detection, the physical access will open as soon as the loop detects a presence. If you combine this modus WITHOUT presence detection, output 1 will permanently be activated and the physical access will remain permanently open.
Please check the compatibility of your physical access with the latter configuration. Some automatic barriers could be configured to close automatically after a while, even with our permanent open command.

The Tariff column is only available when, for the controller in question, at least one payment device has been activated at Features/Options.

On row level you can only select a Tariff if the same row has "Normal/Controlled" in the Mode column.

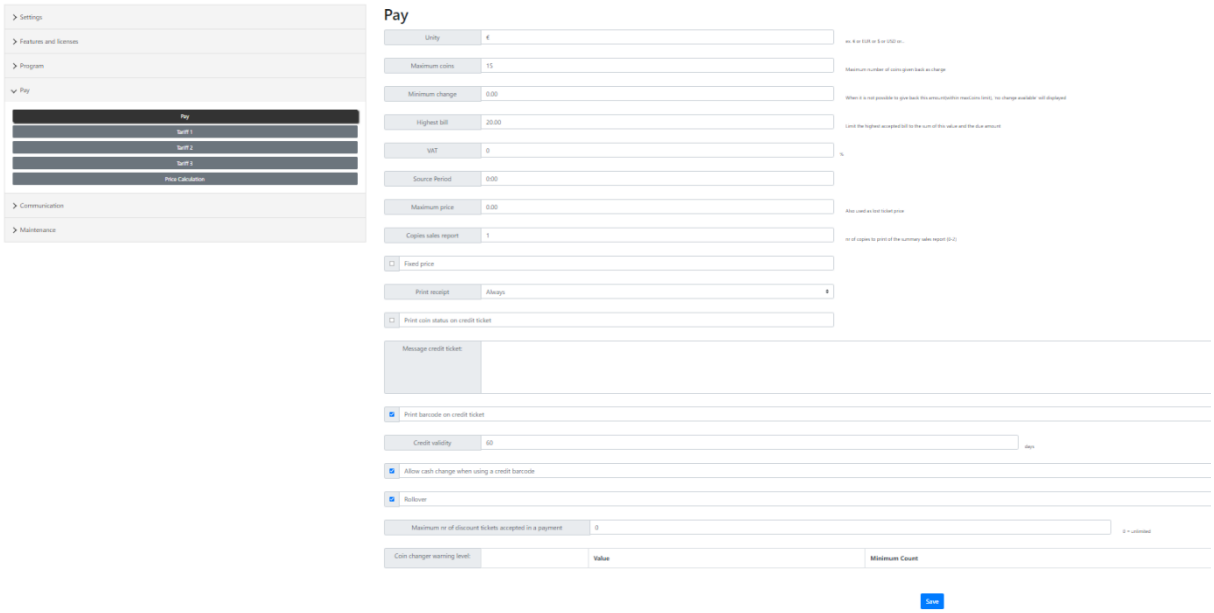
The Dynamic Preset column is only available when, for the controller in question, Dynamic Preset has been selected for one of the controller inputs (see Settings>Input).

On row level you can only select a Dynamic Preset if the same row has "Normal/Controlled" in the Mode column.

3.3.8 Pay

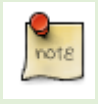
Go to Settings>Pay>Pay. In the example below, the CU5 controller has al possible payment devices activated (coins recycler, banknotes recycler and bank terminal).

3.3.8.1 Pay



- Unity: Enter your currency here, either as a symbol or not.
- **Maximum coins**: This is the maximum number of coins that the controller will give back as change. If this number is not enough to give change (because your stock of banknotes is empty for instance), a ticket will be printed indicating a credit amount. Example: for a transaction of 4.00 € the user inserts a bank note of 20.00 €. If the number of maximum coins has been fixed at 5 and there are no banknotes available to be given as change, the user will only recover a maximum of 10.00 € (5x2€). A receipt will then be printed indicating a credit of 6.00 €. It is important to set this feature to a reasonable value. This to prevent the coins recycler from using a large amount of low value coins, when no high value coins or banknotes are available.
- **Minimum change**: If it is not possible to give back this amount of change (without exceeding the Maximum coins setting) the message 'no change available' will be shown on the CU5 display. If enabled the error relay will be activated and/or an email sent.

- **Highest bill**: The highest bill accepted will be the due amount + this setting. So when for ex. highest bill is 20€ only bills up to 20€ will be accepted when the due amount is below 30. When the due amount is above 30€, 50€ bills will be accepted too.
- **VAT**: This value is expressed in %. Put "0" and there will be no VAT printed on the ticket.
- **Source period**: An entry ticket usually contains a minimum time validity for the exit columns (in case the parking lot would be full). With this function you determine whether and how much of this period becomes payable when the visitor exceeds the minimum time validity.
- **Maximum price**: Represents the maximum amount that the controller is allowed to charge. It also represents the cost of a lost ticket.
- **Copies sales report**: Corresponds to the number of copies of offline sales reports that the controller will generate when scanning a logon user command card.
- **Fixed price:** When checked, the user will be charged a fixed amount (=maximum price) without having to scan a barcode first. In this case the Fixed Price is obviously also the Maximum Price.
- **Print receipt**:



With regard to the printing of a receipt, we want to point out the distinction between bank- or DAS-related information. The two parameters mentioned below (Ask and Always) only relate to DAS information that the CU5 will print or not on receipts (= barcode, title, subtitle, etc....). In some cases the bank card issuer and/or the transaction acquirer "force" pay stations to print information regarding the electronic payment on the payment receipt even if you chose Ask for "Print receipt".

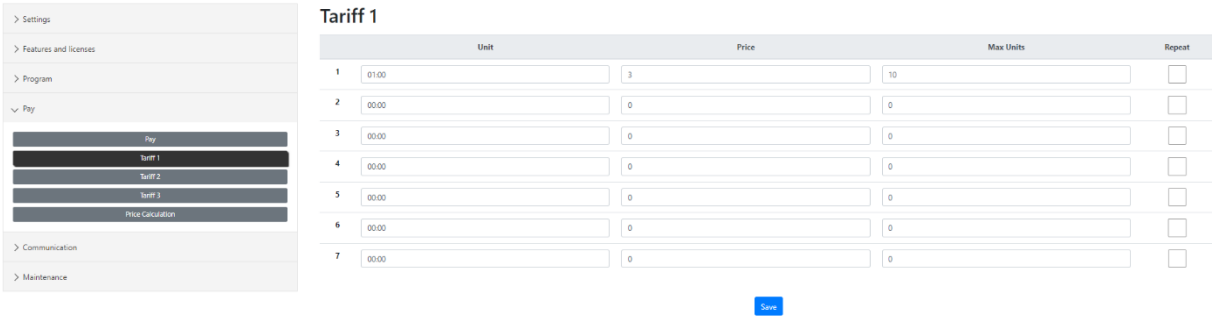
  - Always: The controller will print a ticket with each payment transaction.
  - Ask: The controller will only print a receipt after pressing the "receipt" button after payment.

- **Payment & access info separated on receipt:** When enabled, the controller will print a dashed line underneath the payment information together with the words "Please tear here".
- **Print coins status on credit ticket**: This option prints the quantity of coins in each coins changer tube at the time that the controller prints a credit note.
- **Message credit ticket**: Free message that can be printed on a credit ticket. This message could for instance be the procedure to follow for the refund of the credit amount.
- **Print barcode on credit ticket**: When this box is checked, the controller will print a barcode that can be used as a means of payment or rebate/discount for a future payment on the same controller.
- **Credit validity:** Determine here the number of days the credit barcode will be valid.
- **Allow cash change when using a credit barcode**: When enabled, you allow the controller to give change after scanning a credit barcode ticket. For example, a user who has a € 5.00 credit ticket and has to pay € 2.00 will receive € 3.00 in change after scanning his credit ticket.
- **Rollover:** If you have configured at least two parking tariffs and a program that switches between these, the Rollover function allows you to determine what you charge to customers who would overlap the time period associated with both tariffs. Here is an example for a customer that would use the car park from 4.30PM to 5.30PM
  - **Tariff 1:** 1€/h from 6AM to 5PM
  - **Tariff 2:** a fixed amount of 5€ between 5PM and 6AM
  - **Total amount due when Rollover is NOT checked:** 6€ (1€ + 5€)
  - **Total amount due when Rollover is checked:** 1€ (from 4.30PM to 5.30PM at tariff1).
- **Maximum number of discount tickets accepted in a payment:** Enter a number here if you wish to limit the number of credit tickets allowed per transaction.

- **Coin changer warning level:** The coins recycler has 6 tubes that autofill automatically and therefore serve as a stock for change money. You can determine here which minimum quantity you don't want to exceed in each tube. In the menu Communication you then can determine which action to trigger when this limit is reached: "Controller out of order" and/or "Activation of an error output" and/or "Sending an e-mail".

3.3.8.2 Tariff 1, 2 & 3

You can configure up to three different parking tariffs. These tariffs can be used according to time slots that you define with Program 1 and Program 2 (see **3.3.7**):



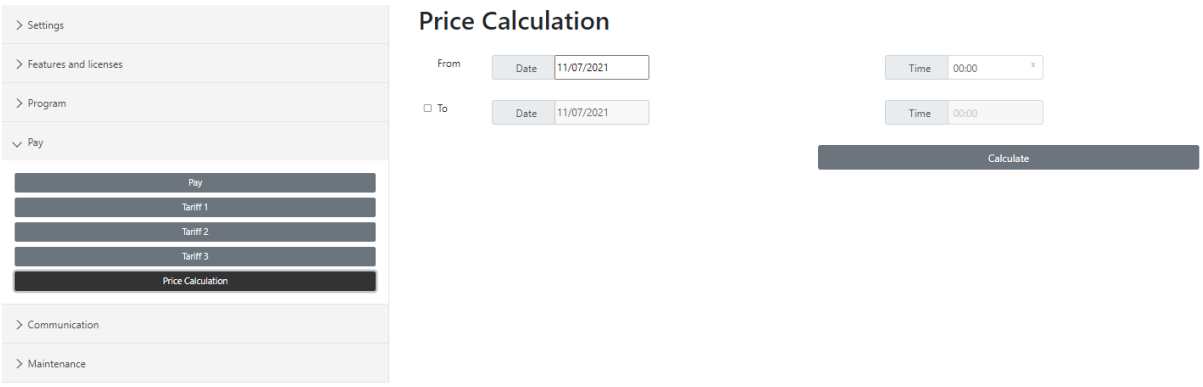
- Unit: Time unit you want to charge, by minute, by hour....
- Rate : Time unit cost
- Max units: Maximum number of units you want to charge. If for example only one line is completed, the amount will remain fixed.
- Repeat: When enabled this function will loop all the lines that have been included. For instance, when enabling this function for line 1 & 2, the loop will be: 1 – 2 – 1 – 2 – 1 – 2 - … When enabled for all three lines, all 3 lines will be repeated: 1 – 2 – 3 – 1 – 2 – 3 - … When enabled for lines 2 & 3, the loop would be: 1 – 2 – 3 – 2 – 3 – 2 – 3 - … This option makes it possible to omit the "Max Units" field. So in the example above, if Repeat is not checked, after 10 units the total amount to pay will be fixed and equal to 1 Unit x 3 euro x 10 Max units is 30.00 €. If the Repeat box is checked, the maximum amount that the user can pay will be limited to the amount you chose for the field "Maximum price" in the chapter Pay (see **3.3.8.1**).

On the principle a started unit is due. For example, if you charge € 4.00 per hour, the user will have to pay € 4.00 from the first minute, which will result in the following:

- From 00:00 to 0:59 · 4.00 €
- From 01:00 to 1:59 · 8.00 € and so on.

In most cases we advise you to work with smaller units such as 15 minutes or 10 minutes.

3.3.8.3 Price calculation

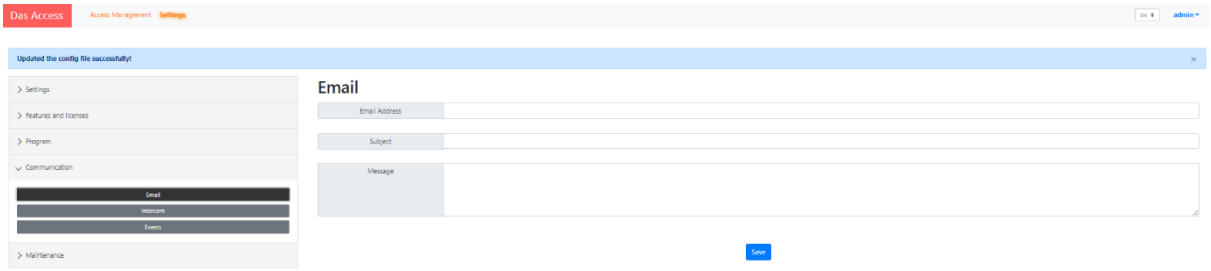


3.3.9 Communication

Depending on the features/options you've bought, you'll see up to three sections: Email, Intercom and Events.

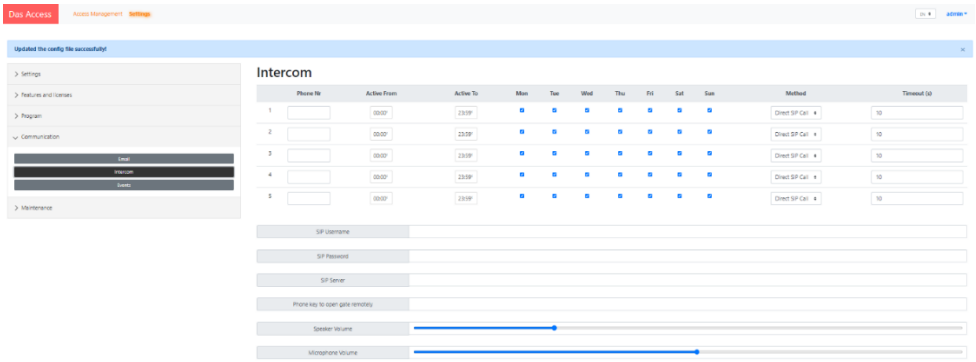
3.3.9.1 E-mail

The window Email only appears when the option "Email" is enabled under Features and Licenses. See **3.3.6**. Here you determine the subject, message and email address(es) to which the controller will send e-mails.



Separate e-mail addresses by ";" if you want the controller to send e-mails to more than one address.
We advise you to include at least the name of the controller in the message so the mail recipient will clearly know from which controller the e-mail came from.

3.3.9.2 Intercom



Each CU5v2 controller comes standard with an integrated speaker and microphone and embedded VOIP intercom software. The latter is a commercial option that can even be activated at any time in the menu "Features & Options" either for a free-trial period of 30 days or permanently by completing an optional license code or by scanning a specific barcode that you need to order with your supplier. We offer three ways to deploy our VOIP intercom:

Direct SIP calls: In this case, the CU5v2 controllers are connected to the same LAN to which the SIP telephones are linked. With ProConfig Embedded you then determine the "cascade sequence" according to which SIP phones will be called directly (no landlines nor mobile phones) - this solution requires no local VOIP server nor VOIP software.

Via local IP-PABX (= Private Automatic Branch Exchanger): In this case, the CU5v2 controllers are connected to the same LAN to which the IP-PABX is linked. With ProConfig Embedded you then enter the login details of the IP-PABX server (user name, password and server name). This IP-PABX will then further handle the calls. This configuration allows to call SIP phones and/or landline and/or mobile numbers, depending on the configuration of the IP-PABX.

Via a public VOIP server. Enter the login details of a public VOIP provider (user name, password and server name) so the CU5v2 controller knows to which VOIP server to connect. This provider will then further handle the calls (we suggest the provider 3Stars, see below). The connection with a provider is always done in one direction (from controller to provider). That's why you do not need to complete the VOIP subscription with phone numbers. However, as DAS supports the DTMF protocol, the push buttons of a phone can be used to activate an output of the CU5 with which the phone is in connection.

Connecting with a public VOIP server can be done in two ways. Wired and wireless. Both ways allow calls to fixed and mobile numbers.

- *Wired:* CU5v2 controllers connected to a LAN that allows connection with a public VOIP provider on the internet (for instance 3Stars, see below).

- *Wireless:* Via 4G/5G (using our optional modem/router Wlint3). In this case you need both a subscription with a public VOIP provider and a SIM card with data subscription. This configuration allows the processing of multiple intercom calls simultaneously using one data subscription (data communication can be shared). The intercom calls must then come from CU5v2 controllers that are in the same network that is connected to the modem/router.

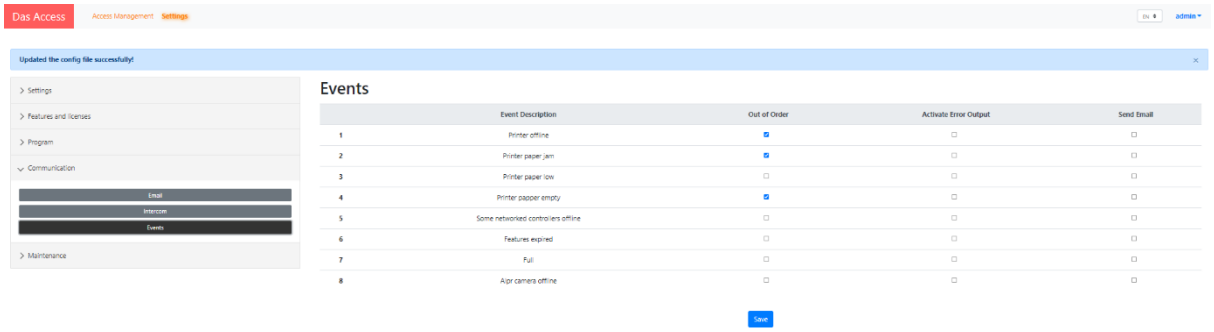
As VOIP over a mobile data connection is sometimes made difficult by mobile operators, DAS has validated and therefore suggests the provider 3Stars. The 3Stars call rates were at the time of writing: 0.025€/min for landline numbers and 0.05€/min for mobile phones. Ask DAS for a subscription file. DAS does not assist in support of other providers for all reasons stated above.

DAS allows calling up to five phone numbers according to a cascade sequence. A mix of the above three options can be used to determine this sequence (Direct SIP calls, via local and/or public VOIP servers).

We do not offer a GSM voice solution because 3G USB modems are hardly or no longer available and because 4G/5G USB modems do not support GSM voice technology.

3.3.9.3 Events

Depending on the number of activated options/features for your controller, you can see a list of up to twenty events for which you can determine up to three actions. When all three actions checked, these actions can take place simultaneously. The available actions are: Out of order (the controller stops working and displays the message "Out of order") and/or Activate error output (this is by default output s2) and/or Send e-mail (the controller then sends an e-mail).



The messages that the CU5 sends with the event "Printer not connected / not ready" will clarify whether it is a printer that has lost its connection or a printer that is connected but reports an error.

1. Printer not connected / not ready.
2. Printer paper jam.
3. Printer paper low: *The printer is equipped with a sensor that detects the amount of paper on the roll. Upon reaching a minimum paper quantity, the printer can print a 'paper low' message on the tickets and trigger an alarm.*
4. Printer paper empty
5. Printer not connected.
6. Scanner offline
7. RFID reader offline
8. Coinchanger offline
9. Coinchanger error
10. Coinchanger cassette removed
11. No change available
12. Bill acceptor offline
13. Bill acceptor error
14. Bill acceptor cassette removed
15. Bank card terminal offline
16. Bank card terminal error
17. Some networked controllers offline
18. Features expired
19. Full: this event refers to the functionality "Counting". See **0**.
20. Alpr camera offline

In order to avoid unnecessary/false e-mail alarms the tablet will only send an "event alarm e-mail" after that event (see Error! Reference source not found.) is occurring for several seconds.

If applicable, we recommend that you always check the "Out of order" action for the events: Printer not connected / not ready, Printer paper jam, Printer paper empty and Scanner offline. Do this also for the coins recycler and the bank card terminal if this is the only means of payment in your payment station.

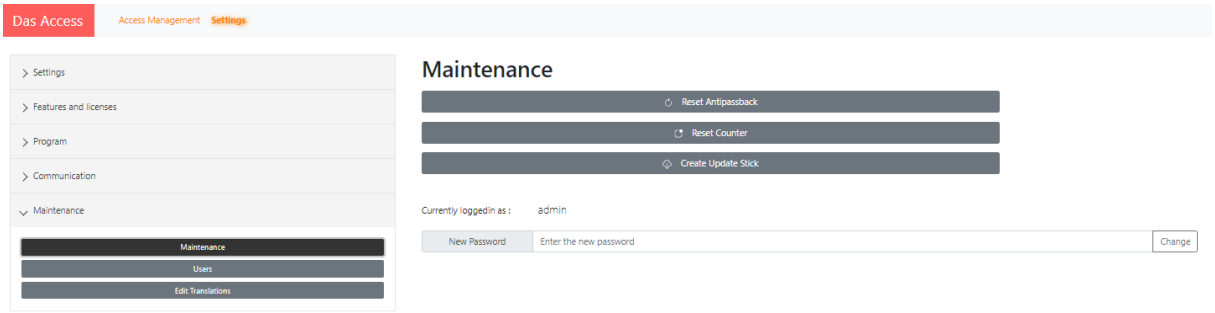
The action "Out of order" has the advantage that these words will be displayed on the LCD screen (in addition to the reason for the technical failure, at the bottom of the screen), so that there can be no misunderstanding for the user as to why the controller refuses to grant access.

For a slave camera ANPR camera you have the option to check all three available actions for the event "ANPR camera offline". For a master ANPR camera however, only the "Send e-mail" action makes sense.

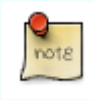
For sending an email, the CU5 can only be triggered by a status change of an event. If the status does not change after that, the CU5 will not send a second mail about the same event.

3.3.10 Maintenance

3.3.10.1 Maintenance



- Reset anti-passback: Is a one-off command that allows to set the APB counters to zero. This operation will automatically be applied to all users (both regular and temporary) that have an access rule for which the function APB has been activated. From then on, the APB status of these users is unknown and they all will be accepted at their first scan.
- Reset counter: Manually determine to which number you want to reset the counter. This action will be applied to all controllers included in your counter network.
- Create Update Stick: This function allows to download a CU5 configuration file from ProConfig Embedded to a USB stick so that you can then update the configuration of all affected **standalone/offline** CU5 controller (= a CU5 that is not connected to ProConfig Embedded):
  - By simply plugging the USB stick into the controllers
  - By e-mailing the configuration file(s) on that USB stick to an on-site-person so that they then can save this file to the root of a USB stick and plug it in the controller that needs to be updated.
  - We refer to the manual "ProConfig Offline" for all available offline update procedures.



A file created via the "create update stick" procedure can only be used to update a controller via a USB stick.
If you want to copy the configuration file from controller A to controller B, you can download the configuration file from a controller A to a USB stick, rename that file with the DASid number of controller B and then insert that same USB stick into controller B plugs.

- New password**:** If necessary, set a new password here. You can also do this by clicking on your username at the top right of your screen.

3.3.10.2 Users

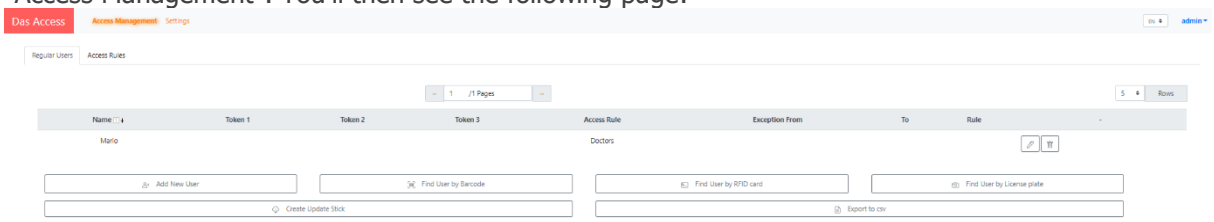
Determine here, for each software user, their name, password and software permissions.

3.3.10.3 Edit translations

This menu allows you to customize both controller display and (when applicable) ticket messages for a specific controller. For example: the default display message 'Welcome' could be replaced with 'Welcome to DAS Access&Revenue Control'.

3.3.11 Access Management

Now that you've finished configuring the Settings menu, which includes CU5 and temporary users settings, you are ready to configure your regular users too. At the top left of your screen, click on "Access Management". You'll then see the following page:

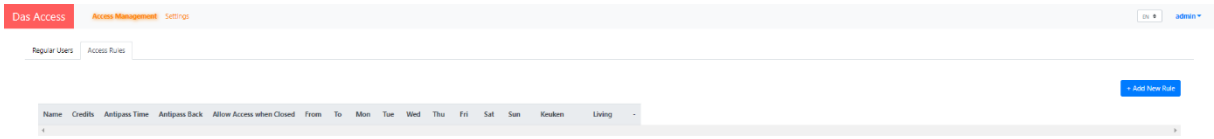


ProConfig Embedded allows you to manage your regular users assigning them access rules associated with up to three different identifiers simultaneously (also called tokens): a barcode, an RFID card and a license plate. Let's start with Access Rules.

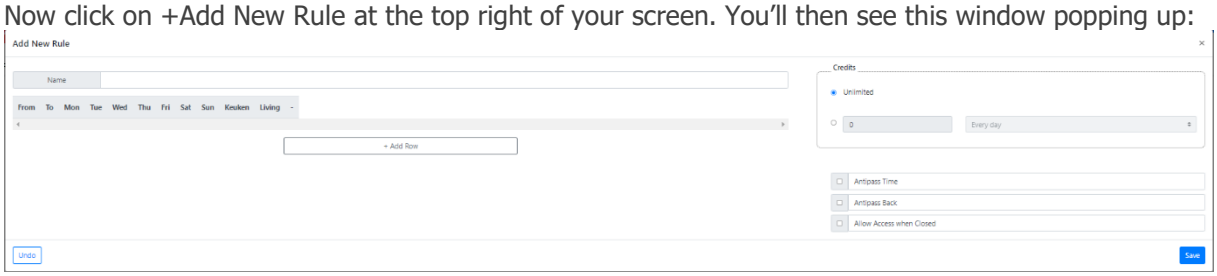
3.3.11.1 Access rules

We assume here that you have already entered controllers in Settings>Settings>CU5 network (see chapter **3.3.5.5**).

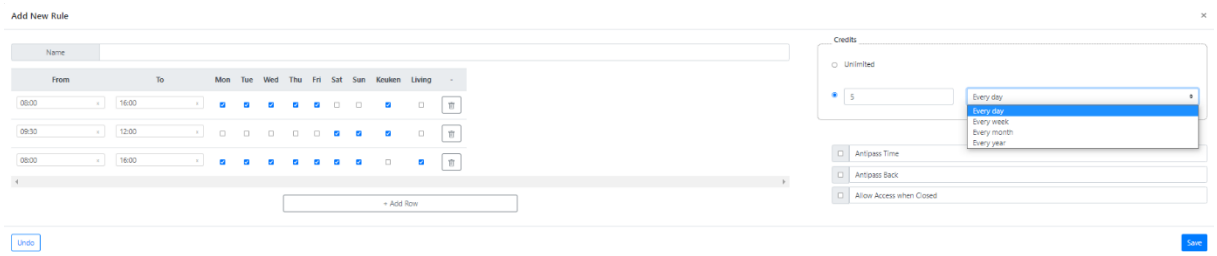
At the top of your screen, click on Access Management>Access Rules. You'll then see the following page:



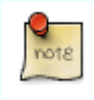
Now click on +Add New Rule at the top right of your screen. You'll then see this window popping up:



- Now start by giving this new access rule a name. We advise you to choose a name whose association with the access rule seems logical to you. This can be the name of a user group (e.g. "Doctors") or a specific location (e.g. "First floor").
- Then click on +Add Row and determine per row for which controllers you want to apply a From/To value and on which weekdays. An access rule can consist of multiple rows.
- Determine whether you want to apply unlimited or limited credits (see **3.3.5.3**) and/or anti-passback and/or anti-passtime (see **3.3.5.4**) to this access rule.
- Allow access when closed: With this function you overrule the closed status of controllers at times when you have access according to your access rule. This is the equivalent of a passe-partout (master key) for physical keys. This could allow you to ensure that the Closed mode is still applied for the temporary users, while it is overruled for (some) regular users.



This is an example of how an access rule can look like. We'll now start by entering regular users.

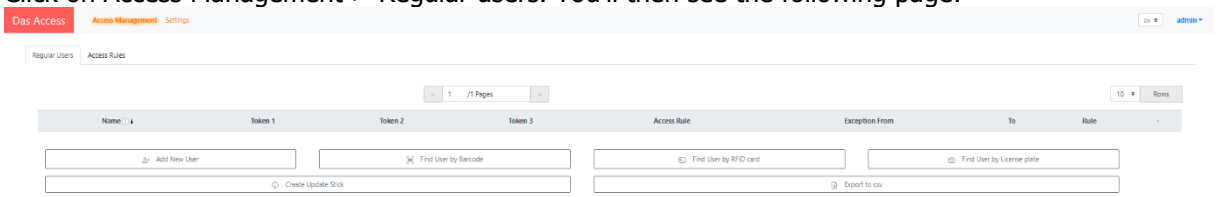


The Credits principle is applied differently in the case of networked or standalone controllers. For networked controllers, Credits is valid for the entire group of controllers. With standalone controllers, Credits is valid for each controller separately. Example:

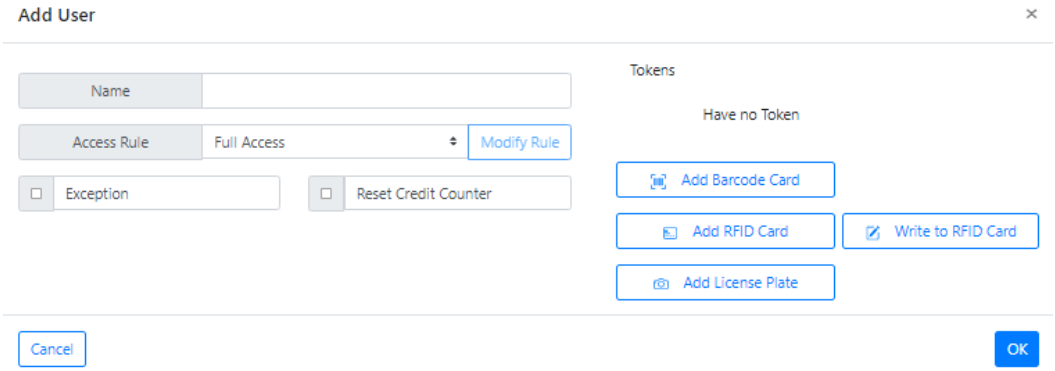
- Two **networked** controllers, two-credits identifier:
  - One IN and one OUT controller = 2x go inside and 2x go outside (**four** passages).
  - Two OUT controllers = go twice on any of the controllers (**two** passages).
- Two **standalone** controllers, two-credits identifier:
  - One IN and one OUT controller = 2x go inside and 2x go outside (**four** passages).
  - Two OUT controllers = go twice on **both** controllers (**four** passages).

3.3.11.2 Regular users

Click on Access Management > Regular users. You'll then see the following page:

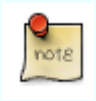


Now click on Add New User. You'll then see the following popup:



- Enter the user's name
- Select the access rule you want to apply for this person. If you wish to apply an access rule that doesn't exist yet, click on "Modify Rule" and start creating a new access rule (see chapter **3.3.11.1**).
- Click on Exception if you temporarily want to activate an alternative access rule for this regular user.
- Click on Reset Credit Counter if you want to reset the credit counter value to zero for this regular user.
- ProConfig Embedded allows to assign up to three different identifiers (also called tokens):
  - Barcode:
    - DAS barcode: Assign a specific 28-digits DAS regular-user-barcode by entering manually these 28 digits or by scanning the barcode to our USB desktop barcode enroller/scanner.
    - Third party barcode: Enroll and use non-DAS barcodes by scanning them at our USB desktop scanner or by entering manually the numerical value of the barcode here.
  - RFID: DAS by default use 13.56Mhz Mifare cards. *Contact your DAS supplier in the case you would need 125Khz.*
    - RFID card initialized by DAS: Assign an RFID card by entering manually its 28-digits -digits (printed on the card) or by scanning it to a DAS USB desktop RFID scanner.
    - RFID cards that were not initialized by DAS: Assign an RFID card by scanning it to a DAS USB desktop RFID scanner.
  - License plate: Assign a license plate number by entering it manually.
- Write to RFID card: When clicking on "Write to RFID card", ProConfig Embedded writes the access rights on the Mifare card and sends these rights to the CU5 you are connected with which in turn sends these rights to all networked controllers involved in the update. Offline controllers save these access rights to their internal database either by copying them when they scan the card or during a USB-stick-update procedure.

With Mifare cards that have not been initialized by DAS, we use the (easy to copy and therefore unsafe) UUID number as card identity. With DAS Mifare cards we use the card identity, printed on the card (and that we securely encrypted in one of the card memory sector, making this card identity thus unaccessible/unusable for others.



ProConfig Embedded allows you to activate up to three different identifiers per regular user (barcode, RFID card and license plate), but you could for instance also assign three license plates or any other combination.

Please skip spaces when manually encoding barcode numbers, RFID card numbers, or license plates.

3.3.11.3 Finding regular users by barcode card, RFID card or license plate

Go to Access Management > Regular Users:

- Click on Find User by Barcode. Manually enter the 28-digits numerical value of the DAS barcode (without spaces between the digits) or scan the barcode using our handheld scanner.
- Click on Find User by RFID Card. Manually enter the 28-digits numerical value of the DAS RFID card (without spaces between the digits) or scan that card using a desktop RFID reader.
- Click on Find User by License Plate. Manually enter the license plate number (without spaces between letters and/or numbers).

3.3.11.4 Creating a USB stick update file

Click on "Create Update Stick" to create a .users file that contains all user-related info. You can then use this file to perform an offline update procedure of the user configuration of all controllers involved, using a USB stick.

3.3.11.5 Exporting

Click on "Export to CSV" to create a .csv file that contains all user-related info.