SIEMENS
Ingenuity for life

SiPass integrated MP2.75/76

Salto integration V1.1

www.siemens.com/buildingtechnologies

SiPass integrated MP2.75/76

Salto integration V1.1

Table of contents

1. General Function

General function:

The Salto access control system will provide the possibility to handle so called "Data on Card readers" or also called "Data on Card System". Data on Card readers not wired to a controller. The access conditions is stored on the card itself and the access decision will be made by the Data on Card reader.
To provide the advantages of the offline system it is possible to connect the Salto system to SiPass integrated.

Data on Card reader advantages	Data on Card reader disadvantages
• No wiring needed • No problems with historic monuments, marble, glass, etc • No distance limitation • Quick mounting • No power connection needed, battery powered	• No door monitoring, a forced opened door will not be recognized • Access control changes will only be transferred to the access card if the card will be presented to a Salto update reader • If a card is lost or stolen it is not possible to block the card immediately. A card can only be blocked via programming unit or via the "Network on card" function, where a "black list" will be forward • Access bookings will only be known if the card will be presented to a Salto online reader

<u>Integration SiPass integrated – Salto:</u>

The Salto system connection will provide the possibility to use the advantages of offline and online readers.

The system operator can handle the access conditions for both systems via SiPass integrated.

All readers, online or offline will be handled in SiPass integrated in the same way (access rights).

Note:
Site Plan monitoring of Salto readers are not possible.

Transfer from SiPass integrated to Salto:

- Cardholder
- Access rights
- Access Groups
- Time schedules

All data transferred to Salto after saving the record. A manual download option is available too at the Salto bus configuration (Config Client / Components).

Transfer from Salto to SiPass integrated:

- Cardholder
- Reader
- Locker
- Zones (Group of Salto readers)
- Access rights (can be disabled by a config file change, please contact support)

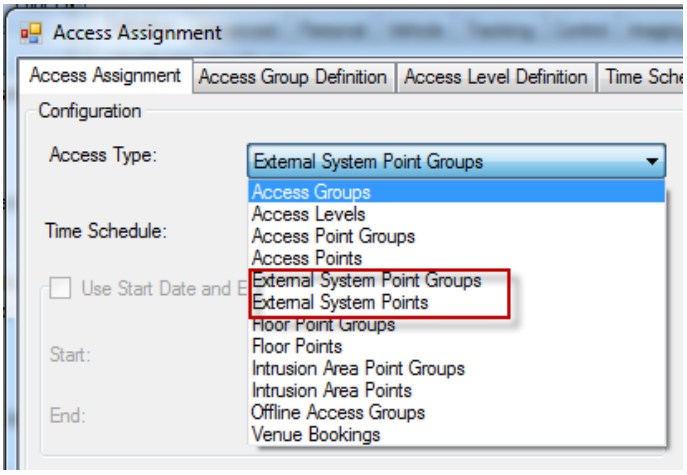
Data transfer from Salto to SiPass are not dynamic, the upload option at the Salto bus configuration have to be used. The scheduled upload function is not needed after finishing the installation.

Note:

Salto can handle up to 96 access rights per card. If more than 96 Data on Card readers are in use the readers have to be grouped to zones. A Salto zone is containing minimum one maximum all Salto readers. For further information please contact the Salto support.

The Salto zones must be transferred via PPD to each Salto Data on Card reader, see Chapter 7.3 Programmer PPD.

Inside SiPass, Salto Zones are listed as “External System Point Groups” and Salto Readers are the “External System Points”.



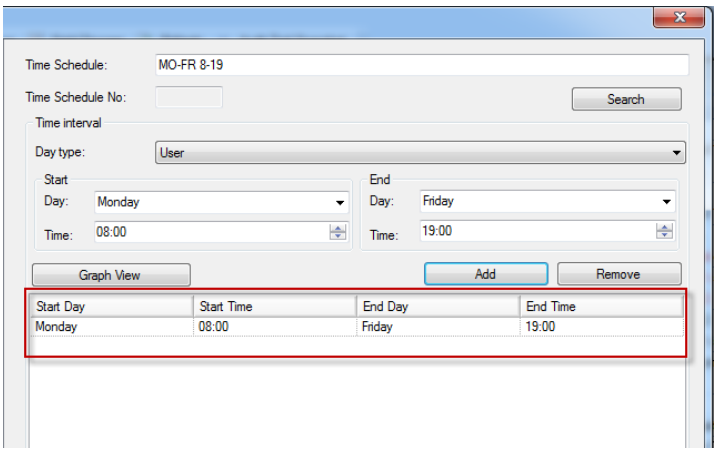
2. Salto limitations

If a Salto system is connected to SiPass some limitations must be considered.

The below items are the current known limitations, it could be further limitations that not known now or introduced by a higher Salto version that has not tested with SiPass integrated.
Please refer to the release note getting the information which Salto version is released for the corresponding SiPass integrated version.

Known Salto Limitations:

1. Salto can't handle equal cardholder names (First and Last name equal).
   Work around described at section: 5. Salto installation.
2. Time schedule names longer than 34 characters
3. Access Level names longer than 34 characters
4. Access Group names longer than 32 characters
5. Time schedules that end not at midnight like below



6. Salto readers assigned more than one time to an access group.
   This can happen if the same Salto reader is part of two or more access levels assigned to the same access group.

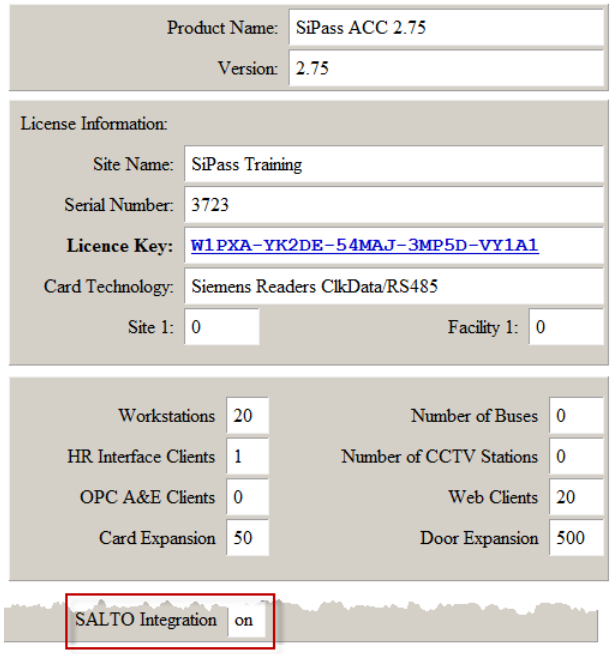
General recommendation:

Do not combine SiPass and Salto readers inside an Access Level or Access Group.
Do not combine Access Levels with different assigned Time Schedules inside one Access Group.

As long the Access Group not containing Access Levels with different time Schedules assigned Salto accept double assignment of readers.

3. SiPass / Salto license keys

Two SiPass licenses are be needed to enable the Salto function.
The SiPass integrated base license must include the “Salto Integration” and the separate Salto Bus license with door count for the offline doors.



Product Name:	SiPass ACC 2.75
Version:	2.75

License Information:

Site Name:	SiPass Training
Serial Number:	3723
Licence Key:	W1PXA-YK2DE-54MAJ-3MP5D-VY1A1
Card Technology:	Siemens Readers ClkData/RS485
Site 1:	0
Facility 1:	0

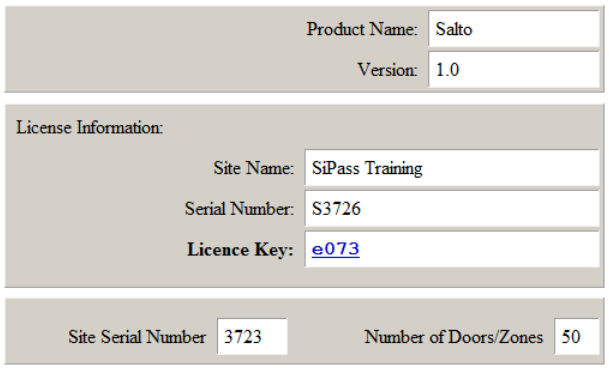
Workstations	20	Number of Buses	0
HR Interface Clients	1	Number of CCTV Stations	0
OPC A&E Clients	0	Web Clients	20
Card Expansion	50	Door Expansion	500

SALTO Integration	on

Copy and paste is faster than entering it manually:

SiPass Base License:

Site Name: **SiPass Training**
Serial Number: **3723**
License Key:
W1PXA-YK2DE-54MAJ-3MP5D-VY1A1



Product Name:	Salto
Version:	1.0

License Information:

Site Name:	SiPass Training
Serial Number:	S3726
Licence Key:	e073

Site Serial Number	3723	Number of Doors/Zones	50

Salto Bus License:

Serial: **S3726**
Validity: **e073**
Door: **50**

The SiPass integrated “Salto Bus License“ must fit to the SiPass integrated base license.
The “Salto Bus License“ has to be entered at the Config Client Components dialogue at the Salto Bus dialog.

4. Salto devices

Salto Online Reader (Wall Reader):
General the Salto system can handle online and Data on Card readers.
The online readers can write and read data from and to the card.
During the read and write procedure the reader is flashing blue.
The online reader write the cardholders access conditions for offline doors access to the card. Bookings stored on the card the will be read out and transferred to Salto by the online reader.
Minimum one online reader per system is required updating the access rights.

Salto Data on Card reader:
The Salto Data on Card readers will read the personal access conditions of the card.
If the presented card is valid the door will be opened.
Additional the personal bookings can be written on the card.
This additional function must be activated for each door.
Also the “black list” can be read from the cards and stored at the Data on Card reader.
If a black listed card will book at the Data on Card reader, the reader will write a blocking flag into the card, now the black listed card can’t be used anymore.

Portable Programming Device (PPD):

The Data on Card reader parameterization will be done with the PPD.
Therefore the PPD will be connected direct at the Data on Card reader.
The PPD will be used to define the Salto settings and to which Salto system the Data on Card reader belongs to.
Via the PPD it is also possible to read out card bookings or battery state from the Data on Card readers.
If the PPD is connected later on to the Salto system via USB, the stored offline information will be uploaded and displayed at the Salto and SiPass system.
It is also possible to transfer the "Black list" or open doors via the PPD.
If the battery is empty via the PPD the door can still be opened.

Salto encoding station: „EC90EN"
This is the dongle of the system hosting the keys.
The EC90USB can't used.

If Salto is connected to SiPass integrated the EC90EN is used as a dongle.
The cardholder access conditions will be written via SiPass Operation Client with a different enrolment reader like HID OMNIKEY 5422 connected via USB to the SiPass Op Client.

The HID OMNIKEY 5022 is a USB connected encoder and works together with SiPass integrated.
Any HID reader we list inside the corresponding release note can be used.

5. Salto installation

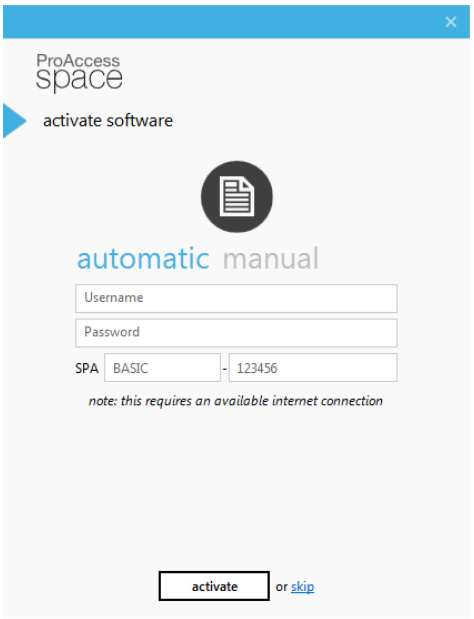
SiPass integrated installation:

First SiPass integrated has to be installed because Salto will use the same SQL database like SiPass integrated (if SiPass and Salto are located at the same PC).

Salto installation:

Please consider that the Salto application installation and configuration is explained inside this document on a base level. Please join a Salto training to be able handling Salto as needed on site. Salto related question need to be raised at your local Salto support.

Since SiPass 2.75 it is required to use the Salto Space application. The older SALTO v12.xx is since 2.70 SP1 not compatible anymore.
Salto Space requires any time a valid license entered at the end of the Salto Space setup.

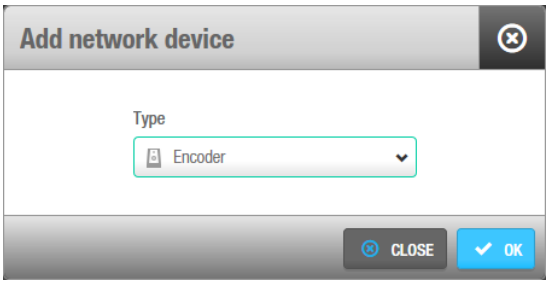


5.1 Configure the EC90EN

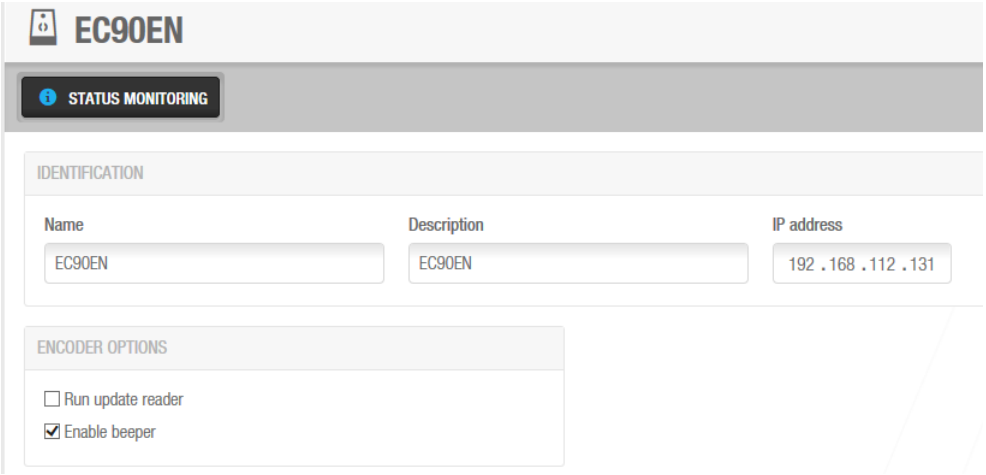
The EC90EN is used a dongle if Salto is connected via the SHIP protocol to SiPass.

SiPass send an encoding request to Salto and the EC90EN will flash and beep short (if activated). This reaction is the confirmation that the encoded card will be written with the correct Salto information.
Without the LED flash / beep the card is not successful encoded also if SiPass report back a success encoding messages.

System => SALTO Network => ADD => Encoder

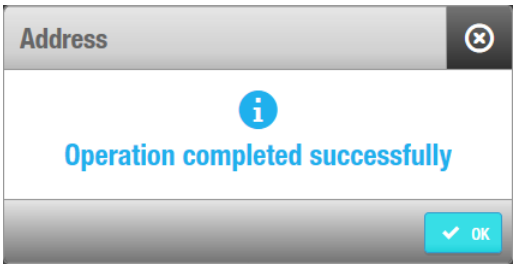


Assign a name and the IP address and save the unit, now the “Address” button will be enabled.



Press and keep the button at the back site of the EC90EN until the LED start to flash.
Press the “Address” button.

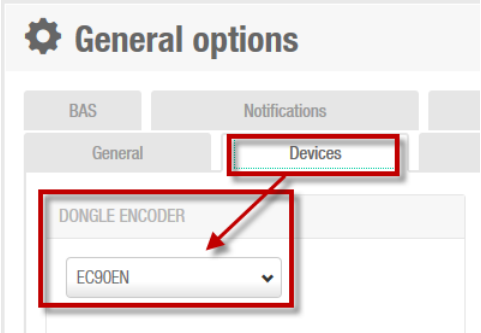
The unit is now configured.



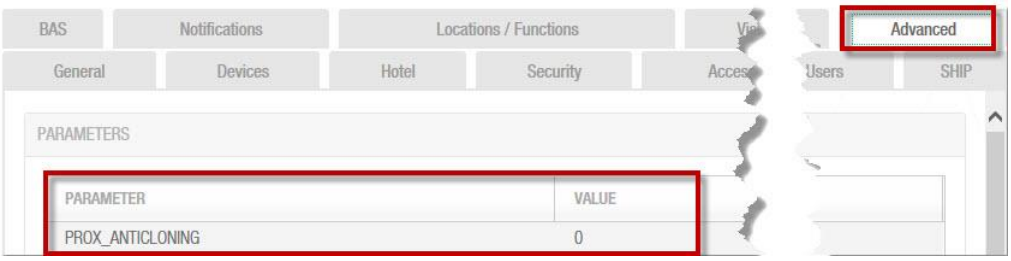
5.2 Salto connection settings

The following described settings required for the correct operation with SiPass.
Several settings need to be performed at: System => General Options

1. Assign the EC90EN as Dongle Encoder



2. Disable PROX_ANTICLONING at the “Advances” tab



Settings for Prox-anti-cloning need to be disabled
“PROX_ANTICLONING=0”

3. The value EXTID need to be added to the User ID configuration

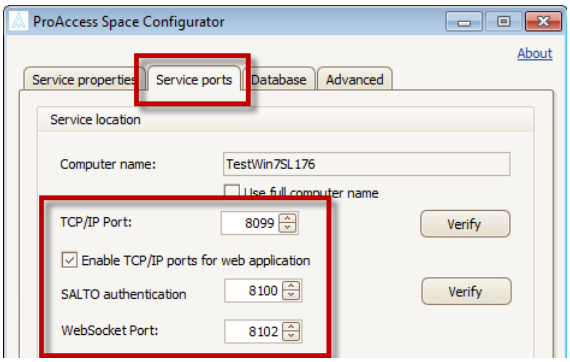
The EXTID is a unique number and offers an easy workaround for the limitation that Salto can’t handle identical cardholder names.

4. To enable the communication to SiPass integrated the SHIP protocol needs to be enabled. (SHIP = Salto Host Interface Protocol)

<u>Enable "SALTO SERVER (SHIP)" option only!</u>

A TCP/IP Port has to be defined e.g. 7878
This TCP/IP port needs to be entered into SiPass, see at section: 6. SiPass connection settings.

Note:
At the "Salto Space Configurator" tab "Service Ports" are TCP/IP ports too.
These TCP/IP ports are used to communicate between Salto service and the Salto DB.
It is required that this Service ports are **<u>different</u>** to the SHIP port value defined before!



<u>If the same ports are used the up/download between Salto and SiPass will not work!</u>

SALTO Space is now set up to be able to communicate with SiPass.

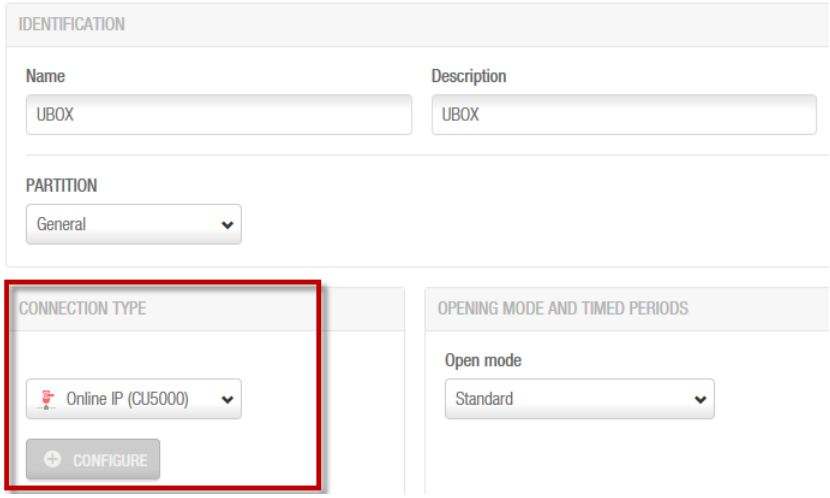
5.3 Configuration of a Salto online reader (UBOX or CUxxxx)

The online reader or UBOX will update (write) the offline access rights to the card.

It is recommended to mount the online reader(s) at the main entrance doors or at a central location, to get the offline rights written to the card without the need to visit a special reader/location. Consider the read and write process requires to present the card for longer time in front of the reader.

How to enter an online door:

Access points => ADD => enter name and select the correct connection type



Assign the IP=>Address to the online reader:

Configure Connection – enter the IP Address

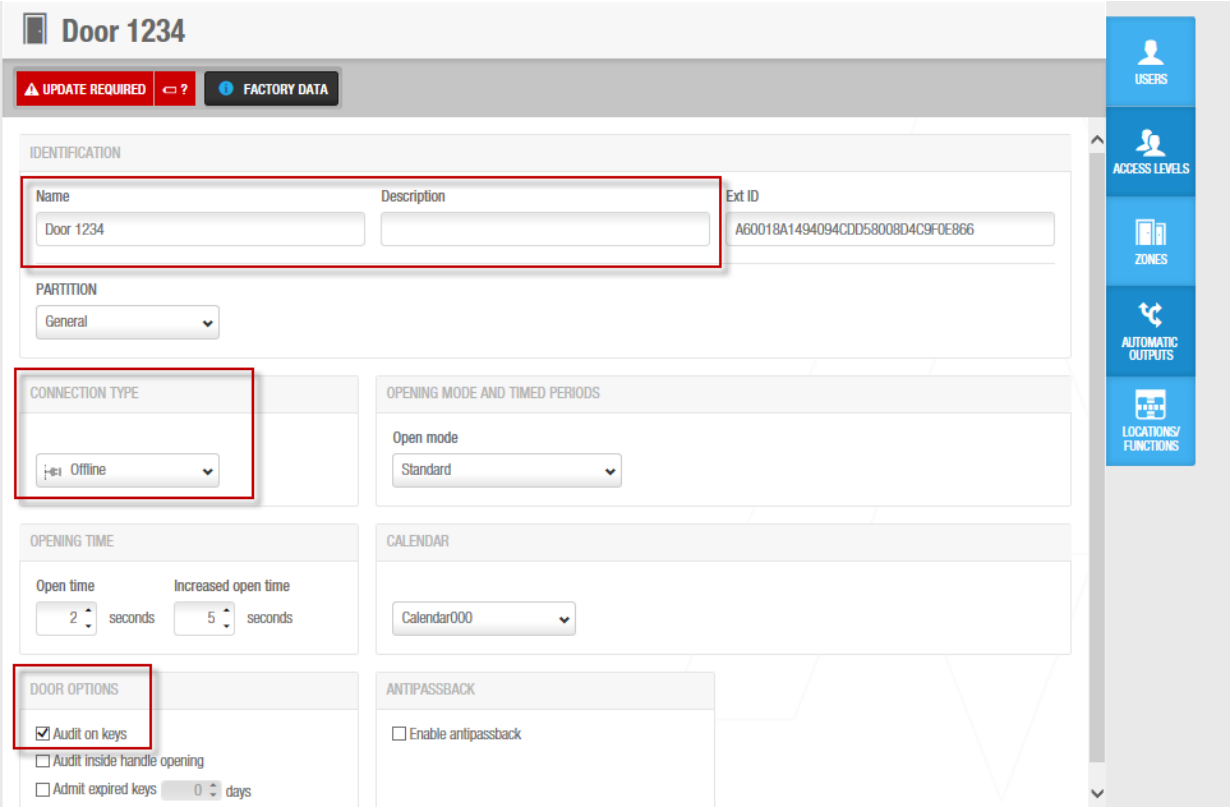
Peripherals => Monitoring of online locks => Maintenance
(only possible if the service is up and running)

5.4 Configuration of a Salto offline access point

Two kind of Salto offline access points are supported by SiPass, Doors (cylinders / door fittings) and Lockers.

<u>How to create an access point:</u>

Access points => Door/Locker => Add => Name / Description => connection type "Offline" => Save



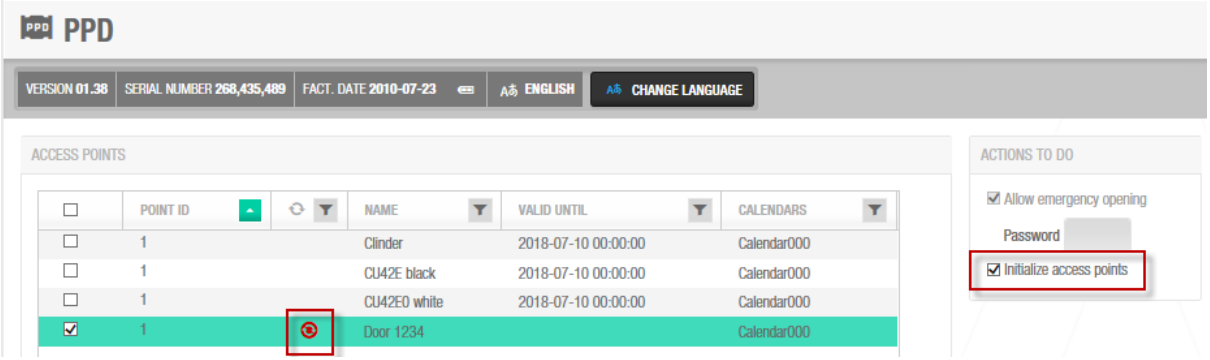
It is recommended to enable the Door Options „Audit on keys".
Please contact Salto for further support.

The "UPDATE REQUIRED" status shows that an update via PPD is needed.

5.5 Programmer PPD

Via System => PPD the new access point config need to be loaded into the PPD.

If the access point update sign will be displayed an update via PPD is required.



<u>How to download the offline access points to the PPD:</u>

- Connect the PPD via USB
- System => PPD
- Select the access points with the update sign
- Enable "initialize access points"
- Download to the PPD
- Connect the PPD to the access point

This is necessary for new access point added to Salto.

<u>Prepare the PPD to download data into the offline access point:</u>

- For new doors select in the PPD menu „Initialize door"
- Press "OK" message "CONNECT TO LOCK" must be displayed
- Connect the PPD to the Data on Card reader. (Via the special 3=>pin plug)
- The successful "Initialization" will be displayed at the PPD

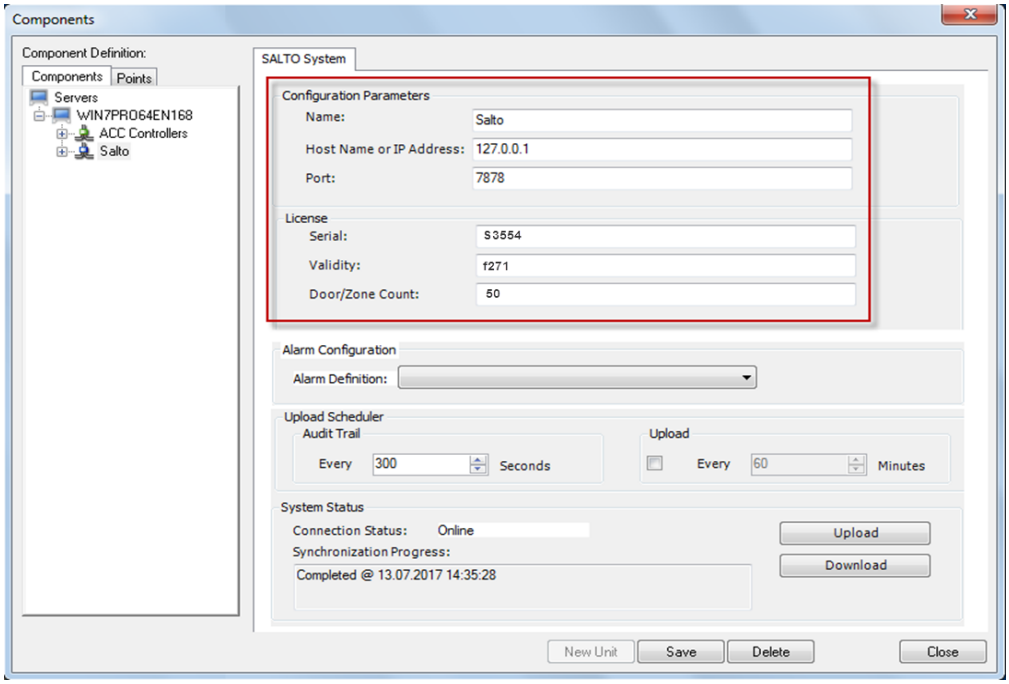
If the PPD will be connected after initialize the access point the status battery state and valid until will be transferred to Salto.

POINT ID	NAME	VALID UNTIL	CALENDARS
1	Clinder	2018-07-10 00:00:00	Calendar000
1	CU42E black	2018-07-10 00:00:00	Calendar000
1	CU42E0 white	2018-07-10 00:00:00	Calendar000
1	Door 1234	2018-07-12 00:00:00	Calendar000

6. SiPass connection settings

In SiPass Configuration Client the Salto Bus needs to be created and defined.

- System => Components => Server Name => New Bus => Salto System
- Enter a Name for the bus like “Salto”
- Enter IP Address or Name of the PC where the Salto service is up and running
- Enter the Port as defined in Salto (see 5.2. Salto connection settings)
- Enter the Salto License details (page 6) and save



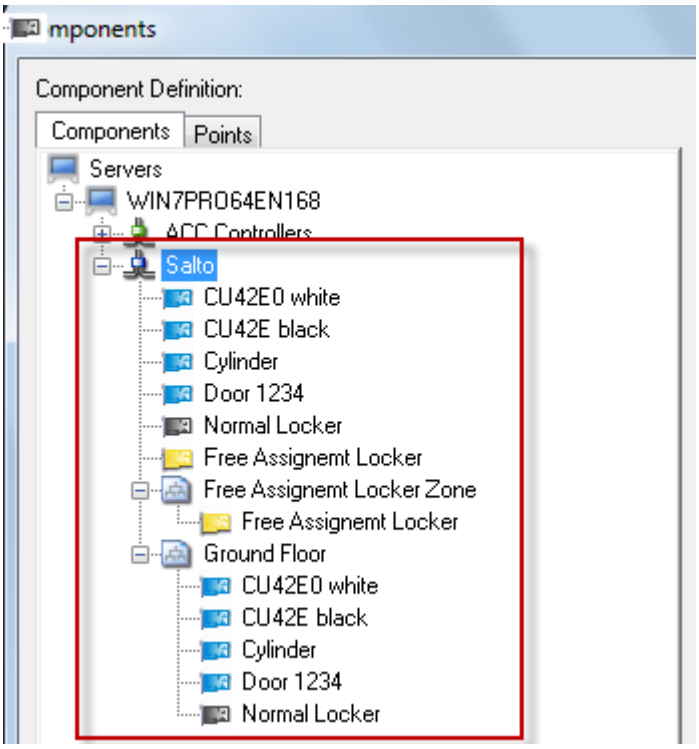
As soon SiPass is successfully connected with the Salto system the upload of the existing Hardware can be started.

The Salto Service has to be started to establish the connection to SiPass.
Upload: from Salto to SiPass integrated
Download: from SiPass integrated to Salto

Modifications inside SiPass that affect Salto parts are downloaded to Salto without a delay. Modification inside Salto, e.g. a new reader or zone, will be uploaded by following the Upload interval or if the upload button is pressed.

Note: By default the Upload interval is deactivated, activation only recommended during system setup and hardware changes. No need after hand over the system to the customer.

Recommendation: At Salto only hardware configuration should be performed. Any cardholder related modification should be done via SiPass integrated.
So a scheduled upload is not needed after hand over the system to the customer.
Customer operator only has to use SiPass as front end for both systems.
Offline doors and offline zones (group of Data on Card readers) are listed in SiPass integrated at the Salto bus.



It is not possible to configure the Salto HW under SiPass.
The only possibility is to assign an Alarm class to the Salto units.

Note: After the upload it could be necessary to close and reopen the Component dialog before the new added units are listed.

Symbol	Color	Access point type
	Blue	Door (Offline or Wall Reader)
	Grey	Locker

	Yellow	Free Assigment Locker
	White	Zone

7. Salto cards

Salto in combination SiPass integrated is compatible with Mifare Classic 1k/4k and Mifare DESFire 2k/4k/8k cards.

If Mifare Classic are used SiPass integrated will allocate minimum 10 sectors.
Default Salto encoding profile see: 7.1 Mifare Classic encoding profile.

Proximately 7 sectors used for the offline access conditions.
The additional sectors will be used to store the bookings on the card.
If 15 sectors will be used for Salto, more space is available to store the bookings.

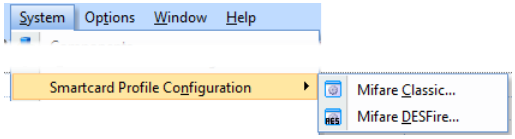
The sectors for Salto mustn't be contiguous, e.g. Sectors 1=>6 and 8=>15 can be used too.

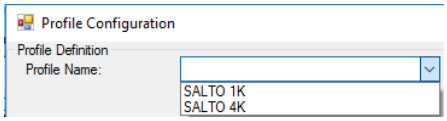
DESFire EV1 cards can be used and programmed by SiPass integrated since MP2.6.
Theses card are available in 2, 4 and 8 KB, see 7.2 Mifare DESFire encoding profile

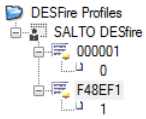
Minimum 1024 byte should be used for Salto.

7.1 Mifare Classic encoding profile UID

In the SiPass Configuration Client Smartcard Profile Configuration 3 default profiles are available for Salto card encoding. 2x Classic 1x DESFire

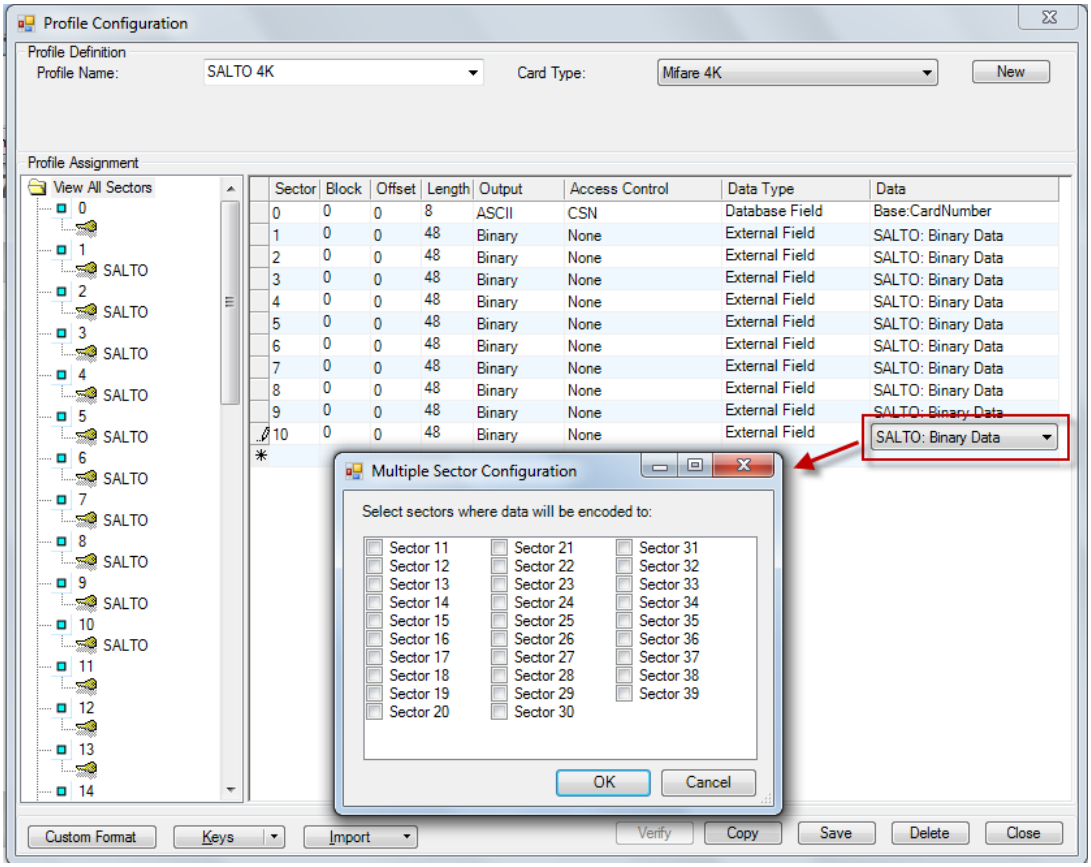






SALTO 1k and 4k profile has by default 10 sectors of the card configured for the Salto offline function.

A trick opens a small wizard and additional sectors can be activated.
To open the wizard: Data Column => reselect => “SALTO: Binary Data”
The result is the below dialogue:



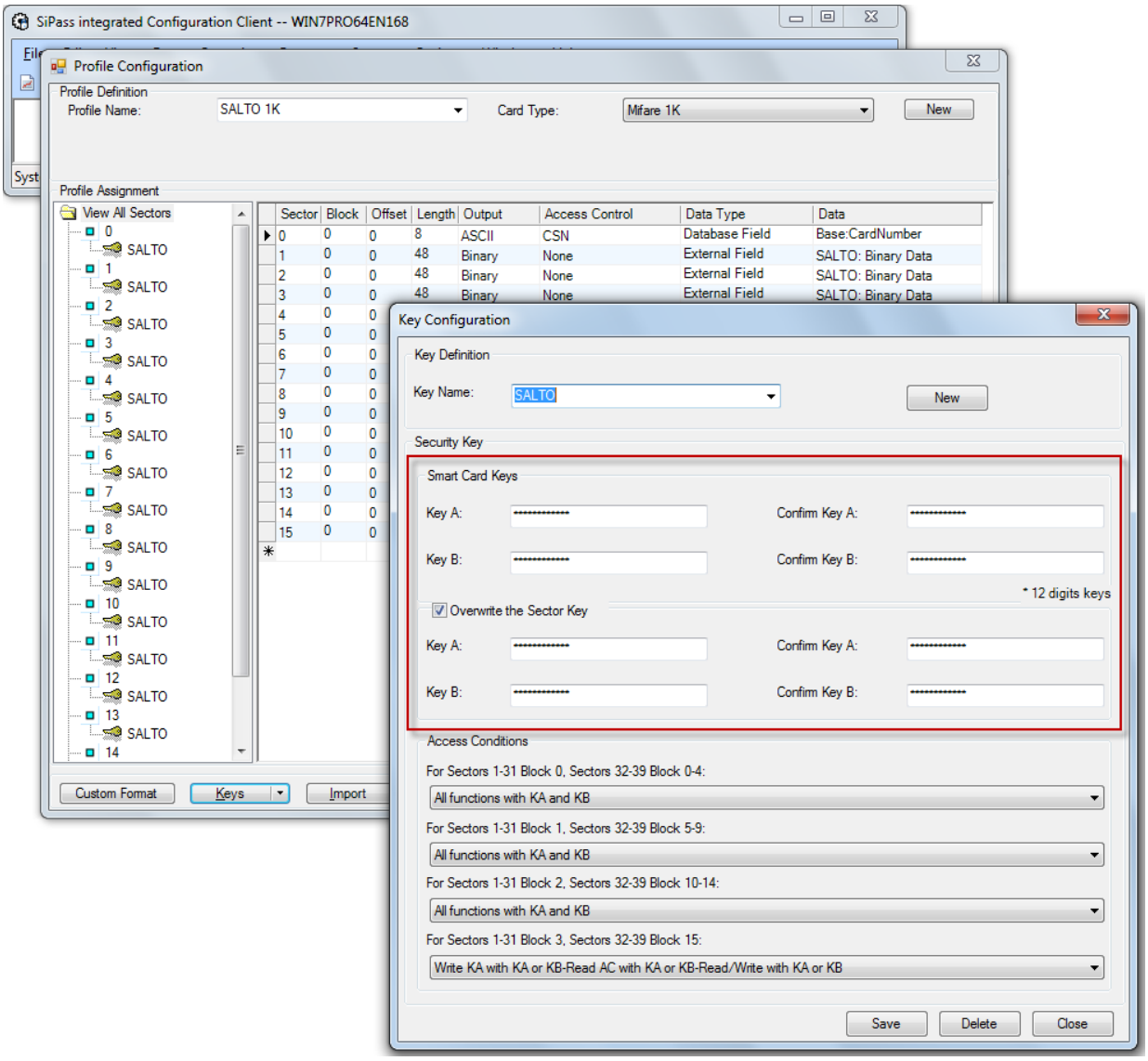
Now the additional needed sectors can be selected.

This trick can also be used if a new profile has to be created for Salto encoding.
This is necessary if the Salto option is added to the license afterwards.
No default profiles are created that can be used.

Site dependent, the Salto Mifare Keys must be entered individually.
The default listed key “Salto” is only a placeholder, the correct Mifare A and B key hast to be entered.

Each Site will get his individual Salto SAM=>Key (Mifare A and B key).
The Sector Keys the same for all Salto Mifare sectors.

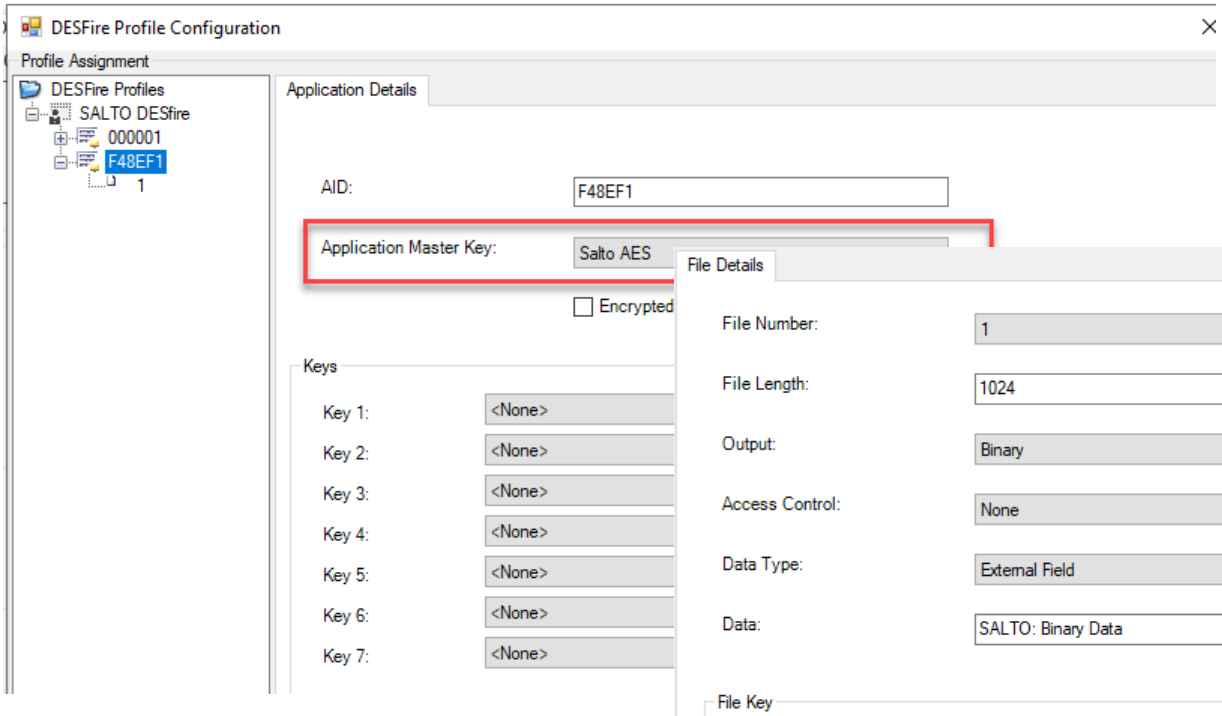
The key have to be entered into the section “Overwrite the Sector Key”.
At the “Smart Card Keys” section the transport key of the Mifare card has to be entered.
If it is new Mifare Classic card 12 times F have to be entered: FFFFFFFFFFFF

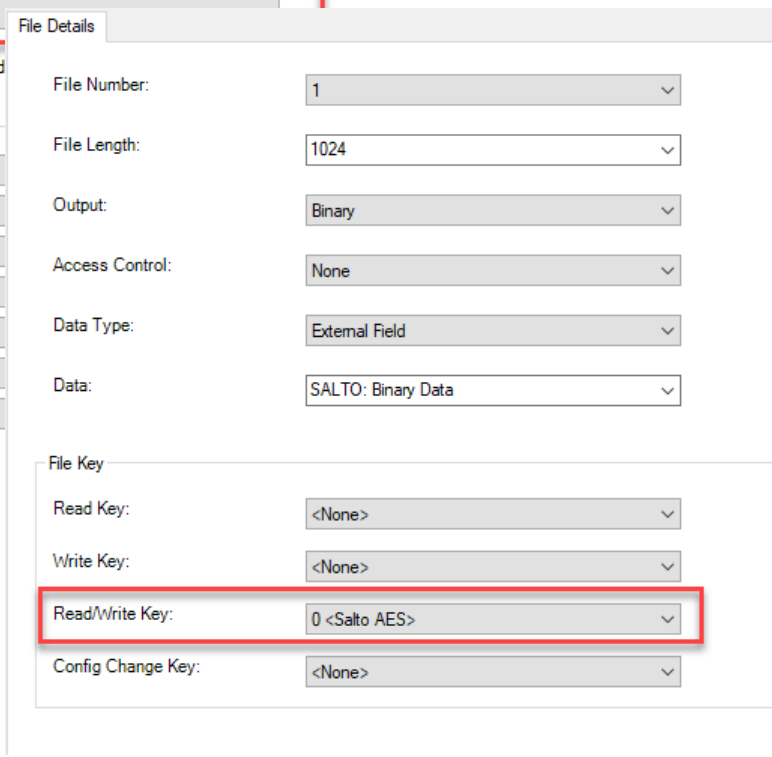


Note: We recommend not modifying the section "Access Conditions". Only for persons that have a good knowledge about the Mifare Classic possibilities.

7.2 Mifare DESFire encoding profile UID

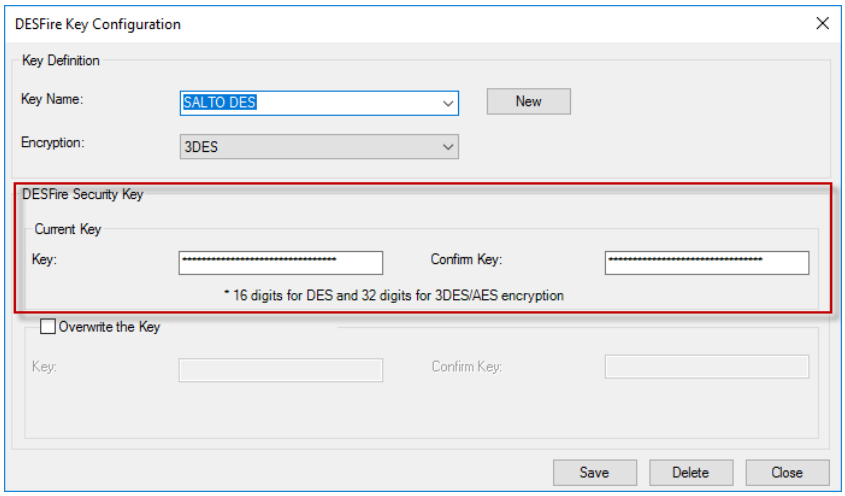
It is possible to use Mifare DESFire cards in combination with Salto too.
A default encoding profile is available also for DESFire.





If the default Salto DESFire profile is used only the DESFire
keys needs to define.

Open the default DESFire key with the name "SALTO DES" and enter the key into the section DESFire Secure Key – Current Key.



The key is delivered by Salto (SAM Key).

Salto is supporting 3DES or AES encryption, Salto is suggesting using the 3DES key because of the lower reading distance if AES is used.

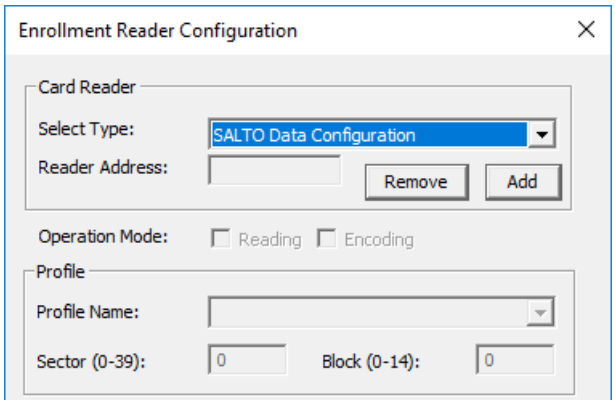
Note: Card Master Key (PICC) is the master key of a DESFire card.
The PICC is needed to create a new Application. If you only want to read an existing Application File information you do not need the PICC.

7.3 SiPass enrolment reader configuration UID

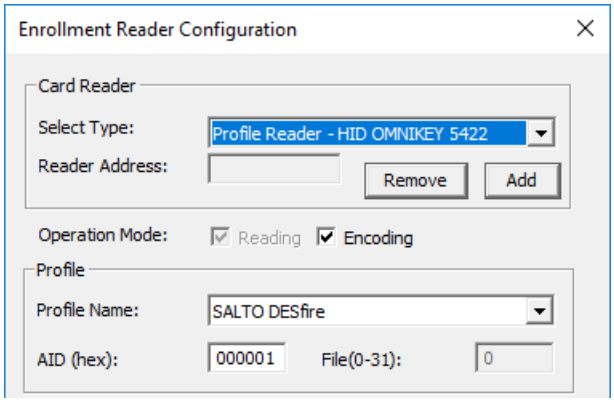
SiPass/Salto card enrolment requires 2 enrollment devices which must be defined in SiPass integrated Operation Client:

- The EC90EN encoder from Salto must be connected to the PC where the Salto Service is running.

In SiPass the EC90EN will be defined as "Salto Data Configuration".

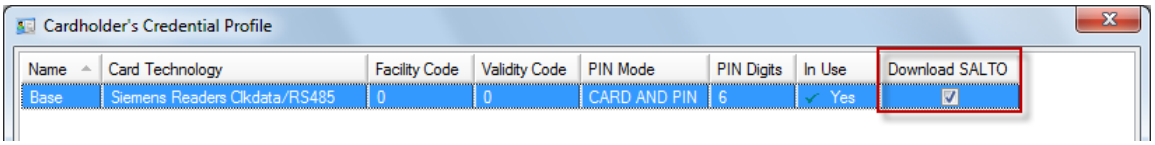


- The HID OMNIKEY 5422 is connected to a SiPass Operation Client and configured like below shown.

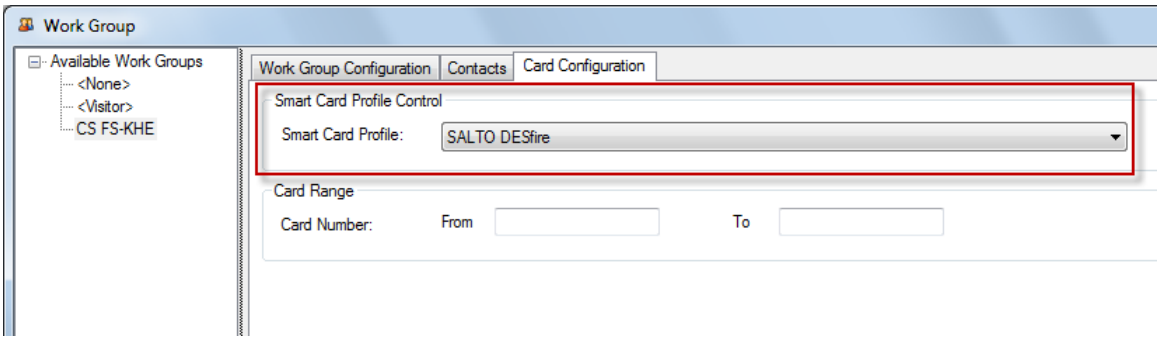


7.4 Further necessary settings for the Salto connection

The Salto download needs to be activated at the Credential Profile. All new cardholders with the dependent credential profile will get the Salto activation automatically.

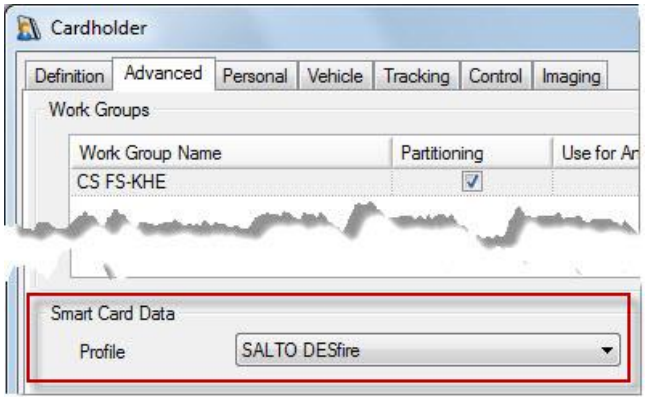


<u>Automatic Encoding => Profile assignment:</u>
Via the Workgroup dialog it is possible to assign which encoding profile will be assigned automatically and used for the cardholders which belongs to the work group.



With the above setting it is not possible to assign individual encoding profile to cardholder which belongs to the Workgroup containing a Smart Card Profile.

Cardholder "Advanced" tap:

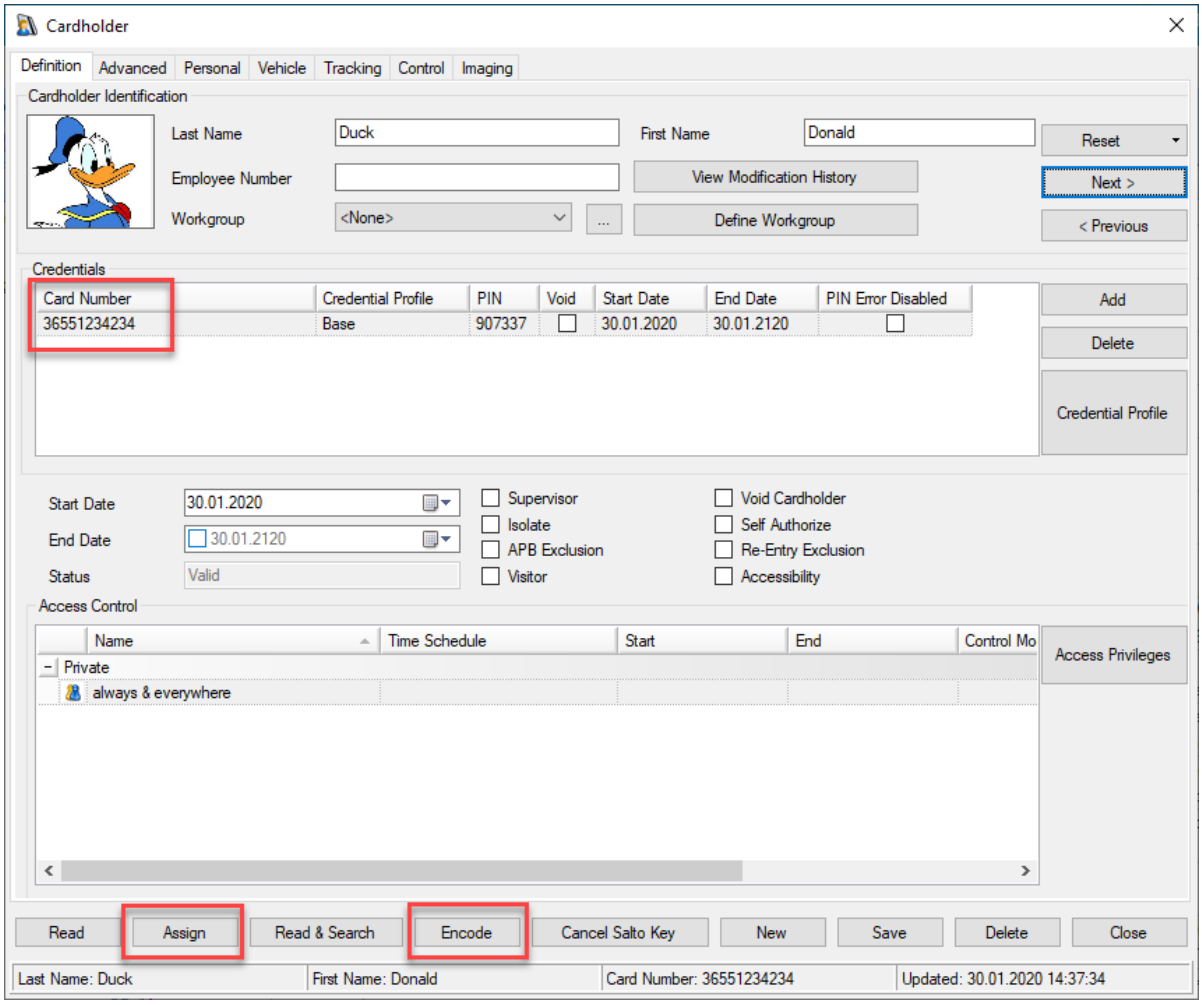


If a different Smart Card profile is needed a Work Group without above configuration need to be assigned to the cardholder.

Consider maybe access rights assigned via works group too.

7.5 Card Encoding

The cardholder dialogue offers the possibility to encode the card with the profile assigned to the particular cardholder.
Simple place the Mifare card, that should assign the Cardholder, on the enrolment reader and press “Assign”. The UID of the Mifare card will be read and insert into the Card Number field.
Next step is to encode the card, all offline (Salto) access rights that are assigned to the cardholder will be written to the card.
In the background, the cardholder will be downloaded to Salto.



Info:
If a card is encoded by SiPass, the EC90EN (connected to Salto) will feedback with a short beep (if activated) and the LED flash short. If this reaction is not occurring the encoding is not successful and the card is not valid encoded and will not work at the Salto access points.

8. Black list function for Salto cards

The Salto access rights are stored on card (Data on card), if a card is lost there is no possibility to void the card compared to a reader that connected to SiPass integrated reader interfaces.

Salto offers so called “Blacklist” functionality that using any Salto card as transport layer to transfer the card which should be blocked. Salto call this function “network on card”.

Because the validity date defined directly at the card, it is not possible to block the card immediately if the card has been stolen or lost.

Possibilities to block the card:

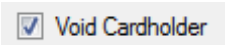
- The card number have to be overwritten in SiPass with a new card number or deleted, the old/lost card will be deleted once presented at an Salto online reader.

- Network on card – If a card is blocked Salto will create a “Black List”
  All cards (that update on the online reader) will forward the Black List to the data on card readers of Salto.
  If a Black Listed card is presented, the Data on Card readers will delete the validation of the Black Listed card.

A feedback of the card blocking will be forward to Salto by any presented card.
The “Blacklist” will be updated.

Please contact Salto for more detailed information.

Note:
If the card is voided in SiPass the corresponding card will not be added to the Salto black list and will not be deleted!

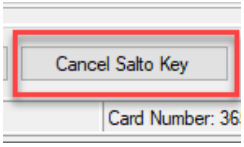
SiPass 

=> Salto 

It is recommended to overwrite the existing card number or remove the card number from the cardholder.

This step will add the old card to the Salto Blacklist.

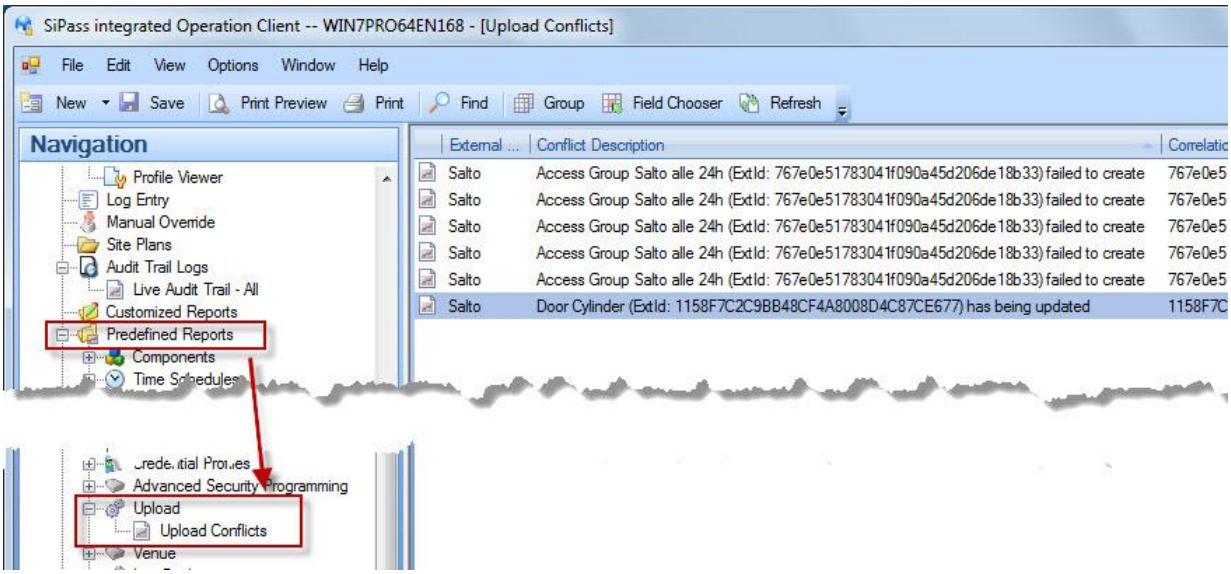
Since 2.76 the operator has the possibility to cancel the Salto Key.
This is needed because Void a cardholder inside SiPass will not add the Salto Key to the so-called Blacklist.



9. SiPass Explorer reports

The “Upload Conflicts” report shows the synchronization conflicts.

Not related to the last upload, all conflicts occurred ever listed without a time information.



10. Configuration for encoded card number

In general it is possible to use instead of the UID of the Mifare card an encoded card number like described inside the training document Mifare DESFire Facility MP2.75_EN or Mifare Classic Facility_MP2.7x_EN.

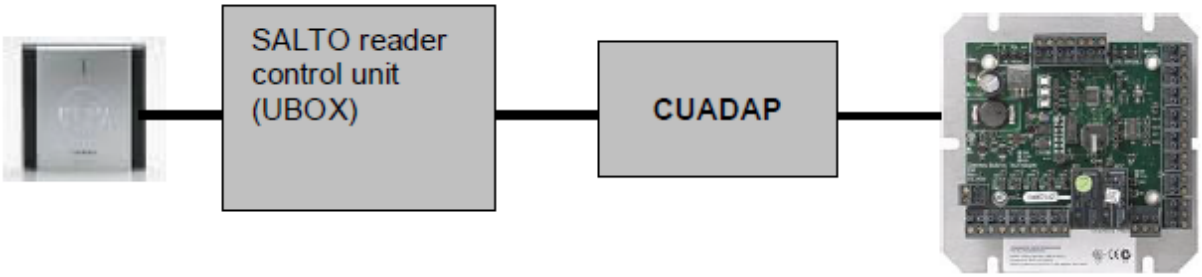
This request further configuration on Salto site and will not described here.

If you plan to combine Mifare Facility (Classic or DESFire) encoding together with Salto please contact technical support center for further information.

11. Connection Salto online reader to RIM (via CU500/UBOX)

It is possible to connect Salto online reader via CUxxxx (UBOX) to a RIM (SRI, DRI or ERI) of SiPass integrated.
This is needed if the Salto online reader should be included for Antipasback (APB) for example.

For this connection the Salto devise CUADAP is required.
Via Wiegand protocol the data will be transferred to the SiPass DRI.

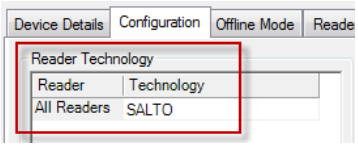


UBOX	CUADAP	RIM
EXP A	CU A // Rx/D0	D0
EXP B	CU B // Tx/D1	D1
	0V	0V
	+V	12V

The Salto reader will send the Serial Number (UID) to the SiPass RIM.

<u>The correct DIP switch setting for the CUADAP is:</u>
Mifare Classic : 11XX1101 for 34 bit Wiegand and or
Mifare DESFire : 11XX1000 for ROM 56 or 11XX1001 for ROM 58

The corresponding DRI card technology is Salto.
This reader technology is compatible with the above listed Wiegand formats.

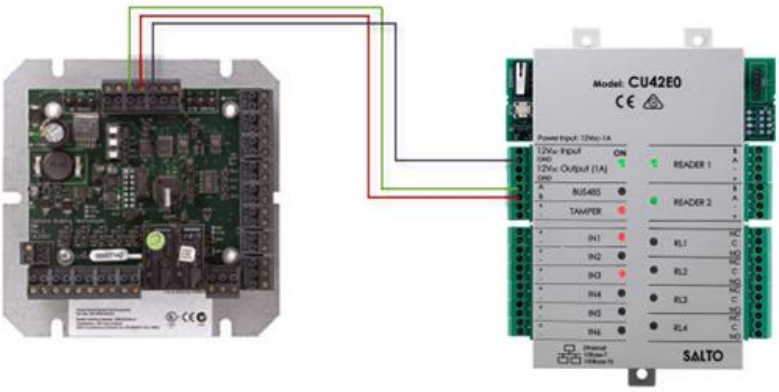


12. Connection Salto online reader to RIM (via CU42E0)

Salto introduced a new unit to the marked only compatible with Salto SPACE.
The CU42E0 is a Wall reader unit too but have the possibility to communicate with the SiPass RIM (DRI/ERI) via RS485 CerPass reader protocol.

How to setup the CU42E0 itself will not described here, please contact Salto support.

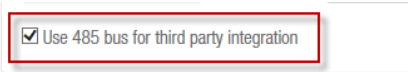
Wiring:



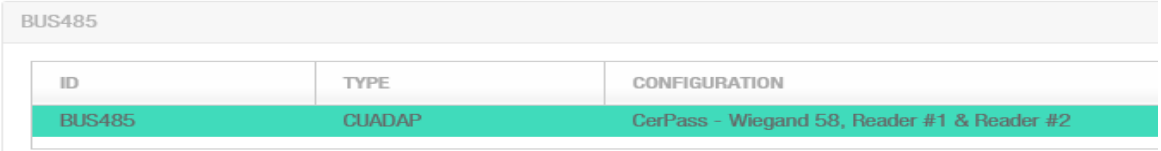
RIM		CU42E0
Rx/-	-	B (BUS485)
Tx/+	-	A (BUS485)
0V	-	GND Input

Configuration:

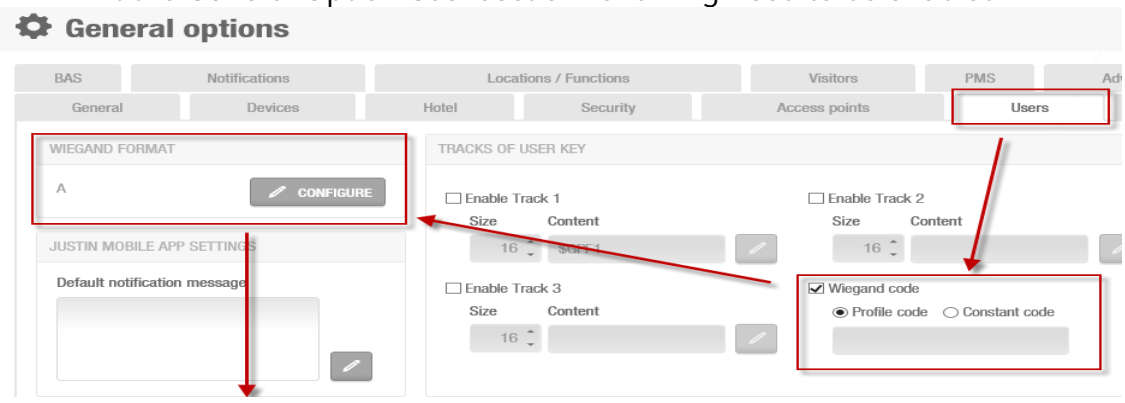
- The 485 bus communication need to be activated



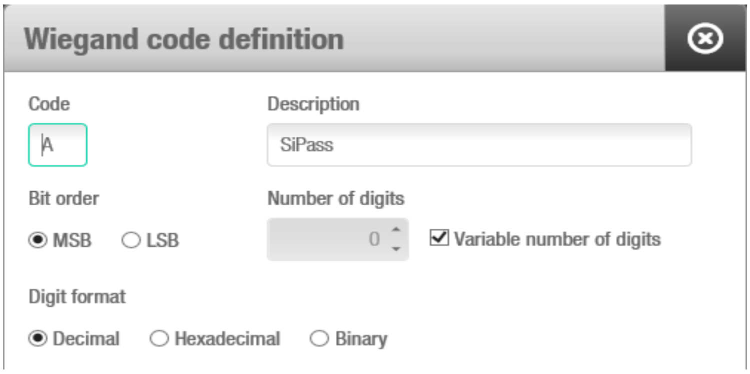
- Choose “CerPass – Wiegand 58”



- At the General Option User section following need to be enabled



- At the section User => Wiegand Format



Wiegand code definition

Code: A

Description: SiPass

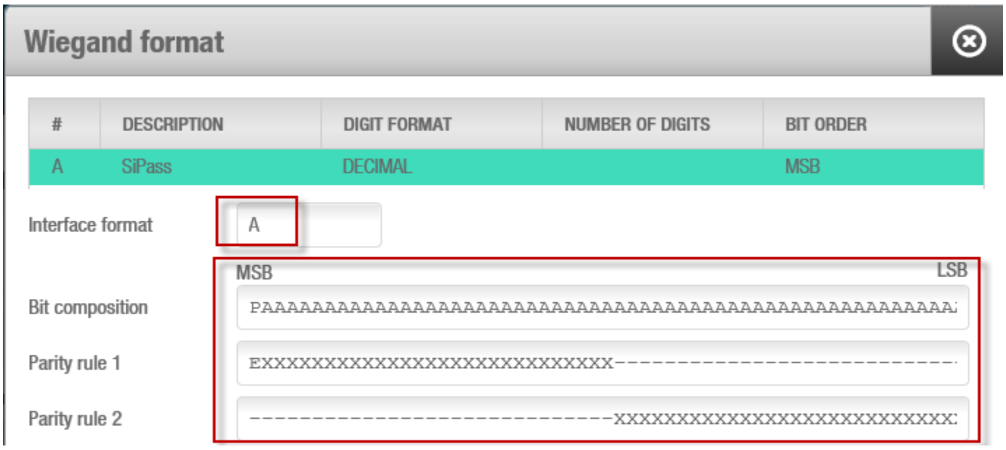
Bit order: ● MSB ○ LSB

Number of digits: 0 ☑ Variable number of digits

Digit format: ● Decimal ○ Hexadecimal ○ Binary

- Copy past the below string to the corresponding fields

  PAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
  AP
  EXXXXXXXXXXXXXXXXXXXXXXXXXXXX-----------------------------
  -----------------------------XXXXXXXXXXXXXXXXXXXXXXXXXXXXO



Wiegand format

#	DESCRIPTION	DIGIT FORMAT	NUMBER OF DIGITS	BIT ORDER
A	SiPass	DECIMAL		MSB

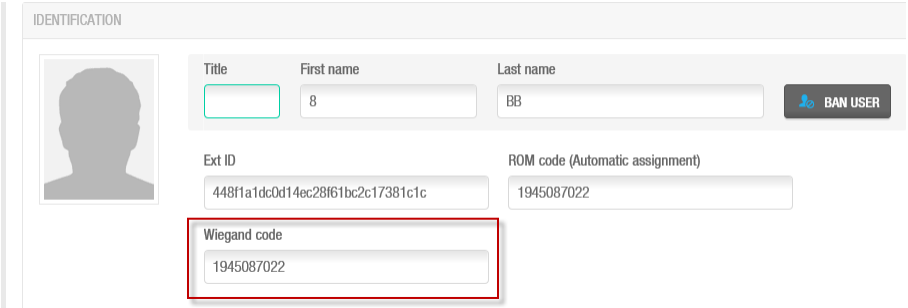
Interface format: A

Bit composition: PAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Parity rule 1: EXXXXXXXXXXXXXXXXXXXXXXXXXXXX---------------------------

Parity rule 2: -----------------------------XXXXXXXXXXXXXXXXXXXXXXXXXXX

- Any cardholder transferred from SiPass to Salto SPACE get the card number transferred to the SPACE DB Field *Wiegand code*.



If a card is presented to a Salto reader connected to the CU42E0, the Wiegand number is transferred via the RS485 connection to the SiPass RIM.

13. Automatic key assignment (UID)

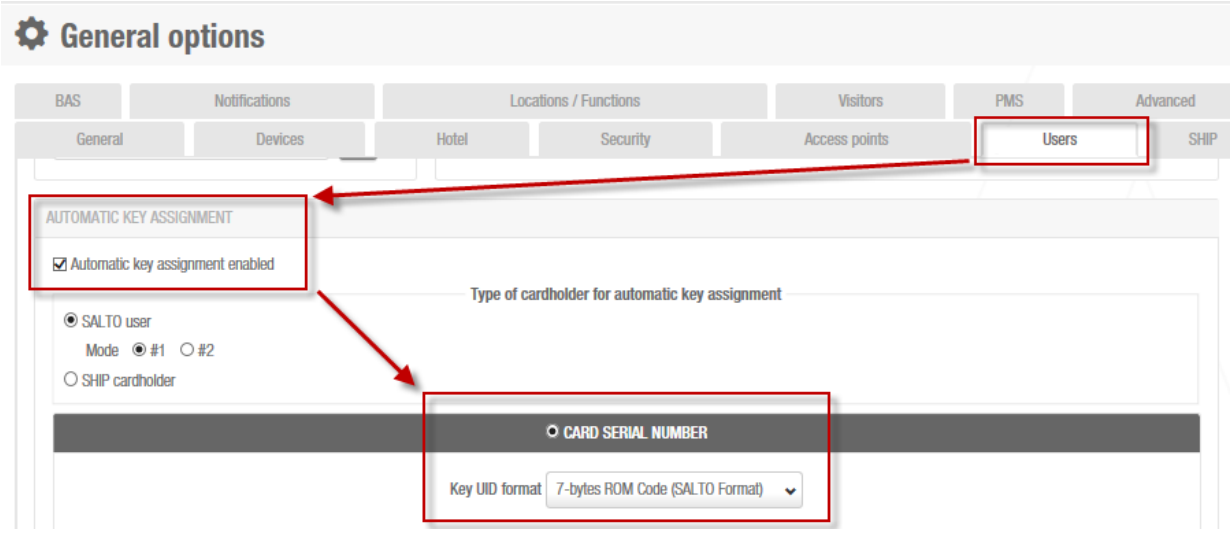
Salto is offering a function called “automatic card assignment”.
It is not necessary to encode the card with help of an enrolment reader connected to a SiPass Client.
This function could be helpful if e.g. the Web Client of SiPass integrated is used to create new cardholder.
The UID of the assigned card will be transferred to Salto together with the cardholder details and the assigned Salto access rights.

If the particular Mifare card is shown on any Salto online reader the card will be encoded and is working.

This function must be enabled/configured at Salto.

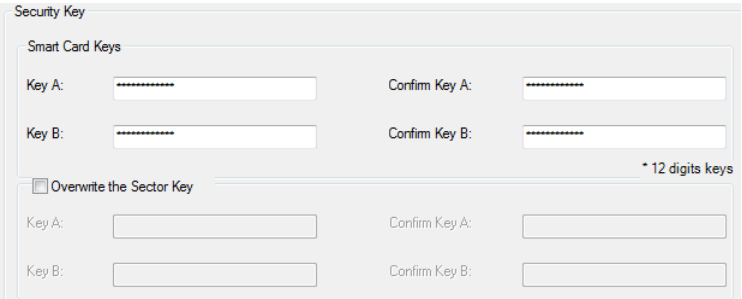
<u>The dialogs below will be found in:</u>
System => General Options => User

The “7-byte ROM Code (Salto Format)” hast to be selected.



Note:
Cards encoded this way <u>can’t be re-encoded via SiPass</u> if the before described encoding profile used.

The Mifare key of the site need to be entered to the Smart Card Key section and no Overwrite the Sector Key enabled.

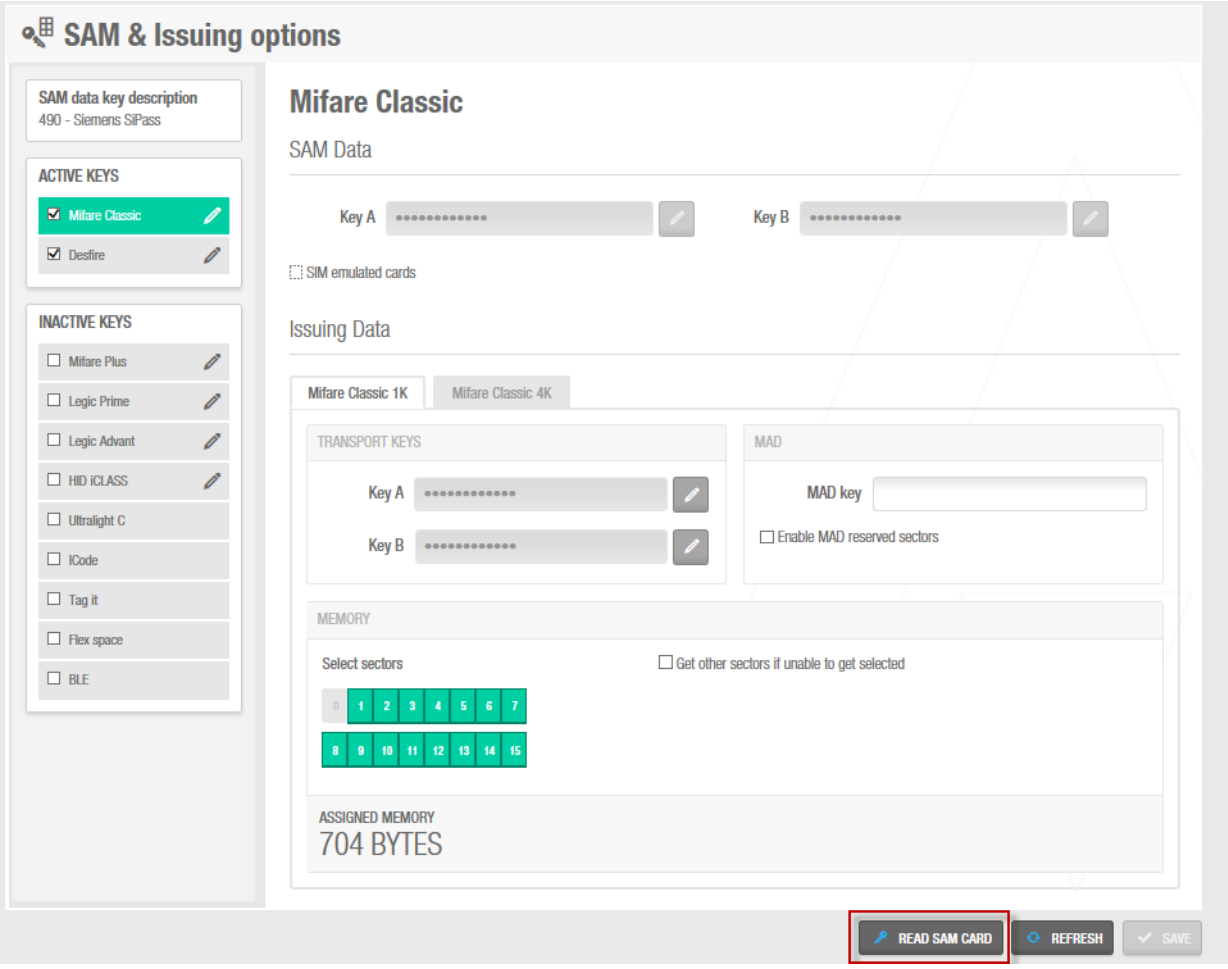


SAM and issuing data:

It is requested to assign the SAM card to the Salto system.

System => SAM & Issuing options

Place the SAM card at the EC90EN and read SAM card, the result should look like the below example.



Last step is to define the numbers of Sectors that should be used for Mifare 1k, 4, and DESFire.

Contact Salto support for further information if required.

14. Salto Wireless RF Doors

In general the Wireless RF Doors function of Salto can be used in combination with SiPass.

The only function participating of the RF function is the events of the Data on Card readers are reported to SiPass faster.

No need to present the card to an update reader reading the movement of the cardholder.

Further function, supported by Salto, like control a Salto access point are not implemented into SiPass.

Salto Space need to be operated additional.
So the benefit of one user interface for SiPass and Salto is not longer present.

Please contact Salto if you do not have the knowledge how to setup the RF function and which HW are required additional.