Version 4

Integrating with the Salto SALLIS RF lock system

Document created with reference to Controller firmware V2.5.0.16523

Inner Range Pty Ltd
ABN 26 007 103 933

1 Millennium Court, Knoxfield, Victoria 3180, Australia
PO Box 9292, Scoresby, Victoria 3179, Australia
Telephone: +61 3 9780 4300 Facsimile: +61 3 9753 3499
Email: enquiries@innerrange.com Web: www.innerrange.com

The Salto System

The Salto SALLIS system is a wireless RF locking system that connects to an Access Control System which they call the Host.

The wireless communications are managed by a Salto device, named the Router, which controls one or more Nodes through a 4-wire bus that includes the power supply. Each Node can communicate with one or more Salto wireless locks.

The Host communicates with the Router through an RS485 or Ethernet link depending on the Router device.

The wireless locks are an All-In-One unit that includes a reader, lock and handles. The wireless locks read from the cards the same data that is used by other "standard" readers from the Host. When the Salto interface is online, the decision to grant access is made by the Host. The card data that is sent from the Router to the Host is the card's Unique ID. There are two types of Salto SALLIS locks that are supported at this time; the Mifare lock and the Prox lock.

From a Mifare lock, the card's Unique ID can be made up from the card's IDCode (also known as the CSN or UID) and or an AcCode (Access Code) that is in an encrypted Sector of the card (encrypted sectors are not yet supported with Integriti). These wireless locks are compatible with Mifare Classic, Mifare Plus, Desfire & Desfire EV1 cards.

From a Prox lock, the card's Unique ID is made up from the card data. The data that is sent from the Router to the Host is the card data length and the card data (E.g. Wiegand Raw `(26) = 1A00000000000000033C1EB5`). Cards that have a card data length of up to 37 bits have been used.

Salto Installation

The Salto 485 Router is connected to the Host through 4 wires:

- 2 wires A and B for RS485 communication
- 2 wires for power supply

The Nodes are connected to the Router through a second bus of 4 wires. The distance between the Router and the last Node can be up to 1200 meters according to the wire chosen and the number of Nodes attached to the bus.

The Router and the Nodes are powered by 12 VDC from the Host. Up to 24 VDC can be used without problems. The Router has a current consumption of 75 mA and the current consumption of each Node is 45 mA.

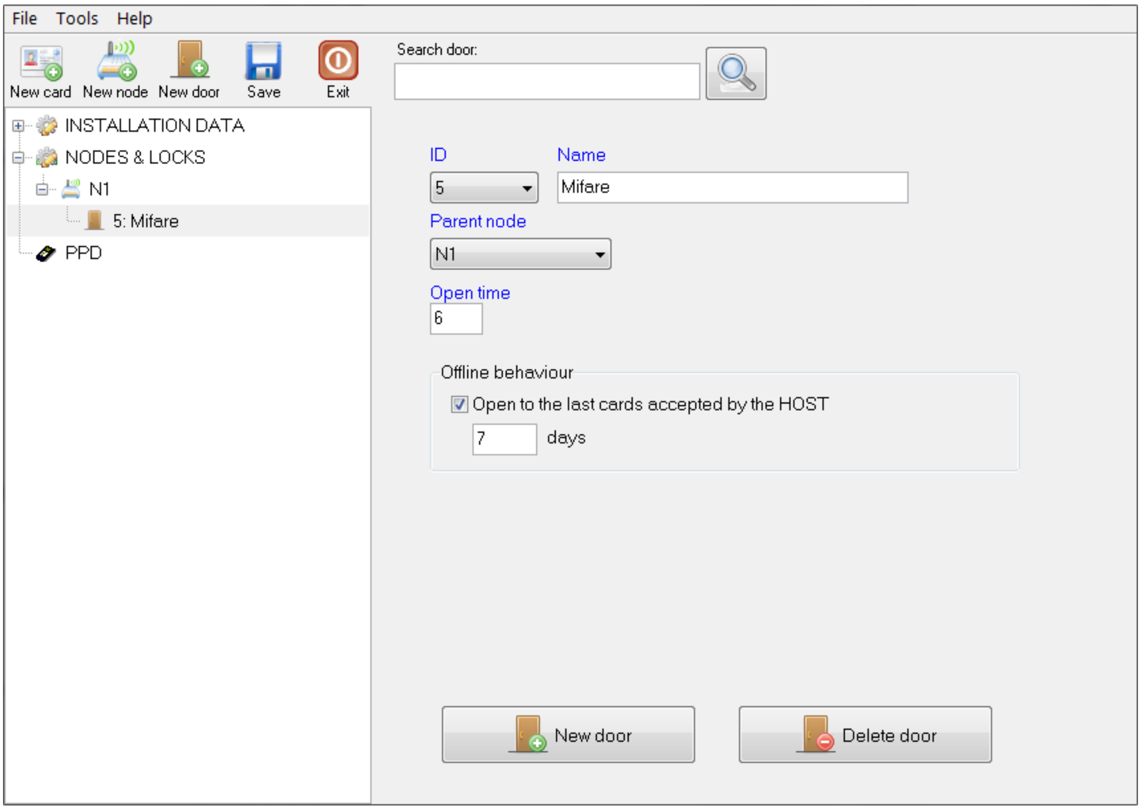
The maximum number of locks controlled by the Salto 485 Router is 16. The maximum distance between the wireless lock and a Node is 10 meters.

Salto Setup

The Salto system is configured using a SALLIS Setup Tool which is a Windows program and a Portable Programmer Device (PPD). The setup process is:

- In the SALLIS program define:
  - The list of Nodes with their MAC address.
  - The list of locks with their description and the Node assigned to it.
  - The radio parameters.
  - The card parameters.
  - The lock parameters (some of these parameters are also configured by the Host).
- Download the data to the PPD.
- Initialise the Router and the locks with the PPD.

The PPD is also a diagnosis tool and a way to open the lock in case of a battery failure.



ID: 5

Name: Mifare

Parent node: N1

Open time: 6

Offline behaviour

☑ Open to the last cards accepted by the HOST

7 days

Figure 1: SALLIS program used to configure the Salto Router and Salto Locks

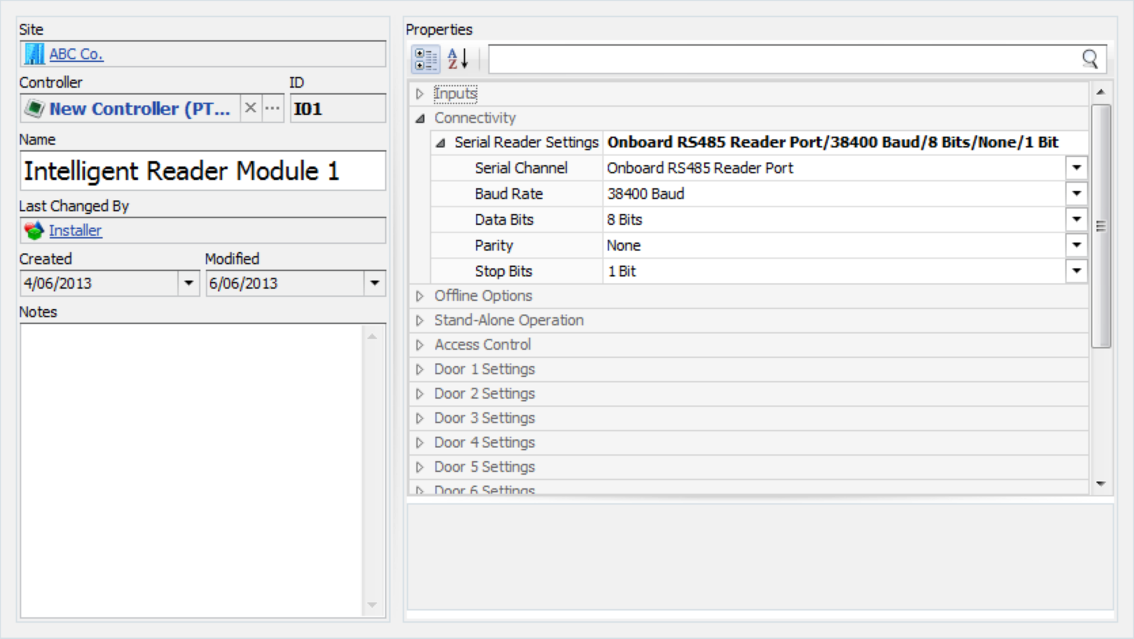
Interface between Integriti and Salto Router

As mentioned above there are two types of the Salto Router, the RS485 version and the Ethernet version. Currently the Integriti Controller only interfaces with the RS485 Salto Router. This implies that the Integriti Controller needs a physical interface to communicate with the Salto Router. The Integriti Controller has many UART ports available for connection to external devices.

The development of the Salto interface was performed using an Integriti Security Controller (ISC) connected to the Integriti Salto SALLIS 8 Door Interface which have on-board RS485 ports. The Salto interface has also been exercised with a Unibus UART using its on-board RS485 ports.

Regardless of the physical interface used, the port configuration should always be as per Figure 2 below.

While the Integriti Salto SALLIS 8 Door Interface appears as an intelligent Reader Module, please note that there are a number of options (Input, Offline Options, Stand-Alone Operation, Access Control, Door X Settings) that are not used at all in this mode of operation.



Site	ABC Co.
Controller	New Controller (PT...
ID	I01
Name	Intelligent Reader Module 1
Last Changed By	Installer
Created	4/06/2013
Modified	6/06/2013
Notes	

Properties

Inputs	
Connectivity	
Serial Reader Settings	**Onboard RS485 Reader Port/38400 Baud/8 Bits/None/1 Bit**
Serial Channel	Onboard RS485 Reader Port
Baud Rate	38400 Baud
Data Bits	8 Bits
Parity	None
Stop Bits	1 Bit
Offline Options	
Stand-Alone Operation	
Access Control	
Door 1 Settings	
Door 2 Settings	
Door 3 Settings	
Door 4 Settings	
Door 5 Settings	
Door 6 Settings	

Figure 2: Port configuration to communicate with the Salto Router

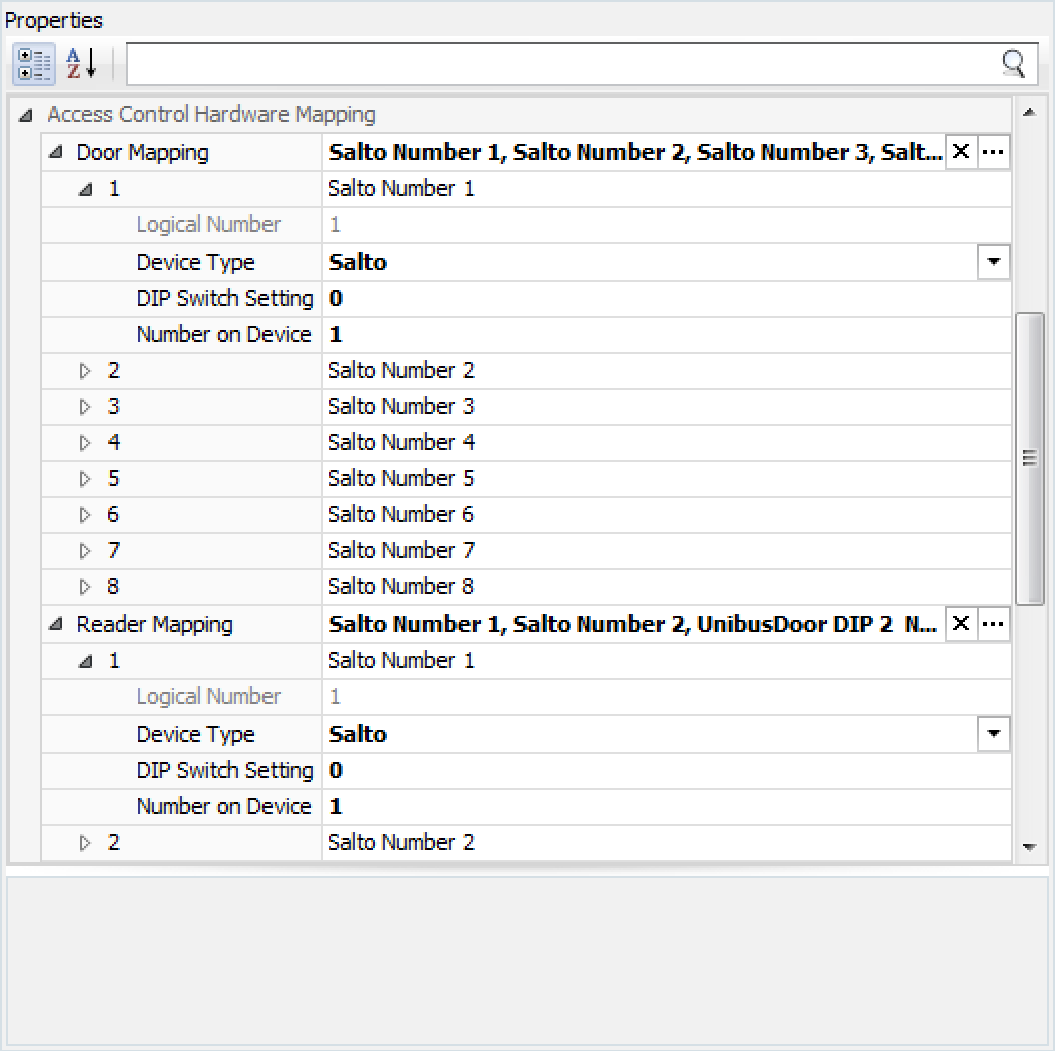
Integriti Door Mapping and Reader Mapping

For the Integriti system to know which Salto lock is associated with which logical door on the Integriti module, the Door Mapping and Reader Mapping must be configured appropriately. The Door/Reader Mapping is a flexible interface that allows any physical hardware to be associated with any logical door/reader of the Integriti module. Because a Salto lock is an All-In-One unit where the lock hardware and reader hardware are physically the same thing, when configuring the Door/Reader Mapping for the Integriti module both the door number and reader number should be configured the same. An example of this is shown below in Figure 3.

When configuring the Door/Reader Mapping of and Integriti module for Salto lock hardware, the following settings should be applied:

1. The Device Type should be set to "`Salto`"
2. The DIP Switch value should be set to "`0`"
3. The Number on Device value should be set to the Salto Lock ID (as configured in the SALLIS software)

NOTE: An example of these settings is shown below in Figure 3.



Properties

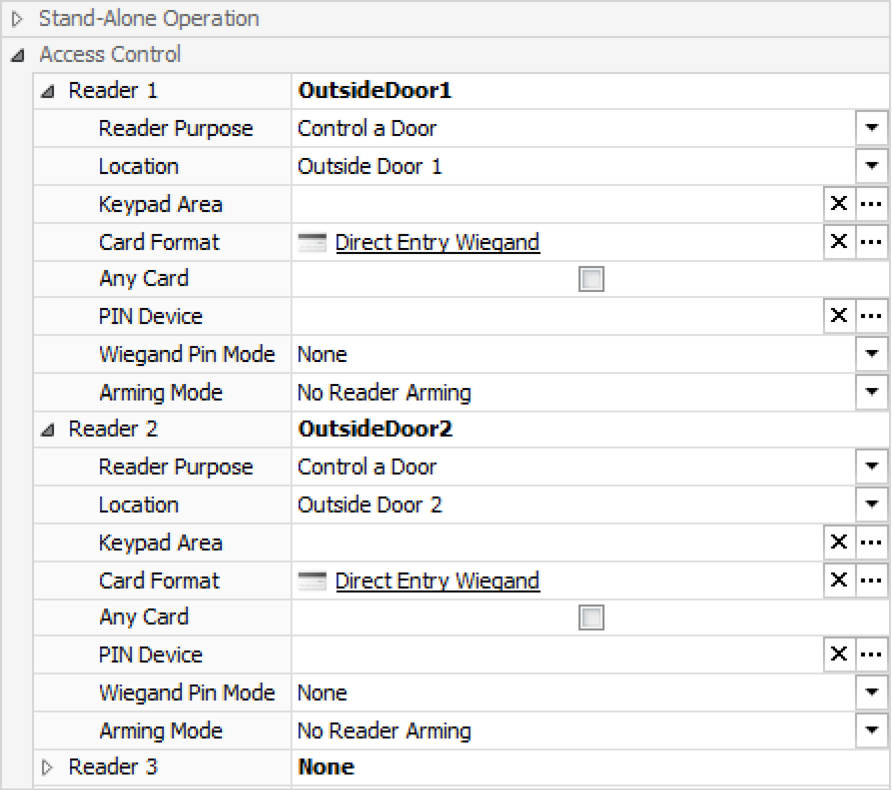
◢ Access Control Hardware Mapping	
◢ Door Mapping	**Salto Number 1, Salto Number 2, Salto Number 3, Salt...**
◢ 1	Salto Number 1
Logical Number	1
Device Type	**Salto**
DIP Switch Setting	**0**
Number on Device	**1**
▷ 2	Salto Number 2
▷ 3	Salto Number 3
▷ 4	Salto Number 4
▷ 5	Salto Number 5
▷ 6	Salto Number 6
▷ 7	Salto Number 7
▷ 8	Salto Number 8
◢ Reader Mapping	**Salto Number 1, Salto Number 2, UnibusDoor DIP 2 N...**
◢ 1	Salto Number 1
Logical Number	1
Device Type	**Salto**
DIP Switch Setting	**0**
Number on Device	**1**
▷ 2	Salto Number 2

Figure 3: Detailed Door and Reader mapping for the Integriti modules

Configuring the reader module for access control

Each individual reader that has been mapped to a Salto Router will require changes to the access control records.

The 'Location' and 'Card Format' options for a typical installation should be set as per Figure 4 below.



▷ Stand-Alone Operation	
◢ Access Control	
◢ Reader 1	**OutsideDoor1**
Reader Purpose	Control a Door
Location	Outside Door 1
Keypad Area	
Card Format	Direct Entry Wiegand
Any Card	□
PIN Device	
Wiegand Pin Mode	None
Arming Mode	No Reader Arming
◢ Reader 2	**OutsideDoor2**
Reader Purpose	Control a Door
Location	Outside Door 2
Keypad Area	
Card Format	Direct Entry Wiegand
Any Card	□
PIN Device	
Wiegand Pin Mode	None
Arming Mode	No Reader Arming
▷ Reader 3	**None**

Figure 4: Reader module Access Control configuration

Once configured, doors can be put in and out of free access ('office mode') simply by locking and unlocking the door entity. Door actions take roughly 4-8 seconds to execute. The time will vary greatly depending on a number of environmental conditions.

There is only one setting for managing card caching. This option is found in the controller programming under 'Module Details' > 'General Behaviour' > 'Salto Cache Duration'. The value determines the number of days that card caching should be stored for. Card caching is managed by the Salto reader. If a valid card has been presented to a reader prior to communications going offline, the card will be given access if the last access event was within the specified 'Salto Cache Duration'.

Access control events

Access control events such as door forced and DOTL can be utilised by mapping the associated door module system inputs as required.

The only reported door states are DOTL and Forced.

The following table lists the available system inputs.

System Input	Name	Alarm state	Sealed state
I*xx*:S13	I*xx* Door1 Fault	Lock has generated a low battery alarm.	Lock battery is OK.
I*xx*:S14	I*xx* Door2 Fault		
I*xx*:S15	I*xx* Door3 Fault		
I*xx*:S16	I*xx* Door4 Fault		
I*xx*:S17	I*xx* Door5 Fault		
I*xx*:S18	I*xx* Door6 Fault		
I*xx*:S19	I*xx* Door7 Fault		
I*xx*:S20	I*xx* Door8 Fault		
I*xx*:S21	I*xx* Door1 Forced	Lock has generated an intrusion alarm.	Lock is closed.
I*xx*:S22	I*xx* Door2 Forced		
I*xx*:S23	I*xx* Door3 Forced		
I*xx*:S24	I*xx* Door4 Forced		
I*xx*:S25	I*xx* Door5 Forced		
I*xx*:S26	I*xx* Door6 Forced		
I*xx*:S27	I*xx* Door7 Forced		
I*xx*:S28	I*xx* Door8 Forced		

System Input	Name	Alarm state	Sealed state
I*xx*:S29	I*xx* Door1 DOTL	Salto door is left open for 1 minute.	Lock is closed.
I*xx*:S30	I*xx* Door2 DOTL		
I*xx*:S31	I*xx* Door3 DOTL		
I*xx*:S32	I*xx* Door4 DOTL		
I*xx*:S33	I*xx* Door5 DOTL		
I*xx*:S34	I*xx* Door6 DOTL		
I*xx*:S35	I*xx* Door7 DOTL		
I*xx*:S36	I*xx* Door8 DOTL		
I*xx*:S69	I*xx* Rdr1 Fault	Salto router loses communication with the Salto lock.	Communications are restored.
I*xx*:S70	I*xx* Rdr2 Fault		
I*xx*:S71	I*xx* Rdr3 Fault		
I*xx*:S72	I*xx* Rdr4 Fault		
I*xx*:S73	I*xx* Rdr5 Fault		
I*xx*:S74	I*xx* Rdr6 Fault		
I*xx*:S75	I*xx* Rdr7 Fault		
I*xx*:S76	I*xx* Rdr8 Fault		

Features of the Integriti integration with the Salto system

The configuration of each lock is setup by the Host during the initial communications with the Salto Router. Additionally, when the Integriti door programming is changed the lock's new configuration is sent to the Salto Router. The Salto Router is responsible for sending the lock configuration wirelessly to the Salto lock.

When using the Integriti Salto SALLIS 8 Door Interface a subset of the Salto events are sent via the Integriti LAN to the Integriti Controller to generate review.

The date and time in the Salto system is configured when the communication with the Salto Router is first established. The Integriti Salto SALLIS 8 Door Interface periodically updates the Salto Router with the current time.

When something happens on the Salto lock a "lock event" is generated by the Salto lock and is sent via the Salto Router to the Host (the Integriti Salto SALLIS 8 Door Interface). These lock events are processed to generate review entries and to control the appropriate system inputs in Integriti (E.g. DOTL, Door forced etc.).

When communication with the Salto Router is first established, the Salto locks are set to the same state as their associated logical Integriti doors. Periodically the states of the Salto locks are requested by the Integriti Salto interface. If a lock's state is found to be different than its associated logical door, then the lock is set be the correct state.

In Integriti when a door is set to allow access by anyone (free access) the door is said to be Unlocked and when access is restricted to those who have permissions through the door, the door is said to be Locked. The equivalent naming for this in Salto is called Office Mode. When access is restricted Office Mode is disabled and when access is allowed by anyone Office Mode is enabled.

The Salto locks have a feature where they can cache the card details for valid card access attempts and if the Salto lock becomes offline it will grant access to these cards. The card cache duration is configurable via the Integriti module's configuration and its units are in days. The number of cards that can be cached by the Salto locks can be up to around 600.

When a card is presented at the Salto lock the card data is sent to the Host via the Salto Router. The Host is then responsible for sending a response indicating if the card (the User) is allowed or denied access through the Salto lock. To add a card to a User, if the card data is known then this data can be manually entered via the software or LCD Terminal. Alternately, using N-bit wiegand Direct Entry the card can be assigned to a User via the LCD Terminal or via the software.

Limitations of the Salto SALLIS Integration

- The Salto RS485 Router is capable of a maximum 16 locks whereas the Integriti Controller is capable of a maximum of 8 doors.

- The Salto Mifare locks have a “privacy” button that is not supported by the current Integriti Salto interface. This is because the current logic within the Integriti Controller that is used to evaluate access permissions does not have such a concept.

- In Salto the equivalent of Integriti’s Backup Cards is called Emergency Codes. Emergency Codes are not yet implemented in the Salto interface.

- In Salto the equivalent of Integriti’s Time Period is called a Time Table. Time Tables are only used in conjunction with Emergency Codes and hence are not required to be implemented.

- In Salto the equivalent of Integriti’s Holidays is called a Calendar. Calendars are only used in conjunction with Time Tables and hence are not required to be implemented.

- There is a limitation in Integriti Controller with the amount of card data that can be processed. Currently the Salto interface can only process up to 8 bytes (64 bits) of card data whereas the maximum card data that can be sent from the Salto lock (via the Salto Router) to the Host is 26 bytes (208 bits).

- Temporarily unlocking a Salto lock is not supported due to the design differences between the Integriti and Salto systems. In Integriti the way that a temporarily unlocked door is achieved is that an Action triggers a door to be unlocked for a period of time where the time is passed as a parameter. In Salto a command is sent to say “grant access” as a lock action to the Salto lock. This action unlocks the lock for a period that has been previously configured during the lock configuration.

- The Salto Mifare locks have provision for the AcCode of Mifare cards to be used. The AcCode is typically stored in an encrypted “Sector” on a card and a “key” is needed in order for the reader to decrypt the data. Currently Integriti does not have the infrastructure to support all of the parameters required to provide the Salto lock (or any other readers) with enough information to be able to decrypt any encrypted Sectors. Additionally, as Inner Range does not produce any Mifare type cards the card’s AcCode is not used.

- Request to exit (REX) is not supported. Door handle operation is logged to Integriti review only. Sample output:

  ```
  Salto RS485 (Ixx) Lock Event - LockID# x, Date & Time:
  xx/xx/xx xx: xx: xx, Description: Open with inside handle
  ```