



Integrating with the Salto SALLIS RF lock system

Document created with reference to Controller firmware V20.0.0.37986



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 three types of Salto SALLIS locks that are supported at this time; the Mifare lock, Mifare lock with built in keypad and the Prox lock.

From a Mifare locks, 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 . These wireless locks are compatible with Mifare Classic, Mifare Plus, Desfire & Desfire EV1 cards. Encrypted sectors are supported when the config details and encryption key are set, for example, with SIFER-C-Aperio (DESFIRE) cards and MIFARE Classic 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) = 1A000000000000000033C1EB5). 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, however, the Integriti ILAM and IAC only support a maximum of 8 Locks, whilst the SLAM is limited to a maximum of 2. 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).
- Connect the PPD to the Personal Computer using USB and select Download data.
- 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.

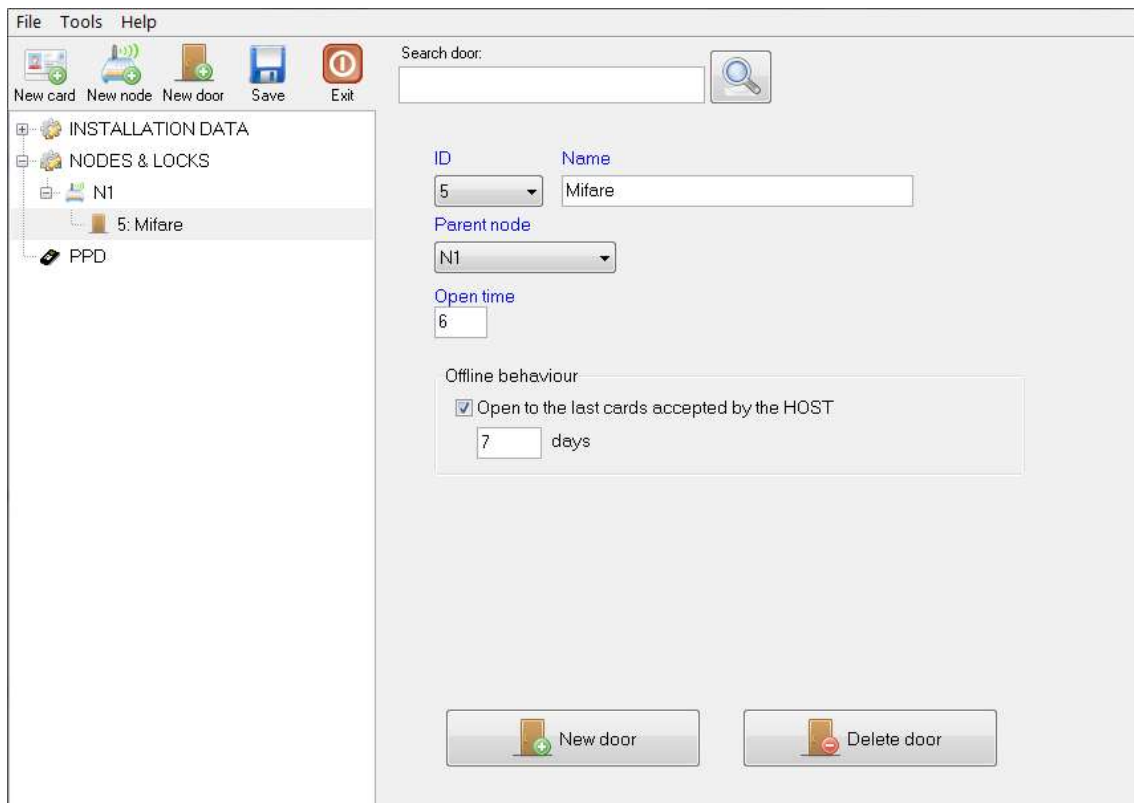


Figure 1: SALLIS program used to configure the Salto Router and Salto Locks



Figure 2: Salto PPD used to program the Salto Router and Salto Locks

Interface between Integriti and Salto Router

Salto provides two types of the Router - the RS485 version and the Ethernet version.

Currently, the Integriti Controller and LAN modules only interface with RS485 Salto Router.

The RS485 Reader communications interface on LAN modules are automatically configured when the Salto Reader mode is selected.

The Integriti Access Controller (IAC) has a dedicated RS485 Reader port for Lock / Reader interface. This is automatically configured when a Salto Lock is selected.

The Integriti Intelligent LAN Access Module (ILAM), provides support for up to 8 Salto Sallis locks. 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.

The Integriti Standard LAN Access Module (SLAM), provides support for up to 2 Salto Sallis locks.

The Integriti Security Controller (ISC) provide no direct Salto Sallis interfacing. An ILAM or SLAM can be used with the ISC for Salto Sallis Lock integration.

Integriti Reader and Door Access Control Programming

For the Integriti system to know which Salto lock is associated with which logical door on the Integriti module, the Reader and Door Access Control must be configured appropriately. The Reader and Door Access Control 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 Reader/Door Access Control programming for the Integriti module both the door number and reader number should be configured the same.

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

1. The Device Type should be set to "Salto"
2. The Number on Device value should be set to the Salto Lock ID (as configured in the SALLIS software)
3. The 'Location' and 'Card Format' options for a typical installation should also be set.

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

Save setting  when configuration completed.

Readers	
Reader 1	Salto
Number	1
Reader Purpose	Control a Door
Location	Outside Door 1
Keypad Area	
Locker / Bank	
Card Format	Direct Entry Wiegand
Any Card	<input type="checkbox"/>
PIN * Toggles Area	<input type="checkbox"/>
Wiegand Feedback Mode	Standard
PIN Device	
Pin Mode	(None)
Arming Mode	No Reader Arming
Operator Challenge Mode (Ask PC)	(None)
Skip Known Review	<input type="checkbox"/>
Reader 2	On-Board (Wiegand)

Door Access Control	
Door 1	
Door 1 Hardware	Salto #1
Hardware Type	Salto
Lock Number	1
Unibus Dip Switch Number	0
Enable Reed input	<input type="checkbox"/>
Enable Tongue input	<input type="checkbox"/>
Door 2	
Door 2 Hardware	On-Board

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

Configuring the module Door



A module Reader and associated Door Access Control requires a Door to be configured. Each individual reader that has been mapped to a Salto Router will require changes to the access control records.

Select the Door by clicking on the '...' as shown below in Figure 4.

Door Access Control	
Door 1	
Door 1 Hardware	Salto #1
Hardware Type	Salto
Lock Number	1
Unibus Dip Switch Number	0

Figure 4: Adding Door

This will allow selection of an existing Door or creation of a new Door.

To Create a new Door, select the  drop down and select the  item, as shown in Figure 5 below.

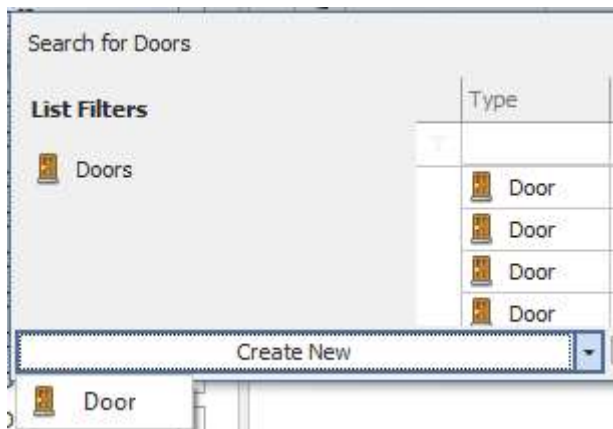


Figure 5: Creating Door

This will allow editing of the new Door entity using the screen shown in Figure 6

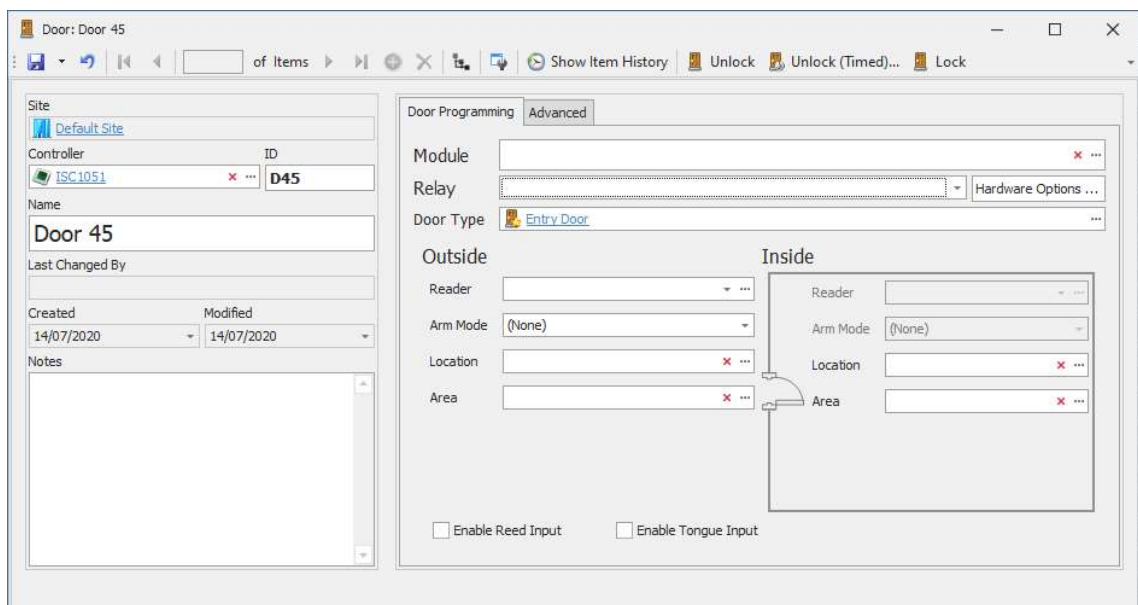



Figure 6: Editing new Door

Enter the following parameters :

1. Name – Enter a name that accurately describes the door.
2. Module – by clicking the ellipses ('...') and selecting the module type and number
3. Relay – Select 'Salto Lock x Salto x', where x is the Salto Lock number that was set in the Door Access Control screen.
The correct settings should be automatically generated by the Integriti software.
4. Reader – Select "Rx Salto x" where x is the Salto Reader Number set in the Readers screen.
The correct settings should be automatically generated by the Integriti software.
5. Set any other required settings such as Door Type, Locations and Areas
6. Set any Advanced options such as modified unlock times, and Free Access behaviour

Save the Door settings  when configuration completed.

Close the window by selecting the .

Double click the newly created Door or an existing to add to the Reader Module configuration.

Save the Reader Module settings  to include the new Door.

Other 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 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
Ixx:S13	Ixx Door1 Fault	Lock has generated a low battery alarm.	Lock battery is OK.
Ixx:S14	Ixx Door2 Fault		
Ixx:S15	Ixx Door3 Fault		
Ixx:S16	Ixx Door4 Fault		
Ixx:S17	Ixx Door5 Fault		
Ixx:S18	Ixx Door6 Fault		
Ixx:S19	Ixx Door7 Fault		
Ixx:S20	Ixx Door8 Fault		
Ixx:S21	Ixx Door1 Forced	Lock has generated an	Lock is closed.

System Input	Name	Alarm state	Sealed state
Ixx:S22	Ixx Door2 Forced	intrusion alarm.	
Ixx:S23	Ixx Door3 Forced		
Ixx:S24	Ixx Door4 Forced		
Ixx:S25	Ixx Door5 Forced		
Ixx:S26	Ixx Door6 Forced		
Ixx:S27	Ixx Door7 Forced		
Ixx:S28	Ixx Door8 Forced		
Ixx:S29	Ixx Door1 DOTL		
Ixx:S30	Ixx Door2 DOTL		
Ixx:S31	Ixx Door3 DOTL		
Ixx:S32	Ixx Door4 DOTL		
Ixx:S33	Ixx Door5 DOTL		
Ixx:S34	Ixx Door6 DOTL		
Ixx:S35	Ixx Door7 DOTL		
Ixx:S36	Ixx Door8 DOTL		
Ixx:S69	Ixx Rdr1 Fault	Salto router loses communication with the Salto lock.	Communications are restored.
Ixx:S70	Ixx Rdr2 Fault		
Ixx:S71	Ixx Rdr3 Fault		
Ixx:S72	Ixx Rdr4 Fault		
Ixx:S73	Ixx Rdr5 Fault		
Ixx:S74	Ixx Rdr6 Fault		
Ixx:S75	Ixx Rdr7 Fault		
Ixx:S76	Ixx 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 (IAC / ILAM / SLAM). 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 to 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).
- 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
```