

Protege WX SALLIS Integration
Application Note

ICTProtege**WX**.[®]

The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited. Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Copyright © Integrated Control Technology Limited 2003-2017. All rights reserved.

Last Published: 13/11/2017 15:54

Contents

- SALLIS Integration 4
- Supported Versions 5
- RF Channels 6
- SALLIS Wiring 7
 - PoE Router 7
 - RS-485 Router 8
- SALLIS Programming Application Setup 9
 - Creating a new SALLIS Database File 9
 - Configuring the Router 10
 - Configuring a Node 12
 - Configuring a Wireless Lock 13
 - Programming Card Details for Sector 13 Programmed Cards 13
 - Using a PPD 14
- ProtegeWX Setup 15
 - Salto PoE Router 15
 - Salto RS-485 Router 18
 - Programming SALLIS Sector 13 Programmed Cards 22
 - Supported Door Options 22
 - Trouble Inputs 27
- Contact 28

SALLIS Integration

The following instructions outline basic SALLIS configuration, and the steps needed to setup the SALLIS locks within ProtegeWX. It is advised that you consult the SALLIS installation manual for further information.

SALLIS integration is a licensed feature that enables you to use SALLIS standalone wireless locking devices within the ProtegeWX system using SALLIS wireless technology. SALLIS locks communicate wirelessly via Nodes that are connected to either a PoE router or an RS-485 Router. Both the standard controller (PRT-WX-DIN) and the single door controller (PRT-WX-DIN-1D) can be used with the SALLIS PoE router and the SALLIS RS-485 router.

If you are using SALLIS wireless locks and ICT proximity readers and/or cards on the same site and require instructions on using sector 13 Mifare Classic cards, ensure that you read through the following topics:

- Configuring the Router for Sector 13 Card Operation (see page 11)
- Programming Card Details for Sector 13 (see page 13)
- Programming the Sector 13 AES Encryption Key (SALLIS PoE Router) (see page 16)
- Programming the Sector 13 Mifare Classic AES Encryption Key (SALLIS RS-485 Router) (see page 19)
- Programming the Sector 13 AES Encryption Key (Individual SALLIS Locks) (see page 21)
- Programming SALLIS Sector 13 Cards (see page 22)



The AES encryption key required for sector 13 Mifare Classic programming is supplied by ICT.

Important:

Connection via RS-485 capable reader ports will only work with hardware revisions of PRT-WX-DIN that are equipped with added RS-485 reader functionality on the reader ports. This is easily determined by checking the reader ports on the front panel of the controller.

Hardware revisions that are equipped with added RS-485 reader functionality have NA and NB labels beneath the D0 and D1 labels:



Earlier revisions of the hardware do not have the NA and NB labels, and do not have the added RS-485 reader functionality:



All versions of the PRT-WX-DIN-1D come equipped with RS-485 reader functionality.

Supported Versions

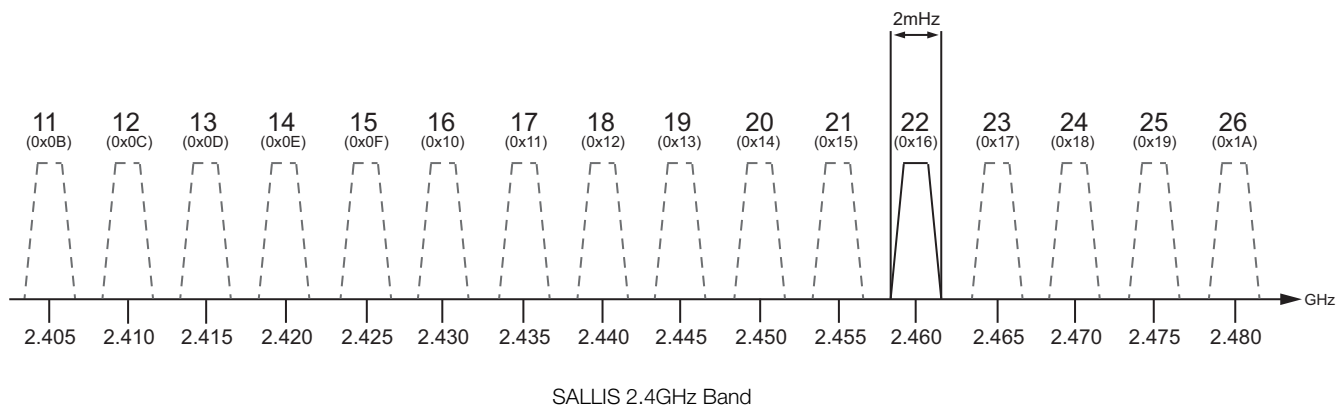
ProtegeWX SALLIS integration has been tested and verified with the following versions:

Software		
SALLIS Programming Application	Version 3.3.0.12	
ProtegeWX Controller Firmware		
PRT-WX-DIN / PRT-WX-DIN-1D	2.10.030 or above. Sector 13 Mifare Classic card configuration is available in version 4.00.274 and above.	
SALLIS XS4		
Mifare XS4 Reader	Version 04.10	Firmware No. 0008
Control XS4	Version 01.14	Firmware No. 0061
Escutcheon and GEO RF Module	Version 02.00	Firmware No. 0038
125kHz XS4 Reader	Version 01.06	Firmware No. 0074
SALLIS GEO		
Mifare + Control GEO	Version 01.11	Firmware No. 0090
Legic + Control GEO	Version 01.00	Firmware No. 0094
125kHz + Control GEO	Version: Not Available	Firmware No. 0098
Escutcheon and GEO RF Module	Version 02.00	Firmware No. 0038
SALLIS Peripherals		
SALLISROUT485	Version 01.12	Firmware No. 0059
SALLISROUTPoE	Version 01.07	Firmware No. 0072
SALLISNODE	Version 02.00	Firmware No. 0060
SALLISNODE MINI	Version 02.00	Firmware No. 0071

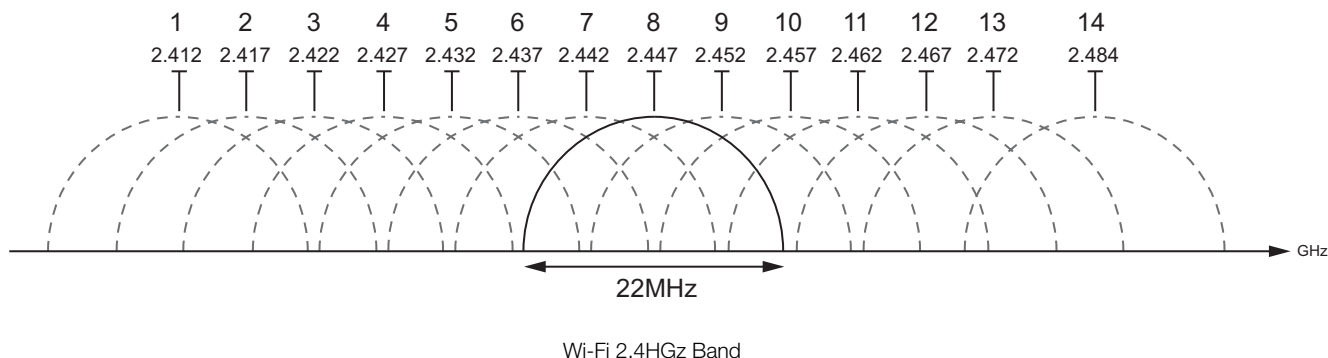
RF Channels

With wireless networks, you may find it difficult to predict the behavior of radio waves and detect the presence of interfering signals without conducting an RF site survey. As SALLIS operates on a 2.4GHz band - the same band as Wifi, Bluetooth, cordless phones and even microwave ovens - it is important to identify any devices that could affect the operation of your SALLIS system before wiring and installing the hardware.

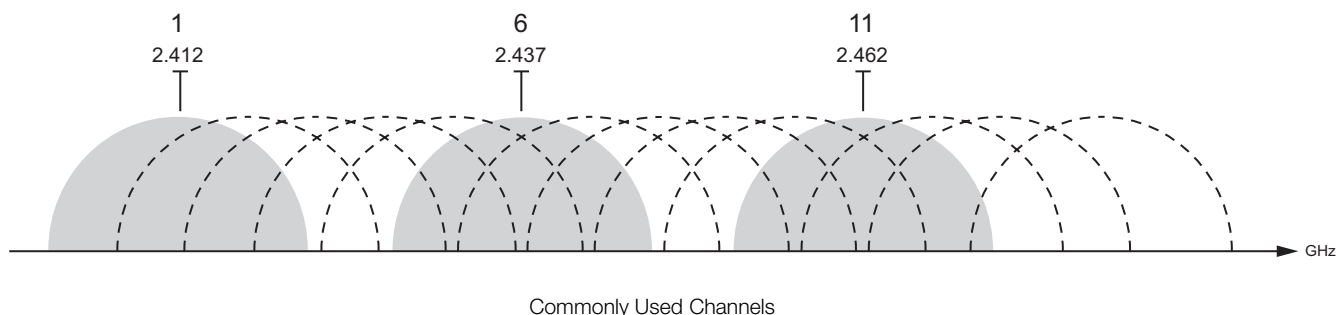
SALLIS wireless locks use a communication protocol based on the IEEE 802.15.4 standard with 16 separate channels that occupy 2MHz of bandwidth from 2405MHz to 2480MHz. An RF site survey can determine which of the 16 channels a SALLIS router should use.



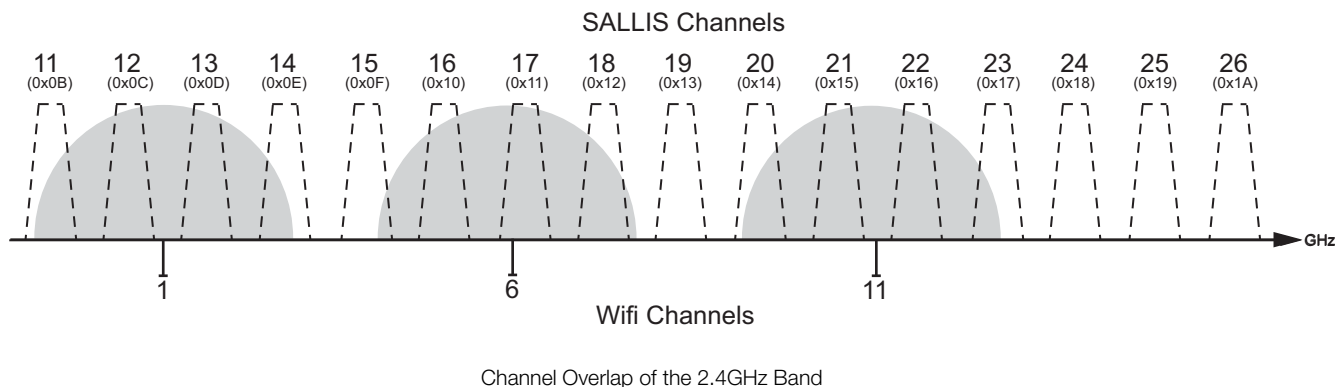
As an example, we can look at how Wi-Fi can affect the operation of SALLIS when it is operating on the same 2.4GHz band. Wi-Fi generally operates on a standard of the IEEE 802.11 communication protocol divided into 14 channels, each occupying 22MHz of bandwidth from 2412MHz to 2484MHz.



The commonly used channels are 1, 6 and 11 as they are the only channels that do not share frequency space within the band.



From the results of an RF site survey, you can determine which of the channels the Wifi network is using. With this information, you can see which of the SALLIS channels will be the least affected by the Wi-Fi network. The diagram below shows that the channels 11, 14, 15, 19, 20, 23, 24, 25, and 26 are the least likely to incur interference from the Wi-Fi network and are the ones that should be used.



SALLIS Wiring

After finding a suitable location for the SALLIS hardware, the SALLIS router needs to be wired to a ProtegeWX Controller in order to facilitate communications between the two systems.

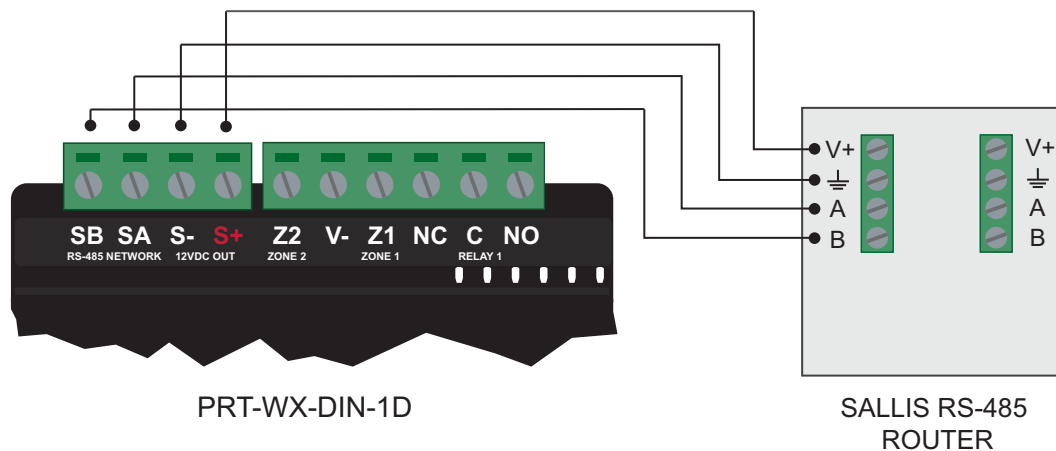
The following topics address how to wire the SALLIS PoE router and the SALLIS RS-485 to both ProtegeWX controllers. These topics do not cover how to wire a node to a SALLIS router.

For instructions on how to wire a SALLIS node to a SALLIS router, and for a comprehensive list of the limitations (including wiring restrictions and requirements) that apply to the SALLIS hardware, consult your SALLIS installation manual.

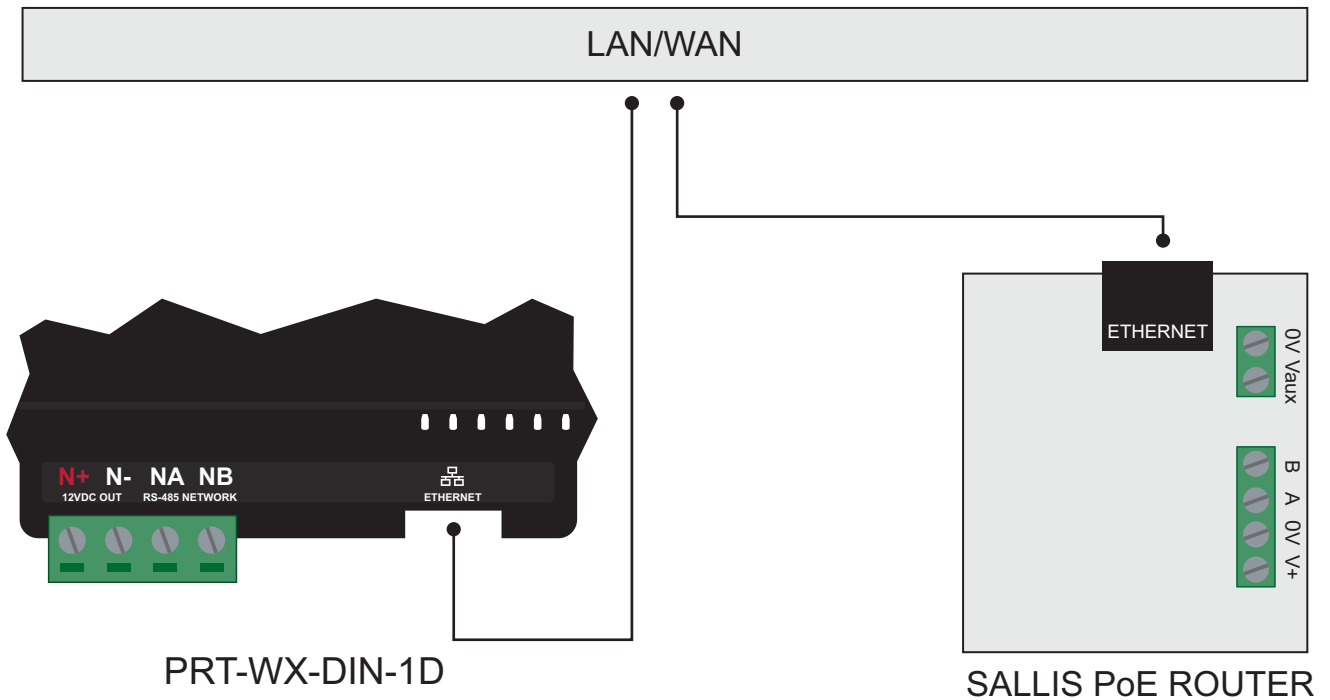
PoE Router

The SALLIS PoE router can be used to control up to 32 locks within ProtegeWX. Both the standard and single door controllers can be connected to a SALLIS PoE router via a PoE switch, providing the router with a power supply and a network connection.

If a non-PoE switch is used, power can be supplied to the router through a power adapter that supplies 500mA at 12VDC. Power supplies can be directly connected to the router via the 0V and Vaux ports.



PRT-WX-DIN to SALLIS PoE Router

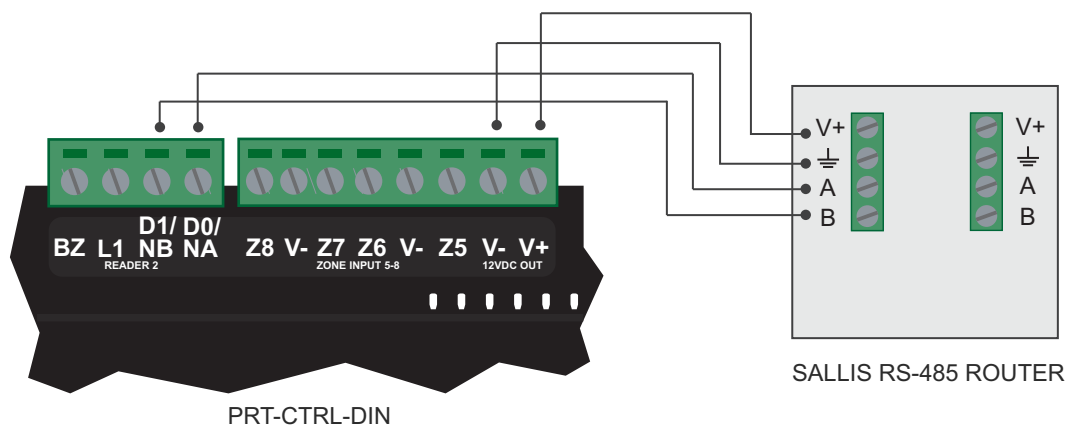


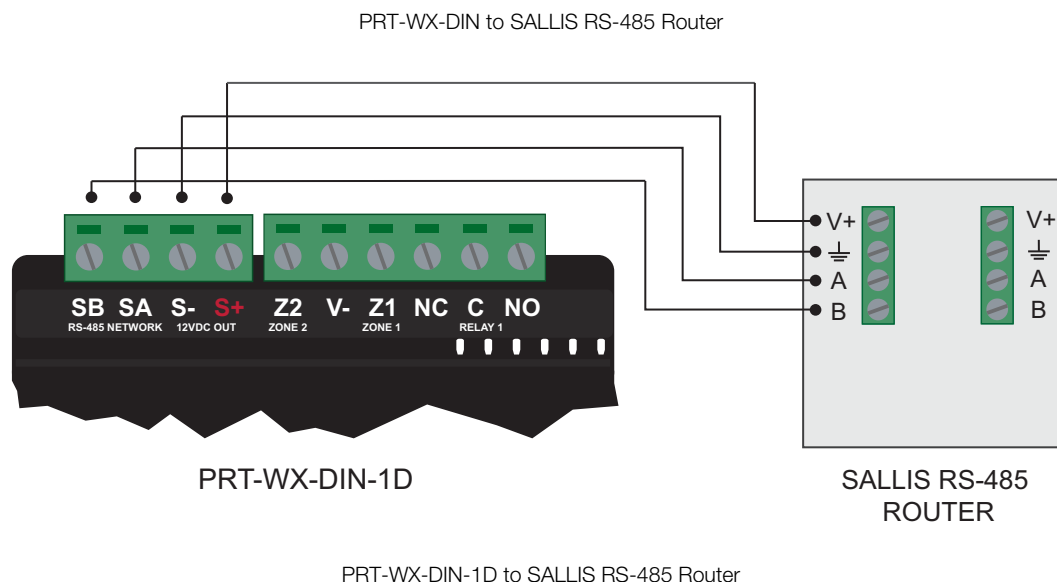
PRT-WX-DIN-1D to SALLIS PoE Router

RS-485 Router

The SALLIS RS-485 router can be used to control up to 16 locks within ProtegeWX. Both the standard and single door controllers can be connected to a SALLIS RS-485 router using one of the onboard RS-485 enabled network ports.

Power can also be supplied directly from the standard controller to the router via the V- and V+ ports and from the single door controller via the S- and S+ ports. This configuration provides the router with a network connection and a power supply.





SALLIS Programming Application Setup

SALLIS is a software application that manages the SALLIS routers, locks, nodes and cards.

This integration using software version 3.3.0.12. To check whether you are running this version of SALLIS, navigate to **Help | About** from within the SALLIS Programming Application.

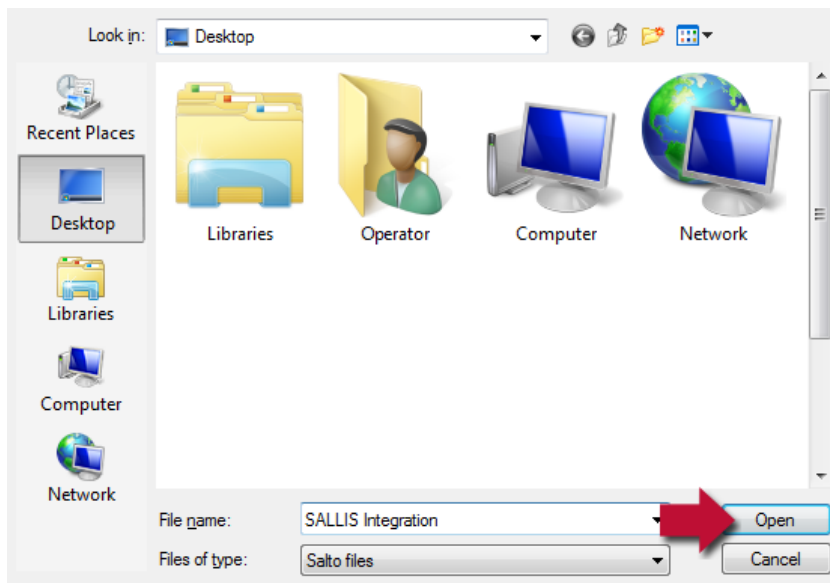


Creating a new SALLIS Database File

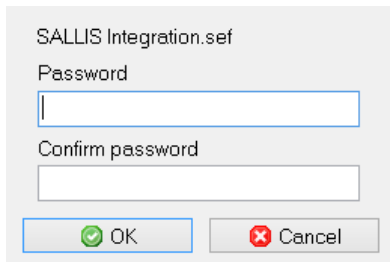
Before configuring the router, you need to create a new database file. Each router requires its own database file.

1. Open the SALLIS application and select **New** from the **File** menu

2. Enter a name for the router file and click **Open**



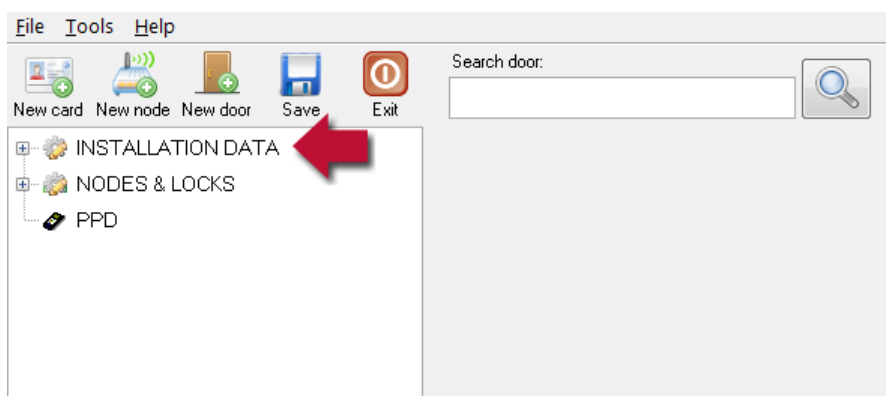
3. If authentication is required to access the database file, enter a password and click **OK**
If authentication is not required, leave the password fields blank and click **OK**



Configuring the Router

This topic outlines a standard SALLIS router setup. For information on how to configure a router to support locks reading sector 13 Mifare Classic cards, refer to [Configuring the Router for Sector 13 Mifare Classic Card Operation](#) (see page 11).

1. From within the SALLIS application, click the **Installation Data** tab



2. Select the **Router Model** you are using
3. Enter a **Name** for the router
4. Set the **UID** to **8** and the **AcCode** to **0**
5. Enable or disable the **Door Beep**
6. Select the **RF Channels** the router will be using

The RF channels selected should be determined by the results of an RF site survey

Router model

☐ RS485

☒ Ethernet-PoE

Name

SALLIS Router 1

Notes

IDCode size

UID: 8

AcCode: 0

☒ Enable door beep

Site RF channels

☐ 11 (2405 MHz)	☐ 12 (2410 MHz)	☐ 13 (2415 MHz)	☐ 14 (2420 MHz)
☒ 15 (2425 MHz)	☒ 16 (2430 MHz)	☐ 17 (2435 MHz)	☐ 18 (2440 MHz)
☐ 19 (2445 MHz)	☒ 20 (2450 MHz)	☒ 21 (2455 MHz)	☒ 22 (2460 MHz)
☐ 23 (2465 MHz)	☐ 24 (2470 MHz)	☐ 25 (2475 MHz)	☐ 26 (2480 MHz)

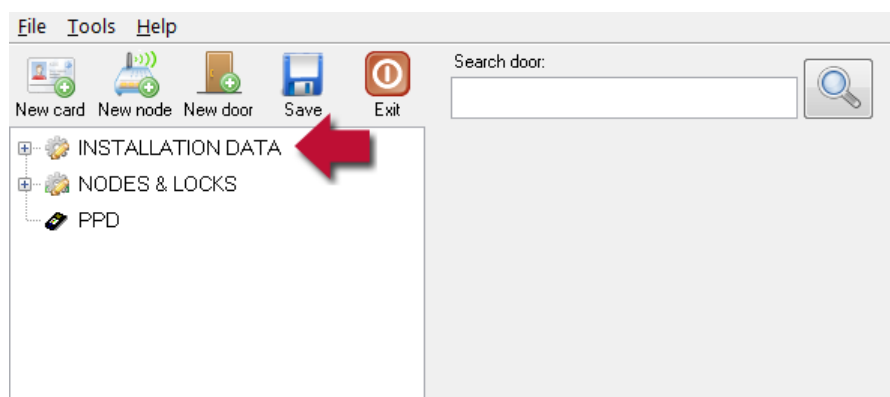
7. Click **Save**

Configuring the Router for Sector 13 Programmed Card Operation

This section is specific to integrations requiring sector 13 programmed cards for sites using both SALLIS wireless locks and ICT proximity readers and/or cards. For information on how to configure other card types, refer to the SALLIS Installation and Maintenance Guide.

If you are using SALLIS wireless locks and ICT proximity readers on the same site, follow the steps below to enable the reading of Sector 13 programmed cards on SALLIS wireless locks. This ensures that the same number is read by both SALLIS wireless locks and ICT proximity readers and removes the need for badging each card at a reader to retrieve their numbers.

1. From within the SALLIS application, click the **Installation Data** tab



2. Select the **Router Model** you are using
3. Enter a Name for the router
4. Set the **UID** to **8** as we expect 8 bytes for the UID of the card
5. Enter **16** into the **AcCode** field as we expect 16 bytes for the encrypted data stored on sector 13 of the cards used
6. Enable or disable the **Door Beep**

7. Select the **RF Channels** the router will be using

The RF channels selected should be determined by the results of an RF site survey. Refer to RF Channels (see page 6) for more information.

Router model

☐ RS485

☒ Ethernet-PoE

Name

SALLIS Router 1

Notes

IDCode size

UID: 8

AcCode: 16

☒ Enable door beep

Site RF channels

☐ 11 (2405 MHz)	☐ 12 (2410 MHz)	☐ 13 (2415 MHz)	☐ 14 (2420 MHz)
☒ 15 (2425 MHz)	☒ 16 (2430 MHz)	☐ 17 (2435 MHz)	☐ 18 (2440 MHz)
☐ 19 (2445 MHz)	☒ 20 (2450 MHz)	☒ 21 (2455 MHz)	☒ 22 (2460 MHz)
☐ 23 (2465 MHz)	☐ 24 (2470 MHz)	☐ 25 (2475 MHz)	☐ 26 (2480 MHz)

8. Click **Save**

Configuring a Node

1. Click **New Node** to configure a node
2. Set the **ID** of the node
3. Enter a **Description** to easily identify the node
4. Enter the **MAC Address** of the node. The MAC address will be a six character code located inside the node's casing

If you are using the internal node of the SALLIS PoE router, locate the two stickers located inside the router's casing labeled MAC address. The internal node's MAC address is the single six character code.

ID Node

N1

Description

SALLIS Node 1 (Internal)

MAC address

0091CC

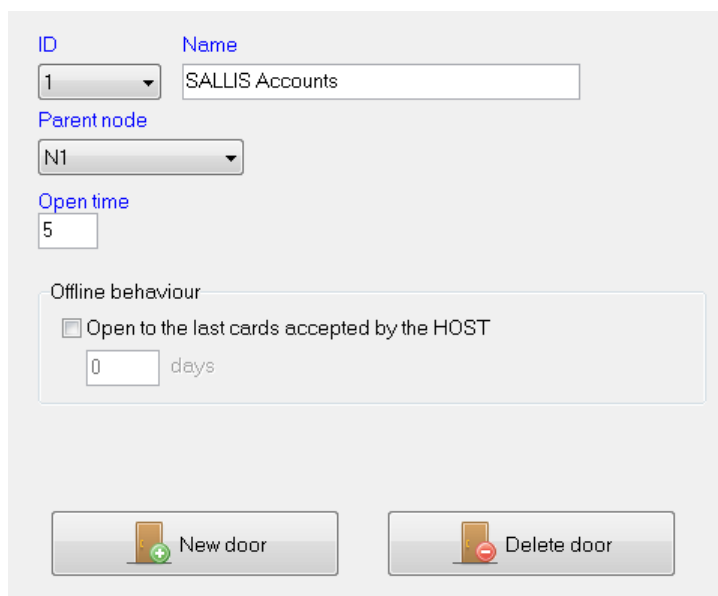
 New node

 Delete node

5. Click **Save**

Configuring a Wireless Lock

1. Click **New Door** to configure a wireless lock
2. Select an **ID** for the door. This will be used by ProtegeGX as the **Configured Address**
3. Enter a **Name** for the door. Ideally this should correspond to the location or purpose of the door
4. Select the **Parent Node** that the lock is associated with
5. Set the **Open Time** to 5 (seconds)
6. By default the **Open to Last Card Accepted by the HOST** option is enabled. When enabled, only cards that have been presented to the lock in the days specified can open the door
7. Disable the **Open to Last Card Accepted by the HOST** option



The screenshot shows a configuration window for a new door. It has the following fields and controls:

- ID**: A dropdown menu with '1' selected.
- Name**: A text input field containing 'SALLIS Accounts'.
- Parent node**: A dropdown menu with 'N1' selected.
- Open time**: A text input field containing '5'.
- Offline behaviour**: A section containing a checkbox labeled 'Open to the last cards accepted by the HOST' which is currently unchecked, and a text input field containing '0' followed by the word 'days'.
- Buttons**: Two buttons at the bottom, 'New door' (with a door icon and a green plus) and 'Delete door' (with a door icon and a red minus).

8. Click **Save**

Programming Card Details for Sector 13 Programmed Cards

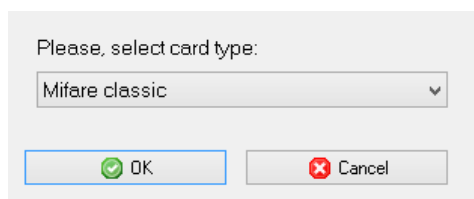
This section is specific to integrations requiring sector 13 programmed cards for sites using both SALLIS wireless locks and ICT proximity readers and/or cards. For information on how to configure other card types, refer to the SALLIS Installation and Maintenance Guide.

If your integration uses sector 13 programmed cards, follow the steps below to configure the card details.

1. Click **New Card**



2. From the drop down, select **Mifare Classic**



The screenshot shows a dialog box titled 'Please, select card type:'. It has a dropdown menu with 'Mifare classic' selected. At the bottom, there are two buttons: 'OK' (with a green checkmark) and 'Cancel' (with a red X).

3. Enter a **Name** for the card
4. Set the **Format** to **Direct**
5. Leave the **First Byte** set to **0**

6. Leave the **Size** set to **16**
7. From the drop down, select **13** for the **Sector Number**
8. Leave the **Block Number** set to **0**
9. Leave the **Key Type** set to **A**

10. From the **Key** section, click the ellipsis button (...) to program the predetermined Mifare Key supplied by ICT
11. Enter the key into both the **Key** and **Confirm key** fields
12. Click **OK**

13. Click **Save**

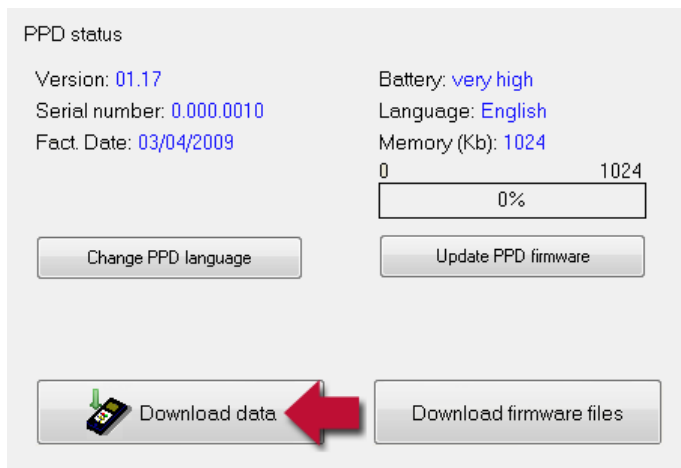


Using a PPD

The final step is to load the router file onto a PPD and transfer the data to each of the wireless locks.

1. Connect the PPD to a USB port
2. Select **PPD** from the sidebar

3. Click **Download Data**



PPD status

Version: 01.17
Serial number: 0.000.0010
Fact. Date: 03/04/2009

Battery: very high
Language: English
Memory (Kb): 1024
0 1024
0%

Change PPD language Update PPD firmware

Download data Download firmware files

4. Once the file has been synced, the information can be uploaded to the wireless locks

The data remains valid on the PDD for 15 days.

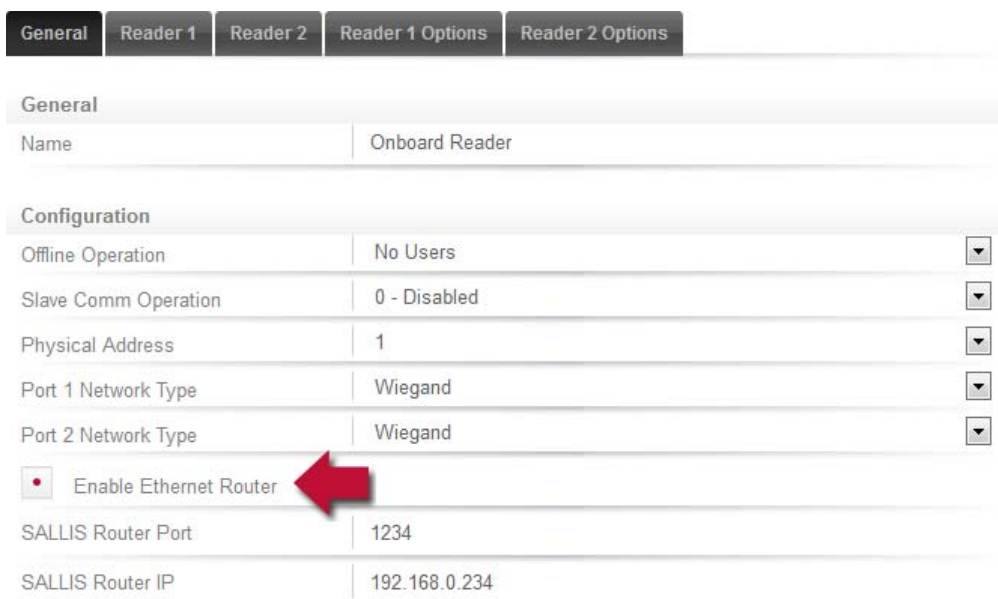
ProtegeWX Setup

Once all the of the SALLIS programming is complete, the controller's onboard reader needs to be configured for use with a SALLIS router. Each wireless lock must then be added as a smart reader.

Salto PoE Router

Configuring the Onboard Reader Port

1. Navigate to **Expanders | Reader Expanders** and select the **Onboard Reader**
2. Select the **Enable Ethernet Router** option
3. Enter the **Router Port** and **Router IP** address



General Reader 1 Reader 2 Reader 1 Options Reader 2 Options

General

Name Onboard Reader

Configuration

Offline Operation No Users

Slave Comm Operation 0 - Disabled

Physical Address 1

Port 1 Network Type Wiegand

Port 2 Network Type Wiegand

☒ Enable Ethernet Router

SALLIS Router Port 1234

SALLIS Router IP 192.168.0.234

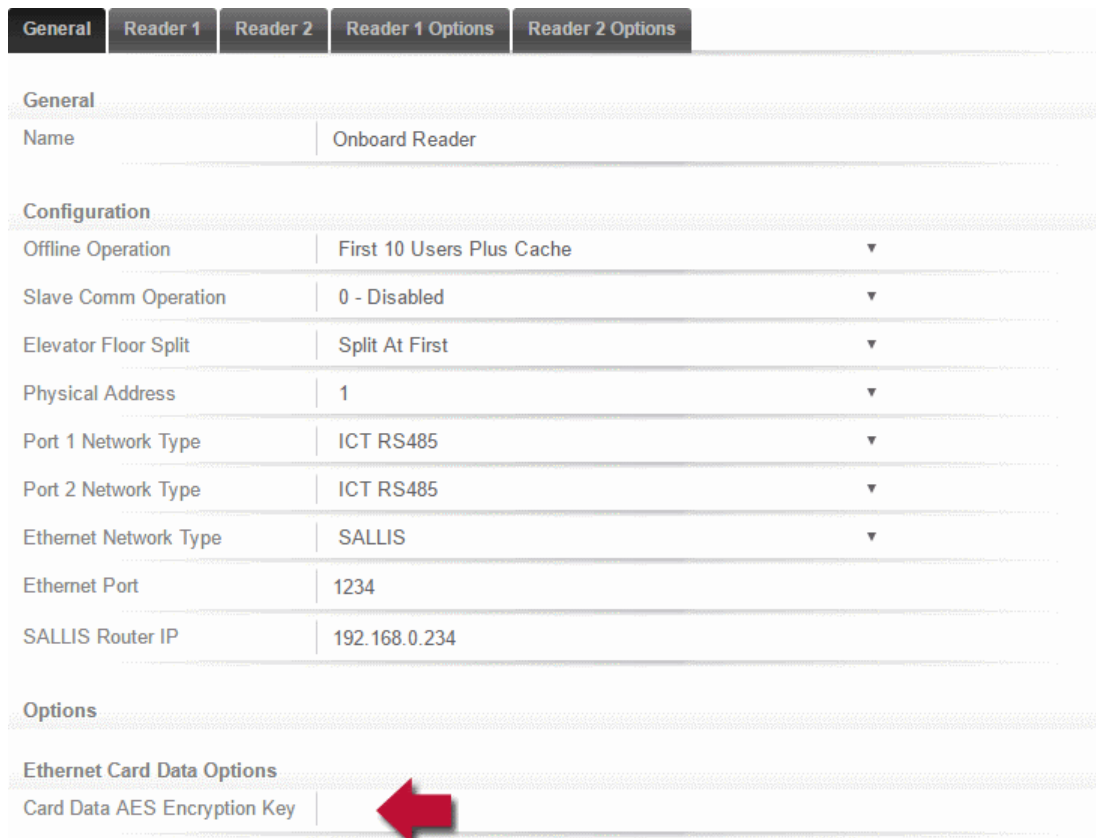
4. Click **Save**

Programming the Sector 13 AES Encryption Key (All Ethernet Connected SALLIS Locks)

This section is specific to integrations requiring sector 13 programmed cards for sites using both SALLIS wireless locks and ICT proximity readers and/or cards.

If you are using sector 13 programmed cards and require the AES encryption key to only apply to the SALLIS PoE router (and the SALLIS wireless locks communicating with the SALLIS PoE router), you need to enter the key into the **Custom Reader Format** section of the **Reader Expanders** menu.

1. Navigate to **Expanders | Reader Expanders | General** and select the onboard reader of the controller connected to the SALLIS PoE router
2. From the **Ethernet Card Data Options** section, enter the AES encryption key supplied by ICT



General		
Name	Onboard Reader	
Configuration		
Offline Operation	First 10 Users Plus Cache	▼
Slave Comm Operation	0 - Disabled	▼
Elevator Floor Split	Split At First	▼
Physical Address	1	▼
Port 1 Network Type	ICT RS485	▼
Port 2 Network Type	ICT RS485	▼
Ethernet Network Type	SALLIS	▼
Ethernet Port	1234	
SALLIS Router IP	192.168.0.234	
Options		
Ethernet Card Data Options		
Card Data AES Encryption Key		

3. Click **Save**

Adding Smart Readers

1. Navigate to **Expanders | Smart Readers** and click **Add**
2. Enter the **Name** for the lock
3. Set the **Expander Address** to that of the onboard reader (in most cases 1)
4. Set the **Expander Port** to **Ethernet**
5. Enter the **Address** of the lock (as assigned from the SALLIS application)

The screenshot shows the 'General' tab of the Smart Reader configuration form. It has two sections: 'General' and 'Configuration'. The 'General' section has a 'Name' field with the value 'SALLIS Lock - Accounts Office'. The 'Configuration' section has three fields: 'Expander Address' with value '1', 'Expander Port' with value 'Ethernet', and 'Configured Address' with value '1'. Each field in the configuration section has a dropdown arrow on the right.

General	
Name	SALLIS Lock - Accounts Office

Configuration	
Expander Address	1
Expander Port	Ethernet
Configured Address	1

6. Click **Save**

Smart Reader Options

Additional programming for the locks can be done from the **Reader** tab of the **Smart Readers** menu.

The screenshot shows the 'Reader' tab of the Smart Reader configuration form. It has two sections: 'Configuration' and 'Misc Options'. The 'Configuration' section has two fields: 'Reader 1 Location' with value 'Entry' and 'Reader 1 Door' with value 'Accounts Office'. Each field has a dropdown arrow on the right. The 'Misc Options' section has four options, each with a checkbox: 'Disarm Area For Door On Access' (unchecked), 'Allow Access When Area Armed' (unchecked), 'Log Reader Events' (unchecked), and 'Display Card Detail When Invalid' (checked with a red dot).

Configuration	
Reader 1 Location	Entry
Reader 1 Door	Accounts Office

Misc Options	
☐	Disarm Area For Door On Access
☐	Allow Access When Area Armed
☐	Log Reader Events
☒	Display Card Detail When Invalid

Configuration

- Set the **Reader Location** to **Entry** or **Exit**
- Select the **Door** that the lock is associated with

Misc Options

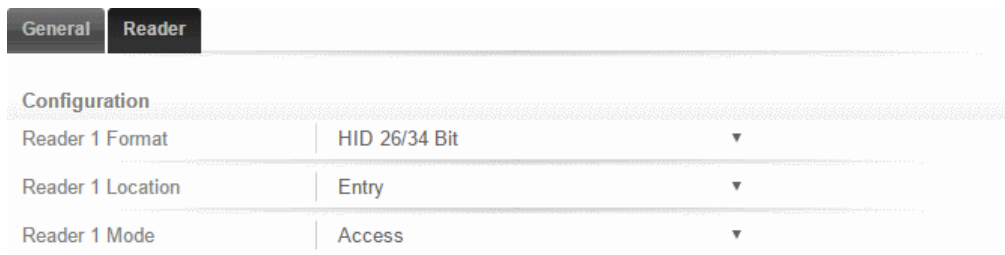
- When the **Disarm Area For Door On Access** option is enabled, unlocking the door will disarm the defined inside area if the lock is used for entry and disarm the outside area if the lock is used for exit. When this option is disabled the lock will not perform any disarm functions
- When the **Allow Access When Area Armed** option is enabled, a user can gain access through the door even when the inside area is armed. When disabled, a user will be denied access through the door if they do not have permission to disarm the inside area
- When the **Log Reader Events** option is enabled, events associated with the lock will be logged
- When the **Display Card Detail When Invalid** option is enabled, full card data will be displayed when a user attempts to unlock the lock with an invalid card

Programming the Sector 13 AES Encryption Key (Individual SALLIS Locks)

This section is specific to integrations requiring sector 13 programmed cards for sites using both SALLIS wireless locks and ICT proximity readers and/or cards.

If you are using Sector 13 programmed cards and require the AES encryption key to only apply to a specific SALLIS Wireless Lock you need to enter the key into the **Card Data Options** section of the **Smart Readers | Reader** menu.

1. Navigate to the **Expanders | Smart Readers** and select the smart reader required
2. Select the **Reader** tab
3. Ensure that the **Reader Format** is set to **HID 26/34 Bit**



The screenshot shows the 'Reader' tab in a configuration interface. Under the 'Configuration' section, there are three rows: 'Reader 1 Format' set to 'HID 26/34 Bit', 'Reader 1 Location' set to 'Entry', and 'Reader 1 Mode' set to 'Access'. Each row has a dropdown arrow on the right.

4. From the **Card Data Options** section, enter the AES encryption key supplied by ICT
 - The **Read Non ICT Programmed Sector Data** option enables the reading of card sector data not programmed by ICT, but means that the reader / lock will no longer read ICT programmed sector data.



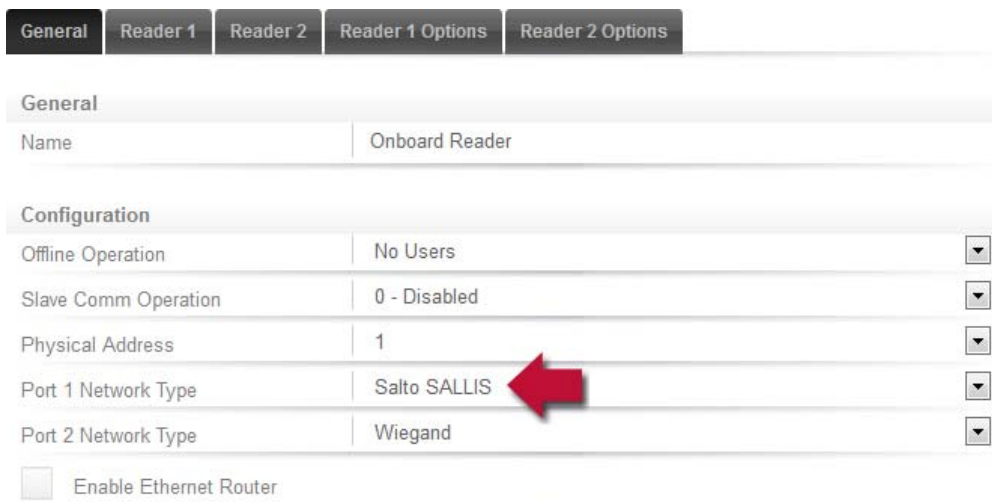
The screenshot shows the 'Card Data Options' section. It includes a text input field for 'Card Data AES Encryption Key' and a checkbox labeled 'Read Non ICT Programmed Sector Data'.

5. Click **Save**.

Salto RS-485 Router

Configuring the Onboard Reader Port

1. Navigate to **Expanders | Reader Expander** and select the **Onboard Reader**
2. Set the **Port Network Type** to **Salto SALLIS** for the port that the router is wired to



The screenshot shows the 'Reader Expander' configuration interface. The 'General' tab is selected, showing 'Name' as 'Onboard Reader'. Under the 'Configuration' section, 'Port 1 Network Type' is set to 'Salto SALLIS', which is highlighted with a red arrow. Other settings include 'Offline Operation' (No Users), 'Slave Comm Operation' (0 - Disabled), 'Physical Address' (1), and 'Port 2 Network Type' (Wiegand). There is also an 'Enable Ethernet Router' checkbox.

3. Click **Save**

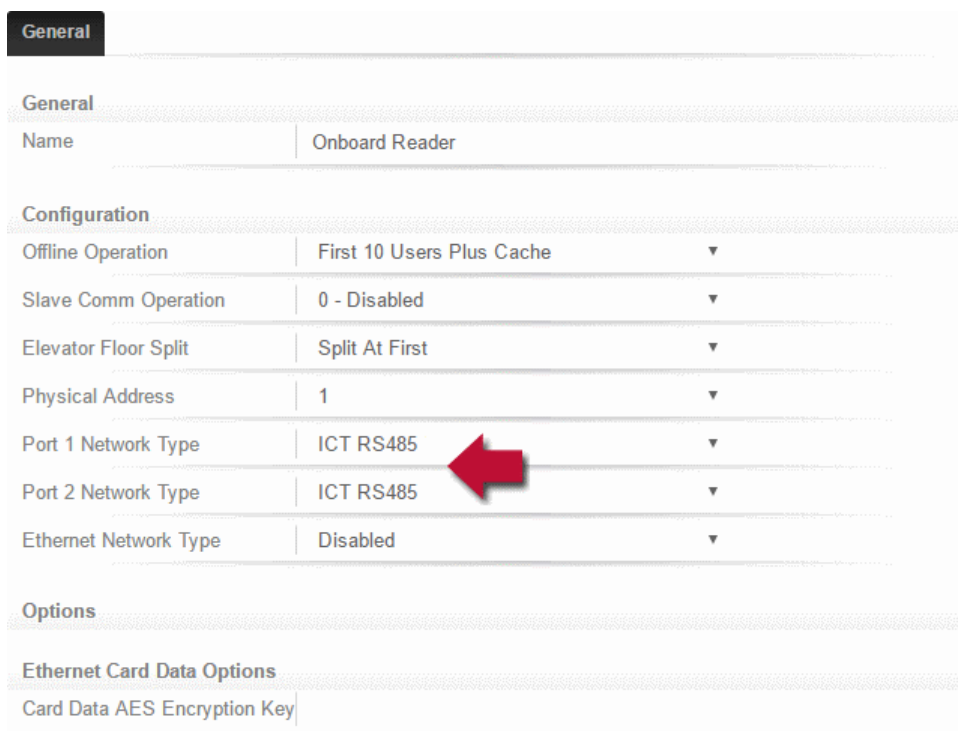
Programming the Sector 13 AES Encryption Key (All Reader Port Connected SALLIS Locks)

This section is specific to integrations requiring sector 13 programmed cards for sites using both SALLIS wireless locks and ICT proximity readers and/or cards.

If you are using the same encryption key for each lock connected to the same reader port, you can apply the key globally to the reader port. To do this you need to change the network type of the reader port as this feature is not available when it is configured for SALLIS integration.

If you want to apply an encryption key to each individual lock, refer to Programming the Sector 13 AES Encryption Key (Individual SALLIS Locks (see page 21).

1. Navigate to **Expanders | Reader Expanders** and select the controller's onboard reader expander
2. Change the required **Port Network Type** from **Salto SALLIS** to **ICT RS485** and click **Save**



General

General

Name | Onboard Reader

Configuration

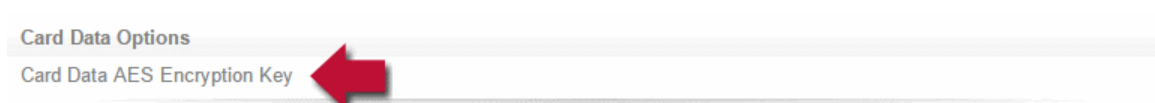
Offline Operation	First 10 Users Plus Cache	▼
Slave Comm Operation	0 - Disabled	▼
Elevator Floor Split	Split At First	▼
Physical Address	1	▼
Port 1 Network Type	ICT RS485	▼
Port 2 Network Type	ICT RS485	▼
Ethernet Network Type	Disabled	▼

Options

Ethernet Card Data Options

Card Data AES Encryption Key

3. Select the corresponding **Reader** tab
4. From the **Card Data Options** section, enter the AES encryption key supplied by ICT and click **Save**



Card Data Options

Card Data AES Encryption Key

5. Select the **General** tab and change the **Port Network Type** back to **Salto SALLIS**.

General

General

Name	Onboard Reader
------	----------------

Configuration

Offline Operation	First 10 Users Plus Cache	▼
Slave Comm Operation	0 - Disabled	▼
Elevator Floor Split	Split At First	▼
Physical Address	1	▼
Port 1 Network Type	Salto SALLIS	▼
Port 2 Network Type	Salto SALLIS	▼
Ethernet Network Type	Disabled	▼

Options

Ethernet Card Data Options

Card Data AES Encryption Key

6. Click **Save**

Adding Smart Readers

1. Navigate to **Expanders | Smart Readers** and click **Add**
2. Enter a **Name** for the lock
3. Set the **Expander Address** to that of the onboard reader (in most cases 1)
4. Set the **Expander Port** that the SALLIS router is wired to
5. Enter the **Configured Address** of the lock (as assigned from the SALLIS application)

General **Reader**

General

Name	SALLIS Lock - Accounts Office
------	-------------------------------

Configuration

Expander Address	1	▼
Expander Port	1	▼
Configured Address	1	▼

6. Click **Save**

Smart Reader Options

Additional programming for the locks can be done from the **Reader** tab of the **Smart Readers** menu.

Configuration	
Reader 1 Location	Entry
Reader 1 Door	Accounts Office

Misc Options	
☐	Disarm Area For Door On Access
☐	Allow Access When Area Armed
☐	Log Reader Events
☒	Display Card Detail When Invalid

Configuration

- Set the **Reader Location** to **Entry** or **Exit**
- Select the **Door** that the lock is associated with

Misc Options

- When the **Disarm Area For Door On Access** option is enabled, unlocking the door will disarm the defined inside area if the lock is used for entry and disarm the outside area if the lock is used for exit. When this option is disabled the lock will not perform any disarm functions
- When the **Allow Access When Area Armed** option is enabled, a user can gain access through the door even when the inside area is armed. When disabled, a user will be denied access through the door if they do not have permission to disarm the inside area
- When the **Log Reader Events** option is enabled, events associated with the lock will be logged
- When the **Display Card Detail When Invalid** option is enabled, full card data will be displayed when a user attempts to unlock the lock with an invalid card

Programming the Sector 13 AES Encryption Key (Individual SALLIS Locks)

This section is specific to integrations requiring sector 13 programmed cards for sites using both SALLIS wireless locks and ICT proximity readers and/or cards.

If you are using Sector 13 programmed cards and require the AES encryption key to only apply to a specific SALLIS Wireless Lock you need to enter the key into the **Card Data Options** section of the **Smart Readers | Reader** menu.

1. Navigate to the **Expanders | Smart Readers** and select the smart reader required
2. Select the **Reader** tab
3. Ensure that the **Reader Format** is set to **HID 26/34 Bit**

Configuration	
Reader 1 Format	HID 26/34 Bit
Reader 1 Location	Entry
Reader 1 Mode	Access

4. From the **Card Data Options** section, enter the AES encryption key supplied by ICT

- The **Read Non ICT Programmed Sector Data** option enables the reading of card sector data not programmed by ICT, but means that the reader / lock will no longer read ICT programmed sector data. Do not enable this option if you require the reader / lock to read ICT programmed sector data and additional sector data.

Card Data Options

Card Data AES Encryption Key

☐ Read Non ICT Programmed Sector Data

5. Click **Save**.

Programming SALLIS Sector 13 Programmed Cards

This section is specific to integrations requiring sector 13 programmed cards for sites using both SALLIS wireless locks and ICT proximity readers and/or cards.

The ICT encoder client is used to program sector 13 on SALLIS encoded cards. For more information on the steps required, contact ICT.

Supported Door Options

Once a SALLIS lock has been configured within ProtegeGX, various door options can be set.

SALLIS locks can be programmed to have many of the core features of hardwired doors, however some options are not supported. The following runs through the options that can be enabled.

- SALLIS locks can be fully integrated with user's access levels and access can be granted or denied based on doors, door groups and schedules
- SALLIS locks can be setup to enter office mode (unlock and stay unlocked for a period of time) in response to a schedule or an area state change, or from an **Unlock latched** manual command
- Areas can be linked to SALLIS locks so a user with suitable access rights can disarm an area based on door access, or be denied access based on the current state of an area.
- Only single badging of a door is supported
- At the time of writing this application note, the current SALLIS firmware does not provide up to date lock and door state feedback. As a result, when operating in restricted access mode, the state of the lock is displayed as **Unknown**

Doors | General

General	Outputs	Options	Advanced Options	Events
---------	---------	---------	------------------	--------

General	
Name	Warehouse Entry

Setup	
Door Type	Card Only 
Slave Door	- Not Set - 
Area Inside Door	- Not Set - 
Area Outside Door	- Not Set - 
Unlock Schedule	Never 
Door Pre-alarm Delay Time	30 
Door Left Open Alarm Time	45 
Interlock Door Group	- Not Set - 

Commands	
Commands	

Setup

- **Door Type:** Must be set to **Card Only**
- **Slave Doors:** Supported only when a hardwired door is used as the slave
- **Area Inside Door:** Supported
- **Area Outside Door:** Supported
- **Unlock Schedule:** Supported
- **Door Pre-alarm Delay Time:** Not supported
- **Door Left Open Alarm Time:** Not supported
- **Interlock Door Group:** Supported

Doors | Outputs

General	Outputs	Options	Advanced Options	Events
Lock Output				
Lock Output	- Not Set -			
Lock Output Group	- Not Set -			
Lock Activation Time	5			
Pre-Alarm Output				
Pre Alarm Output	- Not Set -			
Pre Alarm Output Group	- Not Set -			
Pre Pulse On Time	0			
Pre Pulse Off Time	0			
Door Left Open Output				
Left Open Alarm Output	- Not Set -			
Left Open Alarm Output Group	- Not Set -			
Left Open Pulse On Time	0			
Left Open Pulse Off Time	0			
Door Forced Open Output				
Forced Open Output	- Not Set -			
Forced Open Output Group	- Not Set -			
Forced Open Pulse On Time	0			
Forced Open Pulse Off Time	0			

Lock Output

- **Lock Output/Output Group:** Supported, and operates in parallel with the lock. Generally this would be left as - Not Set - unless used for a specific requirement
- **Lock Activation Time:** Only supported for the defined Output and Output Group. The lock programming will override this

Pre-Alarm Output

- **Pre Alarm Output/Output Group:** Not supported
- **Pre Alarm Pulse On Time:** Not supported
- **Pre Alarm Pulse Off Time:** Not supported

Door Left Open Output

- **Left Open Alarm Output/Output Group:** Supported
- **Left Open Alarm Pulse On Time:** Supported
- **Left Open Alarm Pulse Off Time:** Supported

Door Forced Open Output

- **Forced Open Output/Output Group:** Supported
- **Forced Open Pulse On Time:** Supported
- **Forced Open Pulse Off Time:** Supported

Doors | Options

General	Outputs	Options	Advanced Options
---------	---------	---------	------------------

Door Options

☐ Always Check Unlock Schedule

☐ Enable Open/Close Events On Schedule

☒ Enable Pre-Alarm Events

☒ Enable Left Open Events

☐ Relock On Door Close

☒ Unlock Door On REX

☐ Unlock Door On REN

☐ Schedule Operates Late To Open

Door Options 2

☐ Door Lock Follows Inside Area

☐ Door Lock Follows Outside Area

☐ Prevent Unlock On Schedule If Inside Area Armed

☐ Prevent Unlock On Schedule If Outside Area Armed

☐ Area Disarmed AND Schedule Valid Unlock Door

☐ Area Disarmed OR Schedule Valid Unlock Door

☐ Enable Access Taken on REX/REN Events

☐ Prevent Slave Unlock On Inside Area

Door Options

- **Always Check Unlock Schedule:** Supported
- **Enable Open Close Events On Schedule:** Not supported
- **Enable Pre-Alarm Events:** Not supported
- **Enable Left Open Events:** Not supported. Left open events (and other Salto lock events) can be enabled by selecting **Log Reader Events** under the Smart Reader programming
- **Relock On Door Close:** Not supported. Will be overridden by the SALLIS programming
- **Unlock Door On REX:** Not supported
- **Unlock Door On REN:** Not supported
- **Schedule Operates Late To Open:** Not supported

Door Options 2

- **Door Lock Follows Inside Area:** Supported
- **Door Lock Follows Outside Area:** Supported
- **Prevent Slave Unlock On Inside Area:** Supported
- **Prevent Unlock On Schedule If Inside Area Armed:** Supported
- **Prevent Unlock On Schedule If Outside Area Armed:** Supported
- **Area Disarmed AND Schedule Valid Unlock Door:** Supported
- **Area Disarmed OR Schedule Valid Unlock Door:** Supported
- **Enable Access Taken On REX/REN Events:** Not supported

Doors | Advanced Options

General

Outputs

Options

Advanced Options

Advanced Options

☐

Lock Out REX When Inside Area Armed

☐

Deny Entry if Inside Area is Armed

☐

Deny Exit if Outside Area is Armed

☐

Disable Door Alarms on Schedule Unlock

☐

Prompt User for Access Reason Code

☐

Enable Access Taken on Door Unlock Events

Extended Access Time Options

Door Extended Access Time0

Advanced Options

- **Lock Out REX When Inside Area Armed:** Not Supported
- **Deny Entry if Inside Area is Armed:** Supported
- **Deny Exit if Outside Area is Armed:** Supported
- **Disable Door Alarms on Schedule Unlock:** Supported
- **Prompt User for Access Reason Code:** Not Supported
- **Enable Access Taken on Door Unlock Events:** Not supported

Extended Access Time Options

- **Door Extended Access Time:** Not supported

Trouble Inputs

For reporting purposes the Onboard Reader trouble inputs are linked to the SALLIS door locks using an OR function.

The linked inputs are:

Module Type	Input	Name	Description
Reader Expander	13	Offline	Router is offline with ProtegeWX for RS485 routers.
Reader Expander	12	Offline	Router is offline with ProtegeWX for Ethernet routers.
Door (select appropriate SALLIS door)	1	Door Forced	One of the SALLIS locks has a door forced condition. The reader log records which lock it is.
Door (select appropriate SALLIS door)	2	Door Left	One of the SALLIS locks has been left open. The reader log records which lock it is.
Door (select appropriate SALLIS door)	4	Battery Low	SALLIS lock has a low battery. The reader log records which lock it is.
Door (select appropriate SALLIS door)	6	Door offline	SALLIS lock is offline with SALLIS router. The reader lock records which lock it is.

Contact

Integrated Control Technology welcomes all feedback.

Please visit our website (<http://www.ict.co>) or use the contact information below.

Integrated Control Technology

P.O. Box 302-340
North Harbour Post Centre
Auckland
New Zealand

4 John Glenn Ave
Rosedale
North Shore City 0632
Auckland
New Zealand

Phone: +64-9-476-7124

Toll Free Numbers:

0800 ICT 111 (0800 428 111) - New Zealand

1800 ICT 111 (1800 428 111) - Australia

1855 ICT 9111 (1855 428 9111) - USA/Canada

Email: sales@ict.co or support@ict.co (<mailto:support@ict.co>)

Web: www.ict.co



APAC

Integrated Control Technology Limited
4 John Glenn Avenue, Rosedale, Auckland 0632
PO Box 302-340, North Harbour, Auckland 0751, New Zealand
Email: sales@ict.co Toll Free: (0800) 428 111 Phone: 64 (9) 476 7124

AMERICAS

Integrated Control Technology (USA) LLC
5265 S Rio Grande Street, Suite 201, Littleton, CO 80120
Email: ussales@ict.co Toll Free: (855) 428 9111 Phone: 720 442 0767

EMEA

Integrated Control Technology (Europe) Limited
St Mary's Court, The Broadway, Amersham, HP7 0UT, UK
Email: emeasales@ict.co Phone: 44 0 1494 590494

Designers & manufacturers of integrated electronic access control, security and automation products.

Designed & manufactured by Integrated Control Technology Ltd.

Copyright © Integrated Control Technology Limited 2003-2017. All rights reserved.

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of these products, neither Integrated Control Technology Ltd nor its employees, shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the Integrated Control Technology policy of enhanced development, design and specifications are subject to change without notice

www.ict.co