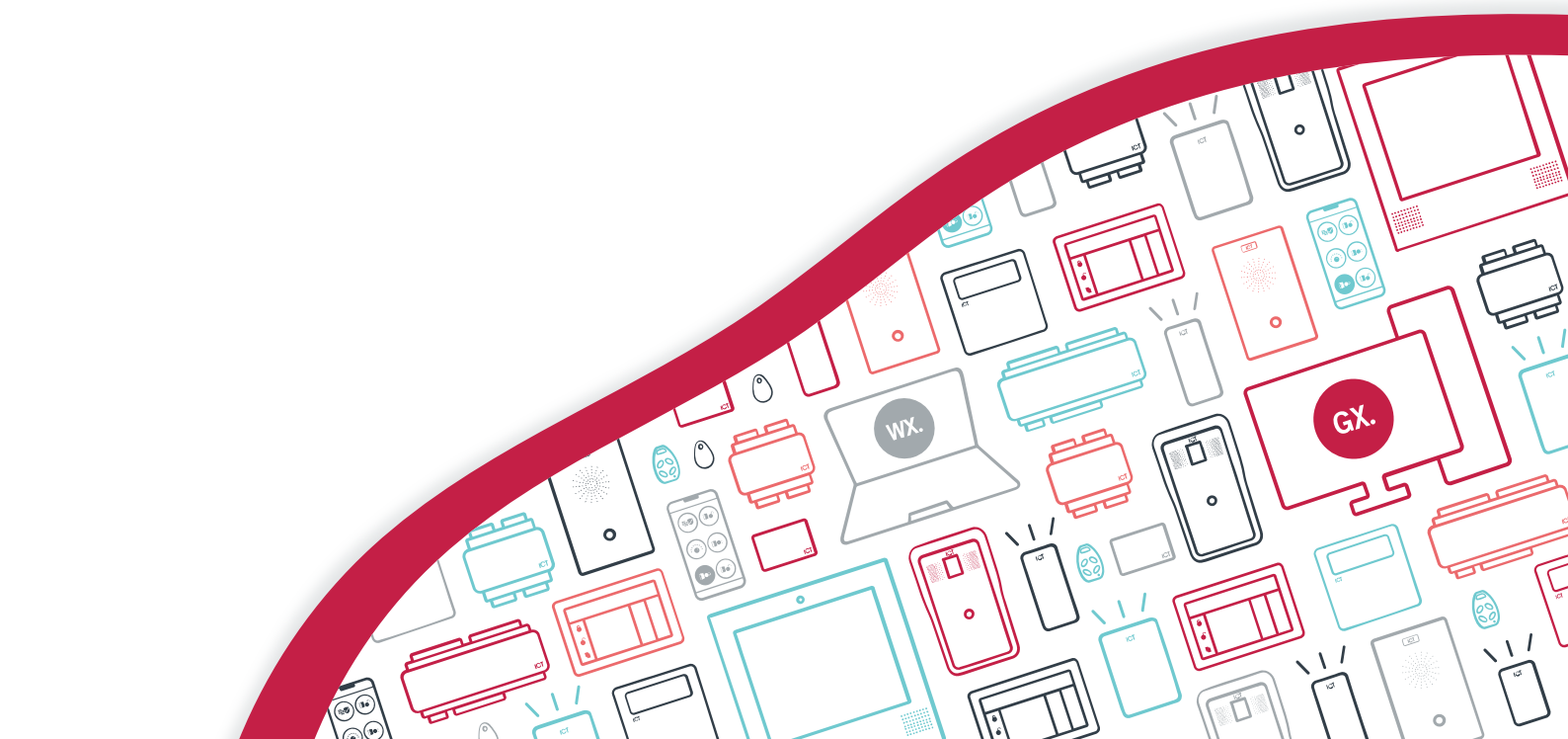
AN-148

Salto SALLIS Integration in Protege GX

Application Note



Last Published: 13-May-22 10:23 AM

Contents

Introduction

SALLIS integration is a licensed feature that enables SALLIS standalone wireless locking devices to be used within the Protege GX system. Using SALLIS wireless technology, SALLIS locks communicate wirelessly via nodes that are connected to either a PoE router or an RS-485 Router. The Protege GX controller communicates with the SALLIS router via the onboard reader. Both the standard Protege GX controller and the single door controller support communication with SALLIS PoE and RS-485 routers.

* Only controllers with RS-485 functionality on the reader ports support this integration. See more below.

Important:

Connection via RS-485 is only supported with hardware revisions of controllers that are equipped with the 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 RS-485 reader functionality have the NA and NB labels beneath the D0 and D1 labels, as shown below.

Earlier revisions of the controller hardware that do not have the NA and NB labels (as in the example below) do not have the added RS-485 reader functionality.

All one door controllers come equipped with RS-485 reader functionality.

Prerequisites

- One Salto SALLIS Door License (Ordering code: PRT-GX-DOR-SL) for each connected wireless lock.
- A Protege GX controller running version 2.08.583 or higher or higher.
  - ICT encrypted DESFire card configuration is available in version 2.08.874 and above.
  - SALLIS locks with keypads are supported in version 2.08.860 and above.
- The SALLIS Programming Application is required to configure the routers and locks for the integration.
- All relevant version requirements as listed in the following Supported Versions section.

The instructions in this application note outline the SALLIS configuration required for this integration, and the steps needed to set up the SALLIS locks within Protege GX. For additional information on SALLIS configuration, it is advised that you consult the SALLIS installation manual.

Supported Versions

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

Software		
Protege GX software	Version 4.0.128 or higher	
SALLIS programming application	Version 3.3.012	
Firmware		
Protege GX controller	Version 2.08.583 or higher	
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

Note: Not all SALLIS models have been tested, and specific models may require testing and validation.

Lock Compatibility

While many SALLIS lock variations are compatible with this integration, including locks with keypads, ICT is unable to confirm or guarantee the compatibility of any specific model or version without prior testing.

The integration occurs between the Protege GX controller and the SALLIS router. The controller does not directly integrate with the SALLIS locks. Compatibility of specific locks is dependent upon their compatibility with the supported router versions and the required configuration, including credential formats.

Lock functionality will also be dependent upon their compatibility and ability to perform the supported door functionality as outlined in Supported Door Options (see page 16).

Sector 13 MIFARE Classic and ICT Encrypted DESFire

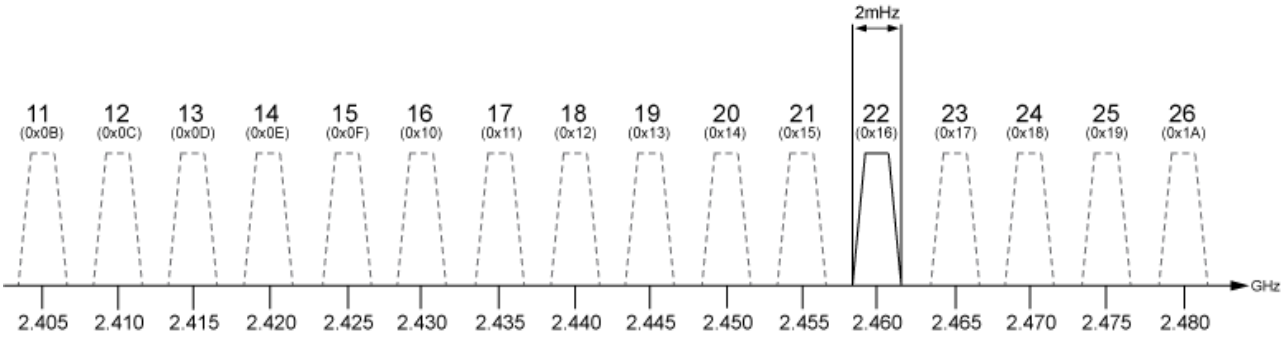
The following topics provide instruction on using encrypted sector 13 MIFARE Classic cards or ICT encrypted DESFire cards, when using SALLIS wireless locks and ICT proximity readers and/or cards on the same site.

The AES encryption key required for sector 13 MIFARE Classic programming or ICT encrypted DESFire programming is supplied by ICT. Please contact the ICT support team to obtain your encryption key.

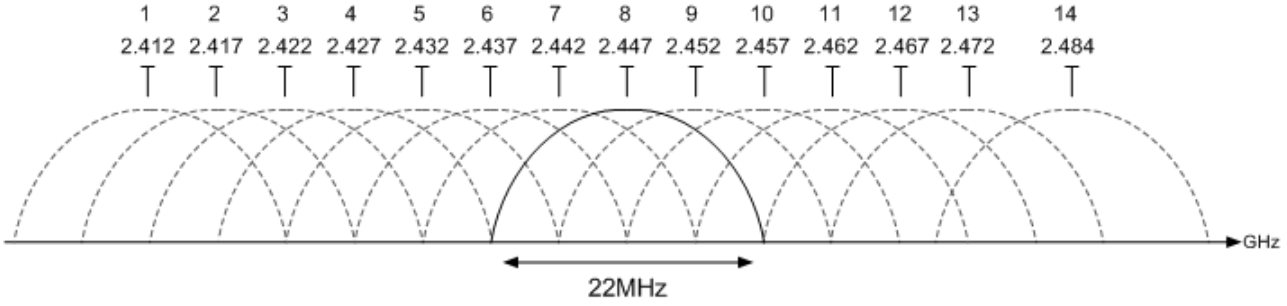
RF Channels

SALLIS operates on a 2.4GHz band - the same band as Wi-Fi, Bluetooth, cordless phones and even microwave ovens - so it is important to identify any devices that could affect the operation of your SALLIS system before wiring and installing the hardware. Predicting the behavior of radio waves and detecting the presence of interfering signals can be difficult with wireless networks, so conducting an RF site survey is recommended.

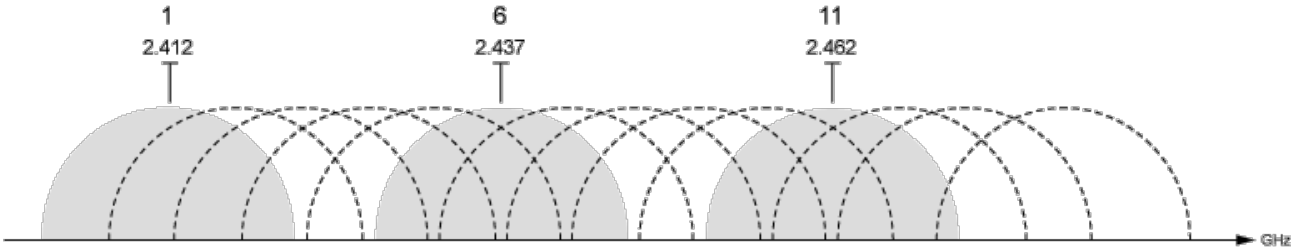
SALLIS wireless locks use a communication protocol based on the IEEE 802.15.4 standard with 16 separate channels that occupy 2MHz of bandwidth from 2405MHz to 2480MHz. An RF site survey can determine which of the 16 channels a SALLIS router should use.



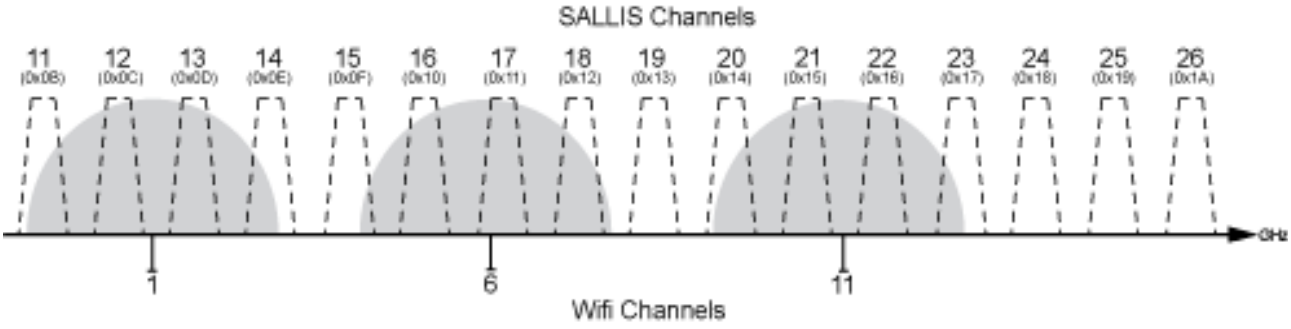
As an example, we can look at how Wi-Fi can affect the operation of SALLIS when it is operating on the same 2.4GHz band. Wi-Fi generally operates on a standard of the IEEE 802.11 communication protocol divided into 14 channels, each occupying 22MHz of bandwidth from 2412MHz to 2484MHz.



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 Wi-Fi network is using. With this information, you can see which of the SALLIS channels will be least affected by the Wi-Fi network. The diagram below shows that channels 11, 14, 15, 19, 20, 23, 24, 25 and 26 are the least likely to incur interference from the Wi-Fi network, so these would be the most effective channels to use for your SALLIS network.



SALLIS Wiring

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

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

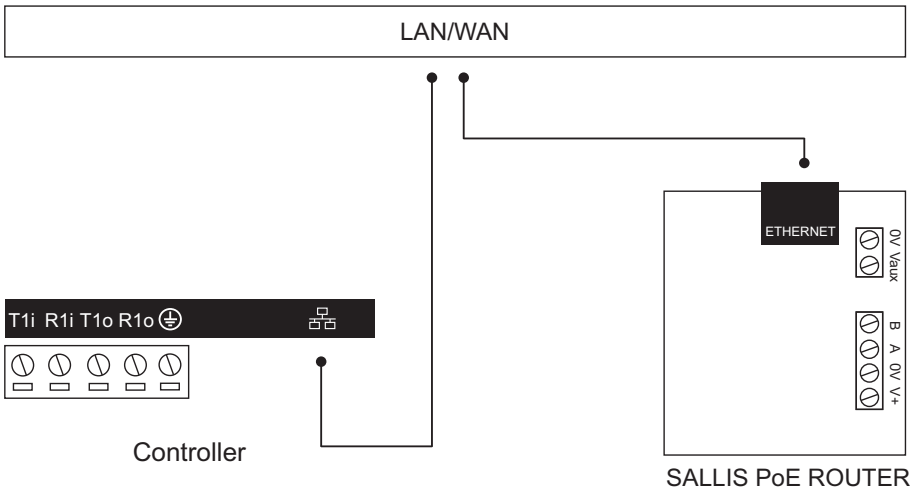
For instructions on how to wire a SALLIS node to a SALLIS router, and for a comprehensive list of the limitations (including wiring restrictions and requirements) that apply to the SALLIS hardware, consult your SALLIS installation manual.

PoE Router

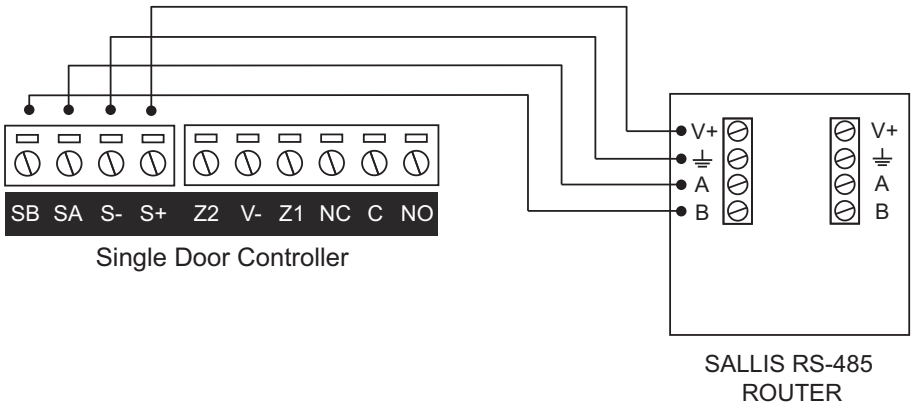
A SALLIS PoE router can control up to 64 locks. Protege controllers support connection to a SALLIS PoE router via a PoE switch, which provides the router with a power supply and a network connection.

If you are using a non-PoE switch, you can supply power to the router through an adapter that supplies 500mA at 12VDC. You can connect power supply directly to the router via the 0V and Vaux ports.

Controller to SALLIS PoE Router



Single Door Controller to SALLIS PoE Router

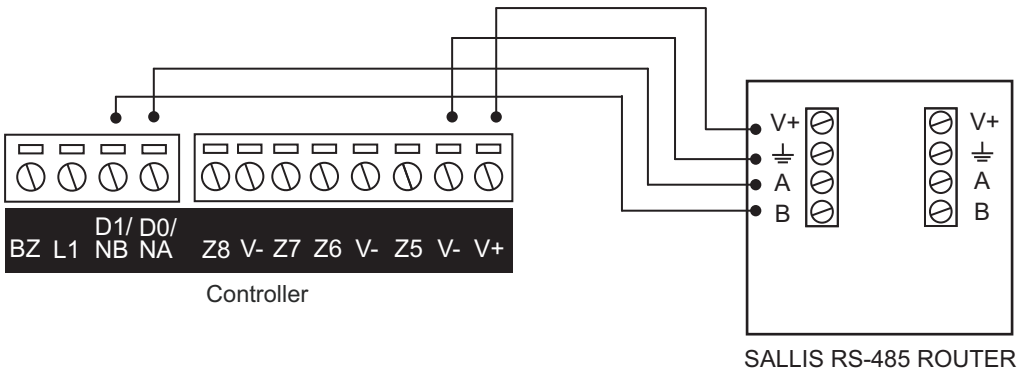


RS-485 Router

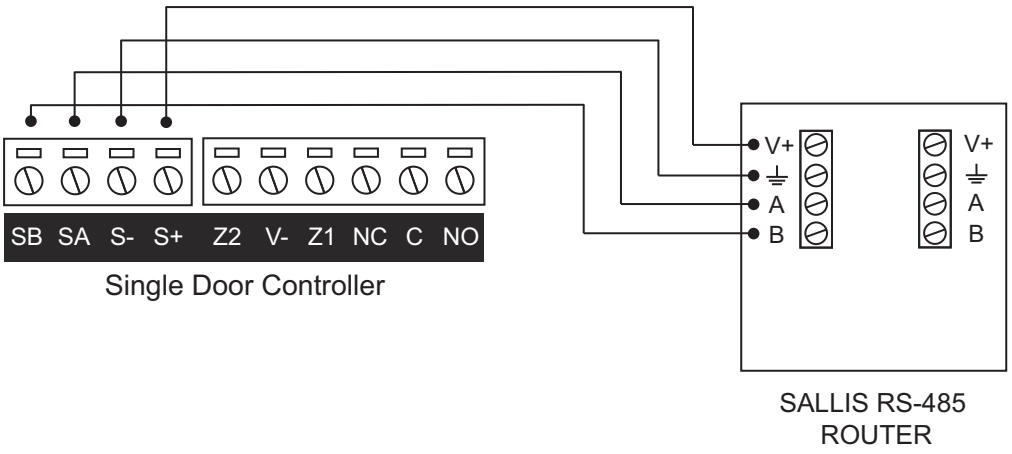
The SALLIS RS-485 router can control up to 16 locks. Protege controllers support connection to a SALLIS RS-485 router using one of the onboard RS-485 enabled network ports.

You can also supply power 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.

Controller to SALLIS RS-485 Router



Single Door Controller to SALLIS RS-485 Router



SALLIS Programming Application Setup

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

This integration supports software version **3.3.012**. 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

Each SALLIS router requires its own database file. To create a new 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. Authentication:
   - 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. If you are configuring a router to support encrypted cards programmed with Sector 13 MIFARE or ICT DESFire encoding, refer to the next topic.

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** as required.
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. For more information, see RF Channels (page 6).
7. Click **Save**.

Configuring the Router for Encrypted Card Operation

This section is specific to integrations requiring sector 13 MIFARE Classic programmed cards or ICT encrypted DESFire 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 encrypted cards on SALLIS wireless locks.

This ensures that the encrypted card number is read and recognized identically by both SALLIS wireless locks and ICT proximity readers.

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. Set the **AcCode** field to 16, as we expect 16 bytes for the encrypted data stored on the cards.

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. For more information, see RF Channels (page 6).

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. This 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.

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 as the **Configured Address** for the corresponding Protege smart reader record.
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. Disable the **Open to Last Card Accepted by the HOST** option. This is enabled by default, and when enabled only cards that have been presented to the lock in the days specified can open the door.
7. Click **Save**.

Programming Card Details for Sector 13 Encrypted Cards

This section is specific to integrations requiring sector 13 MIFARE Classic 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 MIFARE Classic programmed cards, follow the steps below to configure the card details.

1. Click **New Card**.
2. From the drop down, select MIFARE Classic.
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 **Sector Number** dropdown, select 13 .
8. Leave the **Block Number** set to 0.
9. Leave the **Key Type** set to A.

10. In the **Key** section, click the **[...]** 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**.

Programming Card Details for DESFire Encrypted Cards

This section is specific to integrations requiring ICT encrypted DESFire 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 ICT encrypted DESFire programmed cards, follow the steps below to configure the card details.

1. Click **New Card**.
2. From the drop down, select Desfire.
3. Enter a **Name** for the card.
4. Set the **Format** to Direct.
5. Leave the **Start address** set to 0.
6. Leave the **Size** set to 16.
7. In the **AID** field, enter the AID supplied by ICT, in reverse byte order.
   (i.e. if the supplied AID is F52313, you would enter 1323F5)
8. Leave the **Key Number** set to 0.
9. Leave the **File Number** set to 0.
10. Leave the **Comm. Settings** set to As indicated by card.
11. Set the **AMK type** to AES.
12. In the **Key** section, click the **[...]** button to program the predetermined DESFire Key supplied by ICT.
13. Enter the key into both the **Key** and **Confirm key** fields.
14. Click **OK**.
15. 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**.
4. Once the file has been synced, the information can be uploaded to the wireless locks.

The data remains valid on the PPD for 15 days.

Protege GX Setup

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

SALLIS PoE Router

Follow the steps below to configure the controller for connection with a SALLIS POE router.

Configuring the Onboard Reader Port

1. Navigate to **Expanders | Reader Expanders** and select the controller's **Onboard Reader**.
2. Set the **Ethernet Network Type** to SALLIS.
3. Enter the **Ethernet Port** that SALLIS will use to communicate with the controller. This can be configured on the SALLIS PoE router. The default is 1234.
4. Enter the **SALLIS Router IP** address.
5. Click **Save**.

Adding Smart Readers

Each SALLIS wireless lock needs to be added as a smart reader.

1. Navigate to **Expanders | Smart Readers** and select the controller that will communicate with the SALLIS router that this lock is connected to.
2. Click **Add** to create a smart reader that will represent a SALLIS lock.
3. Enter the **Name** for the lock.
4. Set the **Expander Address** to the **Physical Address** of the controller's onboard reader expander (in most cases 1).
5. Set the **Expander Port** to Ethernet.
6. Set the **Configured Address** of the lock, as assigned in the SALLIS application (see page 11).
7. Click **Save**.

Smart Reader Options

Additional programming for the locks can be configured in the **Reader** tab of the **Smart Readers** menu.

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 (such as 'door left open' events) will be logged.

- When the **Display Card Detail When Invalid** option is enabled, full card data will be displayed when a user attempts to access the lock with an invalid card. This allows you to right click on the event and assign the credential to a user.

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

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

If you are using encrypted cards and require the same AES encryption key to apply to all 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.

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

1. In the **Ethernet Card Data Options** section, enter the **Card Data AES Encryption Key** supplied by ICT.
2. Click **Save**.

Programming the AES Encryption Key (Individual SALLIS Locks)

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

If you are using encrypted cards and require the AES encryption key to only apply to specific SALLIS wireless locks, you need to enter the key into the **Card Data Options** section of the lock's corresponding smart reader record.

1. Navigate to the **Expanders | Smart Readers** and select the smart reader that represents the lock.
2. Select the **Reader** tab.
3. Ensure that the **Reader Format** is set to **HID 26/34 Bit**.
4. In the **Card Data Options** section, enter the **Card Data AES Encryption Key** supplied by ICT.
   - The **Read Non ICT Programmed Sector Data** option enables the reader / lock to read card sector data not programmed by ICT, but means that it 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.
5. Click **Save**.

SALLIS RS-485 Router

Follow the steps below to configure the controller for connection with a SALLIS RS-485 router.

Configuring the Onboard Reader Port

1. Navigate to **Expanders | Reader Expanders** and select the controller's **Onboard Reader**.
2. For the reader port that the SALLIS router is wired to, set the **Port Network Type** to **Salto SALLIS**.
3. Click **Save**.

Adding Smart Readers

Each SALLIS wireless lock needs to be added as a smart reader.

1. Navigate to **Expanders | Smart Readers** and select the controller that will communicate with the SALLIS router that this lock is connected to.
2. Click **Add** to create a smart reader that will represent a SALLIS lock.
3. Enter the **Name** for the lock.
4. Set the **Expander Address** to that of the controller's onboard reader expander (in most cases 1).
5. Set the **Expander Port** to the reader port the SALLIS router is wired to.
6. Set the **Configured Address** of the lock, as assigned in the SALLIS application (see page 11).
7. Click **Save**.

Smart Reader Options

Additional programming for the locks can be configured in the **Reader** tab of the **Smart Readers** menu.

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 (such as 'door left open' events) will be logged.
- When the **Display Card Detail When Invalid** option is enabled, full card data will be displayed when a user attempts to access the lock with an invalid card. This allows you to right click on the event and assign the credential to a user.

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

This section is specific to integrations requiring encrypted 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 RS-485 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 AES Encryption Key (Individual SALLIS Locks).

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**.
3. Select the corresponding **Reader** tab.
4. In the **Card Data Options** section, enter the **Card Data AES Encryption Key** supplied by ICT.

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

Programming the AES Encryption Key (Individual SALLIS Locks)

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

If you are using encrypted cards and require the AES encryption key to only apply to specific SALLIS wireless locks, you need to enter the key into the **Card Data Options** section of the lock's corresponding smart reader record.

1. Navigate to the **Expanders | Smart Readers** and select the smart reader that represents the lock.
2. Select the **Reader** tab.
3. Ensure that the **Reader Format** is set to **HID 26/34 Bit**.
4. In the **Card Data Options** section, enter the **Card Data AES Encryption Key** supplied by ICT.
   - The **Read Non ICT Programmed Sector Data** option enables the reader / lock to read card sector data not programmed by ICT, but means that it 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.
5. Click **Save**.

Programming Encrypted SALLIS Cards

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

Programming sector 13 MIFARE and ICT encrypted DESFire on SALLIS encoded cards is achieved using the ICT Encoder Client. For information on the steps required, refer to the ICT Encoder Client User Manual, or contact the ICT support team for assistance.

Supported Door Options

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

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

- SALLIS locks can be fully integrated with user access levels and access can be granted or denied based on doors, door groups and schedules.
- SALLIS locks can be configured 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 that 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 at a door is supported. Multi-badge arming is not supported.
- The supported SALLIS firmware does not provide up to date lock and door state feedback. As a result, when the lock is operating in restricted access mode, the status is displayed as Unknown.

Doors | General

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

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 such as a door pump.
- **Lock Activation Time**: Only supported for the lock output or output group defined above. The SALLIS lock programming will override this value.

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

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

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, via the SALLIS router they are connected to.

The linked inputs are:

Module Type	Input	Name	Description
Reader Expander	12	Offline	SALLIS PoE Router is offline with Protege GX.
Reader Expander	13	Offline	SALLIS RS-485 Router is offline with Protege GX.
Door (select appropriate SALLIS door)	1	Door Forced	One of the SALLIS locks has a door forced condition.
Door (select appropriate SALLIS door)	2	Door Left	One of the SALLIS locks has been left open.
Door (select appropriate SALLIS door)	4	Battery Low	A SALLIS lock has a low battery.
Door (select appropriate SALLIS door)	6	Door offline	A SALLIS lock is offline with the SALLIS router.

If any of the SALLIS door locks goes into one of the trouble states, the trouble input will activate. The reader log will record which lock triggered the trouble state.

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.