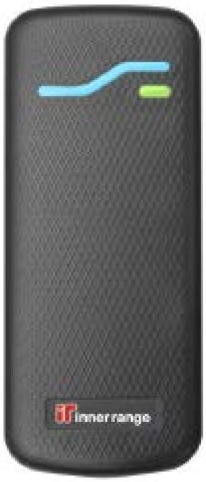
Version 5

integriti

INTEGRATED SOLUTIONS

Using SIFER readers



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

Introduction

The SIFER card reader is a smart card reader designed and manufactured by Inner Range. It is a multi-drop RS-485 based reader that employs 128 bit AES encryption from the card right through to the door module, providing a far superior level of security than that of traditional Wiegand based card readers. SIFER readers utilise the MIFARE DESfire EV1 card format.

As SIFER readers utilise a superset of the OSDP protocol, the readers may also be deployed on any system capable of using OSDP. Up to 16x SIFER readers may be connected to the dedicated RS-485 reader port on the Integriti Intelligent LAN Access Module (ILAM) or the Integriti Access Controller (IAC), or up to 4x SIFER readers may be connected to the Integriti Standard LAN Access Module (SLAM), for full reader-in/reader-out operation. SIFER readers are IP 67 rated and available with site specific encryption keys.

It is important to note that the first release version of the SIFER reader is restricted and specifically configured to support the Inner Range SIFER DESfire EV1 cards only. It is anticipated that subsequent versions of the SIFER reader will support the ability to read the CSN of other 13.56Mhz MIFARE based cards.

SIFER cards have a 7 Byte (56 bit) Card Serial Number (CSN) that can be used and read by other MIFARE based readers.

It is expected that SIFER readers and cards will be predominately deployed on new sites. For SIFER readers to be installed within an existing site, new Inner Range SIFER cards would need to be issued to all users.

The SIFER reader utilises the non-proprietary Open Supervised Device Protocol (OSDP) for bi-directional communication. Compared to Wiegand, OSDP is more secure, uses fewer wires, can be wired over a longer range and supports a multi-drop topology.

Please refer to the SIFER data sheet for detailed specifications, part numbers and other technical information. http://www.innerrange.com/pd/Card-Readers-Cards/Integriti-Readers/SIFER-Reader

The use of SIFER readers requires Integriti Controller firmware version 4.0.1 or later and Integriti software version 4.0.3 or later.

Reader serial numbers

SIFER readers have their own unique serial number printed on the back of the reader. This number is factory configured and cannot be changed. Please refer to the hardware installation manual for information on where to locate the serial number on the reader.

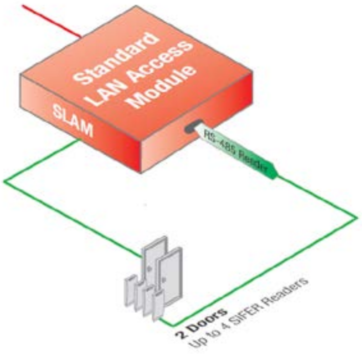
As SIFER readers are attached to an Integriti RS-485 reader port, the readers will automatically appear in Integriti System Designer software.

Reader connectivity

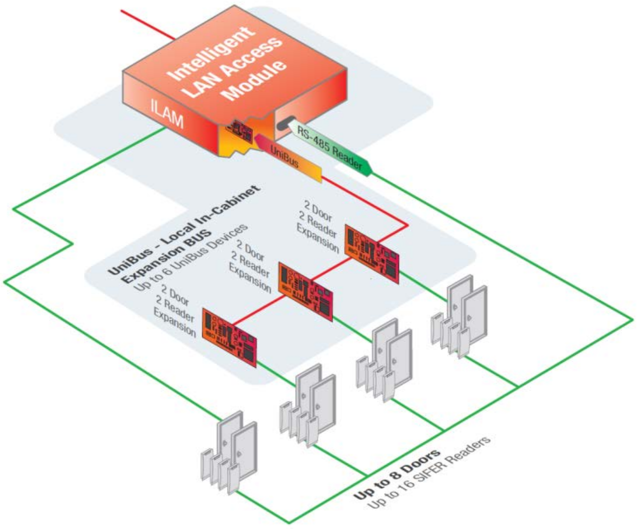
An Integriti Standard LAN Access Module (SLAM) accommodates 2x doors and 4x SIFER readers (or 2x Wiegand readers).

An Integriti Intelligent LAN Access Module (ILAM) accommodates up to 8x doors and 16x SIFER readers (or up to 8x Wiegand readers).

An Integriti Access Controller (IAC) accommodates up to 8x doors and 16x SIFER readers (or up to 8x Wiegand readers).

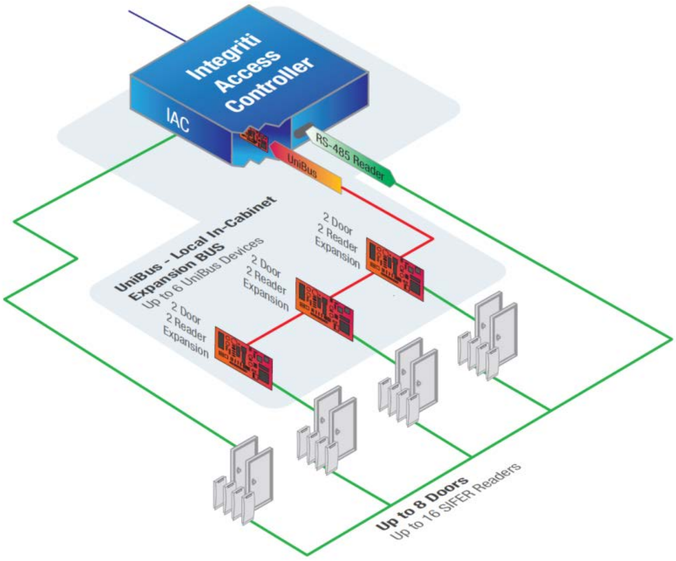


SLAM



Intelligent LAN Access Module
ILAM
RS-485 Reader
UniBus
UniBus - Local In-Cabinet Expansion BUS
Up to 6 UniBus Devices
2 Door 2 Reader Expansion
2 Door 2 Reader Expansion
2 Door 2 Reader Expansion
Up to 8 Doors
Up to 16 SIFER Readers

ILAM



Integriti Access Controller
IAC
RS-485 Reader
UniBus
UniBus - Local In-Cabinet Expansion BUS
Up to 6 UniBus Devices
2 Door 2 Reader Expansion
2 Door 2 Reader Expansion
2 Door 2 Reader Expansion
Up to 8 Doors
Up to 16 SIFER Readers

IAC

SIFER programmer (USB connected)

SIFER Programming Station (For Installer)

SIFER Enrolment Station (For End-User)

The SIFER Programming Station for installers comes with a small Windows® based application to enable card programming. The SIFER Enrolment Station is an optional accessory for end-users that connects to the Integriti client workstation for easy card enrolment.

SIFER card format

Card numbers are configurable to any number between 1 – 4.3 billion (4,294,967,295).

Site code numbers are configurable to any number between 1 – 16.7 million (16,777,215), with exception for site codes 1000-1099 (inclusive), which are reserved by Inner Range.

SIFER cards are 56 bits in length with 24 bits dedicated to the site code and 32 bits to the card number.

Bits:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Site Code:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Card Number:																				

Bits:	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
Site Code:	21	22	23	24																
Card Number:					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Bits:	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
Site Code:																
Card Number:	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

SIFER card & fob options

Three card and fob ordering options are available:

1. **SIFER-P**: Pre-programmed ‘stock’ cards with the card number printed. The most cost-effective option but card customisation is not allowed. With more than four billion card numbers available each SIFER-P card is guaranteed to be unique.

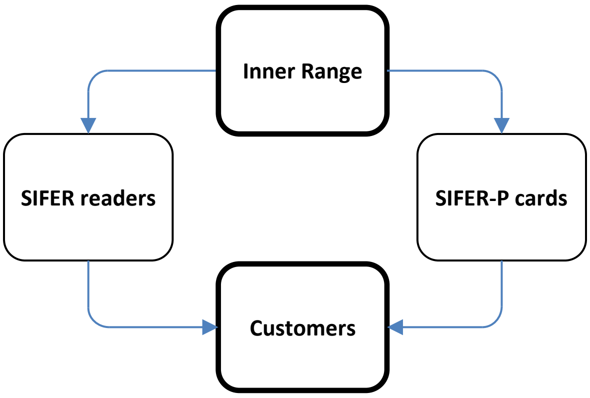
2. **SIFER-U**: User Programmable cards that allow an installer to customise the card number, site code and specify their own encryption key. Printed with the factory card number. A ‘Gold Card’ service for guaranteed unique encryption keys is also offered for SIFER-U.

3. **SIFER-C**: Custom batch orders configured by the factory according to the specified card number range, site code and printing options. A guaranteed unique encryption key is provided by Inner Range. SIFER-C cannot be re-programmed at a later stage by the installer or the factory.

The SIFER card type is easily identifiable via the “SIFER-P”, “SIFER-U” or “SIFER-C” tag physically printed on the card or fob.

1. SIFER-P (pre-programmed cards)

Inner Range sells SIFER readers and SIFER-P pre-programmed cards to customers.



SIFER-P cards are encrypted using the Inner Range SIFER Global Key.

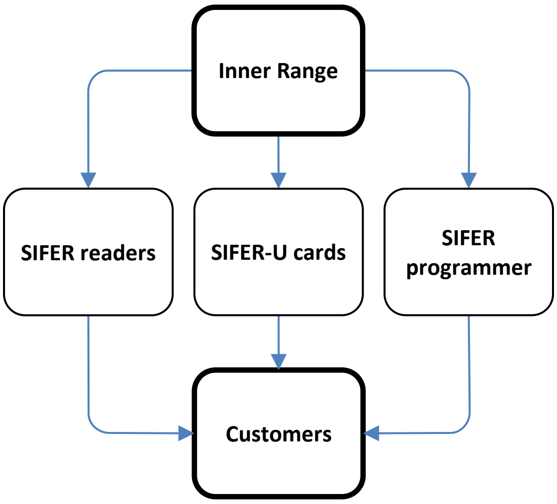
SIFER-P readers are pre-programmed to decrypt the Inner Range SIFER Global Key.

All SIFER-P cards are programmed by Inner Range with the Inner Range SIFER Global Key, a default site code of 1001 and a unique card number. Inner Range guarantees uniqueness of card numbers so that no two card numbers that leave the Inner Range factory will ever be duplicated. SIFER-P cards are 'locked' and do not allow any credential customisation.

All SIFER-P cards have the card number laser etched onto the card.

2. SIFER-U (user programmable cards)

Inner Range sells SIFER readers, SIFER-U user programmable cards and a SIFER programmer to the customer.



SIFER-U cards are programmed by Inner Range with the Inner Range SIFER Global Key, a default site code of 1001 and a unique card number. As opposed to SIFER-P cards, SIFER-U cards are 'unlocked' and allow credential customisation.

The SIFER Programmer allows the installer to encode card details of their own choosing, namely:

- Card Number
- Site Code
- Encryption Key (32 HEX Digits)

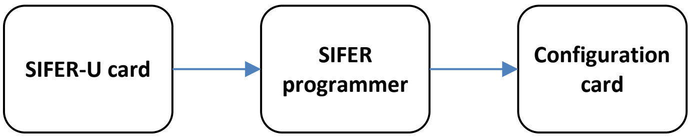
Whilst it is technically possible, it is not recommend that the installer change the card number because the card number is already unique when leaving the Inner Range factory and the card number is also laser etched onto the card. If desired, the installer may change the card number to any number between 1 – 4.3 billion (4,294,967,295).

The SIFER programmer mandates that a custom site code and custom encryption key must be applied for any card customisation. It is therefore not possible to retain the default site code of 1001 or the default Inner Range SIFER Global Key on customised cards.

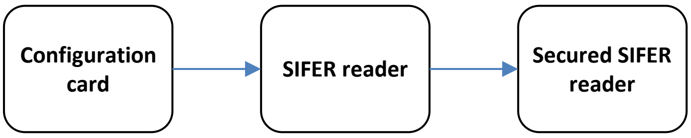
The custom site code may be any number between 1 – 16.7 million (16,777,215), with exception for site codes 1000-1099 (inclusive), which are reserved by Inner Range. The custom encryption key is generated from a 32 digit hexadecimal string that the installer assigns. Because a custom encryption key must be applied, the SIFER readers at the site must be updated to decrypt the new custom encryption key. A configuration card can be created by the SIFER Programmer to program the SIFER readers to operate with the new custom encryption key.

In this configuration, the installer will enter their custom site code and custom encryption key into the SIFER programmer using the provided software. The installer will then:

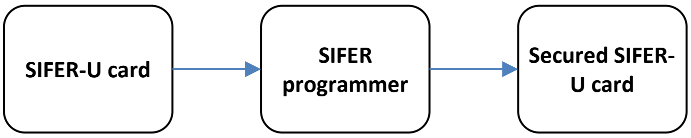
1. Create configuration cards out of SIFER-U user programmable cards to configure the SIFER readers on site with the custom encryption key



2. Secure the readers (with the custom encryption key) using configuration cards



3. Secure the user programmable cards by programming them with the custom site code and custom encryption key using the SIFER programmer



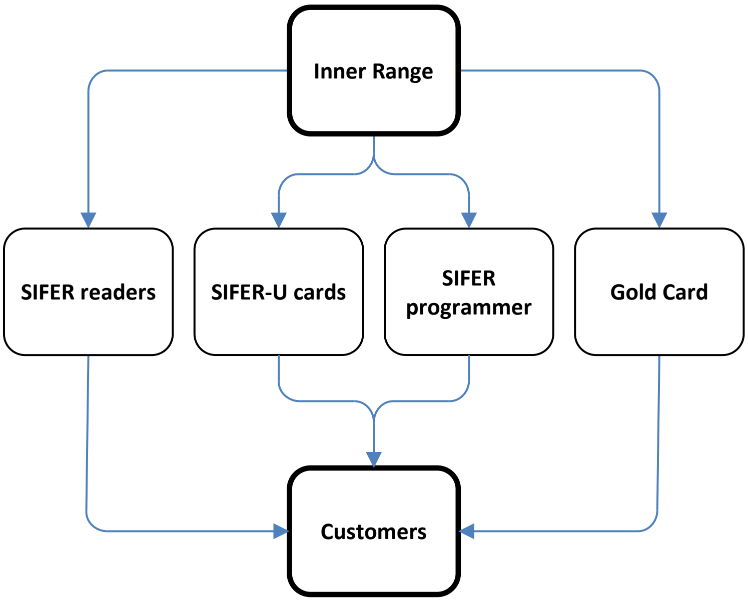
Once the SIFER readers have been configured with the custom encryption key, the SIFER readers will not be able to read SIFER-P pre-programmed cards, only secured SIFER-U cards that have had additional secured data added using the same custom encryption key.

SIFER-U Gold Card Service

As an alternative to the installer specifying a custom encryption key, Inner Range offers a 'Gold Card' service, providing the installer with a special Gold Key Configuration Card ('Gold Card'). The Gold Card delivers a guaranteed unique custom encryption key.

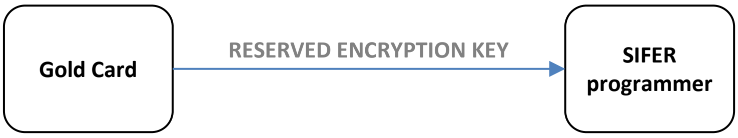
Inner Range assigns a unique encryption key allocated from the reserved 'Gold Card' range. The encryption key is then associated with the customer and site to facilitate future card orders. The encryption key is securely stored within Inner Range and protected in such a way that nobody (including Inner Range staff) can ever view the encryption key. Being a reserved key, the key can never be manually entered using a SIFER programmer.

Inner Range sells SIFER readers, SIFER-U user programmable cards, a SIFER programmer and a Gold Card to the customer.

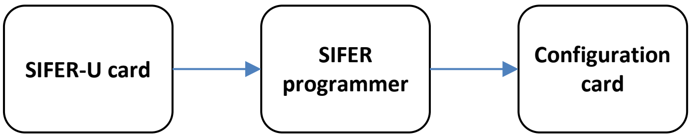


Installers:

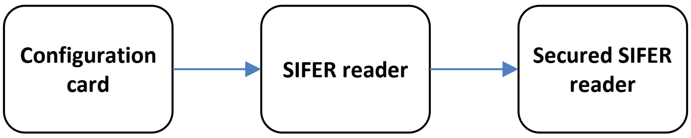
1. Use the Gold Card to input the reserved encryption key into the SIFER programmer



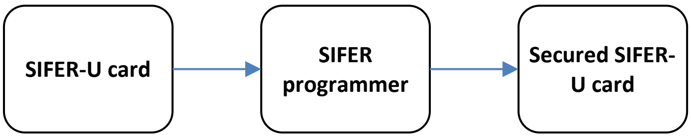
2. Create configuration cards out of SIFER-U user programmable cards to configure the SIFER readers on site with the reserved encryption key



3. Secure readers (with the reserved encryption key) using configuration cards



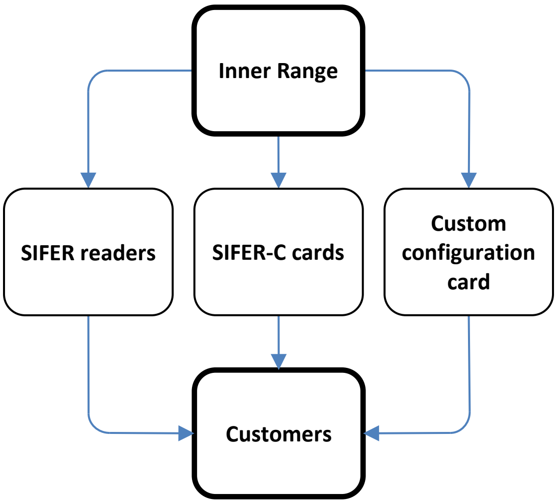
4. Secure the user programmable cards by programming them with the custom site code and the reserved encryption key using the SIFER programmer



The Gold Card, SIFER card programmer and any configuration cards created should be kept in a secure location because they hold the reserved encryption key.

3. SIFER-C (custom programmed cards)

Inner Range sells SIFER readers, SIFER-C custom programmed cards and, if required, a custom configuration card to the customer.



The SIFER-C ordering option allows a customer to place a custom batch order of cards with the factory. Inner Range shall configure the cards according to the specified card number range, site code and printing options.

SIFER-C cards cannot use the default Inner Range SIFER Global Key. When an initial order is made, Inner Range assigns a unique encryption key allocated from the reserved 'Gold Card' range. The encryption key is then associated with the customer and site to facilitate future card orders. The encryption key is securely stored within Inner Range and protected in such a way that nobody (including Inner Range staff) can ever view the encryption key. Being a reserved key, the key can never be manually entered using a SIFER programmer.

SIFER-C cards are created by the factory and are then permanently 'locked'. **It is important to note that SIFER-C cards cannot be re-programmed at a later stage by the installer or the factory**, as opposed to SIFER-U cards which permit re-programming.

A custom configuration card is supplied with the custom programmed cards, negating the need to use a SIFER programmer to create a configuration card. The Installer will then:

1. Secure the readers using the custom configuration card

Custom configuration card
SIFER reader
Secured SIFER reader

Understanding Configuration Cards

By default, SIFER readers are configured to only read cards with the Inner Range SIFER Global Key. A special configuration card can be created by the installer using the SIFER Programmer. This configuration card can then be used to reprogram the SIFER readers so that each reader on a site can operate with the corresponding new cards with the custom encryption key produced by the installer for that site.

SIFER readers are receptive to configuration cards for 5 minutes after power up. This time cannot be changed and the reader will remain receptive to configuration cards for the full 5 minutes, even if a configuration card has already been presented during the 5 minute period. During this period, the practice of presenting the configuration card twice within 5 seconds at each SIFER reader will program the reader with the updated custom encryption key.

When a configuration card is presented to a default reader in the 5 minute receptive period, the reader will beep, the main LED will turn purple and the small LED will flash purple for 5 seconds. If the configuration card is not presented again within the 5 seconds, the reader will simply revert to normal operation. If the configuration card is presented again within the 5 second period, the reader will change encryption key to the custom encryption key on the configuration card, the reader will beep and flash the main LED green for 1 second to confirm it is now secured.

Once a reader has been secured in this way, it can be un-secured with the same configuration card. If the correct configuration card is presented to a secured reader within the 5 minute receptive period, the reader will beep, the main LED will turn purple and the small LED will flash green (instead of purple) for 5 seconds. If the card is not presented again within 5 seconds, the reader will simply return to normal (secured) operation. If the configuration card is presented again within the 5 second period, the reader encryption key shall be converted back to the default Inner Range SIFER Global Key, the reader will beep and both LEDs will display green for 1 second to confirm it has now returned to the default state.

After the 5 minute receptive period has lapsed, any configuration cards (with the correct key) presented will cause 3 seconds of continuous tone and red flashing main LED indicating that use of the configuration card is not allowed.

Adding a SIFER reader to a door

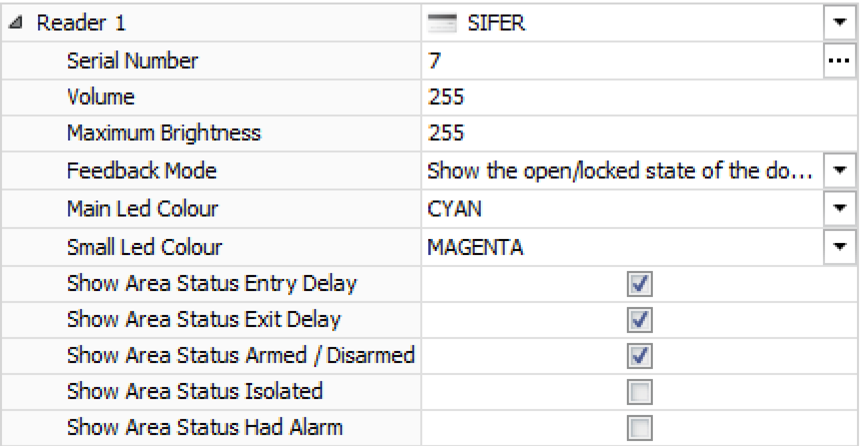
When SIFER readers are attached to an Integriti module, the readers will automatically address and come online if the following conditions are met:

- The reader module has at least one spare slot (a reader slot set to 'None').
- The total number of SIFER readers supported by the reader has not been exceeded.
- The *OSDP Options* » *OSDP_DisableAutoAddressing* option is not ticked.
- None of the readers are non-OSDP serial readers (e.g. Salto or Aperio).

Check the hardware manual for the reader module to determine the total number of SIFER readers supported.

SIFER reader configuration options

Allow approximately 10 seconds for SIFER reader programming changes to take effect.



Reader 1	SIFER
Serial Number	7
Volume	255
Maximum Brightness	255
Feedback Mode	Show the open/locked state of the do…
Main Led Colour	CYAN
Small Led Colour	MAGENTA
Show Area Status Entry Delay	☑
Show Area Status Exit Delay	☑
Show Area Status Armed / Disarmed	☑
Show Area Status Isolated	□
Show Area Status Had Alarm	□

Option	Description
`Serial Number`	The serial number of the SIFER reader. Please refer to the hardware installation manual for information on where to locate the serial number on the reader.
`Volume`	Configurable between 0 (off) and 255 (loudest).
`Maximum brightness`	Configurable between 0 (off) and 255 (brightest).

Feedback Mode	The five options available are: - (None) - Show the area state of the area specified by 'Keypad Area' item. - Show the area state of the area on the same side of the door as this reader. - Show the area state on the other side of the door to this reader. - Show the open/locked state of the door associated with this reader.
Main LED colour	Select from 1 of 23 colours (including black / off)
Small LED colour	Select from 1 of 23 colours (including black / off)
Show area status entry delay (Small LED)	If the 'Feedback Mode' has been set to show an area state and this option is enabled, the reader will slow flash green and play a slow chime sound.
Show area status exit delay (Small LED)	If the 'Feedback Mode' has been set to show an area state and this option is enabled, the reader will slow flash green and play a slow chime sound.
Show area status armed / disarmed (Small LED)	If the 'Feedback Mode' has been set to show an area state and this option is enabled, the reader will show green for disarmed and red for armed.
Show area status isolated (Small LED)	If the 'Feedback Mode' has been set to show an area state and this option is enabled, the reader will show amber when an input is isolated.
Show area status had alarm (Small LED)	If the 'Feedback Mode' has been set to show an area state and this option is enabled, the reader will fast flash red and play a repeating two tone chime sound.

SIFER heartbeat monitoring

SIFER readers may be monitored for their connection state. In this way, an alarm can be raised if a reader loses connection with the host door module.

All SIFER readers have a dedicated system input. These system inputs can be assigned to a system area for alarm processing should any input go into the alarm state. The reader fault system inputs are mapped as follows:

Integriti Standard LAN Access Module (SLAM)

- Rxx:S19 – Reader 1 and Reader 3
- Rxx:S20 – Reader 2 and Reader 4

Integriti Intelligent LAN Access Module (ILAM)

- Ixx:S69 – Reader 1
- Ixx:S70 – Reader 2
- Ixx:S71 – Reader 3
- Ixx:S72 – Reader 4
- Ixx:S73 – Reader 5
- Ixx:S74 – Reader 6
- Ixx:S75 – Reader 7
- Ixx:S76 – Reader 8
- Ixx:S77 – Reader 9
- Ixx:S78 – Reader 10
- Ixx:S79 – Reader 11
- Ixx:S80 – Reader 12
- Ixx:S81 – Reader 13
- Ixx:S82 – Reader 14
- Ixx:S83 – Reader 15
- Ixx:S84 – Reader 16

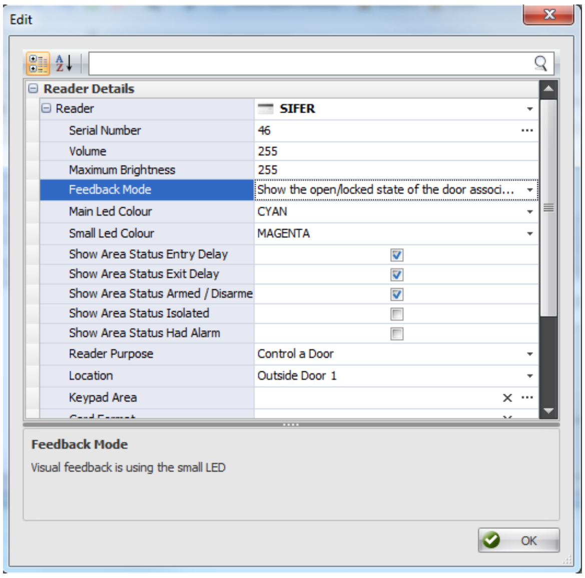
Integriti Access Controller (IAC)

- C01:S90 – Reader 1
- C01:S91 – Reader 2
- C01:S92 – Reader 3
- C01:S93 – Reader 4
- C01:S94 – Reader 5
- C01:S95 – Reader 6
- C01:S96 – Reader 7
- C01:S97 – Reader 8
- C01:S98 – Reader 9
- C01:S99 – Reader 10
- C01:S100 – Reader 11
- C01:S101 – Reader 12
- C01:S102 – Reader 13
- C01:S103 – Reader 14
- C01:S104 – Reader 15
- C01:S105 – Reader 16

Using SIFER as DOTL buzzer

SIFER readers have an in-built buzzer than can be used as a local Door Open Too Long (DOTL) annunciator. This may negate the need to purchase and install a separate buzzer.

Within the reader module programming, change the “Feedback Mode” to “Show the open/locked state of the door associated with this reader”. Then within the door programming, change the “Door Open Too Long Time” to a value greater than the default of 0 seconds.

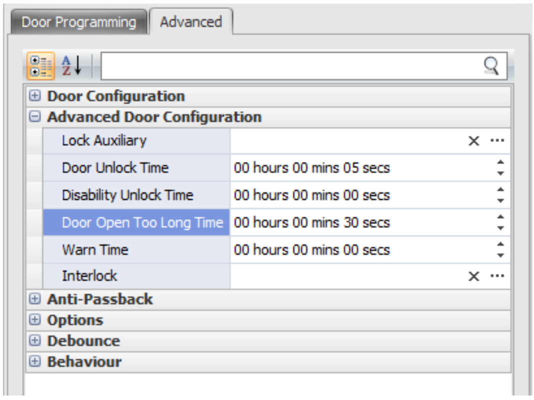


Reader Details

Reader	SIFER
Serial Number	46
Volume	255
Maximum Brightness	255
Feedback Mode	Show the open/locked state of the door associ...
Main Led Colour	CYAN
Small Led Colour	MAGENTA
Show Area Status Entry Delay	☑
Show Area Status Exit Delay	☑
Show Area Status Armed / Disarme	☑
Show Area Status Isolated	☐
Show Area Status Had Alarm	☐
Reader Purpose	Control a Door
Location	Outside Door 1
Keypad Area	

Feedback Mode

Visual feedback is using the small LED



Door Configuration

Advanced Door Configuration

Lock Auxiliary	
Door Unlock Time	00 hours 00 mins 05 secs
Disability Unlock Time	00 hours 00 mins 00 secs
Door Open Too Long Time	00 hours 00 mins 30 secs
Warn Time	00 hours 00 mins 00 secs
Interlock	

Anti-Passback

Options

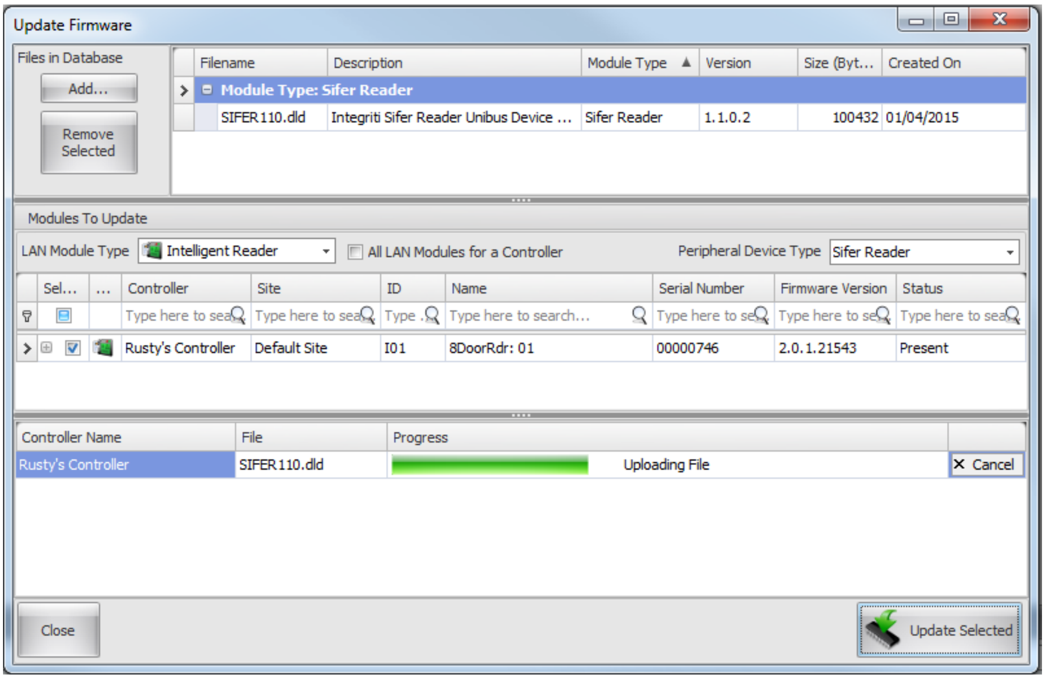
Debounce

Behaviour

If successfully configured, the SIFER reader associated with the door should provide a continuous pulsating tone when the DOTL system input is in alarm. When the DOTL system input has been restored (i.e. door is closed and reed switch is sealed), the buzzing will immediately stop.

SIFER firmware update

The firmware in SIFER readers may be updated through Integriti software in the same process used to update Integriti hardware modules. The update process will take approximately 10 minutes. Select the SIFER firmware file, choose the appropriate reader module type under “LAN Module Type”, under “Peripheral Device Type” choose “SIFER Reader”, tick the Controller to send the firmware file to and then select “Update Selected”.



Filename	Description	Module Type	Version	Size (Byt...	Created On
Module Type: Sifer Reader					
SIFER110.dld	Integriti Sifer Reader Unibus Device ...	Sifer Reader	1.1.0.2	100432	01/04/2015

LAN Module Type: Intelligent Reader □ All LAN Modules for a Controller Peripheral Device Type: Sifer Reader

Sel...	...	Controller	Site	ID	Name	Serial Number	Firmware Version	Status
☑		Rusty's Controller	Default Site	I01	8DoorRdr: 01	00000746	2.0.1.21543	Present

Controller Name	File	Progress
Rusty's Controller	SIFER110.dld	Uploading File

SIFER reader states

State	Description
Powered on.	• Reader Beep. • Single green flash.
Powered, waiting for address / unaddressed / unable to communicate with the controller.	• The main LED will alternate between White and Grey. • The small LED will fade in and out blue.
Powered, online.	• The reader will play an ascending ‘online’ tone. • The main LED will be cyan. *Note: This value can be changed.* • The small LED will be magenta. *Note: This value can be changed.*

Common problems

Begin by reviewing the hardware installation manual.

- Ensure the readers have been installed correctly according to the hardware manual.
- Make sure the readers have been connected to the correct port on the reader module.

Make sure the Integriti software, module firmware and SIFER firmware are up to date. Please refer to section 10.3 – ‘Maintaining Firmware’ of the ‘System Configuration Handbook’ for more details.

Problem	Resolution
SIFER reader does not appear in the Inside / Outside Reader drop down options. **SIFER reader is not getting an address / has not played ‘online’ tone.**	• Ensure the Door record you are configuring belongs to the controller that the reader is attached to. • Check the reader is attached to a reader “RDR RS-485” port. • Make sure you have not exceeded the total number of readers the module supports. • The ‘OSDP_DisableAutoAddressing’ option should be un-ticked. • Ensure the firmware on the controller and readers are up to date. • Cycle power to the SIFER reader.
SIFER reader is not updating when I change settings.	• Make sure your controller, module and software versions are all up to date. • Check the supported number of readers for the module has not been exceeded. • Changes can take roughly 10 seconds.
Enrolment fails.	• Confirm the controller firmware revision is compatible with the Integriti version you are using.
Reader is not responding to SIFER cards.	• Ensure the cards and readers are configured to use the same security key.