Mullion Reader

User Manual

VR50M-MF **VR20M-MF**

VANDERBILT

Document ID: A-100410-e

Edition date: 16.06.2022

Data and design subject to change without notice. / Supply subject to availability.

© 2022 Copyright by Vanderbilt

We reserve all rights in this document and in the subject thereof. By acceptance of the document the recipient acknowledges these rights and undertakes not to publish the document nor the subject thereof in full or in part, nor to make them available to any third party without our prior express written authorization, nor to use it for any purpose other than for which it was delivered to him.

MIFARE and MIFARE Classic are trademarks of NXP B.V.

MIFARE DESFire are registered trademarks of NXP B.V. and are used under license.

Hereby, Vanderbilt International (IRL) Ltd declares that this equipment type is in compliance with the following EU Directives for CE marking:
• Directive 2014/30/EU (Electromagnetic Compatibility Directive)
• Directive 2014/53/EU (Radio Equipment Directive)
• Directive 2011/65/EU (Restriction of the use of certain hazardous substances Directive)
The full text of the EU declaration of conformity is available at: http://van.fyi?Link=DoC

DA
DE
EN
ES
FR
SV

http://van.fyi?Link=Mullion_Reader

Table of Contents

1 Introduction

The VR20M-MFand VR50M-MF are mullion-mount card readers with modern anti-hacking security over OSDP and support for the traditional Wiegand protocol. When installed as part of a secure system over OSDP, the communication from the reader or the controller they are connected to cannot be compromised. The readers are made of hard wearing materials and will endure most weather conditions. The readers are easy to mount and can be mounted on a flat surface. The readers can be cleaned with most kinds of domestic detergents. All readers have a multicolour light frame. The VR50M-MF has a keypad for PIN code.

2 Technical data

	VR20M-MF	VR50M-MF
Protocol	OSDP or Wiegand	OSDP or Wiegand
Interface to controller	RS485 or Wiegand	RS485 or Wiegand
Operating voltage (Rated voltage 12-24 VDC)	8.5 – 30.0VDC	8.5 – 30.0VDC
Power consumption	DC 12V 43mA Peak 168mA DC 24V 26mA Peak 100mA	DC 12V 60mA Peak 220mA DC 24V 40mA Peak 125mA
Tamper protection	Yes	Yes
Card technology	MIFARE™	MIFARE
Card compatibility	MIFARE Classic MIFARE Plus MIFARE DESFire EV1/ EV2	MIFARE Classic MIFARE Plus MIFARE DESFire EV1/ EV2
Reading distance	MIFARE Classic-up to 6 cm MIFARE Plus-up to 6 cm MIFARE DESfire EV1/ EV2-the card must be held to the reader	MIFARE Classic-up to 6 cm MIFARE Plus-up to 6 cm MIFARE DESfire EV1/ EV2-the card must be held to the reader
Indicators	3 x LED (red/yellow/green) 1 x Buzzer Multicolour light frame	3 x LED (red/yellow/green) 1 x Buzzer Multicolour light frame
Keypad	No	Yes
Operating temperature	- 40°C to + 70°C	- 40°C to + 70°C
IP rating	IP55	IP55
IK class	08	08
Housing	Zinc cast metal bezel with polycarbonate plastic front	Zinc cast metal bezel with polycarbonate plastic front
Color	Black, matt chrome	Black, matt chrome
Dimensions (WxHxD) mm	Surface mounted: 48 x 129 x 22	Surface mounted: 48 x 129 x 24
Weight	219g	225g
Serviceable parts	None	None
Standards	EN50131-3:2009, Grade 3, Class III SSF1014:5, Grade 3, Class III	EN50131-3:2009, Grade 3, Class III SSF1014:5, Grade 3, Class III

Cable length guide

Mode	Max. Cable Length	Cable
OSDP	1 km.	Screened twisted pair (For example; Belden 9501)
Wiegand	30m	Screened multicore (For example; Belden 9538)

3 Safety regulations

General

- Follow all warnings and instructions marked on the device.
- Keep this document for reference purposes.
- Please consider any additional country-specific, local laws, safety standards, or regulations concerning installation, operation, and disposal of the product.

Liability claim

- Do not make any changes or modifications to the device.
- Use only spare parts and accessories that have been approved by the manufacturer.

3.1 UL Compliance

This device complies with UL 294.

Operation is subject to the following conditions:

- The reader shall be connected to a compatible UL 294 listed control unit. The readers have been UL evaluated with the AC5102 control unit.
- This device must be powered from power limited/class 2 supply.

Warning

Changes or modifications not expressly approved by the party responsible for compliance could void the User`s authority to operate the equipment.

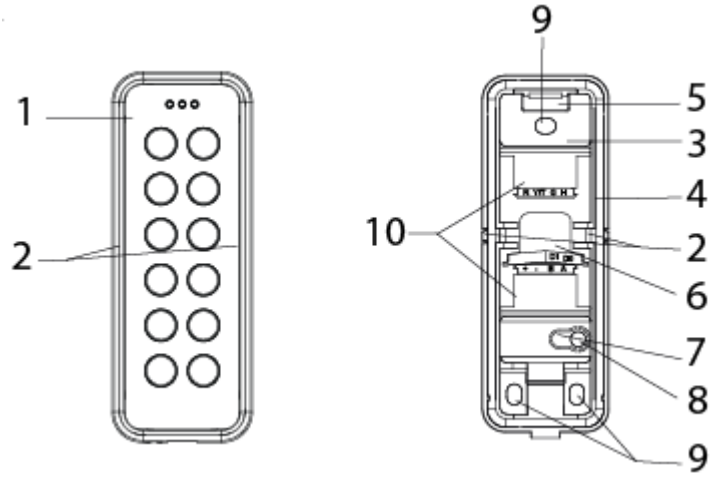
Performance levels per UL294 are

- Destructive attack – Level I
- Line Security – Level I
- Endurance – Level IV
- Standby – Level I

4 Reader components and package contents

The following diagrams identify the reader components and the items that come packaged with the reader.

4.1 Reader components



1	Front	**6**	Location where cables can come through the back
2	Knockouts x 2	**7**	Tamper base
3	Base	**8**	Screw for tamper protection
4	Gasket	**9**	Mounting holes
5	Hook	**10**	Upper and lower terminal block locations

4.2 Package contents

1	+ - B A terminal block for OSDP and Wiegand (lower terminal block)
2	R Y/T G H terminal block for Wiegand (upper terminal block)
3	Mounting/Tamper screws
4	Cover screw
5	Opening tool

5 Mounting and connecting

The mullion readers are surface-mounted readers. The readers can be mounted with cables led through the back of the unit or led in from either side through knockout gaps.

For wiring details please refer to:

- *Connecting the cables* on page 13.

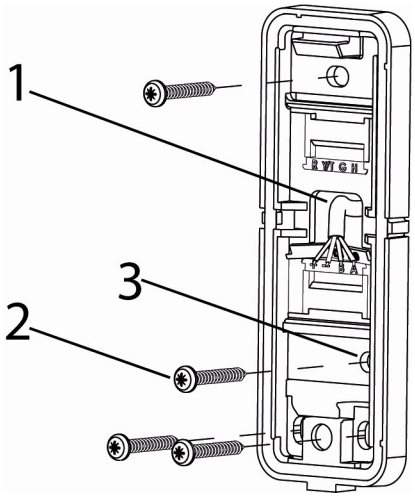
5.1 Mounting a reader

To ensure a close fit, mount the reader on a flat surface (mounting surface should not have depths or deviations of > 1mm).

Seal the cable entry through the base gasket with silicon to avoid ingress of dust, water, and draft. Endure that there is no silicon between the wall and the gasket, remove residue sealant if necessary.

To attach the base to a surface:

1. Make a small hole in the back of the base gasket (item 1 in the diagram below). Use this hole to feed the cable through the gasket and into the reader base.
2. Remove the fabric around the cable entry point on the back of the reader to avoid water channeling to the inside of the reader.
3. Attach the base to the wall with three screws: one in the middle at the top of the base, and one in each of the corners at the bottom of the base.



1	Cable entry through base gasket
2	Tamper screw
3	Tamper base

4. If tamper protection is required, fix the screw (item 2) into the tamper base (item 3). Do not over-tighten the screw as this can damage the tamper base.
5. Continue to follow the instructions detailed in *Connecting the cables* on page 13.

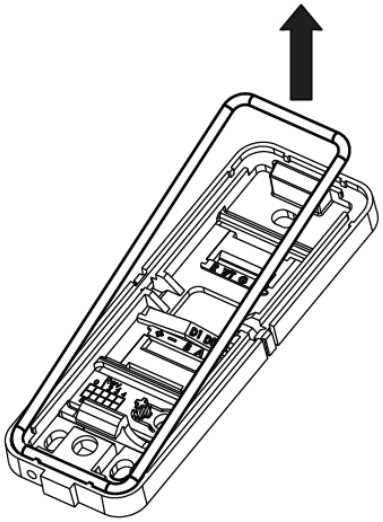
5.2 Mounting a reader with cables fed from the side

Warning

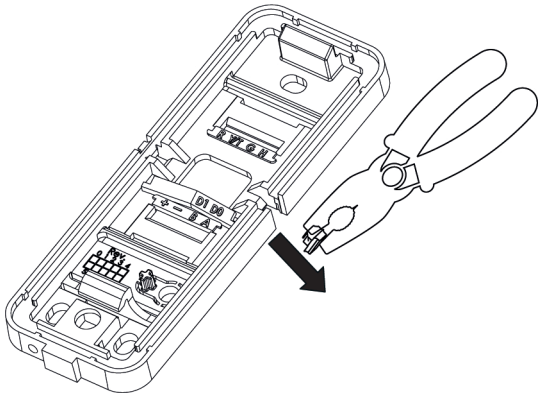
Mounting the unit with the cable led in from either side through knockout gaps does not comply with UL 294.

If the cables are fed from the side:

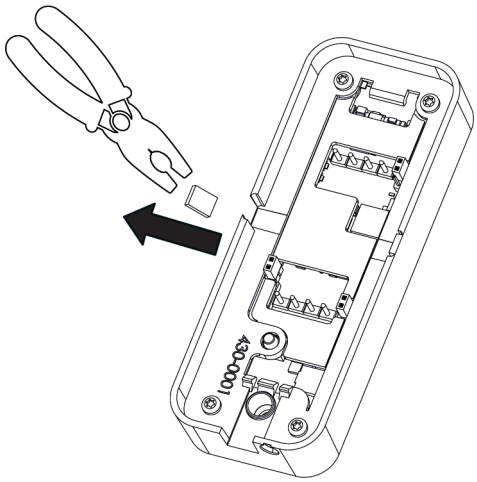
1. Remove the gasket from the base.



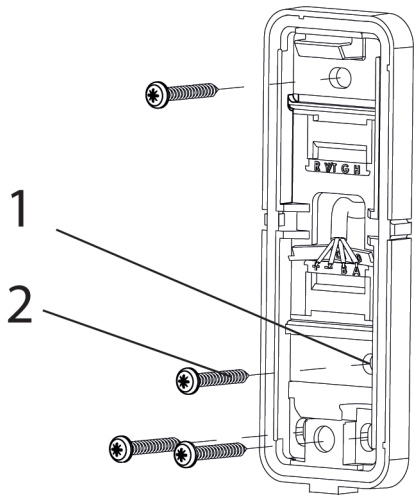
2. Identify which of the knockouts the cables should be fed through.
3. Use a pliers to pull the knockout away from the base.



4. Remove the corresponding knockout on the cover.



5. Attach the base to the wall with three screws: one in the middle at the top of the base and one in each of the corners at the bottom of the base.



1	Tamper base
2	Tamper screw

6. If tamper protection is required, fix the screw into the hole on the tamper base. Do not over tighten the screw as this can damage the tamper base.
7. Feed the cables through the opening and reinsert the gasket. Follow the instructions for *Connecting the cables* on the next page.

Vanderbilt recommend sealing the gap that the knockout creates with a silicon sealant. Do this after you have closed the reader. Please note that a reader with a removed knockout does not meet the standard for IP 55.

5.3 Connecting the cables

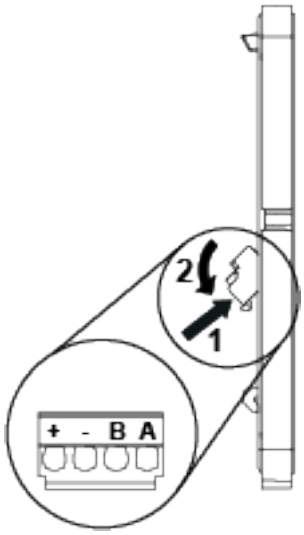
5.3.1 Connecting the reader in OSDP mode

Use the terminal block marked +-BA (see item 1 in *Package contents* on page 9) and a twisted screened cable with min. 2 pairs to connect the cables in OSDP mode.

1. Attach the cables according to the respective indicators on the second, +-BA terminal block (lower terminal block) and the base:

Reader	Controller
+	+12V
-	0V
B	B
A	A

2. Insert the ridge on the end of the terminal block marked +-BA into the slot marked +,-,B,A.



3. Gently push the terminal block towards the base until it clicks.
4. Push the cables back.

Please note that you must set the Jumpers to configure your application.

For more information on setting the Jumpers in OSDP mode see *Setting the Jumpers for OSDP* on page 16.

For more information on setting the Jumpers in Wiegand mode see *Setting the Jumpers for Wiegand* on page 17.

On the reverse of the front plate, Jumper 3 is used to determine EOL (see the diagram in *Connecting the cables* above). By default EOL is ON and the reader acts as the last reader on the bus. However, if the reader is an intermediate reader on the bus, Jumper 3 must be removed.

5.3.2 Connecting the reader in Wiegand mode

Use the terminal blocks marked +-BA and RY/TGH (see item 1, item 2 in *Package contents* on page 9) and a twisted screened multicore cable (4 pairs + screen) such as Belden 9538 to connect the reader in

Wiegand mode.

1. Attach the cables according to the respective indicators on the communication and power terminal block (+-BA terminal block (lower terminal block)):

Reader	Controller
+	+12V
-	0V
B	Wiegand D1
A	Wiegand D0

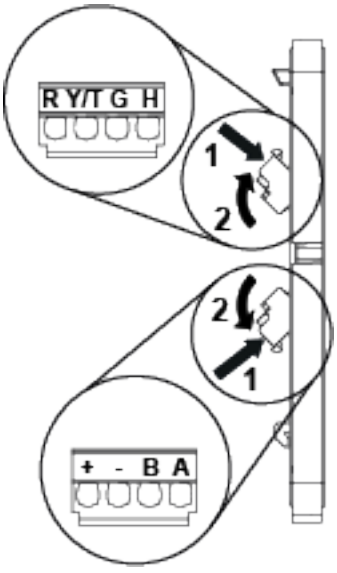
2. Attach the cables on the LED, tamper, and horn terminal block (RY/TGH terminal block (upper terminal block)):

Reader	Controller (Generic)	Controller (SPC)	Controller (ACT)
R	Red LED	VO1	Red
Y/T*	Tamper input	Zone Input (tamper)[1]	Tamper input[1]
G	Green LED	VA1	Green
H	Buzzer output	System Output[1]	Buzzer output[1]
*The Tamper output (default setting) connection may alternatively be configured to provide a Yellow input to the reader. The Tamper output/ Yellow input options are mutually exclusive.			
[1]This connection is optional.			

When the tamper output option is configured there is no yellow indication input. In this instance, you can turn on the yellow indication LED by setting both the red and green indication inputs low. Both the red and green indication LEDs are turned off at this time.

The buzzer is activated by setting the horn input low. The buzzer is deactivated by setting the horn input high.

3. Insert the ridge on the end of the upper or lower terminal block into the corresponding slot.

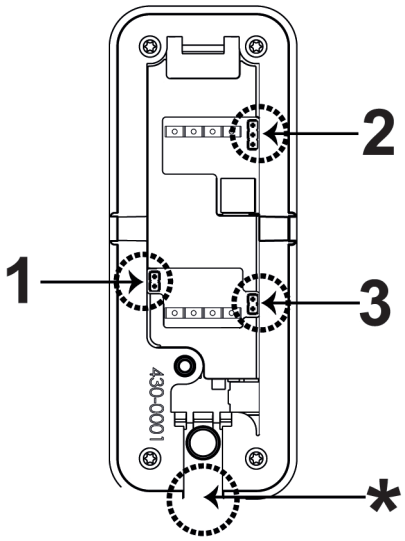


4. Gently push the terminal block towards the base until it clicks.
5. Remove the Jumper 3 (see the diagram in *Connecting the cables* on page 13). Jumper 3 is used to determine EOL. By default the reader has EOL ON. EOL is always off in Wiegand mode.

Please note that you must set the Jumpers to configure your application. For more information on setting the Jumpers in Wiegand mode see *Setting the Jumpers for Wiegand* on page 17.

5.4 Setting the Jumpers

There are three jumpers inside the front of the reader. Use the jumpers to set the reader to OSDP or Wiegand mode, to set OSDP Addressing or Wiegand format, and to set the End Of Line (EOL) status for the reader.

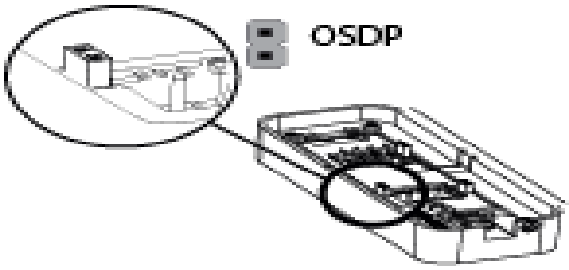


1	Set reader to OSDP or Wiegand mode
2	Set OSDP addressing or Wiegand formats
3	Set End Of Line (EOL) status for the reader
*****	This indicates the bottom of the reader

5.5 Setting the Jumpers for OSDP

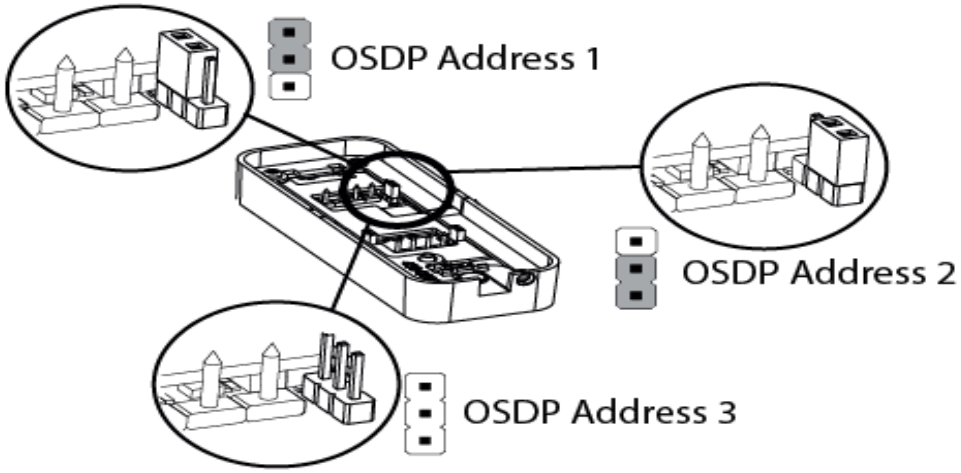
The diagrams below show how to position the Jumpers to get the desired functions from the terminal blocks. Note that the EOL is ON for a sole reader or for the last reader on the RS485 bus.

Jumper 1



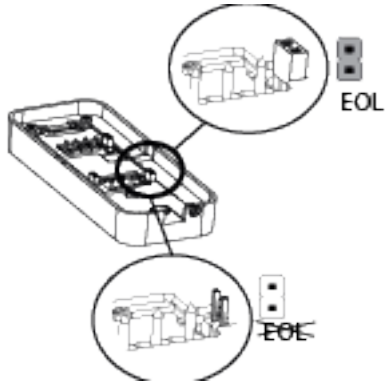
Jumper 1 is ON to select OSDP.

Jumper 2



- Jumper 2 is ON the first two pins for OSDP Address 1.
- Jumper 2 is ON the bottom two pins for OSDP Address 2.
- Jumper 2 is OFF for OSDP Programmable Address.

Jumper 3



- Jumper 3 is ON to enable EOL.
- Jumper 3 is OFF to disable EOL.

5.6 Setting the Jumpers for Wiegand

By default, the VR20 and VR50 Mullion readers are configured to transmit standard mode 32 Bit Wiegand, 37 Bit Wiegand, or 56 Bit Wiegand.

Some installations may require transmission in Reverse Mode for 26 Bit Wiegand, 32 Bit Wiegand or 56 Bit Wiegand.

If you are adding this reader to an existing Reverse Mode installation, you must follow the procedure to program the reader to Reverse Mode Wiegand.

For more information, please refer to:

- *Reverse mode Wiegand* on page 19.

If the existing installation uses 26 Bit Wiegand, you must follow the additional procedure to program the reader to transmit in Reverse Mode 26 Bit Wiegand.

For more information, please refer to:

- *Reverse mode Wiegand* on the next page.

Only one of the two modes may be configured at a time.

Wiegand - Standard mode transmission

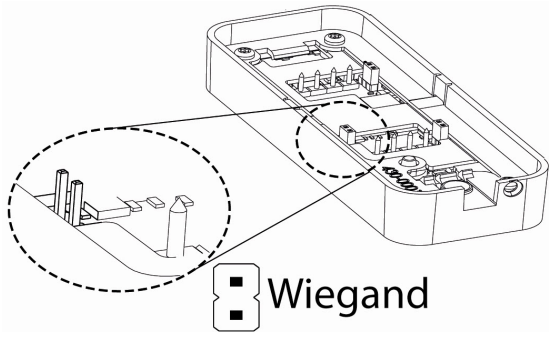
Wiegand	Standard transmission	Re-program necessary
56 Bit	Yes	No
37 Bit	Yes	No
32 Bit	Yes	No
26 Bit	No	

Wiegand - Reverse mode transmission

Wiegand	Reverse mode transmission	Re-program necessary	Procedure	Mandatory additional procedure
56 Bit	Yes	Yes	*Programming a reader for reverse mode transmission* on page 20	No
37 Bit	No			
32 Bit	Yes	Yes	*Programming a reader for reverse mode transmission* on page 20	No
26 Bit	Yes	Yes	*Programming a reader for reverse mode transmission* on page 20	*Programming a Reverse mode transmission reader for 26 Bit Wiegand* on page 20

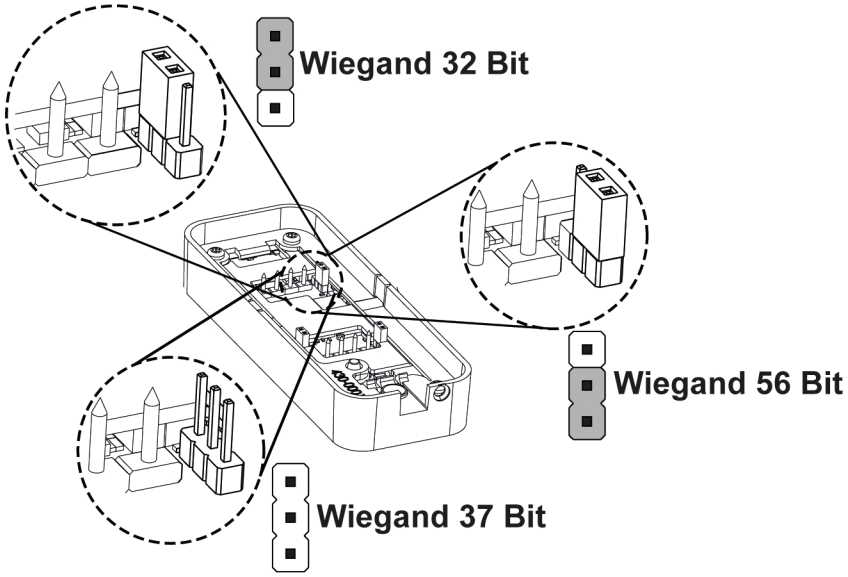
The diagrams below show how to position the Jumpers to get the desired functions from the terminal blocks. Note that in Wiegand mode EOL is not fitted. Wiegand can be set at 32 bit, 37 bit, or 56 bit.

Jumper 1



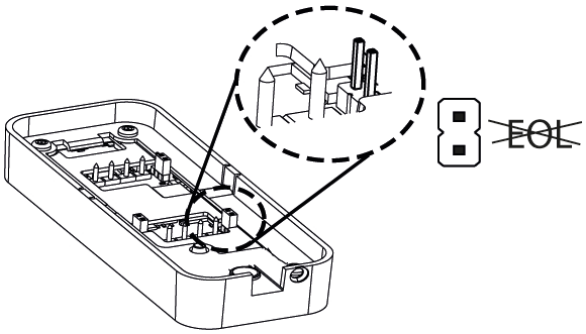
Jumper 1 is OFF to select Wiegand.

Jumper 2



- Jumper 2 is ON the first two pins for Wiegand 32 bit.
- Jumper 2 is ON the bottom two pins for Wiegand 56 bit.
- Jumper 2 is OFF for Wiegand 37 bit.

Jumper 3



- Jumper 3 is OFF to disable EOL.
- Jumper 3 is always OFF in Wiegand mode.

5.7 Reverse mode Wiegand

Some installations may require transmission in Reverse Mode for 26 Bit Wiegand, 32 Bit Wiegand or 56 Bit Wiegand.

To add a reader to an existing Reverse Mode installation, you must follow the procedure to program the reader to Reverse Mode Wiegand. For more information, see *Programming a reader for reverse mode transmission* on the facing page.

If the existing installation uses 26 Bit Wiegand, you must follow an additional procedure to program the reader to transmit in Reverse Mode 26 Bit Wiegand. For more information, see *Programming a Reverse mode transmission reader for 26 Bit Wiegand* on the facing page.

Only one of the two modes may be configured at a time.

5.8 Programming a reader for reverse mode transmission

To provide backwards compatibility to V1.08, V1.09, and V1.12 Mullion readers, you can program the reader for Reverse mode transmission.

1. Remove the Base of the reader from the Front of the reader.
2. Power down the reader if connected.
3. Connect the green LED control input (G) to the Tamper input (Y).
4. Place Jumper 2 in the lower position.
5. Remove Jumper 1.
6. Power up the reader.
   The reader beeps the affirmation tone and the green indication LED flashes. The reader is now in VR firmware 1.X Wiegand compatible mode.
7. Power down the reader.
8. Disconnect the Green from the Tamper connection.
9. Place Jumper 2 in the appropriate position for the number of Weigand bits.
   For 32 Bit Wiegand, place Jumper 2 in the upper position.
   For 56 Bit Wiegand, place Jumper 2 in the lower position.
   For 26 Bit Wiegand you must re-progamme the reader into 26 Bit mode.
10. Continue with the installation.

5.8.1 Reverting to standard mode Wiegand

To return the reader to the standard data sequence for Wiegand, follow the steps below:

1. Remove the Base of the reader from the Front of the reader.
2. Power down the reader if connected.
3. Connect the green LED Control input (G) to the Tamper input (Y).
4. Remove Jumper 1 and Jumper 2.
5. Power up the reader.
   The reader beeps the affirmation tone and the green indication LED flashes. The reader is now in standard mode.
6. Power down the reader.
7. Disconnect the Green input from the Tamper connection.
8. Place Jumper 2 in the appropriate position for the number of Weigand bits.
   For 32 Bit Wiegand, place Jumper 2 in the upper position.
   For 56 Bit Wiegand, place Jumper 2 in the lower position.
   For 37 Bit Wiegand , remove Jumper 2.
9. Continue with the installation.

5.9 Programming a Reverse mode transmission reader for 26 Bit Wiegand

The reader may programmed into 26 Bit Wiegand mode as follows;

1. Connect Red input to the Tamper
2. Put J2 in the lower position.

3. Activate the Tamperby removing the back plate.
4. Remove OSDP Jumper 1.
5. Power up the reader.
   The reader beeps an affirmation tone and the RED indication led flashes each second.
6. Power down the reader.
7. Disconnect Red input and Tamper connection.
8. Power up the reader.
   The reader now operates in 26 Bit Wiegand mode regardless of the setting of Jumper 2.

5.9.1 Re-programming a reverse mode transmission reader away from 26 Bit Wiegand

To reverse the reader out of 26 Bit Wiegand mode and to use the setting of Jumper 2 to determine Wiegand Bit mode operation, follow the steps below:

1. Connect Red input to the Tamper
2. Remove Jumper 2.
3. Activate the Tamper by removing the back plate.
4. Remove OSDP Jumper 1.
5. Power up the reader.
   The reader beeps an affirmation tone and the RED indication led flashes each second.
6. Power down the reader.
7. Disconnect the Red input and the Tamper connection.
8. Place Jumper 2 in the appropriate position for the number of Weigand bits (upper position for 32 Bit, lower position for 56 Bit, and remove for 37 Bit).
9. Power up the reader.

- The RED indication LED flashes twice if the reader is configured for 26 Bit Wiegand operation.
- The GREEN indication LED flashes twice if it is configured for Reverse transmission mode.
- Both The RED & GREEN indication leds flash twice simultaneously if the reader is configured for Reverse transmission mode and 26 Bit Wiegand operation.

5.10 Default Configuration Card

The Default Configuration card configures the reader for

- Standard Wiegand transmission mode
- Wiegand bit mode dependent on Jumper 2
- ACT MIFARE card printed number on card
- DESfire UID.

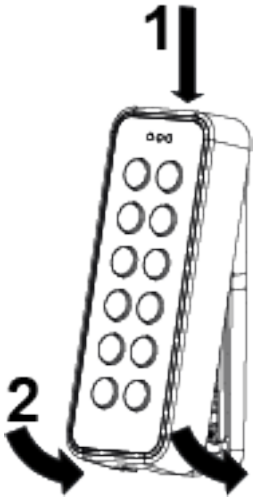
5.10.1 37 Bit Wiegand.

37 Bit Wiegand operation is compatible with ACT MIFARE / DESfire readers.

6 Closing the reader

To close the reader:

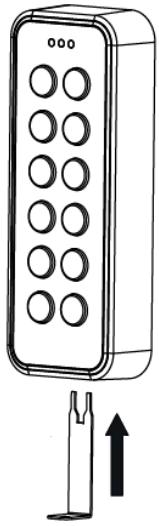
1. Holding the front of the reader at an angle, insert the hook on the top of the base into the corresponding slot in the front of the reader and slide down.
2. Gently press in the bottom of the reader front until the snap lock confirms a secure attachment.
3. Screw the cover screw (see number 4 in *Package contents* on page 9) into the bottom of the reader.



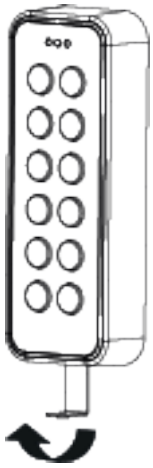
7 Disassembling the reader

7.1 To disassemble the reader:

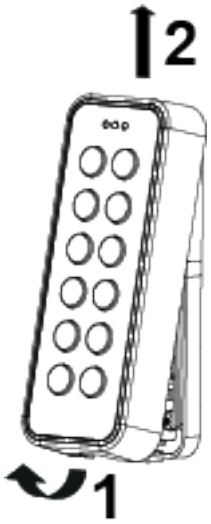
1. Remove the cover screw.
2. Insert the opening tool in the slot between the base and the front and push gently upwards.



3. Use the opening tool to pull the reader outwards and upwards.



4. When the front of the reader is disconnected from the snap lock, lift the front and slide upwards to disengage from the hook at the top.



7.2 To remove the terminal block:

1. Push down gently on the end of the terminal block marked with either +-BA or RY/TGH.
2. Tilt the terminal block away from the base.

8 Default settings

Reading MIFARE Classic	UID
Reading MIFARE Plus SL1 – SL3	UID
Reading MIFARE DESFire EV1	UID
Communications mode	OSDP (to change to Wiegand mode remove Jumper 1 and Jumper 3)
Backlight	Always on (change with 3CT tool)
Bus address	1 (Up to eight are supported)
Wiegand output	26/32/37/56 Bit
Wiegand key PIN burst	4/8 Bits
Light frame	Follows Red, Green LED inputs in Wiegand mode
Tamper/Yellow Connection	Tamper output (change to yellow LED with 3CT tool)
Wiegand heart beat mode	OFF
Time-out for configuration card (keypad backlight turns off when this timeout expires subsequent to last keypress)	3 seconds
Activation time-out	30 seconds
Hold-off time for card read	100 milliseconds
Reception for card (time before the same card will be detected in the field again)	Inactive
Min background illumination	12
Max background illumination	255
Off-line indication	Yes
Buzzer volume for key press	2
Buzzer volume for card read	2
System sound	10

8.1 3CT Tool

To change the default configuration of the reader, use the 3CT tool. You can purchase the 3CT tool as a separate download. You can use the 3CT tool to configure MIFARE Classic and DESFire EV1 card formats to be configured along with Wiegand options to be used for the card readers. For further information, please contact Vanderbilt International Ltd.. The 3CT tool configures the format in which user cards are interpreted by the card reader. The 3CT tool supports configuration of the following options: Tamper Output / Yellow Input and Heart beat Mode.

Option	Default setting	Information
Yellow input	Disabled	Selects Tamper Output when disabled
Heart beat mode	Disabled	Ensures a comms message is sent every 10 seconds to controller when enabled

For more information on 3CT please see the User manual for Configuration Card Creation Tool which is included when you purchase the 3CT tool.

The readers use FreeRTOS. For further information, please visit www.freetos.org.

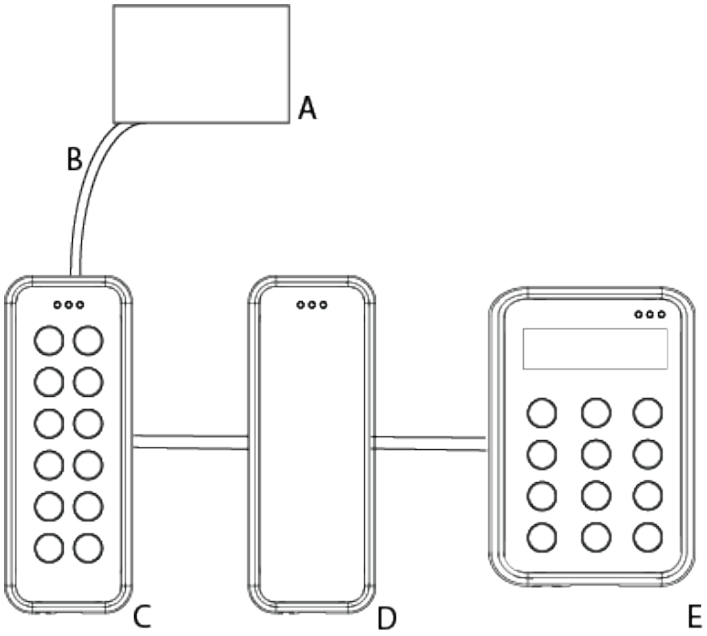
8.2 Setting burst mode using the keypad

The default burst mode is 4 bit. This can be changed to 8 bit. To change from 4 bit to 8 bit burst :

1. Power up the reader while holding the X key. The red and green indicators alternately turn on.
2. Press the key sequence 1818 to specify that 8 bit burst is required.
3. Hold down the ✓ key until you hear the two-tone affirmative beep.
4. To change back to 4 bit burst from 8 bit burst, follow the steps above pressing the key sequence1414 instead of 1818.

9 Connecting the reader to SiPass integrated

9.1 Connecting the reader to SiPass integrated in OSDP mode



A	SiPass integrated RIM (DRI/ERI)
B	Power and A, B (OSDP)
C	Reader 1 (VR50M-MF Mullion reader with keypad)
D	Reader 2 (VR20M-MF Mullion reader)
E	Reader 3 (VR40S-MF MIFARE Reader with keypad and display)

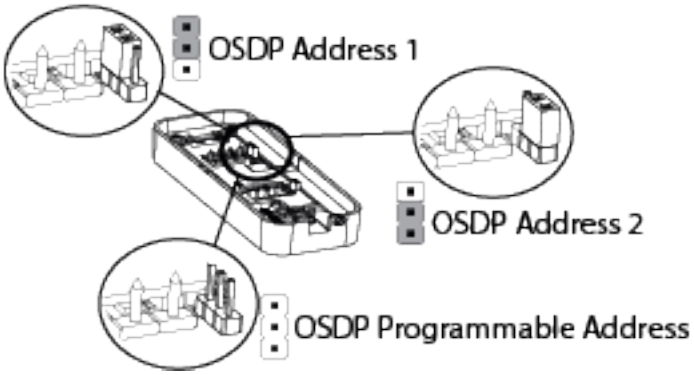
The connection between a reader and a Reader Interface Module (RIM) is as follows:

RIM (DRI/ERI)	VRxx-MF
12 V	+
0V	-
Tx/+	A
Rx/-	B

SiPass integrated can support both the VR and NGCR readers on the same OSDP bus.

9.2 Setting OSDP address for the reader

You can set the reader address to 1 (default setting), 2 , or programmed with a value from 1 to 8 using the Jumper. Place the Jumper in one of the three positions shown in the diagram below to achieve the desired address. Additional addresses are automatically assigned by the controller from 3 to 8 following the order in which the readers are powered up.



When the reader is first powered up, the yellow LED flashes. The flashing lights stop when it is correctly configured to SiPass integrated. This can be tested by holding a card next to the reader. A correctly configured reader acknowledges the card according to the SiPass integrated settings.

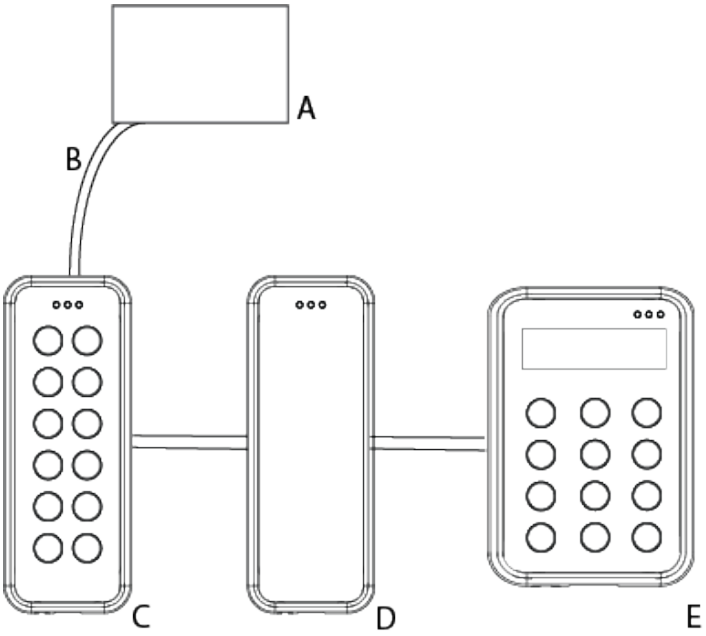
Please note that a new reader will always get the next free bus address. For example, if a reader with bus address 5 is removed and a new reader is installed, the new reader gets address 5.

9.3 Connecting the reader to SiPass integrated in Wiegand mode

For more detail on connecting the reader to SiPass integrated via Wiegand see *Connecting the reader in Wiegand mode* on page 13.

10 Connecting the reader to ACT

10.1 Connecting the reader to ACT in OSDP mode

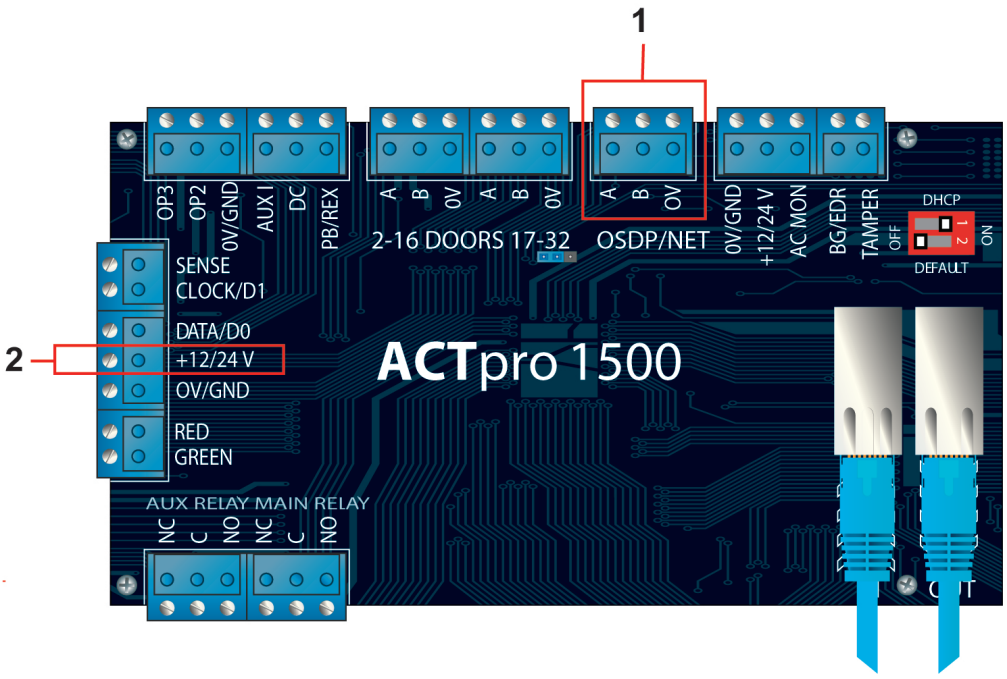


A	ACTpro 1500
B	Power and A, B (OSDP)
C	Reader 1 (VR50M-MF Mullion reader with keypad)
D	Reader 2 (VR20M-MF Mullion reader)
E	Reader 3 (VR40S-MF MIFARE Reader with keypad and display)

ACTpro 1500 can support both the VR and NGCR readers on the same OSDP bus.

The connection between a reader and an ACTpro 1500 is as follows:

ACTpro 1500	VRxx-MF
+12/24 V	+
OSDP/NET 0V	-
OSDP/NET A	A
OSDP/NET B	B



1	A,B,0V
2	+12/24V

1. Connect the cables as shown in the table on the previous page.
2. Use this terminal to supply power to the readers.

10.2 Setting the OSDP address for the reader

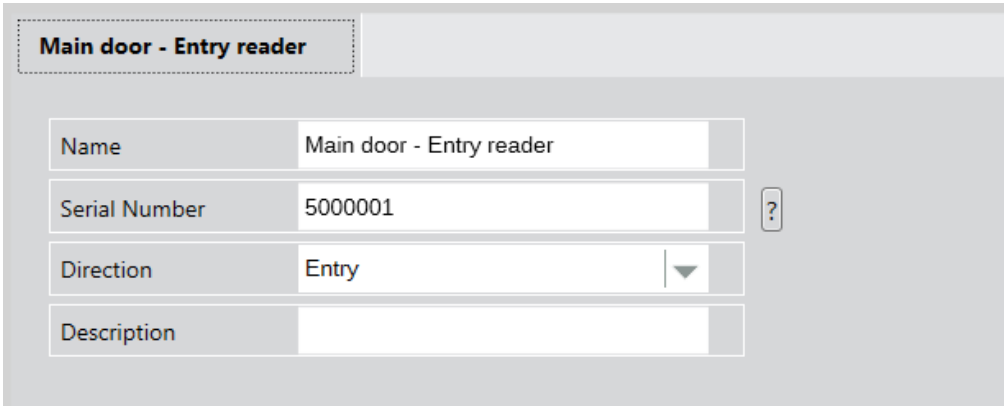
The ACTpro 1500 controller automatically assigns an address to each reader. Therefore, Jumper 2 should be removed for OSDP operation. The serial number of the reader is used to identify and enrol a reader on the system . The serial number can be found on a sticker on the reverse of the front cover of the reader (bordered in red in the image below).

During installation:

- Record the 7 digit serial number.
- Record the door name.
- Record if a reader is an entry or exit reader.

In the OSDP reader section of ACTEnterprise Software input the following attributes:

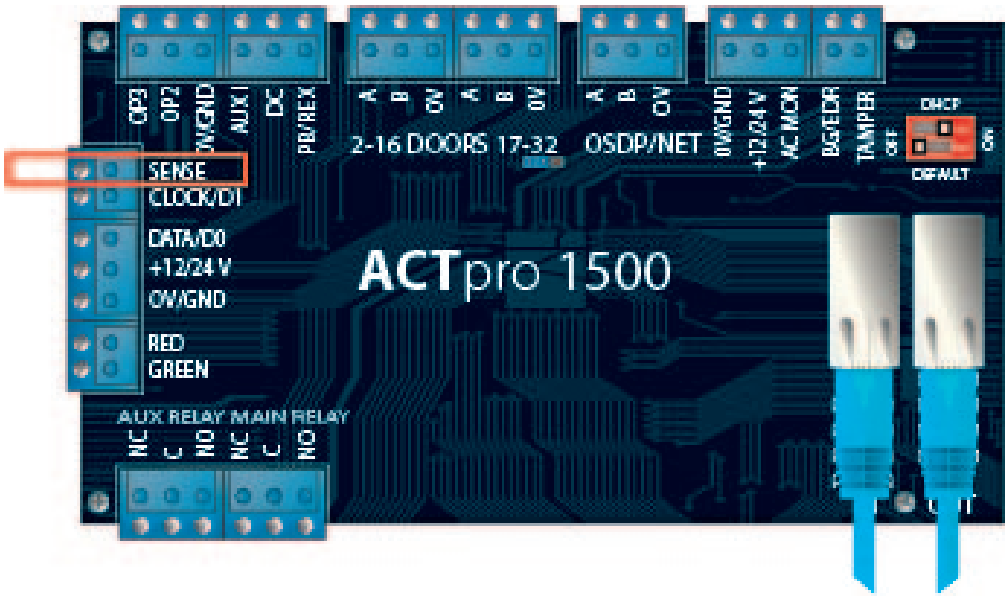
- Name
- Serial number
- Direction



10.3 Connecting the reader to ACT in Wiegand mode

For more detail on connecting the reader to ACT via Wiegand see *Connecting the reader in Wiegand mode* on page 13.

If you are connecting an exit reader in Wiegand mode, you should wire the Terminal A from the reader to SENSE on the ACTpro 1500 (bordered in red on the image below).



10 Adding a Bluetooth Module

Vanderbilt produce a Bluetooth module and frame (VR-BLE-MF, V54504-Z106-A100) for installation with the Mullion reader. The Bluetooth module can be added to a new Mullion reader installation or retrofitted to an existing Mullion reader installation.

This section of the manual contains information to help you to install a Bluetooth module with the Mullion reader in both indoor (IP54) and outdoor (IP55) settings.

For outdoor (IP55) installations, you must fit the self-adhesive backing that is included with the Bluetooth module and frame .

The Bluetooth module can be connected for either Wiegand or OSDP installations.

10.4 Mounting and Connecting a Bluetooth Module

You can install a Bluetooth module with the Mullion reader in both indoor (IP54) and outdoor (IP55) settings.

The Bluetooth module can be retrofitted to an existing Mullion reader installation, or added to a new Mullion reader installation.

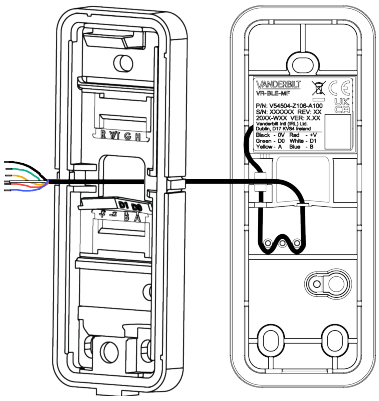
The Bluetooth module can be connected for either Wiegand or OSDP installations.

Important

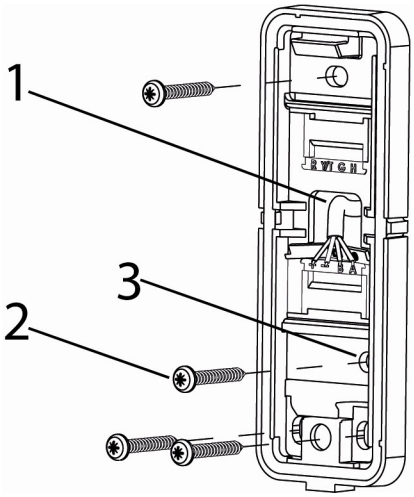
Study the section on *Mounting a reader* on page 10 before you install the Bluetooth module in your Mullion reader.

10.4.1 Indoor (IP54) installation

1. Open the Mullion reader.
2. Separate the reader base from the body of the reader.
3. Feed the cable from the Bluetooth module through the Mullion reader base.



1. Fit the Bluetooth module to Mullion reader base, taking care to route the cable correctly.
2. Attach the base to the wall using the screws that are supplied with the Bluetooth module: one in the middle at the top of the base, and one in each of the corners at the bottom of the base.

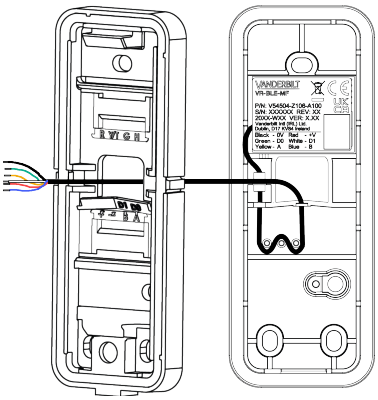


1	Cable entry through base gasket
2	Tamper screw
3	Tamper base

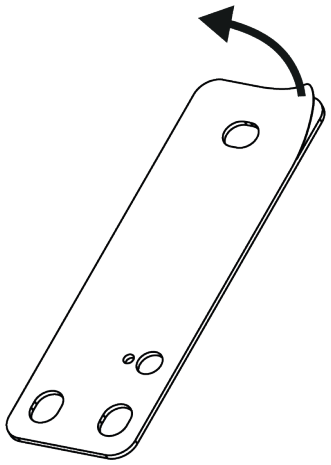
3. If tamper protection is required, fix the screw (item 2) into the tamper base (item 3). Do not over-tighten the screw as this can damage the tamper base.
4. Continue to follow the instructions detailed in *Connecting the cables* on page 13.

10.4.2 Outdoor (IP55) installation

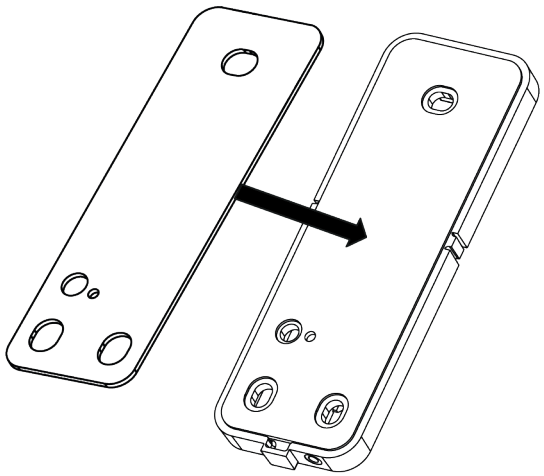
1. Open the Mullion reader.
2. Separate the reader base from the body of the reader.
3. Feed the cable from the Bluetooth module through the Mullion reader base.



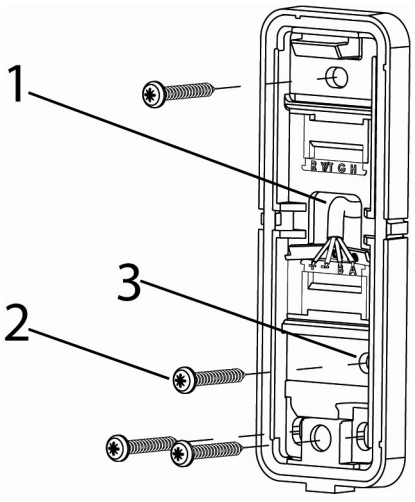
1. Fit the Bluetooth module to Mullion reader base, taking care to route the cable correctly.
2. Peel the backing paper from the self-adhesive foam base that is included with the Bluetooth module.

3. 

4. Apply the self-adhesive foam base to the back of the Bluetooth module frame.



1. Attach the base to the wall using the screws that are supplied with the Bluetooth module: one in the middle at the top of the base, and one in each of the corners at the bottom of the base.



1	Cable entry through base gasket
2	Tamper screw
3	Tamper base

2. If tamper protection is required, fix the screw (item 2) into the tamper base (item 3).

Do not over-tighten the screw as this can damage the tamper base.

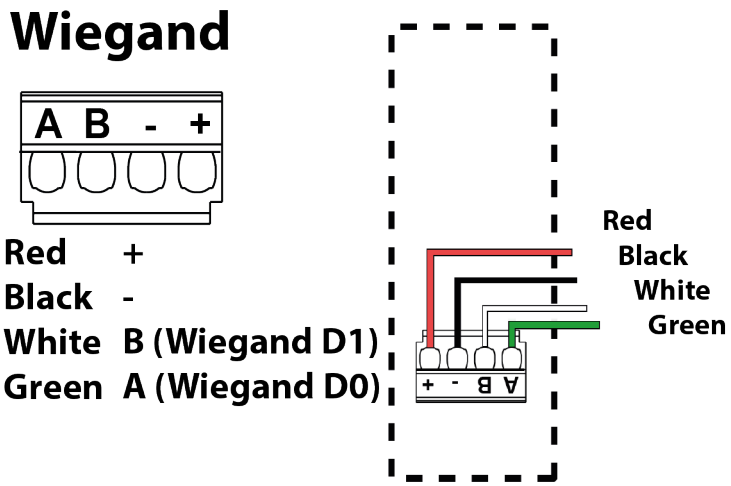
3. Continue to follow the instructions detailed in *Connecting the cables* on page 13.

10.5 Wiring the Bluetooth Module

The Bluetooth module can be connected to the Mullion reader for either OSDP or Wiegand installations.

10.5.1 Wiring the Bluetooth Module for Wiegand

You can connect the Bluetooth module to the Mullion reader for Wiegand operation, using the terminal marked **A B - +**.

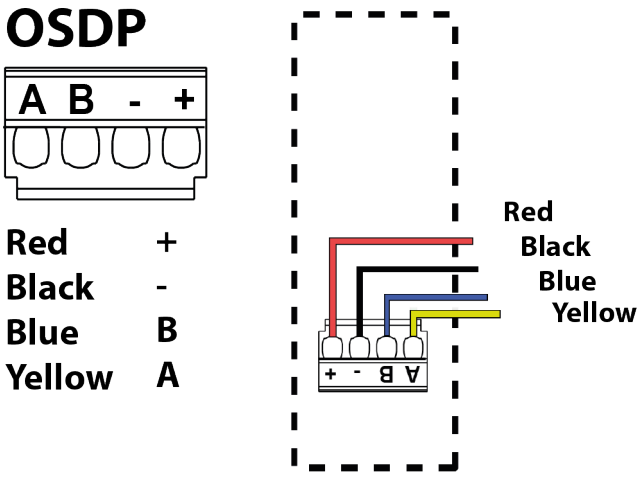


Isolate/terminate the Yellow and Blue wires in case of future use.

10.5.2 Wiring the Bluetooth Module for OSDP

You can connect the Bluetooth module to the Mullion reader for OSDP operation, using the terminal marked AB-+.

The Bluetooth module consumes a unique OSDP address. Vanderbilt recommend that you check your hardware to ensure that sufficient OSDP addresses are available.



Isolate/terminate the Green and White wires in case of future use.

10.6 Issuing Bluetooth Credentials

Vanderbilt's range of Bluetooth Readers is a secure and flexible access solution bringing digital credentials to Android™ and iOS® smartphones. These mobile credentials work in exactly the same way as traditional physical credentials, but the trusted identity, a unique ID number, is held within the smartphone.

VCredential is a cloud-based credential management platform that gives administrators the ability to create and manage Bluetooth credentials independent of the access control platform. The key benefits of the VCredential platform are the intuitive usability of the system and the opportunity to benefit from the latest industry technology trends.

Administrators can perform the following actions through the VCredential platform:

• Create a site (1)

• Add mobile credentials to a site (2)

• Invite a user to create a mobile credential (3)

• Approve a user request for a mobile credential (4)

• Activate a Bluetooth credential for a user (5)

• Manage site settings (6)

10.6.1 Creating a site

An administrator with a VCredential account within can generate mobile user credentials to control entry and/or exit to a site, building and specific areas with-in a site or building. The following procedure describes how to create a site in VCredential.

To create a site:

1. Click **Choose Site > Add New Site**.

2. Enter a **Site Name**.

3. Enter a **Site Email Address**.

Each site on VCredential has a unique email address to ensure that only authorized users will request access to a building or site for their mobile phone. This email account supports both sending and receiving email and will be the address to which VI Mobile ID app users submit authorization requests.

If the selected email address is already in use, you will be notified, and you can try a different one.

4. Select the **Time Zone** of the site.

5. Select the **Use reverse byte encoding for card numbers (Omnis)** check box to reverse the byte order of the card number generated in VCredential. This option is for example required if you use Omnis as the Access Control system.

10.6.2 Adding mobile credentials to a site

Mobile access credentials for use with VCredential can be purchased as a perpetual licence. There are no hidden costs as the price per credential is paid up-front and there are no recurring monthly or yearly charges. Please contact your installer to obtain a licence key for the number of mobile credentials you require for a site.

To add mobile credentials to a site:

1. Click **Choose Site**.

2. Select the site where you want to add a mobile credential and click **Select**.

3. Click **Manage Licences > Add a Licence Key**.

4. Enter the alphanumeric licence key in the format XXXXX - XXXXX - XXXXX – XXXXX.

5. Click **Add Credentials**.

The total number of mobile credentials available to activate users is displayed in the table under **Manage Licences** or in the status bar on the navigation panel.

The navigation panel also displays the following information for the selected site:

• Total number of activated credentials

• Current number of pending invitations

• Total number of credentials available

10.6.3 Sending an invitation to a user

You can initiate the activation process for a Bluetooth token by sending an email to a user.

The invitation email instructs the user to download the VI Mobile ID app from the App Store (iOS) or from Google Play (Android). The invitation email requests the user to enter an activation code in the VI Mobile ID app to complete the authorization cycle.

To invite a user to activate a Bluetooth credential:

1. Click **Invitations > Send new invitation**.

2. Enter the **Username**.

3. Enter the **Email Address**.
A card number displays for the invited user. This card number is uniquely and randomly created on VCredential. Vanderbilt recommends that you check to ensure that the card number is not already in use by your local Access Control system.

4. If the card number is already in use, click **Regenerate** to generate a new random and unique card number in VCredential before submitting the invitation to the user.

5. If you wish to enable the user to configure Bluetooth readers using the VCredential app, select the **Enable reader settings** menu check box and enter a 4-digit PIN.
For more information on the reader configuration options in the VI Mobile ID app, see the VI Mobile ID User Guide.

6. Click **Send Invitation**.

NOTE: PIN required to access reader menu settings as per 1.3 Reader settings through the VI Mobile ID app

10.6.4 Approving a Bluetooth request from a user

As an alternative to you sending an invitation to a user, a user can send a Bluetooth authorization request to you. This feature can be helpful if you do not wish to send a manual invite to each individual user of a site. Instead, you could choose to share your site email address and have the users request a Bluetooth token instead.

To approve a request from a user:

1. Click **Requests** to display a list of the users who have submitted an authorization request.

2. Select the user whose request you want to approve and click **Send credential invite** .

3. Enter the **Username**.

4. Enter the **Email Address**.
A card number displays for the invited user. This card number is uniquely and randomly created on VCredential, however Vanderbilt recommend that you check to ensure that the card number is not already in use by your local Access Control system.

5. If the card number is already in use, click **Regenerate** to generate a new random and unique card number in VCredential before submitting the invitation to the user.

6. If you wish to enable the user to configure Bluetooth readers using the VCredential, select the **Enable reader settings** menu check box and enter a 4-digit PIN.
For more information on the reader configuration options in the VI Mobile ID app, see the VI Mobile ID User Guide.

7. Click **Send invitation**.

10.6.5 Activating a Bluetooth credential

The activation email contains all of the information that a user needs in order to activate the Bluetooth credential.

Click **New Credentials** in the navigation panel to display a list of users you have previously approved for a Bluetooth credential. This panel option can be used as a task list for copying a newly assigned card number to your local Access Control system.

Your Access Control system provider may have chosen to partially or fully integrate the VCredential functionality into the Access Control system for further ease-of-use. For details, please consult the documentation for your Access Control system.

1.2.6 Transferring a Bluetooth credential to a new device

Disabling and transferring an active credential can be a useful tool in the event of:

• User reports a mobile phone as lost

• User reports a mobile phone as stolen

• User needs to transfer a credential to a new device

To transfer an active credential to a new device:

1. Click Active Credentials to display a list of users who have an active credential.

2. Select the user whose credential you want to transfer.

3. Click Transfer credential.

4. Check if the displayed Username and Email Address are associated with the user you would like to transfer the credential for.

5. Select whether to keep the current card number or to issue a new card number.

If you opted to keep the existing card number, the existing card number displays.

6. To enable the user to configure Bluetooth readers using the VCredential, select the Enable reader settings menu check box and enter a 4-digit PIN.

10.6.6 Reactivating a credential

Disabling and reactivating a credential can be a helpful in the event of:

• User leaves the business for a prolonged period of time with the intention of returning to the office

• User deletes a Bluetooth credential by mistake

To disable an active credential:

1. Click Active Credentials to display a list of users who have an active credential.

2. Select the user whose credential you want to disable.

3. Click Deactivate Credential (add new icon)

In order to re-activate a credential:

1. Click Active Credentials to display a list of users who have an active credential.

2. Click the check-box Include deactivated credentials

3. Select the user whose credential you want to disable .

4. Click Deactivate Credential (add new icon)

5.

If a user has difficulties re-activating the credential, you can invite the user to your desk and show them a QR code on your screen.

• Select the user and click Show QR Code (show QR code icon).

Alternatively, you can save the displayed QR code to your local PC and select a different delivery method.

10.7 Changing site settings

You can review and change the settings that you have configured for each site through the VI Mobile ID app. To use the app, you must have an active Bluetooth credential on your mobile phone with advanced access rights to the Bluetooth reader settings in form of a PIN. A Bluetooth credential can be obtained through the process described in 1.2 Issuing a Bluetooth Credential.

Open the VI Mobile ID app on your phone and click **Site settings**.

Select one of the following settings to edit :

- General reader settings
- OSDP reader settings
- Firmware upgrade

For more information on how to use the VI Mobile ID app, scan the QR code below, or go to the URL:

http://van.fyi?Link=VI_Mobile

10.7.1 General reader settings

You can access General settings for the reader through the VI Mobile ID app.

Click **Settings -> Reader settings -> Enter PIN -> General reader settings**

10.7.2 OSDP reader settings

You can access OSDP reader settings for the reader through the VI Mobile ID app.

Click **Settings -> Reader settings -> Enter PIN -> OSDP reader settings**

10.7.2.1 Manual OSDP addressing in ACTpro

The ACTpro system automatically sets up the OSDP address and baud rate for the Bluetooth module when using the auto-detect feature.

To change the pre-set OSDP values,use the VI Mobile ID app.

It is only possible to change the OSDP address. The baud rate cannot be changed.

ACTpro only supports OSDP address 1-16

10.7.3 Defaulting the OSDP settings for a Bluetooth module

The OSDP settings must be reset or defaulted if you wish to move a reader with Bluetooth module and frame to another controller.

To reset or default the OSDP settings for a Bluetooth module and frame:

1. In the VI Mobile ID app, click **Settings -> Reader settings -> Enter PIN -> OSDP reader settings**
2. Manually delete the OSDP address and encryption settings.
3. Click **Set** to commit the changes to the reader.

10.7.3.1 Manual OSDP addressing in SiPass

The SiPass system automatically sets up the OSDP address and baud rate for the Bluetooth module when using the auto-detect feature.

To change the pre-set OSDP values,use the VI Mobile ID app.

10.7.3.2 Manual OSDP addressing in SPC

The SPC system supports OSDP wiring of the Bluetooth module through the use of the OSDP converter. Using OSDP wiring, cable length can be up to 1km.

The SPC system does not automatically set the OSDP address.

You must install an OSDP converter board for each OSDP reader as the SPC system will only recognise the first unit that is connected to the OSDP converter.

To connect a Mullion VR2- or VR 50 reader that is fitted with a Bluetooth module, you must use 2 OSDP converters,

Alternatively, you can use a single OSDP converter to connect the reader and connect the Bluetooth module via Wiegand to the door controller

10.7.3.3 Manual OSDP addressing in Omnis

The Omnis system automatically sets up the OSDP address and baud rate for the Bluetooth module when using the auto-detect feature.

There is no functionality within Omnis to change either the OSDP address or the baud rate.

10.7.4 Firmware upgrade

You can upgrade the firmware on the Bluetooth module through the VI Mobile ID app.

Click **Settings -> Reader settings -> Enter PIN -> Firmware upgrade**

© Vanderbilt 2022

Data and design subject to change without notice.

Supply subject to availability.

Document ID: A-100410-e

Edition date: 16.06.2022

VANDERBILT

vanderbiltindustries.com

@VanderbiltInd Vanderbilt Industries

Issued by **Vanderbilt International Ltd.**
Clonshaugh Business and Technology Park
Clonshaugh, Dublin D17 KV 84, Ireland

vanderbiltindustries.com/contact