MR Manual – MF Ultralight EV1

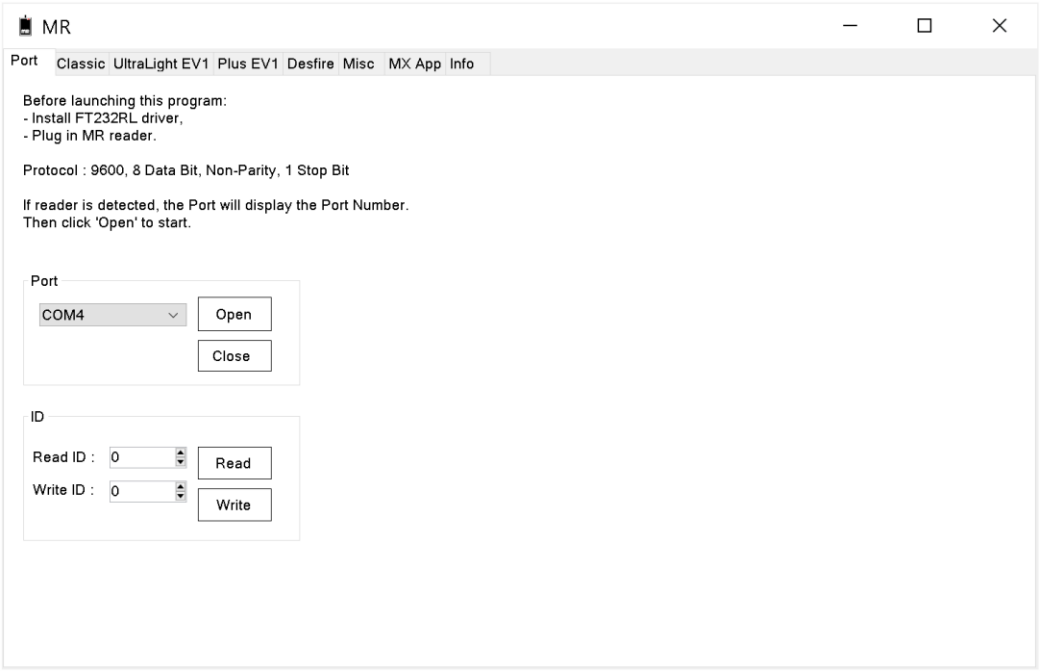
Visit us at www.mylab.my
Email: sales@mylab.my

Please email to us, to get a copy of the MR software.

Contents

1. General

Plug in MR Reader then launch the MR Software. 



Main screen.

If Serial Com Port available, or USB Virtual Com available, it will be shown on screen.

Select the port where reader is connected, then click 

to open port.

Upon open port, reader will send command to get reader ID, and turn on the RF. Getting reader ID should be the first command to execute, because if the ID is not matched, reader will not response.

1.0 Protocol

To ease development, sending and receiving protocols are recorded and saved in the **C:\Mylab\MR** folder, as shown below:

Function : Open Port
6:47:51 PM, TX : 02 00 00 01 50 53 03
6:47:51 PM, RX : 02 00 00 02 00 00 00 03
6:47:51 PM, TX : 02 00 00 02 54 01 55 03

They are briefly explained as below:

Communication Protocol:

Item	Value
Baud rate	9600
Data bit	8
Parity	None
Stop bit	1

For card related command:
TX : 02 / 00 / Reader ID / No of byte / Command / PICC Command / Data / BCC / 03
RX : 02 / 00 / Reader ID / No of byte/ Message / CSN length / Card Serial Number / Card Type / PICC Message / Data / BCC / 03

For hardware setting related command:
TX : 02 / 00 / Reader ID / No of byte / Command / Data / BCC / 03
RX : 02 / 00 / Reader ID / No of byte/ Message / Data / BCC / 03

Item	Length	Meaning
STX (Start of Text)	1	02 Hex
Master ID/MID	1	00 Hex
Reader ID/RID	1	00 – FF hex
No of byte/NOB	1	No of byte in TX Data or RX Data
Command/CMD	1	Refer manual or sending protocol 0 = none 1C hex = readwriteul 1D hex = ulpicc 48 hex = areadsnr 49 hex = areadsnrsize 50 hex = read_id 51 hex = write_id 54 hex = control_rf 6A hex = read_mode 6B hex = write_mode 6D hex = control_beep_led 6E hex = control_beep 6F hex = control_led F0 hex = read_version
PICC Command (Optional)	1	Refer manual or sending protocol
Message/MESG	1	00 – Success, others – Error
CSN length/CSNL	1	0 or 4 or 7 (when 0, there is no serial number returned, hence the Card Serial Number and Card Type column will not be available in the RX protocol too.)
Card Serial Number/CSN	4 or 7	4B or 7B CSN

Card Type/CT	1	Refer Mifare Card Information 08 hex = Mifare Classic 18 hex = Mifare Plus (SL1 or Mixed mode) 20 hex = Mifare Plus (SL3) 20 hex = Mifare Desfire
PICC Message/PMESG	1	Last 4-bit: xA hex – Acknowledge x0 hex – NAK for invalid argument x1 hex – NAK for parity or CRC error x4 hex – NAK for counter overflow x5 hex – NAK for EEPROM write error x7 hex – NAK for EEPROM write error x6 hex – NAK for other error x9 hex – NAK for other error
Data	variable	Transmit or Received string
DF Name (Optional)	17	1B length, 16B DF Name (If Virtual Card is enabled)
BCC	1	Exclusive-Or from byte STX to the byte before BCC
ETX (End of Text)	1	03 Hex

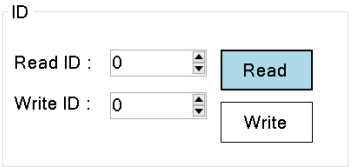
1.1 Reader ID

The default reader ID is 00, it can be changed to other value. In RS485 or multi-drop application, reader with different ID is needed to ensure proper communication.

To set ID value, enter a value in the Write ID numeric box, and then create 'Write'. After you changed the ID, remember to click 

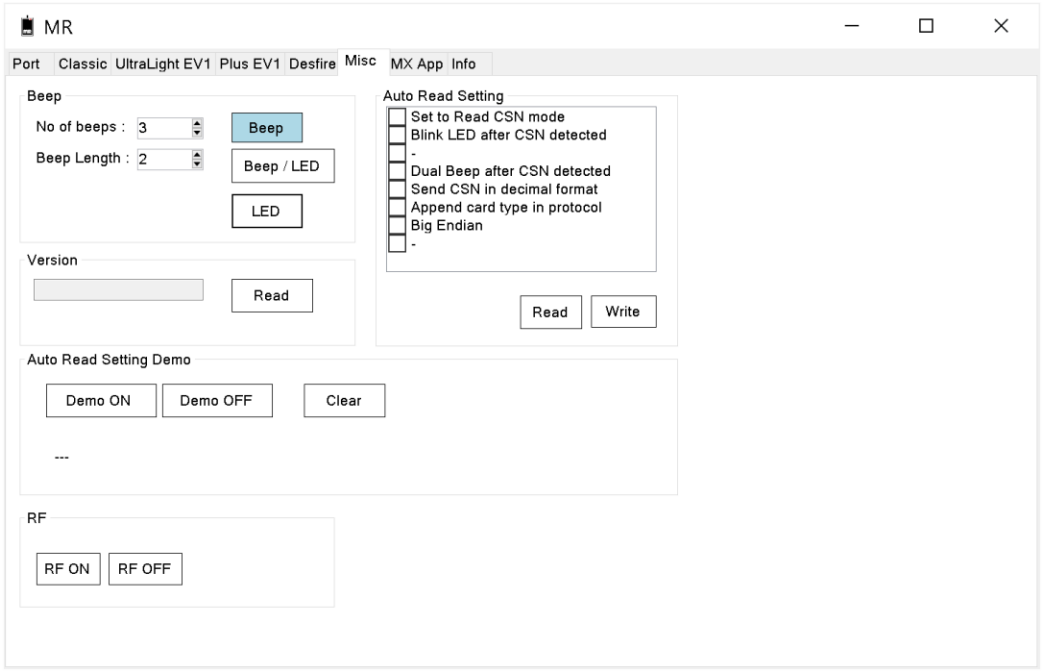
to get the new reader ID, or manually update the read ID numeric box. If not, communication may be fail because the ID in the program is different from the ID in the reader. Therefore, always get the reader ID first before proceeding further.

The value will be saved in the non volatile memory.



1.2 Beep

There are two beep mode available; beep only and beep with LED. Beep with LED will generate beep sound and trigger the on board LED. Multiple beeps can be generated by setting the 'No of beeps' and 'Beep length'.



Click  will generate 3 beeps.

1.3 RF

No communication between card and reader is possible when the RF is turned off. Therefore, it is important to ensure the RF is turned on when accessing the card. By default, the RF is on.

Sometimes it may be necessary to control the RF to reset the card in the field.

To reset RF in the reader field, click  , and then click  .

1.4 Reader Internal EEPROM

The hardware settings, and the authentication keys are saved into the internal EEPROM by using instruction. This is a non-volatile memory, the content will be kept even though power is removed.

Due to security reason, the authentication keys are not readable.

- Please bear in mind that EEPROM is intended to provide nonvolatile storage for configuration data and settings that do not need to change frequently. If an application program were to write to an EEPROM cell frequently it would quickly wear it out, shorten the lifetime of the product.

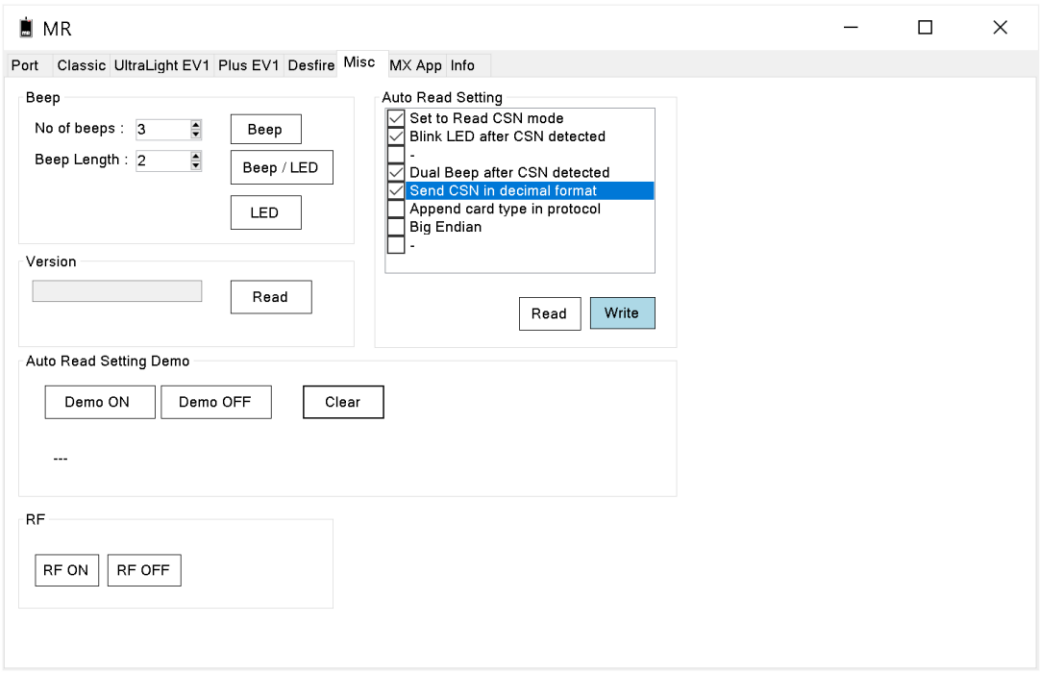
1.5 Remark

After a Mifare card‘s sector has been authenticated successfully, the sector will be opened, and read or write is permitted. The card will remain in the ‘Open’ state until the RF field is reset, or the card is removed from the RF area, then a new authentication is needed.

In the examples given below, the testing result may be different if the RF reset is not performed after changing Key or changing authentication method. Therefore, if the testing result is different from the given answer, kindly reset the RF by calling command ‘RF Off’ and ‘RF On’, or merely remove the card from reader, and then put back the card on the reader. The author has omitted this, to avoid duplicated words and for easy reading. It is also recommended to perform RF reset prior to create new application or new file.

2. How to set to Read Serial Number mode

By default the reader is in Read/Write mode. User can switch the reader to work on Auto Read Serial Number mode by checking the following box. Both 4B and 7B serial number lengths are supported.

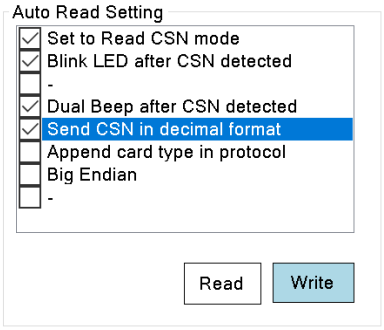


The above setting will switch the reader to work on Read Serial Number mode. When a valid card is detected, it will blink LED, sound two beeps, and send the serial number to Host in decimal and Little Endian format.

Available functions:

a. Set to Read Card SNR mode – Enable Read Serial Number mode, default is Read / Write mode.
b. Blink LED after SNR detected – Blink LED when a valid card is detected.
c. Dual Beep after SNR detected – Sound dual beep when a valid card is detected.
d. Send SNR in Decimal format – Send Serial Number in decimal format, default is sending Serial Number in Hex format.
e. Append Card Type in protocol – Append card type in the protocol. Only if Hex format is enabled, or 'Send SNR in Decimal format' is unchecked.
f. Big Endian – Send Serial Number in Big Endian format, default is sending Serial Number in Little Endian format.

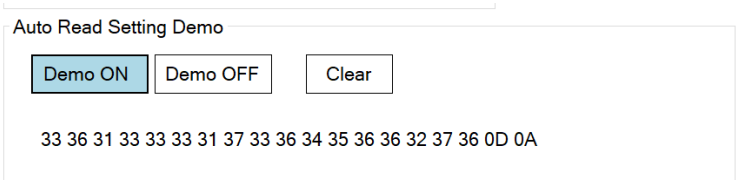
We will try it now by setting the check box as shown below:

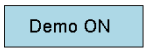


Click 

to send the check box setting to reader.

We will see how it works now by turning on the Demo mode.

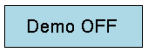


Click 

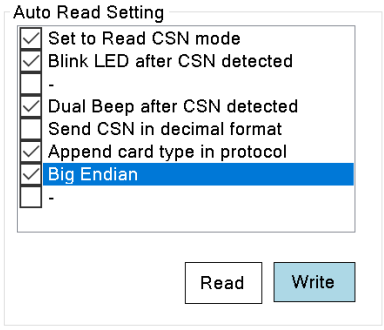
to detect any valid card in the RF field. If available, display the Serial Number in decimal format, blink LED, and sound dual beep.

You may refer Activity text file in C:\Mylab\MR, for detailed protocol received string.

Function : Write Card Setting
12:08:47 PM, TX : 02 00 00 02 6B 1B 70 03
12:08:47 PM, RX : 02 00 00 01 00 03 03
Function : Demo On
12:08:55 PM, RX : 32 34 31 38 31 34 32 31 39 30 0D 0A
12:08:57 PM, RX : 33 36 31 32 35 32 32 36 33 32 33 38 30 31 38 36 30 0D 0A
12:09:07 PM, RX : 33 36 31 33 33 33 31 37 33 36 35 35 34 39 33 31 36 0D 0A

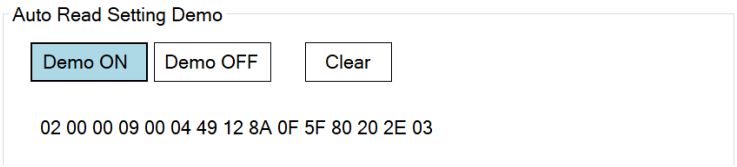
Turn off the demo now by clicking 

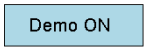
, and try another setting as shown below:

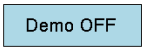


Click 

to send the check box setting to reader. This setting will include the card type in protocol.



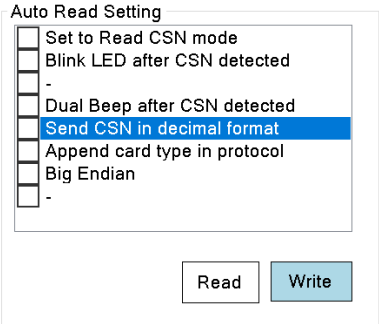
Click  to detect any valid card in the RF field. If card available, it will return the Serial Number in Hex format, append the card type in the protocol, blink LED, and sound beep. As shown in the protocol 02 00 00 09 00 04 49 12 8A 0F 5F 80 20 2E 03, the card type is 20 hex. Refer Chapter 1-0 Protocol, we know that the card is Mifare Desfire or Mifare Plus (SL3).

Always remember to turn off the demo by clicking  .

The setting will be stored as non volatile in the reader's memory.

3. How to set to Read / Write mode

By default the reader is in Read/Write mode. If the reader has been set to Auto Read Serial Number mode, we can switch it back to Read/Write mode by un-checking all the items in the following box, then click Write.



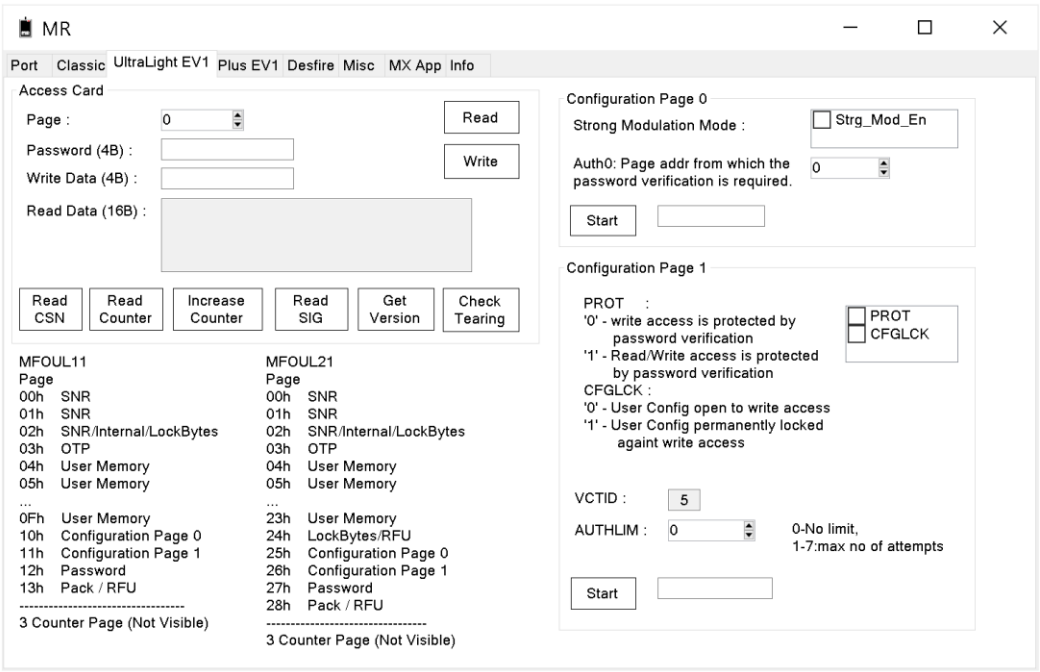
The reader is now in Read/Write mode.

The reader must be in the Read/Write mode in order to follow the examples in the chapters that follow.

The setting will be stored as non volatile in the reader's memory.

4. Mifare Ultralight EV1

Click the 'Ultralight EV1' tab now to enter the page. This program will show you how to access MF Ultralight EV1 card.



Ultralight EV1 main screen.

4.0 Access Method

For new Mifare Ultralight card, the user memory content is free access. It is not protected by password by default. Once the password verification feature is enabled, accessing the card content will require password verification. The default 4B password is FFFFFFFF hex. If the password does not match, an error code will be returned.

4.1 Memory

Depends on the card size, their memory location may be different. User is advised to refer to the card manufacturer's documentation for details.

The card memory is divided into pages, and one page is 4B. But for every Read command, the reader will return 4 pages, or 16B data.

MFOUL11	
Page	**Description**
00h	Serial Number
01h	Serial Number
02h	Serial Number / Internal / LockBytes
03h	OTP
04h	User Memory
05h	User Memory
…	…
…	…

0Fh	User Memory
10h	Configuration Page 0
11h	Configuration Page 1
12h	Password
13h	Pack / RFU
3 counter Page (Not Visible)	

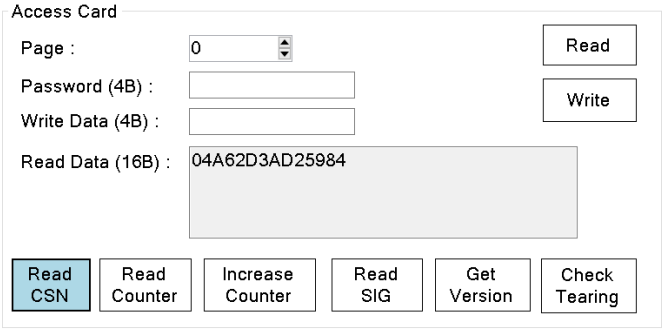
MFOUL21	
Page	**Description**
00h	Serial Number
01h	Serial Number
02h	Serial Number / Internal / LockBytes
03h	OTP
04h	User Memory
05h	User Memory
…	…
…	…
23h	User Memory
24h	LockBytes/RFU
25h	Configuration Page 0
26h	Configuration Page 1
27h	Password
28h	Pack / RFU
3 counter Page (Not Visible)	

4.2 Before we start

As mentioned, password verification is disabled for new MF UL card. But we still include the 4B password in the transmit protocol to maintain the consistency in the communication. In the demo examples below, we fix the password to FFFFFFFF hex, which is the default password of MF UL. We will show you how to change the password in the later chapter.

5. Read Card Serial Number

Place a Card on the USB reader, then click 'Read CSN' to read the unique serial number. This version supports both 4B and 7B serial number. There are displayed in Hex, and is displayed from LSB to MSB.



Click 

to read the card CSN.

Function : UltraLight Read CSN

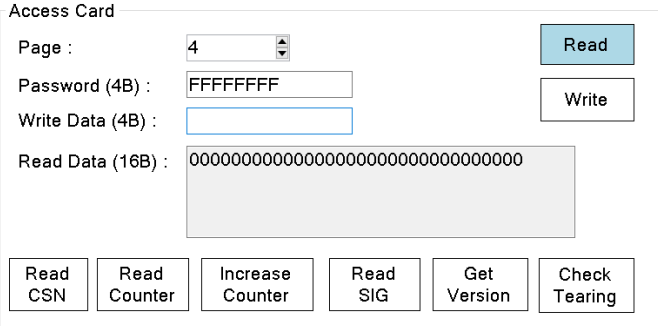
9:36:39 AM, TX : 02 00 00 01 48 4B 03

9:36:39 AM, RX : 02 00 00 09 00 07 04 A6 2D 3A D2 59 84 B6 03

6. Read Page

We will read data located at page 4, refer to the card structure, it is for user memory.

Item	Value
Page	4
Password (4B)	FFFFFFFF



Click 

to read the card content. The reader will return 4 pages, or 16B data. The first 4B is the data of the page, which is page 4. The subsequent 4B data is the data of page 5, and so on.

Function : UltraLight Read

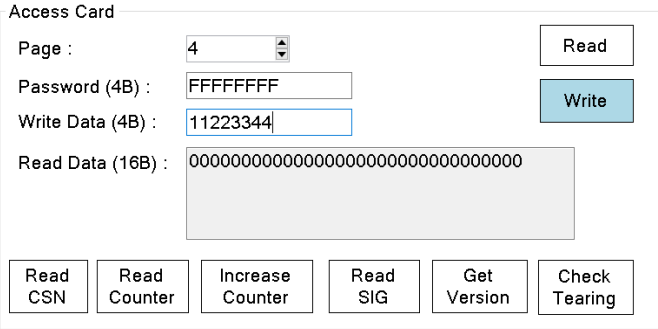
9:46:50 AM, TX : 02 00 00 07 1C 30 FF FF FF FF 04 2D 03

9:46:51 AM, RX : 02 00 00 1B 00 07 04 A6 2D 3A D2 59 84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A4 03

7. Write Page

We will write 4B data to page 4, and then read it out to verify. Please note that when reading card, it return 16B of data, but when writing, we enter only 4B of data.

Item	Value
Page	4
Password (4B)	FFFFFFFF
Write Data (4B)	11223344

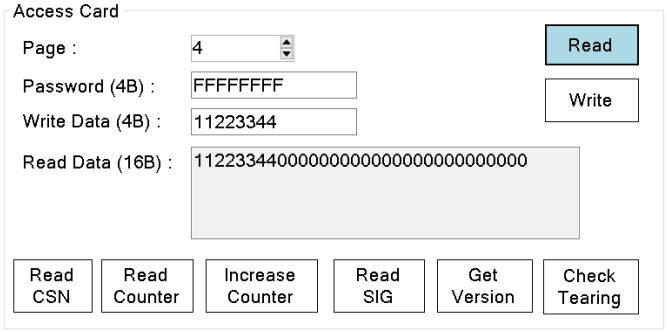


Click 

to write 11223344 hex to page 4.

We will read out the page 4 to verify.

Item	Value
Page	4
Password (4B)	FFFFFFFF



Click 

to read the content of page 4. The returned data shows the previous 'Write' was successful.

Function : UltraLight Write

9:52:06 AM, TX : 02 00 00 0B 1C A2 FF FF FF FF 04 11 22 33 44 F7 03

9:52:06 AM, RX : 02 00 00 0B 00 07 04 A6 2D 3A D2 59 84 00 0A BE 03

Function : UltraLight Read

9:52:08 AM, TX : 02 00 00 07 1C 30 FF FF FF FF 04 2D 03

9:52:08 AM, RX : 02 00 00 1B 00 07 04 A6 2D 3A D2 59 84 00 00 11 22 33 44 00 00 00 00 00 00 00 00 00 00 00 E0 03

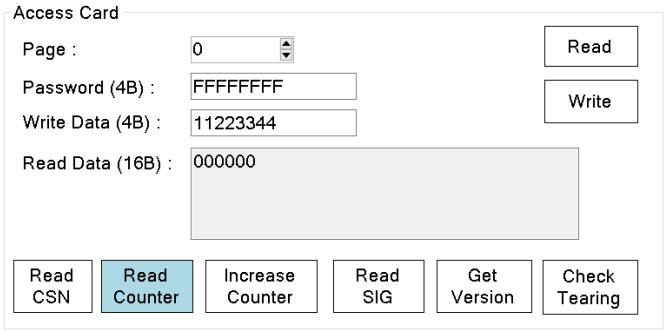
8. Counters

There are 3 counters in the card, for different applications. You may select the counter by setting page 0 to 2. Setting page 0 will select counter 0, page 1 for counter 1, and so on. Select page other then 0 to 2 will return error.

All the counters are 3B long.

We will now read out counter 0, increase the counter by 030000 hex, and then read it out to verify. Even though the counter is 3B long, we will still enter 4B increment value, like in 'Write Page'.

Item	Value
Page	0
Password (4B)	FFFFFFFF

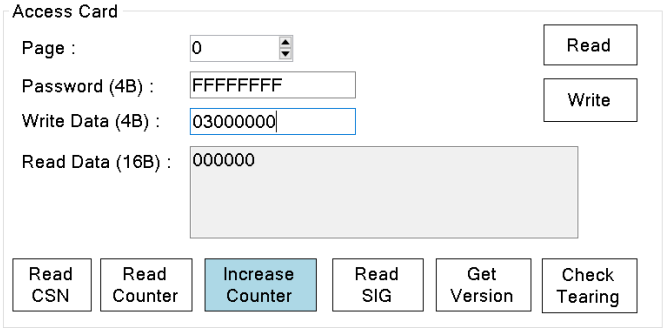


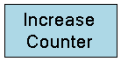
Set page 0 to select counter 0. Click 

, the returned data shows the value is 000000 hex.

Now, we will increase the counter 0 by 030000 hex.

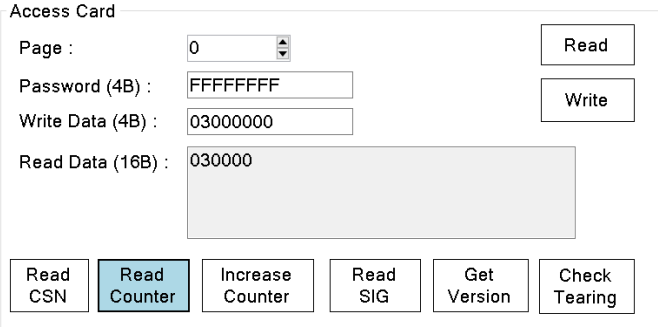
Item	Value
Page	0
Password (4B)	FFFFFFFF
Write Data (4B)	03000000

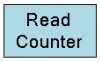


Set page 0 to select counter 0, and set Write Data to 03000000 hex, then click 

.

We will read the counter 0 to verify the content now.



Set page 0 to select counter 0. Click 

the returned data shows the value has been incremented to 030000 hex.

When the counter's value has reached FFFFFF hex, no further increment is allowed.

Counter 1 and 2 work the same, you may try them out.

Function : UltraLight Read Counter

10:05:03 AM, TX : 02 00 00 07 1C 39 FF FF FF FF 00 20 03

10:05:03 AM, RX : 02 00 00 0E 00 07 04 A6 2D 3A D2 59 84 00 00 00 00 00 B1 03

Function : UltraLight Increase Counter

10:10:03 AM, TX : 02 00 00 0B 1C A5 FF FF FF FF 00 03 00 00 00 B3 03

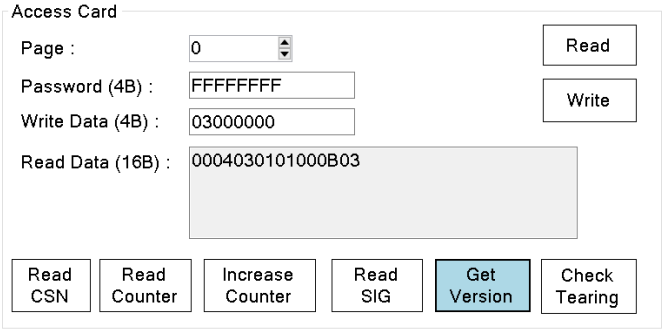
10:10:03 AM, RX : 02 00 00 0B 00 07 04 A6 2D 3A D2 59 84 00 0A BE 03

Function : UltraLight Read Counter

10:12:48 AM, TX : 02 00 00 07 1C 39 FF FF FF FF 00 20 03

10:12:48 AM, RX : 02 00 00 0E 00 07 04 A6 2D 3A D2 59 84 00 00 03 00 00 B2 03

9. Get Version



Click 

to know the card info like: information on the MIFARE family, product version, and storage size. Please refer to the card manufacturer's manual for the detailed explanation of the returned value.

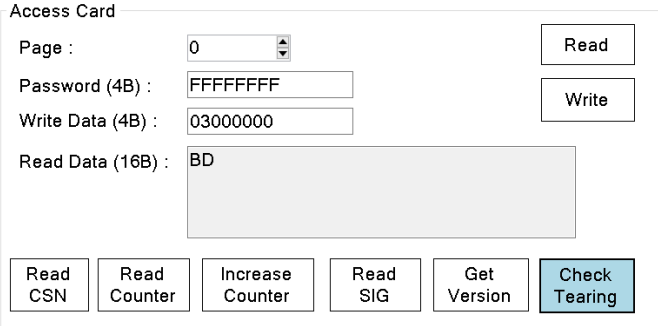
Function : UltraLight Get Version

10:14:40 AM, TX : 02 00 00 02 1D 60 7D 03

10:14:40 AM, RX : 02 00 00 13 00 07 04 A6 2D 3A D2 59 84 00 00 00 04 03 01 01 00 0B 03 A3 03

10. Check Tearing

This command enables the application to identify if a tearing event happened on a counter. Recall that there are 3 counters in the card, so the page address will range from 0 to 2.



Click 

to know if tearing happen during the write operation. The valid value for normal operation is BD hex. If any other value than BD hex is replied on the CHECK_TEARING_EVENT command, a tearing event has happened.

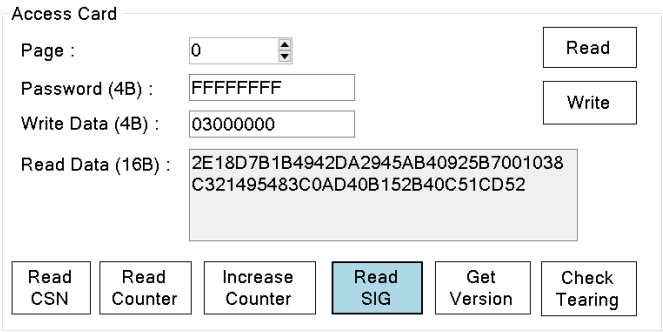
Function : UltraLight Check Tearing

10:18:11 AM, TX : 02 00 00 03 1D 3E 00 22 03

10:18:12 AM, RX : 02 00 00 0C 00 07 04 A6 2D 3A D2 59 84 00 00 BD 0E 03

11. Read SIG

This command will verify the chip originality.



Click 

to know the information of the chip; the 32-byte ECC signature. Please refer to the card manufacturer's manual for the detailed explanation of the returned value.

Function : UltraLight Read SIG

10:19:35 AM, TX : 02 00 00 03 1D 3C 00 20 03

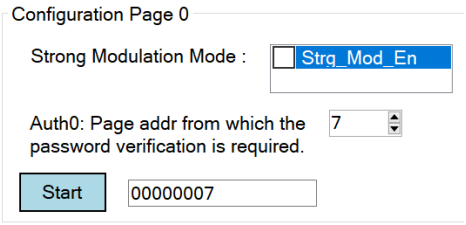
10:19:35 AM, RX : 02 00 00 2B 00 07 04 A6 2D 3A D2 59 84 00 00 2E 18 D7 B1 B4 94 2D A2 94 5A B4 09 25 B7 00 10 38 C3 21 49 54 83 C0 AD 40 B1 52 B4 0C 51 CD 52 66 03

12. Configuration Page 0

Configuration pages are used to configure the memory access restriction of the card.

In the configuration page 0, the items that worth pay attention are:

item	Description
Strong Modulation Mode	Available only in certain card. Please check manual for details.
Auth0	This register defines the page address from which the password verification is required. Example: If this register is set to 7, means accessing page 7 onwards will require password verification. Page 0 to 6, don't need.

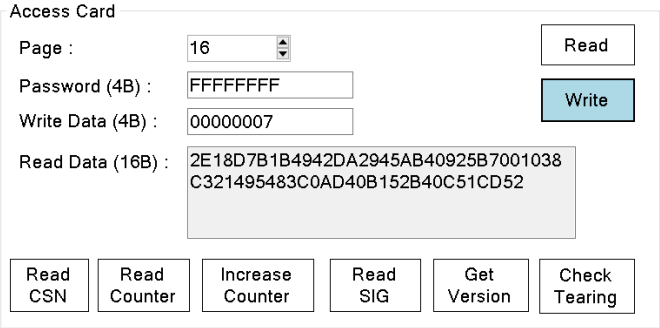


Above setting uncheck the Strong Modulation Mode, and set Auth0 to page 7. Click 

, system will generate a 4B data, and copy this data to the 'Write Data (4B)', as shown below.

Item	Value
Page	16
Password (4B)	FFFFFFFF
Write Data (4B)	00000007

Depends on the card model, the address for Configuration Page 0 may be different from the example shown below. Please check the card manual for details.

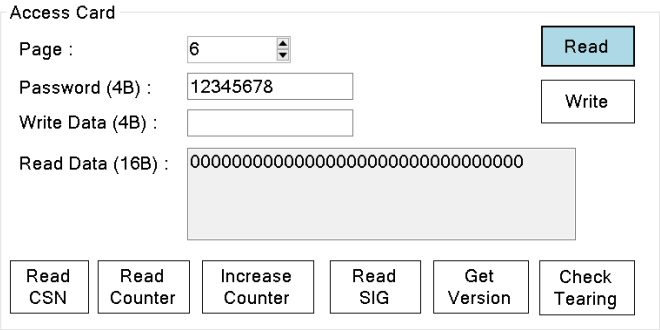


Click 

to program the Configuration Page 0. This setting will make accessing page 7 and above require password verification.

By default, only 'Write' require password verification, 'Read' is free access. We can enable the register so that read and write is protected by password verification. We will do it in Configuration Page 1. But now, only the write access requires password verification.

We will verify it now. We will read and write to page 6.

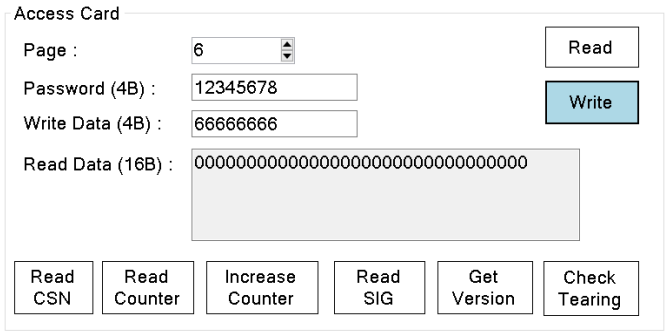


We set the password to 12345678 hex, which is a faulty password, and click 

. The read is successful, and not protected by password.

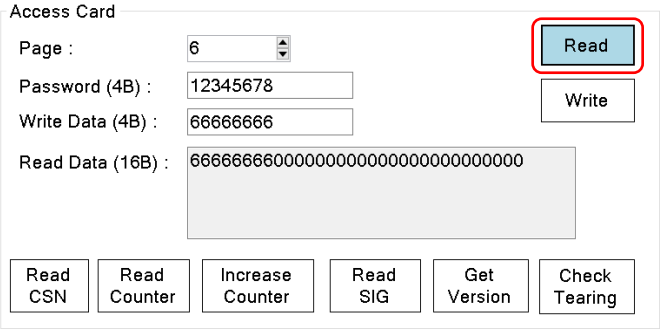
We will click 

to write 66666666 hex to page 6, and then read it out.



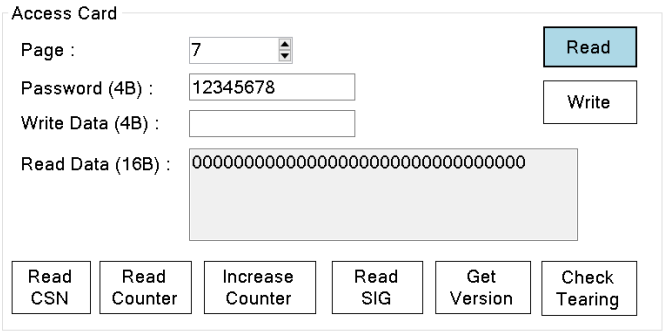
The write is successful, and not protected by password.

We read it out to verify.



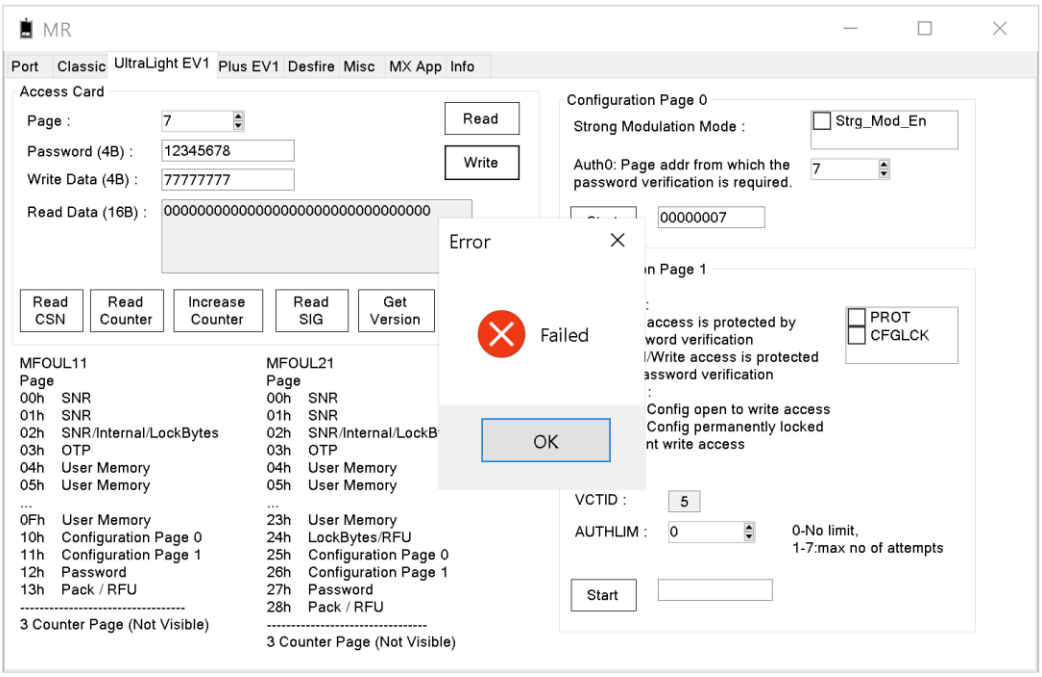
It shows that the previous write was successful. Page 6 is not protected by password.

Now, we will read and write to page 7. Bear in mind that we have set the Auth 0 register to 7, meaning that password verification is required when accessing page 7 and above.



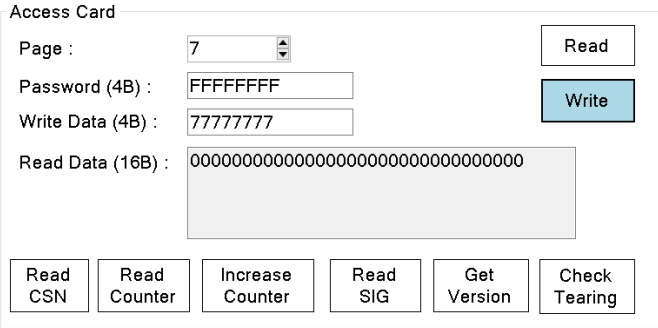
We still use the fault password, 12345678 hex, to access the card. Click Read. The read is successful, and not protected by password.

We will click Write to write 77777777 hex to page 7.



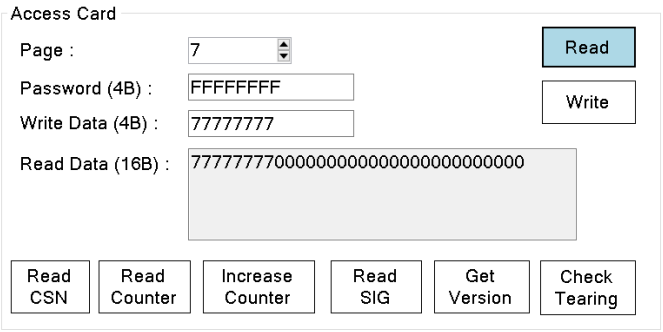
Checking the protocol, it returns error. Therefore, password verification failed. The password 12345678 is not correct. You may need to reset RF or card to view this.

We will now supplying FFFFFFFF hex as password, which is the default 4B password for MF UL, and click Write again.



The write command was successful.

We will read it out to verify.



Above shows the write and read are successful. Hence, confirm the access to page 7 and above requires password verification, and the password is FFFFFFFF hex.

Function : UltraLight Write

10:24:22 AM, TX : 02 00 00 0B 1C A2 FF FF FF FF 10 00 00 00 07 A0 03

10:24:22 AM, RX : 02 00 00 0B 00 07 04 A6 2D 3A D2 59 84 00 0A BE 03

Function : UltraLight Read

10:26:00 AM, TX : 02 00 00 07 1C 30 12 34 56 78 06 27 03

10:26:00 AM, RX : 02 00 00 1B 00 07 04 A6 2D 3A D2 59 84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A4 03

Function : UltraLight Write

10:27:54 AM, TX : 02 00 00 0B 1C A2 12 34 56 78 06 66 66 66 66 B9 03

10:27:54 AM, RX : 02 00 00 0B 00 07 04 A6 2D 3A D2 59 84 00 0A BE 03

Function : UltraLight Read

10:28:33 AM, TX : 02 00 00 07 1C 30 12 34 56 78 06 27 03

10:28:34 AM, RX : 02 00 00 1B 00 07 04 A6 2D 3A D2 59 84 00 00 66 66 66 66 00 00 00 00 00 00 00 00 00 00 00 00 A4 03

Function : UltraLight Read

10:29:44 AM, TX : 02 00 00 07 1C 30 12 34 56 78 07 26 03

10:29:44 AM, RX : 02 00 00 1B 00 07 04 A6 2D 3A D2 59 84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 A4 03

Function : UltraLight Write

10:30:59 AM, TX : 02 00 00 0B 1C A2 12 34 56 78 07 77 77 77 77 B8 03

10:31:00 AM, RX : 02 00 00 01 59 5A 03

Function : UltraLight Write

10:36:18 AM, TX : 02 00 00 0B 1C A2 FF FF FF FF 07 77 77 77 77 B0 03

10:36:18 AM, RX : 02 00 00 0B 00 07 04 A6 2D 3A D2 59 84 00 0A BE 03

Function : UltraLight Read

10:37:06 AM, TX : 02 00 00 07 1C 30 FF FF FF FF 07 2E 03

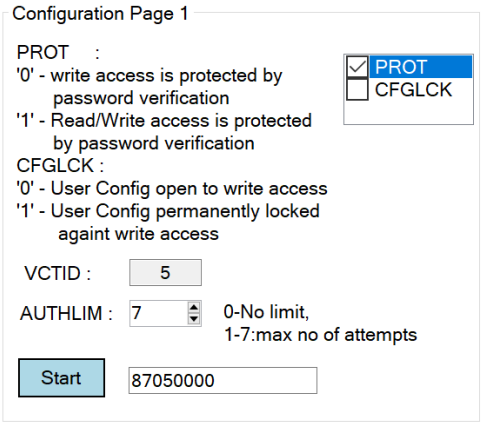
10:37:06 AM, RX : 02 00 00 1B 00 07 04 A6 2D 3A D2 59 84 00 00 77 77 77 77 00 00 00 00 00 00 00 00 00 00 00 A4 03

13. Configuration Page 1

Configuration pages are used to configure the memory access restriction of the card.

In the configuration page 1, the items that worth pay attention are:

Item	Description
PROT	'0' – write access is protected by the password verification. '1' – read and write access is protected by the password verification.
CFGLOK	'0' – user configuration open to write access. '1' – user configuration permanently locked against write access.
AUTHLIM	Limitation of negative password verification attempts 0 – No limitation. 1 to 7 – Maximum number of failed attempts.
VCTID	Virtual Card Type Identifier It is recommended not to change the default value of 05 hex.

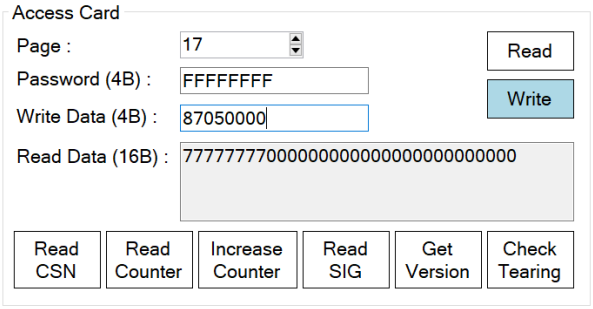


Above setting check the PROT, and set AUTHLIM to 7. Click 

, system will generate a 4B data, and copy this data to the 'Write Data (4B)', as shown below.

Item	Value
Page	17
Password (4B)	FFFFFFFF
Write Data (4B)	87050000

Depends on the card type, the address for Configuration Page 1 may be different from the example shown below. Please check the card manual for details.

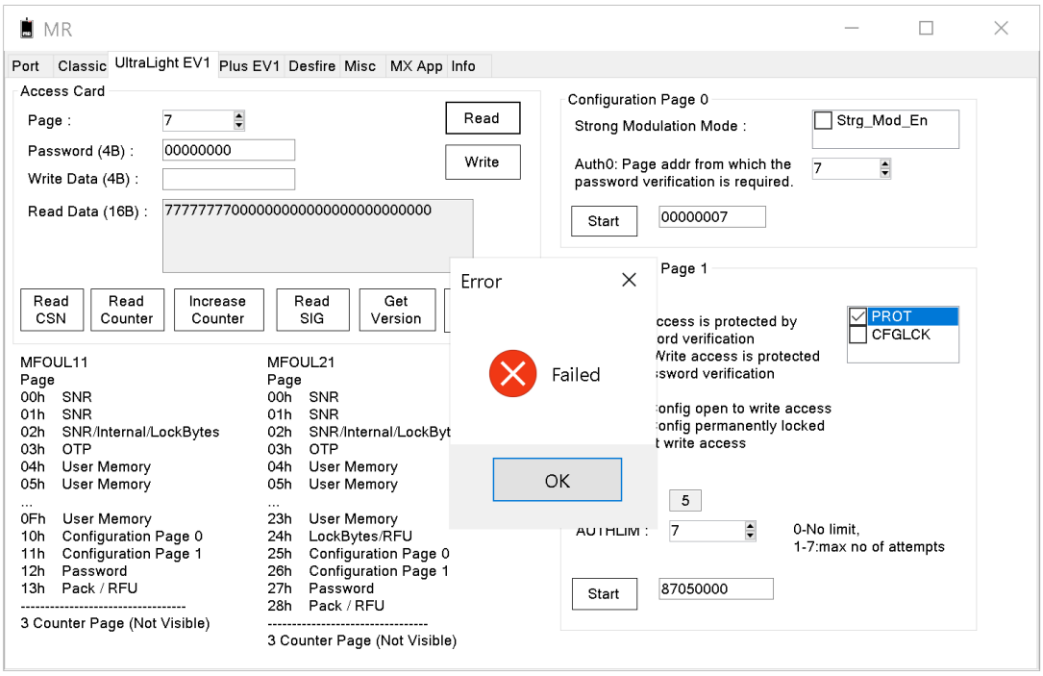


Click 

to program the Configuration Page 1. This setting will make read and write access require password verification, and the number of failed attempts is 7.

We will try the read and write access now. Bear in mind that accessing page 7 and above will require password verification, so we will try to access page 7. First, we supply a false password, 00000000 hex, and then the correct password, FFFFFFFF hex.

Item	Value
Page	7
Password (4B)	00000000
Write Data (4B)	



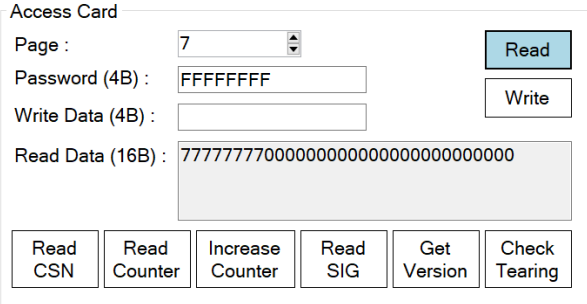
Click 

, but the process was not successful. The protocol shows error. Clearly, read access require password verification now.

Now we set the password correctly.

Item	Value
Page	7
Password (4B)	FFFFFFFF

Write Data (4B)	



Click 

, and now the process was successful. Therefore, read and write access require password verification now.

Also, we have set the AUTHLIM to 7 attempts. If you supply a wrong password for verification, and fail 7 times continuously, the protected memory in the card will be permanently locked. But any successful verification before reaching the limit of failed attempts, will reset the internal error counter to zero.

You may try it yourself.

Function : UltraLight Write

10:41:54 AM, TX : 02 00 00 0B 1C A2 FF FF FF FF 11 87 05 00 00 24 03

10:41:54 AM, RX : 02 00 00 0B 00 07 04 A6 2D 3A D2 59 84 00 0A BE 03

Function : UltraLight Read

10:42:41 AM, TX : 02 00 00 07 1C 30 00 00 00 00 07 2E 03

10:42:41 AM, RX : 02 00 00 01 59 5A 03

Function : UltraLight Read

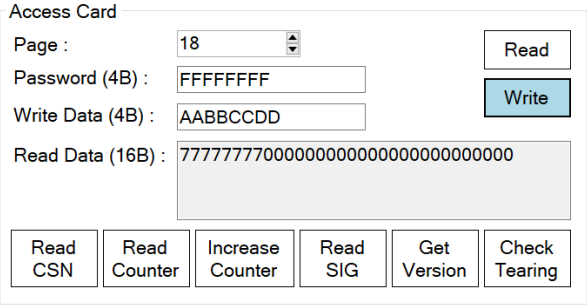
10:44:21 AM, TX : 02 00 00 07 1C 30 FF FF FF FF 07 2E 03

10:44:22 AM, RX : 02 00 00 1B 00 07 04 A6 2D 3A D2 59 84 00 00 77 77 77 77 00 00 00 00 00 00 00 00 00 00 00 A4 03

14. Change Password

We may change the default password to other value for better security. Depends on the card model, the address of the password may be different from the address that shown in this example. The Password register for our sample card is located at page 12 hex, or page 18 in decimal.

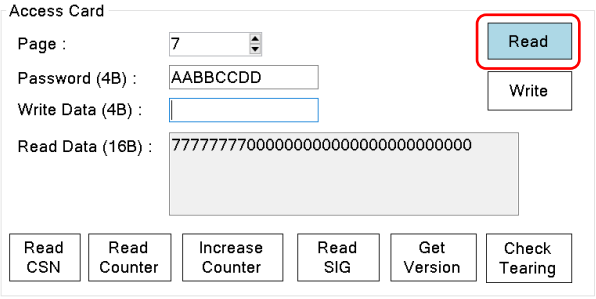
Item	Value
Page	12 hex or 18 decimal
Password (4B)	FFFFFFFF
Write Data (4B)	AABBCCDD



Click 

to change the default password from FFFFFFFF hex to AABBCCDD hex. For this card model, the password register is located at address 12 hex.

We may verify the new password now.



Click 

to read page 7 using new password, OK.

Function : UltraLight Write

10:46:52 AM, TX : 02 00 00 0B 1C A2 FF FF FF FF 12 AA BB CC DD A5 03

10:46:52 AM, RX : 02 00 00 0B 00 07 04 A6 2D 3A D2 59 84 00 0A BE 03

Function : UltraLight Read

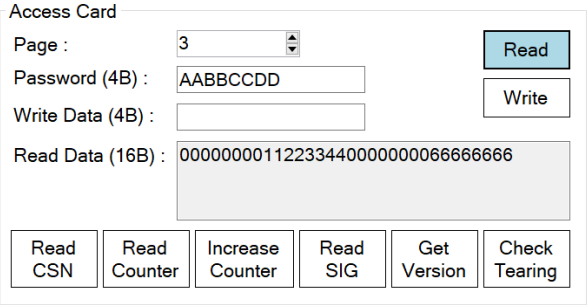
10:47:21 AM, TX : 02 00 00 07 1C 30 AA BB CC DD 07 2E 03

10:47:22 AM, RX : 02 00 00 1B 00 07 04 A6 2D 3A D2 59 84 00 00 77 77 77 77 00 00 00 00 00 00 00 00 00 00 00 A4 03

15. OTP

Page 3 is the 4B OTP page. This memory area can be used as a 32 tick one-time counter. When the bit is set to '1', it cannot be changed back to '0'.

Item	Value
Page	3
Password (4B)	AABBCCDD
Write Data (4B)	

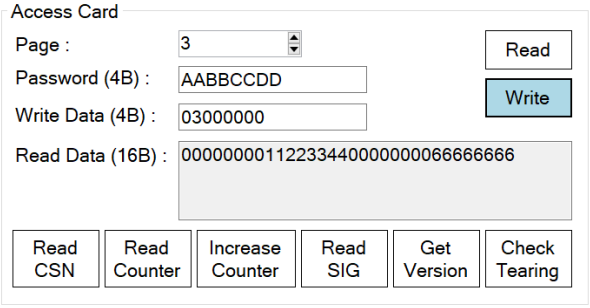


Click 

to read OTP value. The current value is 00000000 hex.

We will now perform two writes to OTP page; firstly 03000000 hex, and secondly 04000000 hex. Then we will read it out.

Item	Value
Page	3
Password (4B)	AABBCCDD
Write Data (4B)	03000000

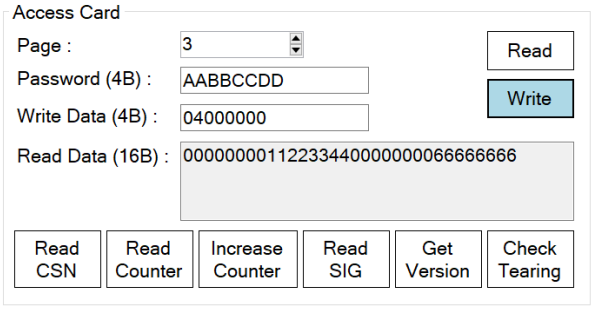


Click 

to write 03000000 hex to OTP page.

Next we will write 04000000 hex to OTP page.

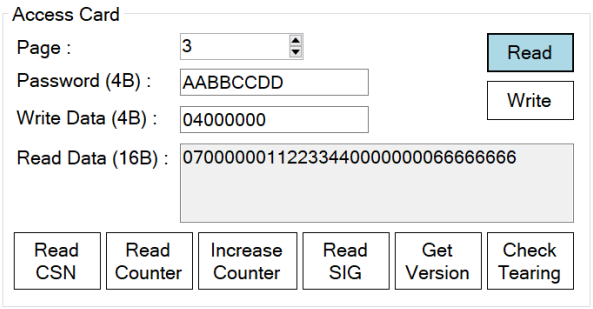
Item	Value
Page	3
Password (4B)	AABBCCDD
Write Data (4B)	04000000



Click 

to write 04000000 hex to OTP page.

Now, we will read out the OTP page.



Click 

to get the OTP value. The current OTP value is 07000000 hex. Once the bit is set to '1', it cannot be rolled back to '0'.

Function : UltraLight Read

10:48:29 AM, TX : 02 00 00 07 1C 30 AA BB CC DD 03 2A 03

10:48:30 AM, RX : 02 00 00 1B 00 07 04 A6 2D 3A D2 59 84 00 00 00 00 00 00 11 22 33 44 00 00 00 00 66 66 66 66 E0 03

Function : UltraLight Write

10:50:32 AM, TX : 02 00 00 0B 1C A2 AA BB CC DD 03 03 00 00 00 B7 03

10:50:32 AM, RX : 02 00 00 0B 00 07 04 A6 2D 3A D2 59 84 00 0A BE 03

Function : UltraLight Write

10:50:34 AM, TX : 02 00 00 0B 1C A2 AA BB CC DD 03 04 00 00 00 B0 03

10:50:34 AM, RX : 02 00 00 0B 00 07 04 A6 2D 3A D2 59 84 00 0A BE 03

Function : UltraLight Read

10:50:45 AM, TX : 02 00 00 07 1C 30 AA BB CC DD 03 2A 03

10:50:45 AM, RX : 02 00 00 1B 00 07 04 A6 2D 3A D2 59 84 00 00 07 00 00 00 11 22 33 44 00 00 00 00 66 66 66 66 E7 03

16. Pack

This is a 16 bit password acknowledge used during password verification.

By default, after successful password verification, the card will return 0000 hex. But you may change it to other value, such as 1122 hex. So after successful password verification, the card will return 1122 hex and not 0000 hex anymore.

But since reader will handle the communication from card internally, this feature is not significant here.

17. End