



IDENTIVE

User Manual

Multi-ISO Keyboard Configurator

Document history

Revision	Date	Author	Description
1.0	April 2013	Timo Baur	Initial version
1.1	September 2013	Timo Baur	Added info about default keys (sec. 8.2) Added info why a tag is needed (sec. 2) Added description for reversed UID option Renamed file name Updated screenshots for GUI V1.3

Content

1. Abstract	3
2. Requirements	3
3. Application start	3
4. Main application screen	4
5. Reader selection	4
6. Import/export configuration	5
7. Keyboard interface settings	5
7.1. General	5
7.2. Tag memory read settings	7
7.3. Set configuration	10
8. Reader configuration	10
8.1. Reader authentication	10
8.2. Tag key settings	11
9. Troubleshooting	12
10. Terms & Abbreviations	13

1. Abstract

The “Identive Multi-ISO Keyboard Configurator” tool enables you to change several settings of the reader’s keyboard interface behaviour as well as tag keys and tag memory location to be read. It provides the following features:

- Enable/disable HID interface
- Enable tag UID (Unique Identification number for chips) reading
- Enable tag memory reading for user defined tag data
- Set access keys in the reader for MIFARE Classic, DESFire and Ultralight C
- Change the default delimiter and character delay to a custom value

2. Requirements

Operating System:	any OS with Java Runtime Environment (JRE)
Screen resolution:	1280x800 or higher
CCID/HID reader firmware:	1.22 or higher
For tag memory reading function:	tag compliant to ISO15693 or ISO14443 (MIFARE Classic 1k/4k, MIFARE Ultralight/Ultralight C, MIFARE DESFire, NTAG 203 or Topaz)
For UID reading function:	all ISO14443 & ISO15693 compliant tags

The configurator needs a card just to connect to the reader before writing the configuration inside the reader’s flash memory. No data from the card is accessed during this process.

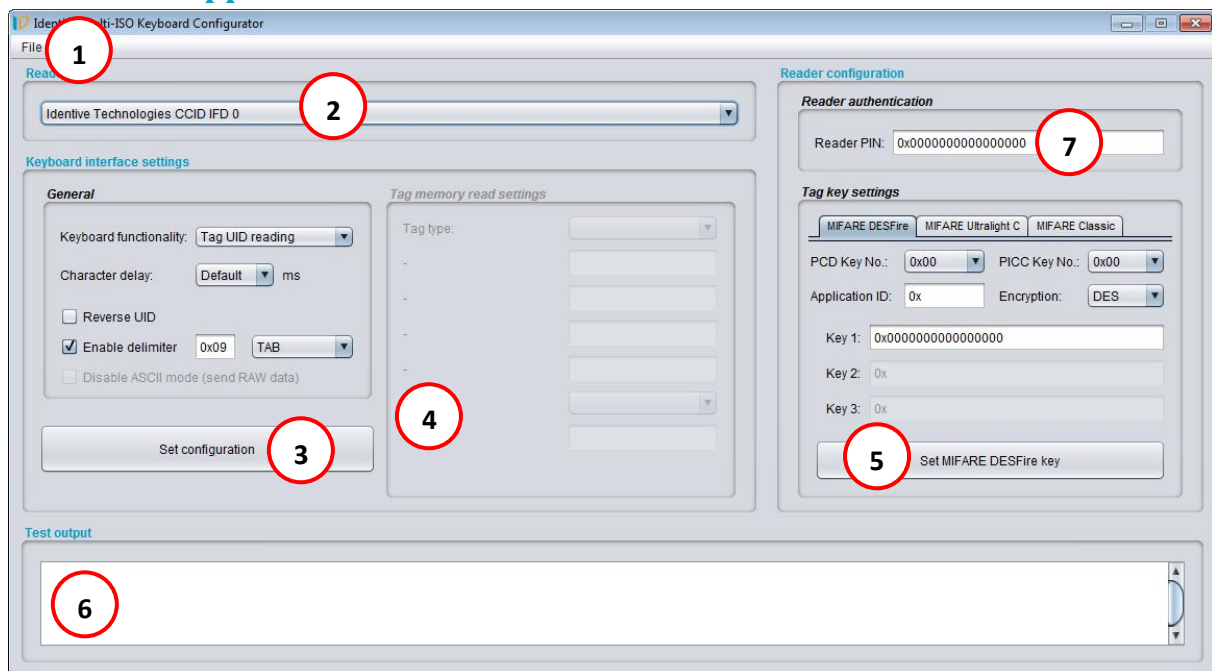
3. Application start

Double click on the application icon (Multi-ISO_Keyboard_Configurator.jar). No installation required, the application will start without further user interaction, if the device is already connected to the host system.



Multi-ISO_Keyboard_C
onfigurator.jar

4. Main application screen

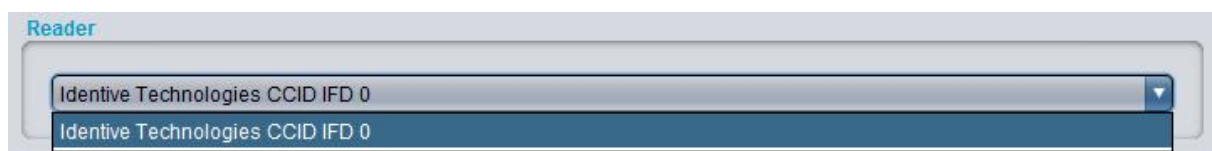


- (1) Import/export keyboard emulation configuration & show application version
- (2) List of connected readers
- (3) Set interface options for keyboard emulation
- (4) Set options for tag memory reading function, if enabled in (3)
- (5) Set authentication options for MIFARE DESFire, Classic and Ultralight C
- (6) Test reader output for the chosen configuration
- (7) Set PIN for reader authentication

5. Reader selection

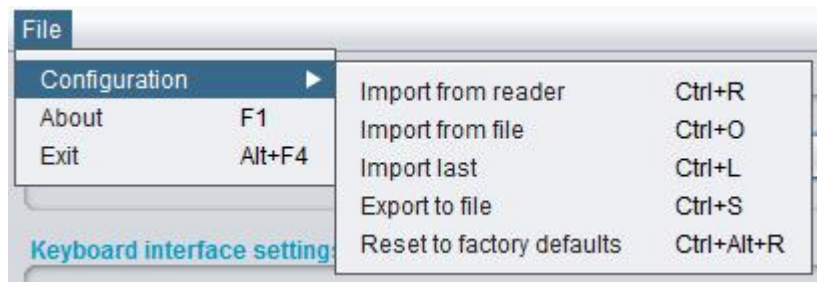
Choose and select the Identive Multi-ISO CCID reader in the “Reader” dropdown menu enumerated as “Identive Technologies CCID IFD x” where ‘x’ indicates the reader number if multiple devices are connected.

Note: Multi-ISO readers with PC/SC firmware loaded will not be listed.



6. Import/export configuration

To import or export configurations for the keyboard emulation function please click on “File” in the menu bar and select “Configuration”:



Options in the “Configuration” sub-menu:

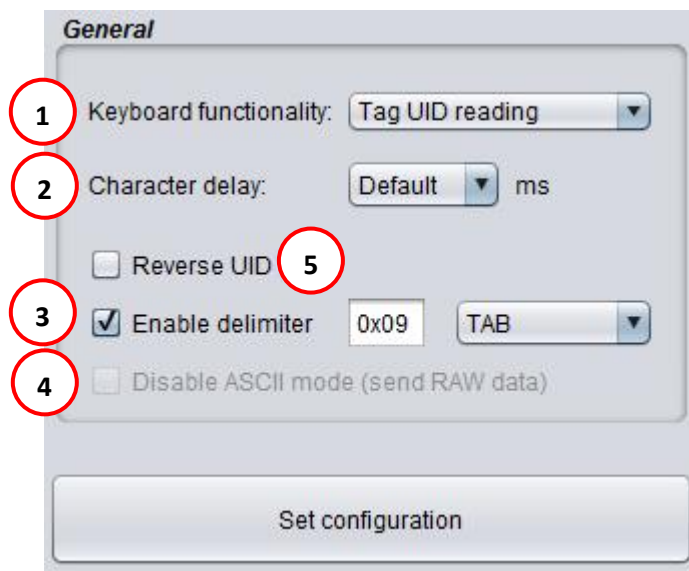
- Import from reader import configuration from the selected reader
- Import from file import configuration from *.cfg file
- Import last import recently used configuration automatically saved as last.cfg in the application folder
- Export to file save the current configuration as *.cfg file
- Reset to factory defaults resets the configuration to firmware default values

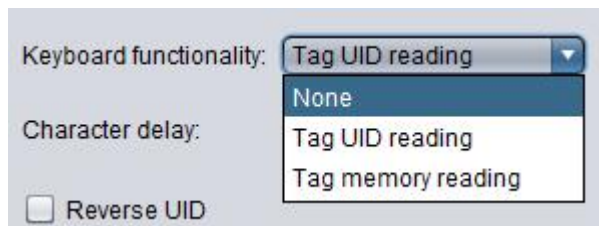
Instead of clicking on a menu item you could also use the respective keyboard shortcut.

7. Keyboard interface settings

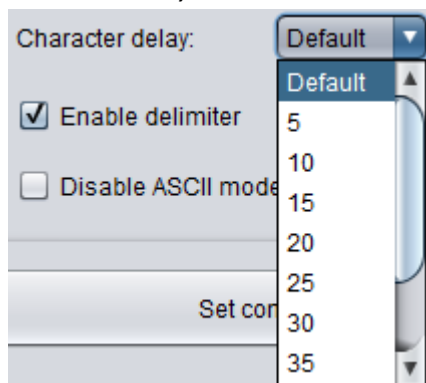
Describes available options for the keyboard interface and how to configure the data output.

7.1. General

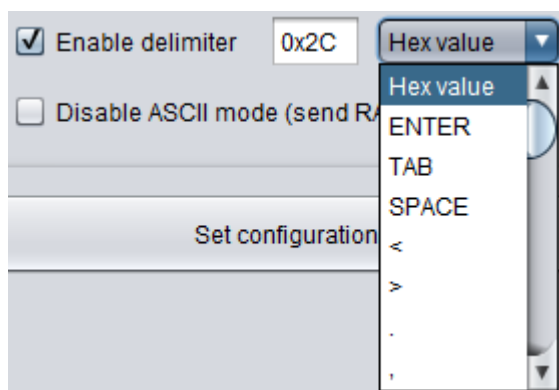


(1) *Keyboard functionality:*

- None = keyboard emulation disabled – CCID still available
- Tag UID reading = automatic output of tag UID (in ASCII)
- Tag memory reading = automatic output of user defined tag memory location (for settings see chapter 7.2)

(2) *Character delay:*

Select the delay to display each character of the data output in milliseconds. Default value set in the firmware is 5 ms.

(3) *Delimiter:*

If you do not want the reader to add a delimiter at the end of each keyboard output untick the checkbox next to “Enable delimiter”. If checkbox is ticked, you can choose the delimiter either by entering the hex value of the desired ASCII code (select “Hex value” in the dropdown list) in the text box (e.g. 0x00 for no delimiter) or select one of the predefined delimiters in the drop down list. The delimiter is always added directly at the end of the sent data. Default delimiter is “TAB”.

Examples:

Tag UID	Delimiter	Keyboard output
D034381	#	D034381#
D034381 & D034382	SPACE	D034381 D034382
D034381 & D034382	ENTER	D034381 D034382

Note: With OS keyboard layout different from English (US) the output may show a different delimiter than the one selected in the application. This is not an error of the reader but a result of the ASCII table for the selected keyboard layout. Technically the application that would wait for the keystrokes would receive the intended hex value as the delimiter.

(4) *Disable ASCII mode (send RAW data):*


If checkbox is ticked, the keyboard output is transferred without ASCII conversion. This function is needed only if the content to be read from the tag memory is already stored in ASCII format and hence the reader need not perform further ASCII conversion but rather could just send the RAW data that is received from the tag to the host.

(5) *Reverse UID*

If checkbox is ticked, the UID output is byte-reversed, e.g. if the chip UID is 4CEA3271 the output will be 7132EA4C. This option only works with CCID+HID firmware version 1.24 or newer.

7.2. Tag memory read settings

If this option was selected in chapter 7.1, step (1) you can define the location of the data you want to output at the cursor position, else continue with chapter 7.3). Inputs are allowed as hexadecimal (e.g. 0x0A) and decimal values.



(1) *Card type:*

Select chip type you want to use with the reader. Available options are:

- ISO15693
- MIFARE Classic 1K
- MIFARE Classic 4K
- MIFARE Ultralight
- MIFARE Ultralight C
- MIFARE DESFire
- NTAG 203
- Topaz

(2) *Tag memory settings:*

Depending on the selection made in (1) various options will be shown. Please refer to the respective tag IC documentation for details.

Tag IC independent settings:

- **Byte offset within block:**
sets the number of bytes to skip until start of reading; enter 0 for no offset
- **Number of bytes to read:**
sets the number of bytes read

(a) **ISO15693:**

Card type:	ISO15693 ▼
Block number:	<input type="text"/>
Byte offset within block:	<input type="text"/>
Number of bytes to read:	<input type="text"/>

(b) **MIFARE Classic 1k / 4k:**

Card type:	MIFARE Classic 1k ▼
Block number:	<input type="text"/>
PCD key number:	<input type="text"/>
Byte offset within block:	<input type="text"/>
Number of bytes to read:	<input type="text"/>

(c) MIFARE Ultralight / Ultralight C:

Card type:	MIFARE Ultralight ▼
Page number:	<input type="text"/>
Byte offset within page:	<input type="text"/>
Number of bytes to read:	<input type="text"/>

(d) MIFARE DESFire:

Card type:	MIFARE DESFire ▼
Application ID:	<input type="text"/>
PICC key number:	<input type="text"/>
File number:	<input type="text"/>
Byte offset within block:	<input type="text"/>
Auth. type:	Plain ▼
Number of bytes to read:	<input type="text"/>

Auth. type:

Please choose the used encryption for authentication with the chip in the pulldown list or select “Plain” in case of no encryption.

Plain ▼
Plain
DES
2K3DES
3K3DES
AES

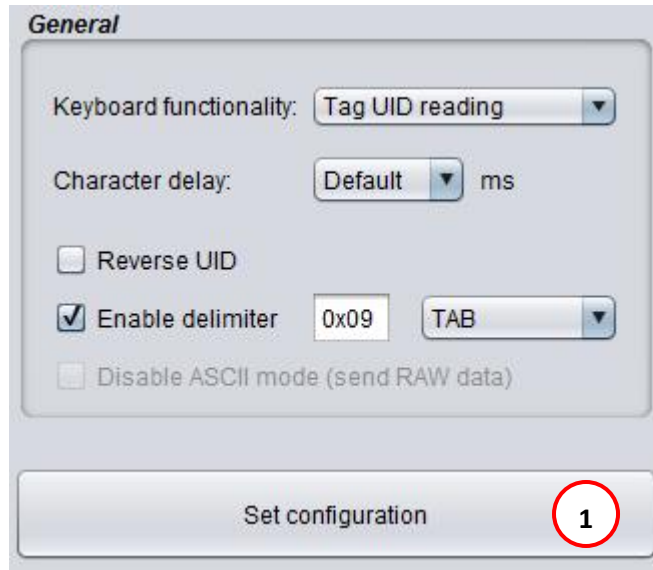
(e) NTAG 203:

Card type:	NTAG 203 ▼
Page number:	<input type="text"/>
Byte offset within page:	<input type="text"/>
Number of bytes to read:	<input type="text"/>

(f) Topaz:

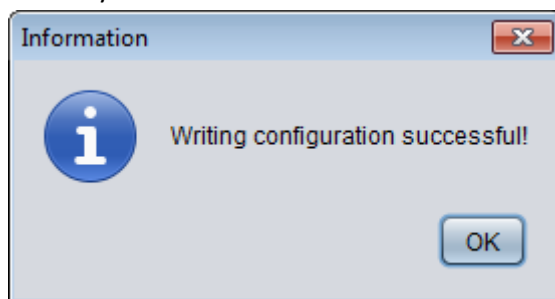
Card type:	Topaz ▼
Block number:	<input type="text"/>
Byte offset within block:	<input type="text"/>
Number of bytes to read:	<input type="text"/>

7.3. Set configuration



(1) Set configuration:

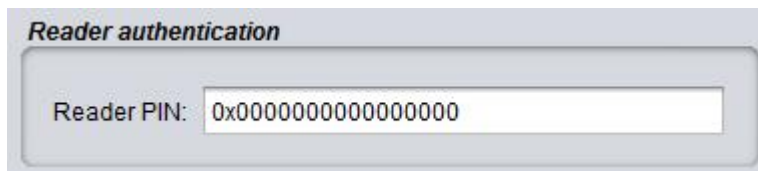
To store the configuration parameters (done in steps 1 – 4) into the reader's configuration sector into you need to place a supported tag on the reader before you click on the "Set configuration" button. If no tag is present an error message is shown. A success message is displayed when the configuration has been stored correctly:



8. Reader configuration

8.1. Reader authentication

To make changes to the tag key settings (see chapter 8.2) the reader PIN is required for authentication purpose. PIN only accepted as hexadecimal value.



8.2. Tag key settings

In this section you can manage the authentication settings for MIFARE Classic, MIFARE DESFire and MIFARE Ultralight C which are needed to communicate with the tag. For DESFire tags you can set authentication keys for each application on the tag. Please check your tag IC documentation for details. Keys are written into the reader's internal flash memory. A fresh reader from the manufacturer is pre-programmed with default keys of the respective card IC. If no keys are set in this section the default keys will be used by the reader.

8.2.1. MIFARE DESFire

The screenshot shows the 'MIFARE DESFire' configuration window. It has three tabs: 'MIFARE DESFire' (selected), 'MIFARE Classic', and 'MIFARE Ultralight C'. The interface includes the following fields and controls:

- PCD Key No.:** A dropdown menu with '0x00' selected.
- PICC Key No.:** A dropdown menu with '0x00' selected.
- Application ID:** A text input field containing '0x'.
- Encryption:** A dropdown menu with 'DES' selected.
- Key 1:** A text input field containing '0x0000000000000000'.
- Key 2:** A text input field containing '0x'.
- Key 3:** A text input field containing '0x'.
- Set MIFARE DESFire key:** A large button at the bottom.

Inputs only allowed in hexadecimal values. After all inputs are made, put a supported tag on the reader and click on “Set MIFARE DESFire key” to load the configuration into the reader. If configuration was successfully written a confirmation is shown, else you will see an error message (see chapter 9).

Notes:

AES in the “Encryption” dropdown list is only available with DESFire EV1 tags. Greyed out key numbers are not supported by the selected encryption method. PCB

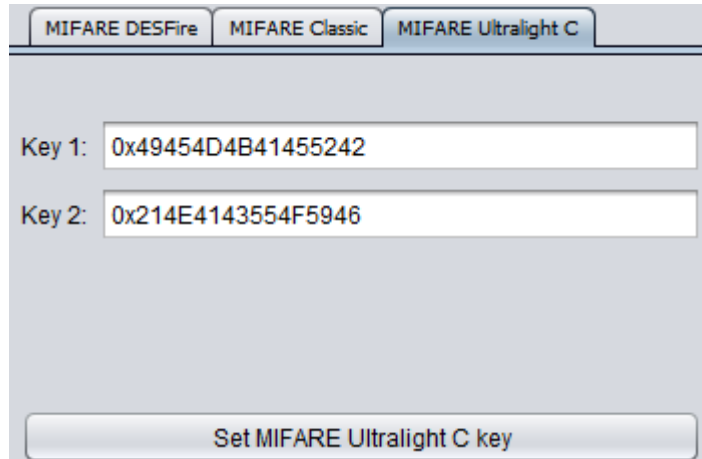
8.2.2. MIFARE Classic

The screenshot shows the 'MIFARE Classic' configuration window. It has three tabs: 'MIFARE DESFire', 'MIFARE Classic' (selected), and 'MIFARE Ultralight C'. The interface includes the following fields and controls:

- Key number:** A dropdown menu with '0x00' selected.
- Key type:** A dropdown menu with 'Type A' selected.
- Key:** A text input field containing '0xFFFFFFFF'.
- Set MIFARE Classic key:** A large button at the bottom.

Inputs only allowed in hexadecimal values. After all inputs are made, put a supported tag on the reader and click on “Set MIFARE Classic key” to load the configuration into the reader. If configuration was successfully written a confirmation is shown, else you will see an error message (see chapter 9)

8.2.3. MIFARE Ultralight C



Inputs only allowed in hexadecimal values. After all inputs are made, put a supported tag on the reader and click on “Set MIFARE Ultralight C key” to load the configuration into the reader. If configuration was successfully written a confirmation is shown, else you will see an error message (see chapter 9).

9. Troubleshooting

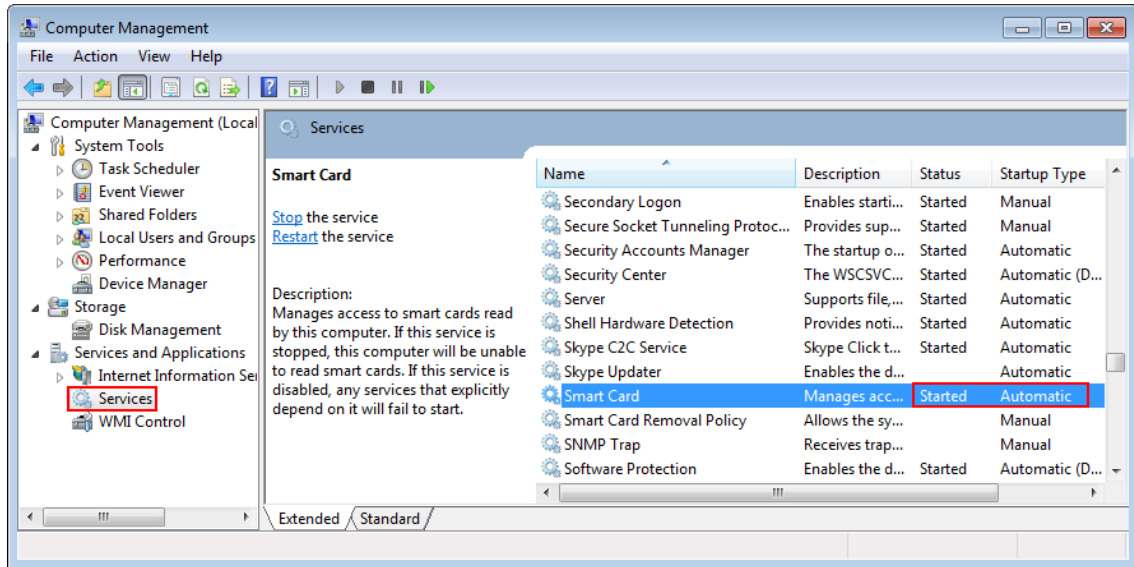
1. Problem:

The Multi-ISO reader with Keyboard Emulation is not shown in the reader list of the tool.

Solution:

Please verify that the “Smart Card” service is *enabled* and start mode is *automatic*.

Right click on the “Computer” icon on the desktop and choose “Manage”. Then move to the services section of the “Computer Management” on the left side and search for “Smart Card” service. Double click on the service entry and make the above mentioned changes:



2. Problem:

When I click on “Set Configuration” I get the error message “Could not create valid APDU command: Invalid Index!”.

Solution:

Please make sure that the reader is connected. If the reader is connected please refer to solution described in 1)

10. Terms & Abbreviations

Terms & Abbreviations	Description
2K3DES	2 Key Triple Data Encryption Standard
3K3DES	3 Key Triple Data Encryption Standard
AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
CCID	Chip Card Interface Device
DES	Data Encryption Standard
IFD	Interface Device
HF	High Frequency (13.56 MHz)
HID	Human Interface Device
PCD	Proximity Coupling Device
PC/SC	Personal Computer/Smart Card
PICC	Proximity Integrated Chip Card
PIN	Personal Identification Number