OMNIKEY 5x27CK Keyboard Wedge Configuration and Custom Report

User Guide

5127-902, Rev E.1

January 2018

hidglobal.com

Copyright

Trademarks

Revision History

Date	Description	Version
January 2018	Added information on OK5425 Gen2 and OK5127 Mini SP1	E.1
March 2016	Added information on OK5127CK-Mini.	E.0
December 2014	Extra detail added to tech order setting.	D.3
May 2014	EM4450 CSN added. Service Pack 3 features added. Additional information for usability.	D.1

Contacts

For additional offices around the world, see www.hidglobal.com/contact/corporate-offices

Americas and Corporate

611 Center Ridge Drive
Austin, TX 78753
USA
Phone: 866 607 7339
Fax: 949 732 2120

Asia Pacific

19/F 625 King's Road
North Point, Island East
Hong Kong
Phone: 852 3160 9833
Fax: 852 3160 4809

Europe, Middle East and Africa (EMEA)

Haverhill Business Park Phoenix Road
Haverhill, Suffolk CB9 7AE
England
Phone: 44 (0) 1440 711 822
Fax: 44 (0) 1440 714 840

Brazil

Condomínio Business Center
Av. Ermano Marchetti, 1435
Galpão A2 - CEP 05038-001
Lapa - São Paulo / SP
Brazil
Phone: +55 11 5514-7100

HID Global Technical Support: www.hidglobal.com/support

Contents

This page intentionally left blank.

Chapter 1

Overview

HID Global's OMNIKEY® 5x27CK readers open new market opportunities for system integrators seeking simple integration and development of readers using the standard Circuit Card Interface Device (CCID).

With the keyboard wedge functionality, users of OMNIKEY 5x27 CK readers can retrieve data from a card that is presented to the reader and directly input the card data into an application using keystroke emulation. This eliminates the need for customers to manually enter the card data into an application.

This guide explains how to setup the reader to use different card types in the Keyboard Wedge mode using the web browser interface.

In order to use the reader browser interface, the EEM-USB driver must be installed.

For installation instructions, see the *OMNIKEY 5x27CK Quick Start Guide* (5127-901).

Note: HID provides various Service Packs for the OMNIKEY 5x27CK. Some functions have been introduced with later Service Packs only. These exceptions are noted in this user guide. For downloading the latest Service Pack for your OMNIKEY 5x27CK reader, access the Developer Center: www.hidglobal.com/developer-center/omnikey-5x27ck.

Service Packs are available in the **Downloads** section, which requires a user account.

Check the firmware version of the OMNIKEY 5x27CK Reader from the General Overview tab in the built-in web interface. See Section 2: Reader Web Based Management Tool Interface.

1.1 References

Document Number	Description
5127-901	Quick Start Guide
5127-903	Software Developer Guide
AN0407	Firmware Upgrade

1.2 Abbreviations and Definitions

The following acronyms and abbreviations may be used in this document:

Abbreviation	Description
ASK	Amplitude Shift Key - a modulation schema for RF communications
BLE	Bluetooth Low Energy
CCID	Contact/Contactless Integrated Device
CHUID	Card Holder Unique Identifier
Config	Short for “Configuration”
CSN	Chip Serial Number
EEM	Ethernet Emulation Mode
FSK	Frequency Shift Key - a modulation schema for RF communications
FW	Firmware
GUID	Global Unique Identifier
HF	High Frequency - 13.56 MHz
HTTP	Hyper Text Transfer Protocol
HW	Hardware
KBW	Keyboard Wedge
LF	Low Frequency - 125 kHz “Prox”
OS	Operating System
PACS	Physical Access Control System
PSK	Phase Shift Key -a modulation schema for RF communications
RCN	Random Chip Number
RFID	Radio Frequency Identification

1.3 Supported RFID Technologies

1.3.1 LF Technologies (125 kHz)

Card Type	Data Availability	Technology
HID Prox	PACS	FSK
AWID Prox		FSK
Indala® Prox		PSK
EM Prox Family		ASK
EM4450 (CSN only)	Serial Number	ASK
HITAG 1, 2 and S	Serial Number	ASK

Note: There are many different card manufacturers that use EM Prox Chips with various programming formats that are operable with the OMNIKEY 5x27.

1.3.2 HF Technologies (13.56 MHz)

Card Type	Data Availability	Technology
iCLASS Seos®	RCN, PACS, Custom	Next Gen Smartcard
iCLASS®	CSN, PACS, Custom	Smartcard
MIFARE Classic®		
MIFARE DESFire EV1®		
MIFARE® Ultralight		
MIFARE DESFire® 0.6	CSN, Custom	
MIFARE Plus®		
CEPAS	CSN, CAN	
PIV	CSN, FASC-N, GUID, 75-bit GSA	
FeliCa	CSN, Custom	
Other ISO14443A	CSN	
Other ISO14443B		
Other ISO15693		

Note: NFC enabled devices that support NFC Card Emulation of one of the HF technology card types above are supported by the OMNIKEY 5x27.

1.3.3 Bluetooth Support (OK5127CK-Mini and OK5427 Gen 2)

HID Seos credentials can be read from any phone with satisfies the following requirements:

- Either Android version 4.3 or later or IOS 7 or later
- Bluetooth 4.0
- HID Mobile Access® app installed and running

This feature is only available on the OK5127CK-Mini and is not available on the original OK5127CK or OK5427CK.

1.4 Modes of Operation

1.4.1 EEEthernet Emulation Mode (EEM)

EEM is enabled by default to manage configuration settings via the embedded web based management tool or over TFTP. EEM operates in addition to any other interface to allow for access to configuration settings.

The only way to recover EEM once disabled is via a configuration card or MIB command in CCID Mode.

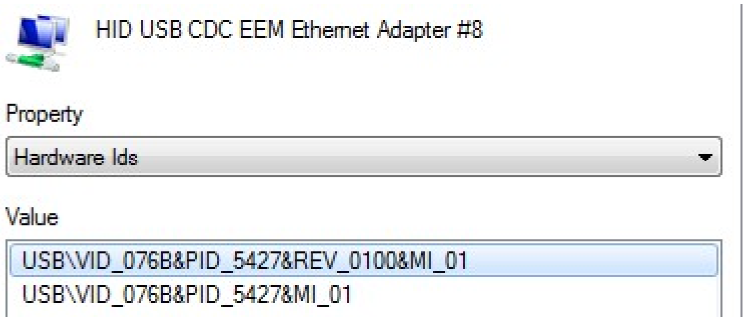
Enumeration

When EEM is operational, the OMNIKEY 5x27 will enumerate with the OS as a Network Adaptor in addition to enumerating as a Smart Card Reader, Keyboard, or Composite USB device. In a windows environment the device shown in device manager is:

HID USB CDC EEM Ethernet Adapter #n (n is the number of occurrence of the device)

The PID/VID for the device in this mode or operation mirrors the PID/VID for the CCID, Keyboard, or custom mode.

CCID Mode Operational



HID USB CDC EEM Ethernet Adapter #8

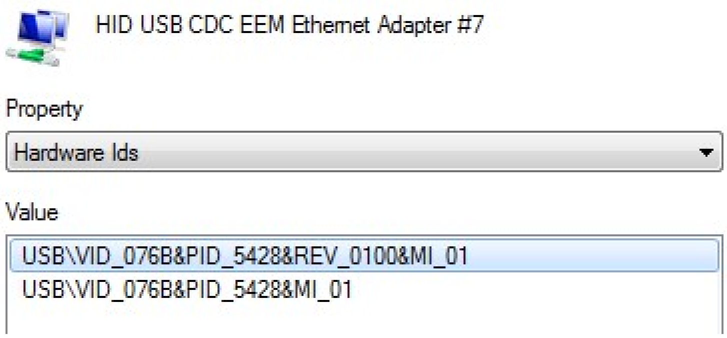
Property

Hardware Ids

Value

USB\VID_076B&PID_5427&REV_0100&MI_01
USB\VID_076B&PID_5427&MI_01

Keyboard Wedge Mode or Custom Report Mode is Operational



HID USB CDC EEM Ethernet Adapter #7

Property

Hardware Ids

Value

USB\VID_076B&PID_5428&REV_0100&MI_01
USB\VID_076B&PID_5428&MI_01

1.4.2 CCID

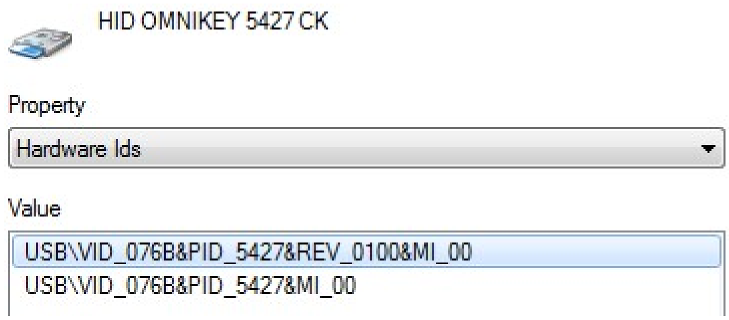
CCID is mainly used for read/write applications or with hosts that cannot support a keyboard input. CCID required an intelligent host and operates as a transparent PC/SC - CCID reader where the host controls every aspect of the card communication.

CCID mode must be active in order to create an OMNIKEY 5x27 configuration card as this requires read/write capability.

CCID mode cannot be operational when Keyboard Wedge mode is operational.

Enumeration

In CCID mode, the OMNIKEY 5427 enumerates with the OS as a Smart Card Reader.



HID OMNIKEY 5427 CK

Property

Hardware Ids

Value

USB\VID_076B&PID_5427&REV_0100&MI_00
USB\VID_076B&PID_5427&MI_00

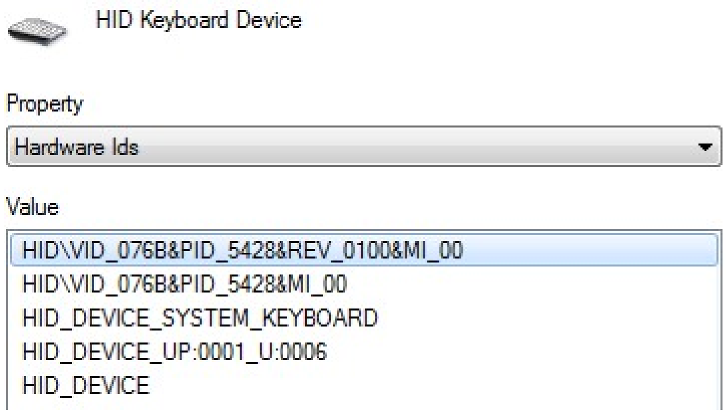
1.4.3 Keyboard Wedge

KBW mode supports read only applications and is fully configurable via the build in web based management tool, TFTP and configuration cards.

In KBW mode, the reader will access, buffer, process and report data as series of keyboard keystrokes to the host as configured.

Enumeration

When operating in KBW mode, the OMNIKEY 5x27 enumerates with the OS as a keyboard device.



HID Keyboard Device

Property

Hardware Ids

Value

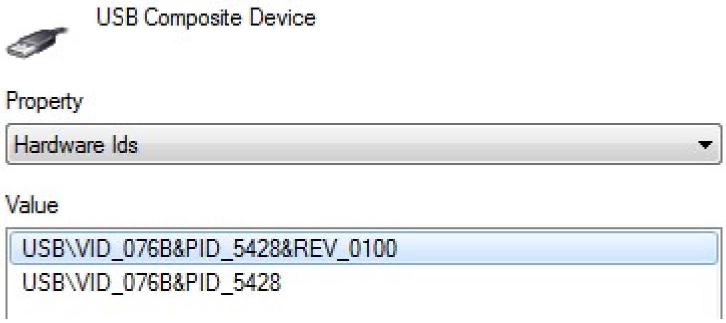
HID\VID_076B&PID_5428&REV_0100&MI_00
HID\VID_076B&PID_5428&MI_00
HID_DEVICE_SYSTEM_KEYBOARD
HID_DEVICE_UP:0001_U:0006
HID_DEVICE

1.4.4 Custom Report

Custom Report mode requires that KBW is enabled within the reader and outputs the configured data as raw HEX and not keyboard keystrokes.

Enumeration

In Custom Report mode the OMNIKEY 5x27 enumerates with the OS as a USB Composite Device in addition to enumerating as a keyboard.



USB Composite Device

Property

Hardware Ids

Value

USB\VID_076B&PID_5428&REV_0100
USB\VID_076B&PID_5428

1.4.5 Special Considerations

Due to the way that some operating systems handle USB devices, HID suggests that anyone using KBW or Custom Report mode designate 2 OMNIKEY 5x27 units for use with their PC to enable the following workflow.

- OMNIKEY 5x27 in KBW Mode - all testing and setup of parameters
- OMNIKEY 5x27 in CCID Mode - programming configuration cards
- Apply all KBW and Custom Report Mode Settings via configuration card

Note: Not following this approach requires that the user of the computer carefully manage the instances of the devices to prevent registry corruption.

Chapter 2

Reader Web Based Management Tool Interface

The OMNIKEY 5x27CK Reader has a built in, web based management tool that can be used to configure many aspects of the reader performance and behavior. This section provides a brief explanation of all the tabs, and the basic functions found under each tab for easy navigation and use.

Note: Due to how the Windows OS manages instances of devices, HID recommends that a single 5427CK device is used to build configurations. The configurations should be applied via configuration cards on a different host OS device. If this cannot be done, care must be taken to manage the device instances in Windows to prevent computer issues.

2.1 Preparations

The web based management tool is intended to allow users to configure device operating parameters manually with an intuitive UI that is easy to understand.

The Web Based UI is simply a user friendly interface which sends commands over to the reader over the EEM HTTP channel. The commands it uses are all documented in the *OMNIKEY 5X27CK Software Developer Guide* (5127-903).

HID suggests all integrators implement configuration/firmware upgrade capability.

When using CCID, it us strongly suggested that users investigate the Abstraction layer call ProcessKeyboardWedge command documented in the *OMNIKEY 5X27CK Software Developer Guide* (5127-903). This will often greatly simplify their application as it transfers much of the sequential process of reading specific data from cards to the reader. It also makes testing and debugging far easier.

2.1.1 Load the Ethernet Emulation Mode (EEM) Driver

The OMNIKEY 5x27 EEM Driver must be downloaded onto the Windows based PC and installed before plugging the reader into the USB port. The EEM Driver can be found on the OMNIKEY 5x27 Developer Center under **Downloads** or at http://www.hidglobal.com/drivers.

The EEM Driver currently supports the following 32 and 64 bit Windows OS versions:

- Windows 10
- Windows 7
- Windows Server 2008
- Vista
- XP

2.1.2 Load a Web Browser

As with any web based application, the internet browser directly affects the user experience. HID Global does everything possible to minimize the impact that different web Browsers have on the user experience. However, with frequent changes and the fact that the tool is an embedded FW web based tool, HID Global cannot fully guarantee interoperability with all web browsers.

Supported Web Browsers (English versions only)

- Internet Explorer, versions 8, 9, 10 and 11 (Compatibility Mode must be disabled)
- Microsoft Edge
- FireFox, version 53
- Chrome, version 58
- Opera, version 45

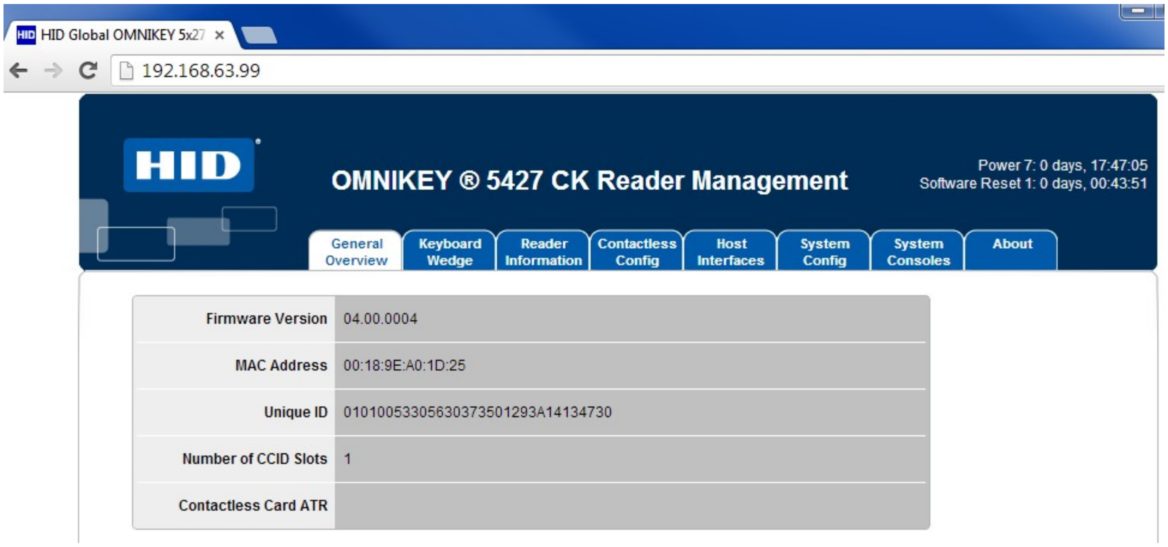
Known issues may exist with different FW revisions of the OMNIKEY 5x27 and specific browsers. Refer to the Firmware (FW) release notes for any known issues.

2.2 Navigating the 5x27CK Web Based Management Tool

Note: The PC used to access the web interface must be prepared as described in Section 2.1: Preparations, then connected to the Reader.

2.2.1 Accessing the Web Interface

1. Start a supported web browser.
2. Enter **http://192.168.63.99/** into the address bar and press **Enter**. The OMNIKEY 5127CK-Mini web server page launches with the General Overview tab selected, which is similar to the following page.



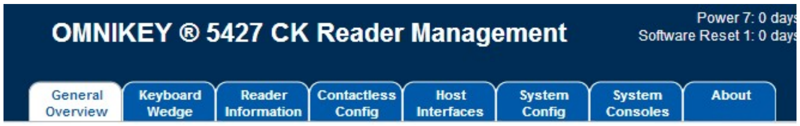
Power 7: 0 days, 17:47:05
Software Reset 1: 0 days, 00:43:51

Firmware Version	04.00.0004
MAC Address	00:18:9E:A0:1D:25
Unique ID	01010053305630373501293A14134730
Number of CCID Slots	1
Contactless Card ATR	

Note: The webserver may look slightly different for the OK5127CK-Mini or OK5427 Gen 2.

2.2.2 Navigating the Tabs

The following table describes the functions of each tab, which are similar to the following page detail.



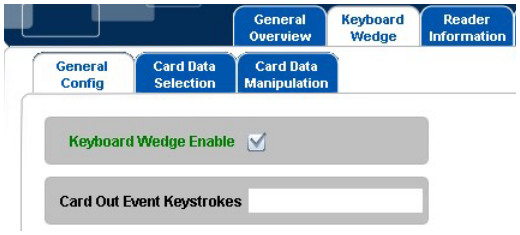
Tab	Description	Intended User Level
General Overview	A quick overview of reader information to include Main FW Version, MAC Address, UID of the reader, No. of CCID slots and the Contactless Card ATR.	Novice
Keyboard Wedge	Keyboard Wedge Setup Parameters.	Novice
Reader Information	Full view of the reader FW and HW state.	Novice
Contactless Config	RF and LED/Buzzer register settings.	Novice
Host Interfaces	Host interface configuration items for USB and Ethernet Emulation Mode.	Advanced
System Config	Reader configuration and FW management to include: ■ Apply, Reset and Store configuration changes ■ Reset all configuration to factory default ■ Load and download complete configuration files ■ Manage FW ■ Change access levels with passwords	FW and Configuration Parameters: Novice Change of access levels: Advanced
System Console	Interface to view actual USB traffic	Advanced
About	Acknowledgements and legal statements	N/A

2.2.3 Changing Settings

Modified settings are green at first and turn black when finalized using the **Apply Changes** option specified in step 3.

Modify Settings

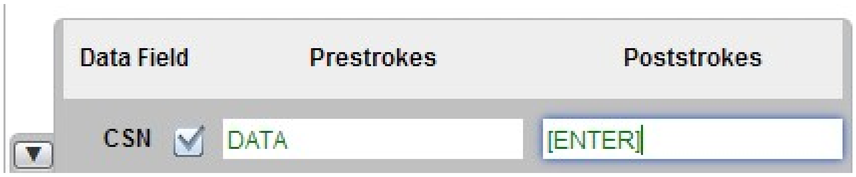
1. Change the configuration parameters as needed. The description or value color changes to green.



Keyboard Wedge Enable ☑

Card Out Event Keystrokes

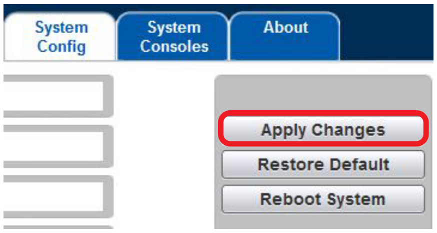
2. Press **Enter** to finalize text field changes including Special Characters such as **Enter**.



Data Field		Prestrokes	Poststrokes
CSN	☑	DATA	[ENTER]

Applying All Settings

3. Navigate to the **System Config** tab and click **Apply Changes**. The changed configuration parameters revert to black

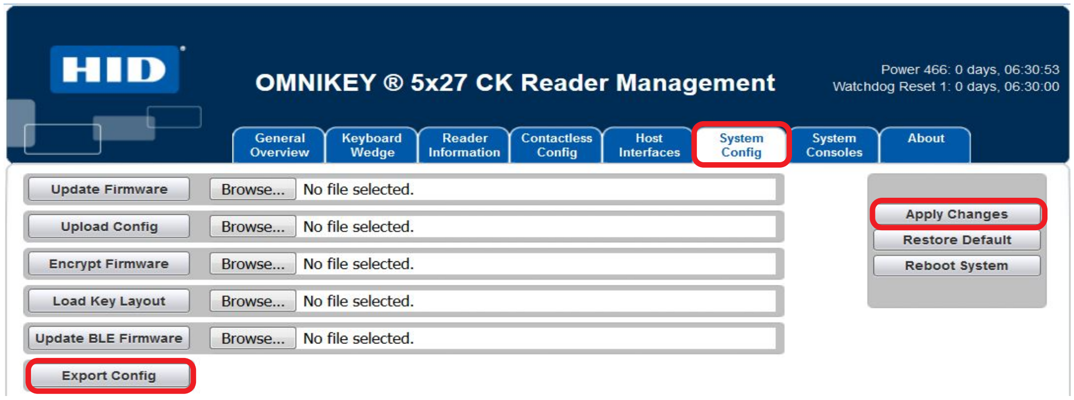


2.2.4 Downloading and Uploading Configurations

Downloading and uploading configuration files is an important feature of the OMNIKEY 5x27. Once a configuration is fully tested, it can be downloaded and used to make a configuration card using the hid_ok5x27ck_configcard_tool that can be downloaded from the Developer's Center.

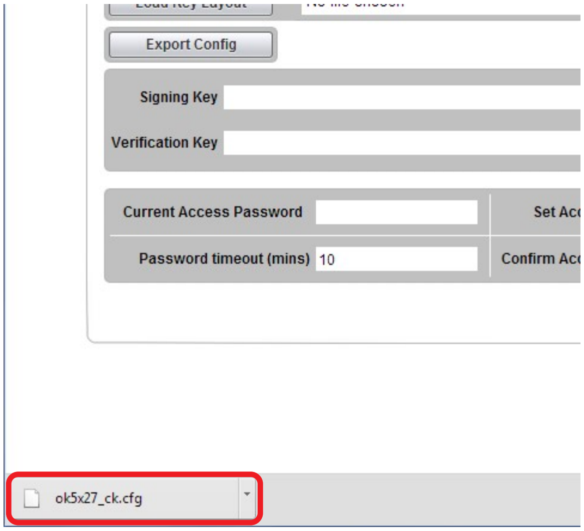
Download a Configuration File

1. On the **System Config** tab, change all configuration settings as needed.
2. Click **Apply Changes**.
3. Click **Export Config**



No file selected.
No file selected.
No file selected.
No file selected.
No file selected.

4. Rename the file to be specific to the configuration for future reference (the file will always be named **OK5x27ck.cfg** upon download).

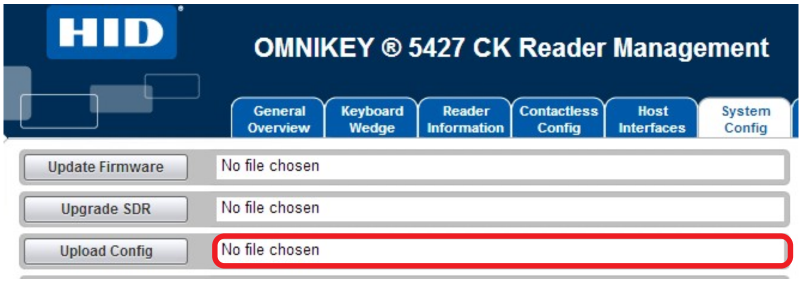


Current Access Password

Password timeout (mins) 10

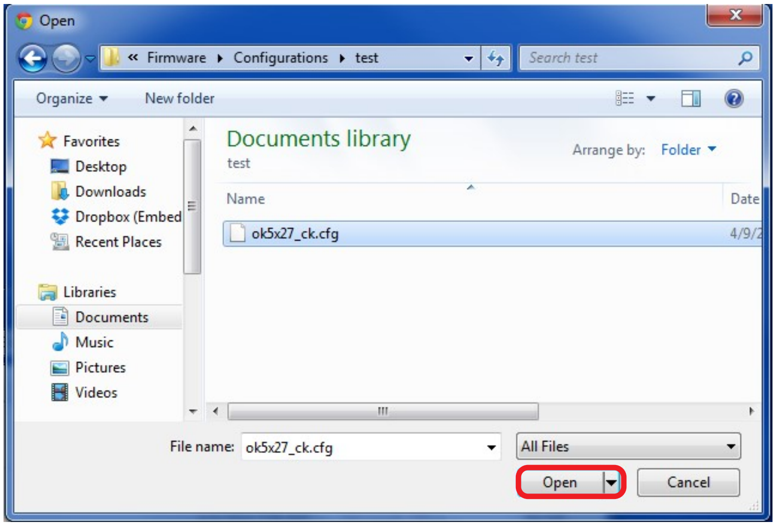
Uploading Configuration File

1. Select a file by clicking in the text box next to the **Upload Config** button.



Update Firmware: No file chosen
Upgrade SDR: No file chosen
Upload Config: No file chosen

2. Search for the configuration file in Windows Explorer, select the file and click **Open**.

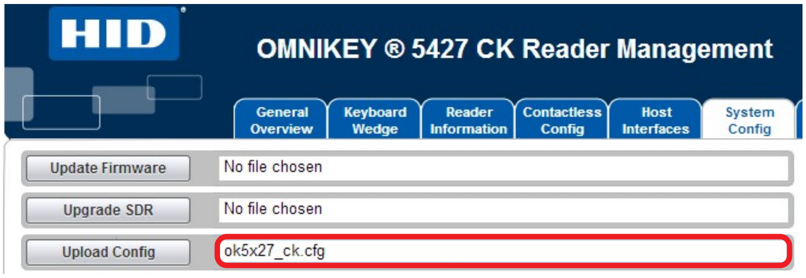


ok5x27_ck.cfg 4/9/2

File name: ok5x27_ck.cfg
All Files

The configuration file name is displayed in the text box.

3. To upload and apply the configuration contained in the file, click the **Upload Config** button.



Update Firmware: No file chosen
Upgrade SDR: No file chosen
Upload Config: ok5x27_ck.cfg

Note: Please bear in mind that DESFire Configuration cards will only update the parameters available in the web server UI and does not load keys, change Indala format, etc. Please contact an HID Sales, Presales Engineer or Field Applications Engineer for more details.

2.2.5 Setting a Web Server Password

The web page management tool for the OK5x27CK can be protected by a password. This restricts access to the web page based management tool only.

Password Entry Options

To set the password, enter the existing access password, the new password, and confirmation of the new password in the password section of the **System Config** tab.

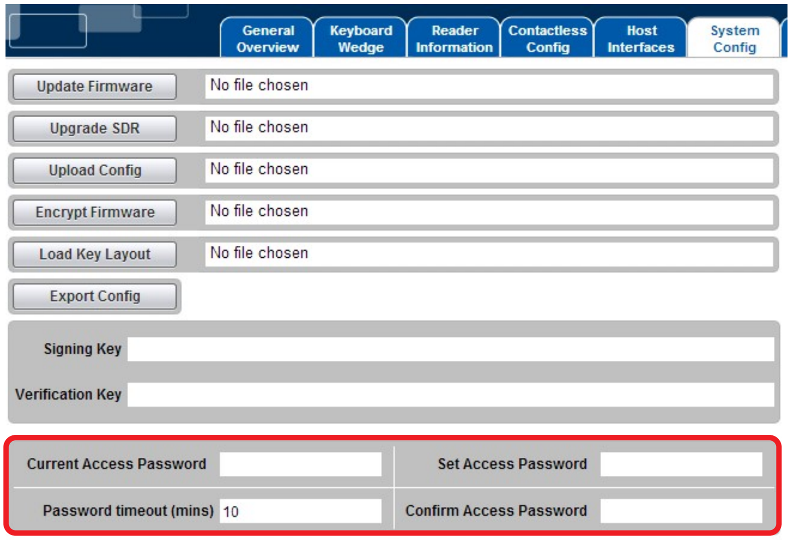
To send the password to the reader, place the cursor in one of the three password fields, then press **Enter**.

If there is no password currently set, leave the **Current Access Password** field blank.

To disable the password, leave both the **Set Access Password** and **Confirm Access Password** fields blank.

Once the password has been sent to the reader it will be necessary to click **Apply Changes** in order for the password to be kept after a system reboot.

The **Password timeout (mins)** field specifies the amount of time in minutes the current login session will last before the user will have to renter the password. To use an infinite timeout enter a value of zero (0).



Update Firmware: No file chosen
Upgrade SDR: No file chosen
Upload Config: No file chosen
Encrypt Firmware: No file chosen
Load Key Layout: No file chosen

Signing Key:
Verification Key:

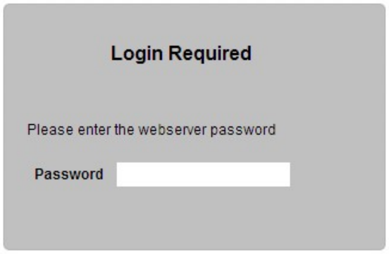
Current Access Password:
Set Access Password:
Password timeout (mins): 10
Confirm Access Password:

If you prefer, this can also be done by sending the following APDU to the reader:

CLA	INS	P1	P2	Lc	Data	
0xFF (Pseudo-APDU)	0x68 (OK5x27CK Command)	0x00 (MIB Command)	0x01 (MIB Control)	Length of password +2	0x05 (Password Entry Command)	ASCII Password + null terminating character

Login screen

Once a password is set, you will be automatically be presented with a log in screen on accessing the webserver. To login, enter the password created previously. If the password is entered incorrectly there will be a delay of several seconds before the password can be entered again.



Login Required

Please enter the webserver password

Chapter 3

Keyboard Wedge Mode

This section provides an exhaustive explanation of the embedded web based OMNIKEY 5x27CK Reader Management tool for Keyboard Wedge users.

The default configuration for the OMNIKEY 5x27CK is **CCID** mode. Before using the Keyboard Wedge Mode, enable Keyboard Wedge in the **Keyboard Wedge** tab.

3.1 Keyboard Wedge Operation Overview

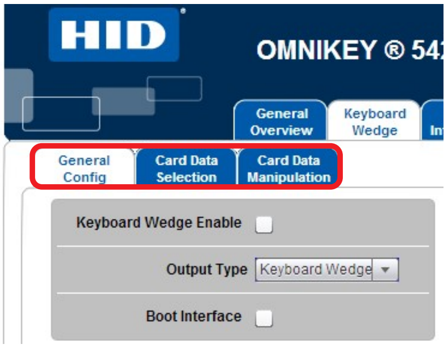
Keyboard wedge operation is a highly configurable read only application of the reader. Care should be taken to configure the product correctly and to only enable the card technologies and data that are needed at each installation individually to lower the likelihood and/or prevent rogue credentials from being introduced to the application.

The ProcessKeyboardWedge command detailed in the *OMNIKEY 5X27CK Software Developer Guide* (5127-903) is the HID recommended implementation.

3.2 Navigating the Keyboard Wedge Configuration Tabs

Note: The **Card Data Selection** and **Card Data Manipulation** tabs work in tandem. When changing the settings for the data output in the **Card Data Manipulation** tab, one is changing the output configuration for the active card technology in the **Card Data Selection** tab.

Tab	Description
General Config	Use this tab to enable and setup general keyboard wedge operational parameters.
Card Data Selection	Use this tab to enable and disable card technologies and select the data to be read from the card and reported across the keyboard interface automatically.
Card Data Manipulation	Use this tab to configure how the data selected in the Card Data Selection tab is output across the keyboard interface. Output options are Binary, Hexadecimal, ASCII, BCD and Decimal



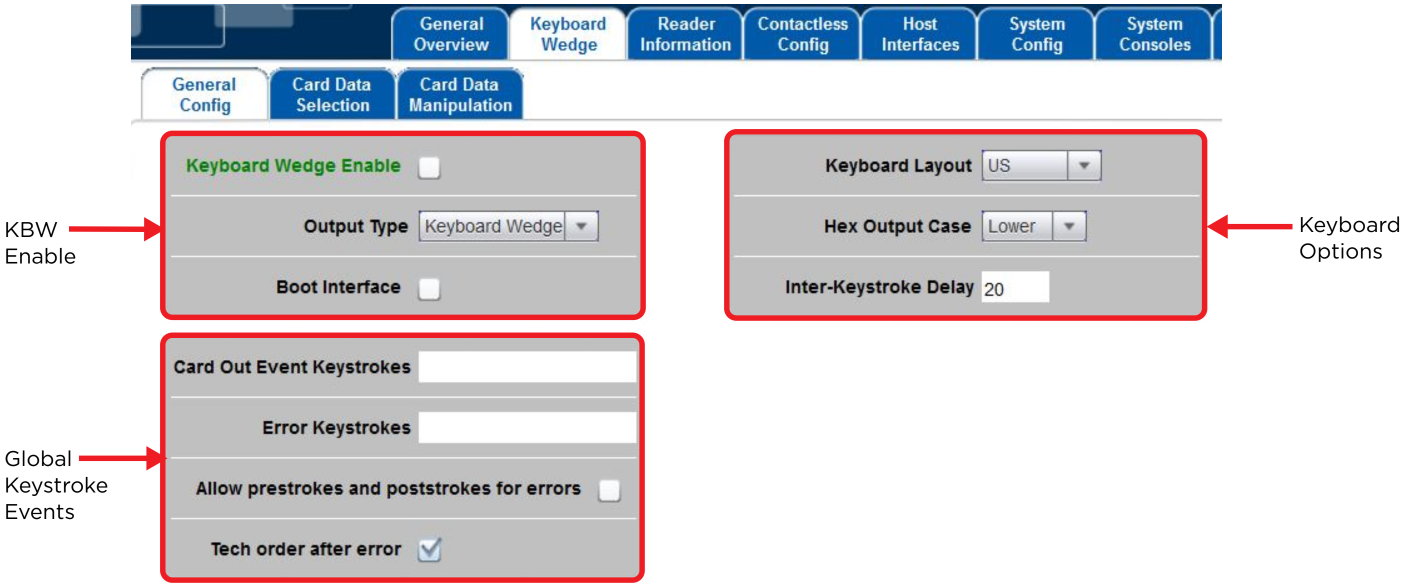
Keyboard Wedge Enable □

Output Type: Keyboard Wedge

Boot Interface □

3.3 General Config Tab

The **General Config** tab allows the user to configure general KBW operational settings that are not dependent on card type.



Keyboard Wedge Enable □

Output Type: Keyboard Wedge

Boot Interface □

Keyboard Layout: US

Hex Output Case: Lower

Inter-Keystroke Delay: 20

Card Out Event Keystrokes:

Error Keystrokes:

Allow prestrokes and poststrokes for errors □

Tech order after error ☑

3.3.1 KBW Enable Options

Keyboard Wedge Enable

To enable the Keyboard Wedge mode, select the **Keyboard Wedge** tab and select the **Keyboard Wedge Enable** option. Return to CCID mode by de-selecting the **Keyboard Wedge Enable** option.

Note: When Keyboard Wedge is selected, the 5x27CK enumerates as a Human-Interface USB device. Therefore, CCID interfaces are not be available. The web interface is available in both CCID and Keyboard Wedge modes.

Output Type (Firmware 03000000 or higher)

Keyboard wedge mode includes two output types, **Keyboard Wedge** and **Custom Report**.

Keyboard Wedge Output

The Keyboard Wedge output is the standard. The device enumerates as a keyboard and outputs the keyboard wedge data as a series of keystrokes.

Custom Report Output

When Custom Report output is enabled the device enumerates as a custom HID USB device and outputs data as raw APDU as follows:

- The packet size is 40 bytes.
- 1st byte is the length of data in the packet.
- 2nd byte is the version of the report.
- The following bytes contain the keyboard wedge data.
- In cases where the data length, version, byte length combine to less than the USB packet size (40 bytes), additional zeros are added for the remaining length.

HID Suggests the use of this mode of operation or using ProcessKeyboardWedge command in PC/SC-CCID mode when connected to a computer or other device. See *OMNIKEY 5X27CK Software Developer Guide* (5127-903).

Many people view this as a higher security option over keyboard wedge because no-one can remove the reader and attach it to a computer to see the data being output by the reader. However, most people only use the “Card Number” from HID PACS Data for non-PACS applications throughout the enterprise (E.g. cafeteria, payment, library, secure print, etc.) So, security is dependent upon the application and risk model.

Boot Interface (Firmware 03000000 or higher)

The Boot Interface option allows the device to advertise support for the keyboard boot interface in its HID device descriptor when it enumerates as a keyboard device. If enabled, the device is operational on host systems that only have minimal USB device handling, without support for full USB descriptor parsing.

3.3.2 Global Keystroke Events

These keystroke events are not card type dependent.

Card Out Event Keystrokes

The OMNIKEY 5x27 reports the keyboard strokes as configured when a supported card is presented and removed from the reader. These events are referred to as Card-in (presented) and Card Out (removed) events.

Card Out defines a set of keystrokes that are sent over the keyboard interface when a card is removed from the reader. Due to the card removal from the reader, those keystrokes are generic (card-independent) and apply to all card types supported by the reader. If the text box is left blank, no action is performed by the OMNIKEY 5x27 reader when a card is removed from the field.

Error Keystrokes

The OMNIKEY 5x27 reports the keyboard strokes as configured when a the reader fails to access, buffer, process and report a specific data field as configured in the **Card Data Selection** tab.

Possible instances of a failure are as follows:

- Multiple RFID tokens of the same ISO protocol are presented simultaneously to the reader and the card that is selected does not contain the data wanted.
- The key loaded and or selected in the reader does not match the key loaded onto the RFID token and access to the data field is denied.

Allow Pre-strokes and Post-strokes for Errors

When enabled, the pre-strokes and post-strokes configured in the **Card Data Selection** tab will be output by the reader upon an error occurring.

3.3.3 Keyboard Options

Keyboard Layout

This selection compensates differences in regional keyboard layouts (for example, different interpretation of Y key on a US and DE keyboard). This setting must be adjusted to the actual setting of the host system in which the 5x27CK is connected.

The following layouts are built into the reader:

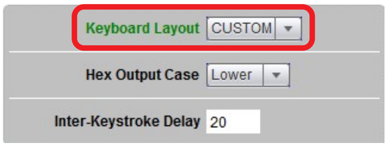
- France
- Germany
- United Kingdom
- United States

Example: A **Y** in the keyboard wedge layout **US** generates a **Z** on a host-PC using the German keyboard layout. Only when the keyboard wedge is configured to **DE** will the **Y** be interpreted correctly as a **Y** on the host-PC.

Custom Layout (Firmware 04000000 or higher)

The reader allows for any keyboard layout to be used with the reader. To use such a layout, follow these steps:

1. Create a keyboard layout file using Microsoft Keyboard Layout Creator.
2. Send the created file to HID tech support. They will convert this file to an encrypted file in the correct format for the reader to interpret.
3. Open the **OK5x27CK** webserver and navigate to the **Keyboard Wedge** tab.
4. Select the **CUSTOM** option from the **Keyboard Layout** drop-down menu.



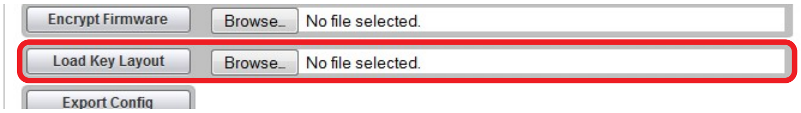
Keyboard Layout CUSTOM

Hex Output Case Lower

Inter-Keystroke Delay 20

5. Navigate to the **System Config** tab.
6. Click **Apply Changes**.
7. For the **Load Key Layout** setting, click **Browse** and select the layout file provided by tech support.

8. Click **Load Key Layout**.



Hex Output Case (Firmware 03000000 or higher)

The Hex Output case option specifies whether hexadecimal output is lower or upper case. The setting applies to all card types.

3.3.4 Card Type Processing Priority

Tech Order After Error

When enabled, the OMNIKEY 5x27 reader will continue processing the card types in order upon a card data processing error occurs.

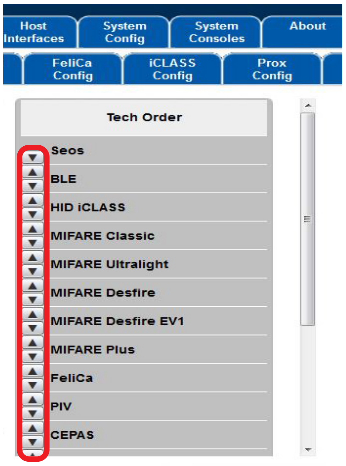
The intended use of this setting is for those installations with a mix of technology cards in place within the enterprise.

Note: When enabled, the output is delayed until all the card data is processed. If a failure occurs, no data is output from the reader for the card type which the error occurs on to include pre- and post-strokes (as if no card were presented). This prevents the host system from having to process unnecessary data. Note also that this may lead to a flickering ATR display if all the card data cannot be correctly processed.

Card Processing Priority

Card processing priority provides the capability to reduce the response time for the application to respond to a card presentation to the reader. HID recommends that the card processing prioritization be configured for each installation of device to ensure that the primary card type has priority.

To configure the card processing priority, go to the **Contactless Config** tab and use the Tech Order arrow buttons shown below.



Tech Order
Seos
BLE
HID iCLASS
MIFARE Classic
MIFARE Ultralight
MIFARE Desfire
MIFARE Desfire EV1
MIFARE Plus
FeliCa
PIV
CEPAS

Note: If Other ISOxxx is configured as the highest priority, the only output reported will be the CSN of the smartcard.

Note: t is best practice to place the card type that is the primary card at the installation in first priority. This will reduce the processing time for the card type and associated data.

3.4 Card Data Selection Tab

The Card Data Selections tab allows setting the keyboard wedge actions once a card is detected by the reader. Card-in events are customizable depending on the detected card type.

3.4.1 Supported Card Types and Protocols

LF Technologies (125 kHz)

Card Type	FW Version	Data Availability	Protocol Polling[1]
FSK (HID and AQID Prox)	01000000 or higher	PACS[2]	Prox
PSK (Indala Prox)	03000000 or higher		
ASK (EM Prox Family)			
HITAG	01.00.0069 or higher		

[1] The Polling Config tab is found under the Contactless Config tab

[2] Prox technologies do not support a CSN and only PACS data is available.

HF Technologies (13.56 MHz)

Card Type	FW Version	Data Availability	Protocol Polling[1]
iCLASS Seos	03000000 or higher	RCN, PACS, Custom	ISO 14443A
iCLASS (includes SR and SE)	01000000 or higher	CSN, PACS, Custom	iCLASS 15693
MIFARE Classic			ISO 14443A
MIFARE DESFire EV1[2]			
MIFARE Ultralight / C			
MIFARE DESFire 0.6		CSN, Custom	
MIFARE Plus[3]			
CEPAS	04000000 or higher	CSN, CAN	
PIV		CSN, CHUID	ISO 14443A & B
Other ISO14443A		CSN	ISO 14443A
Other ISO14443B			ISO 14443B
Other ISO 15693			iCLASS 15693
FeliCa	01.00.0069 or higher	CSN, Custom	FeliCa

[1] The Polling Config tab is found under the Contactless Config tab

[2] MIFARE DESFire EV1 (MAC secured, DES/3DES, 3K3DES and AES encrypted - firmware 02000000 or higher; diversification - firmware 04000000 or higher)

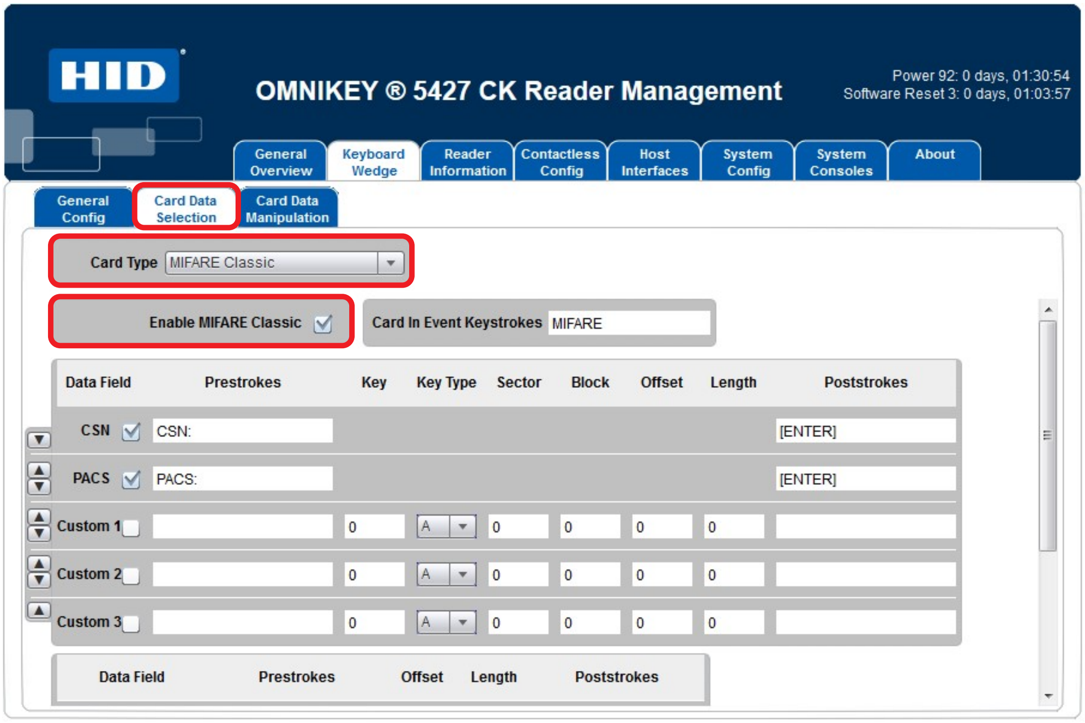
[3] Security Level 3 requires firmware 04000000 or higher

3.4.2 Bluetooth Low Energy (OK5127CK-Mini and OK5427 Gen 2)

In addition to the above technologies the OK5127CK-Mini and OK5427 Gen 2 also support Seos Mobile Access over BLE. This feature is not available on the original OK5127CK or OK5427CK.

Using the Card Data Selection Tab

1. Select Card Type via the drop-down Menu.
   All supported cards are available for configuration in the **Card Type** drop-down menu on the **Card Data Selection** tab. Default configuration is that all card types are active and preset data fields are sent upon card detection.
2. Enable and Disable Card Type Processing.
   Deselect cards through the web server by selecting the **Enable** button on each card page.



OMNIKEY ® 5427 CK Reader Management

Power 92: 0 days, 01:30:54
Software Reset 3: 0 days, 01:03:57

Card Type: MIFARE Classic

Enable MIFARE Classic ☑

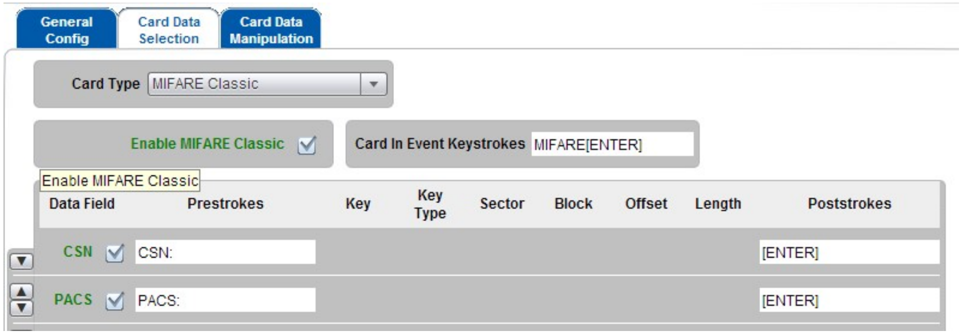
Card In Event Keystrokes: MIFARE

Data Field	Prestrokes	Key	Key Type	Sector	Block	Offset	Length	Poststrokes
CSN ☑	CSN:							[ENTER]
PACS ☑	PACS:							[ENTER]
Custom 1 □		0	A	0	0	0	0	
Custom 2 □		0	A	0	0	0	0	
Custom 3 □		0	A	0	0	0	0	

Data Field	Prestrokes	Offset	Length	Poststrokes

Note: Special considerations for enabling and disabling ISO 14443 Card Types:

- When an ISO14443A card type in enabled, the reader will read, buffer, process and output all parameters as configured to include Card in even and data pre- and post-strokes. An example pf output with MIFARE Classic Card Type Enabled follows:
  MIFARE
  CSN:7d1bf3ae
  PACS:02020097
- When any ISO 14443A card type is disabled, the reader will read and output the CSN and PACS data fields. An example of output with MIFARE Classic Card Type disabled follows:
  CSN + PACS
  7d1bf3ae02020097



General Config | Card Data Selection | Card Data Manipulation

Card Type: MIFARE Classic

Enable MIFARE Classic ☑

Card In Event Keystrokes: MIFARE[ENTER]

Data Field		Prestrokes	Key	Key Type	Sector	Block	Offset	Length	Poststrokes
CSN	☑	CSN:							[ENTER]
PACS	☑	PACS:							[ENTER]

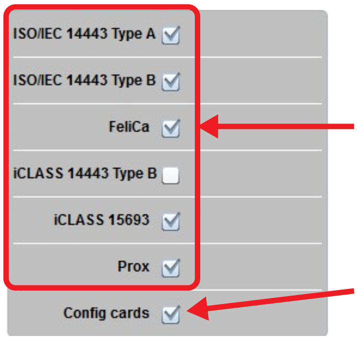
Polling Configuration

The reader only polls for all card protocols enabled in the **Polling Config** tab. The reader ignores all card types unchecked on the **Polling Config** tab.

It is suggested that users create default configuration enabling all parameters wanted, then simply disable the card technologies and protocols not required in order to optimize the reader response/operational timing for the end user.

1. Change priority table
2. Remove unused RF Protocols
3. Change polling Frequency to optimize speed and response of reader

Speak to an HID Sales, Presales Engineer, or Field Applications Engineer for further information.



ISO/IEC 14443 Type A ☑

ISO/IEC 14443 Type B ☑

FeliCa ☑

iCLASS 14443 Type B □

iCLASS 15693 ☑

Prox ☑

Config cards ☑

Enable only the protocols that are needed to provide the best user experience

HID recommends not disabling Config cards

Note: Take account of the **Polling Config** settings in the **Contactless Config** menu. Disabling a card type in the **Card Type** dropdown will not prevent the reader from polling for that card type. De-selecting the card type means that card data will not be sent as configured.

Note: It is suggested to experiment with lower RF Tx/RX rates to better stabilize the RFID interface as most applications will not see a major difference between 106 kbps and 424 kbps as the error rate is higher the higher the TX/RX rate. It is recommended to change ISO14443A/B and Felica to lower rates.

For multi-technology cards, the card type detected is dependent on where the reader is in its polling cycle when the card is presented. Therefore, for card populations involving multi-technology cards, ensure the unwanted card type is switched off in both the **Polling Config** and **Card Data Selection** tabs.

Additional Configuration of Prox Polling Parameters

Since Prox technologies are spread across 3 different modulation schemas (FSK, PSK and ASK); each of these modulation schemas can be enabled/disabled through the reader MIB APDUs. These configurations can be sent via HTTP or the Command Console contained within the **System Consoles** tab.

MIB APDUs to disable/enable polling of Prox modulation schemas:

Modulation Schema	APDUs to Disable	APDUs to Enable
FSK	FF680900011000	Should match setting previously sent
PSK	PSK1 FF680900010100 PSK2 FF680900010200 PSK3 FF680900010400 PSK4 FF680900010800	
ASK	FF680900012000	

All APDUs are required. NB If the reader is loaded with an Indala format other than ASP10022, the APDUs to re-enable PSK reading will be different.

MIB APDUs to verify polling settings of Prox modulation schemas:

Modulation Schema	APDUs to Disable	APDUs to Enable
FSK	FF680900011000	Should match setting previously sent
PSK	PSK1 FF680900010100 PSK2 FF680900010200 PSK3 FF680900010400 PSK4 FF680900010800	
ASK	FF680900012000	

It is recommenced practice to disable any PROX protocols that are not used in order to significantly boost reader performance. It also guards against the fact that PROX cards have no inherent security.

3. Configure Data Fields for each Card Type.

   5x27CK supports preset and custom data fields and keystrokes to be output by the reader in Keyboard Wedge mode.

   Previous to SP3, all pre- and post-stroke, card in, card out and error fields are limited to 7 characters (normal and special combined). From SP3 onwards each one can be up to 250 characters. However, the total memory used by these characters must not exceed 1024 bytes and there is a formatting overhead of 5 bytes per item. (Empty entries do not incur any overhead). For example eight 123 character strings would exactly fill all of the memory available.

Preset Data Fields

Preset data fields represent the cards pre-configured data objects and for the 5x27CK those are the PACS-Bits and CSN. Memory area, key configuration is preset in the 5x27CK; therefore, no configuration is required to access those data fields.

Field	Description
CSN	The Card Serial Number (CSN) is a data string which identifies a Smart card chip.
PACS	The PACS Data is used in Physical Access Control Systems as the credential to identify an individual within a controlled card population. This field is intended to be used when the system is designed to be format agnostic or when the system handles format data such as in a PACS application.
Custom n	Custom data fields are used to access any piece of data programmed on a card outside the CSN and PACS Data.
PACS Custom	PACS Custom allows the user to parse the PACS Data into multiple Data Fields. The most common data fields are: ■ Facility Code ■ Card Number ■ Site Code ■ City Code ■ OEM Code The PACS Format Fields used are dependent upon the PACS Data Format.

Note: CSN is not available for Prox cards.

Note: When using PACS Custom, HID suggests using more the 1 PACS format field. The OMNIKEY 5x27 readers have been updated to support up to 4 fields to support parsing 2 fields of 2 different formats (FW version 04000000 and higher).

Card Serial Number (CSN)

The CSN is open and in the clear. This means that the CSN is not secure and is open to copy and replay. With new NFC mobile devices it is possible for the CSN to be copied and replayed with relative ease.

To better meet security threats such as NFC enabled mobile devices, Next Generation Smartcards and NFC mobile devices use a Random Card Number in place of the CSN. When card type or card emulation uses a Random Card Number, this Random Card Number will be output by the reader. Thus, for these technologies, CSN is not an adequate credential to be used for any application. For instance, the Seos CSN will output a random 4 byte number.

HID suggests migrating away from using the CSN as the credential whenever possible.

Other Considerations for CSN

When the leveraging a CSN credential based PACS database, the application must often support CSN data manipulation to match the database. The OMNIKEY 5x27 always provides the complete CSN transferred during the anti-collision and card selection process when the communication link is established in accordance with smartcard ISO standards.

PACS

The PACS data field is often used to create a PACS format agnostic system or in cases which an entity does not wish to disclose their PACS format.

Custom Data Fields

Custom data fields allow access to custom data stored anywhere in the card user memory. Therefore, configure the custom data field address + length and the access key prior to use. Memory structure, naming conventions and security measures are specific to card type, the web interfaces presents the required configuration input for the selected card type.

Note: For retrieving custom data, ensure the corresponding access keys are available in the OMNIKEY 5x27CK. Enter key references using decimal in the keyboard wedge configuration interface.

For key loading details, see the *OMNIKEY 5x27CK Software Developer's Guide* (5127-903).

Note: Offset and data length are defined as BYTE. In the following example OFFSET = 1, shifts the read zone by one byte and limits it to one byte:

- Data on card (4 bytes total)
  HEX 12345678
  BIN 0001 0010 0011 0100 0101 0110 0111 1000
- Output with OFFSET = 1, LENGTH = 1
  HEX 34
  BIN 0011 0100

For MIFARE DESFire and MIFARE DESFire EV1 cards with linear / cyclical record, set LENGTH to one, since it refers those cards to one record.

PACS Custom Data Fields (Firmware 02000000 or higher)

HID credential physical access information is a unique bit stream that contains several data sections like Facility Code or Card Number. The pre-set data PACS function bits provide the full PACS bits stream. See *Section 3.4.2: Bluetooth Low Energy (OK5127CK-Mini and OK5427 Gen 2)*, step 3.

In case you are extracting only part of the full PACS bit stream, 5x27CK readers provide the function "PACS custom".

When activated, define and send separately up to three (prior to firmware 04000000) or four (firmware 04000000 or higher) data sections within the PACS bit stream over the Keyboard Wedge interface.

This option is available for card types provided with HID PACS bits (HID Prox, HID iCLASS, MIFARE Classic, MIFARE DESFire EV1) and requires Service Pack 1 or higher.

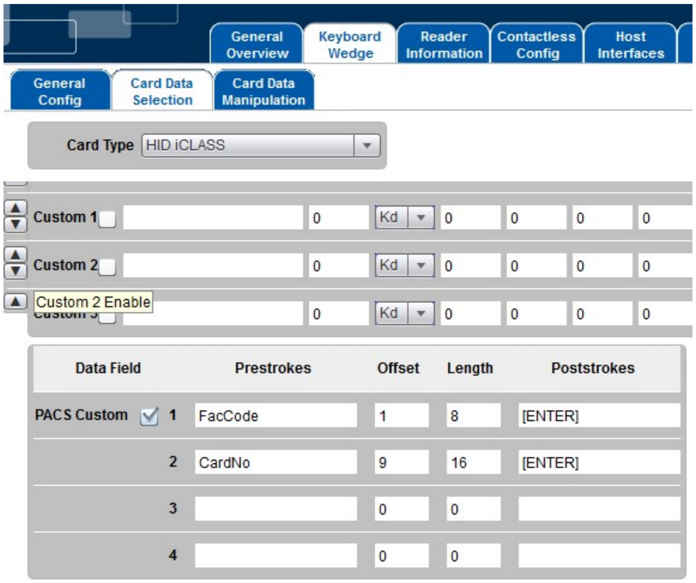
Definition of PACS data sections is done the same way as custom data fields (pre-/ post-strokes, Offset, Length). Since PACS data is typically not organized in full bytes, offset and length input represent bits (and not bytes as with custom data fields).

Furthermore, for each PACS section, define the output type individually.

Example: The configuration below defines two PACS format fields for the H10301 Wiegand Format:

- Facility Code: starting at bit 2 with a length of 8 bits
- Card Number: starting at bit 9 with a length of 16 bits

Prox Card Custom PACS Card Data Selection H10301 Example



Card Type: HID iCLASS

Custom 1 □		0	Kd	0	0	0	0
Custom 2 □		0	Kd	0	0	0	0
Custom 3 □		0	Kd	0	0	0	0

Data Field		Prestrokes	Offset	Length	Poststrokes
PACS Custom ☑	1	FacCode	1	8	[ENTER]
	2	CardNo	9	16	[ENTER]
	3		0	0	
	4		0	0	

Assuming the H10301 PACS Data in 01100100000010011100010010, the keyboard wedge output follows.

▪ FACCODE section in BIN Output	11001000
▪ FACCODE section in DEC Output	200
▪ CARDNR section in BIN Output	0001001110001001
▪ CARDNR section in DEC Output	5001

Note: HID suggests using at least 2 different PACS format fields when parsed PACS data is used for the credential.

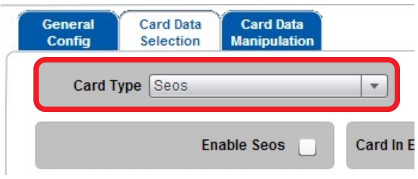
4. Configure Card In Event Keystrokes.

The Card In event defines a generic keystroke header that is sent upfront of any card data. This header is sent upon detection of the selected card type even when no card data is selected in configuration.

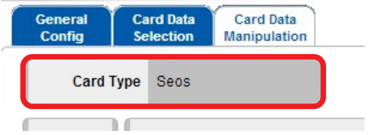
Note: Previous to SP3 all pre- and post-stroke, card in, card out and error fields are limited to 7 characters (normal and special combined). From SP3 onwards each one can be up to 250 characters. However, the total memory used by these characters must not exceed 1024 bytes and there is a formatting overhead of 5 bytes per item. (Empty entries do not incur any overhead). For example eight 123 character strings would exactly fill all of the memory available.

3.5 The Card Data Manipulation Tab

The **Card Data Manipulation** tab and **Card Data Selection** tab work in tandem. Therefore, The **Card Data Manipulation** tab is linked to the specific card type page that is currently active in the **Card Data Selection** tab.



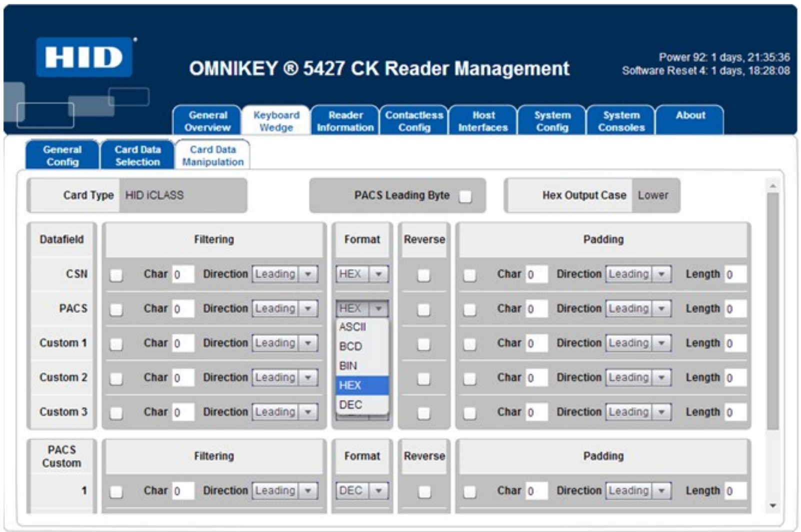
Card Type: Seos



Card Type: Seos

3.5.1 Using the Card Data Manipulation Tab

Format Output Selection



Card Type: HID iCLASS

PACS Leading Byte □

Hex Output Case: Lower

Datafield	Filtering	Format	Reverse	Padding
CSN	□ Char 0 Direction Leading	HEX	□	□ Char 0 Direction Leading Length 0
PACS	□ Char 0 Direction Leading	HEX	□	□ Char 0 Direction Leading Length 0
Custom 1	□ Char 0 Direction Leading		□	□ Char 0 Direction Leading Length 0
Custom 2	□ Char 0 Direction Leading		□	□ Char 0 Direction Leading Length 0
Custom 3	□ Char 0 Direction Leading		□	□ Char 0 Direction Leading Length 0

PACS Custom	Filtering	Format	Reverse	Padding
1	□ Char 0 Direction Leading	DEC	□	□ Char 0 Direction Leading Length 0

The following output types or formats are supported:

BIN (Binary)

The defined read area bit stream is sent to the Host system as 0 and 1 key strokes the same way as how they are stored on the card (there are no leading or trailing bits/keystrokes added).

Example (26 Bit Wiegand PACS Format):

Data on Card	01100100000010011100010010
BIN Output	01100100000010011100010010
OUTPUT = Direct match	

DEC (Decimal)

The defined area bit stream is sent as 0-9 keystrokes to the Host system according to the DEC representation of the bit stream. This conversion is a direct BIN to DEC conversation of the PACS data with no padding.

Example (26 Bit Wiegand PACS Format):

Data on Card	01100100000010011100010010
BIN Output	26224402
Output = direct binary to decimal conversion	

ASCII (American Standard Code for Information Interchange)

The defined area bit stream is sent as ASCII keystrokes to the Host system according to the ASCII representation of the bit stream. Non-printable characters (for example, ACK) are substituted by a period (.).

Note: For many cases, ASCII output format is only useful for data that is programmed in ASCII.

HEX (Hexadecimal)

The defined area bit stream is sent as 0-F keystrokes to the Host system according to the HEX representation of the bit stream.

HEX representation requires the binary structure to be padded to equal a HEX length (multiple of 8 bits). The binary PACS data is always left padded with binary 0s to the closest HEX length value.

Example (26 Bit Wiegand PACS Format):

Data on Card	01100100000010011100010010
BIN Output	01902712
Output = 26 bits left padded with 6 bits to make the bit structure a full-byte-value (32 bits = 4 bytes) and then converted to HEX	

Example (35 Bit Corporate 1000 Test PACS Format):

Data on Card	10111111111111111111111111111111110
BIN Output	05FFFFFFFE
Output = 35 bits left padded with 5 bits to make the bit structure a full-byte-value (40 bits = 5 bytes) and then converted to HEX	

BCD (Binary Coded Decimal)

The defined area bit stream is sent as 0 and 1 keystrokes to the Host system according to BCD representation of the bit stream.

The BCD output conversion sequence is Binary to Decimal and then Decimal to BCD. Each decimal digit is represented across 1 single nibble (4 bits) with a minimum value of 0000 and maximum value of 1001.

Example (35 Bit Corporate 1000 Test PACS Format):

Data on Card	10111111111111111111111111111111110
Decimal Value	25769803774
BIN Output	00100101011101101001100000000011011101110100
Output = 35 bits are converted to DEC (just like the DEC output) which is output in BCD	

PACS Leading Byte (Firmware 03000000 or higher)

PACS data is a binary structure and therefore, normally not a full byte-length-value (8 bits = 1 byte). For example, the H10301 26 bit Wiegand PACS format must be padded to 32 bits before the binary to HEX conversion can take place.

The normal HEX data is simply right padded to the nearest full-byte-length with binary 0s. When PACS Leading Byte is enabled, the binary PACS data is right padded with binary 0s and the number of padding bits is encoded as the PACS Leading Byte.

Example (H10301 26 bit Wiegand PACS Format):

Data on Card	01100100000010011100010010
HEX Output	01902712
HEX Output with PACS Leading Byte Enabled	066409C480
Breaking HEX string into binary PACS Data Output = 066409C480 **Number of bits that are right padded onto the binary PACS data** Binary = **00000110** 0**11001000**0001001110101001**0 **000000** **Facility Code: 200 (DEC)** **Card Number: 5001 (DEC)**	

Example (H10301 26 bit Wiegand PACS Format):

Data on Card	1111111111111100000000000000000010
HEX Output	07FFE00002
HEX Output with PACS Leading Byte Enabled	05FFFC000040
Breaking HEX string into binary PACS Data Output = 05FFFC000040 **Number of bits that are right padded onto the binary PACS data** Binary = **00000101** 111111111111110100000000000000010 **000000** **Company Code: 4095 (DEC)** **Card Number: 1 (DEC)**	

Note: PACS Leading Byte was added to the OMNIKEY 5x27 to support the HEX data output only to enable the OEM application to easily determine the actual PACS data programmed on the card.

Note: Note: The PACS Leading byte will affect all data output formats.

Filtering (Firmware 03000000 or higher)

- **Firmware 03000000:**
  Filter a byte (entered as decimal code) from raw data.
- **Firmware 03000000 or higher:**
  Direction: Leading = filter bytes from the start of raw data, Trailing = filter bytes from end of output data.
- **Firmware 04000000 or higher:**
  The filter character no longer needs to be entered as a decimal coded ASCII value and is entered by the actual keyboard character wanted.

Reverse

The reverse card data manipulation option allows reversing the standard read order of the card data and applies to custom data fields, PACS and CSN. The order is changed on raw byte-level data as depicted below.

Card Data (HEX)	01 02 03 04
Reverse Byte Order output (HEX)	04 03 02 01

The reverse order supports all output formats (BIN, HEX, DEC, BCD and ASCII), though, HEX output with the PACS Leading Byte enabled is when it is mostly used.

Example (H10301 26 bit Wiegand PACS Format)

Output Format	H10301 Output
HEX (Reverse Disabled)	066409C480
HEX (Reverse Enabled)	80C4096406
BIN (Reverse Disabled)	0000011001100100000010011100010010000000
BIN (Reverse Enabled)	1000 0000 1100 0100 0000 1001 0110 0100 0000 0110 8 0 C 4 0 9 6 4 0 6
DEC (Reverse Disabled)	27448165504
DEC (Reverse Enabled)	553044763654 0x80*(2^32) + 0xC4*(2^24) + 0x09*(2^16) + 0x64*(2^8) + 0x06
BCD (Reverse Disabled)	00100111010001001000000101100101010100000100
BCD (Reverse Enabled)	0101 0101 0011 0000 0100 0100 0111 0110 0011 0110 0101 0100 5 5 3 0 4 4 7 6 3 6 5 4

Note: The reverse option starts with the raw byte-level data (HEX value) and then applies the output format manipulation.

Example: (H10301 26 bit Wiegand PACS Format + the following parameters configured):

- Padding Characters of Ls to a fixed output of 48 characters
- PACS Leading Format Enabled

Output Format	H10301 Output
HEX (Reverse Disabled)	05FFFC000040LLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL
HEX (Reverse Enabled)	400000FCFF05LLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL

- The reverse option only affects the raw byte-level data field. Since the PACS Leading Byte is part of the Data Field, the PACS Leading byte is part of the data reversal.
- Firmware 02000000
  In firmware 02000000, Reverse applies only to custom data fields. PACS and CSN bits will not be affected by this command.
- Firmware 03000000
  From version 03000000 and higher, reverse applies to all data fields.

Padding

The output padding feature was added to address the requirement to always receive a static length data output.

- Firmware 0300000:

  Padding bytes are added to the raw data.

  Byte: ASCII character value (in decimal) to add to output string. It is output depending on the Format as specified above. So 48 would be output as 30 in hex or 0 in decimal. Binary is a special case, where only 0, 1, 48 or 49) are allowed - other values will be displayed as 1.

  Direction: Leading = add padding to start of string, Trailing = add padding to end of string.

  Length: Number of output characters to pad out to. This is format-independent, so entering 10 gives you 10 hex digits, 10 decimal digits, 10 ASCII characters, 10 binary bits, etc.

- Firmware 04000000 or higher:

  This feature is changed to support fixed data output requirements. Given this, if the number of padded characters is equal or less than the output string, the padded characters will not be added.

  In addition, the user may now place the actual character in the Char text box instead of its ASCII equivalent.

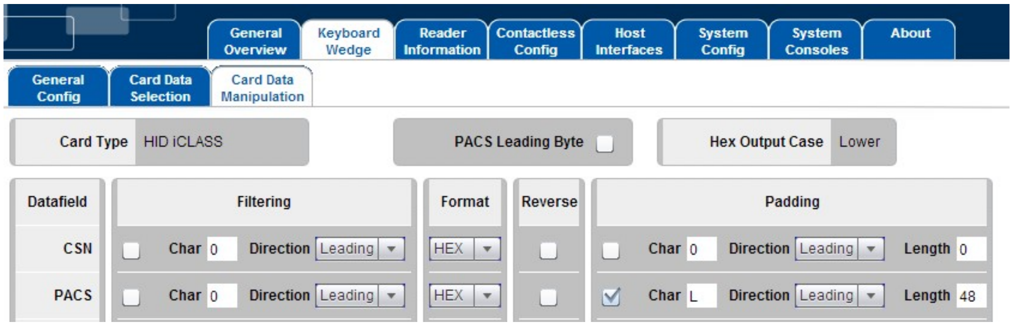
  Note: This should be the last setting configured in the **Card Data Manipulation** tab.

Specific Use Case

The padding feature was meant to support the use case where a host device must always receive a fixed data length.

Note: The fixed data length must exceed the number of characters output by the OMNIKEY 5x27 data field.

Example: A host system must receive a fixed data output length of 48 characters which padded to 40 characters with L. To support this, simply configure the Padding parameters as follows.



Card Type: HID iCLASS
PACS Leading Byte □
Hex Output Case: Lower

Datafield	Filtering			Format	Reverse	Padding			
CSN	□	Char 0	Direction Leading	HEX	□	□	Char 0	Direction Leading	Length 0
PACS	□	Char 0	Direction Leading	HEX	□	☑	Char L	Direction Leading	Length 48

Example: (H10301 26 bit Wiegand PACS Format - Leading L's to equal a fixed length output of 48 characters)

Output Format	H10301 Output
BIN	LLLLLLLLLLLLLLLLLLLLLL01100100000010011100010010
DEC	LLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL26224402
HEX	LLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL01902712
BCD	LLLLLLLLLLLLLLLL00100110001000100100010000000010

Example: (H10304 37 bit PACS Format - Trailing L's to equal a fixed length output of 48 characters)

Output Format	H10301 Output
BIN	0111111111111111100000000000000000010LLLLLLLLLLL
DEC	68718428162LLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL
HEX	0FFFF00002LLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL
BCD	68718428162LLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL

Note: PACS Leading Byte is part of the data sting that is calculated into the padding output.

Building an Output String

The OMNIKEY 5x27 allows the developer to develop an entire output string to include normal text and control characters. This section covers this topic in detail.

Note: Previous to SP3 all pre- and post-stroke, card in, card out and error fields are limited to 7 characters (normal and special combined). From SP3 onwards each one can be up to 250 characters. However, the total memory used by these characters must not exceed 1024 bytes and there is a formatting overhead of 5 bytes per item. (Empty entries do not incur any overhead). For example eight 123 character strings would exactly fill all of the memory available.

3.6 Supported Keystroke & Commands Characters

3.6.1 Supported Printable Characters

All normal printable keyboard ASCII characters are supported by the OMNIKEY 5x27.

Note: This does not include the characters sometimes referred to as extended ASCII which are supported by character encodings such as Windows Code Page 1252.

3.6.2 Pre- and Post-stroke Supported Control Characters

In most cases, keyboard stroke data (Pre and Post, or both) are strings of standard ASCII characters. In addition, use control characters, such as the Enter key. Enclose the control character (key) in brackets [ ], for example, [ENTER].

IMPORTANT:

- For confirming post- or pre-keystrokes in firmware versions below 02000000, press [ENTER], for the reader to perform validity check on the keystrokes.
- For firmware versions 02000000 or above, pressing [ENTER] **is not required**, the reader performs a validity check automatically once the focus is taken from the data field (for example, by pressing the **Tab** key or clicking another data field).
- For valid keystrokes, the font color turns from black to green. The text color remains green until you click **Apply Changes** and the **System Config** tab.
- In case the validity check fails, the font color turns red.

Possible failures include the following:

- Incorrect syntax in control commands
- Exceeding the max length per data field, which is seven (7) characters

The following table lists all supported control characters.

Note: Control characters must be capital letters.

Combine keystrokes with ASCII characters to allow shortcuts on the computer. For example, [ALT]F[CTRL]N[ENTER] creates a new text file when the Notepad application is active on the computer.

Supported Control Characters

Control Character / Key	Abbreviation
End	END
Enter	ENTER
Esc	ESC
Cursor down	DOWN
Cursor up	UP
Cursor left	LEFT
Cursor right	RIGHT
Space	SPACE

Control Character / Key	Abbreviation
Tab	TAB
F1	F1
…	…
F12	F12
Shift	SHIFT
Ctrl	CTRL
Alt	ALT
Delete	DEL
Windows	GUI

3.6.3 Reader Command Keystrokes (Controlling Reader Behavior)

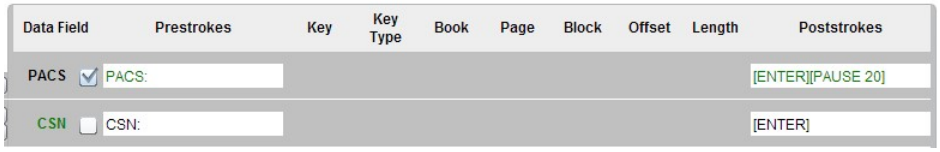
[PAUSE xxx]

The PAUSE character places the OMNIKEY Reader into a hold state where it will not process any cards. This is to allow the host system to process the card data received by the reader and perform additional functions before possibly receiving another dataset from the reader.

The value setting is 1 = 100 milliseconds 'coded in Decimal' as follows (note that the following example shows a pause of 2 seconds).

Note: The following example causes these events to occur before another card can be processed:

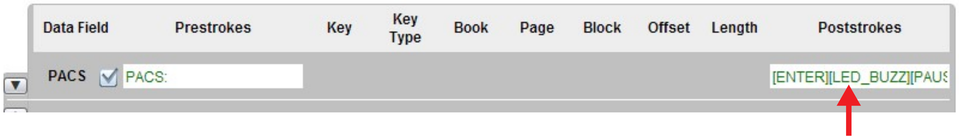
- Outputs the selected data followed by [ENTER].
- Performs the LED/Buzzer Sequence.
- Delays for a 2-second wait period.



Data Field		Prestrokes	Key	Key Type	Book	Page	Block	Offset	Length	Poststrokes
PACS	☑	PACS:								[ENTER][PAUSE 20]
CSN	□	CSN:								[ENTER]

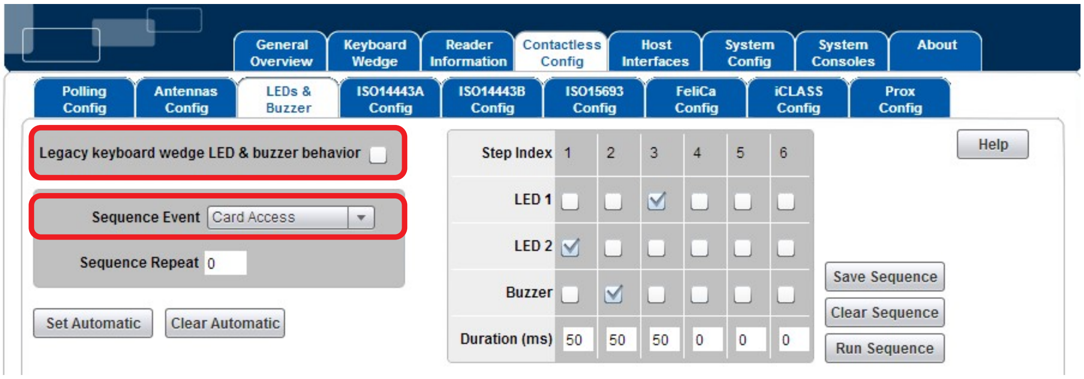
[LED_BUZZ]

The LED_BUZZ character provides the capability to control the LED and Buzzer sequence timing to provide a customized user experience. Each instance of an LED_BUZZ character is placed in the pre or post strokes field, the Card Access LED and Buzzer sequence will initiate as configured in the **LEDs & Buzzer** tab in the **Contactless Config** tab.



Data Field	Prestrokes	Key	Key Type	Book	Page	Block	Offset	Length	Poststrokes
PACS ☑	PACS:								[ENTER][LED_BUZZ][PAUS

To enable this feature, the **Legacy keyboard wedge LED & Buzzer behavior** option must be cleared (not selected).



Legacy keyboard wedge LED & buzzer behavior □

Sequence Event: Card Access

Sequence Repeat: 0

Step Index	1	2	3	4	5	6
LED 1	□	□	☑	□	□	□
LED 2	☑	□	□	□	□	□
Buzzer	□	☑	□	□	□	□
Duration (ms)	50	50	50	0	0	0

3.7 Using All Pre- and Post-stroke Events to Create an Output String and Control Reader Behavior

3.7.1 Card In Event

The 5x27CK lets you customize your output string for a Card In Event. The following objects are available for configuration on the **Card Data Selection** tab:

Card in Event Keystrokes	Option to enter header information to an output string.
Data Fields	Select either the cards preset or custom data field.
Pre-strokes	Keystrokes sent before the data field.
Post-strokes	Keystrokes sent after the data field.

There can be multiple data fields in one output string (for example, PACS bits followed by a custom data field). In this case, ensure the desired data fields are activated and fully configured.

Change the order of the output string data fields by using the up/down arrow buttons (left of the data field names).

Separate data fields from each other by using pre- and post-strokes.

3.7.2 Card Out Event

The 5x27CK lets you define an output string to be sent when a card is taken from the reader.

Note: This output string is sent for each card type and does not support card data.

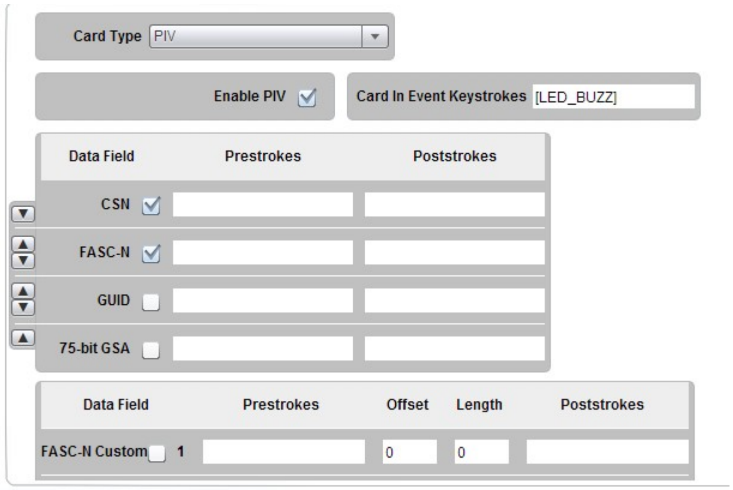
Chapter 4

New Supported Features

4.1 PIV and CEPAS Card Support

The reader supports parsing the FASC-N of PIV card or the CAN of a CEPAS card in a manner identical to that of HID PACS data, with both the options to output full FASC-N/CAN data and partial FASC-N/CAN data via custom fields. In addition to the FASC-N the reader supports 75-bit GSA and GUID output for PIV cards.

PIV Settings



Card Type: PIV

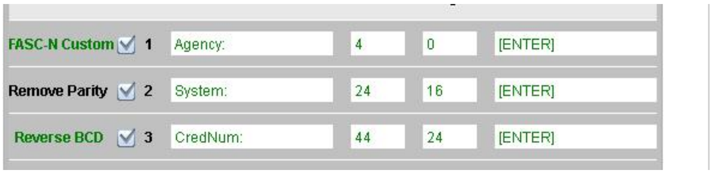
Enable PIV ☑ Card In Event Keystrokes [LED_BUZZ]

Data Field	Prestrokes	Poststrokes
CSN ☑		
FASC-N ☑		
GUID ☐		
75-bit GSA ☐		

Data Field		Prestrokes	Offset	Length	Poststrokes
FASC-N Custom ☐	1		0	0	

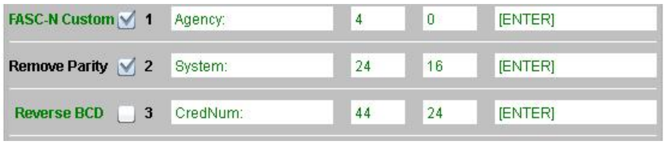
40 Bit BCD FASC-N Settings

The custom FASC-N settings to achieve various BCD outputs are shown below:



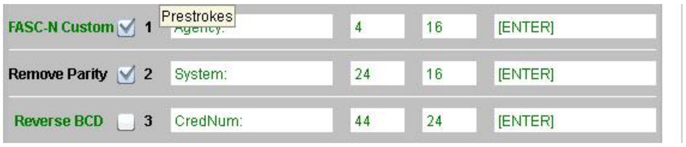
FASC-N Custom ☑	1	Agency:	4	0	[ENTER]
Remove Parity ☑	2	System:	24	16	[ENTER]
Reverse BCD ☑	3	CredNum:	44	24	[ENTER]

40-Bit Reverse BCD FASC-N Settings



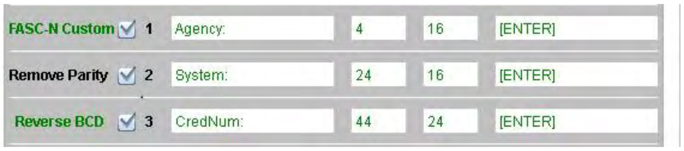
FASC-N Custom ☑	1	Agency:	4	0	[ENTER]
Remove Parity ☑	2	System:	24	16	[ENTER]
Reverse BCD ☐	3	CredNum:	44	24	[ENTER]

64-Bit Reverse BCD FASC-N Settings



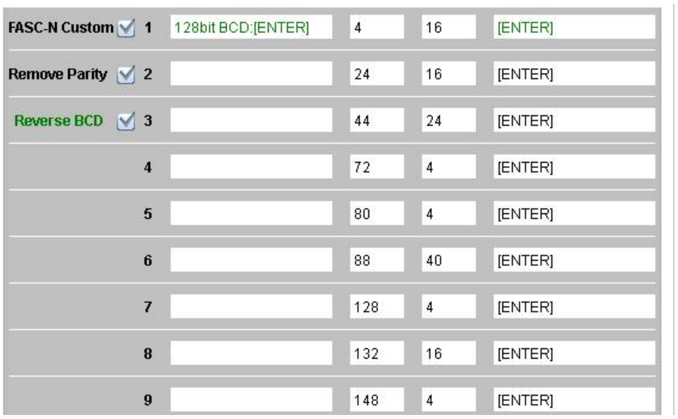
FASC-N Custom	☑	1	Agency:	4	16	[ENTER]
Remove Parity	☑	2	System:	24	16	[ENTER]
Reverse BCD	□	3	CredNum:	44	24	[ENTER]

64-Bit BCD FASC-N settings



FASC-N Custom	☑	1	Agency:	4	16	[ENTER]
Remove Parity	☑	2	System:	24	16	[ENTER]
Reverse BCD	☑	3	CredNum:	44	24	[ENTER]

128-Bit BCD FASC-N Settings



FASC-N Custom	☑	1	128bit BCD:[ENTER]	4	16	[ENTER]
Remove Parity	☑	2		24	16	[ENTER]
Reverse BCD	☑	3		44	24	[ENTER]
		4		72	4	[ENTER]
		5		80	4	[ENTER]
		6		88	40	[ENTER]
		7		128	4	[ENTER]
		8		132	16	[ENTER]
		9		148	4	[ENTER]

4.2 MIFARE DESFire EV1 Diversification Support

The reader supports authentication of the DESFire EV1 application key based on the MIFARE AV1 SAM algorithm. See the MIFARE AV1 SAM data sheet for details. In this algorithm the card key is created by encrypting the eight bytes formed when the card CSN is added to the application key number with the master key. For DES encryption the second and third keys (if used) are generated by encrypting the previously generated keys. If AES encryption is used the diversification bytes are padded with zeroes to make a full block.

To enable this feature select the required encryption algorithm in the **AV1 Diversify** column of the DESFire EV1 **Card Data Selection** tab.

4.3 FeliCa Custom Read from Non Encrypted Areas Supported from FW 01.00.0069

To enable this feature simply select one or more of the custom fields and type in the FeliCa Service Code, block, offset and length of data to read. If the combination of offset and or length means the data goes into the following block this will be read automatically.

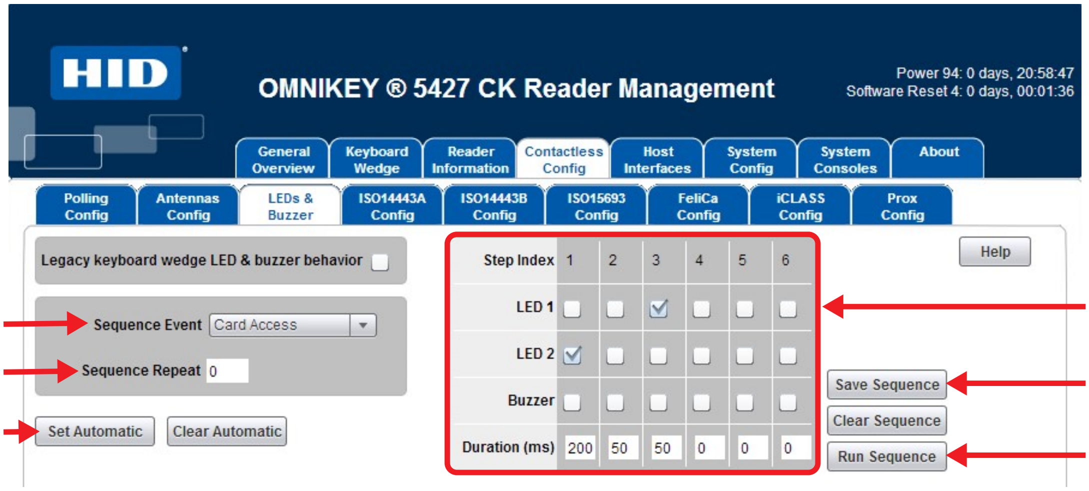
Chapter 5

LED & Buzzer Tab

This section covers how to configure the LED and Buzzer action settings for card events during a card access event.

5.1 Navigating the LEDs & Buzzer Tab

The following illustration refers to steps in Section 5.1.2: Configuring the LED and Buzzer Behavior:



OMNIKEY ® 5427 CK Reader Management

Power 94: 0 days, 20:58:47
Software Reset 4: 0 days, 00:01:36

Legacy keyboard wedge LED & buzzer behavior □

Step 1 → Sequence Event: Card Access

Step 5 → Sequence Repeat: 0

Step 6 → Set Automatic

Step Index	1	2	3	4	5	6
LED 1	□	□	☑	□	□	□
LED 2	☑	□	□	□	□	□
Buzzer	□	□	□	□	□	□
Duration (ms)	200	50	50	0	0	0

Step 2 → LED 1 / LED 2 / Buzzer / Duration (ms) grid

Step 4 → Save Sequence

Step 3 → Run Sequence

5.1.1 Legacy Keyboard Wedge LED & Buzzer Behavior

The legacy LED and buzzer operation is to execute the Card Access Step Index configuration settings at the beginning and another shortly following the 1st. The legacy LED and Buzzer behavior is disabled by default as some users found this to be confusing.

Note: Make sure that the legacy LED and Buzzer behavior is disabled to support the [LED_BUZZ] command character.

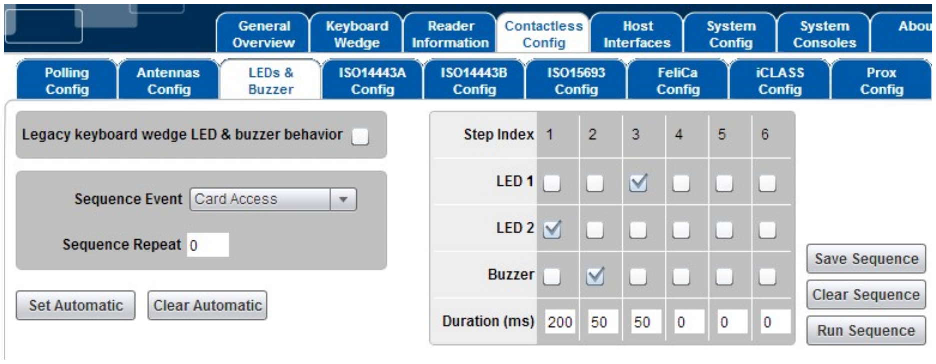
5.1.2 Configuring the LED and Buzzer Behavior

1. Select an event from the Sequence Event drop-down list. The following descriptions clarify each sequence event.

Sequence Events	Description
USB Ready	The LED and Buzzer sequence that occurs once the OMNIKEY 5x27 successfully enumerates with the OS and is ready.
Card Access	The LED and Buzzer sequence that is initiated via the legacy LED and Buzzer behavior (when enabled).
No USB	The LED and Buzzer sequence that occurs once the OMNIKEY 5x27 fails to enumerate with the OS.
Keyboard Wedge	This is the LED sequence that is triggered when the keyboard wedge encounters the special [LED_BUZZ] character in a pre-stroke, post-stroke, card in-strokes, card out-stokes or error strokes field.

2. Configure the LED and buzzer sequence and timing:
   - Sequence: Select a checkbox for each sequence parameter: LED 1, LED 2, and Buzzer.
   - Timing: Enter the duration in milliseconds for each Step Index in the Duration (ms) to define the amount of time in milliseconds that the event shall occur.

   Example: Upon Card Access, start with LED color 2 for 200ms, then buzzer sounds for 50ms, followed by LED 1 for 50ms.



Legacy keyboard wedge LED & buzzer behavior □

Sequence Event: Card Access

Sequence Repeat: 0

Step Index	1	2	3	4	5	6
LED 1	□	□	☑	□	□	□
LED 2	☑	□	□	□	□	□
Buzzer	□	☑	□	□	□	□
Duration (ms)	200	50	50	0	0	0

   Note: Always ensure that you end the card access sequence with the beginning state of the USB Ready Sequence to ensure a smooth transaction and that the colors are reset to the USB Ready state as shown.

3. Select **Run Sequence** to test the sequence.

   Observe the LED and Buzzer behavior to make sure everything is set up correctly. Repeat step 2 and this step as needed.

4. Once the sequence and timing is correct, select **Save Sequence** to save the sequence to memory.
5. In the **Sequence Repeat** field, enter the number of times, from 0 to 255, that the LED and Buzzer sequence will repeat.

   Note: 255 means that this is a permanent change. Thus the value of 255 should only be used for static events such as USB Ready and No USB.

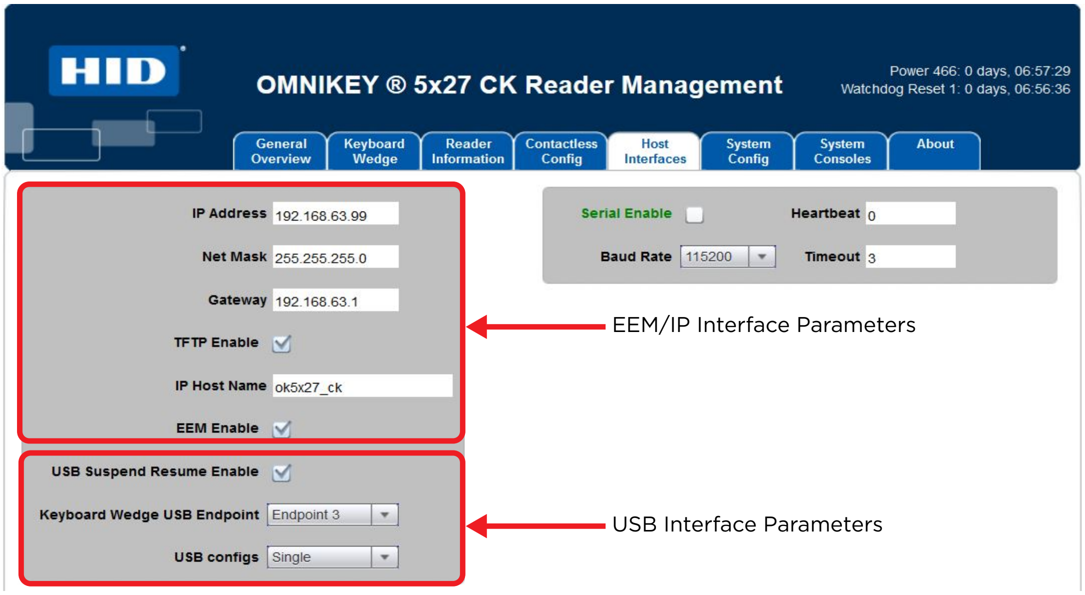
6. Select **Set Automatic** to enable the sequence to automatically run on every event.

Chapter 6

Host Interfaces

The OMNIKEY 5x27 supports multiple host interfaces including USB Endpoints. All the host interface options are manageable via the Host Interfaces tab.

6.1 Navigating the Host Interfaces Tab



Power 466: 0 days, 06:57:29
Watchdog Reset 1: 0 days, 06:56:36

IP Address 192.168.63.99
Net Mask 255.255.255.0
Gateway 192.168.63.1
TFTP Enable ☑
IP Host Name ok5x27_ck
EEM Enable ☑

USB Suspend Resume Enable ☑
Keyboard Wedge USB Endpoint Endpoint 3
USB configs Single

Serial Enable ☐
Heartbeat 0
Baud Rate 115200
Timeout 3

EEM/IP Interface Parameters

USB Interface Parameters

6.1.1 EEM IP Interface Parameters

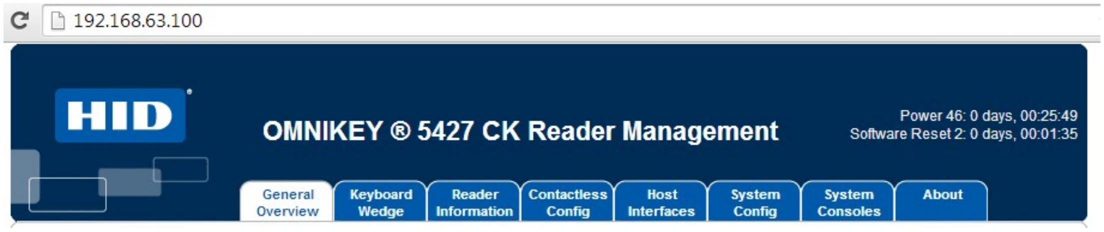
This section allows for the setup of Ethernet Interface parameters. It is suggested that documentation is maintained when changing these parameters.

The OMNIKEY 5x27 Default values are shown above.

Note: A configuration card can reset these settings to default if required.

IP Addressing

IP Address, **Net Mask** and **Gateway** are fully configurable. Once changed, the settings must be supported on the host PC to access the web based management tool. For instance, if the IP Address is changed to 192.168.63.100, this is new setting must be entered as the new URL in the internet browser to access the management tool.



TFTP Enable

When **TFTP** is disabled, the TFTP capabilities of the reader are no longer allowed. For additional information on TFTP, see the *OMNIKEY 5x27CK Software Developer Guide* (5127-903).

IP Host Name

The IP hostname is configurable using the **IP Host Name** text box. The **IP Hostname** is limited to 15 characters in length.

EEM Enable

When the **EEM Enable** option is selected, the OMNIKEY 5x27 will enumerate as a network adaptor and the host/user may access the Web Based Management tool. When not selected (disabled), the Web Based management tool is not accessible.

6.1.2 USB Interface Parameters

USB Suspend Resume Enable

The **USB Suspend Resume Enable** option is not supported by all devices.

Keyboard Wedge USB Endpoint

From the **Keyboard Wedge USB Endpoint** drop-down list, select one of the four USB endpoints that effect device enumeration and USB port transfers.

These options and descriptions are available:

- End Point 0 - Control
- Endpoint 1 - Interrupt Transfers
- Endpoint 2 - Isochronous Transfers
- Endpoint 3 - Bulk Transfers

Note: The Keyboard Wedge USB Endpoint selected only effects the USB enumeration process when Keyboard Wedge is enabled\. This is not a global parameter.

This page intentionally left blank.

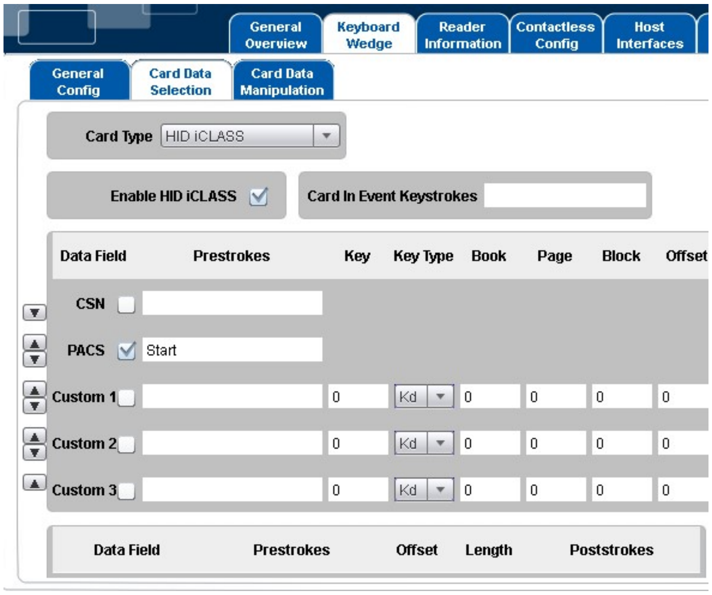
Chapter 7

OMNIKEY 5x27 Configuration Examples

7.1 Example 1 - Reading iCLASS Card PACS Data

1. Enable **Keyboard Wedge** mode.
2. Select the **Keyboard Wedge** tab and select the **Card Data Selection tab**.
3. From the **Card Type** drop-down list, select **HID iCLASS**.
4. Select the **Enable HID iCLASS** option.
5. Select the **PACS** option.
6. In the **PACS Pre-strokes** field, enter **Start**.
7. Press [ENTER].

iCLASS Card PACS Data Example



Card Type: HID iCLASS

Enable HID iCLASS ☑

Card In Event Keystrokes:

Data Field		Prestrokes	Key	Key Type	Book	Page	Block	Offset
CSN	□							
PACS	☑	Start						
Custom 1	□		0	Kd	0	0	0	0
Custom 2	□		0	Kd	0	0	0	0
Custom 3	□		0	Kd	0	0	0	0

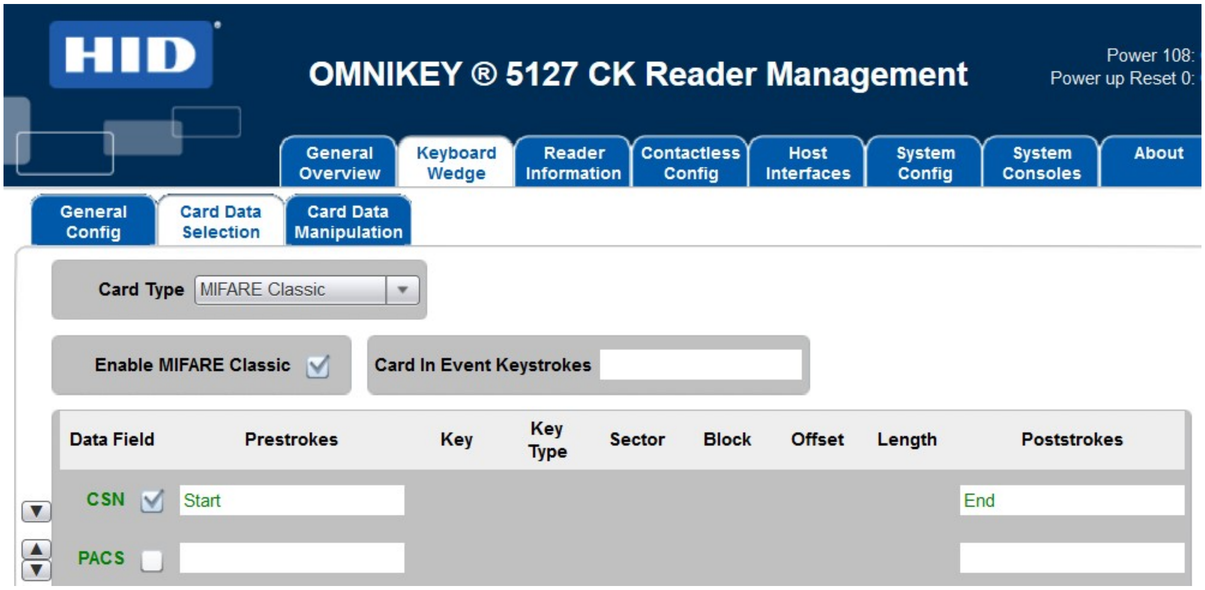
8. Open a text editor and place the iCLASS Sample card into the RFID field over the antenna of the reader.
9. The Keyboard Wedge enters into the editor the word **Start** followed by the PACS data in hexadecimal format.

Example: **Start07FFE00002**

7.2 Example 2 - Reading MIFARE Card CSN

1. Go to the **Keyboard Wedge** tab and select the **Card Data Selection** tab.
2. From the **Card Type** drop-down menu, select **MIFARE Classic**.
3. Select the **Enable MIFARE Classic** option.
4. Select the **CSN** option.
5. Enter **Start** into the Pre-strokes field, press [ENTER].
6. Enter **End** into the Post-strokes field, press [ENTER].

MIFARE Card CSN Example



Card Type: MIFARE Classic

Enable MIFARE Classic ☑

Card In Event Keystrokes

Data Field	Prestrokes	Key	Key Type	Sector	Block	Offset	Length	Poststrokes
CSN ☑	Start							End
PACS □								

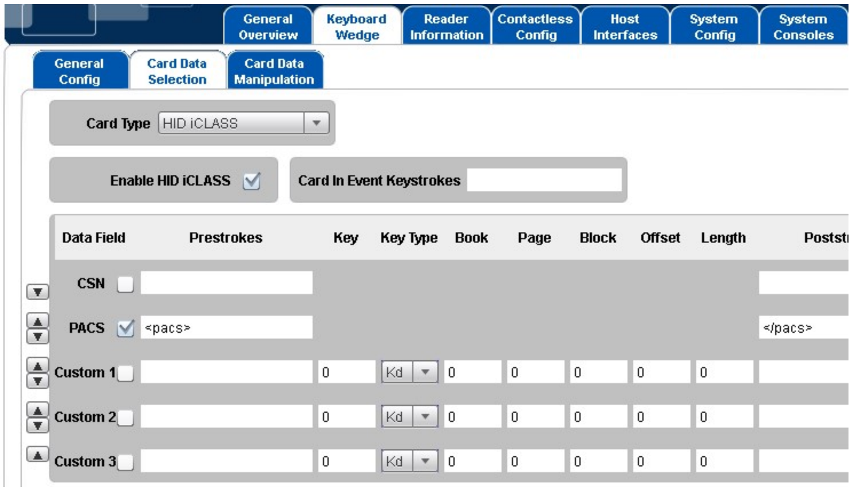
7. Open a text editor and place the MIFARE 1k Sample card into the RFID field over the antenna of the reader.
8. The Keyboard wedge enters into the editor the word **Start** followed by the CSN data in hexadecimal format and the word **End**.

Example: **Start7D1BF3AEEnd**

7.3 Example 3 - HID iCLASS PACS Data Filtering

1. Select the **Keyboard Wedge** tab.
2. Select the **Card Data Selection** tab.
3. From the **Card Type** drop-down menu, select **HID iCLASS**.
4. Select the **Enable HID iCLASS** option.
5. Select the **PACS** option.
6. Enter **<pacs>** into the Pre-strokes text field, press [ENTER].
7. Enter **</pacs>** into the Post-strokes text field, press [ENTER].

HID iCLASS PACS Filtering Card Data Selection Example



Card Type: HID iCLASS

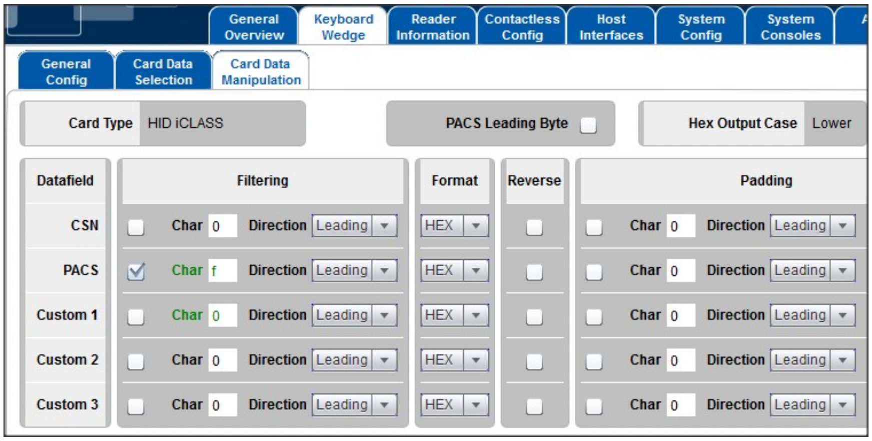
Enable HID iCLASS ☑

Card In Event Keystrokes

Data Field		Prestrokes	Key	Key Type	Book	Page	Block	Offset	Length	Poststr
CSN	□									
PACS	☑	<pacs>								</pacs>
Custom 1	□		0	Kd	0	0	0	0	0	
Custom 2	□		0	Kd	0	0	0	0	0	
Custom 3	□		0	Kd	0	0	0	0	0	

8. Select the **Card Data Manipulation** tab.
9. In the **PACS** row, do the following:
   - In the **Filtering** pane:
     - Select the checkbox.
     - Enter “f” in the **Char** field.
   - In the **Format** pane, verify that **HEX** is selected.

HID iCLASS PACS Filtering Card Data Manipulation Example



Card Type: HID iCLASS

PACS Leading Byte □

Hex Output Case: Lower

Datafield	Filtering				Format	Reverse	Padding			
CSN	□	Char 0	Direction	Leading	HEX	□	□	Char 0	Direction	Leading
PACS	☑	Char f	Direction	Leading	HEX	□	□	Char 0	Direction	Leading
Custom 1	□	Char 0	Direction	Leading	HEX	□	□	Char 0	Direction	Leading
Custom 2	□	Char 0	Direction	Leading	HEX	□	□	Char 0	Direction	Leading
Custom 3	□	Char 0	Direction	Leading	HEX	□	□	Char 0	Direction	Leading

10. Open a text editor and place the iCLASS Sample card into the RFID field over the antenna of the reader.
11. The Keyboard Wedge enters into the editor the text <pacs> followed by the filtered PACS data in hexadecimal format followed by the text </pacs>.

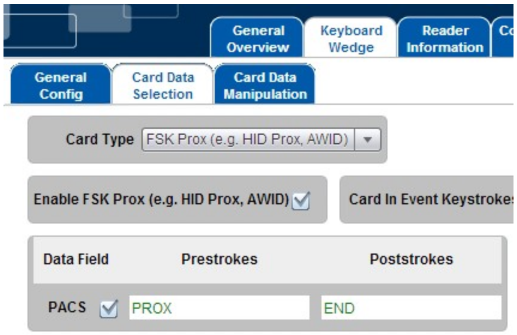
Example: **<pacs>6e1b500f9ff12e0</pacs>**

Note: The character "f" has been filtered out.

7.4 Example 4 - Prox Card PACS Data Padding

1. Select the **Keyboard Wedge** tab.
2. Select the **Card Data Selection** tab.
3. From the **Card Type** drop-down list, select **HID Prox**.
4. Select the **Enable HID Prox** option.
5. Select the **PACS** option.
6. Enter **PROX** into the Pre-strokes field, press [ENTER].
7. Enter **END** into the Post-strokes field, press [ENTER].

Prox Card PACS Padding Card Data Selection Example



Card Type FSK Prox (e.g. HID Prox, AWID)

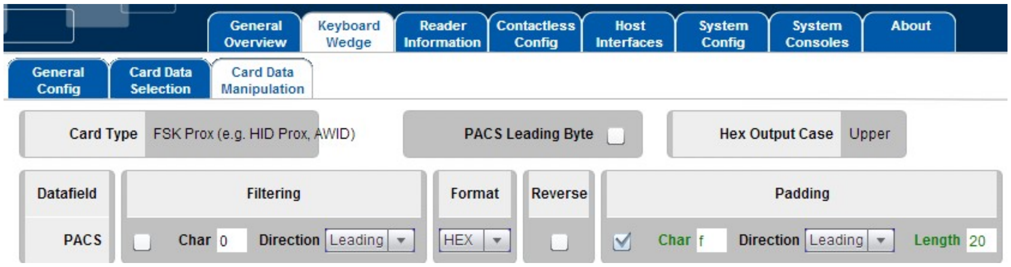
Enable FSK Prox (e.g. HID Prox, AWID) ☑

Card In Event Keystroke

Data Field	Prestrokes	Poststrokes
PACS ☑	PROX	END

8. Select the **Card Data Manipulation** tab.
9. In the **PACS** row of the **Format** pane, select **HEX**.
10. In the **PACS** row in the **Padding** pane, do the following:
    - Select the **PACS** option by selecting the checkbox in the **PACS** row.
    - Enter "**f**" in the **Char** field.
    - Select **Leading** in the **Direction** field.
    - Enter **20** in the **Length** field.

Prox Card PACS Padding Card Data Manipulation Example



Card Type FSK Prox (e.g. HID Prox, AWID)

PACS Leading Byte □

Hex Output Case Upper

Datafield	Filtering	Format	Reverse	Padding
PACS	□ Char 0 Direction Leading	HEX	□	☑ Char f Direction Leading Length 20

11. Open a text editor and place an HID Prox card into the RFID field over the antenna of the reader:
    - If the data on the card is: **10000000100000000001001111**
    - The output in the editor will be: **PROXffffffffffff0202004fEND**

This page intentionally left blank.

Appendix A

Description of Fields

A.1 Enable Card Type

All card types have this option. Enables the keyboard wedge for the relevant card type If not enabled the keyboard wedge will not try to process the card as a Seos card. It may however still try to process it as another card type if it fits more than one type. For example, a MIFARE Classic card could also be processed as a ISO14443A card if the Generic ISO14443A card type is enabled. If the user wishes to block the processing of the particular card type, then they should leave it enabled, but disable all of its data fields.

A.2 Card In Event Keystrokes

All card types have this field. These key strokes will be sent, before outputting any other keyboard wedge data for this card type, even if all other fields are disabled.

A.3 Pre-strokes

There is a pre-strokes setting for every keyboard wedge data field (e.g. CSN, PACS, custom data, etc.). These key strokes are sent before outputting the data for each field. By default pre strokes will not be output if an error occurs reading a field. However, this is not the case if the Tech Order option is disabled and the **Allow Pre-strokes and Post-strokes for Errors option** is enabled.

A.4 Post-strokes

These behave the same as pre-strokes, except that they are output after the data for the relevant field rather than before.

A.5 CSN

This option enables the outputting of the serial number obtained during anti-collision.

A.6 PACS

This option is only enabled for card types which may contain HID PACS data (MIFARE Classic, iCLASS, Seos, BLE Seos, MIFARE DESFire EV1) and LF card types. The option enables the output of the whole of the PAC contained on the card.

A.7 PACS Custom

This option is only enable for card types which may contain HID PACS data (MIFARE Classic, Prox, iCLASS, Seos, BLE Seos, MIFARE DESFire EV1). If enabled allows individual parts of the reader PACS data to be output. Up to four custom fields are provided and each one can be specified independently of the other.

A.7.1 Offset

The offset specifies the position in the PACS data in bits to start outputting data from. Any value between zero and the length of the PACS data is allowed. This value can either be entered in decimal, or in hex. To specify the value in hex the value must be prefixed with "0x".

A.7.2 Length

The length option specifies the number of bits of PACS data, starting from the offset value, to output. This value can either be entered in decimal, or in hex. To specify the value in hex, prefixed the value with "0x".

A.8 iCLASS Custom Fields

Each iCLASS custom has the options listed below.

A.8.1 Key

This is the number of the key slot that the key was loaded to in order to authenticate to the card. Although any value in the range 0-255 will be accepted, the reader normally expects iCLASS keys to be loaded to slots in the range 33-52. The key can be entered either in decimal or in hex (by prefixing them with "0x").

A.8.2 Key Type

This can be Kd or Kc. This specifies the type of iCLASS key used to authenticate to the card. The choice of Kd or Kc depends on the page application limit set in the configuration block of the page being authenticated. Use Kd to authenticate to the area before the application limit and Kc to authenticate to the area after. Refer to the Picopass datasheets for more information.

A.8.3 Book

This is the book address of the iCLASS card to read. The only valid value for 2KS and 16KS cards is zero. For 32KS cards the value can be zero or one.

A.8.4 Page

This is the page address of the chosen iCLASS book to start reading from:

- For 2KS cards or books of 16KS or 32KS cards configured with a single page per book, the only valid value is zero.
- If the book is configured with multiple pages per book, then the valid values are zero to seven.

A.8.5 Block

The block option specifies the block of the page to start reading data from. For 2K pages the valid values are 0 to 31 and for 16K pages the valid values are 0 to 255. The value can be entered either in decimal or in hex (by placing "0x" before the hex value).

A.8.6 Offset

The offset specifies the position within the block in bytes to start reading the data at. Although the size of an iCLASS block is eight bytes, values in the range 0 to 255 bytes are accepted. If the offset is greater than the size of the block then the keyboard wedge will move into the following blocks until the offset has been reached. As with all keyboard wedge options, the value can either be specified in decimal, or in hex. When entering a value in hex the value must be preceding with "0x".

A.8.7 Length

The length specifies the number of bytes to read from the card. The maximum allowed length is 255 bytes. If the number of bytes is greater than the block size (8 bytes), then the keyboard wedge will continue to read the following blocks until the correct number of bytes have been read. However, the keyboard wedge will not be able to continue if the end of the application is reached, as a different key will be needed to authenticate. The value can be entered either in decimal or in hex (by placing "0x" before the hex value).

A.9 MIFARE Classic and MIFARE Plus Custom Fields

A.9.1 Key

This is the number of the key slot that the key was loaded to in order to authenticate to the card. Although any value in the range 0-255 will be accepted, the reader normally expects MIFARE Classic keys to be loaded to slots in the range 0-31. The key number can be entered either in decimal or in hex (by prefixing them with "0x").

A.9.2 Key Type

This can be either type A or type B. This specifies the type of MIFARE key used to authenticate to the card. The choice of type A or type B depends on the access conditions in the sector trailer of the sector being authenticated. Key type A is the most commonly used key type for card reads.

A.9.3 Sector

This is the sector address of the MIFARE Classic card to read:

- For MIFARE Classic 1K, the sector value can be between 0 and 15, inclusive.
- MIFARE Plus 2K, cards can have sector values from 0 up to and including 31.
- For MIFARE 4K, the value can be anything up to and including 39.

The sector value can be entered in decimal or hex. If the value is entered in hex then the value must be written starting with "0x".

A.9.4 Block

The block option specifies the block of the sector to start reading data from:

"For sector values up to and including fifteen the block can be anything from zero up to and including three.

"For sectors greater than fifteen the blocks can be anything from 0 up to and including fifteen.

The value can be entered either in decimal or in hex (by placing "0x" before the hex value).

A.9.5 Offset

The offset specifies the position within the block in bytes to start reading the data at. Although the size of a MIFARE block is sixteen bytes, values in the range 0 to 255 bytes are accepted. If the offset is greater than the size of the block then the keyboard wedge will move into the following blocks until the offset has been reached. As with all keyboard wedge options, the value can either be specified in decimal or in hex. When entering a value in hex the value must be preceding with "0x".

A.9.6 Length

The length specifies the number of bytes to read from the card. The maximum allowed length is 255 bytes. If the number of bytes is greater than the block size (16 bytes), then the keyboard wedge will continue to read the following blocks until the correct number of bytes have been read. However, the keyboard wedge will not be able to continue if the end of the sector is reached as a different key will be needed to authenticate. The value can be entered either in decimal or in hex (by placing "0x" before the hex value).

A.10 MIFARE Ultralight Custom Fields

A.10.1 Key

This is the number of the key slot that the key was loaded to in order to authenticate to the card. If authentication is not required then this value can be ignored. Although any value in the range 0-255 will be accepted, the reader normally expects MIFARE Ultralight keys to be loaded to slots in the range 240-255. The key number can be entered either in decimal or in hex (by prefixing them with "0x").

A.10.2 Page

The page option specifies the page to start reading data from:

- For standard Ultralight, the page can be in the range 0 to 15.
- For Ultralight C, the page value can be up to and including 39.

Note: Although Ultralight C memory continues up to page 47, the remaining pages are not readable.

The value can be entered either in decimal or in hex (by placing "0x" before the hex value).

A.10.3 Offset

The offset specifies the position within the page in bytes to start reading the data at. Although the size of an Ultralight page is four bytes, values in the range 0 to 255 bytes are accepted. If the offset is greater than the size of the page then the keyboard wedge will move into the following pages until the offset has been reached. As with all keyboard wedge options, the value can either be specified in decimal, or in hex. When entering a value in hex the value must be preceding with "0x".

A.10.4 Length

The length specifies the number of bytes to read from the card. The maximum allowed length is 255 bytes. If the number of bytes is greater than the page size (4 bytes), then the keyboard wedge will continue to read the following pages until the correct number of bytes have been read. However, the keyboard wedge will not produce any output if an attempt to read beyond the end of the card memory is made. The value can be entered either in decimal or in hex (by placing "0x" before the hex value).

A.11 MIFARE DESFire and MIFARE DESFire EV1 Custom Fields

A.11.1 App ID

The App ID is the ID of the MIFARE DESFire application to read. This is an integer in the range 1 to 0xFFFFFF (zero is reserved for the PICC master application). ISO application identifiers are not supported. The value can either be entered as a decimal value or as a hex value. Hex values must be written starting with a "0x".

Note: MIFARE DESFire commands and responses encode integer values in little-endian format (LSB first). Therefore this must be taken into account when converting the AID from raw bytes to an integer.

A.11.2 File Num

File Num is the ID of the file on the application to read. This is an integer in the range 0 to 0x1F. ISO file names are not supported. The value can be entered in hex or in decimal. To enter the value in hex, prefix it with "0x".

A.11.3 Offset/Start

This is treated the same as the offset parameter used by the MIFARE DESFire read commands. For reading standard data or backup data files it specifies the position within the file, in bytes, from which the read will start. For value files the value should be less than or equal to four bytes. For record files it specifies the first record to start reading from. This value can be entered in decimal or hex, but if entered in hex, must start with "0x".

A.11.4 Length/Len

This is treated the same as the length parameter used by the MIFARE DESFire read commands. For reading standard data or backup data files it specifies the number of bytes to read in bytes. For value files it must be in the range 0 to 4 bytes inclusive. For record files it specifies the number of records to read. This value can be entered in decimal or hex, but if entered in hex, must start with "0x".

A.11.5 Card Key

This specifies the key number on the MIFARE DESFire card to use for authentication. Valid values for the card key are in the range zero to thirteen. This value can be entered in decimal or hex, but if entered in hex, must start with “0x”.

A.11.6 Rdr Key

This specifies the reader key slot to use for authentication. Values in the range 0-255 will be accepted. However, the reader will normally expect MIFARE DESFire keys to be loaded to slots 240-255. This value can be entered in decimal or hex, but if entered in hex, must start with "0x".

A.11.7 Auth

This should be enabled if the file requires authentication to be read (for example, if the access conditions for the file do not specify free access).

A.11.8 File Type

This specifies the type of MIFARE DESFire file being read. The available types are standard data, backup data, value, linear record and cyclical record. Refer to the MIFARE DESFire datasheet for further information. This file type will be determined based on the command used to create the file when the MIFARE DESFire card was provisioned.

A.11.9 File Comms

This determines the communication type to use when reading the card. The available options are none (no encryption or authentication), MACed (message authenticated, but no encryption) and Encrypt (message signed and encrypted). If the card has not been authenticated then this should be set to none. If authentication has been used then the value should be chosen based on the communication settings used when creating the file to be read.

A.11.10 Encryption

The encryption option specifies the algorithm to use for encryption during authentication, message signing (MACing) and message encryption. The option DES/3DES should be used for both two key triple DES and single key triple DES. For three key triple DES the option 3K3DES should be chosen. AES encryption is also supported via the AES option.

A.11.11 AV1 Diversify (MIFARE DESFire EV1 only)

Specifies the encryption algorithm used when diversifying the MIFARE DESFire key. This will normally match the algorithm used for authentication. This encryption algorithm will then be used to diversify the master key with the same algorithm as used by the MIFARE AV1 SAM, with a diversification input made up of the card key number followed by the card UID.

A.12 PIV Specific Fields

A.12.1 FASC-N

If enabled, this outputs the entire FASC-N value as defined in the PIV specification. The FASC-N is contained within the Card Holder Unique Identifier (CHUID) of the PIV card. For further details of the FASC-N refer to the document "Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems" from the US Government Smart Card Interagency Advisory Board.

A.12.2 GUID

If enabled, this outputs the entire Global Unique Identifier (GUID). The GUID is part of the CHUID. Refer to the document, "Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems" for further details.

A.12.3 75-Bit GSA

This is a special option to output the CHUID data in the special GSA-75 bit format defined in the SIA white paper, "Physical Access Control System (PACS) in a Federal Identity, Credentialing and Access Management (FICAM) Framework". This format is a cut-down version of the CHUID typically used in the access control industry.

A.12.4 FASC-N Custom

This provides the option to output individual parts of the FASC-N. The offset value is the number of bits to start reading data from and the length is the number of bits to read. The output and length values can be specified in decimal or hex. Any hex values must be entered with a prefix of "0x". Up to 9 custom fields are provided to allow all of the components of the FASC-N to be output. Each custom can be set independently of the others.

A.12.5 FASC-N Custom Remove Parity

If this option is set then parity bits will be removed from the FASC-N data before starting to process the FASC-N custom fields.

A.12.6 FASC-N Reverse BCD

If enabled, then each individual nibble of the output will have its bit order reversed before outputting the data.

A.13 CEPAS Custom CAN Fields

The offset and length options allow the user to specify in bits, individual parts of the CEPAS CAN to be output in exactly the same way as with custom PACS output for HID cards. As with custom PACS data, the offset and length values can be entered in decimal or hex. However, if entering the value in hex then the value must start with "0x".

hidglobal.com