

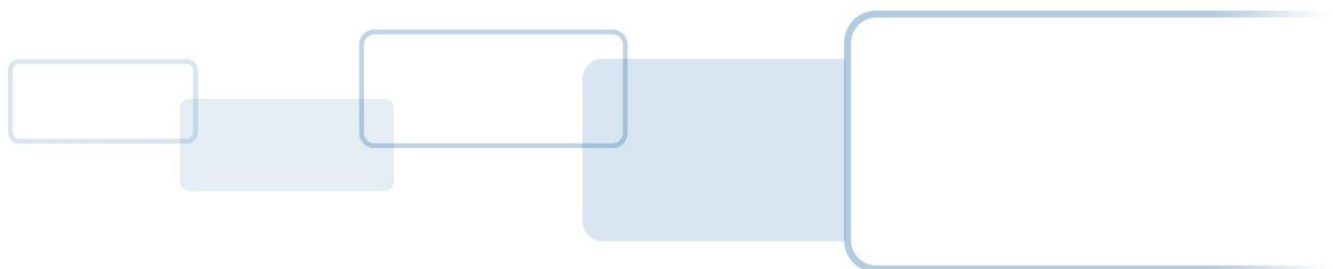


OMNIKEY 5x27CK

Keyboard Wedge Configuration

User Guide

5127-902, Rev. D.3
December 2014



Contents

1	Overview	5
1.1	References	5
1.2	Acronyms and Abbreviations	6
1.3	Supported RFID Technologies	7
1.3.1	8BLF Technologies (125kHz)	7
1.3.2	BHF Technologies (13.56 MHz)	7
1.4	Modes of Operation	8
1.4.1	BEthernet Emulation Mode (EEM)	8
1.4.2	CCID	9
1.4.3	Keyboard Wedge.....	9
1.4.4	Custom Report	10
1.4.5	Special Considerations.....	10
2	Reader Web Based Management Tool Interface.....	11
2.1	Preparations	11
2.1.1	Load the Ethernet Emulation Mode (EEM) Driver	11
2.1.2	Load a Web Browser	11
2.2	Navigating the 5x27 CK Web Based Management Tool.....	12
2.2.1	Accessing the Web Interface	12
2.2.2	Navigating the Tabs	13
2.2.3	Changing Settings	14
2.2.4	Downloading and Uploading Configurations	15
2.2.5	Setting a web server password.....	17
3	Keyboard Wedge Mode	19
3.1	Keyboard Wedge Operation Overview	19
3.2	14BNavigating the Keyboard Wedge Configuration Tabs	19
3.3	General Config Tab	20
3.3.1	KBW Enable Options.....	20
3.3.2	Global Keystroke Events	21
3.3.3	Keyboard Options.....	22
3.3.4	Card Type Processing Priority	23
3.4	Card Data Selection Tab	24
3.4.1	45BSupported Card Types and Protocols	24
3.4.2	Using the Card Data Selection Tab	25
3.5	The Card Data Manipulation Tab.....	31
3.5.1	Using the Card Data Manipulation Tab.....	31
3.6	Supported Keystroke & Commands Characters	38
3.6.1	Supported Printable Characters	38
3.6.2	49BPre and Poststroke Supported Control Characters	38
3.6.3	Reader Command Keystrokes (Controlling Reader Behavior)	39
3.7	Using all Pre/Poststrokes events to Create an Output String and Control Reader Behavior	40
3.7.1	51BCard In Event	40
3.7.2	Card Out Event	40
4	New Supported Features.....	41
4.1	PIV and CEPAS Card Support (firmware 04000000 or higher)	41
4.2	MIFARE DESFire EV1 Diversification Support (firmware 04000000 or higher)	43
5	LEDs & Buzzer Tab	45
5.1	Navigating the LEDs & Buzzer Tab	45
5.1.1	Legacy Keyboard Wedge LED & Buzzer Behavior	45



- 5.1.2 Configuring the LED and Buzzer Behavior 45
- 6 Host Interfaces47**
- 6.1 Navigating the Host Interfaces Tab..... 47
 - 6.1.1 EEM IP Interface Parameters 47
 - 6.1.2 USB Interface Parameters..... 48
- 7 OMNIKEY 5x27 Configuration Examples.....49**
- 7.1 24BExample 1 – Reading iCLASS Card PACS Data 49
- 7.2 Example 2 – Reading MIFARE Card CSN..... 50
- 7.3 Example 3 – HID iCLASS PACS Data Filtering 51
- 7.4 Example 4 – Prox Card PACS Data Padding 53



Copyright

©2011 - 2014 HID Global Corporation/ASSA ABLOY AB. All rights reserved. This document may not be reproduced, disseminated or republished in any form without the prior written permission of HID Global Corporation.

Trademarks

HID GLOBAL, HID, the HID logo, Indala, iCLASS, iCLASS SE, OMNIKEY, and Seos are the trademarks or registered trademarks of HID Global Corporation, or its licensors, in the U.S. and other countries.

MIFARE, MIFARE Classic, MIFARE DESFire and MIFARE DESFire EV1, MIFARE Easy, and MIFARE Ultralight are registered trademarks of NXP B.V. and are used under license.

Revision History

Date	Description	Version
12/16/2014	Extra detail added to tech order setting	D.3
05/14/2014	EM4450 CSN added. Service Pack 3 features added. Additional information for usability	D.1
02/04/2013	Clarified card de-selection section 2.2.1	D.0
02/13/2013	Data selection and Manipulation added	C.0
08/22/2012	Changed product number from 5127CK to 5x27 CK	B.1
06/27/2012	Service Pack 1 Features added: - PACS bits parsing - DEC Output	B.0

Contacts

Americas & 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 Phoenix Road Haverhill, Suffolk CB9 7AE England Phone: +44 1440 711 822 Fax: +44 1440 714 840	Brazil Condomínio Business Center St. Ermano Marchetti, 1435, Building A2 Lapa - São Paulo/SP CEP: 05038001 Phone: 55 11 5514-7100 Fax: 55 11 5514-7109
HID Global Customer Support: support.hidglobal.com	

1 Overview

HID Global's OMNIKEY® 5x27 CK readers open new market opportunities for system integrators seeking simple integration and development of readers using the standard CCID (Circuit Card Interface Device).

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 5x27 CK Quick Start Guide (5127-901).

Note: HID provides various Service Packs for the OMNIKEY 5x27 CK. Some functions have been introduced with later Service Packs only, in such cases you will find these exceptions noted in this user guide. For downloading the latest Service Pack for your OMNIKEY 5x27 CK reader, access the Developer Center: <http://www.hidglobal.com/main/developers/omnikey-5127-ck/>

Service Packs are available in the **Downloads** section.

Check the firmware version of the OMNIKEY 5x27 CK Reader from the **General Overview** tab in the built-in web interface (see Section 0

Reader Web Based Management Tool Interface, page 11).

1.1 References

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

1.2 Acronyms and Abbreviations

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

Acronym or Abbreviation	Definition/Description
HW	Hardware
FW	Firmware
Config	Short for "Configuration"
RFID	Radio Frequency Identification
ASK	Amplitude Shift Key –a modulation schema for RF communications
PSK	Phase Shift Key –a modulation schema for RF communications
FSK	Frequency Shift Key – a modulation schema for RF communications
HF	High Frequency – 13.56 MHz
LF	Low Frequency – 125 kHz 'Prox'
PACS	Physical Access Control System
CSN	Chip Serial Number
RCN	Random Chip Number
EEM	Ethernet Emulation Mode
CCID	Contact/Contactless Integrated Device
KBW	Keyboard Wedge
OS	Operating System
HTTP	Hyper Text Transfer Protocol

1.3 Supported RFID Technologies

1.3.1 LF Technologies (125kHz)

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

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	CSN, CAN	
CEPAS	CSN, FASC-N, GUID, 75-bit GSA	
PIV	CSN	
FeliCa		
Other ISO14443A		
Other ISO14443B		
Other ISO 15693		

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

1.4 Modes of Operation

1.4.1 Ethernet 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.

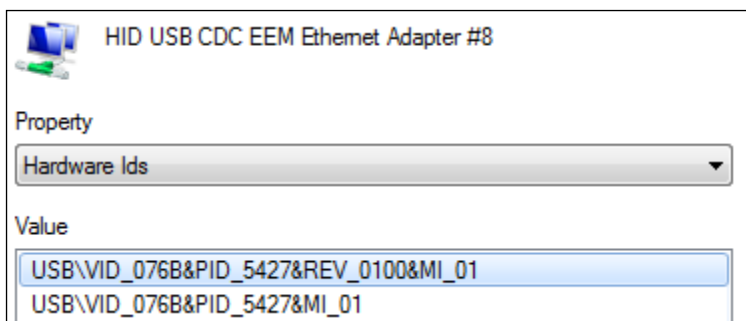
Enumeration

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:

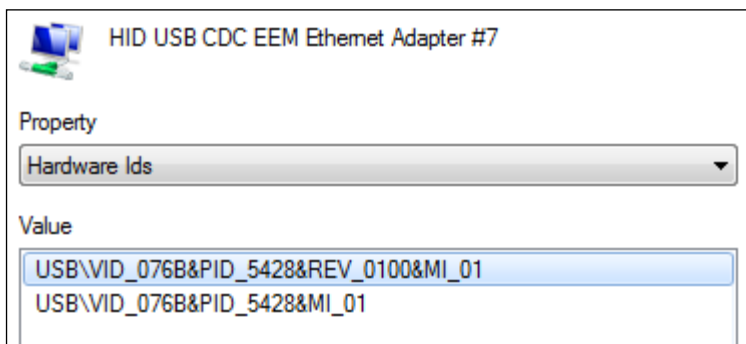
HID USB CDC EEM Ethernet Adapter #n (n is the number of occurrence of the device)

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



Keyboard Wedge Mode or Custom Report Mode is Operational



1.4.2 CCID

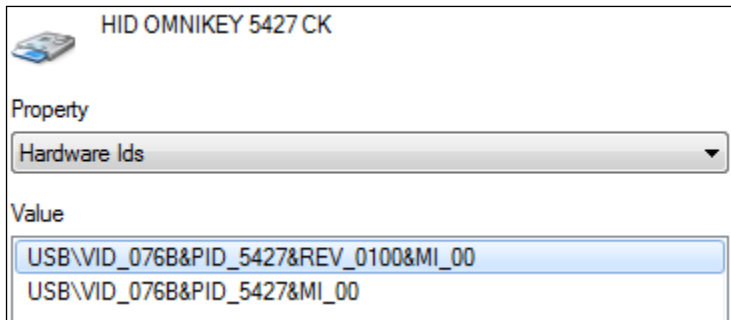
CCID is mainly used for read/write applications or with hosts that cannot support a keyboard input. CCID required an intelligent host and operates as a transparent PC/SC – CCID reader where the host controls every aspect of the card communication.

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.



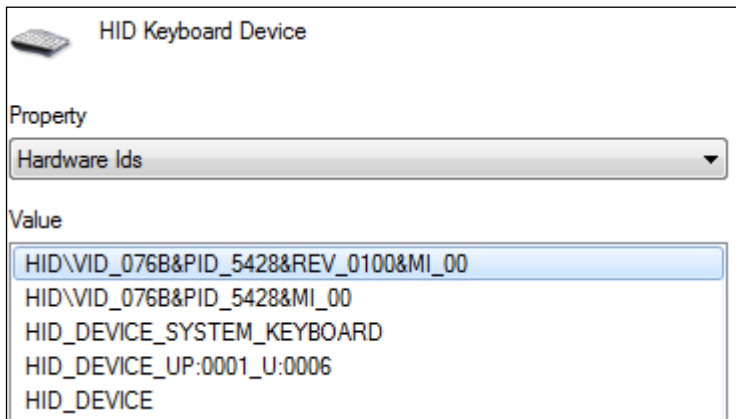
1.4.3 Keyboard Wedge

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.

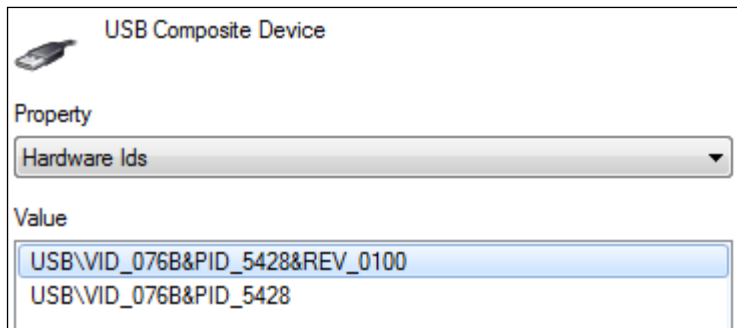


1.4.4 Custom Report

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.



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.

2 Reader Web Based Management Tool Interface

The OMNIKEY 5x27 CK 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

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 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 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 cannot fully guarantee interoperability with all web browsers.

Supported Web Browsers (English versions only)

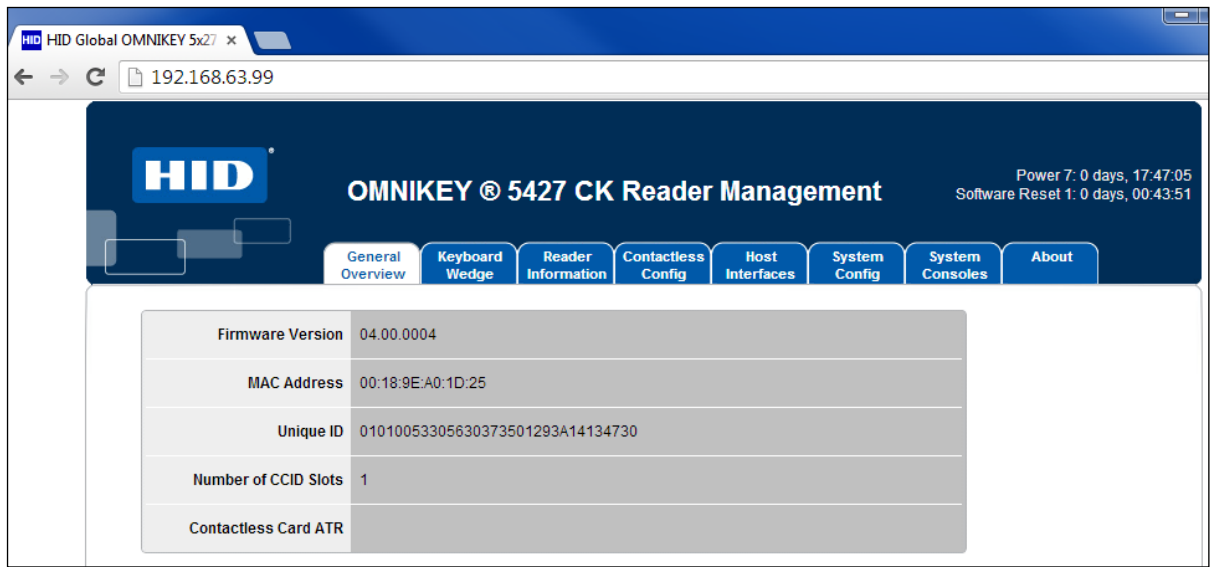
- Internet Explorer, versions 8, 9, 10 and 11
- Compatibility Mode must be disabled
- FireFox, version 28.0
- Chrome, version 33 and 34
- Opera, version 20
- Safari, version 5.1.7

Known issues may exist with different FW revisions of the OMNIKEY 5x27 and specific browsers. Please refer to the FW release notes for any known issues.

2.2 Navigating the 5x27 CK Web Based Management Tool

2.2.1 Accessing the Web Interface

1. Start a web browser on your computer
2. Enter **http://192.168.63.99/** into the address bar and press **Enter**. The web server launches with the **General Overview** page selected.



2.2.2 Navigating the Tabs

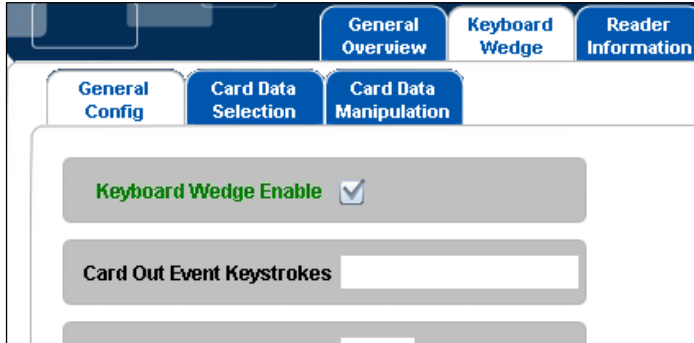
The following list will detail the functions of each tab.



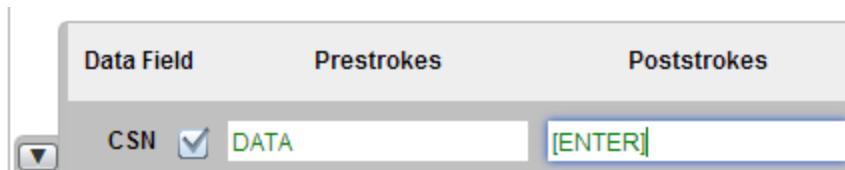
Tab	Description	Intended User Level
General Overview	A quick overview of reader information to include Main FW Version, MAC Address, UID of the reader, No. of CCID slots and the Contactless Card ATR.	Novice
Keyboard Wedge	Keyboard Wedge Setup Parameters	Novice
Reader Information	Full view of the reader 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

When altering configuration parameters the description or value color changes to green.

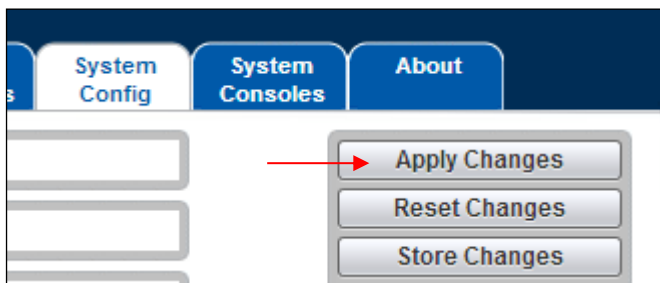


Note: Press **Enter** to finalize text field changes including Special Characters such as [ENTER].



Applying all Settings

To apply all configuration changes, navigate to the **System Config** tab and click **Apply Changes**. The changed configuration parameters revert to black.

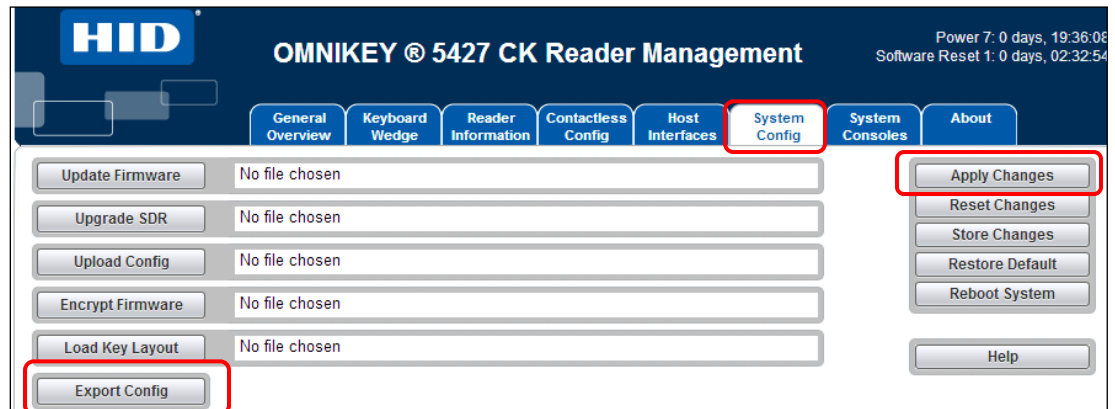


2.2.4 Downloading and Uploading Configurations

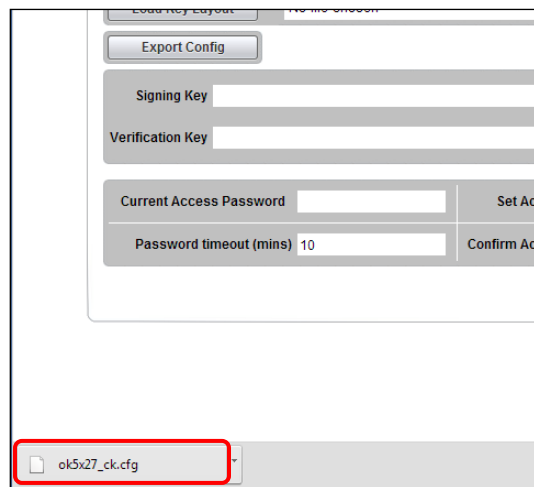
Downloading and uploading configuration files is an important feature of the OMNIKEY 5x27. Once a configuration is fully tested, it can be downloaded and used to make a configuration card using the hid_ok5x27ck_configcard_tool that can be downloaded from the Developer's Center.

Download a Configuration File

1. On the **System Config** tab, change all configuration settings wanted in all tabs.
2. Click **Apply Changes**.
3. Click **Export Config**.

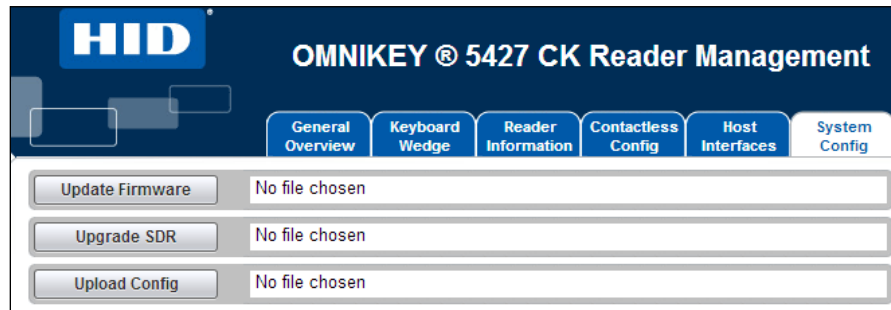


4. Rename the file to be specific to the configuration for future reference (the file will always be named OK5x27ck.cfg upon download).

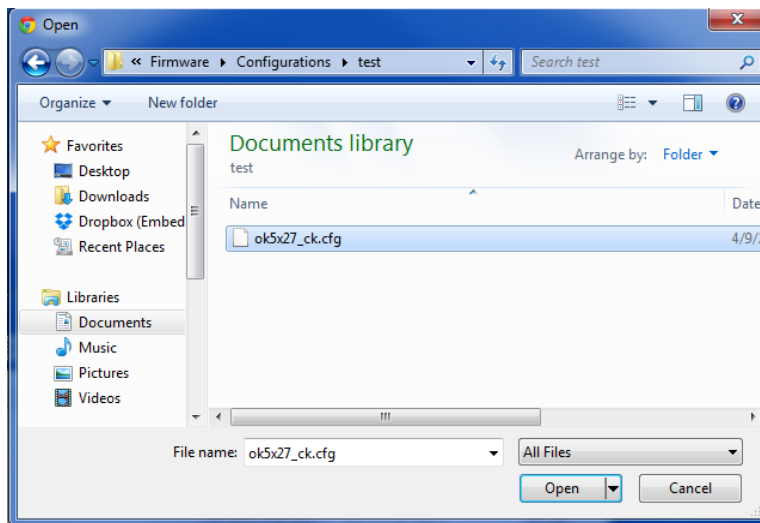


Uploading Configuration File

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



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



3. The configuration file name will now appear in the text box
4. To upload and apply the configuration contains in the file, click the **Upload Config** button



2.2.5 Setting a web server password

The configuration of the OK5x27 CK can be protected by setting a password for the configuration. Once a password is created it will not be possible to access the reader configuration, either via the web server or any of the reader’s programmatic interfaces, without entering the password.

To set the password, enter the existing access password, the new password and confirmation of the new password in the system config tab’s password section. To send the password to the reader hit return when on one of the three password fields. 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 the “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.

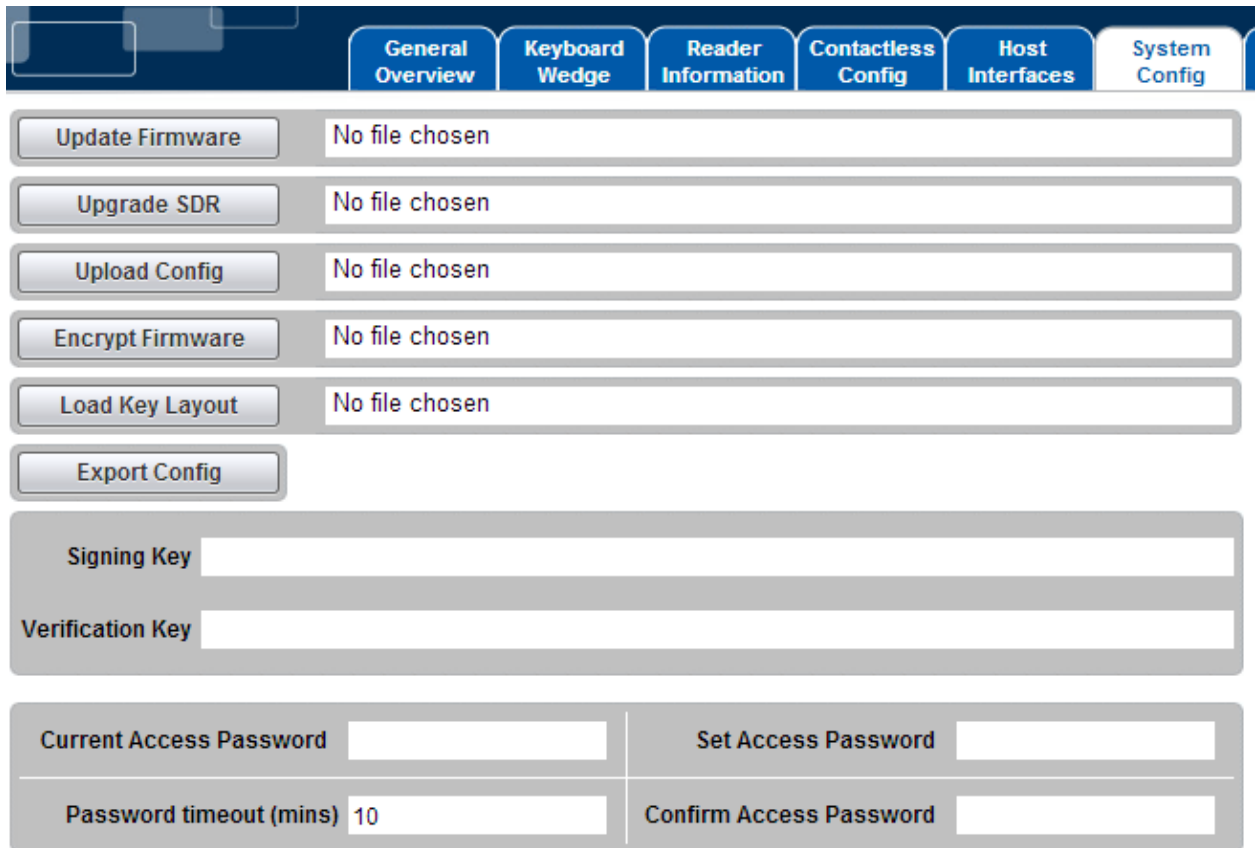


Figure 1: Password Entry options

The password timeout field specifies the amount of time in minutes the current login session will last before the user will have to reenter the password. To use an infinite timeout enter a value of zero.

Once a password is set you will be automatically presented with a log in screen on accessing the webserver. To login, simply 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. If the user prefers 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

Figure 2 Password entry command

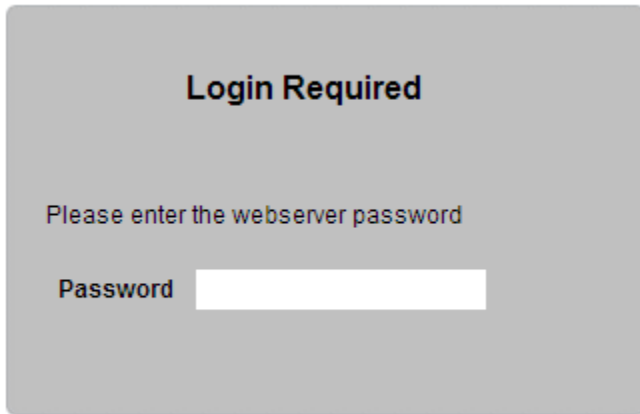


Figure 3 Login screen

3 Keyboard Wedge Mode

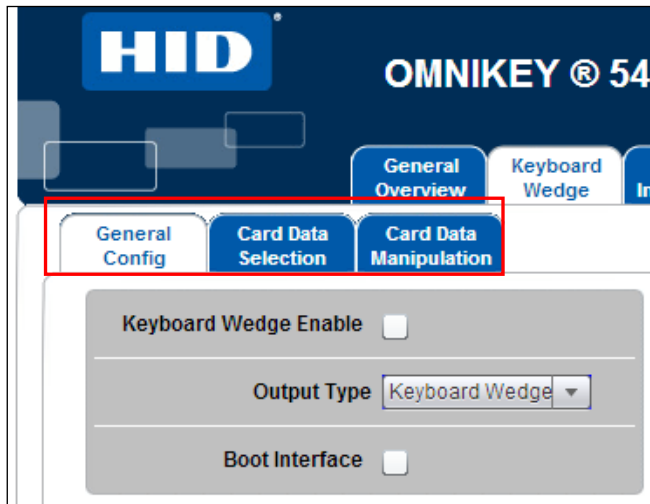
This section provides an exhaustive explanation of the embedded web based OMNIKEY 5x27 CK Reader Management tool for Keyboard Wedge users.

The default configuration for the OMNIKEY 5x27 CK 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.

3.2 Navigating the Keyboard Wedge Configuration Tabs

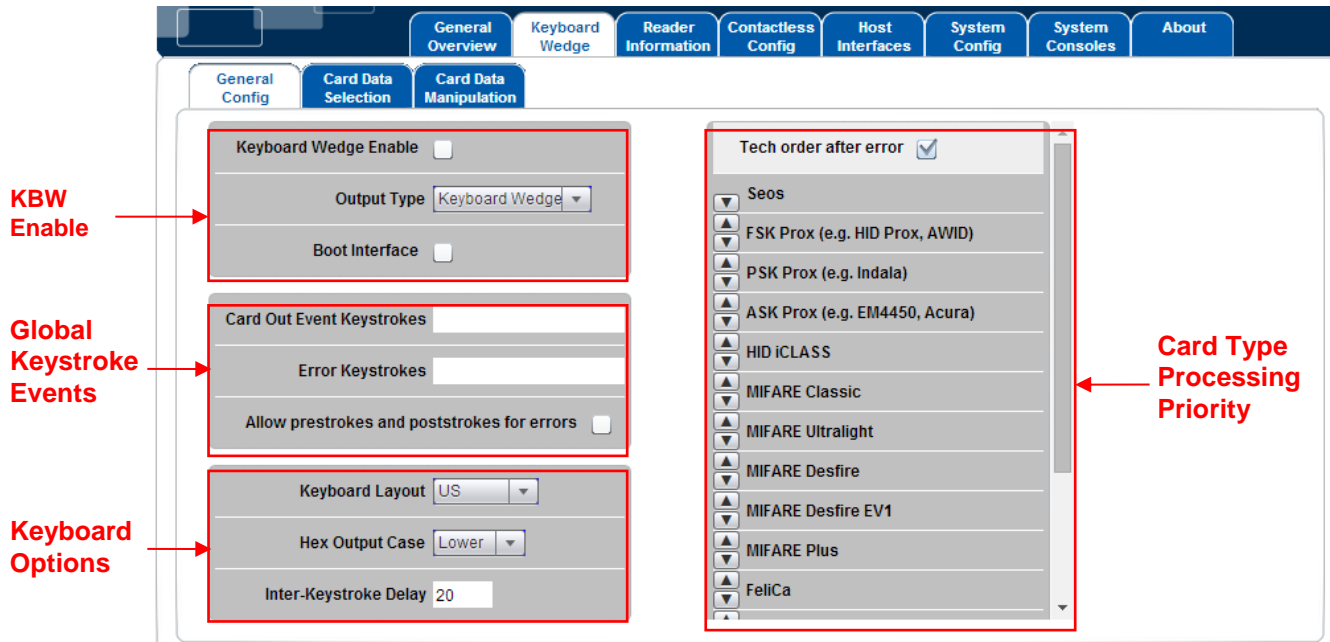


Tab	Description
General Config	Use this tab to enable and setup general keyboard wedge operational parameters.
Card Data Selection	Use this tab to enable and disable card technologies and select the data to be read from the card and reported across the keyboard interface automatically.
Card Data Manipulation	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

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.

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.



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** checkbox. Return to CCID mode by de-selecting the **Keyboard Wedge Enable** checkbox.

Note: When Keyboard Wedge is selected, the 5x27 CK 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 zeroes are added for the remaining length.

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 Prestrokes and Poststrokes for Errors

When enabled, the prestrokes and poststrokes 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 5x27 CK is connected.

The following layouts are built into the reader:

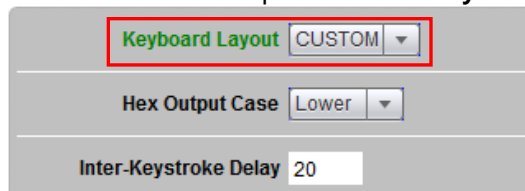
- France
- Germany
- United Kingdom
- United States

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)

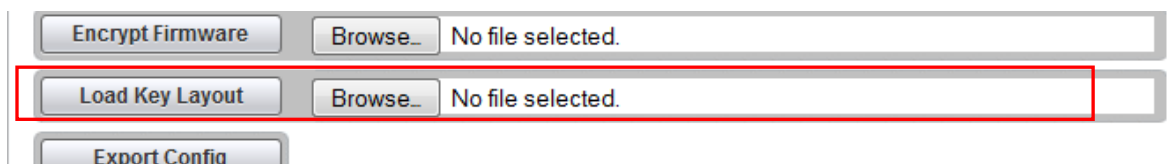
The reader allows for any keyboard layout to be used with the reader. To use such a layout, follow these steps:

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.



The screenshot shows a configuration panel with three sections. The top section has a dropdown menu labeled 'Keyboard Layout' with 'CUSTOM' selected. The middle section has a dropdown menu labeled 'Hex Output Case' with 'Lower' selected. The bottom section has a text input field labeled 'Inter-Keystroke Delay' with the value '20'.

5. Navigate to the **System Config** tab.
6. Click **Apply Changes**.
7. Click on the file selection box next to the **Load Keyboard Layout** button and select the layout file provided by tech support.
8. Click **Load Keyboard Layout**.



The screenshot shows a configuration panel with three buttons and two file selection boxes. The top row has 'Encrypt Firmware', 'Browse...', and 'No file selected.'. The middle row has 'Load Key Layout', 'Browse...', and 'No file selected.'. The bottom row has 'Export Config'.

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/poststrokes (like no card was 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, use the arrow buttons shown below.



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

Note: It 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 (125kHz)

Card Type	FW Version	Data Availability	Protocol Polling*
FSK (HID and AWID Prox)	01000000 or higher	PACS**	Prox
PSK (Indala Prox)	03000000 or higher		
ASK (EM Prox Family)			

* The Polling Config tab is found under the Contactless Config tab

** Prox technologies do not support a CSN and only PACS data is available.

HF Technologies (13.56 MHz)

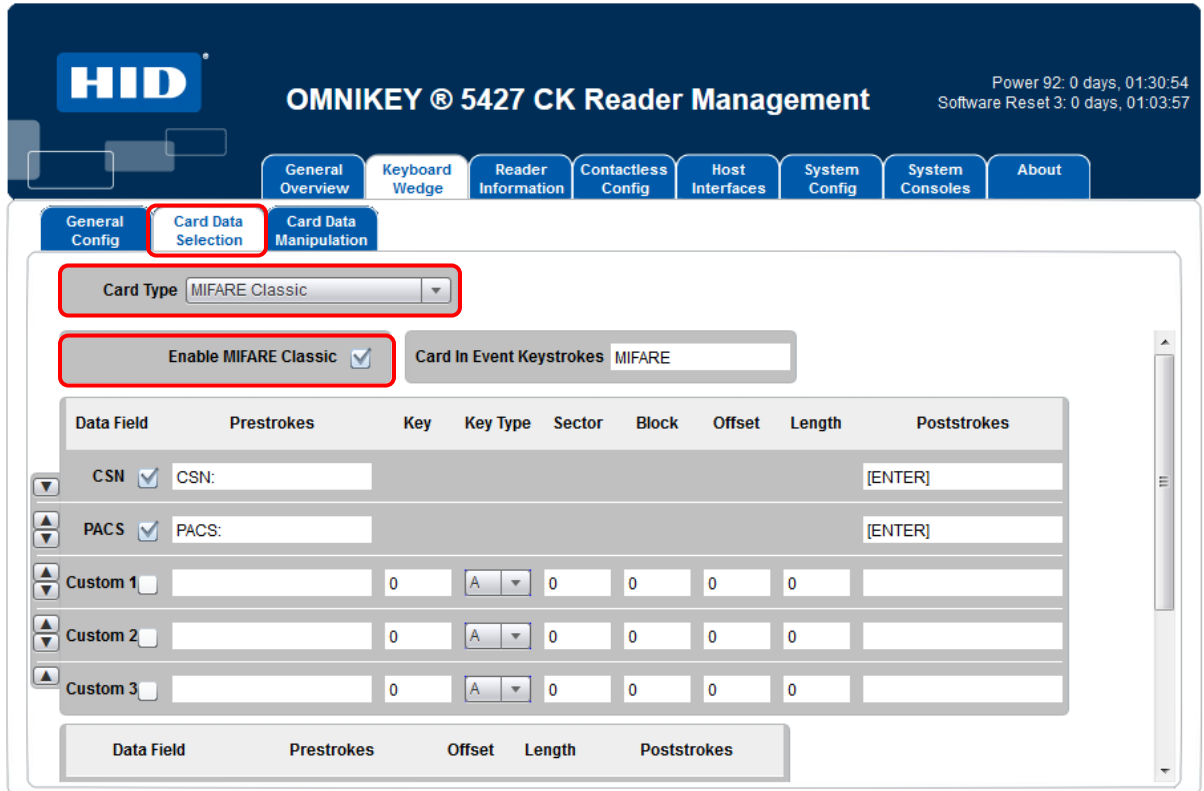
Card Type	FW Version	Data Availability	Protocol Polling*
iCLASS Seos	03000000 or higher	RCN, PACS, Custom	ISO 14443A
iCLASS (includes SR and SE)	01000000 or higher	CSN, PACS, Custom	iCLASS 15693
MIFARE Classic			ISO 14443A
MIFARE DESFire EV1**			
MIFARE Ultralight / C			
MIFARE DESFire 0.6			
MIFARE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

* The Polling Config tab is found under the Contactless Config tab

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

*** Security Level 3 requires firmware 04000000 or higher

3.4.2 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

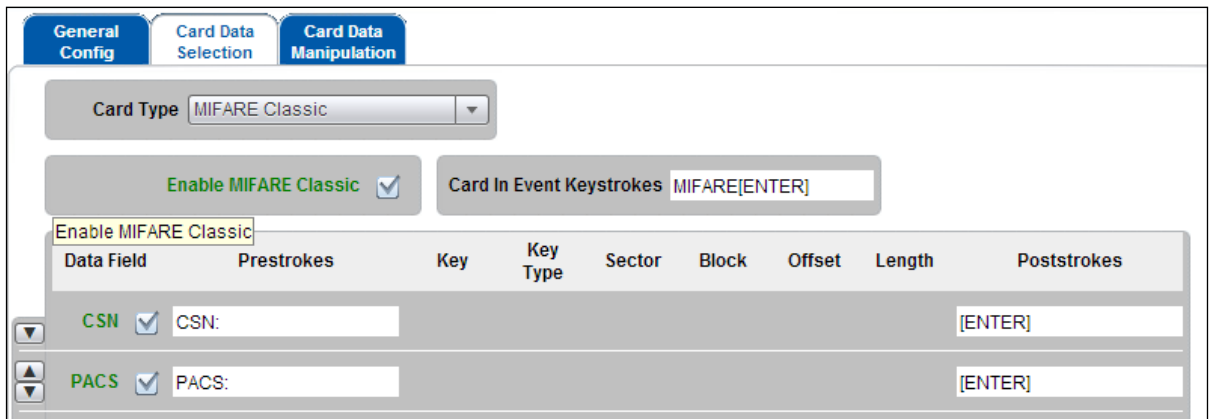
Deselect cards through the web server by selecting the **Enable** button on each card page.

Special Considerations for ISO 14443 Card Types

When an ISO14443A card type is enabled, the reader will read, buffer, process and output all parameters as configured to include Card in even and data pre and poststrokes.

Example: Output with MIFARE Classic Card Type Enabled as shown below:

```
MIFARE
CSN:7d1bf3ae
PACS:02020097
```



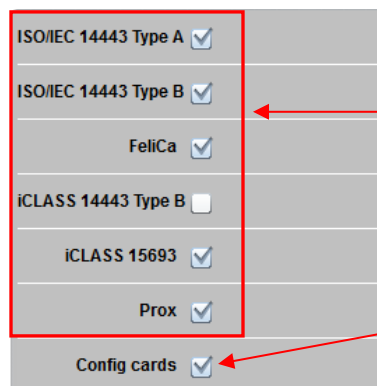
When any ISO 14443A card type is disabled, the reader will read and output the CSN and PACS data fields.

Example: Output with MIFARE Classic Card Type Disabled

CSN + PACS
7d1bf3ae02020097

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.



Only enable the protocols that are needed to provide the best user experience.

HID suggests not to disable Config cards.

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.

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	FF68090102100000	FF680902011000
PSK*	Disable PSK1 FF68090102010000 Disable PSK2 FF68090102020000 Disable PSK3 FF68090102040000 Disable PSK4 FF68090102080000	Read PSK1 FF680902010100 Read PSK2 FF680902010200 Read PSK3 FF680902010400 Read PSK4 FF680902010800
ASK	FF68090102200000	FF680902012000

* 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 Read Setting	Response
FSK	FF680900011000	Should match setting previously sent
PSK*	PSK1 FF680900010100 PSK2 FF680900010200 PSK3 FF680900010400 PSK4 FF680900010800	Should match setting previously sent Should match setting previously sent Should match setting previously sent Should match setting previously sent Should match setting previously sent
ASK	FF680900012000	Should match setting previously sent

3. Configure Data Fields for Each Card Type

5x27 CK supports preset and custom data fields and keystrokes to be output by the reader in Keyboard Wedge mode.

Note: Previous to SP3 all pre/poststroke, 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 5x27 CK those are the PACS-Bits and CSN. Memory area, key configuration is preset in the 5x27 CK; 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 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 anticollision 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 5x27 CK. Enter key references using decimal in the keyboard wedge configuration interface.

See the Software Developer Guide, Chapter 9 for key loading details.

www.hidglobal.com/main/developers/omnikey-5127-ck/

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 bitstream 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 3.4.2.3.1 Preset Data Fields, page 28.

In case you are extracting only part of the full PACS bitstream, 5x27 CK 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 bitstream 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 sections, 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

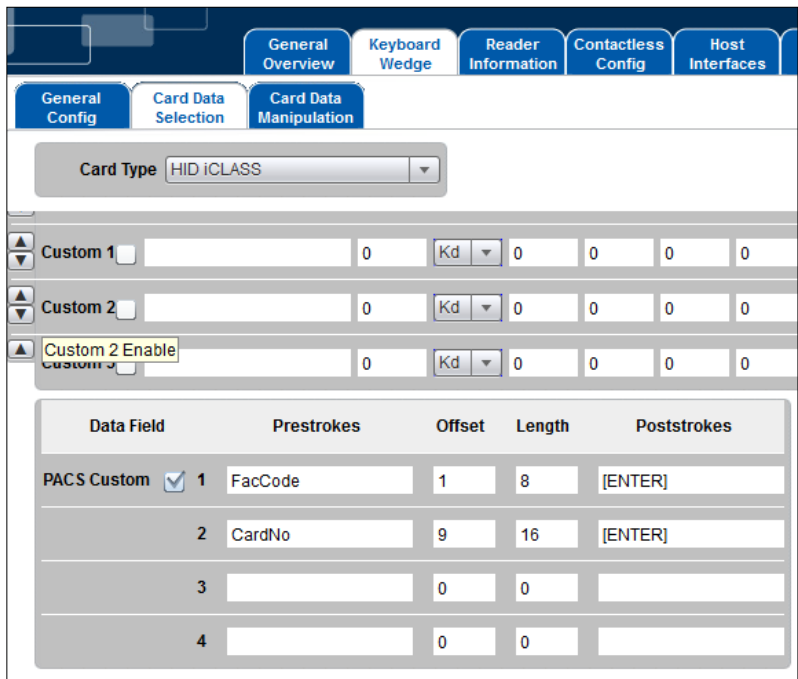


Figure 4 – Prox Card Custom PACS Card Data Selection H10301 Example

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/poststroke, 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.

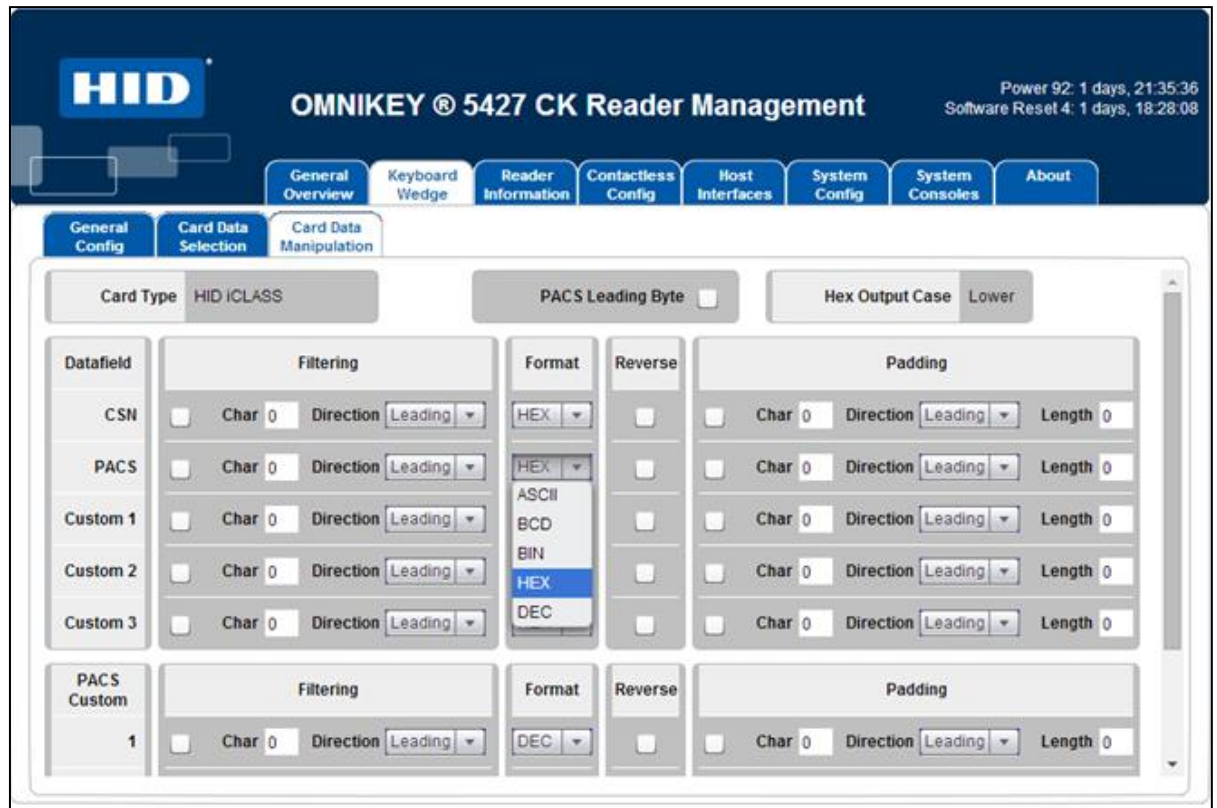
3.5 The Card Data Manipulation Tab

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.



3.5.1 Using the Card Data Manipulation Tab

Format Output Selection



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 conversion of the PACS data with no padding.

EXAMPLE (26 Bit Wiegand PACS Format):

Data on Card	01100100000010011100010010
DEC 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
HEX 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	10111111111111111111111111111110
HEX Output	05FFFFFFE
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 bitstream.

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	10111111111111111111111111111110
Decimal Value	25769803774
BCD Output	0010010101110110100110000000011011101110100
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 01100100000010011101010010 000000 Facility Code: 200 (DEC) Card Number: 5001 (DEC)	

EXAMPLE (35 bit Corporate 1000 Test 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 11111111111111010000000000000010 00000 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 that 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: Notice that the reverse option starts with the raw byte-level data (HEX value) and then applies the output format manipulation.

40 characters with L. To support this, simply configure the Padding parameters as follows.

EXAMPLE: (H10301 26 bit Wiegand PACS Format – Leading L’s to equal a fixed length output of 48 characters)

Output Format	H10301 Output
BIN	LLLLLLLLLLLLLLLLLLLLLLLLLLLLLLLL01100100000010011100010010
DEC	LL26224402
HEX	LL01902712
BCD	LLLLLLLLLLLLLLLLLLLL001001100010001001000100000000010

EXAMPLE: (H10304 37 bit PACS Format – Trailing L’s to equal a fixed length output of 48 characters)

Output Format	H10304 Output
BIN	011111111111111111000000000000000000000010LLLLLLLLLLLLL
DEC	68718428162LLL
HEX	0FFFF00002LLL
BCD	68718428162LLL

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/poststroke, 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 Poststroke 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 , for the reader to perform validity check on the keystrokes.
- For firmware versions 02000000 or above, pressing  **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 - 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.

Table 1 – 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
Tab	TAB
F1	F1
...	...

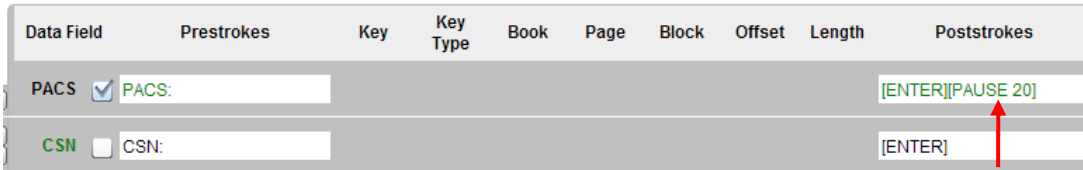
Control Character / Key	Abbreviation
F12	F12
Shift	SHIFT
Ctrl	CTRL
Alt	ALT
Delete	DEL
Windows	GUI

3.6.3 Reader Command Keystrokes (Controlling Reader Behavior)

[PAUSE xxx] (firmware 04000000 or higher)

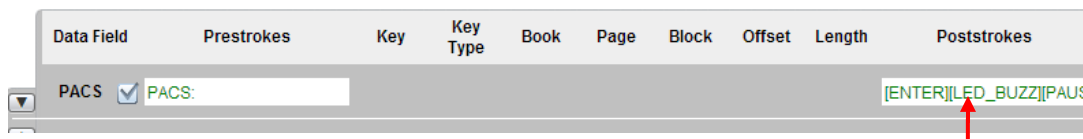
The PAUSE character places the OMNIKEY Reader into a hold state where it will not process any cards. This is to allow the host system to process the card data received by the reader and perform additional functions before possibly receiving another dataset from the reader.

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



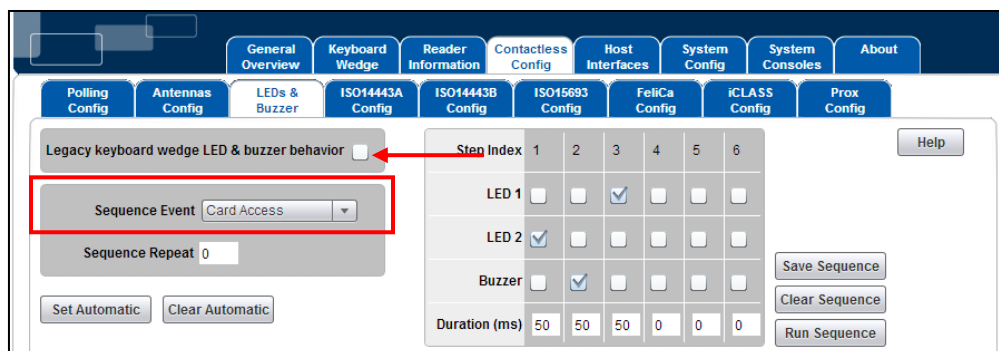
[LED_BUZZ] (firmware 04000000 or higher)

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 located in the **Contactless Config** tab.



Note: The Postrokes Field above is configured to output the selected data and then follow the output with the followed by the LED/Buzzer Sequence and then a 2 second wait period before another card can be processed.

To enable this feature, the following selection box must be deselected as shown below.



3.7 Using all Pre/Poststrokes events to Create an Output String and Control Reader Behavior

3.7.1 Card In Event

The 5x27 CK 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-stroke** Keystrokes sent after the data field.

You can have 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 5x27 CK 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.

4 New Supported Features

4.1 PIV and CEPAS Card Support (firmware 04000000 or higher)

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.

Figure 5: PIV Settings

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

FASC-N Custom <input checked="" type="checkbox"/>	1	Agency:	4	0	[ENTER]
Remove Parity <input checked="" type="checkbox"/>	2	System:	24	16	[ENTER]
Reverse BCD <input checked="" type="checkbox"/>	3	CredNum:	44	24	[ENTER]

Figure 6: 40 bit BCD FASC-N settings

FASC-N Custom <input checked="" type="checkbox"/>	1	Agency:	4	0	[ENTER]
Remove Parity <input checked="" type="checkbox"/>	2	System:	24	16	[ENTER]
Reverse BCD <input type="checkbox"/>	3	CredNum:	44	24	[ENTER]

Figure 7: 40 bit reverse BCD FASC-N settings

Data Field		Prestrokes	Offset	Length	Poststrokes
FASC-N Custom <input checked="" type="checkbox"/>	1	Agency: <small>Prestrokes</small>	4	16	[ENTER]
Remove Parity <input checked="" type="checkbox"/>	2	System:	24	16	[ENTER]
Reverse BCD <input type="checkbox"/>	3	CredNum:	44	24	[ENTER]

Figure 8: 64 bit reverse BCD FASC-N settings

FASC-N Custom <input checked="" type="checkbox"/>	1	Agency:	4	16	[ENTER]
Remove Parity <input checked="" type="checkbox"/>	2	System:	24	16	[ENTER]
Reverse BCD <input checked="" type="checkbox"/>	3	CredNum:	44	24	[ENTER]

Figure 9: 64 bit BCD FASC-N settings

FASC-N Custom <input checked="" type="checkbox"/>	1	128bit BCD:[ENTER]	4	16	[ENTER]
Remove Parity <input checked="" type="checkbox"/>	2		24	16	[ENTER]
Reverse BCD <input checked="" type="checkbox"/>	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]

Figure 10: 128 bit BCD FASC-N settings

4.2 MIFARE DESFire EV1 Diversification Support (firmware 04000000 or higher)

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.

General Overview Keyboard Wedge Reader Information Contactless Config Host Interfaces System Config System Consoles About

Card Data Manipulation

MIFARE Desfire EV1

Desfire EV1 Card In Event Keystrokes

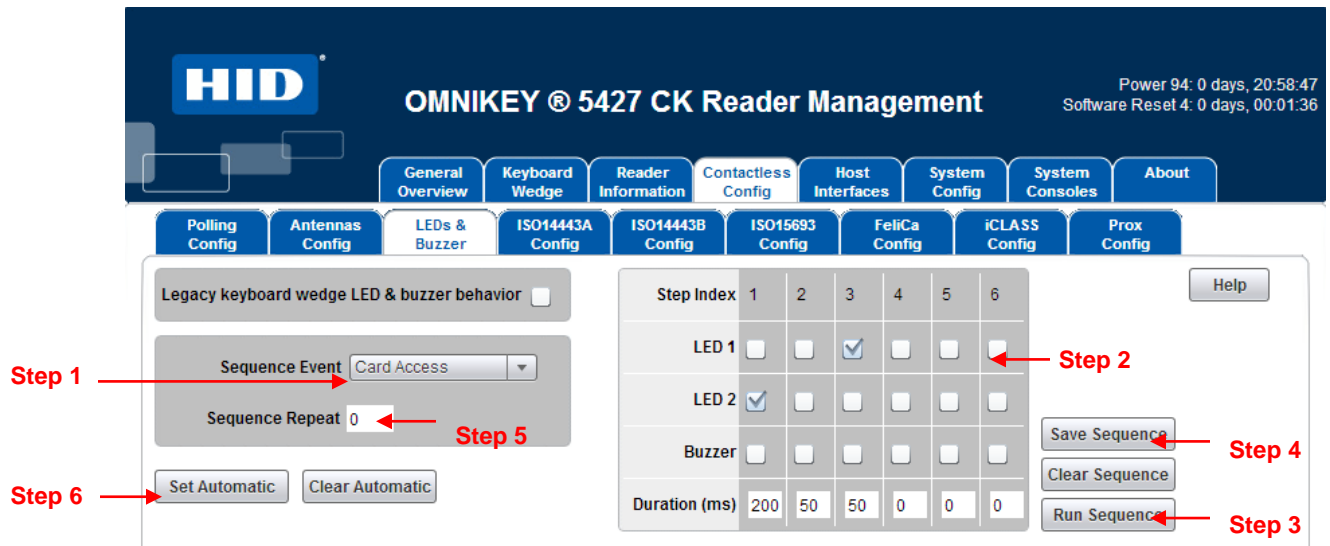
Pre-strokes	App ID	File Num	Start	Len	Card Key	Rdr Key	Auth	File Type	File Comms	Encryption	AV1 Diversify	Post-strokes
	1	0	0	0	0	240	<input type="checkbox"/>	Standard	None	DES/3DES	2KTDES	
	1	0	0	0	0	240	<input type="checkbox"/>	Standard	None	DES/3DES	None	
	1	0	0	0	0	240	<input type="checkbox"/>	Standard	None	DES/3DES	None	

Pre-strokes Offset Length Post-strokes

5 LEDs & 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



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 Sequence Event from the Drop-down Menu

There are 3 sequence events to select from. Choose the event to change.

Sequence Event	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-strokes or error strokes field.

2. Configure LED and Buzzer Sequence and Timing.

Set the sequence through checking the boxes in the rows related to LED 1, LED 2 and Buzzer. Then set the duration for each of the instances by entering 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.

The screenshot shows the 'LEDs & Buzzer' configuration page. On the left, there is a 'Legacy keyboard wedge LED & buzzer behavior' checkbox. Below it, the 'Sequence Event' is set to 'Card Access' and 'Sequence Repeat' is 0. There are 'Set Automatic' and 'Clear Automatic' buttons. On the right, a table defines the sequence:

Step Index	1	2	3	4	5	6
LED 1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
LED 2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Buzzer	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Duration (ms)	200	50	50	0	0	0

Buttons for 'Save Sequence', 'Clear Sequence', and 'Run Sequence' are located to the right of the table.

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. Test the Sequence.

Once the sequence is setup, click the Run Sequence button and observe the LED and Buzzer behavior to make sure everything is set up correctly.

4. Save the Sequence to Memory.

Once the sequence is tested, click the Save Sequence button to save the sequence to memory in the reader.

5. Setup the number of times that the LED and Buzzer Sequence will Repeat.

Use the sequence repeat text box to place a value from 0 to 255.

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.

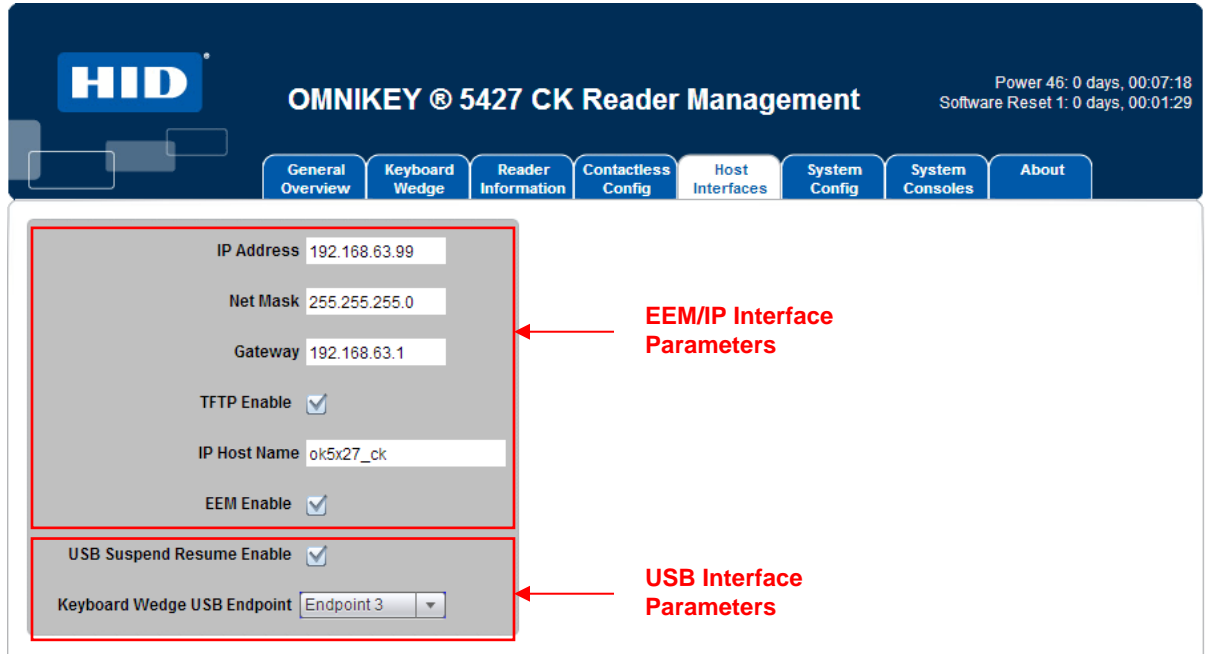
6. Complete and Enable the Sequence to automatically Run on Every Event.

To complete the setup and configure the reader to run the saved sequence, click the Set Automatic button.

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



6.1.1 EEM IP Interface Parameters

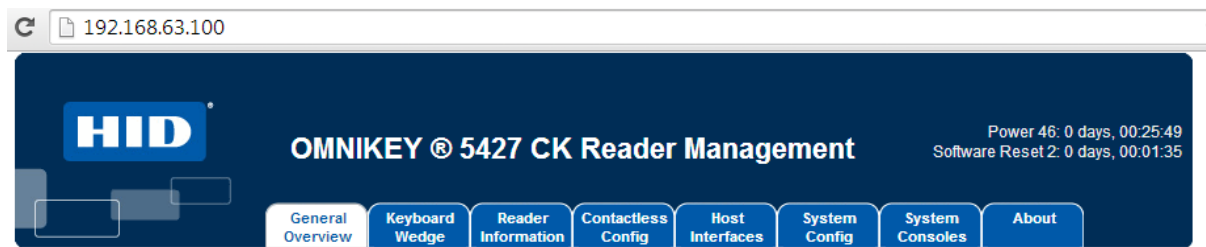
This section allows for the setup of Ethernet Interface parameters. It is suggested that documentation is maintained when changing these parameters.

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 refer to the OMNIKEY 5x27 Software Developer Guide.

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 enabled, the OMNIKEY 5x27 will enumerate as a network adaptor and the host/user may access the Web Based Management tool. When disabled, the Web Based management tool is not accessible.

6.1.2 USB Interface Parameters

USB Suspend Resume Enable (firmware 02000000 or higher)

USB Suspend Resume is not supported by all devices. Please note that with some devices

Keyboard Wedge USB Endpoint (firmware 04000000 or higher)

There are 4 total USB Endpoints that effect device enumeration and USB port transfers.


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

Currently, the USB Endpoint that the OMNIKEY 5x27 operates under is configurable for endpoint 1, 2, or 3 using the Keyboard Wedge USB Endpoint dropdown menu.

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

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 menu, select **HID iCLASS**.
4. Click the **Enable HID iCLASS** checkbox.
5. Click the **PACS** checkbox.
6. In the **PACS Pre-strokes** text field, enter **Start**.
7. Press 

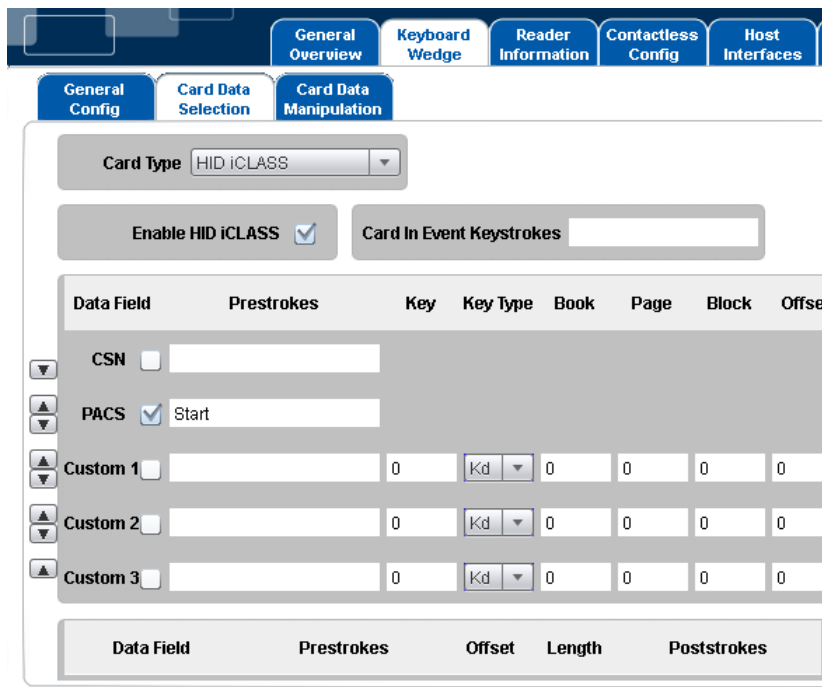




Figure 11 – iCLASS Card PACS Data Example

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. Click the **Enable MIFARE Classic** checkbox.
4. Click the **CSN** checkbox.
5. Enter **Start** into the Pre-strokes text field, press .
6. Enter **End** into the Post-strokes text field, press .

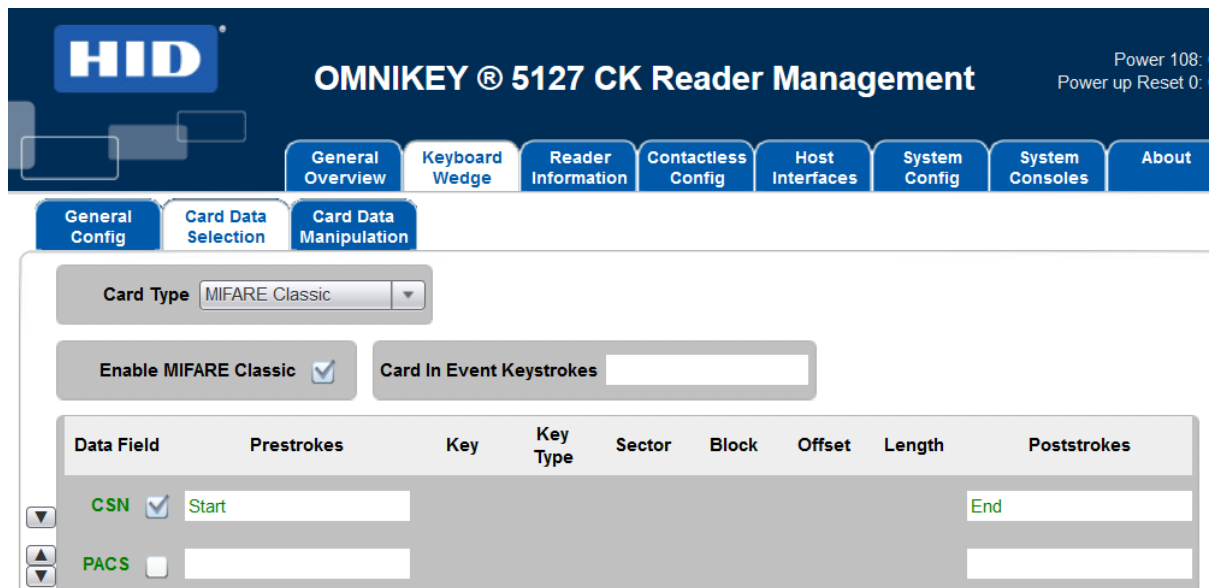




Figure 12 – MIFARE Card CSN Example

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. Go to the **Keyboard Wedge** tab and select the **Card Data Selection** tab.
2. From the **Card Type** drop-down menu, select **HID iCLASS**.
3. Click the **Enable HID iCLASS** checkbox.
4. Click the **PACS** checkbox.
5. Enter **<pacs>** into the Pre-strokes text field, press .
6. Enter **</pacs>** into the Post-strokes text field, press .

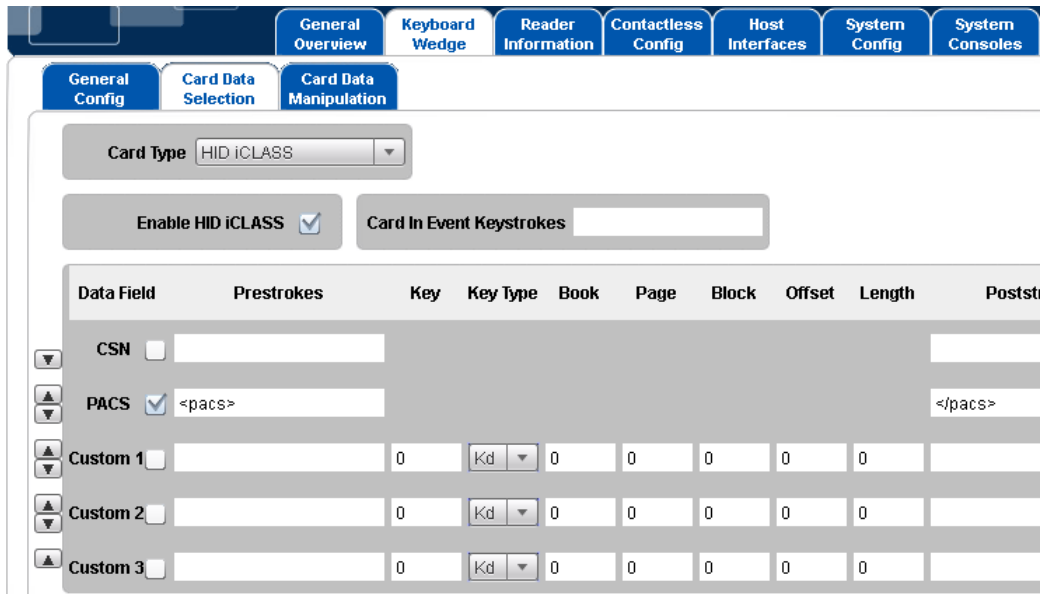


Figure 13 – HID iCLASS PACS Filtering Card Data Selection Example

7. Select the **Card Data Manipulation** tab.
8. Click the check box in the PACS row of **Filtering** box.
9. Make sure **HEX** is selected in PACS row of **Format** box.
10. Enter 'f' in the Char field on the PACS row of the **Filtering** box.

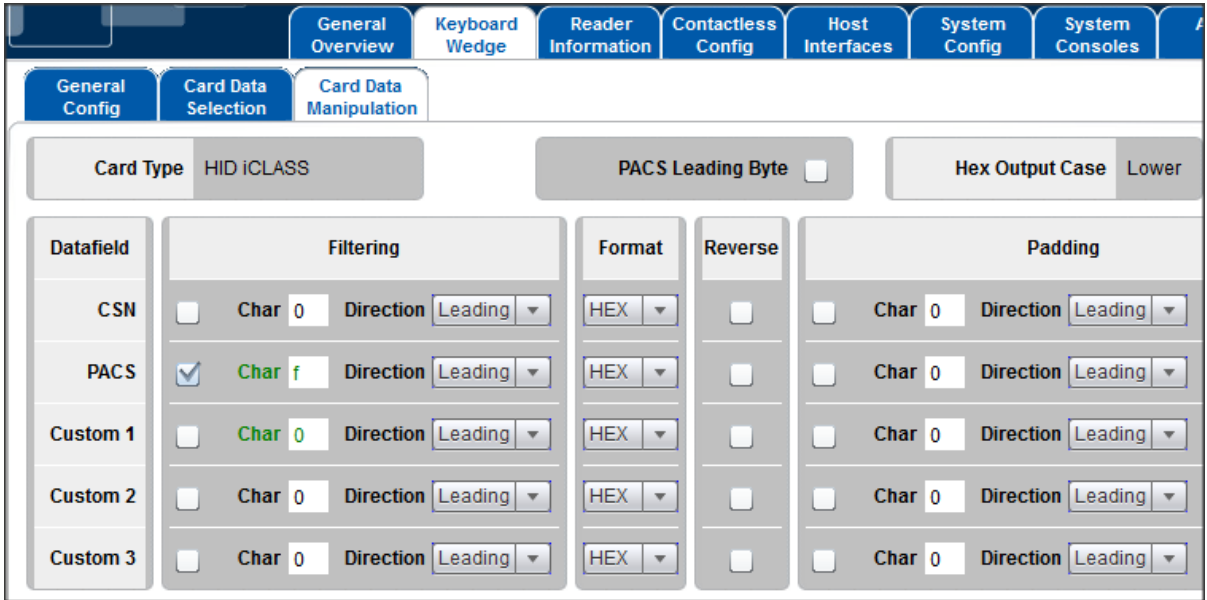


Figure 14 – HID iCLASS PACS Filtering Card Data Manipulation Example

11. Open a text editor and place the iCLASS Sample card into the RFID field over the antenna of the reader.
12. 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. Go to the **Keyboard Wedge** tab and select the **Card Data Selection** tab.
2. From the **Card Type** drop-down menu, select **HID Prox**.
3. Select the **Enable HID Prox** checkbox.
4. Select the **PACS** checkbox.
5. Enter **PROX** into the Pre-strokes text field, press
6. Enter **END** into the Post-strokes text field, press

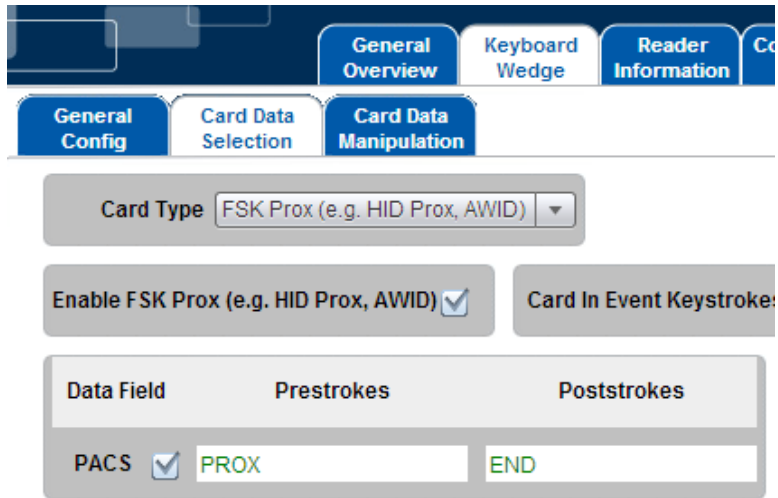
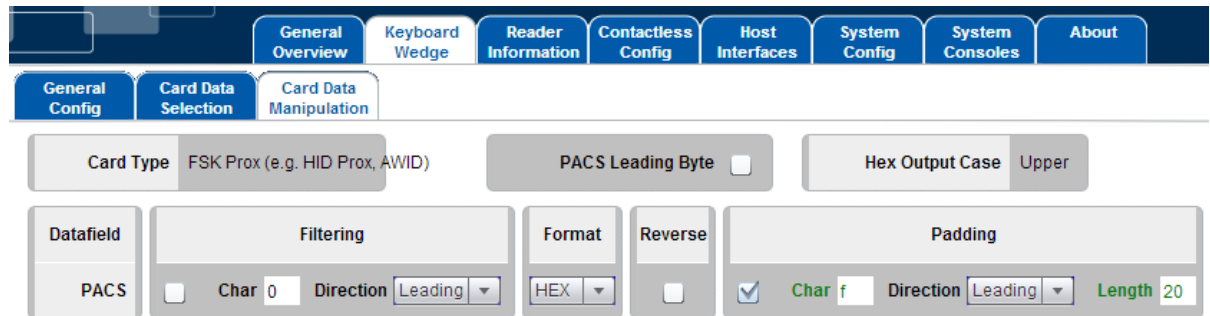


Figure 15 – Prox Card PACS Padding Card Data Selection Example

7. Select the **Card Data Manipulation** tab.
8. Select **HEX** in the PACS row of the Format box.
9. Select the checkbox in the PACS row of the Padding box.
10. Enter 'f' in the Char field in the PACS row of the Padding box.
11. Enter Leading in the Direction field in the PACS row of the Padding box.
12. Enter **20** in the Length field in the PACS row of the Padding box.



The screenshot shows the configuration interface for the HID Prox card. The 'Card Data Manipulation' tab is selected. The 'Card Type' is set to 'FSK Prox (e.g. HID Prox, AWID)'. The 'PACS Leading Byte' checkbox is unchecked. The 'Hex Output Case' is set to 'Upper'. The 'Datafield' section shows 'PACS' with a checkbox that is unchecked. The 'Filtering' section shows 'Char' set to '0' and 'Direction' set to 'Leading'. The 'Format' section shows 'HEX' selected. The 'Reverse' checkbox is unchecked. The 'Padding' section shows a checkbox that is checked, 'Char' set to 'f', 'Direction' set to 'Leading', and 'Length' set to '20'.

Figure 16 – Prox Card PACS Padding Card Data Manipulation Example

13. Open a text editor and place an HID Prox card into the RFID field over the antenna of the reader.
14. Assuming the data on the card is 10000000100000000001001111, the output in the editor will be:
PROXfffffffff0202004fEND

HID Global Headquarters:

North America: +1 949 732 2000

Toll Free: 1 800 237 7769

Europe, Middle East, Africa: +49 6123 791 0

Asia Pacific: +852 3160 9800

Latin America: +52 477 779 1492

support.hidglobal.com

