



Feature Description Document

Understanding Smart Card Options



Purpose

This document provides a detailed understanding of the Smart Card option and its features.

Applies to

TITAN	TFACE	TOUCH 2	SENSE 2	MERGE 2	MYCRO
All Devices	All Devices	All Devices	All Devices	All Devices	All Devices

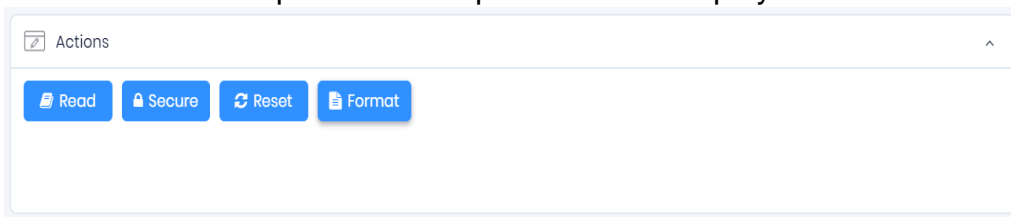
Description

IXM devices come in model variants that are equipped with an internal Smart Card reader for the option of utilizing multi-factor authentication. Smart Cards are RFID access cards that have on-card memory to store biometric data.

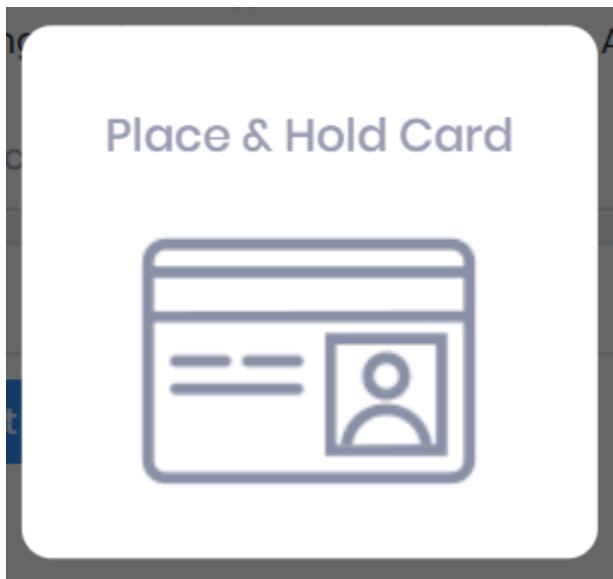
Understanding Smart Card Options

Options:

- a. Different Smart Card options can be performed as displayed in the window.



b. Read Smart Card: Clicking on “Read” prompts a message on the screen for the user to present a Smart Card to the IXM device. Hold to read the record saved on the Smart Card.



c. The Invixium device will read and display all records (by default only the first section will be visible, and users need to expand the remaining sections to view the whole information).

Actions
×

Employee Record

DETAILS

Employee ID 999989	First Name Hardik	Last Name Vadavia	Birth Date -
Employee Type -	Start Date -	End Date -	Card Type MiFare 4K
Serial Number BD13A508	Employee Groups -		

BIOMETRIC INFORMATION

1:N Security -	1:1 Security -	1: N Face Security Medium	1: 1 Face Security Medium
Access Schedules -	Access Rule -	Open Time -	Prox ID -
SmartCard ID -			


GENERAL SETTINGS


Facility Code -	Issue Level -	Anti-Passback Disable	
--------------------	------------------	--------------------------	--

SHIFT

Schedule -	Shift Code -	Holiday No Holiday	Shift Based Access No
---------------	-----------------	-----------------------	--------------------------

Biometric Record

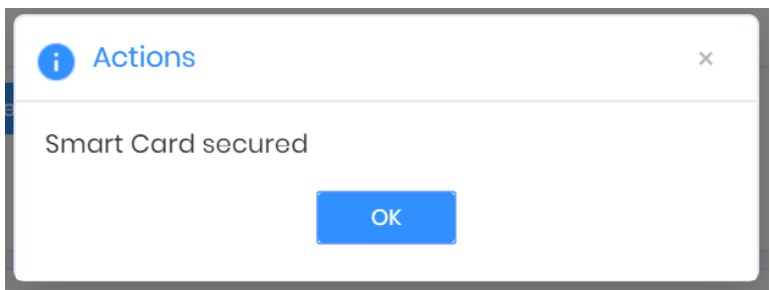
Fingerprint
Right Index Finger
 

Fingerprint
Left Index Finger
 

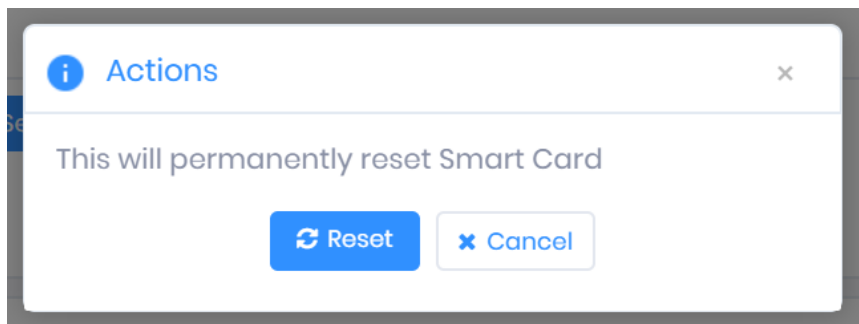
- d. **Secure Smart Card:** Click **Secure** to secure the card, clicking on “Secure” prompts a message on the screen for the user to present a Smart Card to the IXM device. Hold to secure the card.



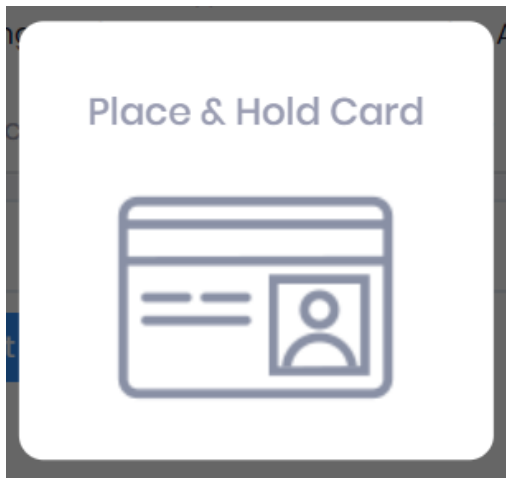
e. A “Smart Card secured” message will be displayed. Click **OK**.



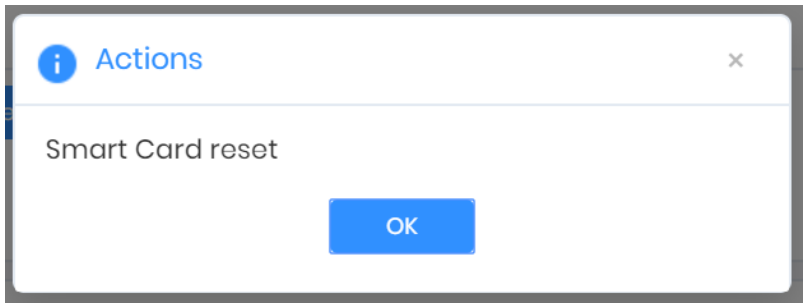
f. Reset smart card: Click **Reset** to reset the Smart Card. Reconfirm the action by clicking on “Reset” in the pop-up dialog. If the “Cancel” option is selected, then no action will be taken.



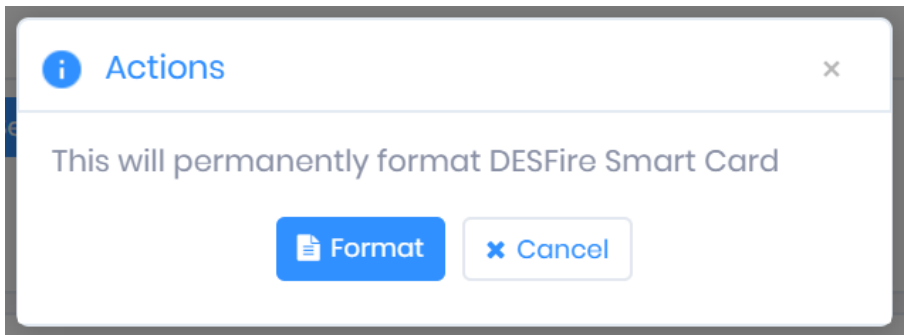
g. Clicking on “Reset” prompts a message on the screen for the user to present a Smart Card to the IXM device and hold to reset the card



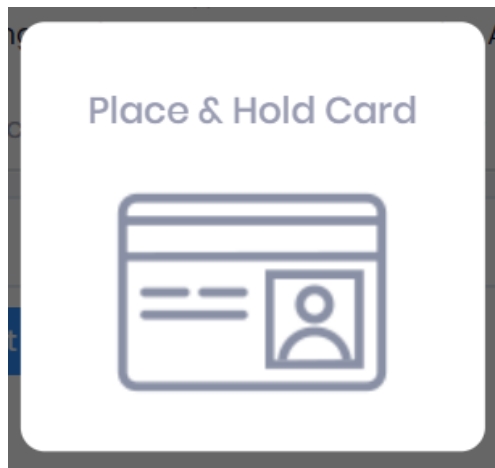
h. A “Smart Card reset” message will be displayed. Click **OK**.



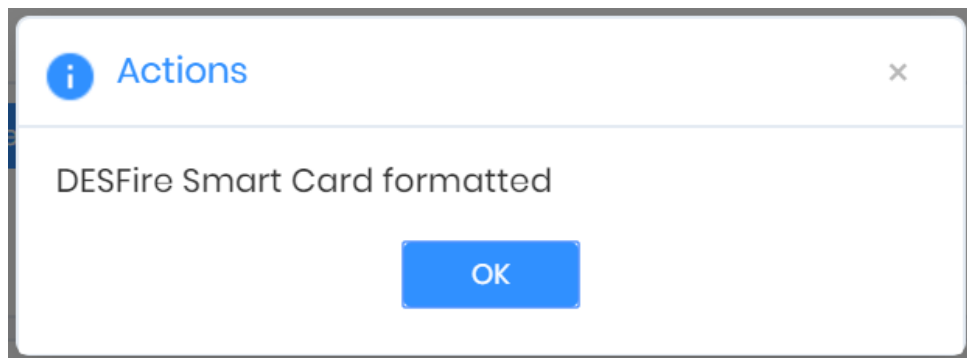
i. Click **Format** to format the card. Reconfirm the action by clicking on “Format” in the pop-up dialog. If the “Cancel” option is selected, then no action will be taken.



j. Clicking on “Format” prompts a message on the screen for the user to present a Smart Card to the IXM device. Hold to format the card.



k. A “Smart Card formatted” message will be displayed. Click **OK**





Key Security Settings

a. To update new keys automatically Toggle “Auto Update” to **ON**.

The screenshot shows the 'Smart Card' settings page for a device with ID 0 and name TSTOUCH2FP2. The device is online. The 'Key Security Settings' section is expanded, showing 'MiFare Key Type' set to 'Key A'. The 'Auto Update' toggle is checked (ON), and the 'Key Encryption' toggle is unchecked (OFF). There are 'APPLY' and 'RESET' buttons at the bottom of the settings section.

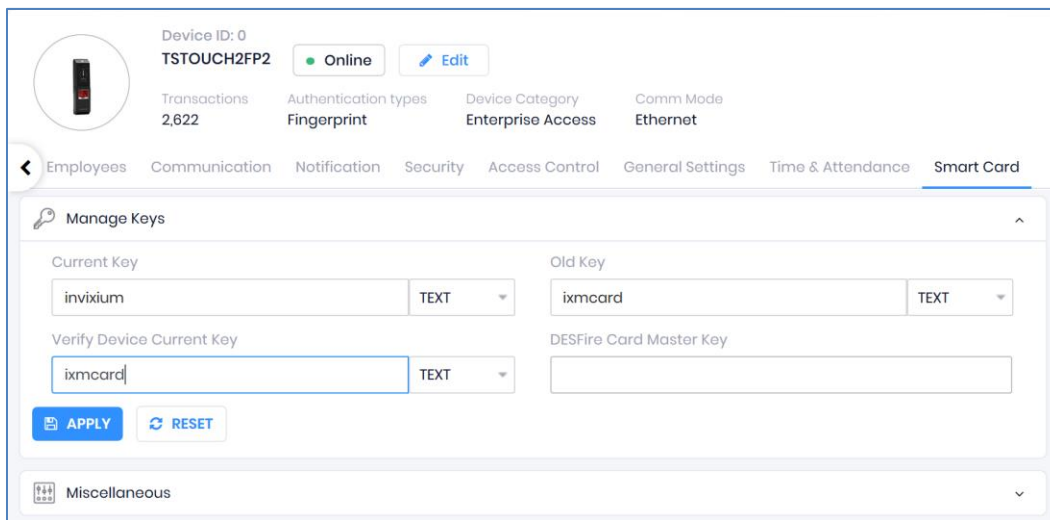
b. To store the key in an encrypted format Toggle “Key Encryption” to **ON**.

This screenshot is identical to the previous one, but the 'Key Encryption' toggle is now checked (ON). The 'Auto Update' toggle remains checked (ON). The 'APPLY' and 'RESET' buttons are still visible at the bottom.

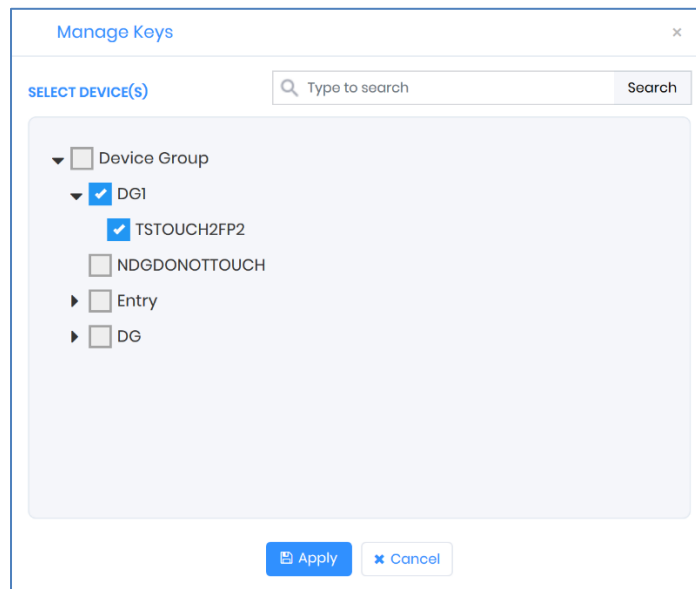
- c. For MIFARE card authentication, Key Type requires an input of either secret KEY A or KEY B.
- d. Click **Apply** to save the modified layout.
- e. A “Smart Card Key Security settings saved” message will be displayed. Click **OK**.

Manage Keys

- a. Fill all the required options as displayed in the Manage Keys Window and click **Apply** to save the modified layout.



- b. It will redirect to device selection to save the modified Layout. Click **Apply** to save the modified Layout on the selected device(s).





c. An Application Log will appear to display the status of success/failure.

The screenshot shows a window titled "Application Logs" with a close button in the top right corner. Inside the window, there is an "Export" button with a download icon. Below the button is a table with the following columns: Details, Status, DeviceName, Date, Reason, and INVIXIU... The table contains one row of data: "Smart Card Keys saved", "Success", "TS TITAN FPLV5", "1/16/2020 5:07:18 PM", and "Sapan". At the bottom of the window, there are navigation arrows and a page indicator showing "1 to 1 of 1 Items".

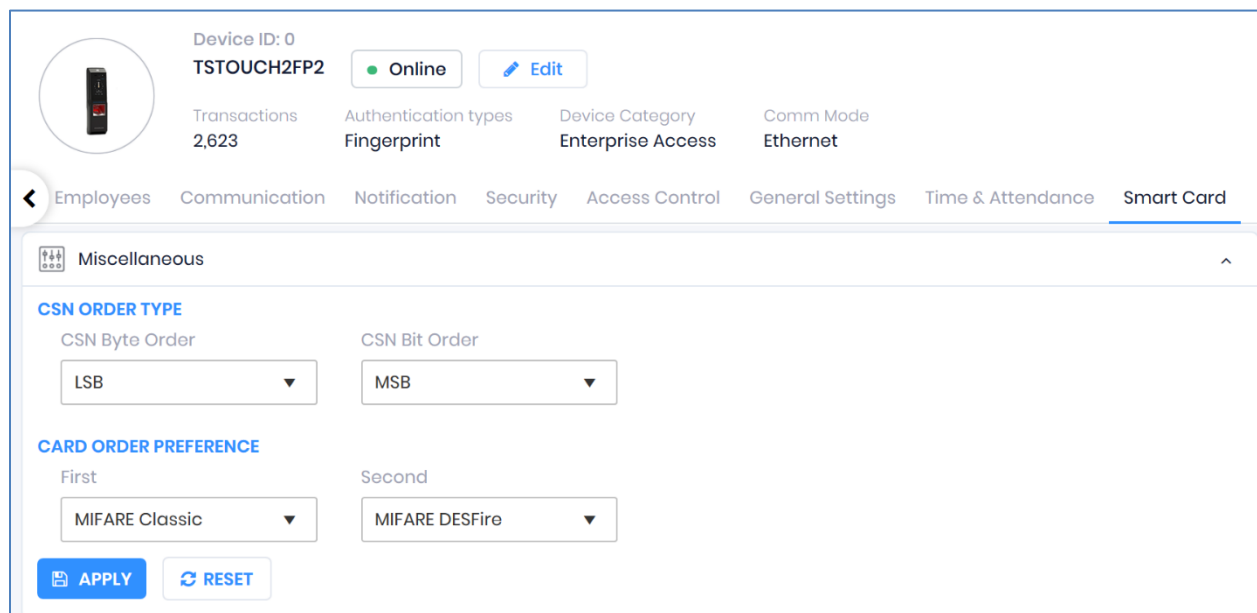
Details	Status	DeviceName	Date	Reason	INVIXIU...
Smart Card Keys saved	Success	TS TITAN FPLV5	1/16/2020 5:07:18 PM		Sapan

Miscellaneous

a. CSN Order Type:

Note: CSN Order Type will be only configurable in FP2, FP4, and FP5 product types.

- IXM WEB allows users to select LSB or MSB values for bit and byte order for Card Serial Number.



Device ID: 0
TSTOUCH2FP2 Online [Edit](#)

Transactions: 2,623 Authentication types: Fingerprint Device Category: Enterprise Access Comm Mode: Ethernet

Employees Communication Notification Security Access Control General Settings Time & Attendance **Smart Card**

Miscellaneous

CSN ORDER TYPE

CSN Byte Order: CSN Bit Order:

CARD ORDER PREFERENCE

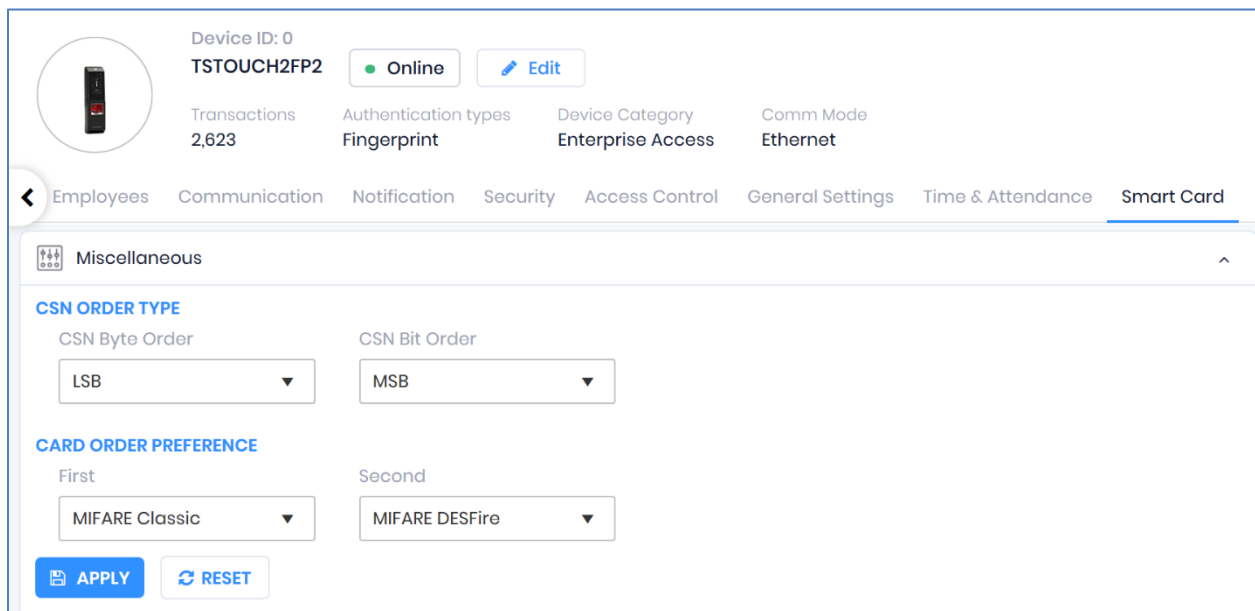
First: Second:

[APPLY](#) [RESET](#)

- Make the required changes to “CSB Byte Order” and “CSN Bit Order” and click **Apply** to save the modified layout.
- A “Smart Card Order saved” message will be displayed. Click **OK**.

b. Card Order Preference:

Note: Card Order Preference will only be configurable in FP2 product types.



Device ID: 0
TSTOUCH2FP2 Online [Edit](#)

Transactions: 2,623 Authentication types: Fingerprint Device Category: Enterprise Access Comm Mode: Ethernet

Employees Communication Notification Security Access Control General Settings Time & Attendance **Smart Card**

Miscellaneous

CSN ORDER TYPE

CSN Byte Order: CSN Bit Order:

CARD ORDER PREFERENCE

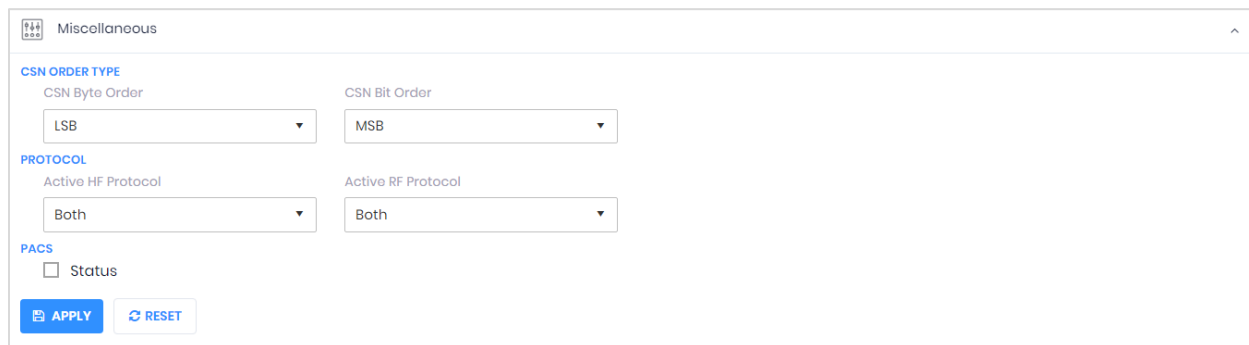
First: Second:

[APPLY](#) [RESET](#)

- Whichever card is selected first will be given the priority.
- Whichever card is selected second it will be given the second priority.

c. Protocol:

Note: Active HF protocol will only be configurable in FP4 and FP5 product types, Active RF protocol will only be configurable in FP5 product types.



Miscellaneous

CSN ORDER TYPE

CSN Byte Order: CSN Bit Order:

PROTOCOL

Active HF Protocol: Active RF Protocol:

PACS

Status

[APPLY](#) [RESET](#)

- Active HF protocol will work according to the selection done from the dropdown i.e: Both, MIFARE, iCLASS.



- Active RF protocol will work according to the selection done from the dropdown i.e: Both, Smartcard, Proxcard.

d. Pacs:

Note: Pacs is configurable for Fp4 and Fp5 product types only.

- By default, Invixium devices read CSN from the card but also allow reading the PACS number from the card.

The screenshot shows the 'Miscellaneous' configuration page. Under the 'CSN ORDER TYPE' section, there are two dropdown menus: 'CSN Byte Order' set to 'LSB' and 'CSN Bit Order' set to 'MSB'. Below these is the 'Active HF Protocol' dropdown set to 'Both'. In the 'PACS' section, the 'Status' checkbox is currently unchecked. At the bottom of the configuration area are 'APPLY' and 'RESET' buttons.

- To read the PACS number from the card, toggle the status of iCLASS PACS to **Active** by checking the box.

This screenshot is identical to the previous one, but the 'Status' checkbox under the 'PACS' section is now checked. Additionally, the 'APPLY' button is highlighted with a red rectangular box.



MIFARE DESFire Reader Configuration

Note: MIFARE DESFire Reader Configuration will only be configurable in FP2, FP4, FP5 product types.

- From **Home** >> Click the **Devices** tab >> Select the required **Device** >> Navigate to **Smart Card** >> Click **Mifare Desfire Configuration**.

The screenshot displays the 'Mifare Desfire Configuration' page for a device named 'FV5 New Camera'. The configuration fields are as follows:

Field	Value
Application ID	16721682
File ID	0
Data Length	0
Data Offset	0
Master Key	[Empty]
Master Key Encryption	None
Application Key	[Empty]
Application Key Encryption	None
Application Key Number	0
Data Communication Mode	Plain
Wiegand Mode	<input type="checkbox"/>

- MIFARE DESFire configuration includes Application ID, File ID, Data length, Data offset, Master key, Master key encryption, Application key, Application key encryption, Application key number, Data communication mode, and Wiegand mode.
- For Master key and Application key, there are three types of encryption: 2K 3DES, 3K 3DES, and AES 128.
- Three types of Data communication modes are Plain, MAC, and Enciphered.



Reader Configuration

Note: Reader configuration will only be configurable for FP4 and FP5 product type.

- From **Home** >> Click the **Devices** tab >> Select the required **Device** >> Navigate to **Smart Card** >> Click Reader Configuration.

The screenshot shows the INVIXIUM web interface for configuring a device. At the top, there is a device profile for 'FV5 New Camera' with a status of 'Online' and an 'Edit' button. Below this, there are several tabs: Overview, Employees, Communication, Notification, Security, Access Control, General Settings, Time & Attendance, and Smart Card (which is currently selected). Under the 'Smart Card' tab, there is a list of configuration options: Manage Keys, Miscellaneous, Revoked Smart Cards, SEOS Card Load Key, SEOS Configuration, Mifare Desfire Configuration, and Reader Configuration. The 'Reader Configuration' option is expanded, showing a 'Configuration Data' input field with a 'HEX' dropdown menu and an 'APPLY' button. An 'Activate Windows' watermark is visible in the bottom right corner of the screenshot.

- Provide a hex key in the configuration data as per requirement.



Support

For more information relating to this Feature Description document, please contact us at support@invixium.com

Disclaimers and Restrictions

This document and the information described throughout are provided in their present condition and are delivered without written, expressed, or implied commitments by Invixium Inc. and are subject to change without notice. The information and technical data herein are strictly prohibited for the intention of reverse engineering and shall not be disclosed to parties for procurement or manufacturing.

This document may contain unintentional typos or inaccuracies.

TRADEMARKS

The trademarks specified throughout the document are registered trademarks of Invixium Access Inc. All third-party trademarks referenced herein are recognized to be trademarks of their respective holders or manufacturers.

Copyright © 2022, INVIXIUM. All rights reserved.