MAGTEK®
SECURITY FROM THE INSIDE

DynaFlex, DynaProx

Utility

User Manual (Windows)

July 2024

Document Number:
D998200402-704

REGISTERED TO ISO 9001:2015

Copyright © 2018 - 2024 MagTek, Inc.
Printed in the United States of America

INFORMATION IN THIS PUBLICATION IS SUBJECT TO CHANGE WITHOUT NOTICE AND MAY CONTAIN TECHNICAL INACCURACIES OR GRAPHICAL DISCREPANCIES. CHANGES OR IMPROVEMENTS MADE TO THIS PRODUCT WILL BE UPDATED IN THE NEXT PUBLICATION RELEASE. NO PART OF THIS DOCUMENT MAY BE REPRODUCED OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, ELECTRONIC OR MECHANICAL, FOR ANY PURPOSE, WITHOUT THE EXPRESS WRITTEN PERMISSION OF MAGTEK, INC.

MagTek®, MagnePrint®, and MagneSafe® are registered trademarks of MagTek, Inc.
Magensa™ is a trademark of MagTek, Inc.
DynaFlex™, DynaFlex Pro™, DynaProx™, DynaFlex II SCRA™, DynaFlex II PED™, and DynaFlex II GO™ are trademarks of MagTek, Inc.

AAMVA™ is a trademark of AAMVA.
American Express® and EXPRESSPAY FROM AMERICAN EXPRESS® are registered trademarks of American Express Marketing & Development Corp.
D-PAYMENT APPLICATION SPECIFICATION® is a registered trademark to Discover Financial Services CORPORATION
MasterCard® is a registered trademark and PayPass™ and Tap & Go™ are trademarks of MasterCard International Incorporated.
Visa® and Visa payWave® are registered trademarks of Visa International Service Association.

ANSI®, the ANSI logo, and numerous other identifiers containing "ANSI" are registered trademarks, service marks, and accreditation marks of the American National Standards Institute (ANSI).
ISO® is a registered trademark of the International Organization for Standardization.
UL™ and the UL logo are trademarks of UL LLC.
PCI Security Standards Council® is a registered trademark of the PCI Security Standards Council, LLC.
EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC. The Contactless Indicator mark, consisting of four graduating arcs, is a trademark owned by and used with permission of EMVCo, LLC.
The *Bluetooth*® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by MagTek is under license.

Google Play™ store, Google Wallet™ payment service, and Android™ platform are trademarks of Google Inc.

Apple Pay®, iPhone®, iPod®, Mac®, and OS X® are registered trademarks of Apple Inc., registered in the U.S. and other countries. iPad™ is a trademark of Apple. Inc. App Store℠ is a service mark of Apple Inc., registered in the U.S. and other countries. IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used by Apple Inc. under license.
Microsoft®, Windows®, and .NET® are registered trademarks of Microsoft Corporation.

NFC is governed by The NFC Forum.

All other system names and product names are the property of their respective owners.

Table 0-1 - Revisions

Rev Number	Date	Notes
10	Oct 5, 2020	Initial Release
20	March 2, 2021	Updated to reflect new GUI change and added one shot excel configuration instruction.
30	April 22, 2021	Updated GUI to support new firmware features.
40	June 3, 2021	- Redesign new GUI - Added checking empty data for Export to File/SendFile - Added filter empty data item to not show up in list view after converted from Excel - Updated latest MMXNET.dll - Fixed Track Enabled (Set) - Updated Context Menu for Convert Excel tool
50	February 23, 2022	- Updated GUI to support manual card entry. - Added buzzer volume, Barcode Reader and QR code image. - Added instruction how to connect device via RS-232.
60	February 7, 2023	- Added support for updating Wireless firmware. - Added BCR and Apple VAS to transaction modes. - Added PIN request.
70	April 17, 2023	- Added Apple VAS transaction options at section 5.2.
700	September 26, 2023	- Added NFC tag support as section 10.
701	November 13, 2023	- Added TIP/TAX support as section 11. - Added Mifare Classic write support as section 10.3.
702	January 3, 2024	- Added support for DynaFlex II GO BLE at section 2.4.
703	February 15, 2024	- Added support for Google Wallet VAS as section 1.4 and section 5.3.
704	July 1, 2024	- Added support for Flexible UI pages as sections 12, 12.1, 12.2, 12.3, 12.4, and 12.5.

LIMITED WARRANTY

MagTek warrants that the products sold pursuant to this Agreement will perform in accordance with MagTek's published specifications. This warranty shall be provided only for a period of one year from the date of the shipment of the product from MagTek (the "Warranty Period"). This warranty shall apply only to the "Buyer" (the original purchaser, unless that entity resells the product as authorized by MagTek, in which event this warranty shall apply only to the first repurchaser).

During the Warranty Period, should this product fail to conform to MagTek's specifications, MagTek will, at its option, repair or replace this product at no additional charge except as set forth below. Repair parts and replacement products will be furnished on an exchange basis and will be either reconditioned or new. All replaced parts and products become the property of MagTek. This limited warranty does not include service to repair damage to the product resulting from accident, disaster, unreasonable use, misuse, abuse, negligence, or modification of the product not authorized by MagTek. MagTek reserves the right to examine the alleged defective goods to determine whether the warranty is applicable.

Without limiting the generality of the foregoing, MagTek specifically disclaims any liability or warranty for goods resold in other than MagTek's original packages, and for goods modified, altered, or treated without authorization by MagTek.

Service may be obtained by delivering the product during the warranty period to MagTek (1710 Apollo Court, Seal Beach, CA 90740). If this product is delivered by mail or by an equivalent shipping carrier, the customer agrees to insure the product or assume the risk of loss or damage in transit, to prepay shipping charges to the warranty service location, and to use the original shipping container or equivalent. MagTek will return the product, prepaid, via a three (3) day shipping service. A Return Material Authorization ("RMA") number must accompany all returns. Buyers may obtain an RMA number by contacting MagTek Support Services at (888) 624-8350.

EACH BUYER UNDERSTANDS THAT THIS MAGTEK PRODUCT IS OFFERED AS-IS. MAGTEK MAKES NO OTHER WARRANTY, EXPRESS OR IMPLIED, AND MAGTEK DISCLAIMS ANY WARRANTY OF ANY OTHER KIND, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

IF THIS PRODUCT DOES NOT CONFORM TO MAGTEK'S SPECIFICATIONS, THE SOLE REMEDY SHALL BE REPAIR OR REPLACEMENT AS PROVIDED ABOVE. MAGTEK'S LIABILITY, IF ANY, SHALL IN NO EVENT EXCEED THE TOTAL AMOUNT PAID TO MAGTEK UNDER THIS AGREEMENT. IN NO EVENT WILL MAGTEK BE LIABLE TO THE BUYER FOR ANY DAMAGES, INCLUDING ANY LOST PROFITS, LOST SAVINGS, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF, OR INABILITY TO USE, SUCH PRODUCT, EVEN IF MAGTEK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY ANY OTHER PARTY.

LIMITATION ON LIABILITY

EXCEPT AS PROVIDED IN THE SECTIONS RELATING TO MAGTEK'S LIMITED WARRANTY, MAGTEK'S LIABILITY UNDER THIS AGREEMENT IS LIMITED TO THE CONTRACT PRICE OF THIS PRODUCT.

MAGTEK MAKES NO OTHER WARRANTIES WITH RESPECT TO THE PRODUCT, EXPRESSED OR IMPLIED, EXCEPT AS MAY BE STATED IN THIS AGREEMENT, AND MAGTEK DISCLAIMS ANY IMPLIED WARRANTY, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

MAGTEK SHALL NOT BE LIABLE FOR CONTINGENT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES TO PERSONS OR PROPERTY. MAGTEK FURTHER LIMITS ITS LIABILITY OF ANY KIND WITH RESPECT TO THE PRODUCT, INCLUDING NEGLIGENCE ON ITS PART, TO THE CONTRACT PRICE FOR THE GOODS.

MAGTEK'S SOLE LIABILITY AND BUYER'S EXCLUSIVE REMEDIES ARE STATED IN THIS SECTION AND IN THE SECTION RELATING TO MAGTEK'S LIMITED WARRANTY.

SOFTWARE LICENSE AGREEMENT

IMPORTANT: YOU SHOULD CAREFULLY READ ALL THE TERMS, CONDITIONS AND RESTRICTIONS OF THIS LICENSE AGREEMENT BEFORE INSTALLING THE SOFTWARE PACKAGE. YOUR INSTALLATION OF THE SOFTWARE PACKAGE PRESUMES YOUR ACCEPTANCE OF THE TERMS, CONDITIONS, AND RESTRICTIONS CONTAINED IN THIS AGREEMENT. IF YOU DO NOT AGREE WITH THESE TERMS, CONDITIONS, AND RESTRICTIONS, PROMPTLY RETURN THE SOFTWARE PACKAGE AND ASSOCIATED DOCUMENTATION TO THE ADDRESS ON THE FRONT PAGE OF THIS DOCUMENT, ATTENTION: CUSTOMER SUPPORT.

TERMS, CONDITIONS, AND RESTRICTIONS

MagTek, Incorporated (the "Licensor") owns and has the right to distribute the described software and documentation, collectively referred to as the "Software."

LICENSE: Licensor grants you (the "Licensee") the right to use the Software in conjunction with MagTek products. LICENSEE MAY NOT COPY, MODIFY, OR TRANSFER THE SOFTWARE IN WHOLE OR IN PART EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT. Licensee may not decompile, disassemble, or in any other manner attempt to reverse engineer the Software. Licensee shall not tamper with, bypass, or alter any security features of the software or attempt to do so.

TRANSFER: Licensee may not transfer the Software or license to the Software to another party without the prior written authorization of the Licensor. If Licensee transfers the Software without authorization, all rights granted under this Agreement are automatically terminated.

COPYRIGHT: The Software is copyrighted. Licensee may not copy the Software except for archival purposes or to load for execution purposes. All other copies of the Software are in violation of this Agreement.

TERM: This Agreement is in effect as long as Licensee continues the use of the Software. The Licensor also reserves the right to terminate this Agreement if Licensee fails to comply with any of the terms, conditions, or restrictions contained herein. Should Licensor terminate this Agreement due to Licensee's failure to comply, Licensee agrees to return the Software to Licensor. Receipt of returned Software by the Licensor shall mark the termination.

LIMITED WARRANTY: Licensor warrants to the Licensee that the disk(s) or other media on which the Software is recorded are free from defects in material or workmanship under normal use.

THE SOFTWARE IS PROVIDED AS IS. LICENSOR MAKES NO OTHER WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Because of the diversity of conditions and PC hardware under which the Software may be used, Licensor does not warrant that the Software will meet Licensee specifications or that the operation of the Software will be uninterrupted or free of errors.

IN NO EVENT WILL LICENSOR BE LIABLE FOR ANY DAMAGES, INCLUDING ANY LOST PROFITS, LOST SAVINGS, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE, OR INABILITY TO USE, THE SOFTWARE. Licensee's sole remedy in the event of a defect in material or workmanship is expressly limited to replacement of the Software disk(s) if applicable.

GOVERNING LAW: If any provision of this Agreement is found to be unlawful, void, or unenforceable, that provision shall be removed from consideration under this Agreement and will not affect the enforceability of any of the remaining provisions. This Agreement shall be governed by the laws of the State of California and shall inure to the benefit of MagTek, Incorporated, its successors or assigns.

ACKNOWLEDGMENT: LICENSEE ACKNOWLEDGES THAT HE HAS READ THIS AGREEMENT, UNDERSTANDS ALL OF ITS TERMS, CONDITIONS, AND RESTRICTIONS, AND AGREES TO BE BOUND BY THEM. LICENSEE ALSO AGREES THAT THIS AGREEMENT SUPERSEDES ANY AND ALL VERBAL AND WRITTEN COMMUNICATIONS BETWEEN LICENSOR AND LICENSEE OR THEIR ASSIGNS RELATING TO THE SUBJECT MATTER OF THIS AGREEMENT.

QUESTIONS REGARDING THIS AGREEMENT SHOULD BE ADDRESSED IN WRITING TO MAGTEK, INCORPORATED, ATTENTION: CUSTOMER SUPPORT, AT THE ADDRESS LISTED IN THIS DOCUMENT, OR E-MAILED TO SUPPORT@MAGTEK.COM.

DEMO SOFTWARE / SAMPLE CODE: Unless otherwise stated, all demo software and sample code are to be used by Licensee for demonstration purposes only and MAY NOT BE incorporated into any production or live environment. The PIN Pad sample implementation is for software PIN Pad test purposes only and is not PCI compliant. To meet PCI compliance in production or live environments, a third-party PCI compliant component (hardware or software-based) must be used.

Table of Contents

Limited Warranty 4
SOFTWARE LICENSE AGREEMENT 6
Table of Contents 8
1 Introduction 10
1.1 About This Document 10
1.2 System Requirements 10
1.3 How to Download, Install, and Launch the Software 10
1.4 Device Requirements 10
2 How to Connect to Devices Using DynaFlex Utility 11
2.1 How to Connect Using the USB Connection 11
2.2 How to Connect Using the RS-232 Connection 13
2.3 How to Connect Using the WLAN Connection 14
2.4 How to Connect Using the Bluetooth LE Connection 15
3 How to Use Device Information 18
4 How to Update Firmware 19
5 How to Use the Transaction Demo 21
5.1 EMV Transaction 21
5.2 Apple VAS Transaction 23
5.3 Google Wallet VAS Transaction 25
5.4 Barcode Transaction 27
6 How to use the Barcode Reader 28
6.1 Barcode Returned Unencrypted 28
6.2 Barcode Returned Encrypted 29
6.3 Show QR Image 30
7 How to Parse Custom TLV Blobs 31
8 How to use Configurations 32
8.1 Get Configuration settings 32
8.2 Configure System settings 33
8.3 Configure Buzzer Volume 34
8.4 Send Selective Configuration 35
8.5 Send Bulk Configuration 37
8.6 Send Bitmap Images (LCD Device Only) 38
8.7 Configure AAMVA Reading 40
8.8 Configure Magnetic Stripe Track Data 41
8.9 Configure the User Event Notification 42
8.10 Change Device-Driven Fallback Behavior 43
8.11 Change Device Display Orientation (LCD Device Only) 44
8.12 Change Signature Timing Window (LCD Device Only) 45

8.13 Change Signature in Batch (LCD Device Only) 46
8.14 Change Signature Capture Control (LCD Device Only) 47
8.15 Display Message on Device (LCD Device Only) 48
8.16 OID Conversion 49
9 How to use Request PIN 50
9.1 Card Supplied PIN 50
9.2 Host Supplied PIN 52
10 How to use the NFC Demo 54
10.1 NFC Type 2 / Mifare Classic Tag - Read 54
10.2 NFC Type 2 Tag - Write 56
10.3 Mifare Classic Tag - Write 58
11 How to use Tip and Tax Demo 62
11.1 Show Tip and Tax from Host-Initiated transaction. 62
11.2 Show Tip and Tax from Device-Initiated Transaction. 65
12 Flexible UI Page 68
12.1 UI Configuration File 68
12.2 Text Page 70
12.3 Buttons Page 72
12.4 Amount Page 74
12.5 Image Page 76
Appendix A Reserved 80

1 Introduction

1.1 About This Document

This document provides instructions to use the ***DynaFlex, DynaProx Utility*** software for demonstrating EMV transactions, configuration, and firmware updating. Supported devices are DynaFlex, DynaFlex Pro, DynaProx, DynaFlex II PED, and DynaFlex II SCRA. It is part of a larger library of documents designed to assist implementers. For details, see the product Support pages on www.magtek.com.

The following documents are essential:

- ***D998200383 DynaFlex Family Programmer's Manual (COMMANDS)***

1.2 System Requirements

- A Windows 10 host with available USB port
- Microsoft .NET 4.6.1 and above installed on the host
- Microsoft Access Database Engine 2016 Redistributable installed on the host
- USB-C cable with USB Type-A or USB-C for host connection
- Software ***1000007406 DynaFlex, DynaProx Utility***, provided by MagTek
- Root Certificate, Sub CA Certificate, and Client private key Certificate as referenced in document ***D998200550 DynaFlex II PED Using Wireless LAN Guide***..

1.3 How to Download, Install, and Launch the Software

To download ***DynaFlex, DynaProx Utility*** software, follow these steps.

1) Download the software with the name ***1000007406.zip (DynaFlex, DynaProx Utility***) from MagTek.
2) Extract the .zip file on the host's hard drive.
3) Install the ***AccessDatabaseEngine.exe*** from the folder ***Access Database Engine*** in the extracted folder.
4) Download and install Microsoft .NET 4.6.1 or above from https://dotnet.microsoft.com/download/dotnet-framework.
5) Launch ***DynaFlexUtility.exe***.
6) See the steps in the sections below to connect to a device.

1.4 Device Requirements

- For Apple VAS and Google Wallet VAS transactions, see instructions for configuration in the SDK document appendix:

  D998200380 MAGTEK UNIVERSAL SDK PROGRAMMER'S MANUAL (MICROSOFT .NET)

2 How to Connect to Devices Using DynaFlex Utility

To connect via an interface listed in the **Connection Type** box, follow these steps.

2.1 How to Connect Using the USB Connection

1) For best results, use the cable that is included with the device.
2) Connect the USB-C end of the cable to DynaFlex device.

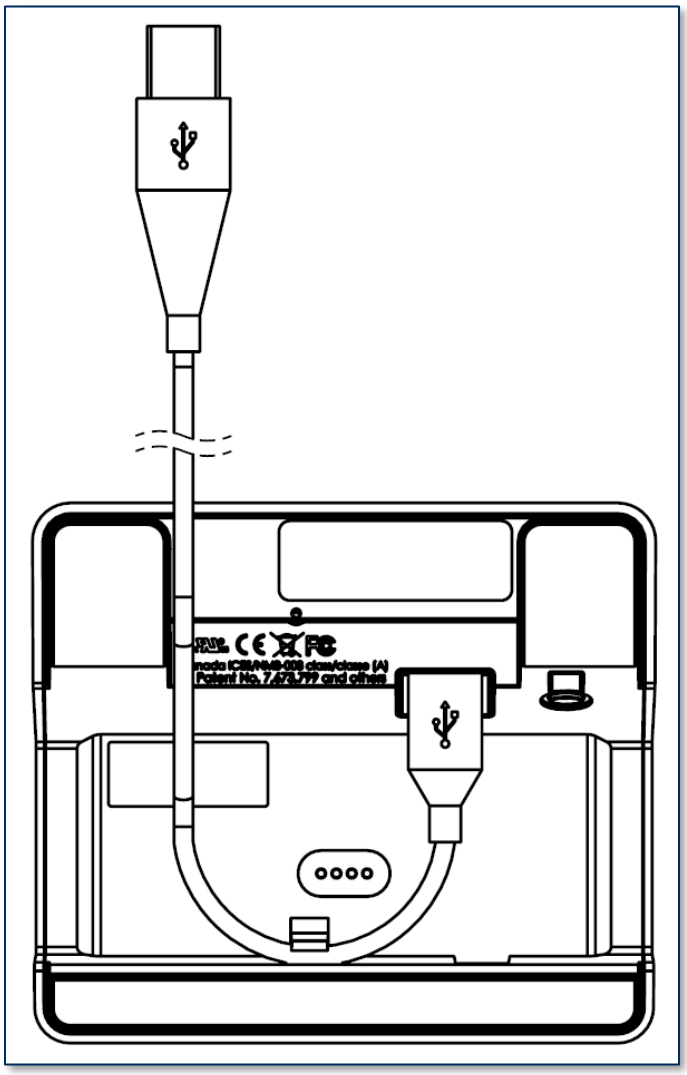
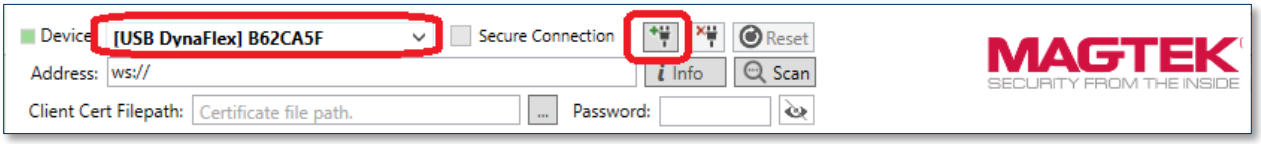


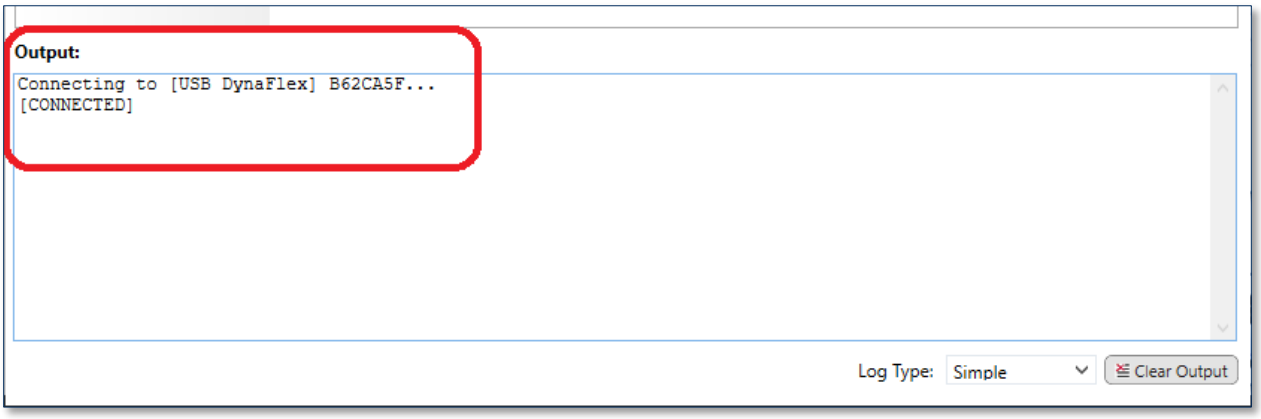
Figure 2-1 - Connecting DynaFlex to a USB Host

3) If you plan to route the cable out the back of the device, route the cable through the cable management clip to change its direction. Even if you are not routing out the back, you may use the cable clip for strain relief, to help stabilize the mechanical connection when cardholders or operators move the device or the cable.
4) Route the cable in the desired direction (e.g., out the back, left, right, or down into the countertop).
5) Connect the other end of the USB cable to the host's USB port.
6) As soon as the device starts receiving power through USB, it automatically powers on.

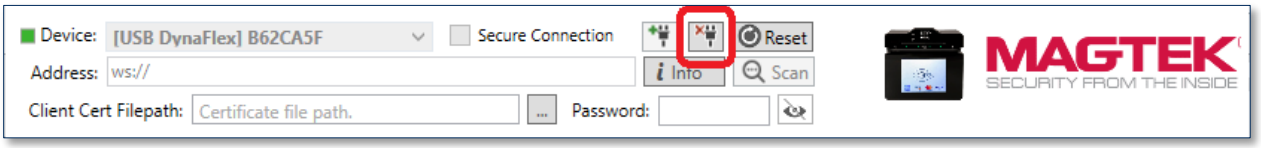
7) Launch the DynaFlex Utility and select **DynaFlex** device in the **Device Type** list, then press the connect button.



8) The **Output** log shows the status of the connection.

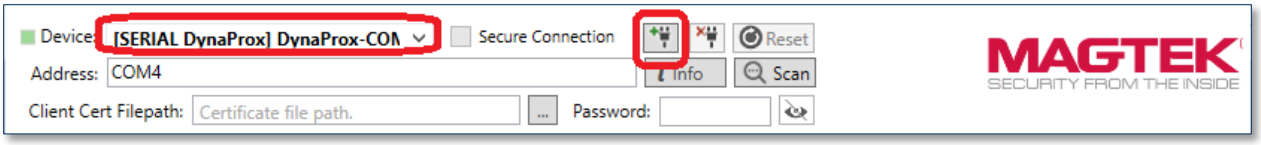


9) To disconnect the device, press **Disconnect** button.

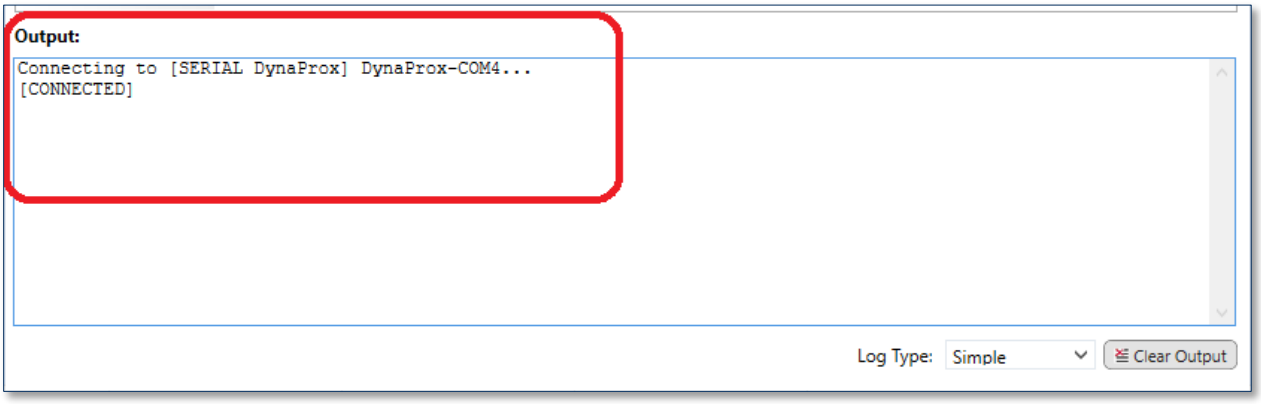


2.2 How to Connect Using the RS-232 Connection

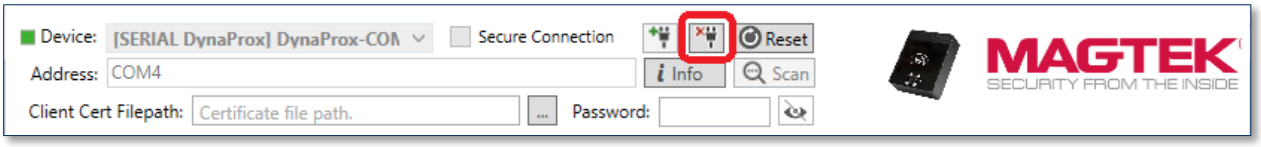
1) Launch the DynaFlex Utility and under the **Device** list select the **SERIAL DynaProx** to which the device is plugged, then press the connect button.



2) The **Output** log shows the status of the connection.



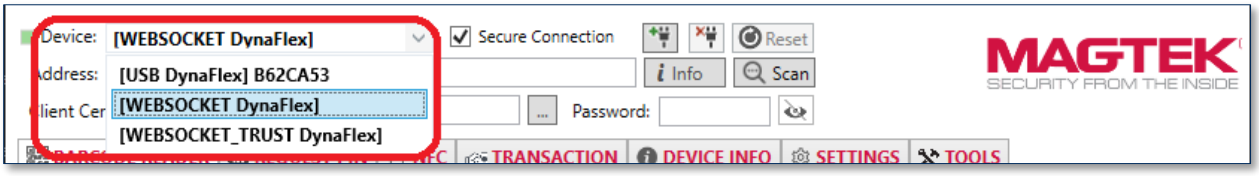
3) To disconnect the device, press **Disconnect** button.



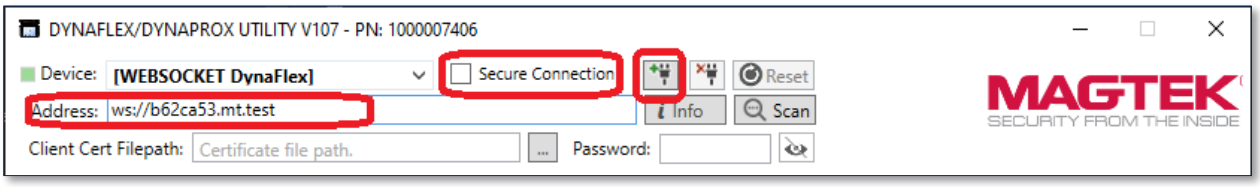
2.3 How to Connect Using the WLAN Connection

Before connecting to WebSocket, please make sure the PC has all the root, and sub CA certificates and the client private key certificate associated with the DynaFlex II PED device installed. Please refer to document ***D998200550 DynaFlex II PED Using Wireless LAN Guide*** for more detail instructions. To connect via Web Socket, follow these steps.

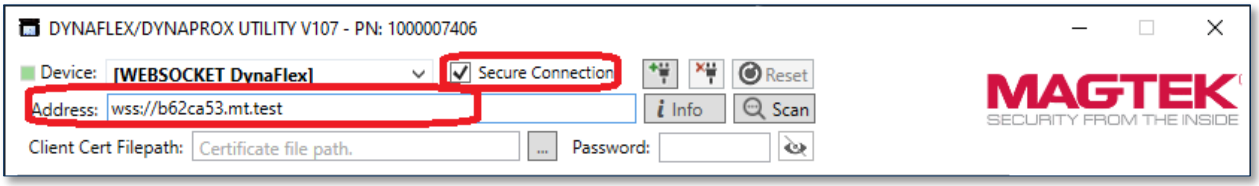
1) Launch the DynaFlex Utility and under the **Device** list select the **[WEBSOCKET DynaFlex]** tor **[WEBSOCKET_Trust DynaFlex]**.



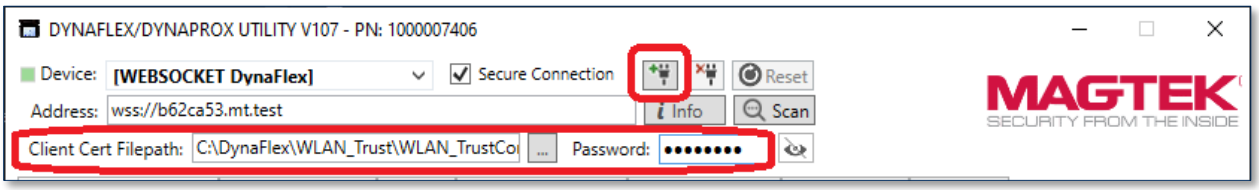
2) For non TLS connection, uncheck **Secure Connection**, enter the WebSocket address **`ws://xxxxxxxxx`**, and then press the green **Connect** button.



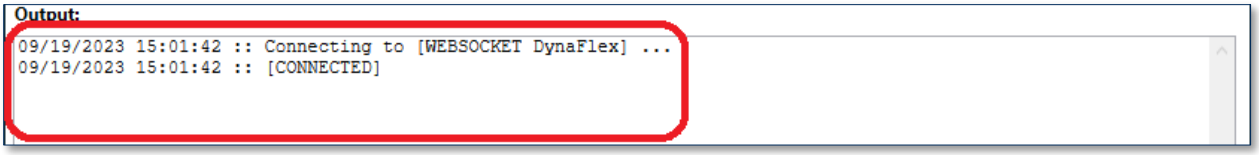
3) For TLS connection, check **Secure Connection**, enter the WebSocket address **`wss://xxxxxxxx`**



4) Browse to the client private key certificate, enter the certificate password, and press the green **Connect** button.



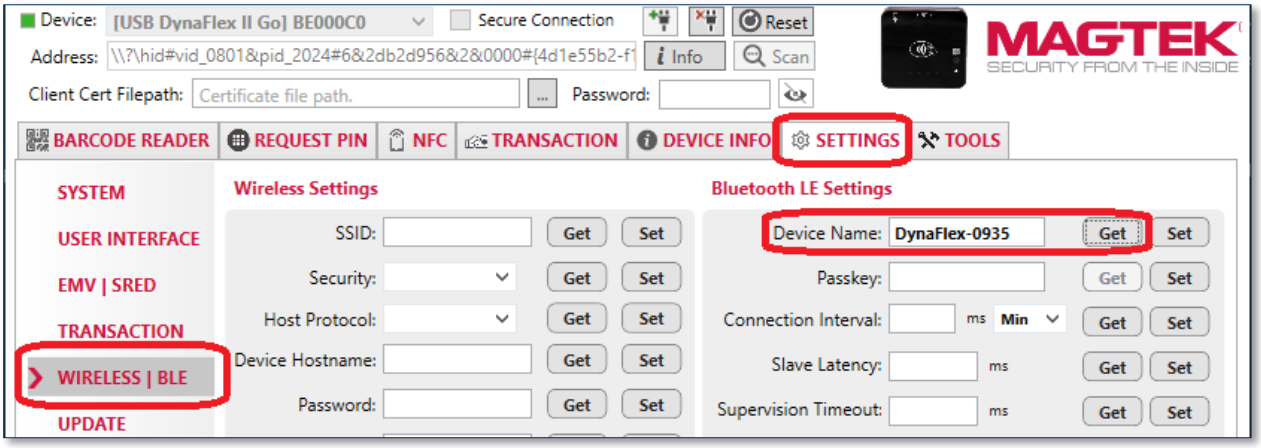
5) The **Output** log will the show the device status as connected as shown below.



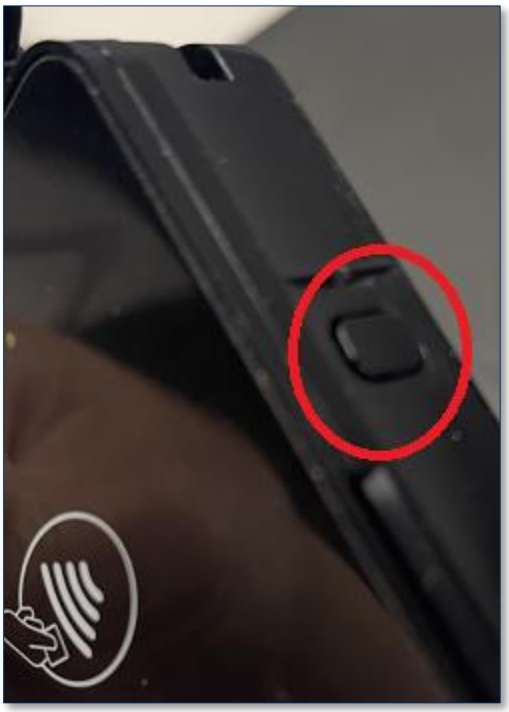
2.4 How to Connect Using the Bluetooth LE Connection

The following instructions are for pairing the DynaFlex II GO to a PC.

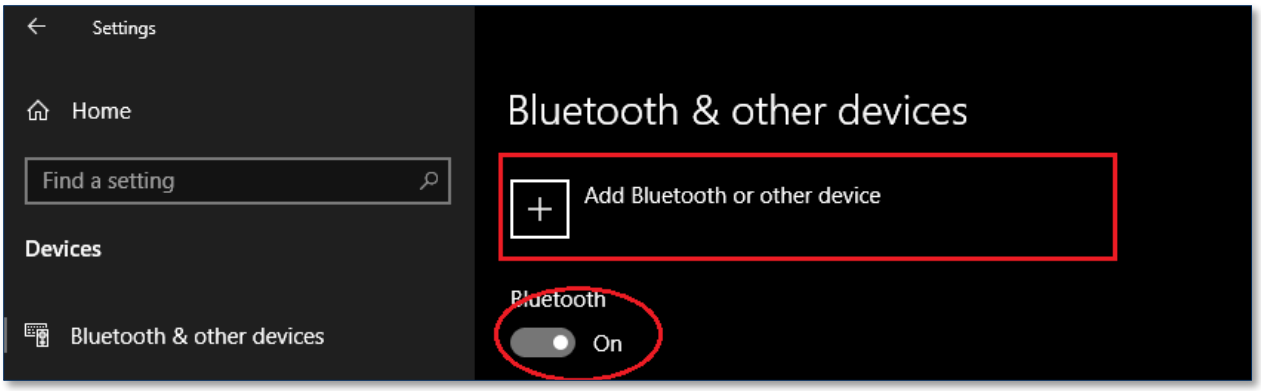
1) Launch the DynaFlex Utility to connect to the device by USB connection. Obtain Bluetooth LE Device name from selectin the **Settings** tab, **WIRELESS / BLE** menu, and at **Bluetooth LE Settings** press the **Get** button for Device Name.



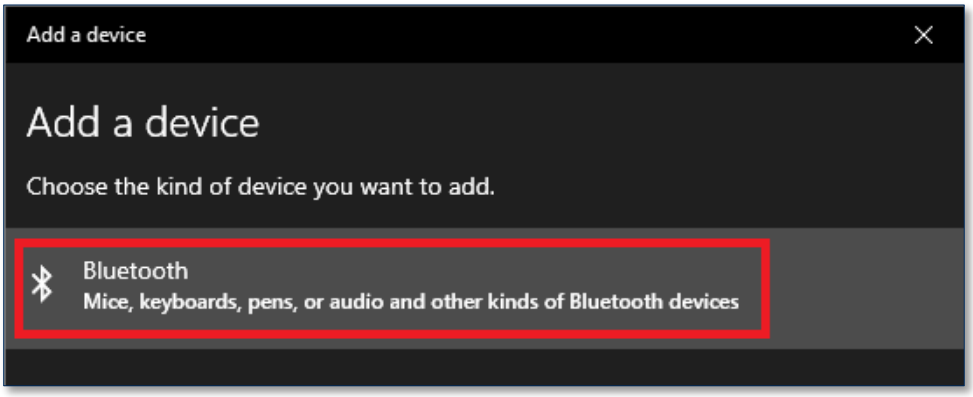
2) Place the device into Pairing Mode by pressing and holding the power button on device until 4 beeps and release the button. The 4th LED will blink green.



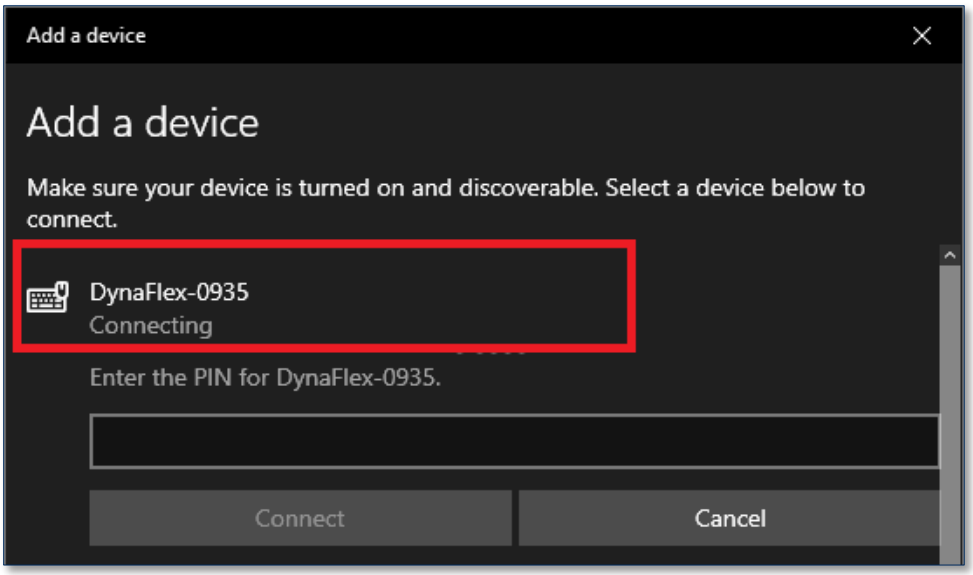
3) On the PC, open **Settings** and choose **Bluetooth & other devices**. Make sure the "Bluetooth" is turned **ON**. On the right panel, choose **Add Bluetooth or other device**.



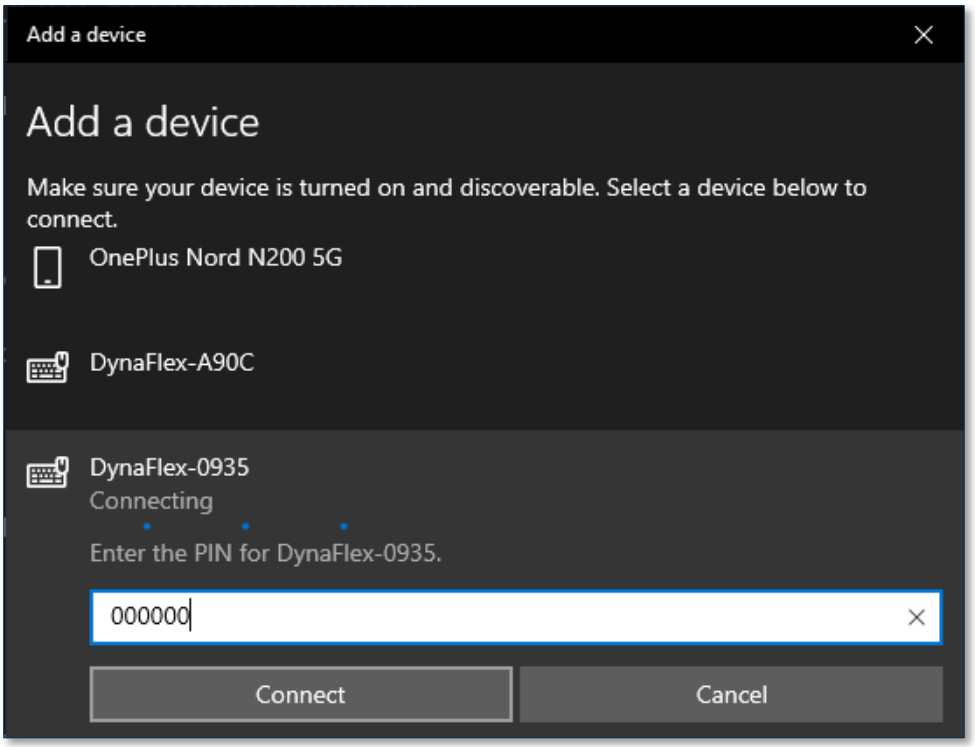
4) At the **Add a device** window, select **Bluetooth**.

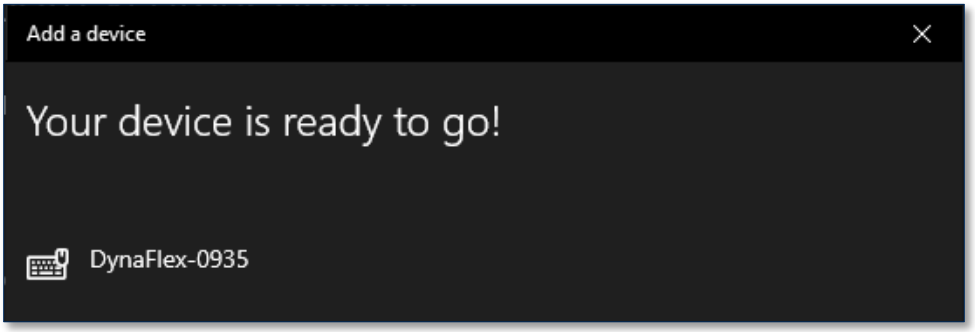


5) To pair, click on the device name that was been retrieved from DynaFlex Utility.

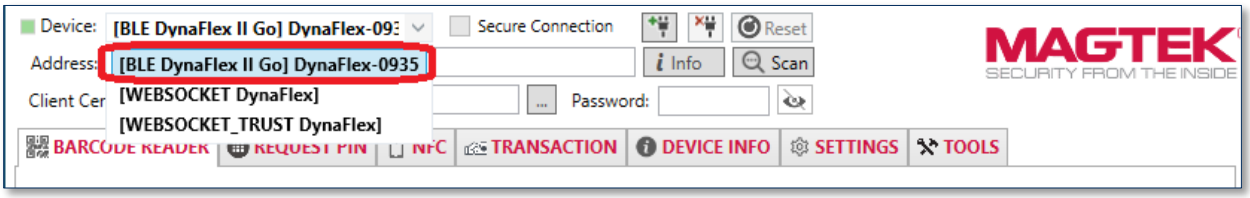


6) Enter the PIN, ("000000" by default), and press **Connect**.





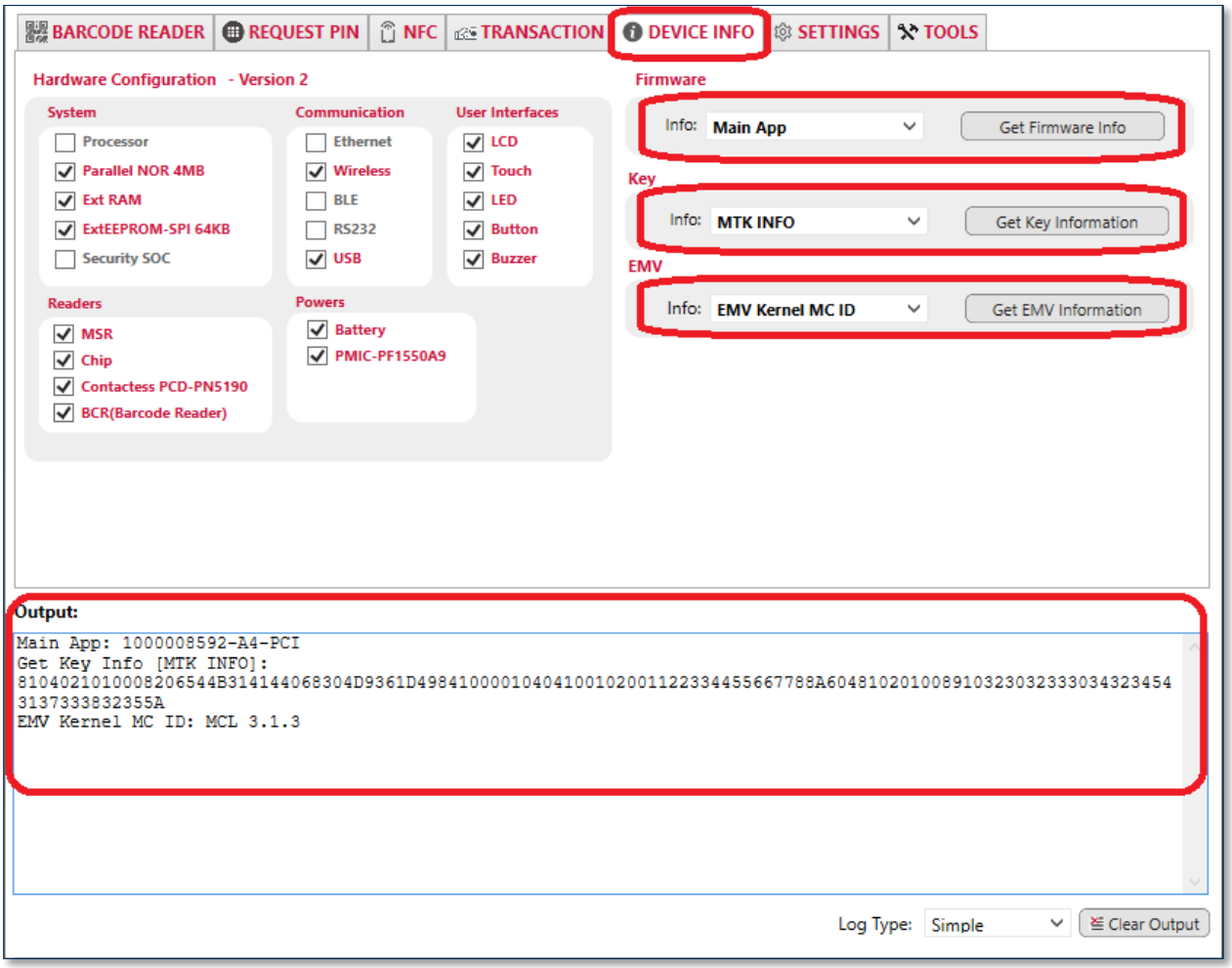
7) Go back to DynaFlex Utility, disconnect the current USB connection.
8) Click on **Device** list to find the added BLE device similar as below.



3 How to Use Device Information

To get the device information follow these steps.

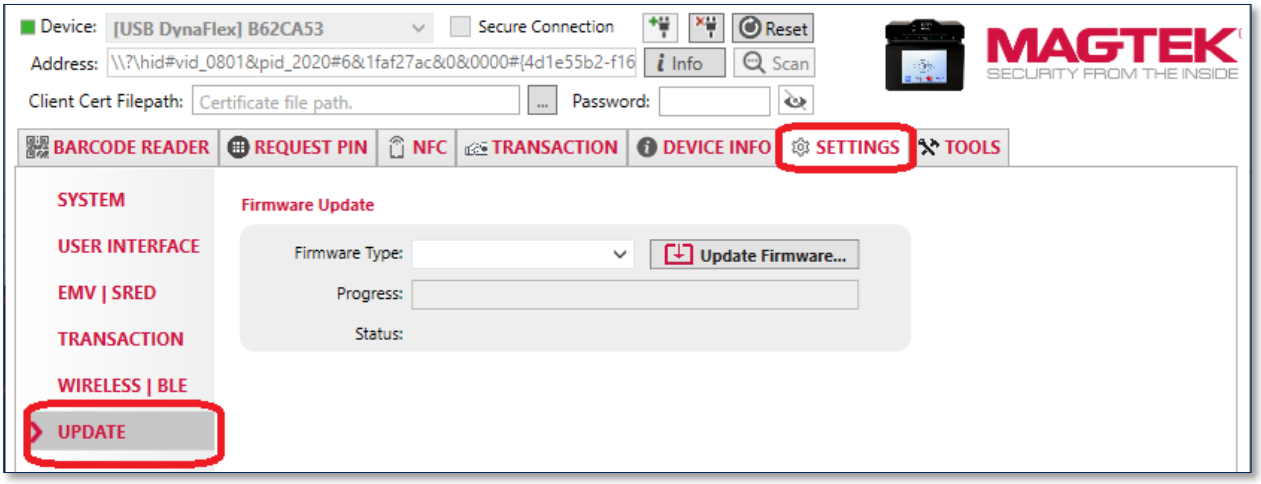
1) Select the **Device INFO** tab, select the desired information to see from the device, and then press the **Get…Information** buttons. The result will be shown similar as below.



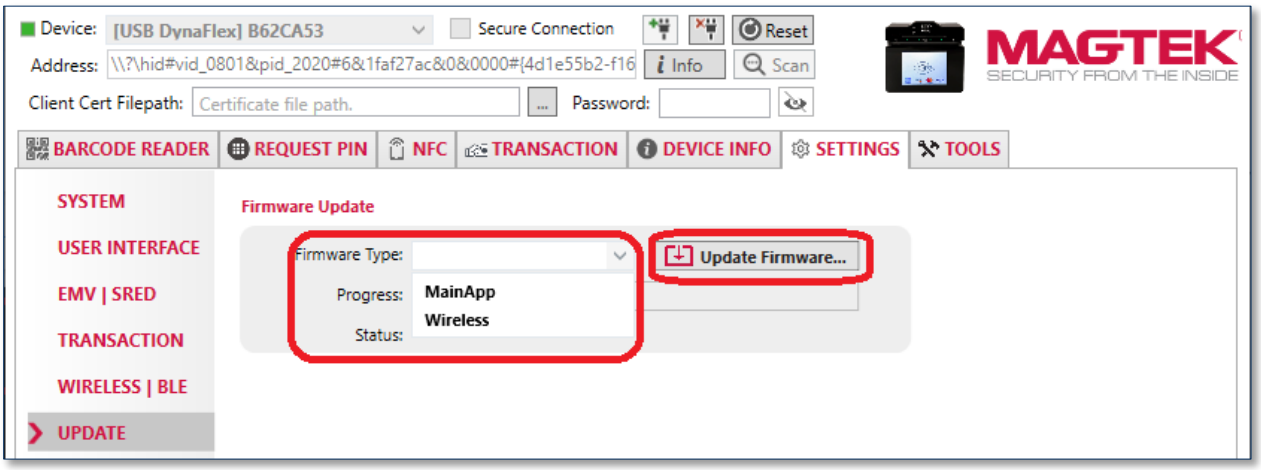
4 How to Update Firmware

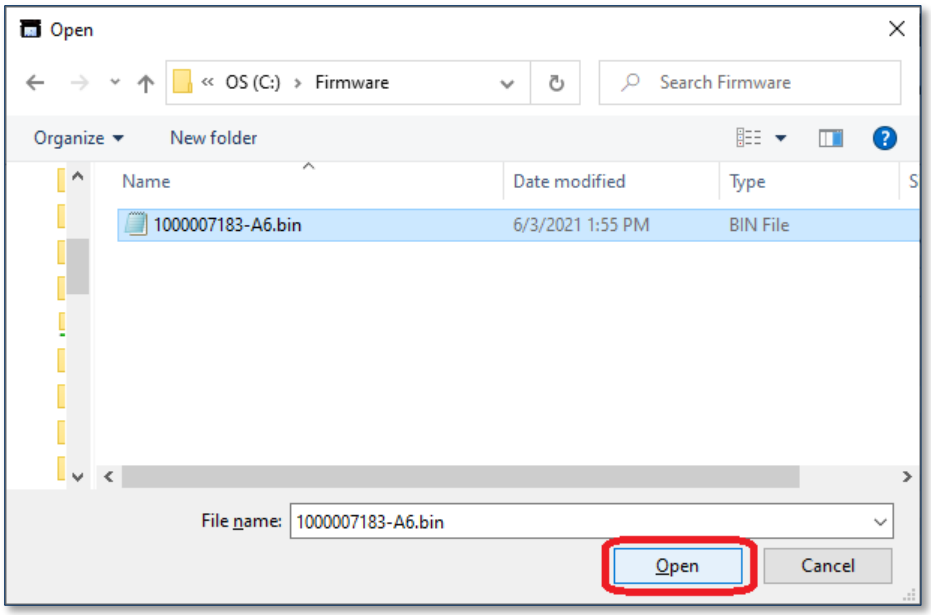
To update firmware, follow these steps.

1) Press the **Settings** tab, and then select the **Update** menu.



2) Select the **Firmware Type**, press the **Update Firmware…** button, select the firmware file, and press the **Open** button.





3) Check the status displayed in the software.

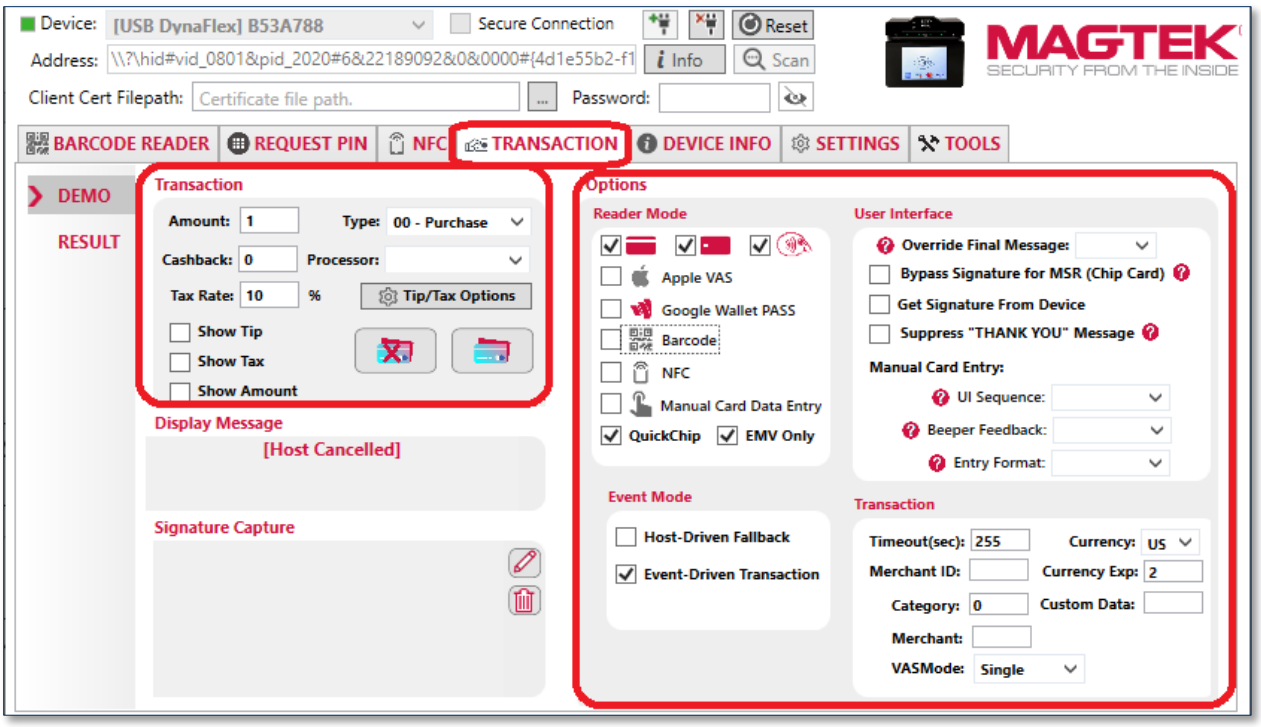
5 How to Use the Transaction Demo

The following instructions detail how to perform EMV transactions using USB. However, the steps are essentially the same for all connection types.

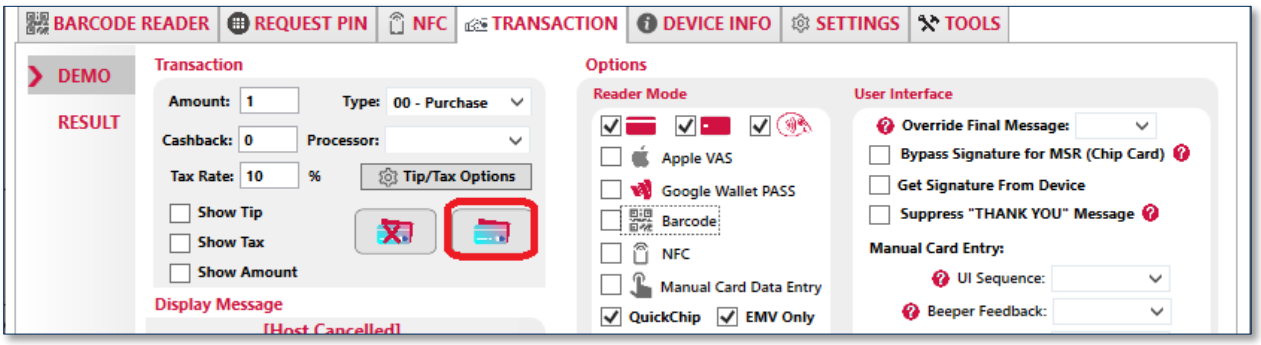
5.1 EMV Transaction

To perform an EMV transaction, follow these steps.

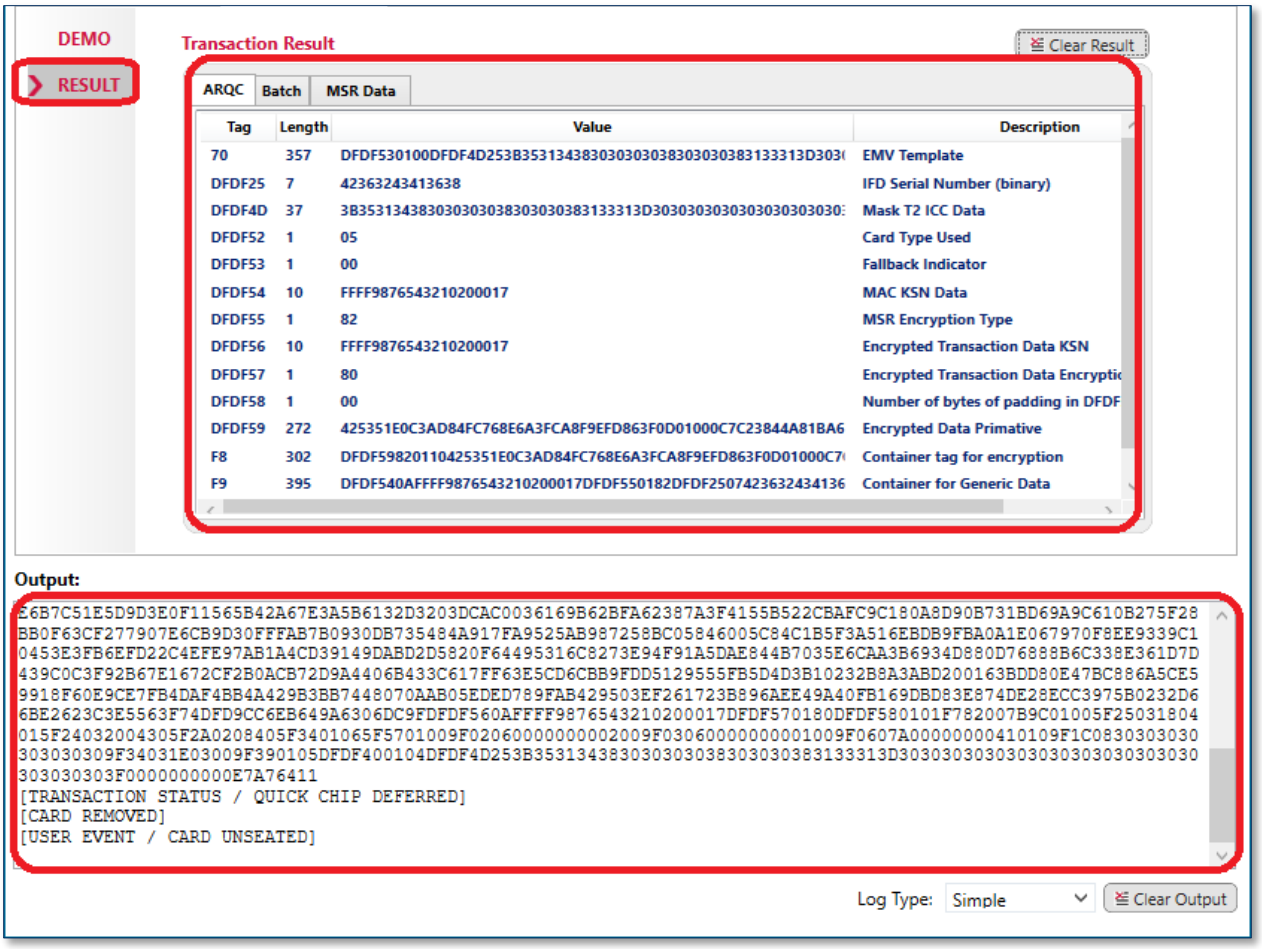
1) Select the **Transaction** tab, select the **DEMO** menu, and then select the desired **Transaction Type**, **Reader Mode**, and **Transaction Options**.



2) Press the **Start EMV Transaction** button to begin the transaction.



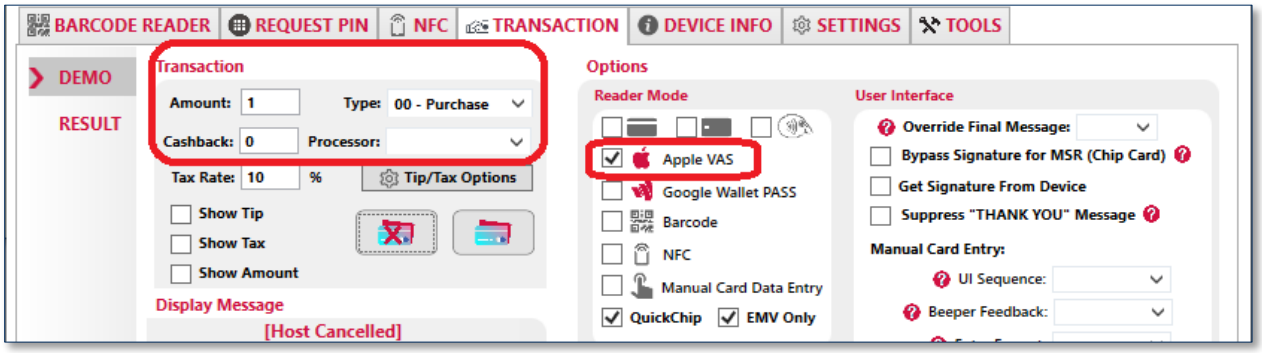
3) Present the payment method to the device.
4) Follow any instructions on the device for application or language selection.
5) To view the transaction result after the transaction is completed, press **RESULT** menu. Parsed details can be seen in the **ARQC**, **Batch**, and **MSR** tabs. The status is displayed in the **Output** log.


DEMO
RESULT
Transaction Result
Clear Result
ARQC
Batch
MSR Data
Tag
Length
Value
Description
70 357 DFDF530100DFDF4D253B3531343830303030383030303831333133D303(EMV Template
DFDF25 7 42363243413638 IFD Serial Number (binary)
DFDF4D 37 3B3531343830303030383030303831333133D3030303030303030303030: Mask T2 ICC Data
DFDF52 1 05 Card Type Used
DFDF53 1 00 Fallback Indicator
DFDF54 10 FFFF9876543210200017 MAC KSN Data
DFDF55 1 82 MSR Encryption Type
DFDF56 10 FFFF9876543210200017 Encrypted Transaction Data KSN
DFDF57 1 80 Encrypted Transaction Data Encryptic
DFDF58 1 00 Number of bytes of padding in DFDF
DFDF59 272 425351E0C3AD84FC768E6A3FCA8F9EFD863F0D01000C7C23844A81BA6 Encrypted Data Primative
F8 302 DFDF59820110425351E0C3AD84FC768E6A3FCA8F9EFD863F0D01000C7(Container tag for encryption
F9 395 DFDF540AFFFF9876543210200017DFDF550182DFDF2507423632434136 Container for Generic Data
Output:
E6B7C51E5D9D3E0F11565B42A67E3A5B6132D3203DCAC0036169B62BFA62387A3F4155B522CBAFC9C180A8D90B731BD69A9C610B275F28
BB0F63CF277907E6CB9D30FFFAB7B0930DB735484A917FA9525AB987258BC05846005C84C1B5F3A516EBDB9FBA0A1E067970F8EE9339C1
0453E3FB6EFD22C4EFE97AB1A4CD39149DABD2D5820F64495316C8273E94F91A5DAE844B7035E6CAA3B6934D880D76888B6C338E361D7D
439C0C3F92B67E1672CF2B0ACB72D9A4406B433C617FF63E5CD6CBB9FDD5129555FB5D4D3B10232B8A3ABD200163BDD80E47BC886A5CE5
9918F60E9CE7FB4DAF4BB4A429B3BB7448070AAB05EDED789FAB429503EF261723B896AEE49A40FB169DBD83E874DE28ECC3975B0232D6
6BE2623C3E5563F74DFD9CC6EB649A6306DC9FDFDF560AFFFF9876543210200017DFDF570180DFDF580101F782007B9C01005F25031804
015F24032004305F2A0208405F3401065F5701009F02060000000002009F0306000000000001009F0607A00000000410109F1C0830303030
303030309F34031E03009F390105DFDF400104DFDF4D253B3531343830303030383030303831333133D3030303030303030303030303030
303030303F0000000000E7A76411
[TRANSACTION STATUS / QUICK CHIP DEFERRED]
[CARD REMOVED]
[USER EVENT / CARD UNSEATED]
Log Type:
Simple
Clear Output

5.2 Apple VAS Transaction

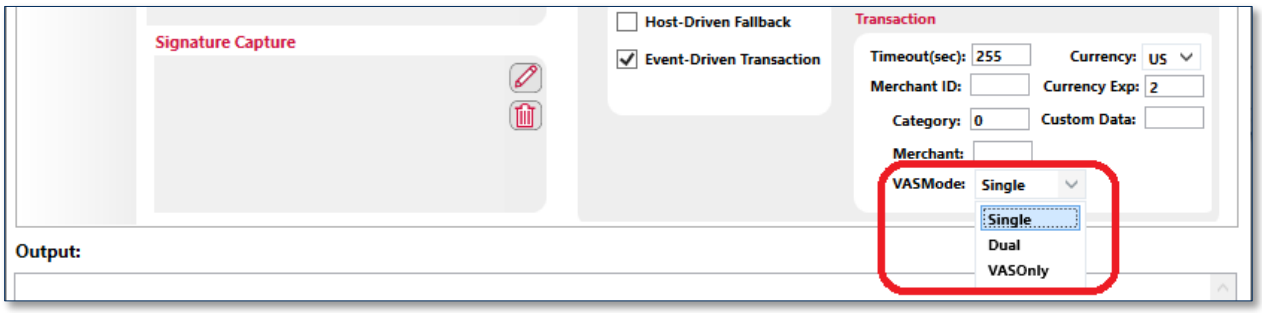
To perform an Apple VAS (value-added service) supported transaction, follow these steps.

1) Select the **DEMO** menu, select the desired **Transaction Type**, and then select the **Apple VAS** option.

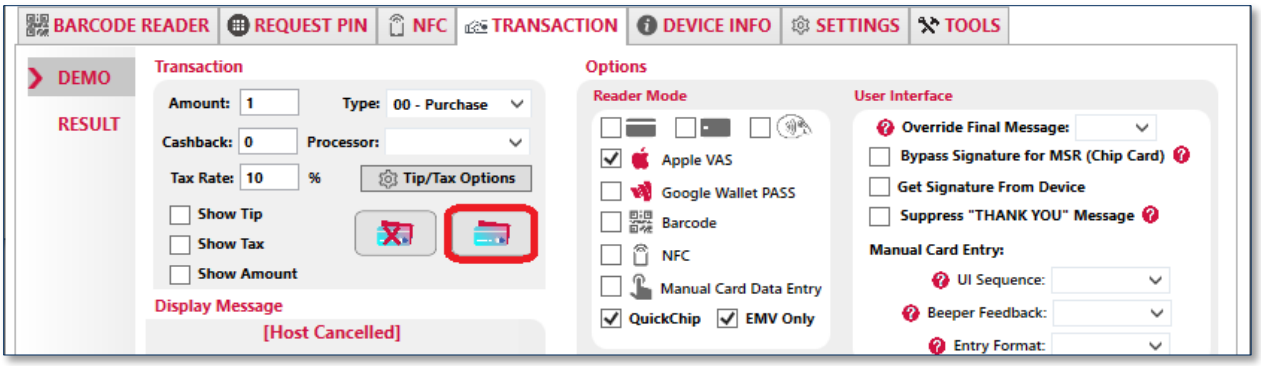


2) Select a VAS mode from the **VASMode** list.

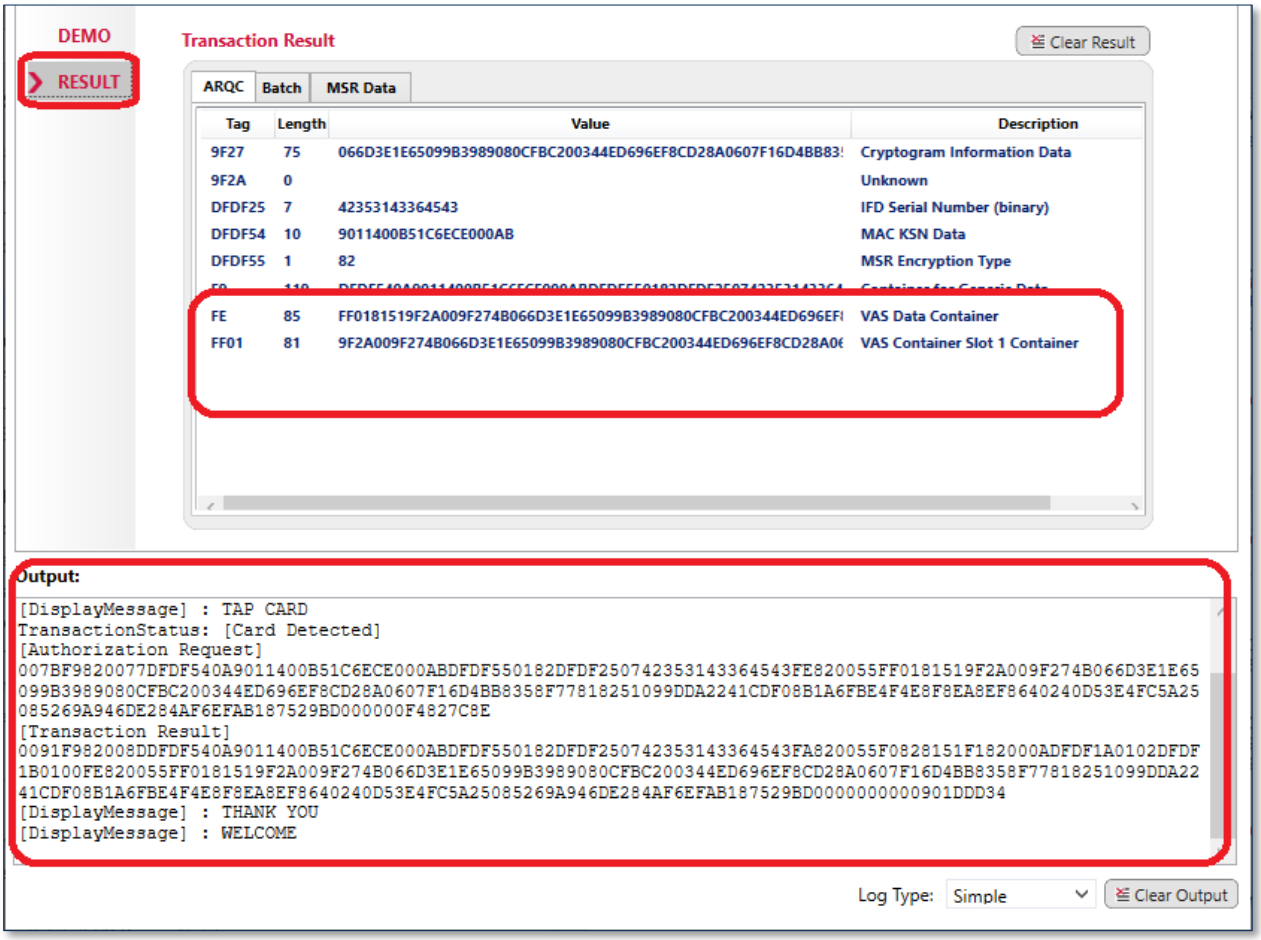
- **Single Mode**
  The device reads only VAS data from a tapped smartphone or reads EMV payment data from a tapped card. When the device sends ARQC to conclude the transaction, it only includes either EMV payment data in container FC for cards, or includes VAS data in FE container for smartphones.
- **Dual Mode**
  The device reads both VAS data and EMV payment data from a tapped smartphone or reads EMV payment data from a tapped card. When device sends ARQC to the host to conclude the transaction, it includes EMV payment data in container FC and includes VAS data, if available, in container FE.
- **VASOnly Mode**
  The device reads only VAS data from a tapped smartphone and does not read data from a tapped card. If the tapped smartphone does not support VAS, the device does not detect or read from the smartphone. When the device send ARQC to conclude the transaction, it includes VAS data in container FE and does not include EMV payment data in container FC.



3) Press the **Start EMV Transaction** button to start the transaction.



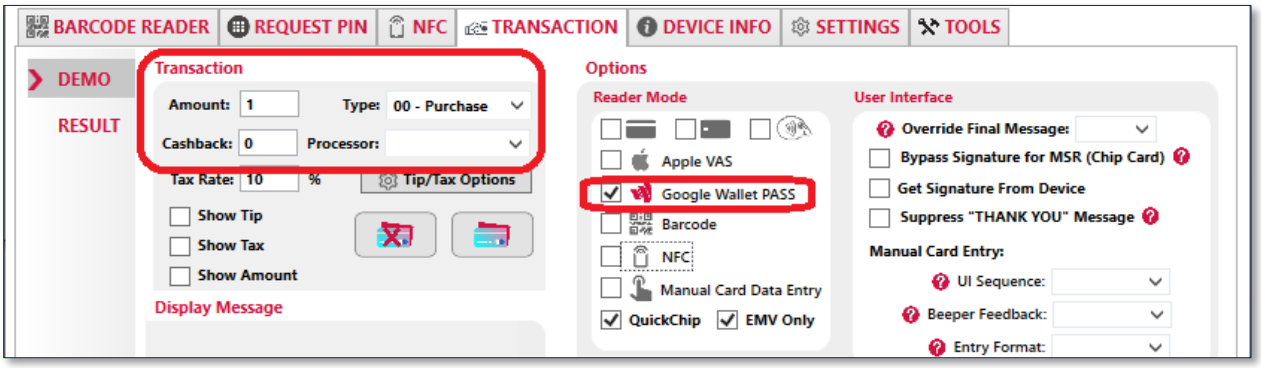
4) Present the payment device near the reader to continue the contactless transaction.
5) To view the transaction result after the transaction is completed, press **RESULT** menu. Parsed details can be seen in the **ARQC** tab, which shows details of the FE TLV object containing the Apple VAS data. The status is displayed in the **Output** log.



5.3 Google Wallet VAS Transaction

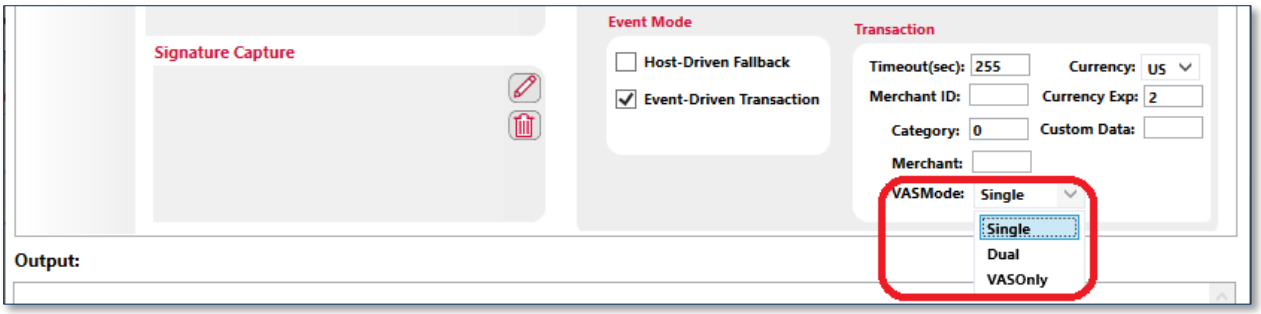
To perform a Google Wallet VAS (value-added service) supported transaction, follow these steps.

1) Select the **DEMO** menu, select the desired **Transaction Type**, and then select the **Google Wallet PASS** option.

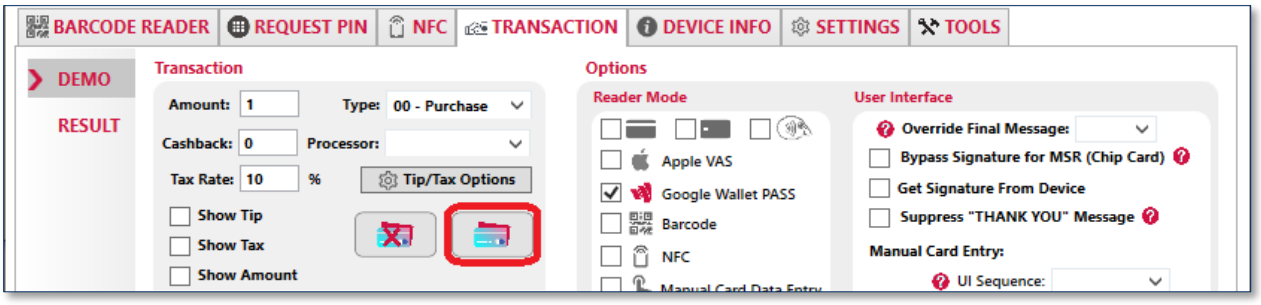


2) Select a VAS mode from the **VASMode** list.

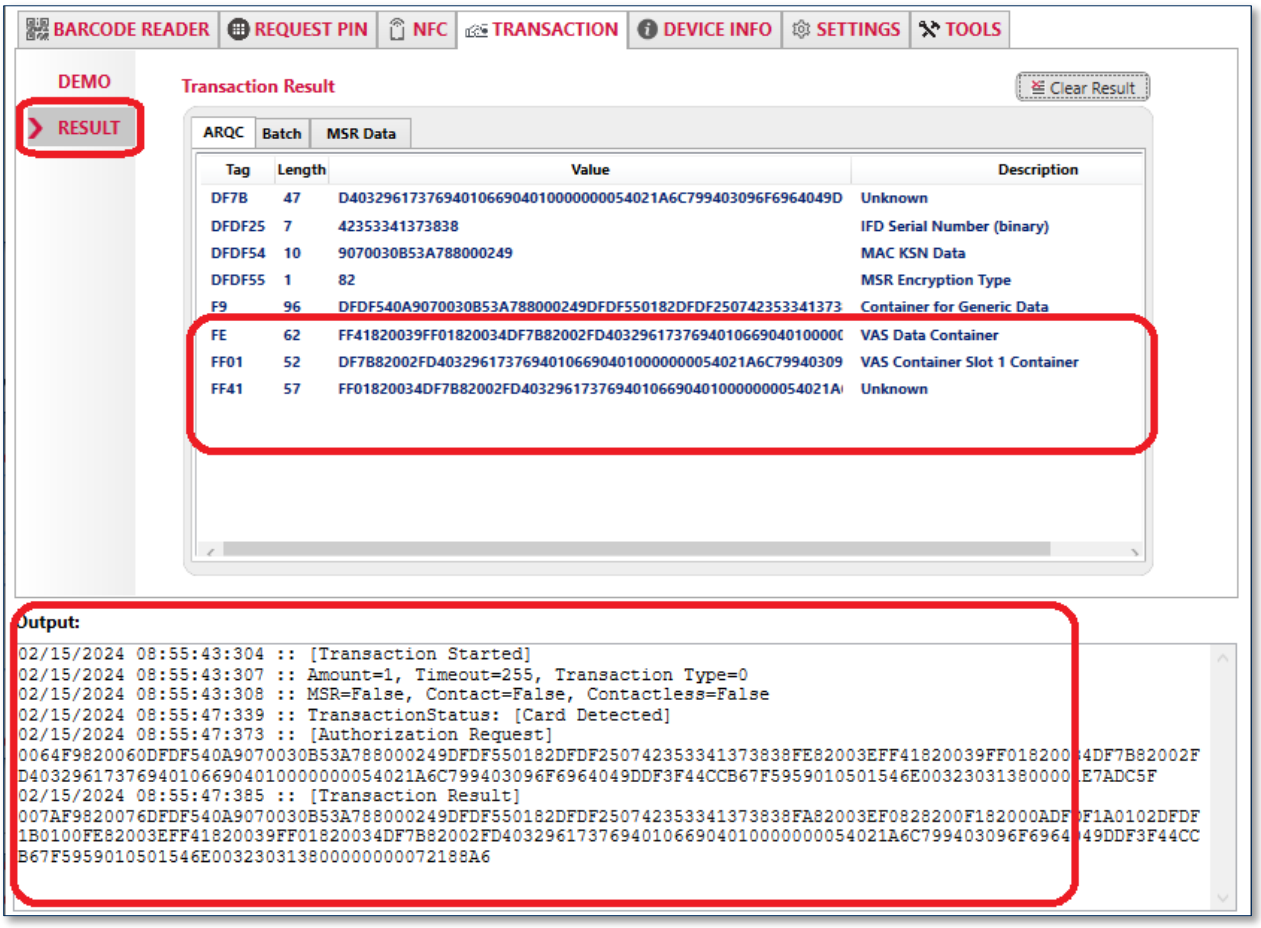
- **Single Mode**
  The device reads only VAS data from a tapped smartphone or reads EMV payment data from a tapped card. When the device sends ARQC to conclude the transaction, it only includes either EMV payment data in container FC for cards, or includes VAS data in FE container for smartphones.
- **Dual Mode**
  The device reads both VAS data and EMV payment data from a tapped smartphone or reads EMV payment data from a tapped card. When device sends ARQC to the host to conclude the transaction, it includes EMV payment data in container FC and includes VAS data, if available, in container FE.
- **VASOnly Mode**
  The device reads only VAS data from a tapped smartphone and does not read data from a tapped card. If the tapped smartphone does not support VAS, the device does not detect or read from the smartphone. When the device send ARQC to conclude the transaction, it includes VAS data in container FE and does not include EMV payment data in container FC.



3) Press the **Start EMV Transaction** button to start the transaction.



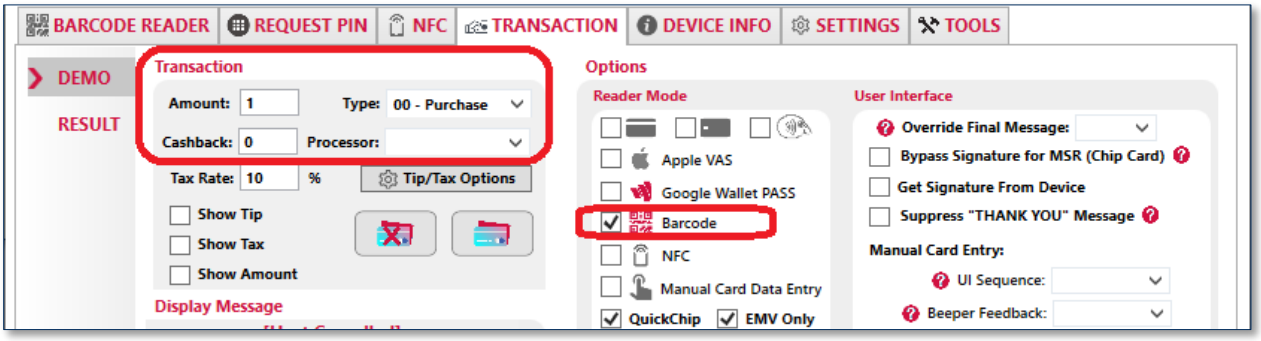
4) Present the payment device with Google Wallet near the reader to continue the contactless transaction.
5) To view the transaction result after the transaction is completed, press **RESULT** menu. Parsed details can be seen in the **ARQC** tab, which shows details of the FE TLV object containing the Google Wallet VAS data. The status is displayed in the **Output** log.



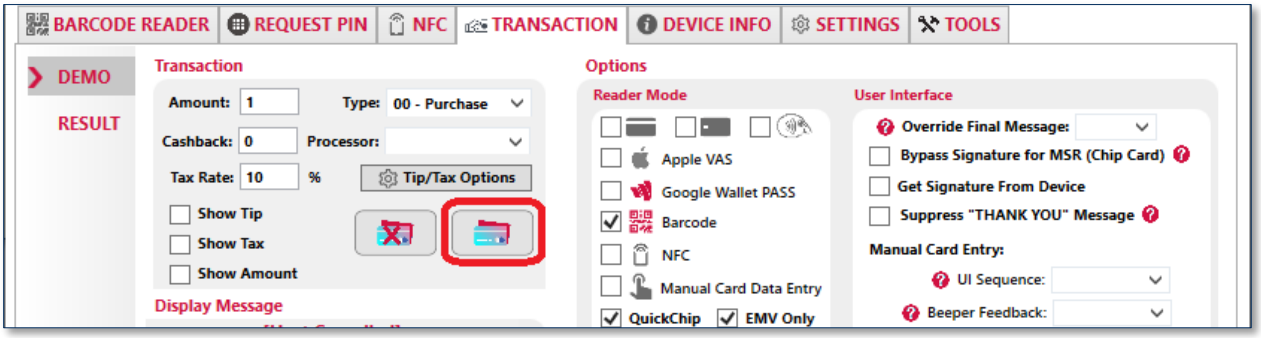
5.4 Barcode Transaction

To perform a Barcode transaction, follow these steps.

1) Locate a barcode that can be accessible by the device such as a mobile app, screen, or print out.
2) Select the **DEMO** menu, select the desired **Transaction Type**, and then select the **Barcode Reader** option.

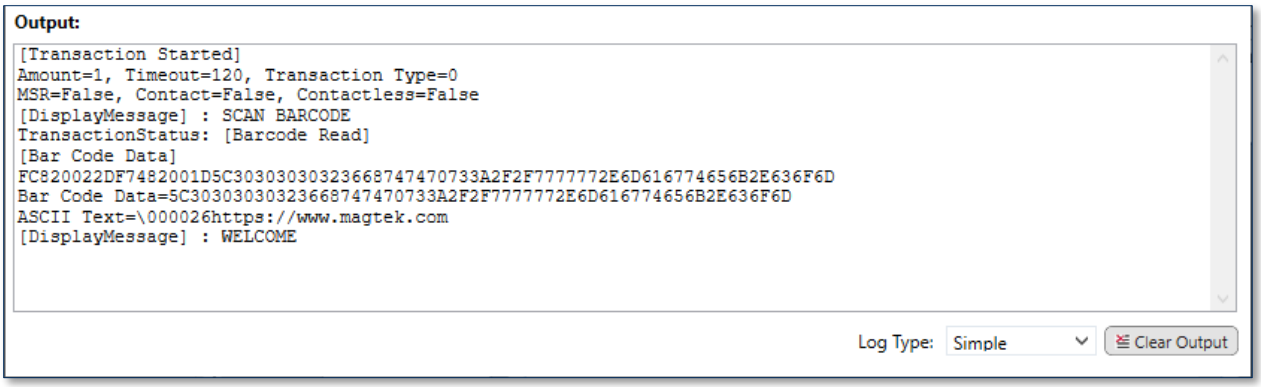


3) Press the **Start EMV Transaction** button to begin the transaction.



4) The BCR LED will turn on. Present a barcode near the device's BCR, which is located at the top center of the device.
5) The BCR LED will turn off after the BCR scan is complete.

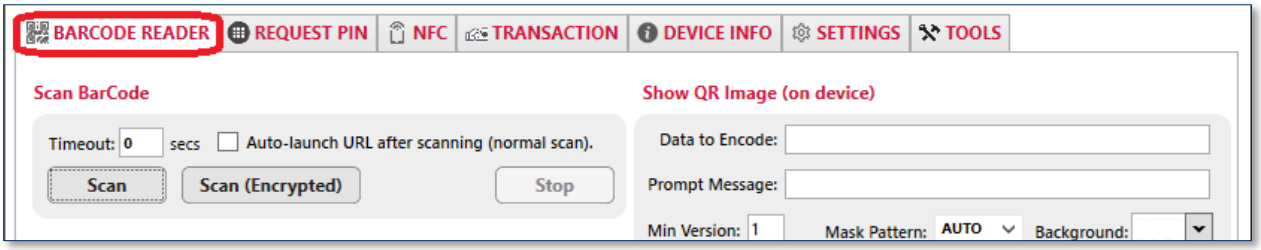
   Note, if the LED flickers but remains on, the scan was not complete. Slowly center the barcode. If centered, slowly move the barcode away from the device. The larger the barcode size, the further away it should be.
6) Barcode data will be shown in the Output section.



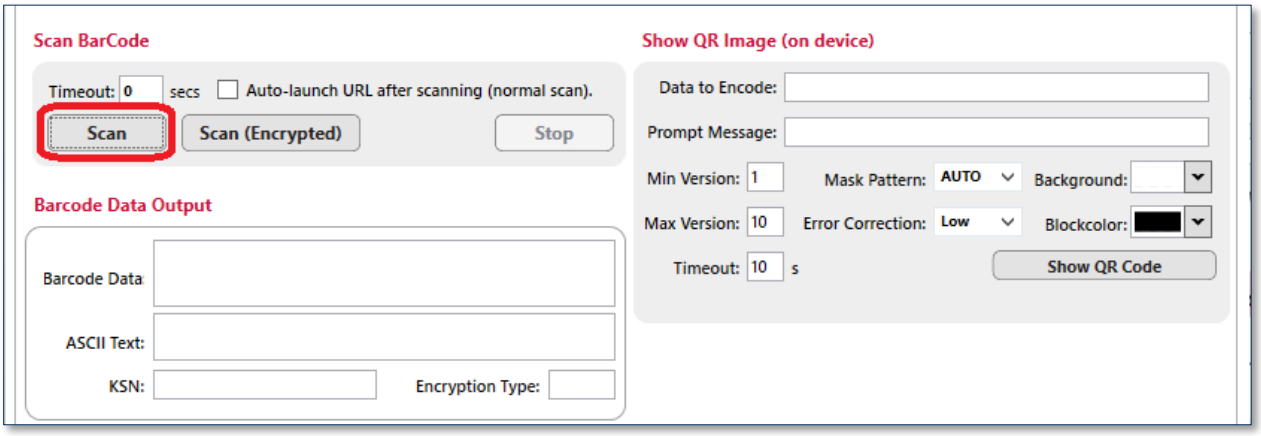
6 How to use the Barcode Reader

6.1 Barcode Returned Unencrypted

1) Select the **BARCODE READER** tab.

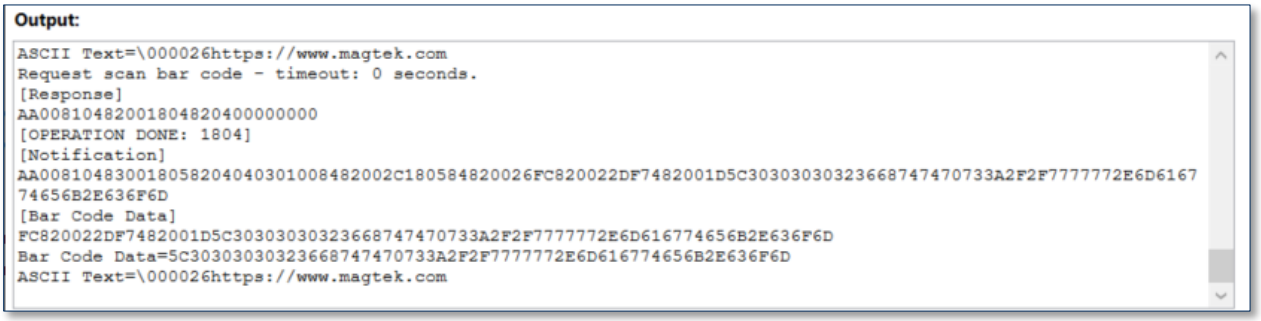


2) Locate a barcode that can be accessible by the device such as a mobile app, screen, or print out.
3) At **Scan BarCode**, press the **Scan** button to begin scanning a barcode.



4) The BCR LED will turn on. Present a barcode near the device's BCR, which is located at the top center of the device.
5) The BCR LED will turn off after the BCR scan is complete.

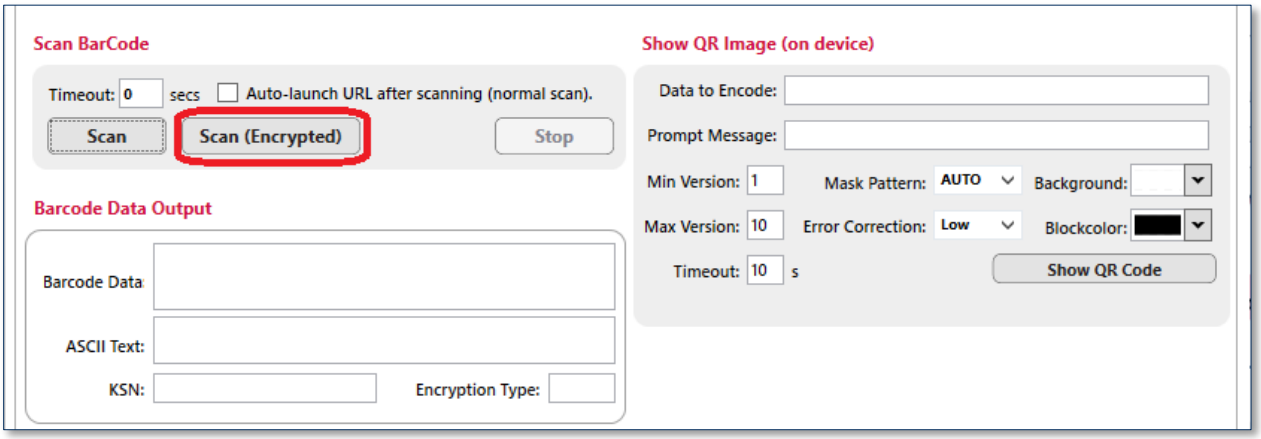
   Note, if the LED flickers but remains on, the scan was not complete. Slowly center the barcode. If centered, slowly move the barcode away from the device. The larger the barcode size, the further away it should be.
6) Barcode data will be shown in the Output section.



6.2 Barcode Returned Encrypted

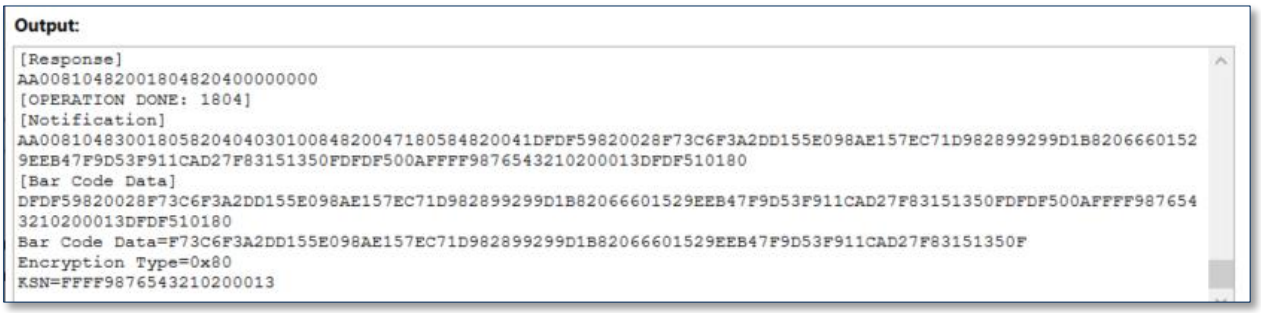
To return the barcode data as encrypted, follow these steps.

1) Locate a barcode that can be accessible by the device such as a mobile app, screen, or print out.
2) At **Scan BarCode**, press the **Scan (Encrypted)** button to begin scanning a barcode.



3) The BCR LED will turn on. Present a barcode near the device's BCR, which is located at the top center of the device.
4) The BCR LED will turn off after the BCR scan is complete.

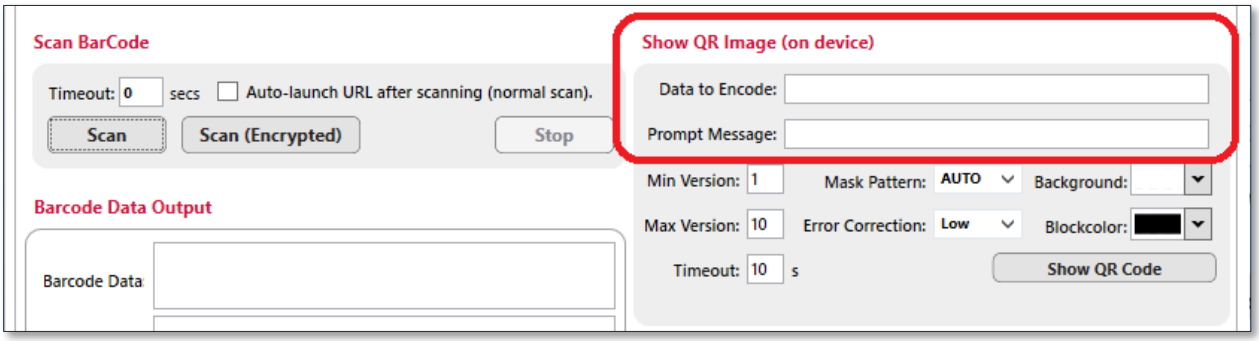
   Note, if the LED flickers but remains on, the scan was not complete. Slowly center the barcode. If centered, slowly move the barcode away from the device. The larger the barcode size, the further away it should be.
5) Encrypted Barcode data will be shown in the Output section.



6.3 Show QR Image

To display a QR code on the device's screen, follow these steps.

1) At **Show QR Image**, enter the data to encode into a QR code. Optionally, enter a prompt.



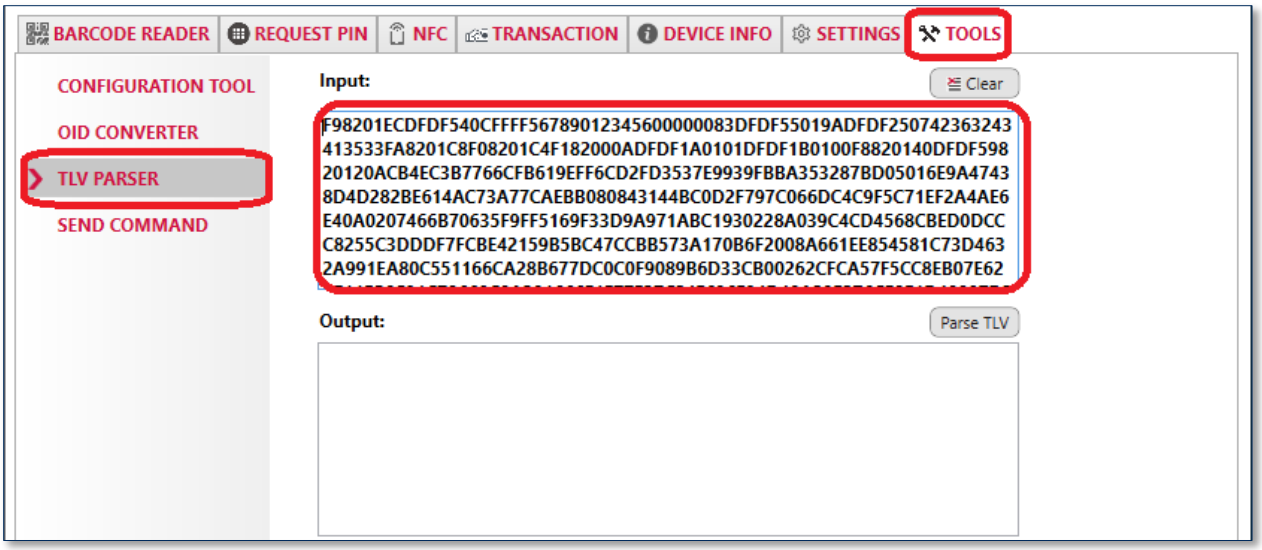
2) Below are example QR code images displayed without a prompt and with a prompt of "MagTek".

7 How to Parse Custom TLV Blobs

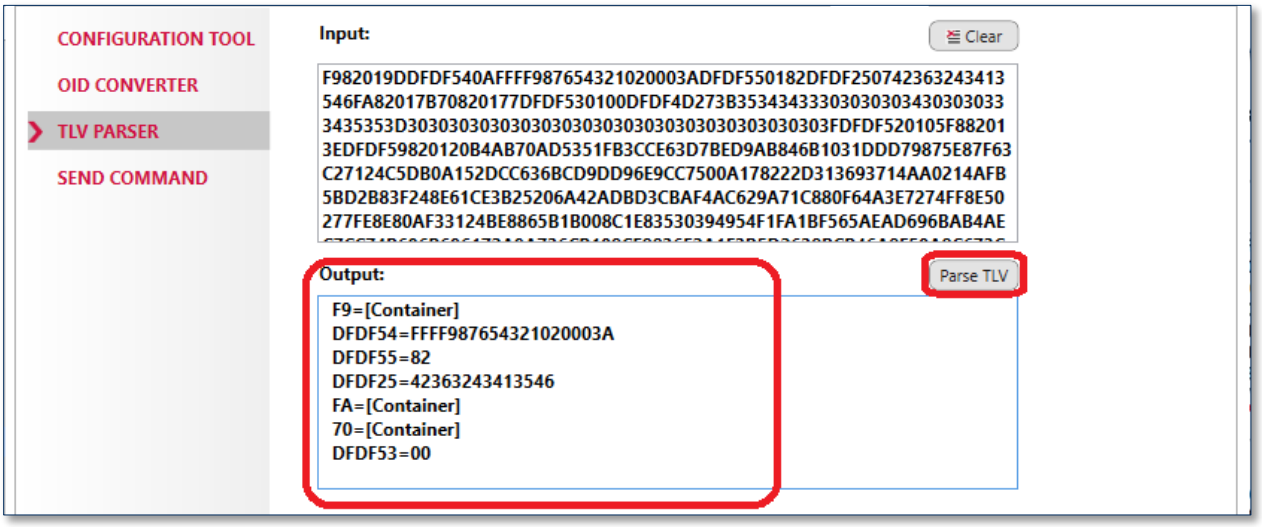
To parse a custom TLV blob, follow these steps.

1) Select the **TOOLS** tab, select the **TLV PARSER** menu, then copy and paste the TLV to be parsed into the **Input** text box.

   Any header bytes representing the size of the TLV object will need to be removed before parsing. In this example shown, the first 2 bytes of the ARQC was removed from the input.



2) Press the **Parse TLV** button to see the parsed result in the **Output** section.

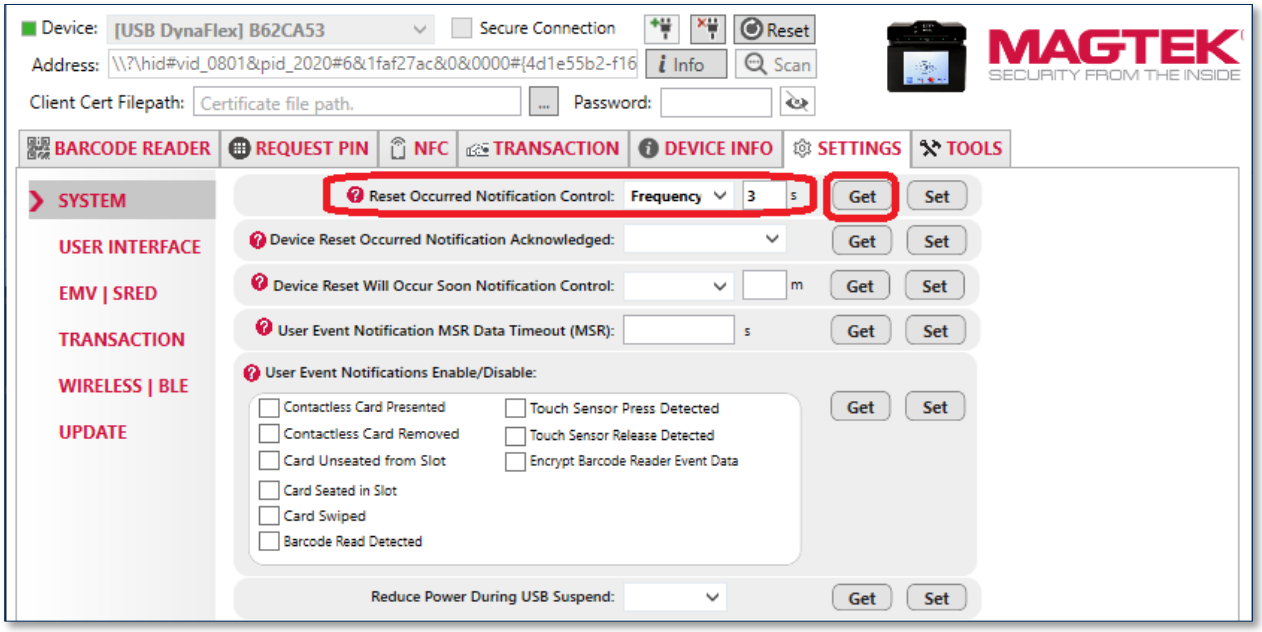


8 How to use Configurations

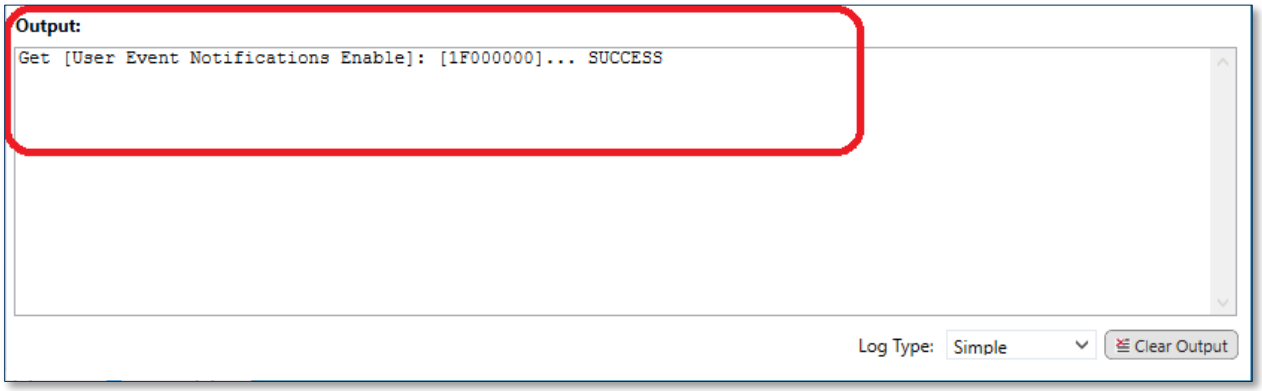
8.1 Get Configuration settings

To read a desired configuration from the device, follow these steps.

1) Select the **SETTINGS** tab, select either one of the **SYSTEM**, **USER INTERFACE**, **EMV**, or **TRANSACTION** menus, select a configuration to read from the device, and then press the **Get** button.



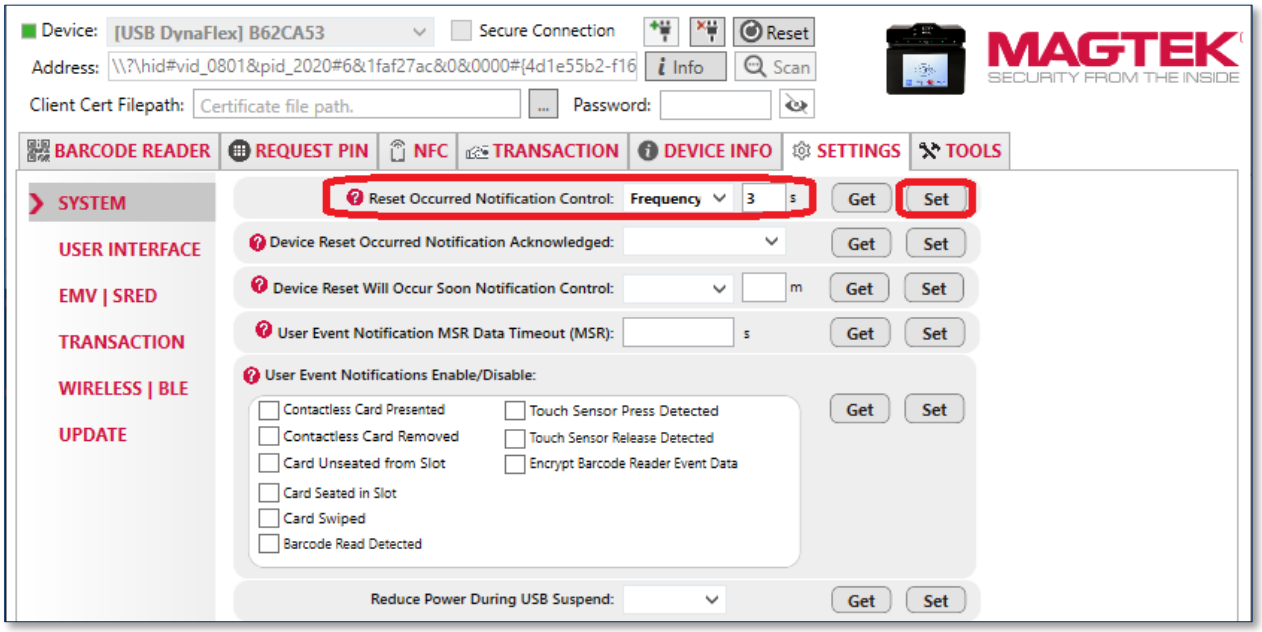
2) Observe the result next to the configuration and in the **Output** log.



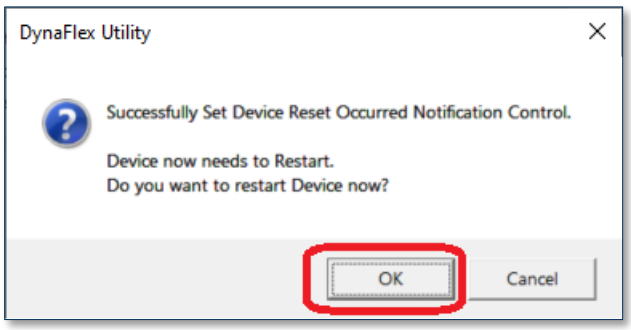
8.2 Configure System settings

To change the device notification settings, follow these steps.

1) Select the **SYSTEM** menu, then select an option in the notification to set for the device, and then press the **Set** button. For more information about the meaning of these settings, see D998200383 DynaFlex Family Programmer's Manual (COMMANDS).



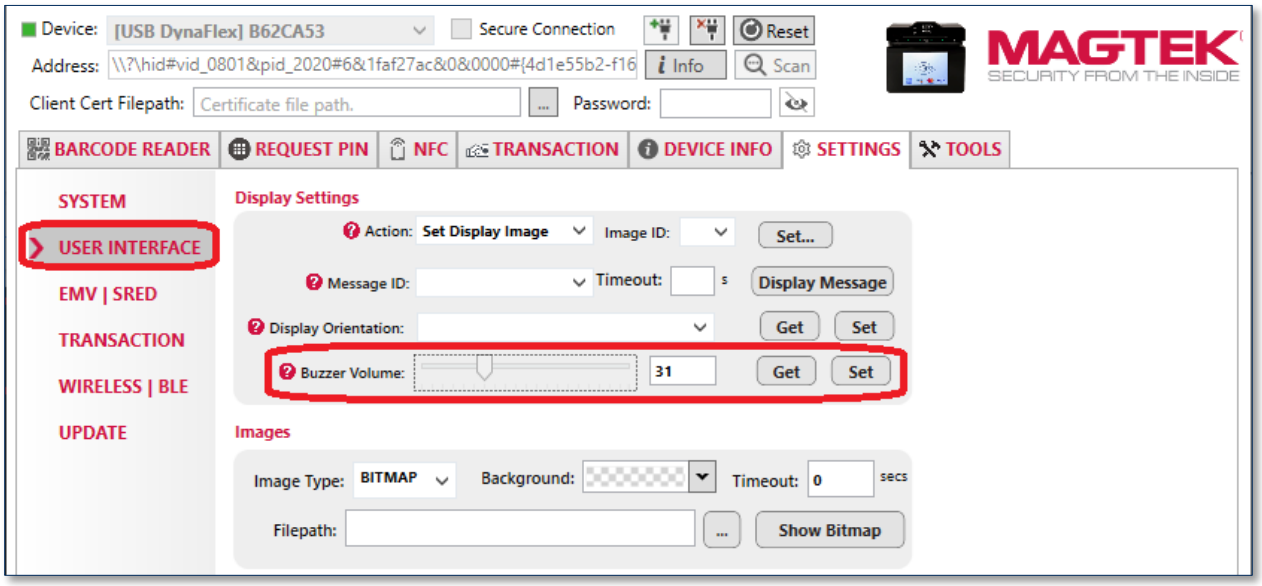
2) Press OK to reset the device when prompted.



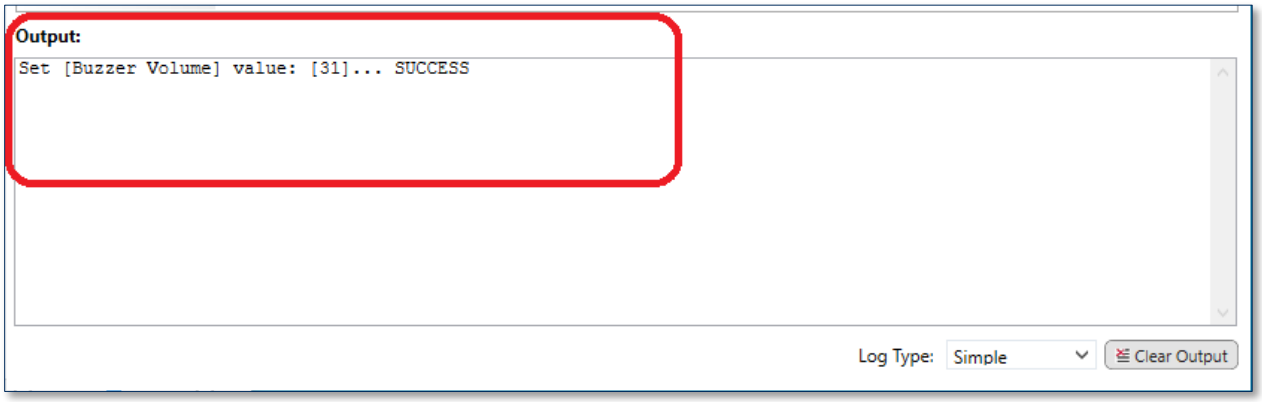
8.3 Configure Buzzer Volume

To configure the buzzer volume during the EMV transaction, follow these steps:

1) Select the **USER INTERFACE** menu. Move the Buzzer Volume setting to desired volume from 1-100, and then press the **Set** button.



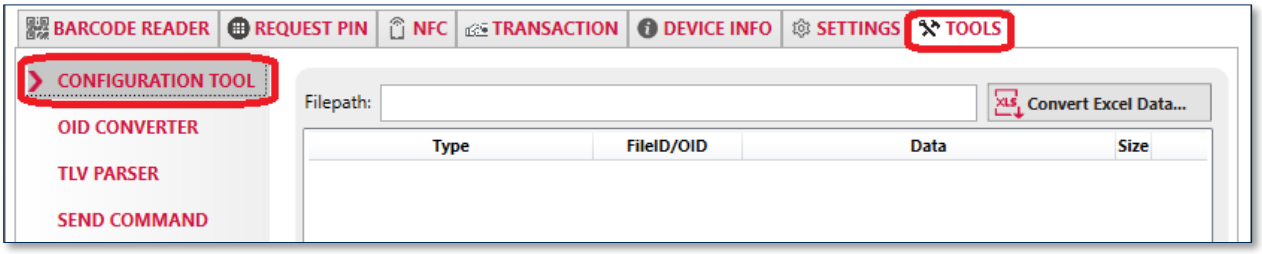
2) Confirm the change in the **Output** section.



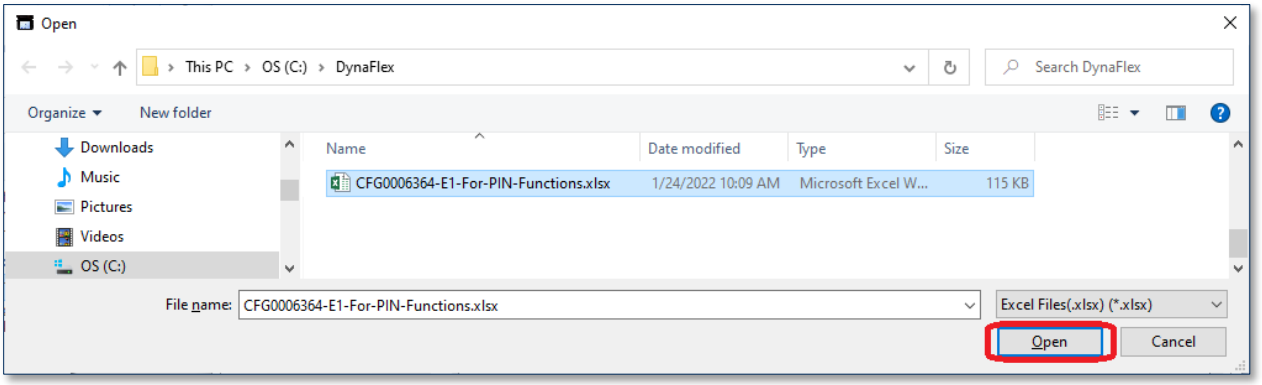
8.4 Send Selective Configuration

To convert an excel configuration file to .bin file and send to the device or save to local drive, follow these steps.

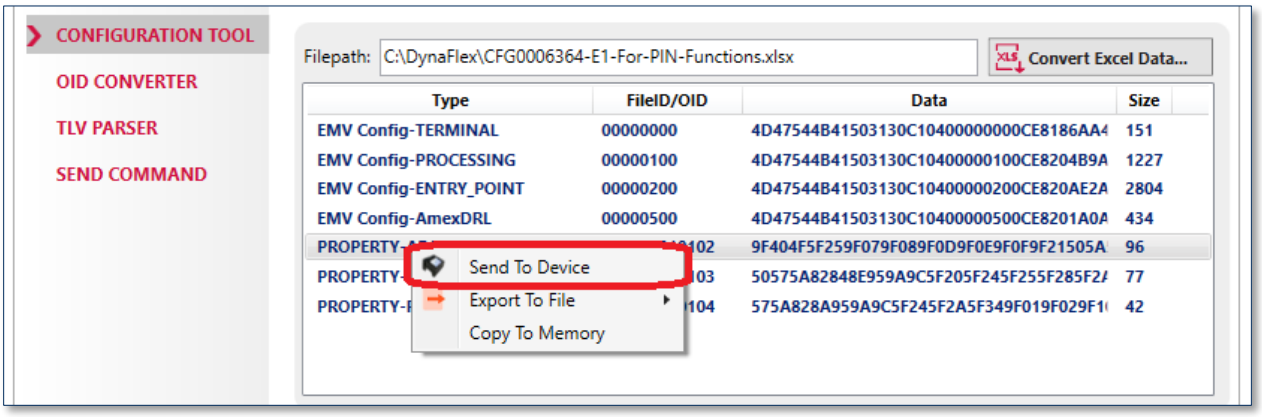
1) Select the **TOOLS** tab, select **CONFIGURATION TOOL**, and then press the **Convert Excel Data** button to browse for the excel configuration file.

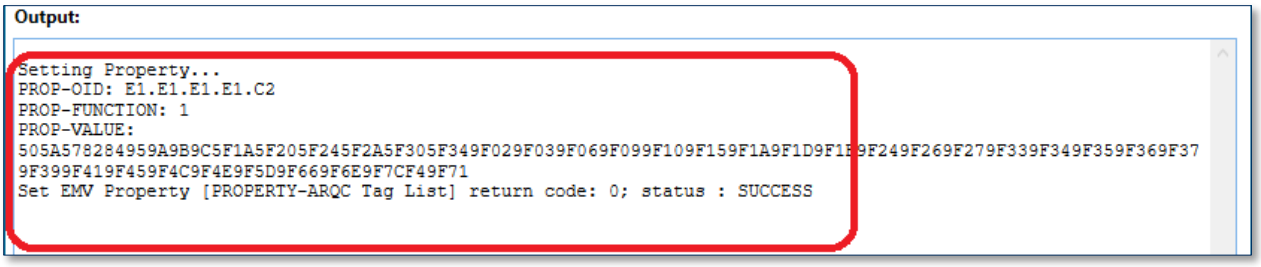


2) Select an excel file, then press the **Open** button.

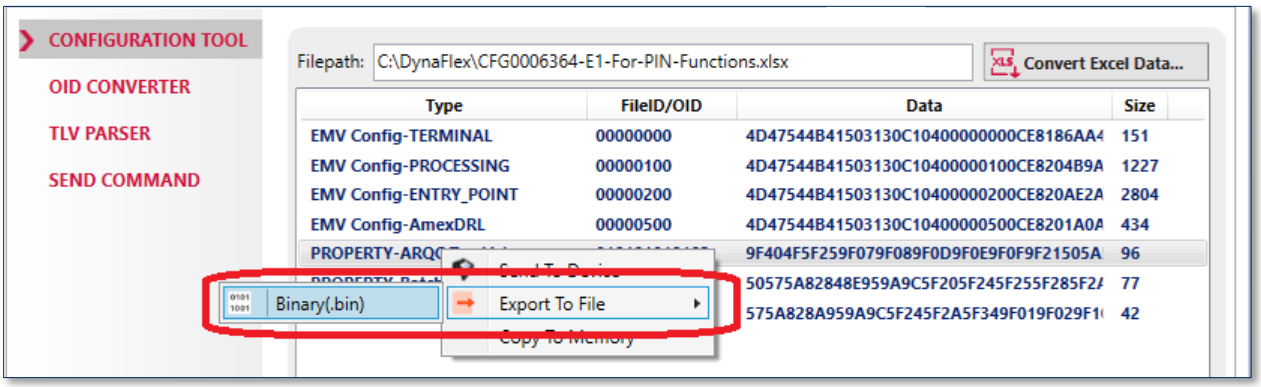


3) To send a file to the device, select a single file or multiple files type using the CTRL key, then right click and select **Send to Device**. The result of will be shown similarly as below.

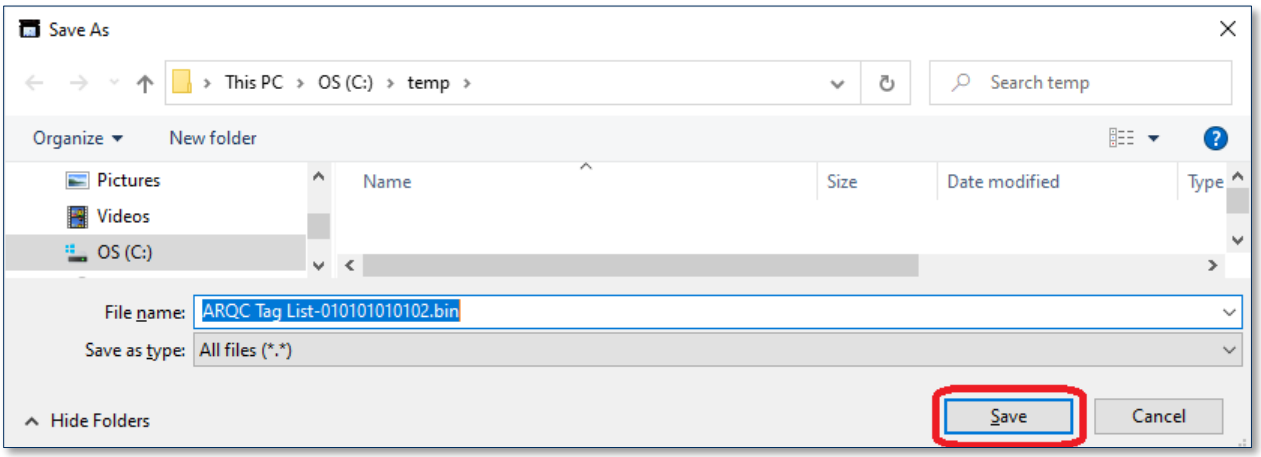




4) To save an individual configuration type, right click on the desire configuration type and select **Export To File**, then select **Binary(.bin)**.



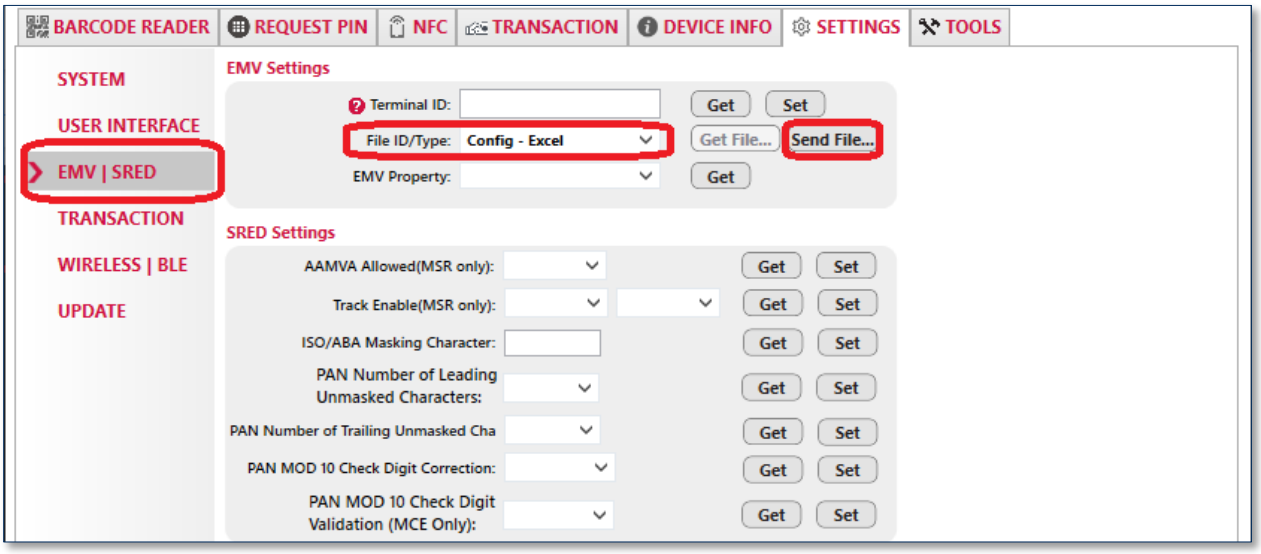
5) Browse to the desired location and press the **Save** button to save the .bin file.



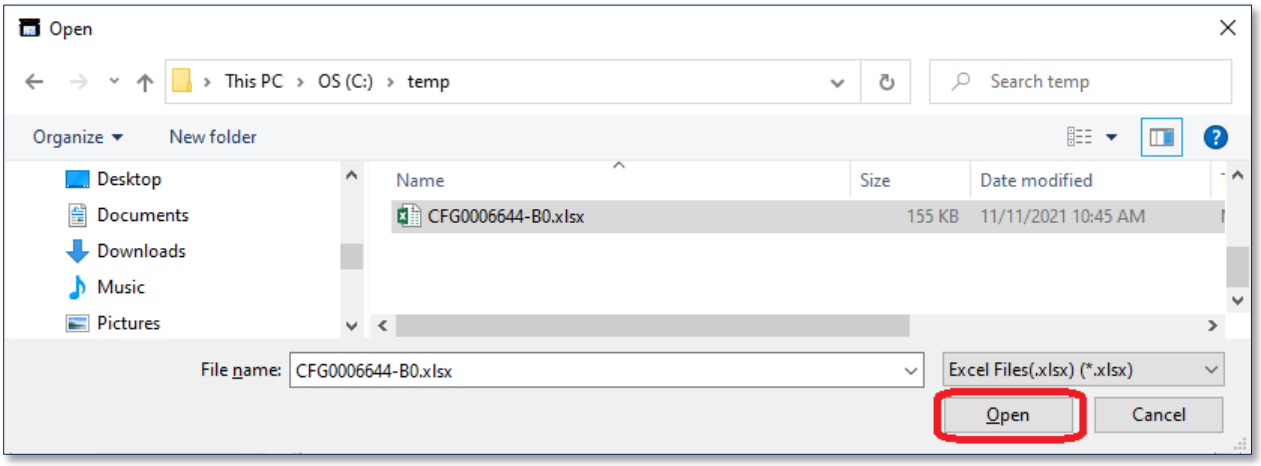
8.5 Send Bulk Configuration

To send an excel file that contains all the configuration data using excel file, follow these steps.

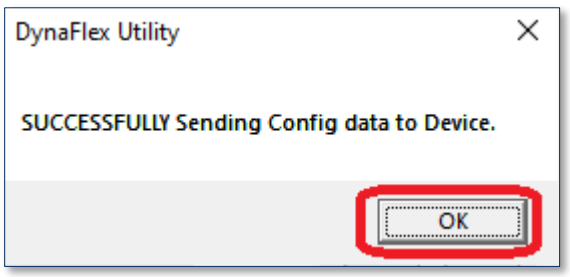
1) Select **Settings Tab** and the **EMV / SRED** menu. At **File ID/Type**, select the **Config – Excel**, and then press the **Send File** button.



2) Browse and select the excel configuration file and press the **Open** button.



3) The software will display a result message. Press the **OK** button to close.



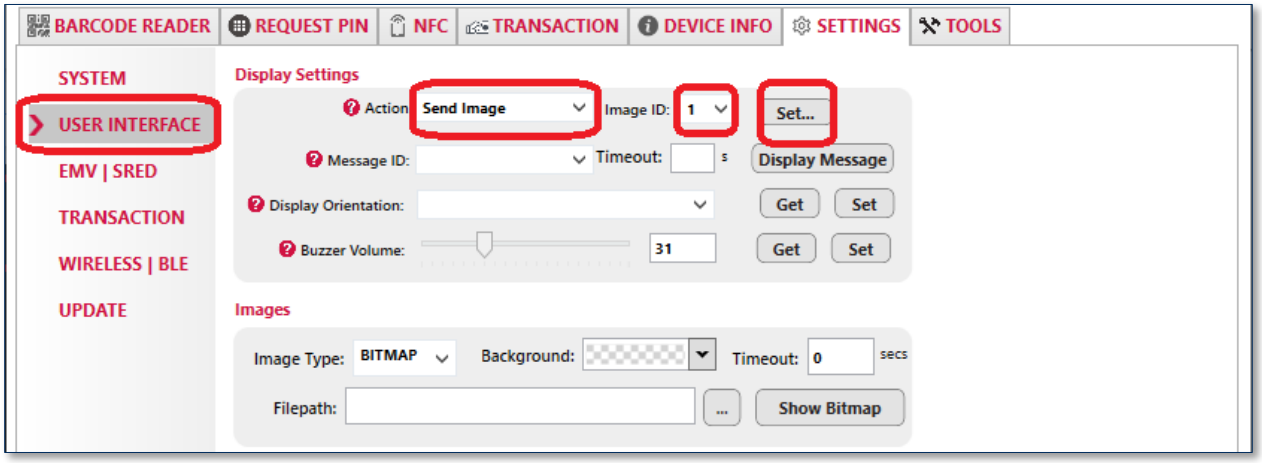
8.6 Send Bitmap Images (LCD Device Only)

Before uploading the image to the device, follow these simple instructions to create device-ready bitmap images.

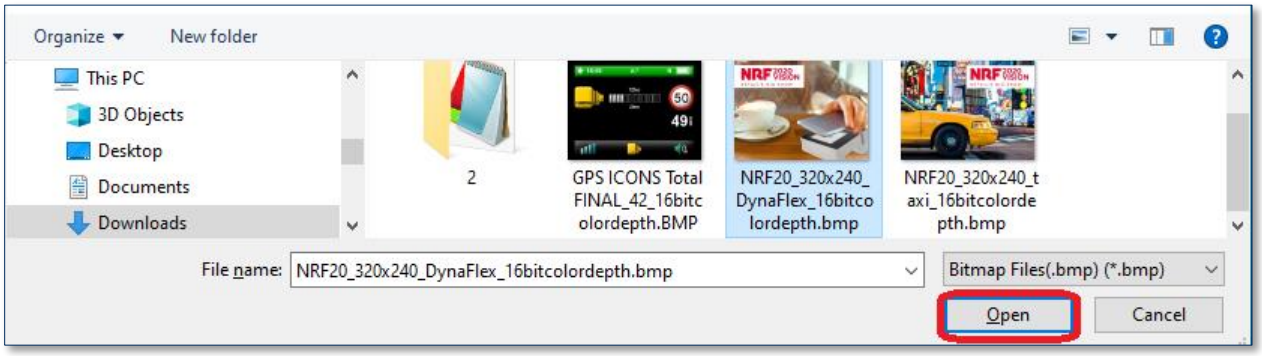
a) In a design program, set the canvas size to 320x240 pixels at 72 ppi/dpi
b) Images must be BMP format, 160KB or smaller with no compression, maximum 320px by 240px, with color depth 16 color, 256 color, 16-bit color, or 24-bit color. Images smaller than the maximum size are centered on the display. Note images at full screen size must be 16-bit color or lower to meet the size requirement.
For details see ***D998200383 DynaFlex Family Programmer's Manual (COMMANDS)***

To send bitmap image files, follow these steps.

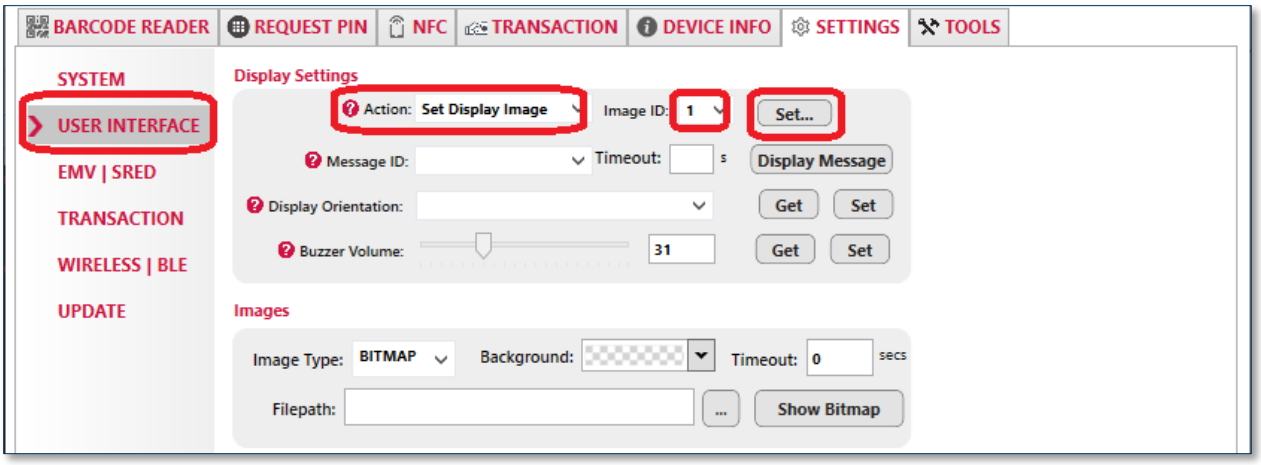
1) Select the **USER INTERFACE** menu, select **Send Image** in the **Action** list, then select the **Image ID** slot (1 to 4) to which the image will be sent, and then press the **Set** button to browse for the image file.



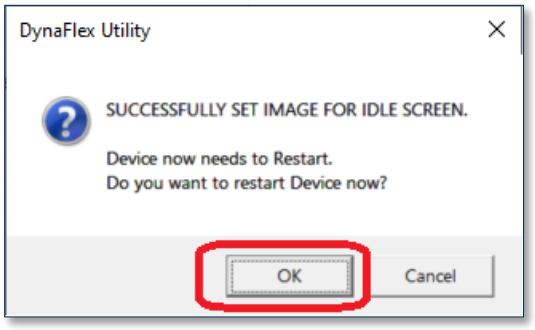
2) Select the bitmap image to be loaded to the device, then press the **Open** button.



3) Follow the same instruction to load the images to other slots.
4) To set which slot is to be used for the idle image, select the **Set Display Image** in the **Action** menu, then select the slot to be shown as the idle image, and press the **Set** button.



5) The software will show a message confirming to restart the device. Press to **OK** button to continue.

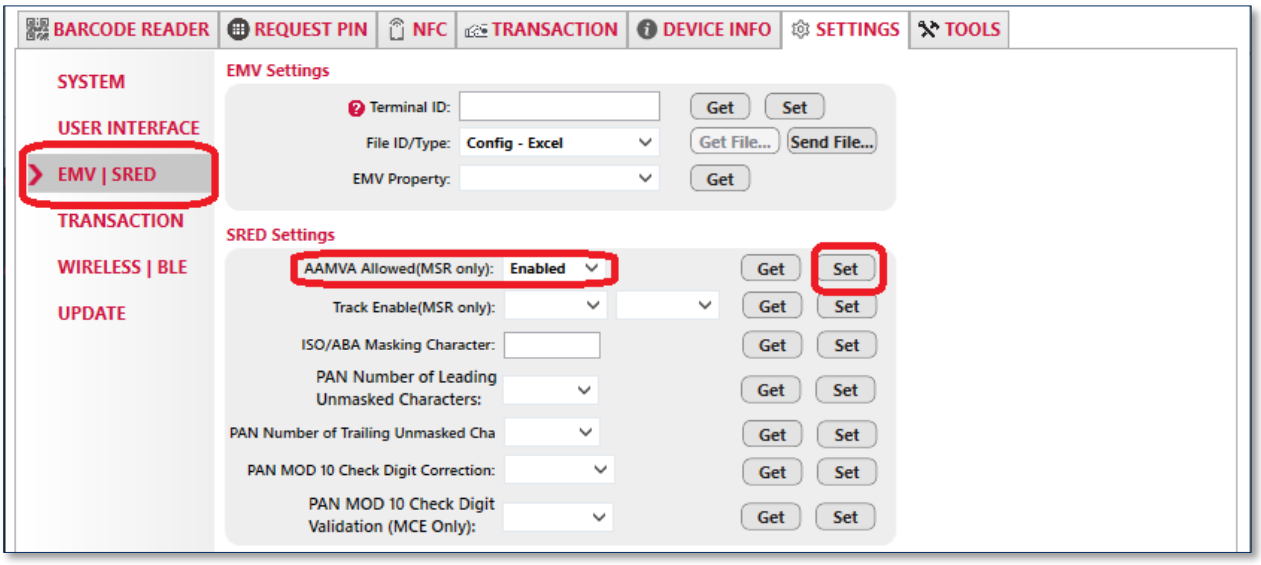


6) The device will restart, and the idle screen will display the image belonging to the slot specified.

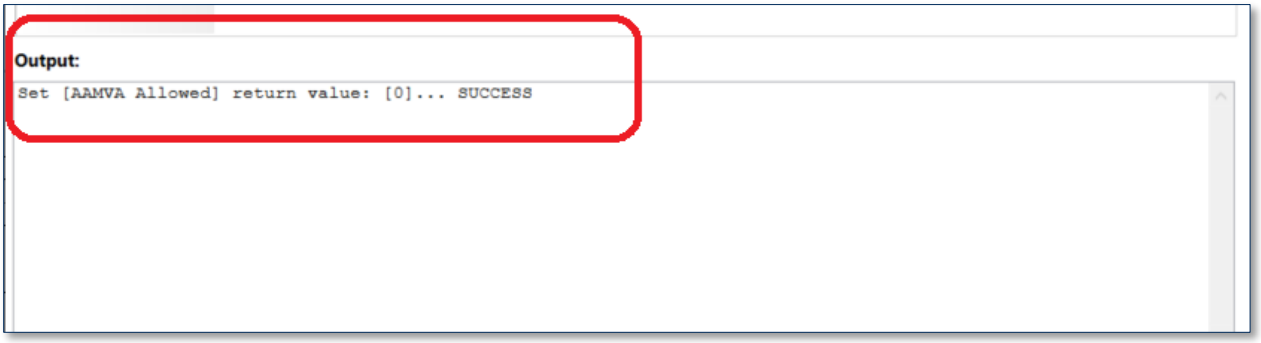
8.7 Configure AAMVA Reading

This property determines whether the device accepts AAMVA (driver's license) and ISO/ABA financial cards. When disabled, the EMV ARQC has Track Status = **Error** for any track that does not comply with ISO/ABA financial card format.

1) Select the **EMV / SRED** menu. At the **AAMVA Allowed** list, select either **Enable** or **Disable**, then press the **Set** button.



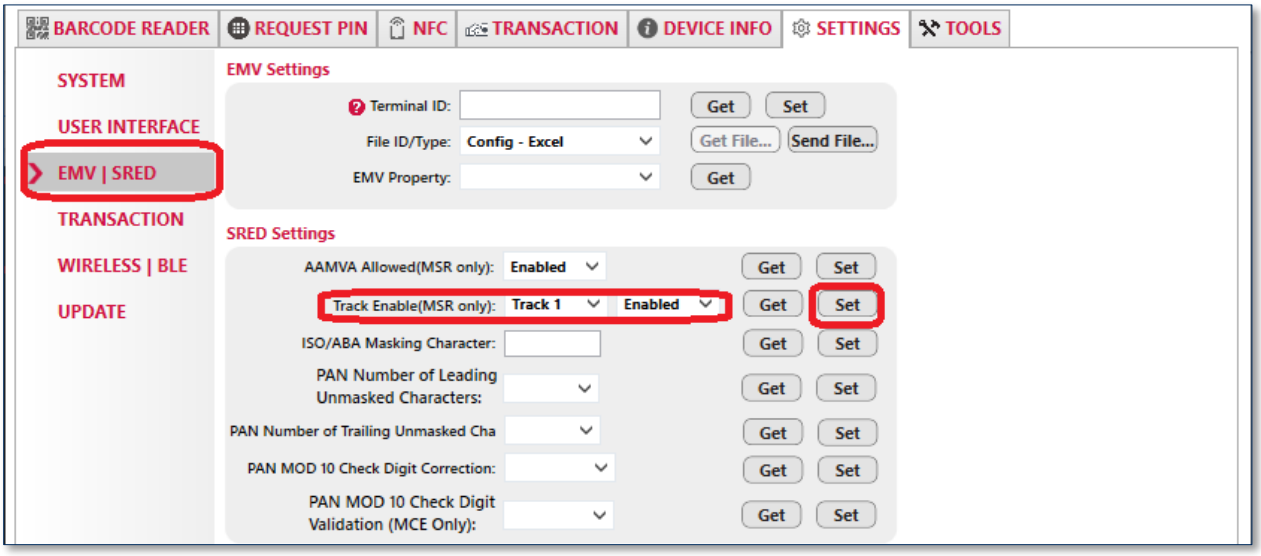
2) Observe the result in the **Output** log.



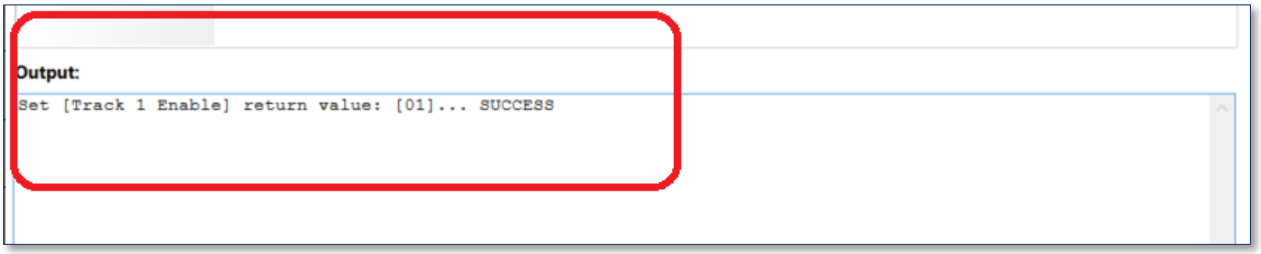
8.8 Configure Magnetic Stripe Track Data

This property determines whether to include or suppress Track 1, Track2, or Track 3 data when reading and transmitting ISO/ABA account information. To enable or disable reading for each track, follow these steps.

1) Select the **EMV / SRED** menu. At **Track Enable(MSR Only)**, select the track to be enabled or disabled, then press the **Set** button.



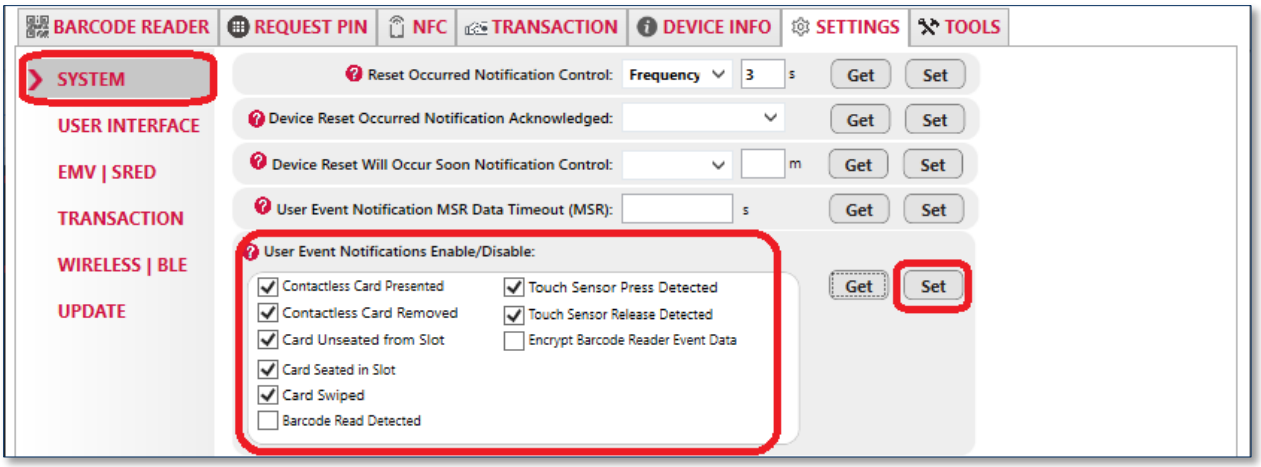
2) Confirm the result in the **Output** log.



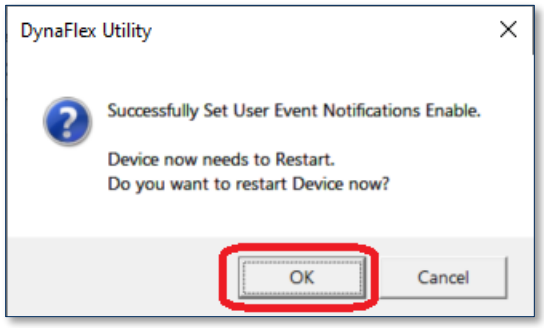
8.9 Configure the User Event Notification

The device only detects these user events and sends these notifications when it is idle. While processing a command (not idle), such as when processing a transaction, the device only sends notifications related to the command it is currently processing. Property change takes effect after the device is power cycled or reset.

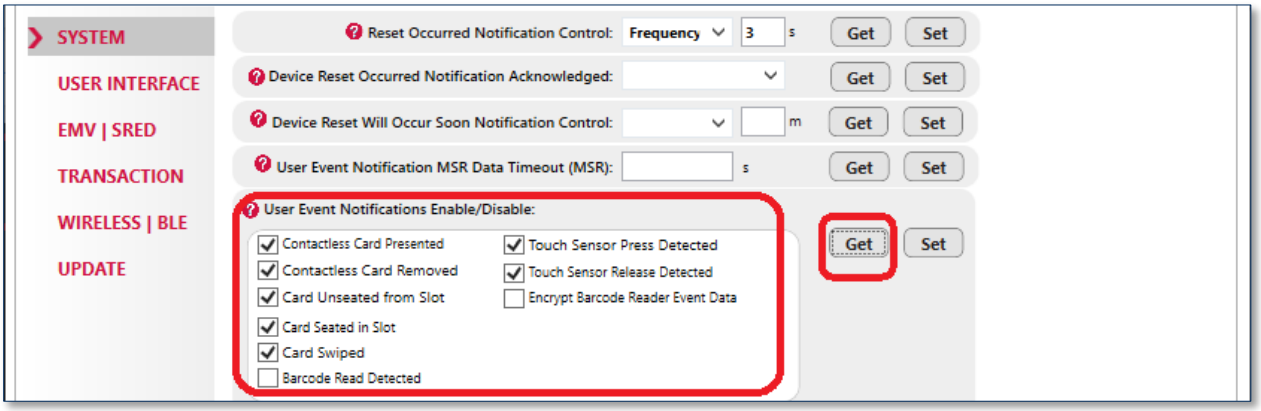
1) Select **SYSTEM** menu. Select the appropriate settings under **User Event Notifications Enable**, and then press the **Set** button.



2) Press the **OK** button to reset the device for the changes to take effect.



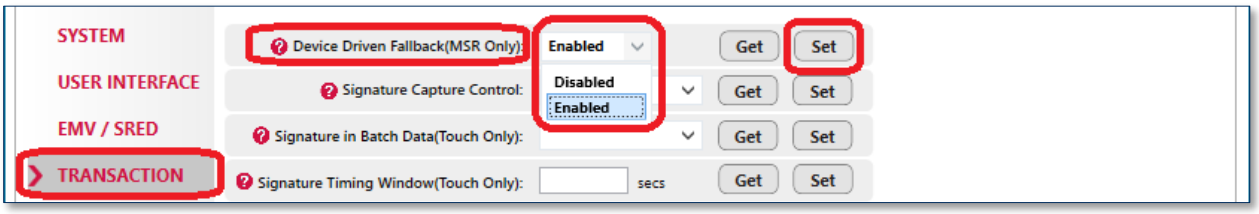
3) Confirm the changes by pressing the **Get** button after the device reset is complete.



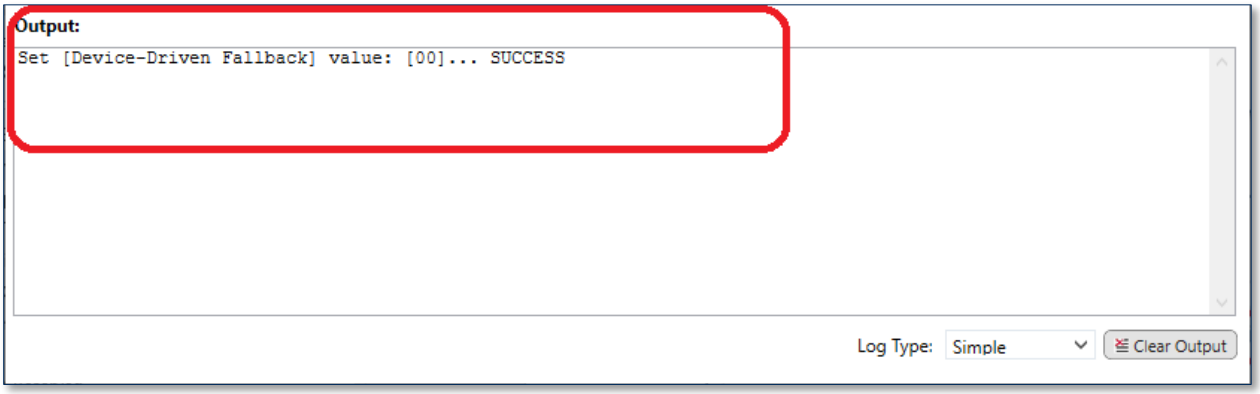
8.10 Change Device-Driven Fallback Behavior

Device-Driven Fallback Behavior is configured so the device automatically performs fallback operations. To enable or disable this behavior, follow these steps.

1) Select the **TRANSACTION** menu. At the **Device Driven Fallback(MSR Only)** list, select either **Enable** or **Disable**, and then press the **Set** button.



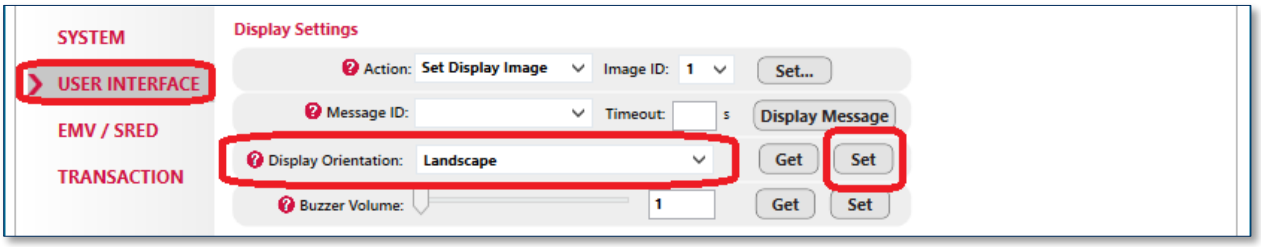
2) Observe the result in the **Output** log.



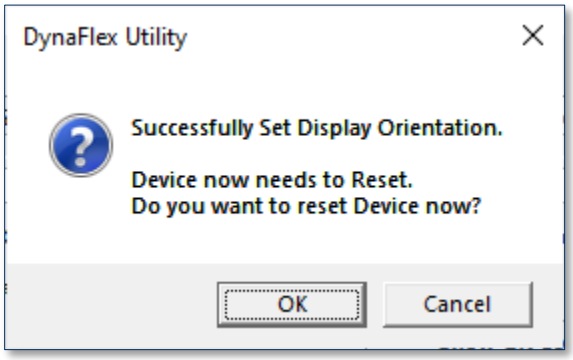
8.11 Change Device Display Orientation (LCD Device Only)

To configure device screen orientation, follow these steps.

1) Select the **USER INTERFACE** menu. At the **Display Orientation** list, select either **Portrait** or **Landscape** mode, and then press the **Set** button.



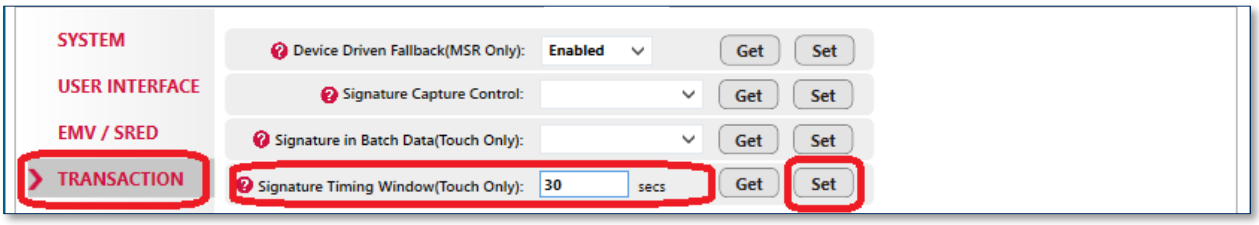
2) Press the **OK** button to reset the device for the setting to take effect.



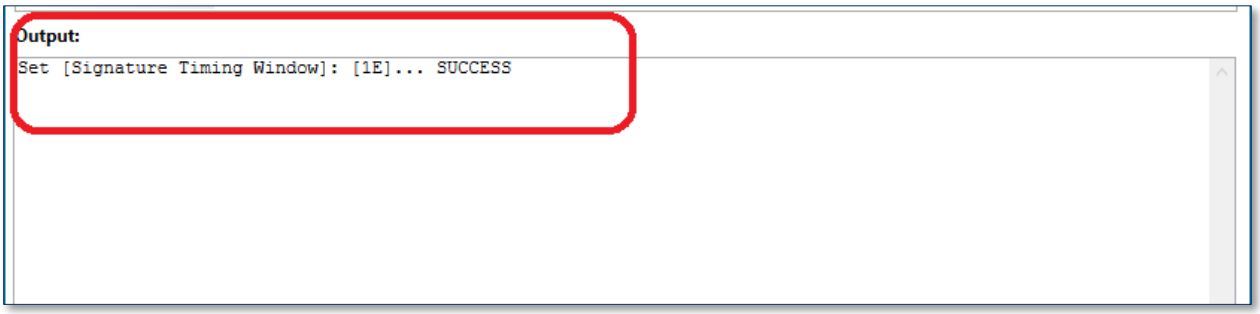
8.12 Change Signature Timing Window (LCD Device Only)

This property determines how long to wait, in seconds, after an EMV transaction is completed that requires a signature capture.

1) Select the **TRANSACTION** menu. At **Signature Timing Window**, enter the desired time in seconds, and then press the **Set** button.



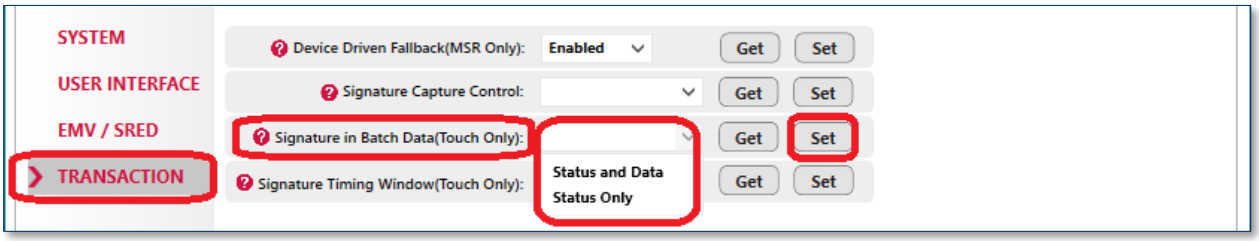
2) Confirm the result in the **Output** log.



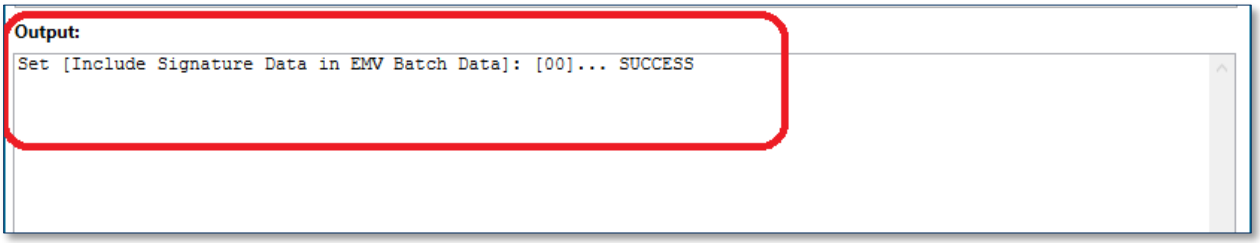
8.13 Change Signature in Batch (LCD Device Only)

To change the signature data in batch, follow these steps.

1) Select **TRANSACTION** menu. At the **Signature in Batch(Touch Only)** list, select the desire signature in batch setting, and then press the **Set** button.



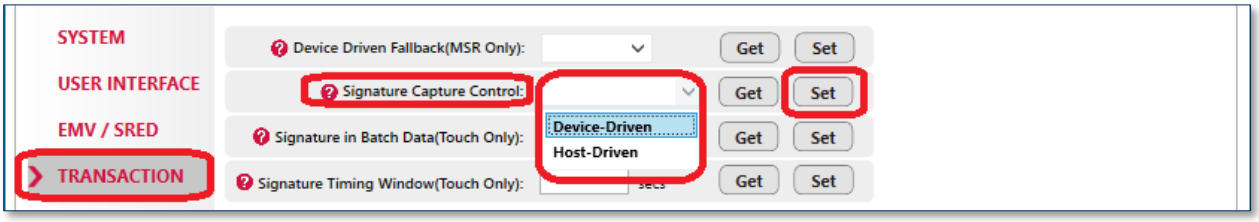
2) Observe the result in the **Output** log.



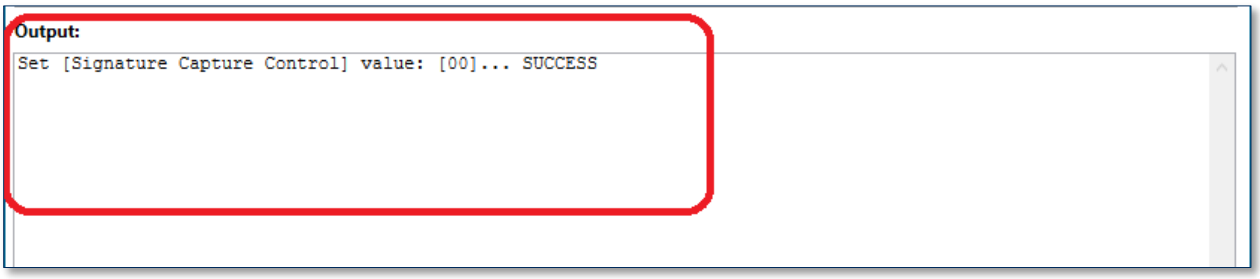
8.14 Change Signature Capture Control (LCD Device Only)

The host can use this property to change whether the device automatically prompts the cardholder for a signature when running EMV Transactions or leaves the requesting of signature capture prompts to the host app.

1) Select **TRANSACTION** menu. At the **Signature Capture Control** list, select either **Device-Driven** or **Host-Driven**, and then press the **Set** button.



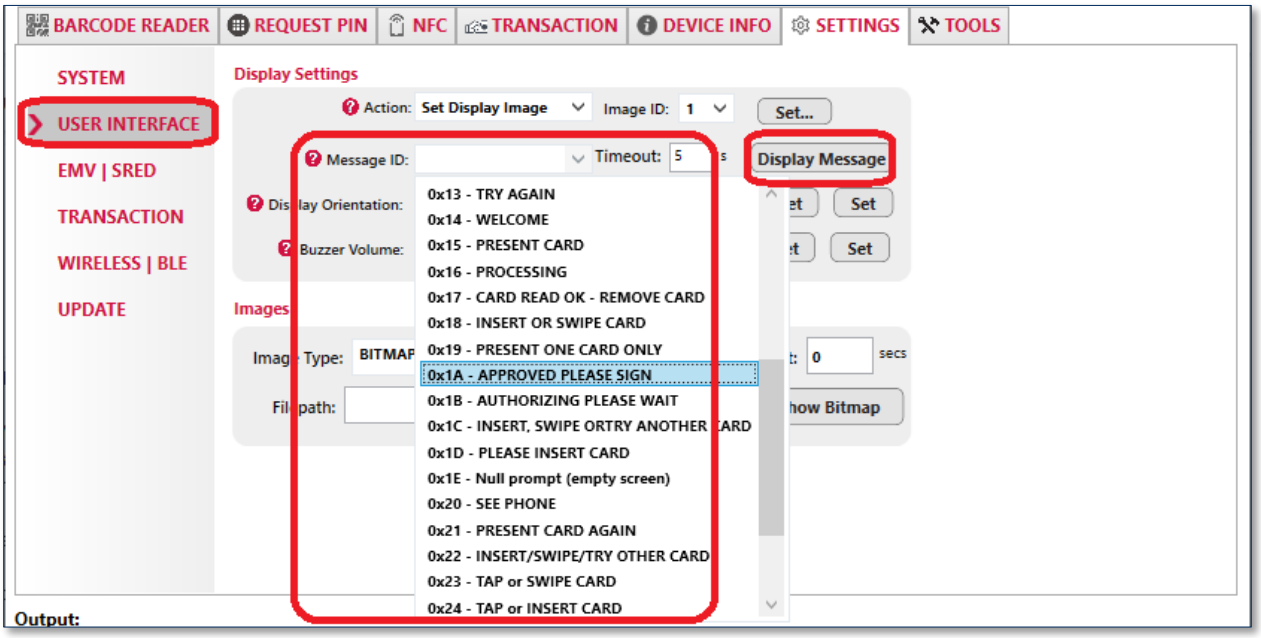
2) Confirm the result in the **Output** log.



8.15 Display Message on Device (LCD Device Only)

To display a pre-programmed message on the device, follow these steps.

1) Select **USER INTERFACE** menu. At the **Message ID** list, select the message to be displayed on the LCD screen, enter the time in seconds, and then press the **Display Message** button.

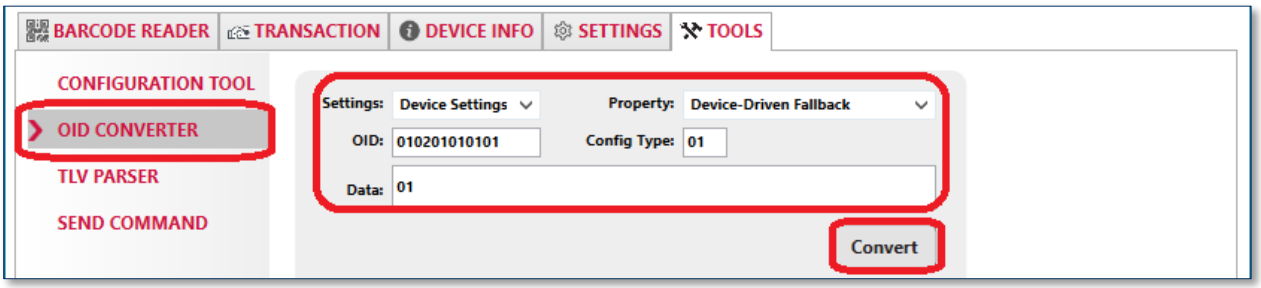


2) See the message on the LCD screen and observe the status in the **Output** log.

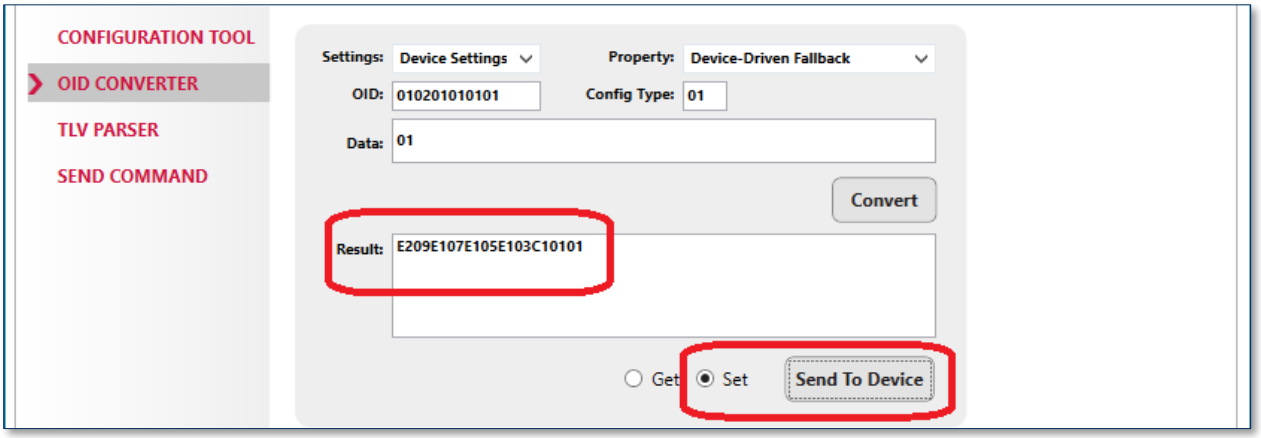
8.16 OID Conversion

This section converts OID property data to send to the device. For constructing the OID see D998200383 DynaFlex Family Programmer's Manual (COMMANDS) for possible combinations of data.

1) Select **TOOLS** tab and select the **OID CONVERTER** menu. Select a desired setting and enter the appropriate data in the **Data** text box, and then press the **Convert** button.



2) The OID conversion will be shown in the **Result** box. Select the **Set** option and then press the **Send To Device** button to send the converted OID to the device. Reset the device if necessary.



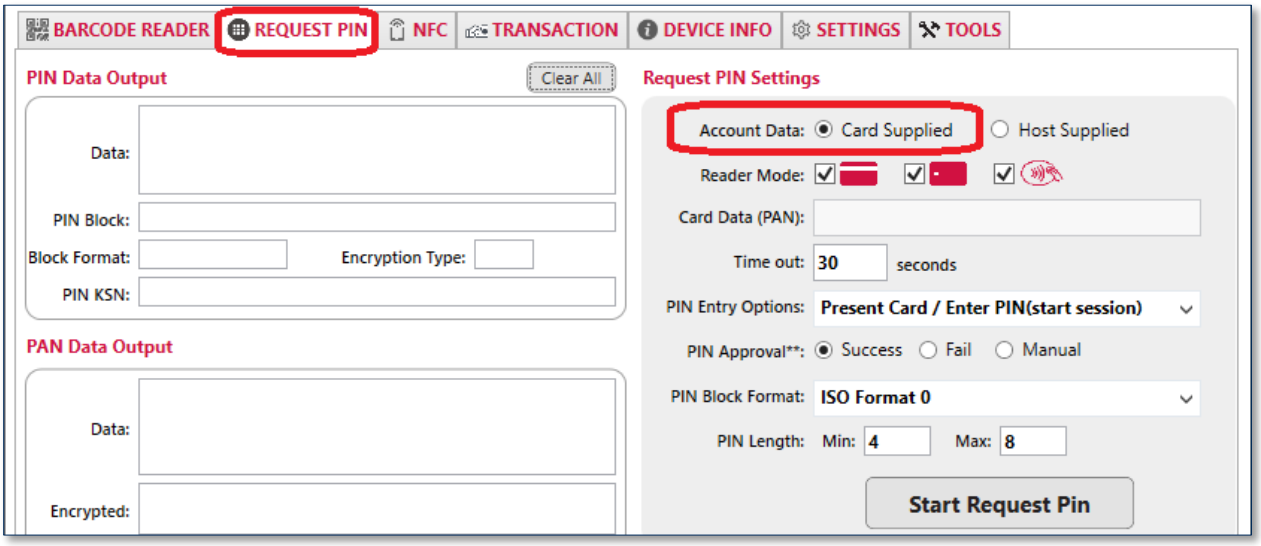
3) Observe the result in the **Output** log.

9 How to use Request PIN

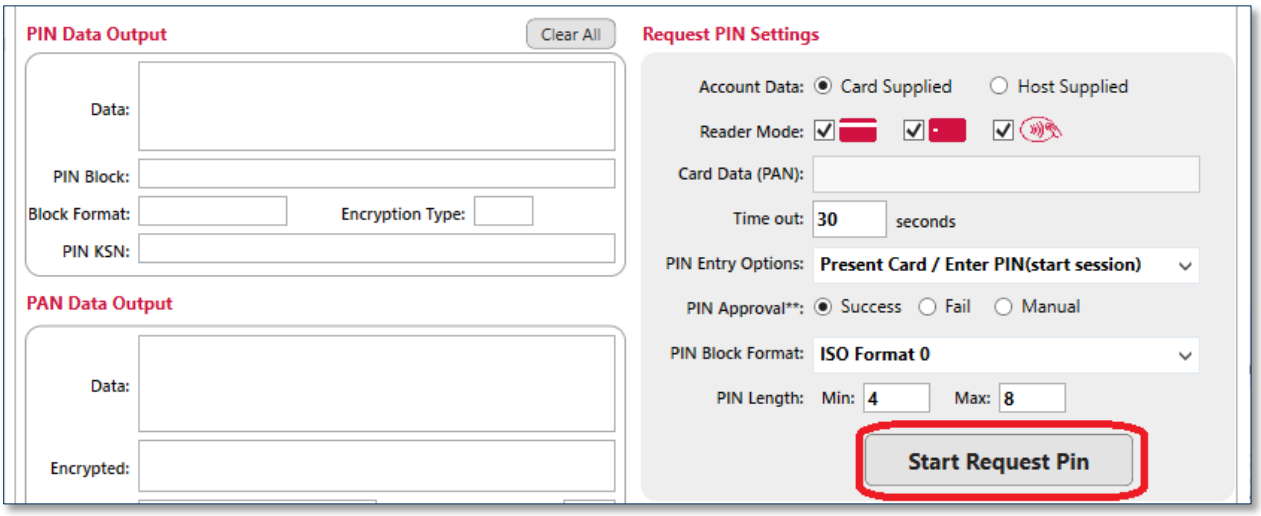
9.1 Card Supplied PIN

This section is to retrieve a PAN from a card and then request a PIN from the card holder. The PAN from the card is used in the formation of the PIN block.

1) Select the **REQUEST PIN** tab, and select the **Card Supplied** option.

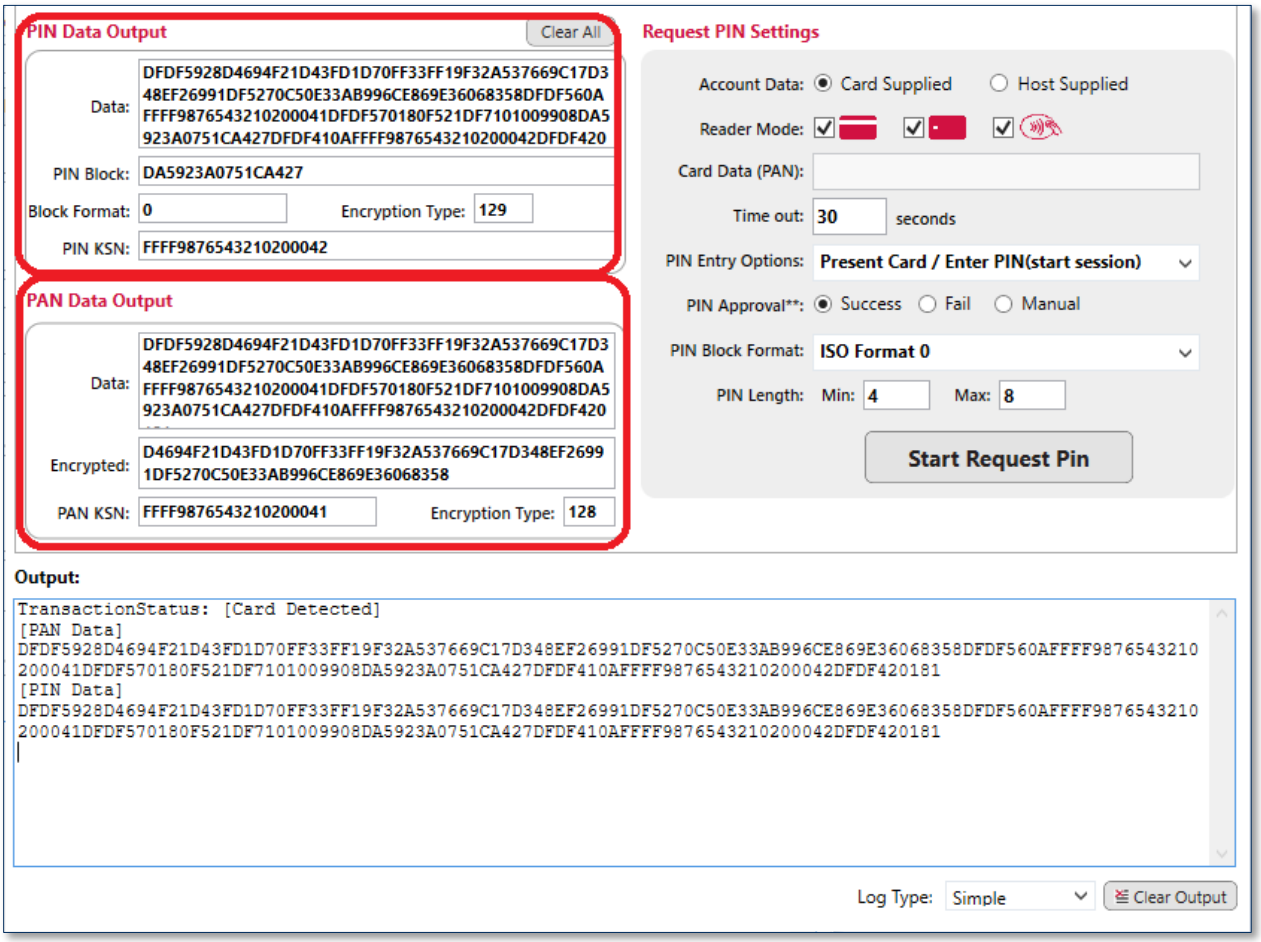


2) Press the **Start Request Pin** button and present a card to the device.

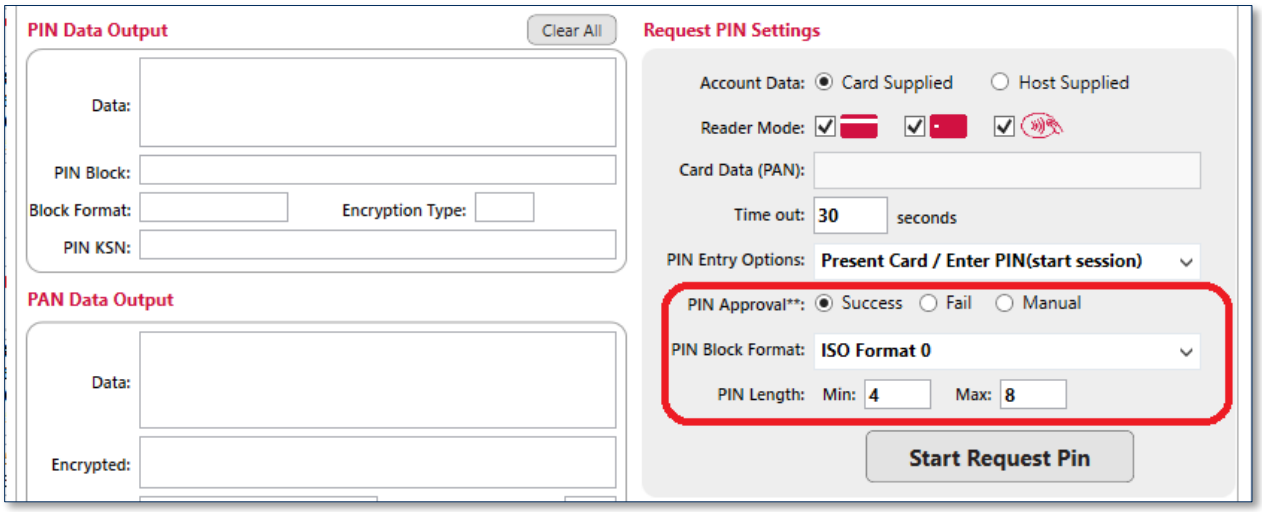


3) After a card is read, enter a PIN on the device screen.

4) PIN and PAN data output are displayed similar as below.



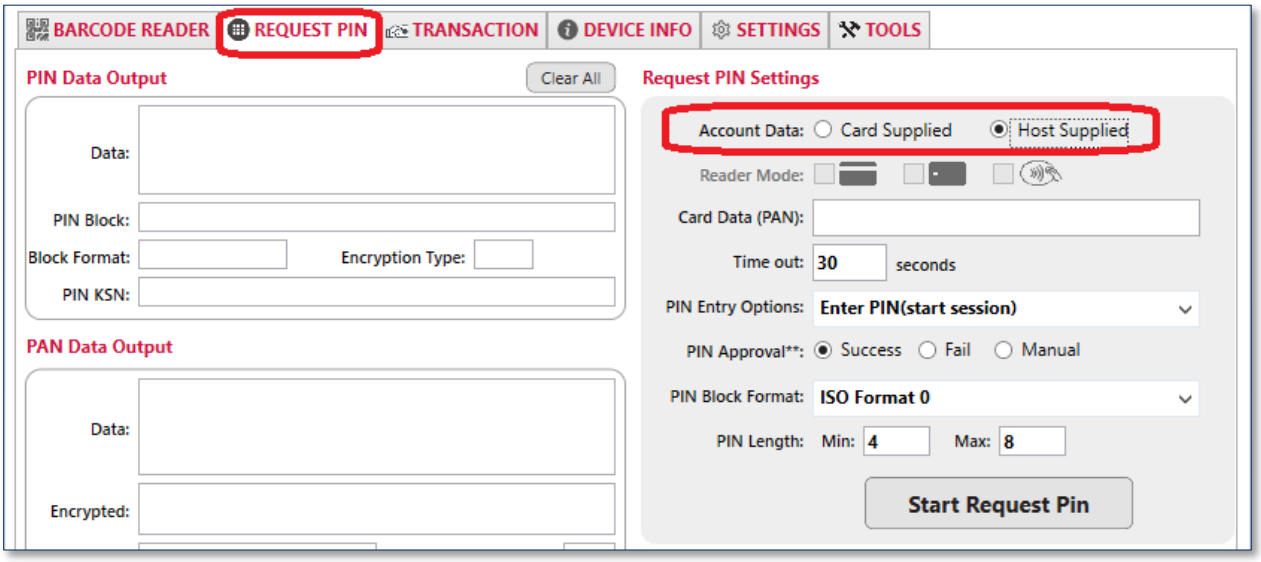
5) To change the approval status shown on the device screen, the PIN block format, or the PIN length, set the request settings, then repeat the request.



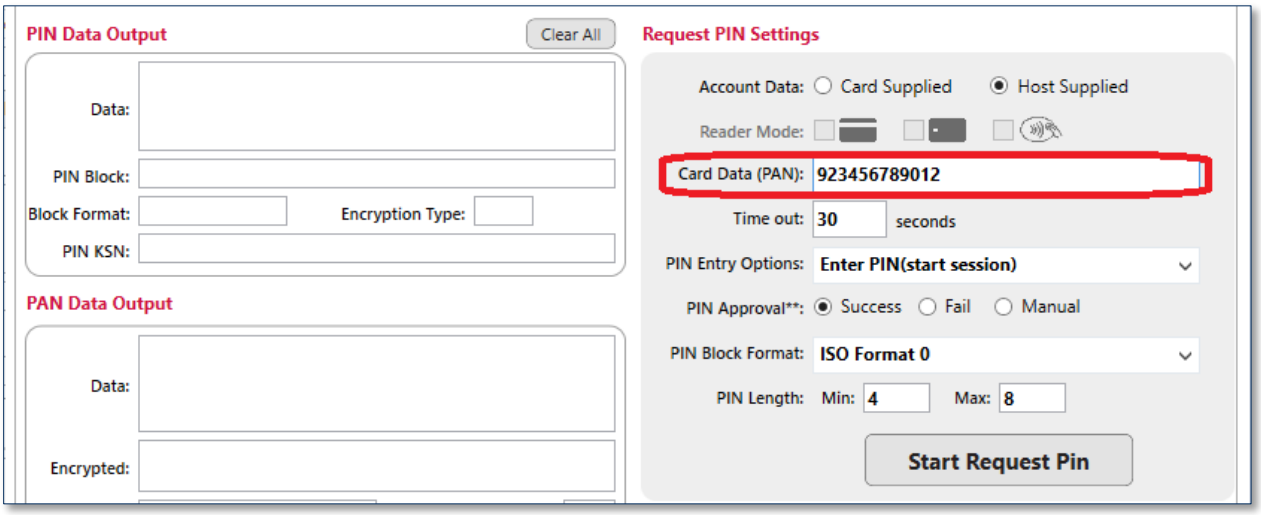
9.2 Host Supplied PIN

This section is to request a PIN from a user without a card. The PAN is supplied by the host application. The PAN supplied is used in the formation of the PIN block.

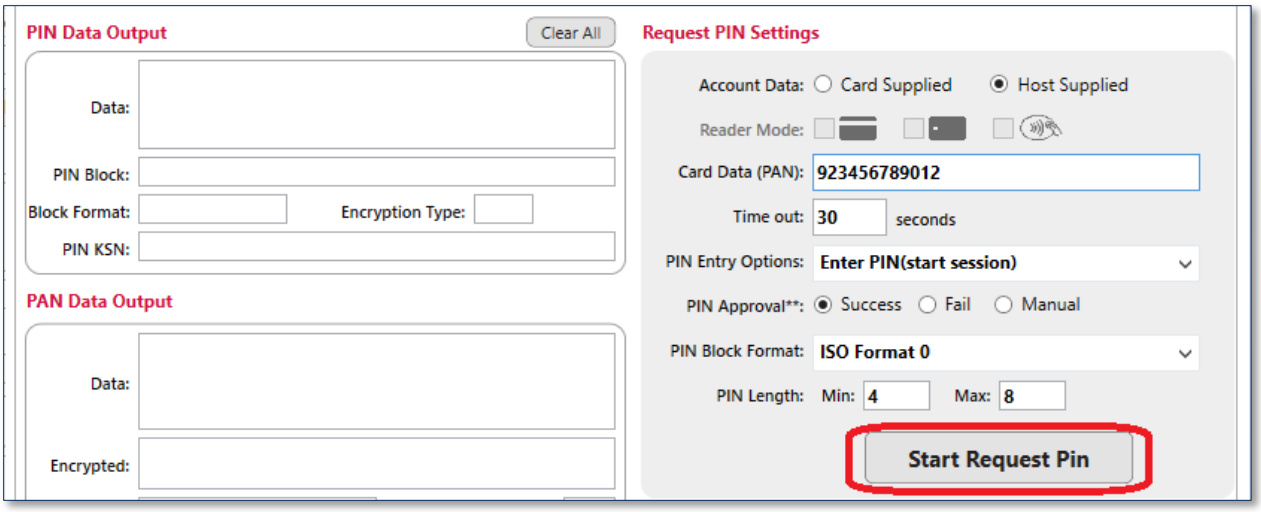
1) Select the **Host Supplied** option.



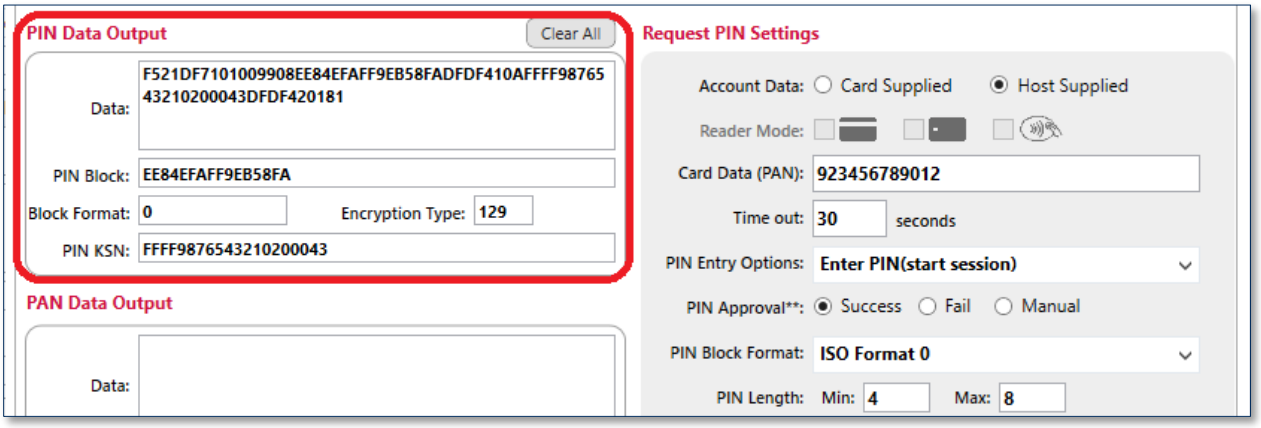
2) Enter a 12 digit PAN for the **Card Data (PAN)**.



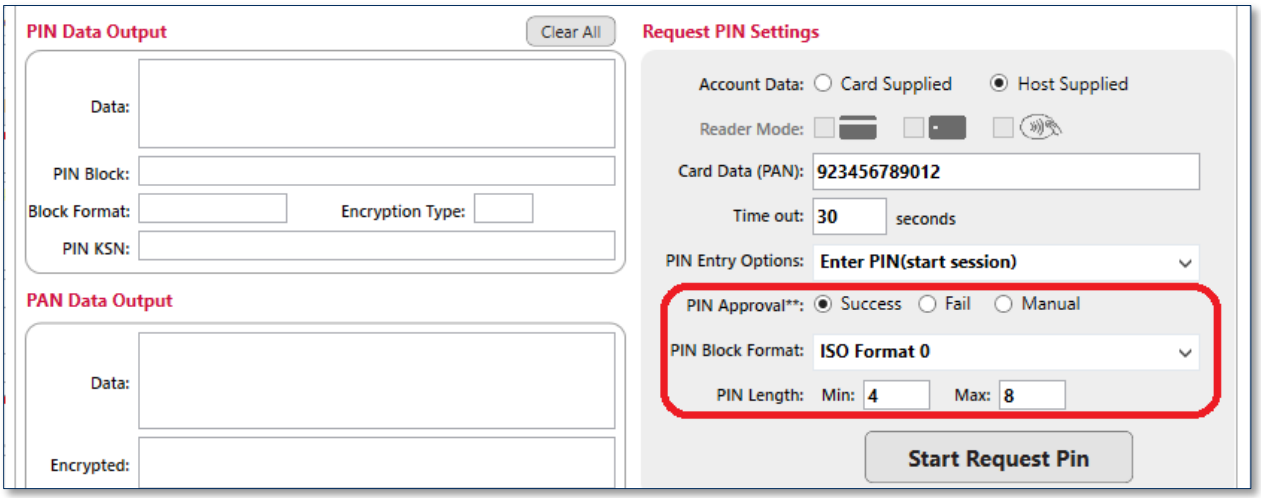
3) Press the **Start Request Pin** button.



4) Enter a PIN on the device screen. PIN data output is displayed similar as below.



5) To change the approval status shown on the device screen, the PIN block format, or the PIN length, set the request settings, then repeat the request.



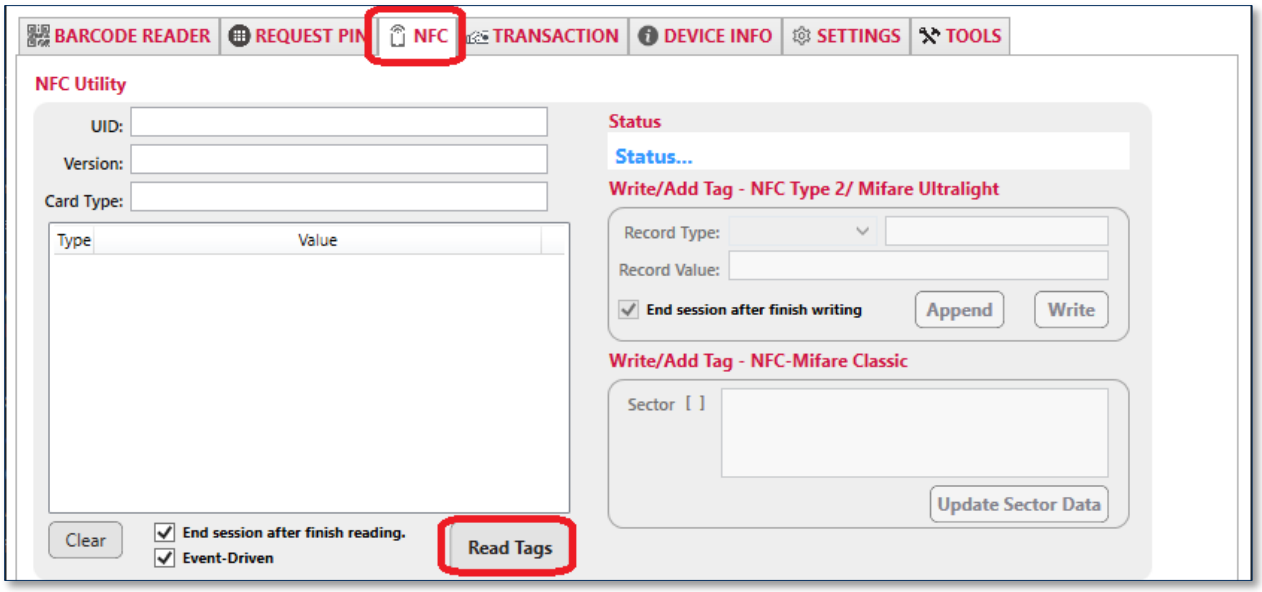
10 How to use the NFC Demo

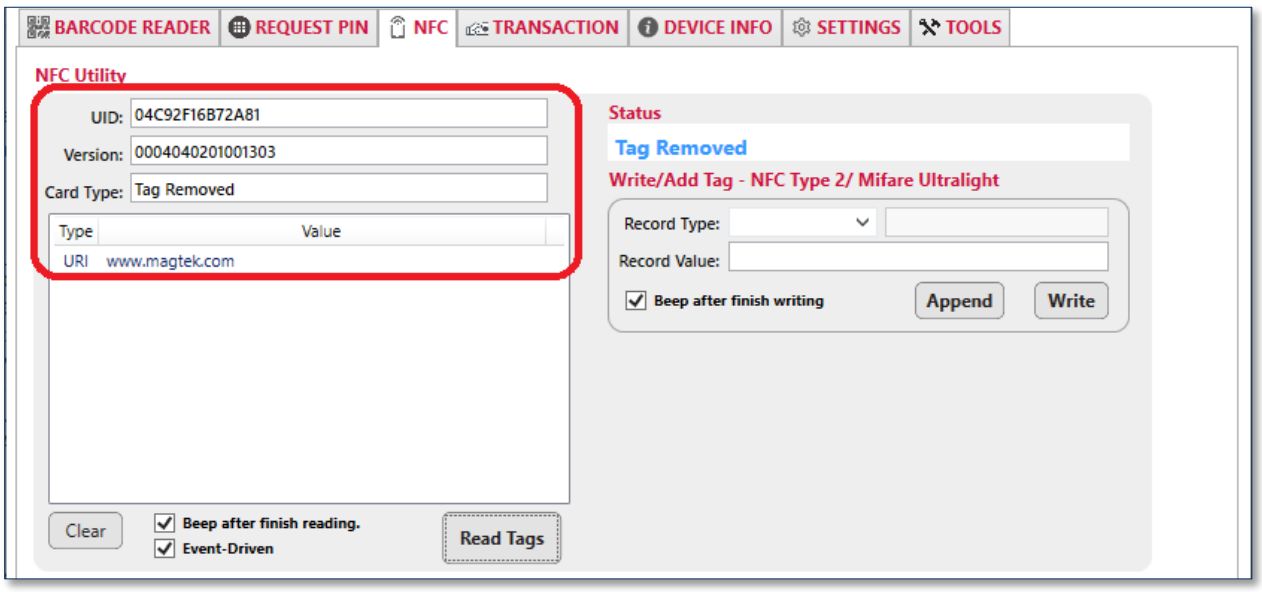
An NFC tag (Near Field Communication) can either be a passive type: card, badge, sticker, or an active type: mobile device.

NFC tag operations involves reading and writing data in small segments. Because of this, it is important to have the NFC tag be at rest during these operations. The usual quick tap is not sufficient. In this section, "Present an NFC tag" means to bring the tag next to the device and leave it there. "Tap and NFC tag" means to bring the tag next to the device long enough to read the tag. The Output log will stop scrolling when reading or writing is complete.

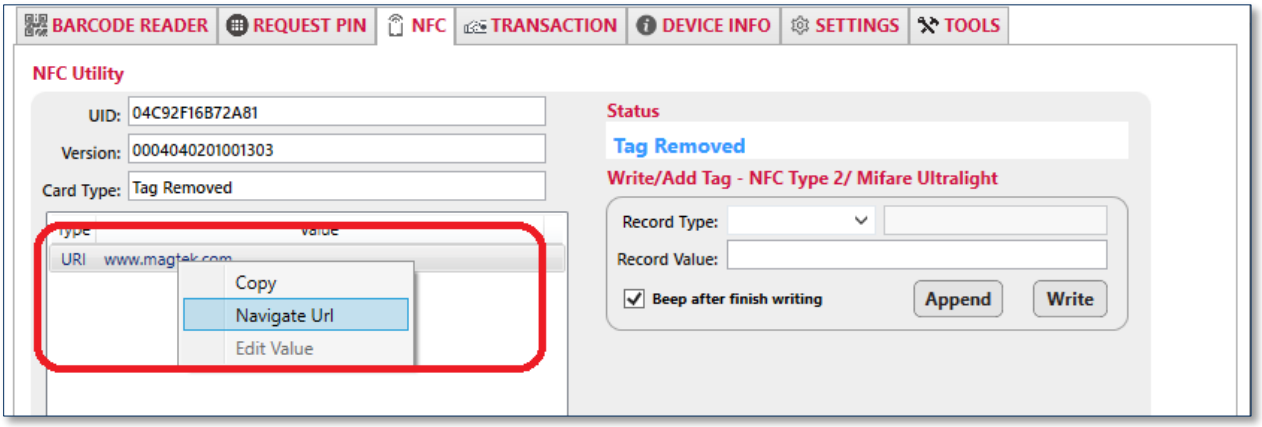
10.1 NFC Type 2 / Mifare Classic Tag - Read

1) Select the **NFC** tab. To retrieve the records on the NFC tag, press the **Read Tags** button and tap an NFC Type 2 tag or Mifare Classic tag to the device.

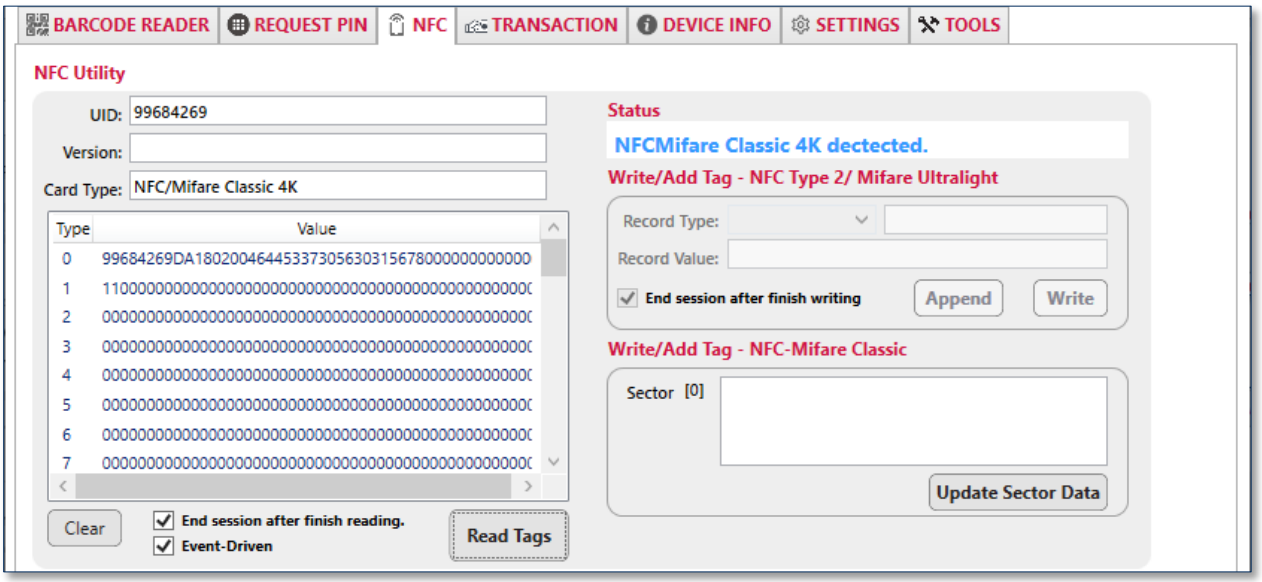




2) When there is only one tag record present and its type is URI, the app will launch a browser to the URI.
3) When there is more than one tag record, to navigate to a URL, right click a record and press on **Navigate Url** as shown below.



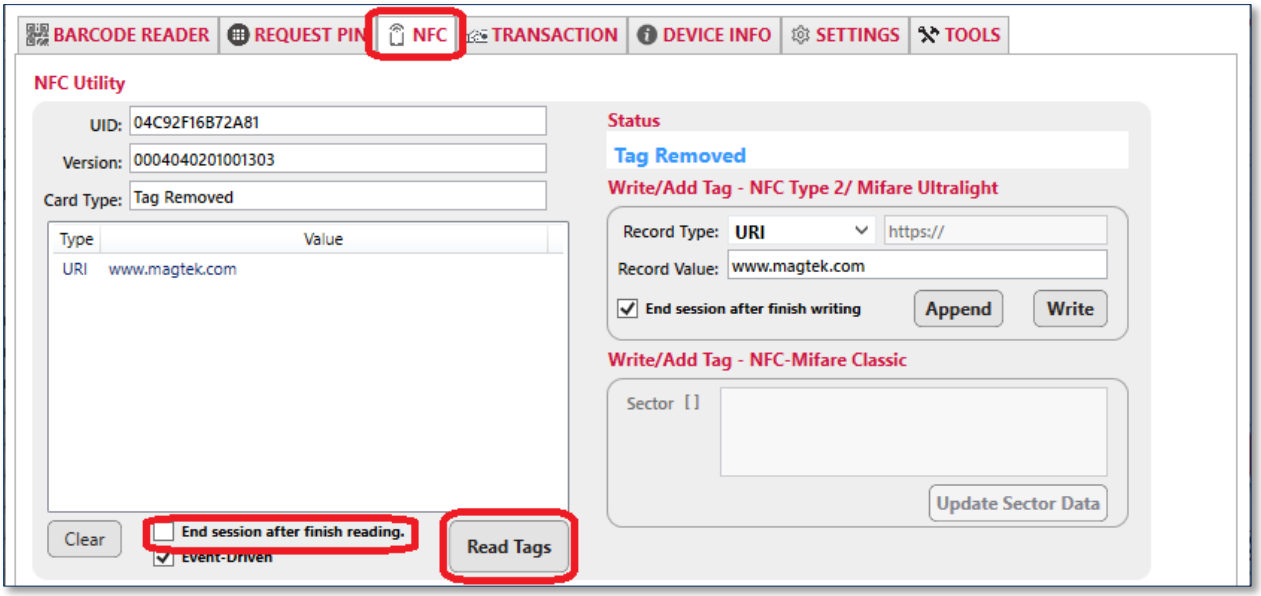
4) Additionally, when the **Event-Driven** feature is checked-on and the device has the Contactless Card user event notification enable, the NFC tag can be read by tapping the tag without need of pressing the **Read NFC Tags** button. The app will receive a detection notification and then automatically send the command to read NFC tag.
5) When the **End session after finish reading** check box is enabled, the device can repeatedly read the same NFC tag without need to remove it. The NFC is automatically turned off after the read. When the **End session after finish reading** check box is disabled, the NFC tag must be removed before a tag can be read again.
6) When reading a Mifare Classic tag, the Sectors will be shown similar as below.



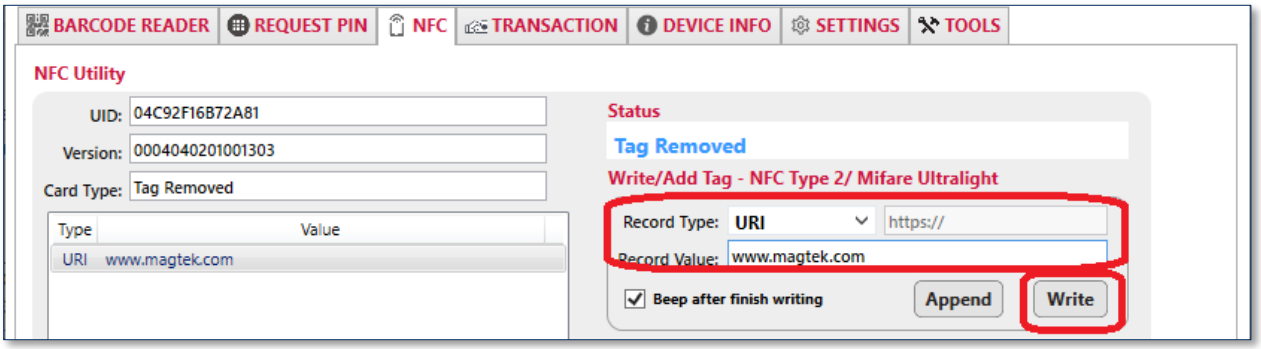
10.2 NFC Type 2 Tag - Write

Writing to an NFC Type 2 tag involves reading and writing data in small segments. Because of this, it is important to have the tag be at rest during these operations. The usual quick tap is not sufficient. In this section, "Present an NFC tag" means to bring the tag next to the device and leave it there.

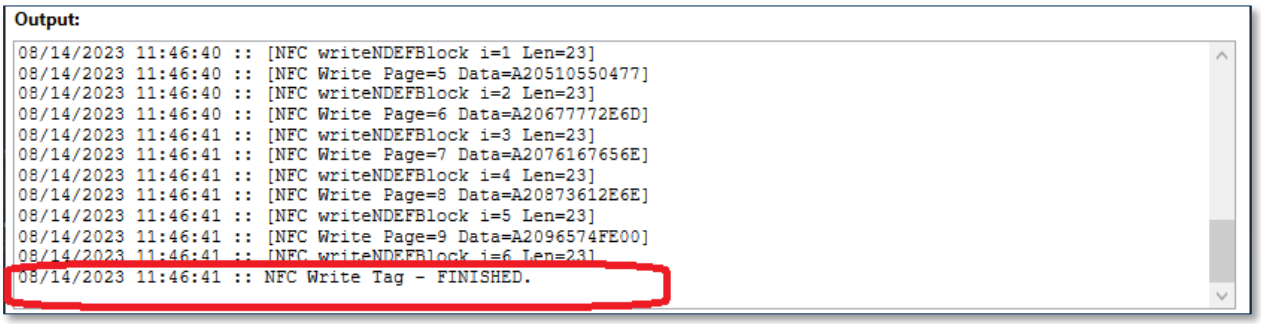
1) Select the **NFC** tab, uncheck **End session after finish reading**, press the **Read Tags** button, and then present an NFC Type 2 tag.



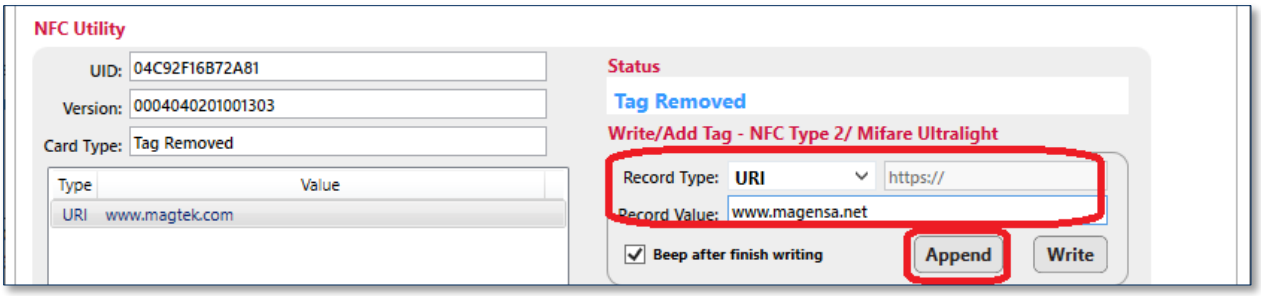
2) Select a **Record Type**, enter a **Record Value**, and then press the **Write** button.

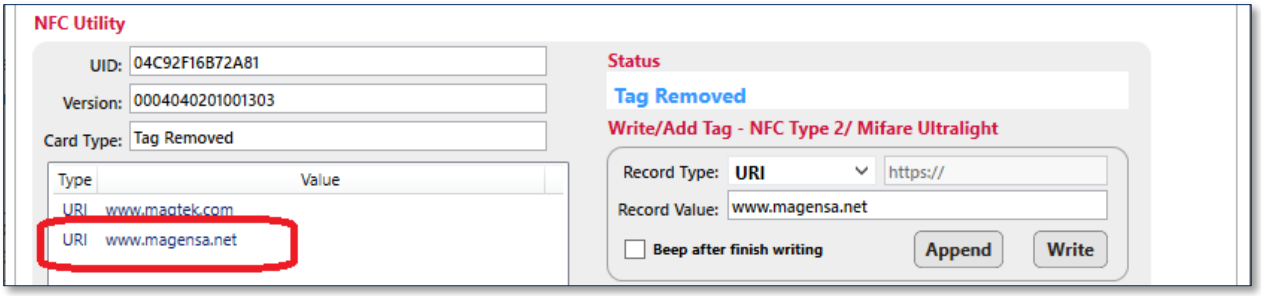


3) After the Write is complete, the **Output** will be shown as below.

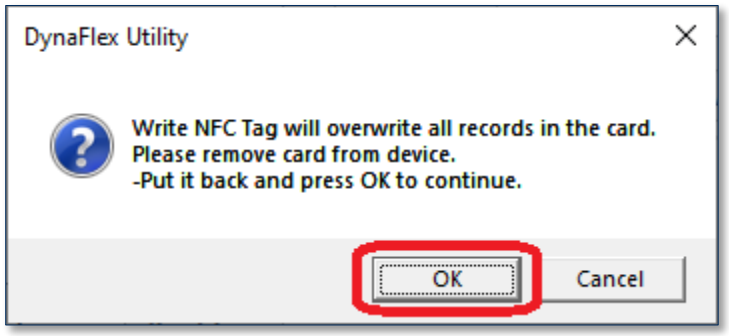


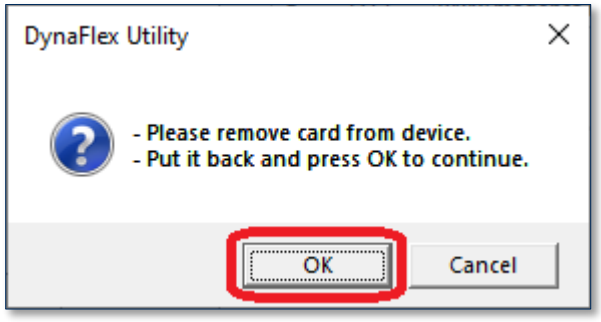
4) To add additional records, select a **Record Type**, enter a **Record Value**, and then press the **Append** button.





5) If the NFC Type 2 tag is removed from the device before performing either Write or Append, the app will prompt to present the card. This is because the NFC module must to be armed after NFC Type 2 tag removal. Follow the instructions and press OK button.

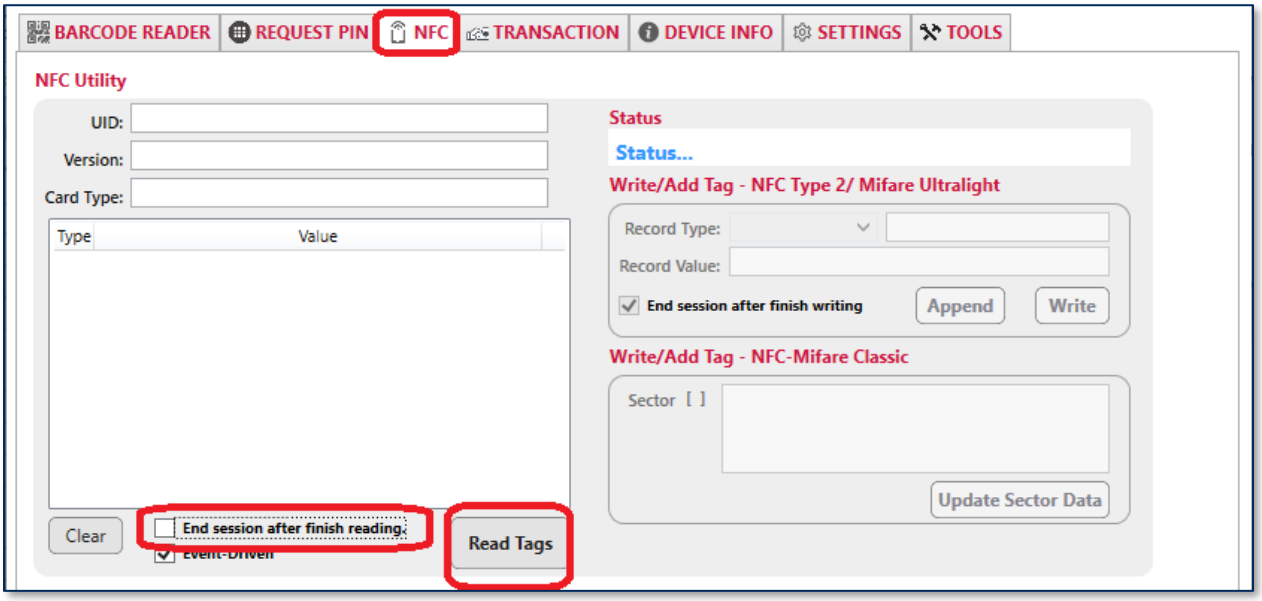




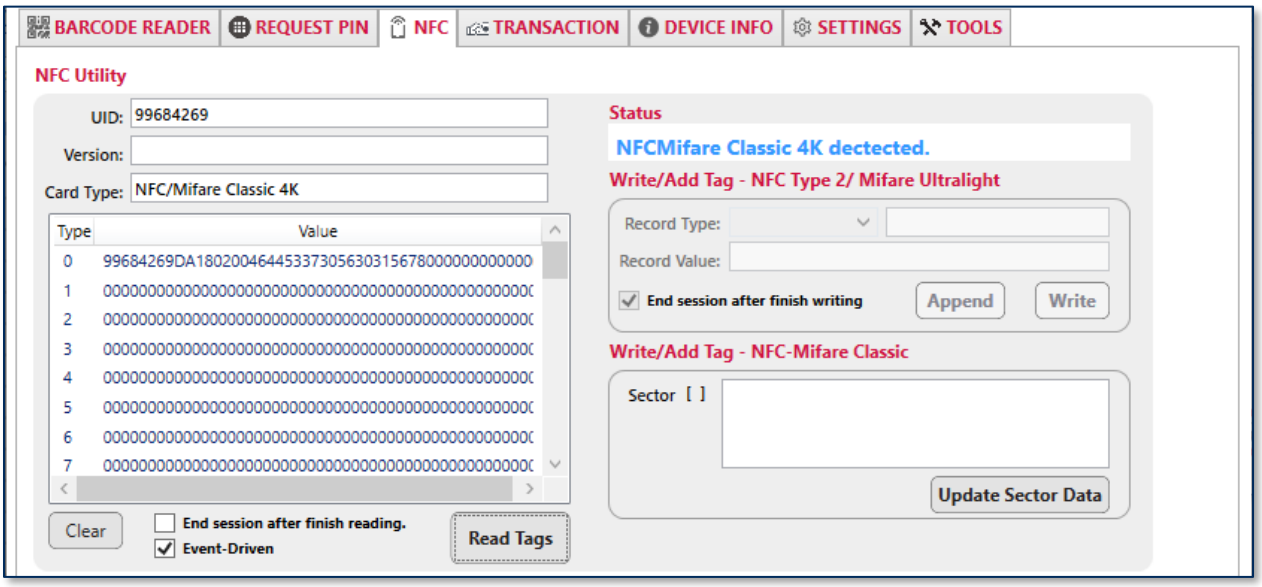
10.3 Mifare Classic Tag - Write

Writing to a Mifare Classic tag involves reading and writing data in small segments. Because of this, it is important to have the tag be at rest during these operations. The usual quick tap is not sufficient. In this section, "Present an NFC tag" means to bring the tag next to the device and leave it there.

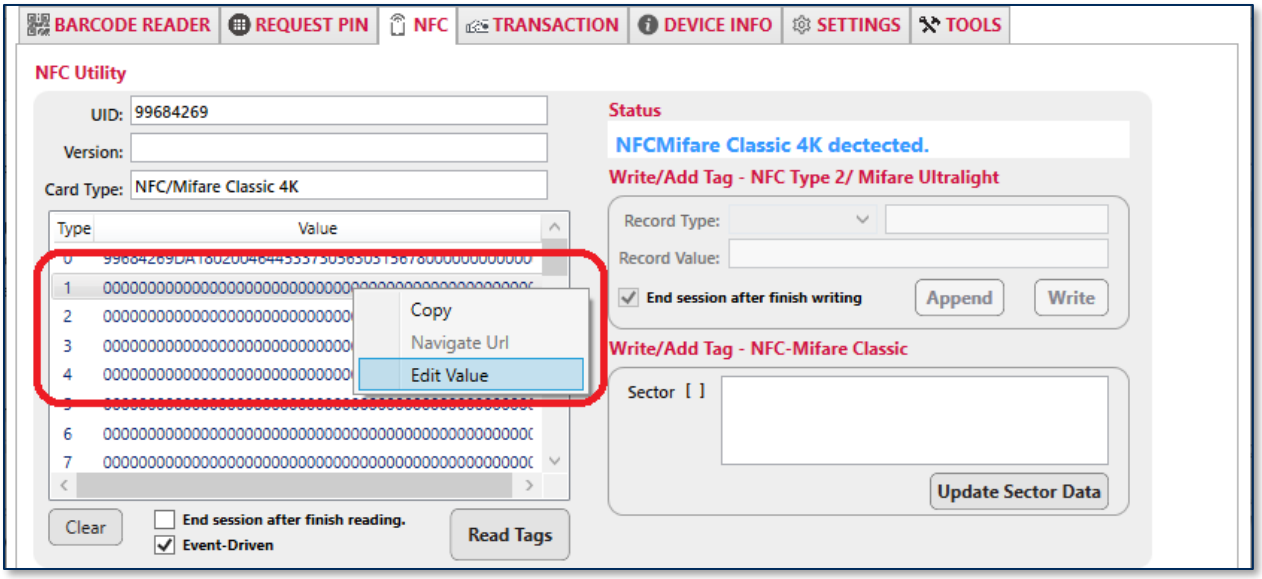
1) To write to a Mifare Classic tag, select the **NFC** tab, uncheck **End session after finish reading**, press the **Read Tags** button. Present a Mifare Classic tag and leave the tag next to the device.



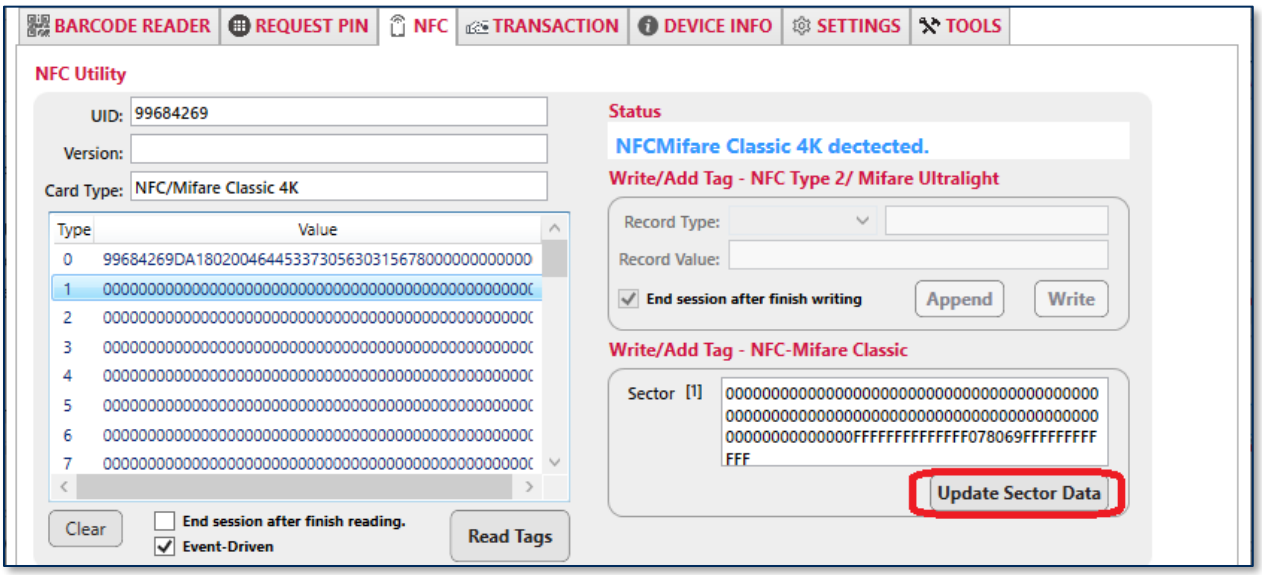
2) Each sector of the Mifare Classic tag will be read.



3) Right-click on a Sector, and select **Edit Value**.



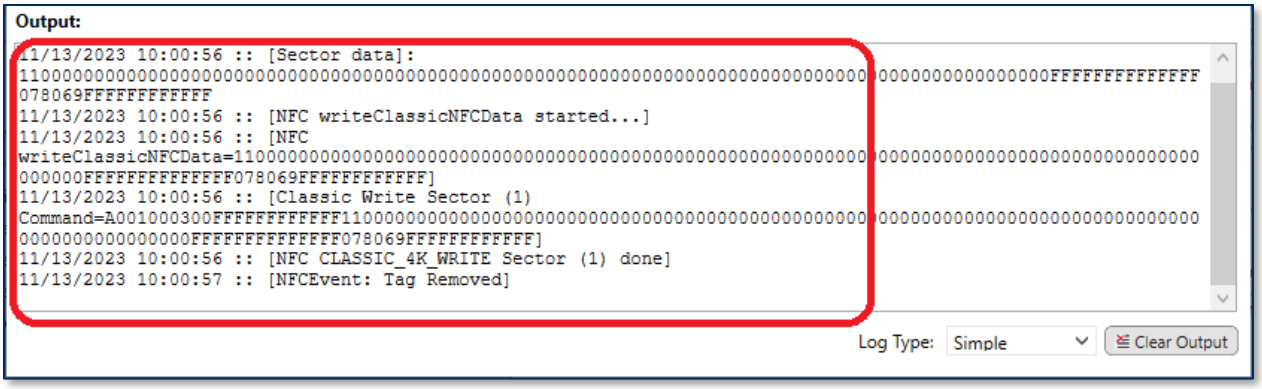
4) Edit the value of the Sector and then press the **Update Sector Data** button.



Details for modifying a Sector/Block

- Each Sector is composed of Blocks but are not shown as individual Blocks in this demo.
- Block updating must be its full length i.e. 16 byte block has to be 16 bytes.
- At Sector 0, Block 0 is reserved.
- Sector blocks vary by card and within a card. Some Sectors hold 4 Blocks, some 16 Blocks.
- The last Block of each Sector stores key data for accessing the Sector. It is best to not change Block 3 or Block 15 during testing of the demo.

5) At the Output log, wait until the writing operation is completed with a single beep sound. Scroll up to view the records written similar to as shown here.


Output:
11/13/2023 10:00:56 :: [Sector data]:
11000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000FFFFFFFFFFFFFF078069FFFFFFFFFFFF
11/13/2023 10:00:56 :: [NFC writeClassicNFCData started...]
11/13/2023 10:00:56 :: [NFC writeClassicNFCData=11000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000FFFFFFFFFFFFFF078069FFFFFFFFFFFF]
11/13/2023 10:00:56 :: [Classic Write Sector (1)
Command=A001000300FFFFFFFFFFFF11000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000FFFFFFFFFFFFFF078069FFFFFFFFFFFF]
11/13/2023 10:00:56 :: [NFC CLASSIC_4K_WRITE Sector (1) done]
11/13/2023 10:00:57 :: [NFCEvent: Tag Removed]
Log Type:
Simple
Clear Output

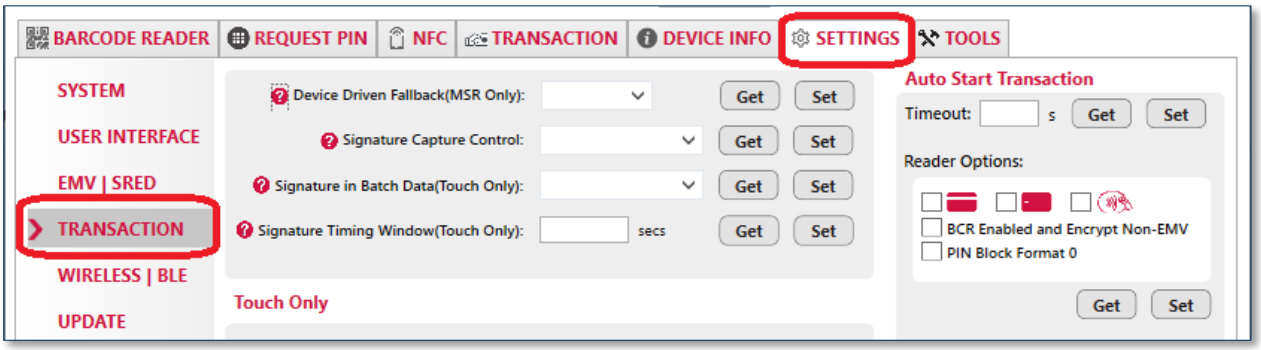
D

11 How to use Tip and Tax Demo

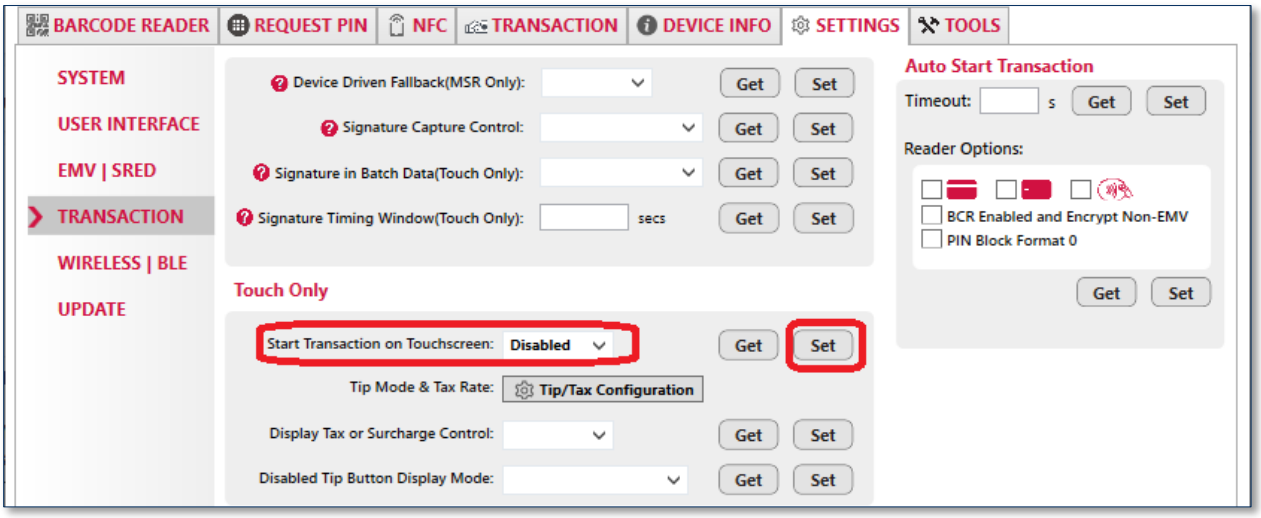
11.1 Show Tip and Tax from Host-Initiated transaction.

In Host-Initiated mode, the transaction is started from the app.

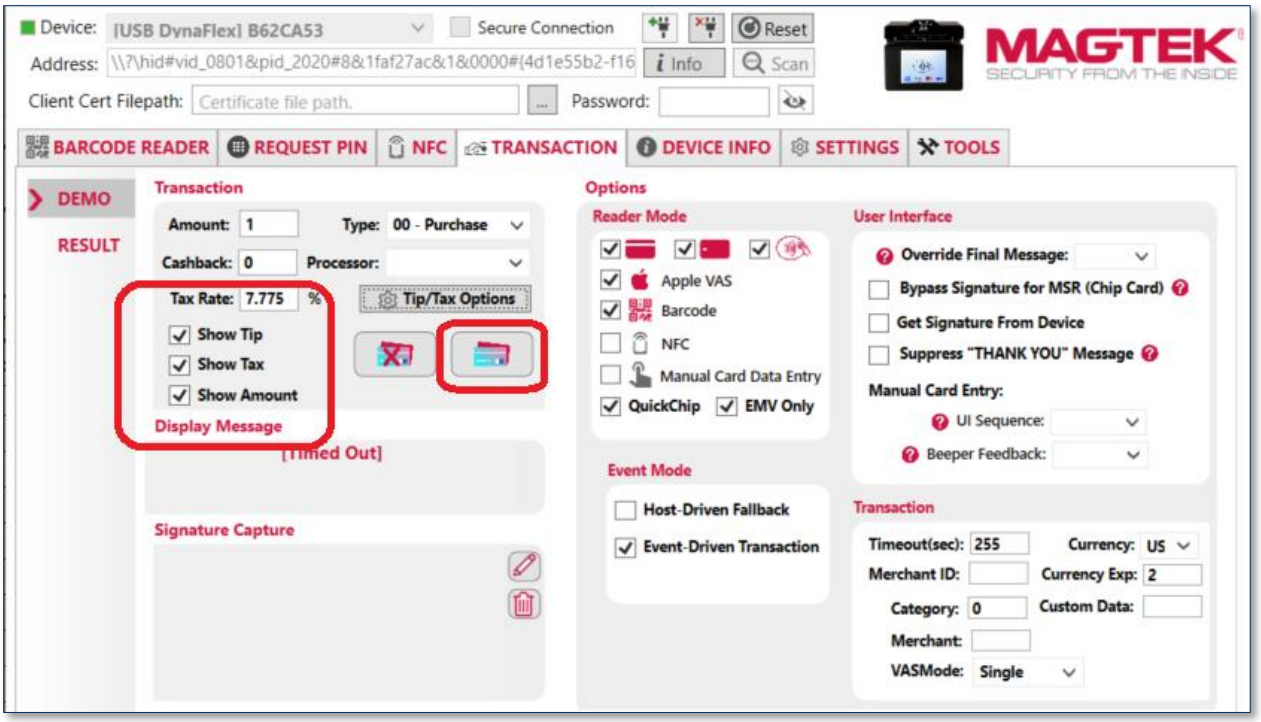
1) Open the **Settings** tab and select **Transaction**.



2) Under **Start Transaction on Touchscreen**, select **Disabled**, then press the **Set** button.



3) To perform transactions with Tip/Tax option displayed on the device screen, check **Show Tip**, **Show Tax** and **Show Amount**., and then press the **Start** button.



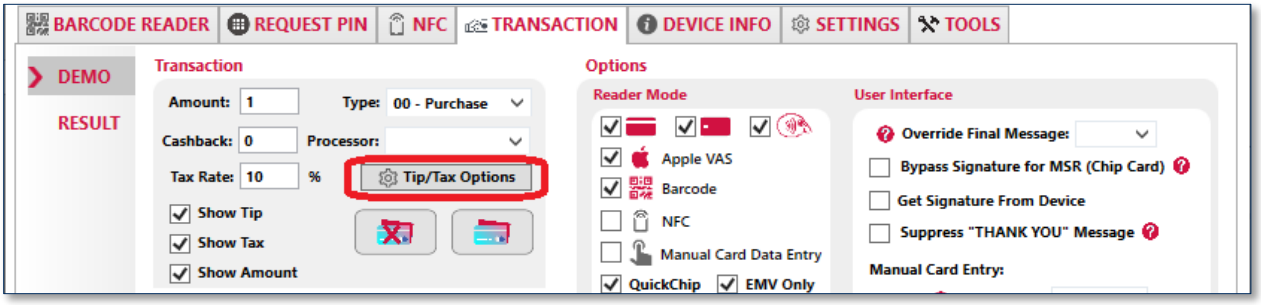
The device screen will prompt to select the tip amount.

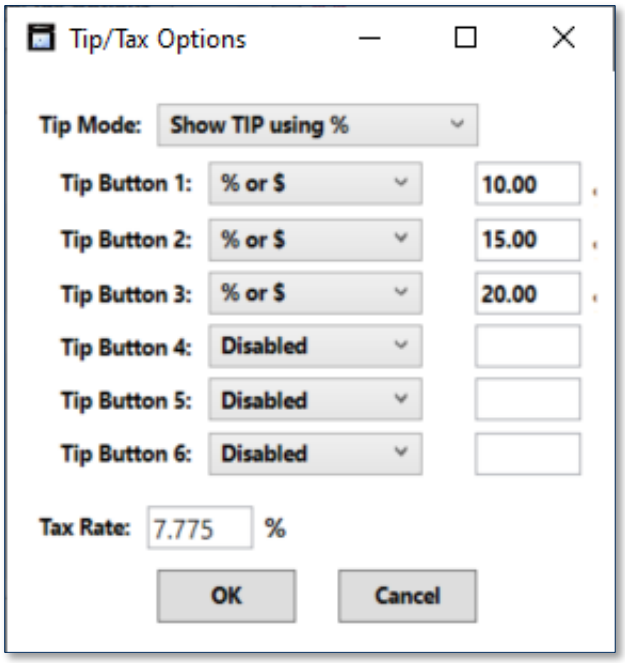
To enter an amount not shown, press **Custom** to enter the custom amount.

After select the amount, press the **Submit** button on the screen. After submitting, continue with the transaction by presenting the payment method. The Tip amount may be edited before presenting the payment method by pressing **Edit Tip** on the screen.

Customize Tip/Tax

Press the **Tip/Tax Options** buttons to customize the tip/tax.





- Tip Mode
  - **Show TIP using %** - Display as a percent at the start of the transaction.
  - **Show TIP using $** - Display as a dollar value at the start of the transaction.
  - **Show +TIP button using %** - Only display as a percent when the +TIP button is pressed on the screen. Present card is displayed first.
  - **Show +TIP button using $** - Only display as a dollar value when the +TIP button is pressed on the screen. Present card is displayed first.

- Tip Buttons 1 to 6
  - **% or $** - Display percent or dollar.
  - **Custom** - Allow custom tip to be entered.
  - **NO TIP** - Removes any tip applied.
  - **Disabled** - Disables the button.

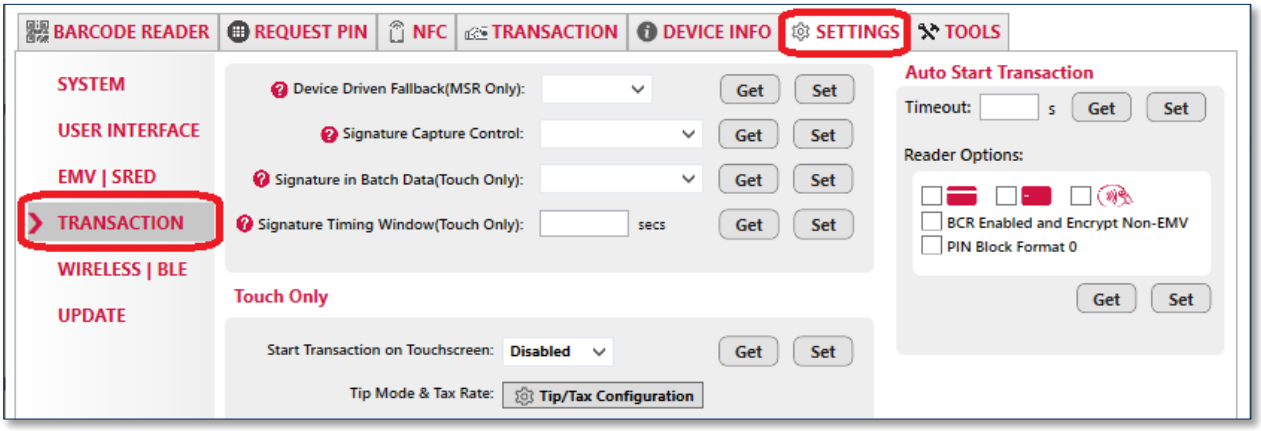
- Tax Rate – Tax rate calculated on the amount without tip.

11.2 Show Tip and Tax from Device-Initiated Transaction.

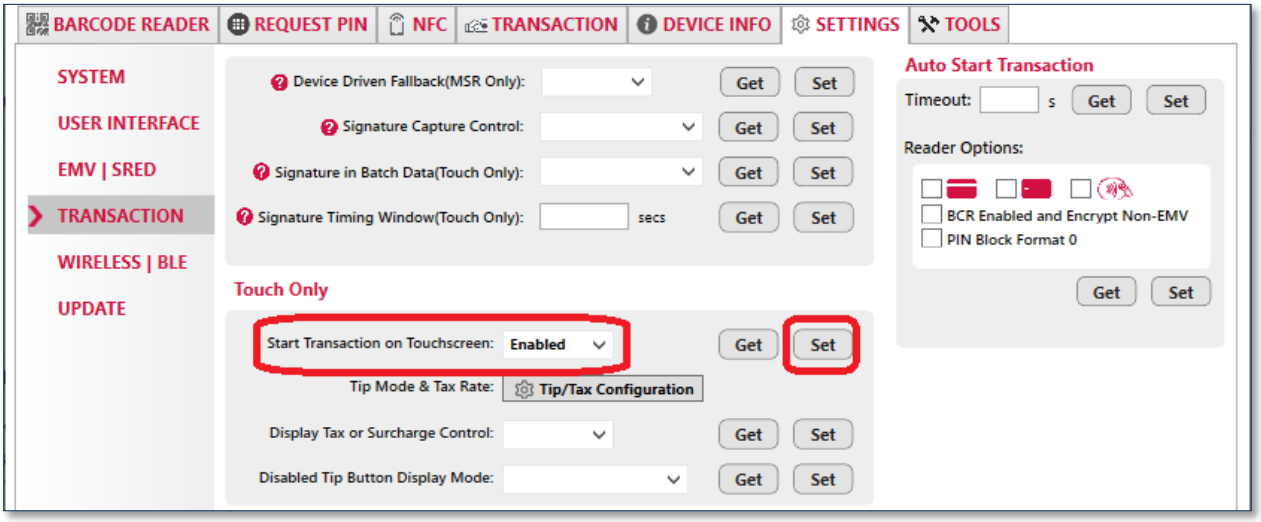
In Device-Initiated mode, the transaction is started from the device screen. The operator enters amounts. The app is notified of the start of the transaction and receives the transaction data.

To use this mode, please make sure the device is connected via WLAN. Please refer to section ***2.3 How to Connect Using the WLAN Connection*** to set up the device in WLAN mode.

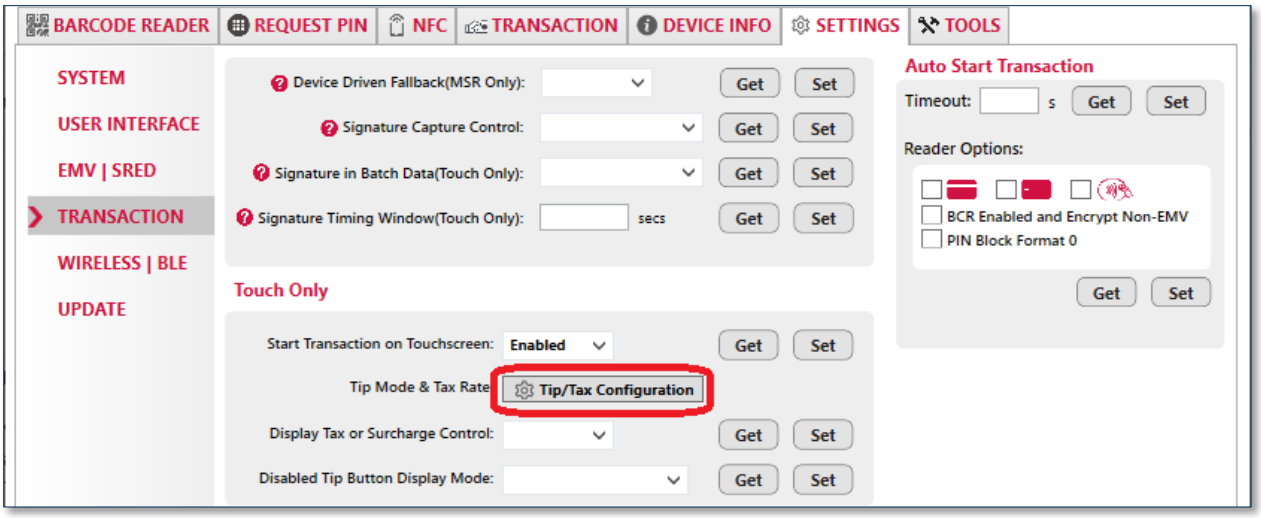
1) Open the **Settings** tab and select **Transaction**.



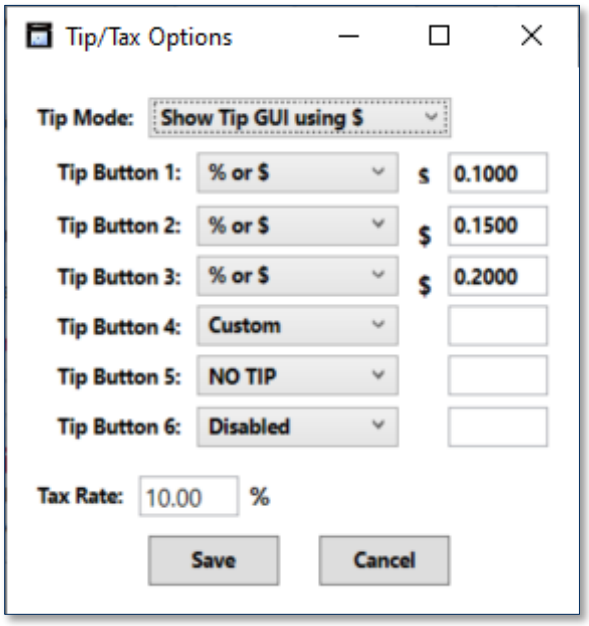
2) Under **Start Transaction on Touchscreen**, select **Enabled**, and then press the **Set** button.



3) Press the **Tip/Tax Configuration** button.



4) Select the desired **Tip Mode**, enter values for % or $, enter **Tax Rate**, and then press the **OK** button.



- Tip Mode
  - **Show TIP using %** - Display as a percent at the start of the transaction.
  - **Show TIP using $** - Display as a dollar value at the start of the transaction.
  - **Show +TIP button using %** - Only display as a percent when the +TIP button is pressed on the screen. Present card is displayed first.
  - **Show +TIP button using $** - Only display as a dollar value when the +TIP button is pressed on the screen. Present card is displayed first.

- Tip Buttons 1 to 6
  - **% or $** - Display percent or dollar.
  - **Custom** - Allow custom tip to be entered.

- **NO TIP** - Removes any tip applied.
- **Disabled** - Disables the button.

- Tax Rate – Tax rate calculated on the amount without tip.

5) On the device screen, press **Start Sale**, and then follow the on-screen instructions to complete the transaction.

12 Flexible UI Page

The following section is for displaying Flexible User Interface (UI) pages.

UI pages allow for interaction by selection of customized buttons, and display of images. UI pages are composed of Titles, Text lines, Buttons, Amount buttons, Images, and Functional buttons. Functional buttons are situated at the bottom of the screen. A host app sends the contents of: Text lines, Amount buttons, and Images, in real time to the device for display. However, for Titles, Buttons, and Functional buttons, the messages are pre-existing inside the device. Hence, a host app only sends the string ID number assigned to a specific text message. The ID and text messages are defined by a UI configuration file.

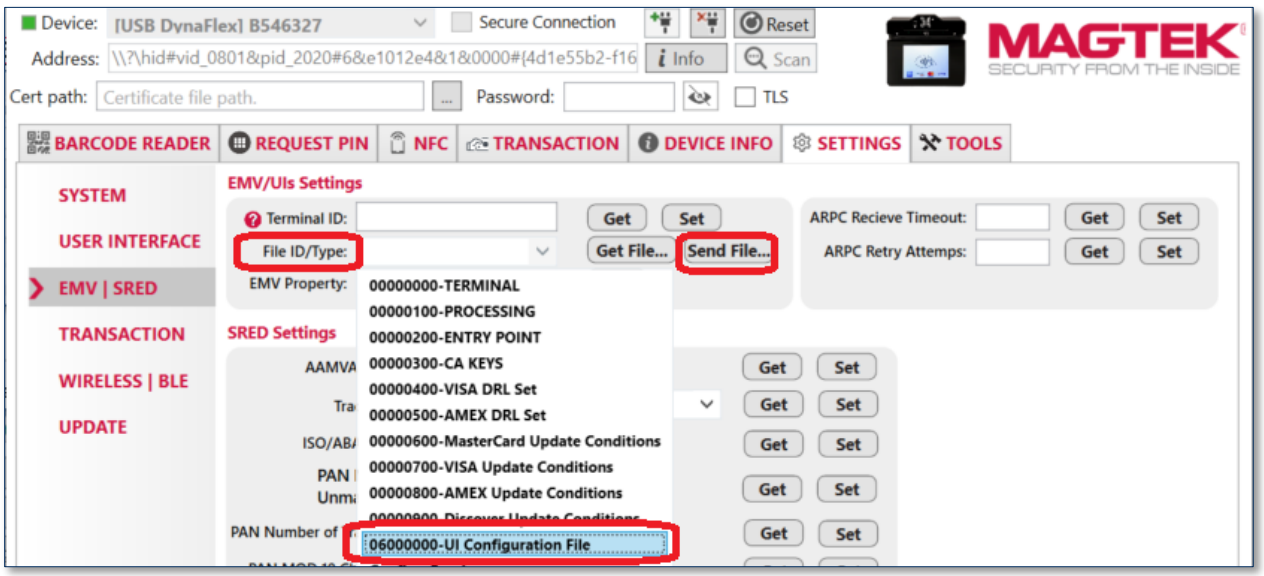
A UI configuration file may be configured by a customer, but ultimately is signed at MagTek. The device will only accept a signed UI configuration file.

12.1 UI Configuration File

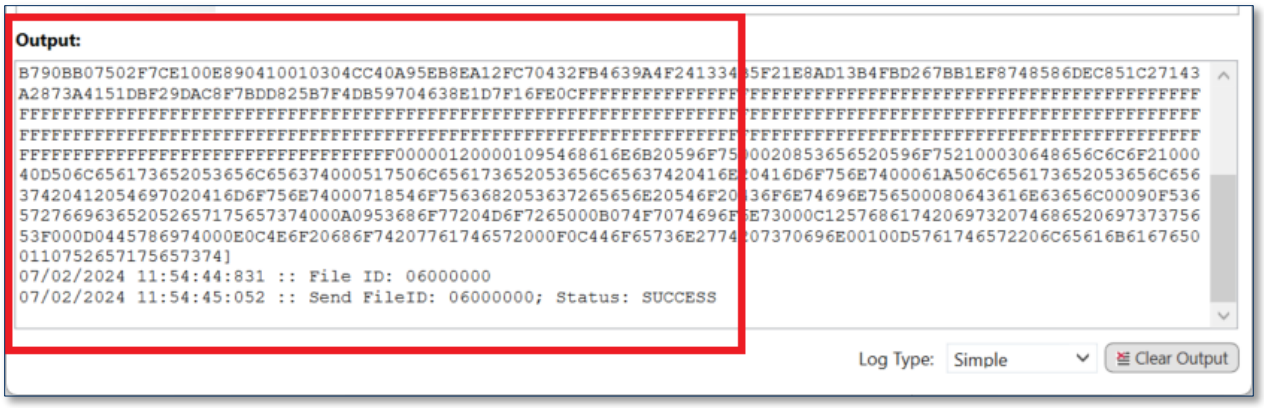
To send a UI Configuration file to the device, follow these steps.

1) Select the **Settings** tab and **EMV | SRED** menu. **File ID/Type**

2) At **File ID/Type**, select **06000000-UI Configuration File** and press the **Send File** button to browse for the UI Configuration file (.BIN) file.

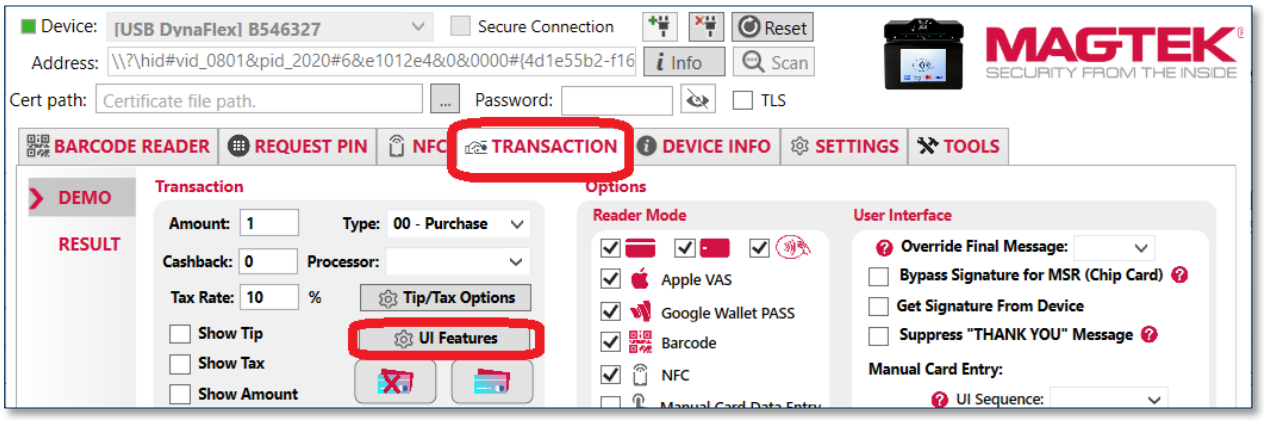


3) After a file is chosen, see the progress in the **Output** log. On completion, the status will show **SUCCESS** similarly as below.

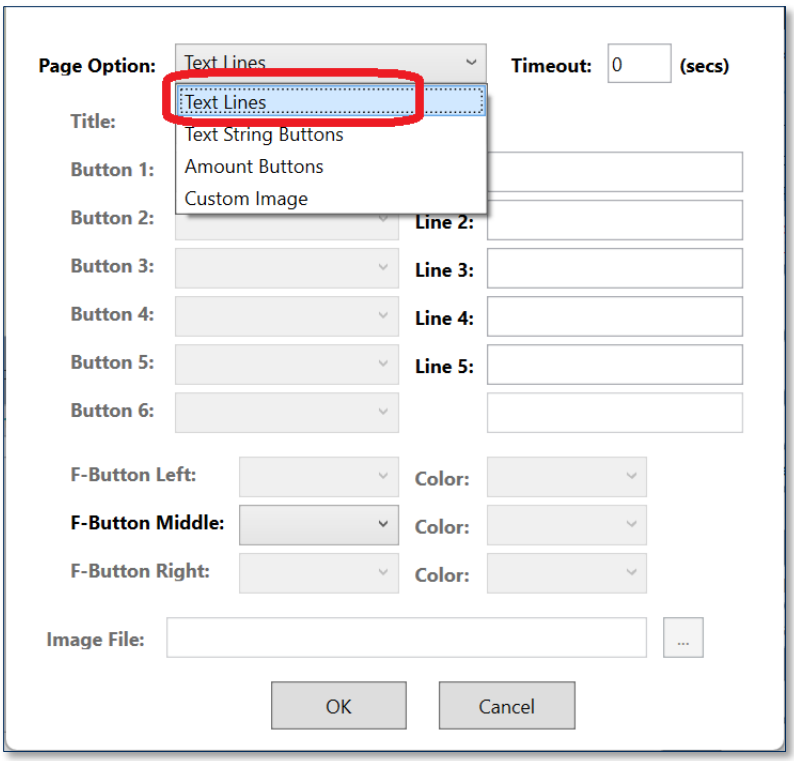


12.2 Text Page

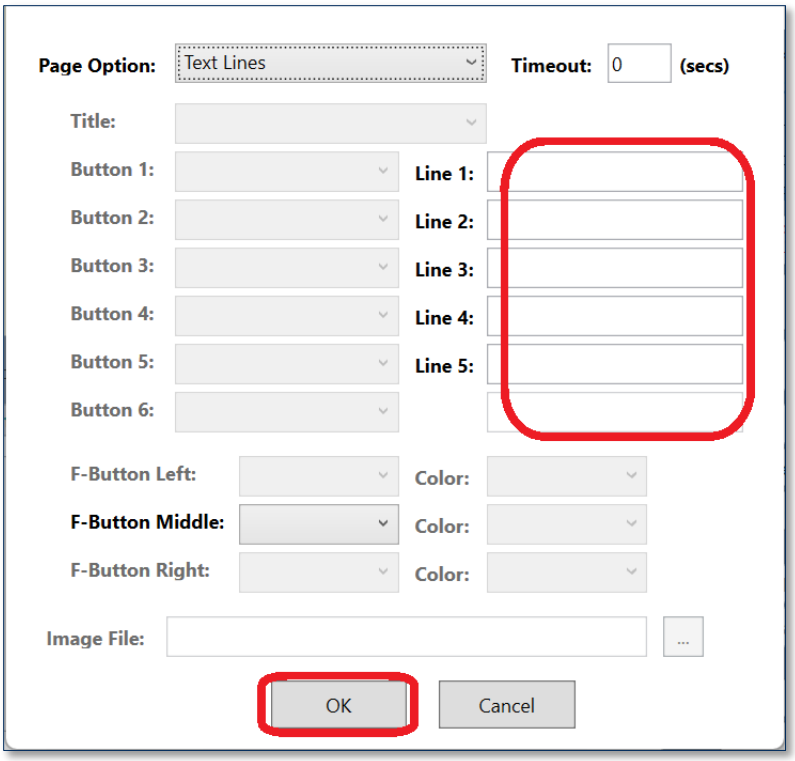
1) To display a multi Text line UI page on the device's screen, select the **TRANSACTION** tab, and press the **UI Features** button.



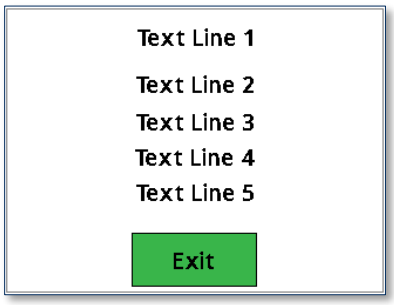
2) At **Page Option** list, select **Text Lines**.



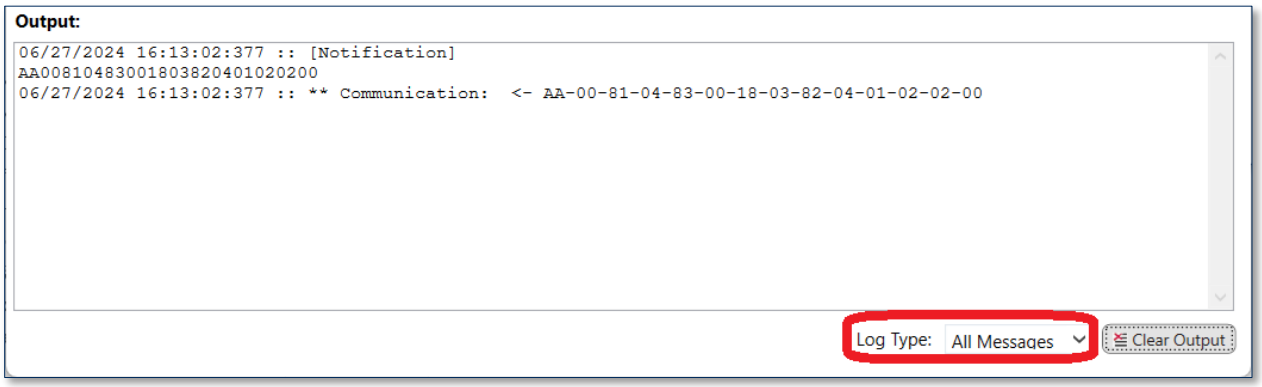
3) Enter from 1 to 5 lines of text to be displayed in each text box, and then press the **OK** button. Only 0 seconds (no timeout) is currently supported.



4) The UI page will be shown on the device's screen similarly as below.

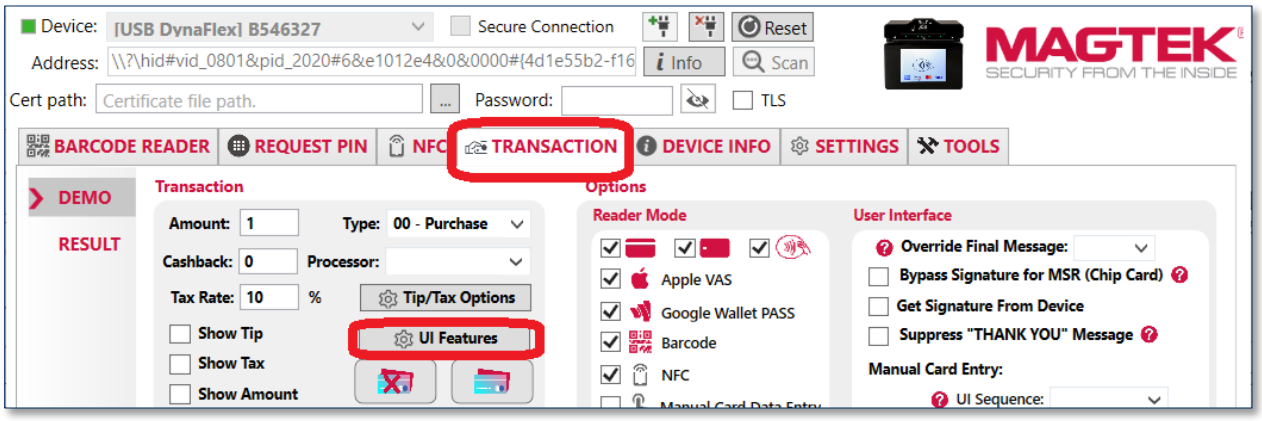


5) Each time a UI button is pressed on the screen, the device sends a notification similarly as shown below. Functional Middle button reports as 2 similarly as shown below. Text lines are not reported.

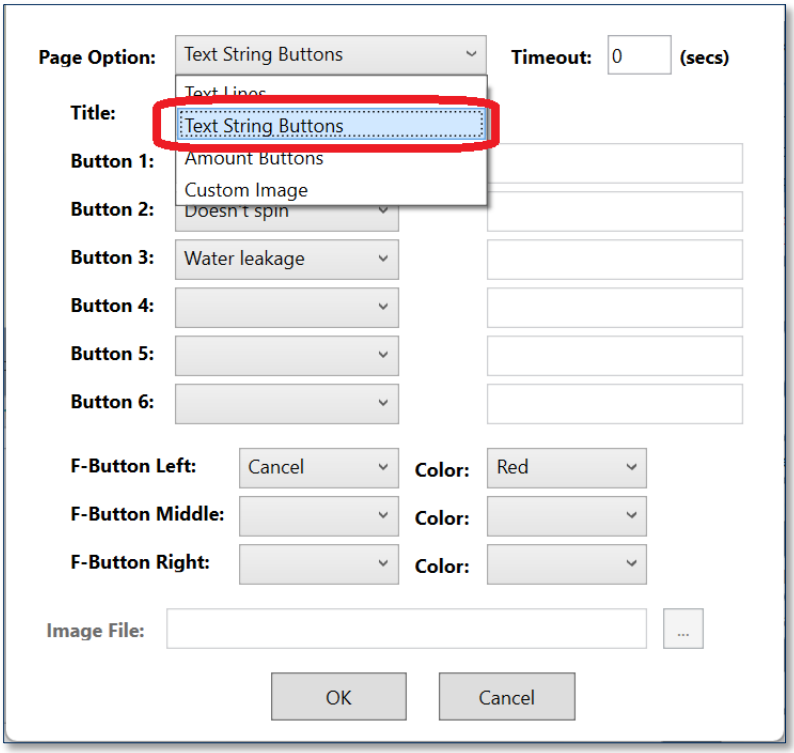


12.3 Buttons Page

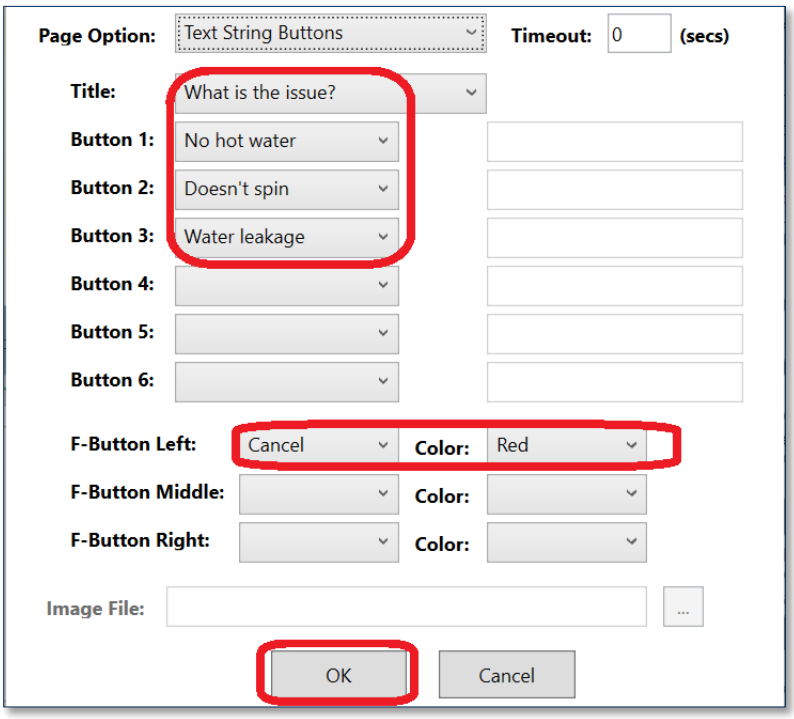
1) To display a Buttons UI page on the device's screen, select the **TRANSACTION** tab, and press the **UI Features** button.



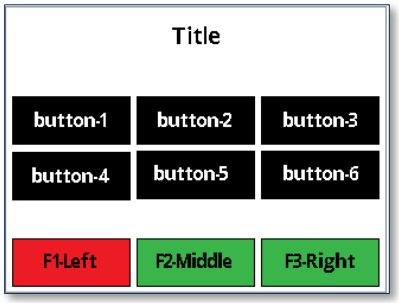
2) At **Page Option** list, select **Text String Buttons**.



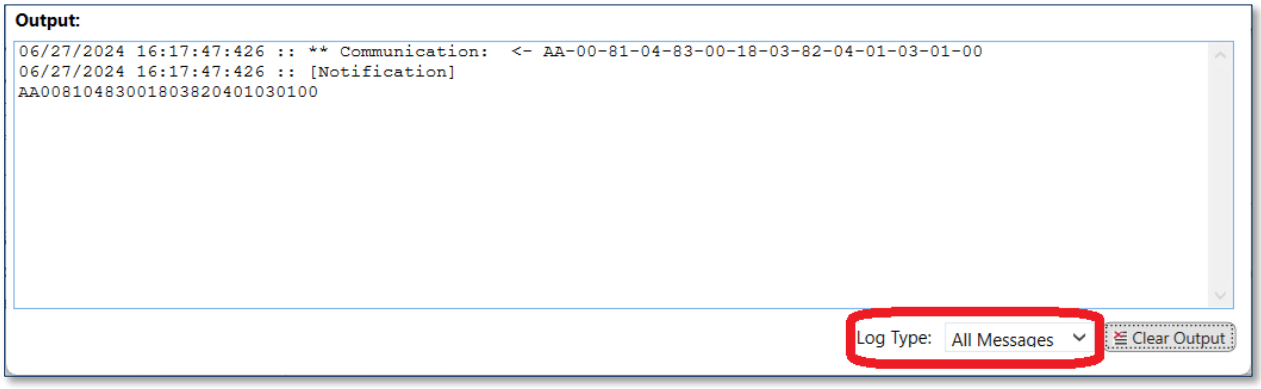
3) Select a message for **Title** and **Buttons**. For Functional buttons **F-Button**, select a message and a color of the button. After selections, press the **OK** button. Selections here are actually string IDs but are represented as text.



4) The UI page will be shown on the device's screen similarly as below.

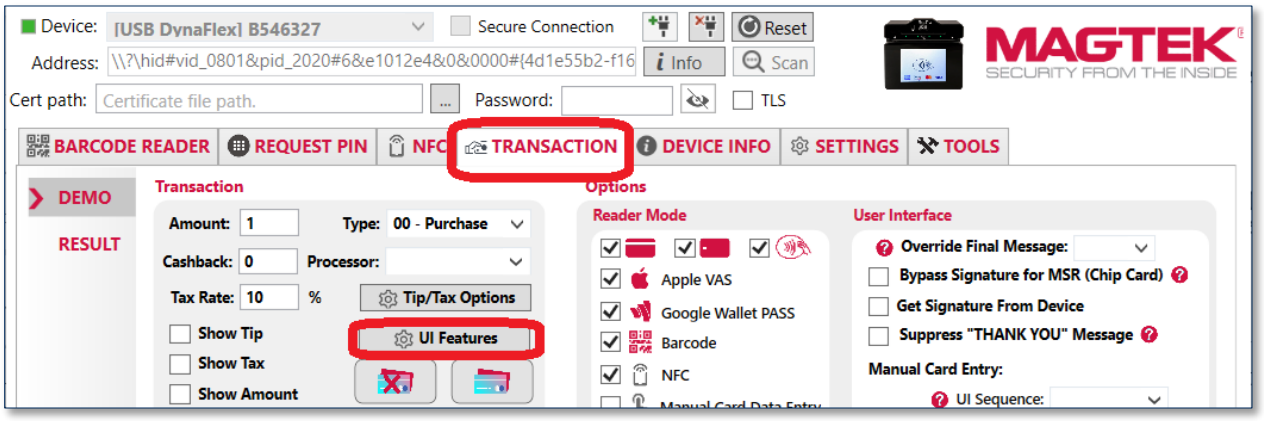


5) Each time a UI button is pressed on the screen, the device sends a notification similarly as shown below.

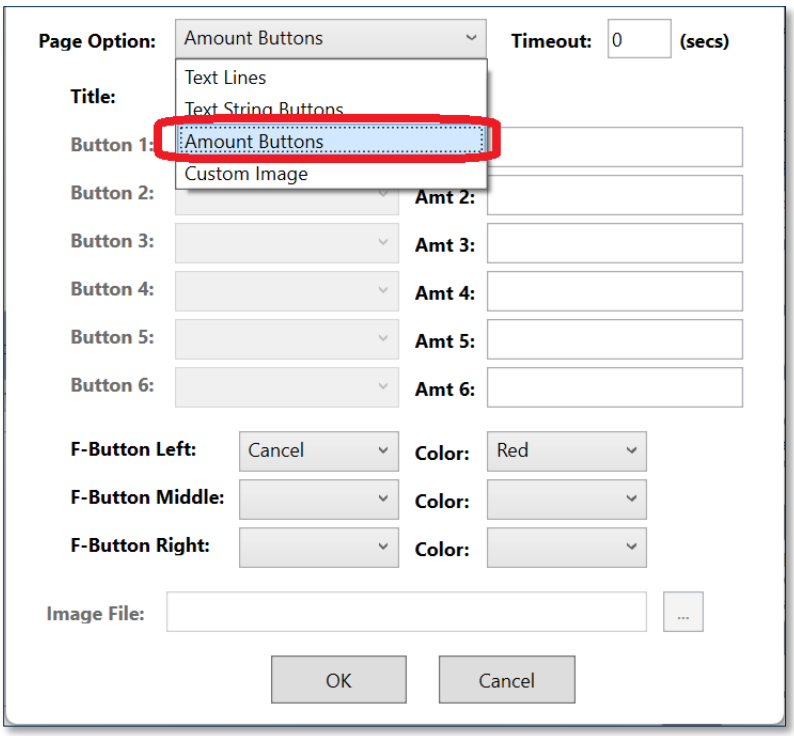


12.4 Amount Page

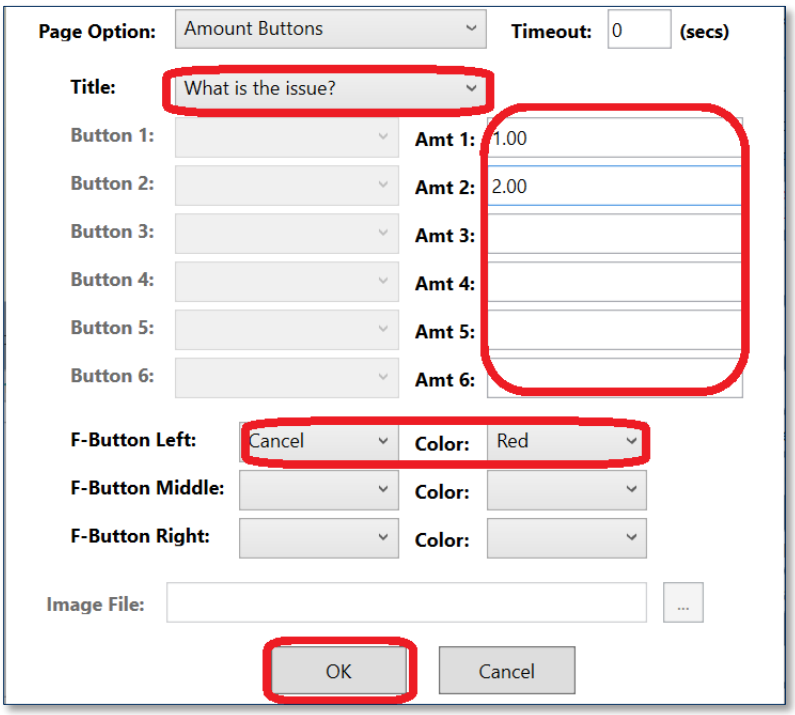
1) To display an Amount UI page on the device's screen, select the **TRANSACTION** tab, and press the **UI Features** button.



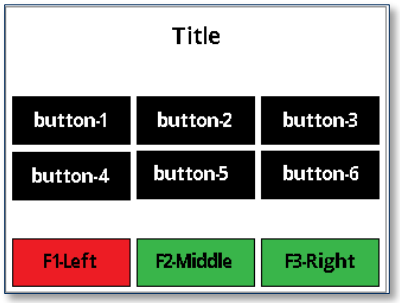
2) At **Page Option** list, select **Amount Buttons**.



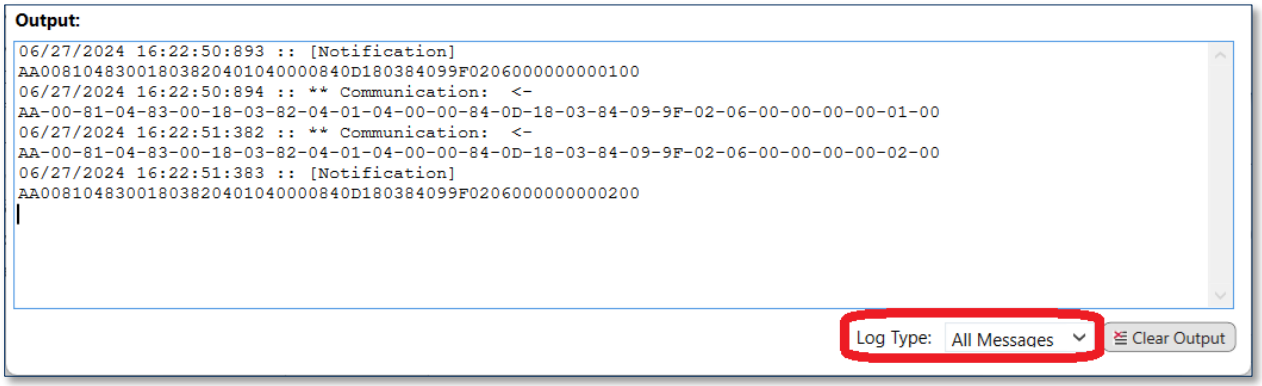
3) Select a message for **Title** and enter the dollar value in each text box for **Amt**. For Functional buttons **F-Button**, select a message and a color of the button. After selections, press the **OK** button. Here, the Title and Functional buttons are actually string IDs but are represented as text.



4) The UI page will be shown on the device's screen similarly as below.

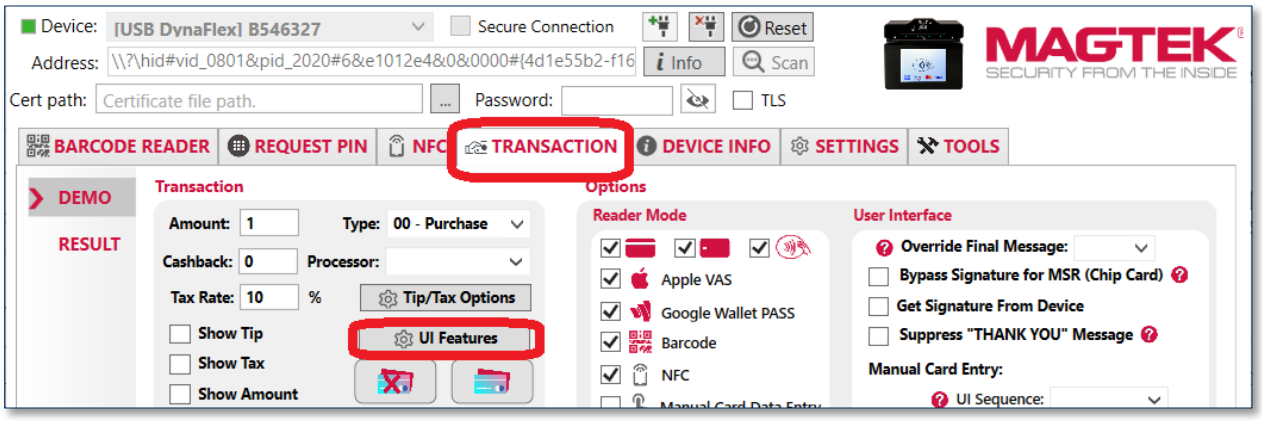


5) Each time a UI button is pressed on the screen, the device sends a notification similarly as shown below. Amount buttons report a value.

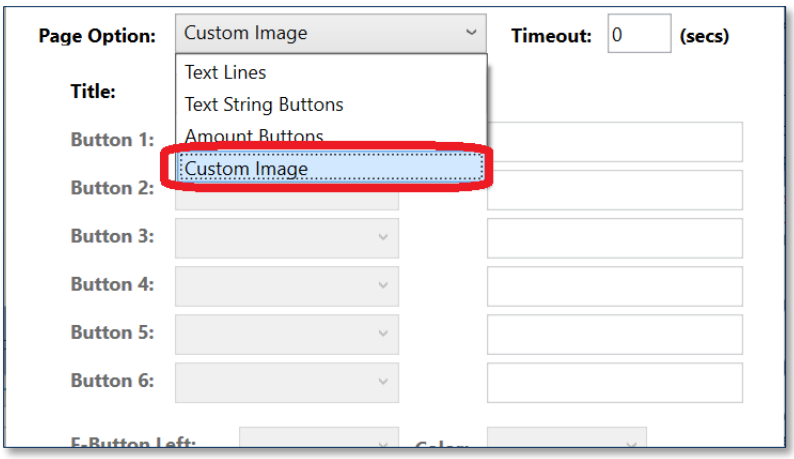


12.5 Image Page

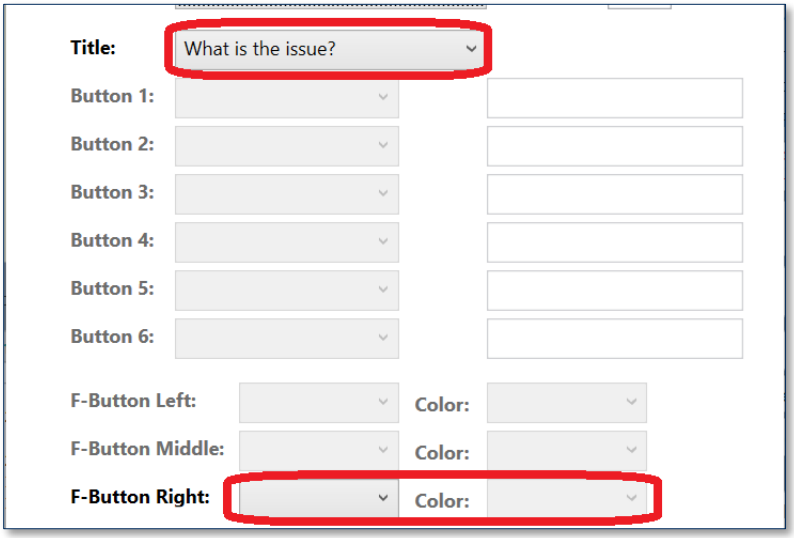
1) To display an Image UI page on the device's screen, select the **TRANSACTION** tab, and press the **UI Features** button.



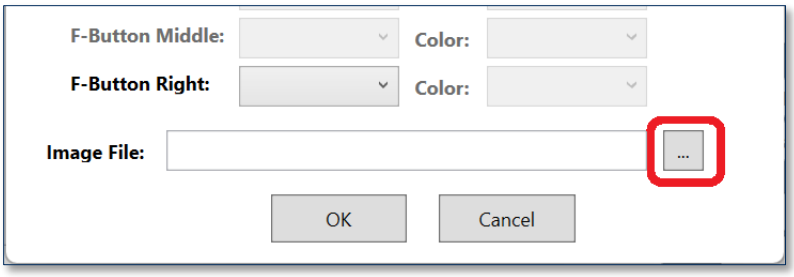
2) At **Page Option** list, select **Custom Image**.



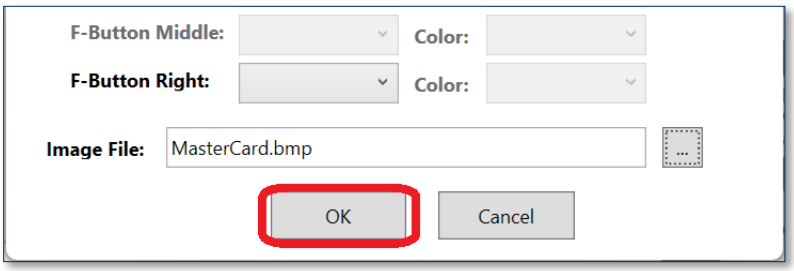
3) Select a **Title** and the **F-Button** option.



4) Press **...** to browse for the BMP image file.

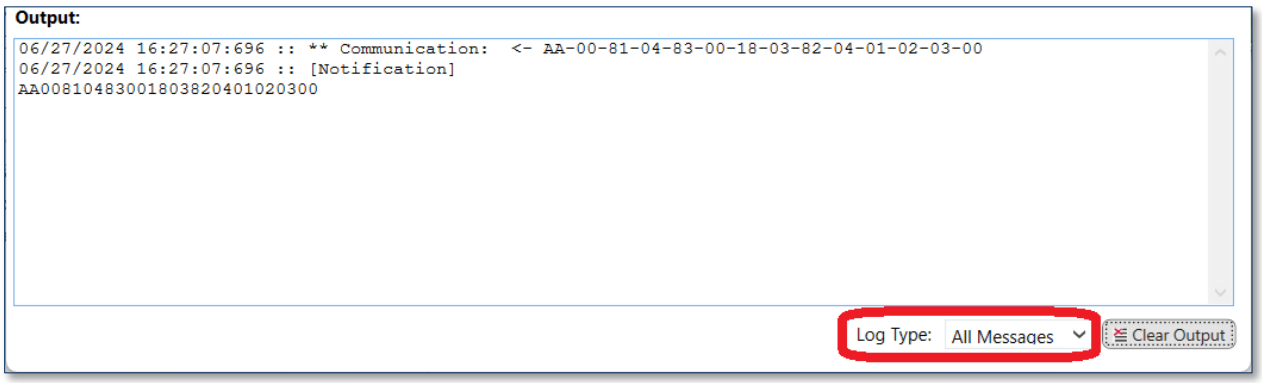


5) After an image file is chosen, press the **OK** button.



6) The UI page will be shown on the device's screen similarly as below.

7) Each time a UI button is pressed on the screen, the device sends a notification similarly as shown below. The Functional Right button reports as 3.



Appendix A Reserved