DynaFlex and DynaFlex Pro

Three-way Secure Card Reader Authenticators
Installation and Operation Manual

April 2020

Document Number:
D998200382-10

REGISTERED TO ISO 9001:2015

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.

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^{SM} 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.

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

Table 0-1 - Revisions

Rev Number	Date	Notes
10		Initial Release

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.

FCC INFORMATION

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Changes or modifications not expressly approved by MagTek could void the user's authority to operate this equipment.

CANADIAN DECLARATION OF CONFORMITY

This digital apparatus does not exceed the Class B limits for radio noise from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe B prescrites dans le Réglement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conformé à la norme NMB-003 du Canada.

INDUSTRY CANADA (IC) RSS

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) This device may not cause interference, and (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) L'appareil ne doit pas produire de brouillage, et (2) L'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

CUR/UR

This product is recognized per Underwriter Laboratories and Canadian Underwriter Laboratories 1950.

CE STANDARDS

Testing for compliance with CE requirements was performed by an independent laboratory. The unit under test was found compliant with standards established for Class B devices.

EU STATEMENT

Hereby, MagTek Inc. declares that the radio equipment types **Wideband Transmission System** (802.11 wireless and Bluetooth Low Energy), and **Non-Specific Short Range Device** (contactless) are in compliance with ***Directive 2014/53/EU***. The full text of the EU declarations of conformity is available at the following internet addresses:

- https://www.magtek.com/Content/DocumentationFiles/D998200238.pdf.
- https://www.magtek.com/Content/DocumentationFiles/D998200296.pdf

AUSTRALIA / NEW ZEALAND STATEMENT

Testing for compliance with AS/NZS standards was performed by a registered and accredited laboratory. The unit under test was found compliant with standards established under AS/NZS CISPR 32 (2013), AS/NZS 4268 Table 1, Row 59 DTS 2400-2483MHz SRD (802.11), and AS/NZS 4268 (2017) Table 1, Row 43 13.553-13.567MHz (contactless reader).

UL/CSA

This product is recognized per ***UL 60950-1, 2nd Edition, 2011-12-19*** (Information Technology Equipment - Safety - Part 1: General Requirements), ***CSA C22.2 No. 60950-1-07, 2nd Edition, 2011-12*** (Information Technology Equipment - Safety - Part 1: General Requirements).

ROHS STATEMENT

When ordered as RoHS compliant, this product meets the Electrical and Electronic Equipment (EEE) Reduction of Hazardous Substances (RoHS) European Directive 2002/95/EC. The marking is clearly recognizable, either as written words like “Pb-free,” “lead-free,” or as another clear symbol (Pb).

PCI STATEMENT

PCI Security Standards Council, LLC (“PCI SSC”) has approved this PIN Transaction Security Device to be in compliance with PCI SSC’s PIN Security Requirements.

When granted, PCI SSC approval is provided by PCI SSC to ensure certain security and operational characteristics important to the achievement of PCI SSC’s goals, but PCI SSC approval does not under any circumstances include any endorsement or warranty regarding the functionality, quality or performance of any particular product or service. PCI SSC does not warrant any products or services provided by third parties. PCI SSC approval does not under any circumstances include or imply any product warranties from PCI SSC, including, without limitation, any implied warranties of merchantability, fitness for purpose, or non-infringement, all of which are expressly disclaimed by PCI SSC. All rights and remedies regarding products and services which have received PCI SSC approval shall be provided by the party providing such products or services, and not by PCI SSC.

SAFETY

This product has been evaluated by multiple safety certification agencies, including Underwriters Laboratories (UL) and the United States Federal Communications Commission (FCC Class A and Class B), and is designed to protect both the user and the device. This document is written specifically to work in conjunction with these safety and integrity features to protect the user and the device. It is very important to follow all steps in the product documentation carefully, in the order in which they are described, and at the recommended times. Failure to do so could result in personal injury, and / or cause damage to the device, and / or void the product warranty.

SAFETY REQUIREMENTS

⚠ CAUTION

Never do any of the following:

- DO NOT use a ground adapter plug to connect equipment to a power socket-outlet that lacks a ground connection terminal.
- DO NOT attempt any maintenance function that is not specifically described in this manual or in other ExpressCard 3000 instructional documents published by MagTek.
- DO NOT remove any of the covers or guards that are fastened with screws. There are no user-serviceable areas within these covers.
- DO NOT override or “cheat” electrical or mechanical interlock devices.
- DO NOT use EC3000 supplies or cleaning materials for other than their intended purposes.
- DO NOT operate the equipment if you or anyone else have noticed unusual noises or odors.

Consider the following before operating the ExpressCard 3000:

- Connect the EC3000 to a properly grounded AC power socket-outlet. If in doubt, have the socket-outlet checked by a qualified electrician. Improper connection of the device’s grounding conductor creates a risk of electric shock.
- Place the EC3000 on a solid surface that can safely support the device’s weight plus the weight of a person leaning against it (such as a service technician).
- Be careful when moving or relocating the device. Use proper lifting techniques.
- Use materials and supplies specifically designed for MagTek devices. Using unsuitable materials may result in poor performance, and in some cases may be hazardous.

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.

Table of Contents

1 Introduction

1.1 About DynaPro Go

MagTek's DynaPro Go is a handheld secure PIN entry device that is ideal for credit, prepaid, gift, and debit cards for mobile point of sale applications where you need unmatched convenience and security. Reduce your interchange rates, reduce chargebacks, and increase your customer satisfaction and sales with DynaPro Go.

DynaPro Go provides a mobile solution that is convenient without sacrificing security. Bring multiple low-cost, yet secure point-of-service terminals directly to the customer wherever and whenever they are ready to buy. The magnetic stripe card reader is capable of reading any ISO or AAMVA encoded magnetic stripe data, the contact chip card slot is located in the bottom of the device ready to read contact chip cards (ICC), and the contactless reader is directly behind the LCD display. The backlit keypad provides a better user experience when used in low-light settings such as taxi cabs.

DynaPro Go meets and exceeds PCI PTS 4.x, SRED security requirements for PEDs. The MagTek MagneSafe Security Architecture (MSA), EMV chip card technology, and NFC capability exceed current PCI requirements. The enclosure and associated electronics form a Tamper Resistant Security Module (TRSM) where attempts to penetrate or modify the device cause all keys to be cleared and/or stop the device from functioning.

DynaPro Go product features include:

- PCI PTS 4.x, SRED
- Meets EMV Level 1 and Level 2 requirements
- Triple DES encryption
- DUKPT key management
- Device/mutual authentication
- Card data authentication
- Tokenization and masked data
- USB and 802.11 wireless connection or USB and Bluetooth LE connection available
- Ergonomic and ruggedized design
- Secured by MagneSafe Security Architecture
- MagnePrint card authentication
- Generates dynamic payment card data with each swipe
- Reads ANSI/ISO/AAMVA cards plus custom formats
- EMV chip card reader
- Fast and reliable magnetic stripe reading
- LCD graphical display
- Backlit keypad
- Reads up to 3 tracks of card data
- Bi-directional read

Table 1-1 - Available Models and Options

Part No.	Description	Color	Mounting	Display	Connection(s)
21078007	DYNAFLEX, PCI, NO DISPLAY, GRAY, USB	Gray	Countertop Handheld Other	None	USB-C
21078008	DYNAFLEX, PCI, NO DISPLAY, GRAY, BLUETOOTH LE	Gray	Countertop Handheld Other	None	USB-C Bluetooth LE
21078009	DYNAFLEX PRO, PCI, TOUCHSCREEN DISPLAY, GRAY, USB	Gray	Countertop Handheld Other	Touchscreen	USB-C
21078010	DYNAFLEX PRO, PCI, TOUCHSCREEN DISPLAY, GRAY, BLUETOOTH LE	Gray	Countertop Handheld Other	Touchscreen	USB-C Bluetooth LE
21078011	DYNAFLEX PRO, PCI, TOUCHSCREEN DISPLAY, GRAY, 802.11 WIRELESS	Gray	Countertop Handheld Other	Touchscreen	USB-C 802.11 Wireless
21078012	DYNAFLEX PRO, PCI, TOUCHSCREEN DISPLAY, GRAY, ETHERNET	Gray	Countertop Handheld Other	Touchscreen	USB-C Ethernet

1.2 Protection for All Points Within the Payment Infrastructure

DynaPro Go delivers industry best practices for data protection, using **triple DES encryption (TDEA/3DES)** and **derived unique key per transaction (DUKPT)** key management. PIN, magnetic stripe, chip card (contact/contactless), NFC, and manually keyed data are encrypted as soon as they are entered into the device. Using proven and tested industry standards gives merchants, processors, issuers, and acquirers the flexibility to outsource or manage decryption services themselves, avoiding the risk imposed by unproven, proprietary encryption algorithms.

When used with **Magensa Solutions** and the **MagneSafe Security Architecture**, the device delivers a layered approach to transaction security that combines encryption, tokenization, authentication, and dynamic data to protect card data. The **MagnePrint® card authentication service** can identify and detect counterfeit magnetic stripe ATM, debit, credit, and gift cards, and render them useless. This state-of-the-art security is designed to identify and prevent fraud before it happens.

The card reader is capable of reading any ISO or AAMVA encoded magnetic stripe data, and includes a contact chip card (ICC) reader on the front of the device under the keypad and a contactless reader behind the LCD display.

1.3 Security and Ease of Integration by Design

DynaPro Go is a durable device designed for easy connection and integration. MagTek is your partner in development, and provides a comprehensive platform of drivers, APIs, and Software Development Kits (SDKs). The SDKs include tools, documentation, and sample code for developing applications on a variety of platforms with different connection options for fast development and easy integration.

DynaPro Go interfaces through standard micro-USB cabling to recharge the battery and to perform synchronization with compliant hosts. Depending on the model, it can also connect wirelessly via a Bluetooth LE connection or via TCP/IP over 802.11 wireless.

1.4 Remote Services

MagTek's secure remote services include key injection and device configuration. These services are compliant with PCI P2PE environments, and eliminate the need for merchants to manage sensitive information such as encryption keys or device configuration settings. This allows the upgrade of keys or device security settings throughout the life of the device in the field.

1.5 Tamper Responsiveness

DynaPro Go's enclosure and its associated electronics have been designed to form a **Tamper-Responsive, Tamper-Evident Secure Cryptographic Device (SCD)**. The covers are securely attached and incorporate sensing circuits to detect any attempts to open the device. Internal spaces within DynaPro Go have been minimized to reduce the possibility of unauthorized modifications.

In addition, any attempt to penetrate or modify the device electronically will cause the device to permanently erase its stored encryption keys, after which the device will cease to function.

1.6 Liquid Crystal Display

The Liquid Crystal Display (LCD) is a backlit 2.4 inch 320x240 pixel QVGA color TFT display with a contactless card reader behind it for "tap the screen" contactless function. The display can either adapt its brightness based on ambient lighting, or stay at a pre-set brightness level. The display shows pre-programmed static and animated messages, including vertical scrolling for longer prompt lists, and animations on the **Swipe Card** and **Insert Card** screens.

1.7 10-Digit Backlit Numeric Keypad With Function Keys

The numeric keypad has well-contoured keys with tactile feedback for convenient entry of PINs or other data. During normal operation, cardholders use the keypad to securely enter PINs and other numeric data (see **Figure 1-1** on page **18**). An audible tone provides feedback when pressing keys, and a backlight makes data entry easy even in low light conditions. The keypad includes additional function keys cardholders may press during a transaction:

- Cardholders can press the green **ENTER** ("OK") key to indicate they have finished their input.
- Cardholders can press the red **CANCEL** ("X") key to halt the current operation. Depending on the context, it may cancel the entire transaction.
- When presented with on-screen selection options, cardholders can press the **Left Function Key**, **Middle Function Key**, or **Right Function Key** to select the desired response.

1.8 Low-Power Standby Modes

To conserve battery power, DynaPro Go enters a low-power mode or powers off in response to a variety of events, including screen timeouts ("Powered Off Mode"), USB Suspend directives from a connected USB host, critically low battery power, and periodic maintenance resets. Details about how DynaPro Go manages and conserves battery power can be found in section **6.6 Power Management**.

1.9 Major Components

The major components of DynaFlex are shown in **Figure 1-1**. In addition to the components shown, the device has a **tamper trigger** recessed in the bottom that is intended for manufacturer use only.

⚠ CAUTION

Do not insert anything into the tamper trigger hole! Doing so will erase all injected keys; the device will stop functioning, and will have to be returned to the manufacturer for re-configuration.

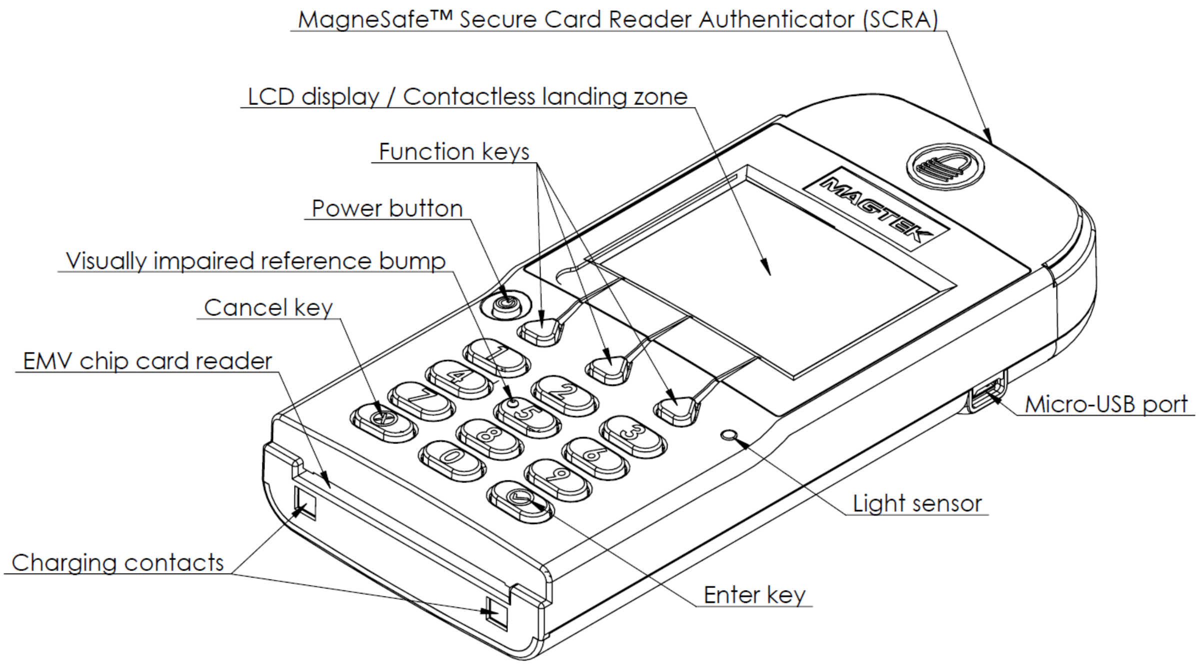

MagneSafe™ Secure Card Reader Authenticator (SCRA)
LCD display / Contactless landing zone
Function keys
Power button
Visually impaired reference bump
Cancel key
EMV chip card reader
Micro-USB port
Light sensor
Charging contacts
Enter key
MAGTEK

Figure 1-1 – DynaPro Go Major Components

1.10 About Terminology

In this document, DynaFlex is referred to as the **device**. It is designed to be connected to a **host**, which is a piece of general-purpose electronic equipment which can send commands and data to, and receive data from, the device. Host types include PC and Mac computers/laptops, tablets, and smartphones. Generally, the host must have **software** installed that communicates with the device and is capable of processing transactions. During a transaction, the host and its software interact with the **operator**, such as a customer service representative, while the device interacts with the **cardholder** (even if the cardholder is using a virtual representation of the card account, such as a smartphone).

2 Planning and Preparation

The guidelines in the following sections are intended to help management and system administrators to plan for the physical and network requirements of deploying and using the DynaFlex family of products, referred to here for brevity as “DynaFlex.” The most effective way to ensure smooth deployment of a solution is to consider these factors before receiving the device.

2.1 Logistical Planning

- Determine what type of **host** DynaFlex will connect to. For a list of supported device types and operating systems, see **Error! Reference source not found. Error! Reference source not found.**. When planning, be sure to include any additional support or devices required by the host and DynaFlex, such as physical locations, mounting, power connections, and charging cradles.
- Determine what **connection** the host will use to communicate with the device. Depending on the device model (see **Table 1-1** in section **1.1 About DynaPro Go**), the connection can be USB, Bluetooth LE, or a TCP/IP network that is equipped with 802.11 wireless or Ethernet. If the host will use the Bluetooth LE connection, make sure the host’s hardware and operating system support **Bluetooth LE Secure Connections**, which were introduced in the ***Bluetooth Core Specification version 4.2***.
- Determine what **software** will be installed on the host and how it will be configured. Software can include operating system, transaction processing software, security software, and so on. If teams other than the software development team will be involved in preliminary device testing, MagTek recommends the solution development team provide a smoke test harness early in the development process to allow basic testing (for example, wireless range testing). In addition, be sure to plan for any additional support required by the software, such as software licenses and network connections. Information about software is provided in section **4.2 About Host** Software.
- Configure the host software to select which combinations of magnetic stripe swipe, EMV contact card insertion, contactless payment tap, and/or manual entry the host will direct the device to accept (see section **6.9 Card Reading**). This decision may differ based on location, situation, and other factors, or may be uniform across all transactions and devices and hosts you are deploying.
- Determine how DynaPro Go will be physically **presented** to the cardholder.
- Select which **connection type** the solution will use. Available connection types include USB, Bluetooth LE, and TCP/IP over 802.11 wireless. Only one connection type can be active at a time. The connection types available in each model are listed in **Table 1-1 - Available Models and Options** on page **15**.
- Determine how DynaPro Go should be **configured**, and specify that configuration when ordering the device. For example:
  - For solutions that use 802.11 wireless, determine whether the device should be **Always Listening** for wireless messages from the host, or creating **Device-Initiated** connections on demand. This will generally depend on whether the solution calls for remote activation of the host from the device, such as table service / line-busting solutions.
  - For solutions that use 802.11 wireless, determine whether the device and host will have their connection secured by TLS. MagTek strongly recommends enabling TLS.
  - Determine whether the LCD display backlight should operate in **Manual** mode (constant brightness) or **Auto** mode (adaptive to ambient light).
- Select and configure a secure workstation advanced operators will use to configure and update the device. The workstation must be configured as follows:
  - Available USB port.

    - A secure means of obtaining files, either via the network (such as SFTP) or via removable media, such as USB flash drives. This is required for certificate setup, installing software tools, copying firmware files, etc.
    - ***99510127 DYNAPRO/DYNAPRO GO/DYNAPRO MINI WINDOWS SDK INSTALL (EXE)*** installed. This software includes the ***MagTek PCI PED Host App Simulator*** tool advanced operators use to configure the device.
- Determine the final set of tools advanced operators will use to configure and update the device. This documentation uses the ***MagTek PCI PED Host App Simulator*** as an example for configuring the device; it can be used for initial pre-deployment testing and development, and as sample code showing how to communicate with the device, but the full solution may call for customized, solution-specific software for configuring the device and updating firmware.
- Determine the **charging schedule(s) and location(s)**. For example, high-traffic mission-critical solutions may benefit from keeping multiple devices charging for fast swap-out. Charging cradles and accessories are available directly from MagTek. Make sure there is an adequate number of USB wall chargers and / or USB ports available for the number of devices you are charging together, and make sure the electrical socket-outlet at a given charging location can support the total load. Solutions using large numbers of devices may benefit from using a large-scale universal USB charger / hub. Details about charging are provided in section **Error! Reference source not found. Error! Reference source not found.**. Details about maximum power consumption are provided in **Error! Reference source not found. Error! Reference source not found.**.
- Determine how to **inspect** devices upon arrival, upon installation, and periodically during live usage, to ensure malicious individuals have not tampered with them. Details about inspection are provided in section **4.1 About Inspection**.
- Develop procedures for maintaining the device(s). Detailed guidance is provided in section **6.12 How to Enter Passcodes**.
- Determine how to **train** operators. Training may include material from section 5 **Configuration** and section 6 **Operation**.
- Review the device's PCI **Security Policy**, posted to the PCI web site www.pcisecuritystandards.org under **Approved PIN Transaction Security (PTS) Devices**, for additional information about using the device securely.

2.2 Network Planning

If DynaPro Go will communicate with the host via TCP/IP and an 802.11 wireless access point, network administrators should do the following before deployment:

1) If the device will have TLS enabled (see section **2.1 Logistical Planning**):
    a) Coordinate with your sales representative to obtain the **certificate chain** that must be installed on the host to enable TLS communication with the device. The certificate chain provided by MagTek contains a set of SHA-256 signed 2048-bit RSA certificates and 2048-bit RSA keys, which provides a balance between security and performance.
    b) Make sure the host supports at least one of the cipher suites listed in **Table 2-1**. The device will not negotiate any ciphers not listed there. The table lists ciphers in descending order of cipher strength; MagTek recommends the host should have the strongest available cipher enabled. By default, the device comes with a SHA-256 signed 2048-bit RSA certificate and ECC SECP256R1 certificate installed, which support all of the listed ciphers.
2) Determine how the **IP addresses** of all DynaPro Go devices and the host will be allocated, and plan a way to share the plan with the advanced operators who will be configuring devices.
3) The device configuration supports connection to only one access point. Make sure there is adequate **signal strength** between the access point and all locations where the device will operate wirelessly.
4) The device supports WPA Personal wireless security. Make sure the access point is configured to support one of **WPA2-PSK (TKIP)**, **WPA2-PSK (AES)**, or **WPA2-PSK (TKIP/AES)**. MagTek recommends using **WPA2-PSK (AES)**.
5) Plan a way for the access point **SSID** and **passcode** to be available to the advanced operator who will be configuring devices.
6) Determine whether to use **MAC filtering** on the access point and plan a way for device MACs to be added to the list.
7) If the device and host will use **static IP addresses**, allocate those addresses and determine what Gateway and Subnet Mask the devices should use.
8) Determine whether the solution will use **IP addresses** or **DNS names** for the host and the device. Note that on some operating systems, the TLS implementation may *require* the host to connect to the device by DNS name, or the TLS handshake may fail to authenticate the device because of a naming mismatch between the DNS name and the Common Name (CN) or Alternate Name embedded in the Device TLS Certificate.
9) Determine what **ports** the device and host will use to communicate, and make sure the required **protocols** are supported. See **Table 2-2 - Protocols and Ports**.
10) DynaPro Go does not require an Internet gateway.

Table 2-1 - Supported TLS Cipher Suites

Supported TLS Cipher Suites
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA

Table 2-2 - Protocols and Ports

Protocol	Default Port
ARP	N/A
RARP	N/A
DHCP Client	Standard (UDP out, bind to 67/68 on server)
DNS Client (Only when using Device Initiated mode)	Standard (UDP out, bind to 53 on server)
TCP outbound requests to host (Only when using Device Initiated mode)	Must be specified and configured
TCP Inbound requests from host	TCP Port 26 (configurable)
IGMP	N/A
IPv4	N/A
UDP	N/A
ICMP	N/A
Gedday DNS Service Discovery (Only when using Device Initiated mode)	53

3 Handling and Storage

⚠CAUTION

Proper handling of the device throughout delivery, assembly, shipping, installation, usage, and maintenance is very important. Not following the guidelines in this document could damage the device, render it inoperable, and/or violate the conditions of the warranty.

3.1 Handling to Avoid Damage

Upon receiving the device, inspect it to make sure it originated from an authentic source and has not been tampered with.

From device delivery through assembly, shipping, installation, usage, and maintenance, the device must not be exposed to conditions outside the ratings in **Appendix A Technical Specifications**.

If the device is exposed to cold temperatures, adjust it to warmer temperatures gradually to avoid condensation, which can interfere with the operation of the device or cause permanent damage.

Do not drop or shake the device.

For information about ongoing maintenance of the device, such as cleaning, see section **7 Maintenance**.

3.2 Handling to Avoid Accidental Tamper

This device implements active tamper detection, which uses a small amount of electricity even when the device is completely powered off. The device ships with the battery charged to approximately 60%, which provides a shelf life of at least 6 months, and up to a year. Storage conditions (such as storage above 77°F / 25°C) strongly affect this duration. If the rechargeable battery is allowed to completely discharge, the device's tamper detection feature uses the device's non-rechargeable backup battery. If both batteries are allowed to completely discharge, the device interprets this as tampering.

Upon detecting tampering, the device locks down and must be returned to the manufacturer to reset. To avoid accidental tamper events, follow these precautions:

- Charge the device for 12 hours immediately upon receipt to extend its shelf life.
- Before storing the device, make sure the battery is charged to at least 40%.
- Before storing the device, activate Airplane Mode (wireless not advertising). See section **6.6.6 How to Turn Bluetooth LE Advertising On and Off**.
- When stored, recharge the device for 12 hours at least every 6 months.
- Do not drop or shake the device.
- Do not attempt to disassemble the device.
- Do not expose the device to excessive heat or cold (see **Error! Reference source not found. Error! Reference source not found.**).

4 Installation

Installing DynaPro Go is straightforward: The acquirer configures the Certificate Authority, public keys, terminal and payment brand settings before deployment; end users need only set up a host with appropriate software, configure the software, and connect the device to the host. This section provides general information about solutions that incorporate DynaPro Go, including host software, connecting the device, and charging the device.

4.1 About Inspection

It is important to regularly and thoroughly inspect a device in live usage, and its immediate surroundings, to make sure malicious individuals have not tampered with it. MagTek recommends inspection training for all device operators, and an inspection schedule with checkpoints in place to make sure inspections are being done as specified and as scheduled. MagTek provides an easy-to-follow guide for inspecting the device in ***D998200133 DYNAPRO GO DEVICE INSPECTION***.

Before the device is deployed, it is also important to inspect the packaging to make sure it has not been tampered with in storage or in transit. MagTek provides details for inspecting the integrity of the device's packaging in ***D998200134 DYNAPRO GO PACKAGE INSPECTION***.

4.2 About Host Software

In any solution, DynaPro Go is connected to a host, which must have software installed that knows how to communicate with the device, and which is capable of processing transactions. To set up the host to work with DynaPro Go, follow the installation and configuration instructions provided by the vendor of the host or the host software. For information about developing custom host software, see section 8 **Developing Custom Software**.

4.3 Connecting to a Host

4.3.1 About Connecting to a Host

The following sections provide steps for connecting DynaPro Go to a host via the various available physical connection types.

4.3.2 How to Connect DynaPro Go to a Host or Charger via USB

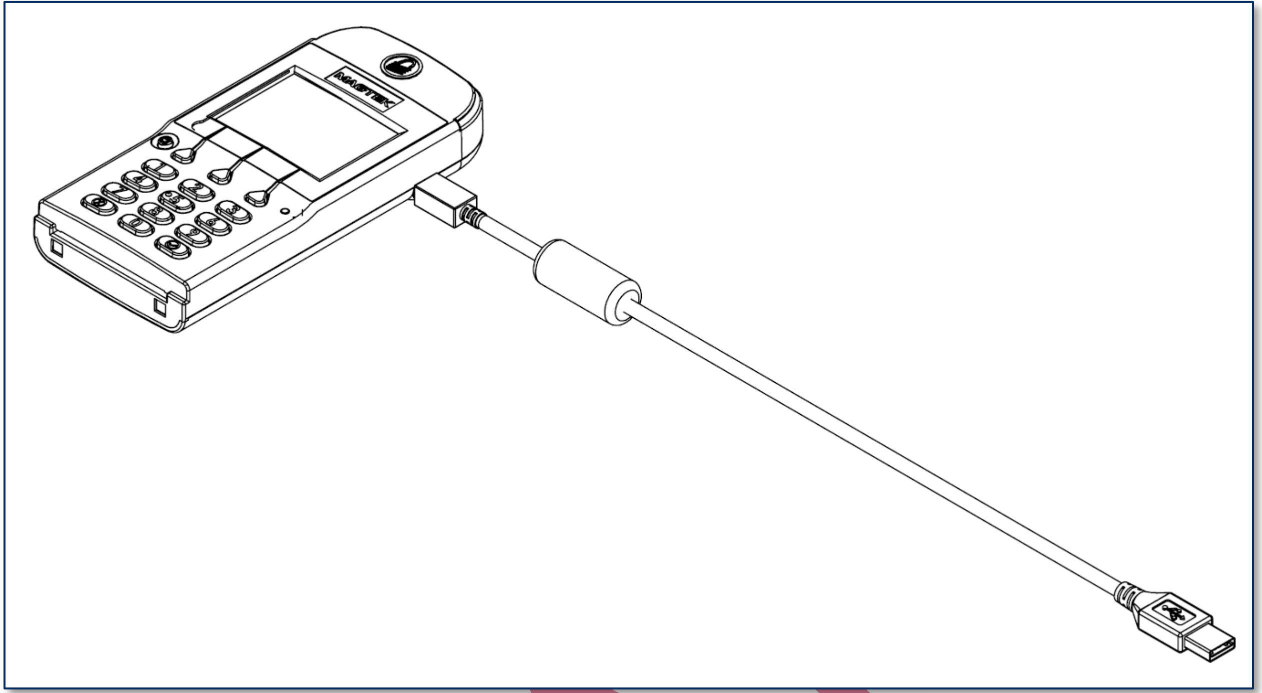
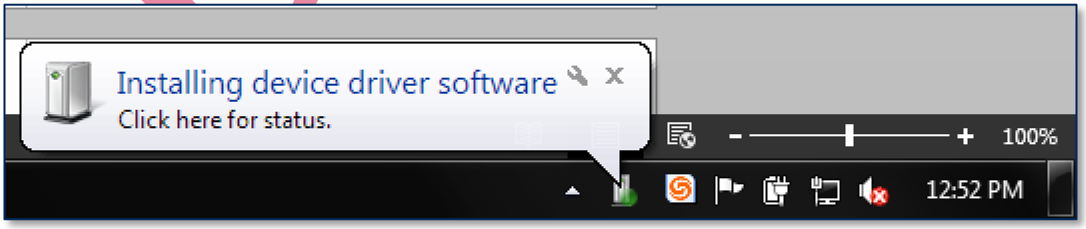


Figure 4-1 - Connecting DynaPro Go to a USB Host or USB Charger

To connect DynaPro Go to a USB host or charger using the micro-USB port, follow these steps:

1) In any order:
   - Connect the small end of the USB cable to DynaPro Go as shown in **Figure 4-1**.
   - Connect the large end of the USB cable to the charger or to the host's USB port.
2) As soon as DynaPro Go starts receiving power through USB, it automatically powers on.
3) If you want DynaPro Go to communicate with the host via USB (as opposed to merely using it as a power source to charge the battery), make sure its active connection is set to USB. See section **5.2 How to Change the Active Connection**.
4) If the specific DynaPro Go serial number you are connecting has not been connected to the host before, the device shows No Host Connection on the display, and the Windows system tray on the host reports it is Installing device driver software.



Installing device driver software

Click here for status.

5) When connecting to some hosts, Windows may show an error message reporting Device driver [software] was not successfully installed or Device unplugged. The error is harmless and the device may work immediately; if not, disconnect the device from the USB port, then re-connect it.

6) After successfully connecting to the host operating system via USB, the device shows **Welcome** on the display (see section **6.4 About the Touchscreen Display**).

4.3.3 How to Connect DynaPro Go to a Host via 802.11 Wireless

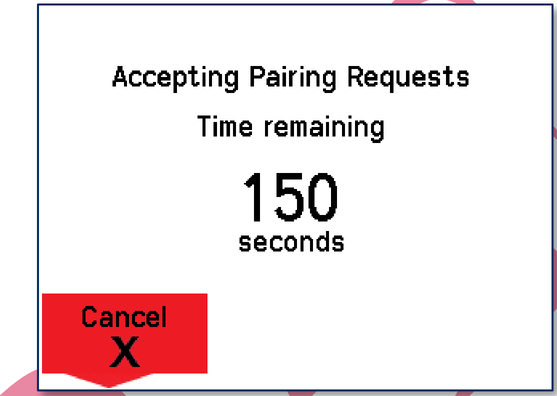
To connect DynaPro Go to a host or charger using the 802.11 wireless connection, follow these steps:

1) Make sure the wireless access point, network, device, and host are set up properly and tested according to the steps in section **5.3 How to Configure Network Settings (ADVANCED)**.
2) Power on the device and make sure the device's active connection is 802.11 wireless, using the steps in section **5.2 How to Change the Active Connection**.
3) Make sure the device is connected to the wireless network by checking the status icons. For details, see section **6.4 About the Touchscreen Display**.

4.3.4 How to Connect DynaPro Go to a Host via the Bluetooth LE Connection

To connect DynaPro Go to a host via the Bluetooth LE connection, follow these steps:

1) Make sure the host's hardware and operating system support **Bluetooth LE Secure Connections**, which were introduced in the ***Bluetooth Core Specification version 4.2***.
2) On the host, install and configure the software you intend to use with DynaPro Go.
3) Power on the device and make sure the battery is charged. Note that it is not always necessary to explicitly turn on the device before using it; if the device is not powered on, it will start powering on when a host establishes a connection.
4) Make sure the device's active connection is set to Bluetooth LE, using the steps in section **5.2 How to Change the Active Connection**.
5) Press Left Function Key 1 2 3 Right Function Key to enable the device to accept Bluetooth LE pairing requests for up to three minutes. The device indicates it is accepting pairing requests, and displays the remaining time.

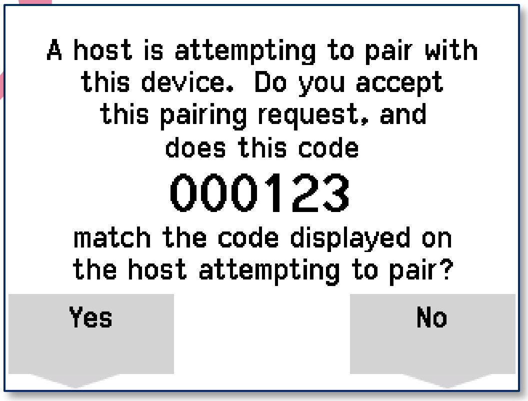


Accepting Pairing Requests

Time remaining

150
seconds

6) On the host, scan for Bluetooth devices, and select the device you want to pair to. On Windows and Android hosts, use the operating system's Bluetooth setup features. On iOS hosts, you must use custom host software designed specifically to pair with DynaPro Go (see section 8 **Developing Custom Software**).
7) The device responds to the pairing request by showing a 6-digit passcode on the display, and the host software should show a matching passcode. If the device does not show the passcode or the host fails to pair, make sure the host's operating system and Bluetooth hardware support **Bluetooth LE Secure Connections**, which were introduced in the ***Bluetooth Core Specification version 4.2***.



A host is attempting to pair with this device. Do you accept this pairing request, and does this code

000123

match the code displayed on the host attempting to pair?

8) If the passcodes on the host and device match, press the function key below **Yes** to accept the pairing request, and perform any corresponding actions on the host. The device shows a confirmation screen for a short time to indicate the operator has accepted the request. If the passcodes do not match, press the function key below **No** and try again.

9) If pairing fails for any reason, the device will refuse pairing requests even if the countdown is still active. To attempt pairing again, repeat the steps above, starting with the key sequence to enable pairing.

10) Make sure the device is connected to the host by checking the device's status icons (section **6.4 About the Touchscreen Display**) or **Connection Status Screen**.

11) The device stays powered on until the host terminates the Bluetooth LE connection, or until an operator or cardholder powers off the device using the power button (see section **Error! Reference source not found. Error! Reference source not found.**). Powering off causes the device to close the Bluetooth LE connection, but the device continues to advertise so the host can re-establish a connection and power on the device automatically when needed. To conserve power, make sure the device is powered off either automatically or manually when it is not in use.

4.4 Mounting tDynamo

4.4.1 About Mounting

tDynamo’s design provides two mount points: A **Lanyard Mount Point** and a **Locking Mount Point** (see section Error! Reference source not found. Error! Reference source not found.). The two mount points can be used in various combinations:

- The lanyard mount point can be used to hang the device for convenient storage and/or handling in handheld sales solutions.
- The locking mount point can be used with the optional docking stand (shown in **Figure 4-2**) mounted to a countertop for stability in stationary sales solutions.
- The locking mount point can also be used with custom brackets to mount to other devices or surfaces.
- The docking stand can also be used in unlocked mode, and optionally combined with the lanyard mount point, for quick grab-and-go and convenient drop-in charging between handheld sessions.

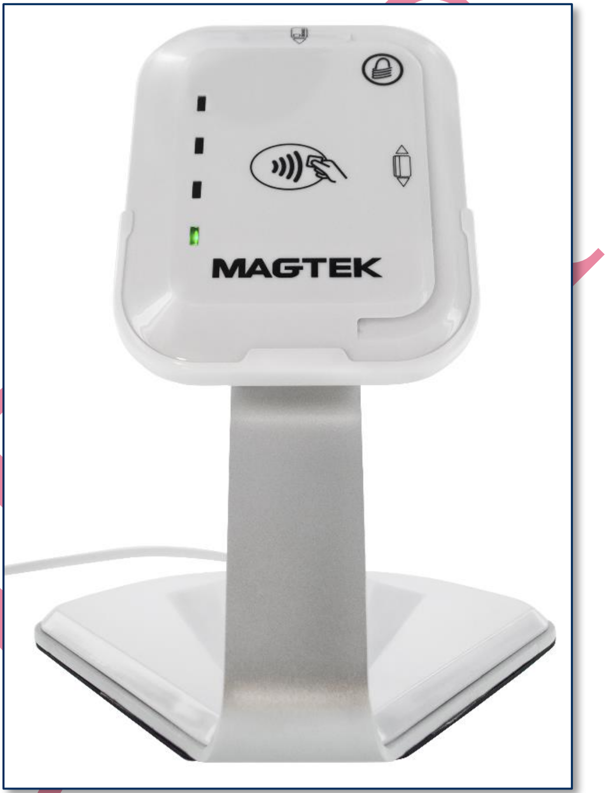


Figure 4-2 - tDynamo Installed On Optional Docking Stand

4.4.2 How to Mount the Docking Stand

To mount the docking stand to a countertop, follow these steps (see **Figure 4-3**):

1) Determine where the docking stand should be placed: Factors to consider include cable length, cardholder and operator ergonomics, and access for cleaning, maintenance, and repair.
    a) If the docking stand will be used for charging in handheld operations, unobstructed removal is also a consideration.
    b) If the device will be permanently docked for cardholder use, placing the stand so it hangs slightly over the edge of the countertop may provide the least obstructed swipe path.
2) Open the protective cap over the mounting hole on the base of the docking stand.
3) Place the docking stand at the desired location and mark the center of the mounting hole on the countertop, then set the docking stand aside.
4) Drill a ¼" hole all the way through the countertop.
5) Line up the hole in the stand over the hole in the countertop.
6) Thread the included bolt through docking stand's mounting hole and the countertop hole.
7) Fasten the included knob to the bolt and tighten it.
8) Replace the docking stand's protective cap.
9) Connect the docking stand's USB cable to the host.

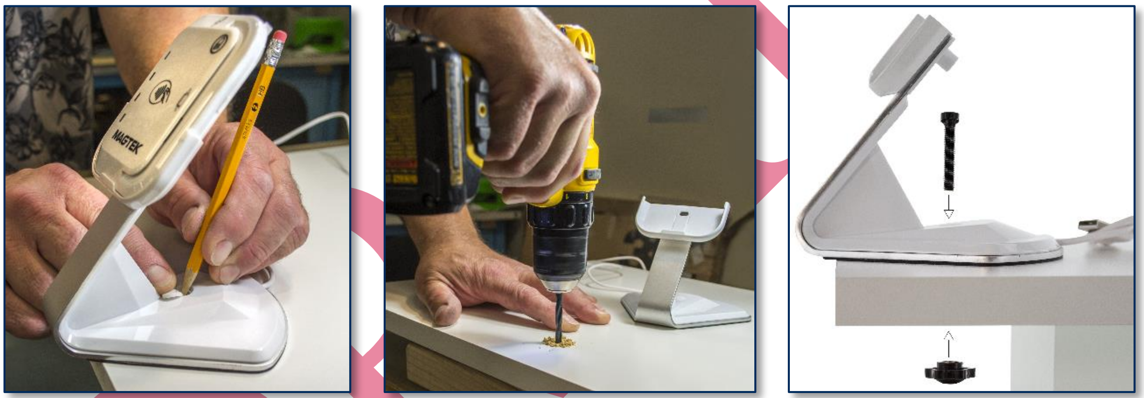


Figure 4-3 - Optional Docking Stand Assembly

4.4.3 How to Temporarily Dock tDynamo

To temporarily dock the device in the docking stand for convenient charging, follow these steps:

1) If the docking stand will be mounted to a countertop, follow the steps in section **4.4.2 How to Mount the Docking Stand** to do that first.
2) Make sure the docking stand is connected to a USB power source.
3) Make sure the device's docking stand contacts are clean and unobstructed.
4) Place the device all the way into the docking stand. The device powers on automatically and begins charging.

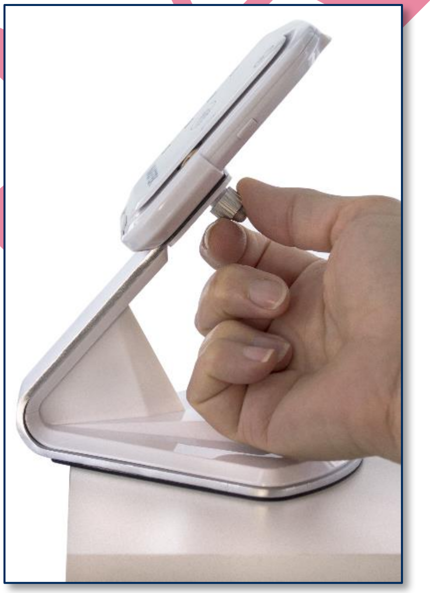
4.4.4 How to Permanently Dock tDynamo

NOTICE

Do not leave the round key installed in the docking stand. The key is designed to be removed to deter unauthorized removal of the device.

To permanently attach the device to the docking stand, follow these steps:

1) Make sure tDynamo is configured to use the docking contacts as its primary connection. If it is configured to use another connection, use that connection first to change the configuration.
2) Follow the steps in section **4.4.3 How to Temporarily Dock tDynamo** to place the device on the docking stand.
3) Use the included round key to turn the locking screw on the back of the stand to lock the device in place.



4) Remove the key and set it aside for future use, such as for cleaning or servicing the device. It has a key ring / string hanger loop integrated into its handle for convenient storage.
5) Make sure the device is firmly locked into the stand.

5 Configuration

The device has many commands the host software can use to change and monitor its behavior. They are documented in detail in ***D998200136 DYNAPRO GO PROGRAMMER'S REFERENCE MANUAL (COMMANDS)***.

In addition, when the device is on the Welcome screen or showing an error message, operators can view or change some configuration options using the keypad and display. **Table 5-1** provides details for using these features.

Table 5-1 - Keypad Configuration Features

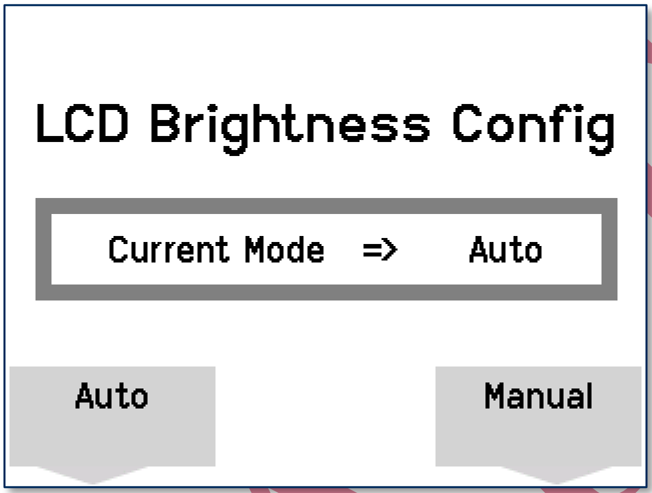
Operation	Key Sequence	Notes
Open Host Connection	Left Function Key 1 2 3 Right Function Key	When the device has an 802.11 wireless connection and is configured to not be always listening for incoming connections, this key sequence opens an unsecured TCP/IP connection to the host and requests the host initiate a secured connection. When the device has Bluetooth LE connection, this key sequence enables the device to accept pairing requests from a host for up to three minutes.
LCD backlight mode	Left Function Key 5 2 2 Right Function Key	Changes the mode of the LCD display backlight between Auto and Manual. See section **5.1 How to Configure the LCD Display Brightness**.
LCD backlight brightness	Left Function Key 5 2 3 Right Function Key	Available if the host software has not configured the device to use AUTO LCD brightness based on the light sensor. See section **5.1 How to Configure the LCD Display Brightness**.
Keypad backlight mode	Left Function Key 5 3 3 Right Function Key	Changes the mode of the keypad backlight between Auto and Default. See section **Error! Reference source not found. Error! Reference source not found.**.
Change Active Connection	Left Function Key 4 5 6 Right Function Key	Toggles the device's active connection between possible connection types. See section **5.2 How to Change the Active Connection**.
Show firmware details	Left Function Key 7 8 2 Right Function Key	Displays a page showing firmware information about the device. See section **6.4.2 Firmware** .
Show contactless details	Left Function Key 7 8 1 Right Function Key	Displays a page showing information about the contactless functions and other non-PCI features of the device. See section **6.4.3 Contactless and Other Details**.
Show EMV details	Left Function Key 7 8 3 Right Function Key	Displays a page showing information about the EMV functions of the device. See section **6.4.4 EMV Details**.

Operation	Key Sequence	Notes
Show Health and Safety Details	Left Function Key 7, 8, 0 Right function key	Displays a page showing Health & Safety information about the device. See section **6.4.5 Health and Safety Information**.
Show wireless status	Left Function Key 6 2 2 Right Function Key	Displays a page showing information about the device’s 802.11 wireless or Bluetooth LE connection. See section **6.4.6 Connection Status Screen**.
Toggle Network Connection Mode	Left Function Key 4 5 9 Right Function Key	Displays a page to confirm changing between Always Listening and Device Initiated Network Connection Modes. See section **5.3.4 How to Configure the Device for 802.11 Wireless**.

5.1 How to Configure the LCD Display Brightness

The device’s LCD display has a backlight that can be configured to either remain at a constant user-selected brightness level (**Manual mode**) or adapt its brightness to ambient lighting based on the device’s light sensor (**Auto mode**). The factory default of the device is **Manual** mode at **75%** brightness.

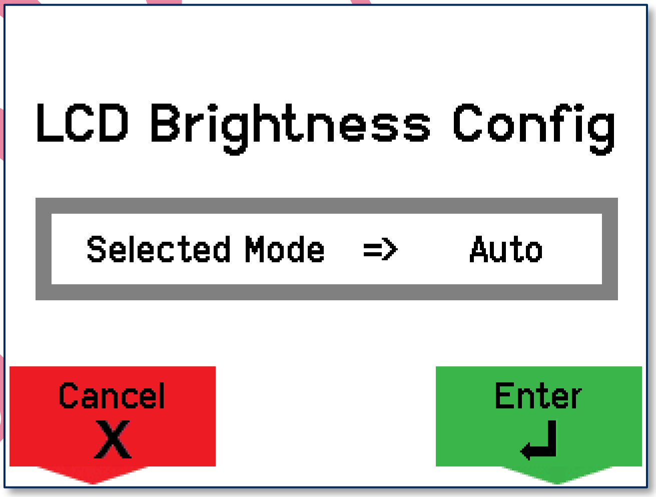
To change the LCD display backlight mode, on the **Welcome** screen, press **Left Function Key** **5** **2** **2** **Right Function Key** to open the **LCD Brightness Config** screen.



LCD Brightness Config

Current Mode => Auto

The **LCD Brightness Config** screen shows the mode the LCD display backlight is currently using. To change the mode, press the function key below the selection you want, then press the **Enter** key to save the change. To exit without saving changes, press the **Cancel** key or wait 10 seconds for the device to return to the **Welcome** screen.



LCD Brightness Config

Selected Mode => Auto

5.1.1 LCD Display Brightness Auto Mode

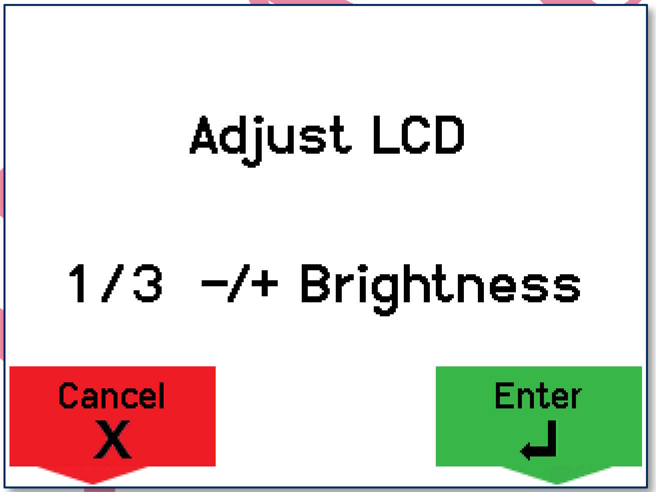
When the display brightness is set to **Auto** mode, the device adjusts the LCD backlight brightness automatically based on ambient light detected by the light sensor (see section **1.9 Major Components**). The brightness levels the device selects are shown in **Table 5-2**. When the device is in **Auto** mode, the key combination to manually set LCD brightness is not available.

Table 5-2 - LCD Display Brightness Levels

Light Level	LCD Brightness Level
High	Maximum (99%)
Medium	High (75%)
Low	Medium (60%)
Very Low	Low (45%)

5.1.2 LCD Display Brightness Manual Mode

When the display brightness is set to **Manual** mode, the device keeps the LCD backlight brightness at a constant level the user can select. The factory default is **High** (75% brightness). To change the constant brightness level, on the **Welcome** screen, press **Left Function Key** **5** **2** **3** **Right Function Key** to show the **Adjust LCD** screen.



Adjust LCD

1/3 -/+ Brightness

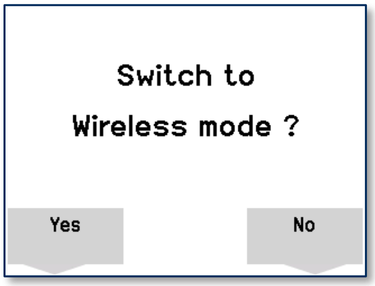
Select the desired brightness by pressing the **1** key to decrease and the **3** key to increase, then press the **Enter** key to save the change. To exit without saving changes, press the **Cancel** key or wait 10 seconds for the device to return to the **Welcome** screen.

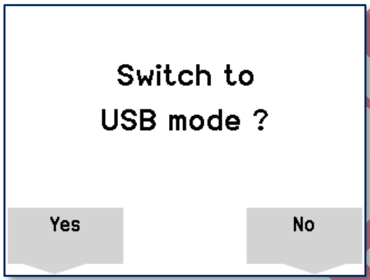
5.2 How to Change the Active Connection

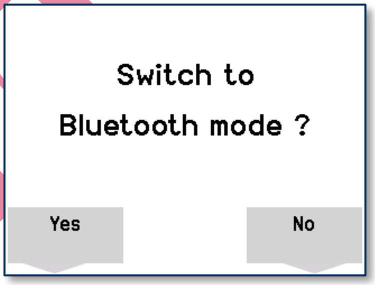
DynaPro Go supports multiple connection types, but only one interface can be active at a time. Initial configuration requires the host to use the USB port, but after configuration, generally a live deployed solution will not require changing the Active Connection.

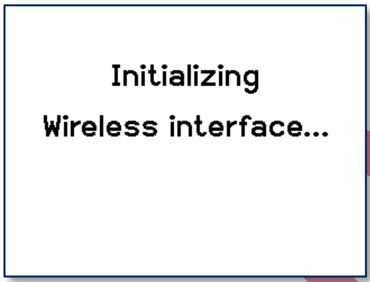
To change the active connection, on the **Welcome** screen, press **Left Function Key** **4** **5** **6** **Right Function Key** to show a confirmation screen to begin using the currently inactive connection type.

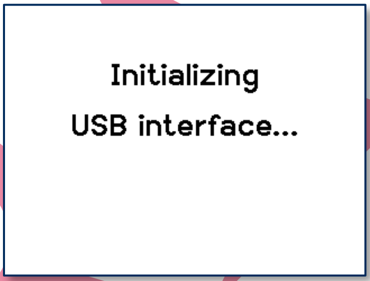
To change the active connection and return to the **Welcome** screen, press the **Enter** key or the function key below **Yes**. To exit without changing the active connection, press **Cancel** key or the function key below **No**, or wait 10 seconds for the device to return to the **Welcome** screen.

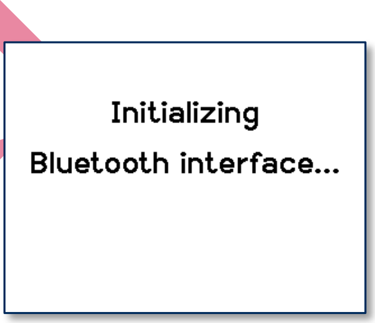

Switch to
Wireless mode ?


Switch to
USB mode ?


Switch to
Bluetooth mode ?


Initializing
Wireless interface...


Initializing
USB interface...


Initializing
Bluetooth interface...

5.3 How to Configure Network Settings (ADVANCED)

This section and its subsections provide step-by-step instructions for configuring the 802.11 wireless network, the device, and the host the device will connect to.

The Device TLS Certificates and their corresponding private keys are generated and injected by the manufacturer. The private key cannot be accessed directly. MagTek provides the Host TLS Certificate chain to the customer for installation on the host.

5.3.1 How to Configure the Network to Support 802.11 Wireless Connections

To prepare the network for DynaPro Go and the host to communicate via the 802.11 wireless connection, network and device administrators should do the following before deployment:

1) Perform all steps in section **2.2 Network Planning**. MagTek recommends performing these steps before receiving the devices so the network will be ready when they arrive.
2) If the solution is using static IP addresses for either the host or the device, pre-register them on the DHCP server, and provide the IP addresses, gateways, and subnet masks to the advanced operator who will configure the devices.
3) If the access point is using wireless MAC filtering, make sure the devices' MAC addresses are in the list of allowed devices. Each device's MAC address is available via keystrokes (see section **6.4.6 Connection Status Screen**) or may be on the label / box.
4) Make sure the network and all firewalls are configured so the device and host can communicate using the specified protocols and port(s). See **Table 2-2** on page **23**.
5) Provide the wireless access point SSID and passcode to the advanced operator who will configure the devices.

5.3.2 How to Configure the Host for 802.11 Wireless

To set up the host to communicate with the device via 802.11 wireless, follow these steps:

1) Talk to your reseller or MagTek Support Services to request a .p12 file containing certificate chains and a private key to install on the host, and a password to decrypt the .p12 file.
2) Install the .p12 file in the **Trusted Root Certification Authorities** portion of the host operating system's certificate store. The steps are operating system specific, and instructions are widely available (for example, here).
3) If the .p12 file's contents are not properly installed in the host's certificate store, the host software will fail to connect to the device using TLS on the 802.11 wireless connection. After importing the .p12 file, verify the following:
    a) Check the list of installed certificates to make absolutely sure certificates **PCI3xROOTCA**, **PCI3xDev-SubCA**, and **DynaPro Go Host TLS** have imported correctly.
    b) Check that the private key was imported successfully by attempting to export the **DynaPro Go Host TLS** certificate. If the key was installed correctly, the export utility will ask if the private key should also be exported. If no key exists, the utility will not show the export key prompt.
4) Check the host operating system's network configuration (for example, using regedit in Windows) to make sure cipher suites are enabled per the guidance in section **2.2 Network Planning**.
5) If the solution is using DNS names, configure the host operating system to register the desired DNS name. The steps are operating system specific.
6) If the solution is setting the device's Network Connection Mode to **Device Initiated**:
    a) Determine the host's IP address or DNS name for use in section **5.3.4 How to Configure the Device for 802.11 Wireless**.
    b) Make sure the host's firewall is configured to allow incoming requests from the device on the port specified in the solution design.
7) Make sure the host's firewall is configured to allow bidirectional direct socket communication using TCP on the configured port. See **Table 2-2 - Protocols and Ports**. If the firewall restricts traffic by IP address, determine the device's IP address and configure the firewall accordingly.
8) Install the point of sale / transaction processing host software.
11) Configure the host software to communicate with DynaPro Go using the appropriate IP address / DNS name and port.

5.3.3 About Configuring the Device for 802.11 Wireless

⚠ CAUTION

DynaPro Go ships from the manufacturer with TLS **Enabled**. This setting can be set to **Disabled** by the customer, which may be useful for initial network setup and testing. **MagTek strongly recommends that TLS always be Enabled when it is deployed in the field.**

Before DynaPro Go can communicate securely with the host using the 802.11 wireless connection, an advanced operator must configure it with solution-specific, network-specific, and host-specific settings. The steps in the following sections use the ***MagTek PCI PED Host App Simulator*** (also known as ***PCIPED_HASim***) to show examples of the device configuration sequence; this tool can be used for initial pre-deployment testing and development, and as sample code showing how to communicate with the device, but production rollout of the solution may call for custom software advanced operators would use to configure the device and update firmware.

For further details about using the ***MagTek PCI PED Host App Simulator***, see ***D998200168 IPAD, DYNAPRO, DYNAPRO MINI, DYNAPRO GO PIN ENTRY DEVICE SIMULATION SOFTWARE INSTRUCTION***.

DynaPro Go can be configured to communicate with the host using 802.11 wireless in one of two **Network Connection Modes**:

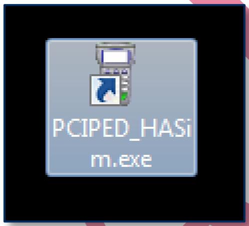
- In **Device Initiated** mode, the device does not listen for incoming connections, and instead expects to initiate connections with the host on demand. In this mode, the device sends a notification to the host requesting that the host initiate a handshake for a secured TLS connection, and opens a listening socket for a limited period of time for the host to initiate the connection.
- In **Always Listening** mode, the device keeps a TLS listening socket open that allows an authenticated host to connect at any time.

In both cases, provided TLS is set to **Enabled**, DynaPro Go 802.11 wireless network connections use TCP/IP protocol secured by TLSv1.2 using x509 certificates, and the device enforces a requirement of mutual authentication between the device and the host. If the host attempts to initiate an unauthenticated connection, the device refuses the connection and shows **OFFLINE** and an error code on the display (see section **6.4 About the Touchscreen Display**). To clear this status, an operator should press key sequence **Left Function Key** **1** **2** **3** **Right Function Key**.

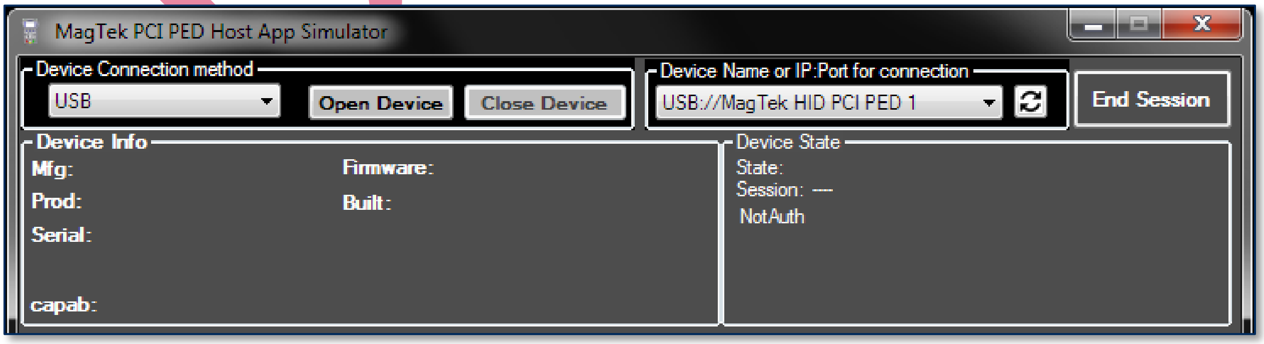
5.3.4 How to Configure the Device for 802.11 Wireless

To configure the device so a host can connect to it via 802.11 wireless, follow these steps:

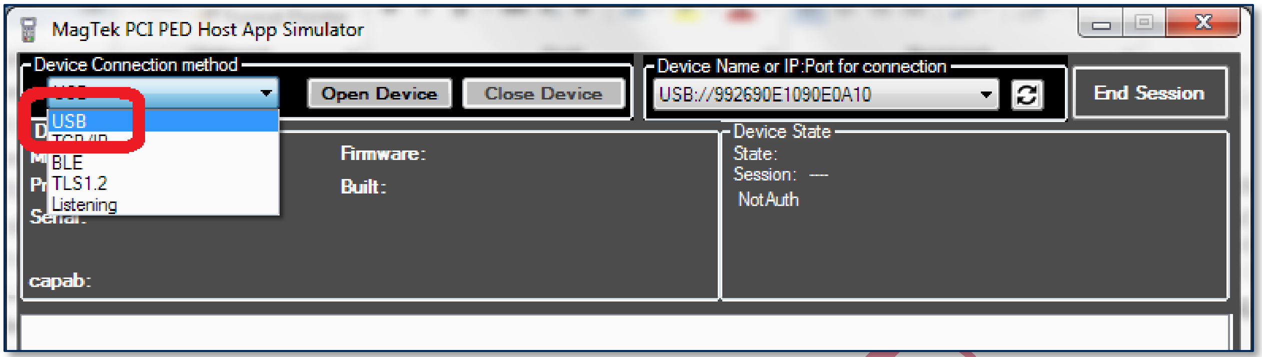
1) Gather the SSID and passcode for the 802.11 wireless access point the device will connect to.
2) If the solution is using static IP addresses, gather the IP address, gateway, and subnet mask to use.
3) If the secure Windows workstation for advanced users has not already been set up, set it up as follows:
    a) Obtain a copy of ***99510127 DYNAPRO/DYNAPRO GO/DYNAPRO MINI WINDOWS SDK INSTALL (EXE)*** from MagTek and run the installer **99510127-rev.exe**.
    b) In Windows Explorer, open the SDK installation location. By default:
        i) On Windows 64-bit workstations, the default location is **C:\Program Files (x86)\MagTek\PCI PED Windows SDK\Sample Code\DotNET Host Simulator Demo\Object**.
        ii) On Windows 32-bit workstations, the default location is **C:\Program Files\MagTek\PCI PED Windows SDK\Sample Code\DotNET Host simulator Demo\Object**.
    c) For convenience, create a shortcut to **PCIPED_HASim.exe** on the desktop.



4) Make sure no other MagTek devices are connected to any of the host's USB ports.
5) Power on the device.
6) Make sure the device is in USB mode by checking the current Active Connection icon at the top of the display. Use **Left Function Key** **4** **5** **6** **Right Function Key** to change it if necessary.
7) Connect the device to the host's USB port (see section **4.3.2 How to Connect DynaPro Go to a Host or Charger via USB**). At the end, the device drivers are installed on the test workstation, and the device is powered on, shows the USB icon at the top of the display (indicating the device Active Connection is USB), and shows **Welcome** on the display.
8) Launch **PCIPED_HASim.exe** to show a **MagTek PCI PED Host App Simulator** window.



9) Under **Device Connection method**, select **USB**.

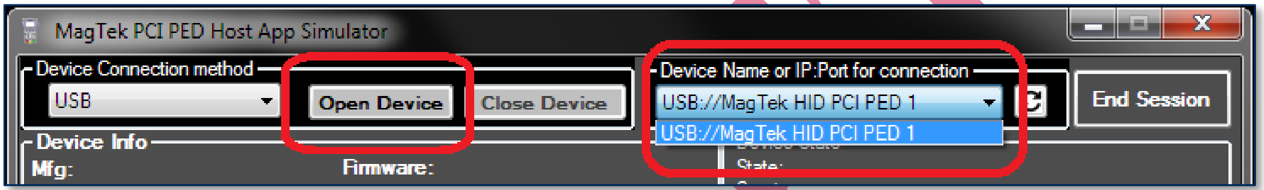


Device Name or IP:Port for connection: USB://992690E1090E0A10

Session: ---

NotAuth

10) In the **Device Name** list, select the serial number or name of the device you want to connect to, then press the **Open Device** button.

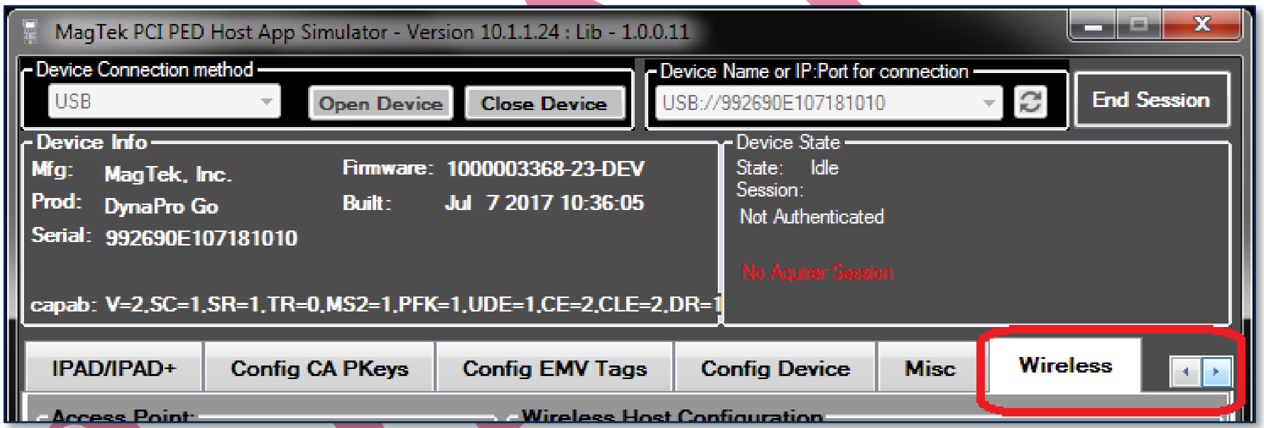


Device Connection method: USB

Device Name or IP:Port for connection: USB://MagTek HID PCI PED 1

USB://MagTek HID PCI PED 1

11) Use the right and left arrow buttons in the tab bar to scroll the tab bar, then select the **Wireless** tab.



Device Connection method: USB

Device Name or IP:Port for connection: USB://992690E107181010

Mfg: MagTek, Inc.

Prod: DynaPro Go

Serial: 992690E107181010

Firmware: 1000003368-23-DEV

Built: Jul 7 2017 10:36:05

capab: V=2,SC=1,SR=1,TR=0,MS2=1,PFK=1,UDE=1,CE=2,CLE=2,DR=1

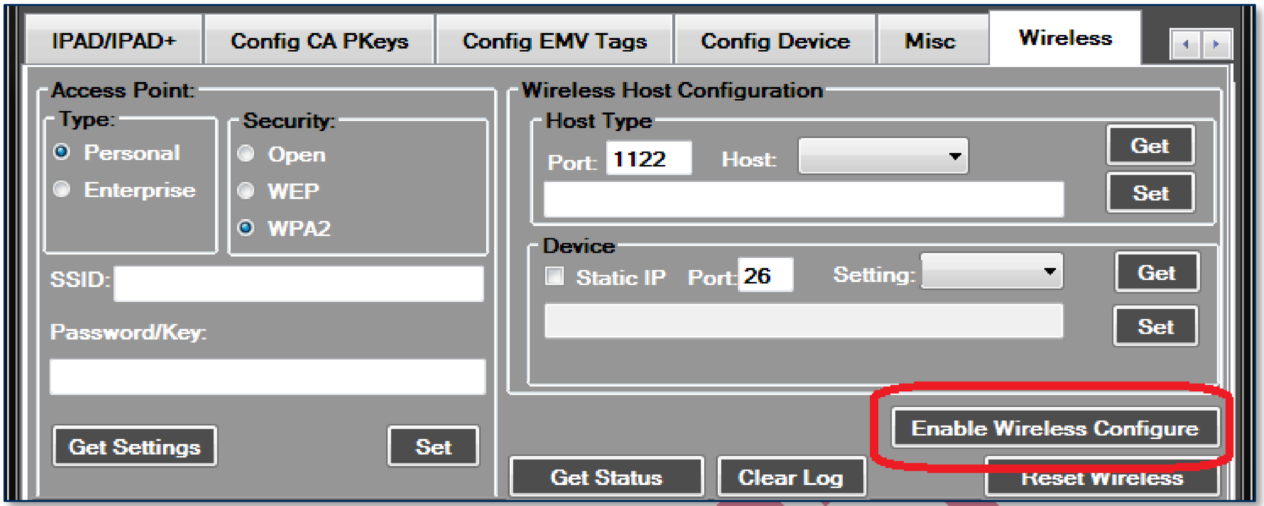
State: Idle

Session:

Not Authenticated

No Aquirer Session

12) In the **Wireless Host Configuration** group, press the **Enable Wireless Configure** button.

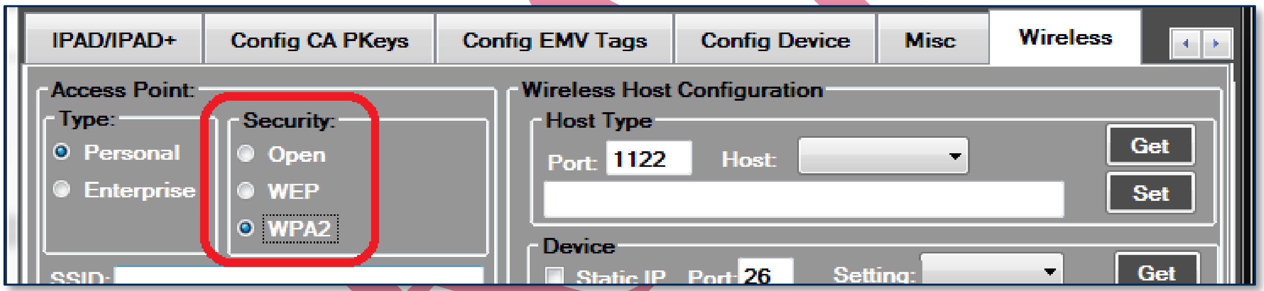


Access Point:
Type: ● Personal ○ Enterprise
Security: ○ Open ○ WEP ● WPA2
SSID:
Password/Key:

Wireless Host Configuration
Host Type
Port: 1122 Host:
Device
□ Static IP Port: 26 Setting:

13) When the device screen prompts **Enter Admin Passcode**, enter the device admin passcode on the device keypad: **1** **3** **9** **7** **2** **6** **8** **4** **Enter**.

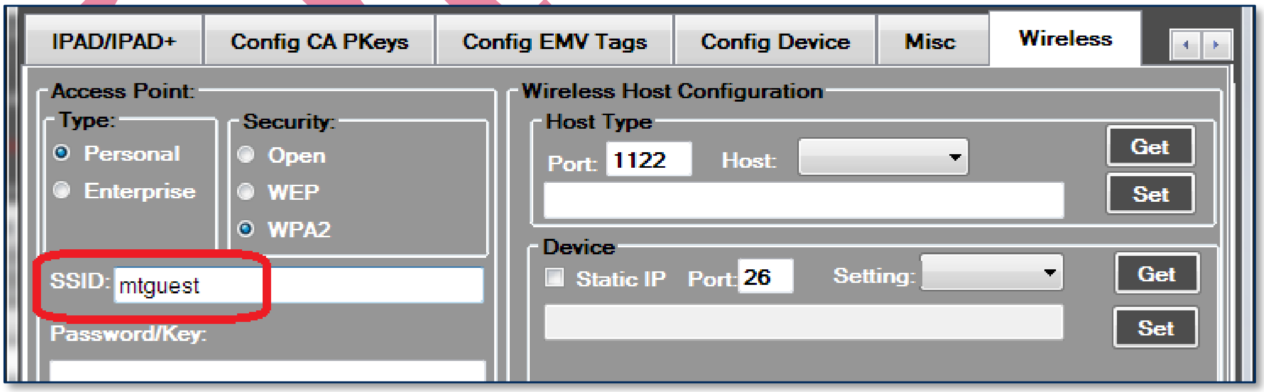
14) In the **Access Point** group, select the **Security** algorithm of the wireless access point the device should connect to. For this device, the access point must use is **WPA2**. Leave the access point **Type** set to **Personal**.



Access Point:
Type: ● Personal ○ Enterprise
Security: ○ Open ○ WEP ● WPA2
SSID:

Wireless Host Configuration
Host Type
Port: 1122 Host:
Device
□ Static IP Port: 26 Setting:

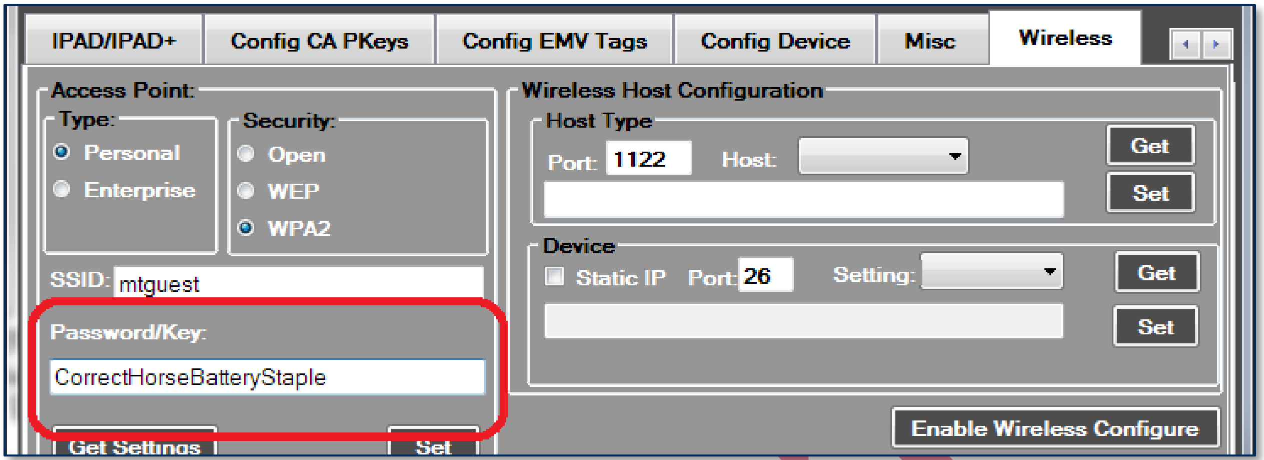
15) Enter the Service Set ID (**SSID**) of the wireless access point you are connecting to.



Access Point:
Type: ● Personal ○ Enterprise
Security: ○ Open ○ WEP ● WPA2
SSID: mtguest
Password/Key:

Wireless Host Configuration
Host Type
Port: 1122 Host:
Device
□ Static IP Port: 26 Setting:

16) Enter the **Password/Key** for the wireless access point.



Type: ● Personal ○ Enterprise

Security: ○ Open ○ WEP ● WPA2

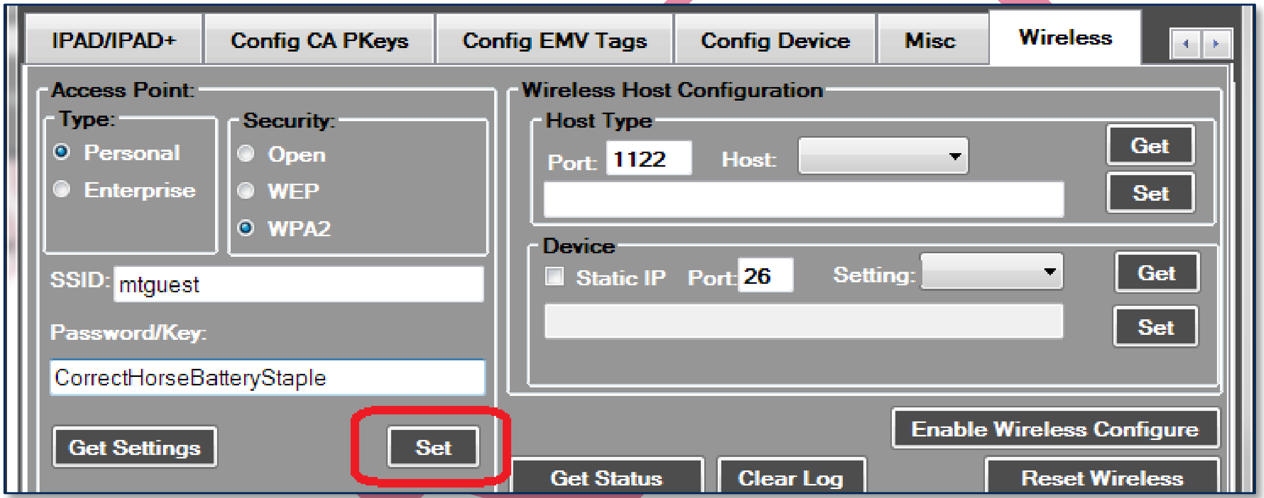
SSID: mtguest

Password/Key: CorrectHorseBatteryStaple

Port: 1122

□ Static IP Port: 26

17) Press the **Set** button to save the settings to the device.



Type: ● Personal ○ Enterprise

Security: ○ Open ○ WEP ● WPA2

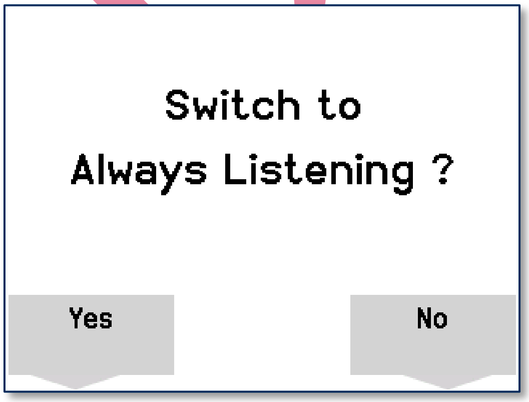
SSID: mtguest

Password/Key: CorrectHorseBatteryStaple

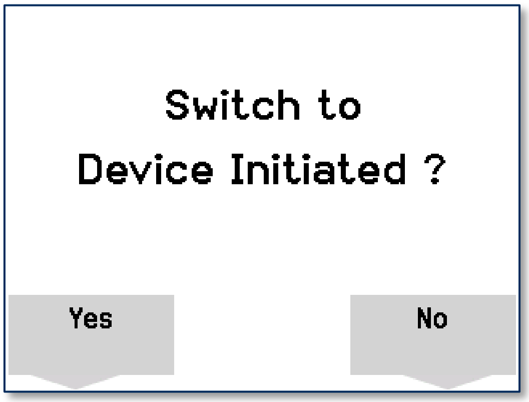
Port: 1122

□ Static IP Port: 26

18) Make sure the device is configured to use the Network Connection Mode that corresponds to the solution design. On the **Welcome** screen, press **Left Function Key** **4** **5** **9** **Right Function Key** to initiate a toggle between **Device Initiated** mode and **Always Listening** mode, and press the function key below **Yes** or **No** to accept or reject the change.

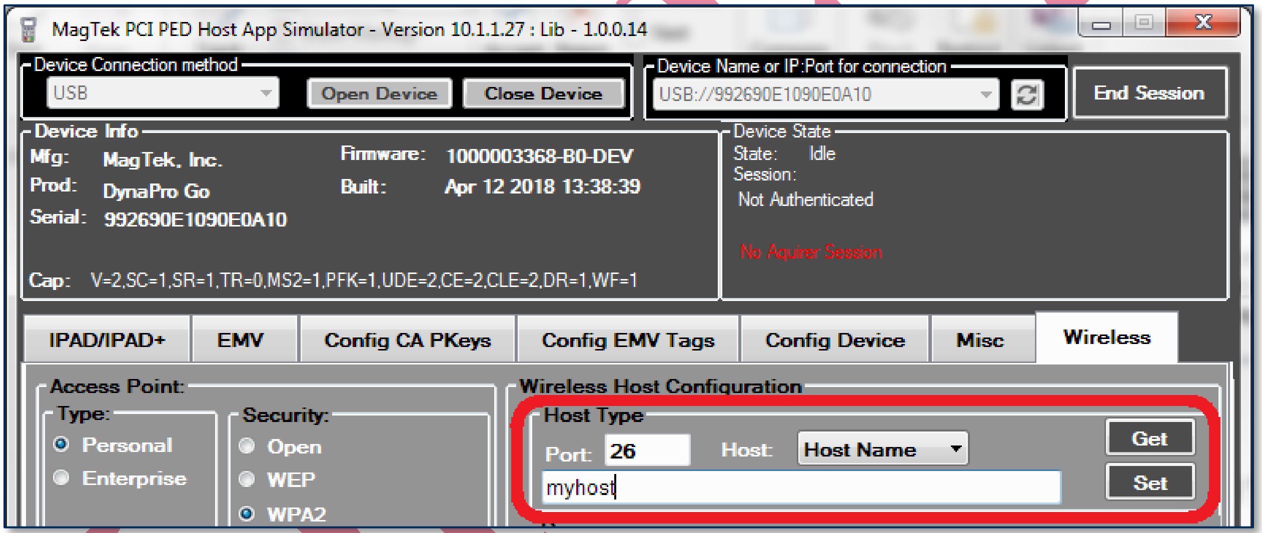


Switch to
Always Listening ?



Switch to
Device Initiated ?

19) To configure the device to use **DHCP** and a dynamic IP address, turn off the **Static IP** checkbox and press the **Set** button. To configure the device to use a **static** IP address, follow these steps:
    a) In the **Device** section of the **Wireless** tab, turn on the checkbox for **Static IP**.
    b) Select **Static IPv4** in the **Setting** dropdown list, and fill in the desired **Port** and IP address.
    c) Select **Gateway** in the **Setting** dropdown list, and fill in the desired Gateway IP address.
    d) Select **Subnet Mask** in the **Setting** dropdown list, and fill in the desired Subnet Mask.
    e) Press the **Set** button to save all settings to the device.
20) If the Network Connection Mode is **Device Initiated**, configure the device to connect to the correct listening host using the **Host Type** box:
    a) Use the **Host** dropdown list to select whether the device should connect to the host by DNS name or by static IP address.
    b) Fill in the host **Port** to use when initiating a connection.
    c) Fill in the host's IP address or DNS name.
    d) Press the **Set** button to save the settings to the device.



MagTek PCI PED Host App Simulator - Version 10.1.1.27 : Lib - 1.0.0.14

Device Connection method: USB

Device Name or IP:Port for connection: USB://992690E1090E0A10

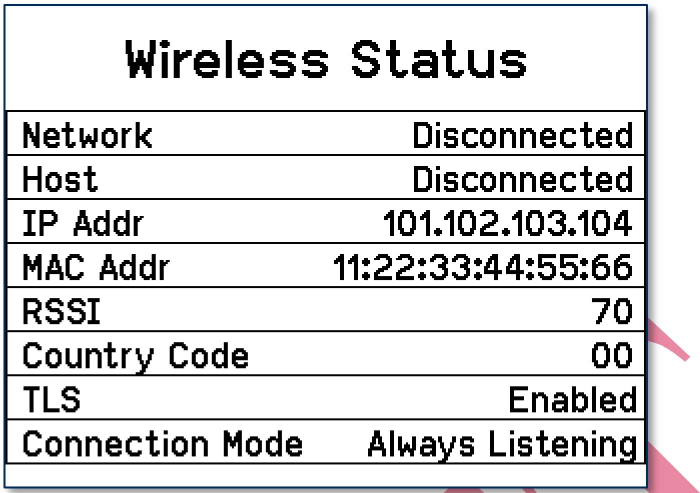
Device Info
Mfg: MagTek, Inc.
Prod: DynaPro Go
Serial: 992690E1090E0A10
Firmware: 1000003368-B0-DEV
Built: Apr 12 2018 13:38:39
Cap: V=2,SC=1,SR=1,TR=0,MS2=1,PFK=1,UDE=2,CE=2,CLE=2,DR=1,WF=1

Device State
State: Idle
Session:
Not Authenticated
No Aquirer Session

Access Point:
Type: ● Personal ○ Enterprise
Security: ○ Open ○ WEP ● WPA2

Wireless Host Configuration
Host Type
Port: 26
Host: Host Name
myhost

21) Make sure the 802.11 wireless access point is configured and available before proceeding.
22) Change the Active Connection to 802.11 Wireless (see section **5.2 How to Change the Active Connection**). The screen shows a wireless network icon at the top to indicate that the current active connection is 802.11 wireless (see section **6.4 About the Touchscreen Display**).
23) If the access point is available, the device shows **Connecting Wireless** on the display, then if it successfully connects to the access point, shows **Welcome**. If the device can not connect to the access point, it shows **OFFLINE** and error codes specifying why (see section **6.4.1 Welcome Screen**).
24) On the **Welcome** screen, press **Left function key**, **4**, **7**, **2**, **Right function key**. The device shows a page about the 802.11 wireless connection.
25) Write down the **IP Address** and press the **Cancel** key to return to the **Welcome** screen.



Wireless Status

Network	Disconnected
Host	Disconnected
IP Addr	101.102.103.104
MAC Addr	11:22:33:44:55:66
RSSI	70
Country Code	00
TLS	Enabled
Connection Mode	Always Listening

26) The device is now configured for hosts to connect to it using the wireless access point.

27) To enable or disable TLS, set the **TLS 1.2** checkbox to **Enabled** (checked) or **Disabled** (unchecked). On changing, the device will show the new TLS mode on the display.

28) To perform basic connection testing, leave the **MagTek PCI PED Host App Simulator** window open and follow the steps in section **5.3.5 How to Test the 802.11 Wireless Connection**.

5.3.5 How to Test the 802.11 Wireless Connection

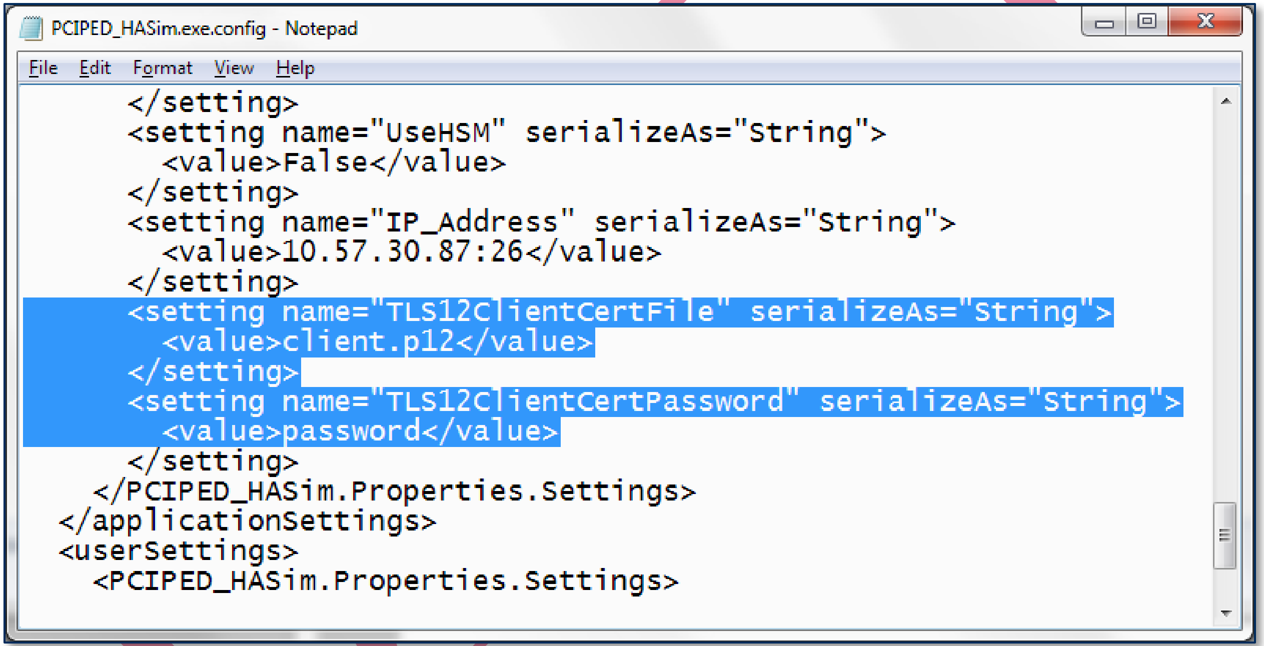
To test the device's wireless connection regardless of whether it is configured for **Always Listening** or **Device Initiated** mode, follow these steps:

1) Obtain the device's IP address using Left function key, 4, 7, 2, Right function key.
2) Open a command prompt on the host and enter ping xx.xx.xx.xx where xx is IP Addr from the device's display. If the request times out, the network connection is not working.
3) To test that the device's DNS name is properly registered with the DNS server, follow these additional steps:
   a) Obtain the 16-character device serial number from its label, and prefix it with the string TLS to form a 19-character **device name**.
   b) In the command prompt, enter ping TLSxxxxxxxxxxxxxxxx where **TLSxxx…** is the device name. If the request times out, the device is not registered with the DNS server, and the host will only be able to reach it using the numerical IP address.
4) If the device is configured for **Always Listening**, continue testing by following the steps in section **5.3.5.1 How to Test an Always Listening Wireless Connection**. If the device is configured for Device Initiated, continue testing by following the steps in section **5.3.5.2 How to Test a Device Initiated Wireless Connection**.

5.3.5.1 How to Test an Always Listening Wireless Connection (TLS Enabled)

To connect to the device and test the 802.11 wireless connection when the device is in **Always Listening** mode and has TLS Enabled, follow these steps:

1) Make sure the network, host, and device are properly configured (see previous sections).
2) If PCIPED_HASim.exe is running, close it.
3) Test that there is adequate signal strength between the access point and all locations where the device will operate wirelessly. In each location, open the **Connection Status Screen** and make sure the Received Signal Strength Indicator level (RSSI) is greater than 40.
4) If the device has TLS Enabled:
   a) Place the .p12 file containing the host certificate chain in the installation folder where PCIPED_HASim.exe is installed.
   b) In the same folder, open PCIPED_HASim.exe.config in a text editor. Change the value of TLS12ClientCertFile to the name of the .p12 file. Change the value of TLSClientCertPassword to the password to decrypt the .p12 file.

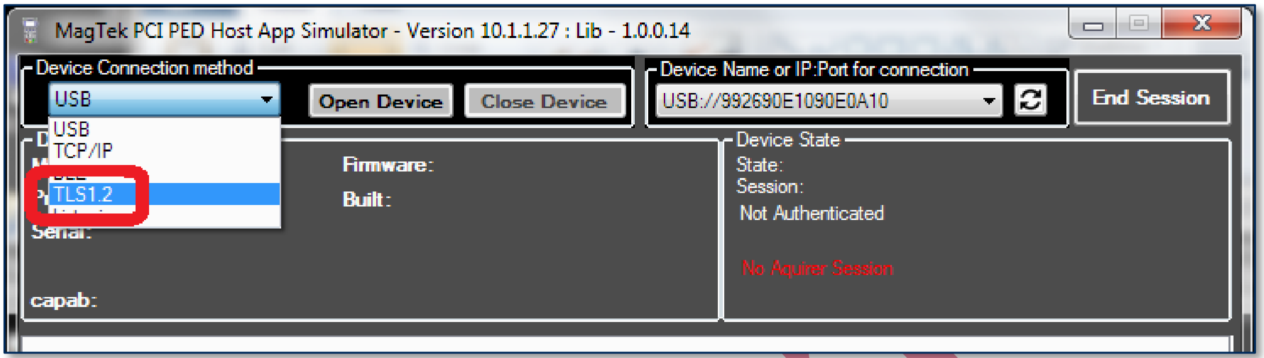


```
   </setting>
   <setting name="UseHSM" serializeAs="String">
    <value>False</value>
   </setting>
   <setting name="IP_Address" serializeAs="String">
    <value>10.57.30.87:26</value>
   </setting>
   <setting name="TLS12ClientCertFile" serializeAs="String">
    <value>client.p12</value>
   </setting>
   <setting name="TLS12ClientCertPassword" serializeAs="String">
    <value>password</value>
   </setting>
  </PCIPED_HASim.Properties.Settings>
 </applicationSettings>
 <userSettings>
  <PCIPED_HASim.Properties.Settings>
```

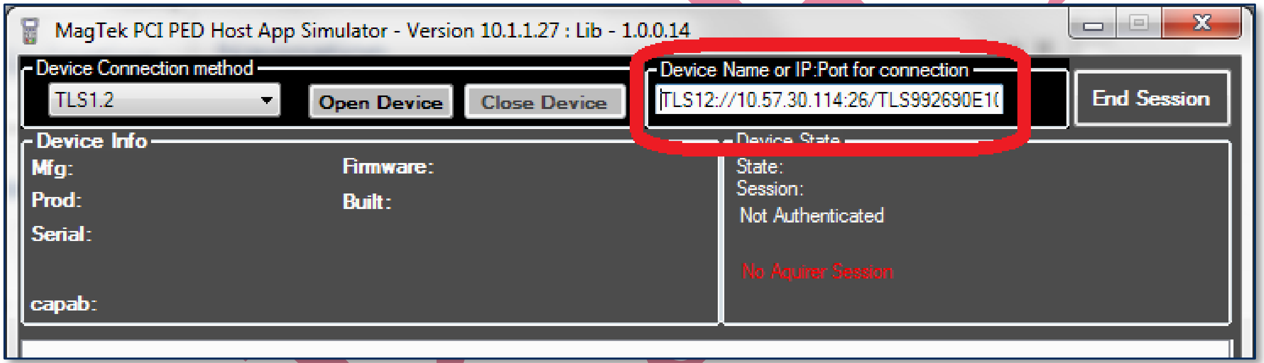
   c) Save and close the file.
   d) Install the .p12 file in the **Trusted Root Certification Authorities** portion of the test host's operating system certificate store. The steps are operating system specific, and instructions are widely available (for example, here).
   e) If the .p12 file's contents are not properly installed in the host's certificate store, the host software will fail to connect to the device using TLS on the 802.11 wireless connection. After importing the .p12 file, verify the following:
      i) Check the list of installed certificates to make absolutely sure certificates PCI3xROOTCA, PCI3xDev-SubCA, and DynaPro Go Host TLS have imported correctly.
      ii) Check that the private key was imported successfully by attempting to export the DynaPro Go Host TLS certificate. If the key was installed correctly, the export utility will ask if the private key should also be exported. If no key exists, the utility will not show the export key prompt.

5) Launch **PCIPED_HASim.exe**.

6) Under **Device Connection method**, select **TLS1.2** (if TLS is Disabled, select **TCP/IP** instead).

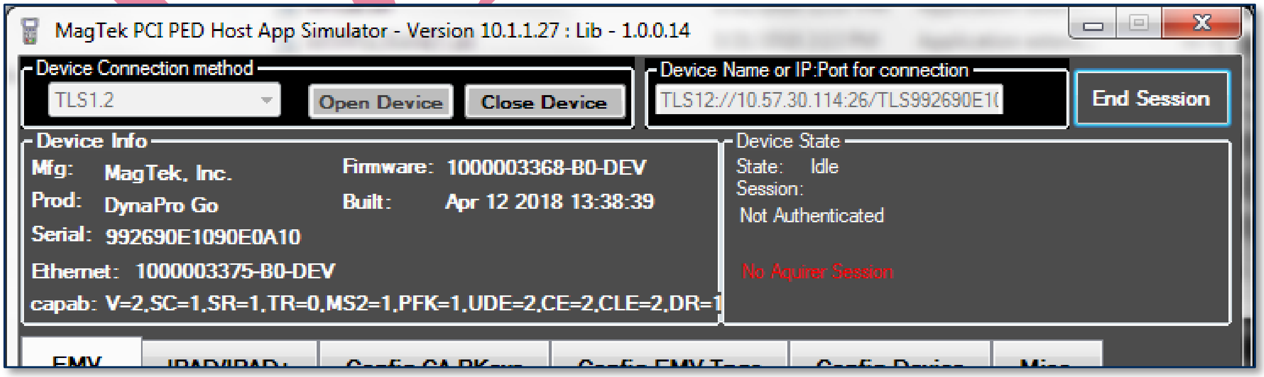


5) In the **Device Name or IP Port for Connection** field, enter **TLS12://aaa.bbb.ccc.ddd:Port/TLSxxxx**, where **aaa.bbb.ccc.ddd** is the IP address of the device, **Port** is the server port of the device (default is port 26), and **TLSxxxx** is the device name.



6) Press the **Open Device** button.

7) If the connection is successful, the device shows **Welcome** on the display, the tool shows the device information, and setup is complete. If the connection is not successful, the tool will show an error. Some failures may also show error codes on the device display.



Mfg: MagTek, Inc.
Prod: DynaPro Go
Serial: 992690E1090E0A10
Ethernet: 1000003375-B0-DEV
capab: V=2,SC=1,SR=1,TR=0,MS2=1,PFK=1,UDE=2,CE=2,CLE=2,DR=1
Firmware: 1000003368-B0-DEV
Built: Apr 12 2018 13:38:39
State: Idle
Session:
Not Authenticated
No Aquirer Session

7) To continue testing, you may use the various tabs in the **MagTek PCI PED Host App Simulator** window to send commands to the device through the wireless connection or to receive transaction data.

5.3.5.2 How to Test a Device Initiated Wireless Connection

The SDK does not provide tools for testing the 802.11 wireless connection when the device is in **Device-Initiated** mode. To test the device in this mode, use the actual host that will be used in the solution:

1) Make sure the network, host, and device are properly configured (see previous sections).
2) Test that there is adequate signal strength between the access point and all locations where the device will operate wirelessly. In each location, open the **Connection Status Screen** and make sure the Received Signal Strength Indicator level (**RSSI**) is greater than **40**.
3) Follow the steps in section **6.7 How to Start a Handheld Transaction Using 802.11 Wireless**.

6 Operation

6.1 About Operating Modes

During operation, tDynamo transitions between distinct modes, each of which implements different device behavior:

- **Reset Mode** occurs when the operator presses and the recessed reset switch or holds the pushbutton for 5 to 10 seconds. After resetting, the device progresses to Powered Off Mode. If the device is connected to USB power, it immediately progresses to Discoverable Mode.
- **Powered Off Mode** is the shipping mode of the device. The operator can power off by pressing and holding the pushbutton, and the device enters this mode automatically if it has been in Sleep Mode for a configurable timeout period. When powered off, the device consumes practically no power. To move the device from Powered Off Mode to Discoverable Mode, press the pushbutton briefly or connect the device to USB power.
- **Battery Status Mode** is a short mode that uses all four Status LEDs to report the current charge level of the device's rechargeable battery (see section Error! Reference source not found. Error! Reference source not found.). The operator activates this mode by tapping the pushbutton briefly in Discoverable Mode or Connected Mode. The device automatically exits to the previous mode after a short period of time.
- **Discoverable Mode** is the device's normal waiting state. The operator activates this mode when the device is not connected to USB by briefly pressing the pushbutton once while in Powered Off Mode. In Discoverable mode, the device remains paired with any previously paired Bluetooth LE hosts, but is not connected to transmit data. Upon entering Discoverable Mode, the device advertises itself over Bluetooth LE, and any paired Bluetooth LE host may initiate a connection. To move the device from Discoverable Mode to Pairing Mode, press and hold the pushbutton for about two seconds until the General Status LED flashes, then release the pushbutton. If the device is not connected to USB power, it moves from Discoverable Mode to Sleep Mode automatically when its configurable timeout period has passed. If the device is configured to transmit data over USB and is connected to a USB host, it progresses from Discoverable Mode to Connected Mode when the host software establishes a USB connection.
- **Pairing Mode** is activated while the device is powered on by pressing the pushbutton for two seconds and waiting for the General Status LED to flash, then releasing the pushbutton. In this mode, an unpaired Bluetooth LE host may initiate pairing. Upon entering Pairing Mode, the device advertises over Bluetooth LE, and continues to be pairable until a Bluetooth LE host pairs with it or until a 2-minute timeout period expires. Upon successful pairing, the device enters Discoverable Mode.
- **Connected Mode** occurs when the host software establishes a connection either via Bluetooth LE or USB, generally in response to the host software's graphical user interface. In this mode, the host and the device can both initiate communication, and it is the Bluetooth LE host's responsibility to terminate the connection and return the device to Discoverable Mode to save power when an active data connection is no longer needed for the current transaction. If the device is not connected to USB power, it moves from Connected Mode to Sleep Mode automatically when its configurable Sleep Mode timeout period has passed. If the device is connected to a Bluetooth LE host, it does not advertise and is not discoverable by other Bluetooth LE hosts. If the device is connected to a USB host, it continues to advertise and is discoverable by Bluetooth LE hosts.
- **Sleep Mode** is a low-power standby state. The device enters this mode automatically when it is not connected to USB power and has been unused (no user input, no communication with the host) for a configurable timeout period. In this mode, the device turns off all wireless functions. To move the device from Sleep Mode to Discoverable Mode, press the pushbutton briefly or connect the device to

USB power. The device moves from Sleep Mode to Powered Off Mode automatically when its configurable Power Off timeout period has passed.

6.2 Operation Overview

When DynaPro Go is ready to begin a new transaction, it shows Welcome on the LCD display.

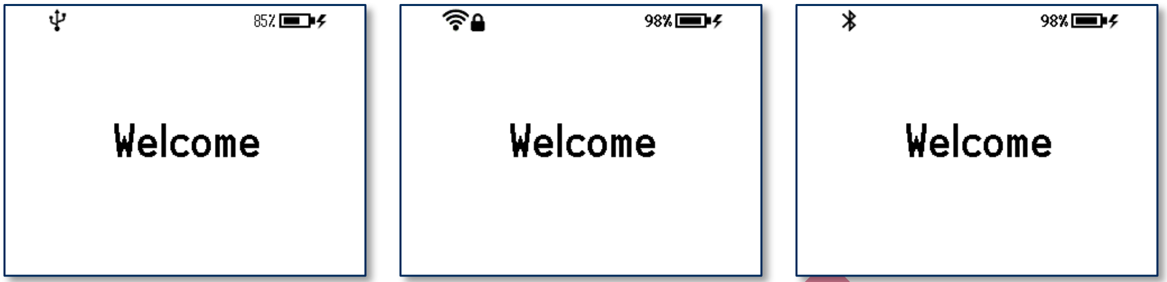


Figure 6-1 - Examples of Welcome Screen (Ready for a New Transaction)

During normal operation, the operator initiates a transaction from the host, and the cardholder enters data on the device's keypad in response to prompts on the LCD display. Transaction types may include new accounts, teller window applications, checking, savings, mortgages, retail transactions, or any other type of transaction where there is interaction between the cardholder and the operator. For each transaction type, the host software can direct the device to prompt the cardholder for any combination of magnetic stripe swipe, EMV contact card insertion, and/or contactless payment tap, and the transaction flow on the device may differ depending on what the host software specifies and what the cardholder does. Section **6.9 Card Reading** provides examples of the cardholder experience for each type of payment. **Figure 6-2** shows a typical point of sale (POS) transaction sequence.

If the device can not read payment data, it may request the cardholder repeat the action, or request the cardholder revert to a different form of payment (such as using the magnetic stripe reader instead of the chip card slot). The device may also prompt the cardholder to identify the card type, such as debit or credit. If the transaction requires a PIN (such as in banking or debit card transactions), the device prompts the cardholder to enter one. In the case of an EMV transaction with a successful chip read, the device uses the transaction amount and the chip card's on-chip risk management to decide whether to process the transaction offline or require online approval.

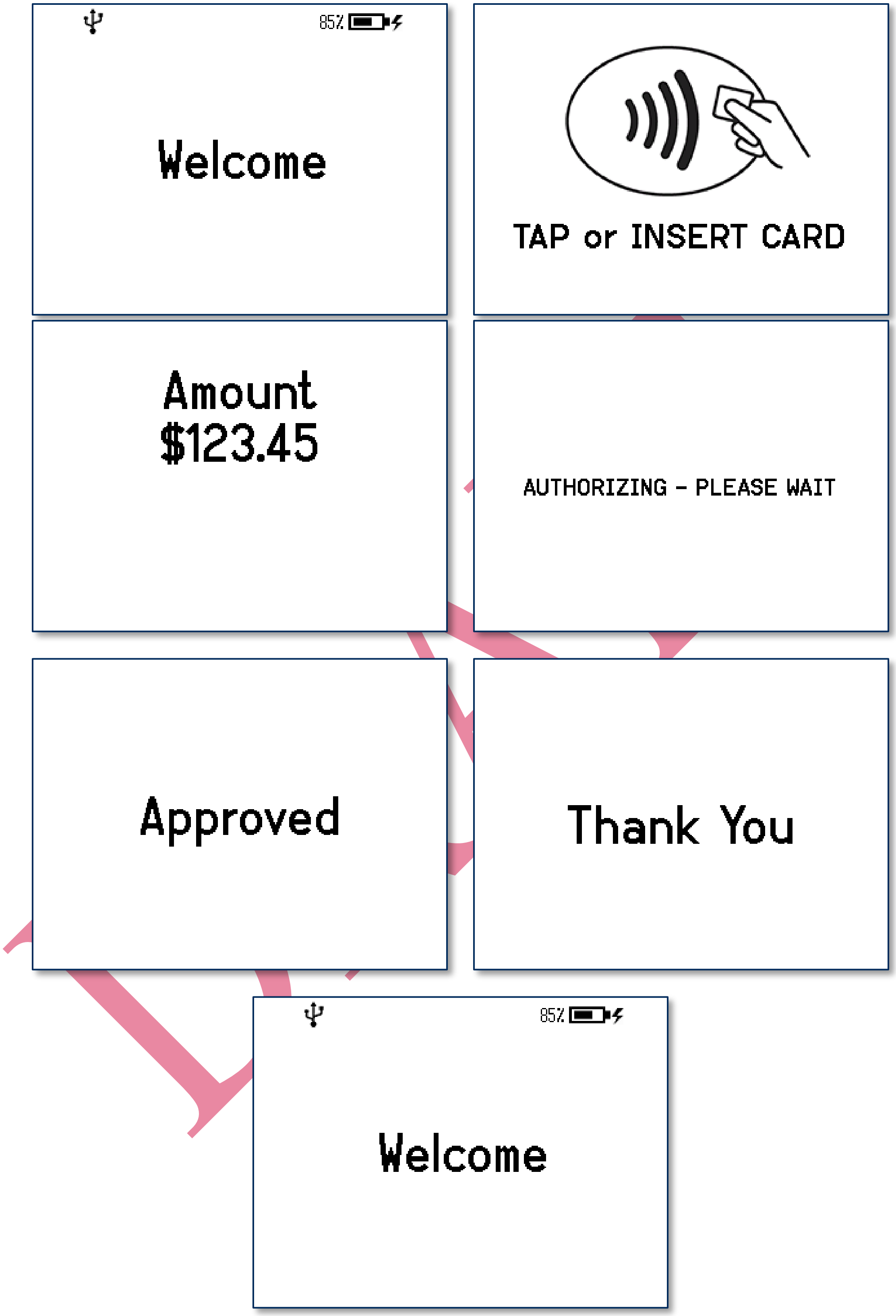


Figure 6-2 - Typical Transaction Sequence

6.3 About the Status LEDs

DynaFlex provides four RGB LEDs directly below the chip card insertion slot (see section **1.9 Major Components**):

- The meaning of each LED depends on the device's operating mode. See **Table 5-1**. The operating mode where operators will most commonly need to explicitly read the device's status is **Active idle**.
- LED colors have specific meanings, as described in **Table 6-2**. They are based on international conventions for traffic light colors, with additional colors reserved for unusual / special cases.
- LED blinking patterns have specific meanings as well, as described in **Table 6-3**. In short, blinking generally means something is in process inside the device, and solid indicates a persistent state that would require an operator or cardholder to take action to change. One major exception is a device-wide functional failure state, such as a tamper state, where all LEDs flash urgently to call the attention of an advanced operator to intervene.

In this manual, specific combinations of LED colors and blinking patterns are specified in more detail in the sections where they are relevant, and use the same icons in the tables below to indicate color and blinking patterns. For example, information about how the LEDs show the device's connection status is in section **4.3 Connecting to a Host**.

Table 6-1 - DynaFlex LED Allocation

In This Context	LED1	LED2	LED3	LED4
Active idle or Active in transaction with **tap disabled**	Power	Connection	Ready for Swipe or Insert	Card Read Result
Active in any transaction with **tap enabled**, EMV design guidelines govern	Armed for Tap	Tap Read Progress	Tap Read Progress	Card Read Result
Device-wide failure	During major failures (such as tamper), **LED1-LED4** report the nature of the failure based on the most likely steps required to resolve it.			

Table 6-2 - DynaFlex LED Colors

Color	Means
🔴 Red	Stop or stopped Example: **Stop** using device: Battery is about to run out of charge.
🟡 Yellow	Wait or waiting Example: **Waiting** for host to connect.
🟢 Green	Go, going, or went Example: Host is connected, device is ready to **Go**.

Color	Means
Other Colors	Reserved

Table 6-3 - DynaFlex LED Patterns

Color	Means
Solid 🔴🟡🟢🔵	**Solid** LED light generally requires an operator or cardholder to take action to change the state the LED is reporting. Example: Host is connected. Cardholder or host would have to disconnect. Example: Host is disconnected. Host would have to initiate connection.
Blinking ◉◉◉◉	**Blinking** LED generally means the device is in the process of doing / attempting something. Blink duty cycle and blink period are generally selected to show urgency or ongoing progress through a series of steps. Example: Device is attempting to connect to the 802.11 access point.
Short time 🔴🟡🟢🔵	LEDs sometimes light for a **short time** to indicate some process has ended (success or failure) and the device is going to transition to another state soon. Example: Successful card read.

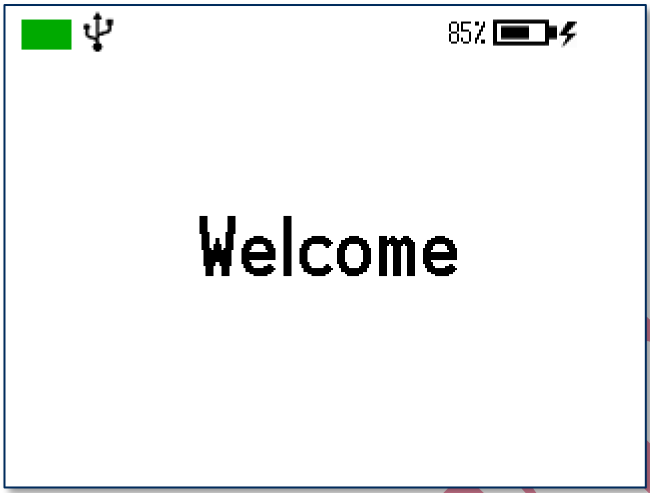
6.4 About the Touchscreen Display

6.4.1 Welcome Screen

The device reports its current status in a set of icons at the top of the Welcome screen. **Table 6-4** shows the icons and their meanings. For example, in **Figure 6-3**, the device is connected to a USB host, the battery level is OK, the device is charging, and it is idle, waiting for the host to initiate a transaction.

Table 6-4 - Status Icon Meanings

Status Icon	Meaning
🟩	A green rectangle appears briefly at the upper left corner of the display every 5 seconds to indicate the device is **Idle**; the device is connected to a host and is ready for the host to initiate a transaction. During tap-enabled transactions, the device uses a strip of four green rectangles at the top of the screen to indicate the progress / success of a tap. See section **6.9.4 How to Tap Contactless Cards / Devices** for details.
🔌	Device's Active Connection is set to USB.
📶	Device's Active Connection is set to 802.11 wireless. The number of dark bars indicates the strength of the signal the device is receiving from the wireless access point (commonly known as RSSI).
ᛒ	Device's Active Connection is set to Bluetooth LE.
🔓 and 🔒	TLS security on the 802.11 wireless connection is Disabled (red open padlock) TLS security on the 802.11 wireless connection is Enabled (black closed padlock)
🔋	Battery is fully charged.
🔋	Battery is OK, between 20% and 95% charged.
🪫	Battery is low, between 10% and 20% charged.
🪫	Battery is critically low, between 3% and 10% charged.
🪫	Battery is empty, below 3% charged.
⚡	Battery is charging.

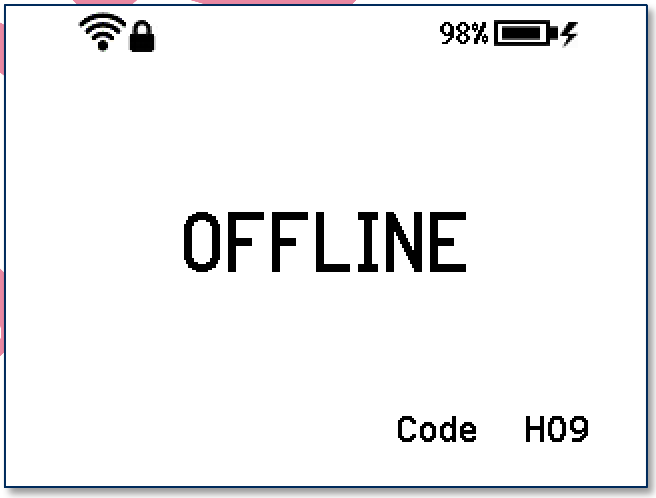


Welcome

Figure 6-3 - Welcome Screen Example

The device may show text other than “Welcome” under certain conditions:

- No Host Connection instead of “Welcome” means the device’s Active Connection is set to USB or Bluetooth LE, but the device is not yet connected to a host.
- Waiting for Host instead of “Welcome” appears when the **Network Connection Mode** is set to **Device Initiated**, and the device has sent the initial request to the host for it to call back and establish a secured connection.
- OFFLINE instead of “Welcome” means the device is not ready for normal operation. When this occurs, the display shows a reason code in the lower right corner. Codes that start with C, H, K, or S indicate a problem that requires the device be returned to the supplier for service or replacement. **Table 6-5** provides full explanations of the prefixes of all OFFLINE codes. ***D998200136 DYNAPRO GO PROGRAMMER'S MANUAL (COMMANDS)*** provides detailed explanations of every individual numerical code, geared toward solution designers.



OFFLINE

Code H09

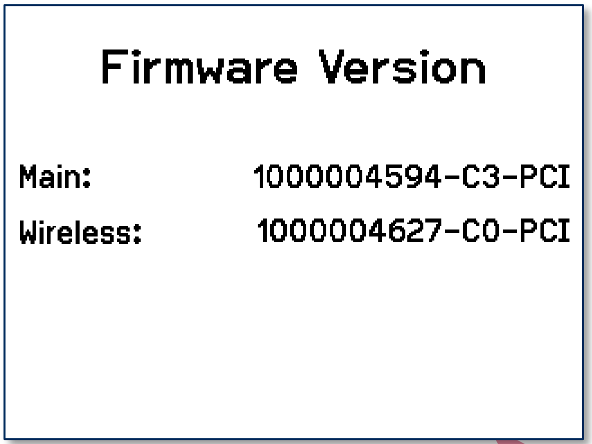
Figure 6-4 - Welcome Screen Showing OFFLINE

Table 6-5 - Device Offline Code Prefixes

Code	Description
A	An offline code beginning with A indicates the device is awaiting authentication. This is a normal condition when a device is configured to require authentication (security level 4). Authentication by the host is required to return it to the Welcome screen.
C	An offline code beginning with C indicates the device is missing a certificate. MagTek recommends repairing or replacing the device.
H	An offline code beginning with H indicates a hardware problem. MagTek recommends repairing or replacing the device.
K	An offline code beginning with K indicates a problem with either the magnetic stripe reader or PIN key. If the device is new, it is likely it has not been loaded with a PIN Key, and should be returned to the supplier for key loading. If a K-code appears after the device has been deployed and used for a long period of time, the K-code indicates one or both DUKPT keys have been exhausted. MagTek recommends contacting the supplier for a replacement.
S	An offline code beginning with S indicates a security element failure. This code can be triggered by severe handling of the device or strong interference by a nearby source of electromagnetic field (EMF) interference. Try moving the device away from any suspected EMF source; if the error persists, the device should be repaired or replaced.
W	An offline code beginning with W indicates an issue or a transient condition pertaining to the device's 802.11 wireless connection.

6.4.2 Firmware Version

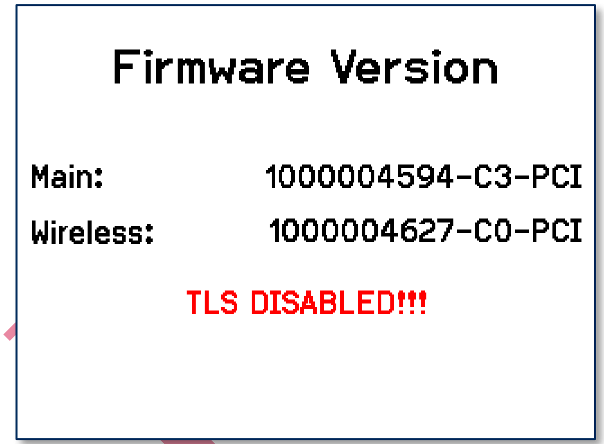
To see details pertinent to the device's PCI certification status, including the installed main firmware and wireless firmware part numbers and revision numbers and a warning if TLS is disabled, on the **Welcome** screen, press the sequence **Left function key**, **7**, **8**, **2**, **Right function key**. To return to the **Welcome** screen, press the **Cancel** key. To determine a device's PCI certification status, compare the contents of this screen to the device's listing on www.pcisecuritystandards.org, ***Approved PTS Devices***. Note that in PCI listings, lowercase "x" is a wildcard meaning 'any single character.'



Firmware Version

Main: 1000004594-C3-PCI

Wireless: 1000004627-C0-PCI



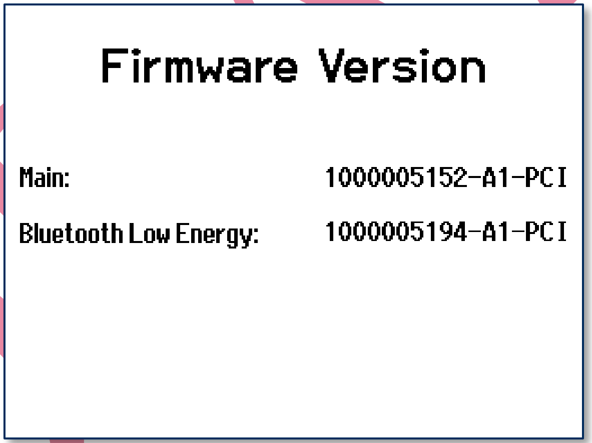
Firmware Version

Main: 1000004594-C3-PCI

Wireless: 1000004627-C0-PCI

TLS DISABLED!!!

Figure 6-5 - Firmware Version Screen for 802.11 Wireless Devices



Firmware Version

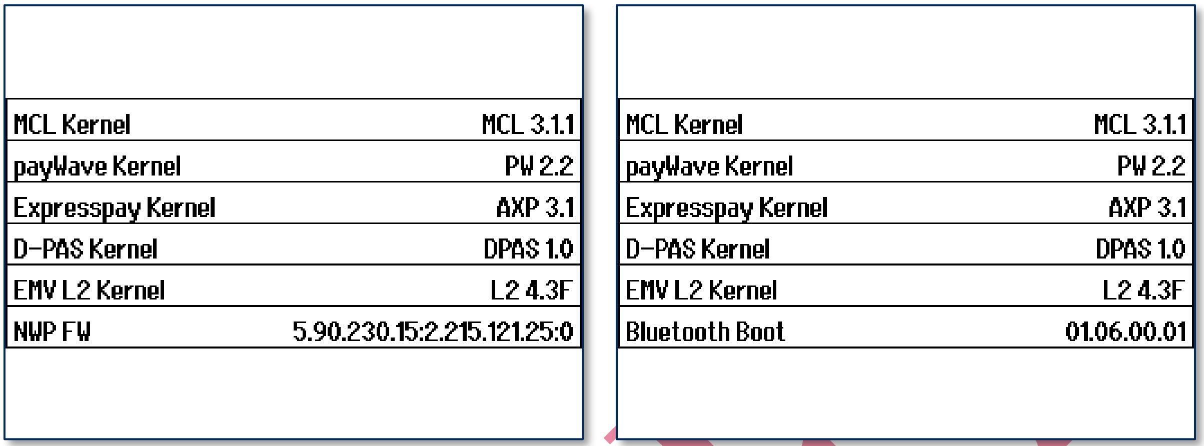
Main: 1000005152-A1-PCI

Bluetooth Low Energy: 1000005194-A1-PCI

Figure 6-6 - Firmware Version Screen for Bluetooth LE Devices

6.4.3 Contactless and Other Details

To see information about the device’s contactless feature and other non-PCI-related version details, on the **Welcome** screen, press the sequence **Left function key**, **7**, **8**, **1**, **Right function key**. To return to the **Welcome** screen, press the **Cancel** key.



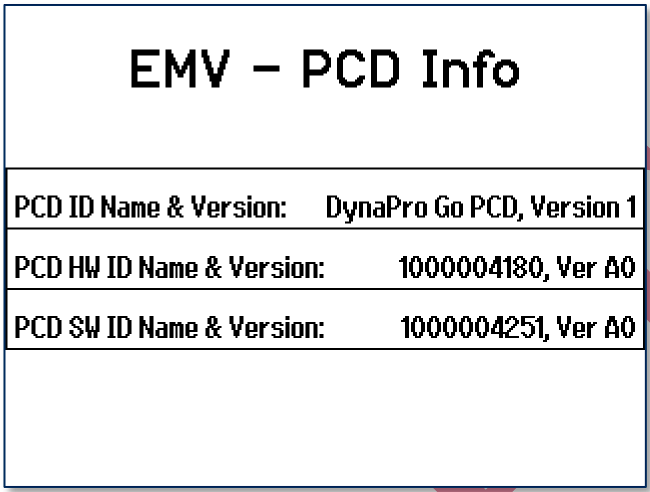
MCL Kernel	MCL 3.1.1
payWave Kernel	PW 2.2
Expresspay Kernel	AXP 3.1
D-PAS Kernel	DPAS 1.0
EMV L2 Kernel	L2 4.3F
NWP FW	5.90.230.15:2.215.121.25:0

MCL Kernel	MCL 3.1.1
payWave Kernel	PW 2.2
Expresspay Kernel	AXP 3.1
D-PAS Kernel	DPAS 1.0
EMV L2 Kernel	L2 4.3F
Bluetooth Boot	01.06.00.01

Figure 6-7 - Examples of Contactless and Other Device Details Screens

6.4.4 EMV Details

To see information pertinent to the device's EMV certification, on the **Welcome** screen, press the sequence **Left function key**, **7**, **8**, **3**, **Right function key**. To return to the **Welcome** screen, press the **Cancel** key.

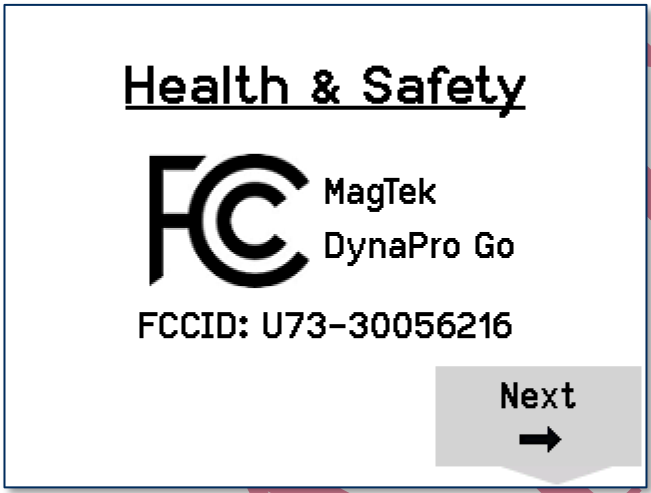


EMV - PCD Info

PCD ID Name & Version:	DynaPro Go PCD, Version 1
PCD HW ID Name & Version:	1000004180, Ver A0
PCD SW ID Name & Version:	1000004251, Ver A0

6.4.5 Health and Safety Information

The device implements electronic labels ("e-labels") that report its Health and Safety certification information. To access them, on the **Welcome** screen, press the sequence **Left Function Key**, **7**, **8**, **0**, **Right function key**. This brings up a page similar to **Figure 6-8**, with indicators on the bottom that show more information is available by scrolling. Press **Left Function Key** and **Right Function Key** to scroll to the previous and next e-label. To return to the **Welcome** screen, press the **Cancel** key, or wait 10 seconds.



Health & Safety

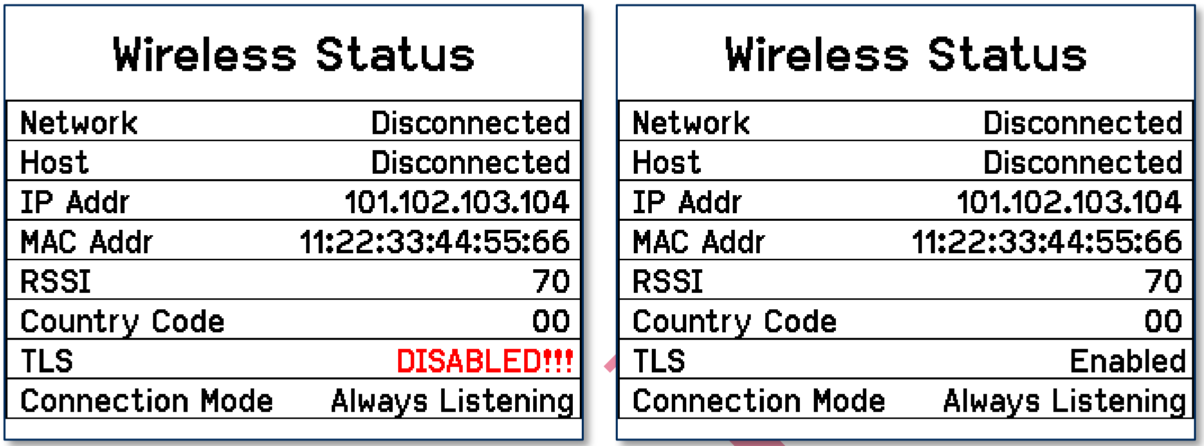
MagTek
DynaPro Go

FCCID: U73-30056216

Figure 6-8 - Health and Safety Screen 1

6.4.6 Connection Status Screen

In addition to the icons at the top of the display, the device has a **Wireless Status** or **Bluetooth Status** screen that reports deeper details about the device's 802.11 wireless or Bluetooth LE connection. To access it, on the **Welcome** screen, press the sequence **Left Function Key**, **6**, **2**, **2**, **Right function key**. This brings up a screen similar to the figures below. To return to the **Welcome** screen, press the **Cancel** key.



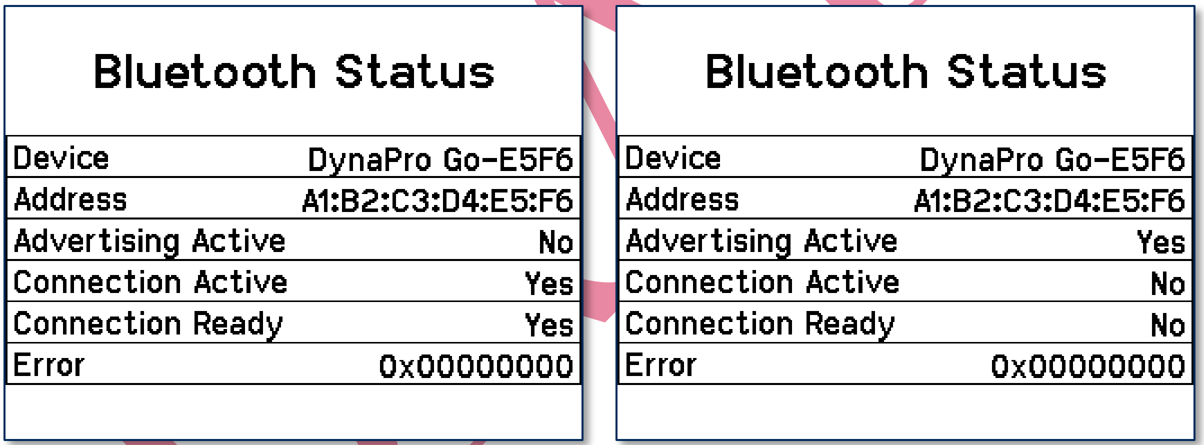
Wireless Status

Network	Disconnected
Host	Disconnected
IP Addr	101.102.103.104
MAC Addr	11:22:33:44:55:66
RSSI	70
Country Code	00
TLS	DISABLED!!!
Connection Mode	Always Listening

Wireless Status

Network	Disconnected
Host	Disconnected
IP Addr	101.102.103.104
MAC Addr	11:22:33:44:55:66
RSSI	70
Country Code	00
TLS	Enabled
Connection Mode	Always Listening

Figure 6-9 - 802.11 Wireless Status Screen



Bluetooth Status

Device	DynaPro Go-E5F6
Address	A1:B2:C3:D4:E5:F6
Advertising Active	No
Connection Active	Yes
Connection Ready	Yes
Error	0x00000000

Bluetooth Status

Device	DynaPro Go-E5F6
Address	A1:B2:C3:D4:E5:F6
Advertising Active	Yes
Connection Active	No
Connection Ready	No
Error	0x00000000

Figure 6-10- Bluetooth LE Status Screen

For compatibility with similar MagTek devices, this screen may also launch with keystrokes **Left function key** **4** **7** **2** **Right function key**.

In addition to information about the device, the **Bluetooth Status** screen shows whether the device is currently advertising (**Advertising Active**), whether the host has established a Bluetooth LE connection (**Connection Active**), and whether the host has secured that connection and configured it to properly communicate with the device (**Connection Ready**). **Connection Ready** must show **Yes** before the device can process transactions. It is normal for the device to stop advertising after the host has established a connection. The **Error** value is reserved for future use.

6.5 About Sounds

tDynamo’s beeper provides feedback to operators and cardholders about the internal state of the device:

- The device sounds one short beep on startup to test the beeper and indicate the device is powered on.
- The device sounds one short beep after it has successfully read a contactless tap, and the cardholder can safely remove the card or device from the contactless landing zone.
- The device sounds two beeps when an operator cancels a pending EMV transaction.
- The device sounds two short beeps when an operator successfully powers it off.

6.6 Power Management

6.6.1 About Power

This device incorporates a built-in Lithium-ion rechargeable battery, which requires very little maintenance. It is not subject to “charge memory” and therefore does not require deep discharge cycles to restore its charge capacity like many other battery technologies.

When properly powered through its USB port, the device powers on automatically, remains powered on, and draws power both for operation and for recharging the battery (see section **Error! Reference source not found. Error! Reference source not found.**). While charging, the device consumes more power from the USB connection than when the battery is fully charged. The device stops charging the battery when it determines it is optimally full, to prevent overcharging.

If the device is not connected to USB power, or if the USB connection does not provide enough power, the device powers itself using the rechargeable battery. When the battery discharges to a critically low level, the device powers down automatically. In this state, the device continues to power its active tamper detection circuitry using the device’s non-rechargeable backup battery. If both batteries are allowed to completely discharge, tamper detection engages, and the device must be returned to the manufacturer to reset. To minimize battery drain and prevent this from occurring:

- When charging, make sure the device is receiving enough power from the USB connection (battery level should increase even when device is in use).
- Power the device OFF when not in use (see section **Error! Reference source not found. Error! Reference source not found.** and section **6.6.6 How to Turn Bluetooth LE Advertising On and Off**).

The device’s rechargeable battery is designed to last hundreds of charging cycles, but with time and / or with use, its charge capacity will naturally degrade. To maintain the battery’s charge capacity as much as possible, follow these guidelines:

- Do not discharge the battery to 0%. Create a charging schedule that recharges the battery well before it is fully depleted.
- Store the device at the lowest reasonable temperatures within its specified storage temperature range (see **Error! Reference source not found. Error! Reference source not found.**; below 77°F / 25°C is optimal). Temperature is the most critical factor in extending battery life.
- Store the device with the battery charged to less than 100% (40% is optimal).

6.6.2 How to Check Battery Level

To check the battery charge level, make sure the device is powered on and awake, then briefly tap the pushbutton. The Status LEDs light to show the battery level as follows:

- **One** LED = Battery level is **under 50%**
- **Two** LEDs = Battery level is between **50% and 70%**
- **Three** LEDs = Battery level is between **70% and 90%**
- **Four** LEDs = Battery level is **above 90%**

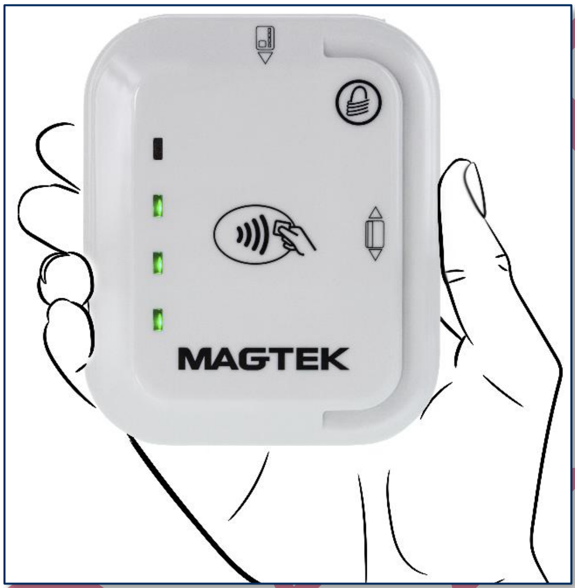


Figure 6-11 - Status LEDs Showing Battery Level

When the device is in Connected mode (see section **6.1 About Operating Modes**), the General Status LED blinks periodically to indicate the device is ready for the host to send a command or for a cardholder to swipe a magnetic stripe card. The color of the blink indicates the battery level. See section **6.3 About the Status LEDs** for details.

Custom host software may also query the device and show its current charge level on the host display at all times for convenience. For details, see section Error! Reference source not found. Error! Reference source not found..

6.6.3 How to Charge the Battery

DynaPro Go has an onboard rechargeable battery to supply its own power when it is not powered through its USB port. The battery must be periodically recharged by connecting it to the available charging cradle, or to a USB port or stand-alone USB charger. Both the charging cradle and the device require a USB power supply that can provide at least **500mA @ 5V**.

To charge the device using a micro-USB cable, connect it to a USB charger, or to a USB host as shown in section **4.3.2 How to Connect DynaPro Go to a Host or Charger via USB** on page **27**.

To charge the device in the charging cradle **for power only (no USB communication)**:

1) Connect the charging cradle to a USB port or to a USB charger.
2) Place the device in the charging cradle with the charging contacts pointing into the charging cradle and the LCD display facing front.

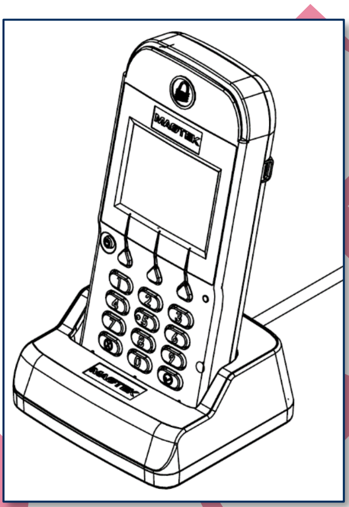


Figure 6-12 - Device In Charging Cradle

A full recharge cycle for a completely drained battery takes approximately 6 hours.

tDynamo has an onboard rechargeable battery to supply its own power when it is not powered through its USB-C connector or docking stand connectors. The battery must be periodically recharged by connecting it to the optional docking stand, or to a USB port or stand-alone USB charger using a USB-C cable. Both the docking stand and the USB-C connector require a USB connection that can provide at least **500mA @ 5V**. A full recharge cycle for a completely drained battery takes approximately 4.5 hours.

To charge the device using a USB-C cable, connect it to a USB charger or to a USB host as shown in section Error! Reference source not found. Error! Reference source not found..

To charge the device in the docking stand, see section **4.4.3 How to Temporarily Dock tDynamo**.

6.6.4 How to Power On / Wake Up from Sleep Mode / Power Off

The device powers on in several ways:

- An operator presses and holds the **Power button** for one to two seconds.
- An operator connects the device to USB power.
- The host establishes a Bluetooth LE connection. This only works if the device is advertising (see section **6.6.6 How to Turn Bluetooth LE Advertising On and Off**).

After powering on, the device displays the **Welcome** screen and the current device status (see section **6.4 About the Touchscreen Display**).

The device powers off in several ways:

- The operator presses the **Power button** for two seconds to display a **Power Off?** screen with a **Yes** / **No** selection, then presses the function key below **Yes**. While the device is powering off, it displays a **Powering Off…** screen for three seconds before the display turns off. In this mode, if the device implements a Bluetooth LE connection, it continues to advertise. While on the prompt screen, the operator may also cancel powering off and return to the **Welcome** screen by waiting 10 seconds or by pressing the function key below **No**.
- If the device has a Bluetooth LE connection, it powers off automatically a few seconds after the host closes the connection.
- If the device implements a Bluetooth LE connection, it powers off automatically if the host does not have an active Bluetooth LE connection and there has been no operator or cardholder activity during a configurable timeout period.
- The operator resets the device as described in section **Error! Reference source not found. Error! Reference source not found.**.
- The device powers off automatically to conserve power when it does not have an active connection to the host and is not connected to USB power, and there has been no operator or cardholder activity during a configurable timeout period. The device shows **Sleeping…** for three seconds before the display turns off. To wake it up, press and hold the **Power button** for one to two seconds or connect it to USB power.

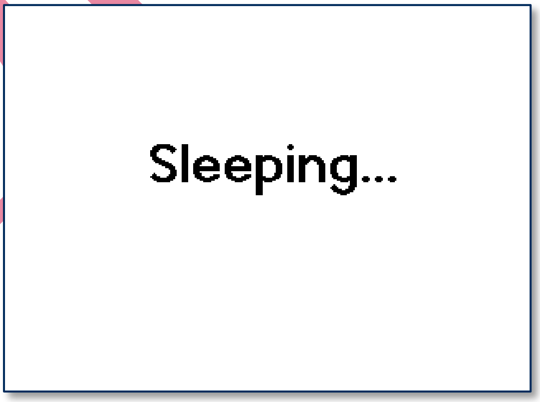

Sleeping...

Figure 6-13 - Device Powering Off Automatically After Timeout

If all LEDs are off, the device is in Powered Off mode. If the General Status LED is solid red and LED 3 is solid green, the device is in Sleep Mode. To power on the device or to wake it from Sleep Mode, tap the pushbutton. In response, the device lights all of the Status LEDs to perform a quick LED test, then transitions to either Discoverable Mode or Connected Mode. For details, see section **6.1 About Operating Modes** and section **6.3 About the Status LEDs**.

To power off the device, press and hold the pushbutton for 5 to 10 seconds until all LEDs turn off and the device beeps twice.

6.6.5 How to Force Reset

To force the device to reset, use a small tool such as a paperclip to carefully press the reset switch recessed inside the small hole on the back of the device (see Error! Reference source not found.).

An operator can perform a hard reset to a “deep off” state by pressing and holding the power button for 15 seconds, then releasing it. In all cases, the device indicates it is resetting by powering off the display:

- On some devices, the device resets while the operator is holding the button.
- On some devices, the operator must release the button after holding it for 15 seconds, then release it to reset the device.

After performing a hard reset, if the device is connected to USB power, it will immediately power back on. If the device is battery powered, operators can power it on the usual way (see section **Error! Reference source not found. Error! Reference source not found.)**.

The device also resets to the “deep off” state if the battery is allowed to completely discharge (see section **6.6.7 About Battery Warnings and Automatic Reset**).

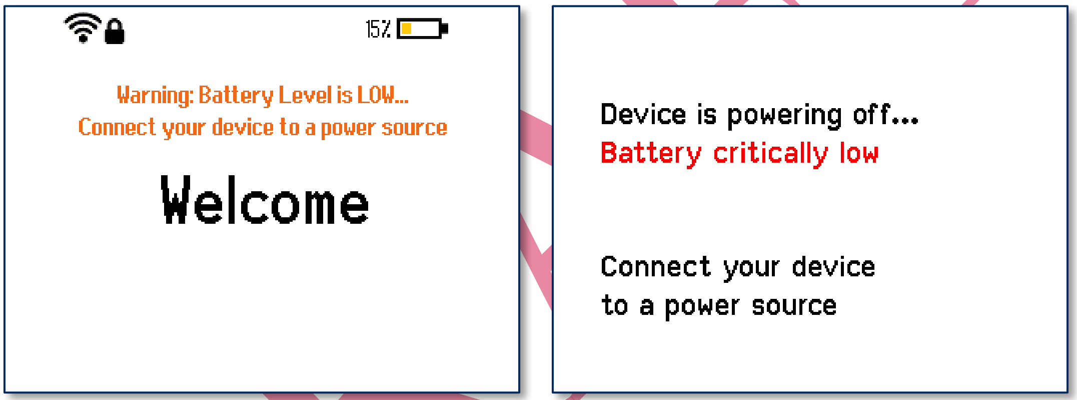
6.6.6 How to Turn Bluetooth LE Advertising On and Off

In its default configuration, the device’s Bluetooth LE module can be put into a deep sleep mode where it does not advertise, which saves power and stops radio emissions for airline travel. The device’s processor and display also power down in this mode, which is known as **Airplane Mode**. Operators can put the device into Airplane Mode by performing a hard reset (see section **Error! Reference source not found. Error! Reference source not found.**). Upon powering back on, the device will resume advertising.

For information about reconfiguring the device to behave differently from defaults, see the references provided in section 8 **Developing Custom Software**.

6.6.7 About Battery Warnings and Automatic Reset

When the battery is running low, the device shows Warning: Battery Level is LOW… Connect your device to a power source on the Welcome screen. When the battery is discharged to the point that the device can no longer function properly, the device attempts to complete any pending transaction, then shows Device is powering off … Battery critically low for three seconds before resetting automatically. See section **Error! Reference source not found. Error! Reference source not found.** for details on recharging. See section **Error! Reference source not found. Error! Reference source not found.** for information about device behavior in the reset state.



15%

Warning: Battery Level is LOW...
Connect your device to a power source

Welcome

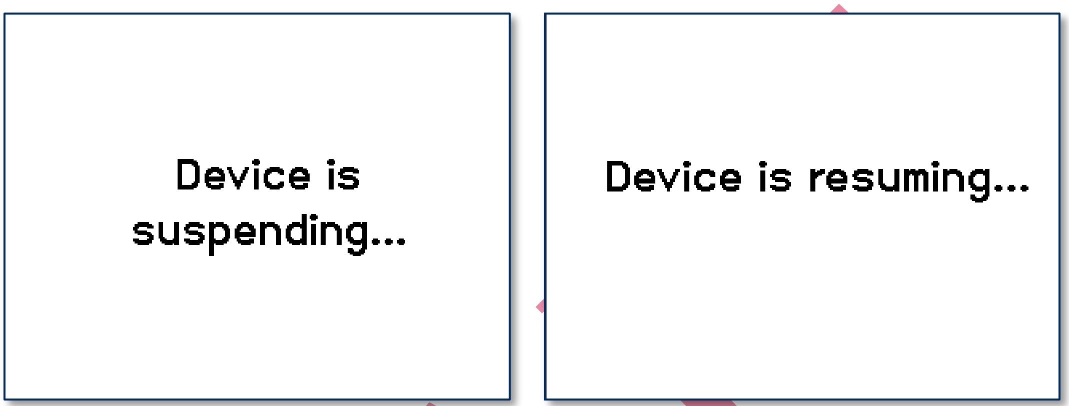
Device is powering off...
Battery critically low

Connect your device
to a power source

Figure 6-14 – Battery Level is LOW Warning / Battery Critically Low

6.6.8 About USB Suspend

When the device is connected to a host via USB and its Active Connection is set to USB (see section **5.2 How to Change the Active Connection** and section **4.3.2 How to Connect DynaPro Go to a Host or Charger via USB**), the host can use standard USB functions to put the device into **USB Suspend** mode. When this happens, the device shows **Device is suspending…** for three seconds before the display goes blank. When the host wakes up the device from USB Suspend, the device shows **Device is resuming…** for three seconds, then returns to normal operation. The operator can also resume by pressing and holding the **Power button** for two seconds.



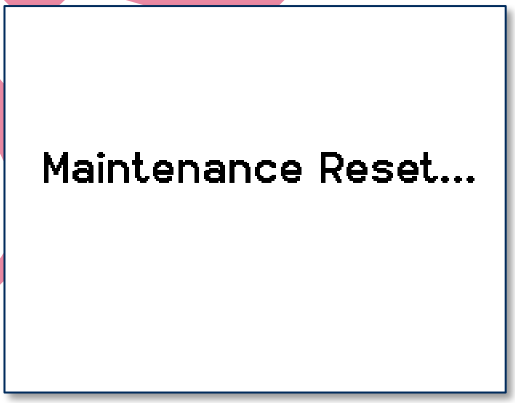
Device is suspending...

Device is resuming...

Figure 6-15 - Device Responding to Host-initiated USB Suspend

6.6.9 About Maintenance Reset

For security purposes, the device is designed to perform an automatic maintenance reset periodically to clear all data from memory. When the device has been on continuously for 23 hours, it stops responding to new commands, shows **Maintenance Reset…** on the display, and performs a full reset. If a transaction is pending, the device waits a reasonable period of time for the transaction to complete before resetting. At the end of the automatic maintenance reset, the device powers back on and returns to normal operation.



Maintenance Reset...

Operators can reset the device manually by powering it off and powering it back on. It is also possible for the host software to initiate a device reset by sending a command.

6.7 How to Start a Handheld Transaction Using 802.11 Wireless

DynaPro Go models that provide an 802.11 wireless connection can be configured to start transactions in one of two ways: **Always Listening**, where an operator would generally initiate a transaction from a point of sale or similar host, or **Device-Initiated**, where an operator initiates a transaction from the device keypad.

In solutions designed for handheld / roving operation using **Device-Initiated** mode, an operator uses the device keypad to remotely signal the host to start a transaction by following these steps:

1) Make sure the device is connected to a wireless access point and has good signal strength (see section **6.4 About the Touchscreen Display)**.
2) On the **Welcome** screen, press **Left Function Key** **1** **2** **3** **Right Function Key**. The device sends a signal to the host that it wants to initiate a transaction, and shows **Waiting for Host** on the display.
3) The host responds to the request by initiating a connection (if TLS is enabled, the connection will be secured by TLS). If the host doesn't respond, the device shows an error on the display and terminates the operation. If the error was a temporary issue (such as a network outage or out of range), the operator may repeat the previous steps to initiate the transaction again.
4) Depending on how the host software is designed, the host sends various messages requesting that the cardholder or operator enter additional information, and the device requests payment as described in section **6.9 Card Reading**.
5) If the device is not charging, and there is no network activity or user interaction for 2 minutes, the device closes the wireless connection automatically and powers down to conserve power. If this occurs in the middle of a transaction, the host should cancel the transaction and the operator should repeat these steps to initiate the transaction again.

In solutions designed for transactions initiated at the point of sale using **Always Listening** mode, an operator uses the point of sale to start a transaction by following these steps:

1) Make sure the device is powered on.
2) Make sure the device is connected to a wireless access point and has good signal strength (see section **6.4 About the Touchscreen Display)**.
3) Start the transaction using the point of sale's interface (see the point of sale documentation for details). Depending on how the host software is designed, the host sends various messages requesting that the cardholder or operator enter additional information, and the device requests payment as described in section **6.9 Card Reading**.
4) If the device is not charging, and there is no network activity or user interaction for 2 minutes, the device closes the wireless connection automatically and powers down to conserve power. If this occurs in the middle of a transaction, the operator should cancel the transaction on the point of sale and repeat these steps to initiate the transaction again.

6.8 How to Start a Handheld Transaction Using the Bluetooth LE Connection

To initiate a transaction when the device is connected to the host via the Bluetooth LE connection, follow these steps:

1) Start the transaction using the point of sale's interface (see the point of sale documentation for details). After the host establishes a Bluetooth LE connection to the device, the device powers on automatically. If it does not, power on the device manually, make sure the device's active connection is set to Bluetooth LE (see section **6.4 About the Touchscreen Display** and section **5.2 How to Change the Active Connection**), and make sure the device is advertising (see section **6.6.6 How to Turn Bluetooth LE Advertising On and Off**).
2) Depending on how the host software is designed, the host sends various messages requesting that the cardholder or operator enter additional information, and the device requests payment as described in section **6.9 Card Reading**.
3) Upon completion of the transaction, the host software should close the Bluetooth LE connection. After a short period of time, the device powers off automatically to conserve power.

6.9 Card Reading

6.9.1 About Reading Cards

The steps for starting a transaction and reading a card or contactless payment device are different depending on tDynamo's configuration and on the design of the host software. Host software developers should see section Error! Reference source not found. Error! Reference source not found. for implementation references. The solution developer should provide solution-specific instructions for operators to follow. A transaction generally follows this essential flow:

1) An advanced operator has already made sure tDynamo is configured properly and is connected to the host (see section Error! Reference source not found. Error! Reference source not found.). When the device is connected to the host via USB and powered by the USB-C connector or docking stand, the host software may always keep a connection open to the device. When connected to the host via Bluetooth LE, the device must already be paired with the host, and the host must be initiate a Bluetooth LE connection to process a transaction, then would generally disconnect after the transaction is complete to conserve power.
2) The operator makes sure tDynamo is receiving power either from its rechargeable battery or from one of the USB connections, and is awake and powered on (see section **6.6.4 How to Power On / Wake Up from Sleep Mode / Power Off** and section Error! Reference source not found. **About the Status LEDs**).
3) The operator uses the host user interface (for example, a point of sale) to finalize a transaction amount, then initiates a transaction.
4) The host communicates with the device, and reports to the operator when the device is ready.
5) The operator directs the cardholder in presenting payment.
6) The cardholder interacts with the device to present payment. The following sections provide additional details about presenting each of the available payment methods.
7) Because the device does not have its own display, the device may send messages to the host prompting the cardholder to perform certain actions; the host software should process these requests by displaying the requested messages, and depending on the placement of the host display(s), the operator may need to relay the messages to the cardholder. For example:
    a) If the device can not read the card, it may prompt the cardholder to swipe, insert, or tap again.
    b) If the device repeatedly can not read a chip card, it may revert to using the magnetic stripe reader instead of the chip card slot. This is known as **EMV fallback**.
8) The device reports the success or failure of the transaction to the host, which should report the results to the operator.

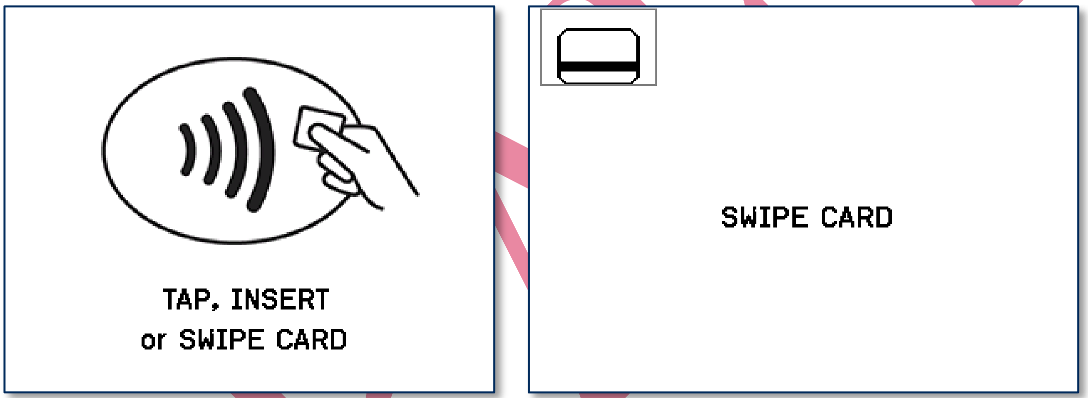
6.9.2 How to Swipe Magnetic Stripe Cards

To swipe magnetic stripe cards, cardholders should:

1) Wait for the device to display an action prompt (see **Figure 6-16** for examples).
2) Locate the magnetic stripe reader on the top of the device, shown in **Figure 6-17**.
3) Orient the card with the magnetic stripe facing away from the padlock logo on the magnetic stripe reader.
4) Swipe the card through the magnetic stripe reader.

If the device can not read the card's magnetic stripe data, it prompts the cardholder to swipe the card again. If the device notifies the host that it is unable to read payment information for the transaction, the host software may choose to revert to prompting the operator to enter card data manually (see section **6.9.5 How to Enter Card Information Manually)**.

Immediately after the user swipes a magnetic stripe card, the device disables the option to use the contactless interface. If the cardholder needs to revert to a contactless card or device for payment while a transaction is in process, the operator should cancel the transaction and start again.



TAP, INSERT
or SWIPE CARD

SWIPE CARD

Figure 6-16 - Example Card Swipe Screens

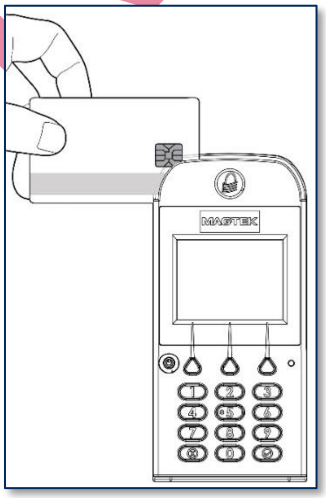


Figure 6-17 - Swiping a Magnetic Stripe Card

6.9.3 How to Insert Contact Chip Cards

To insert contact chip cards, cardholders should:

1) Wait for the display to show an action prompt. If the host has directed the device to accept contactless payments for the transaction, the device toggles between the transaction amount and an action prompt (see **Figure 6-18** for examples).
2) Locate the slot on the front of the device shown in **Figure 6-19**.
3) Orient the chip card so the chip faces the ceiling and toward the slot.
4) Insert the chip card into the slot, then push gently on the card until it stops. There should not be any substantial resistance until the chip card is fully inserted.
5) Wait for the device to prompt with REMOVE CARD, then remove the card.

If the device can not communicate with the chip card, it prompts the cardholder to INSERT AGAIN up to three times, then prompt the cardholder to use the magnetic stripe reader (if the host has directed the device to accept magnetic stripes for the transaction). If the device notifies the host that it is unable to read payment information for the transaction, the host software may choose to revert to prompting the operator to enter card data manually (see section **6.9.5 How to Enter Card Information Manually)**.

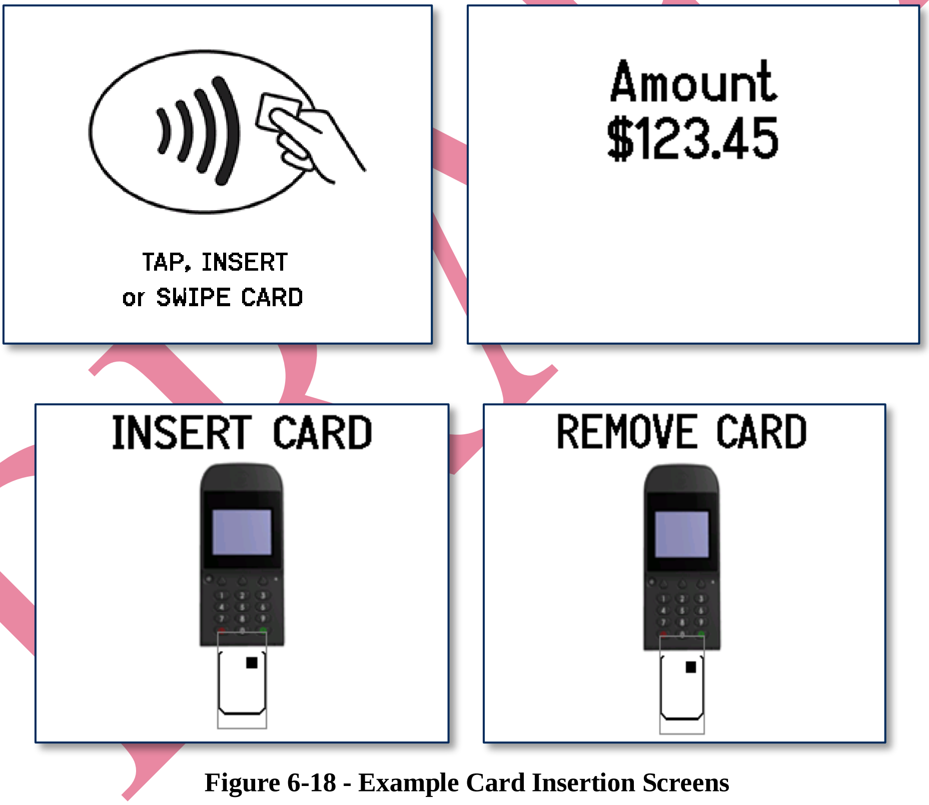


Figure 6-18 - Example Card Insertion Screens

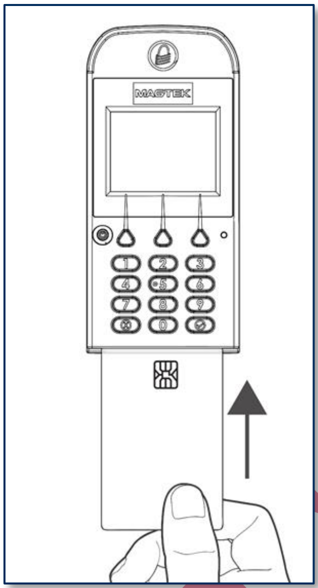


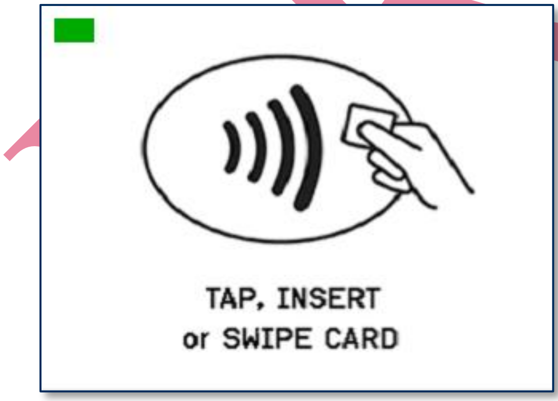
Figure 6-19 - Inserting a Chip Card

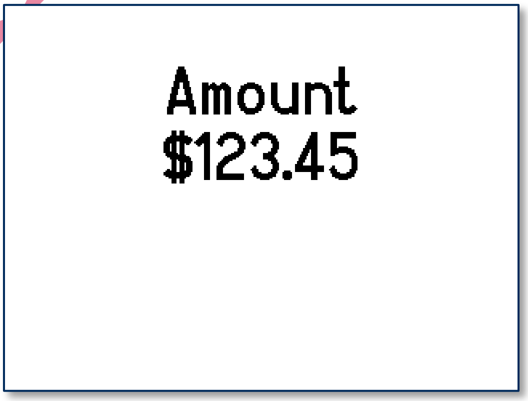
6.9.4 How to Tap Contactless Cards / Devices

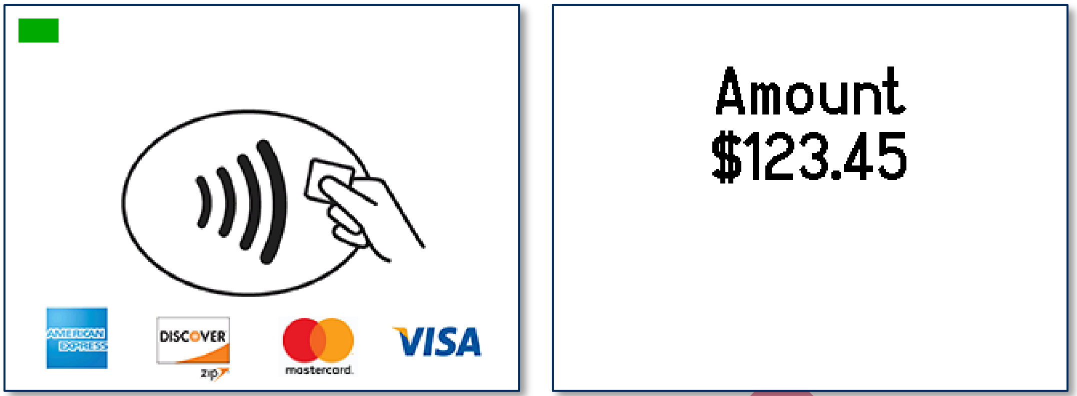
To tap a contactless card or smartphone, cardholders should:

1) Wait for the display to toggle between the transaction amount and an action prompt (see **Figure 6-20** for examples). The device also shows a solid green rectangle at the upper left corner of the display indicating it is ready for a tap.
2) If the cardholder is using an electronic payment device, such as a smartphone, make sure the payment device has NFC turned On and has a payment app configured to process transactions. For details, see the documentation provided by the smartphone manufacturer and payment app publisher.
3) Wait until the device's General Status LED lights solid green, indicating it is ready for a tap.
4) Briefly hold the card, smartphone, or other contactless payment device over the contactless landing zone, indicated by the EMVCo Contactless Indicator symbol on the device's face (see Error! Reference source not found.). The device quickly shows two solid green rectangles at the upper left to show it is processing, then three rectangles to show it has successfully read the tap, then four rectangles to show the read is complete (see **Figure 6-22**). The device also beeps when the read is complete.
5) Wait for the four Status LEDs to light green and for the device to beep. Because each smartphone model may have its NFC antenna placed differently, the ideal tap position may vary by make and model. For example, Samsung users may need to center the phone on the contactless landing zone, while Apple users may need to tap the top of the phone on the contactless landing zone.
6) Remove the card or electronic payment device from the contactless landing zone.

If the device can not communicate with the card, smartphone, or other contactless payment device, it may prompt the cardholder to tap again, or to insert the card, or to use the magnetic stripe reader. The rules the device uses to choose when to revert to a different payment type are driven by the various payment brand specifications and by the list of payment types the host software has directed the device to accept for the transaction. If the device notifies the host that it is unable to read payment information for the transaction, the host software may choose to revert to prompting the operator to enter card data manually (see section **6.9.5 How to Enter Card Information Manually)**.


TAP, INSERT
or SWIPE CARD


Amount
$123.45



Amount
$123.45

Figure 6-20 - Example Contactless Transaction Screens

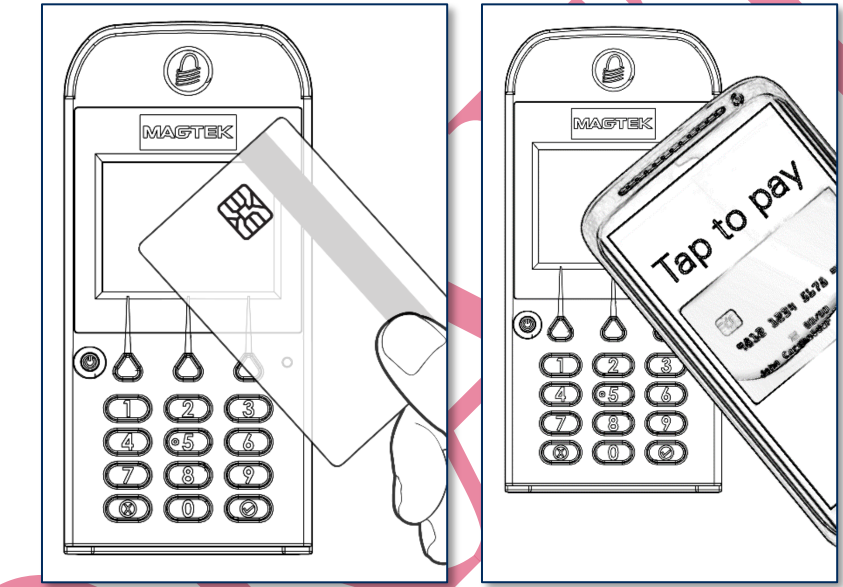


Figure 6-21 – Tapping a Contactless Card / Smartphone

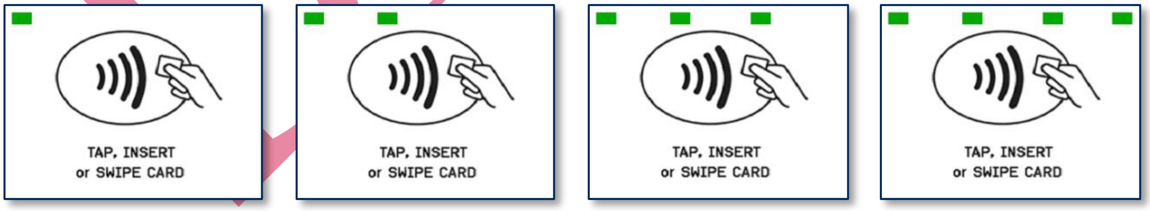
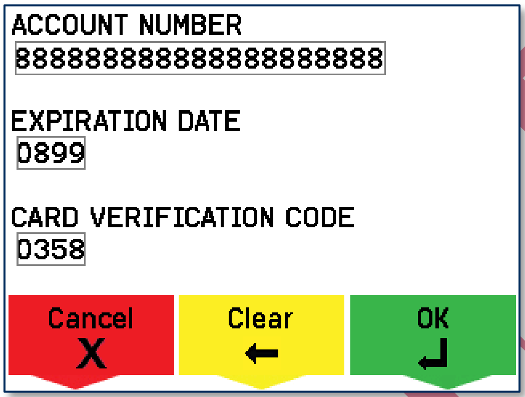


Figure 6-22 - Tap Read Is Complete

6.9.5 How to Enter Card Information Manually

Upon failing all available methods for reading the cardholder's payment information, or upon transaction timeout or a user-initiated **Cancel** operation, the host software and operator may opt to enter card data manually, as shown in **Figure 6-23**.

During manual entry, the device expects the account number to be between 16 and 19 digits long, the expiration date to be 4 digits long, and the card verification code (generally found on the rear of the card for MasterCard and Visa, or the front of the card for American Express) to be 3-4 digits long.



ACCOUNT NUMBER
888888888888888888888

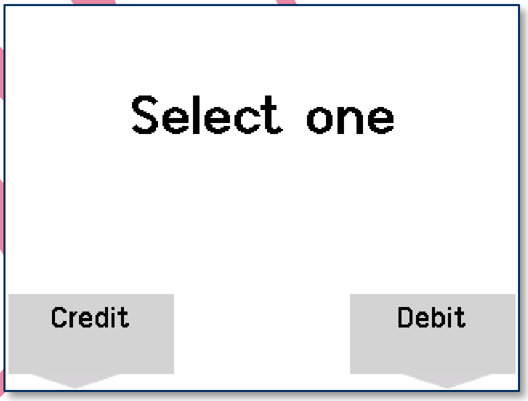
EXPIRATION DATE
0899

CARD VERIFICATION CODE
0358

Figure 6-23 - Example of User Screen to Manually Enter Card Data

6.9.6 How to Select the Card Type

In a retail setting, the transaction might require the cardholder to select the card type (for example, Credit or Debit). For example, **Figure 6-24** shows the device is prompting the cardholder to press a function key on the keypad to select **Credit** or **Debit**.

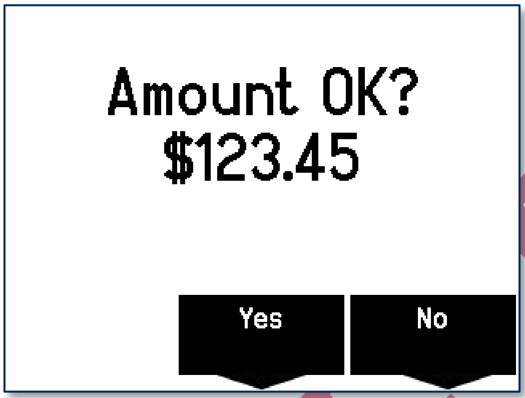


Select one

Figure 6-24 - Example of User Screen to Select Card Type

6.10 How to Verify the Transaction Amount

In a retail setting when the customer selects **Credit**, the device prompts them to verify the amount of the transaction. The customer can select **Yes** or **No** using the function keys below the selections available on the screen, as shown in **Figure 6-25**.

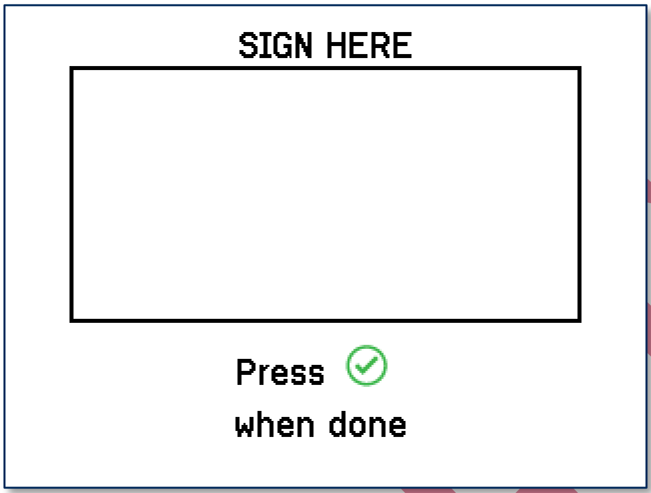


Amount OK?
$123.45

Figure 6-25 - Example User Screen to Verify Amount

6.11 How to Use Signature Capture

When prompted to SIGN HERE, cardholders should use the tips of their fingers to press and glide against the screen. **Do not use a stylus or other hard object.**



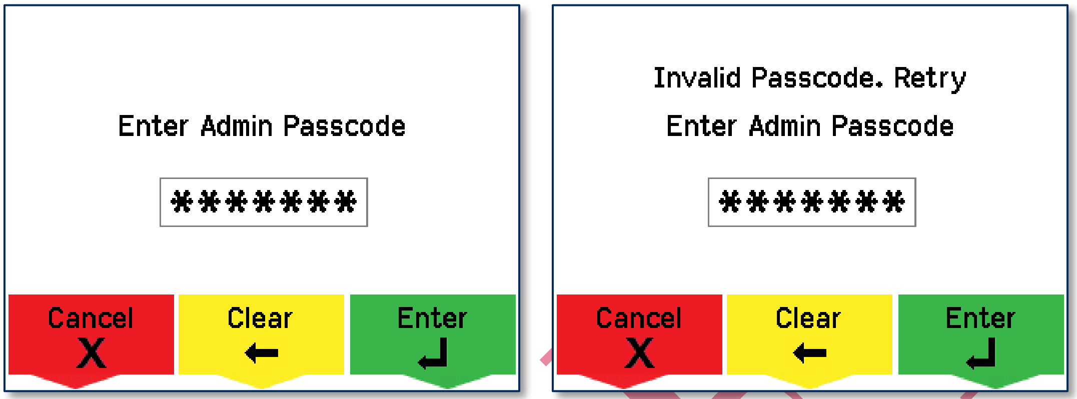
SIGN HERE

Press ✓

when done

6.12 How to Enter Passcodes

Some device operations require the operator to enter a passcode before the operation can proceed. In these cases, the device's display prompts the operator to **Enter Admin Passcode**. The operator should key in **1** **3** **9** **7** **2** **6** **8** **4** **Enter**. The device shows asterisks masking the passcode the operator is entering. If the operator makes a mistake, the **Clear** button clears the passcode field so the operator can start over, and the **Cancel** button cancels the operation that required the passcode.



Enter Admin Passcode

****

Invalid Passcode. Retry

Enter Admin Passcode

****

Figure 6-26 - Passcode Prompt Screens

7 Maintenance

7.1 Mechanical Maintenance

Periodic cleaning of DynaPro Go's exterior may be required. To clean the outside of DynaPro Go, including the LCD display, wipe down the device with a soft, damp cloth and then wipe with a dry cloth.

MagTek's double-sided cleaning card ***96700004*** is designed to clean the magnetic read head in the MSR swipe path and the contact pins inside all chip card contact readers. Keeping both of these components clean is essential to the device's functioning. MagTek recommends swiping and inserting a cleaning card once per week to avoid card misreads.

⚠CAUTION

To avoid damaging the read head, only clean the card path with approved cleaning cards. DO NOT use liquid cleaning products or insert any other objects into the device.

7.2 Updates to Firmware, Documentation, Security Guidance

In addition to the security guidance in the product manuals, MagTek may provide updates to this document, as well as supplemental security guidance or notices regarding vulnerabilities, at www.magtek.com. MagTek advises checking the product's home page periodically for the most up-to-date information.

Any firmware updates addressing product features, bugs, or security vulnerabilities are also posted to www.magtek.com or may be sent directly to affected customers. To update the device's firmware:

1) Obtain the firmware image to install.
2) Download the firmware package ***1000003817 SOFTWARE, FIRMWARE UPDATE, MTPPSCRA GUI, IPAD, DYNAPRO, DYNAPRO MINI, DYNAPRO GO*** from MagTek.
3) Follow the instructions in ***D998200145-REV.pdf*** included in the firmware update utility's **Document** subfolder.

8 Developing Custom Software

Custom host software uses the same underlying device command set for all tDynamo connection types (USB or Bluetooth LE). The device commands are wrapped differently depending on the physical connection type and the device's configuration. The following sections provide high-level information about communicating with the device via the various physical connection types in various software development frameworks, and provide pointers to available SDKs, which include sample code. All product documentation and SDKs are available for download by searching for the product name on www.magtek.com and navigating to the **Support** tab.

Custom host software can communicate with DynaPro Go using the same command set across all available connection types. The host must wrap device commands slightly differently depending on the connection type.

MagTek produces software development kits (SDKs) with API libraries that provide higher-level functions wrapped around the direct communication protocols like USB and TCP/IP. They also include sample code which the solution development team can compile to demonstrate and test the device, and copy / rewrite to jumpstart solution development. These libraries and sample code simplify the development of custom applications that use DynaPro Go:

- ***99510124 DYNAPRO / DYNAPRO MINI / DYNAPRO GO SDK FOR IOS***
- ***99510129 IPAD / DYNAPRO / DYNAPRO MINI / DYNAPRO GO SDK FOR ANDROID***
- ***99510127 IPAD / DYNAPRO / DYNAPRO MINI / DYNAPRO GO SDK FOR WINDOWS***, which bundles libraries for C++, Java/Java Applets, Microsoft .NET, and Microsoft .NET PCL.

In addition to the SDK API libraries, custom software on any supported operating system can communicate directly with the device using the operating system's native USB, TCP/IP, or Bluetooth LE libraries. For more information about sending commands directly, see ***D998200136 DYNAPRO GO PROGRAMMER'S REFERENCE MANUAL (COMMANDS)***.

8.1 USB-Based Custom Software

MagTek produces software development kits (SDKs) with API libraries that provide higher-level functions wrapped around **USB HID** communication protocols. These libraries simplify the development of custom host software that interfaces with tDynamo. See:

- ***99510109 SOFTWARE, SDK, ADYNAMO, BULLET, DYNAMAG, DYNAMAX, DYNAWAVE, EDYNAMO, IDYNAMO 6, MDYNAMO, TDYNAMO, UDYNAMO (ANDROID)***
- ***99510132 SOFTWARE, SDK, ADYNAMO, DYNAMAG, DYNAMAX, DYNAWAVE, EDYNAMO, IDYNAMO 6, MDYNAMO, TDYNAMO, UDYNAMO (WINDOWS .NET)***
- ***99510133 SOFTWARE, SDK, DYNAMAG, DYNAMAX, DYNAWAVE, EDYNAMO, IDYNAMO 6, MDYNAMO, TDYNAMO (WINDOWS C++ / JAVA)***

In addition to MagTek's SDKs, custom software on any operating system can communicate directly with the device using the operating system's native USB libraries and protocols. For details, see ***D998200226 TDYNAMO PROGRAMMER'S MANUAL (COMMANDS)***.

8.2 Bluetooth LE-based Custom Software and Apps

MagTek produces software development kits (SDKs) with API libraries that provide higher-level functions wrapped around **Bluetooth LE** communication protocols. These libraries simplify the development of custom host software that interfaces with tDynamo. See:

- ***99510109 SOFTWARE, SDK, ADYNAMO, BULLET, DYNAMAG, DYNAMAX, DYNAWAVE, EDYNAMO, IDYNAMO 6, MDYNAMO, TDYNAMO, UDYNAMO (ANDROID)***
- ***99510111 SOFTWARE, SDK, ADYNAMO, DYNAMAX, EDYNAMO, IDYNAMO, IDYNAMO 6, KDYNAMO, SDYNAMO, TDYNAMO, UDYNAMO (IOS)***.

In addition to MagTek's SDKs, custom software on any operating system can communicate directly with the device using the operating system's native Bluetooth LE libraries and protocols. For details, see ***D998200226 TDYNAMO PROGRAMMER'S MANUAL (COMMANDS)***. In this case, the device acts as a server/peripheral, and the host acts as a client/central. The custom software wraps commands in simple Get/Set wrappers, and should use whatever Bluetooth LE library is appropriate for the chosen software development framework. For example, iOS custom apps use Apple's `CoreBluetooth` Framework, for which sample code is available in the form of Apple's Temperature Sensor app; see https://developer.apple.com/library/IOS/samplecode/TemperatureSensor/Introduction/Intro.html.

8.3 For More Information

For more information about developing custom applications that integrate with tDynamo, see the MagTek web site or contact your reseller or MagTek Support Services.

Appendix A Technical Specifications

DynaFlex Technical Specifications	
Reference Standards and Certifications	
Identification Cards Integrated Circuits with Contacts (ISO/IEC 7816-1, 2, 3, & 4) EMV ICC Specifications for Payment Systems Version 4.3, L1 Contact and L2 Contact Encryption: TDEA (3DES)-CBC using DUKPT FCC Title 47 Part 15 Class B CE Level B EMC CE Safety UR/CUR UL Recognized MasterCard TQM California Proposition 65 (California) IPC-A-610 Class II Assembly EU Directive Waste Electrical and Electronic Equipment (WEEE) EU Directive Restriction of Hazardous Substances (RoHS) Universal Serial Bus Specifications 1.1, 2.0	
Physical Characteristics	
Dimensions (L x W x H):	2.60 in. W x 1.47 in. H x 0.30 in. T (66mm x 37.3mm x 7.7mm)
Weight	0.5 oz. (14g)
Supported Mounting Options:	Solution-specific enclosure with card slot, screws, and inserts
Card Read Characteristics	
Magnetic Stripe Reader:	Optional separate module connected to Auxiliary SPI or UART port
Magnetic Stripe Decoding:	Not Applicable
Magnetic Swipe Speeds:	Not Applicable
EMV Contact Reader:	EMVCo L1 and L2 Contact Reader
EMV Contactless Reader:	Optional separate module connected to Auxiliary UART port
User Interface Characteristics	
Status Indicators:	Port for General Status LED (Red/Green/Amber)
Display Type:	Not Applicable
Display Size (viewable area):	Not Applicable
Display Resolution:	Not Applicable
Keypad:	Not Applicable
Security Characteristics	
Certifications:	PCI PTS 4.x Certified Secure Card Reader (SCR) with SRED
Tamper Protection:	Not Applicable

DynaFlex Technical Specifications	
Code Protection:	Not Applicable
Eavesdrop Protection:	Not Applicable
Electrical Characteristics	
Power Inputs:	USB powered via Micro-USB B jack
Power Outputs:	400mA @ 5.0V available on Auxiliary UART port 100mA @ 3.3V available on Auxiliary SPI port
Battery Type:	Not Applicable
Battery Capacity:	Not Applicable
Battery Charge Time:	Not Applicable
Battery Time, Standby:	Not Applicable
Battery Time, Transactions:	Not Applicable
Voltage Requirements:	5 VDC from USB port
Current Draw:	300mA from USB port when not driving auxiliary devices 500mA from USB port maximum
Data Storage:	Not Applicable
Communication Characteristics	
Wired Connection Types:	Micro-USB B, compatible with USB 1.1, USB 2.0 Vendor-defined USB Human Interface Device (HID) data format
Wireless Connection Types:	Not Applicable
Wireless Range:	Not Applicable
Wireless Frequency:	Not Applicable
Software Characteristics	
Tested Operating System(s):	USB: Windows 7, Windows 8.1, Windows 10
Environmental Resistance	
Ingress Protection:	Not Applicable
Operating Temperature:	32°F to 113°F (0°C to 45°C)
Operating Relative Humidity:	5% to 90% non-condensing
Storage Temperature:	-4°F to 149°F (-20°C to 65°C)
Storage Relative Humidity:	5% to 90% non-condensing
Vibration Resistance:	Not Applicable

DynaFlex Technical Specifications	
Shock Resistance:	Not Applicable
ESD Tolerance (EMVCo):	±12kV air discharge when device is properly earth grounded
ESD Tolerance (FCC/CE):	±4kV contact discharge / ±8kV air discharge when properly grounded
Vapor Resistance:	Test Gasoline-96 RON (Reference Gasoline); Reference Fuel C; Diesel 2007 Emission Certification Fuel (Reference Diesel); E10; E25; E85; M15; Road-Use Diesel; Road Use Unleaded
Reliability	
Shelf Life:	Not Applicable
Magnetic Read Head Life:	Not Applicable
ICC Read Head Life:	500,000 card insertions
Battery Shelf Life:	Not Applicable
Battery Cycle Life:	Not Applicable