

DynaPro Go

Handheld PIN Pad Device with MSR/Contact/Contactless Installation and Operation Manual



March 2018

Document Number:
D998200129-10

REGISTERED TO ISO 9001:2008

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® is a registered trademark of MagTek, Inc.
MagnePrint® is a registered trademark of MagTek, Inc.
Magensa™ is a trademark of MagTek, Inc.
MagneSafe™ is a trademark of MagTek, Inc.
DynaPro™ and DynaPro Mini™, are trademarks of MagTek, Inc.
IPAD® 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.
Apple Pay® is a registered trademark to Apple Inc.
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.
PCI Security Standards Council® is a registered trademark of the PCI Security Standards Council, LLC.
EMVCo™ and EMV™ are trademarks of EMVCo and its licensors.
UL™ and the UL logo are trademarks of UL LLC.

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 1-1 - 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 Technical Support 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 ANY 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 Règlement 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 conforme 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 **Non-Specific Short Range Device** (contactless) are in compliance with **Directive 2014/53/EU**. The full text of the EU declaration of conformity is available at the following internet address: <https://www.magtek.com/Content/DocumentationFiles/D998200238.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 ().

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.

1 Table of Contents

Limited Warranty	4
FCC Information	6
Canadian Declaration Of Conformity	6
Industry Canada (IC) RSS.....	6
CUR/UR.....	6
CE STANDARDS.....	7
EU Statement.....	7
Australia / New Zealand Statement	7
UL/CSA	7
RoHS STATEMENT.....	7
PCI Statement	7
1 Table of Contents.....	8
2 Introduction	11
2.1 About DynaPro Go	11
2.2 Protection for All Points Within the Payment Infrastructure.....	13
2.3 Security and Ease of Integration by Design	13
2.4 Remote Services	13
2.5 Peace of Mind	Error! Bookmark not defined.
2.6 Tamper Responsiveness	13
2.7 Liquid Crystal Display.....	13
2.8 10-Digit Backlit Numeric Keypad With Function Keys	14
2.9 Low-Power Standby Modes.....	14
2.10 Major Components.....	15
2.11 About Terminology	15
3 Planning and Preparation	16
3.1 Logistical Planning.....	16
3.2 Network Planning.....	18
4 Installation.....	19
4.1 About Inspection.....	19
4.2 About Software	20
4.3 About Connecting to a Host	20
4.3.1 How to Connect DynaPro Go to a Computer Host or Charger via USB	20
4.3.2 How to Connect DynaPro Go to a Host via 802.11 Wireless	21
5 Configuration.....	22
5.1 How to Configure the LCD Display Brightness.....	23
5.1.1 LCD Display Brightness Auto Mode.....	24
5.1.2 LCD Display Brightness Manual Mode.....	24

5.2	How to Configure the Keypad Backlight	25
5.3	How to Change the Active Connection	26
5.4	How to Configure Network Settings (ADVANCED)	27
5.4.1	How to Configure the Network to Support 802.11 Wireless Connections	27
5.4.2	How to Configure the Host for 802.11 Wireless	28
5.4.3	How to Configure the Device for 802.11 Wireless	29
5.4.4	How to Test the 802.11 Wireless Connection	34
6	Operation	35
6.1	Overview	35
6.2	How to Read Device Status	37
6.2.1	Welcome Screen Status Icons	37
6.2.2	Device Details Screens	38
6.2.3	Health and Safety Information	40
6.2.4	Wireless Status Screen	40
6.2.5	OFFLINE Screen	41
6.3	Power Management	42
6.3.1	How to Charge the Battery	42
6.3.2	How to Power On / Power Off	43
6.3.3	Battery Warnings and Automatic Power Off	43
6.3.4	Sleep Mode	44
6.3.5	USB Suspend	44
6.3.6	Maintenance Reset	44
6.4	How to Start a Handheld Wireless Transaction	46
6.5	Card Reading	47
6.5.1	How to Swipe Magnetic Stripe Cards	47
6.5.2	How to Insert Contact Chip Cards	48
6.5.3	How to Tap Contactless Cards / Devices	50
6.5.4	How to Enter Card Information Manually	52
6.5.5	How to Select the Card Type	52
6.6	How to Verify the Transaction Amount	53
6.7	How to Enter PINs	54
6.8	How to Use Signature Capture	54
6.9	How to Enter Passcodes	55
7	Maintenance	56
7.1	Mechanical Maintenance	56
7.2	Updates to Firmware, Documentation, Security Guidance	56
8	Developing Custom Software	57
Appendix A	Technical Specifications	58

2 Introduction

2.1 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 unit cause all keys to be cleared and/or stop the unit 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
- Wireless and USB connection
- 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 2-1 - Available Models and Options

Part No.	Description	Cable	USB	802.11	Bluetooth	BLE	Sig Cap.
30056215	DYNAPRO GO DEMO / TEST, SIGCAP, 802.11 WIRELESS	micro-USB	Yes	Yes	No	No	Yes
30056216	DYNAPRO GO PCI, SIGCAP, 802.11 WIRELESS	micro-USB	Yes	Yes	No	No	Yes

2.2 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.

2.3 Security and Ease of Integration by Design

DynaPro Go is a durable device made for easy connection. 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 for fast development and easy integration.

DynaPro Go can interface through standard micro-USB cabling to recharge the battery and to perform synchronization with compliant hosts, or connect via TCP/IP over 802.11 wireless. The display module is a backlit display and the keypad has well-contoured keys with tactile feedback for convenient entry of PINs or other data.

2.4 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.

2.5 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 unit. 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 unit to permanently erase its stored encryption keys, after which the device will cease to function.

2.6 Liquid Crystal Display

The Liquid Crystal Display (LCD) screen is a 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.

2.7 10-Digit Backlit Numeric Keypad With Function Keys

During normal operation, cardholders use the device's numeric keypad to securely enter PINs and other numeric data (see **Figure 2-1** on page 15). 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.

2.8 Low-Power Standby Modes

To conserve battery power, DynaPro Go enters low-power mode or powers off in response to a variety of events, including screen timeouts ("Sleep 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 **6.3 Power Management**.

2.9 Major Components

The major components of DynaPro Go are shown in **Figure 2-1**. In addition to the components shown, the device has a **tamper trigger** recessed in the bottom that is intended for manufacturer use only.

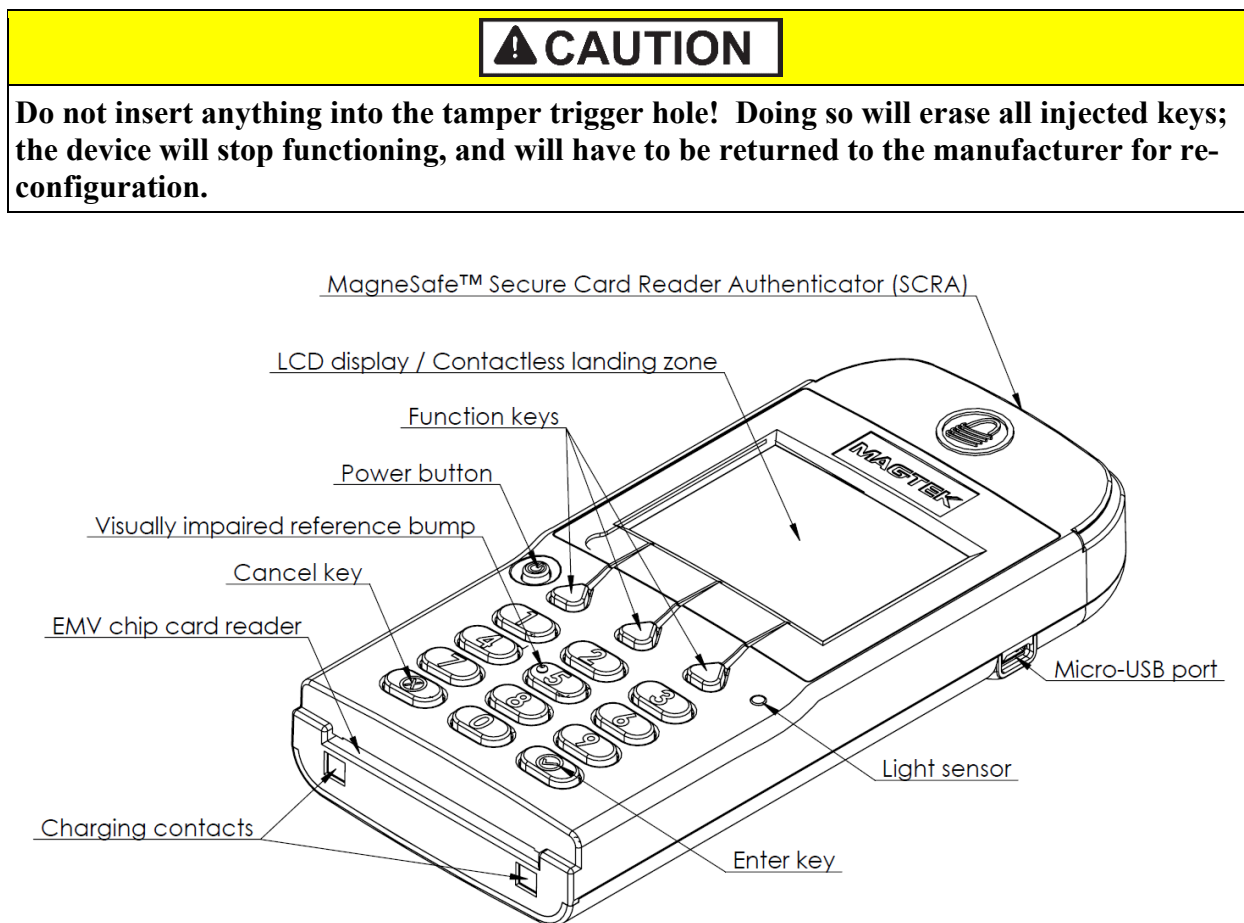


Figure 2-1 – DynaPro Go Major Components

2.10 About Terminology

In this document, DynaPro Go 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).

3 Planning and Preparation

The guidelines in the following sections will assist management and network administrators in planning for the physical and network requirements of deploying and using DynaPro Go. The most effective way to ensure smooth deployment of a solution is to consider these factors before receiving the device.

3.1 Logistical Planning

- Determine what type of **host** DynaPro Go will connect to. This can be a computer with a USB port or connected to a TCP/IP network that is equipped with 802.11 wireless. When planning, include any additional support or devices required by the host and DynaPro Go, such as physical locations, mounting, power connections, and charging cradles.
- 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. Include any additional support required by the software, such as network connections. Information about software is provided in section **4.2 About 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 **6.5 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 and TCP/IP over 802.11 wireless, and only one interface can be active at a time. The connection types available in each model are listed in **Table 2-1 - Available Models and Options** on page 12.
- Determine how DynaPro Go should be **configured**, and specify that configuration when ordering the device. For example:
 - Determine whether the device should be **Always Listening** for wireless messages from the host, or creating **Device-Initiated** connections on demand.
 - 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.
 - **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.
 - It may also need a browser connection to a certificate authority (CA) for downloading certificates.
- 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 **6.3.1 How to Charge the Battery**. Details about maximum power consumption are provided in **Appendix A Technical Specifications**.

- 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 **6.9 How to Enter Passcodes**.
- Determine how to **train** operators. Training may include material from section **5 Configuration** and section **6 Operation**.

3.2 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) Coordinate with your sales representative to obtain the certificate chain that must be installed on the host to enable TLS communication with the device.
- 2) Determine how the **IP addresses** of all DynaPro Go devices and the host will be allocated.
- 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 **WPA2-PSK (TKIP)**, **WPA2-PSK (AES)**, or **WPA2-PSK (TKIP/AES)** wireless security. Make sure the access point is configured to support one of these.
- 5) Determine whether to use MAC filtering on the access point and plan a way for MACs for new devices to be added to the list.
- 6) If the device and host will use static IP addresses, allocate those addresses and determine what Gateway and Subnet Mask the devices should use.
- 7) Configure the network's DNS server in one of three ways:
 - a) Register the host as providing an mDNS Service name, or
 - b) Register the host with a DNS name, or
 - c) Don't register the host with DNS, and exclusively use IP address.
- 8) Determine what ports the device and host will use to communicate. By default, the device expects the host connect to **port 26**, must be able to access DNS via UDP using **port 53**, and must be able to access DHCP on **port 67**. Make sure the network and firewalls are configured so the device and host can initiate connections on the selected port(s).
- 9) DynaPro Go does not require an Internet gateway.

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 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 About Connecting to a Host

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

4.3.1 How to Connect DynaPro Go to a Computer Host or Charger via USB

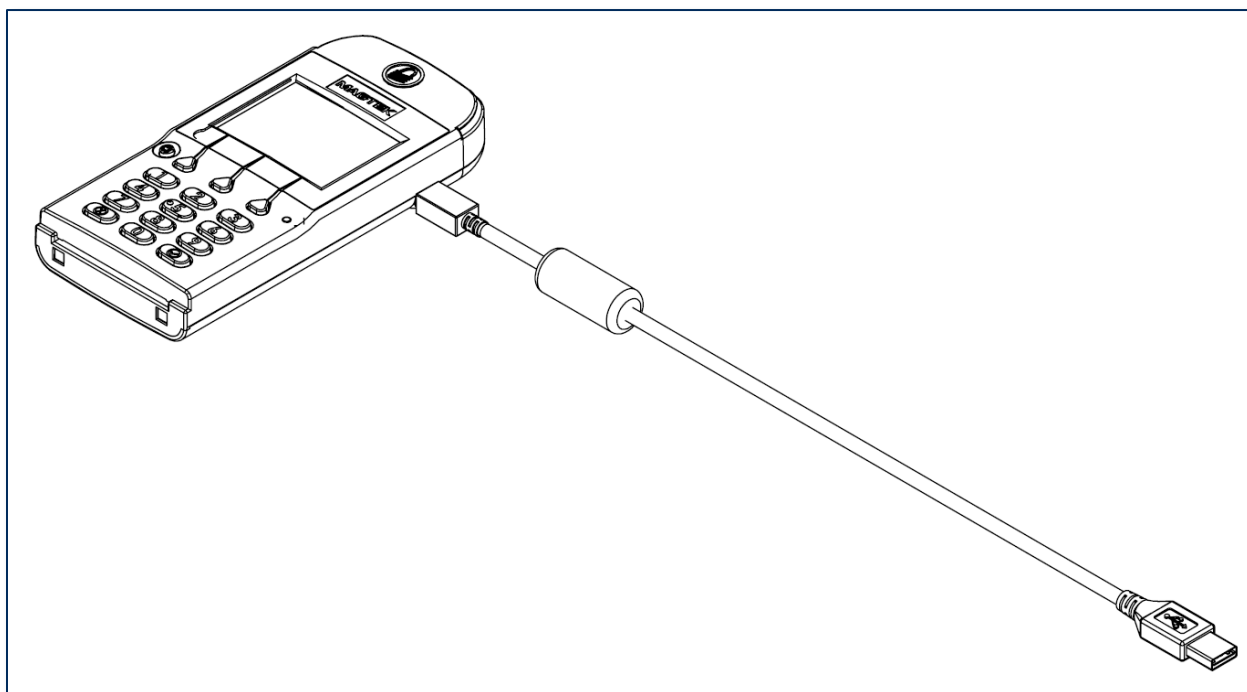
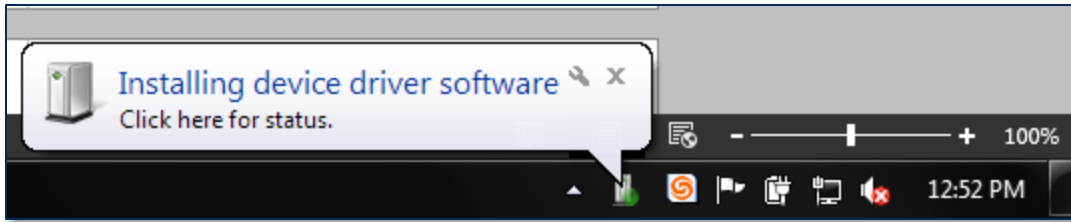


Figure 4-1 - Connecting DynaPro Go to a Computer or USB Charger

To connect DynaPro Go to a host computer 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 computer's USB port.
- 2) As soon as DynaPro Go starts receiving power through USB, it will automatically power 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 it is configured to use the USB connection. See section 5.3 **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 Windows system tray on the host will report it is **Installing device driver software**.



- 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) The device will show the **USB Connected** symbol at the top of the display (see section **6.2 How to Read Device Status**).

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

To connect DynaPro Go to a host computer 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 **5.4 How to Configure Network Settings (ADVANCED)**.
- 2) Power on the device and make sure the device is configured to use the 802.11 wireless connection according to the steps in section **5.3 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 **6.2 How to Read Device Status**.

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, operators can view or change some configuration options using the keypad and display. **Table 5-1** provides details for using these features.

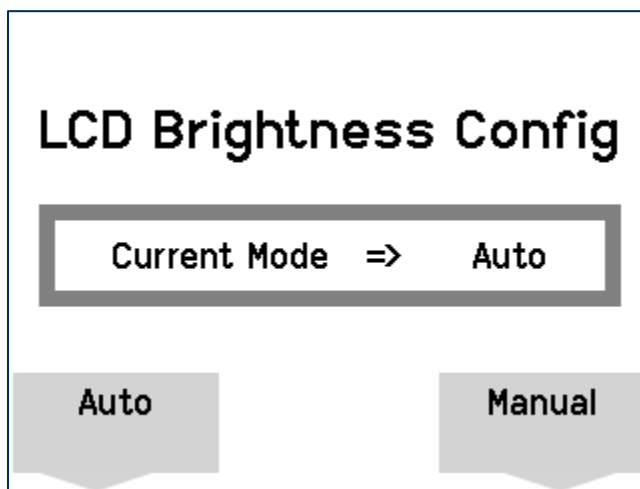
Table 5-1 - Keypad Configuration Features

Configuration Option	Key Sequence	Notes
Open Host Connection	Left Function Key 1 2 3 Right Function Key	When the device is not 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.
Change Active Connection	Left Function Key 4 5 6 Right Function Key	Toggles the device's active connection between possible connection types.
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 5.2 How to Configure the Keypad Backlight .
Show device details	Left Function Key 7 8 2 Right Function Key	Displays a page showing information about the device. See section 6.2.2 Device Details Screens .
Show additional device details	Left Function Key 7 8 1 Right Function Key	Displays a page showing information about the device. See section 6.2.2 Device Details Screens .
Show EMV device details	Left Function Key 7 8 3 Right Function Key	Displays a page showing information about the device. See section 6.2.2 Device Details Screens .
Show wireless status	Left Function Key 6 2 2 Right Function Key	Displays a page showing information about the device's 802.11 wireless connection. See section 6.2.4 Wireless Status Screen .

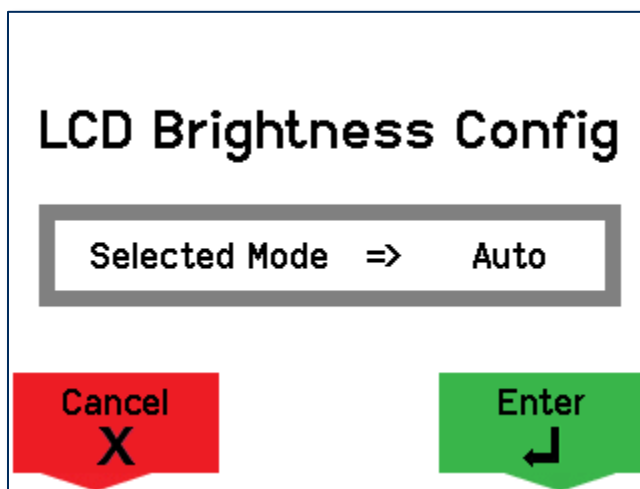
5.1 How to Configure the LCD Display Brightness

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, press **Left Function Key** **5** **2** **2** **Right Function Key** to open the **LCD Brightness Config** screen.



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.



5.1.1 LCD Display Brightness Auto Mode

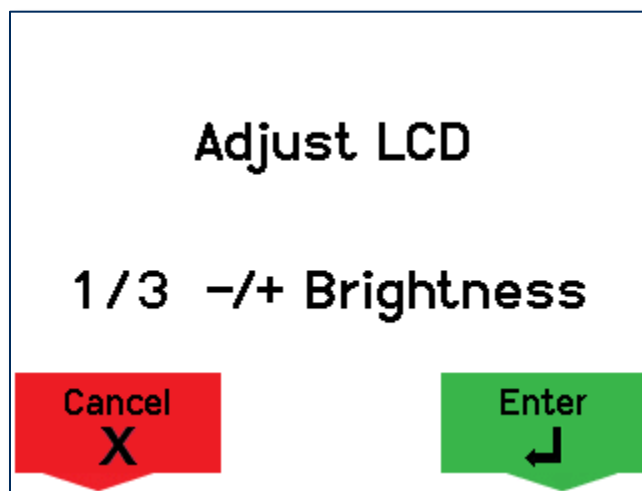
When the display brightness is set to **Auto** mode, the device adjusts the LCD backlight brightness automatically based on ambient light detected by the light sensor (see section **2.10 Major Components**). The brightness levels the device will select are shown in **Table 5-2**. When the device is in **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, press **Left Function Key** **5** **2** **3** **Right Function Key** to show the **Adjust LCD** screen.

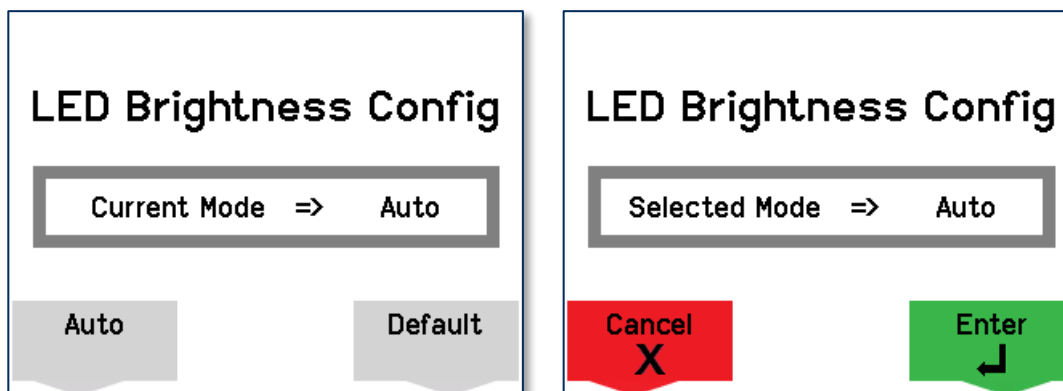


Select the desired brightness by pressing the **1** key to decrease and the **3** key to increase, then press the **Enter** key to save the change. To exit without saving changes, press the **Cancel** key or wait 10 seconds for the device to return to the **Welcome** screen.

5.2 How to Configure the Keypad Backlight

The device's keypad has a backlight that can be configured to either remain at a constant brightness level (**Default mode**) or adapt its brightness to ambient lighting based on the device's light sensor (**Auto mode**). The factory default of the device is **Default** mode, which uses **Maximum** brightness.

To change the keypad backlight mode, press **Left Function Key** **5** **3** **3** **Right Function Key** to open the **LED Brightness Config** screen.



The **LED Brightness Config** screen shows the mode the keypad 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.

When the device is in **Auto** mode, the device adjusts the keypad backlight brightness automatically based on ambient light detected by the light sensor (see section **2.10 Major Components**). The brightness levels the device will select are shown in **Table 5-3**. When the device is in **Default** mode, the device keeps the keypad backlight brightness at **Maximum**.

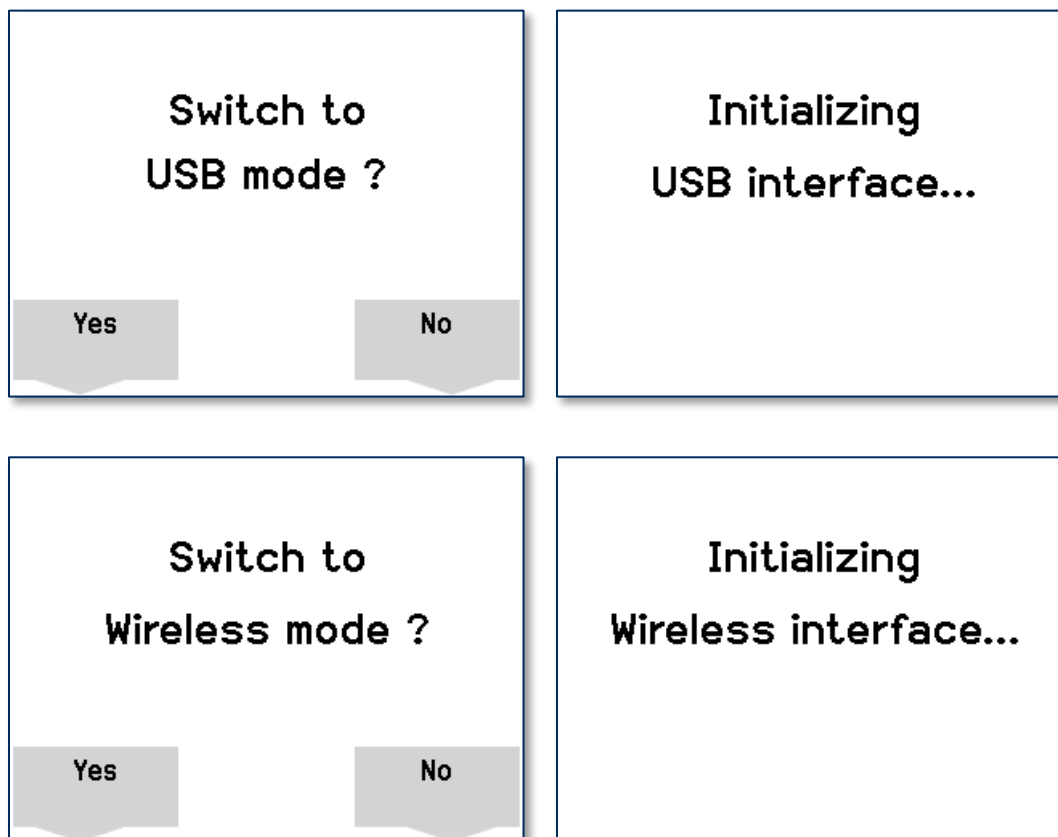
Table 5-3 - Keypad Backlight Brightness Levels

Light Level	Keypad Brightness Level
High	Off (0%)
Medium	Medium (33%)
Low	High (67%)
Very Low	Maximum (100%)

5.3 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 only use one connection type.

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

5.4 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.

DynaPro Go can be configured to communicate with the host using 802.11 wireless in one of two ways:

- In **Device Initiated** mode, the device will not listen for incoming connections, and instead expects to initiate connections with the host on demand.
- In **Always Listening** mode, the device keeps a TLS socket open that allows a single authenticated host to connect.

In both cases, 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 will refuse the connection and report **Configuration Error** on the display.

Both the device certificate and its corresponding private key are generated and injected by the manufacturer. The private key cannot be accessed directly. MagTek provides the device's CA certificate chain to the customer for installation on the host.

5.4.1 How to Configure the Network to Support 802.11 Wireless Connections

When the device first connects to an 802.11 wireless network, it will attempt to contact a DHCP server to acquire a dynamic IP address. If the device is unable to obtain an IP address from a DHCP server, it will continuously report it is **Obtaining IP Address**.

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 **3.2 Network Planning**. MagTek recommends performing these steps before receiving the devices so the network will be ready when they arrive.
- 2) Acquire or generate a TLSv1.2 certificate/key pair and certificate chain for the host. Certificates and keys must be RSA 2048 bit, signature algorithm SHA-256RSA.
- 3) Acquire the TLS Certificate Authority chain for DynaPro Go devices and install in Trusted Root Certification Authorities
- 4) The device can connect to only one access point. 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 **Wireless Status Screen** and make sure the Received Signal Strength Indicator level (**RSSI**) is greater than or equal to **40**.

5.4.2 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:

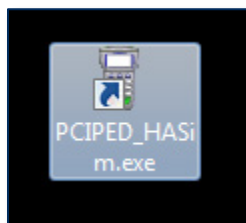
- 1) If the device will use a static IP address, configure the host to use it.
- 2) Load the host's certificate chain to the device using the USB interface. The device validates the certificate chain on upload to make sure it is properly signed, has not expired, and that the chain is valid.
- 3) Install the certificate on the host.
- 4) Check the host's network configuration (for example, using regedit in Windows) to make sure the following cipher suites are enabled:
 - TLS_RSA_WITH_3DES_EDE_CBC_SHA
 - TLS_RSA_WITH_AES_128_CBC_SHA
 - TLS_RSA_WITH_AES_256_CBC_SHA
 - TLS_RSA_WITH_AES_128_CBC_SHA256
 - TLS_RSA_WITH_AES_256_CBC_SHA256
- 5) Determine the host's IP address for use in section **5.4.3 How to Configure the Device for 802.11 Wireless**.
- 6) Make sure the host's firewall is configured to allow bidirectional direct socket communication using TCP on the configured port. The device default is **port 26**.
- 10) Configure the host software to communicate with DynaPro Go using the appropriate IP address and port.

5.4.3 How to Configure the Device for 802.11 Wireless

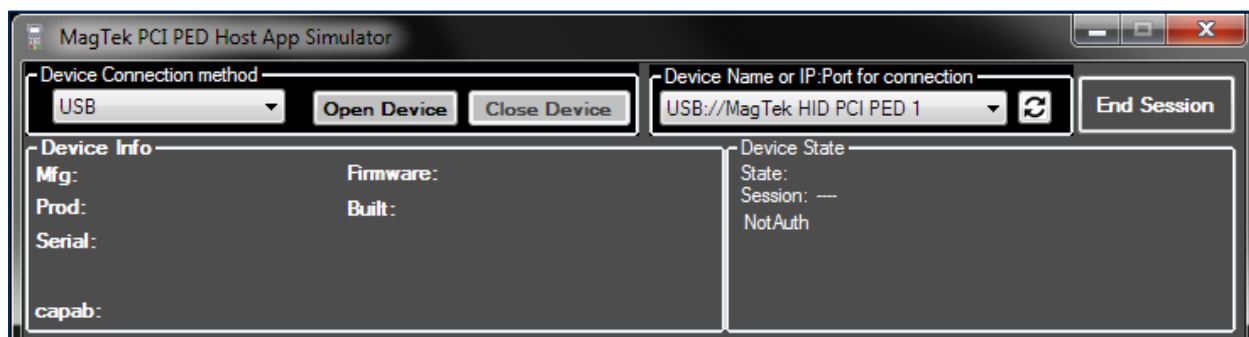
An advanced user or administrator must configure the device to communicate securely with the host using the 802.11 wireless connection. For details about using the **PCIPED_HASim** tool described here, see **D998200168 IPAD, DYNAPRO, DYNAPRO MINI, DYNAPRO GO PIN ENTRY DEVICE SIMULATION SOFTWARE INSTRUCTION**.

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

- 1) Make sure the device you are configuring is properly configured with the TLS certificate for the host the device will connect it to. MagTek or your reseller will generally pre-load these certificates.
- 2) 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, navigate to **C:\Program Files (x86)\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.



- 3) Make sure no other MagTek devices are connected to any of the host's USB ports.
- 4) Make sure the device is powered off and is not connected to a USB port.
- 5) Connect the device to the host's USB port (see section 4.3.1 **How to Connect DynaPro Go to a Computer Host or Charger via USB**). At the end, the device will be powered on and will show the USB Connected icon at the top of the display.
- 6) Launch **PCIPED_HASim.exe** to show a **MagTek PCI PED Host App Simulator** window.



- 7) Under **Device Connection method**, select **USB**.

5 - Configuration



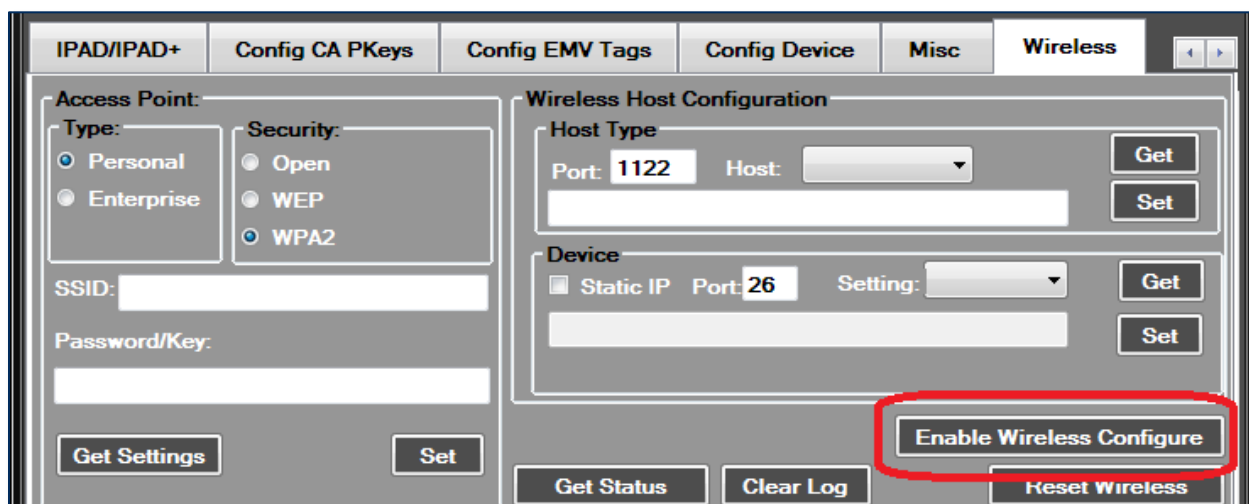
- 8) In the **Device Name** list, select the serial number or name of the device you want to connect to, then press the **Open Device** button.



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



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



- 11) When the device screen prompts **Enter Admin Passcode**, enter the device admin passcode on the device keypad. The default is **8 7 6 5 4 3 2 Enter**.
- 12) 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**.

The screenshot shows the 'Wireless' tab in the configuration menu. Under the 'Access Point' section, the 'Security' sub-section is highlighted with a red box. It contains three radio button options: 'Open', 'WEP', and 'WPA2'. The 'WPA2' option is selected. To the left, under 'Type', the 'Personal' option is selected. The 'Wireless Host Configuration' section on the right shows 'Host Type' with 'Port: 1122' and a 'Host' dropdown menu. Below that, the 'Device' section shows 'Static IP' checked, 'Port: 26', and a 'Setting' dropdown menu. 'Get' and 'Set' buttons are present for each of these sections.

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

This screenshot is similar to the previous one, but the 'SSID' field is now visible and highlighted with a red box. The text 'mtgquest' is entered into the 'SSID' field. The 'Password/Key' field is visible below it but is empty. The 'Security' section remains set to 'WPA2' and 'Personal' type.

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

This screenshot shows the 'Password/Key' field highlighted with a red box. The text 'CorrectHorseBatteryStaple' is entered into this field. The 'SSID' field above it still contains 'mtgquest'. The 'Security' and 'Type' settings are unchanged. At the bottom right, there is an 'Enable Wireless Configure' button.

- 15) Press the **Set** button.

- 16) Press the device's power button for two seconds to turn it off, and use the function keys to select **Yes**. The device will reboot because USB is attached.
- 17) Change the Active Connection to 802.11 Wireless (see section 5.3 How to Change the Active Connection).
- 18) The screen will show a flashing wireless network icon at the top (see section 6.2 How to Read Device Status).
- 19) Press **Left function key**, **7**, **8**, **3**, **Right function key**.
- 20) The device will show a page about the 802.11 wireless connection. Write down the **IP Address** and press the **Cancel** key to close the screen.

WiFi Status	
Network	Disconnected
Host	Disconnected
IP Addr	111.222.333.444
MAC Addr	11:22:33:44:55:66
RSSI	70
Tx Power	0

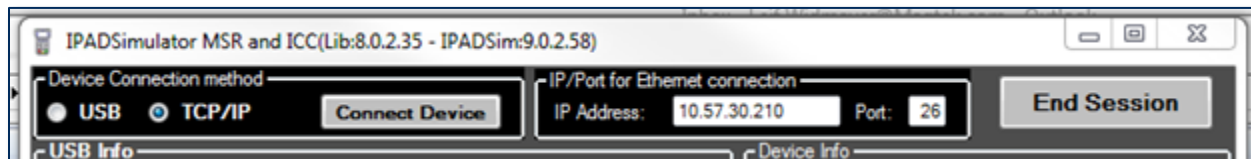
- 21) The device is now configured for hosts to connect to it using the wireless access point.
- 22) Test the connection between the device and the host:
 - a) If the host software is already configured, follow the steps in section 4.3.2 How to Connect DynaPro Go to a Host via 802.11 Wireless.

- b) If you need to perform basic connection testing, leave the **MagTek PCI PED Host App Simulator** window open and follow the steps in section **5.4.4 How to Test the 802.11 Wireless Connection**.

5.4.4 How to Test the 802.11 Wireless Connection

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

- 1) Set up the device to connect to a specific wireless access point and get its IP address using the steps above.
- 2) Launch **IPADSim.exe** to show an **IPADSimulator MSR and ICC (Lib:x.x.x.x - IPADSim:x.x.x.x)** window.
- 3) Under **Device Connection method**, select **TCP/IP**.
- 4) Under **IP/Port for Ethernet connection**, enter the device's IP address and port **26**.



- 5) Make sure the device is powered on and is showing a flashing wireless network icon at the top.
- 6) Press the **Connect Device** button.
- 7) Use the various tabs in the **IPADSimulator** window to send commands to the device through the wireless connection or to receive transaction data.

To connect the device to the host and test the 802.11 wireless connection when the device is in Device-Initiated mode, follow these steps:

6 Operation

6.1 Overview

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

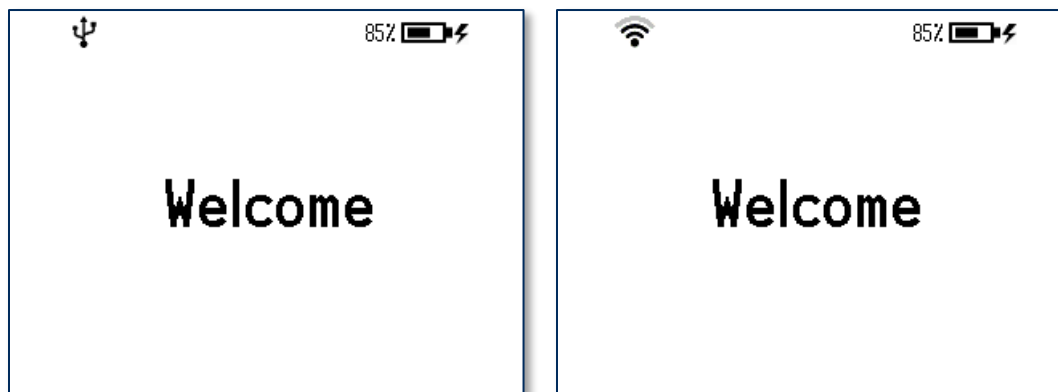


Figure 6-1 - Example of Welcome Screen (Ready for a New Transaction)

During normal operation, the operator will initiate a transaction from the host, and the cardholder will enter 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 **6.5 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 will prompt 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.

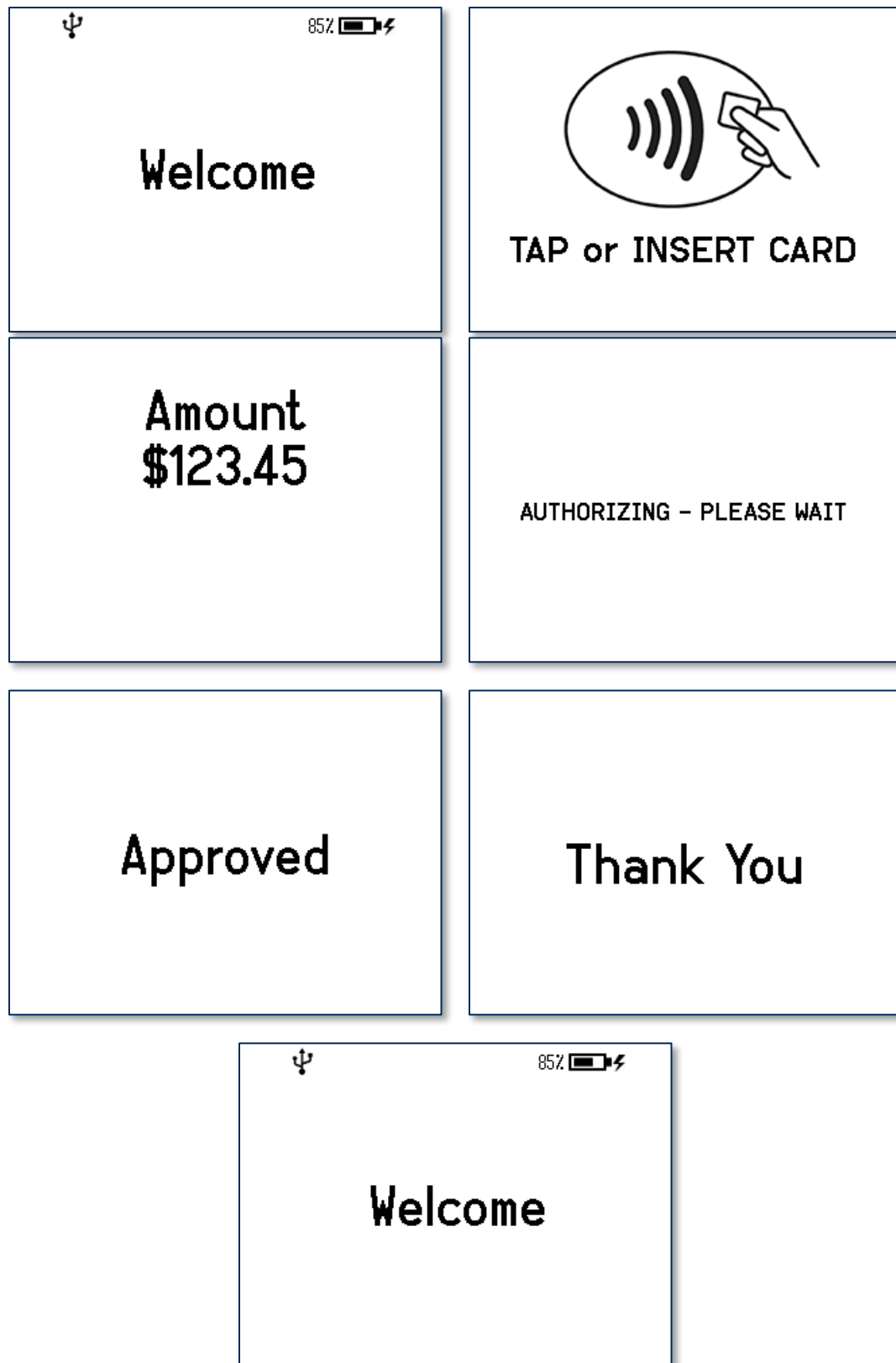


Figure 6-2 - Typical Transaction Sequence

6.2 How to Read Device Status

6.2.1 Welcome Screen Status Icons

The device reports its current status in a set of icons at the top of the **Welcome** screen. **Table 6-1** 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 6-1 - 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 6.5.3 How to Tap Contactless Cards / Devices for details.
	Device's Active Connection is set to USB, and the device has successfully established a USB communication connection with the host.
Solid 	Device's Active Connection is set to 802.11 wireless, the device is connected to a wireless access point, and the device is communicating with the host. The number of bars indicates the strength of the signal the device is receiving from the wireless access point (commonly known as RSSI).
Blinking 	Device's Active Connection is set to 802.11 wireless, the device is connected to a wireless access point, but the device can not connect to the host. The number of bars indicates the strength of the signal the device is receiving from the wireless access point (commonly known as RSSI).
OFFLINE	Device is not connected to a host via any connection type.
	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.
<No indicator>	Battery is not charging.



Figure 6-3 - Status Icons Example

6.2.2 Device Details Screens

In addition to the icons at the top of the display, the device has three screens that report deeper details about the device.

To see information about the device's main firmware part number(s) and revision number(s), 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 corresponding values in the device's listing on www.pcisecuritystandards.org, *Approved PTS Devices*.

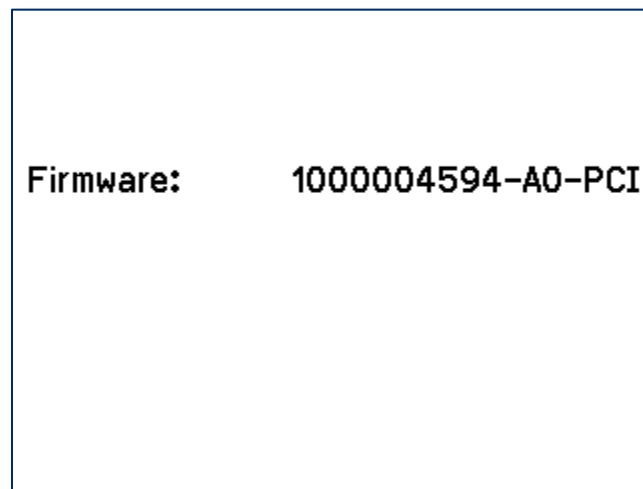


Figure 6-4 - General Device Details Screen

To see details about the device's contactless feature, 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

Figure 6-5 - Contactless Device Details Screen

To see details pertinent to the device's EMV certification, 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

6.2.3 Health and Safety Information

The device implements electronic labels (“e-labels”) that report its **Health and Safety** certification information. To access them, press the sequence **Left Function Key**, **7**, **8**, **0**, **Right function key**. This brings up a page similar to **Figure 6-6**, 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.



Figure 6-6 - Health and Safety Screen 1

6.2.4 Wireless Status Screen

In addition to the icons at the top of the display, the device has a **Wireless Status** screen that reports deeper details about the wireless connection. To access it, press the sequence **Left Function Key**, **6**, **2**, **Right function key**. This brings up a screen similar to **Figure 6-7**. To return to the **Welcome** screen, press the **Cancel** key.

Wireless Status	
Network	Disconnected
Host	Disconnected
IP Addr	111.222.333.444
MAC Addr	11:22:33:44:55:66
RSSI	70
Country Code	00

Figure 6-7 - Wireless Status Screen

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

6.2.5 OFFLINE Screen

The device shows the **OFFLINE** screen to indicate it is not ready for normal operation. The display shows a code in the lower right corner explaining why the device is offline.

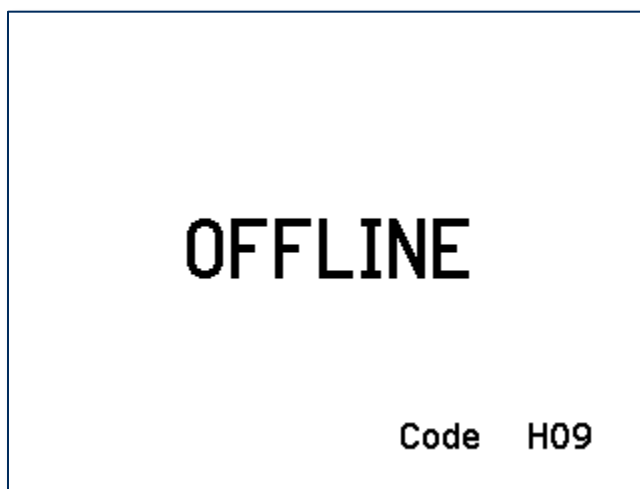


Figure 6-8 - OFFLINE Screen

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 6-2** provides full explanations of the prefixes of all **OFFLINE** codes. For details, see *D998200136 DYNAPRO GO PROGRAMMER'S MANUAL (COMMANDS)*.

Table 6-2 - 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 (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.

6.3 Power Management

6.3.1 How to Charge the Battery

Note

DynaPro Go's Lithium Polymer (LiPo) rechargeable battery will deliver best performance when it is completely or almost completely drained and then receives a full charge, as opposed to other rechargeable battery types that require constant "topping-off" recharging. Using the device until the battery is low will enhance the device's performance and provide a better user experience.

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 **4.3.1 How to Connect DynaPro Go to a Computer Host or Charger via USB** on page 20.

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.

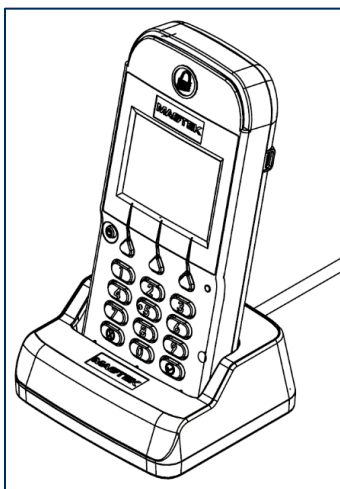


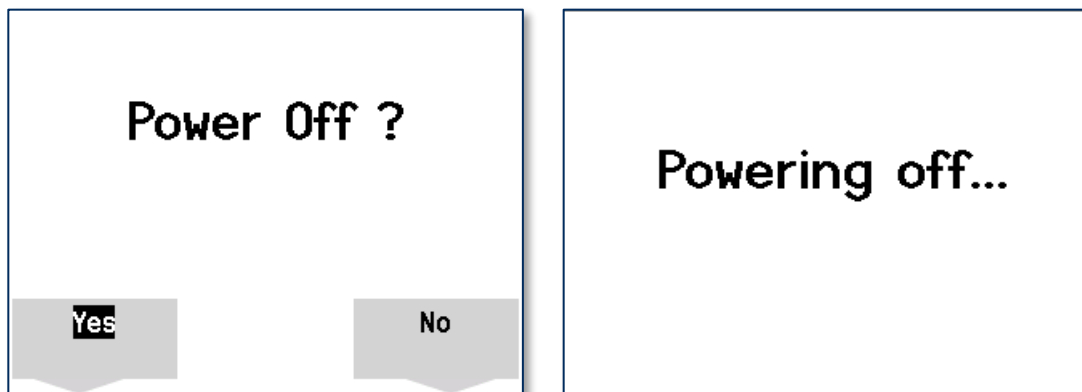
Figure 6-9 - Device In Charging Cradle

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

6.3.2 How to Power On / Power Off

To power on the device, press and hold the **Power button** for one second. Upon powering up, it will display the **Welcome** screen and the current device status (see section 6.2 How to Read Device Status).

To power off the device, press and hold the **Power button** for seven seconds, or press the **Power button** for two seconds to display a **Power Off?** screen with a **Yes** / **No** selection above the left and right function keys. To power off, press the function key below **Yes**. To cancel powering off and return to the **Welcome** screen, either wait 10 seconds or press the function key below **No**. While the device is powering off, the display shows **Powering off...** for three seconds before the display goes blank.



6.3.3 Battery Warnings and Automatic Power Off

When the battery is running low, the device will show **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 powering off automatically. See section 6.3.1 How to Charge the Battery for details on recharging.

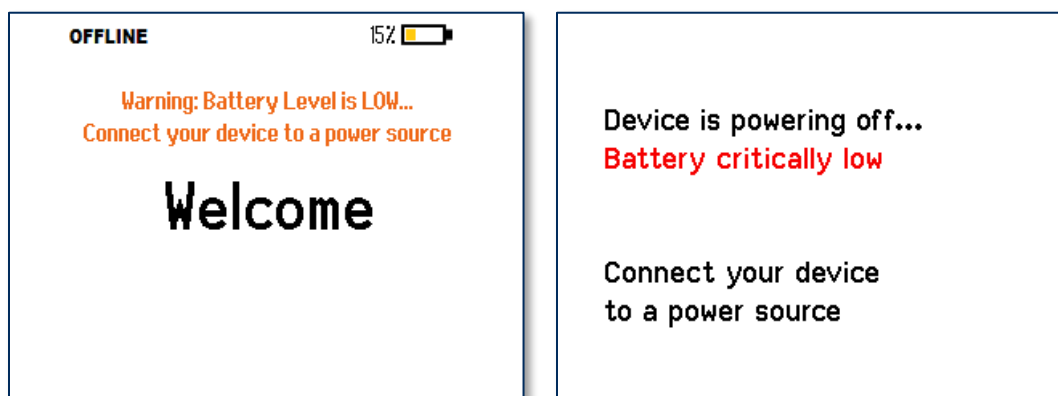


Figure 6-10 – Battery Level is LOW Warning / Battery Critically Low

6.3.4 Sleep Mode

When the device has not received any input from an operator, cardholder, or the host for two minutes, it powers off to conserve battery power. The device shows **Sleeping...** for three seconds before the display goes blank. To wake it up, press and hold the **Power button** for one second.

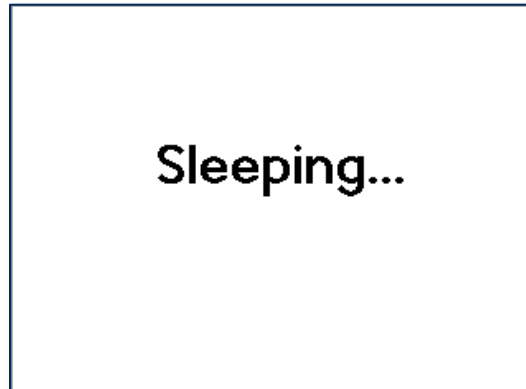


Figure 6-11 - Device Sleeping After Two Minutes Idle

6.3.5 USB Suspend

When the device is connected to a host via USB (see section 4.3.1 **How to Connect DynaPro Go to a Computer 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.

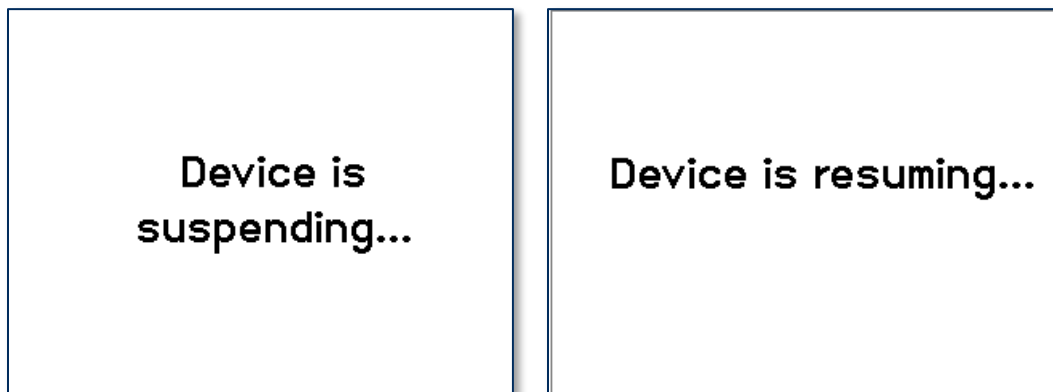


Figure 6-12 - Device Responding to Host-initiated USB Suspend

6.3.6 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 return 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.

6.4 How to Start a Handheld Wireless Transaction

When the device and host are configured for handheld operation using **Device-Initiated** mode, an operator can start a transaction from the device by following these steps:

- 1) Make sure the device is connected to a wireless access point and has good signal strength (see section **6.2 How to Read Device Status**).
- 2) Press **Left Function Key** **1** **2** **3** **Right Function Key**. The device will send a signal to the host that it wants to initiate a transaction.
- 3) Depending on how the host software is designed, the host will send various messages requesting that the cardholder or operator enter additional information, then the device will request payment in the same way as section **6.5 Card Reading**.
- 4) If there is no network activity or user interaction for 30 seconds, the device will close the wireless connection automatically. If this occurs, the host should cancel the transaction and the operator should repeat these steps to initiate the transaction again.

6.5 Card Reading

6.5.1 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 6-13** for examples).
- 2) Locate the magnetic stripe reader on the top of the device, shown in **Figure 6-14**.
- 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 will prompt 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 **6.5.4 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.

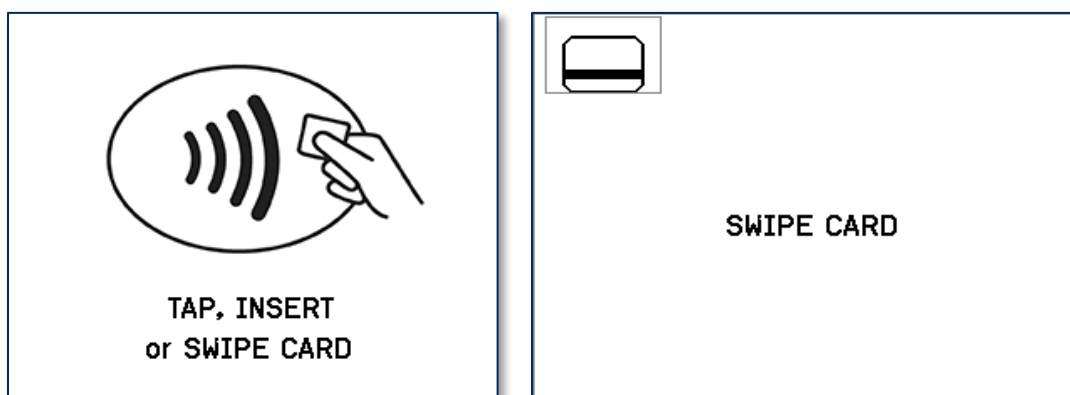


Figure 6-13 - Example Card Swipe Screens

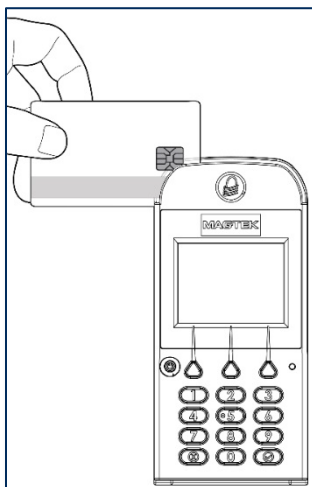


Figure 6-14 - Swiping a Magnetic Stripe Card

6.5.2 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 will toggle between the transaction amount and an action prompt (see **Figure 6-15** for examples).
- 2) Locate the slot on the front of the device shown in **Figure 6-16**.
- 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 will prompt 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 **6.5.4 How to Enter Card Information Manually**).

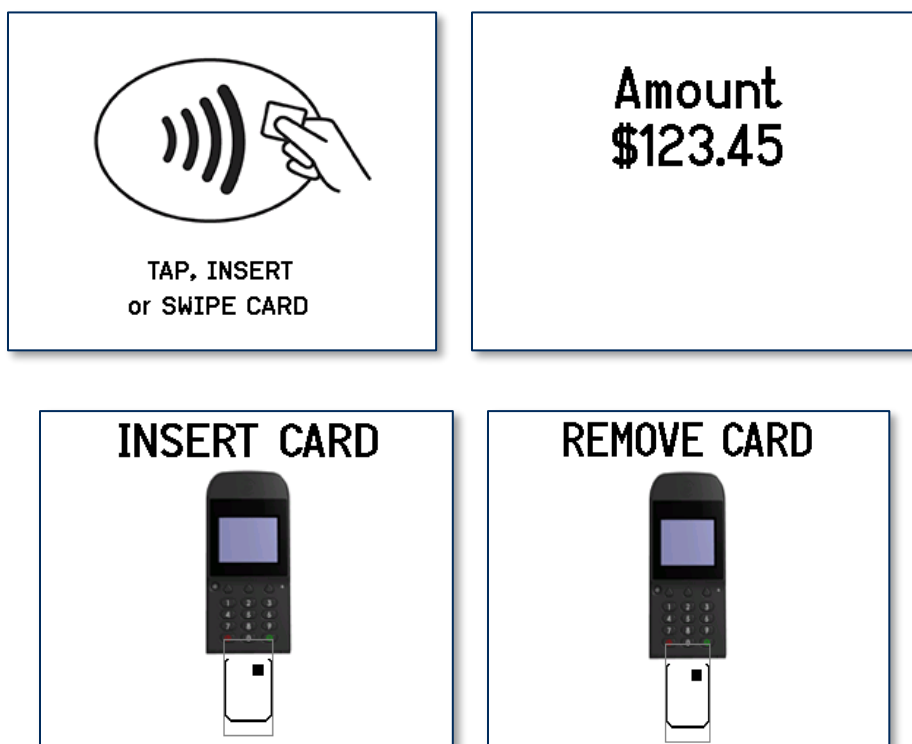


Figure 6-15 - Example Card Insertion Screens

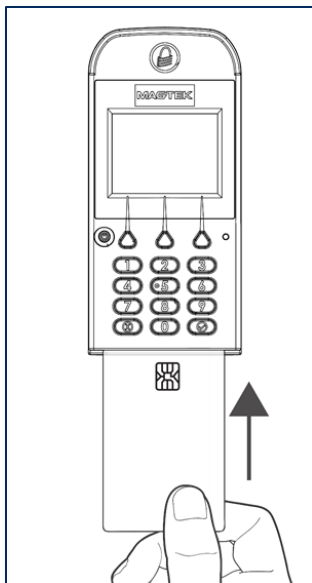


Figure 6-16 - Inserting a Chip Card

6.5.3 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 6-17** 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) Briefly hold the card, smartphone, or other contactless payment device over the contactless logo on the display. 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 6-19**). The device will also beep when the read is complete.

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 6.5.4 **How to Enter Card Information Manually**).

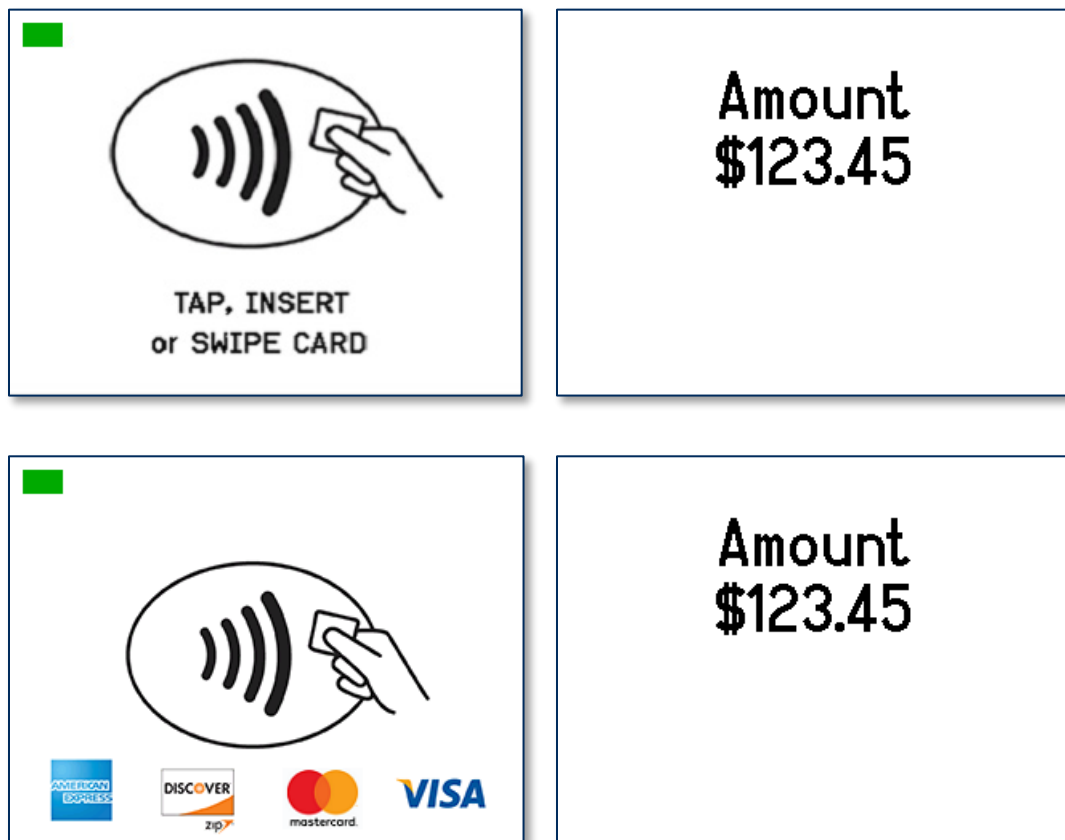


Figure 6-17 - Example Contactless Transaction Screens

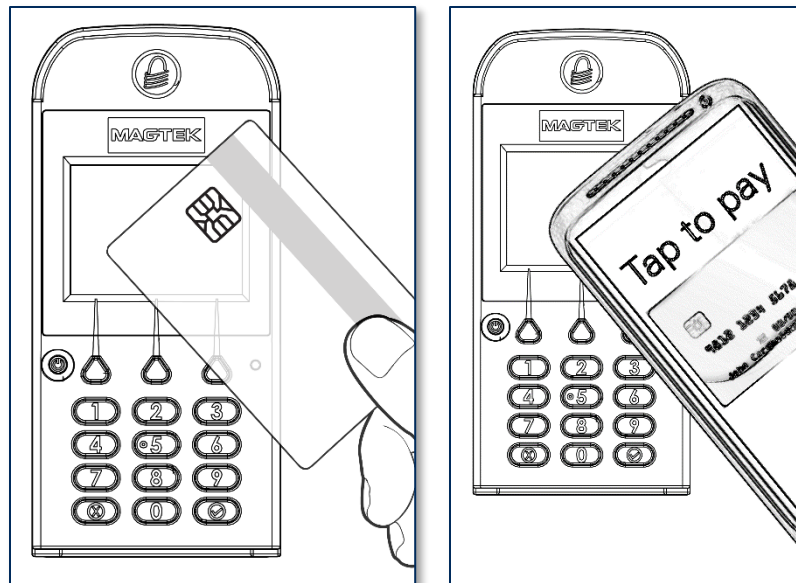


Figure 6-18 – Tapping a Contactless Card / Smartphone

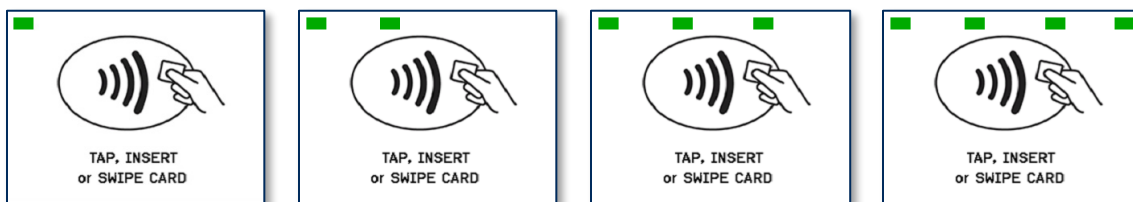
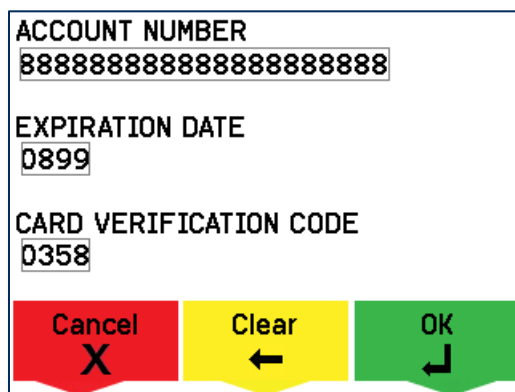


Figure 6-19 - Tap Read Is Complete

6.5.4 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 6-20**.

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
88888888888888888888

EXPIRATION DATE
0899

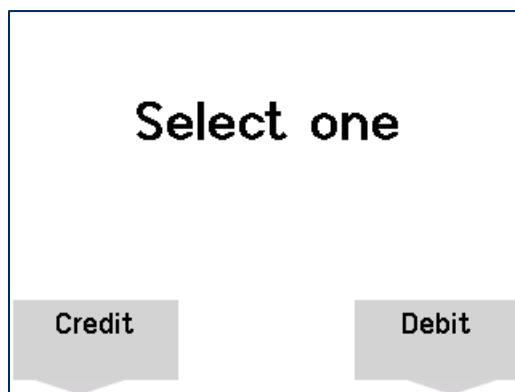
CARD VERIFICATION CODE
0358

Cancel X Clear ← OK ↵

Figure 6-20 - Example of User Screen to Manually Enter Card Data

6.5.5 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 6-21** shows the device is prompting the cardholder to press a function key on the keypad to select **Credit** or **Debit**.



Select one

Credit Debit

Figure 6-21 - Example of User Screen to Select Card Type

6.6 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 6-22**.

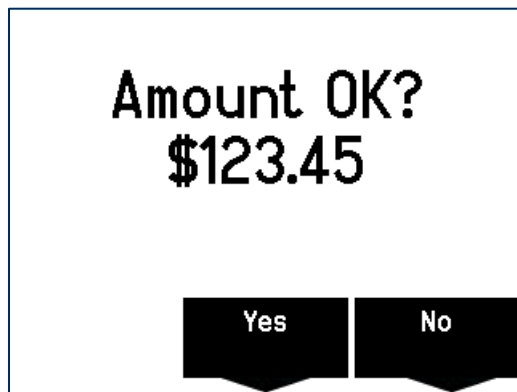


Figure 6-22 - Example User Screen to Verify Amount

6.7 How to Enter PINs

When a transaction requires the cardholder to enter a PIN, the device prompts the cardholder to **ENTER PIN** (see **Figure 6-23**) as required by the financial institution. The device expects the PIN to be between 4 and 12 digits long. After entering the PIN, the cardholder must press the **ENTER** button or the function key below the on-screen **Enter** option.

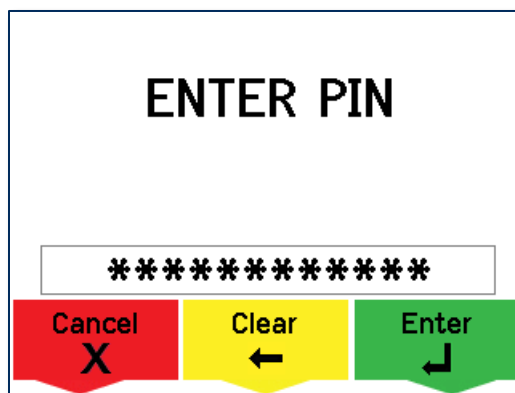


Figure 6-23 - Example of User Screen to Enter PIN

If the double PIN entry option is enabled, the device will prompt the cardholder to enter the PIN a second time. The process for re-entry is identical to the process for the first entry.

6.8 How to Use Signature Capture

Some models of DynaPro Go include touchscreen functionality for signature capture. See the part number label on the device and **Table 2-1 - Available Models and Options** on page 12 to see if the device you are using supports signature capture.



To enter a signature, use the tip of your finger (not a hard object like a fingernail or stylus) to press and glide against the touchscreen surface. Do not use a stylus or other hard object.

6.9 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 will prompt the user to **Enter Admin Passcode**. The operator should enter the passcode (the factory default is **8765432**) and press **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.

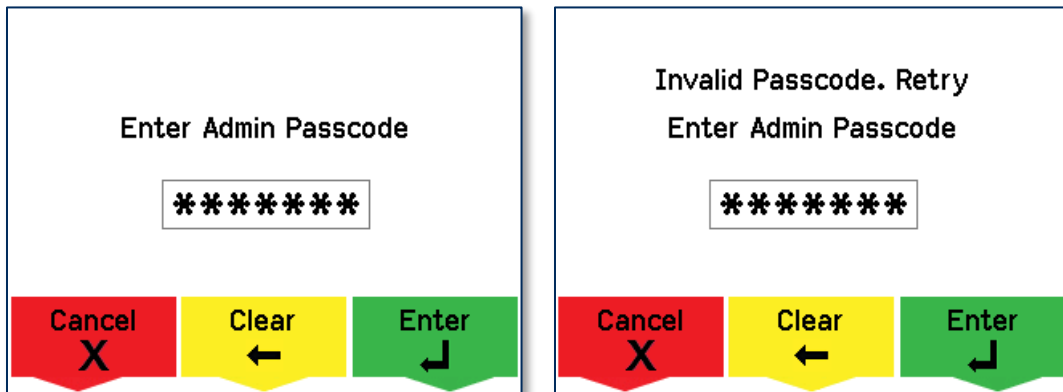


Figure 6-24 - Passcode Prompt Screens

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 unit with a soft, damp cloth and then wipe with a dry cloth.

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 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. These libraries simplify the development of custom applications that use DynaPro Go, and include:

- **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 TCP/IP or USB libraries. For more information about sending commands directly, see **D998200136 DYNAPRO GO PROGRAMMER'S REFERENCE MANUAL (COMMANDS)**.

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

Appendix A Technical Specifications

DynaPro Go Technical Specifications	
Reference Standards and Certifications	
ISO 7810 and ISO 7811, AAMVA TDEA (3DES)-CBC using DUKPT PCI PTS v4.x EMV ICC Specifications for Payment Systems Version 4.3 EMV Contactless Level 1 Book D v2.5 PayPass v3.0.2 payWave v2.1.3b Expresspay v3.0 Discover v1.1 FCC Title 47 Part 15 Subclass C EMC CE Level B EMC CE Safety AS/NZS 4268:2017 UR/CUR UL Recognized MasterCard TQM California Proposition 65 (California) WEEE (EU) IEEE 802.11 b/g/n, IEEE 802.11i-2004 WPA2-PSK, TKIP, AES, SHA-256 TCP/IP secured by Transport Layer Security (TLS) Protocol v1.2 USB 1.1, USB 2.0	
Physical Characteristics	
Dimensions (L x W x H):	6.1 in. (155 mm) x 2.8 in. (71 mm) x 1.0 in. (25.4 mm)
Weight (802.11, No SigCap):	8.85 oz. (251 g)
User Interface Characteristics	
Display Type:	QVGA TFT LCD Color
Display Size (viewable area):	1.97 in. (49.96mm) x 1.48 in. (37.72mm)
Display Resolution:	320x240 pixels 16-bit color depth
Keypad:	Full-travel membrane keypad providing tactile feedback 10 digits, 2 data entry keys, 3 multi-purpose function keys
Card Reader (magnetic stripe):	Triple Track (TK1/2/3), encrypting reader with MagnePrint
Card Reader (chip card):	EMV chip card reader
Contactless Reader:	EMV contactless reader
Acceptable Swipe Speeds:	10 inches per second to 50 inches per second

DynaPro Go Technical Specifications	
Communications Characteristics	
Data Connections:	TCP/IP over 802.11 wireless Micro-USB, implements USB 1.1 and USB 2.0 BLE and Bluetooth wireless (select models)
Wireless Range(s):	Wireless network: 150 ft. (45m) NFC: 1.6 in. (40mm)
Electrical Characteristics	
Battery Capacity:	1700 mAh nominal (rated)
Battery Charge, Powered Off:	1 year (new device)*
Battery Charge, Standby:	6 hours (new device)*
Battery Charge, Active:	
Power Inputs:	micro-USB connector Charging cradle contacts
Maximum Current Draw:	1A
Voltage Requirement:	5VDC
Battery Type:	Lithium Polymer rechargeable for main power Lithium coin cell for backup
RF Frequencies and Power:	802.11 Wireless: Average Power Radiated: 1.02mW (0.08 dBm) Conducted Power = 97.7mW (19.89 dBm) Frequency range 2400 MHz to 2497 MHz Contactless Reader: Radiated Power: 10.34dBm Frequency range: 13.553 MHz to 13.567MHz
Flash Memory:	256 MBit
Software Characteristics	
Tested Operating System(s):	iOS 7.1 and later Android 4.4.2 and later Windows 7, Windows 8.1, Windows 10
Environmental Tolerance	
Operating temperature:	32°F to 113°F (0°C to 45°C)
Operating relative humidity:	10% to 90% without condensation at 23 °C
Storage temperature:	14°F to 140 °F (-10 °C to 60 °C)
Storage relative humidity:	5% to 90% without condensation

DynaPro Go Technical Specifications	
Reliability	
Mechanical Life:	1,000,000 card swipes 500,000 chip card insertions
Battery Shelf Life:	2 years for Lithium coin cell backup
Battery Cycle Life:	500 charge / discharge cycles