

QMFA Wallet

iPhone and Apple Watch
Installation and Operation Manual



October 2025

Document Number:
D998200712-110

REGISTERED TO ISO 9001:2015

Copyright © 2006 - 2025 MagTek, Inc.
Printed in the United States of America

INFORMATION IN THIS PUBLICATION IS SUBJECT TO CHANGE WITHOUT NOTICE. MAGTEK CANNOT BE HELD LIABLE FOR ANY USE OF THE CONTENTS OF THIS DOCUMENT. ANY CHANGES OR IMPROVEMENTS MADE TO THIS PRODUCT WILL BE INCLUDED IN THE NEXT PUBLICATION RELEASE. IF YOU HAVE QUESTIONS ABOUT SPECIFIC FEATURES AND FUNCTIONS OR WHEN THEY WILL BECOME AVAILABLE, PLEASE CONTACT YOUR MAGTEK REPRESENTATIVE.

MagTek®, MagnePrint®, and MagneSafe® are registered trademarks of MagTek, Inc.
Magensa™ is a trademark of MagTek, Inc.
DynaPro™ and DynaPro Mini™, are trademarks of MagTek, Inc.
Qwantum Multi-factor Authentication™, is a trademark of MagTek, All Rights Reserved.

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 StoreSM 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
100	August 2025	Initial Release
110	October 2025	Updated User Interface with Main Menu, Nav Menu, QR Code Scan to add token, Force Touch and other Sharing options.

Table of Contents

Table of Contents	4
1 Introduction	5
1.1 System Overview	5
2 System Requirements	6
3 Token Types.....	6
4 Authentication Options	6
5 Installation and Usage	7
5.1 iPhone	7
5.2 Apple Watch.....	7
5.3 Using the QMFA Wallet.....	7
5.3.1 Main Menu: (Top Right).....	7
5.3.2 Navigation Menu (Bottom of Screen):	7
5.3.3 Using the QMFA iPhone App	8
5.3.4 Adding, Viewing, Editing, and Deleting Tokens	10
Adding a Token	10
Viewing a Token.....	11
Accelerated Access and Sharing Tokens.....	11
Editing a Token	12
Deleting a Token.....	12
Using a Token.....	13
Using the QMFA Apple Watch App.....	14
5.3.5 Use Cases	14
6 Integration & APIs	16
6.1 Troubleshooting & FAQs.....	16
6.2 Support.....	16
Appendix A Glossary of Terms	17
Appendix B Related Documentation.....	18
Appendix C Warranty and Software License	18
C.1 Limited Warranty.....	18
C.2 SOFTWARE LICENSE AGREEMENT	21

1 Introduction

MagTek's Quantum Platform is a next-generation tokenization and authentication framework designed to replace outdated security models with real-time, user-initiated, and cryptographically secure authentication of Quantum Tokens. Quantum Tokens can be used in place of legacy credentials and use for a specific purpose, such as granting access to a facility, to a website, to loyalty points, even stored value for coupons and closed loop payments.

The platform supports both card-present and digital environments, offering a mobile-first, yet flexible approach to eliminate static credentials that contain personally identifiable information (PII), prevent fraud, by strengthening and modernizing access and identity management.

The Quantum Platform is based on an extensive set of APIs, embedded circuits, hardware and services that have been integrated to generate powerful tokens including advanced delivery options, lifecycle management, and redemption services, all backed by powerful Quantum Multi-Factor Authentication or QMFA.

1.1 System Overview

The Quantum Platform is based on an extensive set of APIs, embedded circuits, hardware and services that have been integrated to generate powerful tokens including advanced delivery options, lifecycle management, and redemption services, all backed by powerful Quantum Multi-Factor Authentication or QMFA.

The Quantum Platform consists of three primary components: Quantum Tokens, the QMFA Wallet mobile application, and Quantum APIs that facilitate secure token validation. Authentication occurs by creating tokens within the Quantum Platform, displaying them as QR codes in the QMFA Wallet, in a text message or in an email; then scanning them with a compatible QR Code reader or Dyna Device. For tokens that use Time-Based One-Time Passwords (TOTP), the QMFA Wallet app automatically generates and refreshes codes every 30 seconds. This system is designed to secure both physical and digital entry points, such as doors, portals, point-of-sale terminals and other forms of stored value and loyalty.

QMFA supports a variety of use cases, including corporate access control, multifactor authentication in the banking and credit union arena, secure retail checkout, healthcare facility, couponing, loyalty and stored value, etc.

2 System Requirements

Compatibility:

- iPhone
 - Requires iOS 17.0 or later.
- iPad
 - Requires iPadOS 17.0 or later.
- Apple Watch
 - Requires watchOS 11.0 or later.
- Apple Vision
 - Requires visionOS 1.0 or later.

3 Token Types

QMFA supports several token types to meet a range of security and convenience requirements:

- **Simple text:** Store any plain string of data you need to access quickly.
- **URLs/UIRs:** Tokens that, when scanned, open a specific web link.
- **URLs/URIs with integrated data:** Seamlessly access websites and automatically input token data or TOTP codes into the correct fields.

4 Authentication Options

QMFA supports several options for configuring additional factors of authentication per token:

- **One-Time Codes (OTC):** Receive real-time generated, One-Time Use codes via SMS or email.
- **Timed Access Codes (TACs):** Receive real-time generated, multi-use codes via SMS or email.
- **Time-Based One-Time Passwords (TOTP):** Keep your dynamic security codes readily available using the QMFA Wallet app for iOS.

5 Installation and Usage

Begin by downloading the latest version of the “QMFA Wallet” app, found [Here](#).

5.1 iPhone

The QMFA Wallet app is available on the Apple App Store. After downloading the app, users should grant the necessary permissions, including camera access for QR code display and optional notifications for token-related alerts.

5.2 Apple Watch

To use QMFA on an Apple Watch, the wallet must first be installed on the paired iPhone. Once installed, the companion Apple Watch app can be added through the Watch app on iPhone. Tokens automatically sync between the phone and watch, enabling quick wrist-based access.

5.3 Using the QMFA Wallet

5.3.1 Main Menu: (Top Right)

The Main menu (circle with three dots) serves as your hub for global security, support, and account management.

- **App Health and Support:**
 - Instantly Check for Updates
 - Access the Support Center (Help/FAQs) for immediate assistance
 - View the current App Version

5.3.2 Navigation Menu (Bottom of Screen):

The Navigation menu is a collection of action buttons designed to be easy to access.

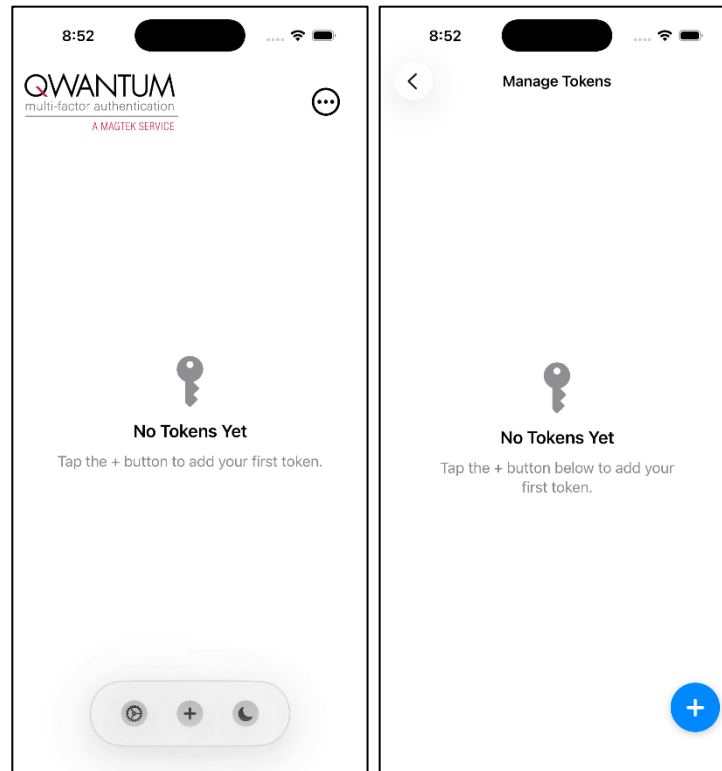
- **View Toggle (List/QR toggle Icon):** Instantly switch the main display. Flip between the **List View**, offering a comprehensive token overview and the **QR Code View**, providing quick, secure access for a single selected credential.
- **Token Management (Cogwheel):** Access the critical **Managed Tokens Page**. This hub now allows you to view all assets and credentials and provides immediate access to their individual properties. *This list will allow the user to change the display order for tokens, which by default is first in and first out. See Sort Order.*
- **New Token Creation (Plus Sign):** Launch the **Add New Token** flow. Quickly import credentials by scanning a properly formatted QPass QR Code or manually entering the data.
- **Contextual Share (Share Sheet Icon):** Access tailored sharing options for the *currently selected* token. This feature provides a secure method for transferring specific data. **Note:** This icon is hidden in the List View to prevent any ambiguity about which token you intend to share.
- **Appearance Toggle (Rightmost Icon):** Instantly switch the entire application between a high-contrast **Dark Mode** and a standard **Light Mode**, optimizing visibility in any environment.

5.3.3 Using the QMFA iPhone App

Begin by downloading the latest version of the QMFA Wallet app, found [Here](#).

After the app is downloaded, a token will need to be added.

1. Tap the **Add** button, located in the middle of the bottom navigation menu. Fill out the form and press **Add Token** to save.
2. Alternatively, press the **cog icon** to the left of the **Add** button the bottom navigation menu to open the Manage Tokens screen.
3. From there, follow the steps by pressing the (+) to display the **Add Token** screen.

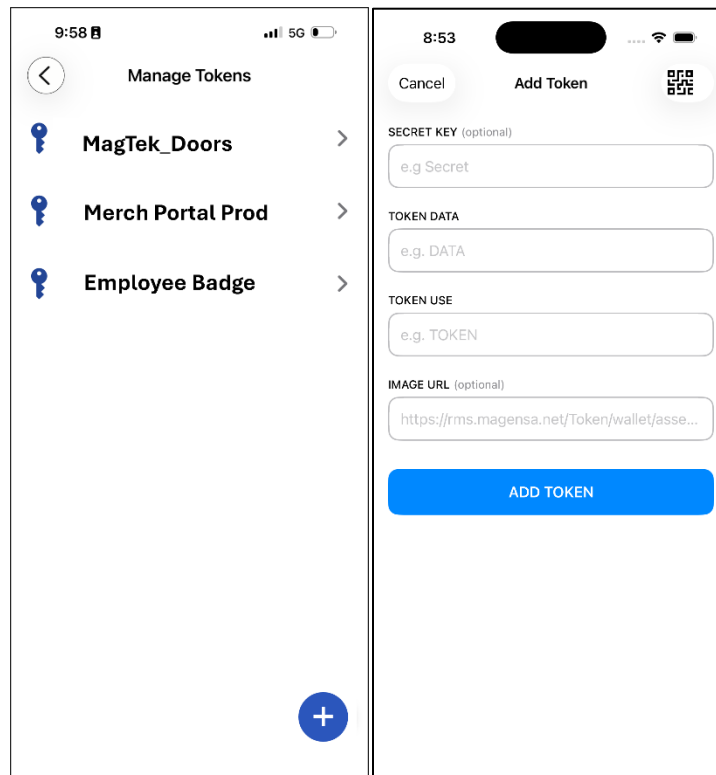


Simplified Management and Personalization

We reduced friction in managing your tokens, making maintenance concise and straightforward.

- **Streamlined Deletion:** On the **Manage Tokens Page**, you can now simply **swipe from right to left** on any token listing to instantly initiate the deletion process.
- **Instant Provisioning:** Adding new credentials is now faster. Use the new **QR Code Scanner** directly on the **Add Token** form to provision a QPass into your wallet instantly.
- **Visual Token Customization:** Personalize your tokens with a distinct visual identity. When creating a new token, specify an **Image URL** to display a custom visual identifier instead of the default MagTek headquarters image. **Crucial Constraint:** The token image cannot be modified after the initial saving process.

- **Sort Order:** This feature provides **enhanced token sorting**, giving users precise control over how tokens appear in the **List View** and on the **Manage Tokens** page. This is done through the use of **Force Touch**. Simply press firmly on a token and then **drag and drop** it to its new place in the list. The preferred order created in the main app will instantly **synchronize** with the tokens displayed in the companion **Apple Watch app**.

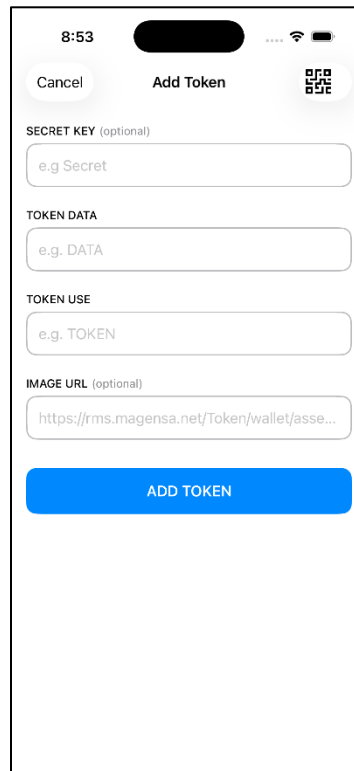


5.3.4 Adding, Viewing, Editing, and Deleting Tokens

Adding a Token

The Add Token Screen Fields appear as follows:

- **Secret Key:** Enter your secret data here. This field is optional.
- **Token Data:** Input your token data here. This is a required field.
- **Token Use:** Specify the token's use here. This is a required field.
- **Image URL:** Specify the token's custom branding image here. This field is optional field.
- **Add Token Button:** Press this button when all relevant fields are entered.



The screenshot shows the 'Add Token' screen of the QMFA Wallet app. At the top, there is a status bar with the time 8:53, a blacked-out notch area, and signal/battery icons. Below the status bar, there are three buttons: 'Cancel' (white with black text), 'Add Token' (white with black text), and a QR code icon (white with black text). The main content area contains four input fields, each with a label and a placeholder text: 'SECRET KEY (optional)' with 'e.g Secret', 'TOKEN DATA' with 'e.g. DATA', 'TOKEN USE' with 'e.g. TOKEN', and 'IMAGE URL (optional)' with 'https://rms.magenssa.net/Token/wallet/asse...'. At the bottom of the form is a large blue button with the text 'ADD TOKEN' in white.

Viewing a Token

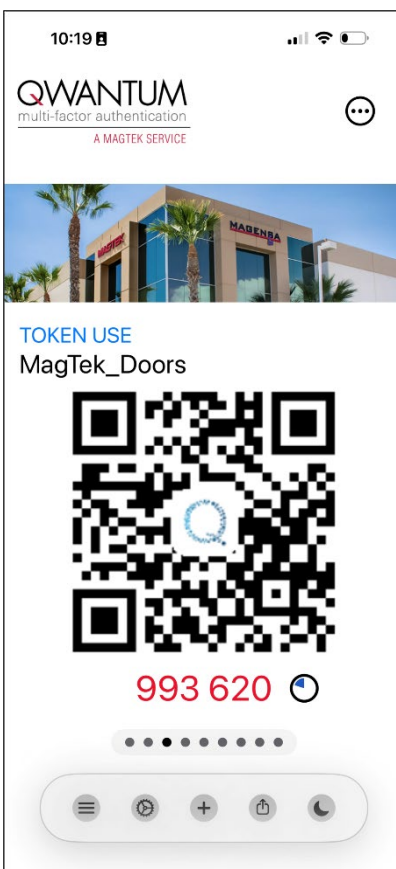
Tokens can be viewed by tapping the View Toggle on the bottom menu (left-most icon) to switch between QR View (swipe side-to-side) and List View (swipe up-and-down).

A QR code for your selected token will appear on your iPhone screen, ready for scanning by an MMS Dyna Family device with BCR or other barcode reader.

Accelerated Access and Sharing Tokens

Accessing and distributing your credentials is now faster and more intuitive. **Force Touch** or **long-press** on any token's QR code to unveil these dynamic, quick-access options:

- **Secure QPass Transfer:** Quickly and safely transfer eligible tokens to another QMFA Wallet user for shared access. **Important:** Tokens containing a token secret or designed for single-user security (like TOTP or OTC) are unique to you and cannot be shared.
- **Open in Browser:** Instantly launch the token's associated website or URL in your device's default browser.
- **External Link Sharing:** Use native iOS sharing options (e.g., Email, AirDrop, Messages) to securely share the web link contained within the token data.
- **Quick Data Copy:** Instantly copy the raw information stored within the QR code directly to your clipboard for use in other applications.



Editing a Token

Changes to a token can be made by modifying fields in the **Edit Token** screen. Press **Save Changes** when all desired changes have been made.

8:53

< Back Add Token

SECRET KEY (optional)

TOKEN DATA

TOTP~adfgds531cf461fgffg111

TOKEN USE

MagTek_Doors

IMAGE URL (optional)

https://rms.magensa.net/Token/wallet/asse...

SAVE CHANGES

DELETE TOKEN

Deleting a Token

On the Managed Tokens Page, simply swipe right-to-left on any token listing to initiate the deletion process. Alternatively, go to the Managed Tokens Page, tap any token to launch its details page and choose the **Delete Token** button.

10:19

QWANTUM
multi-factor authentication
A MAGTEK SERVICE

TOKEN USE
MagTek_Doors

993 620

9:58

Manage Tokens

- MagTek_Doors
- Merch Portal Prod
- Employee Badge

8:53

Cancel Add Token

SECRET KEY (optional)

TOKEN DATA

TOTP~adfgds531cf461fgffg111

TOKEN USE

MagTek_Doors

IMAGE URL (optional)

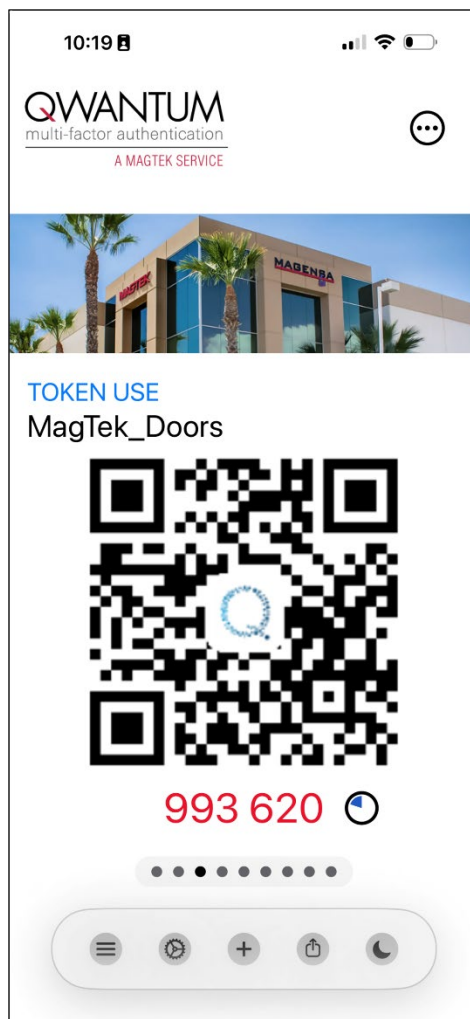
https://rms.magensa.net/Token/wallet/asse...

ADD TOKEN

DELETE TOKEN

Using a Token

1. **Open the App:** Tap the app icon on your iPhone's home screen to launch the QMFA Wallet app.
2. **Select your preferred view:** Use the View Toggle on the bottom menu to switch between QR View (swipe side-to-side) and List View (swipe up-and-down).
3. **Select a Token:** Choose the specific digital token you want to use, identified by its "Token Use."
4. **Display QR Code:** A QR code for your selected token will appear on your iPhone screen, ready for scanning by an MMS Dyna Family device with BCR.
5. **Scan:** Hold your iPhone in front of a QR code reader on an MMS Dyna Family device with BCR. The device automatically reads the necessary information, including any embedded TOTP.
6. **View TOTP (Optional):** If you need to see the TOTP manually for entry, locate it on the screen. It will appear on the phone app in red text beneath the QR Code and it will show a countdown timer changing every 30 seconds from 0 seconds and 30 seconds past the minute.



Additional details:

- When selecting a token, the screen shows:
- QR code for scanning by Dyna Devices with BCR.

- Token Use (left side) above the QR.
- TOTP in red numbers below the QR; updates every 30 seconds.
- A countdown indicator shows time remaining until refresh.

Using the QMFA Apple Watch App

The Apple Watch companion app allows users to access their tokens directly from their wrist. By scrolling through the app, users can select a token and display its QR code for scanning with a Dyna Device. TOTP values are detected automatically during scanning, though users can scroll down to view the code manually if needed.

5.3.5 Use Cases

QMFA is ideal for securing both physical and digital environments. In physical settings, tokens can unlock doors, gyms, and secure facilities. Digitally, they provide password-less login to services like the Magensa Merchant and Reseller Portals or access to loyalty and stored value. Industries such as healthcare, retail, car washes, laundry operators and private clubs benefit from QMFA's ability to simplify authentication without compromising security.

Use Cases for What Can Be Saved to the QMFA Wallet:

Use Case Category	What is Saved (Token Data)	Why it is Saved
Personal Sharing & Networking	vCard / Contact Info (Simple Text / URL)	Quickly share your professional or personal contact information. The recipient simply scans your phone's or watch's QR code to instantly import your details.
Guest Network Access	Wi-Fi Login Credentials (Simple Text)	Eliminate the need to read out complex passwords. Friends and family can easily and instantly join your secure network by scanning the token.
Automated Communication	Email Template QR Code (URL with integrated data)	Allow anyone to instantly generate a pre-formatted email to you (e.g., a service request, lead generation, or feedback) just by scanning the token.
Secure Web Access (Frictionless)	URL with Integrated Data (URL with integrated data)	Automatically log into portals (like the Magensa Merchant Portal) or internal company websites without typing. The token automatically pastes your credentials or a TOTP into the login fields.
High-Security Login	Time-Based One-Time Passwords (TOTP) (TOTP)	Store dynamic, continuously regenerating security codes for third-party systems, providing strong, two-factor authentication without relying on SMS or separate apps.

Use Case Category	What is Saved (Token Data)	Why it is Saved
Physical Access Control	Facility Access Credential (Simple Text / Timed Access Code)	Use your Apple Watch or iPhone as a secure, keyless entry device to unlock doors for private clubs, corporate offices, server rooms, or event venues when scanned by a MagTek Dyna Device.
Single-Use Verification	SMS-Based One-Time Codes (OTC) (OTC)	Securely manage and retrieve single-use codes for transaction approvals, password resets, or high-risk administrative actions.
Quick Information Retrieval	Simple Text String (Simple Text)	Store simple, non-sensitive data you need to access quickly, such as locker combinations, membership numbers, or license plate numbers.
Instant Website Navigation	Simple URL (URL)	Store favorite or frequently accessed websites for one-tap opening in your default browser.

6 Integration & APIs

Developers can integrate QMFA into their systems using published APIs available through the Quantum services. A [Postman](#) sandbox environment supports testing and development, allowing rapid proof-of-concept builds and seamless integration with existing workflows.

6.1 Troubleshooting & FAQs

Common errors include QR codes not scanning, tokens appearing expired, or missing tokens after sync. These issues are typically resolved by adjusting screen brightness, refreshing the token, or ensuring the mobile device is properly paired with Apple Watch.

See [FAQs](#).

6.2 Support

For assistance, contact MagTek support. Additional documentation and integration resources are available at the [QMFA postman collection](#).

Appendix A Glossary of Terms

- API – Application Programming Interface
- FAQs – Frequently Asked Questions
- SDK – Software Developer’s Kit
- QMFA: Qwantum Multi-Factor Authentication
- TOTP: Time-Based One-Time Password
- OTC: One-Time Code (SMS-delivered)
- TAC: Timed Access Code
- BCR: Barcode Reader (on Dyna Devices)

Appendix B Related Documentation

To view or download any of the documents mentioned in this manual, visit <https://www.magtek.com/support>.

Appendix C Warranty and Software License

C.1 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 support@magtek.com

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.

C.2 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 IN 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 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 LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS ALL OF ITS TERMS, CONDITIONS, AND RESTRICTIONS, AND AGREES TO BE BOUND BY THEM. LICENSEE ALSO AGREES THAT THIS AGREEMENT SUPERSEDES ANY AND ALL VERBAL AND WRITTEN COMMUNICATIONS BETWEEN LICENSOR AND LICENSEE OR THEIR ASSIGNS RELATING TO THE SUBJECT MATTER OF THIS AGREEMENT.

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

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