



## PIVCheck Mobile Edition User Guide

Codebench, Inc  
6820 Lyons Technology Circle Ste. 140  
Coconut Creek, FL 33073

Voice: 561.883.3218  
Fax: 954.426.8985  
[www.codebench.com](http://www.codebench.com)

**Codebench**

This page is intentionally left blank.

# Contents



- Chapter 1 About This Manual ..... 1**
  - Typographical Conventions ..... 1
  - Trademarks and Copyrights ..... 2
- Chapter 2 Terminology ..... 3**
  - Acronyms ..... 3
  - Definitions ..... 3
- Chapter 3 Key Features ..... 7**
  - PIVCheck Mobile Edition ..... 7
    - Cardholder Validation ..... 7
    - Cardholder Certificate Validation ..... 7
    - Card Validation ..... 7
  - PIVCheck Plus Mobile Edition ..... 7
    - PACS Registration ..... 7
    - Batch Import ..... 8
    - Operator Override ..... 8
    - Imported Field Mapping ..... 8
    - Certificate Data ..... 8
    - Distributed Configuration ..... 8
    - Centralized Audit Option ..... 8
  - Supported Credential Types ..... 8
- Chapter 4 System Architecture ..... 9**
  - Hardware Configuration ..... 9
  - Software Configuration ..... 9
    - PIVCheck Mobile Edition ..... 9
    - PIVCheck Plus Mobile Edition ..... 10
  - Hardware ..... 10
  - Software ..... 11
    - FIPS 201 Product Compliance ..... 11
    - FIPS 140-2 Level 1 Requirement for PIVCheck Mobile Edition ..... 11
- Chapter 5 Software Installation ..... 13**
  - Installation Options ..... 13
  - Important Notice ..... 13
  - Powering Up ..... 13
  - Downloading PIVCheck Mobile directly on the Mobile Terminal ..... 14
  - Installing PIVCheck Mobile File from a Flash Drive ..... 18

<b>Chapter 6 Configuring the System</b>	<b>19</b>
Licensing the Software	19
Trial License	21
Enter your License Manually	21
Changing the Admin Password	22
Configuring the PACS plug-in on your PC (Plus Only)	23
Authorizing Client Connections	23
Synchronize Configuration (Plus Only)	24
Manually Configuring the PIVCheck Mobile Device	26
Plus Tab (Plus Only)	26
Registration Handling	27
Server Address	27
Server Port	27
PACS Connection Failures	28
Client Not Authorized	28
Incorrect Server IP Address or Network Routing Problem	28
Server Exists but PACS Service is not Running	29
Offline File Folder	29
Application Tab	31
Fingerprint Options	32
Audit Log Folder	34
Error Log Folder	35
Configurable Contact Information	35
Automatic Rollover	36
Devices Tab	36
Blacklist Plug-ins	36
Users	37
User ID	37
Password	37
Role	37
Door Control (Optional)	38
Door Control Configuration Form	39
Communications Status Indicators	41
Saving your Configuration	41
 <b>Chapter 7 Identity Verification</b>	 <b>43</b>
Something you Have (PIV Credential)	43
Something you Know (Knowledge of PIN)	44
PIN Failure	45
PIN Match	46
Something you are (Biometric attributes)	47
Fingerprint Match	47
Scoring	47
Fingerprint Match Threshold	47
Fingerprint Match Failure	48
Certificate Validation	49
The Card Data Window	49
The Application Events Window	49
Identity Authentication	49
Displaying Cardholder Data	49

Photo Tab .....	50
Info Tab .....	50
Events Tab .....	51
PACS Registration (Plus Only) .....	52
Registering the Cardholder .....	52
Saving Credentials Locally .....	53
Canceling Registration .....	53
User Fields .....	54
<b>Chapter 8 Tools .....</b>	<b>57</b>
Synchronize Configuration (Plus Only) .....	57
Batch Import Button .....	57
Batch Import Failure .....	59
Incompatible Data formats .....	59
Export Audit Logs Button .....	61
Audit Data Elements .....	61
Upload to Server (Plus and/or Audit Trail Only) .....	62
Exporting Audit Log to Flash Drive .....	62
Audit Log File Cleanup .....	63
Change Diagnostic Logging Level Button .....	63
Licensing the Software .....	66
<b>Chapter 9 Updating Your Software .....</b>	<b>67</b>
Overview .....	67
Automatic Software Download .....	67
Installing an Executable File via Internet Explorer Download .....	71
Installing an Executable File from a Flash Drive .....	75
<b>Appendix A .....</b>	<b>77</b>
Reference Documents .....	77
<b>Appendix B .....</b>	<b>79</b>
Card Data Containers .....	79
Table 1. PIV Data Containers .....	79
Table 2. TWIC Data Containers .....	81
<b>Appendix C .....</b>	<b>83</b>
Proximity Reader Configuration - DSV2+ ONLY .....	83
Overview .....	83
Procedure .....	83
Preparing the Reader .....	83
Facility and ID Codes .....	83
Keystroke Data .....	83

This page is intentionally left blank.



# ABOUT THIS MANUAL

## TYPOGRAPHICAL CONVENTIONS

This document uses the following typographical conventions:

- Command and option names appear in bold type in definitions and examples. The names of directories, files, machines, partitions, and volumes also appear in bold.
- Variable information appears in *italic* type. This includes user-supplied information on command lines.
- Screen output and code samples appear in a `monospace code` type.

In addition, the following symbols appear in command syntax definitions.

- Square brackets [ ] surround user-supplied optional items.
- Angle brackets < > surround user-supplied values that are required.
- Percentage sign % or the construct "C:\" represents a regular Windows command shell prompt.
- Pipe symbol | separates mutually exclusive values for a command argument.



This symbol denotes important information or values.

## TRADEMARKS AND COPYRIGHTS

Microsoft Windows XP, Microsoft Windows CE, Microsoft .NET, and Microsoft Compact Framework are registered trademarks of Microsoft Corporation.

TWIC is a trademark of the United States Transportation Security Administration (TSA).

*PIVCheck* is a registered trademark of Codebench, Inc. *PIVCheck Mobile*, *PIVCheck Desktop*, *PIVCheck Plus Mobile*, *PIVCheck Plus Desktop*, *TWICCheck*, *TWICCheck Plus Edition*, *OMNICheck*, *OMNICheck Plus* and *PIVCheck Certificate Manager* are trademarks of Codebench, Inc.

All other trademarked or copyrighted names mentioned herein are the property of their respective owners.



# TERMINOLOGY

## ACRONYMS

<i>Abbreviation</i>	<i>Long Form</i>
AIA	Authority Information Access
CA	Certification Authority
CHUID	Cardholder Unique Identifier
CPV	Certificate Path Validation
CRL	Certificate Revocation List
CRLDP	Certificate Revocation List Distribution Points
CTL	Certificate Trust List
FASC-N	Federal Agency Smart Credential Numbers
FIPS	Federal Information Processing Standard
ICC	Integrated Circuit Chip
IDN	Issuer Distinguished Name
OCSP	Online Certificate Status Protocol
PACS	Physical Access Control System
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
QCRL	Quick Certificate Revocation List
SCVP	Server-based Certificate Validation Protocol
TWIC	Transportation Worker Identification Credential
TPK	TWIC Privacy Key
VA	Validation Authority

## DEFINITIONS

- **Administrator**

An *administrator* is an individual authorized to manage one or more desktop or mobile biometric terminals. Administrators are provided additional functionality to based on their login credentials.

- **Cardholder**

A *cardholder* is an individual who has been issued a credential which is supported by our software. For more information refer to “Supported Credential Types” on page 8.

- **Certificate Authority (CA)**

A *certificate authority* (CA) is an entity that issues digital certificates to organizations or individuals. The CA is usually well known and universally trusted. A CA may authorize other entities to issue certificates on its behalf, thereby creating or extending a *chain of trust*. Certificates contain a digital version of this chain so that software can verify each node on the chain of trust is a valid CA, a process called *Certificate Path Validation*.

- **Certificate Revocation List (CRL)**

A CRL is a list of certificates that have been revoked before their expiration by a certificate authority.

- **Mobile Biometric Terminal**

A *Mobile Biometric Terminal* is a mobile, hand-held reader configured with the following components:

- FIPS 201 compliant smart card reader capable of reading PIV-II compliant cards over its contact or contactless smart card interface
- FIPS 201 compliant fingerprint capture device.

The currently supported models are Datastrip's DSV2+<sup>TURBO</sup> and DSV3 EasyRead, MaxID's IDLMAX, DAP's CE3240BWE, MorphoTrak's MorphoCheck and Cross Match's Be.U Mobile. These devices, and/or their card and biometric components have been certified by GSA for use with FIPS 201 CHUID applications.

- **Data Mapping Template**

A data-mapping template provides the ability to map the data fields acquired from a PIV card to the fields in a PACS personnel and/or card database record.

- **Desktop Biometric Terminal**

A desktop biometric terminal is a standard desktop PC, integrated with the following components:

- FIPS 201 compliant smart card reader capable of reading PIV-II compliant cards over its contact interface
- FIPS 201 compliant fingerprint capture device.

- **Installer**

An *installer* is a person responsible for installing PIV acquisition hardware and software.

- **Online Certificate Status Protocol (OCSP)**

The *online certificate status protocol* (OCSP) defines a series of messages between software applications that need to verify whether the issuing CA has revoked an x.509 digital certificate. An OCSP server does not check the validity of any of the certificate in the chain of certificates associated with the end entity (certificate in question).

- **Physical Access Control System (PACS)**

A *physical access control system* (PACS) refers to an integrated unit of software, data, firmware, microcontrollers, and ingress/egress devices that control human access to areas within a facility. A PACS head-end usually consists of one or more servers that communicate with field devices to which doors, turnstiles, and access readers are physically connected.

- **Personal Identity Verification (PIV)**

FIPS 201 *Personal Identify Verification* is a two-part standard, referred to as PIV-I and PIV-II, respectively:

- defines the processes and infrastructures that are used in establishing a person's identity and issuing them a credential.
- defines technical interoperability requirements for those credentials to be used in a variety of applications.

- **Server-based Certificate Validation Protocol (SCVP)**

Server-based certificate validation protocol (SCVP) defines a series of messages between software applications that need to verify whether the issuing ca has revoked an x.509 digital certificate. An SCVP server checks the validity of all

of the certificates in the chain of certificates associated with the end-entity and can return additional information to enable a relying party (client) to make more intelligent decisions regarding the certificate.

- **Transportation Worker Identification Credential (TWIC)**

The Transportation Worker Identification Credential (TWIC) is a standard that is intended to address the unique needs of transportation workers, most notably within the maritime industry. TWIC breeder documents and biometric data are gathered and processed by systems that comply with FIPS 201 PIV-I. TWIC cards are required to be PIV-II compliant and can be read by any PIV-II compliant smart card reader.

The TWIC standard diverges from the PIV-II standard in that it provides for contactless card-reader biometric data exchange, whereas the FIPS 201 PIV-II standard states that biometric data retrieval can only be performed while the card is in physical contact with the reader. The two main factors that drive this are:

- TWIC cards are used in high traffic areas, where a mistyped or forgotten PIN creates delays
- a corrosive maritime environment can impact contact-based readers

- **TWIC Privacy Key (TPK) (TWIC cards only)**

The TWIC privacy key is used to protect cardholder privacy when transmitting biometric templates over a TWIC's contactless interface. An application acquires the TPK from the card's magnetic stripe, the smart card's TPK container, or from a server on a network. *OMNICheck* retrieves this key when the smart card is inserted into the contact reader.

- **User (Operator)**

A *user* is an individual that has been authorized to operate a mobile biometric terminal. *PIVCheck Desktop Edition*, *PIVCheck Mobile Edition* and *OMNICheck* enables its extraction and data import functions after it determines the individual logging into the system is authorized to perform user-level functions.

- **Validation Authority**

A validation authority is a trusted computer-based service that can verify to a relying party that a digital certificate is valid and has not been revoked. A validation authority should always consider the complete certificate hierarchy of issuer, intermediate, and trust anchor certificates before it validates the certificate.

The Tumbleweed Validation Authority (VA) has been tested and certified for use with *PIVCheck Desktop Edition*, *PIVCheck Mobile Edition* and *OMNICheck*. It can be configured as a full-blown Validation Authority (VA) Responder or as a VA Repeater (recommended). In Repeater mode, it will act as a proxy OCSP Responder, caching and issuing signed OCSP responses from a trusted Validation Authority within the Federal PKI.

This page is intentionally left blank.

# KEY FEATURES

## PIVCHECK MOBILE EDITION

*PIVCheck Mobile Edition* is designed to help security personnel to verify cardholder identity and ensure that they possess a valid credential.

### CARDHOLDER VALIDATION

*PIVCheck Mobile Edition* employs a three-factor authentication to verify a cardholder's identity. The cardholder is first prompted for a cardholder PIN. If the PIN is matched, the cardholder's certificates and biometrics are read from the card. The cardholder is then prompted for a fingerprint. If the fingerprint is matched, the certificates on the card are validated using the configured PKI plug-in.

### CARDHOLDER CERTIFICATE VALIDATION

*PIVCheck Mobile Edition* can ensure that each mandatory and optional X.509 certificate extracted from a PIV card is validated in several ways including:

- that the current date is between the notBefore and notAfter dates
- that the certificate was issued by a trusted authority
- that the certificate is not revoked

Certificates are validated using combinations of local and online queries using OCSP or SCVP. For completely offline certificate validation, *PIVCheck Mobile Edition* can check certificates against previously imported CRLs. For TWIC applications, *PIVCheck Mobile Edition* also checks a card's FASC-N against the TSA hot list.

### CARD VALIDATION

*PIVCheck Mobile Edition* issues a GENERAL AUTHENTICATE challenge to the PIV card applet to ensure that it is communicating with an authentic card, not a forgery. If configured, *PIVCheck Mobile Edition* submits the CHUID certificate to a validation authority to check for revocation.

## PIVCHECK PLUS MOBILE EDITION

In addition to the core features offered by *PIVCheck Mobile Edition*, *PIVCheck Plus Mobile Edition* provides the following enhancements.

### PACS REGISTRATION

*PIVCheck Plus Mobile Edition* has the ability to import cardholder data into a PACS. The following information is acquired from a PIV card:

- Cardholder Photograph
- FASC-N
- Certificate Expiration Date
- First, middle, and last name
- TWIC Privacy Key (TWIC cards only)
- Employee Affiliation
- Card Expiration Date
- Agency Card Serial Number
- Issuer Identifier
- Any other data field stored on the PIV card

## BATCH IMPORT

Using *PIVCheck Plus Mobile Edition*, a cardholders data can be stored on a mobile biometric terminal and imported into the PACS at a later time via batch processing.

## OPERATOR OVERRIDE

The *PIVCheck Plus Mobile Edition* operator can choose not to import the data extracted from a given PIV card into the PACS. The extracted card data is not saved or cached.

## IMPORTED FIELD MAPPING

When configured with a PACS plug-in, *PIVCheck Plus Mobile Edition* can map PIV data fields to PACS cardholder fields. Vendor-, product-, and release-specific field mappings and data transformations are specified through the use of data mapping templates.

## CERTIFICATE DATA

*PIVCheck Plus Mobile Edition* inserts PIV authentication certificates and FASC-N into a certificate database. If *PIVCheck Certificate Manager* is installed at the site, these stored PIV authentication certificates are re-validated against a CRL, OCSP/SCVP responder/repeater, or the TSA TWIC hot list on a periodic basis.

Through the use of data mapping templates, stored authentication certificates can be associated with PACS badges. This gives *PIVCheck Plus Mobile Edition* the ability to deny cardholders with revoked credentials access to controlled areas within a secured facility.

## DISTRIBUTED CONFIGURATION

*PIVCheck Plus Mobile Edition* includes a PC-based software component called a PACS plug-in. This software can be installed on the same computer as the PACS or on a separate computer, if necessary. In addition to serving as a broker between mobile biometric terminals and the PACS, the PACS plug-in maintains a site-wide configuration profile for all mobile biometric terminals, making it easy to commission new mobile terminals.

## CENTRALIZED AUDIT OPTION

With *PIVCheck Plus Mobile Edition* configured with the *Audit* option, event logs from each mobile biometric terminal are uploaded to a central database so that audit reporting can be performed from a central location.

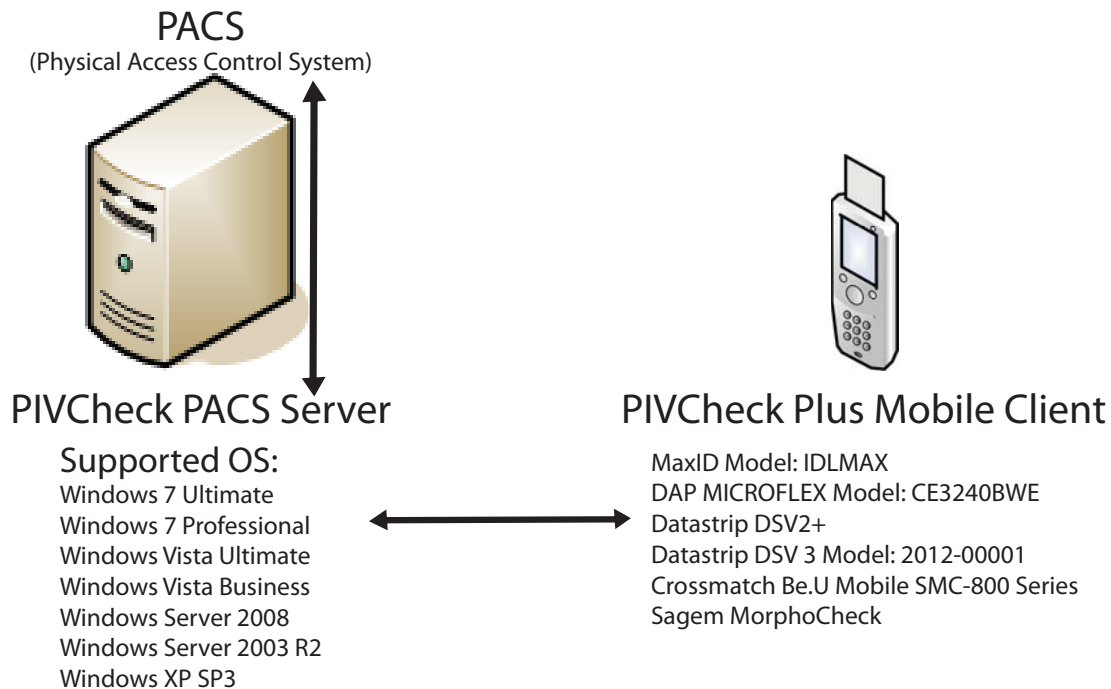
## SUPPORTED CREDENTIAL TYPES

- Transportation Worker Identification Credential (TWIC)
- Personal Identity Verification (PIV, CAC EP)
- Common Access Credential (Legacy CAC)

# SYSTEM ARCHITECTURE

## HARDWARE CONFIGURATION

A typical hardware configuration is shown below. A smart card reader, fingerprint sensor, and randomized PIN pad are integrated into a weather-resistant, ruggedized PDA and are referred to as a mobile biometric terminal. The terminal software prompts the cardholder and operator at each step of the data acquisition process. The mobile biometric terminal collects the data, validates a PIV card with the PKI plug-in or TSA hotlist, and uploads to the PACS (if one exists).



## SOFTWARE CONFIGURATION

*PIVCheck Mobile Edition* can be configured as a stand-alone identity validation system or integrated with a PACS. As a result, there are two possible baseline software architectures.

### PIVCHECK MOBILE EDITION

*PIVCheck Mobile Edition* runs independently with no communication with a PACS server. Cardholder identity is validated using the smart card reader, PIN pad, and fingerprint scanner installed within the mobile biometric terminal.

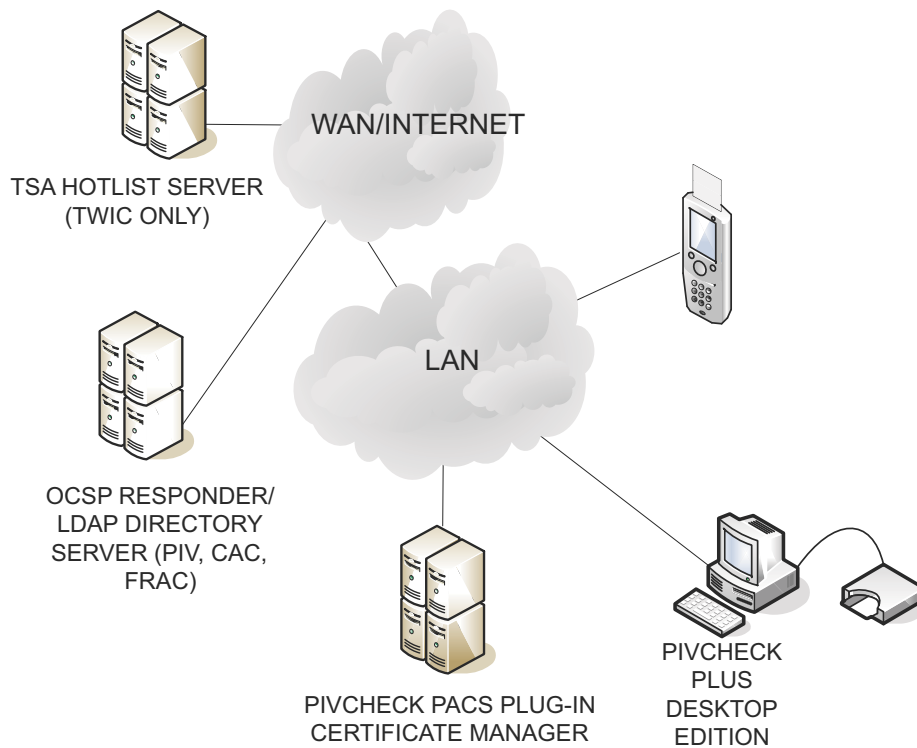
Depending on the environment, the validity and authenticity of a PIV card is verified through communication with an OCSP/SCVP responder/repeater or TSA Hotlist. Other than the event logs, no credential information is stored or forwarded.

Each mobile biometric terminal is configured separately using an administrative account specific to that terminal.



## PIVCHECK PLUS MOBILE EDITION

*PIVCheck Mobile Edition* includes a server-based software component, called a PACS plug-in, which serves as a broker between mobile biometric terminals and the PACS. The functions supported by the PACS plug-in include PACS registration, batch import of cardholder data, mapping data from PIV data fields to PACS cardholder fields, and associating PIV cards with PACS badges. In addition, the PKI data stored by the PACS plug-in can be used by the Certificate Manager to periodically check for revoked credentials.



## HARDWARE

The *PIVCheck Mobile Edition* biometric terminal combines a contact and contact-less smart card reader, a 500 DPI fingerprint sensor for instant matching to a biometric template, and a color digital touch-screen display housed in a compact handheld unit which weighs approximately two pounds. The mobile biometric terminal supports internal wireless communication for data and fingerprint transmission and also identity search and verification against a back-end system.

Specifications for the *PIVCheck Mobile Edition* biometric terminal:

Component	Description
Random Access Memory	Minimum of 32 MB RAM. Recommended 128 MB RAM or greater.
Persistent Memory	Minimum of 256 MB Internal CF
Monitor	<p>Color digital transfective touch screen with stylus.</p> <p>Supported dimensions:</p> <ul style="list-style-type: none"> <li>• 240 horizontal x 320 vertical (portrait)</li> <li>• 320 horizontal x 240 vertical (landscape)</li> <li>• 640 horizontal x 480 vertical (landscape)</li> </ul>

Fingerprint Sensor	Must be <i>FIPS 201 Approved Product List (APL)</i> certified. <a href="http://fips201ep.cio.gov/apl.php">http://fips201ep.cio.gov/apl.php</a>
Biometric Matching Algorithm	Must be <i>FIPS 201 Approved Product List (APL)</i> certified.
Smart Card Interface	Contact interface - Must be <i>FIPS 201 Approved Product List (APL)</i> certified. Contact-less interface - Must be <i>FIPS 201 Approved Product List (APL)</i> certified.
Wireless Protocol	WiFi 802.11b/g

## SOFTWARE

Component	Description
Operating System	Requires Microsoft® Windows® CE 5.0 and .NET Compact Framework 2.0 or greater.
Signature Algorithms	RSA with SHA-1 and PKCS v1.5 padding RSA with SHA-256 and PKCS v1.5 padding RSA with SHA-256 and PSS padding ECDSA with SHA-256, and ECDSA with SHA-384 <sup>a</sup>

a. non-FIPS 140-2 validated implementation

## FIPS 201 PRODUCT COMPLIANCE

This product, when used with *PIVCheck Plus Mobile Edition* and the *PIVCheck Certificate Manager* complies with the following *FIPS 201 Approved Product List* category:

Category	Certificate
Caching Status Proxy	#473
CHUID Authentication System	#485
Authentication Key Reader	#474

## FIPS 140-2 LEVEL 1 REQUIREMENT FOR PIVCHECK MOBILE EDITION

Several FIPS 201 approved product categories involve the use of cryptography. For those operations, PIVCheck software invokes functions supplied by Microsoft's Cryptographic API and Cryptographic Primitives Library. To meet GSA Approved Product List requirements, certain cryptographic functions can only be provided by cryptographic modules that have been certified at FIPS 140-2 Level 1 or better. For APL compliance, PIVCheck Mobile Edition must be deployed on one of the following operating systems:

### Microsoft Windows operating systems and FIPS 140-2 certifications

Operating System	Validated Version	Certificate
Windows CE 5.0 and 5.01	5.00.911762 and 5.01.01603	#560

This page is intentionally left blank.

# SOFTWARE INSTALLATION

## INSTALLATION OPTIONS

*PIVCheck Mobile* might not be pre-installed on the mobile biometric terminal. If a connection to the internet is available, then refer to “Downloading *PIVCheck Mobile* directly on the *Mobile Terminal*” on page 14. If an internet connection is not available, refer to “Installing *PIVCheck Mobile* File from a Flash Drive” on page 18.

## IMPORTANT NOTICE

Please note that the screen capture images shown in this manual are for illustrative purposes only. Screen icons may appear differently if you are using a device which uses a different screen orientation or a device which supports a higher screen resolution. The following screen capture images were acquired from a mobile biometric terminal which has a screen resolution of 240 x 320 and is using the portrait layout.

## POWERING UP

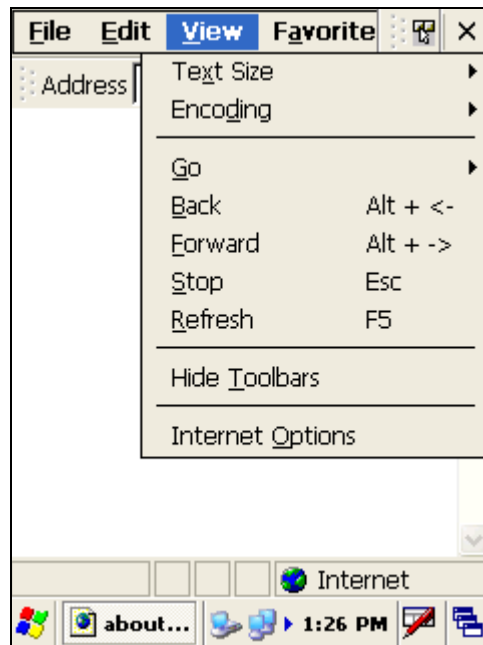


Due to the variances of hardware configurations, please refer to the user manual for detailed instructions on powering on your mobile biometric terminal.

## DOWNLOADING PIVCHECK MOBILE DIRECTLY ON THE MOBILE TERMINAL

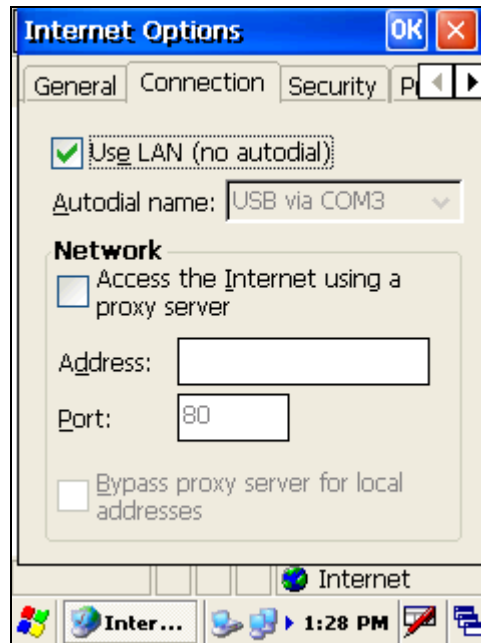
To use this method, you must have an Internet connection and a user name and password to access the Codebench general download site. If you have never used *Internet Explorer* from your mobile biometric terminal, it may need to be configured for Internet access.

Launch *Internet Explorer* and tap *View*.



Tap on *Internet Options* at the bottom.

When the dialog appears, tap on the *Connection* tab. Check the *Use LAN (no autodial)* option.



If you are required to use a proxy server then check the *Access the Internet using a proxy server* option and supply the addressing information for your site.

Tap the *OK* button to save the configuration options.

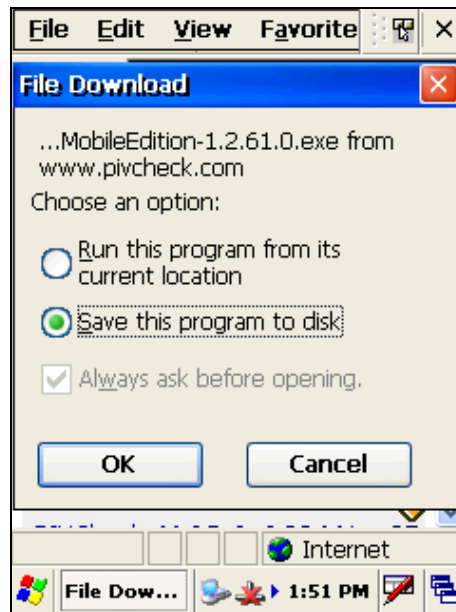
Now you are ready to download the *PIVCheck Mobile* software. Type the following URL into the browser's address bar:

<http://www.pivcheck.com/cabs/>

An authentication dialog will be displayed.

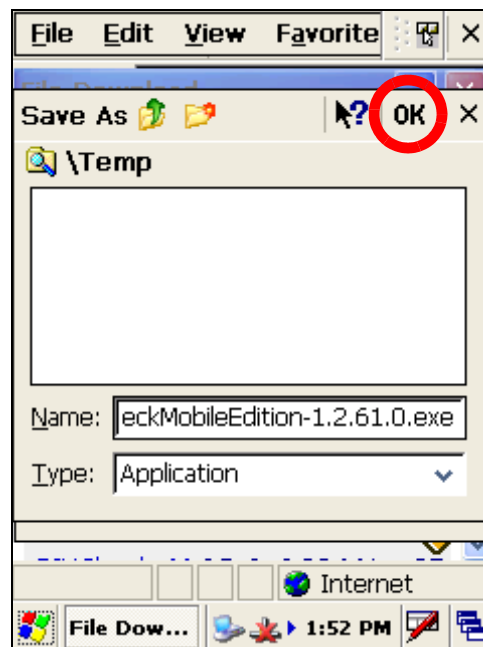


Enter your *User Name* and *Password* into the appropriate fields and tap the *OK* button. If the information is correct, then an *options* dialog will be displayed:



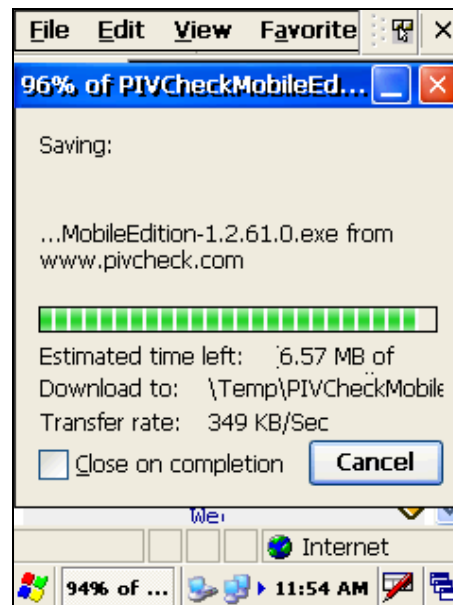
Choose the options as shown above and tap *OK*. The new *PIVCheck Mobile Edition* executable file will be downloaded to the `\Temp` folder on the terminal.

Tap the *OK* button to start the download.

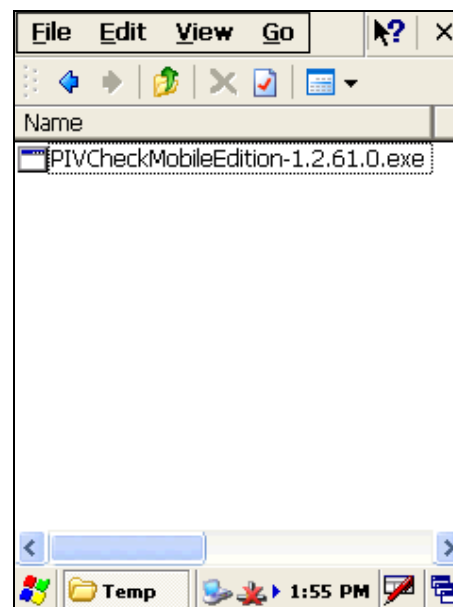




When the file download is complete, close Internet Explorer and tap on *My Device* and navigate to the `\Temp` folder.



Double-tap on the `PIVCheckMobileEdition 1.X.XX.X.exe` file and follow the installation wizard.



## INSTALLING PIVCHECK MOBILE FILE FROM A FLASH DRIVE

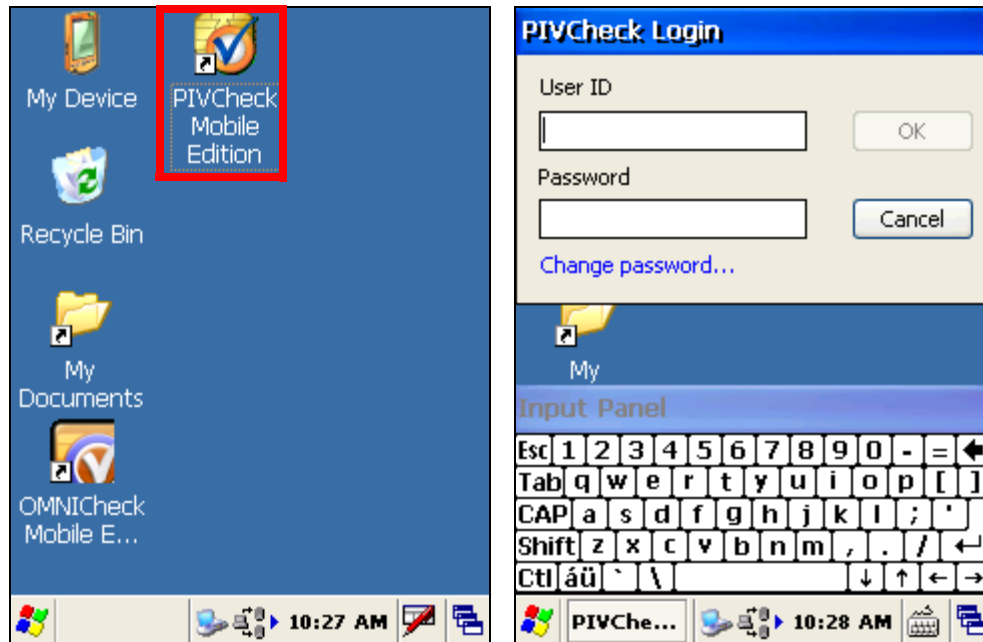
- Copy the *PIVCheck Mobile Edition* executable file onto the flash drive.
- Power up the mobile biometric terminal.
- Insert the flash drive into one of the standard USB ports located on the mobile biometric terminal.
- Double-tap the *My Device* Icon. The flash drive will appear as a *Hard Drive* in this directory.
- Double-tap on the *Hard Drive* directory to reveal the *PIVCheck Mobile Edition* executable file. Copy the executable file from the *My Device > Hard Disk* directory to the *My Device > Temp* directory.
- Double-tap the executable file and follow the installation wizard.

This completes the installation.

# CONFIGURING THE SYSTEM

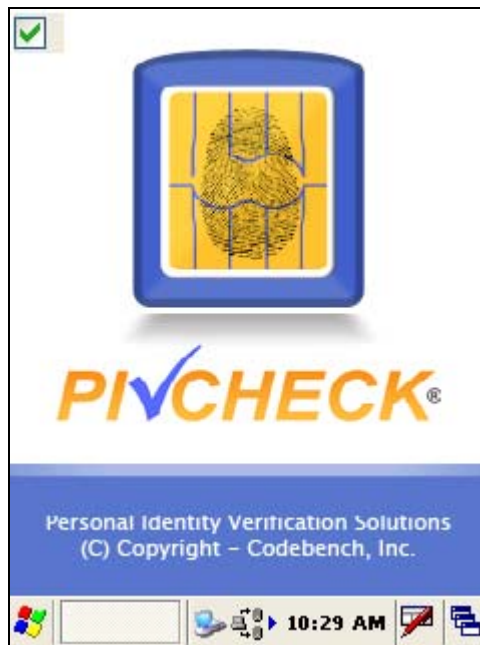
## LICENSING THE SOFTWARE

- 1 Once the Windows CE operating system boots, use your stylus to double-tap the shortcut to *PIVCheck Mobile Edition* icon.
- 2 Enter the default operator *User ID* (*admin*) and *Password* (*password*) using the input panel.



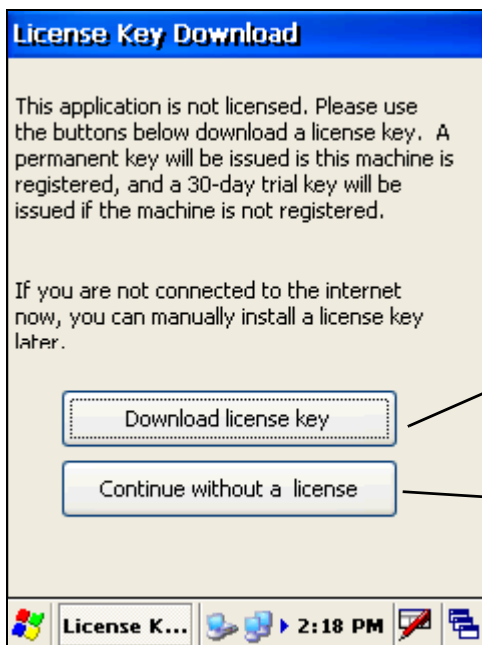
Your system integrator may have changed the default administrative *User ID* and *Password* from the Codebench factory defaults located above. Please consult your system integrator's documentation.

- 3 Press the *OK* button to accept the password and launch the *PIVCheck Mobile Edition* splash screen.



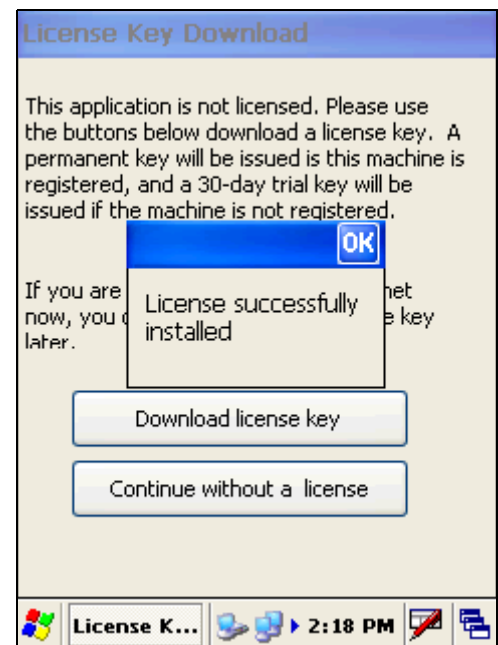
You can disable the splash screen by un-checking the checkbox in the upper left-hand corner.

- 4 If your software has not yet been licensed, the splash screen will be replaced with the *License Key Download* dialog.



An active internet connection is required when **Download license key** is tapped.

Press here to continue with a trial license or to enter your license manually.



## TRIAL LICENSE

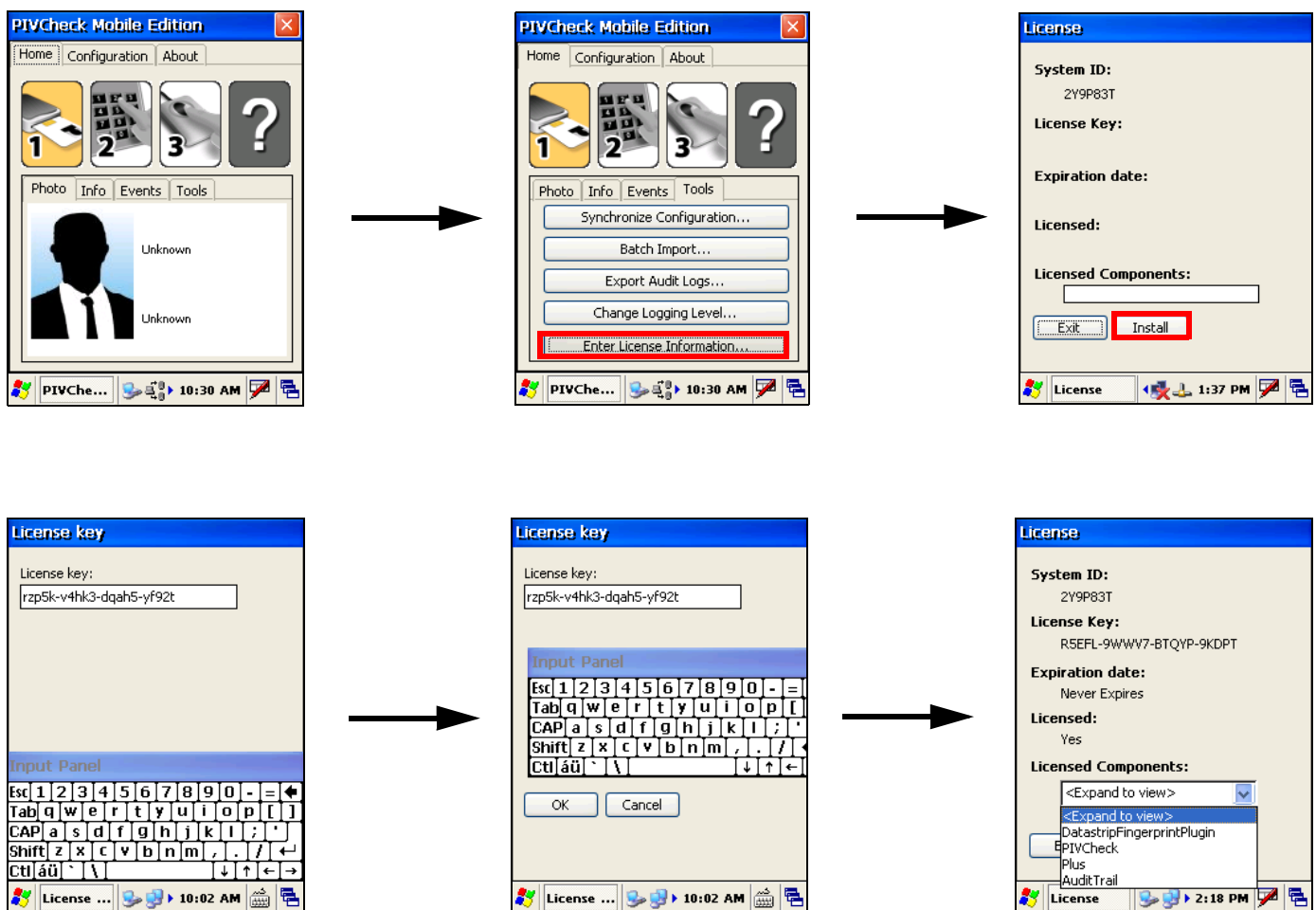
If you wish to evaluate the software for 30 days, press the *Download license key* button. The trial license consists of a fully functional *PIVCheck Mobile Edition*. If you have purchased and registered the product then the online licensing service will reissue your full license, and the *Licensed successfully installed* pop-up will be displayed.



*PIVCheck Plus Mobile Edition* is not available in a trial version. To enable additional features such as Plus or Audit, please contact the Codebench sales team who can enable those features ahead of time for the duration of the trial period.

## ENTER YOUR LICENSE MANUALLY

If you do not have an internet connection or you need to license your software manually, press *Continue without a license*. The main application will load and display the *Home* screen. The following steps show how to add your license key manually.



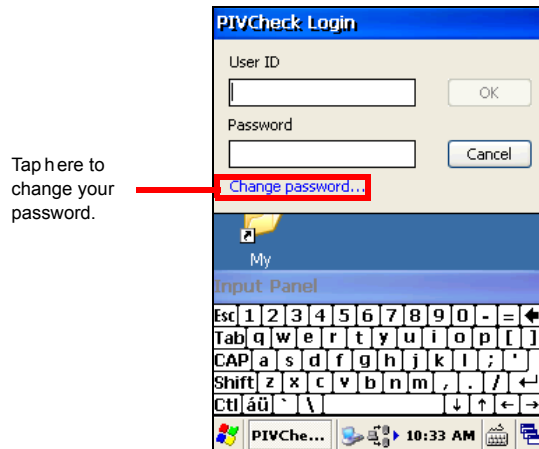
If *PIVCheck Mobile Edition* software has been pre-installed by the terminal manufacturer, then the license key you received with your mobile biometric terminal is synched with the device's unique *system ID*.

Enter the letters, numbers and dashes that make up your license key using the *input* panel. If you mistype a character, use the *delete* key in the upper right-hand corner of the *input* panel to erase your input, then re-enter the correct character.

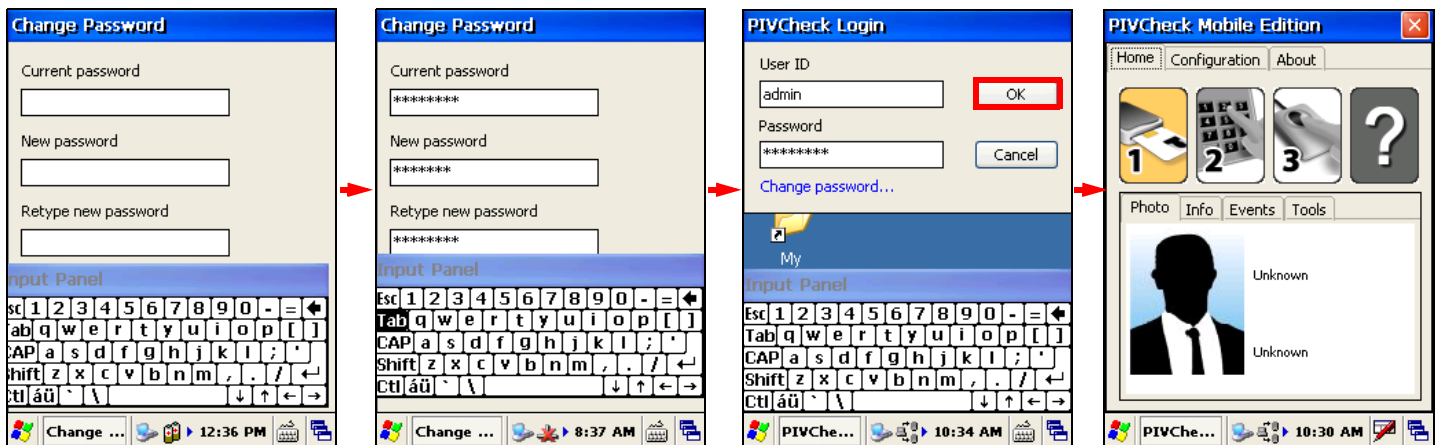
The license key field is now populated, indicating you have successfully licensed *PIVCheck Mobile Edition*. Press the *Exit* button to return to the *Application Configuration* dialog.

## CHANGING THE ADMIN PASSWORD

Out of the box the default username is *admin*, and the default password is *password*. It is strongly recommended that you change the administrative password immediately upon receiving a new mobile biometric terminal. To change the password, re-launch *PIVCheck Mobile Edition*. After the splash screen displays, you will see the *PIVCheck Mobile Edition Login* dialog.



For each field, use your stylus to set the cursor position, and then use the input panel to enter your current password and new password. Next, tap the *Tab* key which dismisses the input panel and reveals the *OK* and *Cancel* buttons. Press the *OK* button to login with your new password and display the *Home* tab.

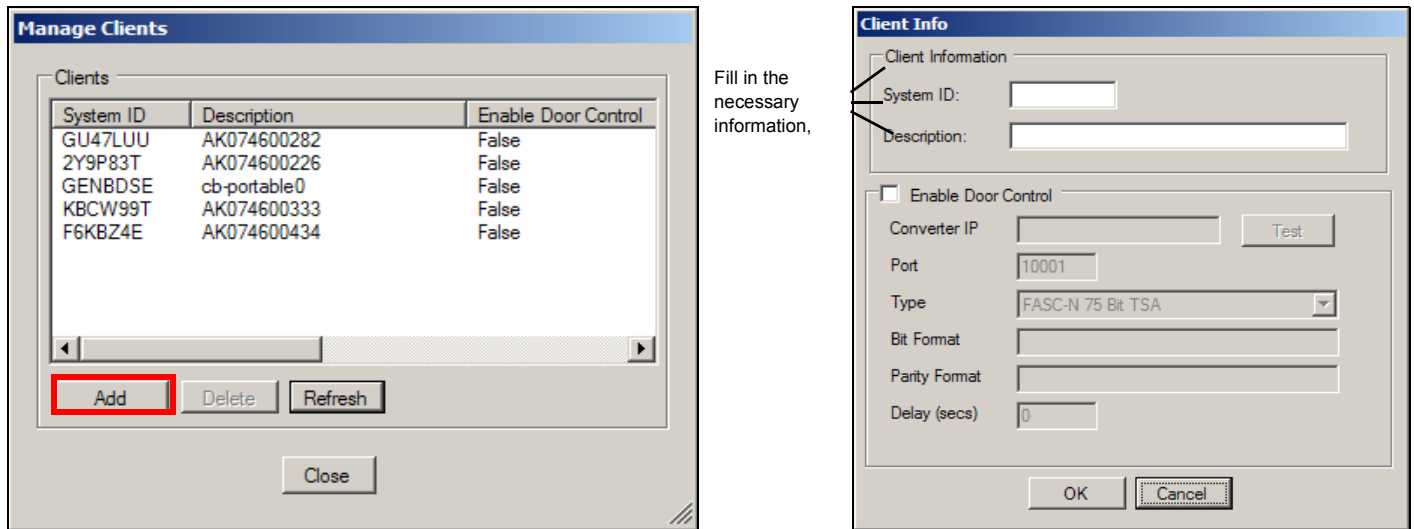


## CONFIGURING THE PACS PLUG-IN ON YOUR PC (PLUS ONLY)

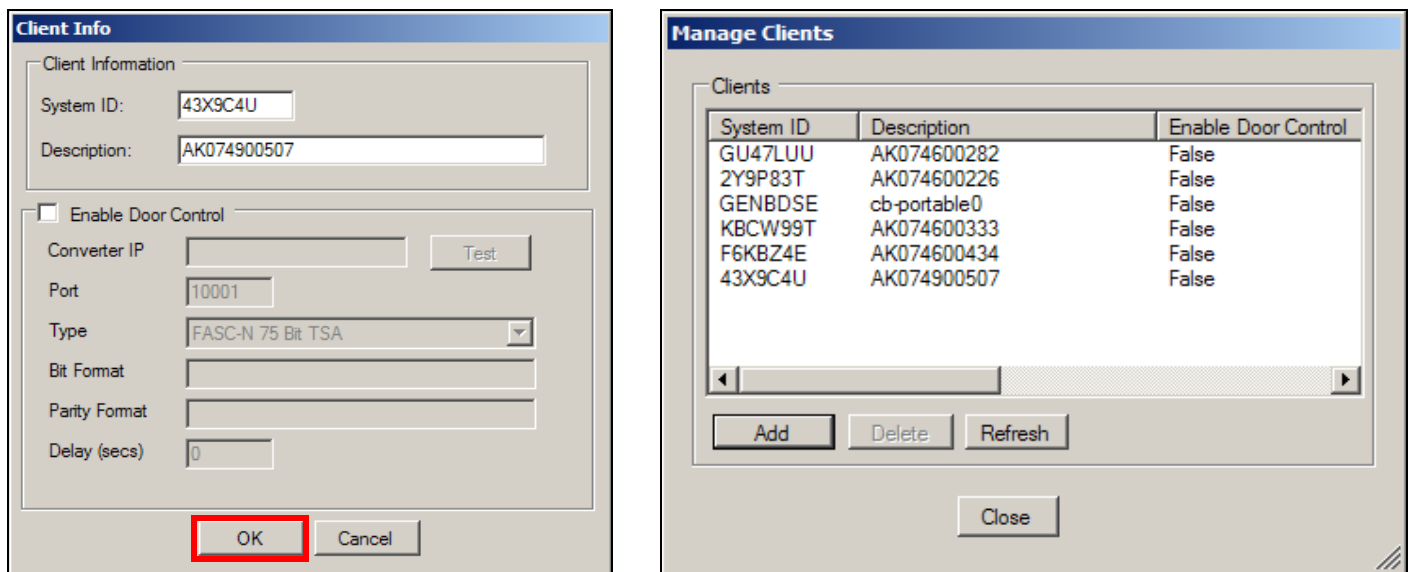
*PACS Service* is a generic term for the vendor-specific *PACS plug-in* that brokers communication between your mobile biometric terminal and the *PACS*.

### AUTHORIZING CLIENT CONNECTIONS

To authorize a client, open the *PACS Service* plug-in on the server click *Tools > Manage Clients*. A list of authorized client *System IDs* will be displayed. If the client you are configuring is not displayed, click the *Add* button and a dialog will be displayed:



The client's *System ID* will be added to the list. The client will now be able to connect to the *PACS Service*.



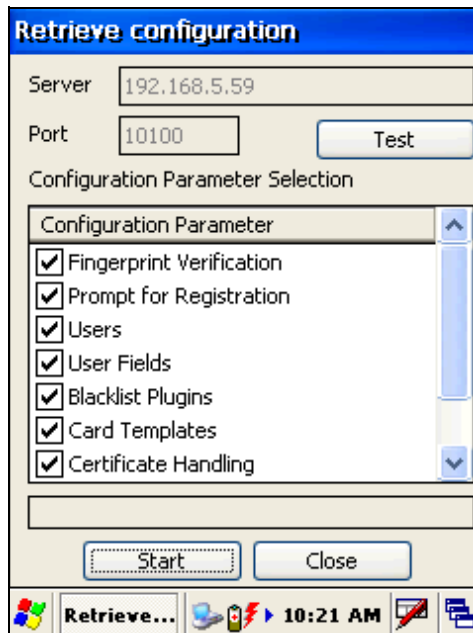


## SYNCHRONIZE CONFIGURATION (PLUS ONLY)

The fastest way to set up the mobile biometric terminal is to synchronize the terminal's local configuration with the profile stored by the PACS Service. Tap the *Home* Tab > *Tools* tab, then tap the *Synchronize Configuration...* button. Verify that the host name and ports are correct.

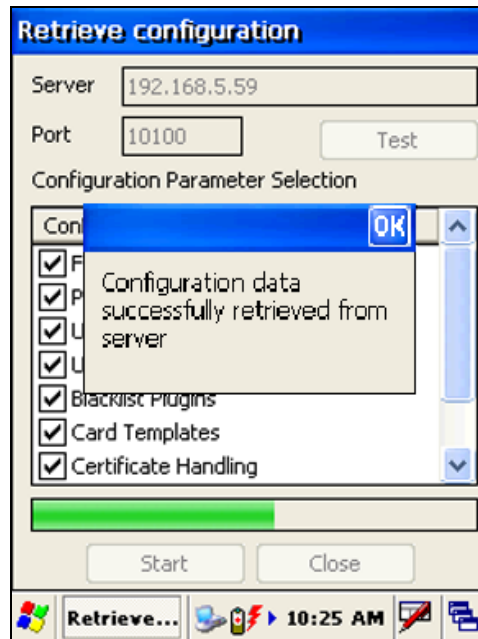


You can test your connection first, if desired.



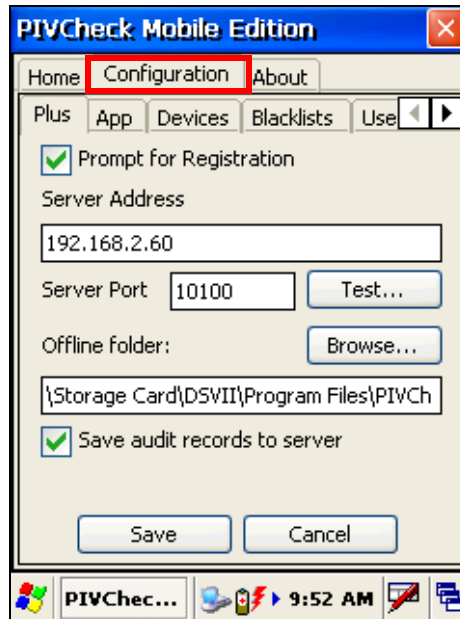
Select which settings you wish to download and tap the *Start* button to commence downloading the configuration profile from the PACS service.

When the configuration has been fully downloaded, the following message will be displayed:



## MANUALLY CONFIGURING THE PIVCHECK MOBILE DEVICE

To configure your mobile biometric terminal, tap the *Configuration* tab. The five sub-tabs which appear are labeled *Plus*, *App*, *Blacklists*, *Users* and *Door Control*. We will address each configuration area in turn.

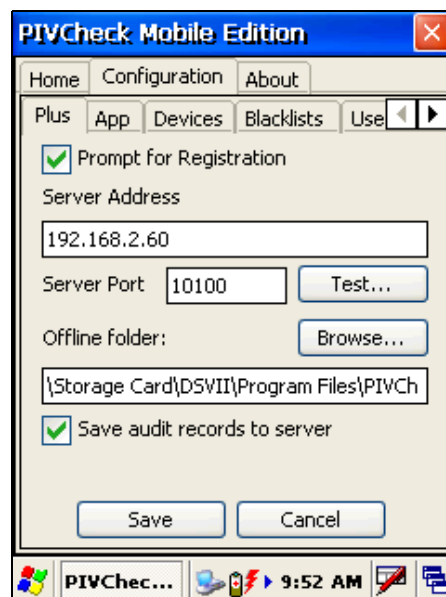


### PLUS TAB (PLUS ONLY)



This section assumes you have successfully configured your mobile biometric terminal to communicate over a LAN, WiFi, or GSM network. To configure your mobile biometric terminal, refer to “Authorizing Client Connections” on page 23.

Select the *Plus* tab to view the PACS service configuration dialog.

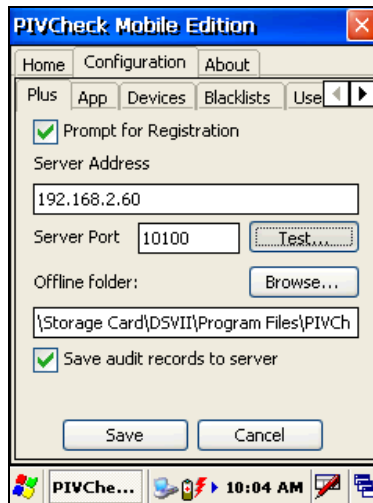


## REGISTRATION HANDLING

If Prompt for Registration is checked, then *PIVCheck Plus Mobile Edition* will always prompt the user to register the card information into the PACS, save the information locally, or cancel. If not checked, *PIVCheck Plus Mobile Edition* will attempt to register the card information automatically.

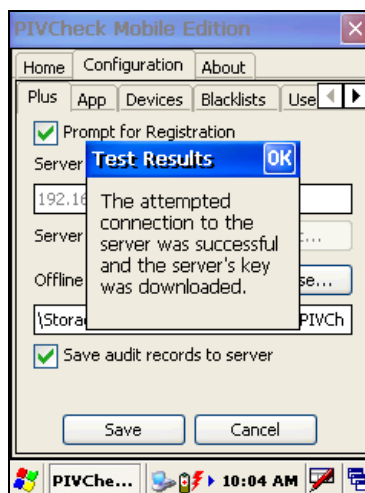
## SERVER ADDRESS

The server address is the IP address of your PACS Service. The PACS server interprets data sent from the terminals, converting it to a format understood by the PACS. The first time the application is run, the Server IP is normally set to localhost. Enter the IP address or hostname of your PACS Service using the Input Panel.



## SERVER PORT

Unless otherwise instructed, do not change the values for the *Server port* field. Press the *Test...* button to connect to your PACS Service. If the connection was successful, you will see the following message. The server looks up the client's System ID and, if found, sends back the encryption key that the client should use to encrypt offline transactions. If the connection was successful, you will see the following message.



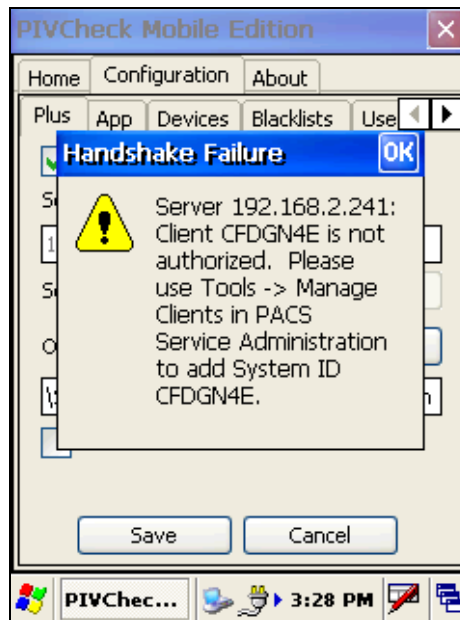
The server looks up the client's *System ID* and, if found, sends back the encryption key that the client should use to encrypt offline transactions.

## PACS CONNECTION FAILURES

This section lists some of the most common conditions that result in a failure when the *Test* button is tapped.

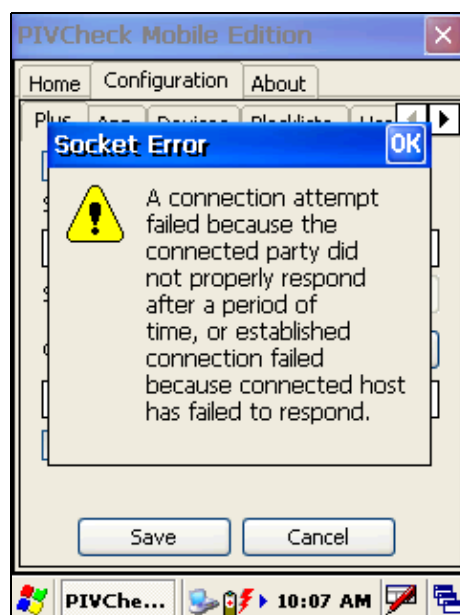
### CLIENT NOT AUTHORIZED

If the client has not been added to the list of authorized clients, the following will be displayed. On the PACS Service Administration GUI, use the *Tools > Manage clients* option to add the client to the server database. Once completed, tap the *Test* button again.



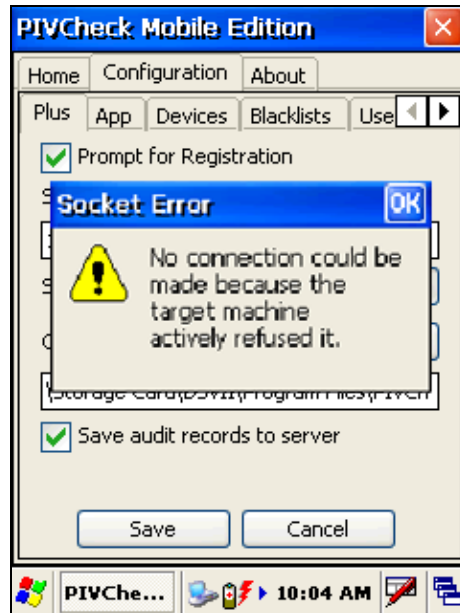
### INCORRECT SERVER IP ADDRESS OR NETWORK ROUTING PROBLEM

You will see the following error dialog if your attempted connection was unsuccessful because the server IP or name was incorrect or the request could not be routed to the server.



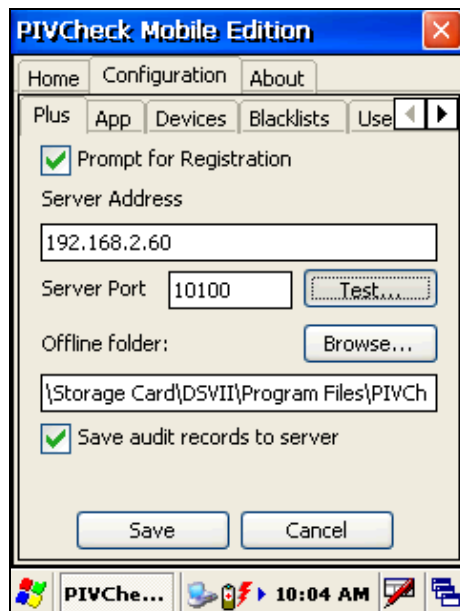
## SERVER EXISTS BUT PACS SERVICE IS NOT RUNNING

Please refer to the PACS Plug-in Administration Guide for your PACS for instructions on how to setup your PACS Service.

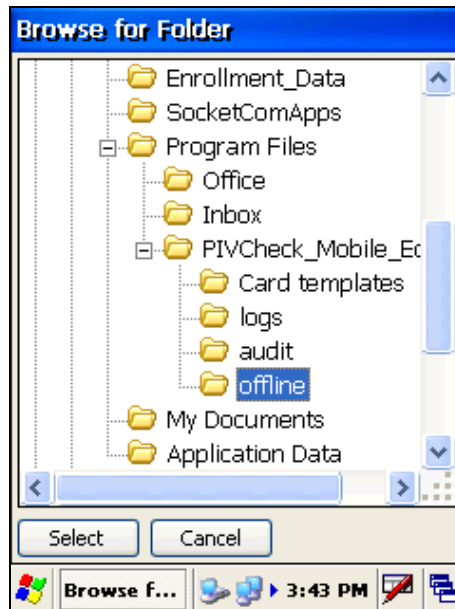


## OFFLINE FILE FOLDER

A default offline file location of `<Application Folder>\offline\` is defined when you install *PIVCheck Mobile Edition*. If you wish to change the name or location of this folder, press the *Browse* button to view the *Folder Selection* dialog.

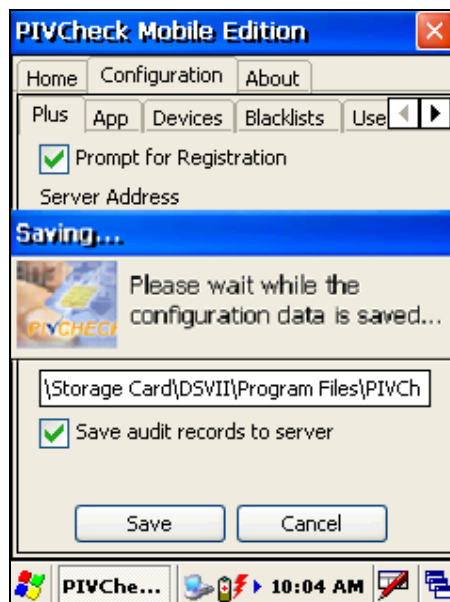


A folder browser will be displayed. The initial location is set to the currently selected folder which should be sufficient for most applications.



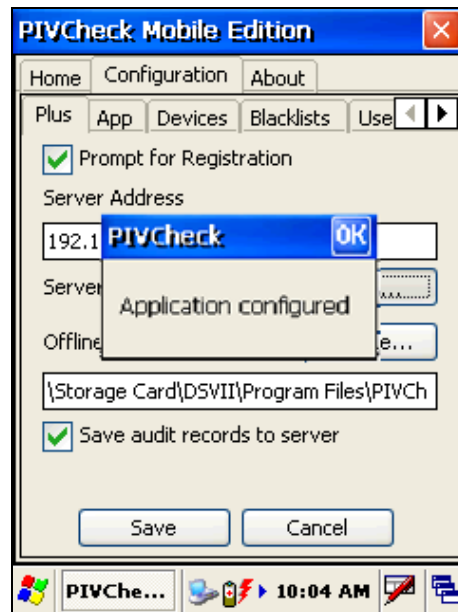
Navigate to a different portion of the file tree and select the new device and folder if you wish to relocate the offline file. Tap *Select* to accept the change.

Press the *Save* button within the *Plus* tab to store your server URL and display the following popup dialog.





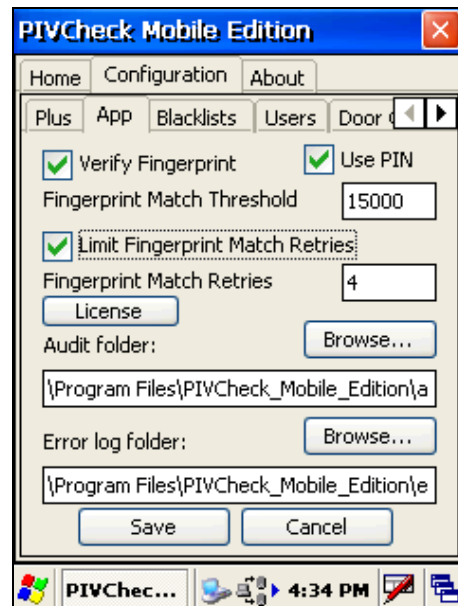
When the configuration has been encrypted and stored on the device the following message is displayed:



Press the *OK* button to return to the *Home* tab.

## APPLICATION TAB


*PIVCheck Mobile Edition* contains several configurations located under the *App* tab. These configurations include *Fingerprint options*, *PIN options*, *Audit log folder location*, and *Error log folder location*.



## FINGERPRINT OPTIONS

### VERIFY FINGERPRINT

If the *Verify Fingerprint* box is checked the cardholder will be prompted to present an index finger for on-card matching. If this box remains unchecked, the cardholder will not be prompted to present his or her finger for a fingerprint scan, the fingerprint data will not be read from the card and the fingerprint data will not be stored in the credential database.


 Verification without biometric matching is not recommended.

### FINGERPRINT MATCH THRESHOLD

This parameter causes *PIVCheck Mobile Edition* to determine the minimum score that is output by the biometric template matcher in order to reduce the incidence of false rejections as well as false matches. This parameter is specific to the matcher installed on the mobile biometric terminal. The first two columns in the table below show the different combinations of mobile biometric terminals using the biometric matcher purchased and installed. The third column shows the lowest recommended threshold to set for your device/matcher combination.

Mobile Biometric Terminal	Biometric Template Matcher	Lowest Recommended Threshold
DAP CE3240BWE	Innovatrics	12300
Datastrip's DSV3	Identix	10
Datastrip's DSV2+ <sup>TURBO</sup>	Identix	10
Datastrip's DSV2+ <sup>TURBO</sup>	NEC	1400
Cross Match Be.U Mobile	Innovatrics	12300
MaxID IDLMAX	Innovatrics	12300

Each template matcher uses its own scale for scoring the degree that two templates match each other.

 The lower the threshold as compared to the recommended threshold, the greater the risk of false matches. The higher the threshold, the greater risk of false rejections. It is suggested to test out your device within a controlled group to find a satisfactory median threshold and to calibrate your unit regularly.


### LIMIT FINGERPRINT MATCH RETRIES

Checking this option will cause *PIVCheck Mobile Edition* to reject any cardholder after a user-defined number of biometric matching attempts.

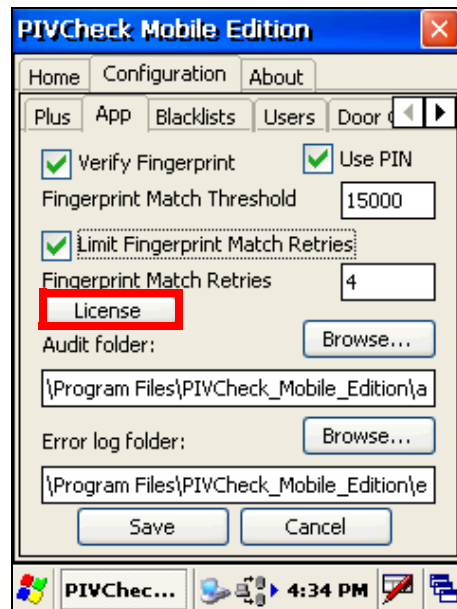
### FINGERPRINT MATCH RETRIES

Use the virtual keypad to set the number of retries to the desired number.

### LICENSE (FINGERPRINT TEMPLATE MATCHER)

 Applies to mobile biometric terminals for which the fingerprint matcher license is not preinstalled.

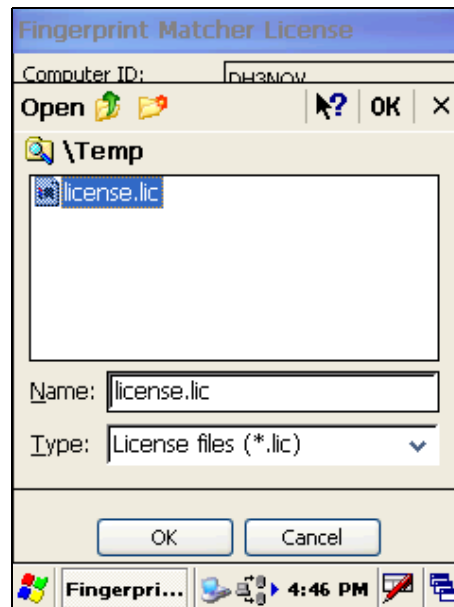
If *PIVCheck Plus Mobile Edition* is being used, and a fingerprint matcher license has been purchased, then press the *License* button.



Press the *Browse* button, then navigate to the location of the license file which was transferred to your mobile biometric terminal from your PC.

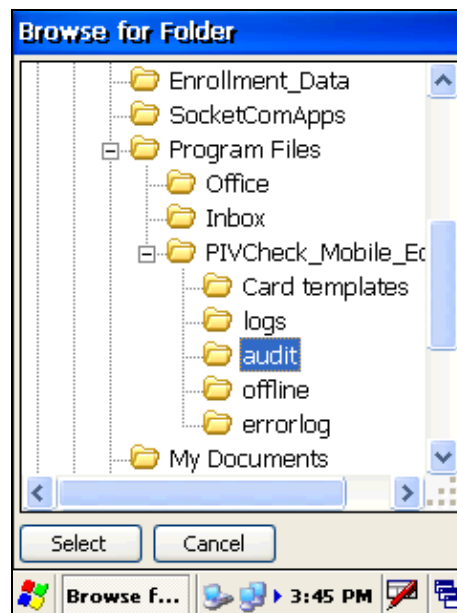


Select the fingerprint matcher license file, then press **OK**. Your fingerprint matcher is now licensed.



## AUDIT LOG FOLDER

The location of the *audit log* is configurable. A default offline file location of `<Application_Folder>\audit\Activity.paf` is defined when you install *PIVCheck Mobile Edition*. If you wish to change the name or location of this folder, press the *Browse* button to view the folder selection dialog.



Navigate to a different portion of the file tree and select the new device and folder. Tap *Select* to accept the change.



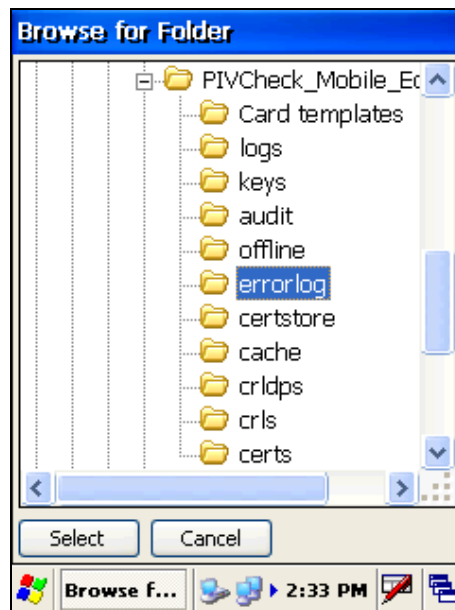
The file name will always be named `Activity.paf`.

## ERROR LOG FOLDER

The error log contains information about errors that the *PIVCheck Mobile Edition* application was unable to handle cleanly. These are generally unexpected conditions such as a missing driver, or certain network errors, or issues with smart cards. Each line of information corresponds to a single trouble ticket and consists of the following columns:

- Operator's User Name
- Time
- Unit ID
- Error Description
- Exception Message
- Contact E-mail
- Contact Phone Number

The location of the error log is configurable. A default offline file location of `<Application Folder> \errorlog\Errors.txt` is defined when you install *PIVCheck Mobile Edition*. If you wish to change the name or location of this folder, press the *Browse* button to view the folder selection dialog.



Navigate to a different portion of the file tree and select the new device and folder if you wish to relocate the error log file. Tap *Select* to accept the change.

## CONFIGURABLE CONTACT INFORMATION

The contact E-mail and contact phone number fields are configurable by editing or copying the following file, `contactinfo.txt` into the *PIVCheck Mobile Edition* folder. The format of this file is:

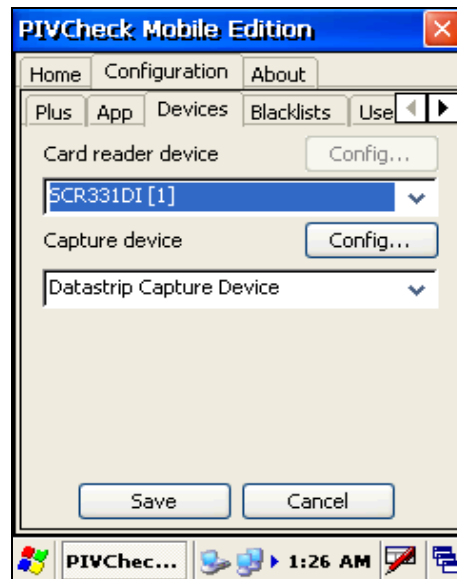
```
helpdesk@somewhere.com, (703) 555-1212
```

## AUTOMATIC ROLLOVER

The current day's trouble ticket file is named `Errors.txt`. However, as of Release 1.2.18.0, this file is created each day after renaming the previous days' file to `Errors. <yyyymmdd>.txt` where `yyyymmdd` are the year, month, and day corresponding to the file's entries. The application stores up to ten (10) days of files in this manner. Files older than 10 days are removed from the folder.

## DEVICES TAB

If PIVCheck detects that there are multiple smart card readers or fingerprint capture devices, the *Devices* tab will be displayed.

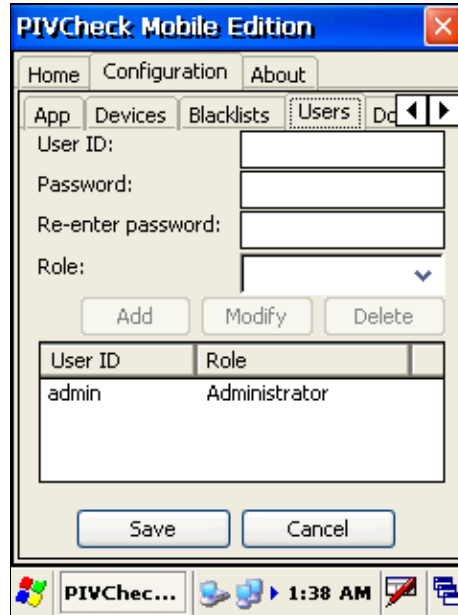


## BLACKLIST PLUG-INS

For more information refer to the *Codebench Blacklist\_Plug-in\_User\_Guide.pdf*. This manual is stored in the *PIVCheck Mobile Edition* program files directory.

## USERS

For security reasons, it is not recommended to perform identity verification or to import data as an administrative user. The *Users* tab allows you to set up user accounts to enable individual access to the device. Each user can have his or her login account.



### USER ID

Create a unique *User ID* for each operator and administrator who will be using this device. The *user ID* must be at least 2 characters long.

### PASSWORD

Create a secure password for each operator and administrator who will be using this device. The password must be at least 8 characters long.

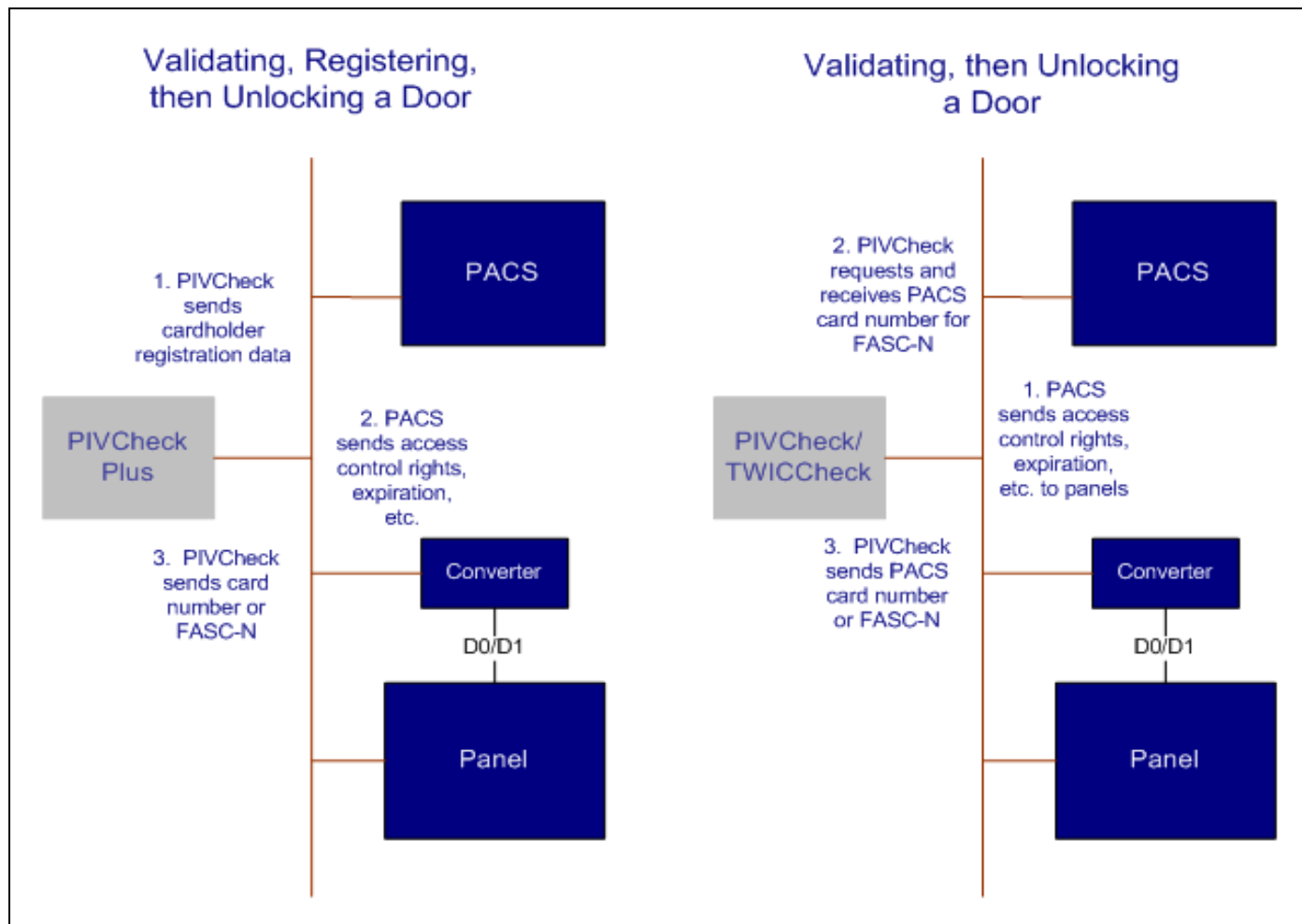
### ROLE

Select the role this user will play. The two options are *operator* and *administrator*. An *administrator* has complete control over all the configuration settings on the mobile device. An *operator* has limited control over the mobile device and its settings. Below is a list of the *operator* roles:

- Scan and validate PIV and TWIC cards.
- View cardholder photo.
- View cardholder information.
- View cardholder events.
- View the *About* tab.
- Batch import of audit information.
- Export Audit logs.
- Change logging level.
- View software license information.

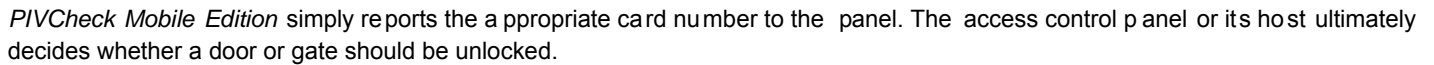
## DOOR CONTROL (OPTIONAL)

The *Door Control* option provides an additional way to validate a *PIV* card. If the card is completely validated and the cardholder's identity has been confirmed, a Wiegand protocol message is sent over the network to a Wiegand data converter. The converter transforms network messages into Wiegand output, producing the same wire protocol expected from a typical PACS reader. Two typical use-case scenarios are shown below.





The door control configuration form is shown below.



By checking this option, *PIVCheck Mobile Edition* will automatically send a Wiegand card number to the specified PACS panel. If the option is unchecked, no attempt is made.

This is the IP address of the Wiegand converter connected to the PACS panel. Network-based panels usually have their own IP address.

Click this button to send a test message to the Wiegand converter. The test message does not include a card number.

This is the TCP port on which the converter is configured to listen for messages.

Two categories of card messages are supported:

- Rev. 05262010

## FASC-NS AND DERIVATIVES

FASC-Ns are normally sent to panels that support newer PACS readers such as HID iClass®. The ability to send FASC-Ns to PACS panels is supported on both *PIVCheck Mobile Edition* and *PIVCheck Plus Mobile Edition*. The following FASC-N Wiegand formats are available:

- 200-bit
- 75-bit GSA
- 75-bit SÄ
- 64-bit
- 48-bit

## PACS CARD NUMBERS

A PACS card number can be sent to the access panel after a person has been validated. This allows a site to use FIPS 201 credentials to unlock doors on a legacy PACS system without upgrading access panel firmware in order to support processing FASC-Ns. The ability to support PACS card numbers is limited to *PIVCheck Plus Mobile Edition*. The PIV card must be pre-registered with *PIVCheck* so that the logical link between FASC-N and PACS card has been established.

The following PACS card Wiegand formats are available:

- 26-bit
- 34-bit
- 36-bit
- HID Corporate 1000
- CASI 3701
- CASI 3702

Additional custom formats can be added as needed.

Although it is best to manage door control from the PACS Server and use the *Synchronize Configuration* tool to download the correct formats for the correct PACS panels, door control functionality can also be customized locally on the mobile client.

## BIT FORMAT

For PACS card number formats, the bit format string shows how card number will be split into site codes and card numbers.

## PARITY FORMAT

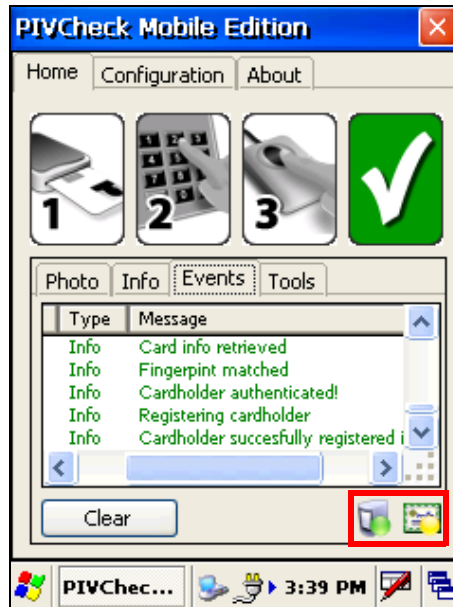
The parity format shows which bits will be used in the calculation of odd and even parity.

## DELAY

If you intend to use the door control to send Wiegand reads after *PIVCheck Plus* registers a new card or cardholder, you may need to impose a delay to allow the card information to propagate from the PACS to the panel. If you are not registering a card into the PACS and are simply using *PIVCheck* as a validation tool, set this to zero.

## COMMUNICATIONS STATUS INDICATORS

The lower right portion of the events tab contains indicators for the last communications for the PACS server (*PIVCheck Plus Mobile Edition* only) and the validation authorities.



The meaning of the indicators are as follows:

	Last communications attempt with PACS service was successful.
	Last communications attempt with validation authority successful.
	Communications attempt with PACS service has not been attempted.
	Communications attempt with validation authority has not been attempted.
	Last communications attempt with PACS service was unsuccessful.
	Last communications attempt with validation authority was unsuccessful.

## SAVING YOUR CONFIGURATION

Press the Save button to store your application choices. Press OK to return to the *Home* tab.

This page is intentionally left blank.

# IDENTITY VERIFICATION

The *PIVCheck Mobile Edition* application employs a three-factor authentication process to validate a cardholder - *something you have*, *something you know*, and *something you are*. The identity authentication process is described in detail within this chapter.

## SOMETHING YOU HAVE (PIV CREDENTIAL)

When *PIVCheck Mobile Edition* is ready to validate a *PIV* or *TWIC* card, the first icon in the three-factor authentication process, representing the integrated card reader, will appear in color.



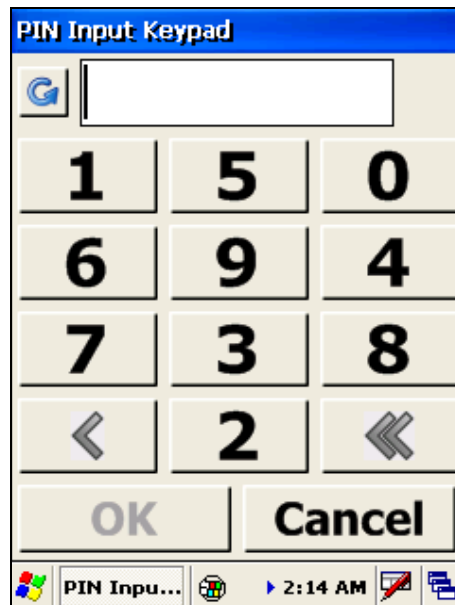
The "*Something You Have*" requirement is met by the fact that a valid *PIV* or *TWIC* card has been inserted into the mobile biometric terminal and the card has properly responded to a cryptographic challenge issued by the *PIVCheck* software. However, no personal information can be read from this card until "*Something You Know*", the cardholder's PIN, has been entered to unlock the card. The information needed to fully authenticate the cardholder requires data that is protected by the cardholder's PIN.

## SOMETHING YOU KNOW (KNOWLEDGE OF PIN)

Once *PIVCheck Mobile Edition* detects an identity card, a virtual PIN pad is displayed, prompting the cardholder to enter his or her PIN. Note that the numbers on the PIN pad are randomly arranged and is rotated to support the point of view of a cardholder.

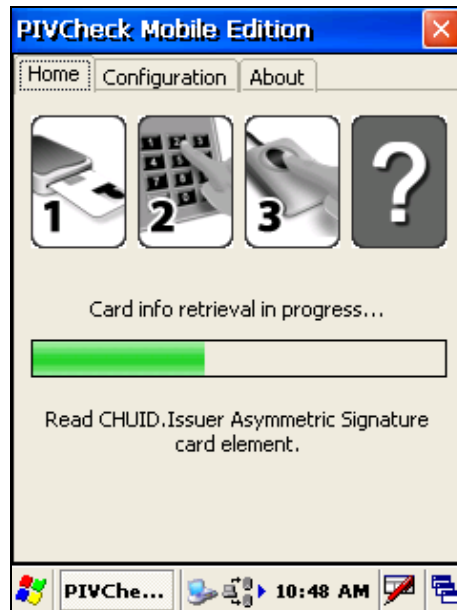


The PIN pad can be transposed to support the point of view of the operator by pressing the *circular blue arrow*.



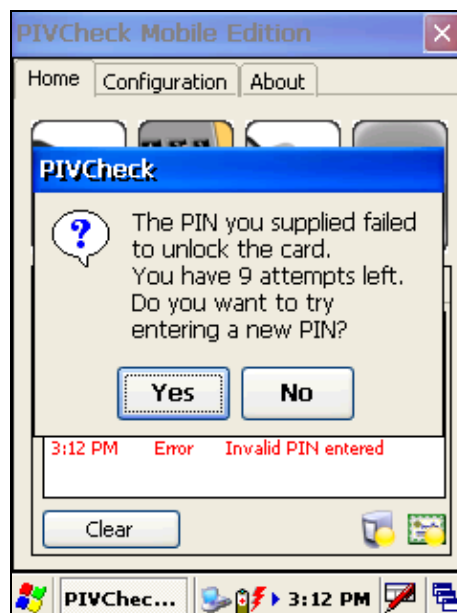
If a PIN is mistyped, individual characters can be erased using the left-pointing arrow (<). All characters in the input field can be erased using the erase button (<<).

Once the PIN is entered and matched with the PIN recorded on the card, *PIVCheck Mobile Edition* extracts the fingerprint templates and all X.509 certificates from the card.



## PIN FAILURE

If the PIN entered by the cardholder cannot be matched against the PIN stored on the card, a popup dialog informs the cardholder the PIN has failed, and will offer a re-try.

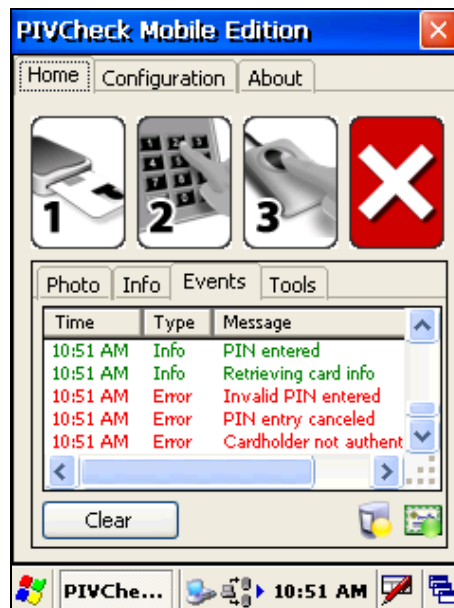


Select **Yes** to redisplay the virtual PIN pad and allow the cardholder to re-enter his or her PIN.



*PIVCheck Mobile Edition* will be unable to perform any further processing on a card for which the number of failed PIN attempts exceeds the maximum number of match attempts configured on the card. Once all the retries have been exhausted, the card's PIN can only be reset by the card issuer. The card issuer is the facility you acquired your card from.

If the *NO* button is selected, the *Events* tab confirms the cardholder is not authenticated.



Once the card is removed, the card reader icon re-appears in color, signaling the system is prepared to validate a new card.

## PIN MATCH

If the PIV PIN is valid all of the information is extracted from the smart card. This includes the following:

- CHUID
- Card Authentication Certificate
- Card Holder Facial Image and digital signature
- Card Holder Fingerprints and digital signature
- Key Management Certificate
- PIV Authentication Certificate
- Printed Information
- Security Object
- TWIC Privacy Key Buffer (if TWIC applet is present)



## SOMETHING YOU ARE (BIOMETRIC ATTRIBUTES)

If the PIN is valid, and the verify fingerprint checkbox was selected during application configuration, a popup dialog prompts the user to help the cardholder place his or her finger on the fingerprint platen. Once a fingertip is detected, *PIVCheck Mobile Edition* prompts the integrated fingerprint reader to capture a live fingerprint.



## FINGERPRINT MATCH

After a few seconds, the biometric produces a fingerprint template from the scanned image. This template is then matched against both fingerprint templates stored on the smart card. If the generated template matches either of the two stored on the card then a match is declared.

## SCORING

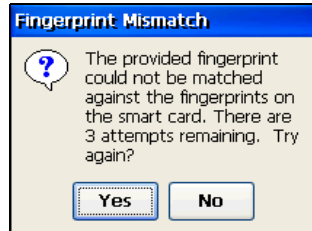
The decision as to whether a cardholder's fingerprint template matches is somewhat arbitrary since different manufacturers' matching algorithms produce scores which must be interpreted by the application. The minimum score produced by a matching algorithm in which a biometric match truly occurred is called the fingerprint match threshold. Virtually every template matching algorithm uses a different scoring system.

## FINGERPRINT MATCH THRESHOLD

The fingerprint match threshold can be adjusted on the *App* tab. For the NEC template matcher 1400 is an acceptable threshold. For the Identix template matcher 10 is an acceptable threshold. For important configuring information and to determine which template matcher is licensed, refer to "Fingerprint Options" on page 32.

## FINGERPRINT MATCH FAILURE

If the cardholder's fingerprint is not matched, a popup dialog informs the operator the scanned fingerprint did not match the fingerprint template stored on the card. Tap the **Yes** button to redisplay the *Present Fingerprint* dialog.

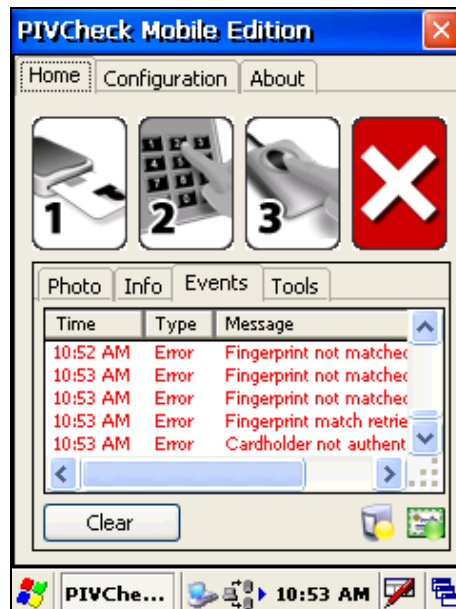


If you tap the **Yes** button, the cardholder can present their finger again. This can repeat for as many retries are available. If you tap the **No** button, both the *Events* tab and the *Not Authenticated* icon confirms the cardholder is not authenticated.

If the maximum number of retries has been reached, the following message will be displayed.



The events window will display the sequence of attempts.



## CERTIFICATE VALIDATION

If the captured fingerprint matches the fingerprint on the card, or the *Verify Fingerprint* option was left unchecked during system configuration, the card's certificates are verified using full PKI validation including checking the revocation status against an OCSP responder or repeater. For TWIC cards, the card's FASC-N is checked against the TSA hot list.

## THE CARD DATA WINDOW

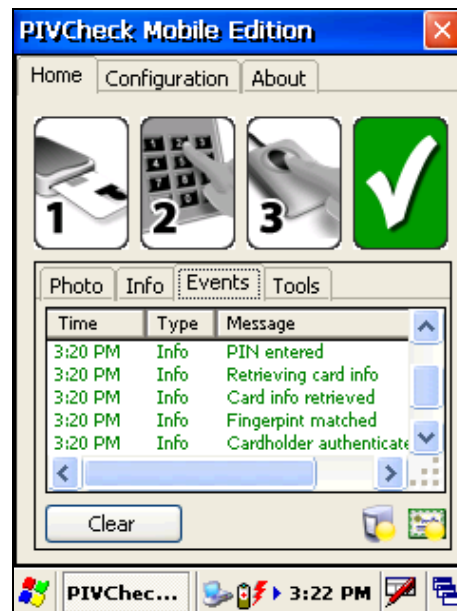
Once a cardholder's certificates have been validated, the *Card Data* window displays the cardholder's photograph, first, middle, and last name, FASC-N, GUID, Expiration Date, and other user-configurable data.

## THE APPLICATION EVENTS WINDOW

The *Application Events* window displays a list of system events associated with system configuration and the validation of a PIV card. Event fields include the time logged, the message type (Info or Error) and a brief description. The window includes a *Clear* button that can be used to clear the window of event messages.

## IDENTITY AUTHENTICATION

Once a card's certificates are verified, the fourth icon across the top of the display becomes a green check, indicating the cardholder has been successfully authenticated.

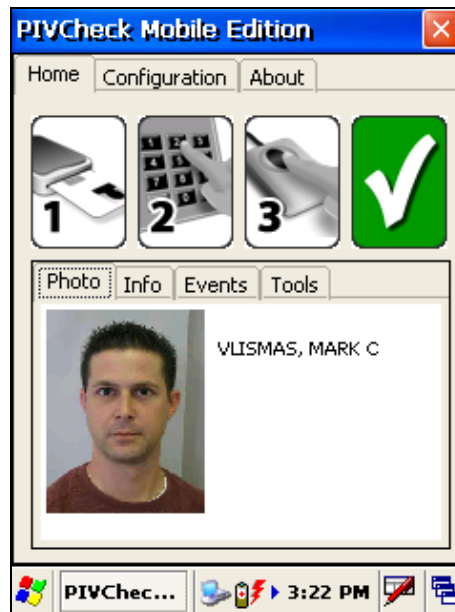


## DISPLAYING CARDHOLDER DATA

Three sub-tabs under the *Home* tab are available to support the *PIVCheck Mobile Edition* operator: *Photo*, *Info*, and *Events*.

## PHOTO TAB

Once a cardholder's certificates have been validated, the *Photo* tab displays the cardholder's photograph, first, middle, and last name.



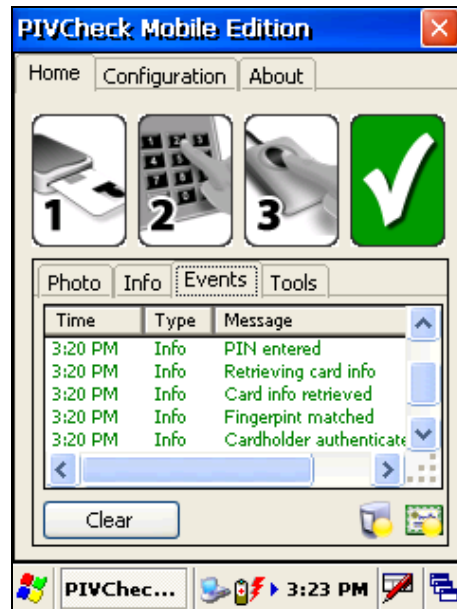
## INFO TAB

The *Info* tab displays the text information stored on a validated PIV card, including the first, middle, and last name, FASC-N, GUID, Expiration Date, and other user-configurable data.



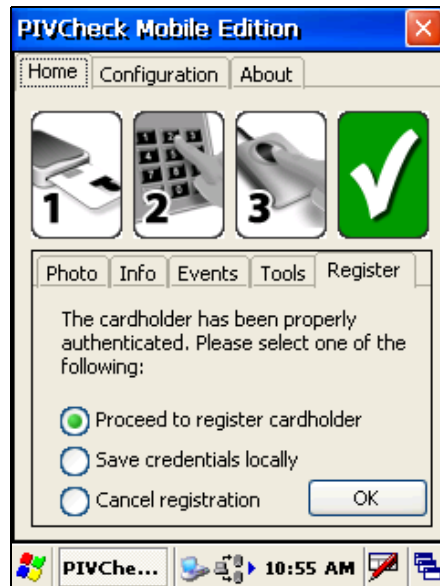
## EVENTS TAB

The *Events* tab displays a list of system events associated with system configuration and the validation of a PIV card. *Event* fields include the time logged, the message type (Info or Error) and a brief description. The window includes a *Clear* button that can be used to clear the window of event messages.



By default, *PIVCheck Mobile Edition* logs system messages to the logs sub-directory within the installation directory. It is sometimes useful to refer to this log when attempting to troubleshoot system errors. Refer to your PACS Plug-in Administration Guide for guidance on configuring the system messages captured in the logs directory.

## PACS REGISTRATION (PLUS ONLY)



With the *Plus* option installed, three registration options are available:

- The operator may attempt to register the cardholder with the PACS
- The operator may save the cardholder's credentials locally
- The operator may choose not to register the cardholder

## REGISTERING THE CARDHOLDER

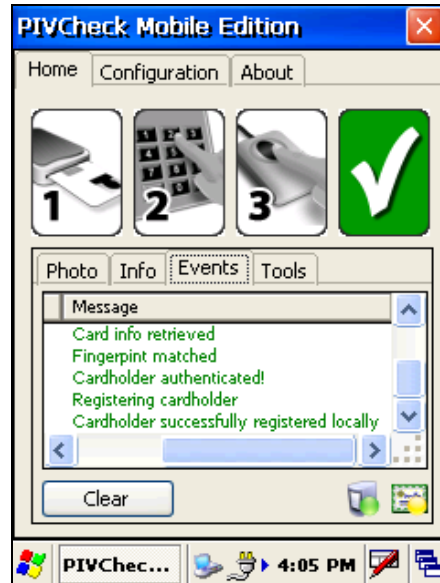
To register a card holder on the PACS, select the first checkbox on the *Register* tab and press the *Ok* button. If the cardholder is registered successfully, a confirmation message appears in the *Events* tab.



Once the card is removed, the *Photo* and *Info* tabs are cleared. The card reader icon re-appears in color, signaling the system is prepared to validate a new card.

## SAVING CREDENTIALS LOCALLY

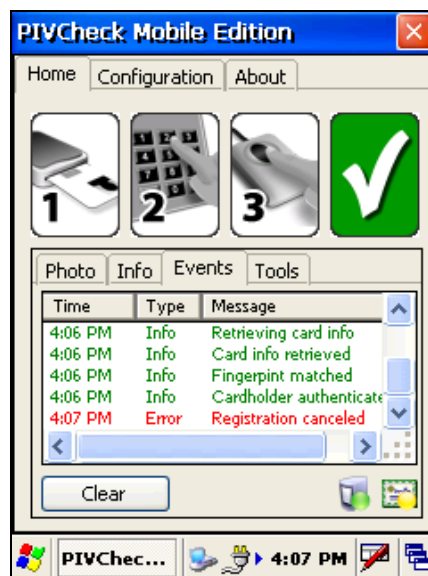
To save a cardholder's credentials locally, select the second checkbox on the *Register* tab and press the *Ok* button. A confirmation appears in the *Events* tab, indicating the cardholder information was successfully stored in a locally encrypted file.



Once the card is removed, the *Photo* and *Info* tabs are cleared. The card reader icon appears in color, signaling the system is prepared to validate a new card.

## CANCELING REGISTRATION

To cancel (skip) cardholder registration, select the third checkbox and press the *Ok* button. As a result, a red system message is displayed in the *Events* tab.



## USER FIELDS

*PIVCheck Plus Mobile Edition* allows administrators to create customized data entry fields known as *User fields*. Once a new *User field* is defined in your PACS data mapping template and downloaded using the *Tools* tab on the mobile biometric terminal, it appears as a new dialog after the *Ok* button is tapped on the *Register* tab.



Please refer to your PACS Plug-in manual for a detailed description on how to define *User fields*.

*User fields* represent a powerful technique for capturing additional cardholder data. One useful example is associating the PIV credentials of a new cardholder with the cardholder's existing PACS badge, as expressed in the following use case.

During PACS registration, a new cardholder is prompted for his or her PACS badge via a *User field*. Both the credentials and the PACS badge of the cardholder are recorded in the Certificate Manager database. During the process of credential re-validation, the Certificate Manager detects the cardholder's credentials have been revoked. As a result, the Certificate Manager retrieves the cardholder's PACS badge and notifies the PACS. This allows the PACS to deny the cardholder access to controlled areas within the facility.



The Certificate Manager can also be configured to notify the PACS when the credentials of an existing cardholder have been revoked. This does not require a *User field*, as the cardholder's PACS badge has already been captured in the cardholder's PACS personnel record.

A *User field* that supports the above use case appears below. Once this *User field* that maps to this dialog is added to the PACS Service data mapping template, and downloaded to the biometric terminal, the cardholder will be prompted for his or her PACS badge during the process of registration. Once the text field is filled out, and the *OK* button on the dialog is pressed, the cardholder's PACS badge will be uploaded to the Certificate Manager database along with the cardholder's credentials, or cached locally for batch processing at a later time.



Just as during normal registration, a confirmation message will appear in the Application events window, letting the operation know the operation was successful.



Once the card is removed, the *Photo* and *Info* tabs are cleared. The card reader icon appears in color, signaling the system is prepared to validate a new card.

This page is intentionally left blank.

# TOOLS

This chapter provides detailed information for the configuration of the following list of tools contained within the *PIVCheck Mobile Edition* application.

- Synchronize Configuration
- Batch Import
- Export Audit Logs
- Change Diagnostic Logging Level
- Licensing the Software

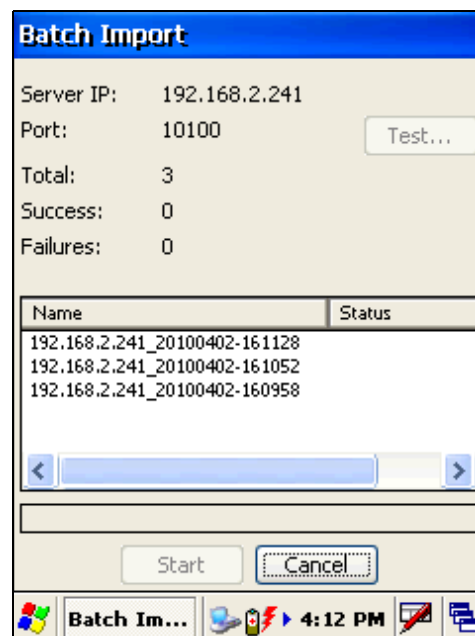
## SYNCHRONIZE CONFIGURATION (PLUS ONLY)

For more information refer to section “Synchronize Configuration (Plus Only)” on page 24..

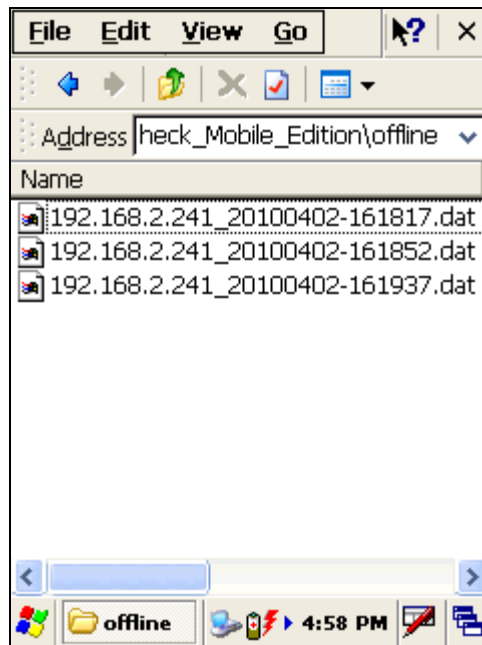
## BATCH IMPORT BUTTON

The Batch Import utility allows you to upload valid cards into the PACS server where they can be registered into the PACS itself. A network connection is required for this.

Press the *Batch Import* button to display the *Batch Import* dialog.

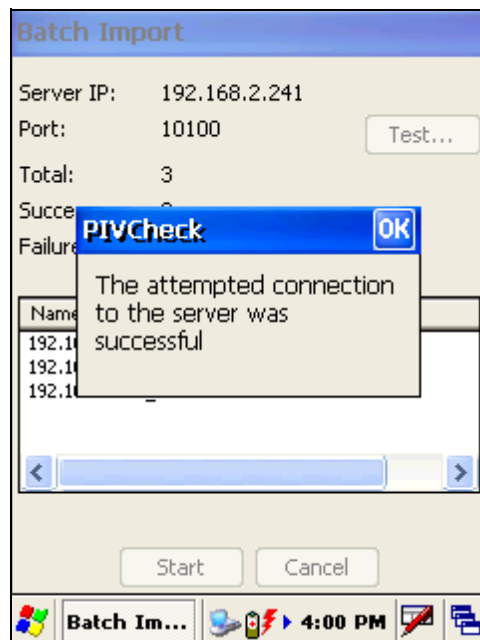


The *Batch Import* utility will automatically refer to the directory containing the <stored>.dat files.

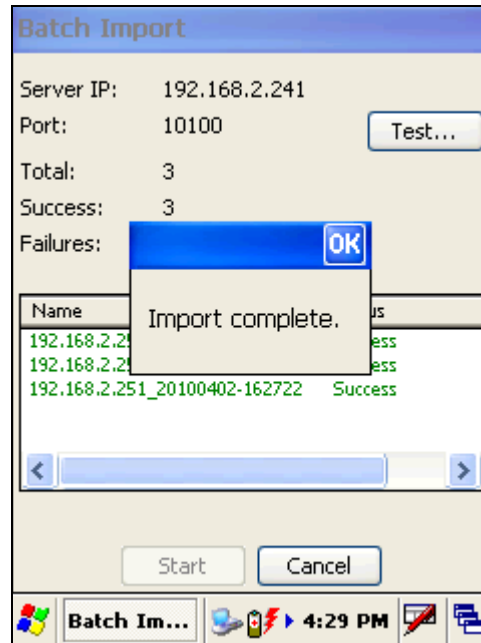


This directory was defined under the *Configuration* tab *Configuration* -> *Plus* -> *Offline folder*. For instructions to setup your offline folder location, see “Offline File Folder” on page 29.

Press the *Test* button to test the server connection to be sure you have connectivity.



After you have tested the PACS Service, press the *Start* button to submit the cached credentials. Note that PKI validation is repeated. This prevents *PIVCheck Plus Mobile Edition* from registering a card for a credential that was revoked while the credential was in temporary offline storage. When the upload is complete, the following message is displayed.

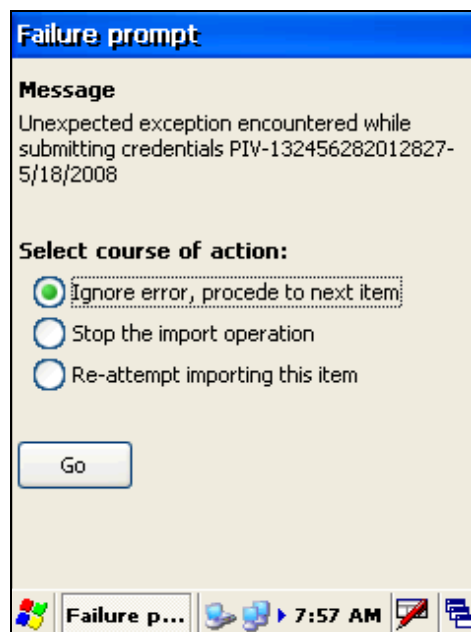


Press the *OK* button to clear the popup dialog, then the *Cancel* button to return to the *Tools* tab.

## BATCH IMPORT FAILURE

### INCOMPATIBLE DATA FORMATS

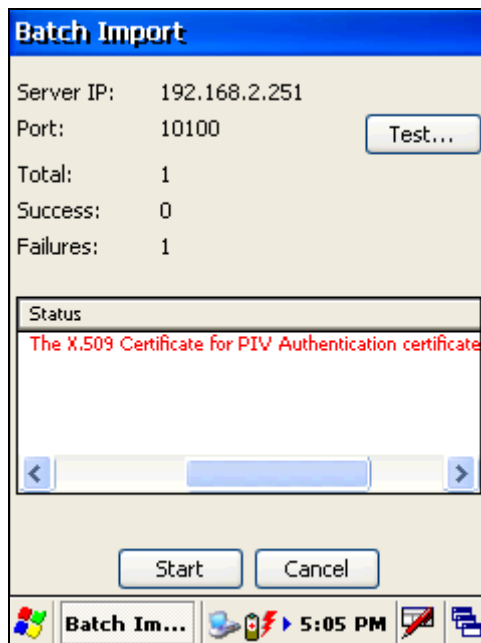
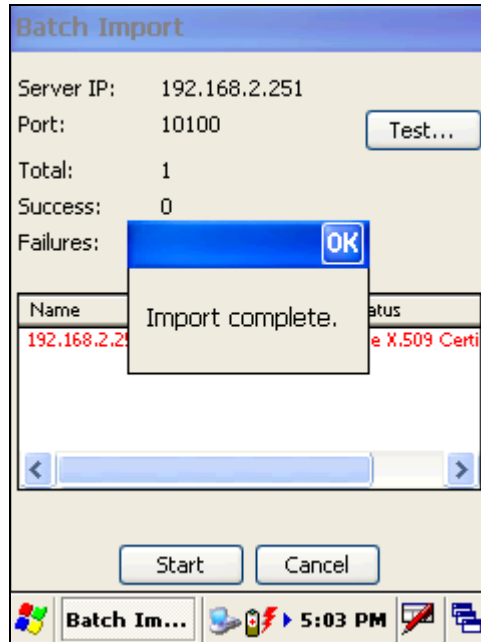
If the batch import utility cannot submit cached cardholder certificates for registration, the *Failure prompt* dialog will appear.



Problems with the batch import utility are often caused by an incompatibility between the data format of a PIV card and the data format of the target PACS personnel record. The purpose of your data mapping file is to synchronize these two sources of data.

## RE-VALIDATION OF CERTIFICATES

Batch import invokes the blacklist plug-ins configured at the server so that certificates that have been stored in the credentials are re-validated before importing the data record into the PACS.



## EXPORT AUDIT LOGS BUTTON

This feature allows the user to convert the encrypted audit log to comma separated values (CSV) format.



If operating in online mode then audit records are sent to the server in real time.

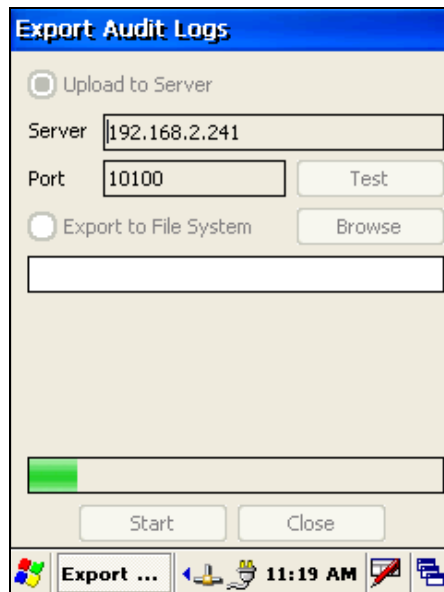
## AUDIT DATA ELEMENTS

Whenever a card is inserted and the PIN is matched, a new activity transaction begins. The following information is available for each transaction:

- Start Date and Time
- TWIC Authentication Mode
- CHUID FASC-N
- Card Holder Name
- Expiration Date and Time
- Number of PIN attempts (including first)
- Verification Date and Time
- CHUID Check Results (Ok, Bad, or Not Checked)
- Biometric Comparison Results (Match, No Match, or Not Configured)
- TSA Hotlist Check Results (Not Found, Found, Not Configured, or Deferred)
- PKI Validation Results (Good, Revoked, Not Configured, or Deferred)
- Operator User Name
- Unit (System) ID (serial number)
- Stop Date and Time
- Overall Result (Authenticated, Not Authenticated)

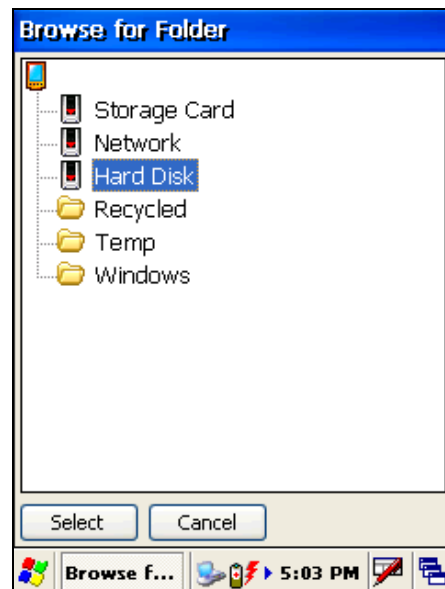
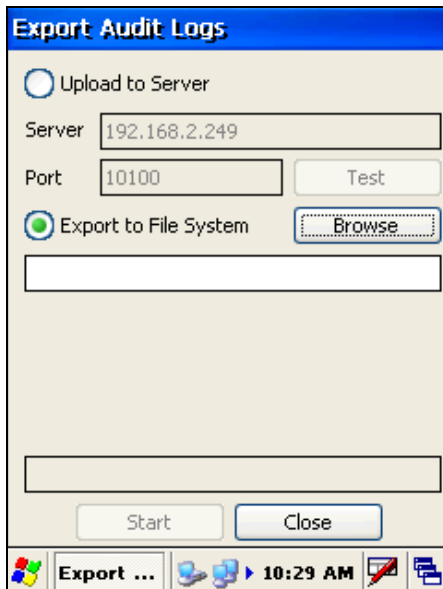
## UPLOAD TO SERVER (PLUS AND/OR AUDIT TRAIL ONLY)

If you are licensed for *PIVCheck Plus Mobile Edition* or *PIVCheck Audit Trail*, you may choose the *Upload to Server* option. This will decrypt the locally cached audit log and insert the records that into the Audit database that is managed by the PACS Service plug-in.



## EXPORTING AUDIT LOG TO FLASH DRIVE

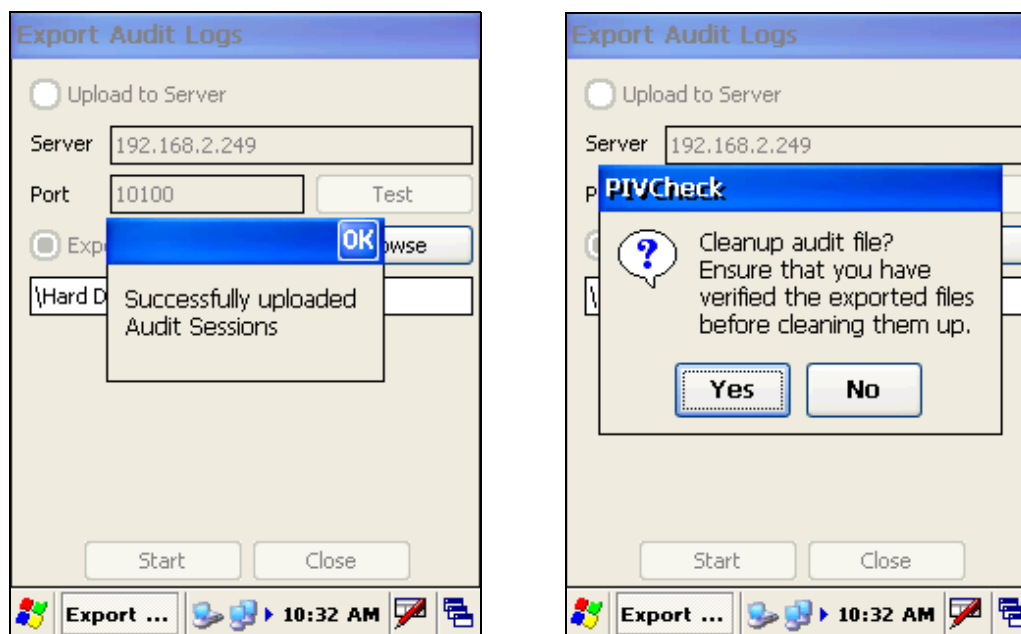
To decrypt the audit log and export it to a flash drive, insert a flash drive into one of the USB ports on the top of the terminal. Then tap the *Export Audit Logs* button. Select the *Export to File System* radial button. Tap on the *Browse* button. A folder browser dialog box will be displayed. Tap on *Hard Disk*. Then tap *Select*. When ready to begin the export, tap the *Start* button on the *Export Audit Logs* screen.





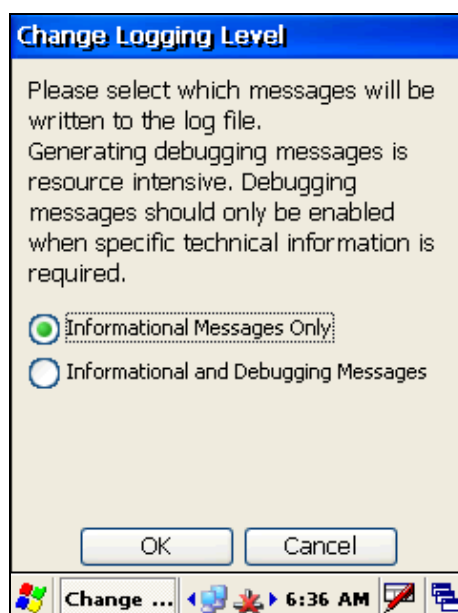
## AUDIT LOG FILE CLEANUP

After the export to server or file is complete, you will be prompted to clear the existing audit file. It is recommended that before you tap the Yes button, you remove the flash drive containing the exported log file and verify the files on a PC. If the file appears to be complete and is not corrupted in any way then tap the Yes button.

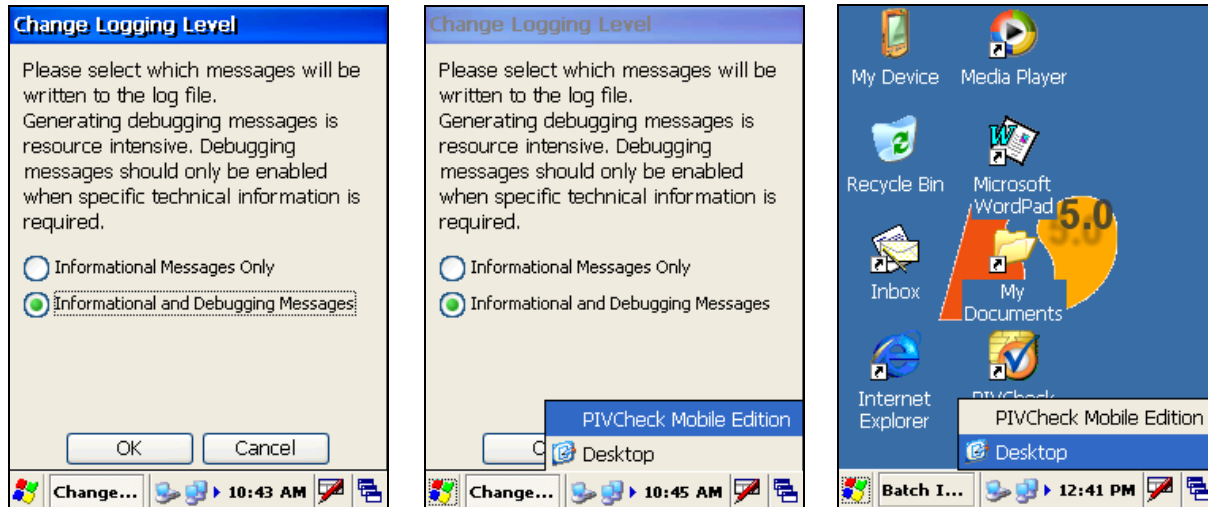


## CHANGE DIAGNOSTIC LOGGING LEVEL BUTTON

This is an advanced feature designed to help debug cards that appear to be incompatible. In the event *PIVCheck Mobile Edition* encounters an error while reading the contents of a card, remove the card from the reader and set the logging level to *Informational and Debugging Messages*.

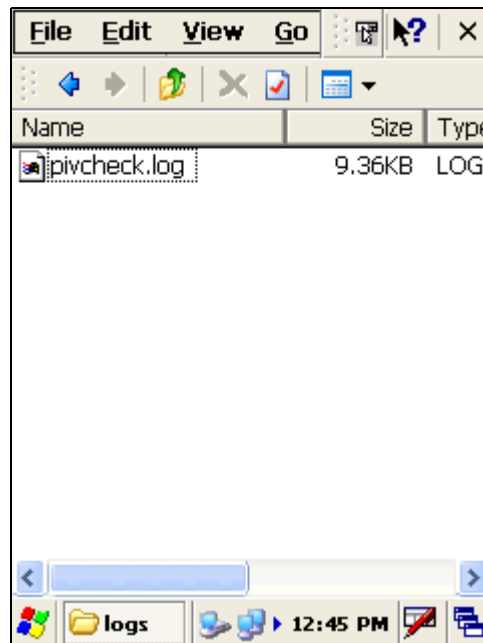


Re-insert the card and repeat the operation that failed. Change the logging level back to *Informational Messages Only*. Then locate the log file by tapping on the icon in the extreme lower right corner and switching to the Desktop.

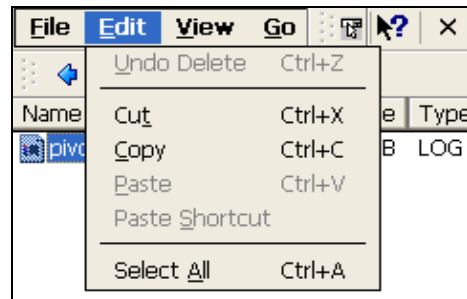


If your mobile biometric terminal has a USB port then insert a flash drive into the USB port. Tap on *My Device* and navigate to the following folder: *Program Files -> Pivcheck\_Mobile\_Edition -> logs*

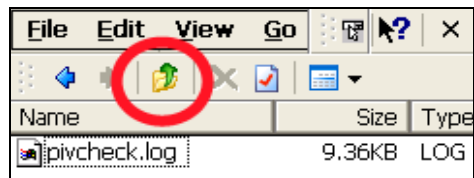
An entry for the diagnostic log file should be displayed.



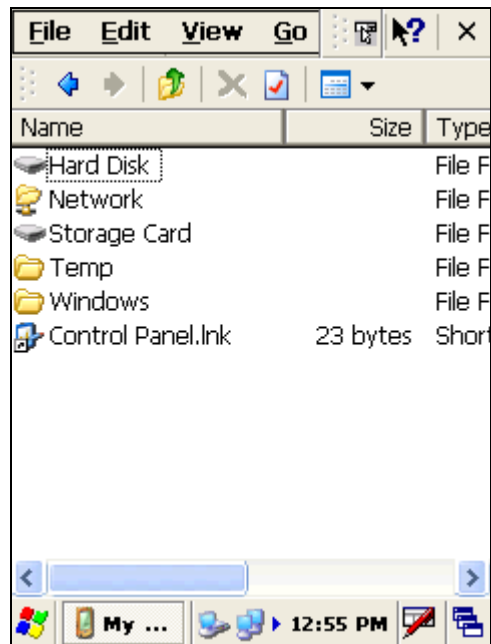
From the *Edit* dropdown menu, tap *Copy*.



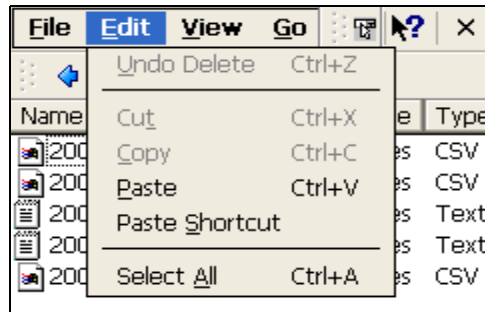
Now, tap on the *Up* arrow on the Windows CE Explorer tool bar.



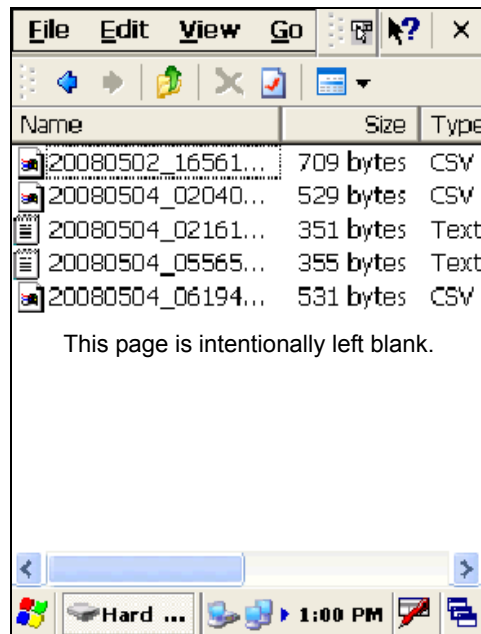
Continue to tap the *Up* arrow until the contents of the uppermost level are displayed:



Select *Hard Disk* to open the contents of the flash drive. Then, drop down the *Edit* menu. The *Paste* option will be enabled:



Tap on *Paste*. The log file should immediately appear:



Remove the flash drive and insert it into a PC. E-mail the log file as an attachment to Codebench Technical Support for analysis. [techsupp@codebench.com](mailto:techsupp@codebench.com)

## LICENSING THE SOFTWARE

For more information refer to section “Licensing the Software” on page 19..

# UPDATING YOUR SOFTWARE

Keeping *PIVCheck Mobile Edition* up to date and compliant with the latest rules and regulations is very important to us. Which is why you should frequently check to ensure that you are running the latest version of your Codebench software.

## OVERVIEW

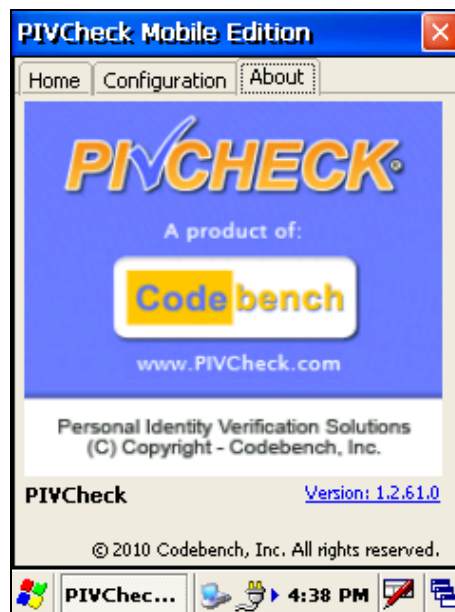
There are multiple ways to upgrade to the latest release of *PIVCheck Mobile Edition*. The method you choose will depend upon whether you have network connectivity and whether your software is properly licensed.

- You can request *PIVCheck Mobile Edition* to upgrade the software.
- Use the *Windows CE Internet Explorer* to download the software and install it manually.
- Copy the software from a flash drive to the mobile biometric terminal and install it manually.

## AUTOMATIC SOFTWARE DOWNLOAD

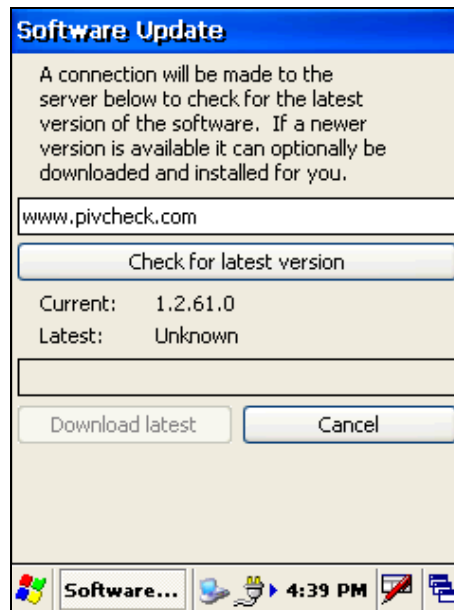
To use this method, you must have an Internet connection and a licensed copy of the software with a revision level of 1.1.5.0 or better.

Remove any cards from the smart card reader then select the *About* tab.

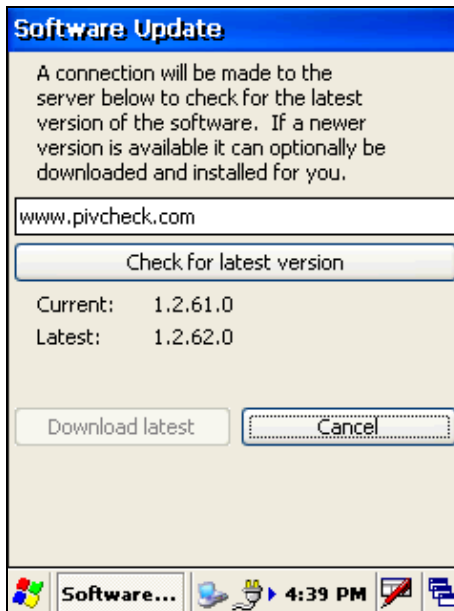


Note that the version number in the lower right corner is a [hyperlink](#). Click the link. The following dialog will be displayed.

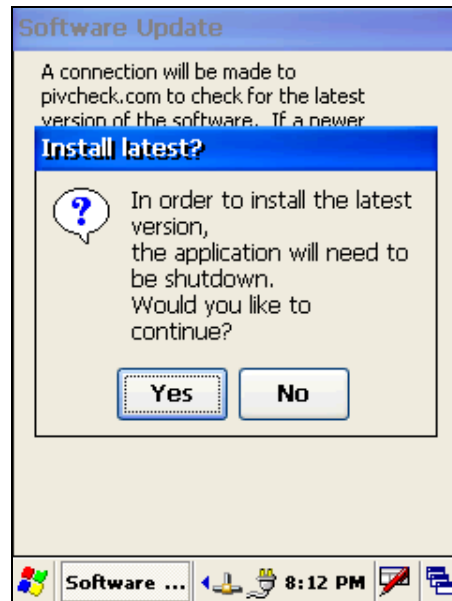
Tap the *Check for latest version* button to see whether any updates are available.



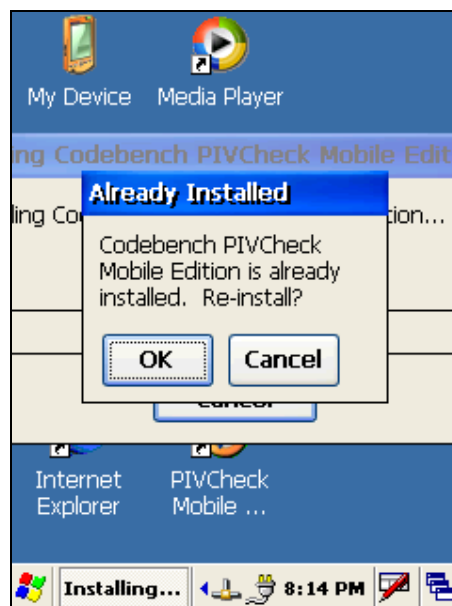
If a newer version is available, it will be displayed as shown in the following illustration.



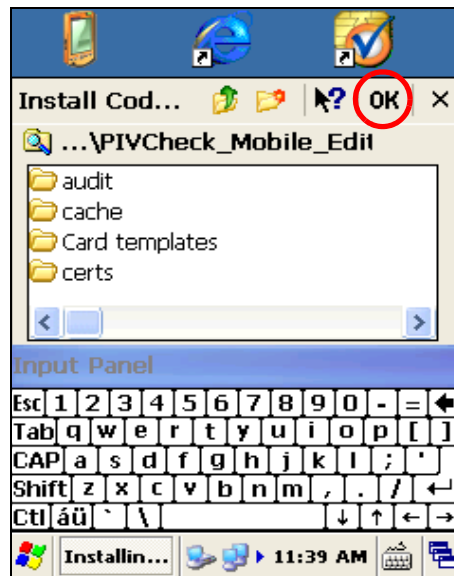
Tap the *Download latest* button to upgrade the software, and the following dialog will be displayed. Otherwise, tap *Cancel* to close the dialog. When the download is complete, you will be prompted to allow the installer to close the current application instance.



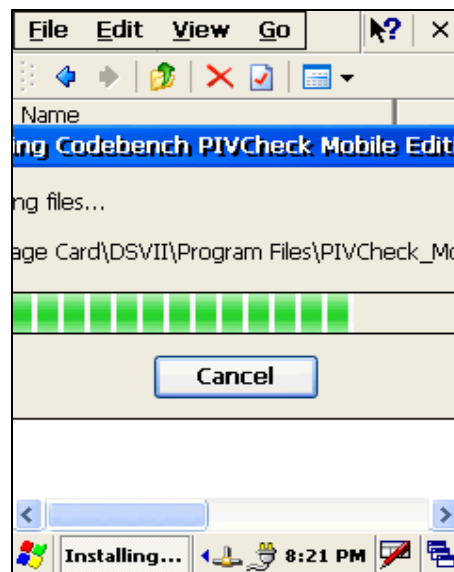
Since *PIVCheck Mobile Edition* is already installed you will be prompted to shutdown the application. Tap *Yes* to continue.



Tap the *OK* button to overwrite the current installation. (Your configuration settings will be preserved).



Tap the *OK* button to proceed with the installation. The progress bar will appear to be truncated at both ends. This is normal Windows CE behavior.



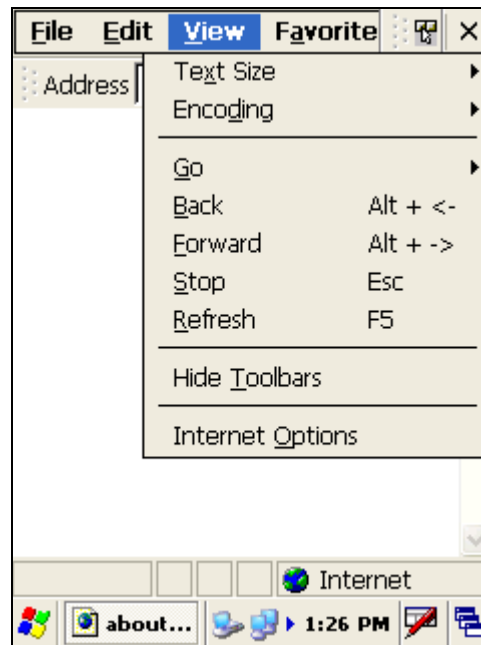


## INSTALLING AN EXECUTABLE FILE VIA INTERNET EXPLORER DOWNLOAD

To use this method, you must have an Internet connection and a username and password to access the Codebench general download site. If you have never used *Internet Explorer* from your mobile biometric terminal, it may need to be configured for Internet access.

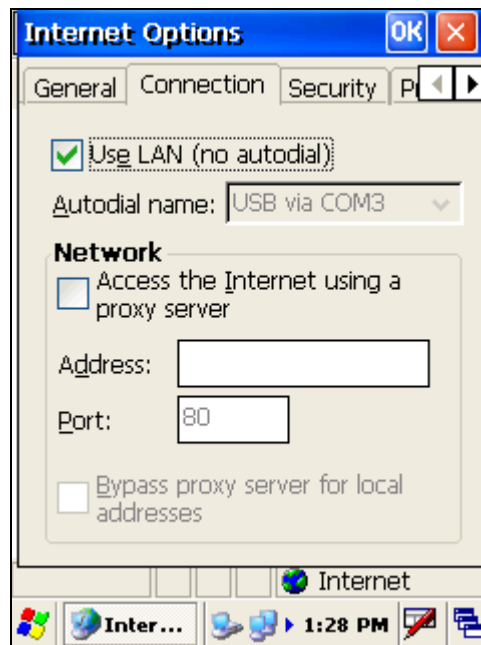
Exit the *PIVCheck Mobile Edition* application.

Launch *Internet Explorer* and tap *View*.



Tap on *Internet Options* at the bottom.

When the dialog appears, tap on the *Connection* tab. Check the *Use LAN (no autodial)* option.



If you are required to use a proxy server then check the *Access the Internet using a proxy server* option and supply the addressing information for your site.

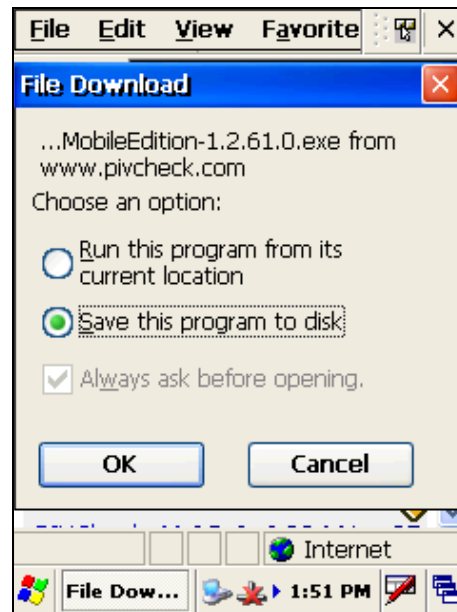
Tap the *OK* button to save the configuration options.

Now you are ready to download a new version of software. Type the following URL in to the browser's address bar:  
<http://www.pivcheck.com/cabs/>

An authentication dialog will be displayed.

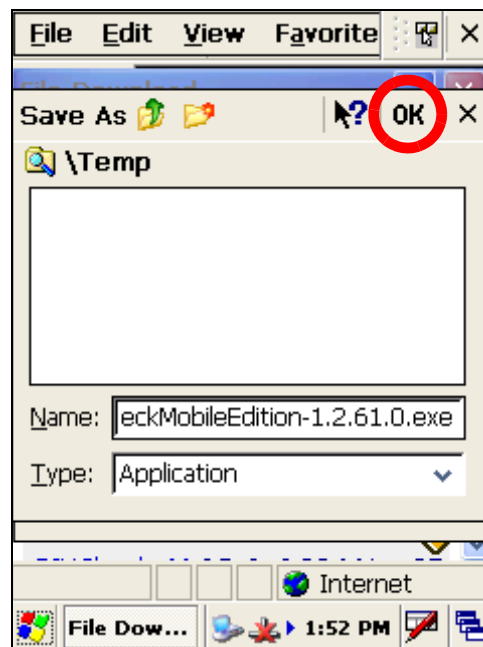


Enter your *User Name* and *Password* into the appropriate fields and tap the *OK* button. If the information is correct, then an *options* dialog will be displayed:

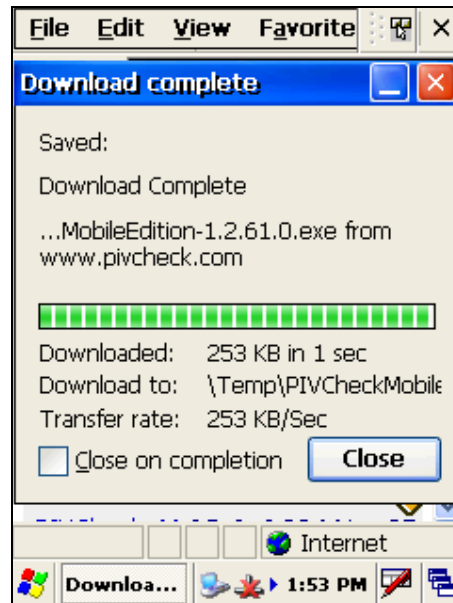


Choose the options as shown above and tap *OK*. The new *PIVCheck Mobile Edition* executable file will be downloaded to the `\Temp` folder on the terminal.

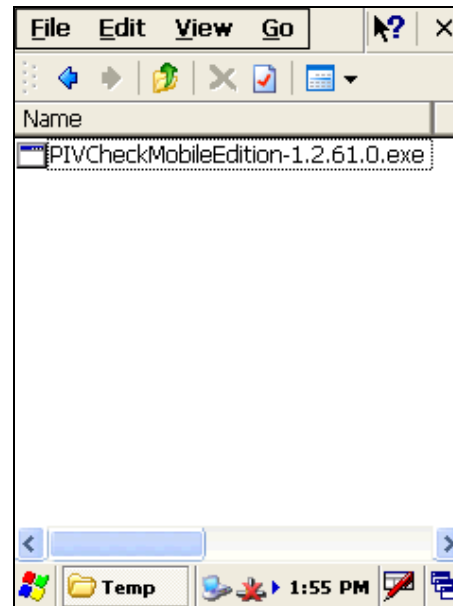
Tap the *OK* button to start the download.



When the file download is complete, close Internet Explorer and tap on *My Device* and navigate to the `\Temp` folder.



Double-tap on the `PIVCheckMobileEdition 1.X.XX.X.exe` file and follow the installation wizard.



## INSTALLING AN EXECUTABLE FILE FROM A FLASH DRIVE

- Copy the executable file onto the flash drive.
- Power up the mobile biometric terminal.
- Insert the flash drive into one of the standard USB ports.
- Double-tap the *My Device* Icon. The flash drive will appear as a *Hard Drive* in this directory.
- Double-tap on the *Hard Drive* directory to reveal the *PIVCheck Mobile Edition* executable file. Copy the executable file from the *My Device > Hard Disk* directory to the *My Device > Temp* directory.
- Double-tap the executable file and follow the installation wizard.

This completes the installation.

This page is intentionally left blank.

# APPENDIX A

## REFERENCE DOCUMENTS

- 1 *Federal Information Processing Standard Publication 201-1 (FIPS 201-1): Personal Identity Verification (PIV) of Federal Employees and Contractors*, NIST, March, 2006
- 2 NIST PIV Program web site, <http://csrc.nist.gov/piv-program>
- 3 *NIST Special Publication 800-63-1: Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*, February 2008.
- 4 *NIST Special Publication 800-73-3: Interfaces for Personal Identity Verification – Part 1: End-Point PIV Card Application Namespace, Data Model, and Representation*, February 2010.
- 5 *NIST Special Publication 800-73-3: Interfaces for Personal Identity Verification – Part 2: End-Point PIV Card Application Card Command Interface*, February 2010.
- 6 *NIST Draft Special Publication 800-76-1: Biometric Data Specification for Personal Identity Verification*, January 2007.
- 7 *NIST Special Publication 800-78-2: Cryptographic Algorithms and Key Sizes for Personal identity Verification*, February 2010.
- 8 *NIST Special Publication 800-79-1 (SP 800-79-1): Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCI's)*, June 2008.
- 9 *NIST Draft Special Publication 800-85 A-1 (SP 800-85 A-1): PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-2 Compliance)*, March 2009
- 10 *NIST Draft Special Publication 800-85 B (SP 800-85 B): PIV Data Model Test Guidelines*, July 2006
- 11 *NIST Draft Special Publication 800-85 B-1 (SP 800-85 B-1): DRAFT PIV Data Model Conformance Test Guidelines*, September 11, 2009
- 12 *NIST Draft Special Publication 800-87 Rev 1 (SP 800-87 Rev 1): Codes for Identification of Federal and Federally-Assisted Organizations*, April 2008.
- 13 *NIST Special Publication 800-116: A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, November 2008.
- 14 *TWIC Reader Hardware and Card Application Specification Version 1.1.1*, May 2008
- 15 TWIC Technical Advisory TA-2008-TWIC001-V1.0, TWIC Reader Functionality Augmentation, September, 2008
- 16 TWIC Technical Advisory TA-2009-TWIC001-V1.0, Format for a TWIC Card with no Fingerprint Biometric Data, March, 2009
- 17 TWIC Technical Advisory TA-2009-TWIC002-V1.0 Additional Error Code Definitions for TWIC Cards, March, 2009
- 18 *Smart Card Alliance Publication Number: PAC-07002: Physical Access Control System Migration Options for Using FIPS 201-1 Compliant Credentials*, September 2007.

This page is intentionally left blank.



# APPENDIX B

## CARD DATA CONTAINERS

**TABLE 1. PIV DATA CONTAINERS**

<i>Container Name</i>	<i>Container ID</i>	<i>Access Rule</i>	<i>Contact / Contactless</i>	<i>Mandatory/Optional</i>
Card Capability Container	0xDB00	Always Read	Contact	Mandatory
Card Holder Unique Identifier	0x3000	Always Read	Contact & Contactless <sup>a</sup>	Mandatory
X.509 Certificate for PIV Authentication	0x0101	Always Read	Contact	Mandatory
Cardholder Fingerprints	0x6010	PIN	Contact	Mandatory
Security Object	0x9000	Always Read	Contact	Mandatory
Cardholder Facial Image	0x6030	PIN	Contact	Optional
Printed Information	0x3001	PIN	Contact	Optional
X.509 Certificate for Digital Signature	0x0100	Always Read	Contact	Optional
X.509 Certificate for Key Management	0x0102	Always Read	Contact	Optional
X.509 Certificate for Card Authentication	0x0500	Always Read	Contact / Contactless	Optional
Discovery Object	0x6050	Always Read	Contact	Optional
Key History Object	0x6060	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 1	0x1001	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 2	0x1002	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 3	0x1003	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 4	0x1004	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 5	0x1005	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 6	0x1006	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 7	0x1007	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 8	0x1008	Always Read	Contact	Optional

Retired X.509 Certificate for Key Management 9	0x1009	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 10	0x100A	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 11	0x100B	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 12	0x100C	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 13	0x100D	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 14	0x100E	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 15	0x100F	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 16	0x1010	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 17	0x1011	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 18	0x1012	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 19	0x1013	Always Read	Contact	Optional
Retired X.509 Certificate for Key Management 20	0x1014	Always Read	Contact	Optional
Cardholder Iris Image	0x1015	PIN	Contact	Optional

a. In September 2007, this was changed from Contact to Contact & Contactless.

**TABLE 2. TWIC DATA CONTAINERS**

<i>Container Name</i>	<i>Container ID</i>	<i>Access Rule</i>	<i>Contact / Contactless</i>	<i>Mandatory/Optional</i>
TWIC Privacy Key Buffer	0xDFC101 (0x2001)**	Always Read	Contact (and Magnetic stripe also)	Mandatory
Card Holder Fingerprints	0xDFC103 (0x2003)**	Always Read	Contact & Contactless	Mandatory
Card Holder Unique Identifier	0x5FC102 (0x3000)**	Always Read	Contact & Contactless	Mandatory
Unsigned Card Holder Unique Identifier	0x5FC104 (0x3002)**	Always Read	Contact & Contactless	Mandatory
Security Object	0xDFC10F (0x9000)**	Always Read	Contact & Contactless	Mandatory

This page is intentionally left blank.

# APPENDIX C

## PROXIMITY READER CONFIGURATION - DSV2+ ONLY

### OVERVIEW

The proximity reader included with the DSV2+<sup>Turbo</sup> may need to be configured to produce the correct bit sequence for the site's proximity cards. This is done by removing the back cover of the DSV2+<sup>Turbo</sup> and reconnecting the proximity reader to a PC so that a new configuration can be downloaded to its NVRAM.

### PROCEDURE

#### PREPARING THE READER

- 1 Download the configuration utility from <http://www.rfideas.com/Software/pcProxConfig.exe> and install it on a Windows XP computer. Do not start the program yet.
- 2 Using a screw driver, remove the back cover from the DSV2+<sup>Turbo</sup> mobile terminal.
- 3 Disconnect the USB cable from the built-in receptacle located between the battery pack and the pcProx reader.
- 4 Ensure that the DSV2+<sup>Turbo</sup> is powered down.
- 5 Disconnect the USB connector between the pcProx reader and the USB extension on the DSV2+<sup>Turbo</sup>.
- 6 Carefully extend the two-inch USB cable from the pcProx reader and connect it to the PC. The led on the pcProx reader will display in red.
- 7 Start the pcProx configuration utility. It will immediately query the PC's USB ports to locate the pcProx reader. Click the Set Keystroke Data tab.

#### FACILITY AND ID CODES

- From the application menu, select *File > Open...* and select the file format for your site. Adjust the information in the Facility (FAC) & ID Codes section to meet your site's requirements.

#### KEYSTROKE DATA

- In the keystroke data section, configure as shown in the following illustration:  
When complete, click the *Write to pcProx* or *AIR ID* button.

This page is intentionally left blank.

# Index

<b>A</b>			
Appendix A			
Reference Documents	77		
Appendix B	79, 83		
PIV Data Containers	79		
TWIC Data Containers	81		
Application Tab			
Audit Log Folder	34		
Configurable Contact Information	35		
Error Log Folder	35		
<b>C</b>			
Certificate Validation	49		
Configuration Options			
Application Tab	31		
Configuring the System	19		
Changing the Admin Password	22		
Enter your License Manually	21		
Licensing the Software	19		
Powering Up	13		
Trial License	21		
<b>D</b>			
Definitions	3		
Administrator	3		
Cardholder	3		
Certificate Authority (CA)	4		
Certificate Revocation List (CRL)	4		
Installer	4		
Online Certificate Status Protocol (OCSP)	4		
Personal Identity Verification (PIV)	4		
Physical Access Control System (PACS)	4		
Server-based Certificate Validation Protocol (SCVP)	4		
Transportation Worker Identification Credential (TWIC)	5		
TWIC Privacy Key (TPK)	5		
User (Operator)	5		
Validation Authority	5		
<b>E</b>			
Export Audit Logs Button			
Audit Data Elements	61		
Audit Log File Cleanup	63		
Exporting Audit Log to Flash Drive	62		
<b>F</b>			
Fingerprint Match	47		
Fingerprint Match Failure	48		
Fingerprint Match Threshold	47		
Scoring	47		
<b>H</b>			
Home Tab			
Tools Tab	57		
<b>I</b>			
Identity Authentication			
The Application Events Window	49		
The Card Data Window	49		
Identity Verification	43		
Something you Have (PIV Credential)	43		
Something you Know (Knowledge of PIN)	44		
<b>K</b>			
Key Features	7		
<b>L</b>			
License			
License (Fingerprint Template Matcher)	32		
Licensing			
Updating Your Software			
Automatic Software Download	67		
Installing a CAB File via Internet Explorer Download	71		
<b>S</b>			
Saving your Configuration	41		
Supported Credential Types	8		
System Specifications	9		
Hardware	10		
Software	11		
<b>T</b>			
Terminology	3		
AIA	3		
CA	3		
CHUID	3		
CPV	3		
CRL	3		
CRLDP	3		
CTL	3		
FASC-N	3		
FIPS	3		
ICC	3		
IDN	3		
OCSP	3		
PACS	3		
PIV	3		
PKI	3		
QCRL	3		
SCVP	3		
TPK	3		
TWIC	3		
VA	3		
Tools Tab	57		
Change Diagnostic Logging Level			
Button	63		
Synchronizing Configuration	57, 66		