



OMNICheck User Guide

Codebench, Inc
6820 Lyons Technology Circle
Coconut Creek, FL 33073

Voice: 561.883.3218
Fax: 561.883.2566
www.codebench.com

Codebench

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

 OMNICheck 7

 OMNICheck Plus Edition 8

 OMNICheck Optional Features 9

 Supported Credential Types 9

Chapter 4 System Specifications 11

 Hardware 11

 Software 11

Chapter 5 Software Installation 13

 Installation Options 13

 Important Notice 13

 Powering Up 13

 Downloading OMNICheck Mobile directly on the Mobile Terminal 14

 Installing OMNICheck File from a Flash Drive 18

Chapter 6 Configuring the System 19

 Licensing the Software 19

 Trial License 21

 Enter your License Manually 22

 Changing the Admin Password 23

 Configuring the PACS plug-in on your PC (Plus Only) 24

 Authorizing Client Connections 24

 Synchronize Configuration (Plus Only) 26

 Manually Configuring the OMNICheck Mobile Device 28

 Plus Tab (Plus Only) 28

 Registration Handling 29

 Enable Online Mode 30

 Server Address 30

 Server Port 31

Send Audit Record to Server.....	31
Lookup Person Data.....	32
PACS Connection Failures	33
Client Not Authorized	33
Incorrect Server IP Address or Network Routing Problem.....	34
Server Exists but PACS Service is not Running	34
Application Tab	36
TWIC Authentication Modes.....	37
Fingerprint Options.....	38
Audit Log Folder	39
Error Log Folder	39
Configurable Contact Information.....	40
Automatic Rollover	40
Blacklist Plug-ins.....	40
Users.....	41
User ID	41
Password.....	41
Role	41
Door Control (Optional).....	42
Door Control Configuration Form	43
Saving your Configuration	45

Chapter 7 Identity Verification 47

CHUID and Active Card Authentication.....	48
Contactless State.....	48
Contact Mode.....	48
Biometric Verification.....	48
Fingerprint Capture.....	48
Fingerprint Match	49
Scoring	49
Fingerprint Match Threshold	49
Fingerprint Match Failure	49
Zero Biometric Card.....	51
Non-TWIC Mode.....	51
Certificate Validation.....	52
The Card Data Window.....	52
The Application Events Window	52
Identity Authentication.....	52

Chapter 8 Non-TWIC Identity Verification..... 53

CHUID and Active Card Authentication.....	54
CHUID Verification.....	54
Contactless State.....	54
Contact Mode.....	54
Entering a PIN to Unlock a Smart Card.....	55
PIN Failure	56
PIN Match	57
Biometric Verification.....	57
Fingerprint Capture	57
Fingerprint Match	58

Scoring	58
Fingerprint Match Threshold.....	58
Fingerprint Match Failure	58
Certificate Validation.....	60
Personal Tab.....	60
Events Tab	60
Identity Authentication.....	60
Legacy CAC or Non-PIV Cards	61
Contact or Contactless.....	61
Contactless.....	61
Validation	61

Chapter 9 Tools..... 63

Synchronize Configuration (Plus Only)	63
Export Audit Logs Button	64
Audit Data Elements	64
Exporting Audit Log to Flash Drive.....	65
Audit Log File Cleanup	66
Change Diagnostic Logging Level Button.....	67
Licensing the Software	71
Trial License	73
Enter your License Manually	73
Synchronizing Data.....	74
Remote.....	75
Local.....	75
Import	76
Export.....	78

Chapter 10 Updating Your Software..... 81

Overview	81
Automatic Software Download.....	81
Installing an Executable File via Internet Explorer Download	85
Installing an Executable File from a Flash Drive.....	90

Appendix A 91

Reference Documents 91

Appendix B 93

Card Data Containers	93
Table 1. PIV Data Containers	93
Table 2. TWIC Data Containers	95

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).

DSV2+^{TURBO} is a registered trademark of Datastrip Corporation.

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 9.

- **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+^{TURBO} 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.

KEY FEATURES

OMNICHECK

OMNICheck is designed to help security personnel to verify cardholder identity and ensure that they possess a valid credential.

- **Hands-free, Contactless Operation**

OMNICheck is optimized for hands-free, contactless operation without the use of a personal identification number (PIN).

- **TWIC Authentication Modes**

OMNICheck verifies TWICs based on the currently selected TWIC authentication mode. The mode can be locally or remotely¹ configured.

- **TSA Hotlist Checking**

OMNICheck can be configured to verify that the cardholder's FASC-N is not on the current TSA Hotlist. The Hotlist can be imported, or can be accessed directly if the mobile biometric terminal is connected to the Internet.

- **TSA Hotlist Integrity Check**

Before validating any FASC-N against the TSA Hotlist, *OMNICheck* computes the MD5 hash of the list itself and compares it with the MD5 hash downloaded from the TSA web site at the time that the list was downloaded. This ensures that the list downloaded from the TSA has not been tampered with.

- **PKI Validation**

OMNICheck can be configured to ensure that each X.509 certificate, including the TSA certificate, is validated with the TSA certificate authority using a CRL, TSA responder or repeater, or TSA responder.

- **Card Validation**

OMNICheck issues a GENERAL AUTHENTICATE challenge to the PIV card applet to ensure that it is communicating with an authentic card, not a forgery. Depending on its configuration, *OMNICheck Plus Edition* submits the CHUID certificate to a local certificate store or online validation authority to check for revocation.

- **Biometric Signature Validation**

OMNICheck verifies that the FASC-N in the Signed Attributes field of the external digital signature on the biometric matches the FASC-N of the card's CHUID.

- **TPK Caching and Merging**

When operating in TWIC authentication modes 3 and 4, *OMNICheck* looks in its local cache for the cardholder's TWIC privacy key (TPK). If the TPK is found, it is used to decrypt the cardholder's biometric template obtained from the TWIC. If the TPK is not found, *OMNICheck* prompts for the card to be inserted into the contact interface where it can be extracted. Once the TPK is obtained and cached, the verification process continues. Newly-acquired TPKs can be merged with an existing TPK store, allowing a site to accumulate and distribute TPKs to other devices. This is done manually using a USB flash drive. See "Synchronizing Data" on page 74 for more details.

- **Exportable Audit Trail**

Each card validation session is logged to an encrypted, serialized data file. The contents of the file can be exported to a removable file. The exported format is comma separated values (CSV).

- **Encrypted Configuration**

All configuration data, passwords, and audit logs are encrypted using RSA-1024 whose unique asymmetric key is securely generated. The device's encryption key can be relocated to removable USB media, thereby rendering the device inoperable until the key is re-inserted.

1. Remote configuration requires the *OMNICheck Plus* or *PIVCheck Plus* option.

OMNICHECK PLUS EDITION

OMNICheck Plus Edition offers all the functionality of *OMNICheck* with the addition of the following features.

- **Network Based Data Synchronization**
OMNICheck Plus Edition can communicate with the PACS Service configured at your site through the online mode feature.
- **Exportable Audit Trail (Export Audit Logs)**
 Same as *OMNICheck* with the added feature of synchronizing a batch of audit logs or upload in real time with the PACS service.
- **Synchronizing TWIC Privacy Key (TPK) databases**
 Similar to TPK Caching and Merging within *OMNICheck*. This added feature allows TPK databases to be synchronized in a batch or in real time with the PACS service.
- **Retrieving previously registered person data, i.e. name, information and card photos**
 This feature allows a *OMNICheck Plus Edition* device to retrieve person data from the PACS service which has been previously registered using *PIVCheck Plus Desktop Edition* or *PIVCheck Plus Mobile Edition*.
- **Synchronizing security policies with the PACS service (Synchronize Configuration)**
 The registered *OMNICheck Plus Edition* devices can update their security policies with PACS service. For example, if the TWIC Authentication mode on the PACS service is changed from mode 1 to mode 3, then this feature synchronizes the *OMNICheck Plus Edition* devices automatically to the same mode.
- **Configuration data defined by the PACS service (Synchronize Configuration)**
 This feature allows a registered *OMNICheck Plus Edition* device to configure itself with additional data which is defined within the PACS service.

OMNICHECK OPTIONAL FEATURES

The following optional features enhance the functionality of your *OMNICheck* software.

- **Door Control**

The Door Control option provides a way to validate a TWIC card and, if the card is completely validated and the cardholder's identity has been confirmed, send a Wiegand protocol signal over the network to a Wiegand data converter, which will unlock a door and provide entry into a facility.

- **Exportable Audit Trail (Included in *OMNICheck Plus*)**

Same as *OMNICheck* with the added feature of synchronizing a batch of audit logs or upload in real time with the PACS service.

- **Plus**

See "*OMNICheck Plus Edition*" on page 8

SUPPORTED CREDENTIAL TYPES

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

SYSTEM SPECIFICATIONS

HARDWARE

The *OMNICheck* 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 *OMNICheck* 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	Color digital transfective touch screen with stylus. Supported dimensions: <ul style="list-style-type: none"> • 240 horizontal x 320 vertical (portrait) • 320 horizontal x 240 vertical (landscape) • 640 horizontal x 480 vertical (landscape)
Fingerprint Sensor	Must be <i>FIPS 201 Approved Product List (APL)</i> certified. http://fips201ep.cio.gov/apl.php
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

OMNICheck requires Microsoft® Windows® CE 5.0 and .NET Compact Framework 2.0 or greater.

SOFTWARE INSTALLATION

INSTALLATION OPTIONS

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

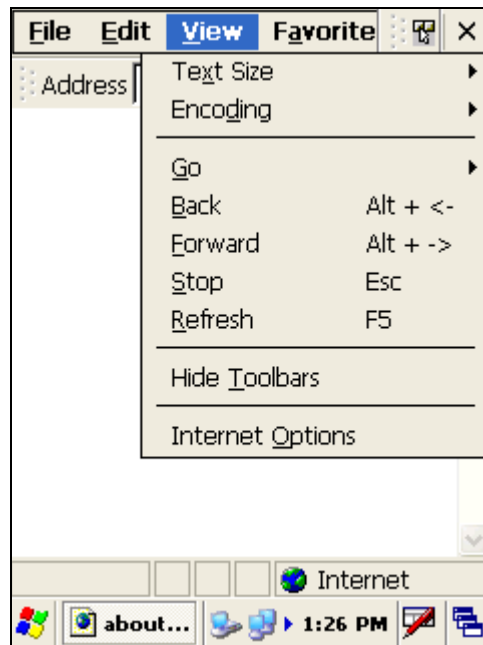


Due to the variances of hardware configurations, please refer to the user manual for detailed instructions on powering on your mobile biometric terminal.

DOWNLOADING OMNICHECK MOBILE DIRECTLY ON THE MOBILE TERMINAL

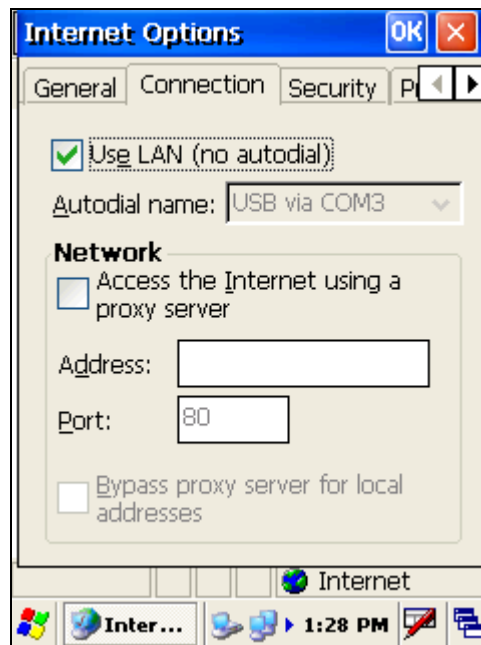
To use this method, you must have an Internet connection and a user name and password to access the Codebench general download site. If you have never used *Internet Explorer* from your mobile biometric terminal, it may need to be configured for Internet access.

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.



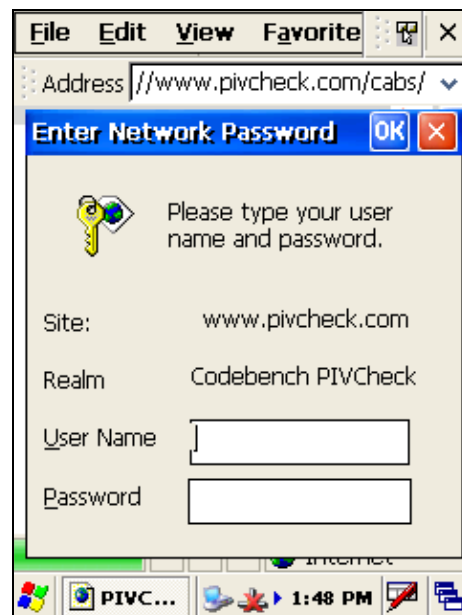
If you are required to use a proxy server then check the *Access the Internet using a proxy server* option and supply the addressing information for your site.

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

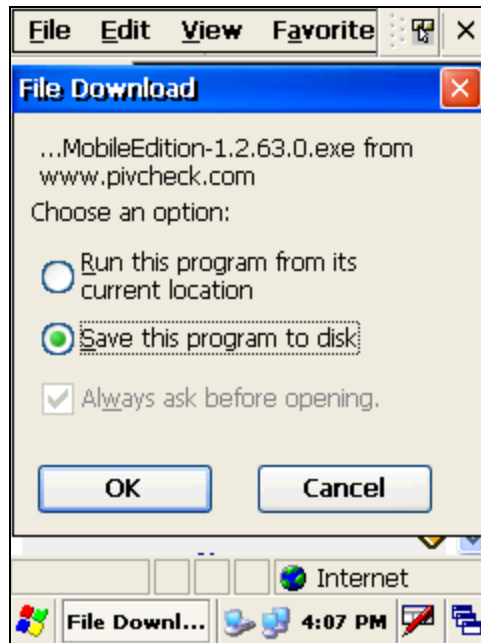
Now you are ready to download the *PIVCheck Mobile* software. Type the following URL into the browser's address bar:

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

An authentication dialog will be displayed.

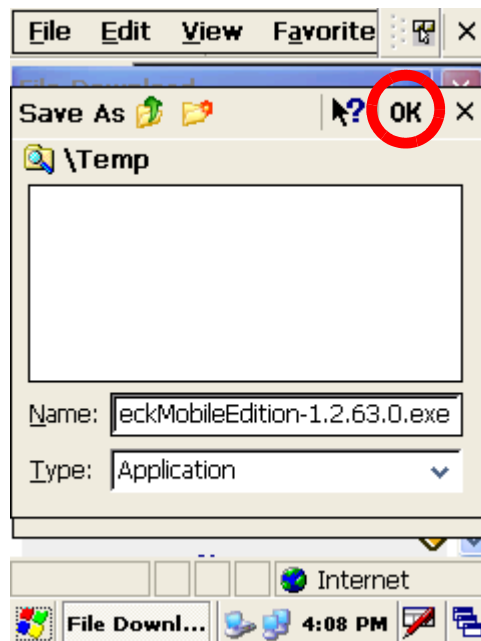


Enter your *User Name* and *Password* into the appropriate fields and tap the *OK* button. If the information is correct, then an *options* dialog will be displayed:

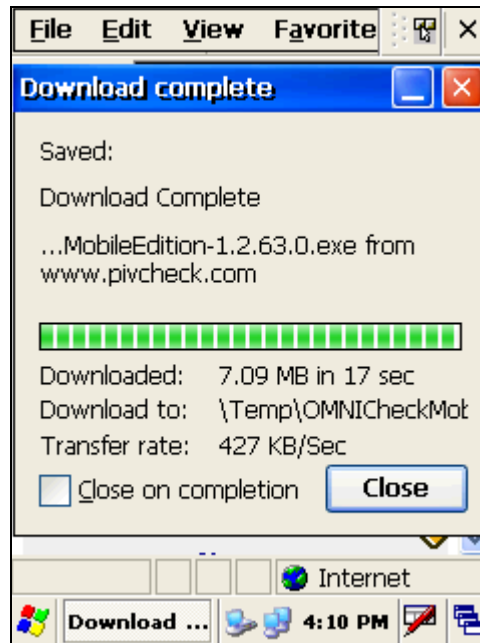


Choose the options as shown above and tap *OK*. The new *OMNlCheck* executable file will be downloaded to the *\Temp* folder on the terminal.

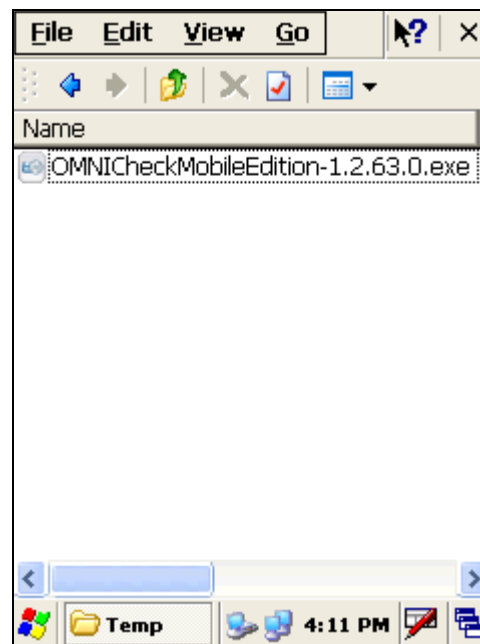
Tap the *OK* button to start the download.



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



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



INSTALLING OMNICHECK FILE FROM A FLASH DRIVE

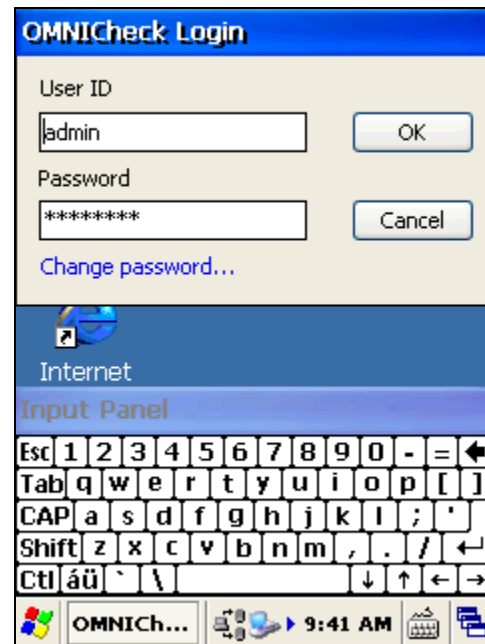
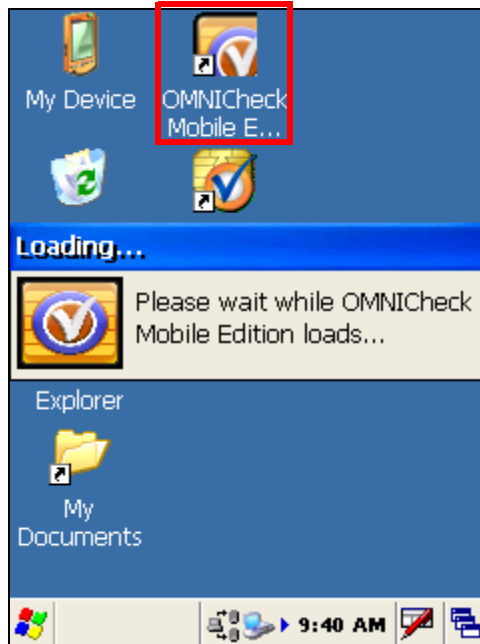
- Copy the *OMNICheck* executable file onto the flash drive.
- Power up the mobile biometric terminal.
- Insert the flash drive into one of the standard USB ports located on the mobile biometric terminal.
- Double-tap the *My Device* icon. The flash drive will appear as a *Hard Drive* in this directory.
- Double-tap on the *Hard Drive* directory to reveal the *OMNICheck* 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 *OMNlCheck* icon.
- 2 Enter the default operator *User ID* (*admin*) and *Password* (*password*) using the input panel.



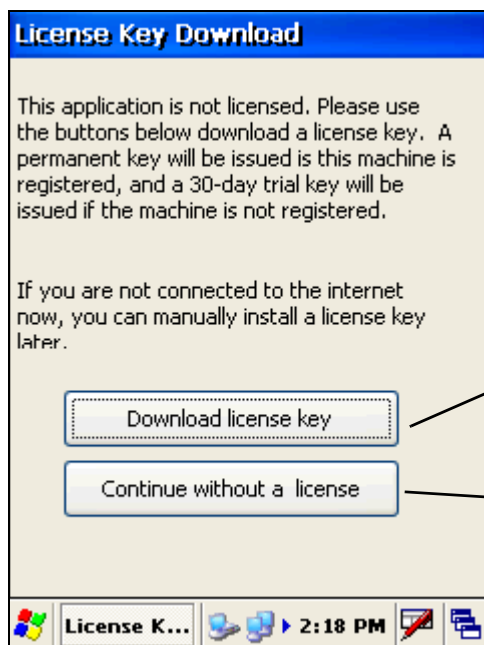
Your system integrator may have changed the default administrative *User ID* and *Password* from the Codebench factory defaults located above. Please consult your system integrator's documentation.

- 3 Press the *OK* button to accept the password and launch the *OMNICheck splash screen*.



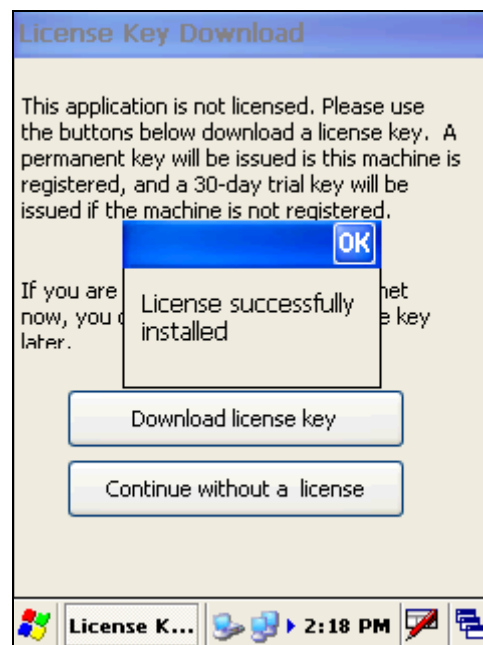
You can disable the splash screen by un-checking the checkbox in the upper left-hand corner.

- 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

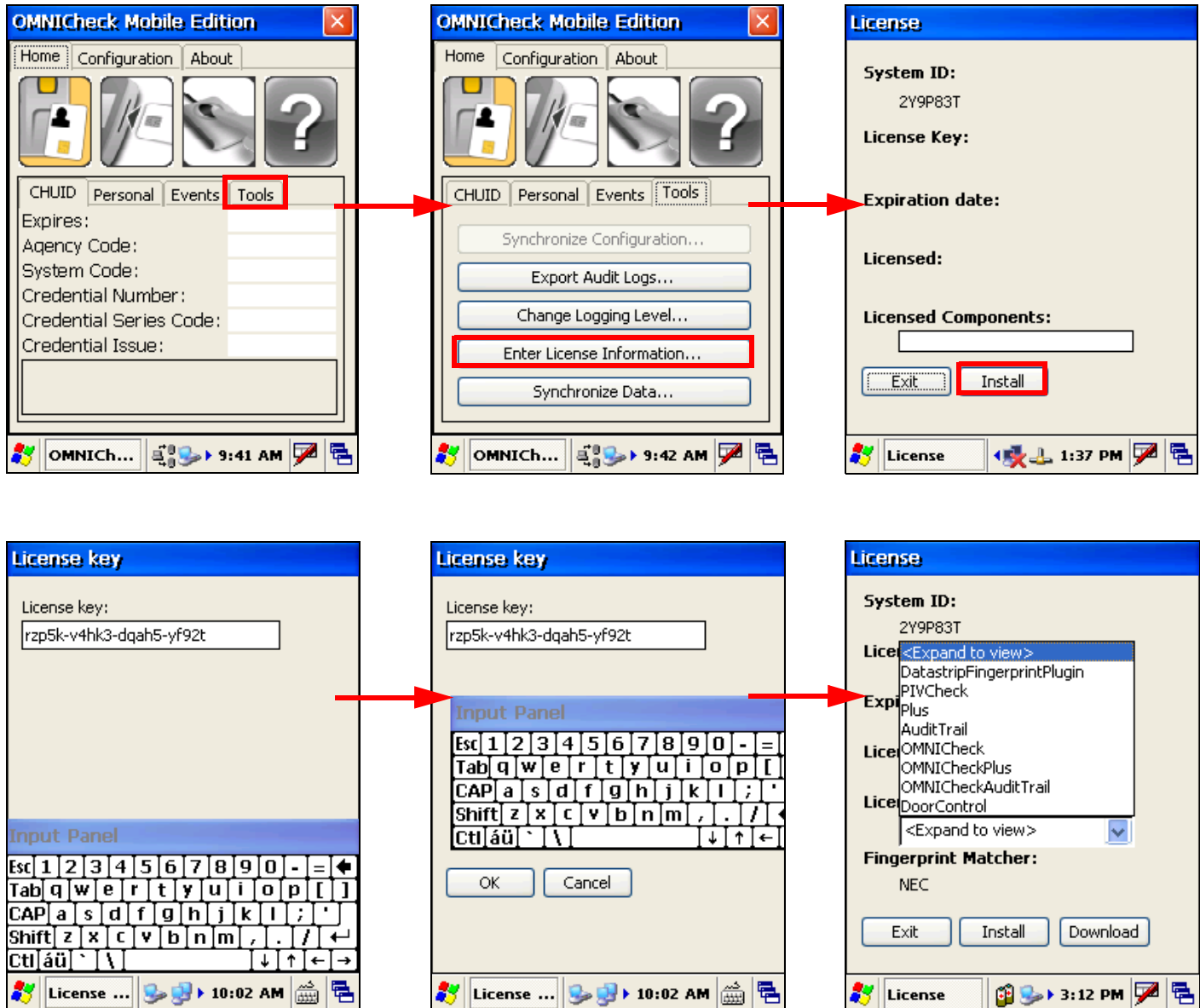
If you wish to evaluate the software for 30 days, press the *Download license key* button. The trial license consists of a fully functional *OMNlCheck*. If you have purchased and registered the product then the online licensing service will reissue your full license, and the *Licensed successfully installed*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



OMNlCheck Plus 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.



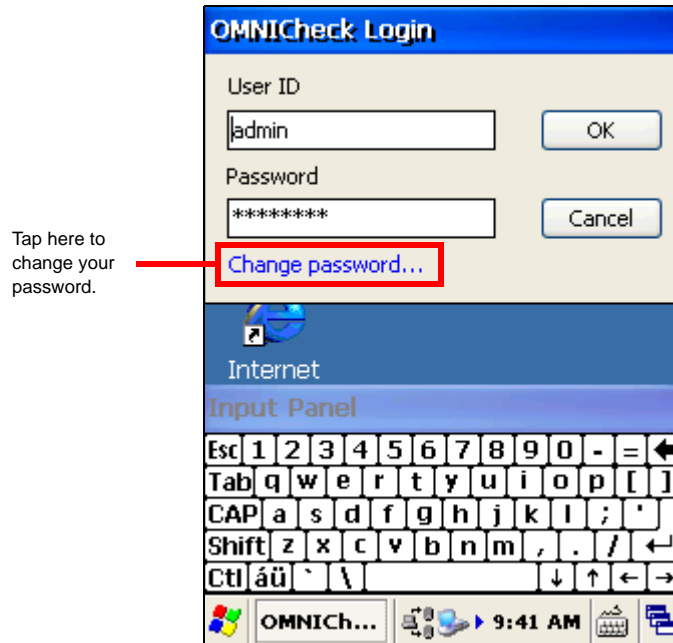
If OMNlCheck software has been pre-installed by the terminal manufacturer, then the license key you received with your mobile biometric terminal is synched with the device's unique *system ID*.

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.

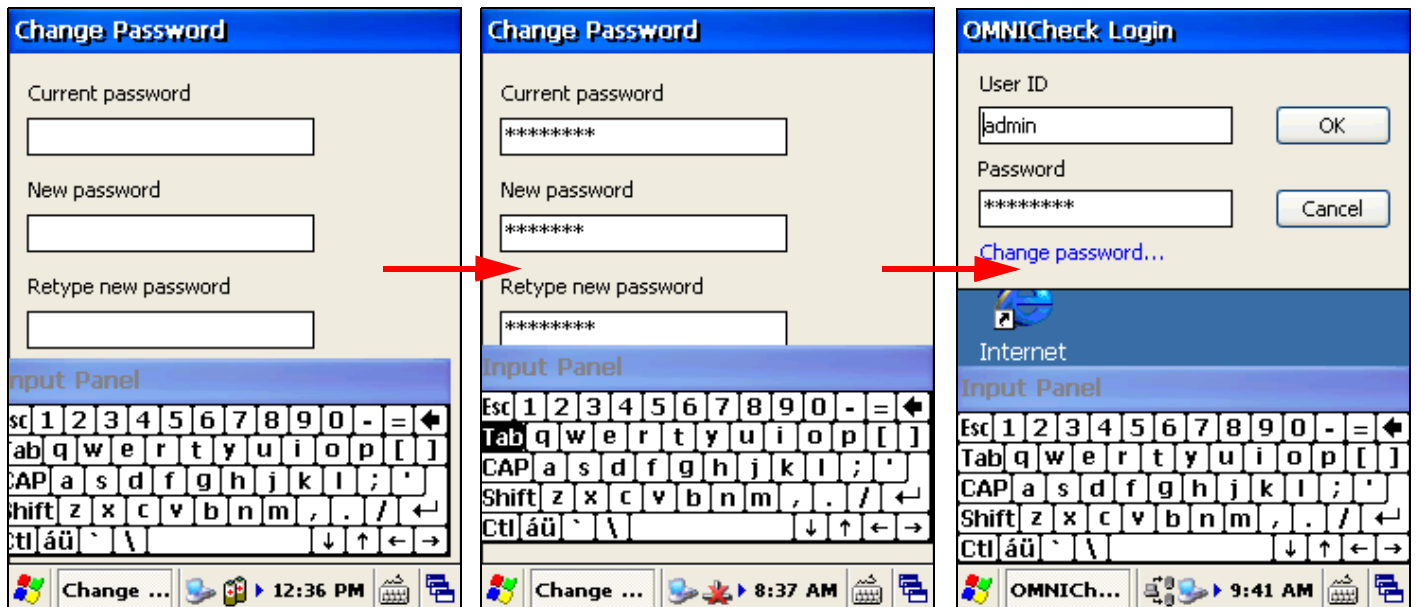
The license key field is now populated, indicating you have successfully licensed OMNlCheck. Press the *Exit* button to return to the *Application Configuration* dialog.

CHANGING THE ADMIN 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 *OMNICheck*. After the splash screen displays, you will see the *OMNICheck Login* dialog.

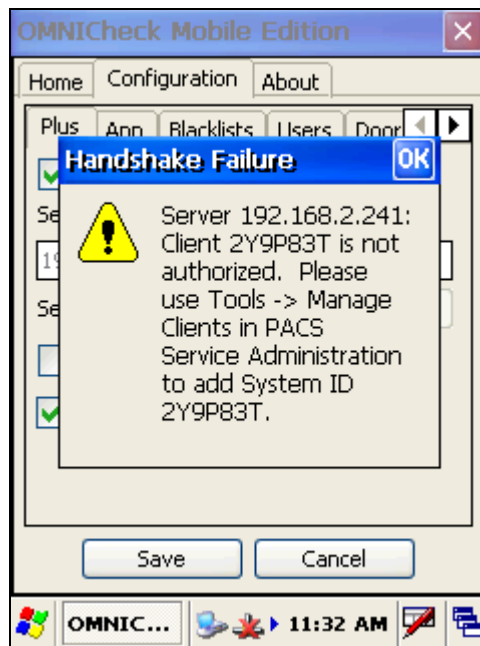


For each field, use your stylus to set the cursor position, and then use the input panel to enter your current password and new password. Next, tap the *Tab* key which dismisses the input panel and reveals the *OK* and *Cancel* buttons. Press the *OK* button to save your new password, and return to the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



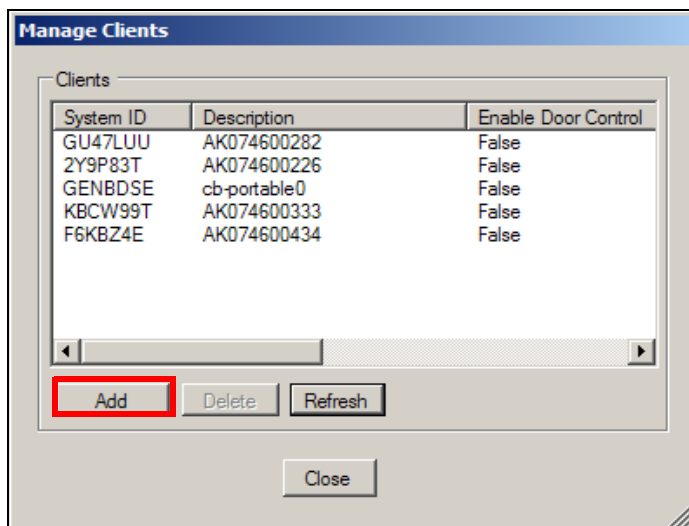
CONFIGURING THE PACS PLUG-IN ON YOUR PC (PLUS ONLY)

PACS Service is a generic term for the vendor-specific *PACS plug-in* that brokers communication between your mobile biometric terminal and the *PACS*. Beginning with *OMNCheck* Release 1.2, all *OMNCheck* clients must be pre-authorized by a *PACS Service* before they can connect for the purpose of uploading audit records and downloading TPKs and person data. A client is uniquely identified by its *System ID*. If the client is not yet authorized, the following message is displayed when you attempt to test the server connection.

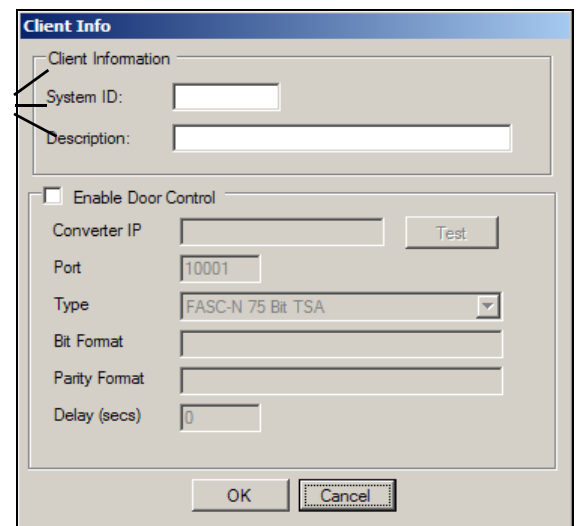


AUTHORIZING CLIENT CONNECTIONS

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:



Fill in the necessary information,



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

Client Info

Client Information

System ID: 43X9C4U

Description: AK074900507

☐ Enable Door Control

Converter IP: Test

Port: 10001

Type: FASC-N 75 Bit TSA

Bit Format:

Parity Format:

Delay (secs): 0

OK Cancel

Manage Clients

Clients

System ID	Description	Enable Door Control
GU47LUU	AK074600282	False
2Y9P83T	AK074600226	False
GENBDSE	cb-portable0	False
KBCW99T	AK074600333	False
F6KBZ4E	AK074600434	False
43X9C4U	AK074900507	False

Add Delete Refresh

Close

On the client, tap the *Configuration* tab. Then select the *Plus* tab. Type in the IP address or name of the computer running the PACS Service and click the *Test* button. If your configuration is correct, the following message will be displayed.

OMNICheck Mobile Edition

Home Configuration About

Plus App Blacklists Users Door

☒ Enable Online Mode

Server: 192.168.1.100

Server:

☐ Ser

☒ Look

Test Results OK

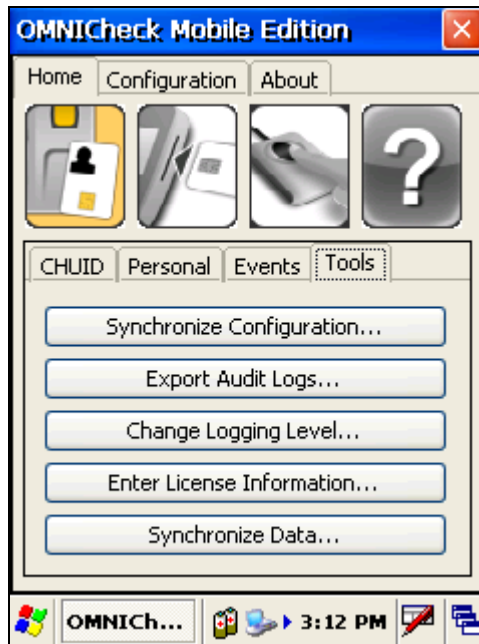
The attempted connection to the server was successful and the server's key was downloaded.

Save Cancel

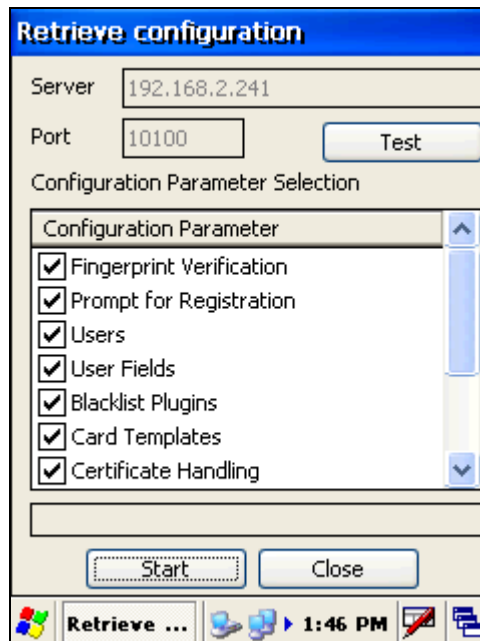
OMNIC... 12:09 PM

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.

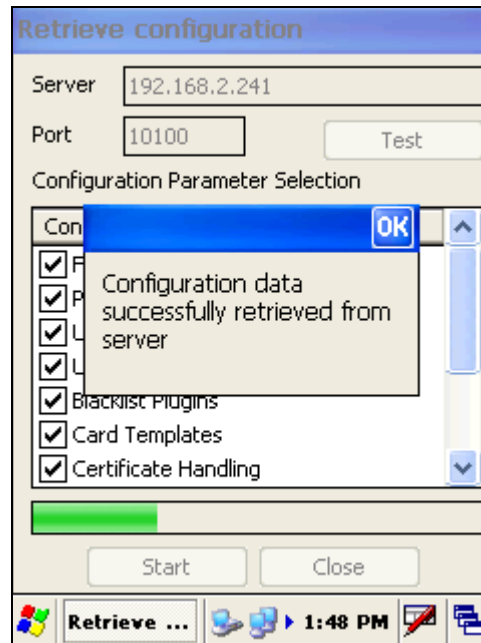


You can test your connection first, if desired.



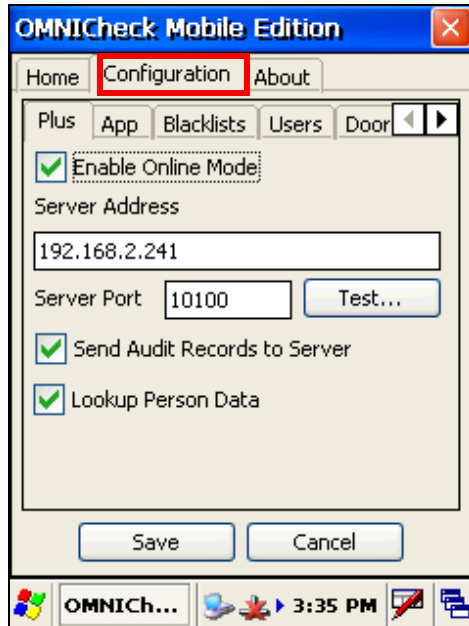
Select which settings you wish to download and tap the *Start* button to commence downloading the configuration profile from the PACS service.

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




MANUALLY CONFIGURING THE OMNICHHECK MOBILE DEVICE

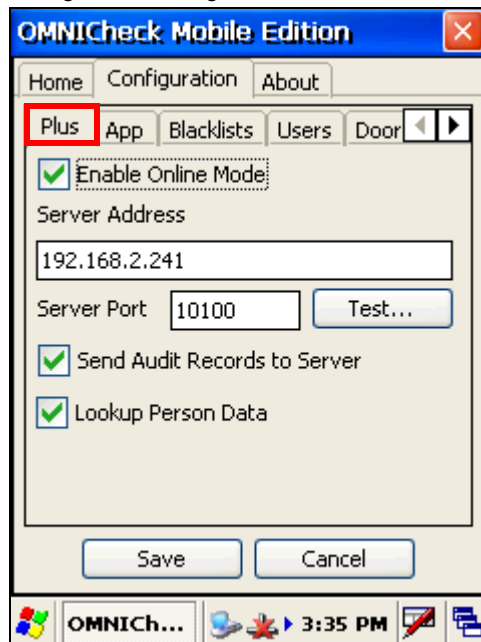
To configure your mobile biometric terminal, tap the *Configuration* tab. The five sub-tabs which appear are labeled *Plus*, *App*, *Blacklists*, *Users* and *Door Control*. We will address each configuration area in turn.



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 24.

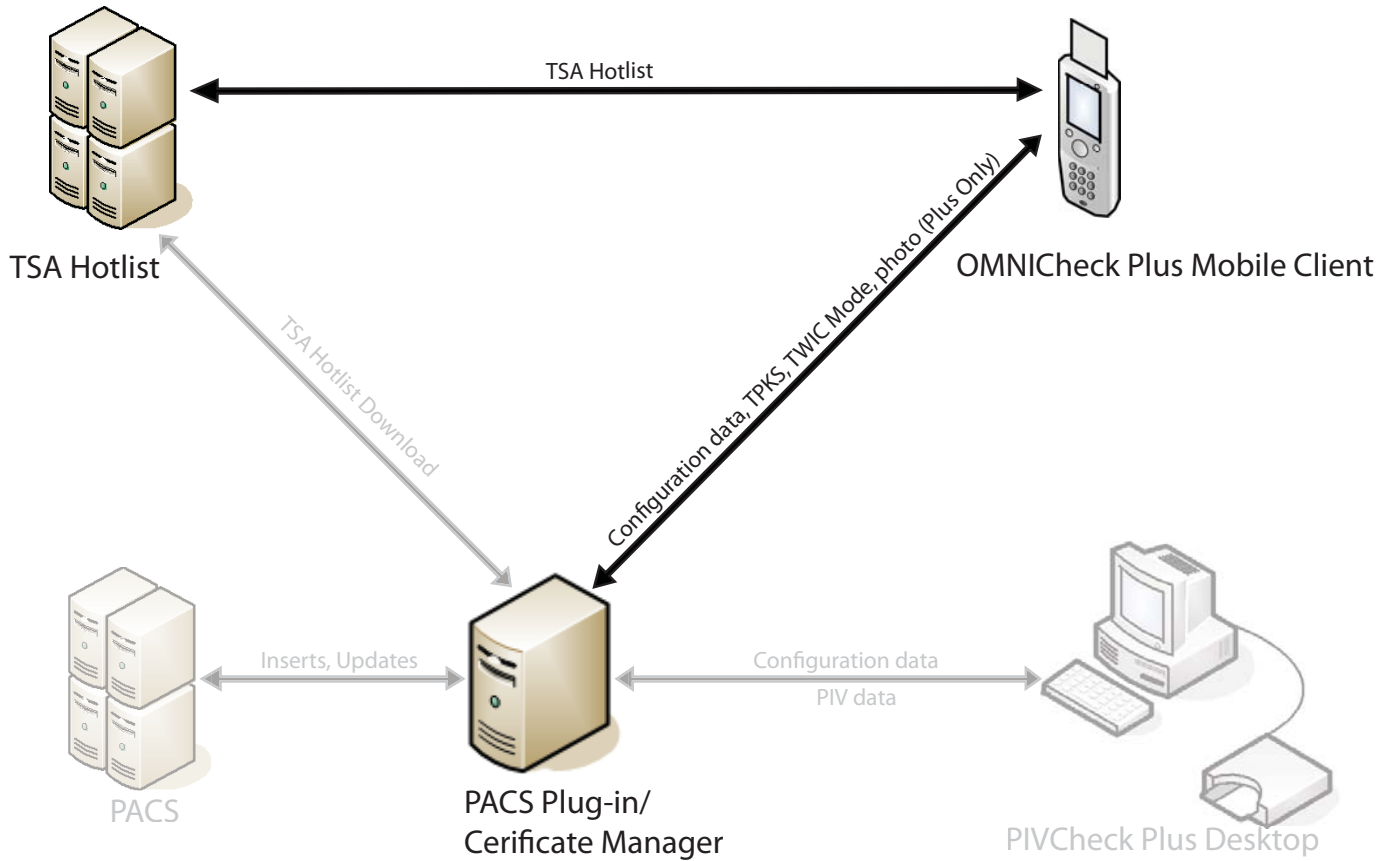
Select the *Plus* tab to view the PACS service configuration dialog.



REGISTRATION HANDLING

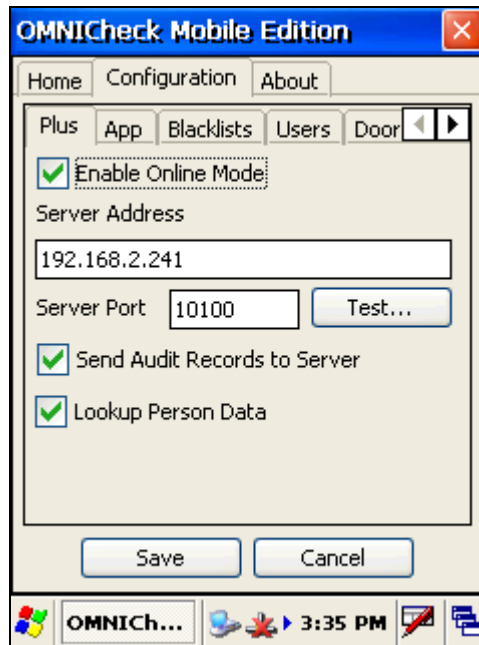
All OMNlCheck devices configured with the *Audit Trail* or *Plus* options at a given site communicate with a single OMNlCheck Service Plug-in running on a server PC. An OMNlCheck Services Plug-in running on a server is hereafter referred to as the OMNlCheck Server. PIVCheck PACS Services Plug-ins can also communicate with OMNlCheck Plus Edition clients. This means that if the site is using PIVCheck Plus Desktop Edition or OMNlCheck Plus to register TWICs into a PACS database, the existing PACS Plug-in can communicate with your OMNlCheck clients.

Refer to the graphic below for a visual understanding of how the communication process works.



ENABLE ONLINE MODE

When the *Enable Online Mode* is selected, the *OMNICheck Plus Edition* device can communicate with the TWIC Server configured at your site.



This section assumes you have successfully configured your *OMNICheck Plus Edition* device to communicate over a LAN or Wi-Fi network.

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.



SEND AUDIT RECORD TO SERVER

If this is selected, audit records, which include the following items, are transmitted in real time after each transaction to the sites TWIC Server.

- Start Date and Time
- TWIC Authentication Mode
- CHUID FASC-N
- Card Holder Name
- Expiration Date and Time
- Number of PIN attempts (including first)
- CHUID Check Verification Date and Time
- CHUID
- Check Results (OK, Bad, or Not Checked)
- Biometric Comparison Results (Match, No Match, or Not Configured)
- Biometric Matcher Type (NEC, Identix)
- Biometric Match Score (of first successful match)
- Biometric Match Failure Count

- 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)
- Added (to database) Date and Time
- Error Description

LOOKUP PERSON DATA

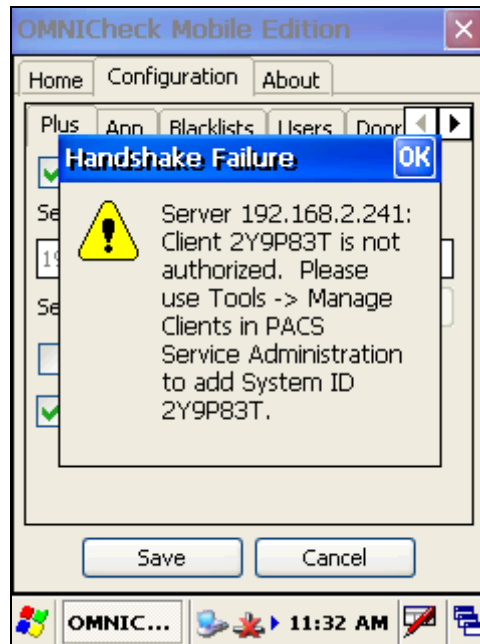
If this is selected, configuration data such as TPKs, TWIC mode and photos are transmitted in real time directly to the *OMNICheck Plus Edition* mobile device.

PACS CONNECTION FAILURES

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

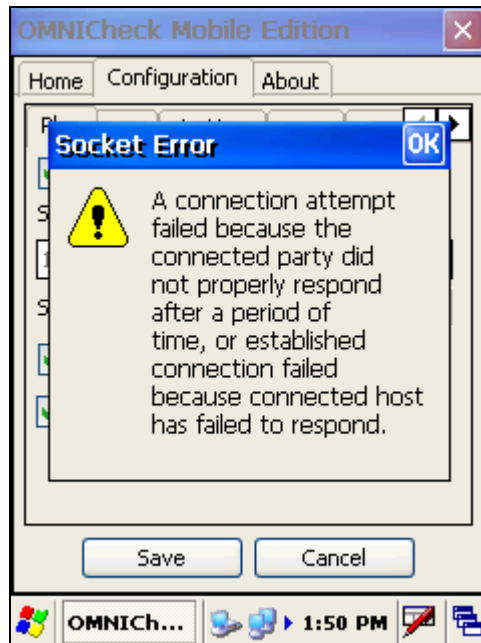
CLIENT NOT AUTHORIZED

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.



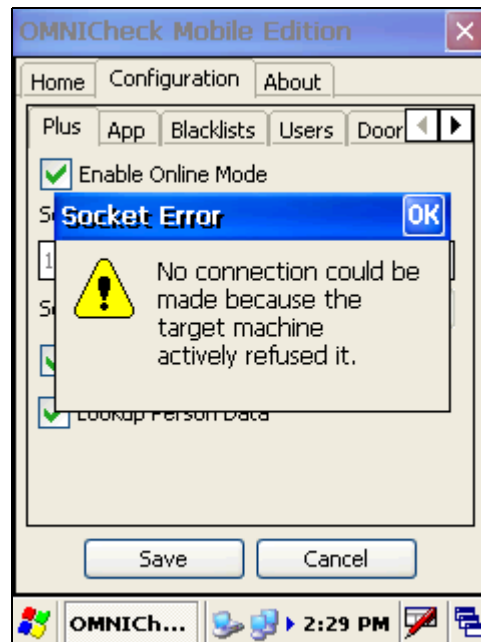
INCORRECT SERVER IP ADDRESS OR NETWORK ROUTING PROBLEM

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. Check that the server address is correct, then try again.

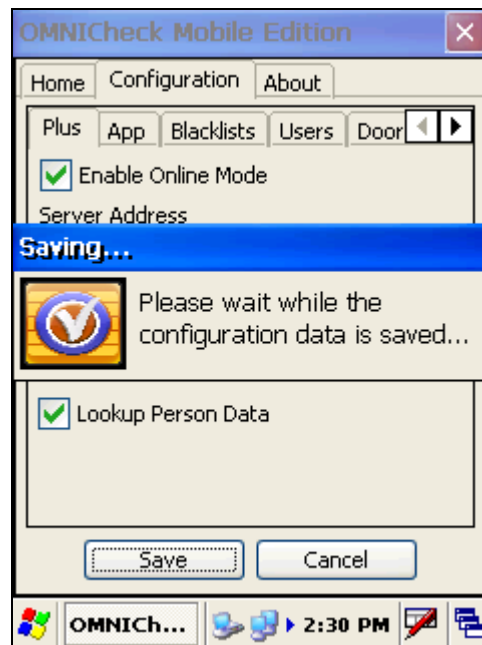


SERVER EXISTS BUT PACS SERVICE IS NOT RUNNING

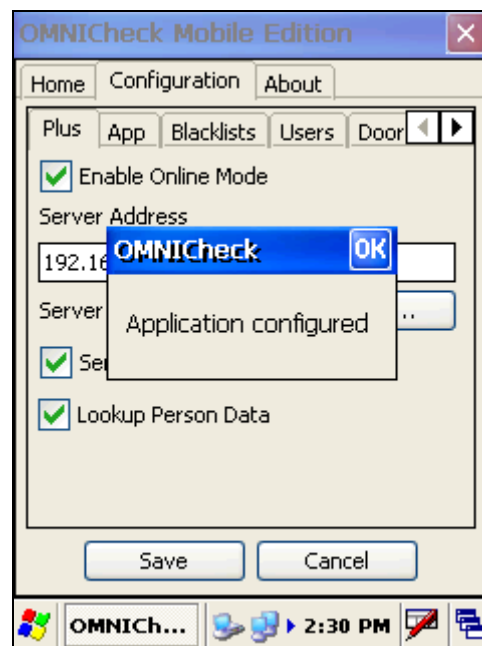
This message occurs when the PACS Service is not running. If you have the PACS Service installed, open the application then start the service. Once the PACS Service starts try pressing *Test* again. For more information on setting up your PACS Service refer to the *PACS Plug-in Administration Guide* for your PACS.



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



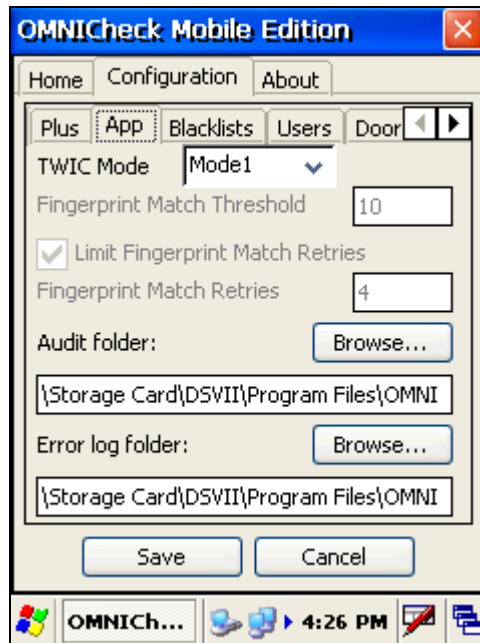
When the configuration has been encrypted and stored on the device the following message is displayed:



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

APPLICATION TAB

OMNlCheck contains several configurations located under the *App* tab. These configurations include *Fingerprint options*, *PIN options*, *Audit log folder location*, and *Error log folder location*. OMNlCheck presents application configuration options under the *App* tab: *TWIC authentication modes*, *fingerprint matching options*, and *folder locations*.



TWIC AUTHENTICATION MODES

The TSA has defined the following TWIC authentication modes to assist sites in creating their own security policies. The following table, "TWIC authentication modes," was extracted from the TWIC Reader Hardware and Card Application Specification Version 1.1.1, May 2008:

Select the desired authentication mode from the TWIC mode drop-down. For more information refer to Appendix C "TWIC Authentication Modes" on page C-1.

Mode	Identification/ Authentication	Definition
1	CHUID Verification	Provides verifiable identification factor, assuming the CHUID digital signature is either verified once, when the user's CHUID is registered in the PACS or that the CHUID is verified each time it is accessed from a TWIC card. Refer to "Reference Documents" on page A-91.
2	Active Card Authentication	Provides single factor authentication at the same level of security as for a PIV Card Authentication operation. The FASC-N and expiration date are present in the Card Authentication certificate which obviates the need to read the CHUID. Refer to "Reference Documents" on page A-91.
3	CHUID Verification + Biometric User Authentication	The cardholder's live biometric sample is compared to a stored biometric reference. The biometric reference template may be read from a TWIC card at each use or stored in the PACS system during PACS registration of the user. Provides single factor authentication. Refer to "Reference Documents" on page A-91.
4	(CHUID) Signing Certificate + Active Card Authentication + Biometric User Authentication	Provides two factor authentication. Refer to "Reference Documents" on page A-91.
Non-TWIC	CHUID Verification + PIN Verification + Biometric User Authentication	<p>PIV Cards - Provides verifiable identification factor, assuming the CHUID digital signature is either verified once, when the user's CHUID is registered in the PACS or that the CHUID is verified each time it is accessed from a Non-TWIC card. The cardholder's live biometric sample is compared to a stored biometric reference. The biometric reference template may be read from a Non-TWIC card at each use or stored in the PACS system during PACS registration of the user.</p> <p>Non-PIV - PIN verification</p>



Note that for modes one (1) and two (2), that the fingerprint match threshold and fingerprint retry limit fields are disabled.

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 *OMNCheck* 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.

<i>Mobile Biometric Terminal</i>	<i>Biometric Template Matcher</i>	<i>Lowest Recommended Threshold</i>
DAP CE3240BWE	Innovatrics	12300
Datastrip's DSV3	Identix	10
Datastrip's DSV2+ ^{TURBO}	Identix	10
Datastrip's DSV2+ ^{TURBO}	NEC	1400
Cross Match Be.U Mobile	Innovatrics	12300
MaxID IDLMAX	Innovatrics	12300
Intermec CN3e	MorphoTrak	9000

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

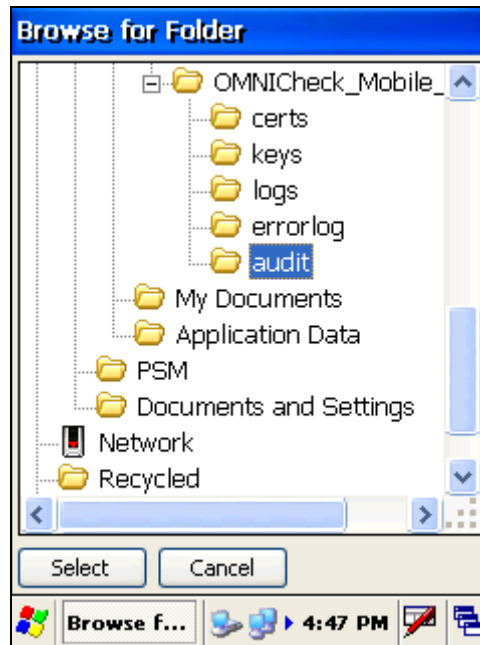
Checking this option will cause *OMNCheck* to reject any cardholder after a user-defined number of biometric matching attempts.

FINGERPRINT MATCH RETRIES

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

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 *OMNICheck*. 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.



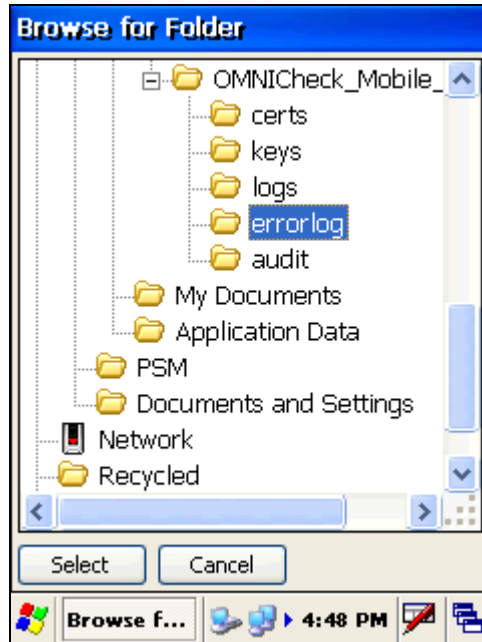
The file name will always be named `Activity.paf`.

ERROR LOG FOLDER

The error log contains information about errors that the *OMNICheck* 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 *OMNICheck*. 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 *OMNICheck* folder. The format of this file is:

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

AUTOMATIC ROLLOVER

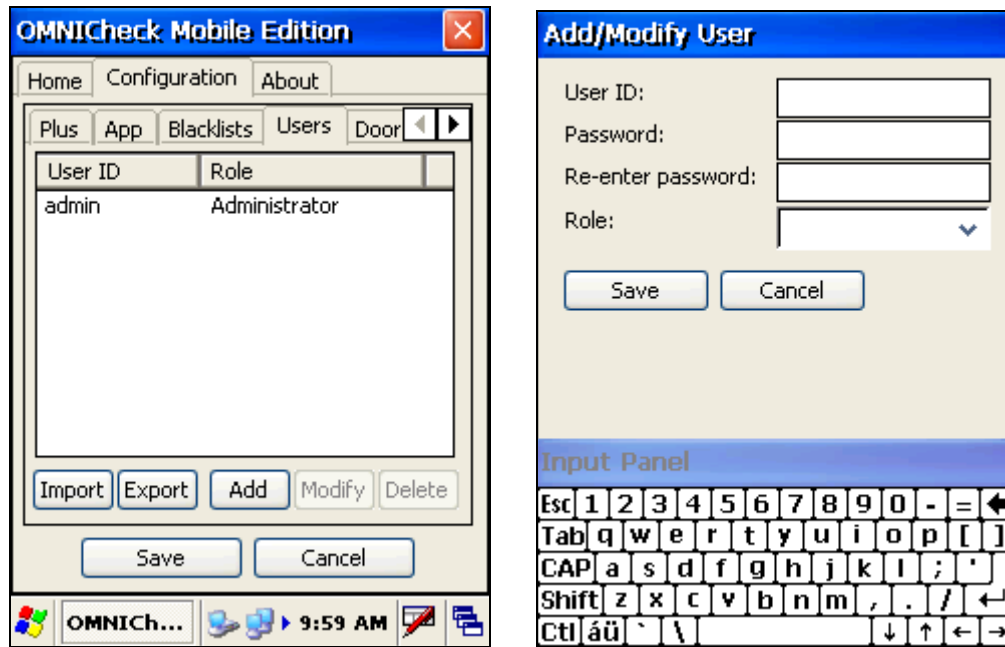
The current day's trouble ticket file is named `Errors.txt`. However, as of Release 1.2.18.0, this file is created each day after renaming the previous days' file to `Errors.<yyyymmdd>.txt` where `yyyymmdd` are the year, month, and day corresponding to the file's entries. The application stores up to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

BLACKLIST PLUG-INS

For more information refer to the *Blacklist_Plug-in_User_Guide.pdf*. This manual is stored in the *OMNICheck* 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.

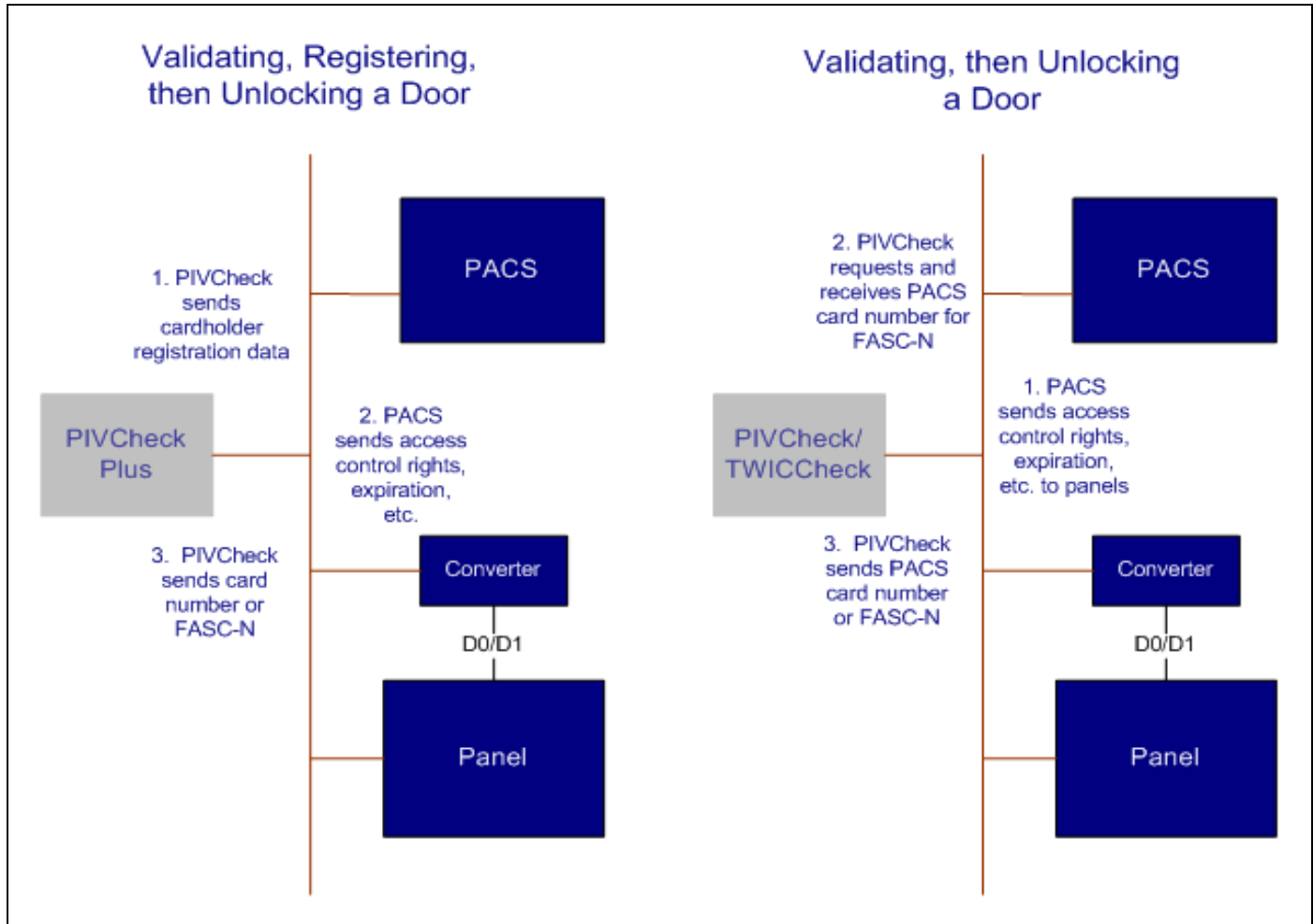
ROLE

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 *TWIC* 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.



DOOR CONTROL CONFIGURATION FORM

The door control configuration form is shown below.

OMNITCheck simply reports the appropriate card number to the panel. The access control panel or its host ultimately decides whether a door or gate should be unlocked.

ENABLE DOOR CONTROL

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

CONVERTER IP

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

TEST

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

PORT

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

TYPE

Two categories of card messages are supported:

- FASC-N or derivatives
- PACS card numbers

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 *OMNITCheck* and *OMNITCheck Plus*. The following FASC-N Wiegand formats are available:

- 200-bit
- 75-bit GSA
- 75-bit TSA
- 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 *OMNICheck Plus*. 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

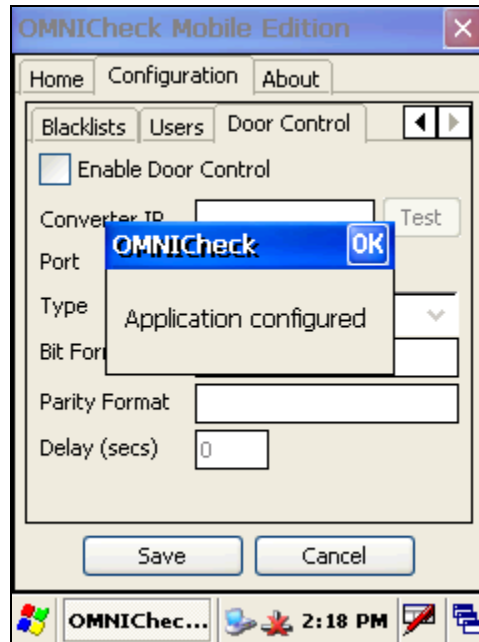
The parity format shows which bits will be used in the calculation of odd and even parity.

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.

SAVING YOUR CONFIGURATION

Press the **Save** button to store your application choices. If the application is configured successfully, the following popup dialog will appear.



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

IDENTITY VERIFICATION

The *OMNICheck* application employs one- and two-factor authentication to validate a cardholder. Something you have and something you are. The identity verification and credential authentication process is described in detail within this chapter.

ICONS



Contactless State

The reader switches to the contactless state whenever it is idle and a new card is presented to the outside of the unit as shown in the graphic shown to the left.



Contact State

The reader switches to contact state under the following two conditions:

- The operator inserts a TWIC or Non-TWIC card into the contact reader
- The reader is in TWIC Authentication Mode 3 or 4 and needs the cardholder's TWIC privacy key (TPK) to decrypt their biometric template.



Biometric Scan

- The reader is in TWIC Authentication Mode 3 or 4 and is prompting the cardholder to place his finger on the sensor.



Not Authenticated

This is the result of one of the following conditions:

- Card read error
- Expired TWIC
- Invalid CHUID signature
- Invalid (possible forged or cloned) card
- Invalid PIN
- Biometric mismatch
- FASC-N is on the TSA Hotlist
- Operator cancels the verification



Authenticated

The card was determined to be valid using the methods prescribed for the given TWIC authentication mode. The following is known:

- CHUID is valid (Authentication Modes 1, 3 and 4)
- PIN Verification
- TWIC is not expired (in all TWIC Authentication Modes)
- TWIC is not forged or cloned (in TWIC Authentication Modes 2 and 4)
- Cardholder is linked to the TWIC (in TWIC Authentication Modes 3 and 4)
- TWIC has not been revoked (in all TWIC Authentication Modes)

CHUID AND ACTIVE CARD AUTHENTICATION

CONTACTLESS STATE

When a TWIC or Non-TWIC is held against the right-hand side of the mobile biometric terminal for more than one second, the contactless state icon will flash. Hold the TWIC or Non-TWIC steady while the icon is flashing. If the TWIC or Non-TWIC is removed from the proximity of the reader in mid-read, an error will occur, and the *Not Authenticated* icon will be displayed.

When the contactless state icon stops flashing a completion chime will be heard. At this point the operator can remove the card from the proximity of the reader.

- 1 In TWIC Authentication Modes 1, 3, and 4 the TWIC's CHUID signature is compared with the TWIC certificate authority. If the CHUID signature is invalid then the *Not Authenticated* icon will be displayed. In TWIC Authentication Modes 2 and 4, a cryptographic challenge is issued to the card. If the response to the challenge is incorrect, then the *Not Authenticated* icon will be displayed.
- 2 The expiration date is compared with the current date. If the expiration date is greater than the current date then the *Not Authenticated* icon will be displayed.

Whenever *OMNCheck* detects a card on the contactless interface when configured for TWIC Authentication Modes 3 and 4, it queries the local device's TPK database to determine whether a TPK already exists for that card. If the TPK is found, then there is no need to obtain it from the magnetic strip or from the contact interface. If the TPK is not found then the contact state icon will begin flashing. Insert the card into the contact slot and refer to "Contact Mode".

CONTACT MODE

When a TWIC is inserted into the smart card reader, the contact state icon will flash while it reads the card. Do not remove the card while the contact state icon is flashing or an error will occur, and the *Not Authenticated* icon will be displayed.

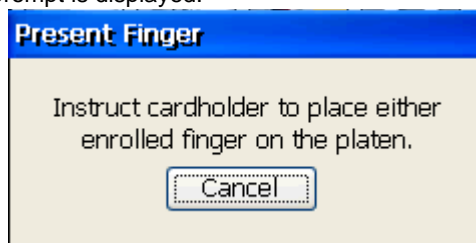
When the contact state icon stops flashing, the completion chime can be heard, and the operator can remove the card.

- 1 The TPK and fingerprint templates are extracted.
- 2 In TWIC Authentication Modes 1, 3, and 4 the TWIC's CHUID signature is compared with the TWIC certificate authority. If the CHUID signature is invalid then the *Not Authenticated* icon will be displayed. In TWIC Authentication Modes 2 and 4, a cryptographic challenge is issued to the card. If the response to the challenge is incorrect, then the *Not Authenticated* icon will be displayed.
- 3 The expiration date is compared with the current date. If the expiration date is greater than the current date then the *Not Authenticated* icon will be displayed.

BIOMETRIC VERIFICATION

FINGERPRINT CAPTURE

Once the card has been read, the following prompt is displayed:



As the prompt suggests, assist the cardholder to place their finger on the scanner as indicated.

FINGERPRINT MATCH

After a few seconds, the biometric template generator 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 28.

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.



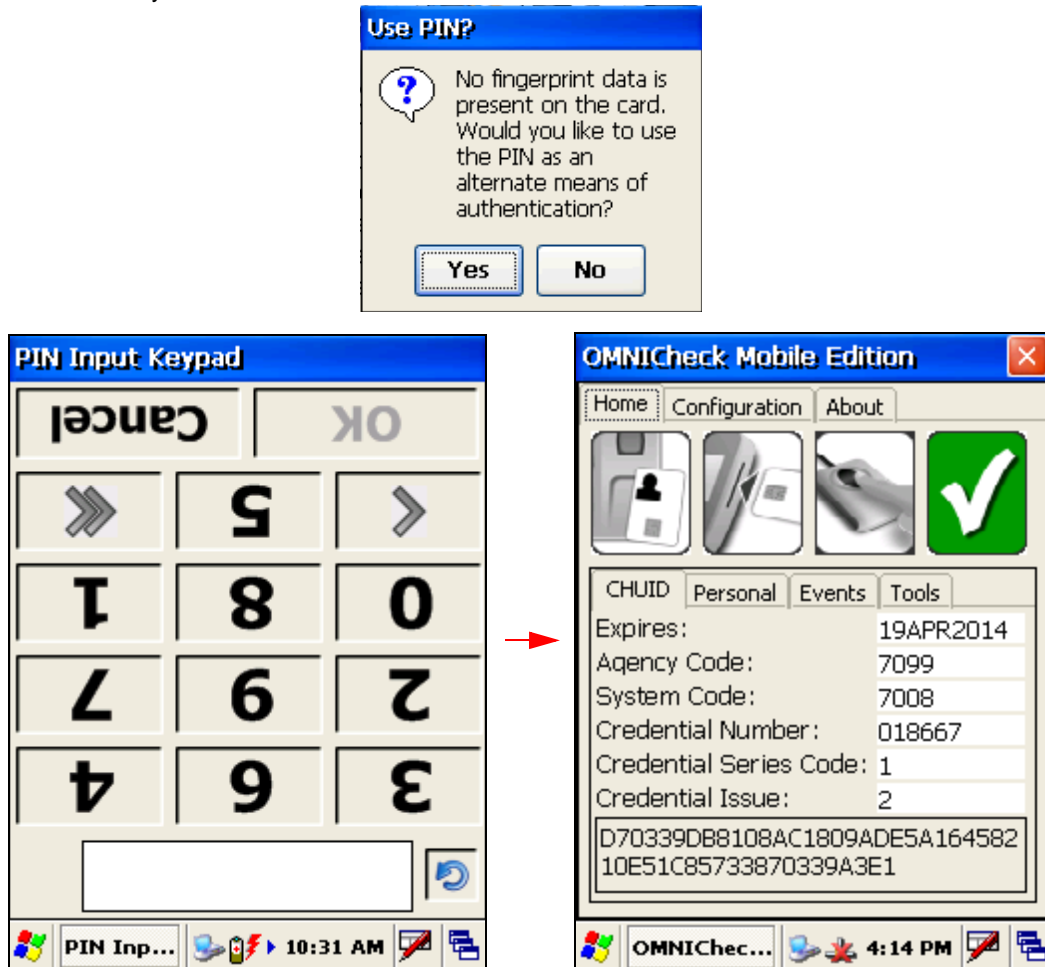
If you tap the *Yes* button, the cardholder can present their finger again. This can repeat for as many retries are available. If you tap the *No* button, both the *Events* tab and the *Not Authenticated* icon confirms the cardholder is not authenticated.

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



ZERO BIOMETRIC CARD

OMNCheck can prompt for a PIN to validate cardholders whose card contains a special CBEFF that indicates that zero fingerprint templates are stored on the card. When OMNCheck encounters a zero biometric card, it pops up the message, "No fingerprint data is present on the card. Would you like to use the PIN as an alternate means of authentication?"



If the card was presented in contactless mode, then the operator is prompted to insert the card. The PIN pad is displayed, prompting the cardholder to enter their PIN.

A valid PIN unlocks the card and shows the cardholder's name and photo which completes the verification.

NON-TWIC MODE

When the authentication mode is set to Non-TWIC, OMNCheck can validate any PIV, CAC, FRAC and Legacy CAC credential. OMNCheck will compare the CHUID signature with the Non-TWIC certificate authority, prompt for a PIN if the card is locked, check for biometrics stored on the card and check fingerprints if available.

CERTIFICATE VALIDATION

If the PKI plug-in is enabled, then the card's certificates are validated.

THE CARD DATA WINDOW

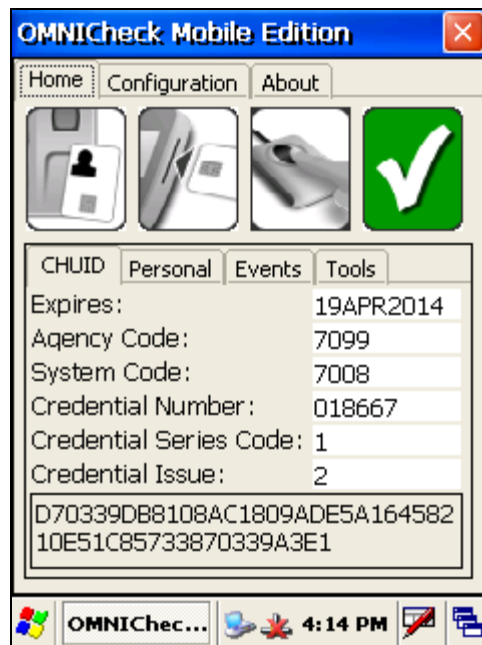
Once a cardholder's certificates have been validated, the *Card Data* window displays the cardholder's photograph, first, middle, and last name, FASC-N, GUID, Expiration Date, and other user-configurable data.

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 is positively verified, the Authenticated icon flashes, indicating the cardholder was authenticated.



Non-TWIC Identity Verification

Using Non-TWIC mode, *OMNCheck* can validate PIV compliant smart cards and legacy CAC credentials. In non-TWIC mode, PIV cards will be authenticated as required by FIPS-201. Non PIV compliant cards will be validated using the features that the card supports.



Please note, not all features are available for all cards.

ICONS



Contactless State

The reader switches to the contactless state whenever it is idle and a new card is presented to the outside of the unit as shown in the graphic shown to the left.



Contact State

The reader switches to contact state under the following two conditions:

- The operator inserts a smart card into the contact reader



Biometric Scan

- The reader is in Non-TWIC Authentication Mode and is prompting the cardholder to place his finger on the sensor.



Not Authenticated

This is the result of one of the following conditions:

- Card read error
- Expired smart card
- Invalid CHUID signature
- Invalid (possible forged or cloned) card
- Invalid PIN
- Biometric mismatch
- Operator cancels the verification



Authenticated

The card was determined to be valid using the methods supported by the card. The following is known:

- CHUID is valid (When using a PIV card)
- PIN Verification (Only for cards which are PIN protected. and the card is inserted in the contact interface)
- Smart card is not expired
- Smart card is not forged or cloned
- Smart card has not been revoked

CHUID AND ACTIVE CARD AUTHENTICATION

CHUID VERIFICATION

A Card Holder-Unique Identifier (CHUID) is one of the specified requirements in FIPS 201. The CHUID identifies the individual within the PIV system. Elements contained within the CHUID include:

- Federal Agency Smart Credential Number (FASC-N).
- Expiration date - the expiration date data element shall specify when the card expires.
- Digital signature of the CHUID - Verified to ensure that the card hasn't been tampered with.

CONTACTLESS STATE

When a PIV compliant smart card is held against the right-hand side of the mobile biometric terminal for more than one second, the contactless state icon will flash. Hold the smart card steady while the icon is flashing. If the smart card is removed from the proximity of the reader in mid-read, an error will occur, and the *Not Authenticated* icon will be displayed.

When the contactless state icon stops flashing a completion chime will be heard. At this point the operator can remove the card from the proximity of the reader.

- 1 In Non-TWIC Authentication Mode the CHUID is read from the card and the CHUID details are displayed under the *CHUID* tab.
- 2 The expiration date is compared with the current date. If the expiration date is greater than the current date then the *Not Authenticated* icon will be displayed.

If the PKI plug-in is enabled refer to "Certificate Validation" on page 60.

CONTACT MODE

When a PIV compliant smart card is inserted into the smart card reader, the contact state icon will flash while it reads the card. Do not remove the card while the contact state icon is flashing or an error will occur, and the *Not Authenticated* icon will be displayed.

- 1 The cardholder will be prompted to enter a PIN to unlock the information on the card. For more information see "Entering a PIN to Unlock a Smart Card" on page 55.
- 2 The CHUID is read from the card.
- 3 The expiration date is compared with the current date. If the expiration date is greater than the current date then the *Not Authenticated* icon will be displayed.
- 4 If the card contains any of the following, then it too will be extracted:
 - Photo
 - Name
 - Rank
 - Stored biometric template
- 5 The cardholder will be prompted to place their enrolled finger onto the biometric platen.

When the contact state icon stops flashing, the completion chime can be heard, and the operator can remove the card.

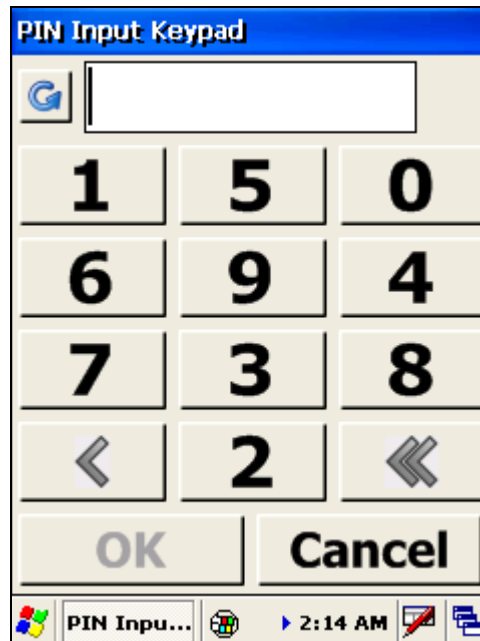
If the PKI plug-in is enabled refer to "Certificate Validation" on page 60.

ENTERING A PIN TO UNLOCK A SMART CARD

Once *OMNlCheck* detects a smart card inserted into the smart card reader, 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.

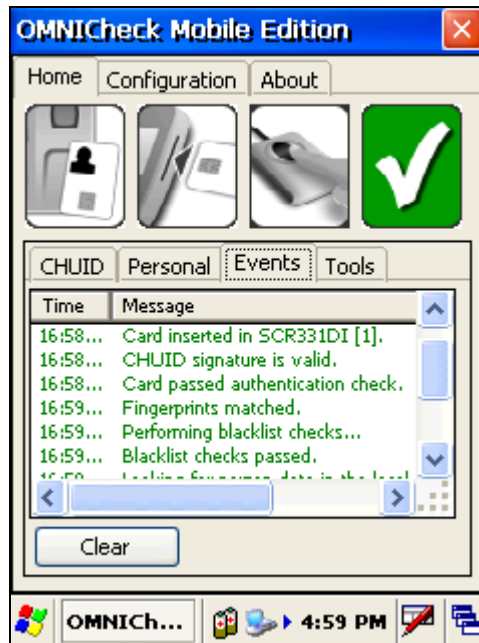


The PIN pad can be transposed to support the point of view of the operator by pressing the *circular blue arrow*.



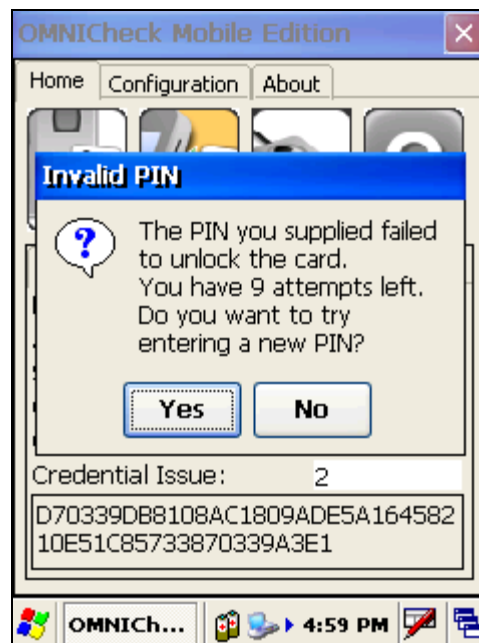
If a PIN is mistyped, individual characters can be erased using the left-pointing arrow (<). All characters in the input field can be erased using the erase button (<<).

Once the PIN is entered and matched with the PIN recorded on the card, *OMNICheck* extracts the CHUID, fingerprint templates and all other available information 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.

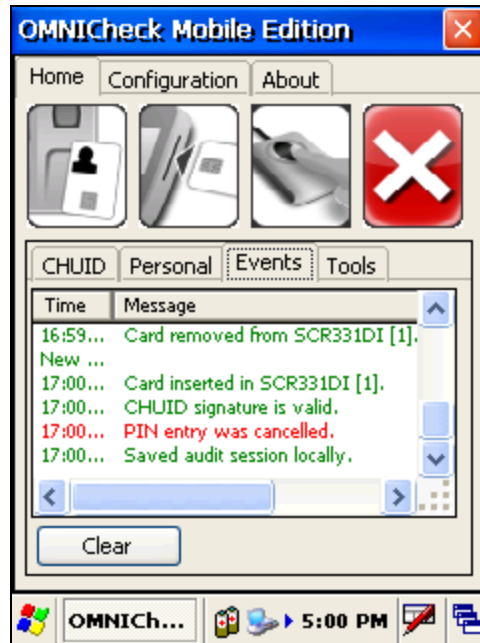


Select **Yes** to redisplay the virtual PIN pad and allow the cardholder to re-enter his or her PIN.



OMNICheck 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

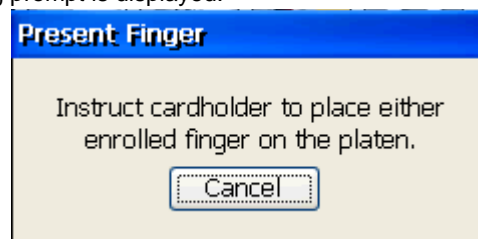
If the PIV PIN is valid all of the information is extracted from the smart card. This includes the following:

- CHUID
- Card Holder Fingerprints and digital signature
- PIV Authentication Certificate

BIOMETRIC VERIFICATION

FINGERPRINT CAPTURE

Once the card has been read, the following prompt is displayed:



As the prompt suggests, assist the cardholder to place their finger on the scanner as indicated.

FINGERPRINT MATCH

After a few seconds, the biometric template generator 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 28.

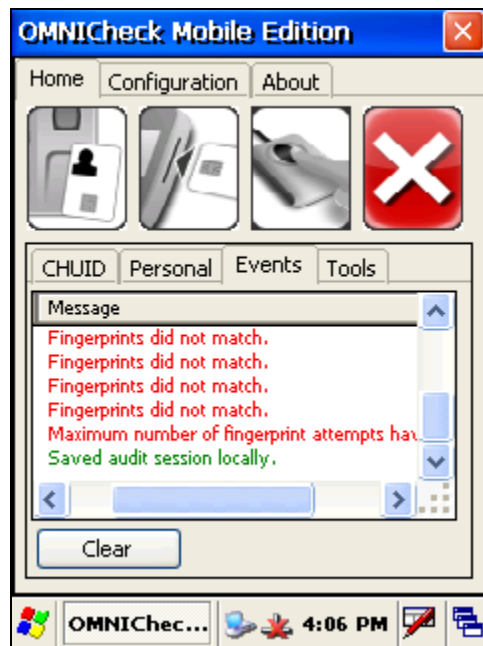
FINGERPRINT MATCH FAILURE

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.



CERTIFICATE VALIDATION



Before *OMNICheck* can use CPV or OCSP to validate the end-entity certificates on a smart card, the local computer's certificate store must be seeded with the issuer CA, intermediate CA (if needed), and the trusted root certificates. If OCSP alone is used, then only the issuer CA certificates are needed. At some sites there may be only one issuer CA certificate for the entire card population. At others, there may be several. The next smart card *OMNICheck* encounters may very well include a certificate whose issuer certificate cannot be located in the local certificate store.

Take caution when adding certificates to your local certificate store. Ensure that the certificate you are adding is from a trusted issuer.

If the PKI plug-in is enabled, then the card's certificates are validated. 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.

PERSONAL TAB

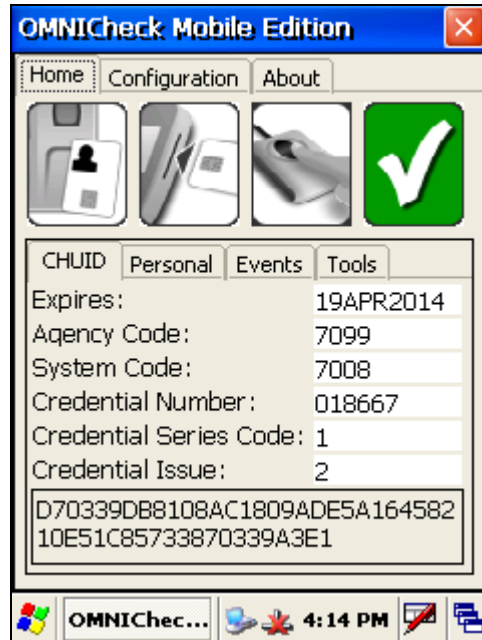
Once a card's data has been read, the *Personal* tab displays the cardholder's photograph, first, middle, last name, and rank.

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.

IDENTITY AUTHENTICATION

Once a card is positively verified, the *Authenticated* icon flashes, indicating the cardholder was authenticated.



LEGACY CAC OR NON-PIV CARDS

CONTACT OR CONTACTLESS

Some cards do not support the use of the contactless interface.

CONTACTLESS

SCENARIO 1

If you place a card against the right-hand side of the mobile biometric terminal for more than one second, the contactless state icon will flash. Hold the card steady while the icon is flashing. If the card is removed from the proximity of the reader in mid-read, an error will occur, and the *Not Authenticated* icon will be displayed.

SCENARIO 2

If you place a card against the right-hand side of the mobile biometric terminal for more than one second, the contactless state icon will flash. If your card is capable of using the contactless interface, but *OMNlCheck* is unable to retrieve vital information from the card, then the contact state icon will flash prompting you to insert the card into the reader.

SCENARIO 3

If you place a card against the right-hand side of the mobile biometric terminal for more than one second and nothing occurs, your card is not capable of using the contactless interface. Please insert your card into the reader.

VALIDATION

In most cases legacy CAC and non-PIV cards do not contain much information to use for validation. *OMNlCheck* will check each card for as much information as possible to validate such as card ID, expiration date and rank.

TOOLS

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

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

SYNCHRONIZE CONFIGURATION (PLUS ONLY)

This feature allows the mobile biometric terminal to be configured by a central host, ensuring that security policies are implemented in a consistent manner. Since network connectivity is required, it is available in the *Plus* edition only. For more information refer to “Synchronize Configuration (Plus Only)” on page 17.



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

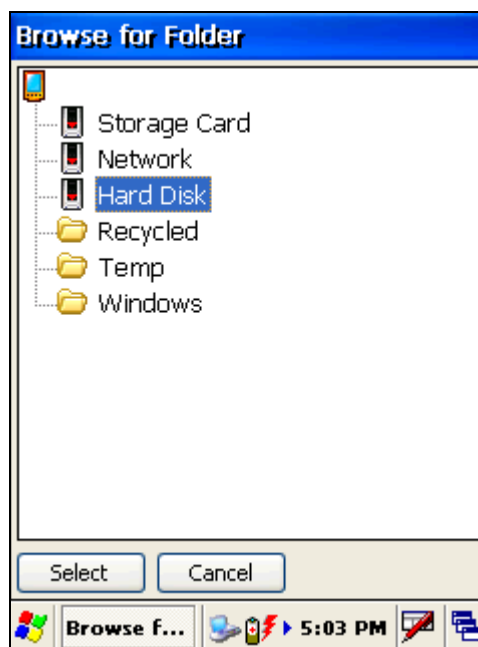
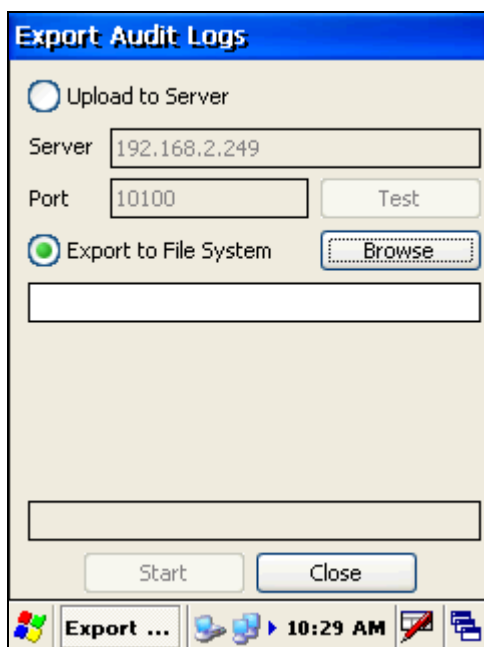
Whenever a card is inserted and the PIN is matched, a new activity transaction begins. The following information is available for each transaction:

- 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)

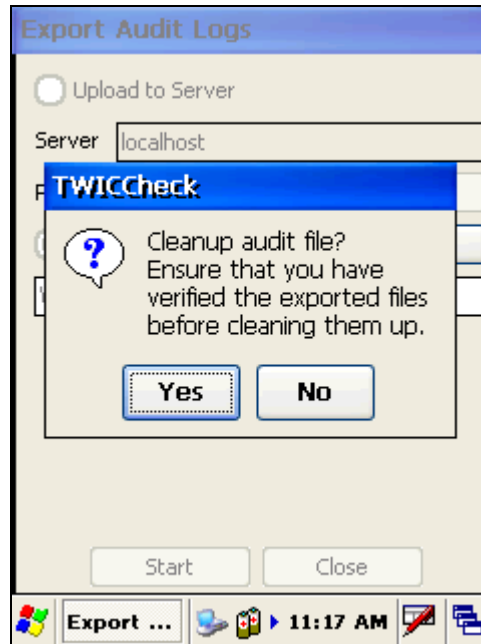
EXPORTING AUDIT LOG TO FLASH DRIVE

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.



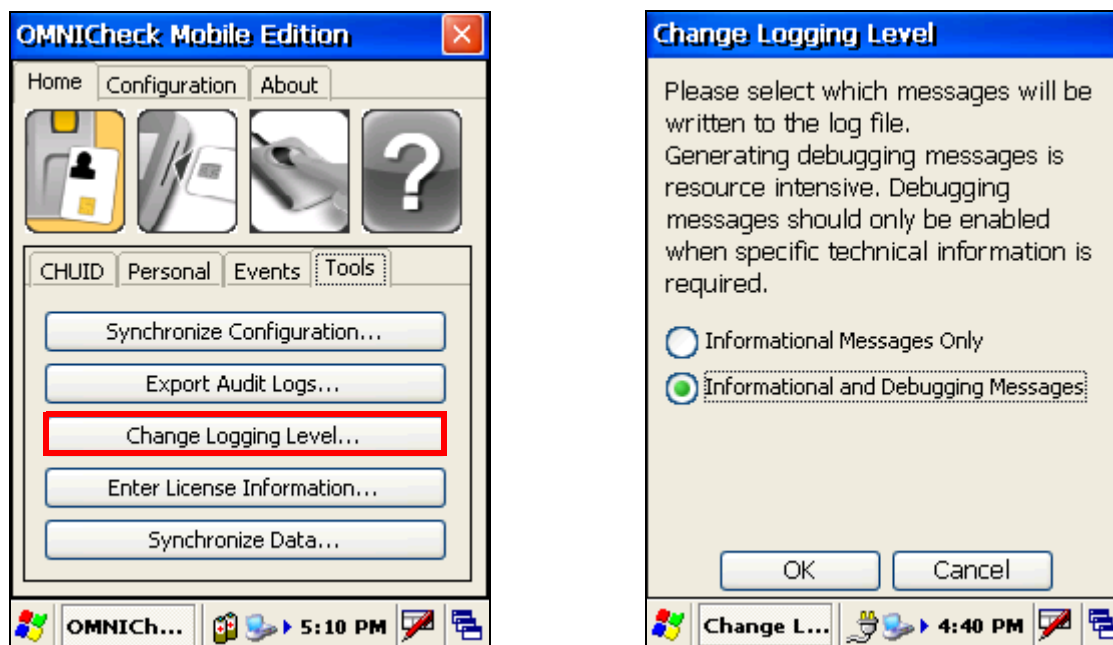
AUDIT LOG FILE CLEANUP

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.

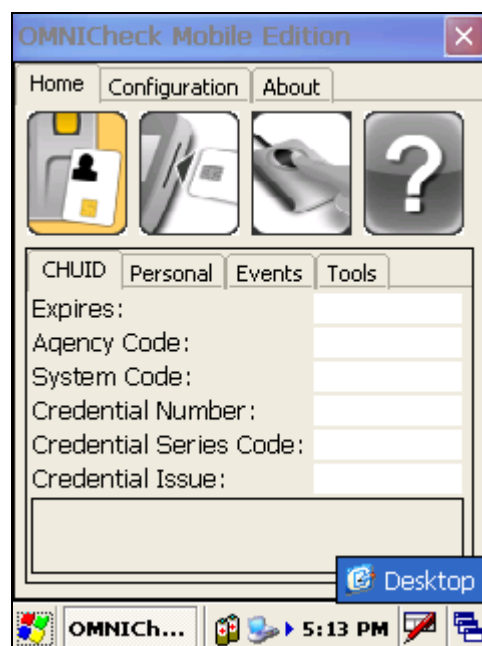


CHANGE DIAGNOSTIC LOGGING LEVEL BUTTON

This is an advanced feature designed to help debug cards that appear to be incompatible. In the event *OMNCheck* 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*.



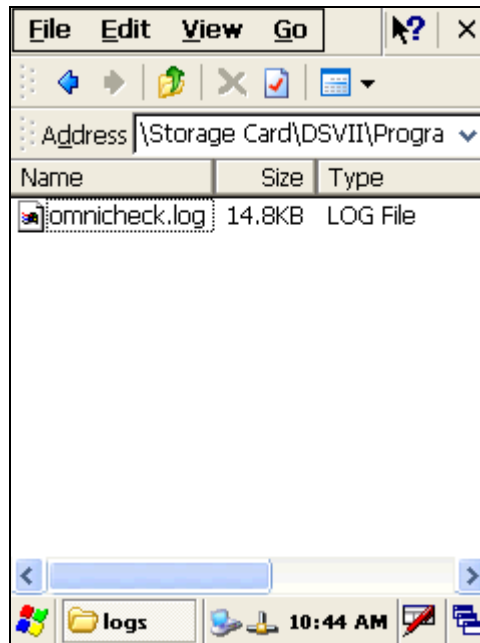
Re-insert the card and repeat the operation that failed. Change the logging level back to *Informational Messages Only*. Then locate the log file by tapping on the icon in the extreme lower right corner and switching to the Desktop.



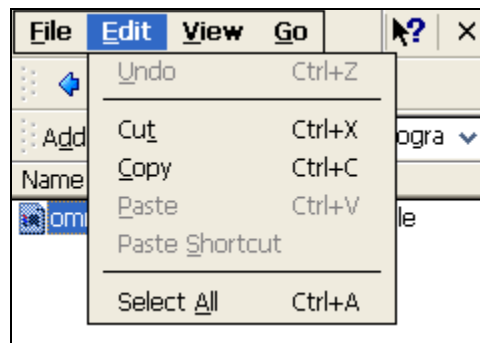
Insert a flash drive into one of the two USB ports on the top of the DSVII. Tap on *My Device* and navigate to the following folder:

`\Storage Card\DSVII\Program Files\OMNICheck_Mobile_Edition\logs`

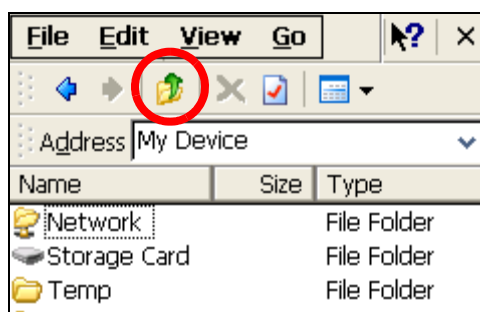
An entry for the diagnostic log file should be displayed.



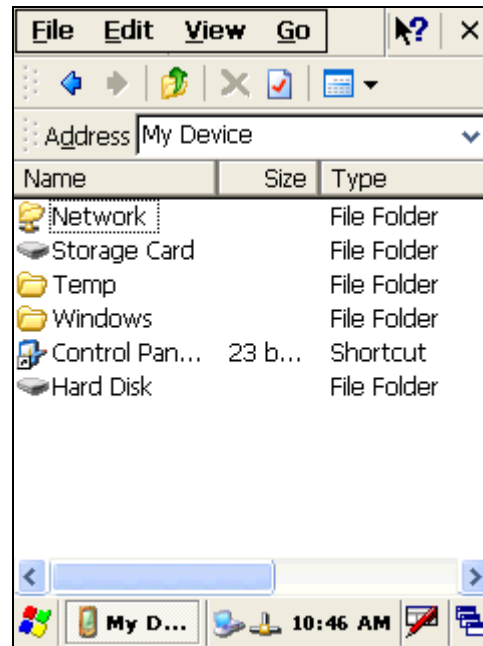
From the *Edit* dropdown menu, tap *Copy*.



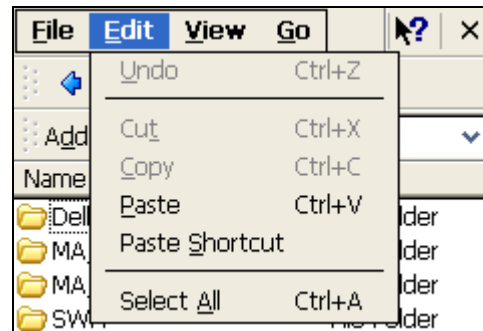
Now, tap on the *Up* arrow on the Windows CE Explorer tool bar.



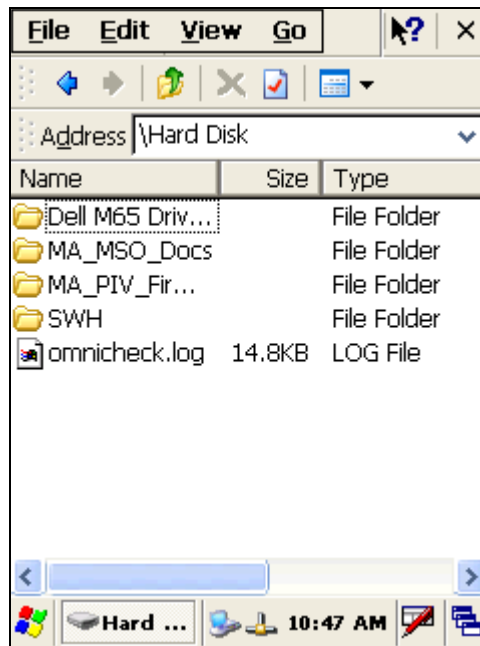
Continue to tap the *Up arrow* until the contents of the uppermost level are displayed:



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



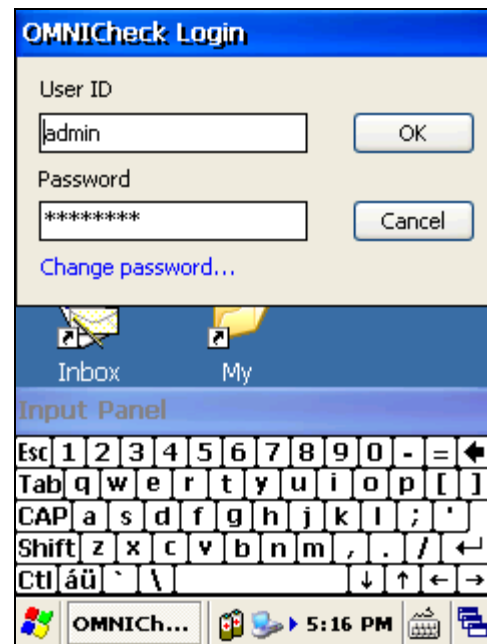
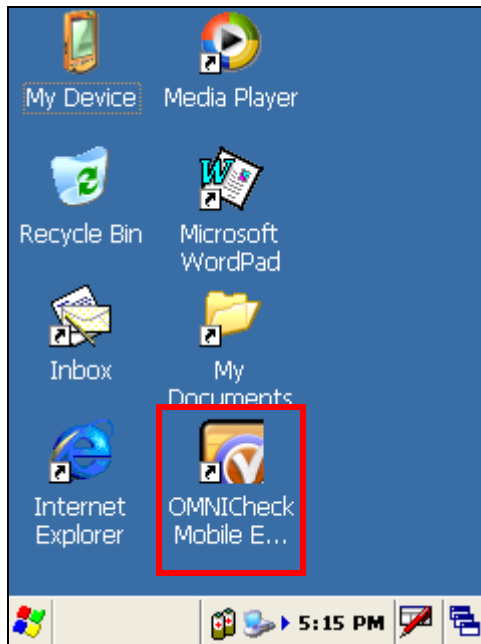
Tap on *Paste*. The log file should immediately appear:



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

LICENSING THE SOFTWARE

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



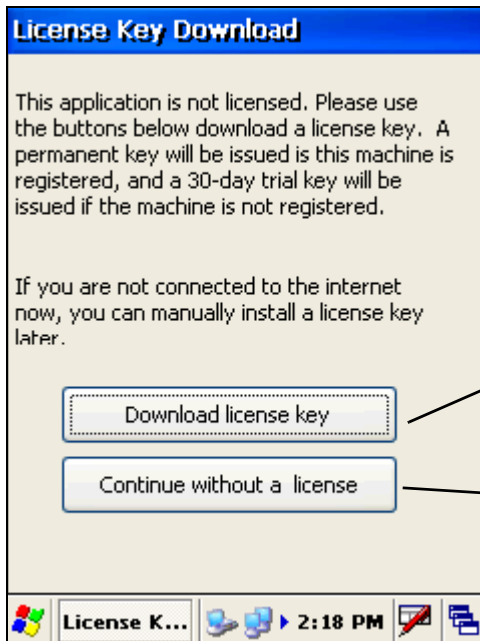
Your system integrator may have changed the default administrative *User ID* and *Password* from the Codebench factory defaults located above. Please consult your system integrator's documentation.

- 3 Press the *OK* button to accept the password and launch the *OMNICheck* splash screen.



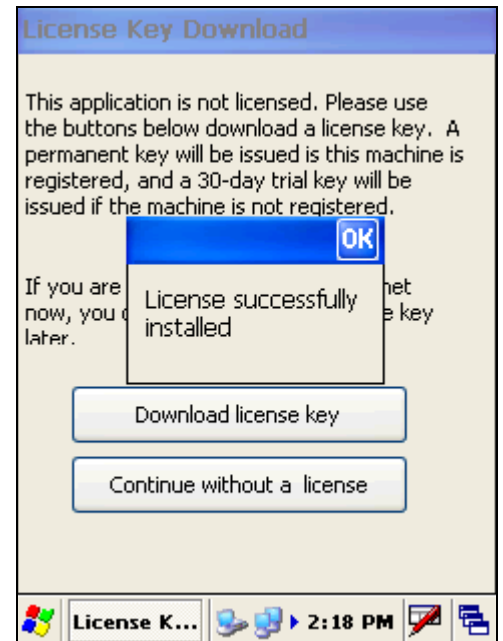
You can disable the splash screen by un-checking the checkbox in the upper left-hand corner.

- 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.

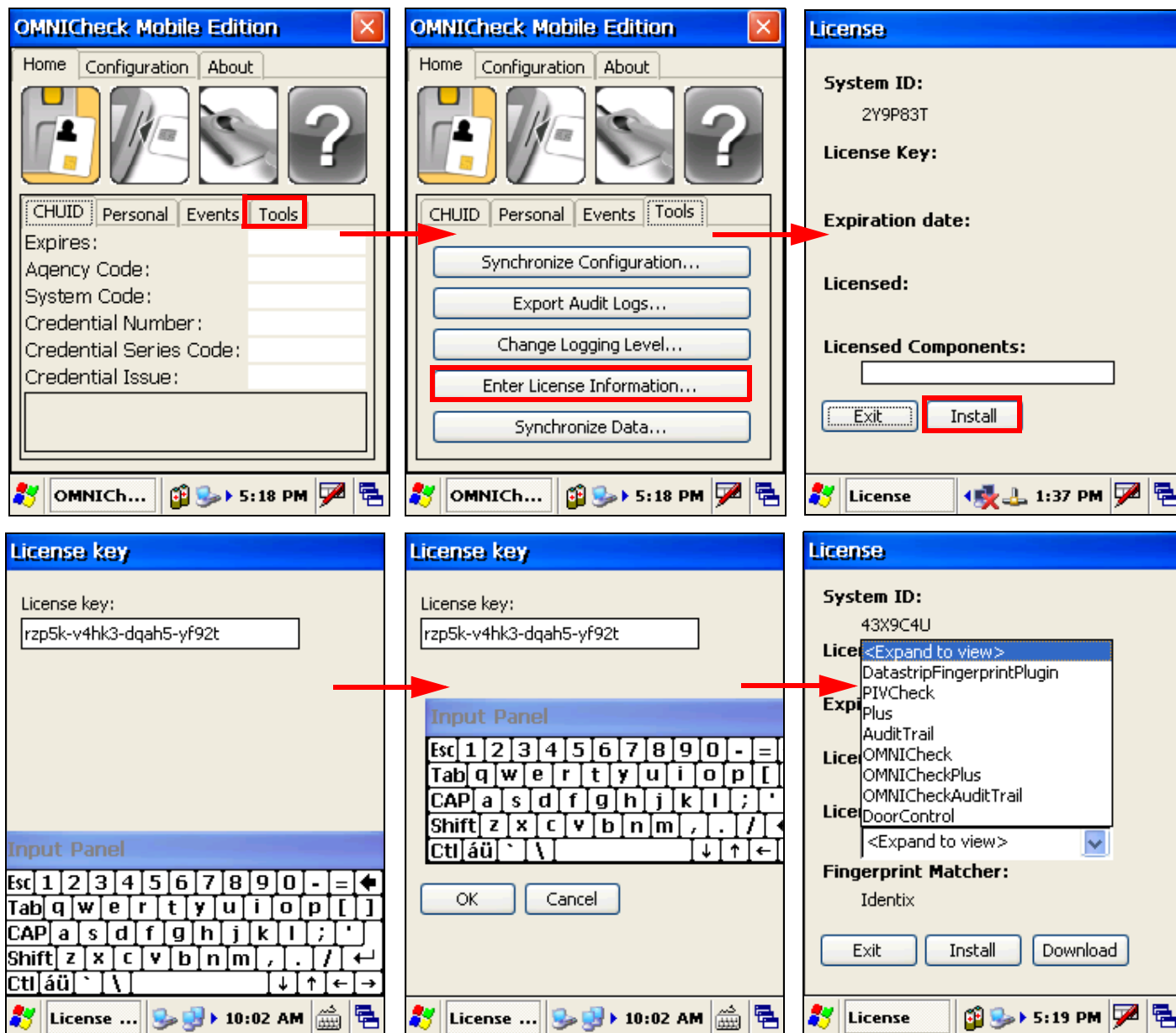


TRIAL LICENSE

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

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 shows how to add your license key manually.



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.

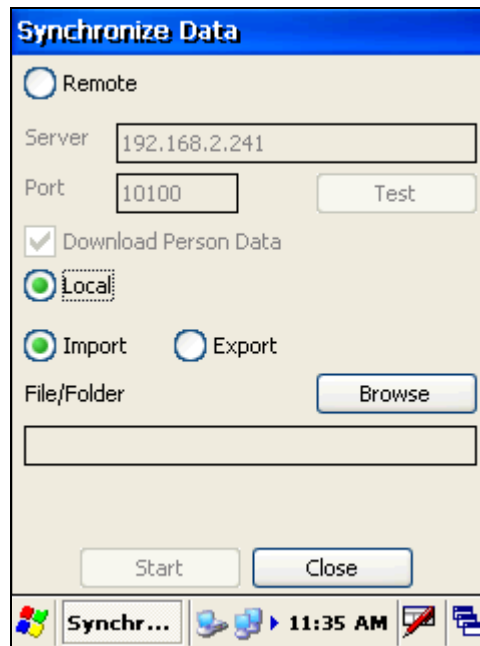
The license key field is now populated, indicating you have successfully licensed *OMNICheck*. Press the *Exit* button to return to the *Application Configuration* dialog.

SYNCHRONIZING DATA

As explained in “CHUID and Active Card Authentication” on page 48, each mobile biometric terminal harvests and inserts every TPK it reads into an encrypted database. The *Synchronize Data* option allows *OMNICheck* devices to share their TPK databases, and for *OMNICheck* clients, to download and cache photos.



The *Synchronize Data* form is displayed.



REMOTE

OMNICheck Plus users can synchronize with a server database over the network using the *Remote* option. On systems without the *Plus* option, it is disabled.

LOCAL

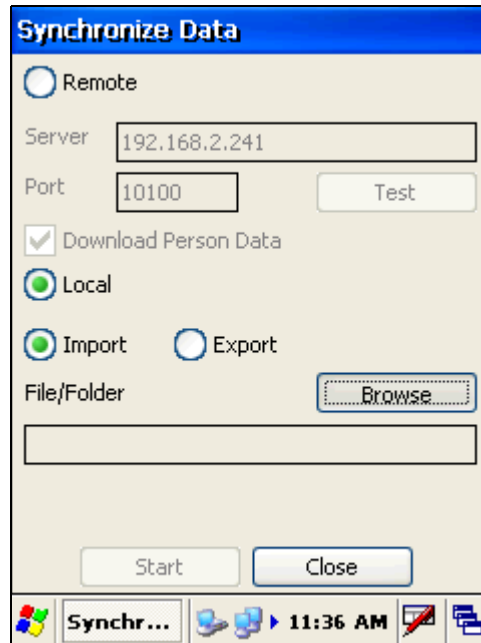
This option enables the operator to synchronize two TPK databases using a flash drive as the intermediary.



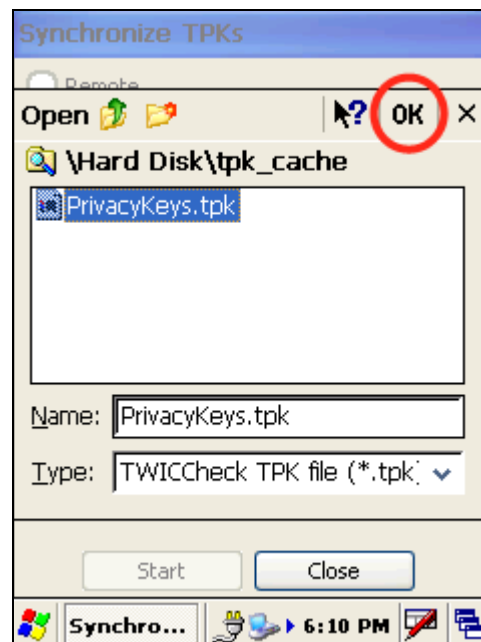
Duplicate keys are always ignored.

IMPORT

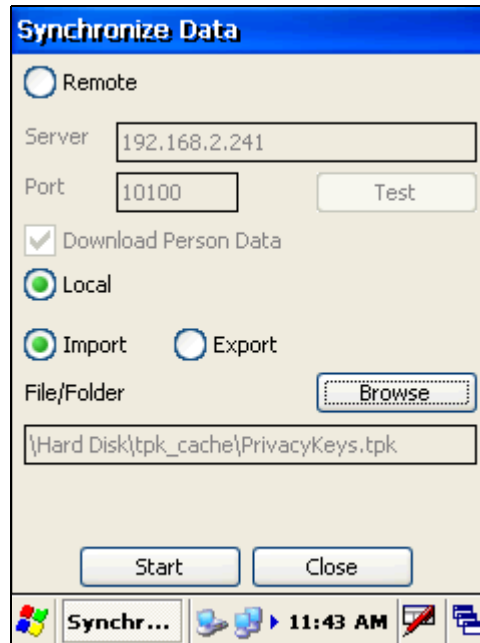
This option imports TPKs from an existing file and adds them to the local TPK database. To import TPKs produced by another device, insert a flash drive that contains an encrypted file named `PrivacyKeys.tpk` that is produced by the procedure detailed in “Export” on page 78. Then tap the *Browse* button.



Navigate to the *Hard Disk* device and locate the file named `PrivacyKeys.tpk` as shown in the example below. Select the file so that its name appears in the *Name* field. Tap the *OK* button.



The file selection form will close and the *File/Folder* field will now contain the full path to the TPK file.

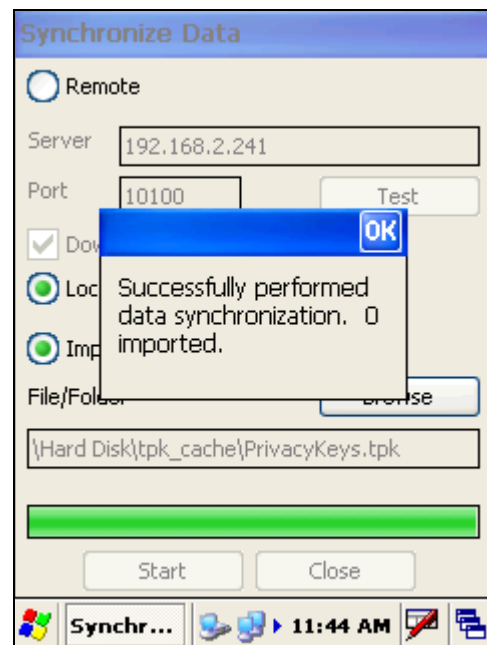
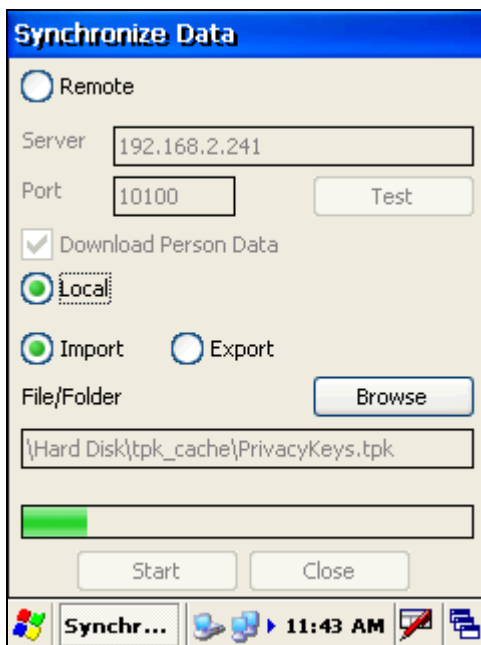


Click the *Start* button to begin importing the TPKS. A progress bar will be displayed as TPKS from the file are imported into the local database.



Duplicate keys are always ignored.

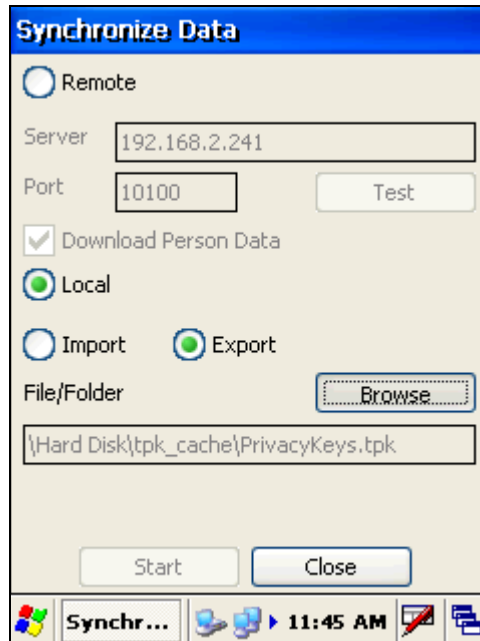
When the operation is complete, a message will be displayed.



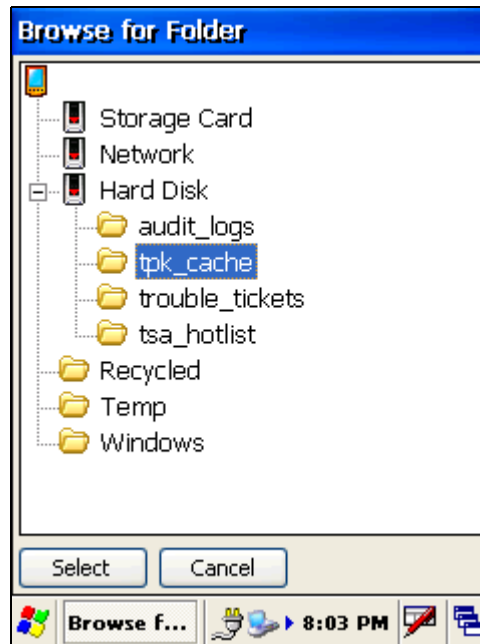
EXPORT

When performing an export, a file named `PrivacyKeys.tpk` is created in the selected folder. If this file already exists, any TPKs are first extracted from that file before it is updated with the TPKs from the local database. The result is that the local database and `PrivacyKeys.tpk` both contain all of the TPKs from both devices.

To get started, tap the *Export* option, then *Browse*.

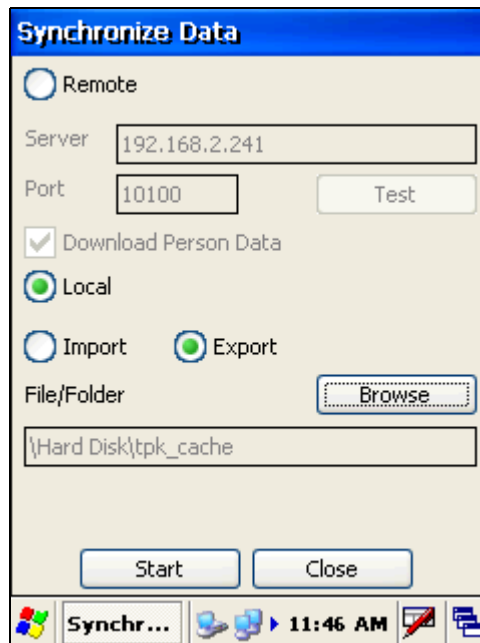


Navigate to the folder where the TPKs will be stored.

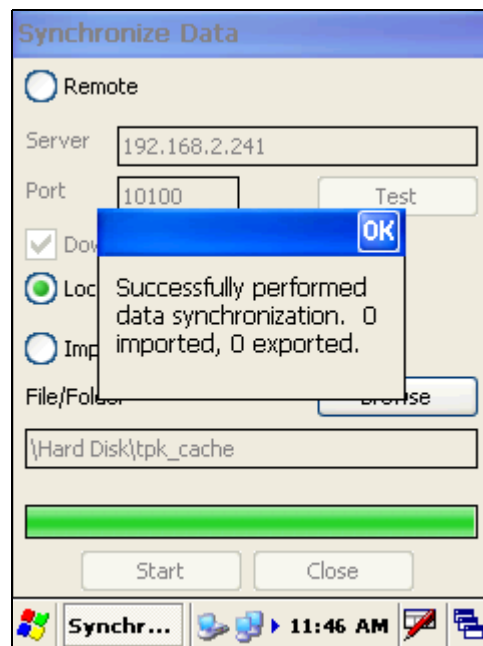


This file, [PrivacyKeys.tpk](#) will not be displayed.

Tap the *Select* button. The folder selection form will close and the selected folder will be displayed in the *File/Folder* field.



Tap the *Start* button to commence the merge.



UPDATING YOUR SOFTWARE

Keeping 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 *OMNlCheck*. The method you choose will depend upon whether you have network connectivity and whether your software is properly licensed.

- You can request *OMNlCheck* 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 the 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.

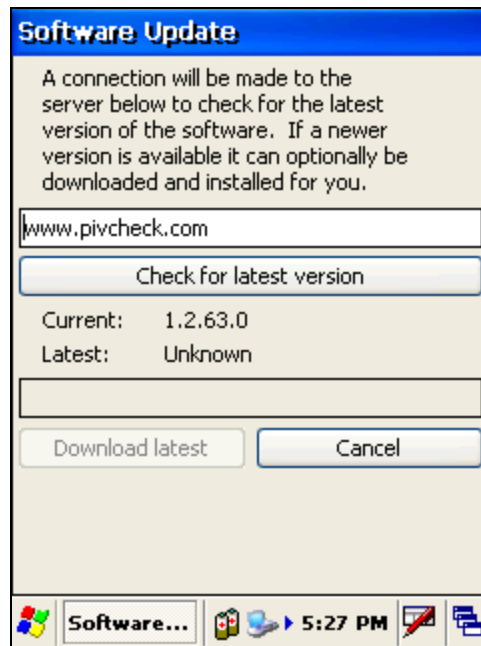
Remove any cards from the smart card reader.

- Select the *About* tab.

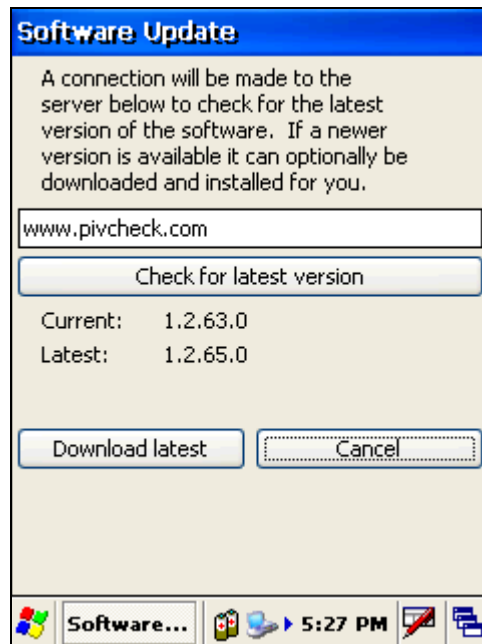


Note that the version number in the lower right corner is a [hyperlink](#). Click the link. The following dialog will be displayed.

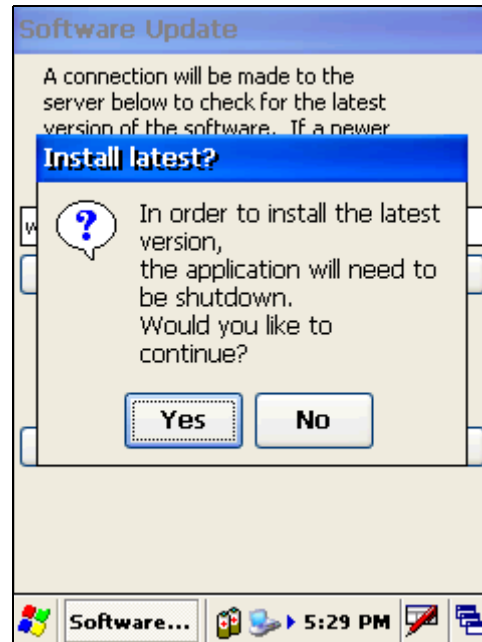
Tap the *Check for latest version* button to see whether any updates are available.



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



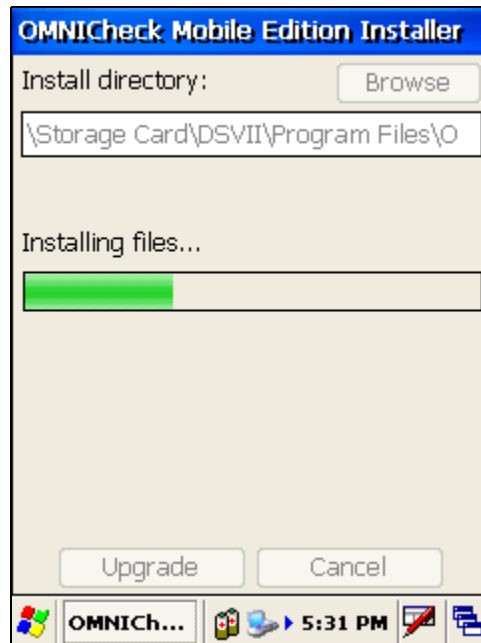
Tap the *Download latest* button to upgrade the software, and the following dialog will be displayed. Otherwise, tap *Cancel* to close the dialog. When the download is complete, you will be prompted to allow the installer to close the current application instance.



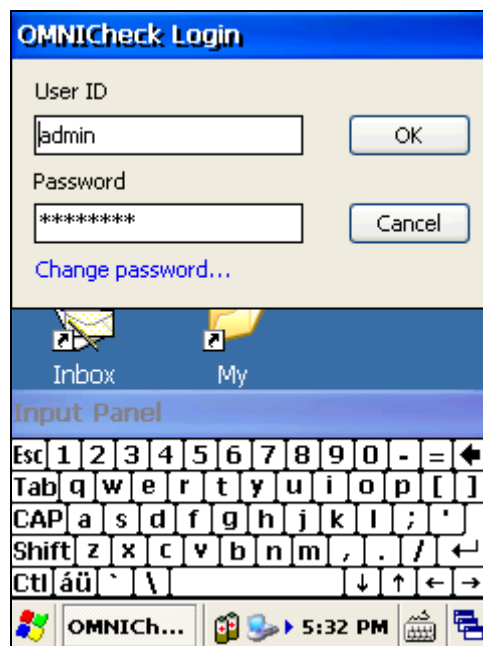
Since *OMNlCheck* is already installed you will be prompted to *Upgrade* the application. Tap *Upgrade* to continue.



The installer will overwrite the current installation. (Your configuration settings will be preserved).



When the upgrade is complete, the application will launch automatically. *OMNCheck* has been upgraded successfully.

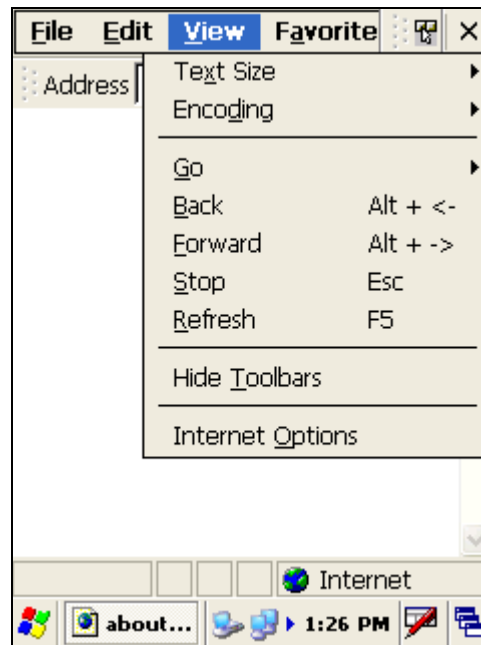


INSTALLING AN EXECUTABLE FILE VIA INTERNET EXPLORER DOWNLOAD

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.

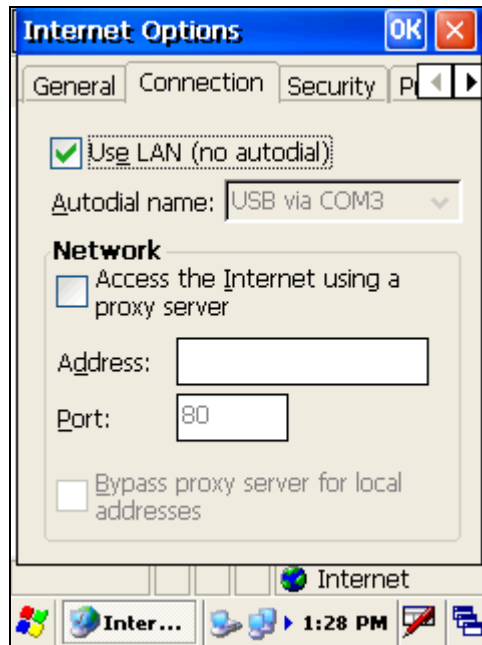
Exit the *OMNCheck* application.

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.

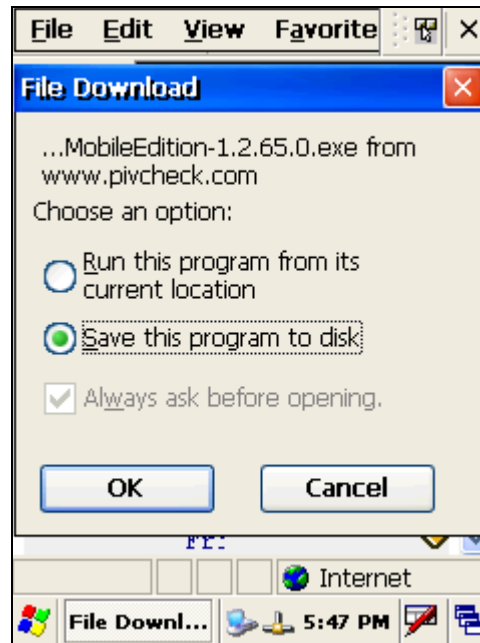
Tap the *OK* button to save the configuration options.

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

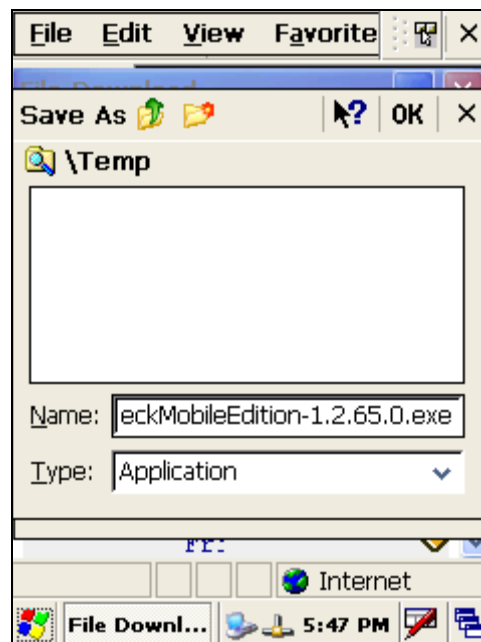
An authentication dialog will be displayed.



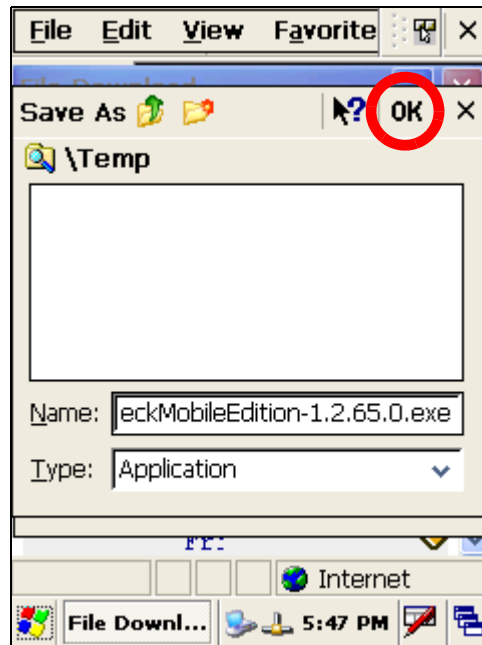
Enter your *User Name* and *Password* into the appropriate fields and tap the *OK* button. If the information is correct, then an *options* dialog will be displayed:



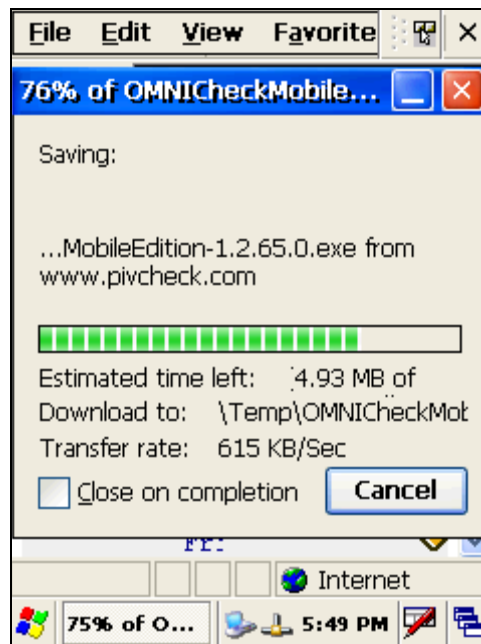
Choose the options as shown above and tap *OK*. The new *OMNlCheck* executable file will be downloaded to the `\Temp` folder on the terminal.



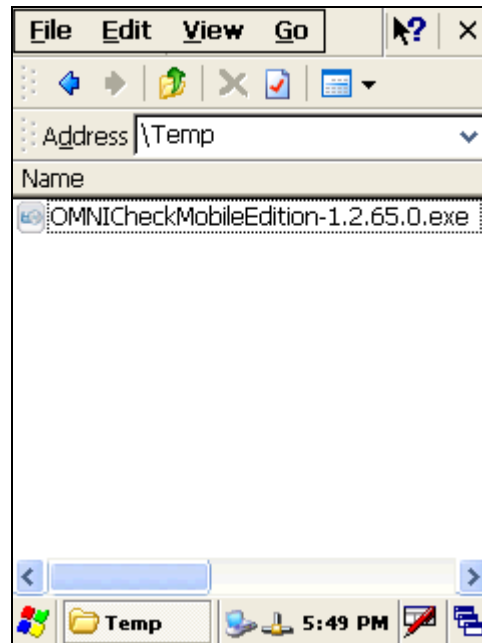
Tap the *OK* button to start the download.



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



Double-tap on the [OMNICheckMobileEdition 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 *OMNICheck* 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.

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.

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 ^a	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

Index

A		
Appendix A		
Reference Documents	91	
Appendix B	93	
PIV Data Containers	93	
TWIC Data Containers	95	
Application Tab		
Audit Log Folder	39	
Configurable Contact Information	40	
Error Log Folder	39	
Fingerprint Options	37	
TWIC Authentication Modes	37	
C		
Certificate Validation	52, 60	
CHUID and Active Card Authentication	48	
Contact Mode	48	
Contactless State	48	
Configuration Options		
Application Tab	36	
Configuring the System		
Changing the Admin Password	19	
Enter your License Manually	22, 73	
Licensing the Software	19, 71	
Powering Up	13	
Trial License	21, 73	
Contact Mode	48, 54	
Contactless State	48, 54	
D		
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	
E		
Export Audit Logs Button		
Audit Data Elements	64	
Audit Log File Cleanup	66	
Exporting Audit Log to Flash Drive	65	
F		
Fingerprint Match		
Fingerprint Match Failure	49	
Fingerprint Match Threshold	49, 58	
Scoring	49, 58	
H		
Home Tab		
Tools Tab	63	
I		
Identity Authentication		
The Application Events Window	52	
The Card Data Window	52	
Identity Verification	47, 53	
K		
Key Features	8	
Biometric Signature Validation	7	
Card Validation	7	
Encrypted Configuration	7	
Exportable Audit Trail	7, 8, 9	
Hands-free, Contactless Operation	7	
PKI Validation	7	
TPK Caching and Merging	7, 8	
TSA Hot List Checking	7	
TSA Hot List Integrity Check	7, 9	
TWIC Authentication Modes	7	
L		
Legacy CAC or Non-PIV Cards	61	
Licensing		
Updating Your Software		
Automatic Software Download	81	
Installing a CAB File via Internet Explorer Download	85	
N		
Non-TWIC		
Biometric Verification	57	
CHUID and Active Card Authentication	54	
Contact Mode	54	
Contactless State	54	
Fingerprint Match		
Fingerprint Match Failure	58	
Identity Authentication		
The Application Events Window	60	
The Card Data Window	60	
S		
Saving your Configuration	45	
Supported Credential Types	9	
Synchronizing Data		
Export	78	
Import	76	
Remote	75	
System Specifications	11	
Hardware	11	
Software	11	
T		
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	63	
Change Diagnostic Logging Level Button	67	
Synchronizing Configuration	63	