

***interTRAX*® MOBILE PIV™**

**Personnel Identification Verification  
Software**

**User Guide**

**Version 4**

**2012**



**Copyright © 2003 - 2012 by Salamander Technologies, Inc.  
Protected by US Patents  
5,573,278; 5,596,652; 5,793,882; 6,761,312; 7,191,934**

# Contents

Contents .....	2
Disclaimer .....	3
1 Introduction to <i>interTRAX</i> ® Mobile PIV™ Software .....	4
Overview .....	4
2 Hardware and Software Requirements .....	5
Mobile Units & Operating Systems .....	5
3 Using <i>interTRAX</i> ® MOBILE PIV™ .....	6
Initial Setup .....	7
Organization Tab .....	7
Assignments Tab .....	8
<i>Add assignment</i> .....	8
<i>Delete assignment</i> .....	8
Server Tab .....	9
Time Tab .....	10
Retrieve Certificate List .....	10
Incident Context .....	11
Add Incident .....	12
Sync .....	13
Report .....	14
End incident .....	15
Scan Cards .....	16
Driver License .....	17
Smart Card .....	18
Checking Certificate .....	18
Validating PIN .....	19
<i>Correct PIN</i> .....	19
<i>Incorrect PIN</i> .....	19
Scan fingerprint .....	20
Validation screen .....	21

## **Disclaimer**

Salamander Technologies, Inc. has made its best efforts to make the *Salamander* system reliable and defect-free; however, any computerized system is subject to malfunction including operator error, undetected system “bugs”, and power or communication outages. Salamander Technologies, Inc. cannot and does not warrant that the system will perform flawlessly at all times and under all conditions.

# 1 Introduction to *interTRAX*® Mobile PIV™ Software

## Overview

The *interTRAX*® **Mobile PIV**™ software is an important part of the *interTRAX*® Suite of software which is setting the standard for resource accountability throughout the United States. The *interTRAX*® Suite was designed with three objectives in mind.

**Simplicity** – The *interTRAX*® Suite uses nationally recognized incident management procedures. The *interTRAX*® barcode is a two dimensional, high capacity barcode and the *interTRAX*® smart card is a contactless RFID card. Both are used to carry a person's database and they allow users to capture and display the data. The barcode contains personal information as well as qualifications. Operators may be trained to use the system in a matter of minutes.

**Survivability** - There are three tiers of survivability in the Salamander System assuring that even a complete breakdown in electronic equipment does not inhibit accountability.

- If external communications are lost, incidents may be run from the COMMAND™ Module.
- If the COMMAND™ Module is inoperable, basic accountability may be maintained via the MOBILE software.
- If electronic devices are not available or inoperable, ID cards can be used for manual accountability.

The *interTRAX*® two dimensional, high capacity barcode and the *interTRAX*® smart card represent the ultimate in a distributed database – they survive even if the host system is destroyed or inoperable.

**Scalability** - The *interTRAX*® Suite was designed to scale so that it is the right size for the needs and budgets of any organization. Small organizations can start with an *interTRAX*® Suite compatible manual accountability system. Medium organizations can purchase a basic *interTRAX*® Suite electronic system for only a few thousand dollars. Large departments can deploy multiple handheld systems as part of a Wireless LAN controlled by a COMMAND™ Module. Organization members as well as all mutual aid organization members and other support organization members may be provided with a barcode or a smart code to assure inoperability when you need it most.

All Salamander applications have the option of synchronizing data over a local area network or directly to the web. 2-way synchronization allows all resource data to be shared between applications. Salamander offers the ability to join applications together at the web level creating a master incident. Incidents joined at the web level 2-way synchronize over a cellular or other web connection.

The *interTRAX*® Suite unites response organizations, mutual aid, and state & national responders with a common machine-readable format and resource data sharing.

## 2 Hardware and Software Requirements

The following hardware is supported by Salamander Technologies, Inc.

### **Mobile Units & Operating Systems**

MOBILE UNIT	MINIMUM OPERATING SYSTEM
DAP Technologies CE3240BW	Microsoft® Windows® CE Version 5.0
Motorola MC75 W/BSCR	Windows Mobile Version 6.0

### 3 Using *interTRAX*® MOBILE PIV™

The *interTRAX*® MOBILE PIV™ software is used for:

- Personnel Identity Verification (PIV) of FIPS 201/FRAC smart-cards
- 3-factor validation that includes Certificate Verification, PIN and Biometric Validation
- Driver License Validation
- Collect information that may be sent to COMMAND™ and *interTRAX*® exchange
- View all reads (DL, CAC, PIV or TWIC) through the *interTRAX*® exchange PIV Activity Report

Tap on the STI MOBILEPIV icon



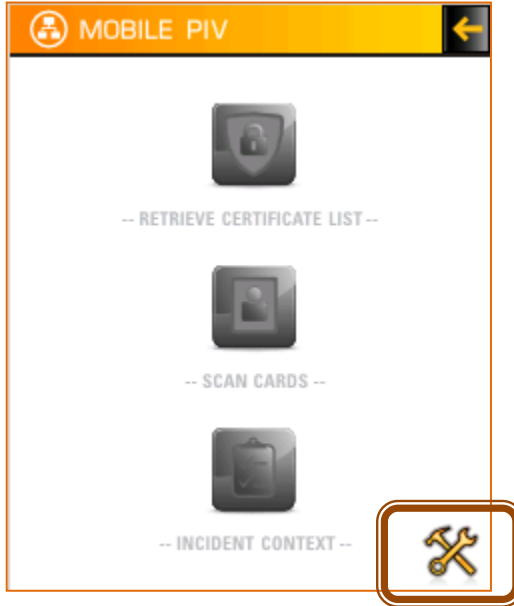
The *interTRAX*® suite MOBILE PIV™ screen will appear



## Initial Setup

Following the initial installation of MOBILE PIV an Organization must be entered. You may also setup Assignments, Server and Time during initial setup.

**Tap** on the **Tools** icon.



### Organization Tab

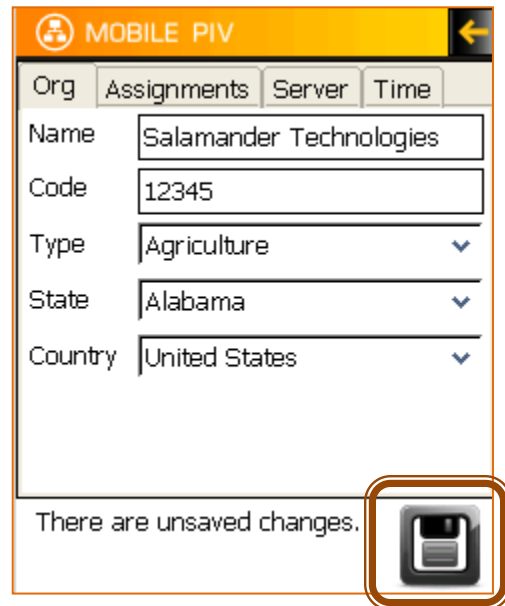
**Enter** the **Name** of the organization.

**Enter** the **Code** which will be supplied by STI. It is a unique identifier and must be entered correctly.

**Enter** the **Type** from the dropdown.

**Enter** the **State** from the dropdown.

**Enter** the **Country** from the dropdown.



**Tap** on the **Save** button to save the organization.

NOTE: The "There are unsaved changes." message will remain on the screen until you tap on the Save button. This may refer to information on any one of the four tabs.

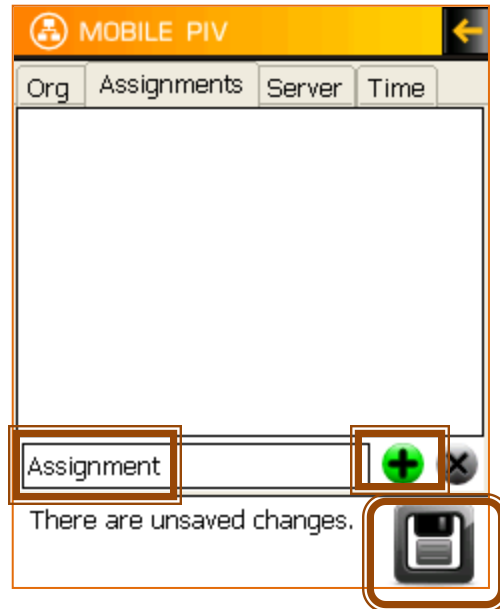
## **Assignments Tab**

### ***Add assignment***

**Enter** the **Assignment** in the box.

**Tap** on the **green +** button to add the assignment. **NOTE:** This does not save the assignment.

**Tap** on the **Save** button to save the assignment. **NOTE:** The “There are unsaved changes.” message will remain on the screen until you tap on the Save button. This may refer to information on any one of the four tabs.

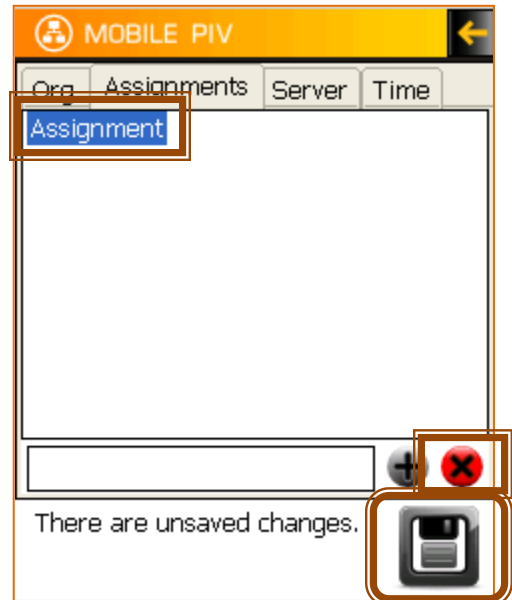


### ***Delete assignment***

**Tap** on the **Assignment** to highlight it.

**Tap** on the **red X** button.

**Tap** on the **Save** button to save the assignment. **NOTE:** The “There are unsaved changes.” message will remain on the screen until you tap on the Save button. This may refer to information on any one of the four tabs.





## Server Tab

### **PIV Server URL**

NOTE: The URL will be supplied by STI.

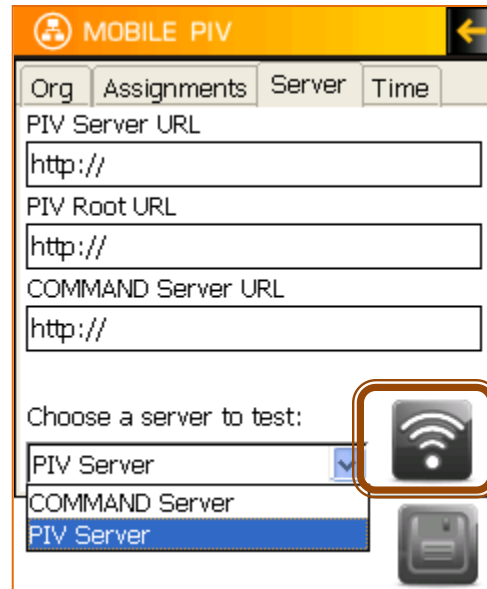
### **PIV Root URL**

NOTE: The URL will be supplied by STI.

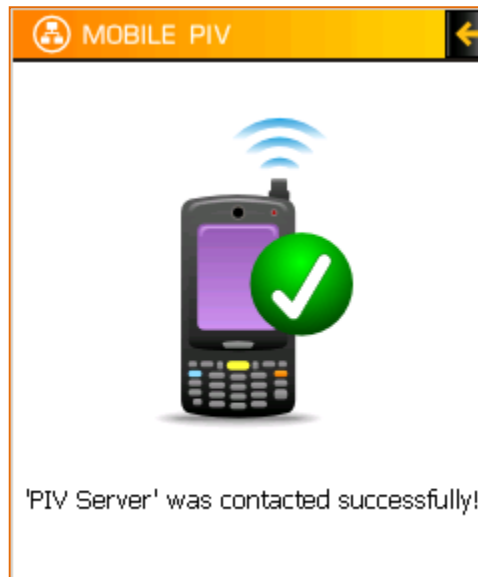
### **COMMAND Server URL**

NOTE: The URL will be supplied by STI.

**Tap** on the **Test Server** button to test the connection. NOTE: To test the PIV Server you must have an active internet connection



A screen will appear with information regarding the success of the connection test.

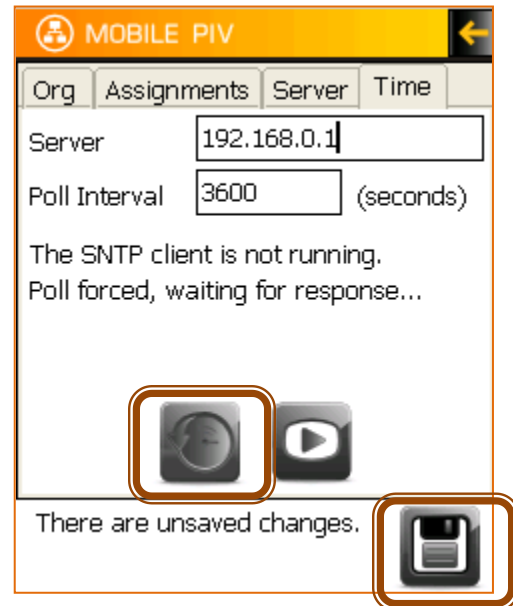


## **Time Tab**

Enter the **IP Address** for COMMAND™.

Tap on the **Poll Forced** button.

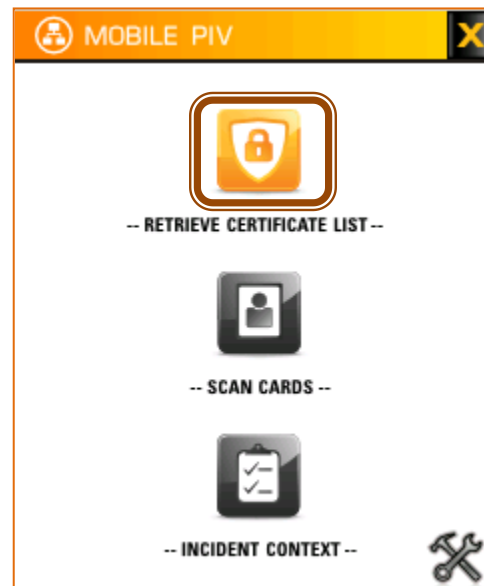
Tap on the **Save** button. NOTE: The “There are unsaved changes.” message will remain on the screen until you tap on the Save button. This may refer to information on any one of the four tabs.



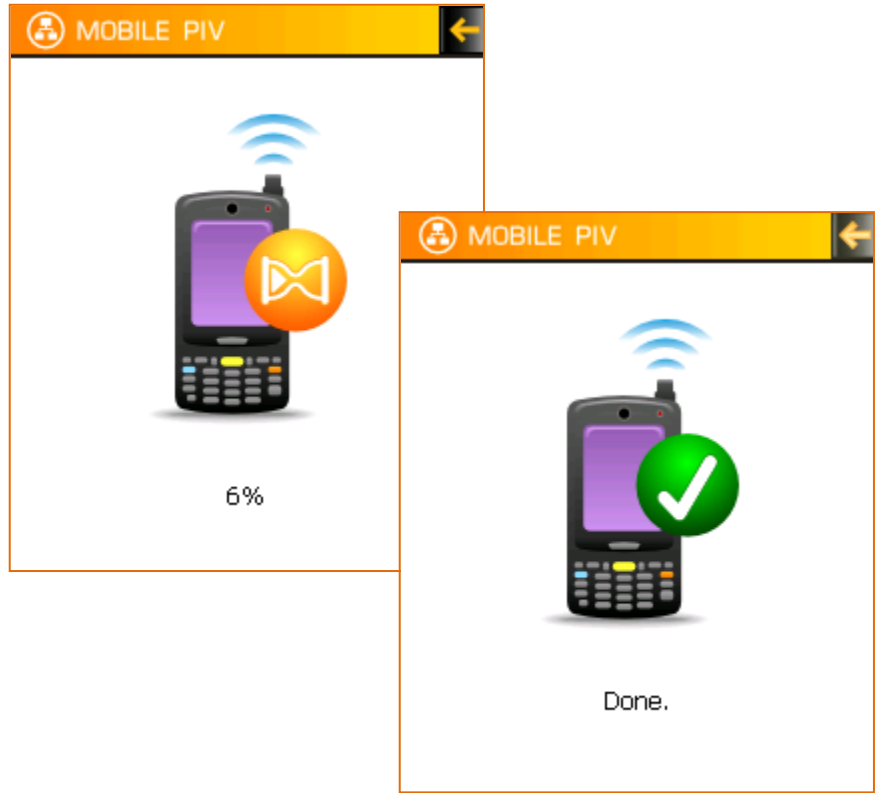
## **Retrieve Certificate List**

NOTE: To retrieve a certificate list you must have an active internet connection

Tap on the **Retrieve Certificate List** button



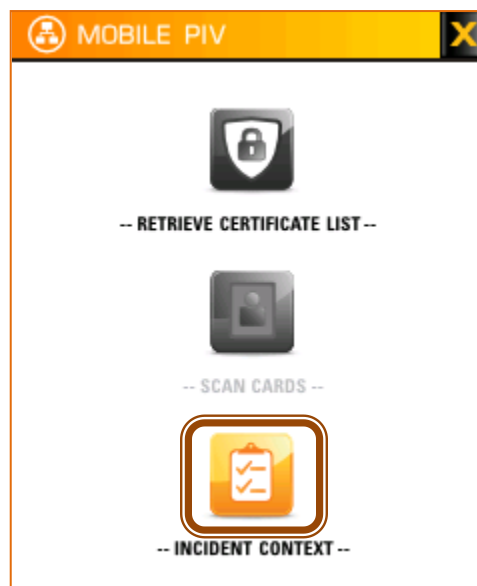
A screen will appear providing the progress of the retrieval



If the Mobile PIV software determines that there is a chance that the certificate data may be out-of-date, the Retrieve Certificate List button will appear Red.

## Incident Context

Tap on the **Incident Context** button.



## Add Incident

Enter the **Incident Name**.

Choose the **Assignment** from the dropdown.

Tap on the **Start** button.

MOBILE PIV

Salamander Technologies

New Incident Name

Assignment

Assignment

An incident has not yet been started.  
Enter a name and tap the 'Start' button.

Start

The **Start Date** and **Time** will appear

Tap on the **arrow** in the right corner of the screen to continue.

MOBILE PIV

Salamander Technologies

New Incident Name

Started on 2009-12-11 at 10:16

Assignment

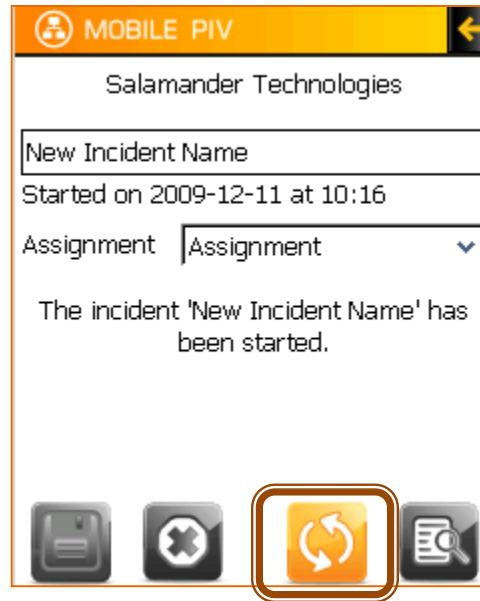
Assignment

The incident 'New Incident Name' has  
been started.

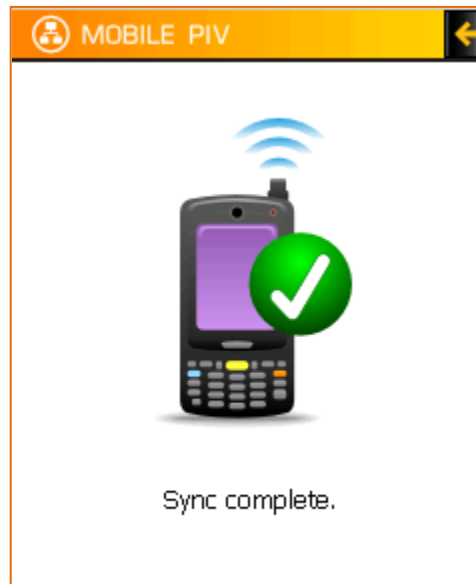
Start

## Sync

**Tap** on the **Sync** button if you are using COMMAND™. This will allow the IC to accept the mobile unit.

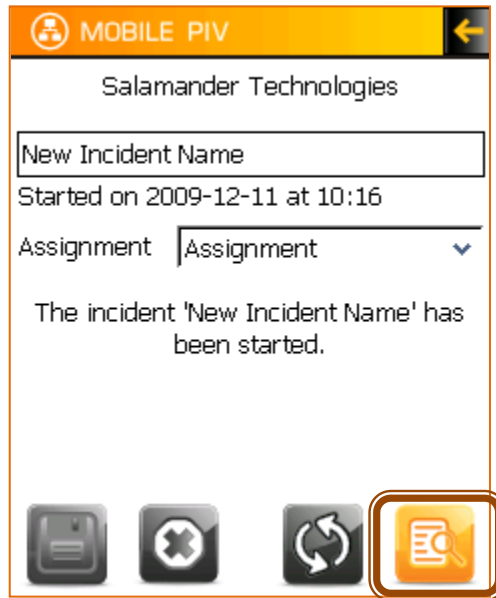


A screen will appear to provide the status of the sync.



## Report

Tap on the **Report** button.



A report will appear with the Activity Date, the Card Holder and the Total Events (scans).

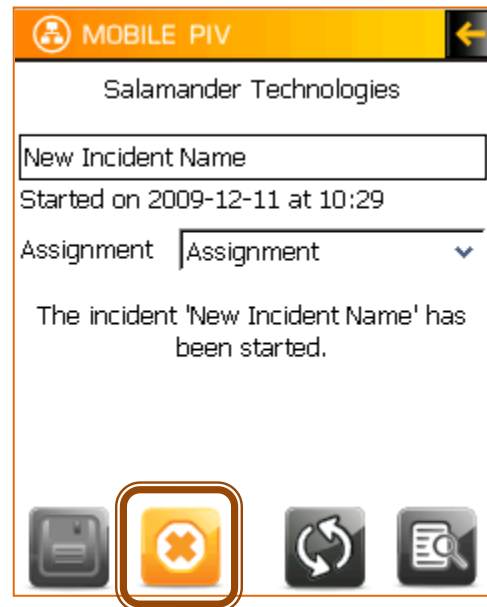
The screenshot shows the MOBILE PIV application interface displaying a report. The header bar is yellow with "MOBILE PIV" and a back arrow. Below the header, there is a table with two columns: "Activity Date" and "Card Holder". The table is currently empty. At the bottom of the screen, it displays "Total Events: 0".

Activity Date	Card Holder
---------------	-------------

Total Events: 0

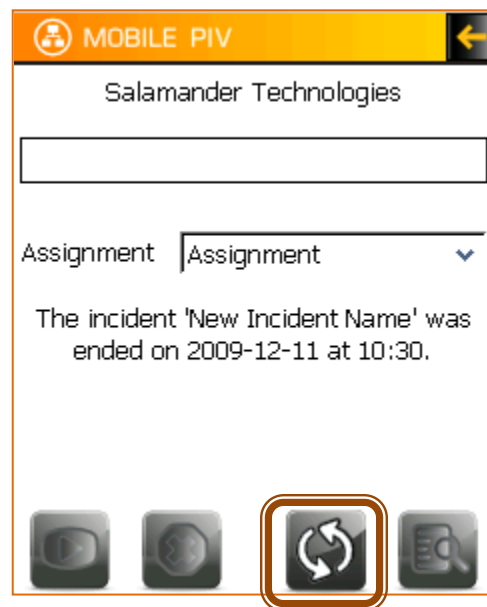
## End incident

**Tap** on the **X** button to end the incident.



NOTE: This ends the incident without asking the user to verify the intention to end. The user will not be able to reopen the incident.

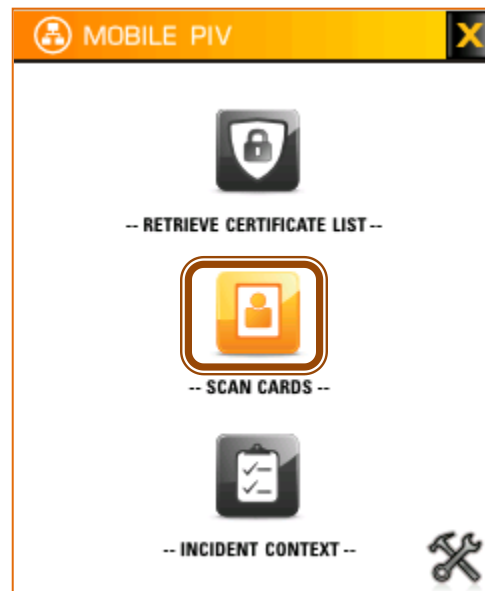
**Tap** on the **Sync** button after you end the incident.



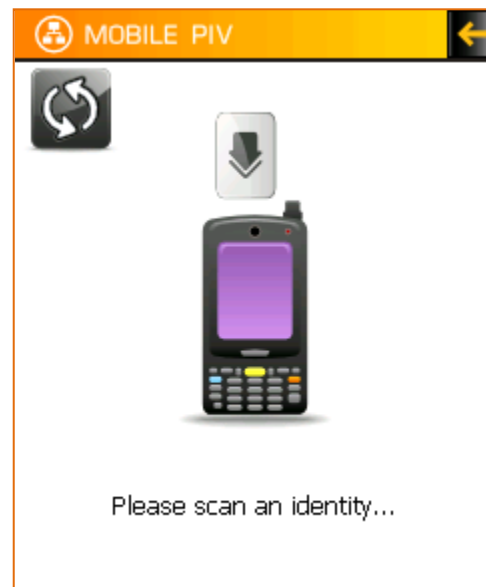
## Scan Cards

If there is an incident in progress the **SCAN CARDS** button will be active.

**Tap** on the **Scan Cards** button.



The **Please scan an identity...** screen will appear.



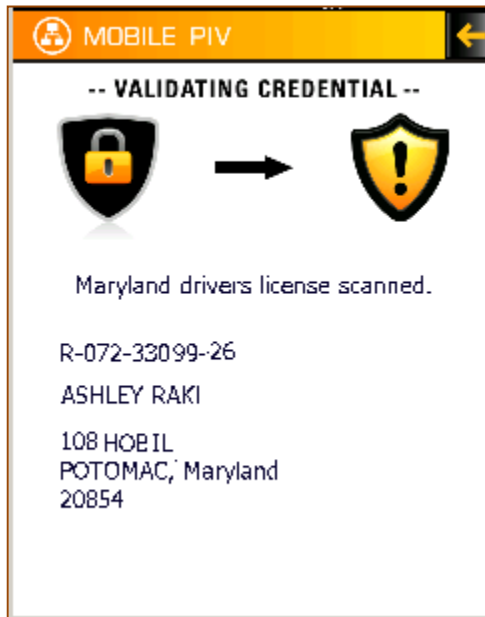


## Driver License

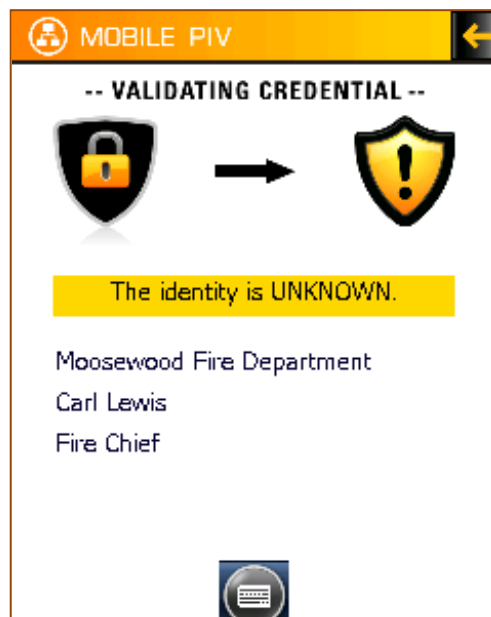
Scan a driver license.

The **Validating Credential** screen will appear.

If the card is validated the personal information will appear.

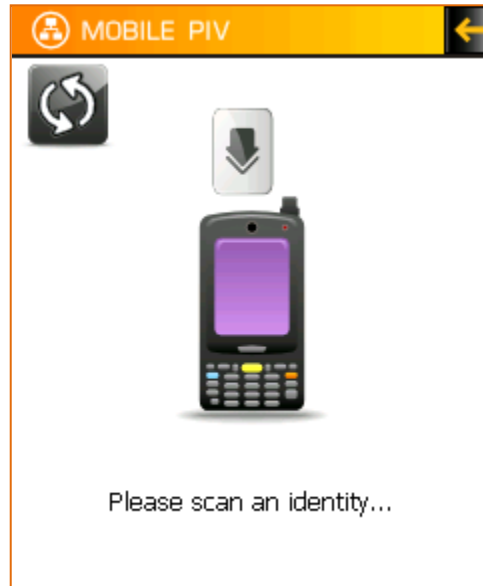


If the card is not validated **The identity is UNKNOWN** screen will appear.



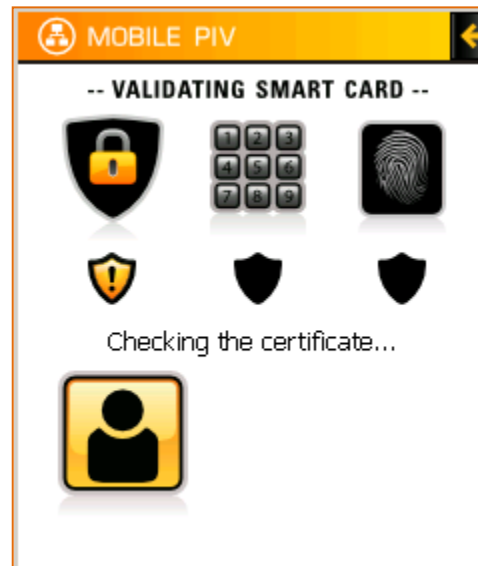
## Smart Card

Scan a Smart Card.



## Checking Certificate

The **Validating Smart Card** screen will appear as the certificate is being checked.

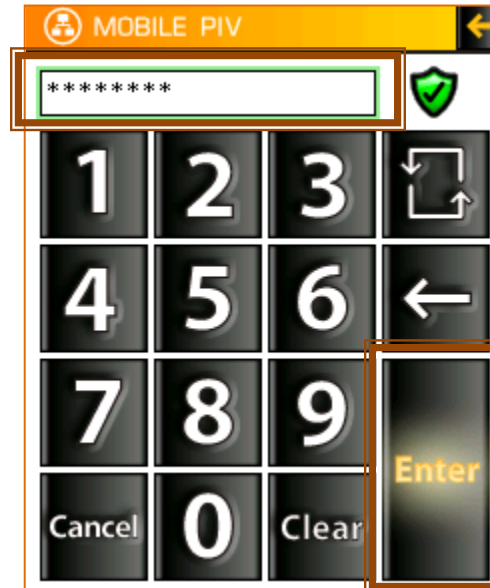


## Validating PIN

The key pad will appear.

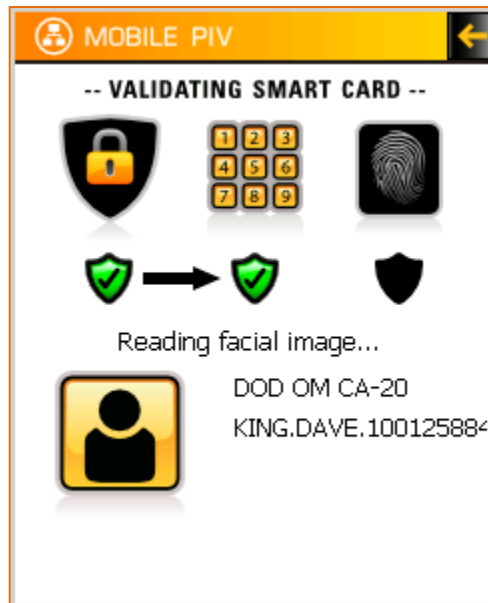
**Enter** the PIN.

**Tap** on the **Enter** button.



### **Correct PIN**

If the PIN is correct the **Reading facial image...** message will appear as the software reads the card.



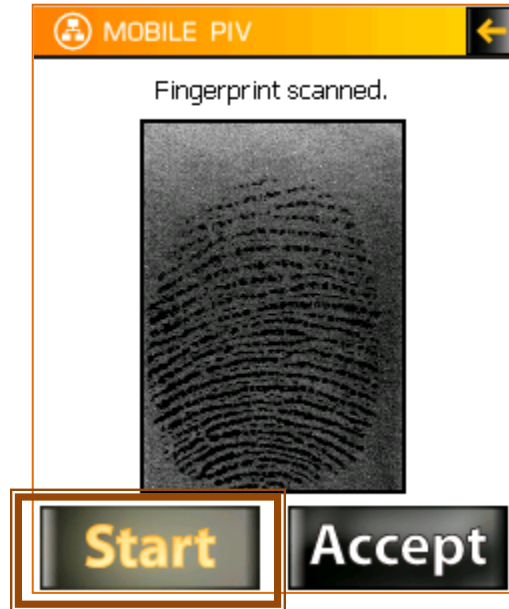
### **Incorrect PIN**

If the PIN is not correct you may try the entry again.

**NOTE:** Tap on the Status icon next to the PIN entry area to see how many failed attempts have been made on the card. Failed attempts are cumulative. Failure to enter the correct PIN prior to reaching the maximum number of failed attempts will lock the card. Once the card is locked it will have to be returned to the issuer.

**Scan fingerprint**  
**Scan a fingerprint.**

**Tap** on the **Start** button to scan the fingerprint.



**Tap** on the **Accept** button to process the fingerprint.



## Validation screen

The screen will appear with the **VALID** message when the process is complete.

