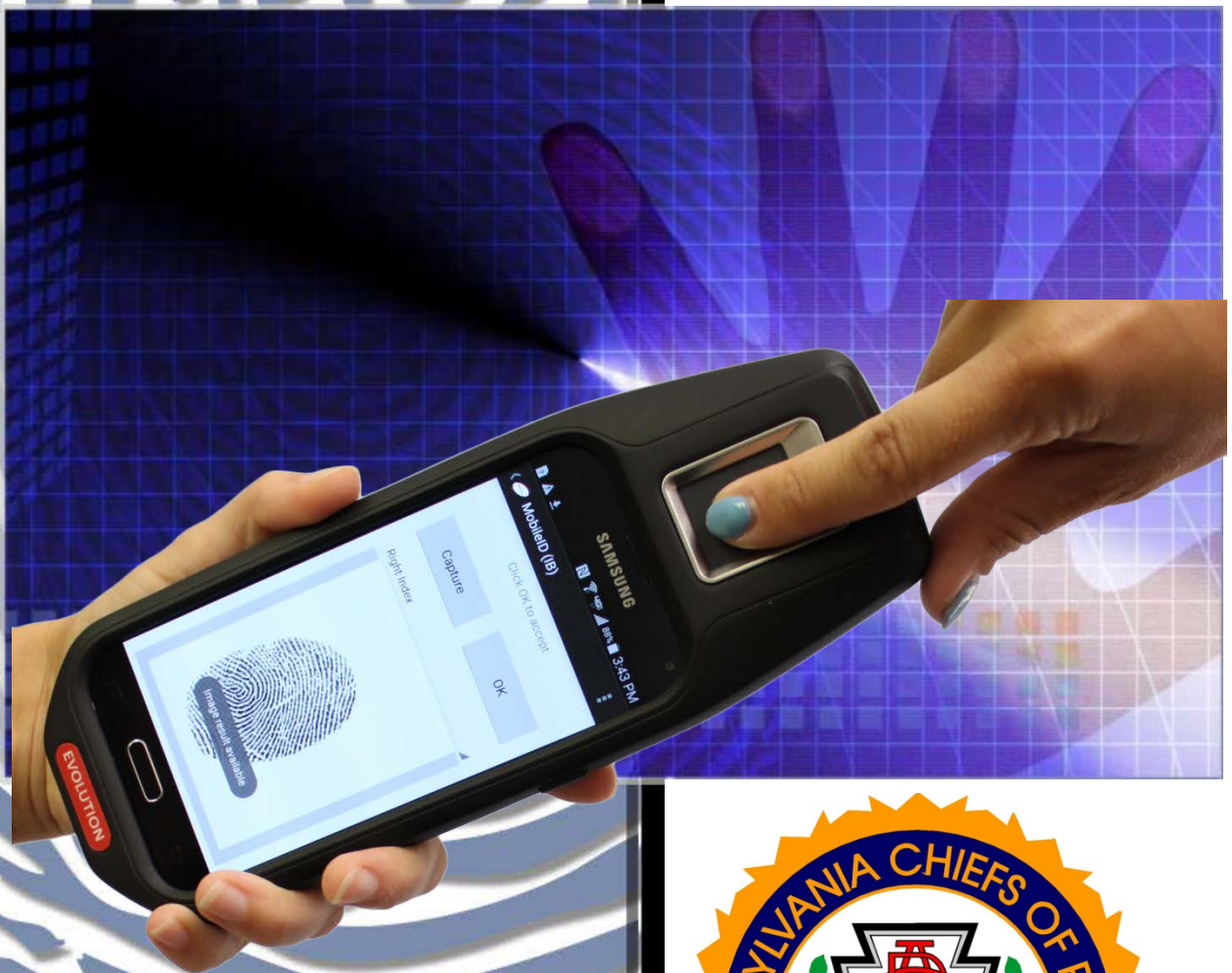


# Training Guide

## PCPA Mobile ID

### Using PA RAPID-ID with Evolution Device from DATAWORKS Plus





## Table of Contents

<b><u>Introduction to the PCPA Mobile ID Project and Mobile ID Training</u></b>	<b>4</b>
<b><u>Learning Objectives</u></b>	<b>4</b>
<b><u>Agency Application Requirements</u></b>	<b>4</b>
<b><u>Agency Appropriate Use Policy</u></b>	<b>5</b>
<b><u>Police interactions with Citizens</u></b>	<b>5</b>
Mere Encounter:	5
Investigatory Detention:	6
Custodial Detention or Arrest:	7
<b><u>Vehicle Investigation (including bicycles)</u></b>	<b>7</b>
Traffic Stop	7
<b><u>Reasonable Suspicion</u></b>	<b>8</b>
<b><u>Probable Cause</u></b>	<b>8</b>
<b><u>Avoiding Bias</u></b>	<b>8</b>
<b><u>Release from Police Custody</u></b>	<b>8</b>
<b><u>Medical Emergencies/Dead Persons</u></b>	<b>8</b>
<b><u>Limited use of Mobile ID</u></b>	<b>9</b>
<b><u>Mobile ID user requires CLEAN certification</u></b>	<b>9</b>
<b><u>Limited Hit Information requires follow-up</u></b>	<b>9</b>
<b><u>PCPA RAPID-ID using DATAWORKS PLUS</u></b>	<b>10</b>
<b><u>Evolution Device</u></b>	<b>11</b>
Evolution Device Overview	11
Turning on the Evolution	12
Turning Off the Evolution	12
Home Screen	12
Charging the Evolution	13
<i>Wired Charging Via USB</i>	13
<i>Wireless Charging Via Dock</i>	13
Maintaining the Evolution	13
<i>Cleaning the Device</i>	13



Adjusting Evolution Settings	14
<b>Capturing Fingerprints</b>	<b>15</b>
Logging in with Two Factor Authentication	15
Fingerprint Capture	17
Additional Options for Fingerprint Capture	18
<b>Responses</b>	<b>21</b>
Hit/No Hit/Possible Hit Responses Returned to Evolution's Transactions Screen	21
View Detailed Responses on Evolution	22
<i>Transactions Screen Options</i>	23
<b>Repository for Individuals of Special Concern (RISC)</b>	<b>24</b>
<b>Troubleshooting</b>	<b>25</b>
System Returns False Positive or 'NO HIT' for Known Subject	25
<i>Check Proper Finger Placement</i>	25
<i>Check Environment/Cleanliness</i>	26
<i>Check Condition of Fingers</i>	26
<b>Support</b>	<b>27</b>
Information to Have Available	27
Opening a Support Ticket	27
Resolving the Problem	27
Obtaining Replacement Parts	27
After-Hours Calls	27
Escalation of Tickets	27



# Introduction to the PCPA Mobile ID Project and Mobile ID Training

---

The Pennsylvania Chiefs of Police in cooperation with the Pennsylvania State Police (PSP) is providing local police the Evolution handheld fingerprint scanner and a dedicated secure cellular network to connect to PCPA secure sever which securely connects to the State Police Automated Fingerprint Identification System (AFIS) and the FBI Repository for Individuals of Special Concern (RISC). These devices and the network are only for law enforcement purposes when specific circumstances apply.

This training is provided to inform the police officers using this equipment under what circumstances it is appropriate to use this device. How current statutes and case law affect the conditions of the use and the limitations of the identification provided. The police officer will also learn how to operate, maintain and troubleshoot the device.

## Learning Objectives

---

After completing this training:

- Officers will be able to describe and identify the three types of encounters outlined by the courts for interactions between police and citizens.
- Officers will be able to identify the circumstances when identification is legally required to be provided by the citizen during a police citizen interaction
- Officers will be able to differentiate the different ways a citizen may identify themselves and the various tools and systems the police use to verify those identifications.
- Officers will be able to describe the circumstance where Mobile ID is an appropriate tool to assist in verifying a citizen's identification.
- Officers will be able to differentiate the possible responses from submitting fingerprints for identification using the Mobile ID device.
- Officers will be able to explain the limitations of fingerprint identification using Mobile ID
- Officers will be able to recognize their responsibility to comply with all PSP, Commonwealth Law Enforcement Assistance Network regulations and policies relative to the use and response received using Mobile ID.
- Officers will be able to demonstrate they can properly use the Mobile ID device.
- Officers will be able to explain their department's policy and procedures for use of the Mobile ID device.

## Agency Application Requirements

---

Access to the PSP MID system will only be provided to Criminal Justice agencies with an Originating Agency Identifier (ORI) on file with PSP. Agencies submitting Mobile ID transactions to the state, please met the following requirements:

- Current CLEAN/USER Agreement (the CLEAN/USER Agreement will be updated to include PSP MID requirements and these are subject to inspection during the triennial Agency CLEAN Audit process).
- Advanced Authentication consistent with FBI CJIS Security Policy.





- Make and model of MID device to be used (only FBI-Approved devices may be used and no personally owned devices will have access to the PSP Mobile Identification (MID) system.
- A copy of the Agency Appropriate Use Policy on Agency letterhead.

Application packets were submitted through the PA Chiefs of Police and were subject to LTW review in the same manner as the Live Scan application process, prior to PSP processing.

## Agency Appropriate Use Policy

Every agency using Mobile ID will have an approved “Appropriate Use Policy” in place prior to operation of Mobile ID and included in the training for their personnel. The policy will limit the use of Mobile ID to those circumstances that meet PSP functional limitations and are generally consistent with state, federal and case law.

The following sections will guide agencies and users to those limited circumstances found to be generally consistent with state, federal and case law. Agencies may choose to even further limit the use of Mobile ID but may not expand the use.

## Police interactions with Citizens

The courts have outlined three levels of interactions between police officers and citizens. The following explains those interactions and when it might be appropriate to use Mobile ID.

### Mere Encounter:

This is a consensual interaction where the officer may ask the citizen questions and generally engage the citizen in conversation. In this interaction, the police officer may ask for identification from the citizen but the citizen is under no obligation to engage the officer or provide identification.

Refusal to comply with requests and conversations DOES NOT provide the officer with any additional suspicion

Police interactions with citizens form the cornerstone of effective police work. Officers must keep in mind that citizen contacts are based on the presumption that the citizen is not under any reasonable suspicion of criminal activity. As such, officers should adhere to the following protocols.

Persons “contacted” may not be detained in any manner against their will or frisked unless reasonable suspicion is established during the contact to believe they present a danger to the officer or that they have committed, are committing or are about to commit a crime.

An officer may not use force or coercion to require a citizen to stop or respond to questions or directions absent any other legal reason.

Officers shall ensure that their actions and requests could not be reasonably perceived by the citizen as a restraint on his or her freedom to leave the officer’s presence. .

Mobile ID is not appropriate in a mere encounter with a citizen.



## Investigatory Detention:

This is an interaction of a non-consensual nature where the officer has developed reasonable suspicion that criminal activity is occurring and the subject of the detention is involved in criminal activity. During this type of interaction, the officer must be able to point to specific articulable facts which lead to reasonable suspicion. In this interaction, the officer may demand identification from the citizen and the citizen must comply with the orders of the officer.

Officers shall conduct an investigatory detention based upon reasonable suspicion that the person detained has committed, is committing, or is about to commit a crime.

Officers shall not prolong the investigatory detention beyond the period necessary to accomplish the purpose of the detention. Officers shall be aware that prolonging an investigatory detention unnecessarily may cause a court to view the detention as an unlawful seizure, if probable cause does not exist for an arrest.

Officers shall take precautionary measures for their own safety during an investigatory detention, including display of firearms or handcuffing the detainee. Officers shall be aware that unnecessary or prolonged display of firearms, handcuffing, and so on during the investigatory detention may cause a court to view the detention as an actual arrest.

Officers who reasonably believe that a person under investigatory detention may pose a threat to their safety shall conduct a frisk or pat-down search of the detainee's clothing for weapons. Officers shall not conduct any further search of an investigatory detainee unless and until it appears that there is probable cause for the arrest of the detainee.

If during the investigatory detention, it becomes apparent that there is probable cause to believe that the detainee has committed a criminal offense, the detainee shall then be placed under arrest, and the procedures for arrest set forth in this policy, including the procedures for a search incident to an arrest, shall then be followed by the arresting officers.

If an officer possesses reasonable suspicion of criminal activity and there are specific factors which lead the officer to believe the subject is armed and poses a threat, the officer is permitted to conduct a Terry Frisk of the person to detect weapons that could be used to harm the officer.

In cases where there is reasonable to demand the citizen's identity, the officer should first use other means to identify the citizen like:

Driver license/Military/Employer Photo ID

Pennsylvania Justice Network (JNET)

PSP CLEAN

Pennsylvania Department of Motor Vehicles (Penn DOT)

When these do not provide a clear identification or when it appears that the citizen is providing false identification, the officer can use the Mobile ID device to search fingerprints in the PSP criminal database and the FBI RISC database of wanted persons, sexual offender registry subject, or known or appropriately suspected terrorist. However, even if this is the case the citizen must not be physically forced to the fingerprint check. They should be advised that the Mobile ID system does not keep a record of their fingerprints.



The officer must use caution when using the Mobile ID device. A citizen that does not have identification or is providing false identification may be a wanted and dangerous person. Officer safety is required always during an investigatory detention and the officer should use the Mobile ID device in a way not to be distracted from officer safety.

As will be covered in a later section, the response to the fingerprint submission is limited and any data supplied must be verified by further inquiry to CLEAN/NCIC. The officer must also protect the data screen for authorized viewing.

## **Custodial Detention or Arrest:**

This is the most intrusive level of police/citizen interaction. Legally, the officer must develop probable cause that the subject citizen is engaged in or has engaged in criminal activity. Once probable cause has been established the subject of the interaction is not free to leave. This situation places the subject under the actual will and control of the arresting officer.

Although the suspect is subject to the will and control of the officer, Mobile ID is only appropriate when there is a need to know the identity immediately, and there are no other sources of identification available. However, the suspect may not be forced to be fingerprinted

## **Vehicle Investigation (including bicycles)**

Police interactions with the drivers and passengers in vehicles is another set of circumstance that present the need to use the Mobile ID device.

### **Traffic Stop**

Police officers have the authority to stop any vehicle where the driver or the occupants are observed violating the law, or where the officer reasonably believes the vehicle driver, or occupants were violating the law. Section 6308 of the Pennsylvania Vehicle Code allows police officers to request to exam the vehicle's registration, proof of financial responsibility, vehicle identification number or engine number or the driver's license, or to secure such other information as the officer may reasonably believe to be necessary to enforce the provisions of the vehicle code. This section also makes it the duty of the vehicle operator including bicycle operators to produce identification.

All motor vehicle stops shall be performed professionally and courteously. The officer needs to maintain a view towards educating the public about proper driving procedures while recognizing and taking steps to minimize the dangers involved in this activity for the officer, the motorist, and other users of the highway.

Before using Mobile ID in a traffic stop all other means of identification should be used.

As previously stated, an officer must use caution when using the Mobile ID device. A citizen that does not have identification or who is providing false identification may be a wanted and dangerous person. Officer safety is required always during an investigatory detention and the officer should use the Mobile ID device in a way not to be distracted from officer safety.

The response to the fingerprint submission is limited and the any data supplied must be verified by further



inquiry to CLEAN/NCIC.

## Reasonable Suspicion

---

In the present context, the totality of the circumstances in each incident or situation that provides an officer with a particularized and objective basis for suspecting legal wrongdoing. The process allows officers to draw on their own experience and specialized training to make inferences from and deductions about the cumulative information available to them. Reasonable suspicion is more than a hunch or feeling that an officer might have about an individual or circumstances. It is based on specific facts that, when taken together with rational inferences, reasonably warrant the vehicle stop.

Reasonable suspicion justifies an investigatory detention or vehicular stop. But, to execute an arrest, the officer must establish probable cause.

## Probable Cause

---

In determining probable cause the arresting officer must examine all the factors and events leading up to the arrest and decide whether these facts, viewed from the standpoint of an objectively reasonable police officer, support the belief that an individual has committed, is committing, or is about to commit a crime.

## Avoiding Bias

---

Officers are prohibited from stopping vehicles or persons under the guise of legal authority when in fact the stop is based solely on the officer's prejudice concerning a person's race, ethnicity, sex, or similar distinction.

## Release from Police Custody

---

During the normal course of police law enforcement, persons will be arrested, booked, fingerprinted via livescan, arraigned by video conference and temporarily held in police custody pending release on bond or transportation to county detention. This process in some police departments involves many persons and lasts through several police shifts. There may be occasions when it is appropriate to check a person's identity using Mobile ID.

The circumstance should be such that other sources of identification are not sufficient or available. Mobile ID should not be used for routine movement of persons in custody at this time. This type of Mobile ID is limited to release from police custody when necessary.

## Medical Emergencies/Dead Persons

---

In cases involving medical emergencies or dead bodies, where the police respond and there is a need for an immediate identification, the Mobile ID may be useful. However, since it searches criminal databases, its use in non-criminal investigations is very limited. Mobile ID should only be used in these cases when other possible means of identification have failed. Mobile ID only returns data from criminal fingerprint files and cannot identify persons that do not have criminal records.





## Limited use of Mobile ID

---

The use of Mobile ID is limited to law enforcement and criminal investigation. Mobile ID fingerprint submissions use resources of the State Police AFIS. The AFIS on a normal basis is performing many important fingerprint processes. Mobile ID is a new function and the impact of multiple agencies using the devices is unknown at this time. Therefore, Mobile ID should only be used when necessary and all other means of identification were used first.

Mobile ID is limited to criminal justice and law enforcement purposes and for a specific agency ORI. All traffic generated over the system shall be made in the performance of the employee's or agencies official duties as they relate to the administration of criminal justice or authorized by law. The dissemination of any information obtained through Mobile ID to anyone outside the criminal justice or law enforcement community is strictly prohibited.

All Mobile ID transactions will be subject to audit by PSP and shall be conducted to ensure compliance with CLEAN/CJIS regulations, federal and state statutes on security and privacy of criminal history record information.

## Mobile ID user requires CLEAN certification

---

All agencies using Mobile ID must update their PSP CLEAN agreement.

Mobile ID users must have completed Mobile ID training and be PSP CLEAN certified as a criminal history user. Mobile ID use is subject to CLEAN regulations and protected by Federal and state Statutes, rules and regulations. Therefore, users must be aware of their surroundings when using Mobile ID to prevent inadvertent secondary disclosure of protected information.

## Limited Hit Information requires follow-up

---

Mobile ID searches the State Police AFIS criminal database and the information returned is limited to State Identification number (SID), names, date of birth and CPIN photo if available. Therefore, a hit is limited to show a person with a criminal record. A State AFIS Hit does not show if the person is wanted. If a hit is returned from AFIS, it is limited to the fact that the fingerprint may belong to a person with a criminal history. It does not show or report any wanted person information. Therefore, it is necessary to make a follow-up inquiry to CLEAN/NCIC to obtain more information including checking for wanted persons. This is another reason that the officer using the Mobile ID system is required to be CLEAN certified.

---



## PCPA RAPID-ID using DATAWORKS PLUS

The RAPID-ID is a mobile identification solution that helps identify a subject through their fingerprint record. The Evolution scanner is an “All-In-One” device which is based upon smartphone technology. Officers use the Evolution scanner to capture fingerprints, which are then sent to PCPA RAPID-ID for transmission to the PSP AFIS for matching results.

The web server sends search requests to one or more fingerprint databases and returns demographic data and mugshot images (if available) to the end user for positive identification of the subject. The Evolution device will indicate whether the prints are ‘No Hit’ or ‘Hit,’ and will display a mugshot, if available. The officer can review details about a positive Hit directly from the Evolution device.



The primary tasks and workflows covered this User Guide include:

- An overview of the Evolution device. See *“Evolution Device Overview,”* starting on page 11.
- How to capture prints and submit transactions. See *“Capturing Fingerprints,”* starting on page 15.
- Viewing the transaction hit or no-hit results on the device and within the RAPID-ID application. See *“Responses”* section, starting on page 21.
- Troubleshooting. See *“Troubleshooting”* section, starting on page 25.
- Contacting technical support. See *Support*, starting on page 27.

## Evolution Device

This section provides an overview of the buttons and features of the device, how to turn the device on and off, charge the device, and maintenance of the device.

### Evolution Device Overview



#### Platen

This is where you capture fingerprints. Be sure the scanner platen is clean before each fingerprinting session.

#### Display Screen

The LCD screen in the middle of the device will show all application menus, captured prints, and RAPID-ID Results. The top right of the screen also includes:

- **Battery Life Gauge**
- **Current Time**

#### Menu Button

This button can be used to access context-sensitive menus or navigate between open applications on the Evolution device.

#### Home Button

This button is used to return the user from an open application back to the Android Home screen. Please note that this does NOT close or exit an application. Certain applications will continue running when this button is pressed.

#### Back Button

This button is used to navigate to the previous menu or screen within an application. The functionality of this button may vary depending upon the current application or menu being displayed.

## Turning on the Evolution

To turn on the Evolution device, press and hold the Power Button on the right side of the device. After the button has been held for a few seconds, the Android device will begin booting up with an on-screen logo displayed, and you can release the power button. Please allow the device to fully boot into the main Home screen.

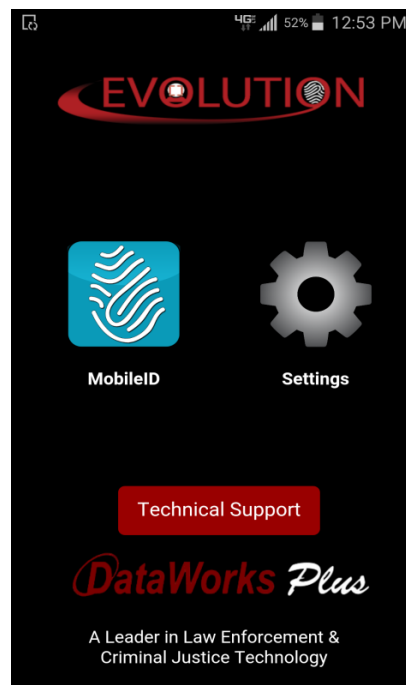
## Turning Off the Evolution

To turn off the Evolution Device press and hold the Power Button on the right side of the device until an on-screen “Device Options” menu is displayed. Press the **Power Off** option from the menu list, and then tap the **Power Off** prompt to confirm device shutdown. The device will then power itself down.



## Home Screen

In the DataWorks Plus' Mobile Device Management Software (MDM), the Home screen will be similar to the following image. It will display icons and descriptions for the apps that are available to you on the Evolution device. The MDM software coupled with cellular data plan and two-factor authentication will enable the Evolution device to be compliant with the FBI CJIS security policy.



## Charging the Evolution

The Evolution device can be charged both via USB connectivity, and wirelessly via device docking.

### ***Wired Charging Via USB***

To charge the Evolution device via USB connectivity, plug a micro-USB cable into the USB slot on the right side of the device. Be sure that the USB cable is plugged into a compatible workstation or AC adapter to ensure proper charging.

### ***Wireless Charging Via Dock***

In addition to USB charging, the Evolution device can be charged wirelessly by connecting it to a device docking station. The device's wireless charging technology will automatically function while attached to a powered-up docking station provided by DataWorks Plus.



#### **Wireless Charging Options**

Wireless car mount or desktop options are available

## Maintaining the Evolution

Keeping your fingerprint scanner clean will help to ensure high quality fingerprint capture. Additionally, do not expose your device to high temperatures / direct sunlight for an extended period of time.

### ***Cleaning the Device***

The Evolution device should be cleaned after every fingerprint scan transaction. To clean the scanner, wipe the platen with a microfiber towel. A microfiber towel can be used to clean the device's LCD screen as needed. The Evolution comes equipped with a screen protector. Screen protectors are recommended to prevent scratching of the LCD glass surface.

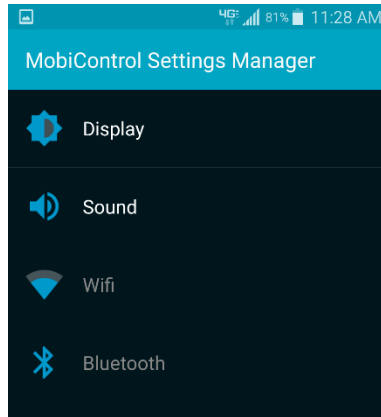


## Adjusting Evolution Settings

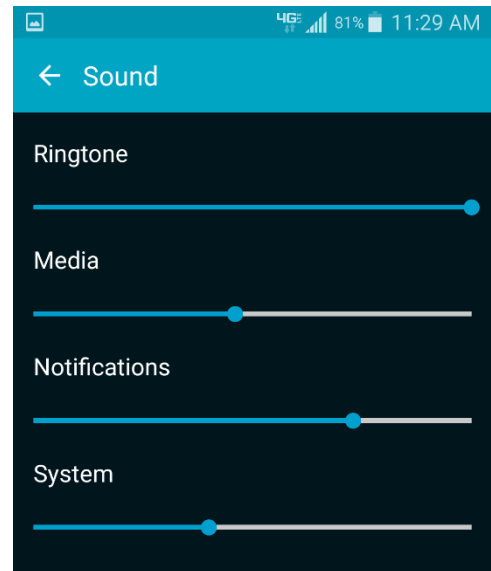
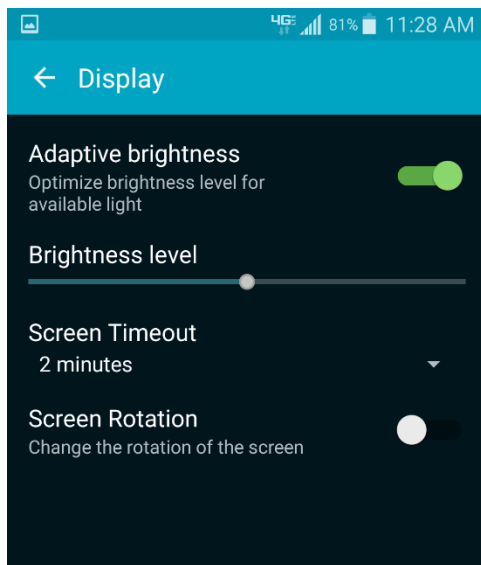
To adjust settings on the Evolution device, tap the “Settings” icon on your Evolution’s home screen.



The Settings Manager screen will be displayed. *Note that Wifi and Bluetooth settings are disabled and unavailable.*



From here, you will be able to make adjustments to the display and sound as shown in the screenshots below.

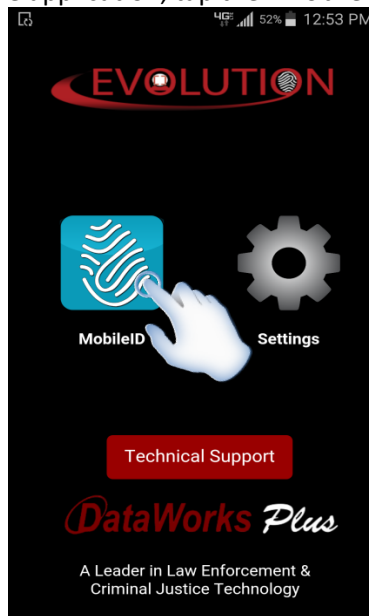


## Capturing Fingerprints

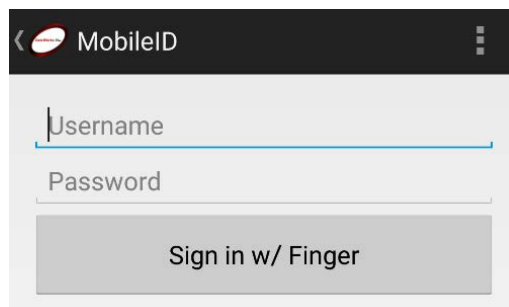
The steps for performing RAPID-ID fingerprint capture and submission have been provided in the following sections.

### Logging in with Two Factor Authentication

Before you can capture fingerprints to perform RAPID-ID transactions, you will need to launch and log into the RAPID-ID application. To open the application, tap the “MobileID” icon on Evolution’s home screen.

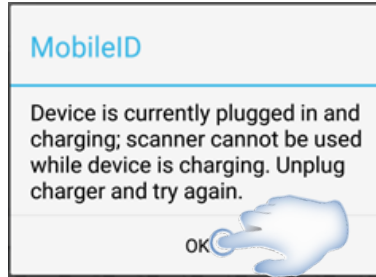


The login screen will be displayed.

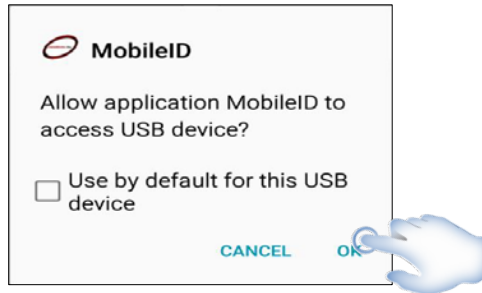


Two-factor authentication is required. Therefore, the Evolution RAPID-ID client requires a user fingerprint in addition to a username and password to login. You will need to perform each of the following steps for authentication:

1. Enter your username and password. The system will then require a fingerprint to complete the authentication process. Select **Sign In w/ Finger** to continue.
2. The power cable must be disconnected before the scanner can initialize. If you get the following pop-up message, tap OK, unplug the power cable, tap Back button, and re-attempt login.

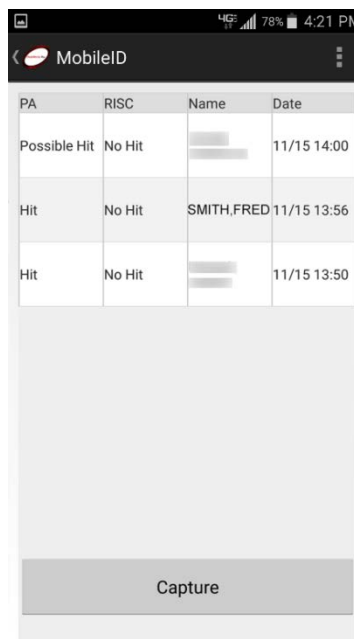


3. If prompted, tap OK on the "Allow application MobileID to access USB device" pop-up message.



4. Place your right index finger on the scanner and allow it to capture.
5. Once the right index finger is captured and authenticated, the transaction screen will be displayed. *NOTE: If this is the first time you are logging into the device, you will be prompted to ENROLL the fingerprint. Select "Yes" to enroll your right index finger or "No" to restart the process.*

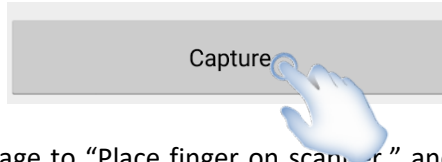
Once you have successfully logged into the application, the RAPID-ID transaction screen will be displayed. This will serve as the Main Menu of the application.



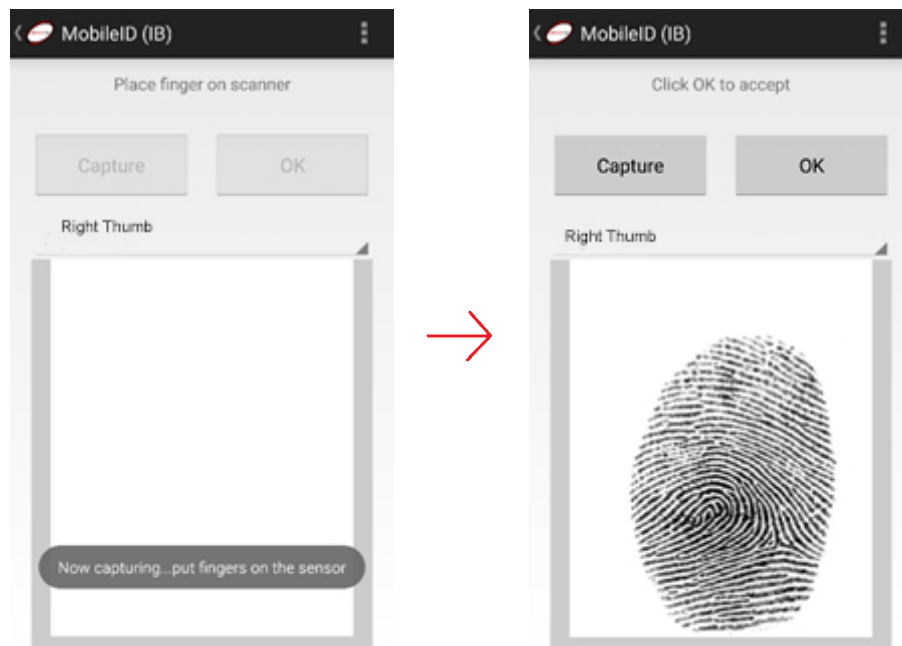
## Fingerprint Capture

To perform fingerprint capture, you will need to complete each of the following steps:

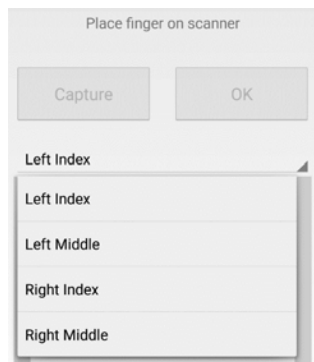
1. Unplug the power cable and tap the on-screen **Capture** button at the bottom of the RAPID-ID application main menu.



2. The user will receive a message to “Place finger on scanner,” and the drop-down menu in the middle of the screen will state which finger to capture. In the following example, the user has been instructed to capture the right thumb. The large white box at the bottom of the screen will show a live image preview of the individual’s finger as it is placed on the platen. **NOTE: In order for the scanner to detect the presence of a finger, the finger must make contact with the metallic bezel.**

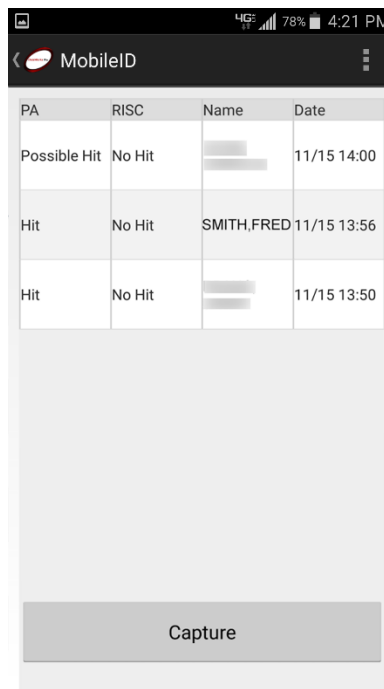


If needed, you can press the “Capture” button to re-attempt the capture again. Otherwise, press the **OK** button to accept the fingerprint and proceed to the left thumb. You will need to capture two finger images for each RAPID-ID transaction.



**NOTE:** If a finger is missing or bandaged, click the arrow at the right of the screen, then select a different finger for capture from the drop-down list.

3. Once the required fingerprints have been captured, they will automatically be submitted for matching against the State and FBI database. The new transaction will be displayed on the transaction list with a "Waiting for Response" status. Transaction results will typically be returned within around 3 minutes. Instructions for viewing detailed response data has been provided in the Responses section of this guide starting on page 19.



## Additional Options for Fingerprint Capture

The fingerprint capture process has an additional options menu which can be accessed by tapping on the three-dot menu drop-down icon (Options Menu) at the top right of the application's main menu screen. A description of the available options has been provided with the following image.

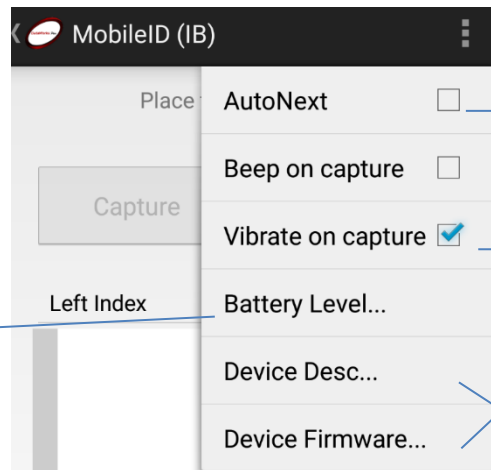


**Beep on capture**

Check this box to allow audible beep notifications on fingerprint capture.

**Battery Level**

Checks the battery level of the device.

**Options Menu Button****AutoNext**

Toggles automatic fingerprint capture.

**Vibrate on Capture**

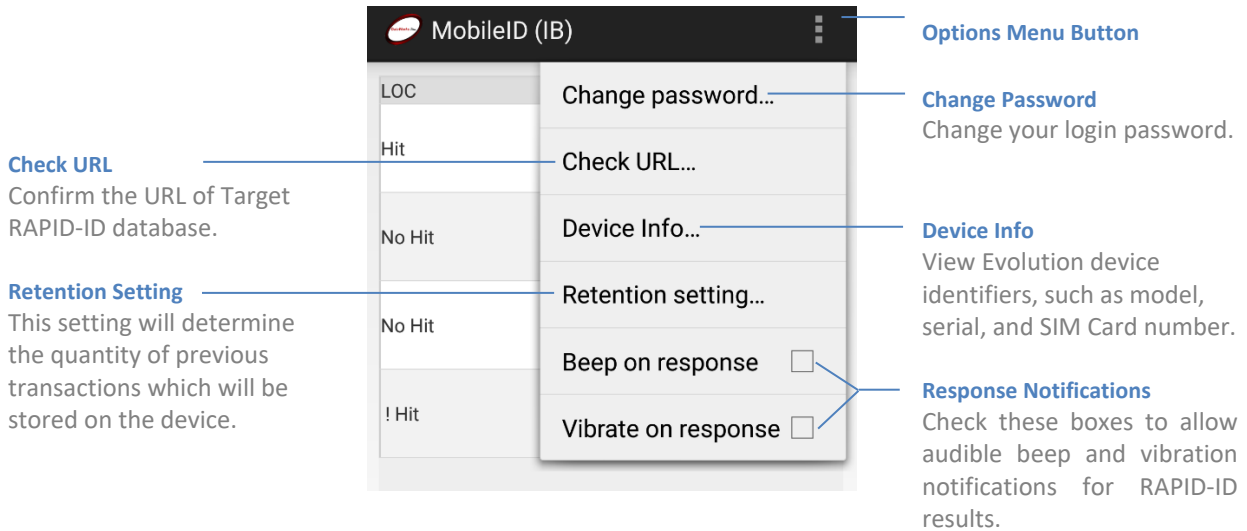
Check this box to allow vibration notifications on fingerprint capture.

**Response Notifications**

View Evolution device identifiers, such as description and firmware version.

### Additional Options for the RAPID-ID Application

The RAPID-ID application has an additional options menu which can be accessed by clicking on the three-dot menu drop-down icon at the top right of the application's main menu screen. A description of the available options has been provided with the following image.



## Responses

### Hit/No Hit/Possible Hit Responses Returned to Evolution's Transactions Screen

Responses will be returned to the Evolution device within a few minutes. Once a RAPID-ID search has been initiated you should receive one of three messages, "Possible Hit", 'No Hit' or 'Hit' on Transaction Status list. Please note that FBI and state results are returned separately, and may have different statuses. New results that have not yet been viewed on the device will have an exclamation mark (!) before them.

The "STATE" (shown PA in following image) and "FBI" columns each display either a Hit or No Hit status for each transaction. In this case, one transaction has received a hit from the state database, but not from the FBI.

#### Transaction History Pane

Each transaction will display three columns of data, including the state's status, FBI status, and Name of transaction. Detailed data is accessible by clicking on the desired transaction on the list.

PA	RISC	Name	Date
Possible Hit	No Hit	[REDACTED]	11/15 14:00
Hit	No Hit	SMITH,FRED	11/15 13:56
Hit	No Hit	[REDACTED]	11/15 13:50

Capture

- **No Hit:** indicates that there were no matching fingerprint records in any of the configured databases.
  - **Hit:** indicates matching fingerprint record(s).
- NOTE:** A 'Hit' in the RAPID-ID system is an indication that the subject's fingerprints match the fingerprint record(s) of those in one or more of the available fingerprint databases. IT DOES NOT NECESSARILY INDICATE THERE ARE ANY OUTSTANDING WARRANTS FOR THE INDIVIDUAL. Further research on other systems is required to make that determination.

## View Detailed Responses on Evolution

To view detailed transaction record information, tap on the desired transaction from the list, and the full set of data from state or FBI will be displayed for review. Tapping the back button (<) at the bottom right next to the Home button will return you to the transaction menu list.

### Back Button

This button will return you to the Transaction List

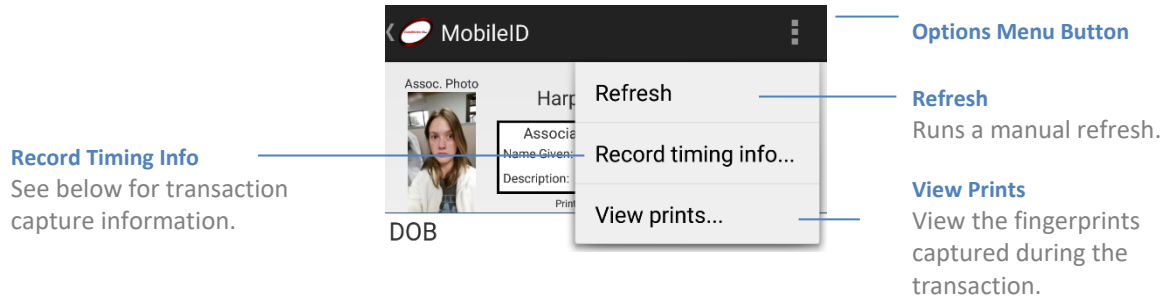
The screenshot shows the MobileID application interface. At the top, the status bar displays 4G LTE, 78% battery, and 4:21 PM. The app header shows a back arrow, the MobileID logo, and a menu icon. Below the header, there are two photo placeholders: 'Assoc. Photo' (a blue silhouette) and 'Hit Photo' (a photo of a man). The name 'SMITH, FRED' is displayed in the center. Below the name is a box labeled 'Association Information' containing 'Name Given:' and 'Description:' fields. A timestamp 'Printed on: 11/15 13:56' is at the bottom of this section. The main content area is titled 'PA Result IDENTIFIED'. Below this, several fields are listed: 'SID' (with a redacted value), 'DOB' (with a redacted value), 'Sex' (M), 'Race' (redacted), 'Height' (510), and 'Weight' (0). At the bottom, there are navigation arrows and the text 'Hit 1 of 2'.

### Record Data

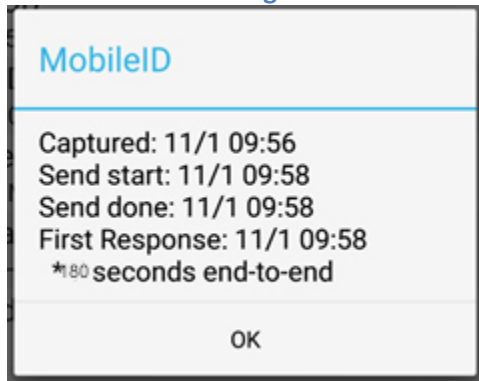
Any record data retrieved from the State or the FBI will be displayed on this screen. If multiple data targets have been retrieved, then the "1 of 1" indicator at the bottom of the screen will show the total number of record result datasets received. You can click on the arrow to scroll through any retrieved data sets if hits from multiple databases are acquired in a single transaction.

### Transactions Screen Options

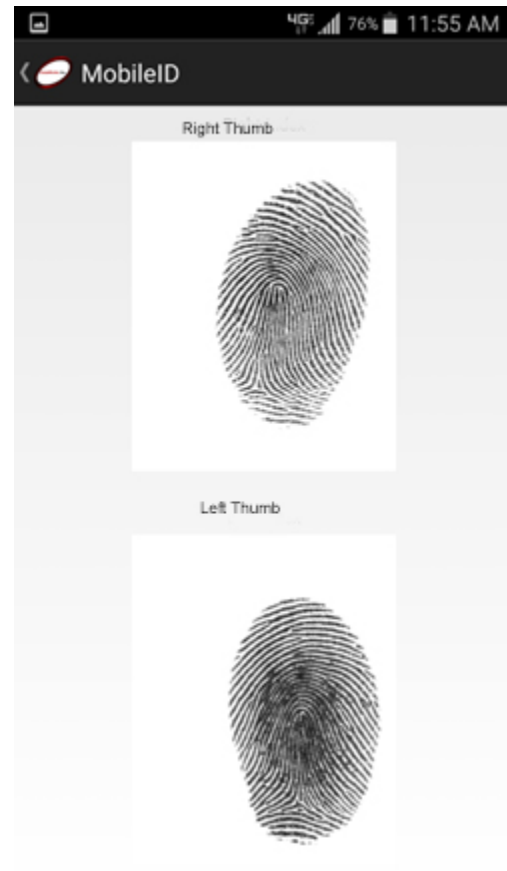
Each transaction has an additional options menu which can be accessed by clicking on the three-dot menu drop-down icon at the top right of the application's main menu screen. A description of the available options has been provided with the following image.



#### Record Timing Info



#### View Prints





## Repository for Individuals of Special Concern (RISC)

---

RISC consist of records of known or appropriately suspected terrorists, wanted persons, registered sexual offenders, and (potentially) other categories of heightened interest warranting more rapid responses to inquiring criminal justice users. Any additional categories proposed for inclusion, such as missing persons or protection order subjects that have associated biometrics currently in NGI could be considered for RISC.

The thumb prints captured by the Mobile ID device are transmitted to the user agency's existing criminal justice infrastructure, then on to the RISC. The RISC will conduct so-called "lights-out" processing using fewer than ten fingerprints. Lights-out processing refers to searches that are conducted entirely by computer automation, without any intervening involvement by humans. The submission will result in an automated search of RISC records and lights-out generation of a response to the requestor's criminal justice infrastructure within ten seconds of the submission. The requestor's criminal justice infrastructure will then forward the response to the requestor's Mobile ID device through its own communication channels. The RISC responses will be either "Hit," "Probable," "No Hit," or "reject."

**Hit.** A Hit response, indicating identification of a highly probable candidate in the RISC. However, a red response is not to be considered a positive identification, but rather the candidate score from the RISC search indicates a high likelihood of identification. (The term "positive identification" currently is reserved for the results of a complete ten-print search and/or confirmation of a match by trained fingerprint examiners.) It will be incumbent on the submitting agency to supplement the RISC response with other information to confirm whether or not the candidate returned is indeed the person whose prints were submitted.

A Hit will contain the following additional information from NGI: the category of hit (e.g., wanted person, sexual offender registry subject, or known or appropriately suspected terrorist), the identified subject's FBI Number (FNU) and master file name, and if requested by the law enforcement official, any available photos of the subject maintained in the NGI Interstate Photo System (IPS).<sup>3</sup>

Furthermore, for Hit responses where underlying details of the hit may be important to officer/public safety (e.g., wanted persons or known or appropriately suspected terrorists), the RISC will cascade an automated inquiry of the National Crime Information Center (NCIC) person files using the matched subject's FNU. If matching NCIC data is located, the RISC response will contain pertinent data fields from the relevant NCIC file(s), including NCIC excerpts indicating the nature of any offenses and any applicable warnings or cautions.

**Probable.** A probable response is a possible hit, indicating identification of a possible candidate (or candidates) in the RISC but one below the level of confidence established for a highly probable match (red response). The yellow response may thus only be used as an investigative tool providing leads for further investigative inquiries.

Probable responses may contain the same type of supplemental information as red responses pertinent to the person(s) identified as a possible match (i.e., yellow responses may contain information from NGI regarding the category of the possible hit and underlying details, name and associated system numbers, and available photos). This may, for instance, include photos or other biographic data of possible candidates that could assist the requestor in ascertaining if the candidate is, or is not, a match.

**No Hit.** A No Hit response indicates no hit (i.e., the search did not locate a viable candidate in the RISC).

**Reject Response.** The RISC will return a reject response when the quality of the RISC submission is too low to be used for a RISC search.

## Troubleshooting

### System Returns False Positive or 'NO HIT' for Known Subject





Generally this is a result of poor fingerprint quality.

**To Capture High Quality Prints:**

- Check Proper Finger Placement
- Check Environment/Cleanliness
- Check Condition of Fingers

#### Check Proper Finger Placement

Examples of good and bad quality fingerprints are shown in the following chart.

Good Quality	Bad Quality - Tip of Print	Bad Quality - Missing Core	Bad Quality - Too High
			
The core (center) of the fingerprint is in the center of the fingerprint and all of the print is captured.	Only the tip of the finger was placed on the scanner, such as in the incorrect example above. The core of the fingerprint is missing.	The finger was placed on the scanner slightly on the side. The core of the fingerprint is missing.	The finger was placed too high on the scanner so that the half of the fingerprint was not scanned.

The finger should be flat on the platen, with the correct amount of pressure. If the finger is pointed when placed on the device then you will not capture a full fingerprint image. If too little pressure is used, then the fingerprint image may be too light. If too much pressure is used, then the fingerprint image may be too dark. It is important to try to capture the entire core of the fingerprint. When placing the finger on the device, try to center the fingerprint on the scanner. If the core of the fingerprint is not captured, then you may not receive a hit against the central server, even if a matching print exists.

**Check Environment/Cleanliness**

(See *Maintaining the Evolution* on page 13.) The type of environment the fingerprint device is being used in may affect the image quality, especially when high amounts of moisture or dust are present. If the scanner has any moisture from the environment or has oil and artifacts from previous captures, then wipe the fingerprint scanner with a microfiber towel.

The cleanliness of the scanner may affect the fingerprint quality image. It is suggested to wipe the scanner clean between capturing fingerprint images to ensure that there is no dirt, residue, dust, or other particles on the pad that may interfere with the fingerprint image being captured.

**Check Condition of Fingers**

The fingers being used may also affect the image quality. The fingers may be too dry, sweaty, or smooth to produce high quality fingerprint images. Each of these circumstances can be fixed to produce a better quality image.

**Wet or Sweaty Fingers**

- If the finger is too wet, the fingerprint image will appear very dark and smeared. If this occurs, use a lint free cloth or small fan to dry the fingers. You should also clean the scanner with a lint free cloth prior to recapturing the fingerprint image to remove any residue left from the previous attempt.

**Dry Fingers**

- If a person's fingers are very dry, the fingerprint image may appear too light and will not be of sufficient quality to use for comparison. This can be rectified by wiping the finger with a moisturizing towel or a small amount of hand lotion. The individual can also wipe their finger along their forehead to add additional moisture to the finger.

**Lack of Fingerprint Detail**

- A smooth fingerprint surface is common among construction workers or with some injuries. If the surface appears to be too smooth to capture a high quality fingerprint image you may need to try to use the non-dominant hand to capture a better fingerprint image since it may not be worn down as much as the dominant hand's fingerprints.

## Support

---

**Call**

• 1-866-632-2780 - Dial 3 for Technical Support

**Email**

• support@dataworksplus.com

### Information to Have Available

It is always helpful if you know the machine name that is having the problem, as well as the type of fingerprint scanner if the problem relates to those devices. We will also ask for the name and phone number of someone near the unit that is experiencing the problem.

### Opening a Support Ticket

When you call in to the toll-free number, our support technicians will open a support ticket for you. This ticket number is available for your records, should you need it, and it ensures that your system problem is accurately handled by our company.

### Resolving the Problem

Calls that come into the support center are logged in our call tracking system. At that point, calls are handled as follows:

1. Assigned to a technician for review and diagnosis.
2. Calls that cannot be diagnosed and handled quickly are escalated to a senior engineer.
3. The ticket may be escalated to a local technician or vendor in the customer's geographical area, if necessary.
4. The senior engineer may work with our development team to resolve software issues.

At all points, the support technician is responsible for keeping the customer updated on the progress of the ticket.

### Obtaining Replacement Parts

Should the technical support department determine that new parts or devices are needed for your equipment, we will issue an RMA from here to send the part directly to your site. When the part arrives, please use the return shipping label to ship the damaged part back to us.

### After-Hours Calls

Technicians are available in-house Monday through Friday from 7:00 A.M. until 6:00 P.M. EST. For after-hours calls, please use the same number listed above and press "3" for support. When prompted, please leave your name and number and our on-call technician will call you back promptly.

### Escalation of Tickets

If a ticket needs to be escalated, a technician will contact Deanna Allen, Director of Technical Support; she will review the ticket and handle appropriately.