# Annapolis Police Department

**GENERAL ORDER**

**Number: I.9**

**Issue Date: March 2013**

**TO:** All Personnel

**SUBJECT**: Portable Fingerprinting Identification System

## PURPOSE

The purpose of this policy is to establish guidelines and operating procedures for the use of portable fingerprint identification devices.

## POLICY

The Annapolis Police Department is providing portable fingerprint identification devices to members within the agency as a tool in the identification of individuals in the field, especially those with no identification documents. These devices are to be used only in conformance with the following procedures and existing law.

## REQUIRED ACTION

I. General

A. The portable fingerprinting device system shall only be used for official business purposes, consistent with agency policy, training and law. Users are advised that assignment of a portable fingerprint identification device does not confer or suggest independence authority to order a citizen to identify him or herself. All existing rules, regulations and laws governing consensual or non-consensual fingerprinting shall be strictly followed.

B. The use of the devices is limited to those members who have been trained and authorized to operate the devices. Passwords to access the system will not be shared or made known to any other individual. Members who have reason to believe their password has been compromised shall immediately notify Information Technology to have the password changed.

C. The portable fingerprinting device system may be used as an investigative tool with limitations. The device can be used incident to an arrest or when the individual gives consent.

EXAMPLES:

1. A citizen is stopped while operating a motor vehicle for a violation of a motor vehicle statute which requires their appearance in court. The operator can produce no identification. Under these circumstances, the detaining officer could conduct a warrant-less arrest, but obtaining positive identification via the portable fingerprinting device system provides the alternative of issuing a traffic citation.
2. An officer has probable cause to believe a citizen has committed a misdemeanor for which a Criminal Citation may be issued but the individual's identity cannot be positively confirmed and there is not a requirement to process the individual under General Order C.13 (i.e. urinating in public) The officer, although authorized by law to arrest the person, may use the portable fingerprinting device system provides an alternative to arrest.

D. Officers will be guided by General C.13 when issuing citations. The portable fingerprint device does not replace the obligation of processing individuals under certain circumstances.

E. The instructions for end users to operate the system are given in Appendix A. Each computer used to connect the device to the databases must be setup to connect via Bluetooth to the device and connect through the VPN to the secured website that accesses the databases.

II. Fingerprint Returns

.

A. When checking an individual's fingerprints users should remember that the system checks the Maryland Automated Identification System (MAFIS) database, and the FBI Repository for Individuals of Special Concern (RISC) database. The MAFIS system has the fingerprints of individuals who were fingerprinted using a digital capture system and those fingerprints which have been converted from paper to digital formats. The RISC database has only those who are wanted for a serious offense, a known or suspected terrorist (KST) or sex offender.

B. Persons who have not been fingerprinted previously and persons whose fingerprints have not been digitized will not show a "hit" in the Portable fingerprinting device system.

C. A "hit" on the portable fingerprinting device indicates only that a match to existing digitized fingerprint records. Any information about the matching individual will be displayed on the computer screen that is connected through a Bluetooth connection.

III. Electronic Record

Officers are reminded that the portable fingerprint unit is an electronic device and capable of storing information when the unit was deployed, who the operator was, who was scanned, the date, and the time the device was used.

Michael A. Pristoop
Chief of Police

| References |
|---|
| 1. Accreditation Standards None<br>2. Reference: General Order C.13, Criminal Citations |

**Revision:** This is a new General Order.

Appendix A

Version 2.0

# Web ID™ with FBI RISC® BlueCheck Quick User Guide

COGENT

Cogent Document # UG-EXT-UG-xxxx-2.0

### Document Revision History

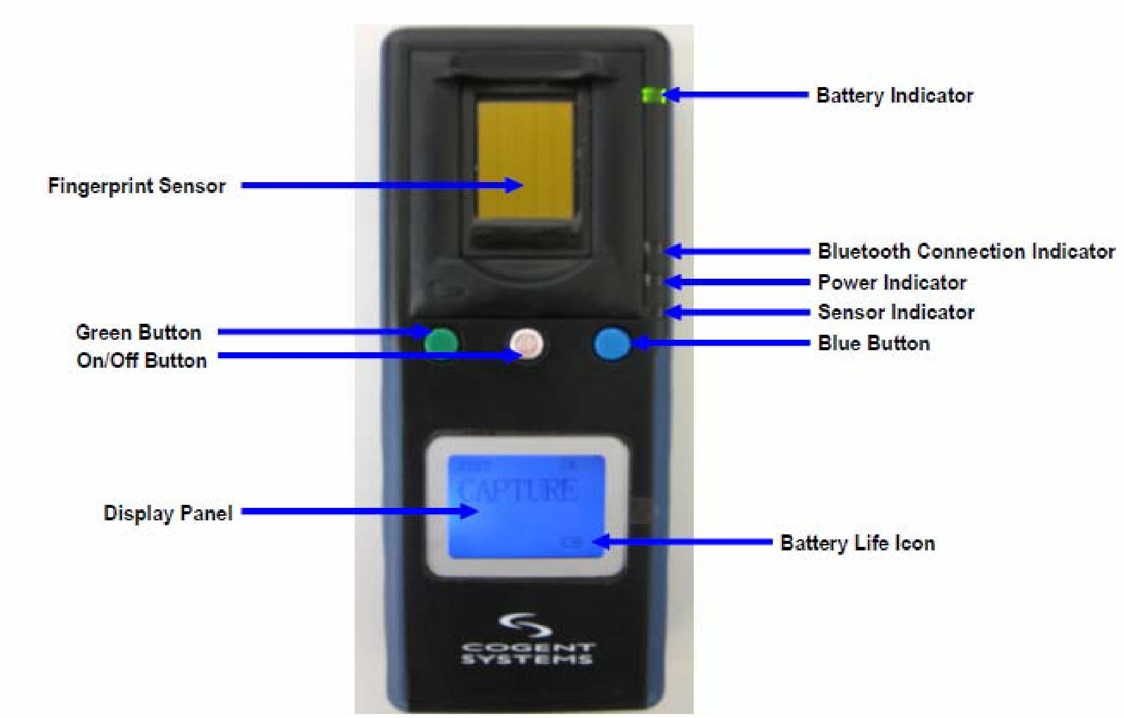
| Version | Date | Author | Comment |
|---|---|---|---|
| 1.0 | 07/2010 | Sonia Robb | Initial version |
| 2.0 | 09/2010 | Sonia Robb | Screenshots updated |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## QUICK USER GUIDE

1. Turn Laptop/Desktop On
2. Log into Windows
3. Plug Bluetooth Adapter in USB port

4. Double Click the **Web ID icon** on your Windows desktop
5. Enter User Name and Password to login
6. Click YES on all Windows Security popup
7. Hold down the On/Off Button until the BlueCheck Device turns on.
8. The Power Indicator will turn red, and *CAPTURE* will be displayed on the Display Panel. In addition, the Bluetooth Connection Indicator* will turn solid blue when the device has established a Bluetooth connection with your computer.
   *You will not be able to send Fast ID any captured fingerprint images until the Bluetooth Connection Indicator has turned solid blue.
9. To capture a subject's fingerprints with the BlueCheck device, ensure that CAPTURE is displayed on the Display Panel

**NOTE:** If the BlueCheck device is turned on before launching the Fast ID application, it may take up to 20 seconds to establish a Bluetooth connection after the application is started.



**Additional Notes:**

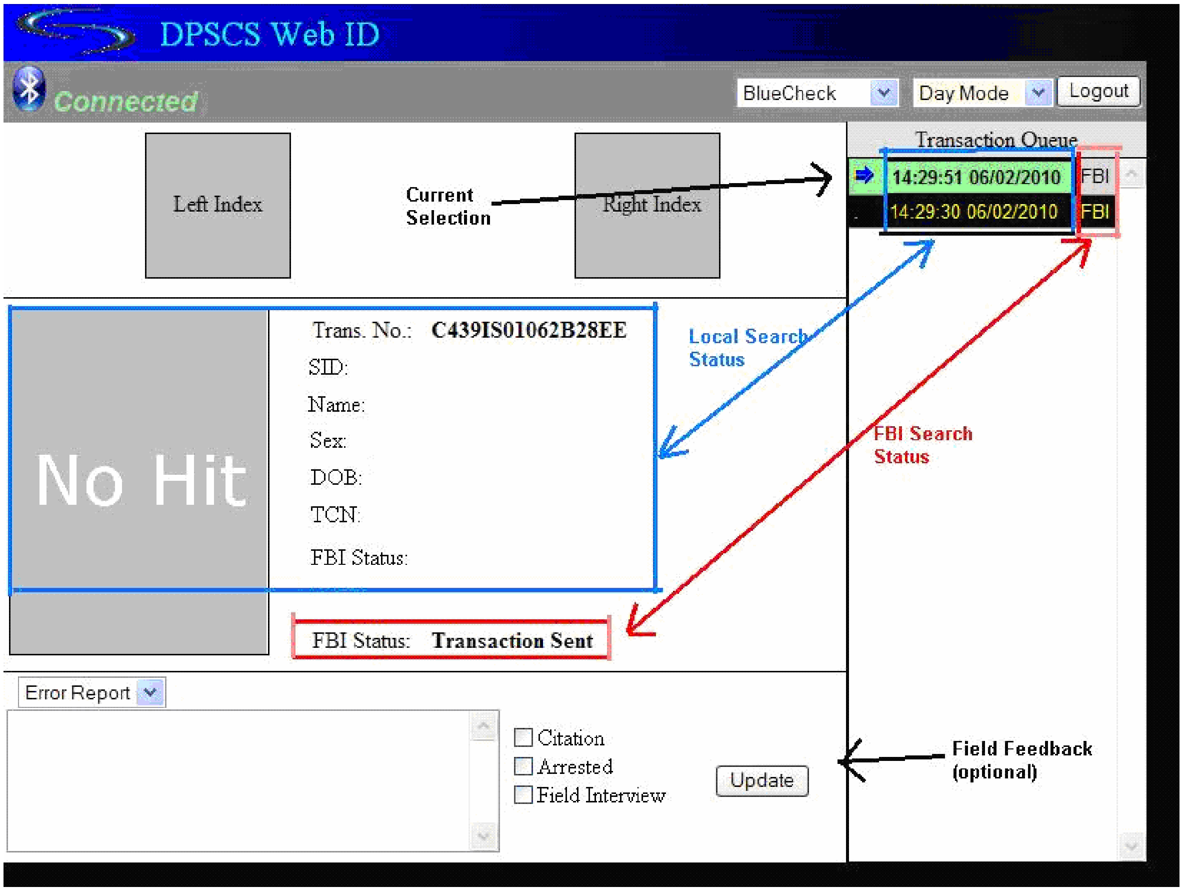
- Click on the **Green Button** ● to navigate BlueCheck device features:

-**CAPTURE** to capture new prints
-**CALIBRATE** to calibrate the device
-**SEND** to send prints that were previously taken but not sent to FAST ID application
-**ESC** to return to CAPTURE mode

- Click on the **Blue Button** ● to navigate fingerprints options:

-**OK** to Capture, Send or Calibrate the BlueCheck device
-**MISS** to skip a finger
-**SEND** to send prints that were previously taken but not sent to FAST ID application

*Please refer to the following screen shot to see a breakdown of the screen layout:*



Transaction Queue

14:29:51 06/02/2010 FBI

14:29:30 06/02/2010 FBI

Trans. No.: C439IS01062B28EE
SID:
Name:
Sex:
DOB:
TCN:
FBI Status:

FBI Status: Transaction Sent

□ Citation
□ Arrested
□ Field Interview

Current Selection

Local Search Status

FBI Search Status

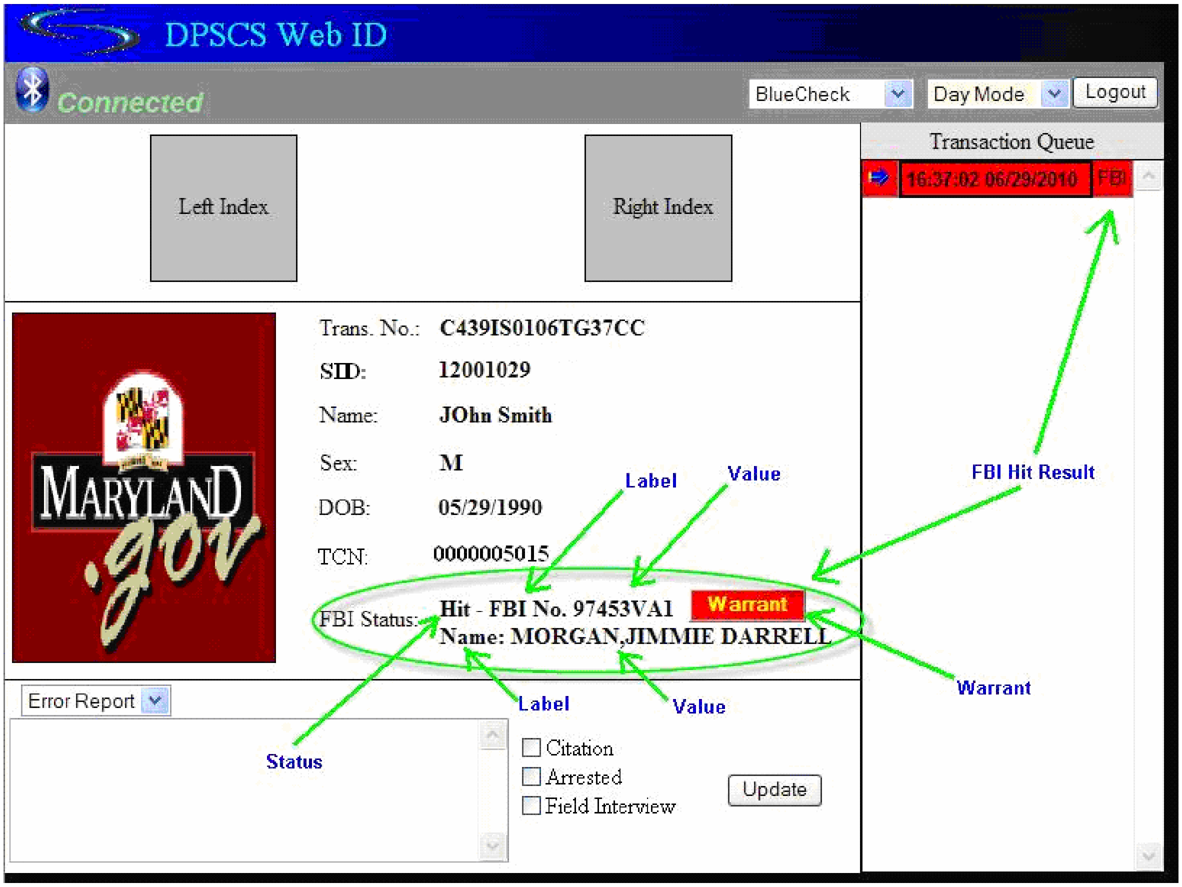
Field Feedback (optional)

1. Transactions in the "Transaction Queue" are identified by transaction time rather than by transaction number for easier identification.

2. The time portion of each transaction represents the local search and he FBI box represents the FBI search.

3. The transaction status are color-coded as below:

| | |
|---|---|
| **Black** | - Errors (Bad Quality, Duplicate Fingers and Server Transmission Error etc) |
| **Gray** | - Searching |
| **Green** | - No hit |
| **Red** | - Hit |
| **Yellow** | - Maybe Hit (as specified by FBI) |



16:37:02 06/29/2010 FBI

Trans. No.: C439IS0106TG37CC

SID: 12001029

Name: JOhn Smith

Sex: M

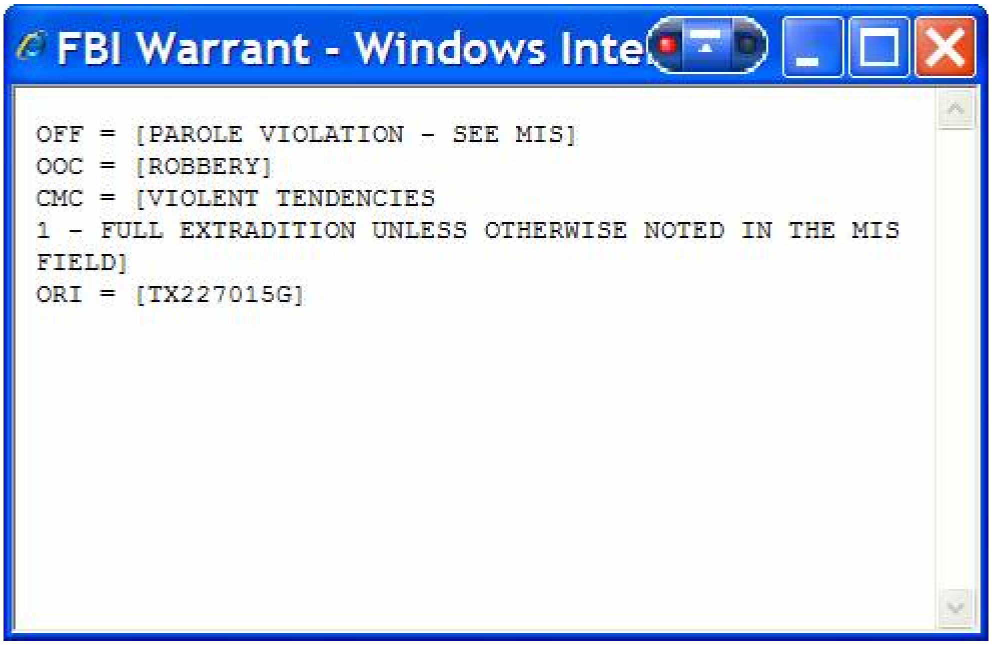
DOB: 05/29/1990

TCN: 0000005015

FBI Status: Hit - FBI No. 97453VA1 Warrant
Name: MORGAN,JIMMIE DARRELL

□ Citation
□ Arrested
□ Field Interview

Here is a sample screen shot of the FBI warrant:



```
OFF = [PAROLE VIOLATION - SEE MIS]
OOC = [ROBBERY]
CMC = [VIOLENT TENDENCIES
1 - FULL EXTRADITION UNLESS OTHERWISE NOTED IN THE MIS
FIELD]
ORI = [TX227015G]
```

Important: Please note that having a “regular” rap sheet in FBI IAFIS will not guarantee a RISC (Repository for Individuals of Special Concern) hit. The person must be wanted, a KST (Known or Suspected Terrorist) or Sex Offender.

Appendix B

▪ Version 1.7

# Web ID™ with BlueCheck® Installation Guide * For S.W.G.I. Users

Cogent Document # IG-EXT-IG-1020-0.0 (4)

**Document Revision History**

| Version | Date | Author | Comment |
|---|---|---|---|
| 1.0 | 04/2009 | Integration Group | Initial version |
| 1.1 | 05/2009 | Integration Group | Updated the document |
| 1.2 | 06/2009 | Integration Group | Updated the document |
| 1.3 | 01/2010 | Sonia Robb | Updated the document |
| 1.4 | 02/2010 | Sonia Robb | Updated the Document |
| 1.5 | 06/2010 | Sonia Robb | Changed download url |
| 1.6 | 07/2010 | Sonia Robb | Changed to new server |
| 1.7 | 10/2010 | Sonia Robb | Updates |
| | | | |
| | | | |

## Contents

## Maryland Web ID with BlueCheck Installation Guide

This guide is only applicable to SWGI users only!

### Edit Host File

1. Navigate to **C:\WINDOWS\system32\drivers\etc**
2. Open the "**hosts**" file with Notepad
3. Enter the following line:

```
10.23.100.237    webid.swgi.dpscs.state.md.us
```

4. Save and close the "hosts" file

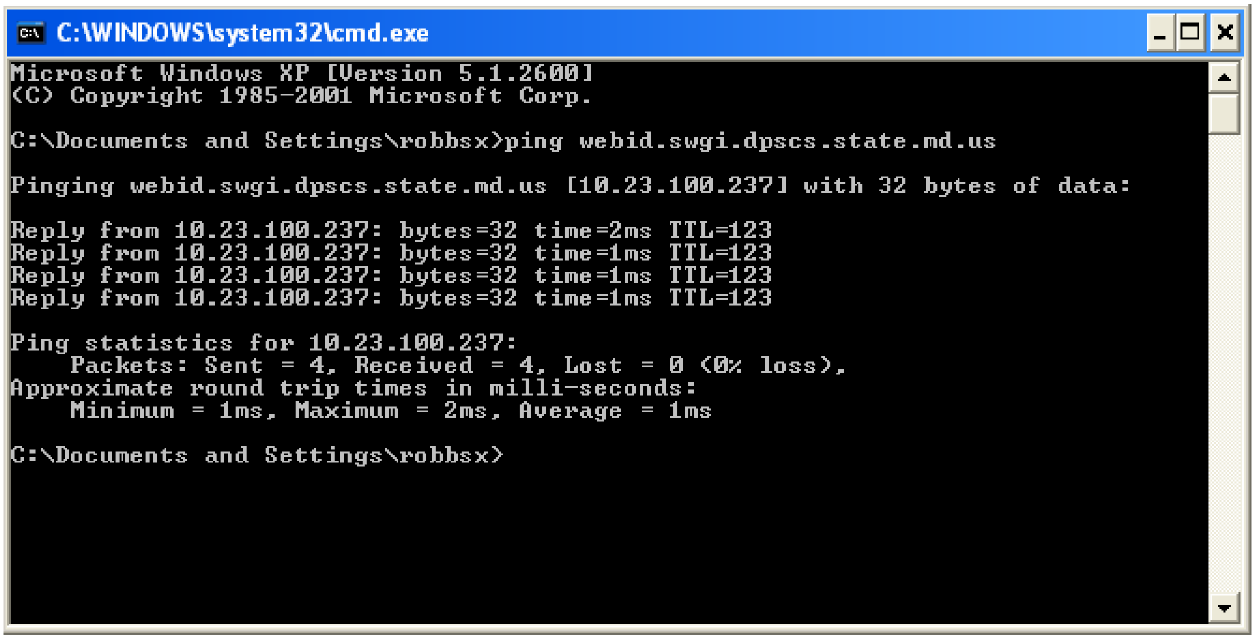
### DNS Resolution

**Check DNS Resolution by running a ping test in dos command window:**

1. Click Start > run > cmd >
2. Click ok
3. At the command prompt: type > ping webid.swgi.dpscs.state.md.us
4. Hit Enter

The result shall be similar to the display below

The "Reply from" line shall read: Reply from 10.23.100.237



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\robbsx>ping webid.swgi.dpscs.state.md.us

Pinging webid.swgi.dpscs.state.md.us [10.23.100.237] with 32 bytes of data:

Reply from 10.23.100.237: bytes=32 time=2ms TTL=123
Reply from 10.23.100.237: bytes=32 time=1ms TTL=123
Reply from 10.23.100.237: bytes=32 time=1ms TTL=123
Reply from 10.23.100.237: bytes=32 time=1ms TTL=123

Ping statistics for 10.23.100.237:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Documents and Settings\robbsx>
```

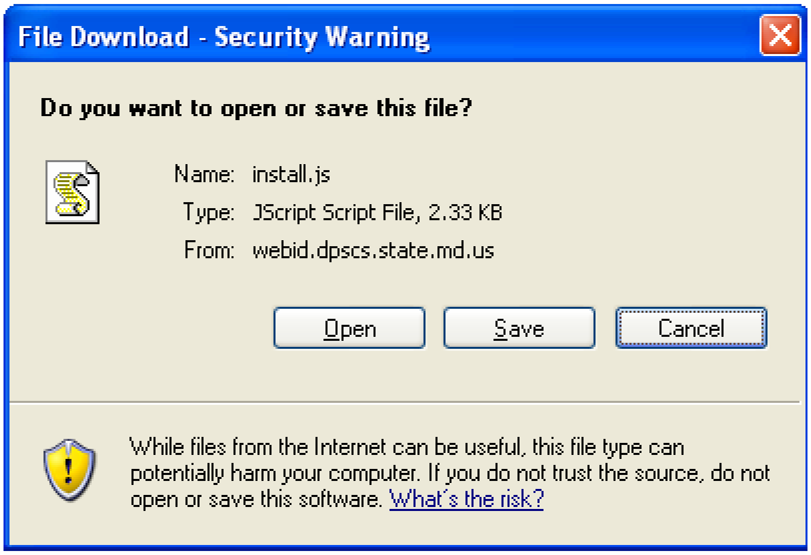
### Install ActiveX Controls

1. Open an Internet Explorer browser

2. Enter the following in the address bar and press **<Enter>**:

   ```
   https://webid.swgi.dpscs.state.md.us/setup/install2.js
   ```

   The **File Download** dialog box will be displayed (*Figure 1*).



File Download - Security Warning

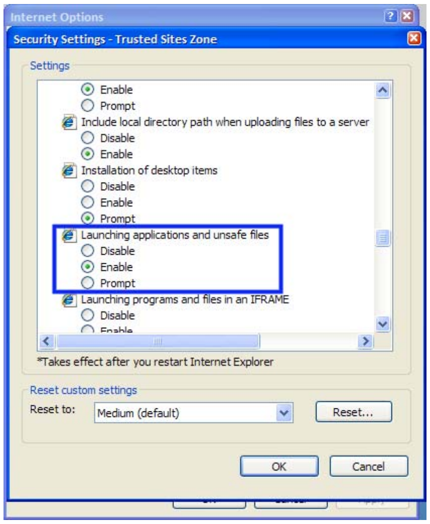
Do you want to open or save this file?

Name: install.js
Type: JScript Script File, 2.33 KB
From: webid.dpscs.state.md.us

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

**Figure 1- File Download Dialog Box**

**NOTE**: If the **File Download** box is not displayed, verify that your Internet Explorer® settings for trusted sites are up to date. "Launching applications and unsafe files" should be set to **Enable** (*Figure 2*).



Internet Options

Security Settings - Trusted Sites Zone

Settings

- ● Enable
- ○ Prompt
- Include local directory path when uploading files to a server
  - ○ Disable
  - ● Enable
- Installation of desktop items
  - ○ Disable
  - ○ Enable
  - ● Prompt
- Launching applications and unsafe files
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Launching programs and files in an IFRAME
  - ○ Disable
  - ○ Enable

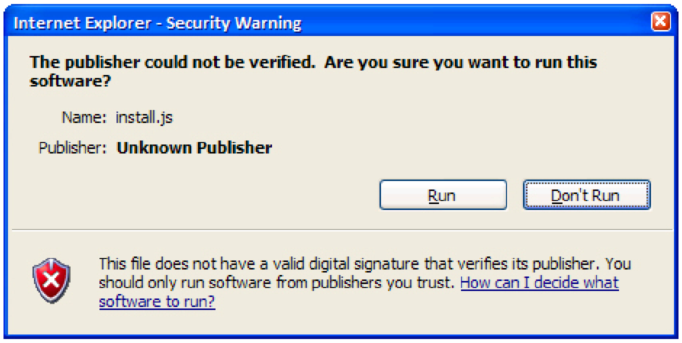
*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: Medium (default)

**Figure 2- Internet Explorer Security Settings – Trusted Sites Zone**

3. Click **Open**. The **Security Warning** dialog box will be displayed (*Figure 3*).



The publisher could not be verified. Are you sure you want to run this software?

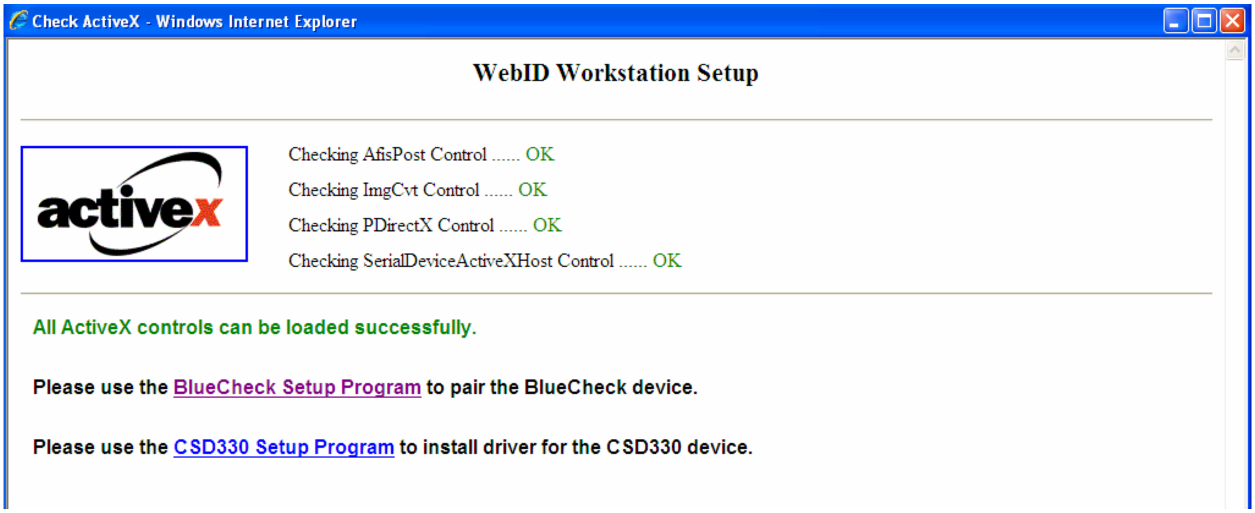
Name: install.js

Publisher: Unknown Publisher

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

Figure 3- Security Warning Dialog Box

4. Click **Run**



WebID Workstation Setup

Checking AfisPost Control ...... OK

Checking ImgCvt Control ...... OK

Checking PDirectX Control ...... OK

Checking SerialDeviceActiveXHost Control ...... OK

All ActiveX controls can be loaded successfully.

Please use the BlueCheck Setup Program to pair the BlueCheck device.

Please use the CSD330 Setup Program to install driver for the CSD330 device.

Figure 4- ActiveX Controls Installed Successfully

5. Do **NOT CLOSE** the browser.

### Install the Linksys® Bluetooth Adapter

To install the Linksys Bluetooth Adapter, plug it in to a USB port on the computer. Windows® will automatically the adapter.

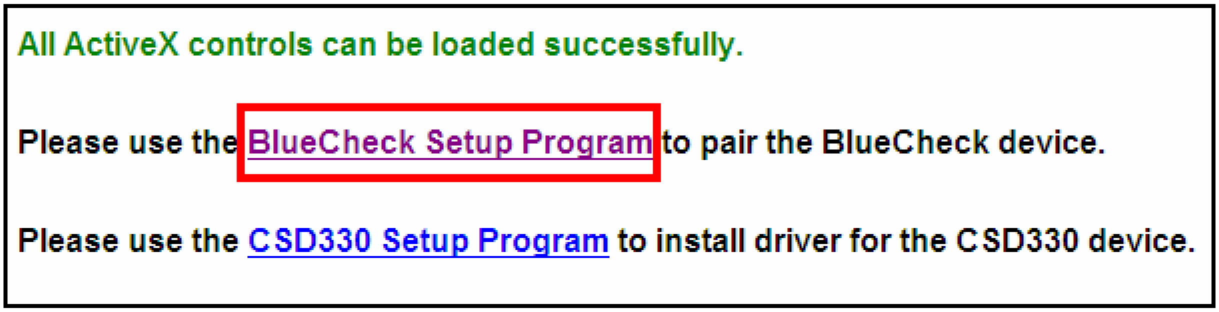
### Pair the BlueCheck with a Bluetooth-Enabled Computer

In order for the two Bluetooth-enabled devices to communicate with each other, you must perform Bluetooth pairing. When this is accomplished, the two devices join what is called a trusted pair relationship. When one device recognizes another device in an established trusted pair, each device automatically accepts communication, bypassing the discovery and authentication process that normally happens during Bluetooth interactions.

**NOTE**: Before pairing, ensure that the Linksys Bluetooth Adapter is plugged in to a USB port.

**To pair the BlueCheck with a Bluetooth-enabled computer:**

1. Click the **Bluecheck setup program** link on the browser.

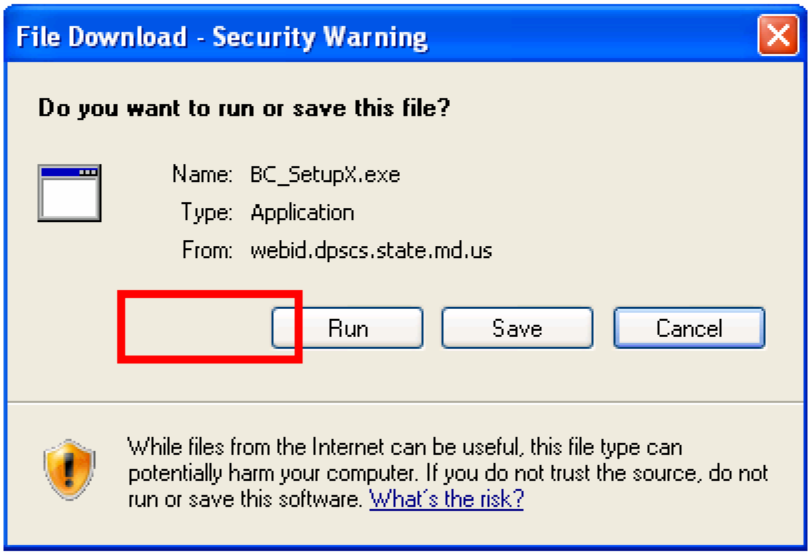


All ActiveX controls can be loaded successfully.

Please use the BlueCheck Setup Program to pair the BlueCheck device.

Please use the CSD330 Setup Program to install driver for the CSD330 device.

2. The **File Download** dialog box will be displayed (*Figure 5*).



File Download - Security Warning

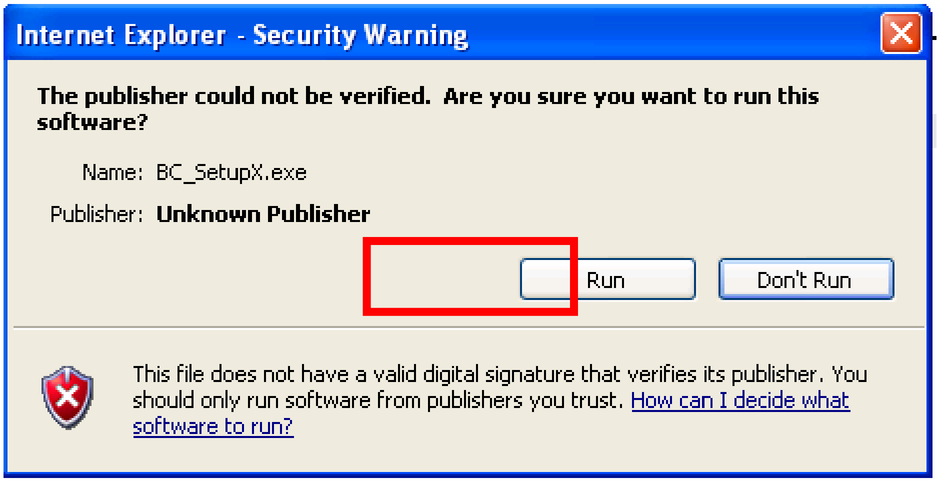
Do you want to run or save this file?

Name: BC_SetupX.exe
Type: Application
From: webid.dpscs.state.md.us

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

**Figure 5- File Download Dialog Box**

3. Click **Run**. The **Security Warning** dialog box will be displayed (*Figure 6*).



Internet Explorer - Security Warning

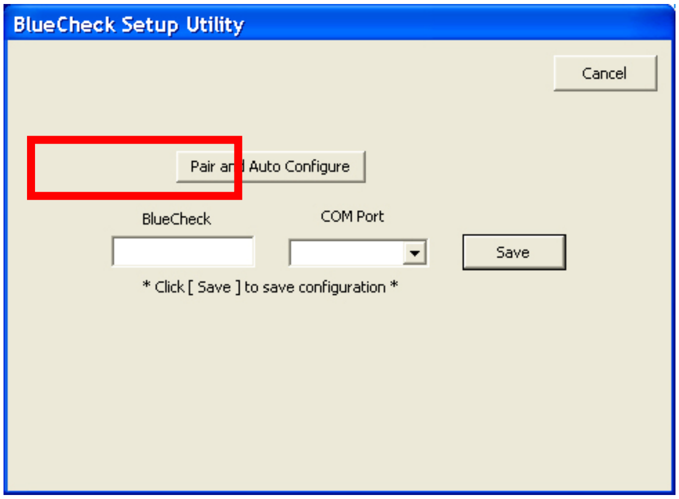
The publisher could not be verified. Are you sure you want to run this software?

Name: BC_SetupX.exe
Publisher: **Unknown Publisher**

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

**Figure 6- Security Warning Dialog Box**

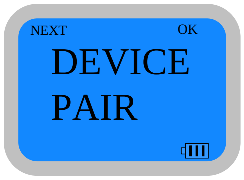
4. Click **Run**. The **BlueCheck Setup Utility** window will be displayed (*Figure 7*).



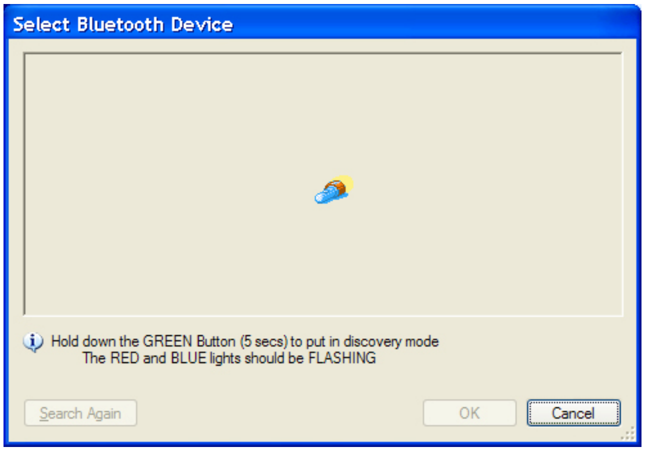
* Click [ Save ] to save configuration *

**Figure 7- BlueCheck Setup Utility Window**

5. Verify that your BlueCheck portable identification device is powered on and in pairing mode.

> **TIP**: To enter pairing mode, press and hold the Green button on the BlueCheck until the red and blue lights are blinking and the display reads *DEVICE PAIR* (*Figure 8*).
>
> 
>
>
> **Figure 8- Device Pair Message on BlueCheck Display**

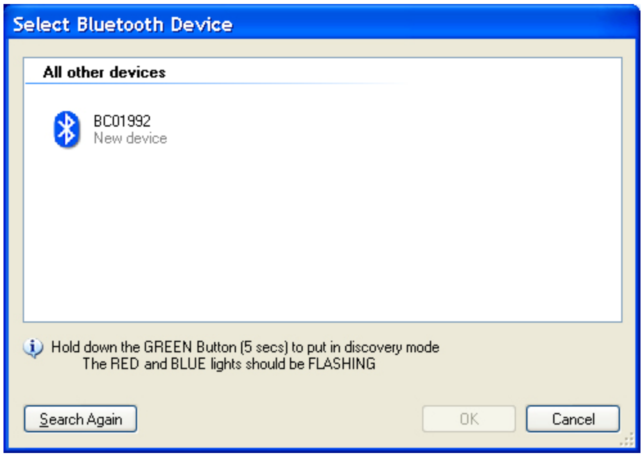
6. Click the **Pair and Auto Configure** button. A window will be displayed, indicating that Windows® is searching for Bluetooth devices in range (*Figure 9*).



Hold down the GREEN Button (5 secs) to put in discovery mode
The RED and BLUE lights should be FLASHING

**Figure 9- Searching for Bluetooth Devices in Range Window**

7. When the search is complete, the **Select Bluetooth Device** window will be displayed, listing available Bluetooth devices (*Figure 10*).



Select Bluetooth Device

All other devices

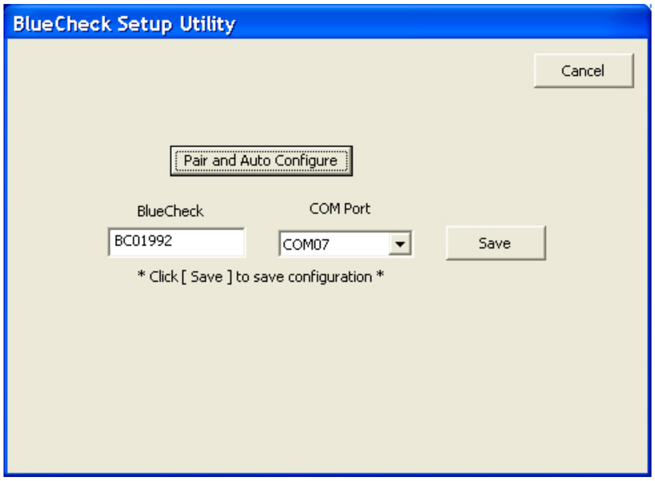
BC01992
New device

Hold down the GREEN Button (5 secs) to put in discovery mode
The RED and BLUE lights should be FLASHING

**Figure 10- Select Bluetooth Device Window**

8. Check the serial number on the back of your BlueCheck. This number should match one of the items displayed in the window.

9. Click the item corresponding to your BlueCheck device, then click **OK**. The **BlueCheck Setup Utility** window will be redisplayed, with your BlueCheck and COM Port shown in the corresponding fields (*Figure 11*).



BlueCheck Setup Utility

BlueCheck: BC01992

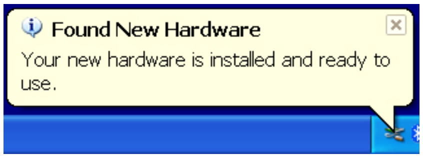
COM Port: COM07

* Click [ Save ] to save configuration *

**Figure 11- BlueCheck Setup Utility with BlueCheck and COM Port Displayed**

10. A series of balloons will be displayed in the computer system tray as the device is automatically configured. When this is complete, a balloon indicating success will be displayed (*Figure 12*). Click **Save** in the **BlueCheck Setup Utility** window to exit the utility.

> **NOTE**: Do not click **Save** in the **BlueCheck Setup Utility** window until the balloon shown in *Figure 12* is displayed. This may take a few seconds to display, as the device is being configured.



Found New Hardware

Your new hardware is installed and ready to use.

**Figure 12- Hardware Installed Successfully**

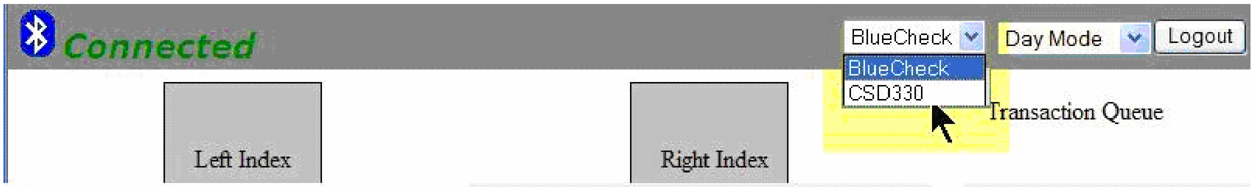
11. Click next to go to the “CAPTURE” screen. You can now use Web ID with BlueCheck.

## Edit the Web ID Icon

1. Rick click the WEB ID icon WebID on the desktop
2. Choose Properties
3. Edit the URL to show: https://webid.swgi.pscs.state.md.us/login
4. Click Apply and Ok to save

## Running the Web ID Application

1. Double click the WEB ID icon on the desktop to open
2. Click Yes on the Security Alert popup (You may not get this prompt)
3. Make sure the URL is: https://webid.swgi.dpscs.state.md.us/login
4. Enter your User Id and password and click Login
5. Pick the BlueCheck from the drop down list if not selected. (Bluecheck is selected by Default)
6. The windows shall display “**Connected**” in green.



7. Make sure that CAPTURE is displayed on the BlueCheck Display Panel (Figure 13)

TIP: To enter Capture mode, press the Green button to toggle between menu options until CAPTURE is displayed on the Display Panel (*Figure 13*).

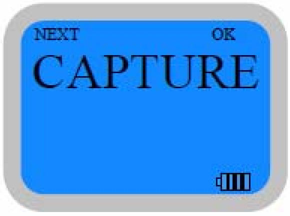


Figure 13- CAPTURE Message on BlueCheck Display

8. Click the Blue button (located above OK on the Display Panel). **R Index Please** will be displayed on the Display Panel.

**Please refer to the Maryland BlueCheck Quick User Guide for information on how to use the Device**