Tech. Note: 20040524008Configuring the AuthenTec Biometric device in Windows

Installation

OUTLINE
1. Download finger print read drivers, software, and software add on
2. Unzip 3 files to a temporary folders
3. Plug in Finger print reader, and load drivers
4. Install software
5. Install software add on
6. Remove Temporary folders

The drivers and application will have to be installed on all workstations where an AuthenTec device will be used, as well as on the Main Back-Office Server.

1. You will need to download the following 3 files: Biometric Fingerprint Drivers, Biometric Fingerprint Software Utility, and Biometric Fingerprint Software Add-On from http://www.posiflexusa.com/support/drivers.html

2. Unzip the 3 zip files to temporary directories i.e. C:\Temp\Driver, C:\Temp\Software, and C:\Temp\Add On.

3. Plug in the finger print reader into the USB port of the station. If you are running Windows XP, Windows will automatically install the drivers. For all other versions of Windows, you will need to point it to the location of the drivers (C:\Temp\Drivers).

4. Go to C:\Temp\Software and run Setup.exe
The Install Wizard appears. Click **Next**.
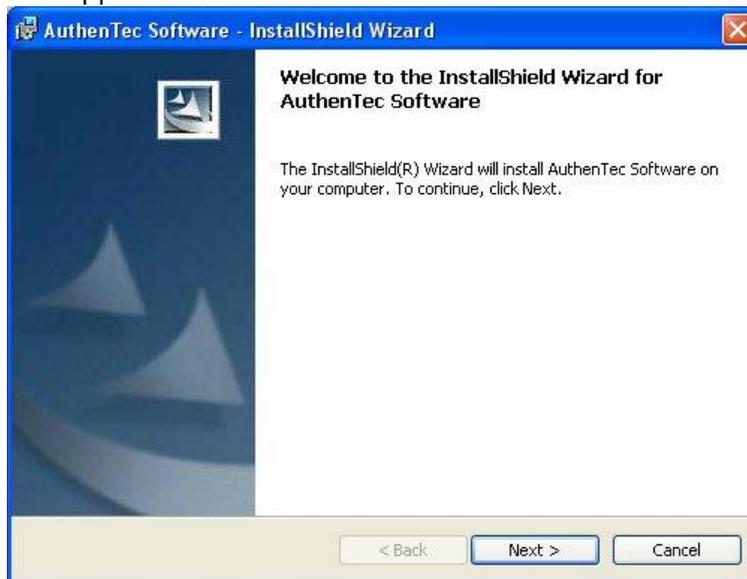
Read the end-user agreement, and if you do agree, select
I Accept the terms in the license agreement, and then click **Next**.

Enter in the Customer information, select **Anyone who uses this computer**, and then click **Next**.
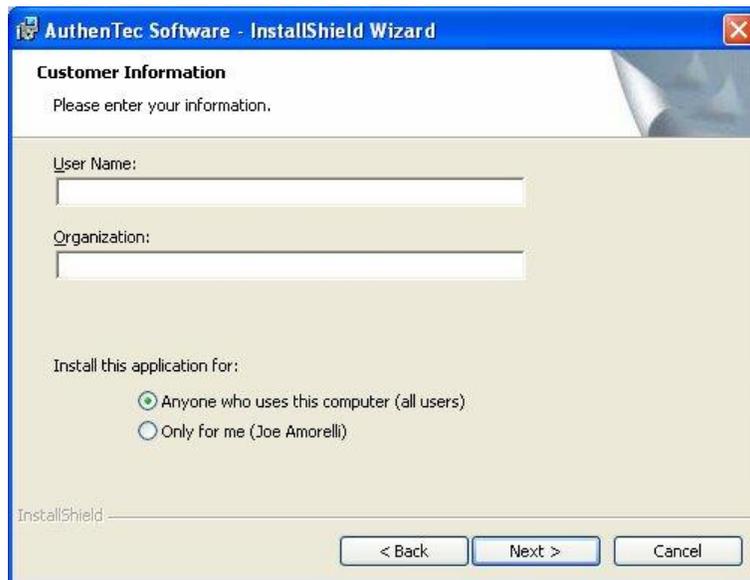
Select **Complete** as the Setup Type, and click **Next**.
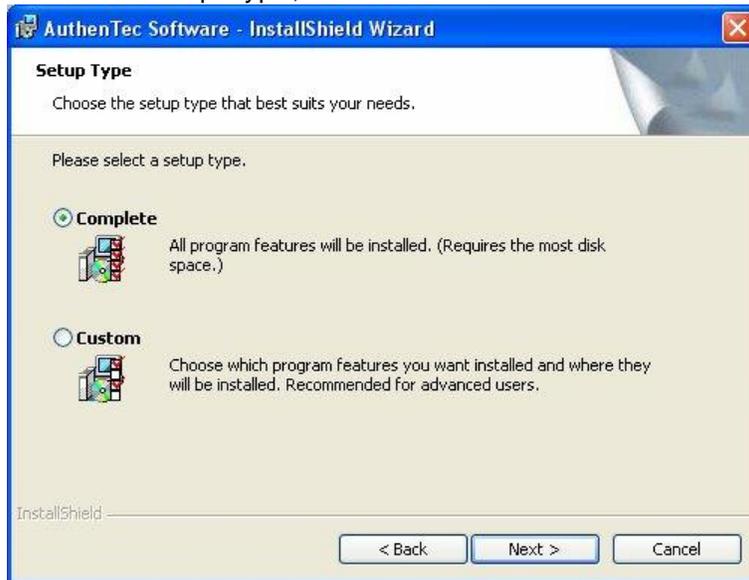
To initiate the software installation, click **Install**.
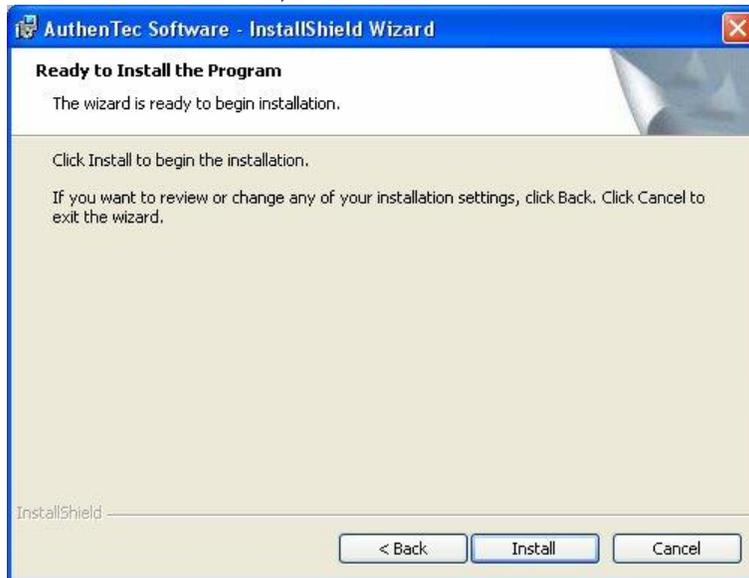
Once installation is complete, click **Finish**.
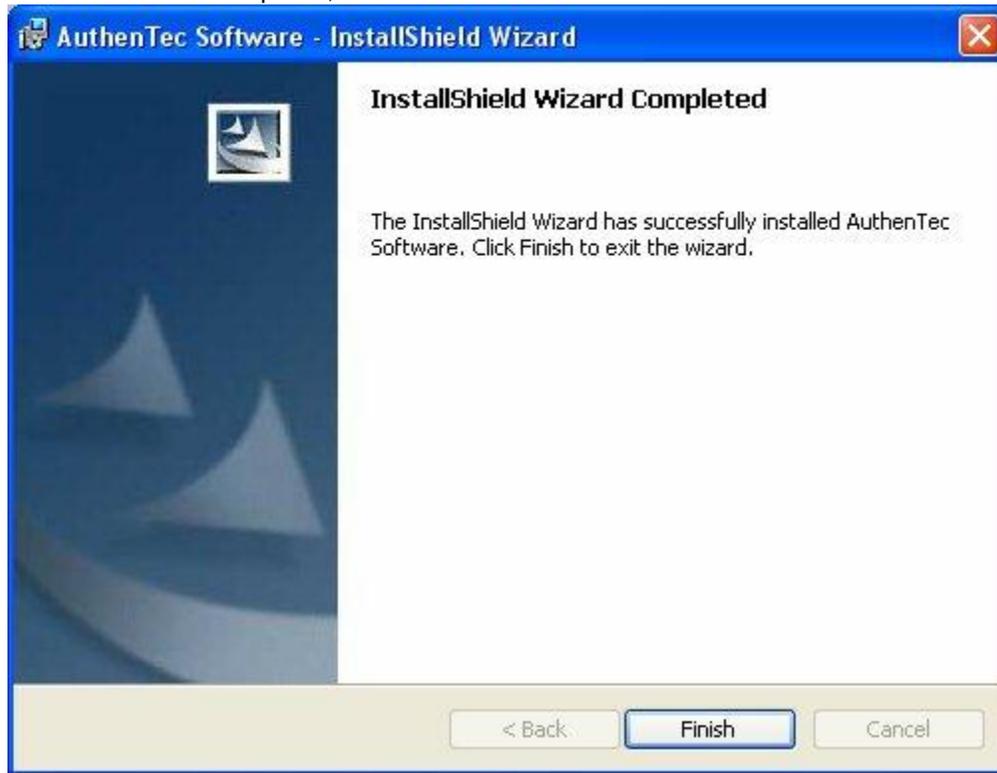
5. Go to C:\Temp\Add On directory and run AT6210.exe. The add-on utility installs itself with no user interaction. At the end of the installation, click on **Finish**. If the system prompts you to reboot, do so.

6. Delete the C:\Temp\ directories you created for this installation.

Repeat steps 2 through 6 for all workstations as well as the main back office server.

Tests

Enrollment Test

The Aware shortcut (highlighted icon) and the ATDatabase.dat file were added to your desktop.

Note: Instructions beyond this point are for testing purposes. You could go straight to the Maitre 'D setup, but we recommend to first test the device outside of Maitre'D. If the device does not work using the following steps, it can not work within Maitre 'D either.

Double click the Aware icon and follow these steps.
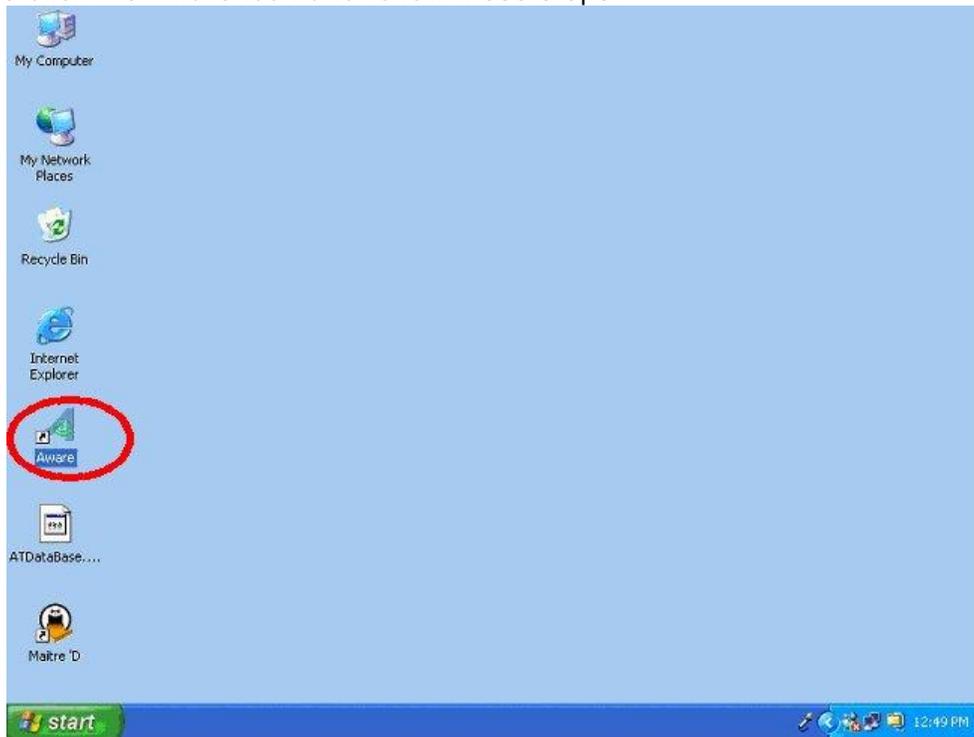
Select **Enroll**.
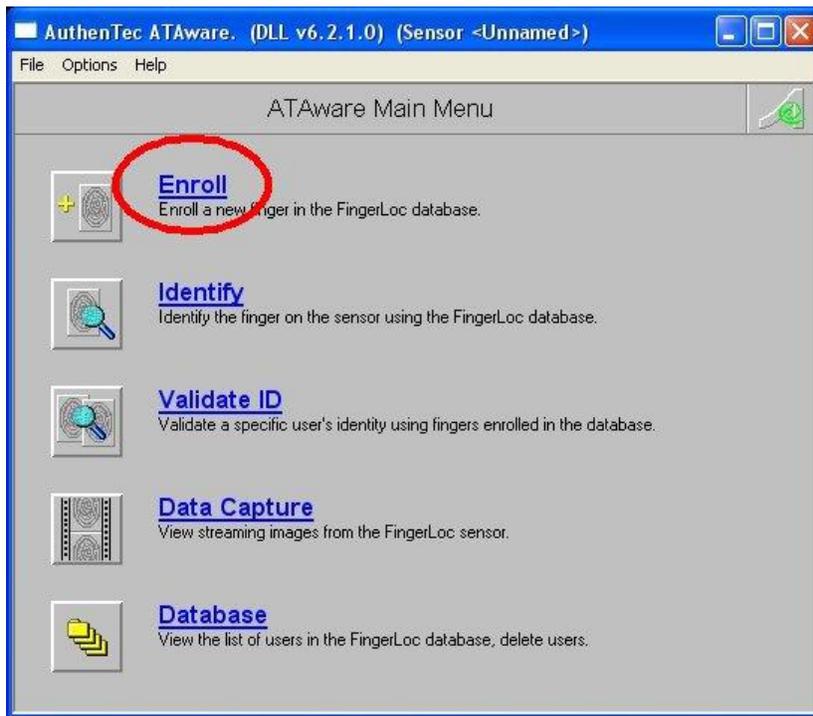
Enter your name in the User ID field, select the finger you will be scanning, and click **OK**.
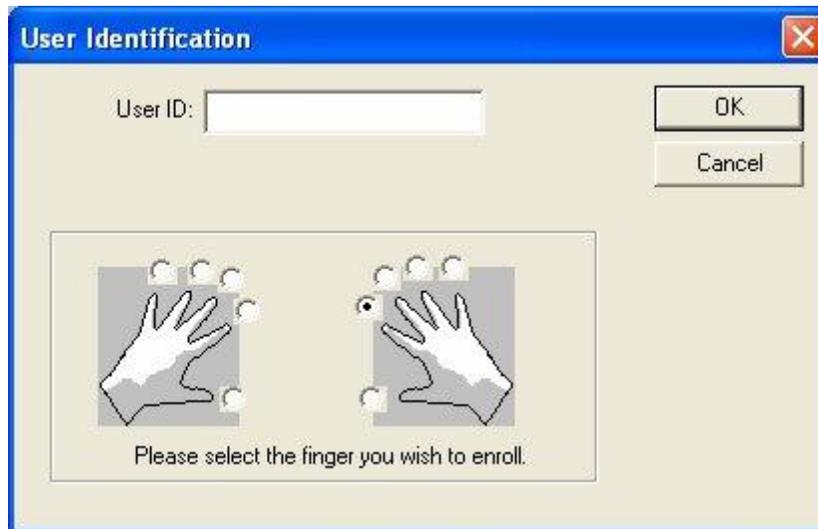
Read the instructions and press **OK**.

Make sure the biometric device is on a fixed and stable surface, and put the ball of your finger on the biometric device. You will be required to scan it three times to save your fingerprint.

Note: During the enrollment process, the fingerprint is saved in the ATDatabase.dat file for later identification.
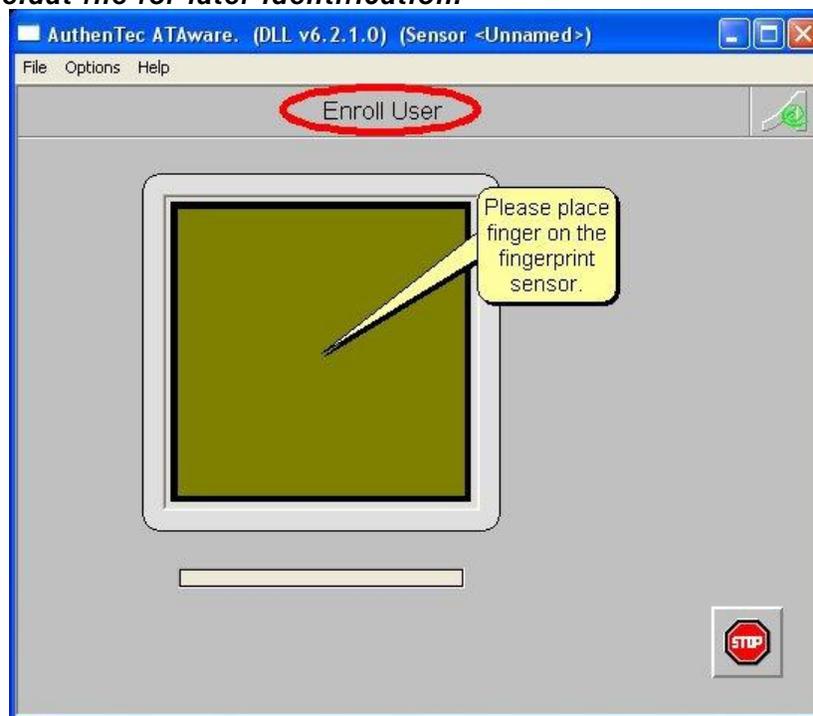
This is the screen after the first fingerprint capture. (In this screen capture, no real fingerprint is shown).
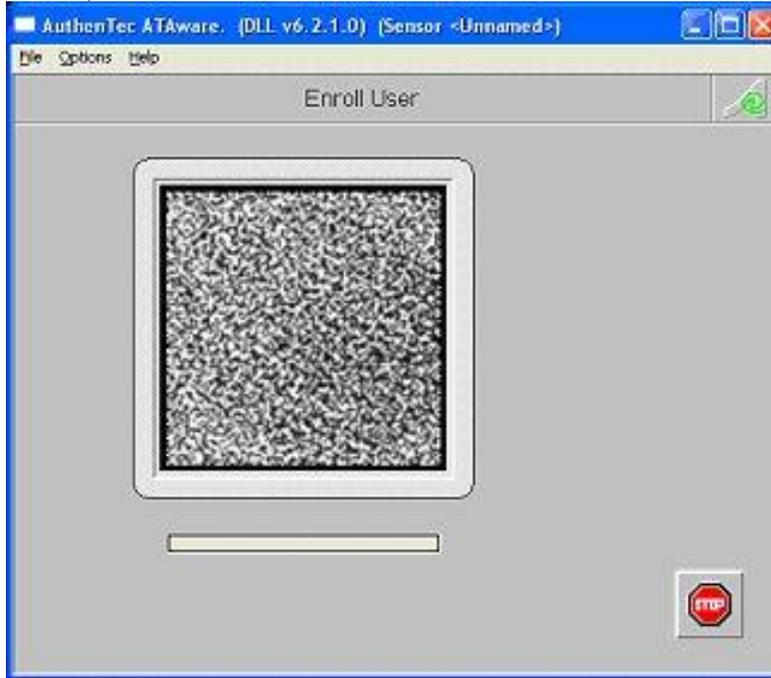
After the second fingerprint capture, notice the indicator circled in red.
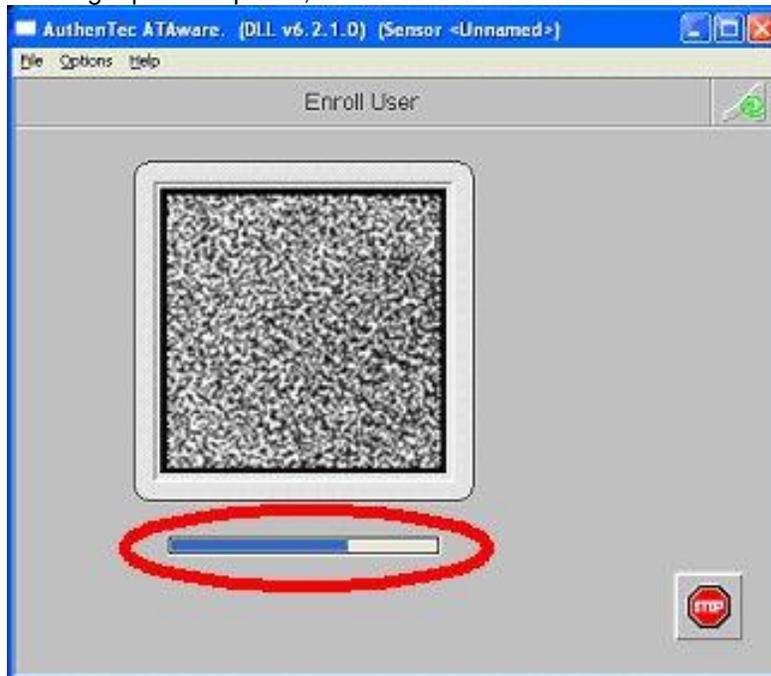
Third time, capture is complete, press ok.

Identification Test

Select **Identify**.
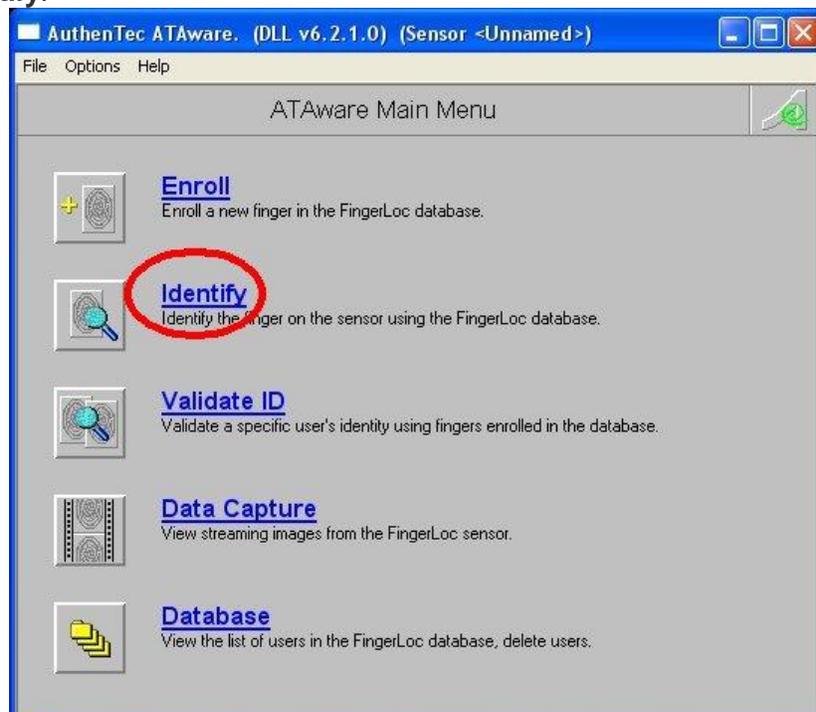
The screen looks similar as during the enrollment process, except for the title. The PC will look through the database and authenticate any user whose fingerprint has

been scanned. Put the ball of your finger on the biometric device and see if the system identifies you.
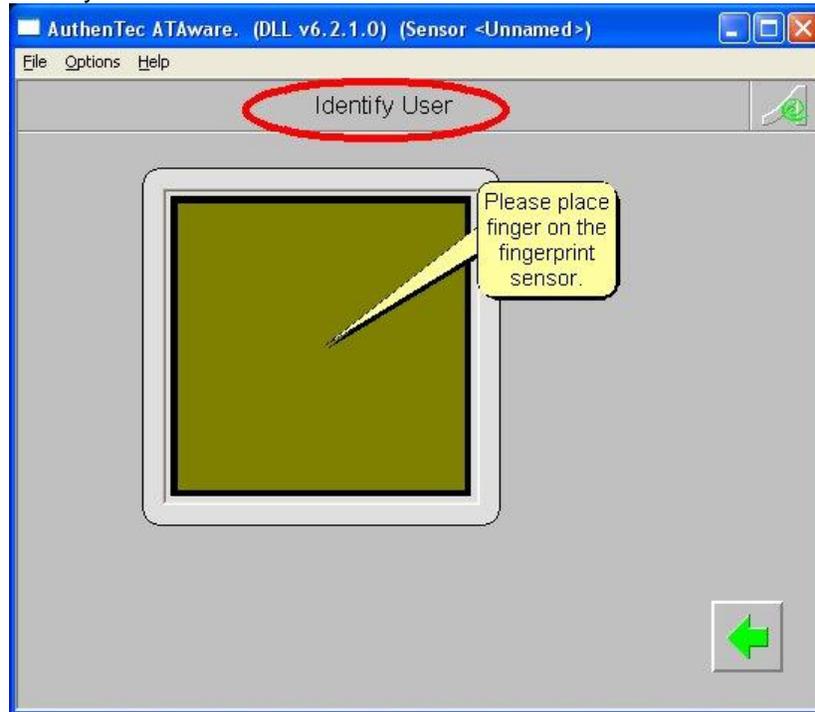
If the biometric device identified you, it will display a message stating, "User (your name) identified. Access granter". The device is working properly, and you are now ready to move on to the Maitre 'D setup.

If the biometric device did not identify you, try going through the enrollment process again, before trying the identification process again. If it still fails to identify you, remove and reinstall the AuthenTec software and drivers, and try again. If all this fails, contact Posiflex at tech.support@posiflexusa.com or (510) 429-7097.

Configuring the AuthenTec Biometric device in Maitre'D

Back-Office Setup

Once the AuthenTec software is installed and tested on the Main Server and all workstations, there is a small amount of configuration to be setup in the Maitre'D Back-Office.

System Configuration / View / Options / Devices
Biometric Reader
Select AuthenTec

POS Control / Workstation / Options / Devices

For each workstation where a biometric device is installed, click **Add**.
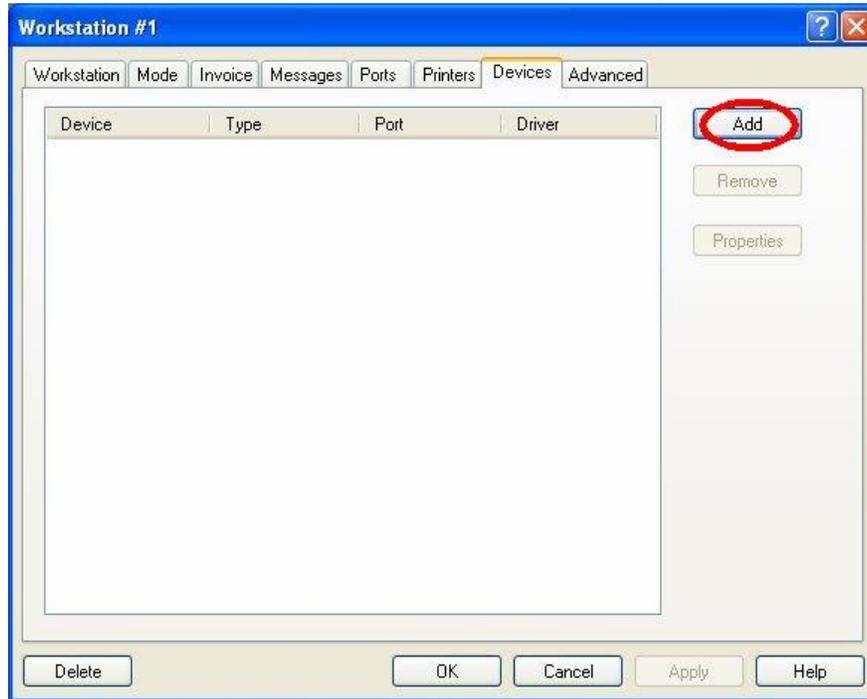
Select **Biometric Reader**, and then click **Setup**.

Select the **AuthenTec** type, and click **OK**.

The Biometric Reader is now setup. Click **OK**.
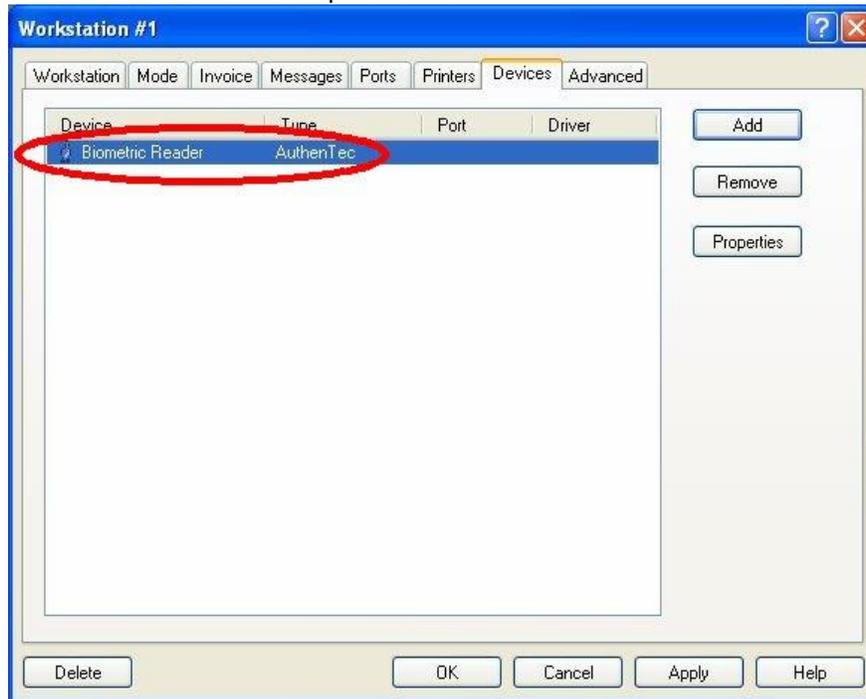
POS Control / Employees / Configuration / Functions / Setup Functions
In the manager configuration, enable **Access Setup**.
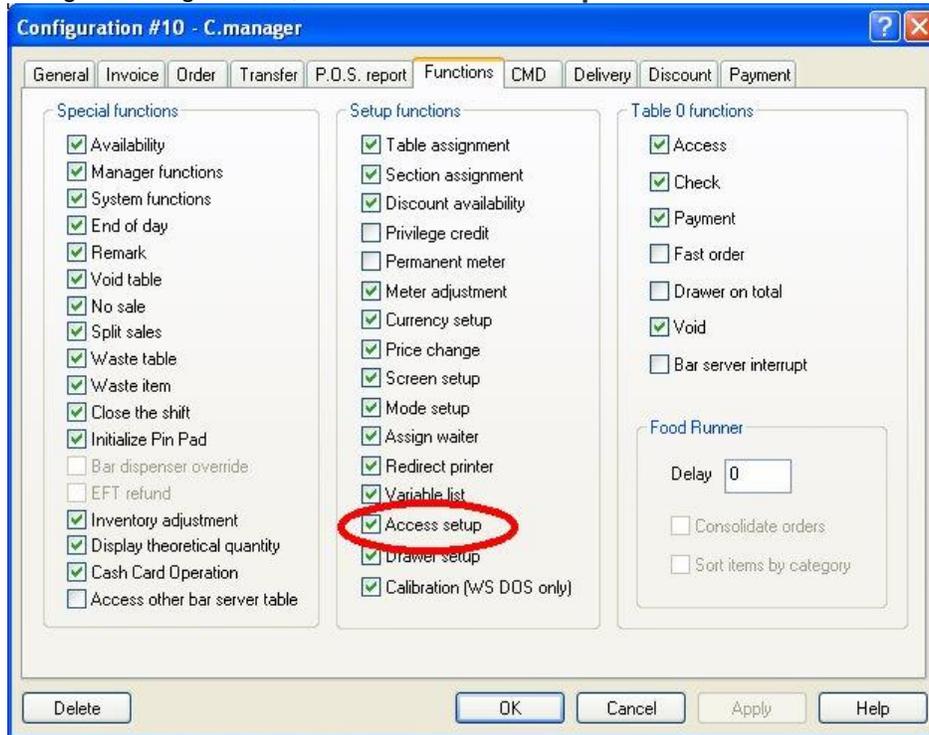
POS Access Setup

On the workstation, use a manager number to access the **Functions** screen. In the **Manager Menu**, touch **Access Setup**.

Select an employee ready to scan a fingerprint.
Note: The employee must have been previously created in the Back-Office before they can be fingerprinted.
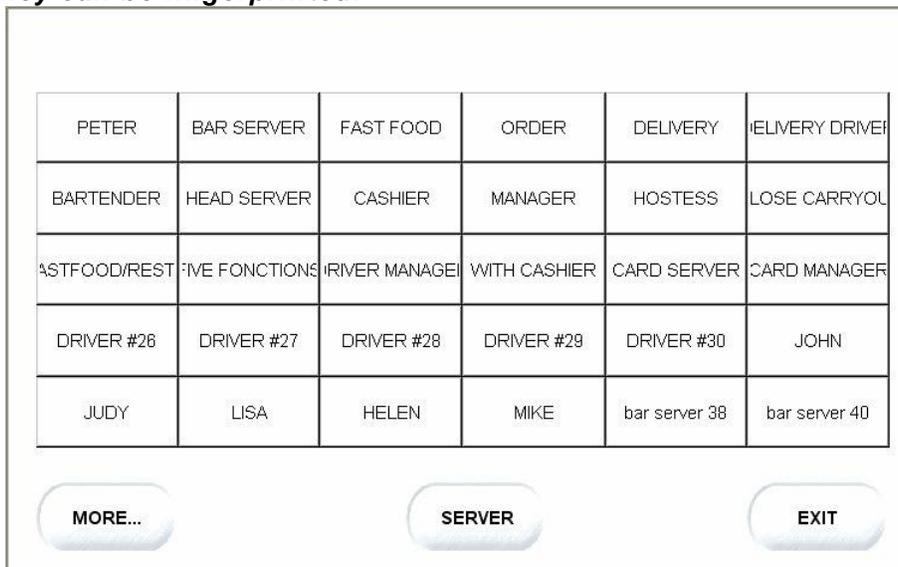
Have the employee put the ball of a first finger on the device. The system will require that this finger be scanned three times.

Waiting for fingerprint #1 (1)

Scan left 3

CANCEL
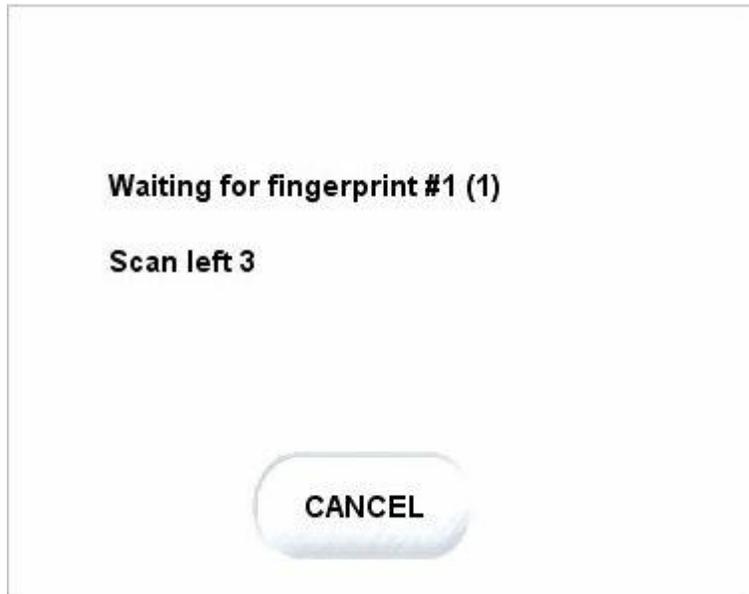
Have the employee put the ball of a different finger on the device, in case the first finger gets hurt, burned or cut. The system will require that this other finger be scanned three times as well.

Waiting for fingerprint #2 (1)

Scan left 3

CANCEL
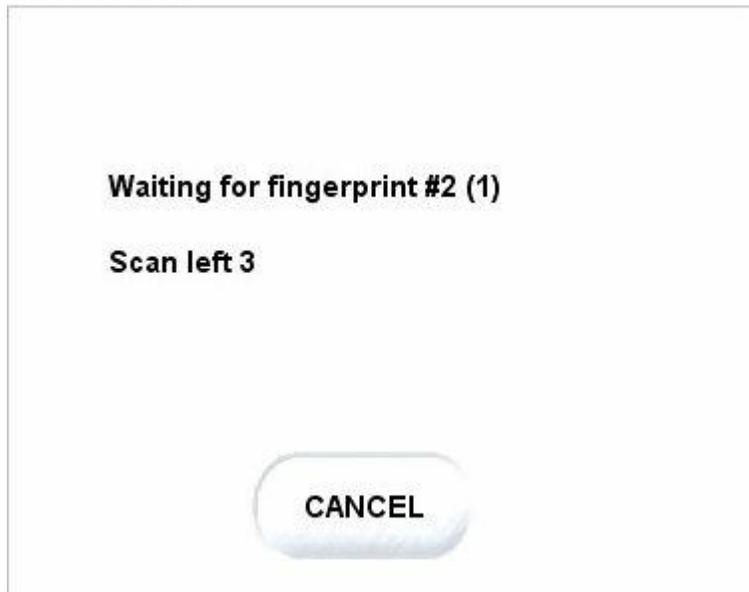
Optional Back-Office Setup

POS Control / View / Options / Security

You can also adjust the way the system uses the biometric device with these options.

Biometric Log on Only:

Enable this option to force employees to use the biometric device, and disable the server's passwords. If this option in disabled, employees will still be able to log on using their server number and password.

Biometric TA Punch Only:

Select this option to force employees to use the biometric device when they punch in, and disable the server's passwords, even if the employee record is linked to a server number and that server number does not need the biometric device to order.

Biometric as Validation Device:

Select this option to use the biometric device only to validate an employee's identity instead of a password. Employees will still have to enter their server number on the workstation to identify themselves, but when the password is required, they will touch the biometric device instead of entering their password. The same will apply when punching in or out with the Time & Attendance module.
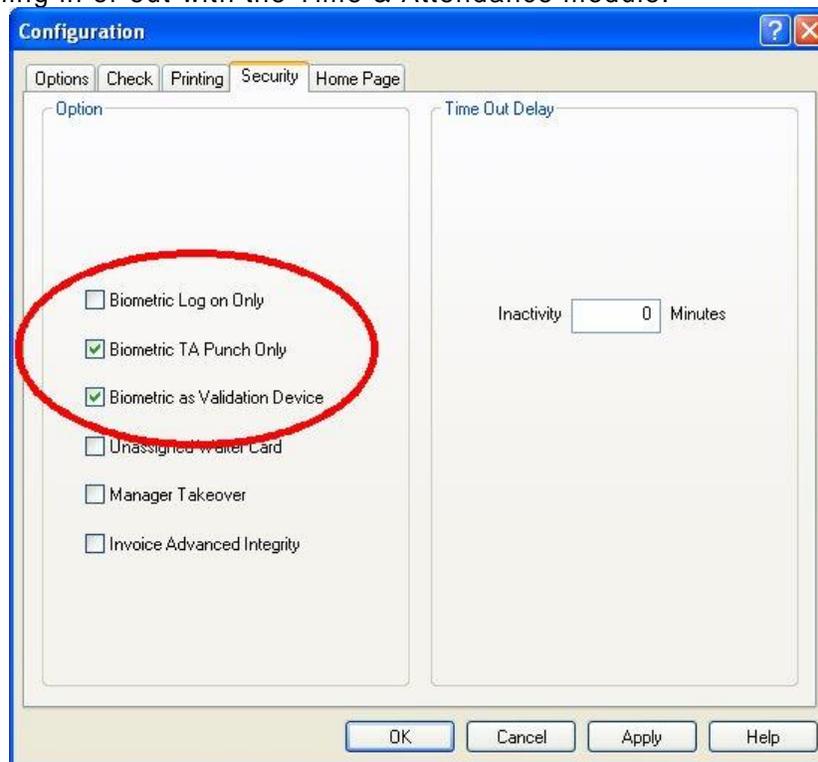
The following is an example of an employee trying to log on without using the biometric device, when **the Biometric Log on Only** option is enabled.