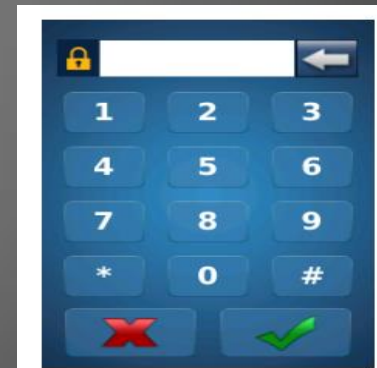
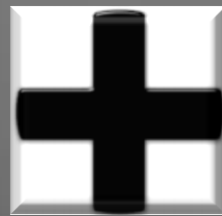


How to use a Finger Then Keypad access

- Design for: Sigma and Sigma Lite +
- For Users to use a Finger AND Keyboard access



Software Screen shots

- Some screen shots might differ slightly from your version of Software

Requirements

- Software
- Morpho Manager
- Get the software from
- <http://service.morphotrak.com/software-links.html>
- You would need a MSO to capture fingerprint enrollments
- You could use **one access reader* to capture fingerprints if you did not have a MSO (**only Sigma and Sigma Lite products*)

- MSO300



Before we begin.....

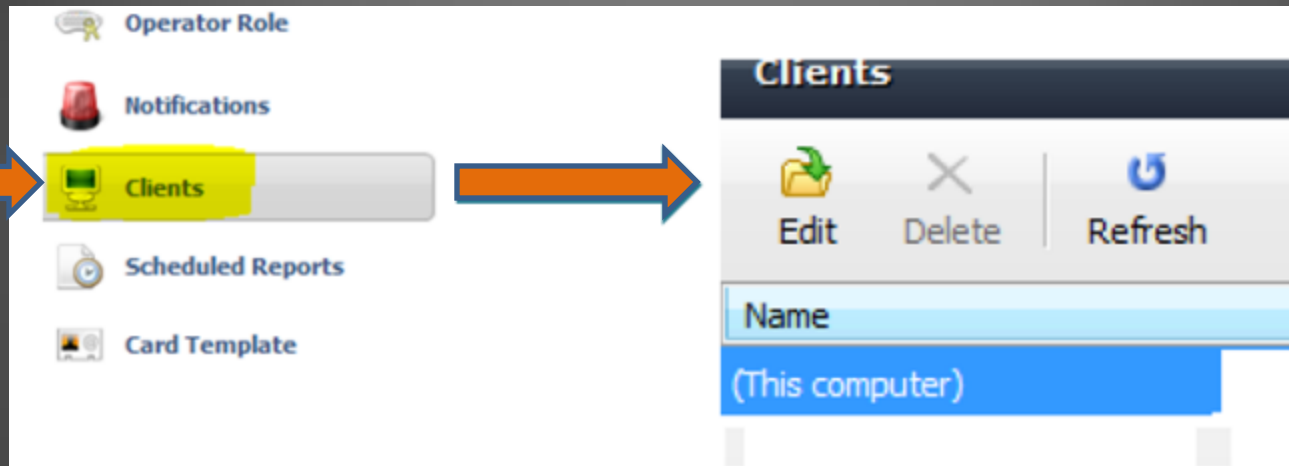
No MSO to capture fingerprints ?

Use a Sigma Or a Sigma Lite for enrollment
(this option only available Morpho Manager
7.X.X and higher)

Follow the next few steps for configuration

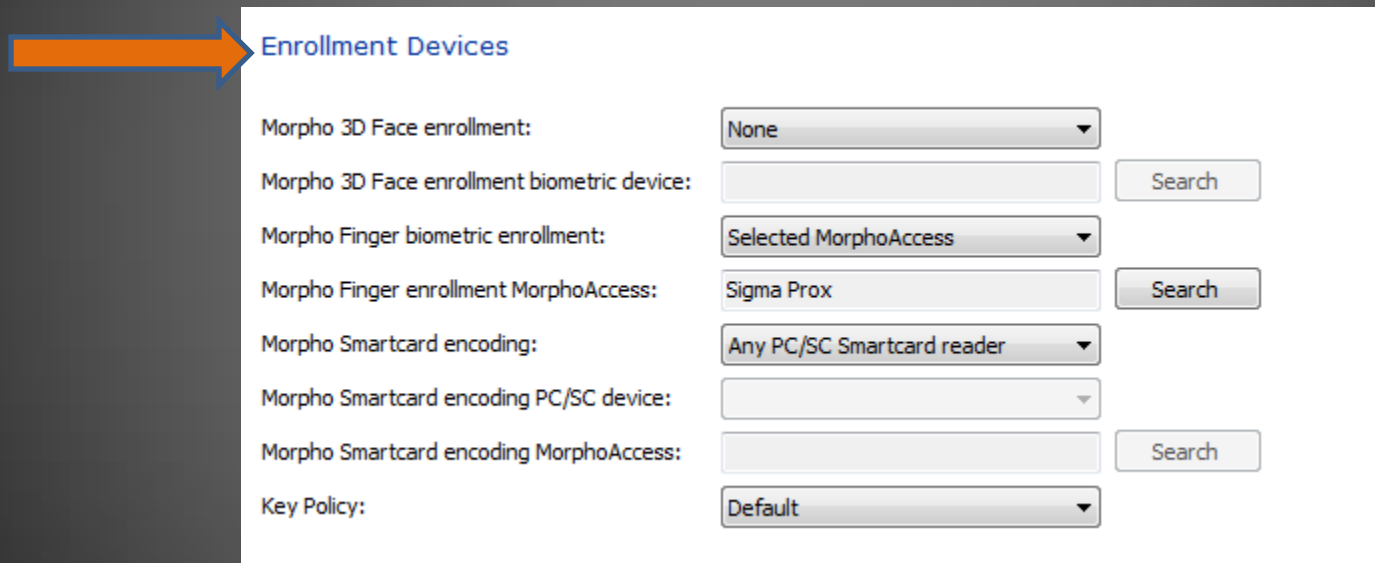
To use a Sigma product to capture fingerprints

- Path>Administration> Client>click (This computer) and Edit



To use a Sigma product to capture fingerprints

- Click next to where it says Enrollment Devices



The screenshot shows a configuration page titled "Enrollment Devices". An orange arrow points to the title. The page contains several configuration items, each with a label, a dropdown menu, and a search button. The items are:

Label	Value	Search Button
Morpho 3D Face enrollment:	None	
Morpho 3D Face enrollment biometric device:		Search
Morpho Finger biometric enrollment:	Selected MorphoAccess	
Morpho Finger enrollment MorphoAccess:	Sigma Prox	Search
Morpho Smartcard encoding:	Any PC/SC Smartcard reader	
Morpho Smartcard encoding PC/SC device:		
Morpho Smartcard encoding MorphoAccess:		Search
Key Policy:	Default	

To use a Sigma product to capture fingerprints

**This is if you want to use a Sigma Family to capture fingerprints

Change Morpho Finger Biometric enrollment >MorphoAccess and Search for your device that you want to use to capture fingerprints

Enrollment Devices

Morpho 3D Face enrollment:

Morpho 3D Face enrollment biometric device:

Morpho Finger biometric enrollment:

Morpho Finger enrollment MorphoAccess:

Morpho Smartcard encoding:

Morpho Smartcard encoding PC/SC device:

Morpho Smartcard encoding MorphoAccess:

Key Policy:

Use drop down arrow for Selected MorphoAccess

Click Search for your device

Click Finish

1. *User Authentication Mode*

➤ Step One

1. *User Authentication Mode*

- Create a User Authentication
- Path>Administration>User Authentication Mode
- Designate the authentication mode you wish to utilize for user placed into this User Policy.

1. User Authentication Mode

Items

- Operator
- Key Policy
- Biometric Device Profile
- Biometric Device**
- Wiegand Profiles
- User Policy
- Access Schedules
- User Distribution Group
- User Authentication Mode**
- Operator Role

Adding User Authentication Mode

Enter details for this User Authentication Mode

Name:

Description:

MA 100, MA J, MA 500, and MA VP Mode:

Morpho 3D Face Mode:

Smartcard encoding will prefer the MA Sigma settings over MA 100, MA J, MA 500, and MA VP mode settings.

1. User Authentication Mode

The screenshot shows a configuration page for 'User Authentication Mode'. On the left is a navigation menu with items: Operator, Key Policy, Biometric Device Profile, Biometric Device, Wiegand Profiles, User Policy, Access Schedules, User Distribution Group, **User Authentication Mode** (highlighted with an orange arrow), Operator Role, and Notifications. The main content area is titled 'Enter MA Sigma, MA Sigma Lite, MA Sigma Lite+, MorphoWave Mode details for this User Authentication Mode'. It contains several settings:

- MA Sigma, MA Sigma Lite, MA Sigma Lite+, MorphoWave Mode: Enabled (dropdown menu, with an orange arrow pointing to a blue 'Enabled' label).
- MA Sigma, MA Sigma Lite, MA Sigma Lite+, MorphoWave Settings (grouped in a box):
 - Download Identifier To Device: (with an orange arrow pointing to a blue 'Check' label).
 - Encode To Smartcard Mode: None (dropdown menu).
 - Template Location: Downloaded To Device (dropdown menu, with an orange arrow pointing to a blue 'Download to Device' label).
 - Pin Location: Downloaded To Device (dropdown menu, with an orange arrow pointing to a blue 'Check' label).
 - Allow Start By Biometric: (with an orange arrow pointing to a blue 'Check' label).
 - Allow Start By Contactless Card: (with an orange arrow pointing to a blue 'Check' label).
 - Allow Start By Keyboard: (with an orange arrow pointing to a blue 'Check' label).
 - Allow Start By Wiegand In: (with an orange arrow pointing to a blue 'Check' label).
 - Require Pin: (with an orange arrow pointing to a blue 'Check' label).
 - Require Template Match: (with an orange arrow pointing to a blue 'Check' label).

At the bottom center, there is a red button labeled 'Click Finish'.

Click Finish

2. *User Policy*

➤ Step Two

2. *User Policy*

- Create new User Policy
- Select the User Policy that this user will belong to. This is an important selection, as the policy will determine Biometric Device access and other access control and time & attendance settings.

2. User Policy

The screenshot shows the 'User Policy' configuration page. On the left is a navigation menu with the following items: Operator, Key Policy, Biometric Device Profile, Biometric Device, Wiegand Profiles, **User Policy** (highlighted with an orange arrow), Access Schedules, User Distribution Group, User Authentication Mode, and Operator Role. The main content area is titled 'Enter the details for this User Policy' and contains the following fields:

- Name:** 'Finger then Keypad' (highlighted with a yellow background and an orange arrow pointing to a blue box labeled 'Name it').
- Description:** An empty text box.
- Access Mode:** A dropdown menu set to 'All Biometric Devices and Clients'.
- Allow MA 500 database selection during user enrollment
- Access Schedule:** A dropdown menu set to '24 hours, 7 days a week'.
- Display extended user details
- Extended User Details:** A checkbox that is unchecked.
- Wiegand Profile:** A dropdown menu set to 'Standard 26 bit' (pointed to by an orange arrow).
- User Authentication Mode:** A dropdown menu set to 'Finger then Keypad' (pointed to by an orange arrow).
- Show Photo Capture Page:** A checkbox that is checked.

At the bottom of the page, there are two blue callout boxes:

- One pointing to the 'User Authentication Mode' dropdown with the text: 'Use the Authentication Mode you created earlier'.
- Another pointing to the 'Wiegand Profile' dropdown with the text: 'Wiegand Profile: Use the Wiegand format that is associated with your Access Control Panel (if using ACP)'.

At the very bottom center, there is a red button labeled 'Click Finish'.

Click Finish

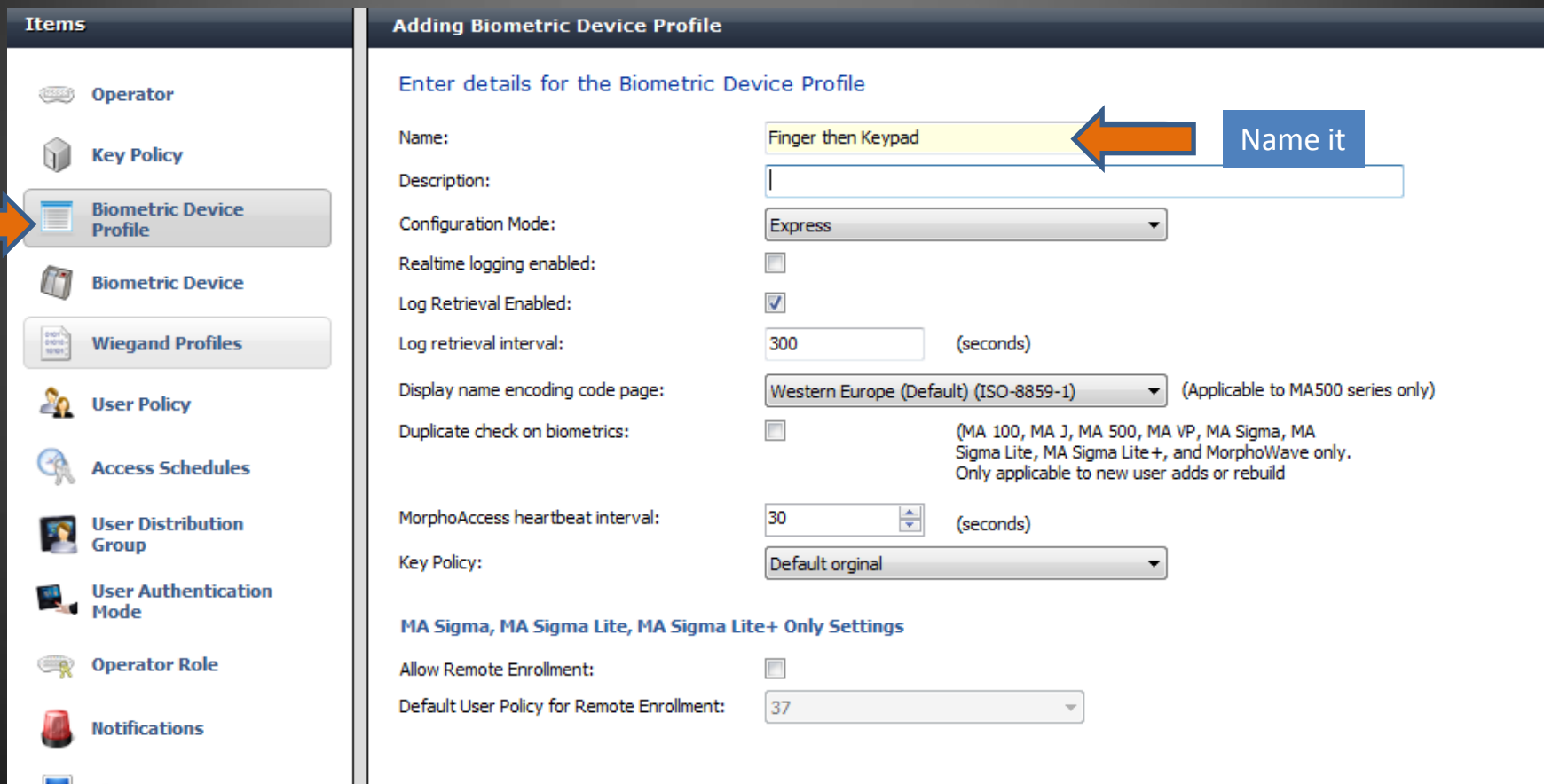
3. Biometric Device Profile

➤ Step Three

3. *Biometric Device Profile*

- Path Administration>Biometric Device Profile
- The Biometric Device Profile will define common settings and parameters for one or more biometric devices. This profile can be applied when adding units into the system from the Biometric Device section of Administration.
- Also called BDP

3. Biometric Device Profile



Items

- Operator
- Key Policy
- Biometric Device Profile**
- Biometric Device
- Wiegand Profiles
- User Policy
- Access Schedules
- User Distribution Group
- User Authentication Mode
- Operator Role
- Notifications

Adding Biometric Device Profile

Enter details for the Biometric Device Profile

Name: **Name it**

Description:

Configuration Mode:

Realtime logging enabled:

Log Retrieval Enabled:

Log retrieval interval: (seconds)

Display name encoding code page: (Applicable to MA500 series only)

Duplicate check on biometrics: (MA 100, MA J, MA 500, MA VP, MA Sigma, MA Sigma Lite, MA Sigma Lite+, and MorphoWave only. Only applicable to new user adds or rebuild)

MorphoAccess heartbeat interval: (seconds)

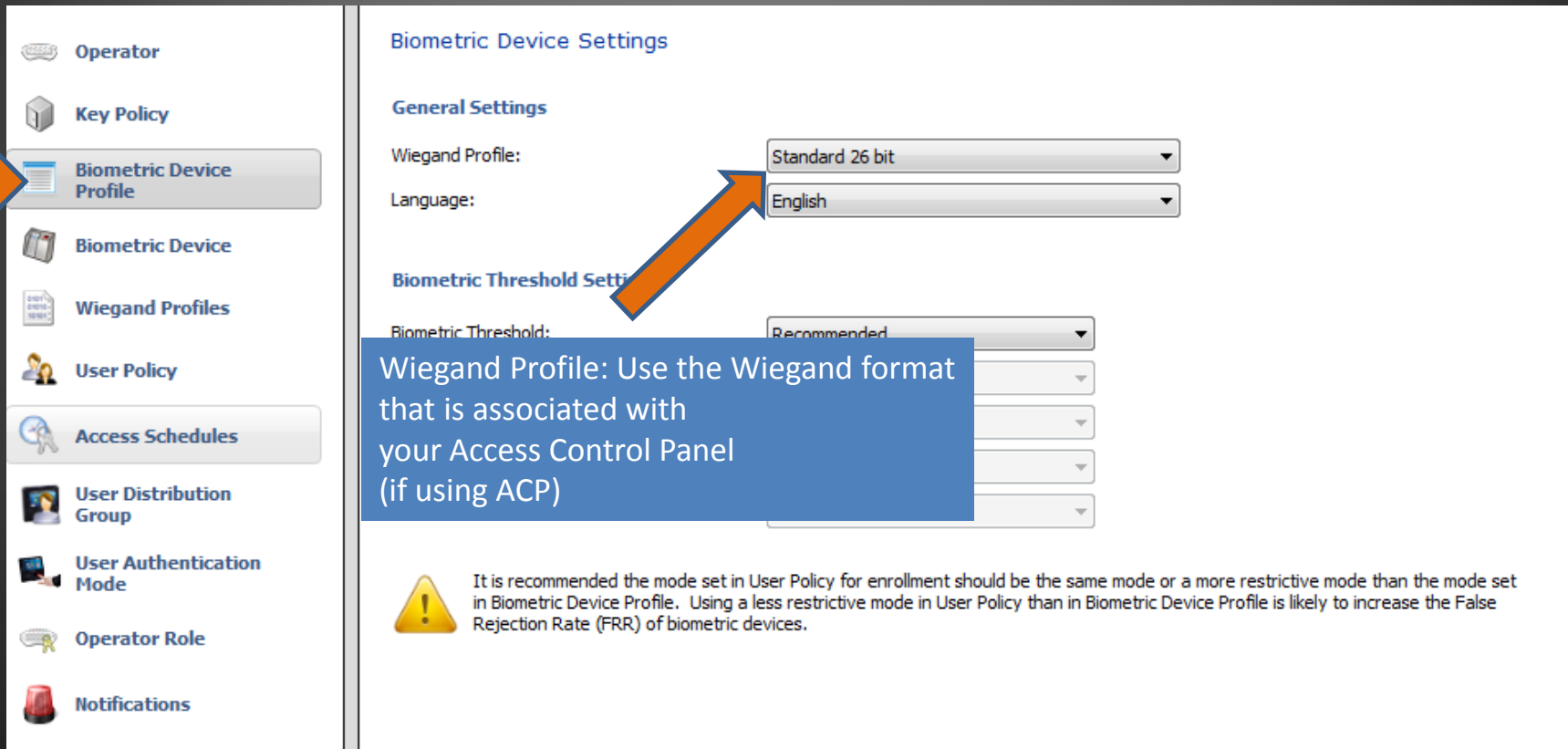
Key Policy:

MA Sigma, MA Sigma Lite, MA Sigma Lite+ Only Settings

Allow Remote Enrollment:

Default User Policy for Remote Enrollment:

3. Biometric Device Profile



Operator

Key Policy

Biometric Device Profile

Biometric Device

Wiegand Profiles

User Policy

Access Schedules

User Distribution Group

User Authentication Mode

Operator Role

Notifications

Biometric Device Settings

General Settings


Wiegand Profile: Standard 26 bit

Language: English

Biometric Threshold Settings

Biometric Threshold: Recommended

Wiegand Profile: Use the Wiegand format that is associated with your Access Control Panel (if using ACP)

 It is recommended the mode set in User Policy for enrollment should be the same mode or a more restrictive mode than the mode set in Biometric Device Profile. Using a less restrictive mode in User Policy than in Biometric Device Profile is likely to increase the False Rejection Rate (FRR) of biometric devices.

3. Biometric Device Profile

Items

- Operator
- Key Policy
- Biometric Device Profile**
- Biometric Device
- Wiegand Profiles
- User Policy
- Access Schedules
- User Distribution Group
- User Authentication Mode
- Operator Role

Adding Biometric Device Profile

Multi-Factor Mode Settings

Multi-Factor Mode: **Biometric Only**

Contactless Smart Card Mode: Contactless Smart Card

Morpho 3D Face Multi-Factor Mode

Mode: Biometric Only

MorphoAccess 100, 500, J, VP Multi-Factor Mode

Mode: Biometric Only

MA SIGMA, MA SIGMA Lite, MA Sigma Lite+ Multi-Factor Modes

Biometric:	<input checked="" type="checkbox"/>
Proximity Card:	<input type="checkbox"/>
Wiegand In:	<input type="checkbox"/>
Keypad:	<input type="checkbox"/>
HID iClass:	<input type="checkbox"/>
Mifare Classic:	<input type="checkbox"/>

Biometric only

Click Finish

4. *Biometric Device*

➤ Step Four

4. *Biometric Device*

- Biometric devices from three different hardware families can be added here; the MA 100, MA J, MA 500, and MA VP family, the MA Sigma, MA Sigma Lite and MA Sigma Lite +, the Morpho 3D Face, the Morph Wave, and the Morpho Tablet Terminal.
- The IP Address on each device must be manually assigned and must be within the IP range of the network. The IP address must not be used by any other device on the network.

4. Biometric Device

Items

- Operator
- Key Policy
- Biometric Device Profile
- Biometric Device**
- Wiegand Profiles
- User Policy
- Access Schedules
- User Distribution Group
- User Authentication Mode
- Operator Role
- Notifications
- Clients

Adding Biometric Device

Enter the details for this Biometric Device

Name: Finger then Keypad **Name it**

Description:

Location:

Asset ID:

Export Value:

Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Hardware Family: MA Sigma, MA Sigma Lite, MA Sigma Lite+

Serial Number:

Hostname\IP Address: 10.1.1.1 **Assign its IP address**

Port: 11010

Biometric Device Profile: Finger then Keypad **Assign the BDP you created earlier**

Include in Time & Attendance Exports:

Change User Onsite / Offsite Status:

Onsite Key: No Key

Offsite Key: No Key

Click Finish

5. User Management

➤ Step Five

5. User Management

- Users are people who will have their biometric data sent to the selected Biometric Device for identification purposes for either access control or time and attendance.


5. User Management



Home Administration **User Management** MSO Identification MorphoWave Identification

Adding User

Enter details for this User

User Policy:  Assign User Policy you created earlier

First Name:

Middle Name:

Last Name:


Date of Birth: Use M/d/yyyy eg. 3/24/1986.

5. User Management

Adding User

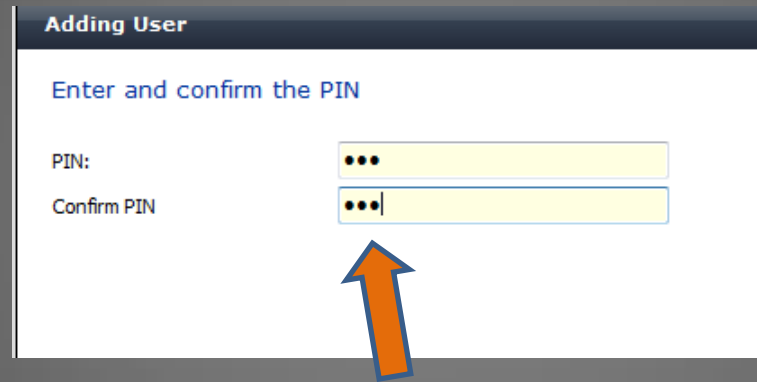
Wiegand Values

User ID



The User ID will be sent to your Access Control Panel
(if using ACP)

5. User Management



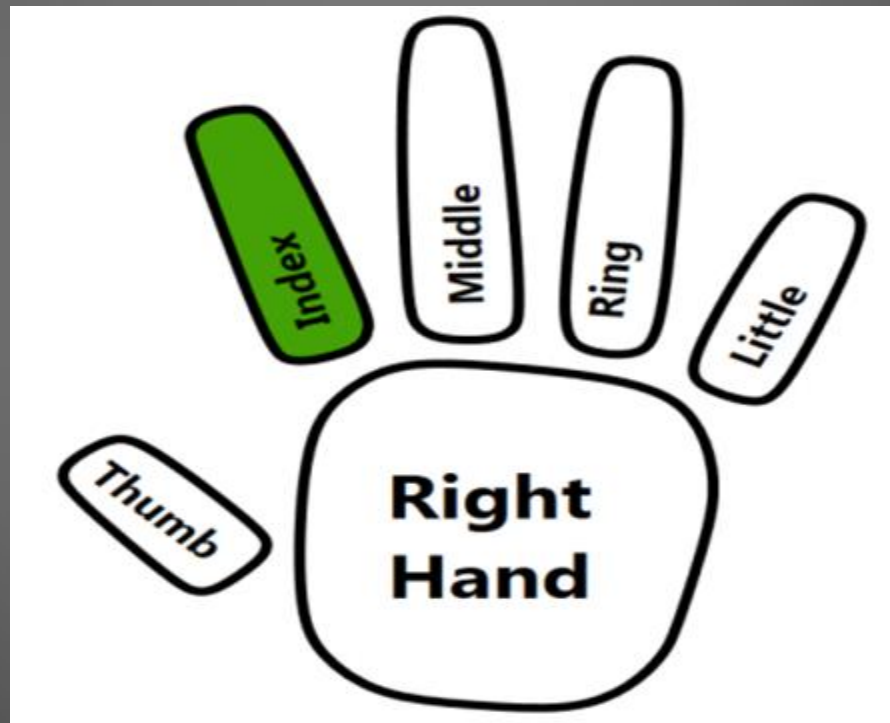
The screenshot shows a window titled "Adding User" with a subtitle "Enter and confirm the PIN". It contains two input fields: "PIN:" and "Confirm PIN". Both fields are currently empty and masked with three dots. An orange arrow points to the "Confirm PIN" field.

Add the Pin code for this User

*Pin code is the extra authentication that is associated with the User ID

5. User Management

- Capture your fingerprints (two fingers mandatory) Use a MSO 300, MSO1300, MSO VP or a Sigma Reader



Click Finish

Website

- Please visit our website, Service.morphotrak.com for software, firmware, videos and PDF's.