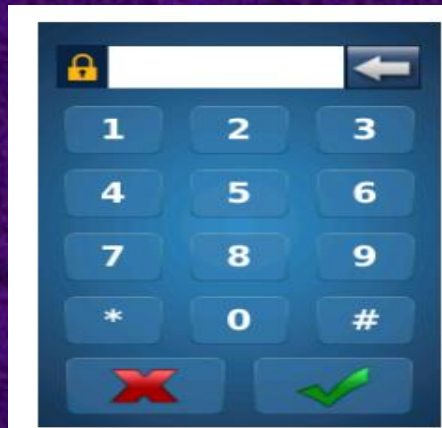


# For Prox Card OR Finger OR Keyboard Access



# Requirements

- **Software**
- **Morpho Manager**
- **\*\*some screen shots might differ than your version**
  
- **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**



# 1. Step One

- Step One

## 7. User Authentication Mode

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

# 1. User Authentication Mode

The screenshot shows the configuration page for a User Authentication Mode. The left sidebar contains a list of menu items: Operator, Key Policy, Biometric Device Profile, Biometric Device, Wiegand Profiles, User Policy, User Distribution Group, User Authentication Mode (highlighted with a black box and a purple arrow), Operator Role, and Notifications. The main content area is titled "Enter Sigma details for this User Authentication Mode" and contains several settings:

- MA Sigma Mode: Enabled (dropdown menu, highlighted with a black box and a blue arrow pointing to a red "Enable" box)
- MA Sigma Settings section:
  - Download Identifier To Device:
  - Encode To Smartcard Mode: None (dropdown menu)
  - Template Location: Downloaded To Device (dropdown menu, highlighted with a black box and a blue arrow pointing to a red "Download to Device" box)
  - Pin Location: None (dropdown menu)
  - Allow Start By Biometric:  (highlighted with a black box and a red box containing the text "Allow Start by Biometric>Check")
  - Allow Start By Contactless Card:  (highlighted with a black box and a red box containing the text "Allow Start by Contactless Card>Check")
  - Allow Start By Keyboard:  (highlighted with a black box and a red box containing the text "Allow Start by Keyboard>Check")
  - Allow Start By Wiegand In:
  - Require Pin:
  - Require Template Match:

Click Finish

## 2. Step Two

- **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. Create a User Policy

The screenshot shows a web interface for configuring a user policy. On the left is a navigation sidebar with icons and labels for 'Operator', 'Key Policy', 'Biometric Device Profile', 'Biometric Device', 'Wiegand Profiles', 'User Policy', and 'Access Schedules'. The main area is titled 'Enter the details for this User Policy' and contains several fields:

- Name:** A text input field containing 'Prox card OR Finger OR Keypad'. A blue arrow points to this field from a red callout box.
- Description:** An empty text input field.
- Access Mode:** A dropdown menu set to 'All Biometric Devices and Clients'. A checkbox below it is labeled 'Allow MA 500 database selection during use' and is unchecked.
- Access Schedule:** A dropdown menu set to '24 hours, 7 days a week'.
- Extended User Details:** A checkbox labeled 'Display extended user details' which is unchecked. A blue arrow points to this checkbox from a red callout box.
- Wiegand Profile:** A dropdown menu set to 'Standard 26 bit'.
- User Authentication Mode:** A dropdown menu set to 'Prox card OR Finger OR Keyboard'. A blue arrow points to this dropdown from a red callout box.
- Show Photo Capture Page:** A checkbox which is checked.

Name it

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

Set the User Authentication Mode to the one you created in Step One

Click Finish or Next



## 2. Create a User Policy

Enter the details for finger biometric options

Finger Biometric Enrollment Minimum Fingers:	<input type="text" value="Two"/>
Preferred Finger One:	<input type="text" value="Left Index Finger"/>
Preferred Finger Two:	<input type="text" value="Right Index Finger"/>
Preferred Duress Finger:	<input type="text" value="Left Middle Finger"/>
Vein / Print Mode:	<input type="text" value="Universal Fast"/>
Show Finger Biometric Capture Page:	<input checked="" type="checkbox"/> (User Authentication Mode requires templates)

No changes need to be made here click Finish



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.

Click Finish

### **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.**

## 3. Step Three

- **Step Three**

# 3. Biometric Device Profile

## ■ Edit or Create a Biometric Device Profile

Home Administration User Management MSO Identification Onsite / Offsite Access Logs

**Items**

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

**Editing Biometric Device Profile**

**Biometric Device Settings**

**General Settings**

Wiegand Profile: Standard 26 bit

Language: English

Key Policy: Default

**Biometric Threshold Settings**

Biometric Threshold: Recommended

MorphoAccess Vein Print Mode: Vein and Fingerprint

MorphoAccess Fingerprint Threshold: 3

Morpho 3D Face Identification Threshold: Medium

Morpho 3D Face Verification Threshold: Low

Change Wiegand format to your ACP requirements

# 3. Biometric Device Profile

Under Multi-Factor>  
change to Custom

**Operator**

- Biometric Device Profile**
- Biometric Device
- Wiegand Profiles
- User Policy
- User Distribution Group
- User Authentication Mode
- Operator Role
- Clients
- Scheduled Reports
- Card Template

### Multi-Factor Mode Settings

Multi-Factor Mode: Custom

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

#### MorphoAccess SIGMA Multi-Factor Modes

Biometric:	<input checked="" type="checkbox"/>	Biometric>Check
Proximity Card:	<input checked="" type="checkbox"/>	Proximity Card>Check
Wiegand In:	<input type="checkbox"/>	
Keypad:	<input checked="" type="checkbox"/>	Keypad>Check
HID iClass:	<input type="checkbox"/>	
Mifare Classic:	<input type="checkbox"/>	
Mifare DESFire:	<input type="checkbox"/>	
Mifare DESFire EV 1:	<input type="checkbox"/>	

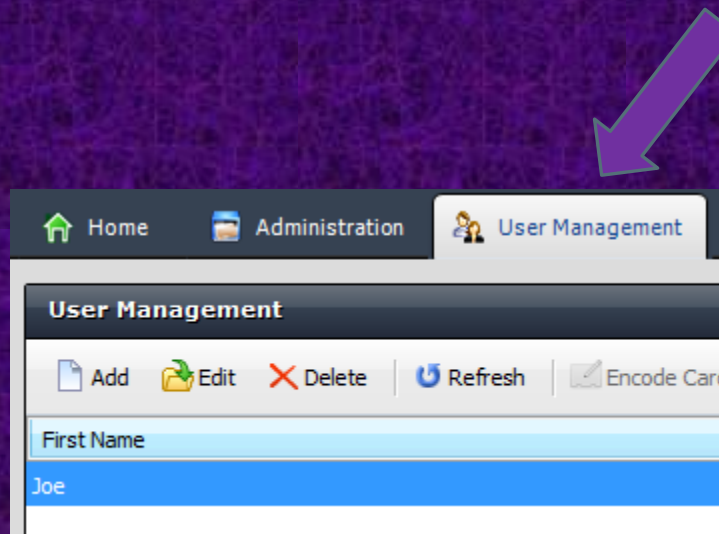
Click Finish

## 4. Step Four

- **Step Four**

## 4. 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.**



## 4. User Management

- **Assign your user Policy**

Enter details for this User

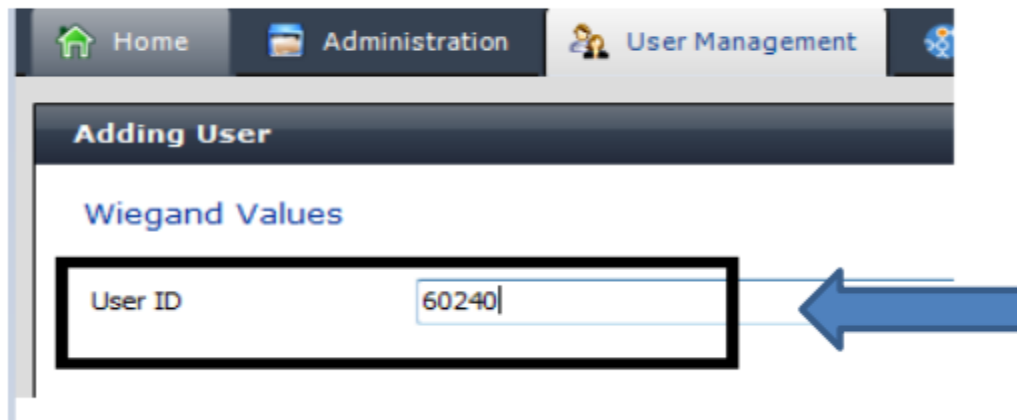
User Policy:	<input type="text" value="Prox card OR. Finger OR Keyboard"/>	
First Name:	<input type="text" value="Joe"/>	
Middle Name:	<input type="text"/>	
Last Name:	<input type="text" value="Smith"/>	
Date of Birth:	<input type="text"/>	Use M/d/yyyy eg. 3/24/1986.



## 4. User Management

- User ID
- Wiegand Value will be associated with your Prox card
- The Keypad value will be the User ID number which is the Prox card number
- The Finger value will be the User ID number which is the Prox card number

- Add the prox card for the User ID

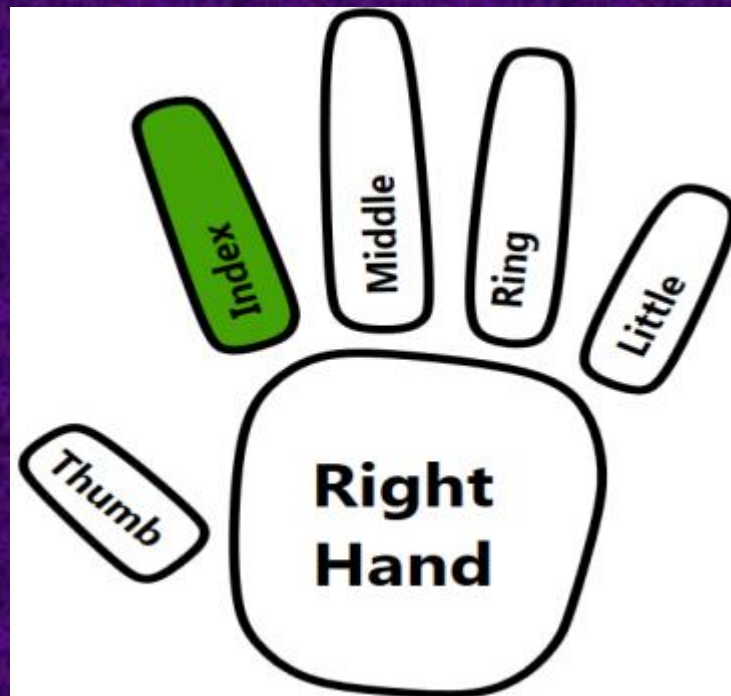


The screenshot shows a web interface for 'User Management'. At the top, there are navigation tabs: 'Home', 'Administration', and 'User Management'. Below the tabs is a header 'Adding User'. Underneath, there is a section titled 'Wiegand Values'. A table with one row is visible, with the first column labeled 'User ID' and the second column containing the value '60240'. The 'User ID' cell is highlighted with a thick black border, and a large blue arrow points to it from the right.

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

## 4. User Management

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

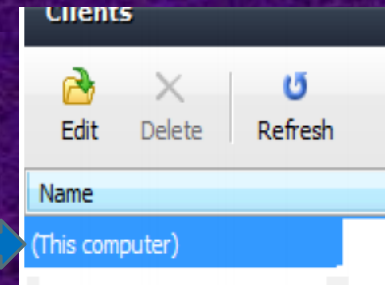
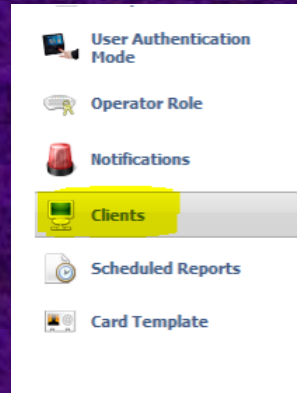


Click Finish

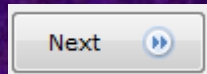
# No MSO to capture fingerprints ? Use a Sigma or a Sigma Lite for enrollment

(this option only available Morpho Manager 7.X.X and higher)

In Morpho Manager  
Go to Client>click  
(This computer) and  
Edit



Click next 5  
times till you  
get to  
Enrollment  
Devices



Change **Morpho  
Finger Biometric  
enrollment** to Selected  
Morpho Access

Enrollment Devices

Morpho 3D Face enrollment: None

Morpho 3D Face enrollment biometric device: Search

Morpho Finger biometric enrollment: Selected MorphoAccess

Morpho Finger enrollment MorphoAccess: sigma Search

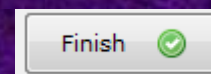
Morpho Smartcard encoding: Selected PC/SC Smartcard reader

Morpho Smartcard encoding PC/SC device: Search

Morpho Smartcard encoding MorphoAccess: Search

Key Policy: Default

Search for the  
reader you want  
to use to capture  
fingerprints



## Website

- Please visit our website,  
[Service.morphotrak.com](http://Service.morphotrak.com) for software,  
firmware, videos and PDF's.