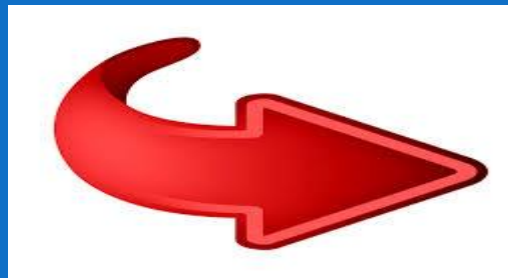
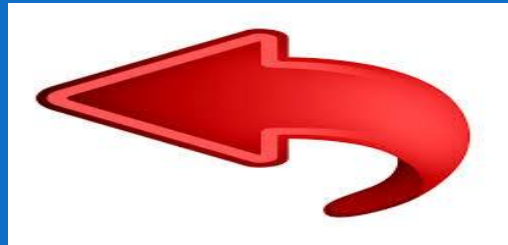


# Prox Card OR Finger



# Requirements

- **Software>Morpho Manager**
- **\*\*some screen shots might differ than your version**
  
- **Get the software at,**  
**<http://service.morphotrak.com/software-links.html>**
  
- **MSO to capture fingerprints**
  
- **\* You can use a one access reader to capture fingerprints (only Sigma and Sigma Lite products) if you did not have a MSO**

# Morpho Manager log in

- **Morpho Manager Default log in**
- **Username=administrator**
- **Password=password**

# 1. 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 a web-based configuration interface for user authentication. At the top, there is a navigation bar with tabs for Home, Administration, User Management, MSO Identification, Access Logs, and Reports. The 'Administration' tab is active. On the left side, there is a sidebar menu with various configuration options: Operator, Key Policy, Biometric Device Profile, Biometric Device, Wiegand Profiles, User Policy, Access Schedules, User Distribution Group, User Authentication Mode (highlighted with a blue arrow), and Operator Role. The main content area is titled 'Adding User Authentication Mode' and contains the following fields and controls:

- Name:** A text input field containing 'Prox OR Finger|' with a blue callout box labeled 'Name It' pointing to it.
- Description:** An empty text input field.
- MA 100, MA J, MA 500, and MA VP Mode:** A dropdown menu currently set to 'None'.
- Morpho 3D Face Mode:** A dropdown menu currently set to 'None'.

Below the dropdowns, there is a warning icon and the text: 'Smartcard encoding will prefer the MA Sigma settings over MA 100, MA J, MA 500, and MA VP mode settings.'

At the bottom right, there is a 'Next' button with a right-pointing arrow icon. A yellow arrow points from the 'Next' button back towards the 'User Authentication Mode' menu item in the sidebar.

# 1. User Authentication Mode

The screenshot shows the 'Adding User Authentication Mode' configuration page in a software interface. The page title is 'Adding User Authentication Mode' and the subtitle is 'MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme and MorphoWave Settings'. The 'Mode' dropdown is set to 'Enabled'. The 'Download Identifier To Device' checkbox is checked. The 'Encode To Smartcard Mode' dropdown is set to 'None'. The 'Template Location' dropdown is set to 'Downloaded To Device'. The 'Pin Location' dropdown is set to 'None'. The 'Allow Start By Biometric' and 'Allow Start By Contactless Card' checkboxes are checked. The 'Allow Start By Keyboard', 'Allow Start By Wiegand In', 'Require Pin', and 'Require Template Match' checkboxes are unchecked. The 'Finish' button is highlighted with a red arrow. The 'User Authentication Mode' item in the left sidebar is highlighted with a blue arrow. Blue arrows point to the 'Enable' button, the 'Download to Device' dropdown, and the checked checkboxes for 'Allow Start by Biometric' and 'Allow start by Contactless Card'.

Home Administration User Management MSO Identification Access Logs Reports

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**

MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme and MorphoWave Settings

Mode: Enabled

Download Identifier To Device:

Encode To Smartcard Mode: None

Template Location: Downloaded To Device

Pin Location: None

Allow Start By Biometric:

Allow Start By Contactless Card:

Allow Start By Keyboard:

Allow Start By Wiegand In:

Require Pin:

Require Template Match:

Enable

Download to Device

Allow Start by Biometric>Check

Allow start by Contactless Card>Check

Finish

## 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 an User Policy

The screenshot shows a web application interface for creating a user policy. The navigation menu on the left includes: Home, Administration, User Management, MSO Identification, Access Logs, and Reports. The main form area is titled "Adding User Policy" and contains the following fields:

- Name: Prox OR Finger (highlighted with a blue box labeled "Name It")
- Description: (empty)
- Access Mode: All Biometric Devices and Clients (dropdown menu)
- Access Schedule: 24 hours, 7 days a week (dropdown menu)
- Extended User Details: (checkbox, unchecked)
- Wiegand Profile: Standard 26 bit (dropdown menu, highlighted with a blue arrow and a callout box: "Change the Wiegand profile to your Prox card format")
- User Authentication Mode: Prox OR Finger (dropdown menu, highlighted with a blue arrow and a callout box: "Set User Authentication Mode to the one you created in Step one")
- Show Photo Capture Page: (checkbox, checked)

A red arrow points to the "Finish" button at the bottom right, which includes a green checkmark icon.



## 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. Biometric Device Profile

Home Administration User Management MSO Identification Access Logs Reports

**Items**

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

**Editing Biometric Device Profile**

Enter details for the Biometric Device Profile

Name:

Description:

Configuration Mode:

Retrieval Enabled:

(seconds)

(MA 100, MA J, MA 500, MA VP, MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme and MorphoWave only. Only applicable to new user adds)

MorphoAccess heartbeat interval:  (seconds)

Key Policy:

**MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme Only Settings**

Allow Remote Enrollment:

Default User Policy for Remote Enrollment:

**Edit or Create a Biometric Device Profile**

**Next**

# 3. Biometric Device Profile

## Biometric Device Settings

### General Settings

Wiegand Profile:

Language:

Realtime logging enabled:

Change the Wiegand profile to your Prox card format

### Biometric Threshold Settings

Biometric Threshold:

MorphoAccess Vein Print Mode:

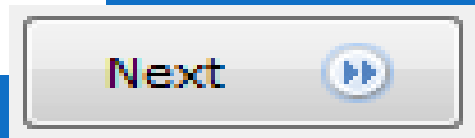
MorphoAccess Fingerprint Threshold:

Morpho 3D Face Identification Threshold:

Morpho 3D Face Verification Threshold:




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

**Editing Biometric Device Profile**

**Multi-Factor Mode Settings**

Multi-Factor Mode: Custom  **Under Multi-Factor> change to Custom**

Contactless Smart Card Mode: Contactless Smart Card

**Morpho 3D Face Multi-Factor Mode**



Mode: Keypad

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

Mode: Biometric Only

**MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme and MorphoWave Multi-Factor Modes**

Biometric:	<input checked="" type="checkbox"/>	Mifare Classic:	<input checked="" type="checkbox"/>	<b>Biometric&gt;Check</b>
Proximity Card:	<input checked="" type="checkbox"/>	Fire:	<input checked="" type="checkbox"/>	<b>Proximity Card&gt;Check</b>
Wiegand In:	<input type="checkbox"/>	Mifare DESFire EV1:	<input type="checkbox"/>	
Clock and Data In:	<input type="checkbox"/>	Keypad:	<input type="checkbox"/>	
HID iClass:	<input type="checkbox"/>	Smart Card Serial Number:	<input type="checkbox"/>	
HID iClass PACS Data:	<input type="checkbox"/>			

 **Finish** 

## 4. Add an Biometric Device

- **Path Administration>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 MorphoWave, and the Morpho Tablet Terminal.**

# 4. Biometric Device

The screenshot shows the 'Editing Biometric Device' configuration page. On the left is a sidebar with a list of items: Operator, Key Policy, Biometric Device Profile, Biometric Device (highlighted), Wiegand Profiles, User Policy, Access Schedules, User Distribution Group, User Authentication Mode, Operator Role, Notifications, Clients, and Scheduled Reports. The main area contains a form with the following fields and values:

- Name: Sigma Prox
- Description: (empty)
- Location: (empty)
- Asset ID: (empty)
- Export Value: (empty)
- Time Zone: (UTC-08:00) Pacific Time (US & Canada)
- Hardware Family: MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme
- Serial Number: (empty)
- Hostname\IP Address: 192.168.1.20
- Port: 11010
- Biometric Device Profile: Default
- Include in Time & Attendance Exports:
- Change User Onsite / Offsite Status:
- Onsite Key: No Key
- Offsite Key: No Key

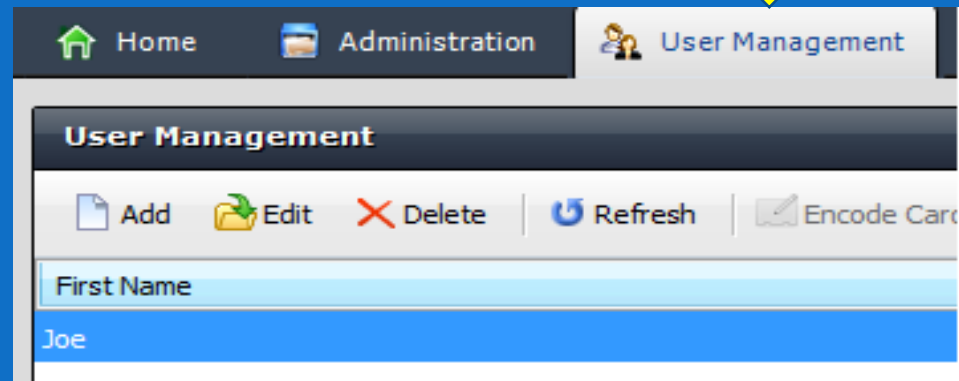
Annotations with blue arrows point to the following fields:

- 'Name It' points to the Name field.
- 'Select your family' points to the Hardware Family dropdown.
- 'Add your IP address' points to the Hostname\IP Address field.
- 'Add the BDP' points to the Biometric Device Profile dropdown.

A red arrow points from the bottom right towards a 'Finish' button with a green checkmark icon.

# 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

## ▪ Assign your User Policy

Enter details for this User

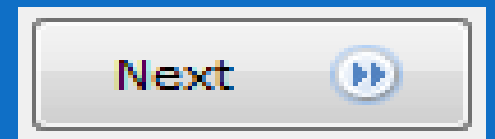
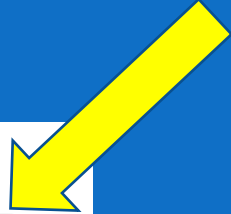
User Policy:

First Name:

Middle Name:

Last Name:

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



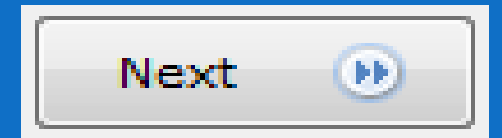



# 5. User Management

The User ID Wiegand Value will be associated with your Prox card number

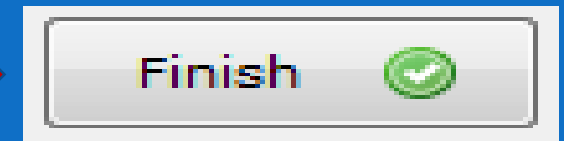
Wiegand Values

User ID	60240
---------	-------



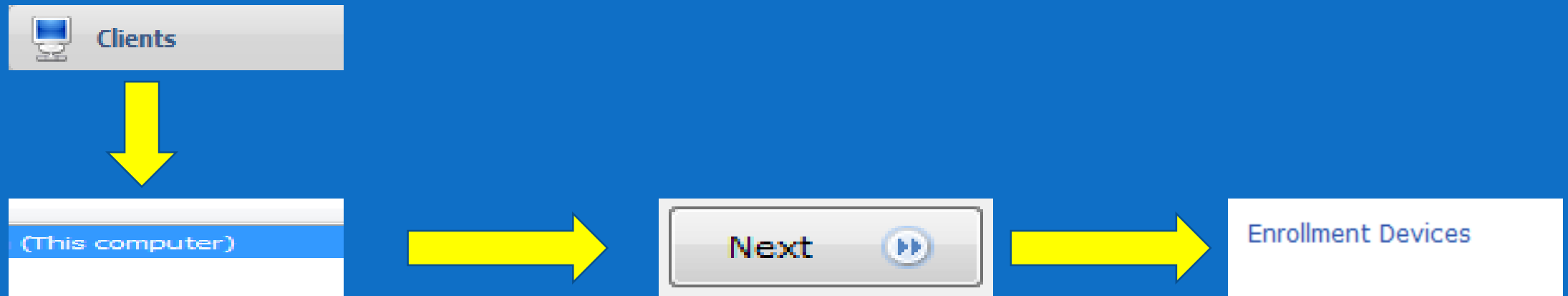
# 5. User Management

- Capture your fingerprint (s) Use a MSO 300, MSO1300, MSO VP or a Sigma Reader



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

- In Morpho Manager
- Go to >Administration>Clients>Edit (This computer)>Click Next 5 times till you get to Enrollment Devices



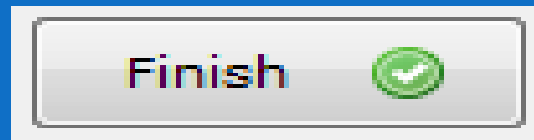
# No MSO to capture fingerprints ? Use a Sigma and Sigma Lite for enrollment

Enrollment Devices

Morpho 3D Face enrollment:	None	
Morpho 3D Face enrollment biometric device:		
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:		
Morpho Smartcard encoding MorphoAccess:		Search
Key Policy:	Default	

Change *Morpho Finger Biometric enrollment* to Selected Morpho Access

Search for your device that 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.