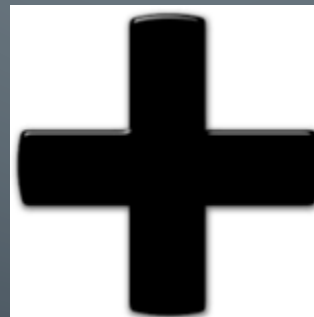
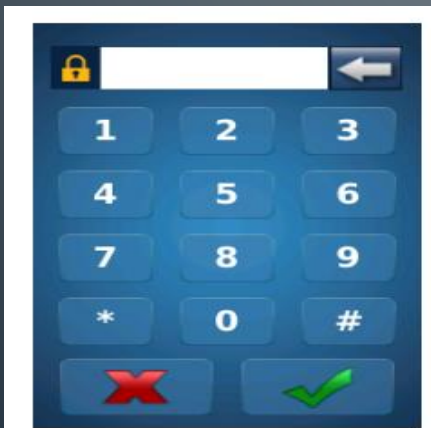
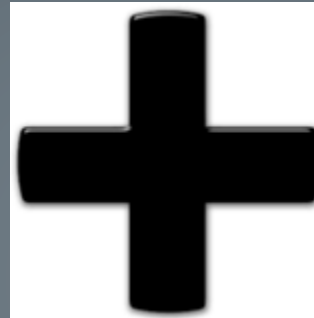


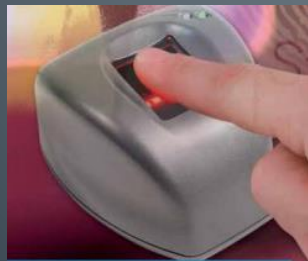
For Prox Card and Finger and Keyboard and Finger



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*)**

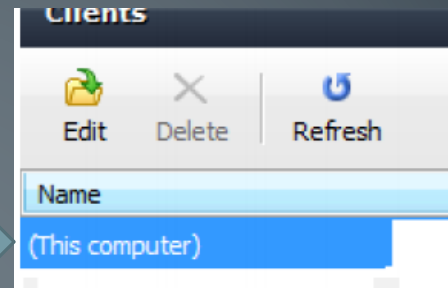
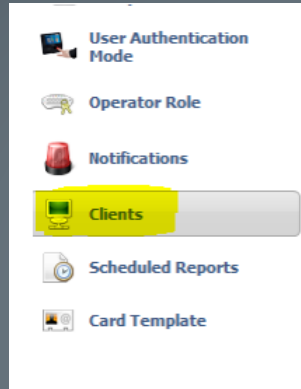
- **MSO300**



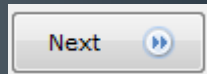
No MSO to capture fingerprints ? Use a Sigma or a Sigma Lite for enrollment

(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:

Morpho 3D Face enrollment biometric device: Search

Morpho Finger biometric enrollment:

Morpho Finger enrollment MorphoAccess: Search

Morpho Smartcard encoding:

Morpho Smartcard encoding PC/SC device:

Morpho Smartcard encoding MorphoAccess: Search

Key Policy:

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

3

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 a configuration page for 'User Authentication Mode'. On the left is a sidebar with 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'. It 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: (highlighted with a black box and a red box containing the text 'Require Template Match >Check')

Click 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 a User Policy

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 User Policy

Enter the details for this User Policy

Name: Prox card and Finger and Keyboard and

Description:

Access Mode: All Biometric Devices and Clients

Allow MA 500 database selection during user e

Time Mask Mode: 24 Hours, 7 Days a Week

Extended User Details: Display extended user details

Wiegand Profile: Standard 26 bit

User Authentication Mode: Prox card and Finger and Keyboard z

Wave Enrollment Minimum Hands: None

Finger Biometric Enrollment Minimum Fingers: Two

Preferred Finger One: Left Index Finger

Preferred Finger Two: Right Index Finger

Preferred Duress Finger: Left Middle Finger

Show Photo Capture Page:

Show Wave Biometric Capture Page:

Show Finger Biometric Capture Page: (User Authentication Mode requires templates)

Name it

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

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

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. Biometric Device Profile

■ Edit or Create a Biometric Device Profile

The screenshot shows a web application interface for managing biometric device profiles. The navigation menu on the left includes items like Operator, Key Policy, Biometric Device Profile (highlighted with a black box and a purple arrow), Biometric Device, Wiegand Profiles, User Policy, User Distribution Group, User Authentication Mode, and Operator Role. The main content area is titled 'Editing Biometric Device Profile' and contains 'Biometric Device Settings'. The 'General Settings' section is highlighted with a black box and contains the following fields:

- Wiegand Profile: Standard 26 bit (dropdown menu, highlighted with a purple arrow)
- Language: English (dropdown menu)
- Key Policy: Default

The 'Biometric Threshold Settings' section includes:

- 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

A text box on the right contains the instruction: "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 type="checkbox"/>
Proximity Card:	<input checked="" type="checkbox"/>
Wiegand In:	<input type="checkbox"/>
Keypad:	<input checked="" type="checkbox"/>
HID iClass:	<input type="checkbox"/>
Mifare Classic:	<input type="checkbox"/>
Mifare DESFire:	<input type="checkbox"/>
Mifare DESFire EV1:	<input type="checkbox"/>

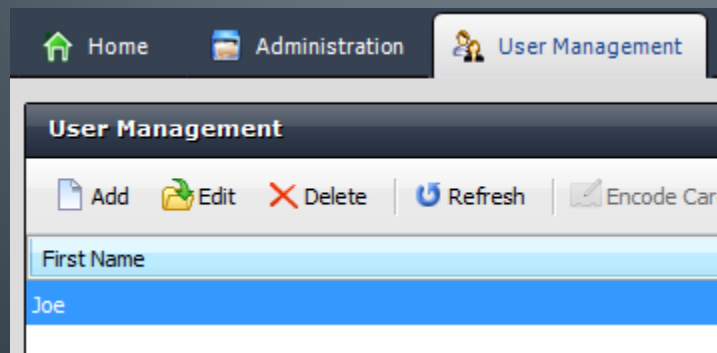
Proximity Card>Check

Keypad>Check

Click Finish

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:

Prox card and Finger and Keyboard and finger

First Name:

Joe

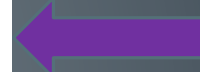
Middle Name:

Last Name:

Smith

Date of Birth:

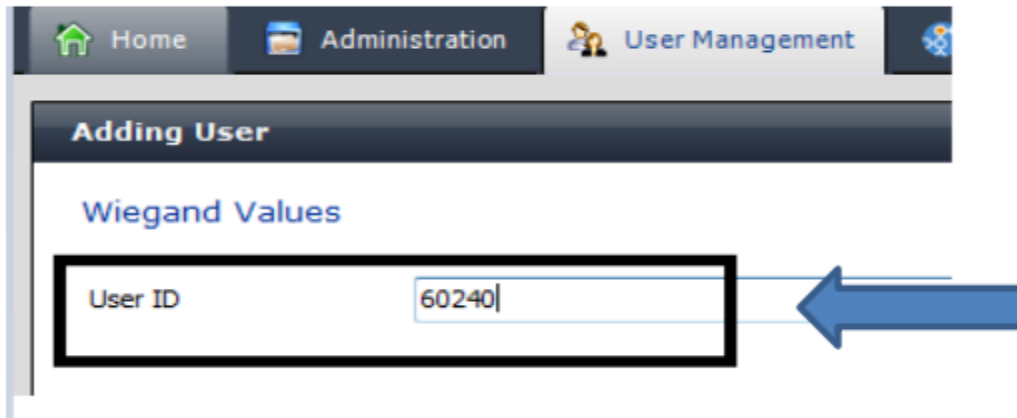
Use M/d/yyyy eg. 3/24/1986.



4. User Management

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

- Add the prox card for the User ID

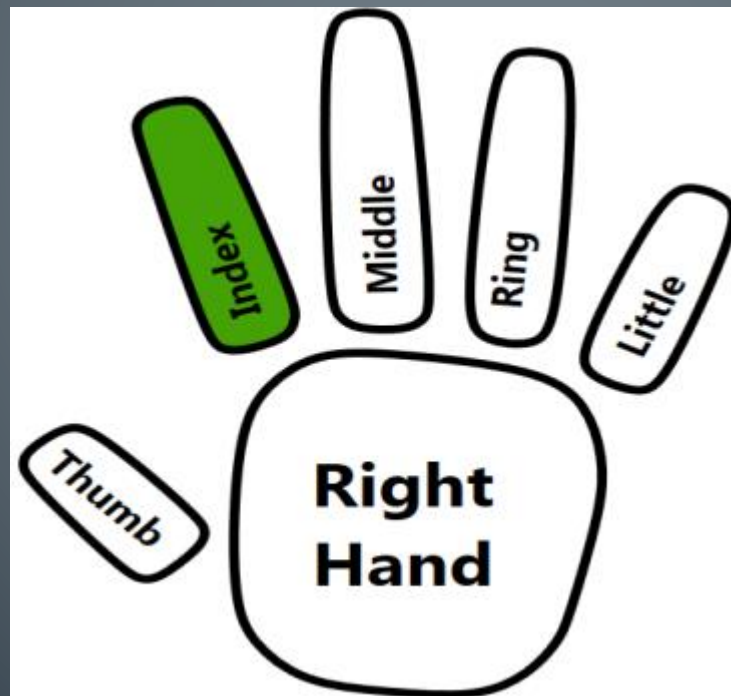


The screenshot shows a web interface with a navigation bar at the top containing 'Home', 'Administration', and 'User Management'. Below the navigation bar is a section titled 'Adding User'. Underneath, there is a heading 'Wiegand Values'. A form field labeled 'User ID' contains the text '60240'. A blue arrow points to the right side of the input field.

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

Website

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