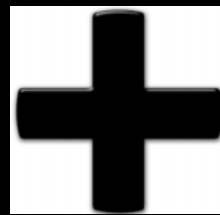
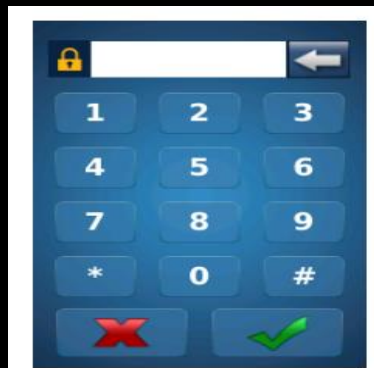


How to use a Keypad AND Finger

- Design for: Sigma and Sigma Lite +
- For Users to use a Keypad numerical ID AND Finger 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*)

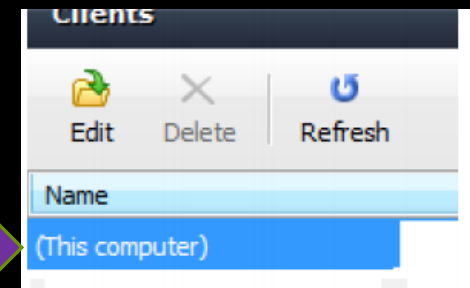
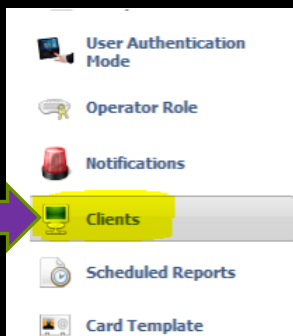
- MSO300



No MSO to capture fingerprints ? Use a Sigma and 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**



Change *Morpho Finger Biometric enrollment* to Selected Morpho Access

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:

Click Finish

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.

User Authentication Mode

- Create a New User Authentication
- Name it

The screenshot shows the configuration page for a User Authentication Mode. On the left is a navigation menu with the following items: Operator, Key Policy, Biometric Device Profile, Biometric Device, Wiegand Profiles, User Policy, Access Schedules, User Distribution Group, User Authentication Mode (highlighted with a purple arrow), and Operator Role. 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 a purple arrow pointing to it and a green "Enabled" button to its right).
- MA Sigma, MA Sigma Lite, MA Sigma Lite+, MorphoWave Settings (grouped settings):
 - Download Identifier To Device: (checkbox with a purple arrow pointing to it and a green "Check" button to its right).
 - Encode To Smartcard Mode: None (dropdown menu).
 - Template Location: Downloaded To Device (dropdown menu with a purple arrow pointing to it and a green "Download to Device" button to its right).
 - Pin Location: None (dropdown menu).
 - Allow Start By Biometric: (checkbox with a purple arrow pointing to it and a green "Check" button to its right).
 - Allow Start By Contactless Card: (checkbox).
 - Allow Start By Keyboard: (checkbox with a purple arrow pointing to it and a green "Check" button to its right).
 - Allow Start By Wiegand In: (checkbox).
 - Require Pin: (checkbox).
 - Require Template Match: (checkbox with a purple arrow pointing to it and a green "Check" button to its right).

Click Finish

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.

User Policy

Name it

The screenshot shows a web-based configuration interface for a User Policy. On the left is a navigation sidebar with the following items: Operator, Key Policy, Biometric Device Profile, Biometric Device, Wiegand Profiles, User Policy (highlighted with a purple arrow), and Access Schedules. The main content area is titled "Enter the details for this User Policy" and contains the following fields:

- Name: Keypad AND Finger (highlighted with a yellow box and a purple arrow pointing to it from the "Name it" text above)
- Description: (empty text box)
- Access Mode: All Biometric Devices and Clients (dropdown menu)
- Allow MA 500 database selection during user enrollment:
- Access Schedule: 24 hours, 7 days a week (dropdown menu)
- Display extended user details:
- Wiegand Profile: Standard 26 bit (dropdown menu, highlighted with a purple arrow from the text box below)
- User Authentication Mode: Keypad AND Finger (dropdown menu, highlighted with a purple arrow from the text box below)
- Show Photo Capture Page:

Use the Authentication Mode you created earlier

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

Click Finish

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.

Biometric Device Profile

The screenshot displays the 'Editing Biometric Device Profile' configuration page. On the left, a navigation pane lists various system items, with 'Biometric Device Profile' highlighted. The main content area is titled 'Biometric Device Settings' and contains a 'General Settings' section. This section includes three dropdown menus: 'Wiegand Profile' (set to 'Standard 26 bit'), 'Language' (set to 'English'), and 'Key Policy' (set to 'Default'). Below this is a 'Biometric Threshold Settings' section with several additional dropdown menus. A callout box with a green background and white text provides instructions for the 'Wiegand Profile' setting.

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

Biometric Device Profile

- Click Next to Multi-Factor Mode

Multi-Factor Mode Settings

Multi-Factor Mode:

Contactless Smart Card Mode:

Morpho 3D Face Multi-Factor Mode

Mode:

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

Mode:

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

Biometric:

Proximity Card:

Wiegand In:

Keypad:

HID iClass:

Mifare Classic:

Mifare DESFire:

Mifare DESFire EV1:

Change to Keypad

Click Finish



User Management

➤ 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.

User Management

- Add the User
- Assign your user Policy



Home Administration **User Management** MSO Identification Onsite / Offsite Access Logs Reports

Adding User

Enter details for this User

User Policy:

First Name:

Middle Name:

Last Name:

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

User Management

- User ID is your Keypad number

Wiegand Values

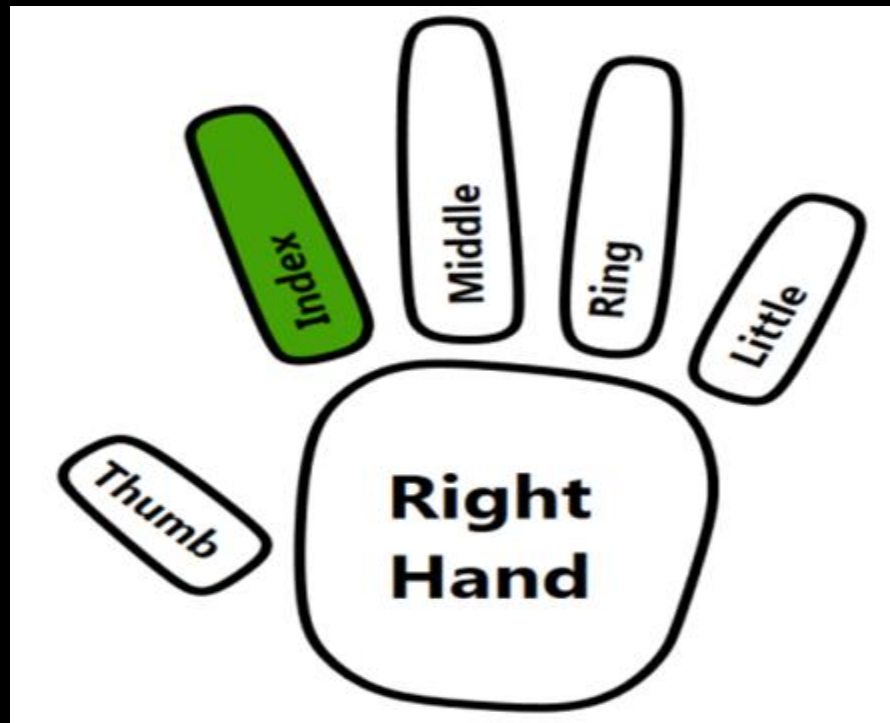
User ID

A screenshot of a web form titled "Wiegand Values". It contains a label "User ID" followed by a text input field containing the number "1234". A purple arrow points from a text box below to the input field.

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

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.