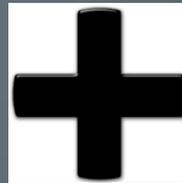


How to use a Keypad and Pin

- Design for: Sigma and Sigma Lite +
- For Users to use a Keypad numerical ID and a Pin code for access



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 a configuration page for a User Authentication Mode. On the left is a navigation sidebar with various settings categories. The main area contains configuration options for MA Sigma, MA Sigma Lite, MA Sigma Lite+, and MorphoWave Mode. Several settings are highlighted with purple arrows and black callout boxes.

Operator

Key Policy

Biometric Device Profile

Biometric Device

Wiegand Profiles

User Policy

Access Schedules

User Distribution Group

User Authentication Mode

Operator Role

Notifications

Enter MA Sigma, MA Sigma Lite, MA Sigma Lite+, MorphoWave Mode details for this User Authentication Mode

MA Sigma, MA Sigma Lite, MA Sigma Lite+, MorphoWave Mode: Enabled **Enabled**

MA Sigma, MA Sigma Lite, MA Sigma Lite+, MorphoWave Settings

Download Identifier To Device: **Download Identifier to Device**

Encode To Smartcard Mode:

Template Location:

Pin Location: **Download to Device**

Allow Start By Biometric:

Allow Start By Contactless Card:

Allow Start By Keyboard: **Allow Start By Keyboard**

Allow Start By Wiegand In:

Require Pin: **Require Pin**

Require Template Match:

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.

User Policy

The screenshot shows the 'Editing User Policy' page. On the left is a navigation menu with items like Operator, Key Policy, Biometric Profile, Biometric, Wiegand Profiles, User Policy (highlighted), User Distribution Group, User Authentication Mode, Operator Role, Notifications, Clients, and Scheduled Reports. The main content area is titled 'Editing User Policy' and contains the following fields:

- Name:** A text input field containing 'Keypad only'. An arrow points to this field with the annotation 'Name it'.
- All Biometric Devices and Clients:** A dropdown menu.
- Extended User Details:** A section containing several dropdown menus and checkboxes:
 - Wiegand Profile:** A dropdown menu set to 'Standard 26 bit'. An arrow points to this field with the annotation 'Wiegand Profile: Use the Wiegand format that is associated with your Access Control Panel (if using ACP)'.
 - User Authentication Mode:** A dropdown menu set to 'Keypad only'. An arrow points to this field with the annotation 'Use the Authentication Mode you created earlier'.
 - Wave Enrollment Minimum Hands:** A dropdown menu set to 'None'.
 - Finger Biometric Enrollment Minimum Fingers:** A dropdown menu set to 'None'. An arrow points to this field with the annotation 'Finger Biometric Enrollment Minimum Finger- None'.
 - Preferred Finger One:** A dropdown menu set to 'Left Index Finger'.
 - Preferred Finger Two:** A dropdown menu set to 'Right Index Finger'.
 - Preferred Duress Finger:** A dropdown menu set to 'Left Mid'.
 - Show Photo Capture Page:** A checked checkbox.
 - Show Wave Biometric Capture Page:** An unchecked checkbox.
 - Show Finger Biometric Capture Page:** An unchecked checkbox.

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.

Biometric Device Profile

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

Items

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

Editing Biometric Device Settings

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

Biometric Device Profile

- Click Next to Multi-Factor Mode

Change Multi-Factor Mode: Keypad

Home Administration User Management MSO Identification Onsite / Offsite Access Logs Re

Items

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

Editing Biometric Device Profile

Multi-Factor Mode Settings

Multi-Factor Mode: Keypad

Contactless Smart Card Mode: Contactless Smart Card

Morpho 3D Face Multi-Factor Mode

Mode: Keypad

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

Mode: Keypad

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

Biometric:	<input type="checkbox"/>
Proximity Card:	<input 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"/>

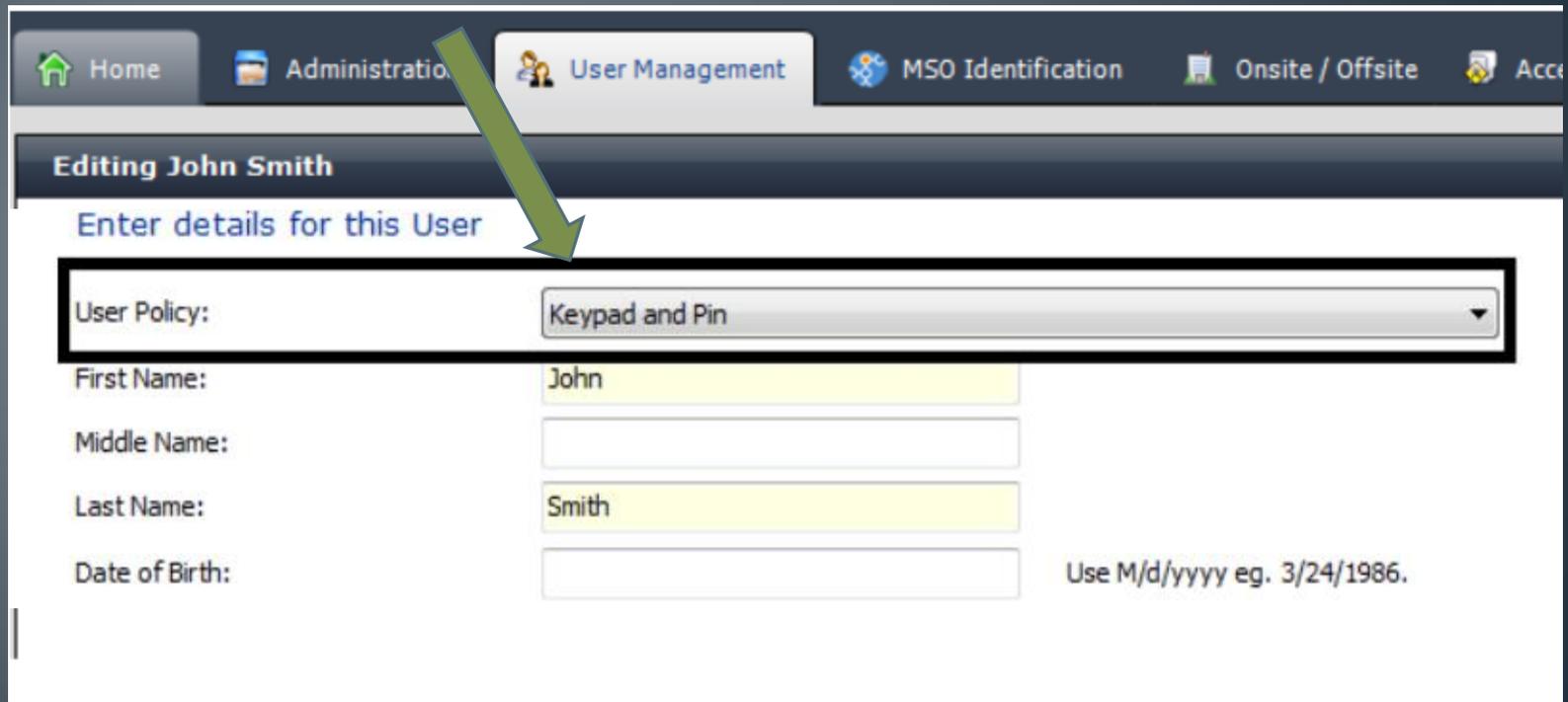
Click Finish

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.

User Management

- Assign your user Policy



The screenshot shows a web application interface for user management. The navigation bar includes links for Home, Administration, User Management (selected), MSO Identification, Onsite / Offsite, and Access. The main heading is 'Editing John Smith' with the instruction 'Enter details for this User'. The 'User Policy' dropdown menu is highlighted with a red box, and a red arrow points to it from the 'Assign your user Policy' bullet point. Below the dropdown are input fields for First Name (John), Middle Name, Last Name (Smith), and Date of Birth. A note indicates the date format: 'Use M/d/yyyy eg. 3/24/1986.'

User Policy:	Keypad and Pin
First Name:	John
Middle Name:	
Last Name:	Smith
Date of Birth:	

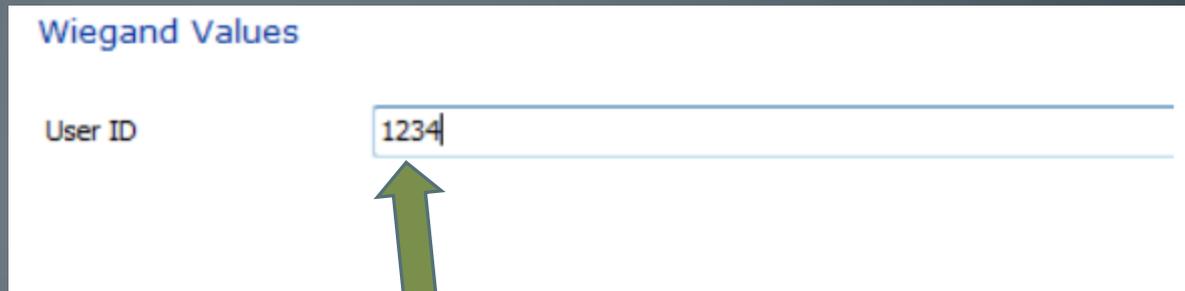
Use M/d/yyyy eg. 3/24/1986.

User Management

- User ID is your Keypad number

Wiegand Values

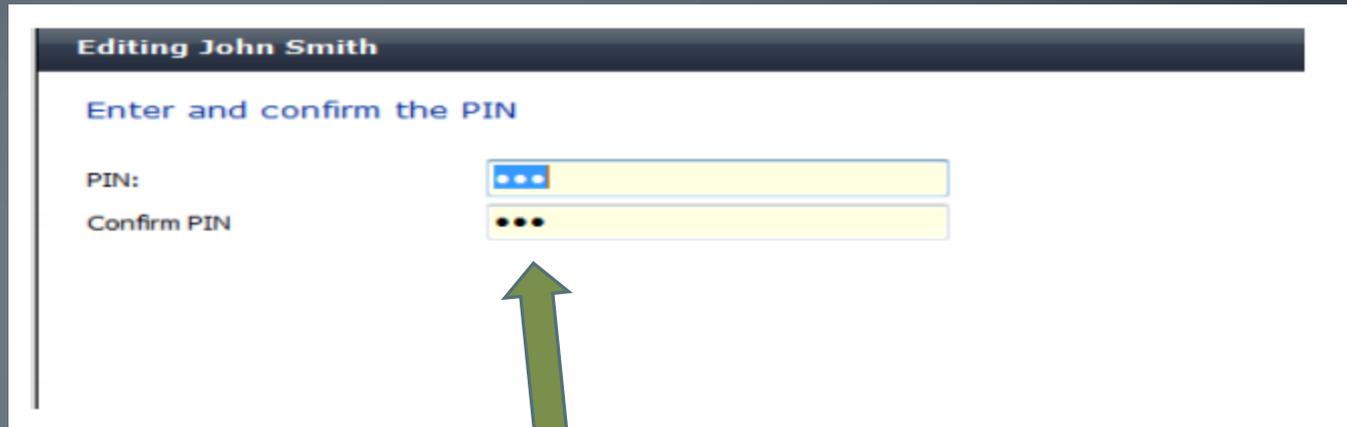
User ID



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

User Management

- Add a Pin Code to that User ID



The screenshot shows a web interface for editing a user. At the top, a dark blue header bar contains the text "Editing John Smith". Below this, the instruction "Enter and confirm the PIN" is displayed in blue. There are two input fields: the first is labeled "PIN:" and the second is labeled "Confirm PIN". Both fields are currently empty and contain three dots, indicating a masked input. A green arrow points upwards from the bottom of the form towards the "Confirm PIN" field.

Click Finish

Website

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