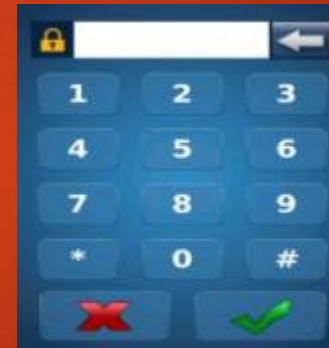
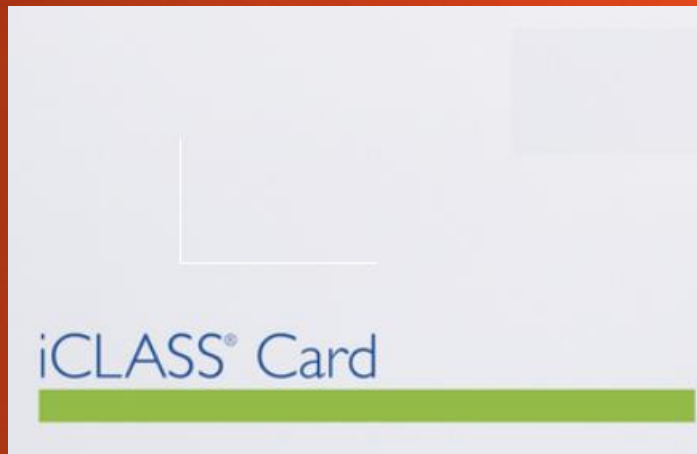


How to use Printed Iclass card and Pin



Requirements

- Type of Reader require for the following configuration:
- **Sigma Iclass**
- **Sigma Lite Iclass Plus****
- **Sigma Extreme Iclass**

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.**

Step One

- Create new User Authentication Mode or UAM

Items

- Operator
- Key Policy
- Biometric Device Profile
- Biometric Device
- Wiegand Profiles
- User Policy
- Access Schedules
- User Distribution Group
- User Authentication Mode

Adding User Authentication Mode

Enter details for this User Authentication Mode

Name: **Name It**

Description:

MA 100, MA J, MA 500, and MA VP Mode:

Morpho 3D Face Mode:



Smartcard encoding will prefer the MA Sigma settings over MA 100, MA J, MA 500, and MA VP mode settings.

Next

Step One

- Continues



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: None


Pin Location:  Downloaded To Device 

Allow Start By Biometric:


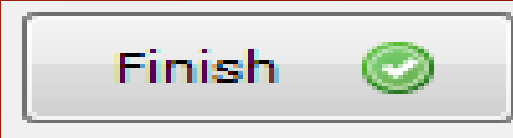
Allow Start By Contactless C: 

Allow Start By Keyboard:

Allow Start By Wiegand In:

Require Pin: 

Require Template Match:

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.**

Step 2

▪ Create new User Policy

The screenshot shows a web-based configuration interface for creating a new user policy. On the left is a navigation menu with the following items: Biometric Device Profile, Biometric Device, Wiegand Profiles, User Policy (highlighted with a yellow arrow), Access Schedules, User Distribution Group, and User Authentication Mode. The main content area is titled "Enter the details for this User Policy" and contains the following fields and options:

- Name:** A text input field containing "Printed Card and Pin". A yellow arrow points to this field, and a yellow box labeled "Name It" is positioned to its right.
- Description:** An empty text input field.
- Access Mode:** A dropdown menu set to "All Biometric Devices and Clients".
- Allow MA 500 database selection during user enrollment
- Access Schedule:** A dropdown menu set to "24 hours, 7 days a week".
- Display extended user details
- Extended User Details:** A section containing:
 - Wiegand Profile:** A dropdown menu set to "Standard 26 bit". A yellow arrow points to this field, and a yellow box labeled "Use the wiegand value of your Iclass card" is positioned to its right.
 - User Authentication Mode:** A dropdown menu set to "Printed Card and Pin". A yellow arrow points to this field, and a yellow box labeled "Use the UAM you created in Step 1" is positioned below it.
- Show Photo Capture Page:** A checkbox that is checked.

At the bottom right, there is a "Next" button with a right-pointing arrow icon. A blue arrow points from the "Use the UAM you created in Step 1" box to the "Next" button.

Step 2

- Continues

Enter the details for finger biometric options

Finger Biometric Enrollment Minimum Fingers:	<input type="text" value="None"/>
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"/>



Change this field to None



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.



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.**

Step 3

Create or Edit a Biometric Device Profile or BDP.

Biometric Device Profile

Biometric Device

Wiegand Profiles

User Policy

Access Schedules

User Distribution Group

User Authentication Mode

Enter details for the Biometric Device Profile

Name: **Name It**

Description:

Configuration Mode:

Log Retrieval Enabled:

Log retrieval interval: (seconds)

Duplicate check on biometrics: (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:

Next

Step 3

- **Continues**

Biometric Device Settings

General Settings

Wiegand Profile: Standard 26 bit - HID PACS

Language: English

Realtime logging enabled:

Biometric Threshold Settings


Biometric Threshold: Recommended

MorphoAccess Vein Print Mode: Universal Fast

MorphoAccess Fingerprint Threshold: 3

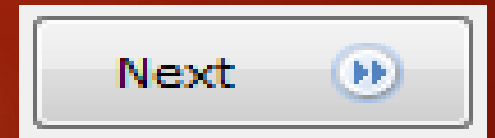
Morpho 3D Face Identification Threshold: Medium

Morpho 3D Face Verification Threshold: Low

 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.

Select 26 PACS or 35 HID Corporate 1000 35 PACS HID

****You might need to created a custom Wiegand format if not in list**



Step 3

- Continues

Multi-Factor Mode Settings

Multi-Factor Mode: ← **Select HID Iclass PACS Data**

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+, MA Sigma Extreme and MorphoWave Multi-Factor Modes

Biometric:	<input type="checkbox"/>	Mifare Classic:	<input type="checkbox"/>
Proximity Card:	<input type="checkbox"/>	Mifare DESFire:	<input type="checkbox"/>
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 checked="" 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.**

Step 4

Biometric Device Profile

Biometric Device

Wiegand Profiles

User Policy

Access Schedules

User Distribution Group

User Authentication Mode

Enter the details for this Biometric Device

Name: **Name It**

Description:

Location:

Asset ID:

Export Value:

Time Zone:

Hardware Family: **Pick the Hardware Family**

Serial Number:

Hostname\IP Address: **Put in the IP address**

Port:

Biometric Device Profile: **Put in the BDP**

Include in Time & Attendance Exports:

Change User Onsite / Offsite Status:

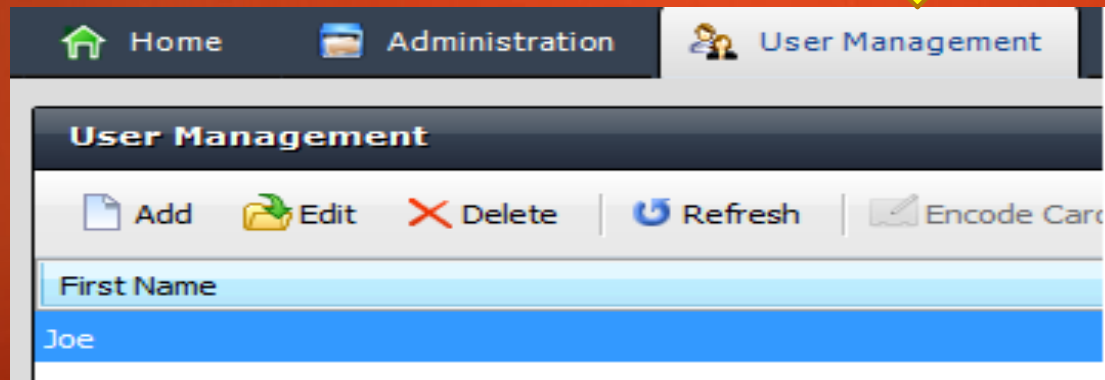
Onsite Key:

Offsite Key:

Finish

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.



Step 5

▪ 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.



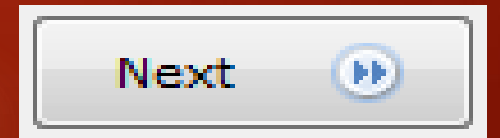
Next 

Step 5

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

Wiegand Values

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



Step 5

Enter your Pin Code

Enter and confirm the PIN

PIN:

••••

Confirm PIN

••••

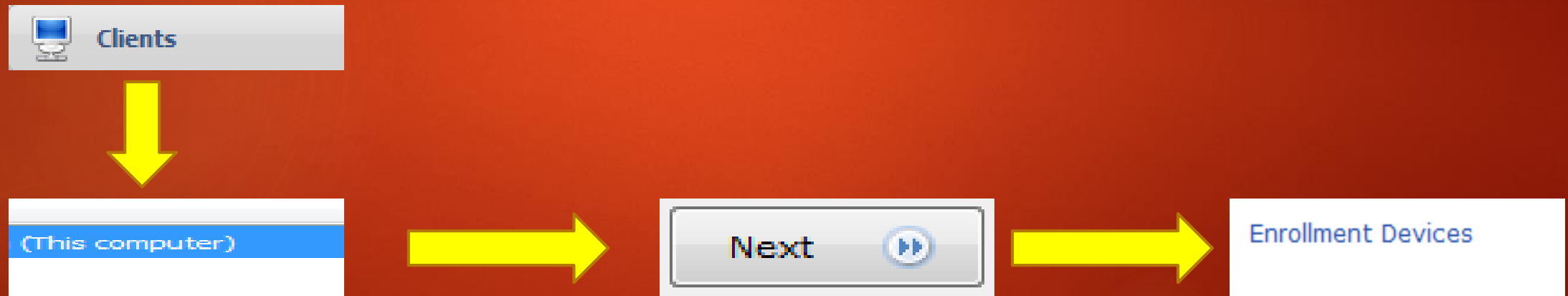


Finish



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



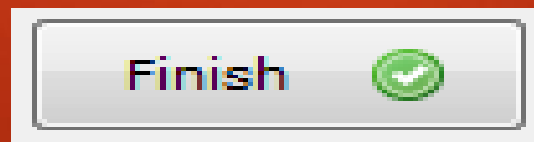
No MSO to capture fingerprints ? Use a Sigma and Sigma Lite for enrollment

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 for software, firmware, videos and PDF's.