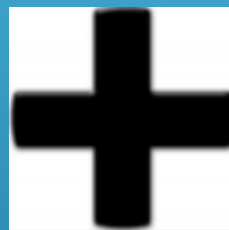


HOW TO USE FINGER AND PIN ACCESS



TO WORK WITH SIGMA ICLASS/ SIGMA ICLASS LITE PLUS, SIGMA EXTREME

ACRONYMS

UP=USER POLICY

BDP=BIOMETRIC DEVICE PROFILE

MM=MORPHO MANAGER

ACP=ACCESS CONTROL PANEL

CSN=CARD SERIAL NUMBER

MORPHOMANAGER DEFAULT LOG IN

USERNAME-ADMINISTRATOR

PASSWORD-PASSWORD

ADD AN BIOMETRIC DEVICE

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 + MA Sigma Extreme, the Morpho 3D Face, the MorphoWave Tower, MorphoWave Compact, and the Morpho Tablet Terminal.

ADD THE DEVICE AS THE EXAMPLE BELOW

- Operator
- Key Policy
- Biometric Device Profile
- Biometric Device**

Enter the details for this Biometric Device

Name: Sigma Iclass

Description:

Location:

Asset ID:

Export Value:

Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Hardware Family: MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme, MA Sigma VP

Serial Number:

Hostname\IP Address: 192.168.1.10

Port: 11010

Biometric Device Profile: Default

Include in Time & Attendance Exports:

Change User Onsite / Offsite Status:

Onsite Key: No Key

Offsite Key: No Key



Finish

CLIENTS



Path Administration>Clients

Clients are computers that have the MorphoManager Client software installed and communicate with a MorphoManager server

Next pages is if you do not own a MSO for capturing fingerprints



ADD YOUR SIGMA TO YOUR CLIENT

Operator

Key Policy

Biometric Device Profile

Biometric Device

Wiegand Profiles

User Policy

Access Schedules

User Distribution Group

User Authentication Mode

Operator Role

Notifications

Clients

Enter the details for this client

Name:

Description:

Location:

Click Next 3 Times

USE A SIGMA TO CAPTURE FINGERPRINTS

Enrollment Devices

3D Face Enrollment

Morpho 3D Face enrollment:

Morpho 3D Face enrollment biometric device:

Contact Enrollment

Morpho Finger biometric enrollment:

Morpho Finger enrollment MorphoAccess:

Contactless Enrollment

Morpho Contactless Finger biometric enrollment:

Morpho Contactless Finger enrollment MorphoAccess:

Smartcard Encoding

Morpho Smartcard encoding:

Morpho Smartcard encoding PC/SC device:

Morpho Smartcard encoding MorphoAccess:

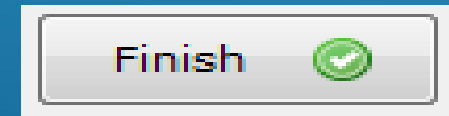
Keys

Key Policy:

DROP DOWN
SELECTED
MORPHOACCESS

SEARCH FOR THE
READER

****IF YOU DO HAVE A MSO NO
CHANGES NEED TO TAKE PLACE**



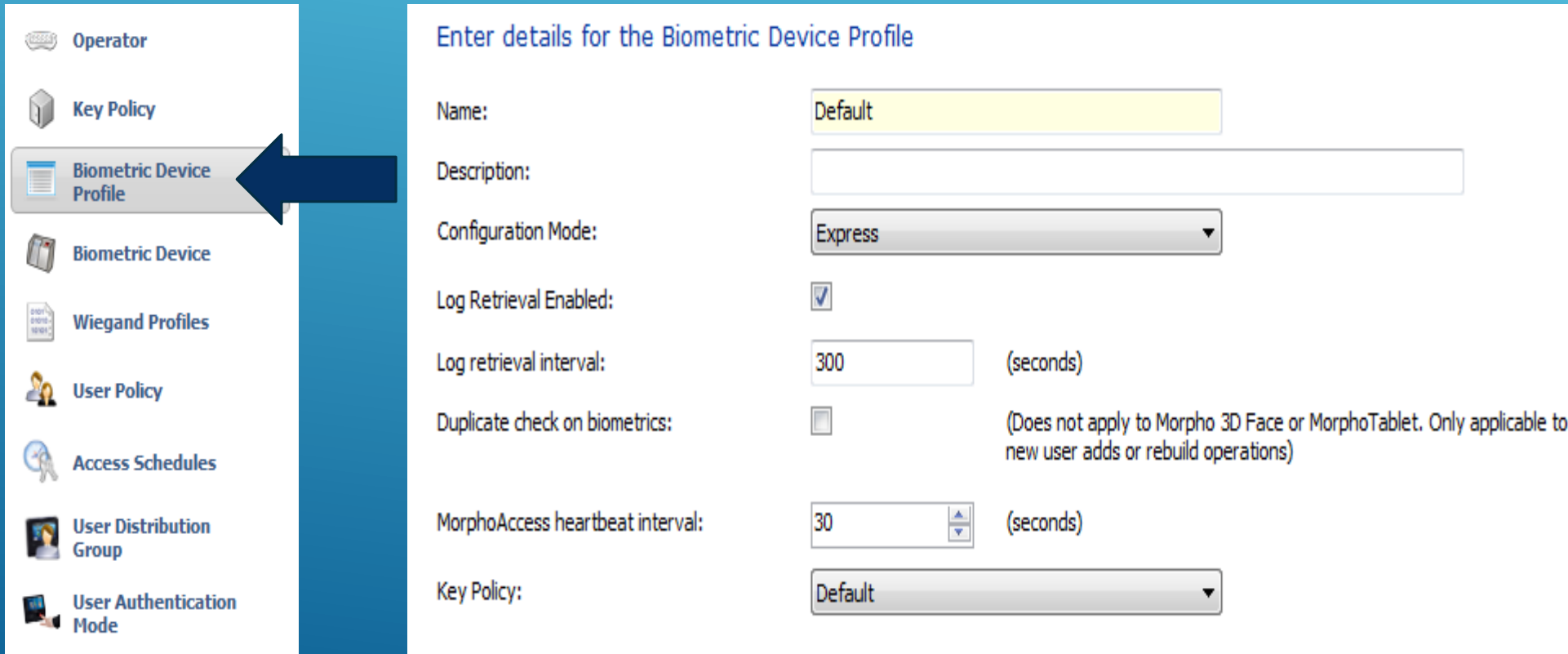
BIOMETRIC DEVICE PROFILE

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

CREATE OR EDIT THE BIOMETRIC DEVICE PROFILE



Operator

Key Policy

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:

Description:

Configuration Mode:

Log Retrieval Enabled:


Log retrieval interval: (seconds)

Duplicate check on biometrics: (Does not apply to Morpho 3D Face or MorphoTablet. Only applicable to new user adds or rebuild operations)

MorphoAccess heartbeat interval: (seconds)

Key Policy:



Next 

BIOMETRIC DEVICE PROFILE

Biometric Device Settings

General Settings

Wiegand Profile: Standard 26 bit

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.



Next 

WIEGAND PROFILE: USE THE WIEGAND FORMAT THAT WILL BE SENT TO THE ACP

BIOMETRIC DEVICE PROFILE

Multi-Factor Mode Settings

Multi-Factor Mode:

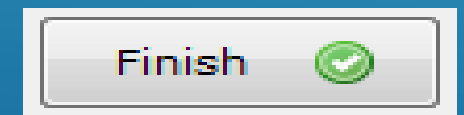
Contactless Smart Card Mode:

Morpho 3D Face Multi-Factor Mode

Mode:

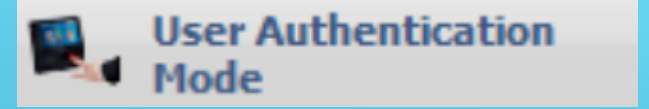
MA 100, MA J, MA 500, MA VP Multi-Factor Mode

Mode:



SET THE MULTI-FACTOR MODE SETTINGS AS EXACTLY AS SHOWN

USER AUTHENTICATION MODE



Path Administration>User Authentication Mode

Create new User Authentication Mode

User Authentication Mode(s) will set which authentication triggers will be utilized by users. The parameters are designated here and then a specific User Authentication Mode will be chosen as part of a User Policy. Users added to the system will have their authentication triggers governed by the User Authentication Mode portion of the User Policy they are placed in.

USER AUTHENTICATION MODE

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


Enter details for this User Authentication Mode

Name:

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.

CREATE A NEW USER AUTHENTICATION MODE



Next 

USER AUTHENTICATION MODE

MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme, MA VP MD, MorphoWave Settings

Mode: ←

Download Identifier To Device:

Encode To Smartcard Mode:

Template Location: ←

Pin Location: ←

Allow Start By Biometric: ←

Allow Start By Contactless Card:

Allow Start By Keyboard:

Allow Start By Wiegand In:

Require Pin: ←

Require Template Match:



Finish

FOLLOW THIS SETTINGS EXACTLY AS SHOWN

USER POLICY



Path Administration>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

CREATE A NEW USER POLICY

Enter the details for this User Policy

Name:

Description:

Access Mode:

Allow MA 500 database selection during user enrollment


Access Schedule:

Extended User Details: Display extended user details

Wiegand Profile:

User Authentication Mode:

Show Photo Capture Page:

Next 

**WIEGAND PROFILE USE THE FORMAT FOR THAT USER
USER AUTHENTICATION MODE IS THE ONE YOU CREATED EARLIER**


USER POLICY

CLICK TWO FOR FINGER BIOMETRICS


Enter the details for finger biometric options

Finger Biometric Enrollment Minimum Fingers:	Two	▼
Preferred Finger One:	Left Index Finger	▼
Preferred Finger Two:	Right Index Finger	▼
Preferred Duress Finger:	Left Middle Finger	▼
Vein / Print Mode:	Universal Fast	▼

Show Finger Biometric Capture Pages

 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.



Next 

USER POLICY

NONE FOR WAVE ENROLLMENTS

Enter the details for wave biometric options

Wave Enrollment Minimum Hands:

None

Show Wave Biometric Capture Page:

Finish



ENROLLMENT PROCESS

USER MANAGEMENT



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

CREATE A NEW USER WITH THE USER POLICY CREATED EARLIER

Enter details for this User

User Policy:

Enabled:

First Name:

Middle Name:

Last Name:

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



Next




POLICY: FINGER AND PIN


USER MANAGEMENT

MANUALLY THE USERS ID

Wiegand Values

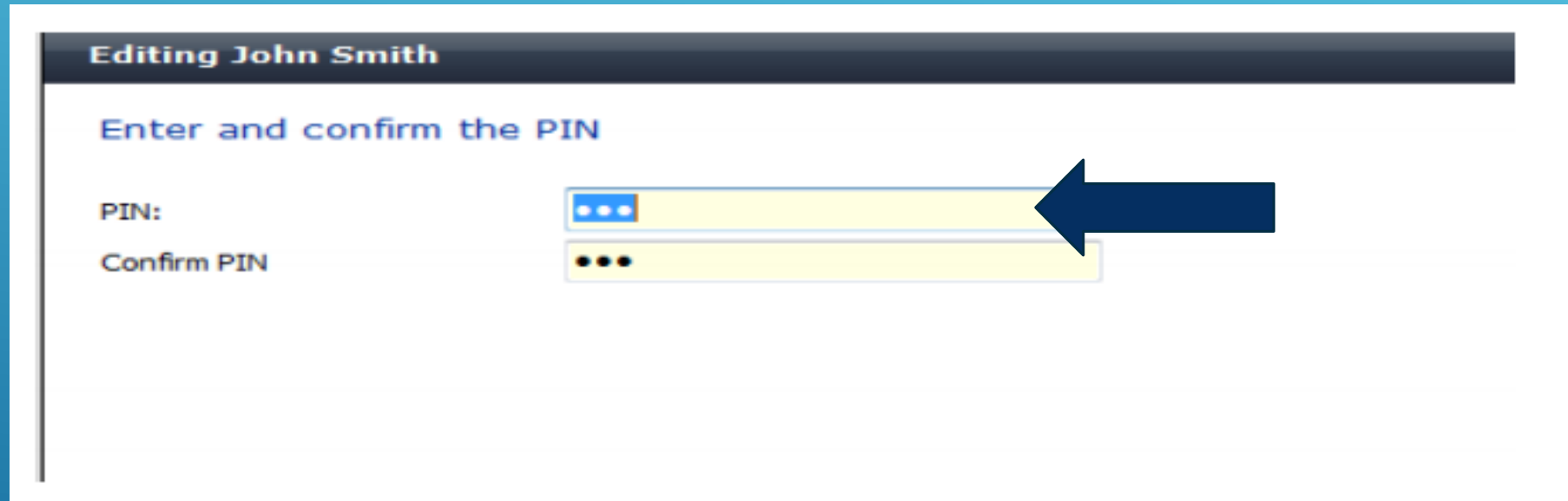
User ID	<input type="text" value="31"/>
---------	---------------------------------



Next 


USER MANAGEMENT

ADD A PIN



The screenshot shows a web interface for editing a user named John Smith. The title bar reads "Editing John Smith". Below it, the instruction "Enter and confirm the PIN" is displayed. There are two input fields: "PIN:" and "Confirm PIN". Both fields are currently empty and masked with dots. A large blue arrow points to the "PIN:" field, and a large red arrow points down from the "Finish" button to the text below.

THE PIN IS ASSORTED WITH THE USER ID

Finish 

FINAL RESOLUTION

ONE USER POLICY NEED TO BE CREATED FOR KEYPAD

USER AUTHENTICATION MODE NEEDS TO BE TIED TO THE USER POLICY

BIOMETRIC DEVICE PROFILE NEEDS TO BE CONFIGURED

YOU CAN VIEW OTHER WIEGAND FORMATS TO COMPARE

THE USER WILL PLACE FINGER THAN THE PIN CODE

THE PIN CODE IS NOT SENT TO THE CONTROLLER ITS ONLY A EXTRA AUTHENTICATION OF THE FINGERPRINT

PIN CODES ARE NOT STORED ON THE ACP

WEBSITE

Please visit our website,
service.morphotrak.com for
software, firmware, videos and
PDF'S