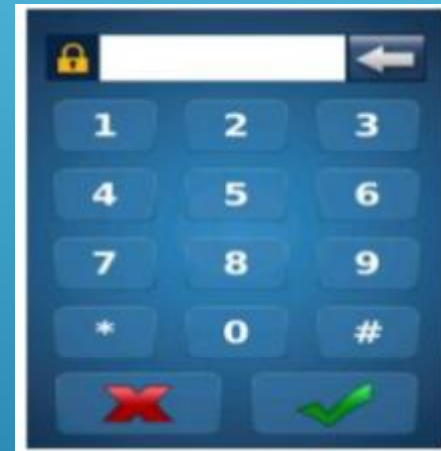
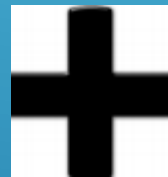
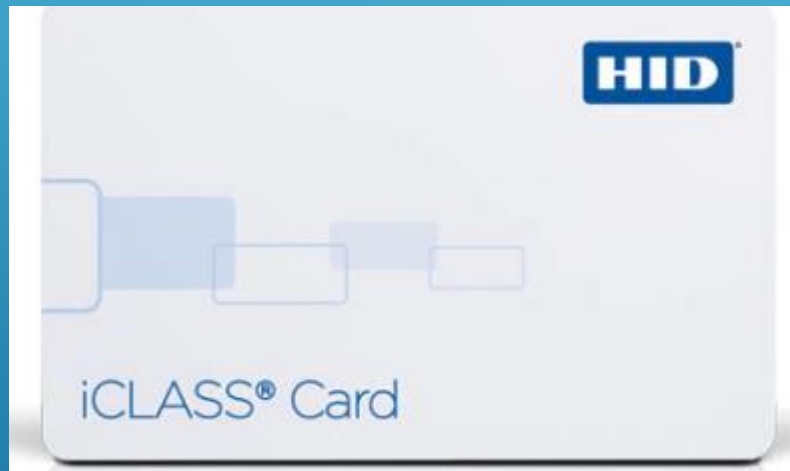


# HOW TO USE PRINTED ICLASS AND PIN



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

# ACRONYMS

UP=USER POLICY

BDP=BIOMETRIC DEVICE PROFILE

MM=MORPHO MANAGER

ACP=ACCESS CONTROL PANEL

CSN=CARD SERIAL NUMBER

UAM=USER AUTHENTICATION MODE

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:

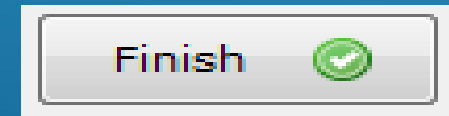
**Keys**

Key Policy:

DROP DOWN  
SELECTED  
MORPHOACCESS

SEARCH FOR THE  
READER

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



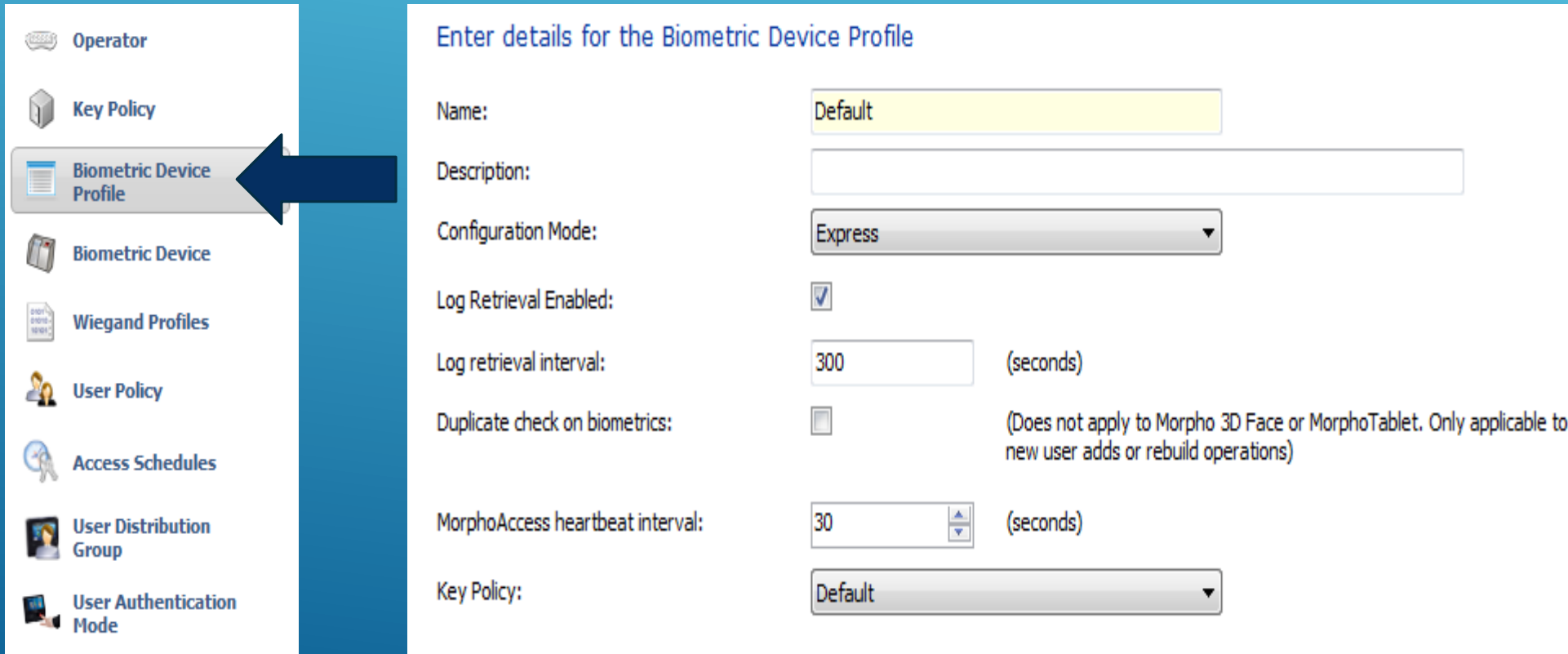
# BIOMETRIC DEVICE PROFILE

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 - HID PACS

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



Next 

**WIEGAND PROFILE: USE STANDARD 26 OR 35 BIT HID PACS DEPENDING ON CARD FORMAT OR ANY FORMAT CAN BE CREATED(CREATED FORMAT HAS TO CONTAIN PACS ELEMENTS)**

# BIOMETRIC DEVICE PROFILE

**Multi-Factor Mode Settings**

Multi-Factor Mode:  ←

Contactless Smart Card Mode:  ←

**Morpho 3D Face Multi-Factor Mode**

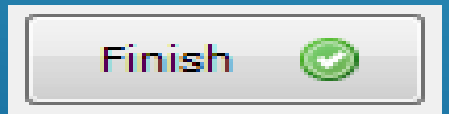
Mode:

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

Mode:

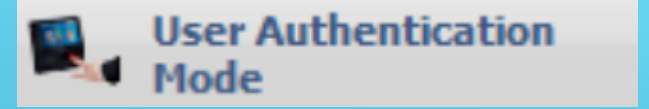
**MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme and MorphoWave Multi-Factor Modes**

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 checked="" type="checkbox"/>		
HID iClass SEOS:	<input type="checkbox"/>		



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**

**Adding 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 and MorphoWave Settings

Mode:  ←

Download Identifier To Device:

Encode To Smartcard Mode:

Template Location:

Pin Location:  ←

Allow Start By Biometric:

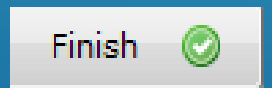
Allow Start By Contactless Card:  ←

Allow Start By Keyboard:

Allow Start By Wiegand In:

Require Pin:  ←

Require Template Match:



**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

**Operator**

**Key Policy**

**Biometric Device Profile**

**Biometric Device**

**Wiegand Profiles**

**User Policy** ←

**Access Schedules**

**User Distribution Group**

**User Authentication Mode**

Enter the details for this User Policy

Name: Printed Card and Pin

Description:

Access Mode: All Biometric Devices and Clients

Allow MA 500 database selection during user enrollment

Access Schedule: 24 hours, 7 days a week

Extended User Details:  Display extended user details

Wiegand Profile: Standard 26 bit ←

User Authentication Mode: Printed Card and Pin ←

Show Photo Capture Page:



Next

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

# USER POLICY

CLICK NONE FOR MINIMUM FINGERS


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"/>



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:

First Name:

Middle Name:

Last Name:

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



Next



POLICY: EXAMPLE PRINTED ICLASS CARD AND PIN

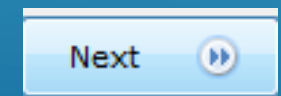
# USER MANAGEMENT

MANUALLY TYPE IN THE PRINTED CARD NUMBER

Wiegand Values

User ID

**THE USER ID IS THE PRINTED ICLASS CARD NUMBER THAT WILL  
BE SENT TO YOUR ACCESS CONTROL PANEL**



# USER MANAGEMENT

ENTER YOUR PIN CODE

Enter and confirm the PIN

PIN:

•••

Confirm PIN

•••



Finish





# FINAL RESOLUTION

ONE USER POLICY NEED TO BE CREATED FOR PRINTED ICLASS CARD AND PIN

USER AUTHENTICATION MODE NEEDS TO BE TIED TO THE USER POLICY

BIOMETRIC DEVICE PROFILE NEEDS TO BE CONFIGURED

IF YOUR ICLASS CARDS FORMAT DOES NOT MATCH THE PRE FORMATS THAT COME WITH MORPHOMANAGER THEN YOU NEED TO KNOW THE FULL STRUCTURE AND CREATED THAT FORMAT

YOU CAN VIEW OTHER WIEGAND FORMATS TO COMPARE

THE USER WILL PLACE THERE CARD THEN PIN

THE CARD NUMBER NOT THE PIN GETS SENT TO THE ACP

SO FOR EXAMPLE USER PLACES CARD 31 TO THE READER THEN ENTER PIN CODE 123 , 31 GETS SENT TO THE CONTROLLER

# WEBSITE

Please visit our website,  
[service.morphotrak.com](http://service.morphotrak.com) for  
software, firmware, videos and  
PDF'S