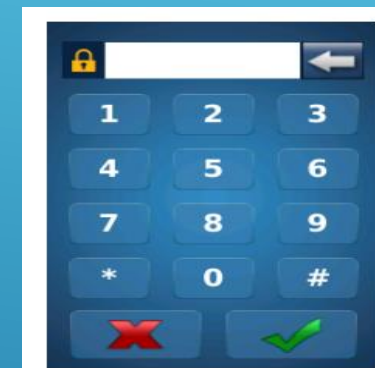
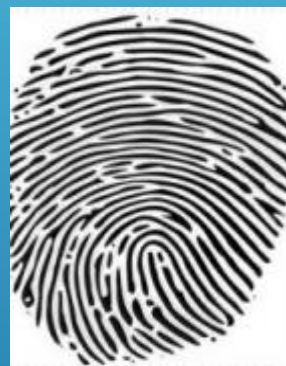
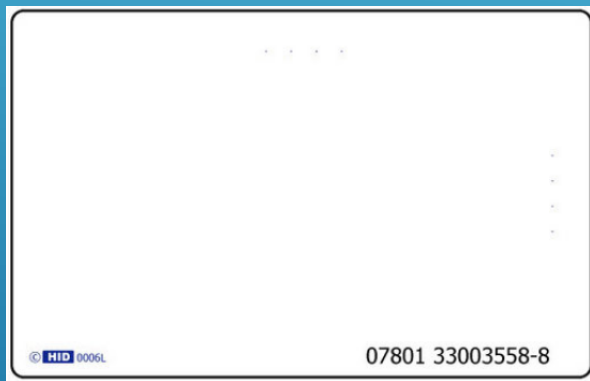


HOW TO USE ENCODED ICLASS CARD AND FINGER AND PIN



TO WORK WITH SIGMA ICLASS/ SIGMA ICLASS LITE, SIGMA EXTRME ICLASS

ACRONYMS

UP=USER POLICY

UAM=USER AUTHENTICATION MODE

BDP=BIOMETRIC DEVICE PROFILE

MM=MORPHO MANAGER

ACP=ACCESS CONTROL PANEL

CSN=CARD SERIAL NUMBER

SI=SYSTEM INTEGRATOR

MORPHOMANAGER DEFAULT LOG IN

USERNAME-ADMINISTRATOR

PASSWORD-PASSWORD

HARDWARE REQUIREMENTS

HID OMNIKEY ,5427 CK OR G2 IS RECOMMENDED
FOR ENCODING (SI RESPONSIBILITY TO PURCHASE)

A MSO TO CAPTURE FINGERPRINT ENROLLMENTS



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:

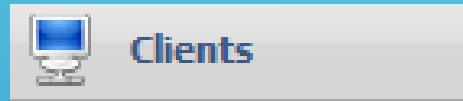
Onsite Key: No Key

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: This PC

Description:

Location:

Click Next until Enrollment Devices

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:

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

**DROP DOWN
SELECTED
MORPHOACCESS**

**SEARCH FOR THE
READER**

**OMNIKEY WILL
SHOW UP HERE OR
USE A SIGMA FOR
ENCODING**



Finish

BIOMETRIC DEVICE PROFILE



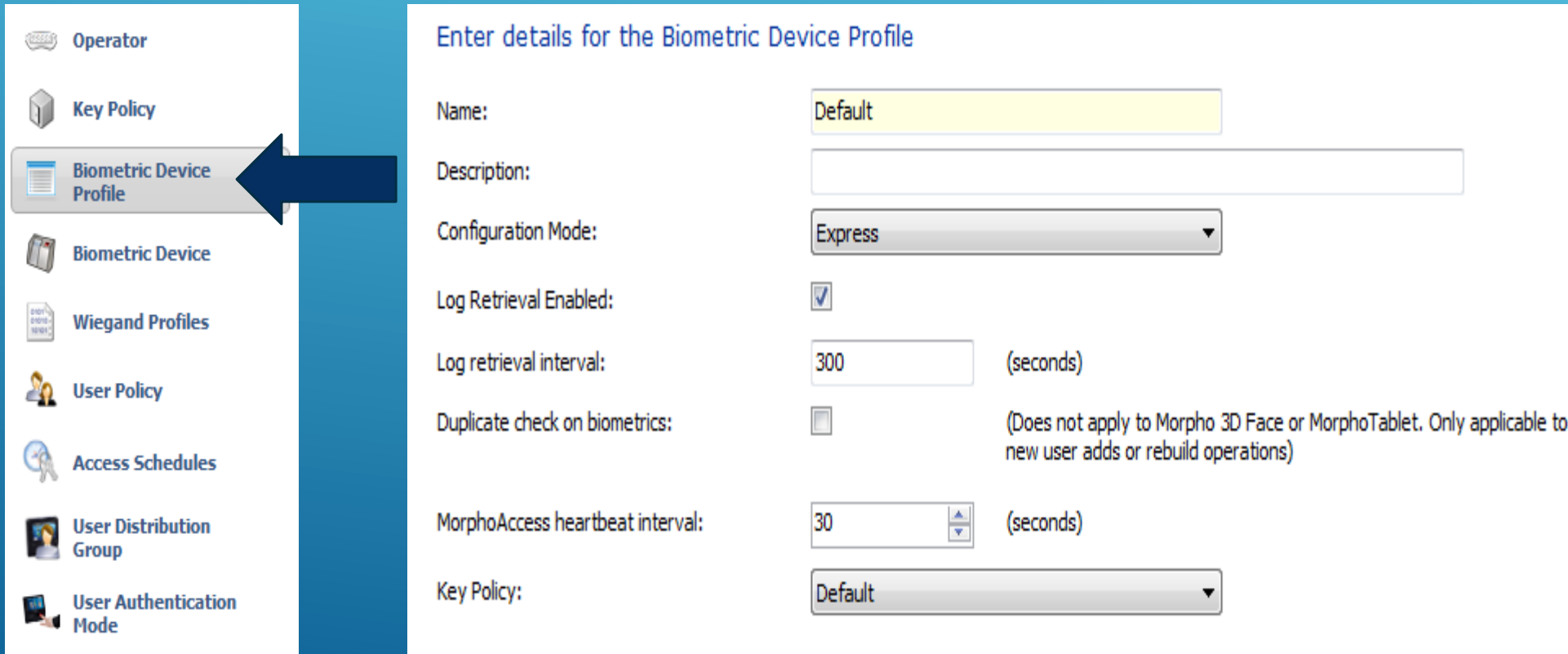
Biometric Device
Profile

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: Default

Description:

Configuration Mode: Express

Log Retrieval Enabled:

Log retrieval interval: 300 (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: 30 (seconds)

Key Policy: Default



BIOMETRIC DEVICE PROFILE

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



Next 

THE WIEGAND PROFILE MUST BE SET TO YOUR FORMAT FOR YOUR PANEL

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:

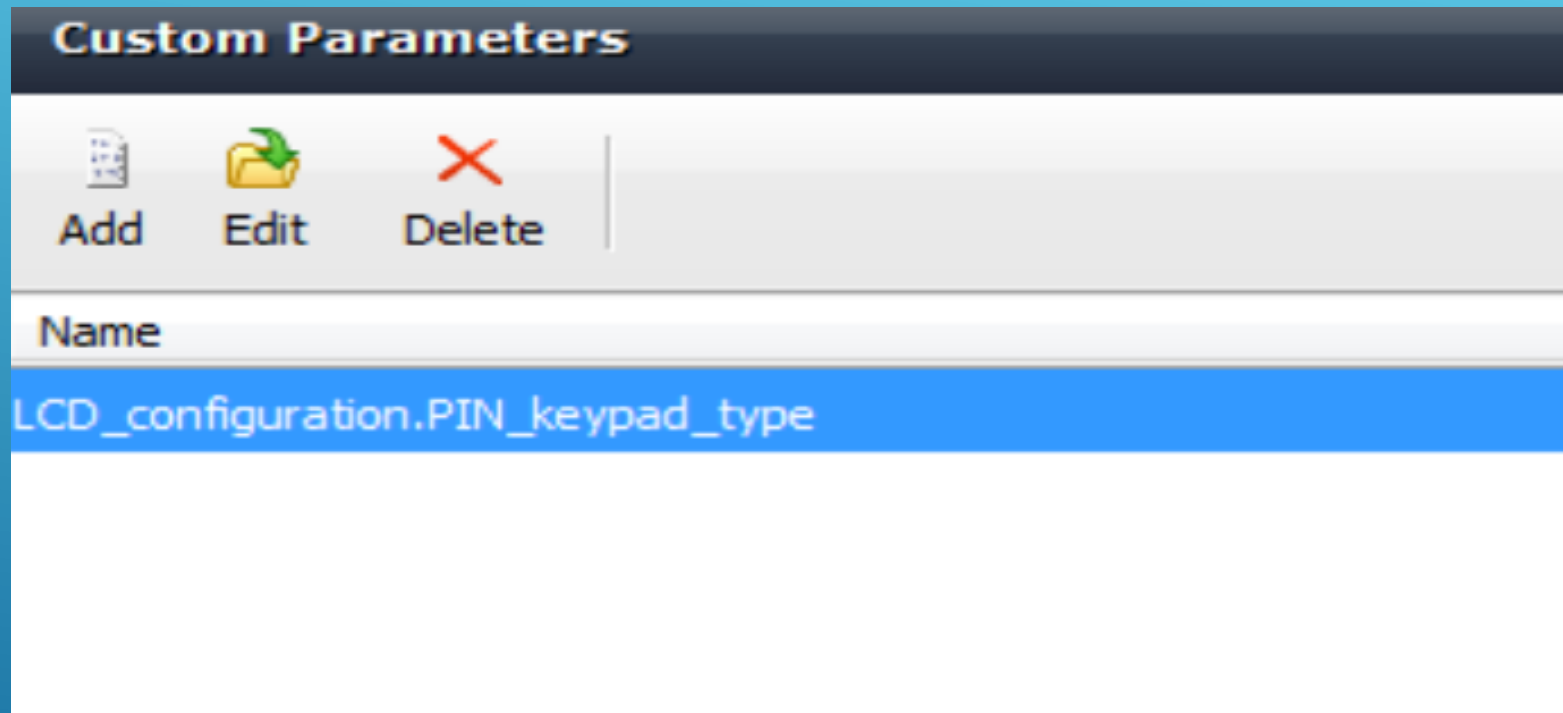
MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme, MA VP MD and MorphoWave Multi-Factor Modes

Biometric:	<input type="checkbox"/>	Mifare Classic:	<input type="checkbox"/>
Proximity Card:	<input type="checkbox"/>	Mifare DESFire 3DES:	<input type="checkbox"/>
Wiegand In:	<input type="checkbox"/>	Mifare DESFire AES:	<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"/>		



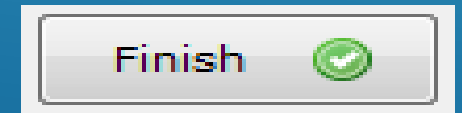
SET THE MULTI-FACTOR MODE SETTINGS AS EXACTLY AS SHOWN

BIOMETRIC DEVICE PROFILE

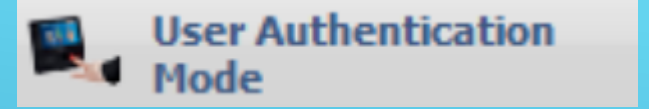


**CLICK NEXT SEVERAL TIMES TILL YOU GET TO CUSTOM PARAMETERS
ADD THIS PARAMETERS EXACTLY AS SHOWN, CASE SENSITIVE**

**LCD_configuration.PIN_keypad_type
VALUE=1**



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:

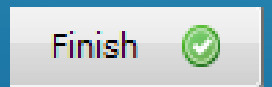
Allow Start By Wiegand In:

Require Pin: ←

Require Template Match: ←



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: Encoded Iclass Card and Finger 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: Encoded Iclass Card and Finger and I

Show Photo Capture Page:

Next

**WIEGAND PROFILE, USE THE WIEGANG FORMAT OF THE ICLASS CARD
USER AUTHENTICATION MODE IS WHAT IS WAS CREATED PREVIOUSLY**

USER POLICY

CLICK TWO FOR FINGER BIOMETRICS

Enter the details for finger biometric options

Finger Biometric Enrollment Minimum Fingers:

Preferred Finger One:

Preferred Finger Two:

Preferred Duress Finger:

Vein / Print Mode:



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



USER POLICY ENCODED ICLASS CARD AND FINGER AND PIN


USER MANAGEMENT

MANUALLY TYPE IN THE ID NUMBER FOR THIS USER

Wiegand Values

User	<input type="text" value="12345"/>
------	------------------------------------



Next 

USER MANAGEMENT

PUT IN THE PIN CODE YOU WANT TO USE

Enter and confirm the PIN

PIN:

●●●

Confirm PIN

●●●|

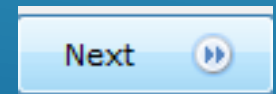
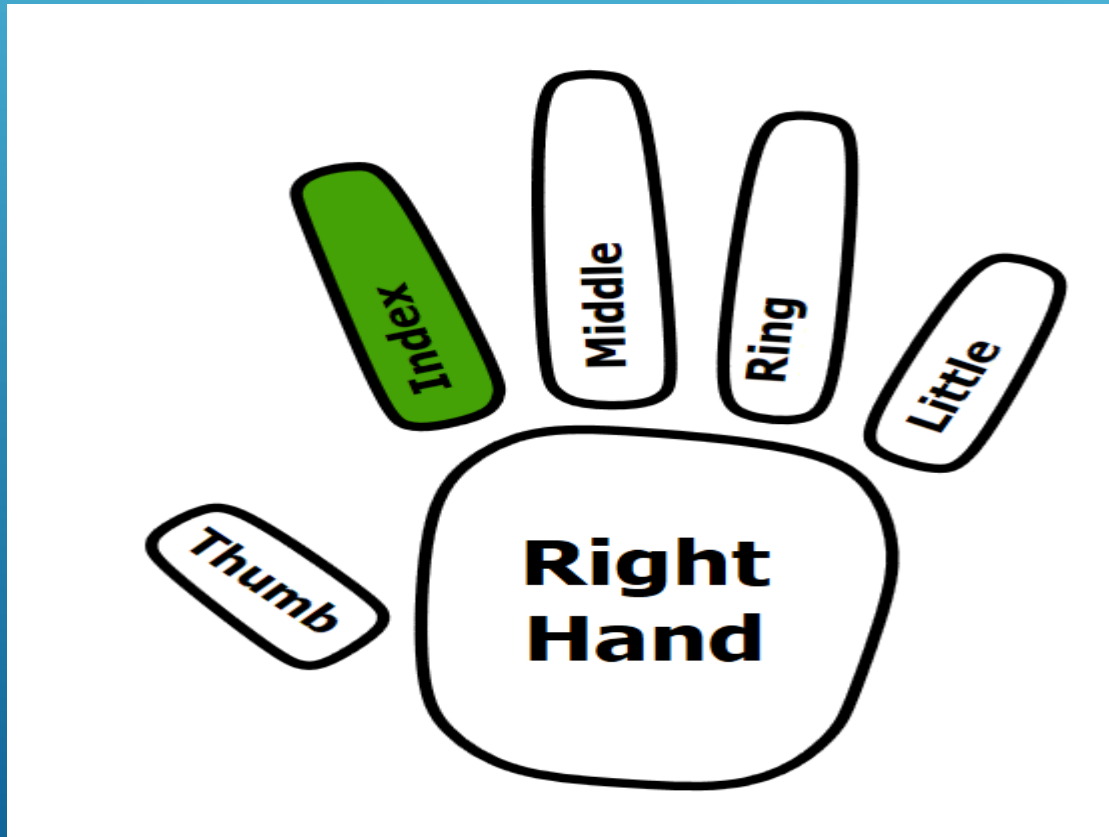


Next



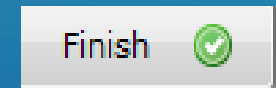
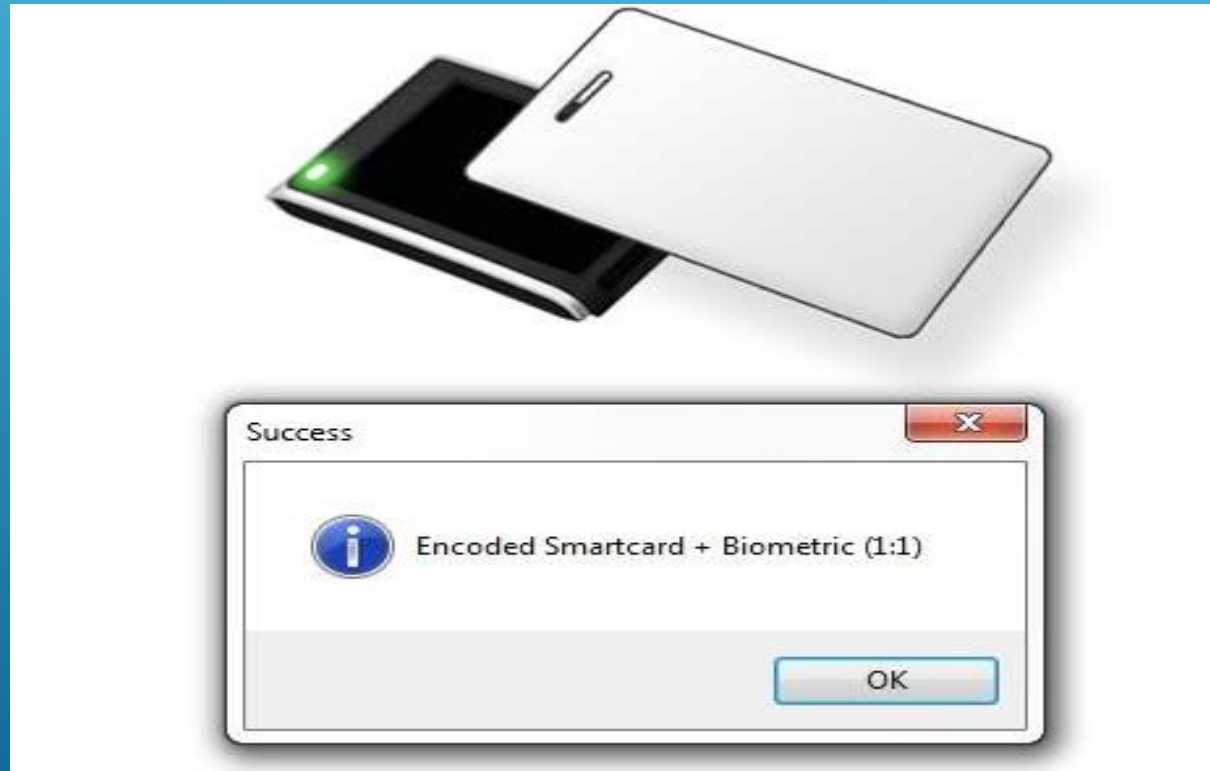
USER MANAGEMENT

CAPTURE YOUR FINGER PRINTS



USER MANAGEMENT

ENCODE THE CARD



FINAL RESOLUTION

ONE USER AUTHENTICATION MODE HAS TO BE CREATED (UAM)

ONE USER POLICY NEED TO BE CREATED WITH THE UAM

BIOMETRIC DEVICE PROFILE NEEDS TO BE CONFIGURED

IF YOUR CARD 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 PIN DOES NOT COME FROM THE PANEL BUT IS STORED ON THE CARD

WEBSITE

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