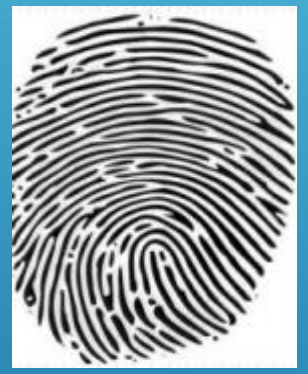
HOW TO USE ENCODED ICLASS CARD AND FINGER AND PIN



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)

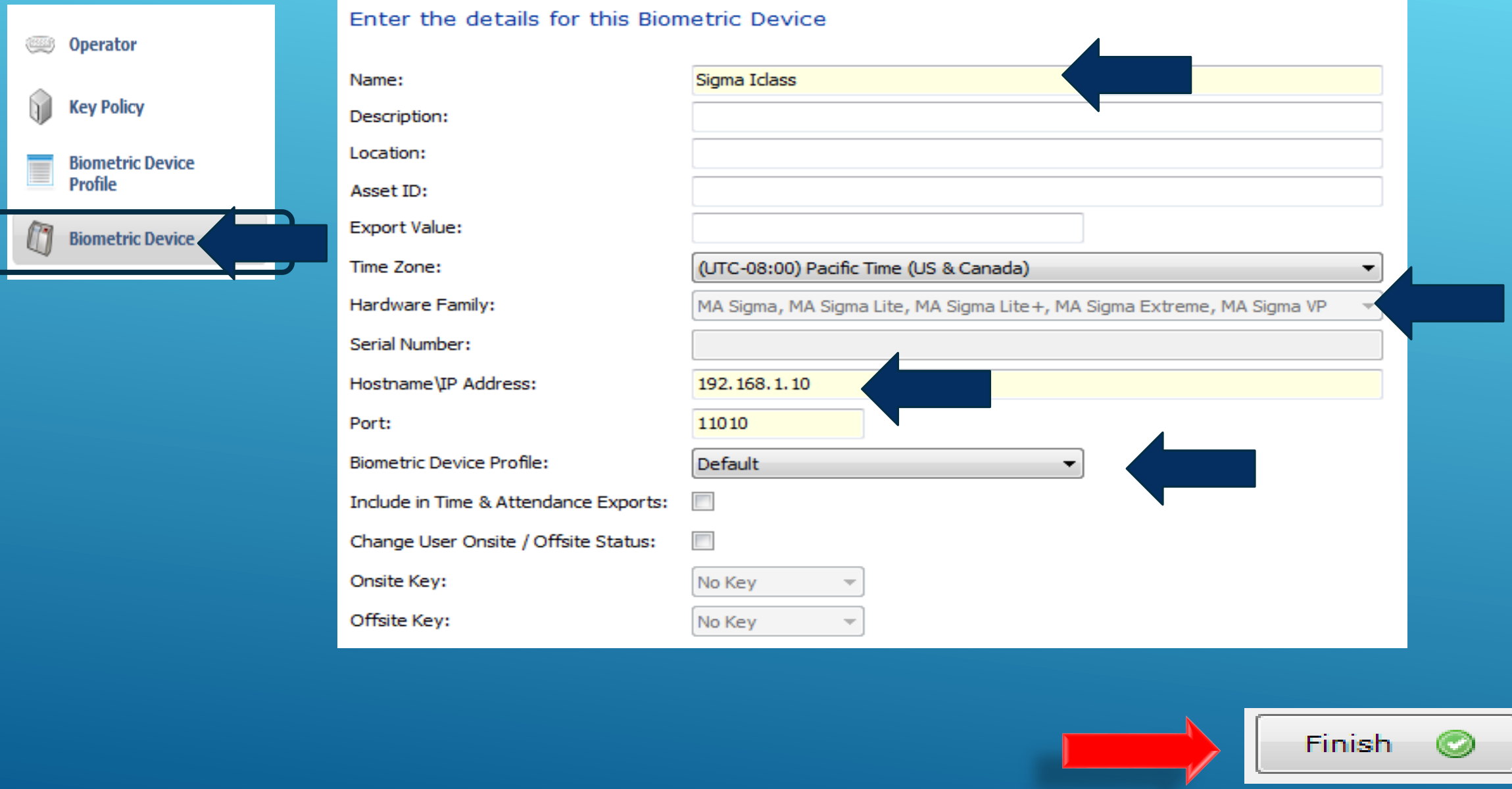
A MSO TO CAPTURE FINGERPRINT ENROLLMENTS

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



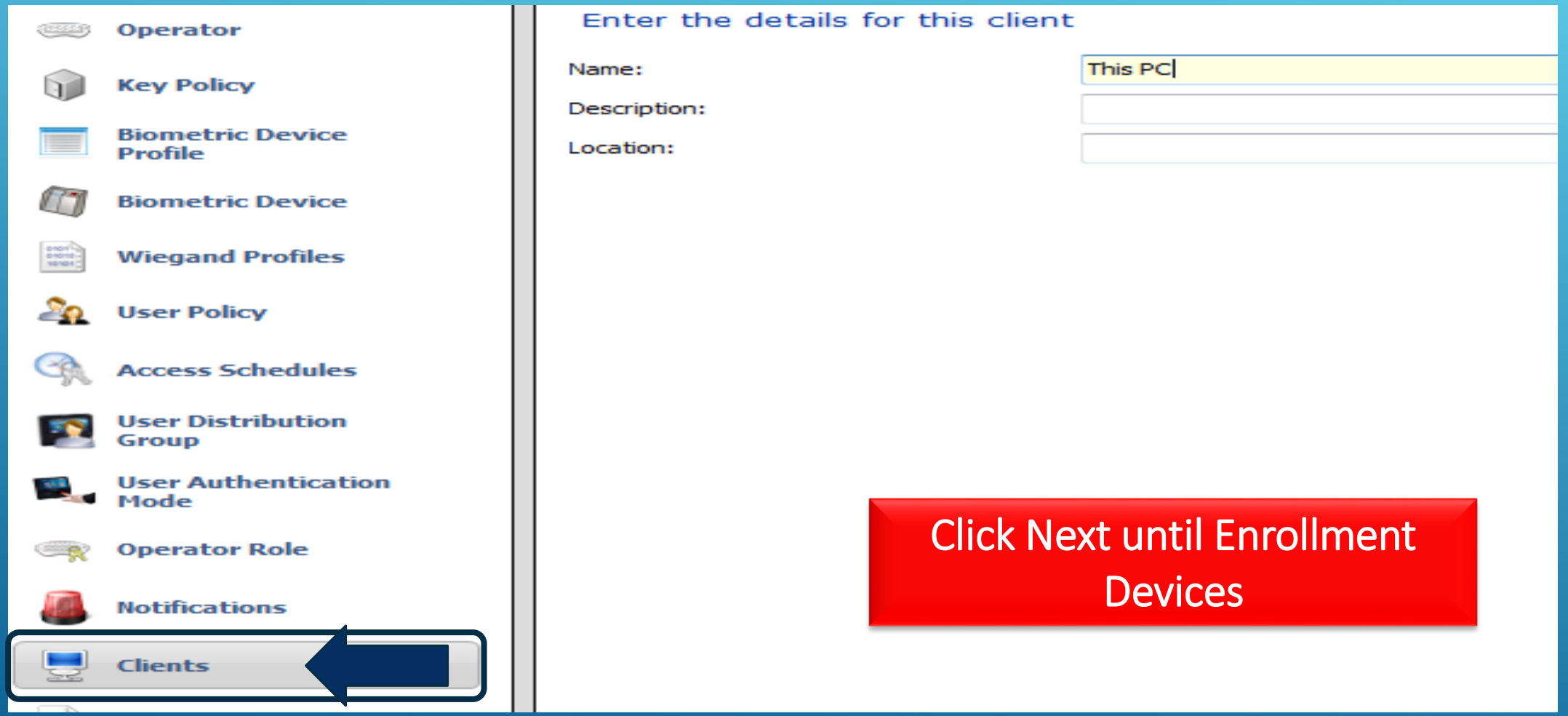
CLIENTS

Path Administration>Clients

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

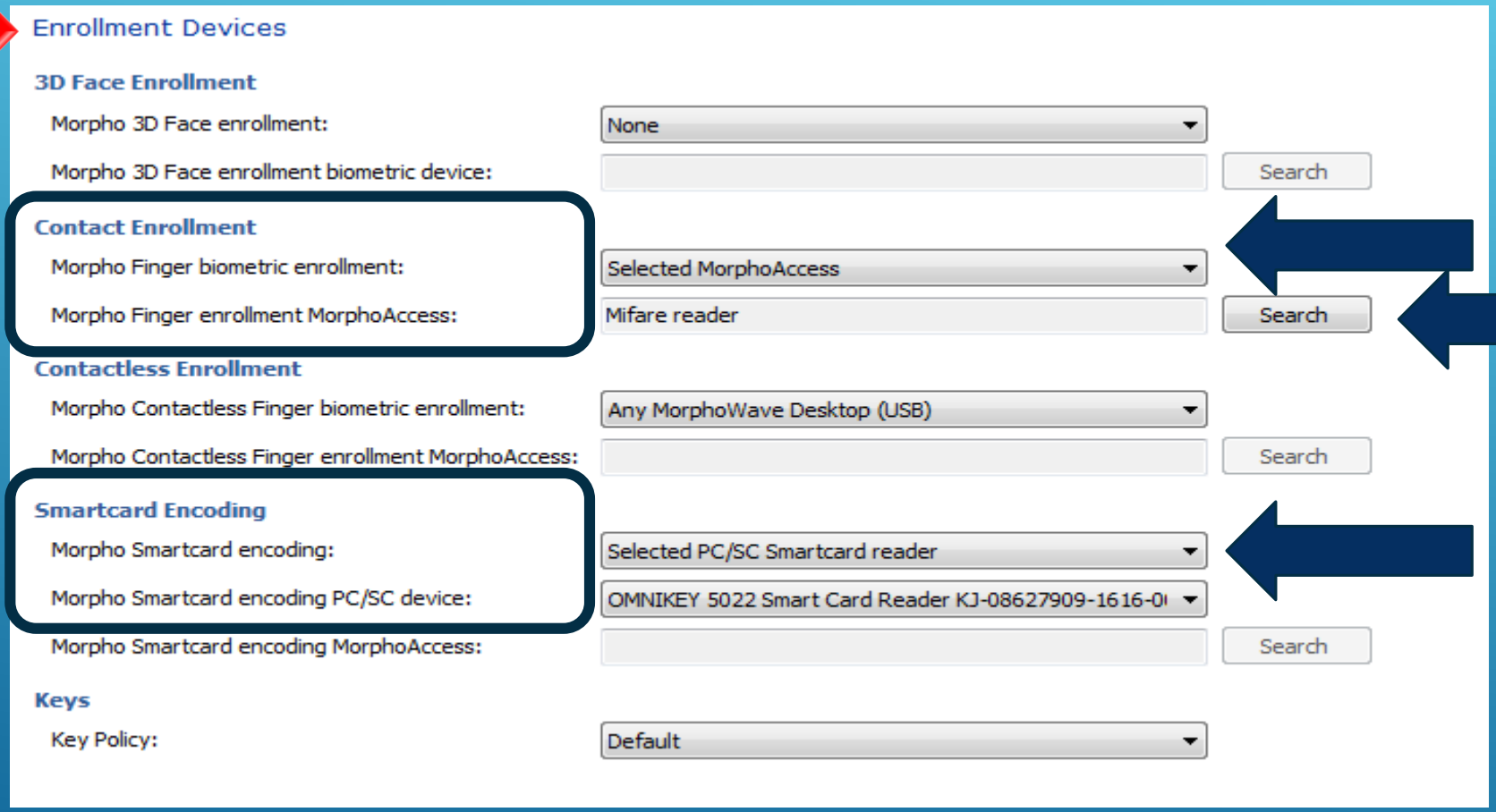
Next pages is if you do not own a MSO for capturing fingerprints

ADD YOUR SIGMA TO YOUR CLIENT



USE A SIGMA TO CAPTURE FINGERPRINTS

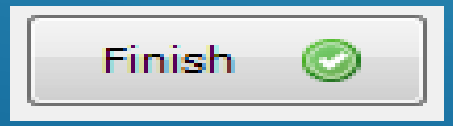
**IF YOU DO HAVE A MSO NO CHANGES NEED TO TAKE PLACE



DROP DOWN SELECTED MORPHOACCESS

SEARCH FOR THE READER

OMNIKEY WILL SHOW UP HERE OR USE A SIGMA FOR ENCODING



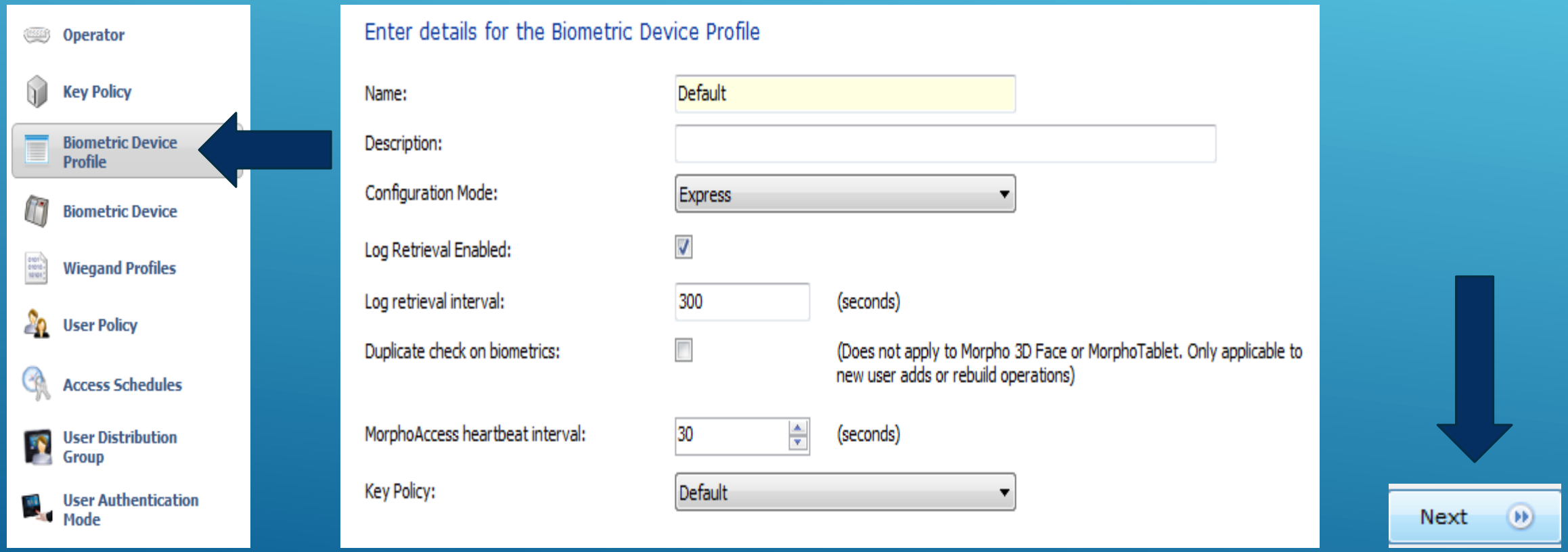
BIOMETRIC DEVICE PROFILE

Path Administration>Biometric Device Profile

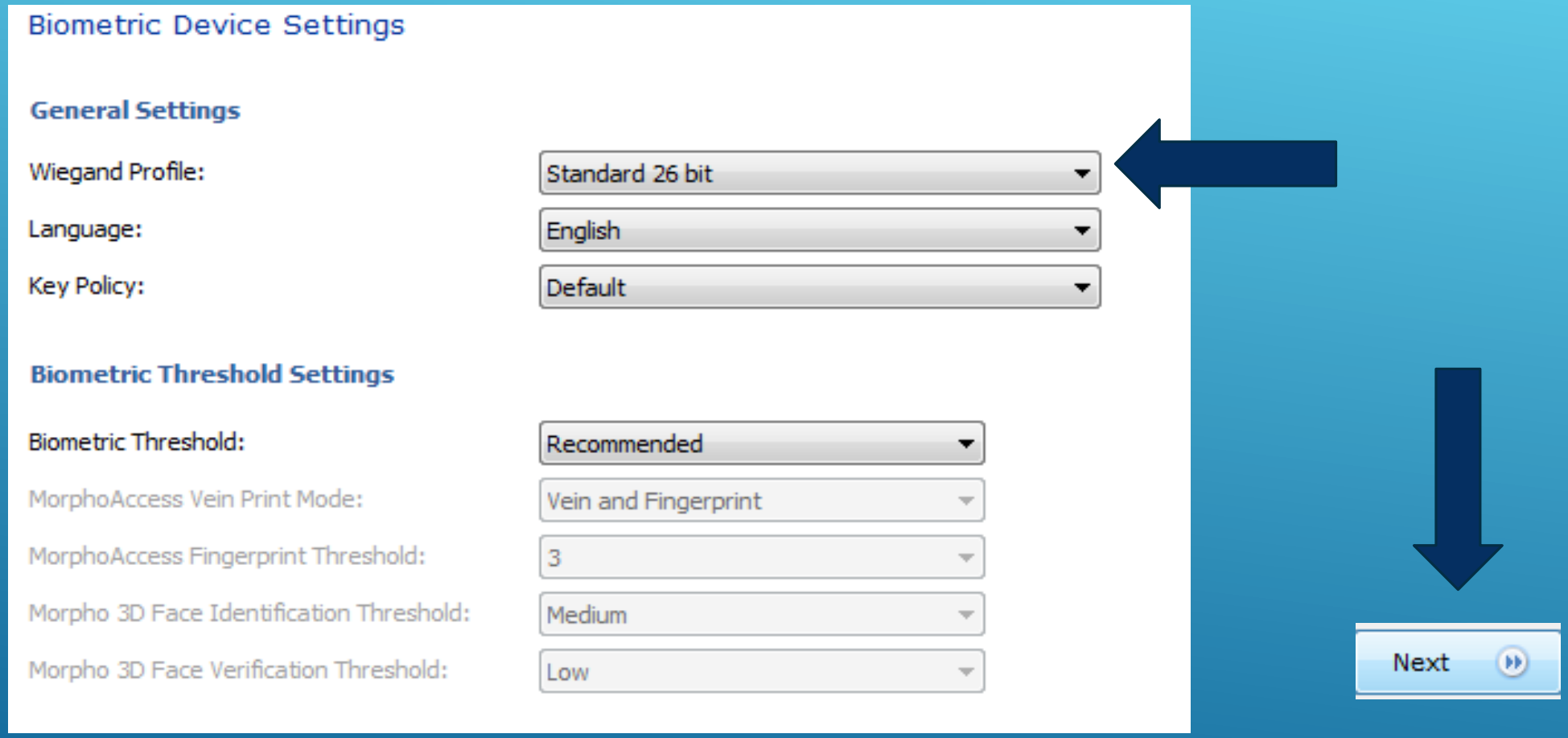
The Biometric Device Profile will define common settings and parameters for one or more biometric devices. This profile can be applied when adding units into the system from the Biometric Device section of Administration

BIOMETRIC DEVICE PROFILE

CREATE OR EDIT THE BIOMETRIC DEVICE PROFILE



BIOMETRIC DEVICE PROFILE

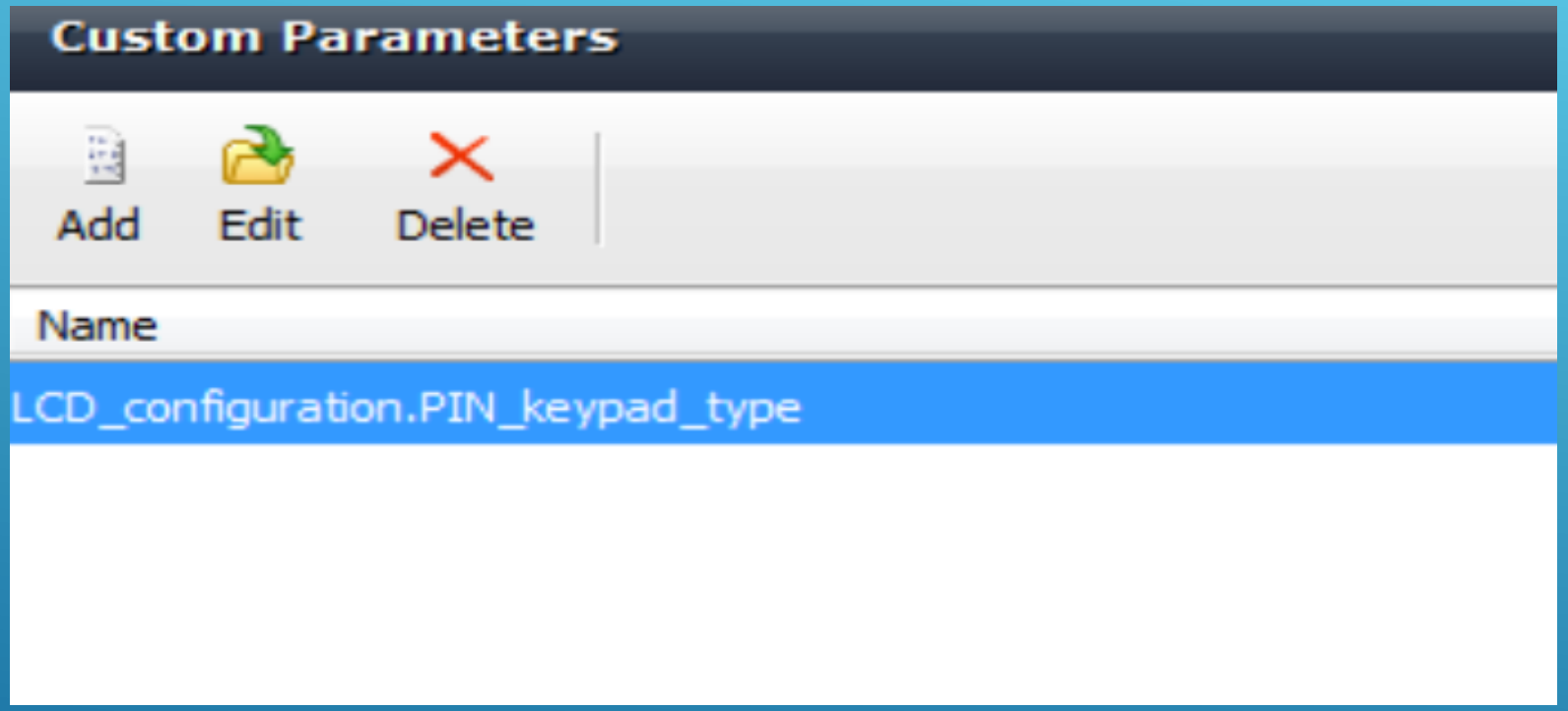


THE WIEGAND PROFILE MUST BE SET TO YOUR FORMAT FOR YOUR PANEL

BIOMETRIC DEVICE PROFILE

SET THE MULTI-FACTOR MODE SETTINGS AS EXACTLY AS SHOWN

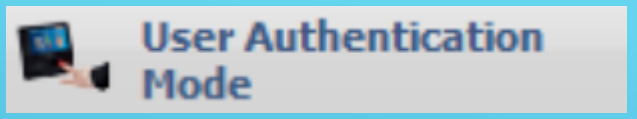
BIOMETRIC DEVICE PROFILE



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

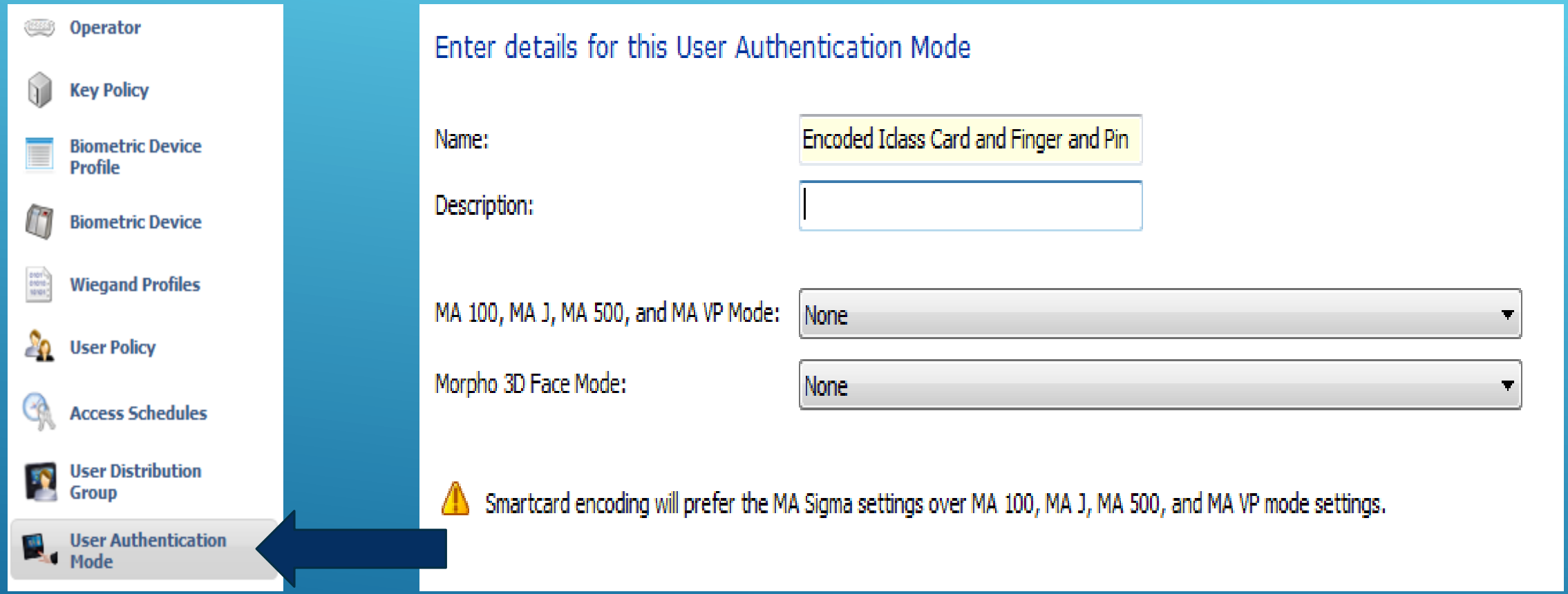


Path Administration>User Authentication Mode

Create new User Authentication Mode

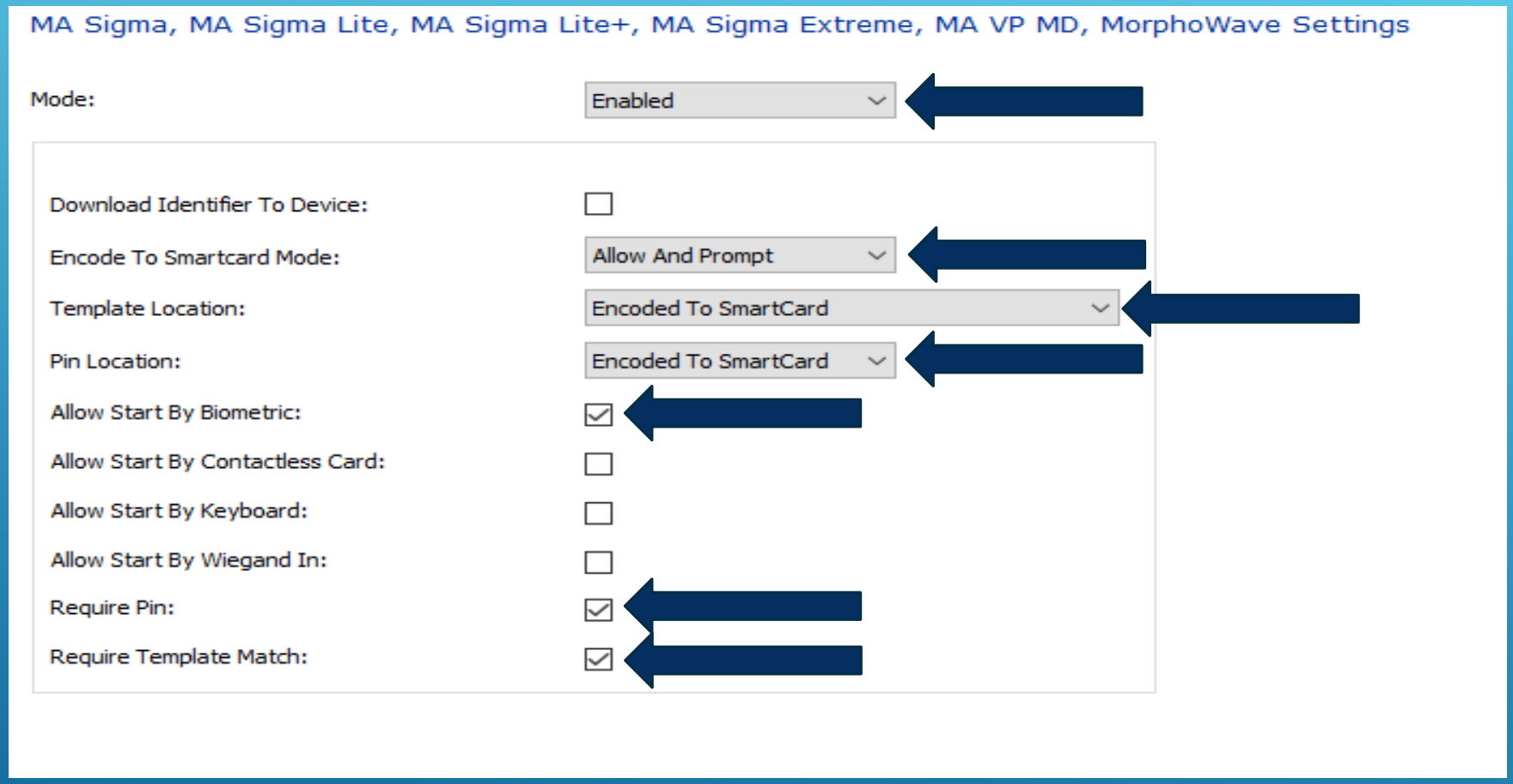
User Authentication Mode(s) will set which authentication triggers will be utilized by users. The parameters are designated here and then a specific User Authentication Mode will be chosen as part of a User Policy. Users added to the system will have their authentication triggers governed by the User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

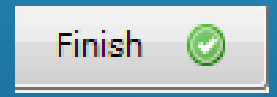
USER AUTHENTICATION MODE



CREATE A NEW USER AUTHENTICATION MODE

USER AUTHENTICATION MODE





FOLLOW THIS SETTINGS EXACTLY AS SHOWN

USER POLICY

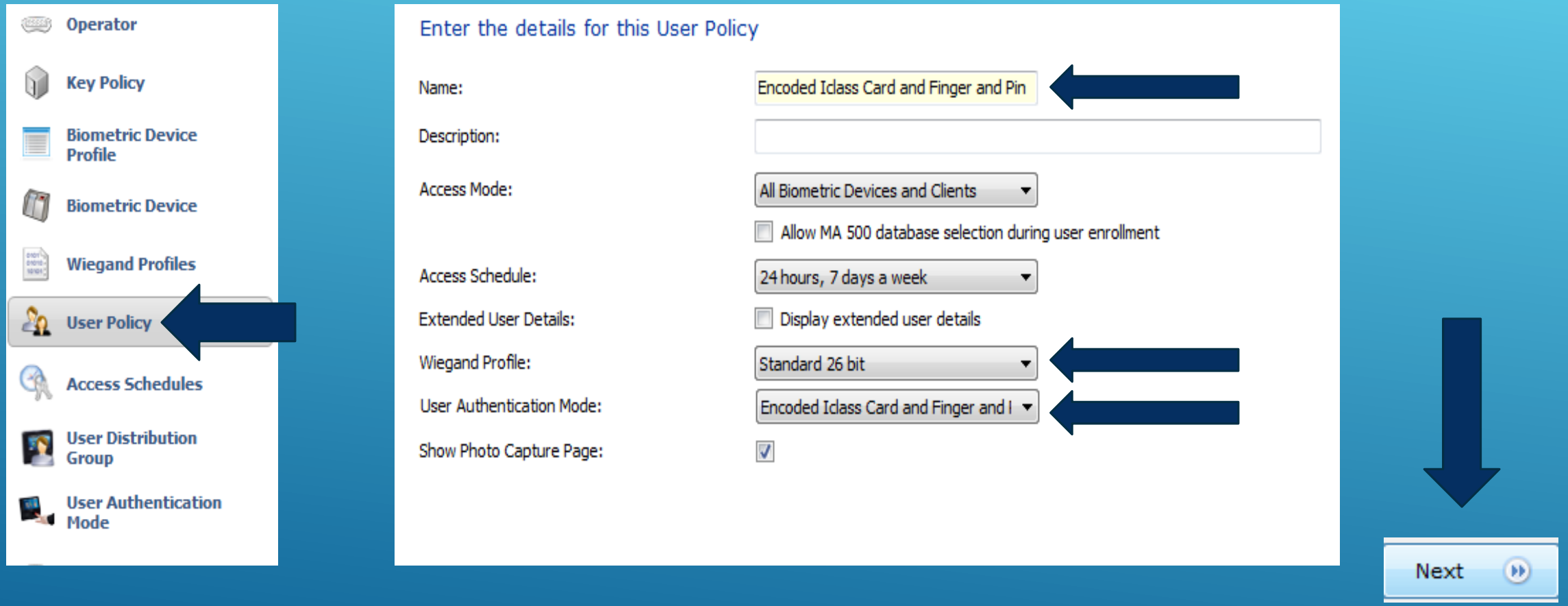
Path Administration>User Policy

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

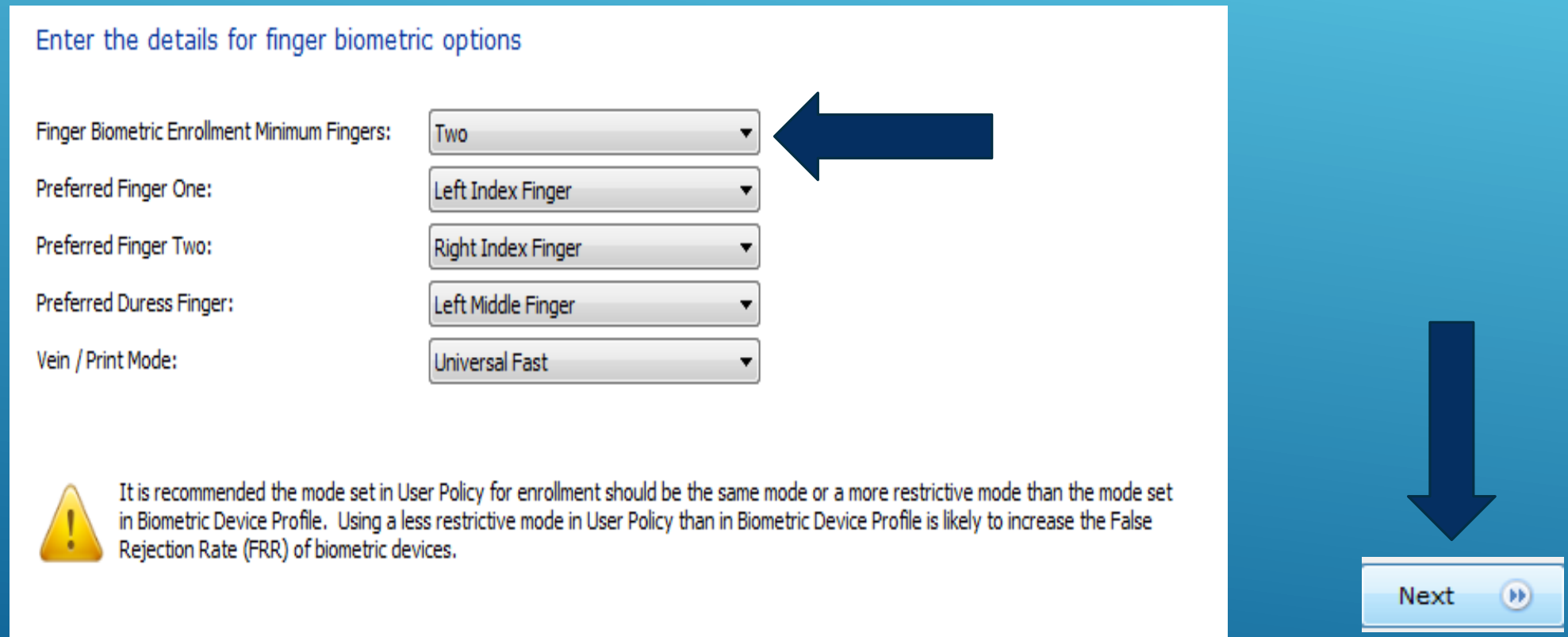
CREATE A NEW USER POLICY



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

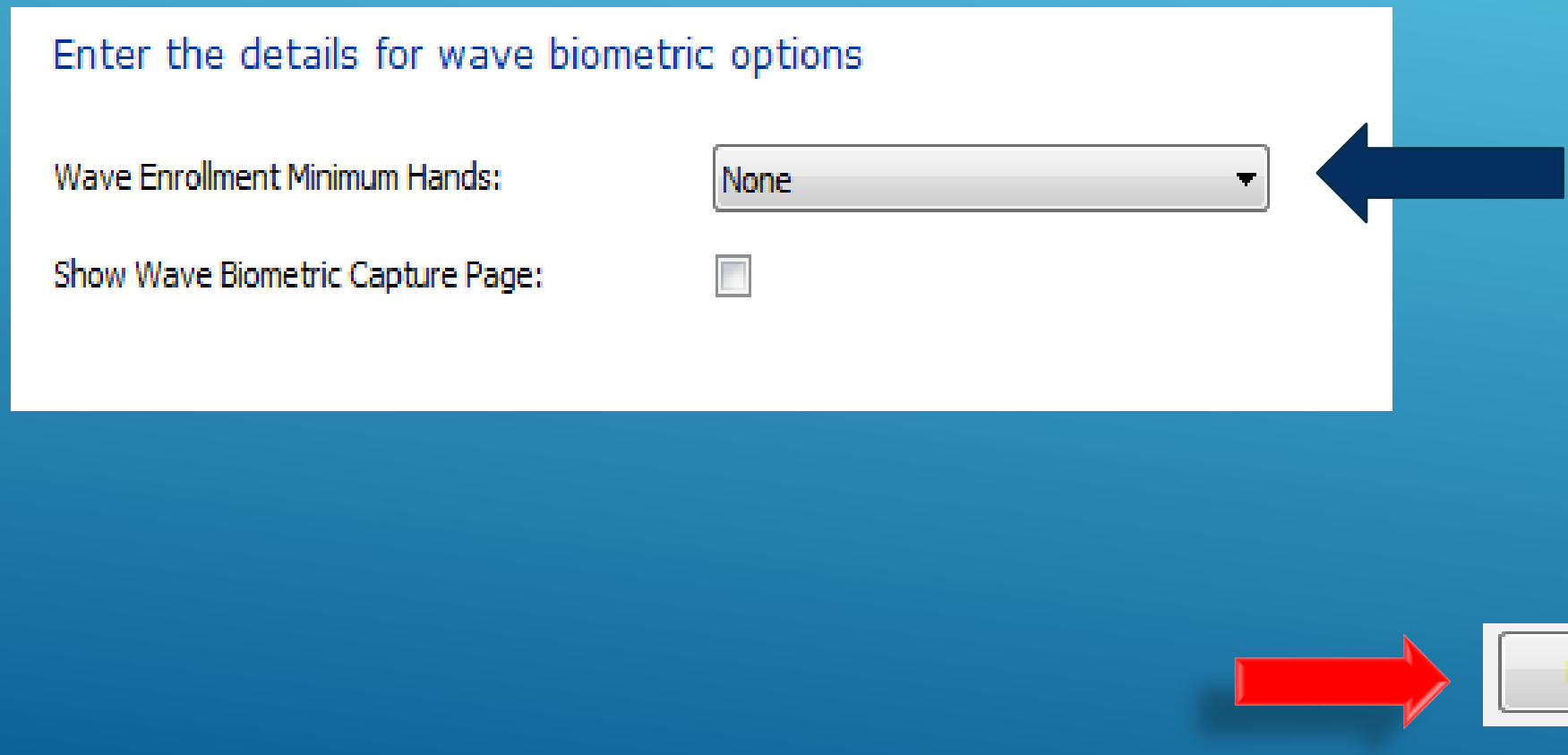
USER POLICY

CLICK TWO FOR FINGER BIOMETRICS



USER POLICY

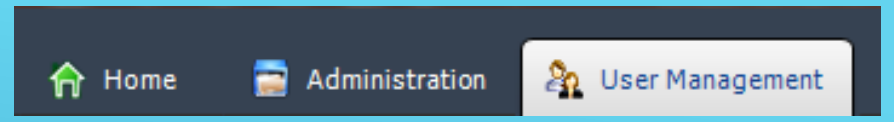
NONE FOR WAVE ENROLLMENTS



ENROLLMENT PROCESS

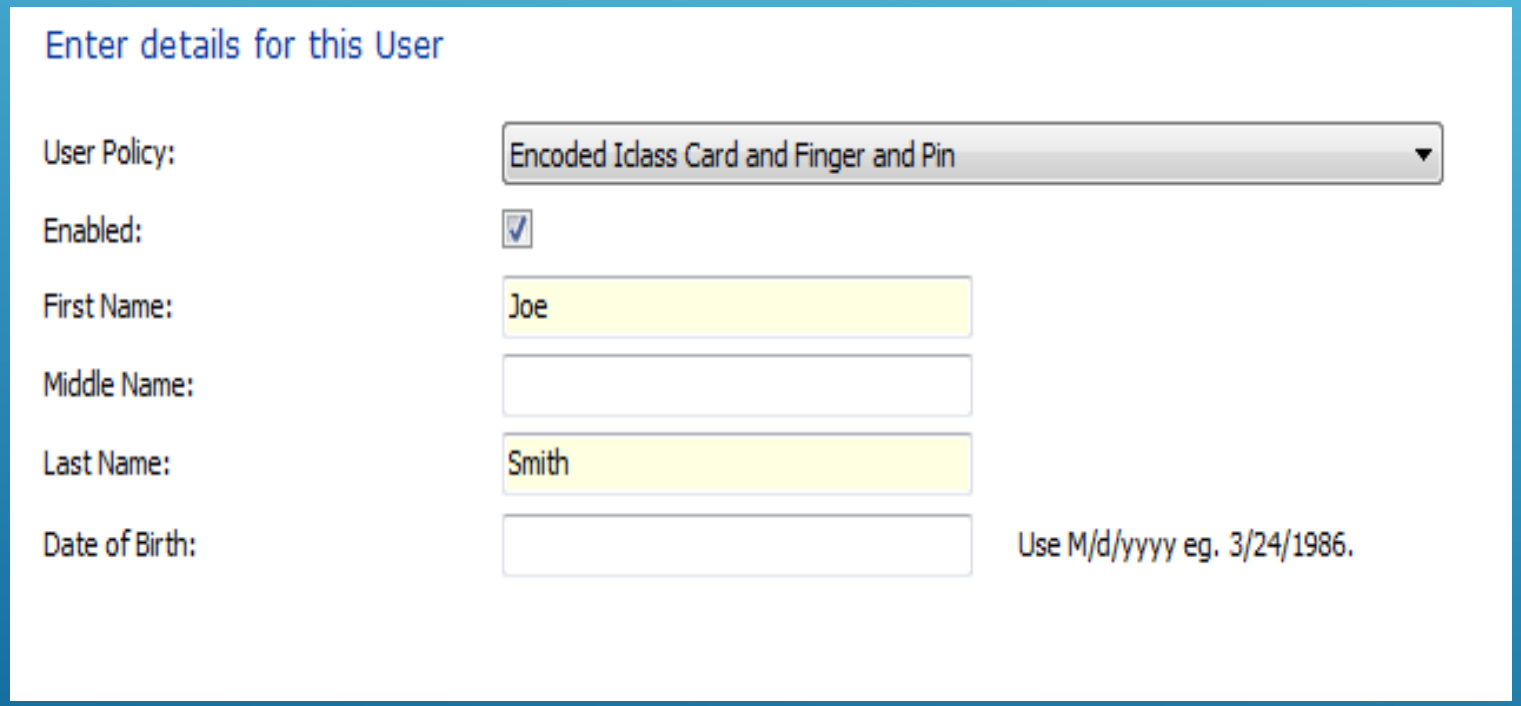
USER MANAGEMENT

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

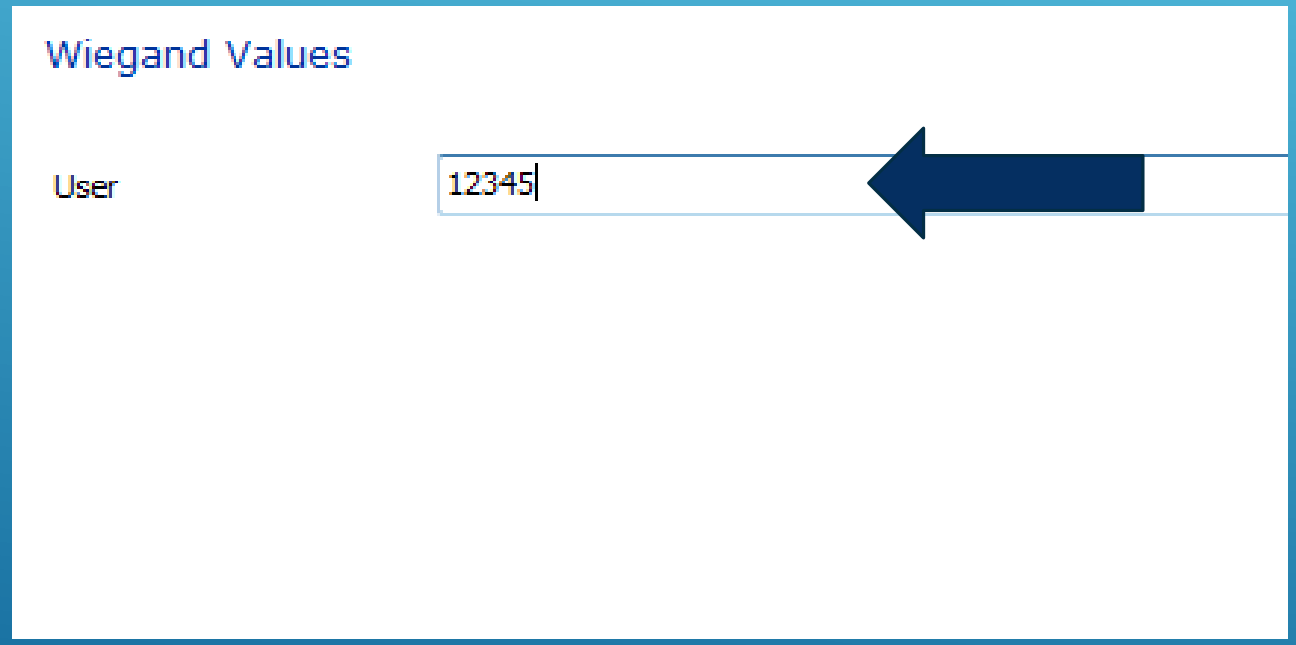
CREATE A NEW USER WITH THE USER POLICY CREATED EARLIER



USER POLICY ENCODED ICLASS CARD AND FINGER AND PIN

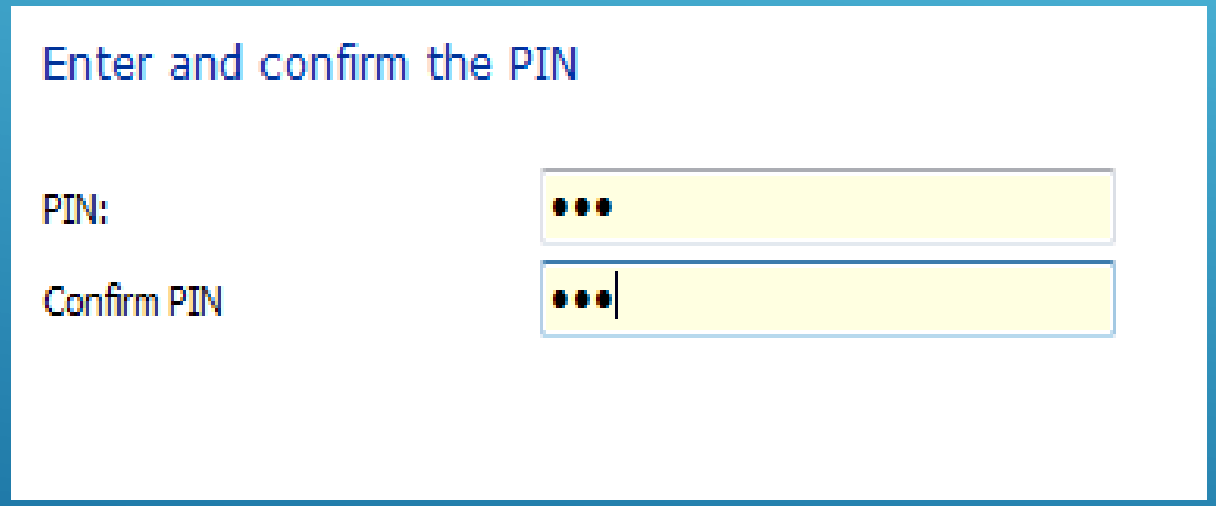
USER MANAGEMENT

MANUALLY TYPE IN THE ID NUMBER FOR THIS USER



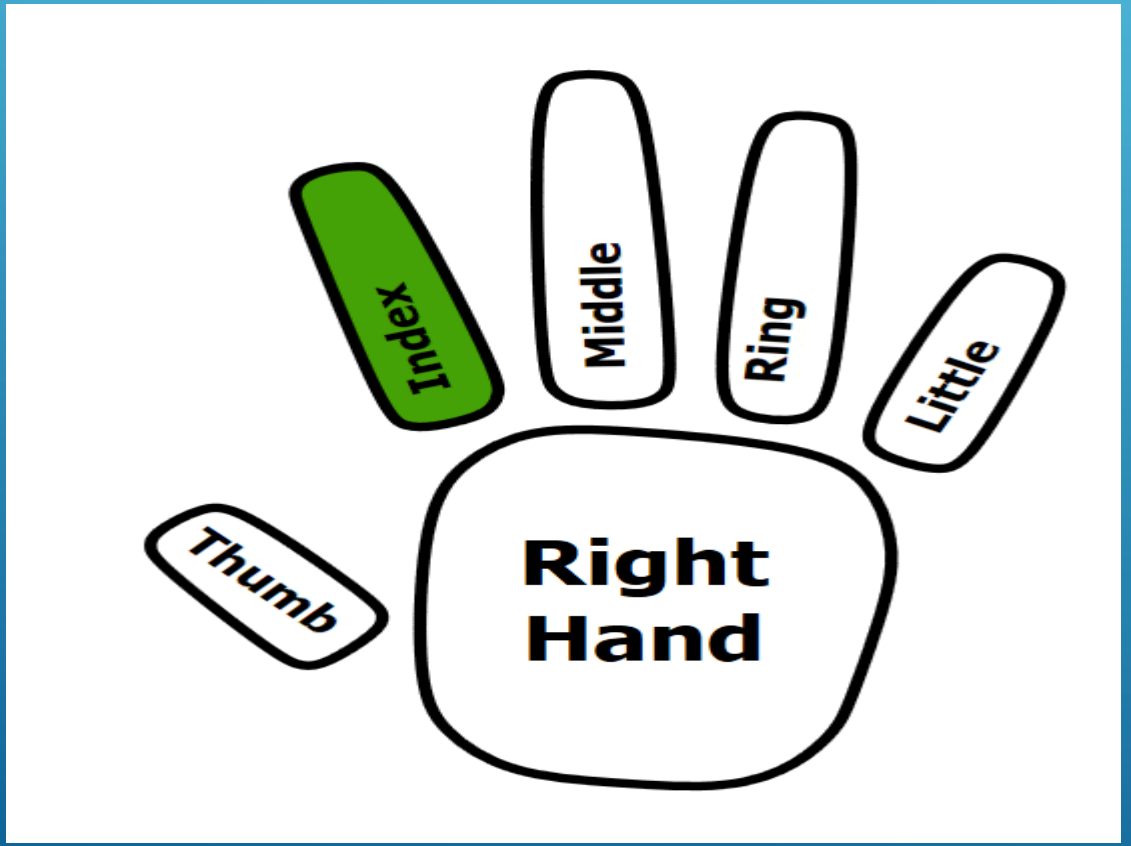
USER MANAGEMENT

PUT IN THE PIN CODE YOU WANT TO USE



USER MANAGEMENT

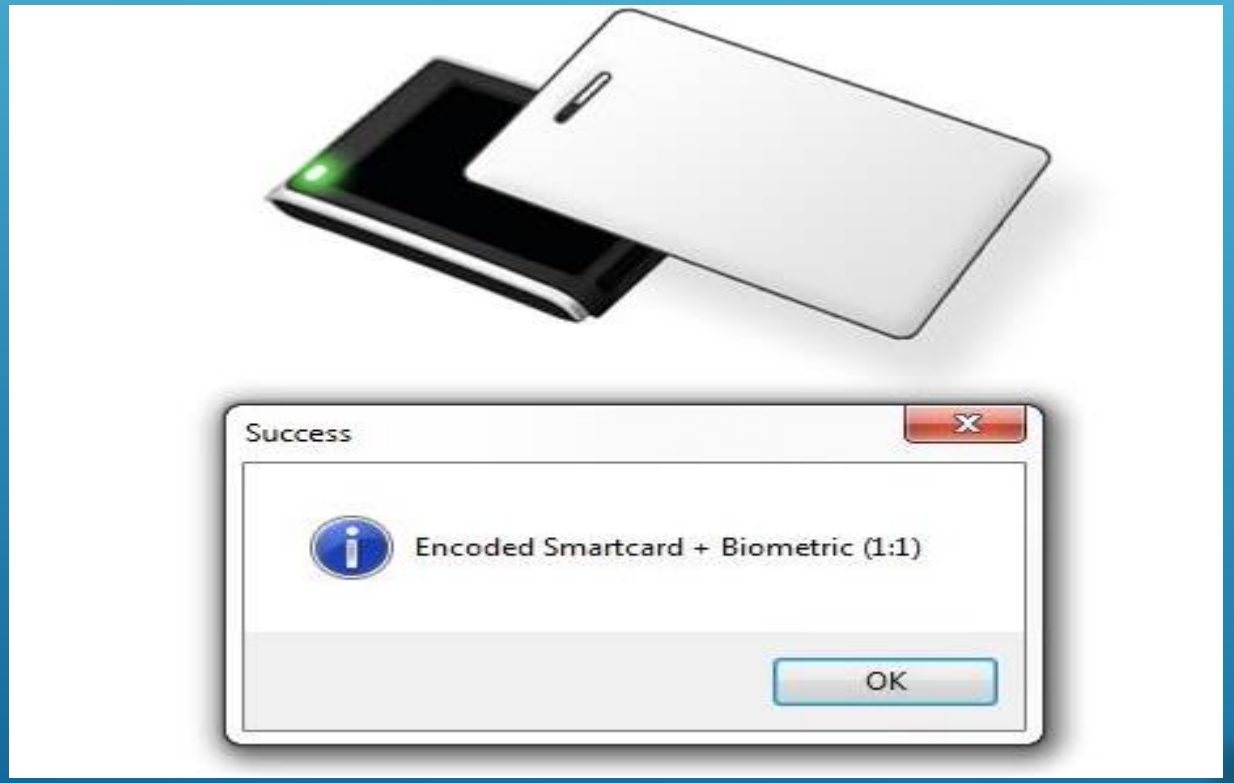
CAPTURE YOUR FINGER PRINTS



Next

USER MANAGEMENT

ENCODE THE CARD



Finish

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