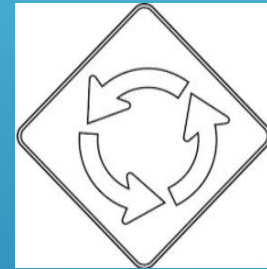


PROX CARD OR FINGER OR KEYPAD FOR SAME USER



TO WORK WITH SIGMA PROX/ SIGMA EXTREME PROX/SIGMA LITE +READERS PROX

ACRONYMS

MWC=MORPHO WAVE COMPACT

UP=USER POLICY

BDP=BIOMETRIC DEVICE PROFILE

MM=MORPHO MANAGER

ACP=ACCESS CONTROL PANEL

CSN=CARD SERIAL NUMBER

MORPHOMANAGER DEFAULT LOG IN

USERNAME-ADMINISTRATOR

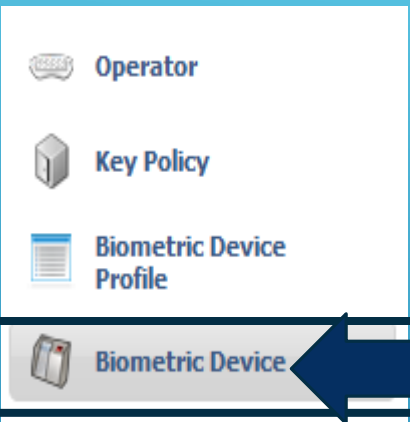
PASSWORD-PASSWORD

ADD AN BIOMETRIC DEVICE

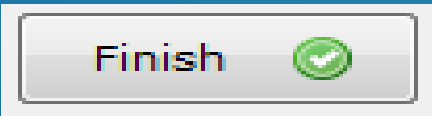
Administration>Biometric Device

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



Items	Editing Biometric Device
Operator	Enter the details for this Biometric Device
Key Policy	Name: <input type="text" value="Sigma Prox"/>
Biometric Device Profile	Description: <input type="text"/>
Biometric Device	Location: <input type="text"/>
Wiegand Profiles	Asset ID: <input type="text"/>
User Policy	Export Value: <input type="text"/>
Access Schedules	Time Zone: <input type="text" value="(UTC-08:00) Pacific Time (US & Canada)"/>
User Distribution Group	Hardware Family: <input type="text" value="MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme"/>
User Authentication Mode	Serial Number: <input type="text"/>
Operator Role	Hostname\IP Address: <input type="text" value="192.168.1.20"/>
Notifications	Port: <input type="text" value="11010"/>
Clients	Biometric Device Profile: <input type="text" value="Default"/>
Scheduled Reports	Include in Time & Attendance Exports: <input type="checkbox"/>
	Change User Onsite / Offsite Status: <input type="checkbox"/>
	Onsite Key: <input type="text" value="No Key"/>
	Offsite Key: <input type="text" value="No Key"/>



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 until you get to 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:

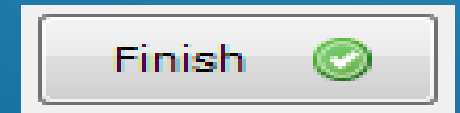
Keys

Key Policy:

DROP DOWN
SELECTED
MORPHOACCESS

SEARCH FOR THE
READER

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



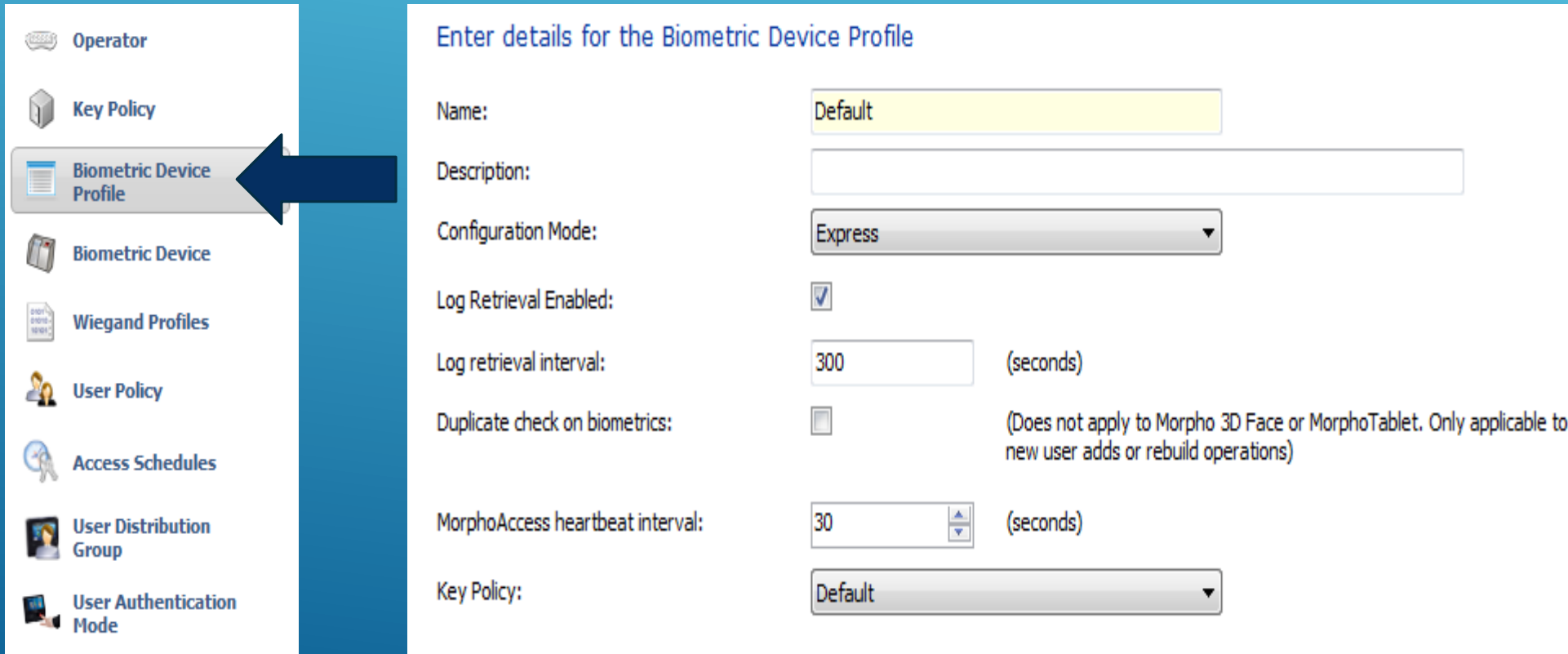
BIOMETRIC DEVICE PROFILE

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: Default

Description:

Configuration Mode: Express

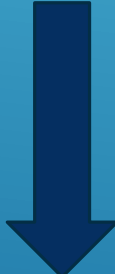
Log Retrieval Enabled:

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



Next



BIOMETRIC DEVICE PROFILE

Biometric Device Settings

General Settings

Wiegand Profile:

Language:

Realtime logging enabled:



Biometric Threshold Settings

Biometric Threshold:

MorphoAccess Vein Print Mode:

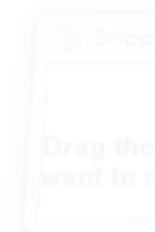
MorphoAccess Fingerprint Threshold:


Morpho 3D Face Identification Threshold:

Morpho 3D Face Verification Threshold:



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 

THE WIEGAND PROFILE IS THE CARD FORMAT

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, VisionPass, and Mor

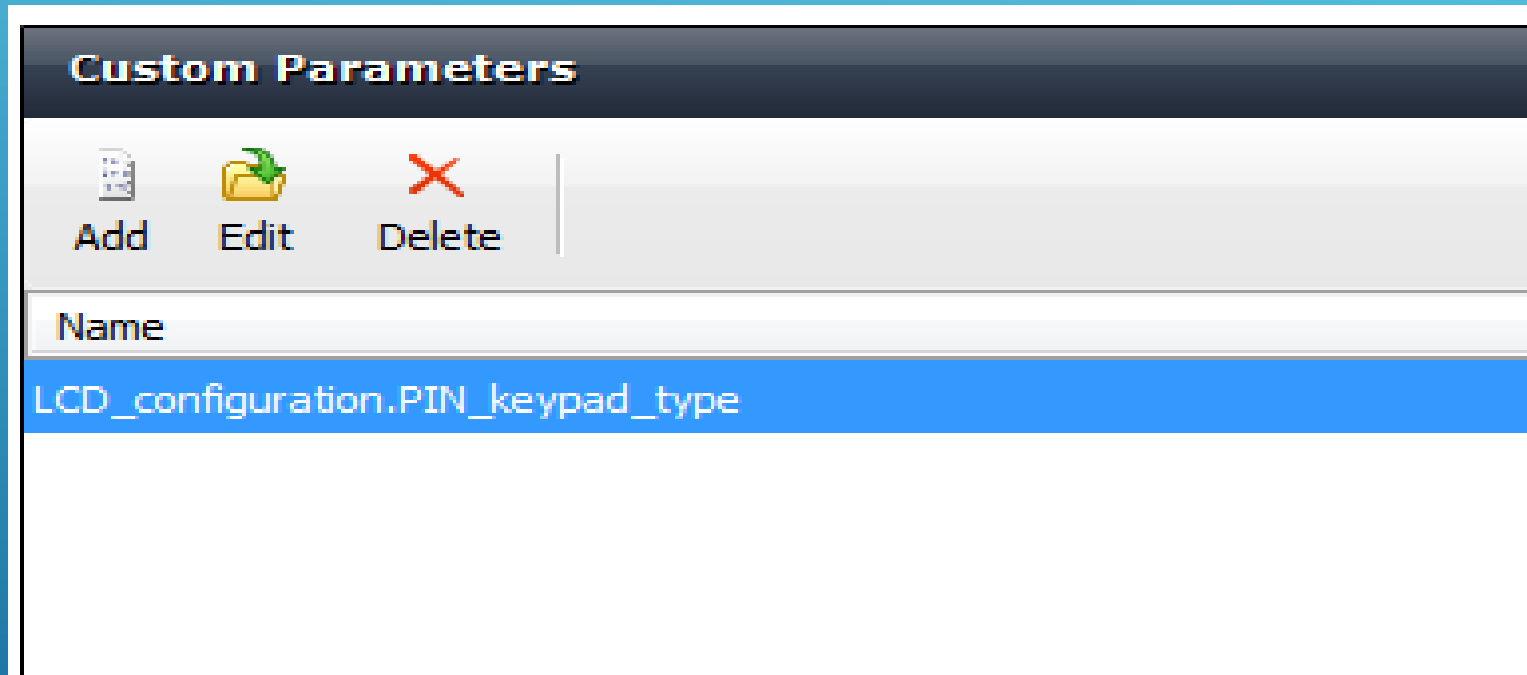
Biometric:	<input checked="" type="checkbox"/>	←	<input type="checkbox"/>
Proximity Card:	<input checked="" type="checkbox"/>	←	ES: <input type="checkbox"/>
Wiegand In:	<input type="checkbox"/>	Mifare DESFire AES:	<input type="checkbox"/>
Clock and Data In:	<input type="checkbox"/>	Keypad:	<input checked="" type="checkbox"/> ←
HID iClass:	<input type="checkbox"/>		
HID iClass SEOS:	<input type="checkbox"/>		

Click next several times till you get to Custom Parameters



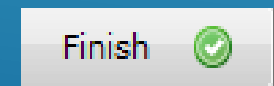
SET THE MULTI-FACTOR MODE SETTINGS AS EXACTLY AS SHOWN

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(s)



Create new User Authentication Mode(s)

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:

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,

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: ←

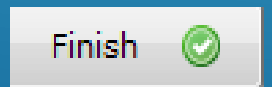
Allow Start By Wiegand In:

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

Home Administration

Items

- 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: Prox card OR Finger OR Keypad

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: Prox card OR Finger OR Keypad

Show Photo Capture Page:



**WIEGAND PROFILE; SELECT THE WIEGAND PROFILE YOU WISH TO USE THE FOR USERS
USER AUTHENTICATION MODE: USE THE ONE YOU CREATED EARLIER**

USER POLICY

CLICK TWO FOR FINGER BIOMETRICS


Enter the details for finger biometric options

Finger Biometric Enrollment Minimum Fingers:	<input type="text" value="Two"/>
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:

Prox card OR Finger OR Keypad

Enabled:

First Name:

Joe

Middle Name:

Last Name:

Smith

Date of Birth:

Use M/d/yyyy eg. 3/24/1986.



POLICY :PROX CARD OR FINGER OR KEYPAD



Next

USER MANAGEMENT

MANUALLY TYPE IN THE PROX CARD NUMBER

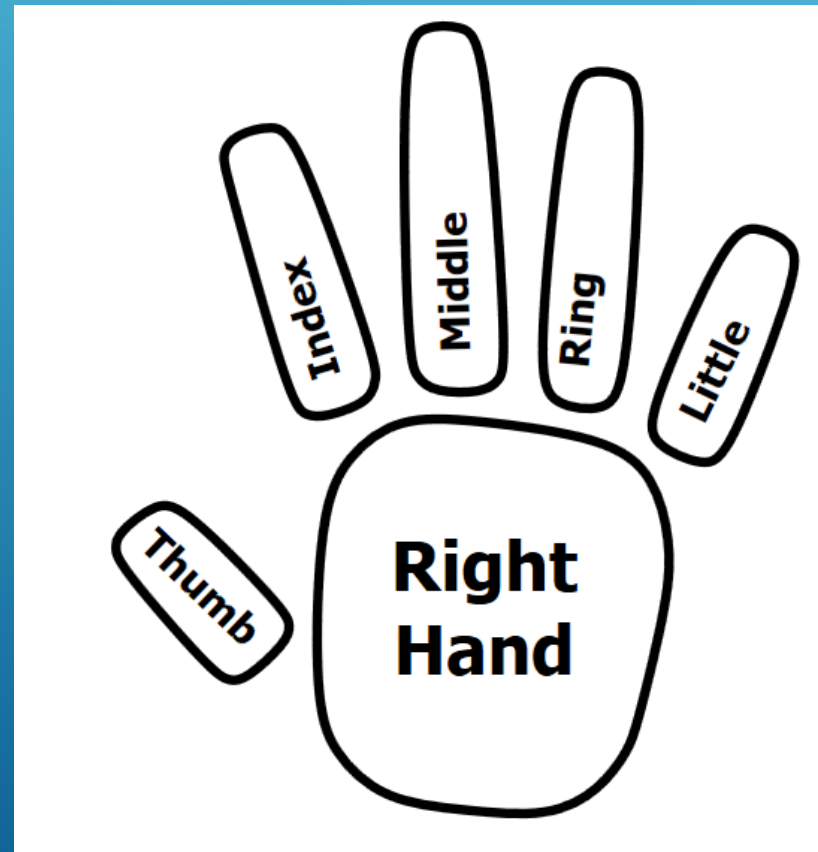
Wiegand Values


User



USER MANAGEMENT

CAPTURE YOUR FINGER PRINTS



Finish 

FINAL RESOLUTION

BDP NEEDS TO BE CONFIGURED FOR KEYPAD OR PROX OR FINGERPRINT

UDP NEEDS TO BE CREATED AND ATTACH TO THE USER POLICY

ONE USER POLICY NEED TO BE CREATED FOR PROX CARD OR FINGER AND OR KEYPAD

THE SIGMA READER READS THE PROX CARD NUMBER WHICH IS ASSOCIATED WITH A USER

THE KEYPAD NUMBER WILL BE THE PROX CARD NUMBER

THE FINGER PRINT WILL BE THE PROX CARD

THE USER HAS THE OPTIONS TO PLACE THERE PROX CARD OR FINGER OR
TYPE IN THE KEYPAD (PROX CARD NUMBER)

WEBSITE

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