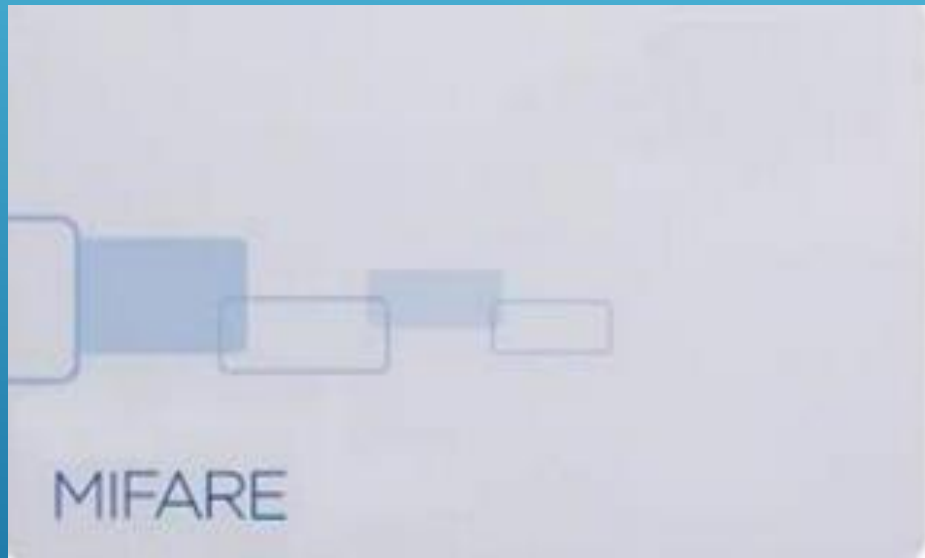


ENCODED MIFARE CARDS AND PIN



and



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

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

 Operator

 Key Policy

 Biometric Device Profile

 Biometric Device

Enter the details for this Biometric Device

Name:

Description:

Location:

Asset ID:

Export Value:

Time Zone:

Hardware Family:

Serial Number:

Hostname \IP Address:

Port:

Biometric Device Profile:

Include in Time & Attendance Exports:

Change User Onsite / Offsite Status:

Onsite Key:

Offsite Key:



Finish



CLIENTS



Path Administration>Clients

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

TO READ THE MIFARE CSN YOU REQUIRE
A OMNIKEY **OR** A SIGMA/SIGMA LITE
MULTI



SIGMA MULTI



USB OMNIKEY 5022

ADD YOUR SIGMA OR OMNIKEY 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

SEARCH FOR YOUR OMNIKEY UNDER SMARTCARD ENCODING

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:

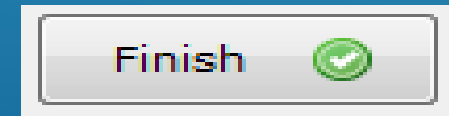
Morpho Smartcard encoding PC/SC device:

Morpho Smartcard encoding MorphoAccess:

Keys

Key Policy:

***IF USING A OMNIKEY**



SEARCH FOR YOUR SIGMA UNDER SMARTCARD ENCODING

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:

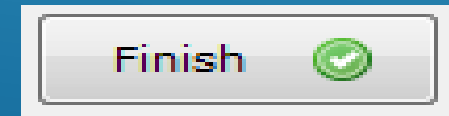
Keys

Key Policy:

DROP DOWN
SELECTED
MORPHOACCESS

SEARCH FOR THE
READER

*IF USING A SIGMA



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:

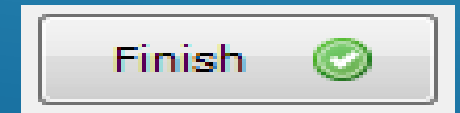
DROP DOWN
SELECTED
MORPHOACCESS



SEARCH FOR THE
READER



****IF YOU 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:

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 MUST WHAT IS REQUESTED BY 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:

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

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



Finish



SET THE MULTI-FACTOR MODE SETTINGS AS EXACTLY AS SHOWN

USER AUTHENTICATION MODE

Path Administration>User Authentication Mode(s)



User Authentication
Mode

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 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 Sigma VP, MorphoWave Settings

Mode: ←

Download Identifier To Device:

Encode To Smartcard Mode: ←

Template Location:

Pin Location: ←

Allow Start By Biometric:

Allow Start By Contactless Card: ←

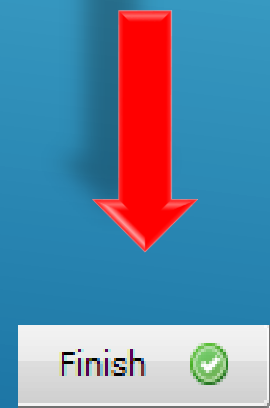
Allow Start By Keyboard:


Allow Start By Wiegand In:

Require Pin: ←

Require Template Match:

FOLLOW THIS SETTINGS EXACTLY AS SHOWN



Finish 

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: Encode 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: Encoded card and Pin

Show Photo Capture Page:

Next

**WIEGAND PROFILE; SELECT THE WIEGAND PROFILE YOU WISH TO USE FOR USERS IN THIS USER POLICY.
USER AUTHENTICATION MODE; IS THE ONE YOUR CREATED EARLIER**

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 



POLICY ENCODE CARD AND PIN

USER MANAGEMENT

ADD YOUR USER ID WIEGAND VALUE THAT WILL
BE ASSOCIATED WITH THIS USER

Wiegand Values

User

123



Next



USER MANAGEMENT

PUT IN YOUR PIN CODE

Enter and confirm the PIN

PIN:

Confirm PIN

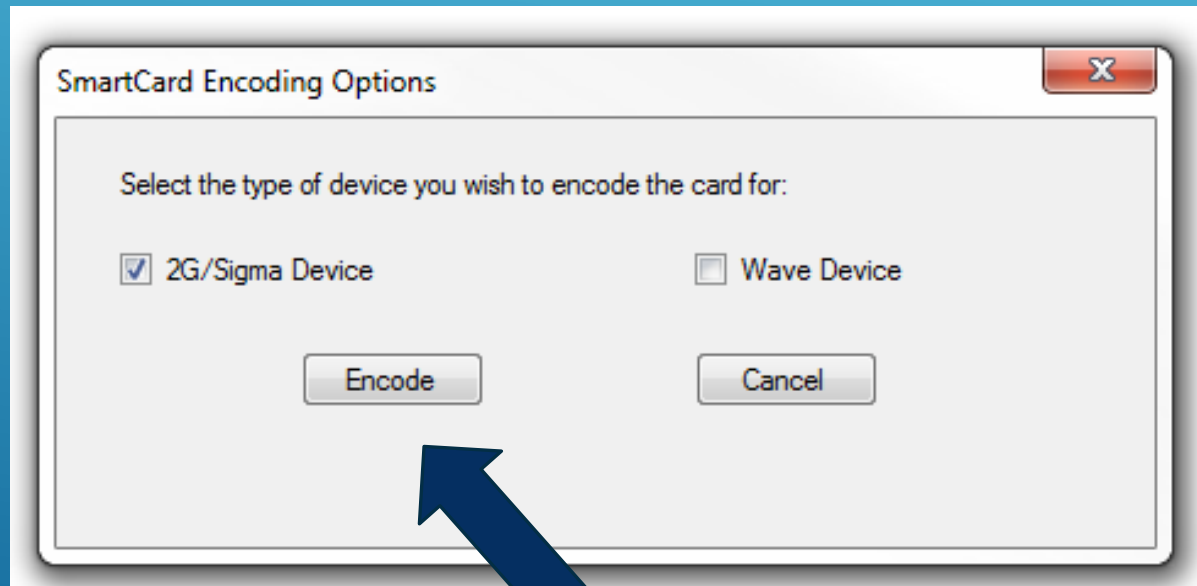


Finish



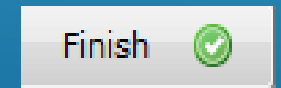
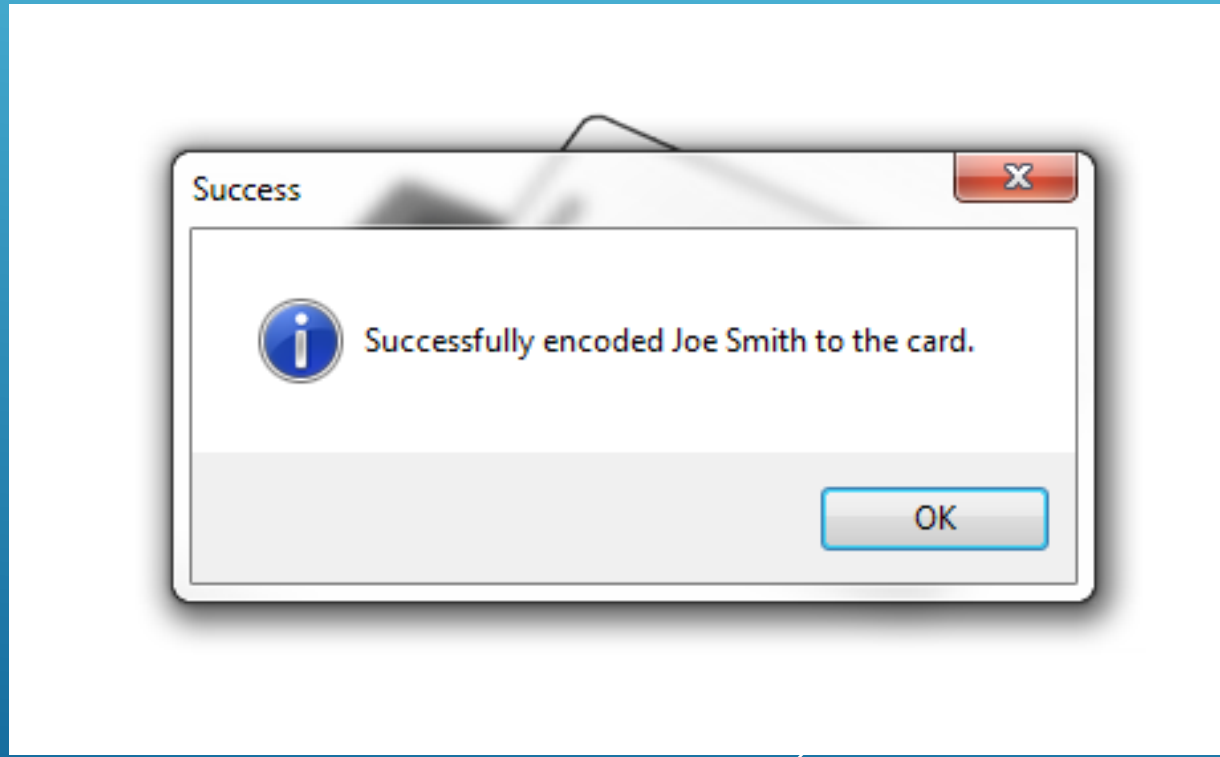
USER MANAGEMENT

ENCODE YOUR CARD



USER MANAGEMENT

FINISHED



FINAL RESOLUTION

ONE USER AUTHENTICATION MODE NEEDS TO BE CREATED

ONE USER POLICY NEED TO BE CREATED

USER POLICY IS ASSOCIATED WITH USER AUTHENTICATION MODE

ONE USER FOR ENCODE CARD AND PIN

ALL THE INFORMATION IS STORE ON THE MIFARE CARD ID AND PIN CODE

WEBSITE

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