

# CSN OF MIFARE CARDS OR FINGER

## CSN FOR VISITORS



TO WORK WITH MULTI SIGMA/ SIGMA LITE READERS

# THIS IS A ADVANCE CONFIGURATION WITH MORPHO MANAGER

**THE GOAL IS TO HAVE ONE SET OF USERS FOR MIFARE CSN OR FINGER  
SECOND SET OF USERS TO BE MIFARE CSN (NO FINGERPRINTS)**

# 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:

Mifare reader

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

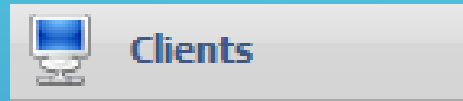
Offsite Key:

No Key

Finish



# CLIENTS



Path Administration>Clients

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

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



**SIGMA MULTI**



**USB OMNIKEY 5427 CK OR G2**



# 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:

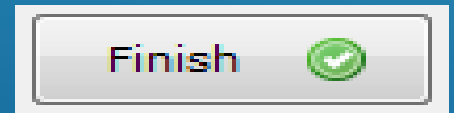
Morpho Smartcard encoding PC/SC device:

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:

**Annotations:**

- Blue arrow pointing to the "Selected MorphoAccess" dropdown: DROP DOWN SELECTED MORPHOACCESS
- Blue arrow pointing to the "Search" button below "Morpho Smartcard encoding 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:

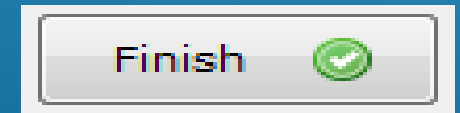
**Keys**

Key Policy:

DROP DOWN  
SELECTED  
MORPHOACCESS

SEARCH FOR THE  
READER

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



# BIOMETRIC DEVICE PROFILE



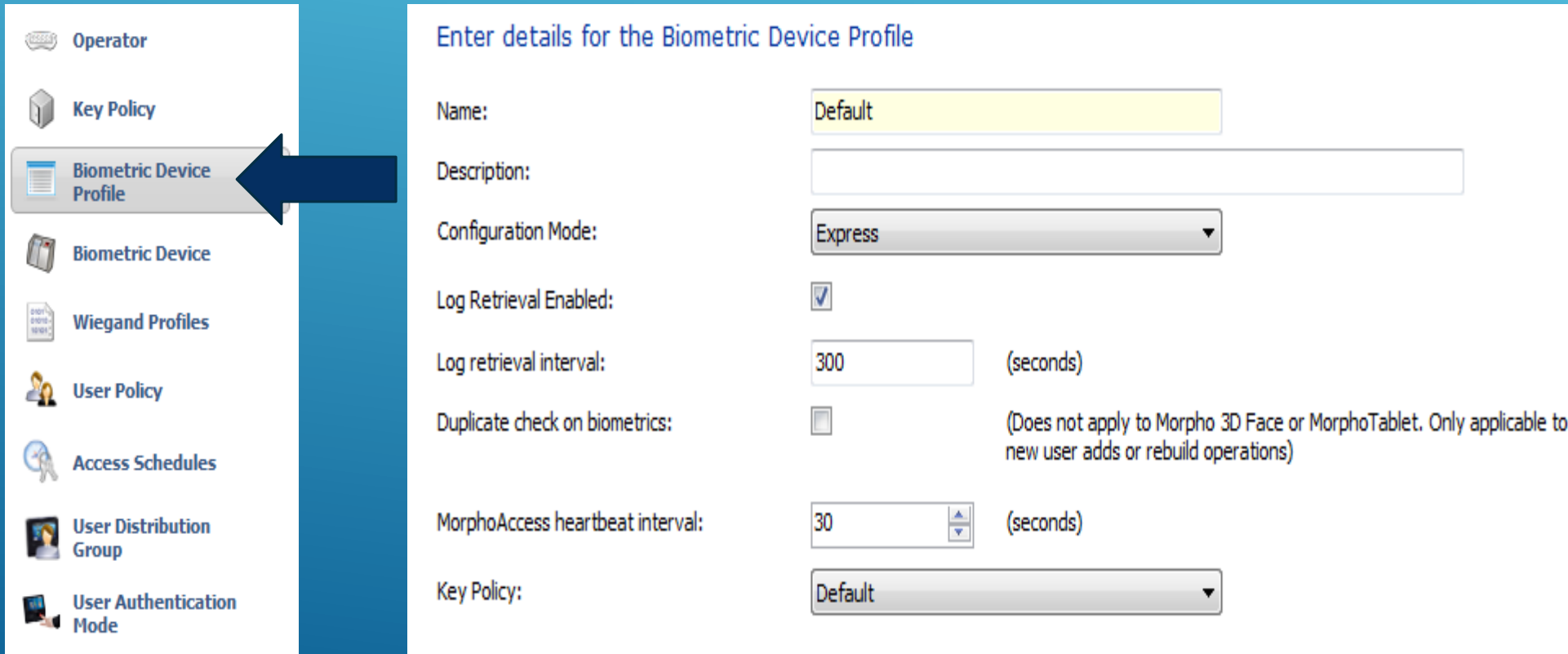
Biometric Device  
Profile

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:

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:



Next 

**THE WIEGAND PROFILE MUST BE SET TO WHATEVER THE MIFARE CARD FORMAT IS**

# 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 checked="" 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"/>		

→



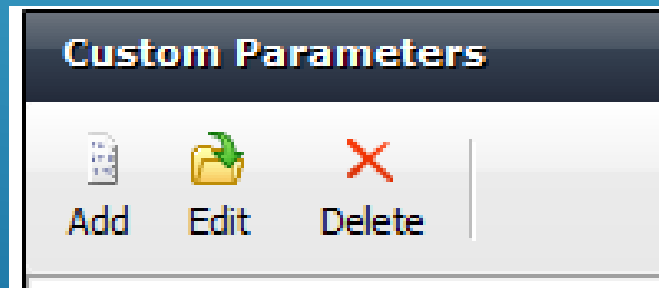
Next 

**SET THE MULTI-FACTOR MODE SETTINGS AS EXACTLY AS SHOWN**

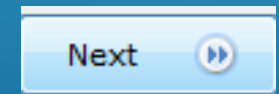
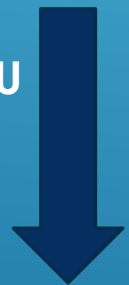


# BIOMETRIC DEVICE PROFILE

THERE IS NO CHANGES NEED TO TAKE PLACE IN THE BDP EXCEPT FOR CUSTOM PARAMETERS.



HIT NEXT SEVERAL TIMES TILL YOU GET TO CUSTOM PARAMETERS



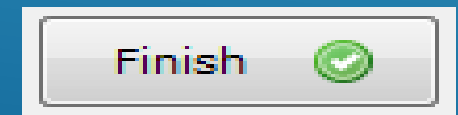
# BIOMETRIC DEVICE PROFILE

Custom Parameters	
Name	Value
ucc.per_user_rules	2
ucc.user_record_reference	1

**ADD ONE PARAMETERS THIS IS CASE SENSITIVE\*\*\***

ucc.per\_user\_rules VALUE OF 2

ucc.user\_record\_reference VALUE OF 1



THE NEXT STEPS IS TO CREATE TWO  
UAM AND TWO UP'S

THE **USER POLICY** DICTATES ON HOW  
THE USER WILL BE VERIFIED BUT A **USER  
AUTHENTICATION MODE** NEEDS TO BE  
CREATED FIRST FOR THAT POLICY

# USER AUTHENTICATION MODE

Path Administration>User Authentication Mode(s)

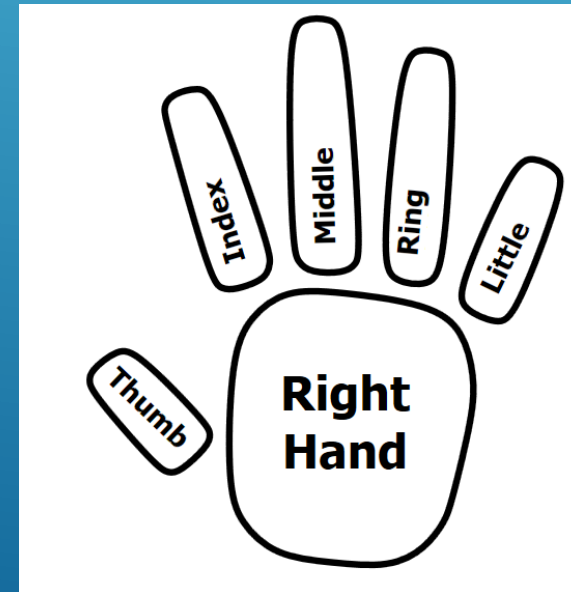
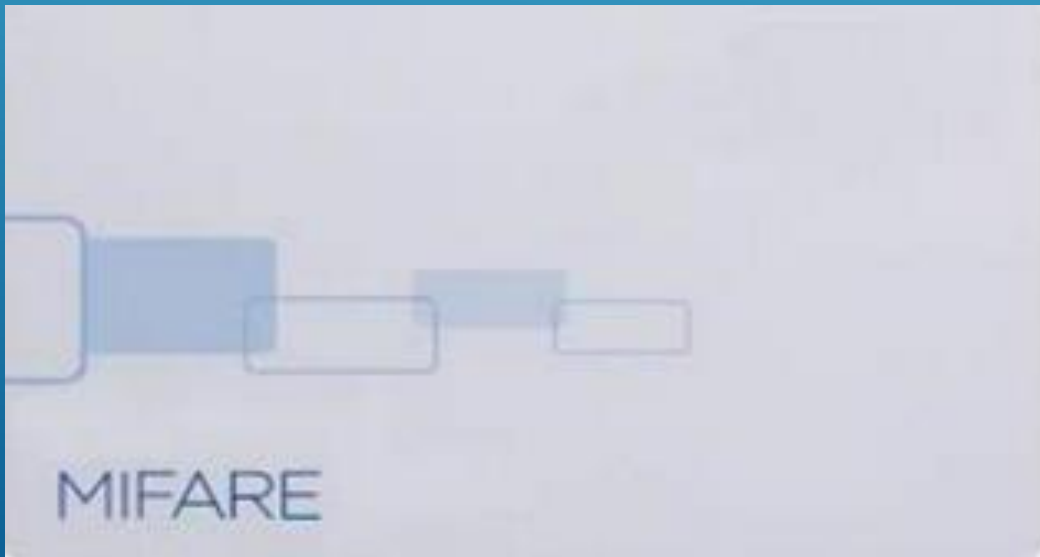


Create new User Authentication Mode(s)

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 1

## UAM FOR MIFARE CSN OR FINGER



# USER AUTHENTICATION MODE 1

- 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 1

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:



Finish

**FOLLOW THIS SETTINGS EXACTLY AS SHOWN**

FINISH



# USER POLICY



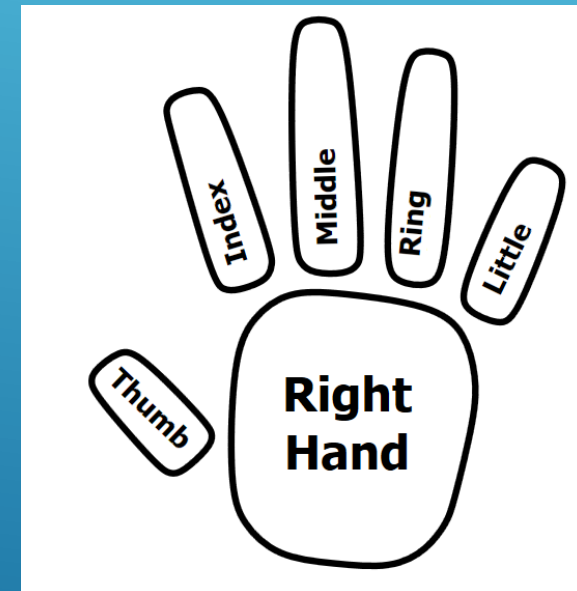
Path Administration>User Policy

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 1

MIFARE CSN OR FINGER



# USER POLICY 1

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: Mifare CSN OR Finger

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: ISO/IEC 14443 CSN 32 bit

User Authentication Mode: Mifare CSN or Finger

Show Photo Capture Page:

Next

WIEGAND PROFILE WILL BE YOUR MIFARE CARD FORMAT  
USER AUTHENTICATION MODE IS THE ONE YOUR CREATED EARLIER

# USER POLICY 1

CLICK TWO FOR FINGER BIOMETRICS

Enter the details for finger biometric options

Finger Biometric Enrollment Minimum Fingers:

Two

Preferred Finger One:

Left Index Finger

Preferred Finger Two:

Right Index Finger

Preferred Duress Finger:

Left Middle Finger


Vein / Print Mode:

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 1

## NONE FOR WAVE ENROLLMENTS

Enter the details for wave biometric options

Wave Enrollment Minimum Hands:

None

Show Wave Biometric Capture Page:



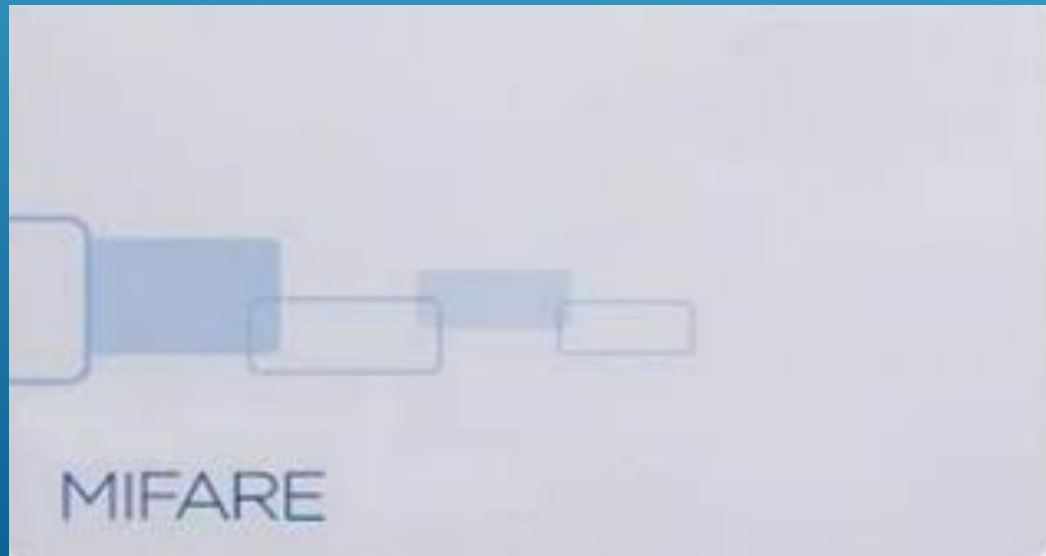
Finish



FINISH

# USER AUTHENTICATION MODE 2

## UAM FOR MIFARE CSN



# USER AUTHENTICATION MODE 2

- 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 2

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:

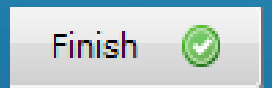
Allow Start By Wiegand In:

Require Pin:

Require Template Match:



**FOLLOW THIS SETTINGS EXACTLY AS SHOWN**



FINISH

# USER POLICY 2

MIFARE CSN ONLY



# USER POLICY 2

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: Mifare CSN

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: ISO/IEC 14443 CSN 32 bit

User Authentication Mode: Mifare CSN

Show Photo Capture Page:

Next

**WIEGAND PROFILE WILL BE YOUR MIFARE CARD FORMAT  
USER AUTHENTICATION MODE IS THE ONE YOUR CREATED EARLIER**

# USER POLICY 2

CLICK NONE FOR FINGER BIOMETRICS


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 2

## NONE FOR WAVE ENROLLMENTS

Enter the details for wave biometric options

Wave Enrollment Minimum Hands:

None

Show Wave Biometric Capture Page:



Finish



FINISH

# ENROLLMENT PROCESS

## USER MANAGEMENT

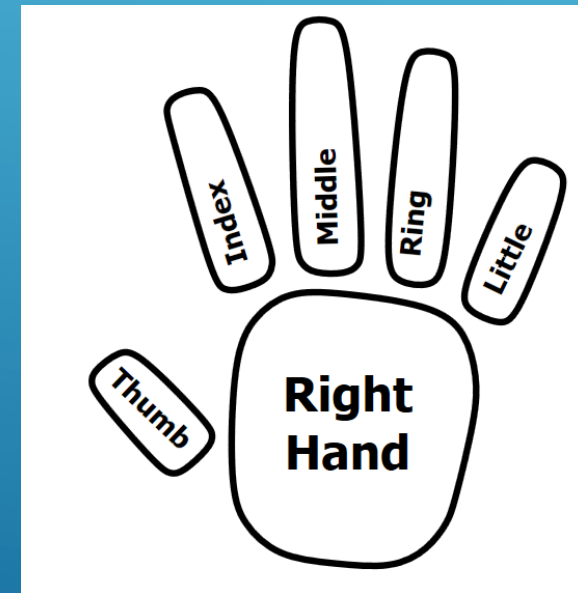
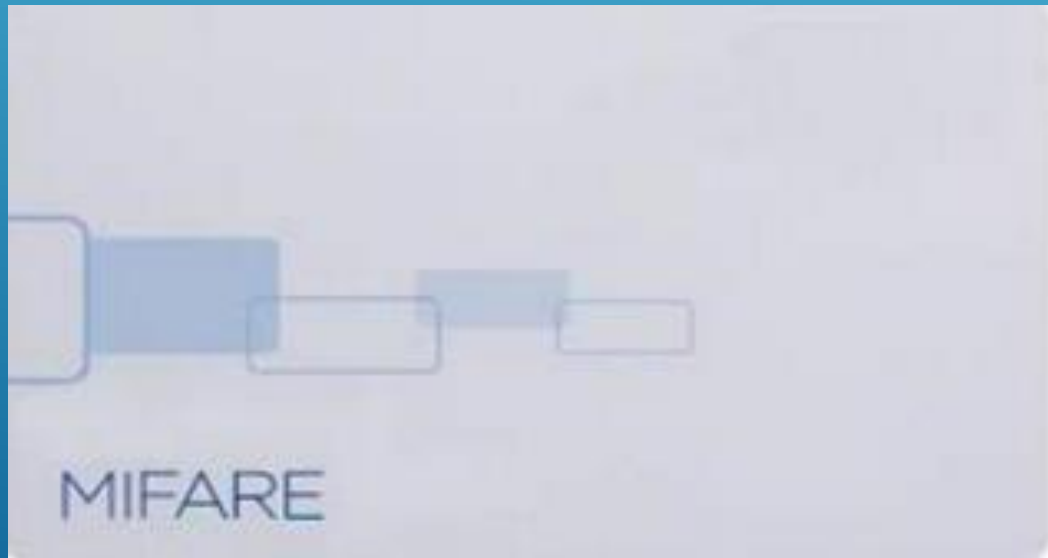


User Management

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.



# POLICY 1 MIFARE CSN OR FINGER



# USER MANAGEMENT

CREATE A NEW USER WITH THE USER POLICY CREATED EARLIER

**Adding User**

Enter details for this User

User Policy:

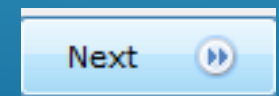
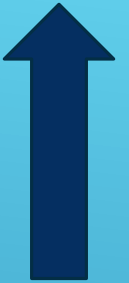
Enabled:

First Name:

Middle Name:

Last Name:

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



POLICY 1 MIFARE CSN OR FINGER


# USER MANAGEMENT

READ THE CSN BY USING EITHER A SIGMA OR OMNIKEY

Wiegand Values

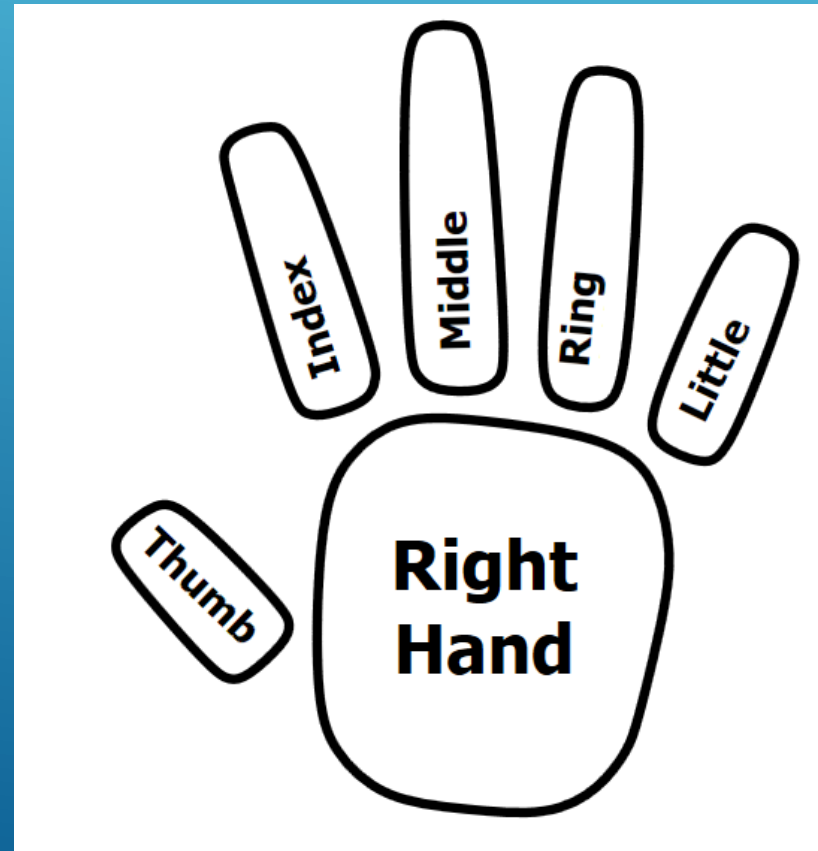
Card Serial Number




Next 

# USER MANAGEMENT

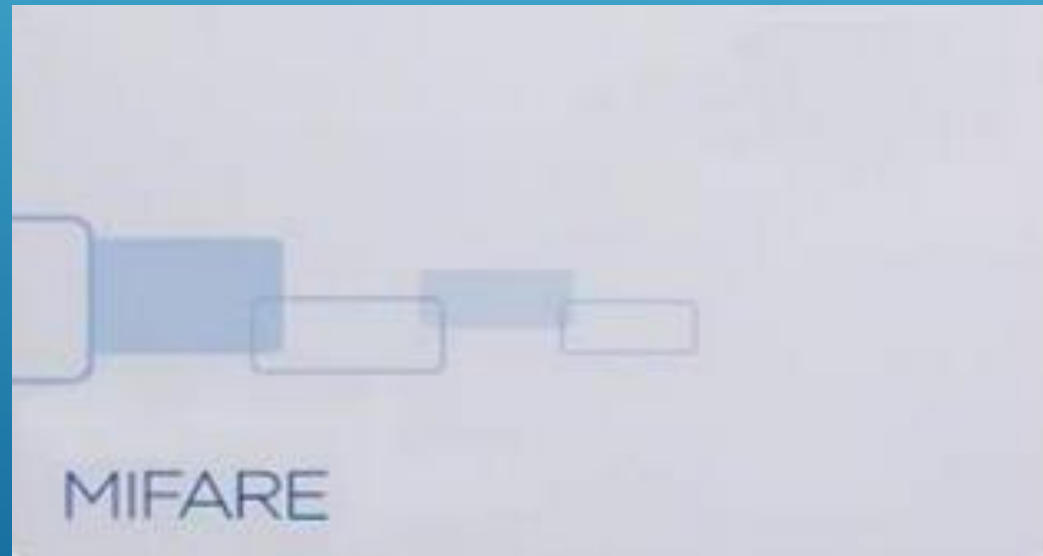
CAPTURE YOUR HAND PRINTS



Finish 

FINISH

# POLICY 2 MIFARE CSN



# USER MANAGEMENT

CREATE A NEW USER WITH THE USER POLICY CREATED EARLIER

Enter details for this User

User Policy: Mifare CSN

Enabled:

First Name: Joe

Middle Name:

Last Name: Smith

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

Next


POLICY 2 MIFARE CSN


# USER MANAGEMENT

READ THE CSN BY USING EITHER A SIGMA OR OMNIKEY

Wiegand Values

Card Serial Number



Finish 



FINISH

# FINAL RESOLUTION

TWO USER AUTHENTICATION NEED TO BE CREATED

TWO USER POLICY NEED TO BE CREATED

EACH USER POLICY IS PER USER BASED

ONE USER FOR MIFARE CSN OR FINGER

ONE USER FOR MIFARE CSN

# WEBSITE

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