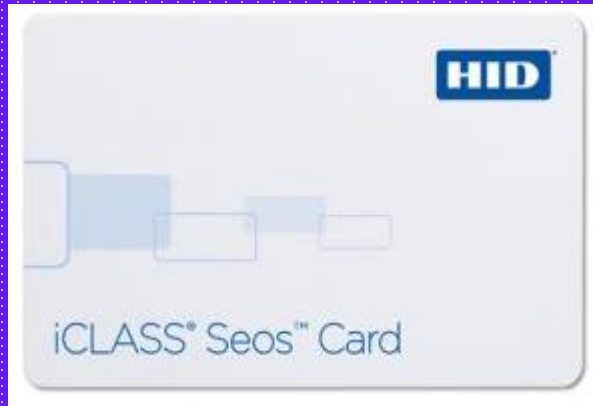


# SEOS Iclass Card and Hand and Pin with the MWC



# STRONGLY ADVICE

IF UNFAMILIAR WITH THE MORPHOWAVE COMPACT?  
PLEASE REVIEW PDF ON SIMPLE SET UP BEFORE HAND

[HTTP://SERVICE.MORPHOTRAK.COM/SUPPORT.HTML](http://service.morphotrak.com/support.html)

**MorphoWave Compact**

MorphoWave Compact Simple set up

# ACRONYMS

MWC=MORPHO WAVE COMPACT

UP=USER POLICY

UAM=USER AUTHENTICATION MODE

BDP=BIOMETRIC DEVICE PROFILE

MM=MORPHO MANAGER

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 MWC AS THE EXAMPLE BELOW

Home Administration User Management Biometric Identification Access Logs Reports

Items

- Operator
- Key Policy
- Biometric Device Profile
- Biometric Device**
- Wiegand Profiles
- User Policy
- Access Schedules
- User Distribution Group
- User Authentication Mode
- Operator Role
- Notifications

### Adding Biometric Device

Enter the details for this Biometric Device

Name: Morphowave Compact

Description:

Location:

Asset ID:

Export Value:

Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Hardware Family: MorphoWave Tower, MorphoWave Compact

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

# Add your MWC 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



# Search for your MWC under Contactless Enrollment

**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:  2

Morpho Contactless Finger enrollment MorphoAccess:   ←

**Smartcard Encoding**

Morpho Smartcard encoding:

Morpho Smartcard encoding PC/SC device:  3

Morpho Smartcard encoding MorphoAccess:

**Keys**

Key Policy:

✓

# WIEGAND

Path Administration>Wiegand

This section allows you to view, add, edit & delete Wiegand Profiles in MorphoManager. Wiegand Profiles define what information is output over the Wiegand Out interface of the Morpho Biometric Devices when a user is identified. This is most typically used in conjunction with an Access Control System.

# Wiegand SEOS PACS

Next couple of pages is how to modify a existing format to add SEOS element ( EXAMPLE ONLY)

- Operator
- Key Policy
- Biometric Device Profile
- Biometric Device
- Wiegand Profiles**
- User Policy
- Access Schedules
- User Distribution Group

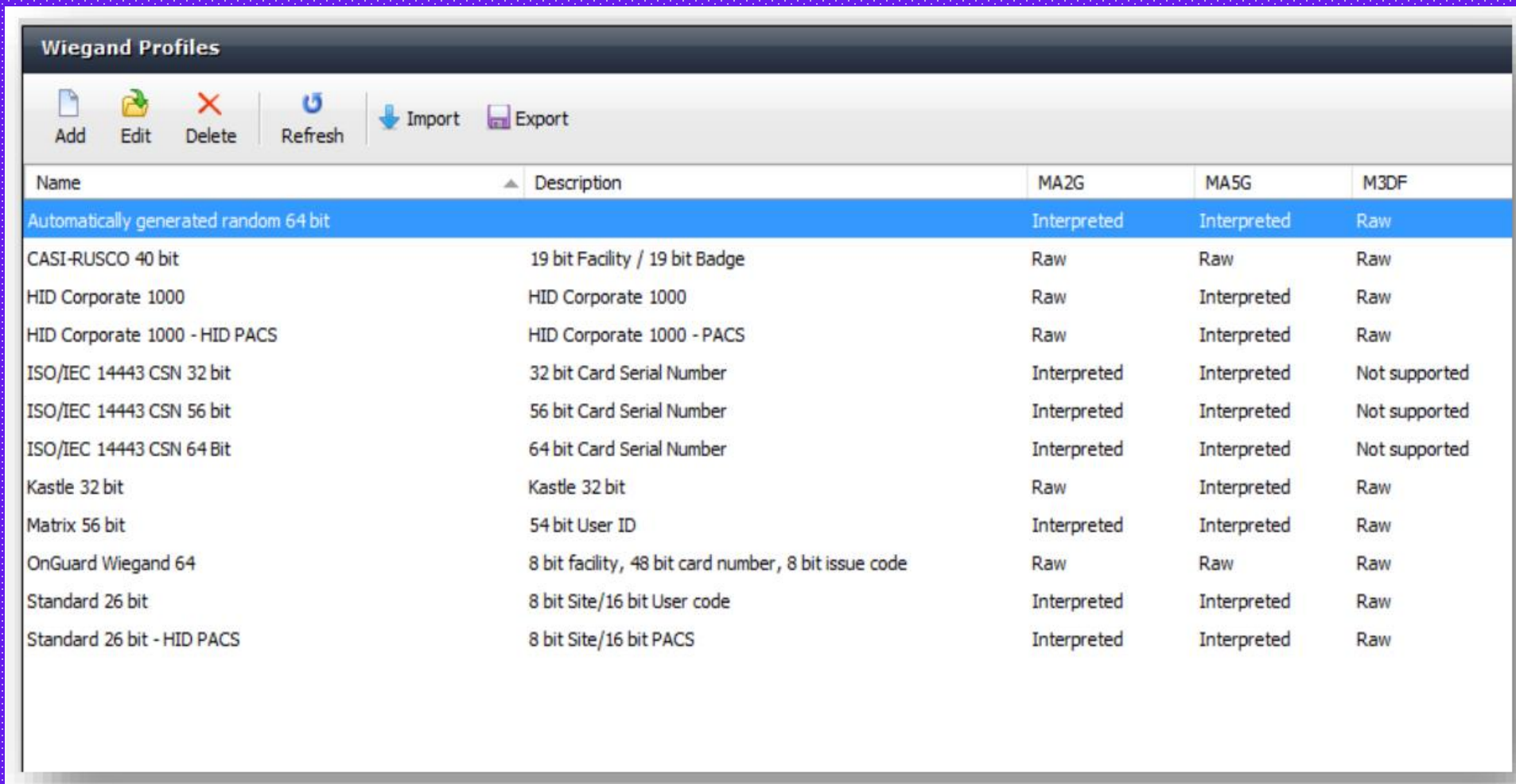
**Wiegand Profiles**

Add Edit Delete Refresh Import Export

Name	Description	MA2G	MA5G	M3DF
Automatically generated random 64 bit		Interpreted	Interpreted	Raw
CASI-RUSCO 40 bit	19 bit Facility / 19 bit Badge	Raw	Raw	Raw
HID Corporate 1000	HID Corporate 1000	Raw	Interpreted	Raw
HID Corporate 1000 - HID PACS	HID Corporate 1000 - PACS	Raw	Interpreted	Raw
ISO/IEC 14443 CSN 32 bit	32 bit Card Serial Number	Interpreted	Interpreted	Not supported
ISO/IEC 14443 CSN 56 bit	56 bit Card Serial Number	Interpreted	Interpreted	Not supported
ISO/IEC 14443 CSN 64 Bit	64 bit Card Serial Number	Interpreted	Interpreted	Not supported
Kastle 32 bit	Kastle 32 bit	Raw	Interpreted	Raw
Matrix 56 bit	54 bit User ID	Interpreted	Interpreted	Raw
OnGuard Wiegand 64	8 bit facility, 48 bit card number, 8 bit issue code	Raw	Raw	Raw
Standard 26 bit	8 bit Site/16 bit User code	Interpreted	Interpreted	Raw
Standard 26 bit - HID PACS	8 bit Site/16 bit PACS	Interpreted	Interpreted	Raw

# Wiegand SEOS PACS

Strongly suggest to create two Wiegand fomats one with SEOS and one NON SEOS of the same format



The screenshot shows the 'Wiegand Profiles' application window. It features a toolbar with icons for Add, Edit, Delete, Refresh, Import, and Export. Below the toolbar is a table listing various Wiegand profiles. The table has five columns: Name, Description, MA2G, MA5G, and M3DF. The first row is highlighted in blue.

Name	Description	MA2G	MA5G	M3DF
Automatically generated random 64 bit		Interpreted	Interpreted	Raw
CASI-RUSCO 40 bit	19 bit Facility / 19 bit Badge	Raw	Raw	Raw
HID Corporate 1000	HID Corporate 1000	Raw	Interpreted	Raw
HID Corporate 1000 - HID PACS	HID Corporate 1000 - PACS	Raw	Interpreted	Raw
ISO/IEC 14443 CSN 32 bit	32 bit Card Serial Number	Interpreted	Interpreted	Not supported
ISO/IEC 14443 CSN 56 bit	56 bit Card Serial Number	Interpreted	Interpreted	Not supported
ISO/IEC 14443 CSN 64 Bit	64 bit Card Serial Number	Interpreted	Interpreted	Not supported
Kastle 32 bit	Kastle 32 bit	Raw	Interpreted	Raw
Matrix 56 bit	54 bit User ID	Interpreted	Interpreted	Raw
OnGuard Wiegand 64	8 bit facility, 48 bit card number, 8 bit issue code	Raw	Raw	Raw
Standard 26 bit	8 bit Site/16 bit User code	Interpreted	Interpreted	Raw
Standard 26 bit - HID PACS	8 bit Site/16 bit PACS	Interpreted	Interpreted	Raw

# Wiegand SEOS PACS

Example to modify wiegand format with SEOS element  
Example 26 bit standard

Name	Description	MA2G	MA5G	M3DF
Automatically generated random 64 bit		Interpreted	Interpreted	Raw
CASI-RUSCO 19 bit	19 bit Facility / 19 bit Badge	Raw	Raw	Raw
HID Corporate 1000	HID Corporate 1000	Raw	Interpreted	Raw
HID Corporate 1000 - HID PACS	HID Corporate 1000 - PACS	Raw	Interpreted	Raw
ISO/IEC 14443 CSN 32 bit	32 bit Card Serial Number	Interpreted	Interpreted	Not supported
ISO/IEC 14443 CSN 56 bit	56 bit Card Serial Number	Interpreted	Interpreted	Not supported
ISO/IEC 14443 CSN 64 Bit	64 bit Card Serial Number	Interpreted	Interpreted	Not supported
Kastle 32 bit	Kastle 32 bit	Raw	Interpreted	Raw
Matrix 56 bit	54 bit User ID	Interpreted	Interpreted	Raw
OnGuard Wiegand 64	8 bit facility, 48 bit card number, 8 bit issue code	Raw	Raw	Raw
Standard 26 bit	8 bit Site/16 bit User code	Interpreted	Interpreted	Raw
Standard 26 bit - HID PACS	8 bit Site/16 bit PACS	Interpreted	Interpreted	Raw

EDIT THE  
26 BIT  
FORMAT

# Wiegand SEOS PACS

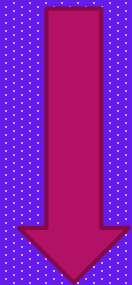
Example to modify wiegand format with SEOS element  
Example 26 bit standard


Enter details for this Wiegand profile

Name:

Description:

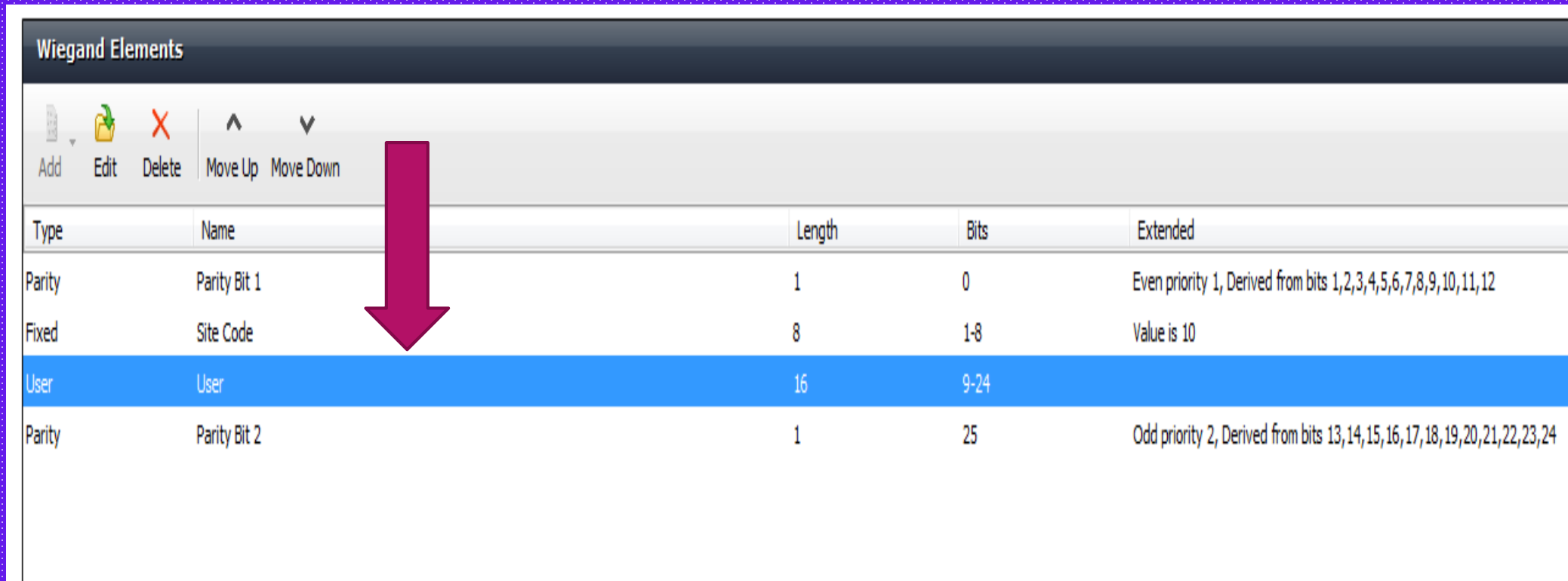
Bit Length:



Next 

# Wiegand SEOS PACS

This is a standard 26 bit structure

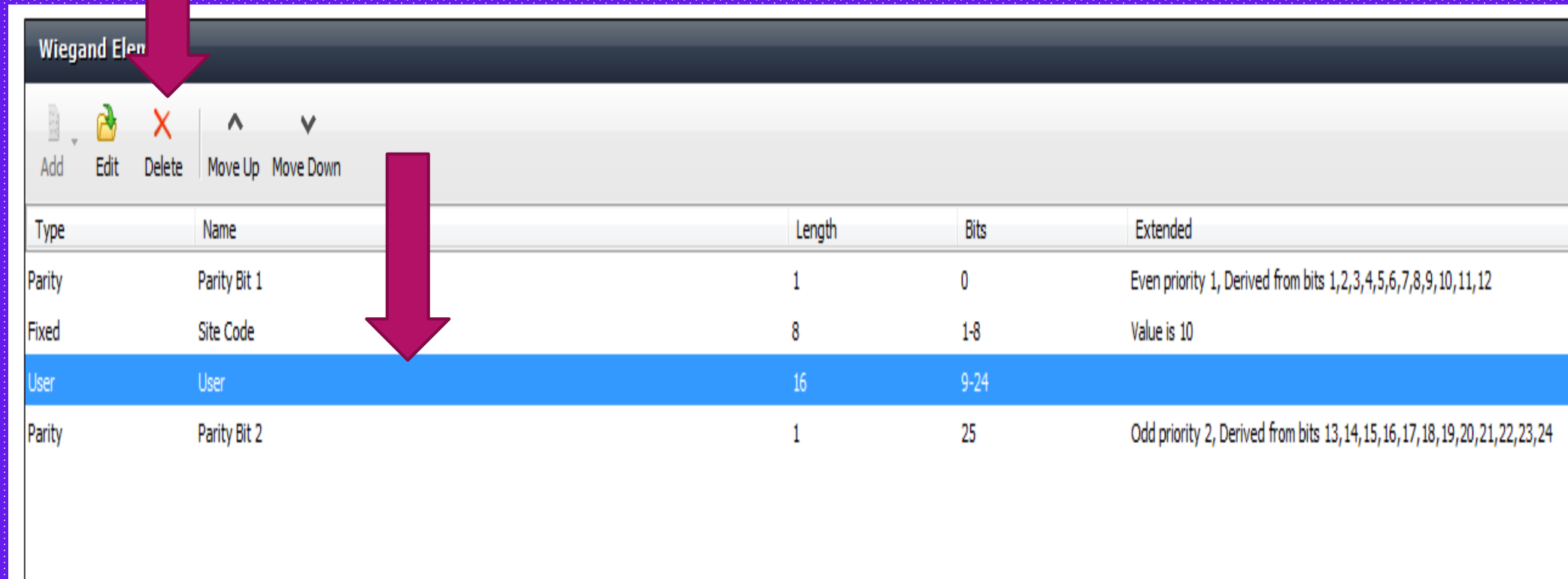


The screenshot shows a software interface titled "Wiegand Elements". It features a toolbar with icons for "Add", "Edit", "Delete", "Move Up", and "Move Down". Below the toolbar is a table with the following columns: "Type", "Name", "Length", "Bits", and "Extended". The table contains four rows of data. The "User" row is highlighted in blue. A large red arrow points downwards from the "Move Down" button area towards the "User" row.

Type	Name	Length	Bits	Extended
Parity	Parity Bit 1	1	0	Even priority 1, Derived from bits 1,2,3,4,5,6,7,8,9,10,11,12
Fixed	Site Code	8	1-8	Value is 10
User	User	16	9-24	
Parity	Parity Bit 2	1	25	Odd priority 2, Derived from bits 13,14,15,16,17,18,19,20,21,22,23,24

# Wiegand SEOS PACS

Delete the User for 16 bits



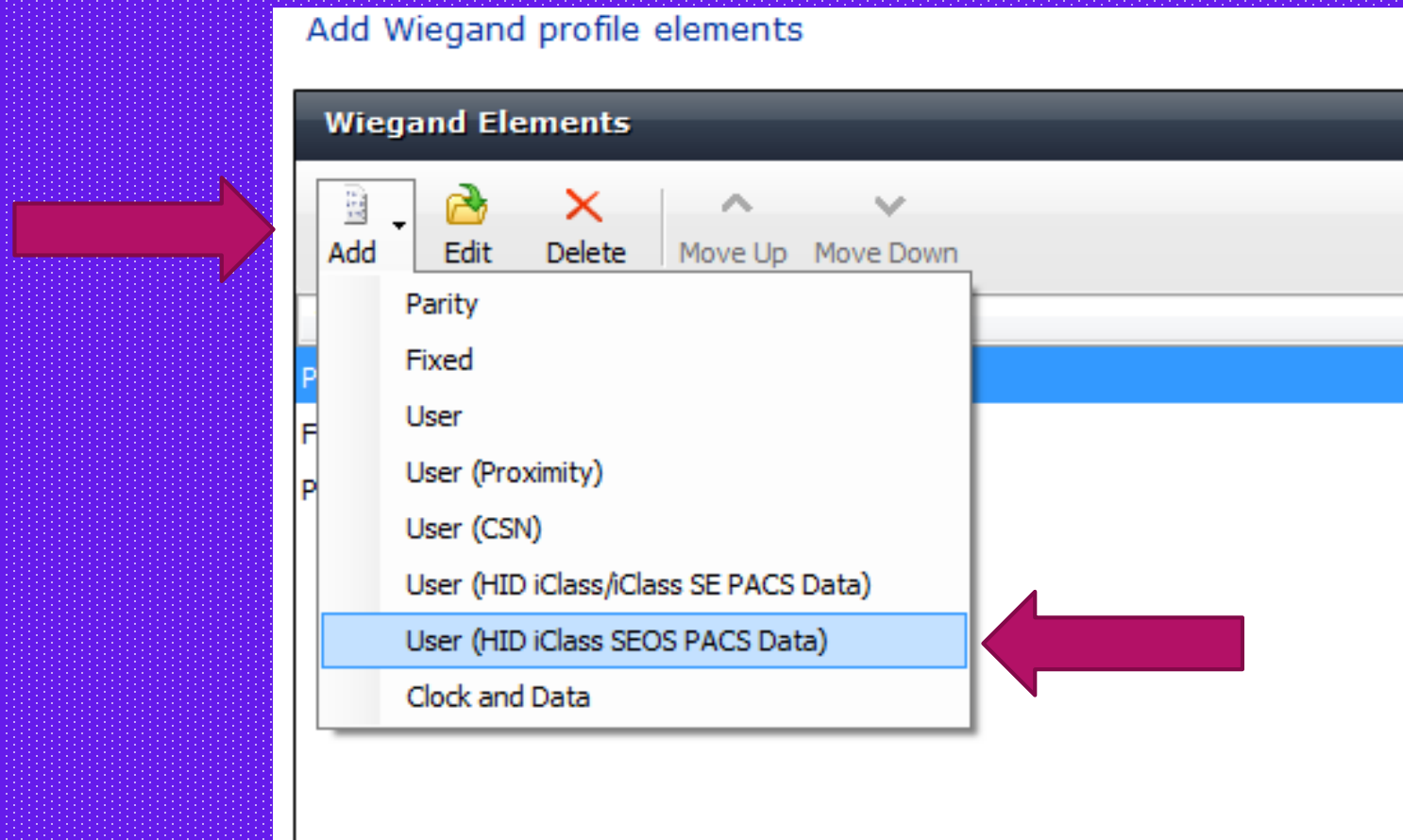
The screenshot shows a software interface for configuring Wiegand elements. At the top, there is a title bar "Wiegand Element" and a toolbar with icons for Add, Edit, Delete, Move Up, and Move Down. Below the toolbar is a table with the following columns: Type, Name, Length, Bits, and Extended. The table contains four rows: Parity Bit 1, Site Code, User, and Parity Bit 2. The "User" row is highlighted in blue. Two red arrows are overlaid on the image: one points to the "Delete" button in the toolbar, and the other points to the "User" row in the table.

Type	Name	Length	Bits	Extended
Parity	Parity Bit 1	1	0	Even priority 1, Derived from bits 1,2,3,4,5,6,7,8,9,10,11,12
Fixed	Site Code	8	1-8	Value is 10
User	User	16	9-24	
Parity	Parity Bit 2	1	25	Odd priority 2, Derived from bits 13,14,15,16,17,18,19,20,21,22,23,24



# Wiegand SEOS PACS

## Add User (HID iclass SEOS PACS Data)



# Wiegand SEOS PACS

Name it and add the length , click next

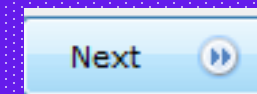
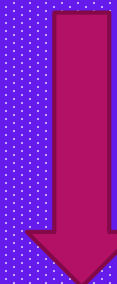
User HID iClass SEOS PACS Data element details

Name:

Hide Value:

Allow Random:

Length:



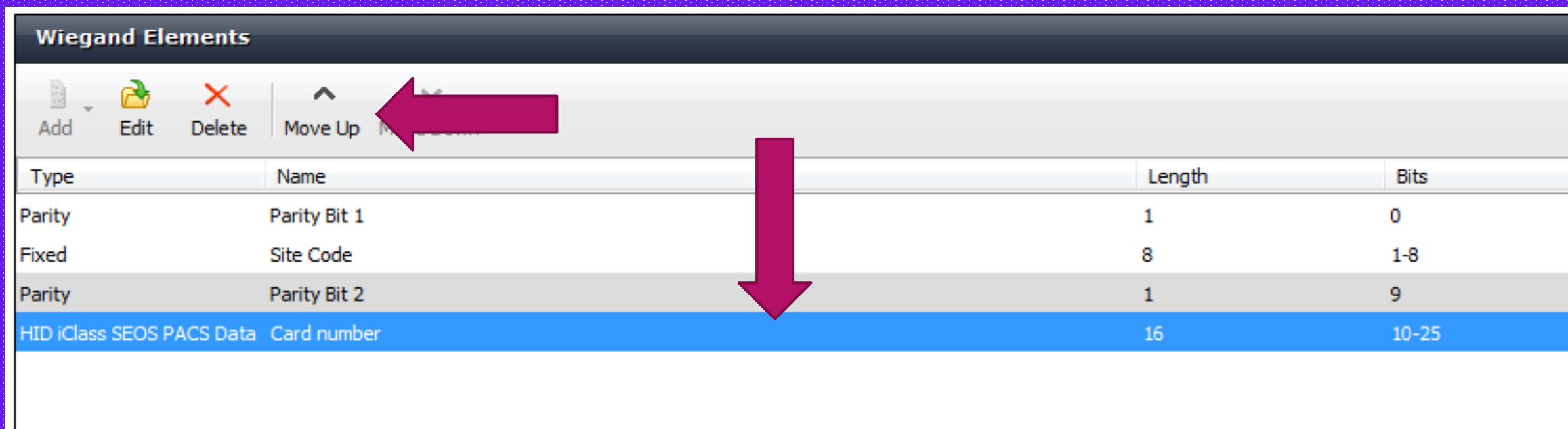
# Wiegand SEOS PACS

Now you added the SEOS PACS data move it up one position

**Wiegand Elements**

Add Edit Delete Move Up Move Down

Type	Name	Length	Bits
Parity	Parity Bit 1	1	0
Fixed	Site Code	8	1-8
Parity	Parity Bit 2	1	9
HID iClass SEOS PACS Data	Card number	16	10-25



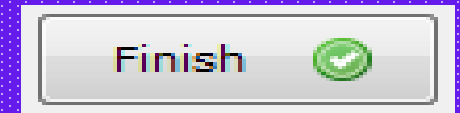
# Wiegand SEOS PACS

This is exactly like a Standard 26 bit but modified for SEOS PACS card number

**Wiegand Elements**



Add Edit Delete Move Up Move Down

Type	Name	Length	Bits
Parity	Parity Bit 1	1	0
Fixed	Site Code	8	1-8
HID iClass SEOS PACS Data	Card number	16	9-24
Parity	Parity Bit 2	1	25



You will see there is a Standard 26 bit and Standard 26 bit with SEOS

Use the Standard for the User Policy and the SEOS for the Biometric Device Profile

Standard 26 bit -		8 bit Site/16 bit PACS
Standard 26 bit - HID PACS		8 bit Site/16 bit PACS
Standard 26 bit - HID SEOS		8 bit Site/16 bit PACS

## Wiegand SEOS PACS

The goal is to get the MWC to read the Print card number off the Iclass SEOS card

Must create or modify the SEOS card format

Strongly suggest that one format is SEOS and one is Non SEOS of the same format

If your card is not listed you would need to pre-create that format first

You would need to know the full structure of that format as well

you can look at the examples of the other Wiegand formats>  
under Wiegand Profiles to guide you

# 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:

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)

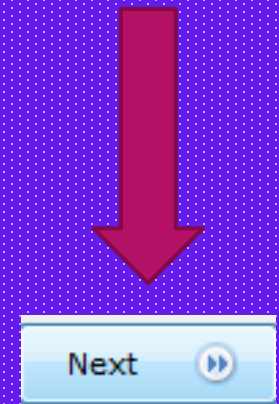
MorphoAccess heartbeat interval:  (seconds)

Key Policy:

**MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme, MA Sigma VP Only Settings**

Allow Remote Enrollment:

Default User Policy for Remote Enrollment:





# Biometric Device Profile

**Biometric Device Settings**

**General Settings**

Wiegand Profile: Standard 26 bit - HID SEOS

Language: English

Realtime logging enabled:

**Biometric Threshold Settings**


Biometric Threshold: Recommended


MorphoAccess Vein Print Mode: Universal Fast

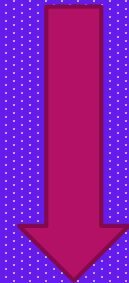
MorphoAccess Fingerprint Threshold: 3

Morpho 3D Face Identification Threshold: Medium

Morpho 3D Face Verification Threshold: Low

 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 BE SET TO WHATEVER THE SEOS CARD FORMAT  
USE THE MODIFY OR ONE YOU CREATED PRIOR**

# 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:

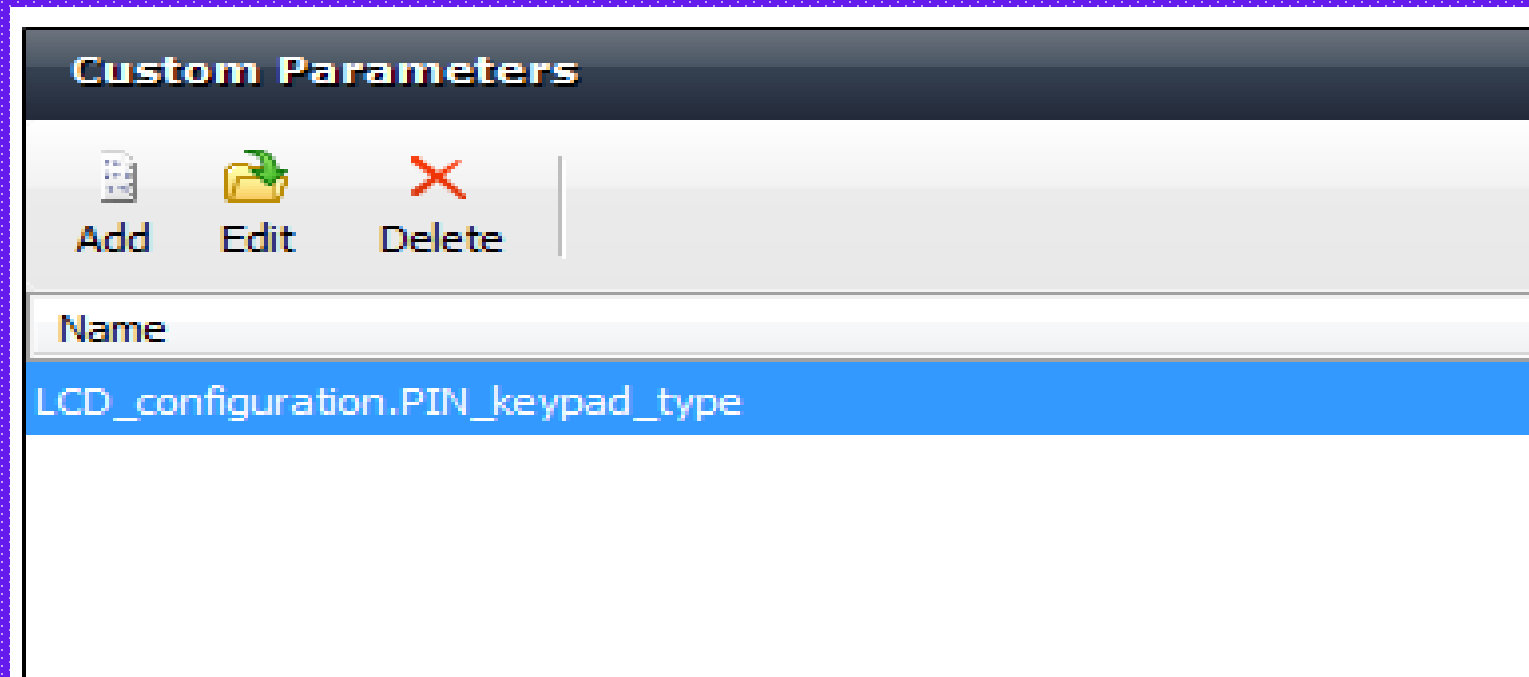
**MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme, MA Sigma VP and MorphoWave Multi-Factor Modes**

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

Next 

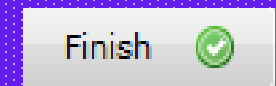
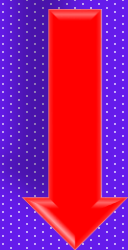
**SET THE MULTI-FACTOR MODE SETTINGS AS EXACTLY AS SHOWN**

# Biometric Device Profile

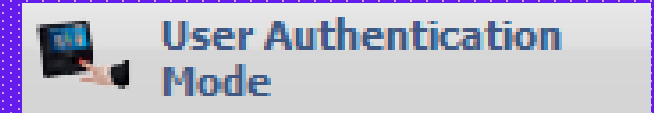


**CLICK NEXT SEVERAL TIMES TILL YOU GET TO CUSTOM PARAMETERS  
ADD THIS PARAMETERS EXACTLY AS SHOWN CASE SENSITIVE\*\***

**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 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: SEOS card and Finger and Pin

Description:

Access Mode: All Biometric Devices and Clients

Allow MA 500 database selection during user enrollment

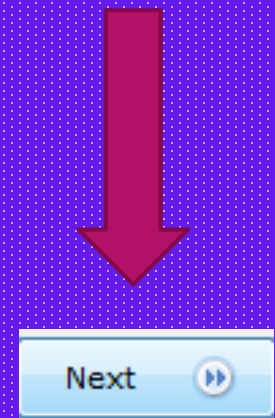
Access Schedule: 24 hours, 7 days a week

Extended User Details:  Display extended user details

Wiegand Profile: Standard 26 bit -

User Authentication Mode: SEOS card and Finger and Pin

Show Photo Capture Page:



**WIEGAND PROFILE , USE A STANDARD FORMAT NON SEOS FORMAT SO YOU CAN MANUALLY TYPE IN THE CARD NUMBER  
USER AUTHENTICATION MODE IS WHAT YOU CREATED EARLIER**



# USER POLICY

CLICK NONE FOR FINGER BIOMETRICS

Enter the details for finger biometric options

Finger Biometric Enrollment Minimum Fingers:

None

Preferred Finger One:

Left Index Finger

Preferred Finger Two:

Right Index Finger

Preferred Duress Finger:

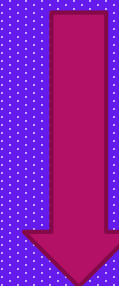
Left Middle Finger

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

**CLICK TWO FOR WAVE ENROLLMENTS**

Enter the details for wave biometric options

Wave Enrollment Minimum Hands:

Two

Show Wave Biometric Capture Page:



Finish



# 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:

SEOS card and Finger and Pin

Enabled:



First Name:

Joe

Middle Name:

Last Name:

Smith

Date of Birth:

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

Next



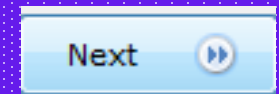
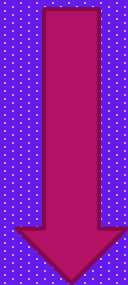
# USER MANAGEMENT

PUT IN THE SEOS PRINTED CARD VALUE

Wiegand Values

Card number	<input type="text" value="112"/>
-------------	----------------------------------

THE SEOS CARD NUMBER WILL BE SEND TO YOUR CONTROLLER AFTER VERIFICATION



# USER MANAGEMENT

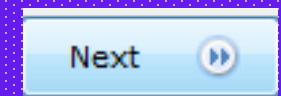
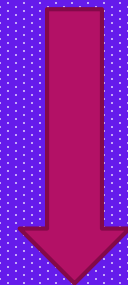
PUT IN THE PIN CODE YOU WANT TO USE

Enter and confirm the PIN

PIN:

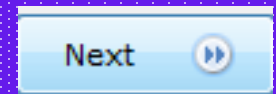
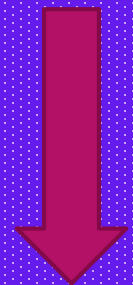
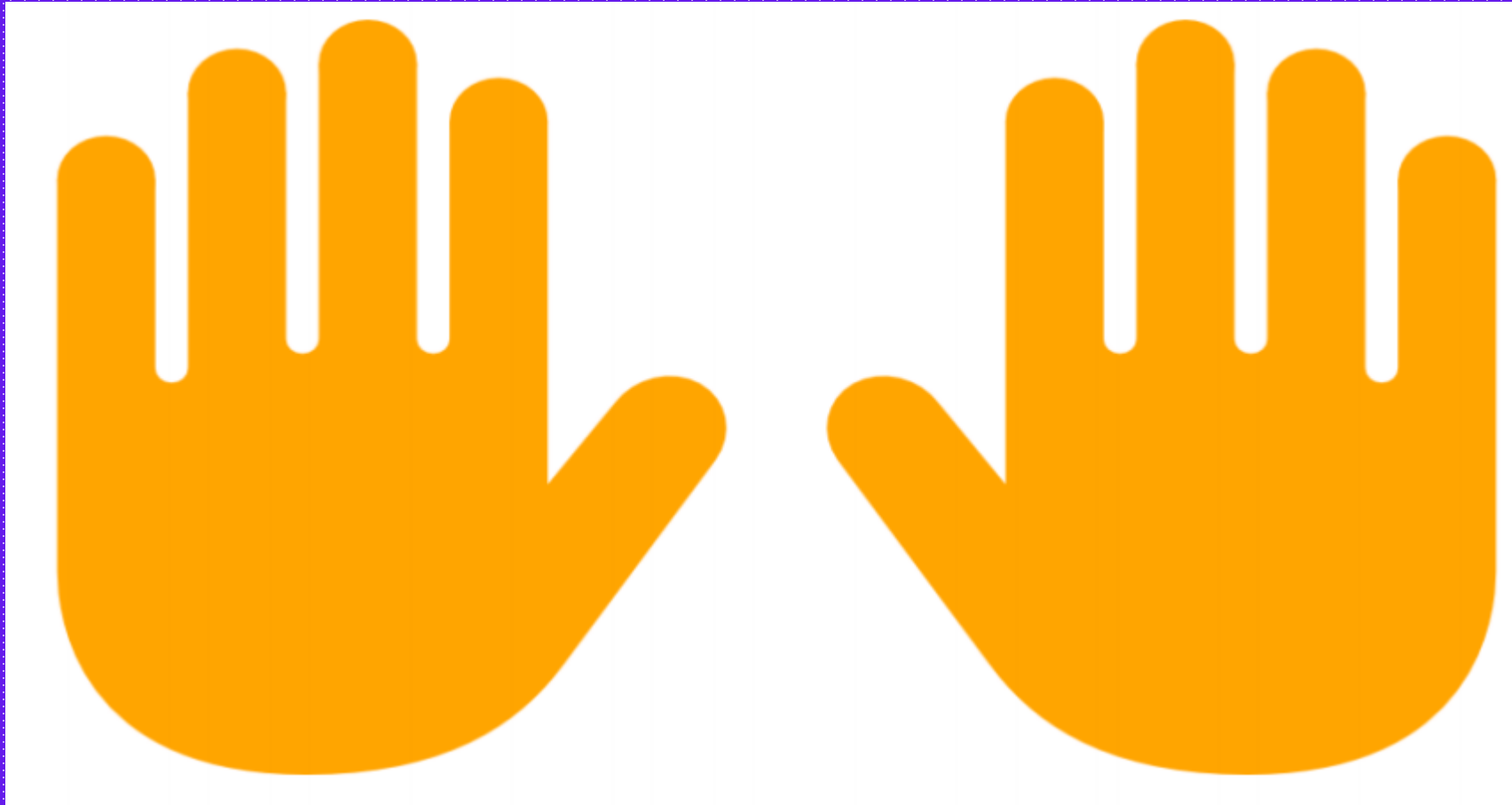
Confirm PIN

THE PIN CODE IS NOT COMING FROM YOUR PANEL, IT IS STORED ON THE DEVICE. IT IS A ADDITIONAL AUTHENTICATION REQUIRED AFTER YOU WAVE YOUR HAND



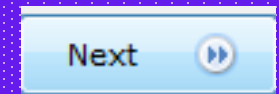
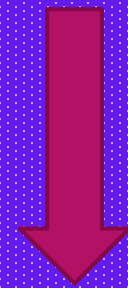
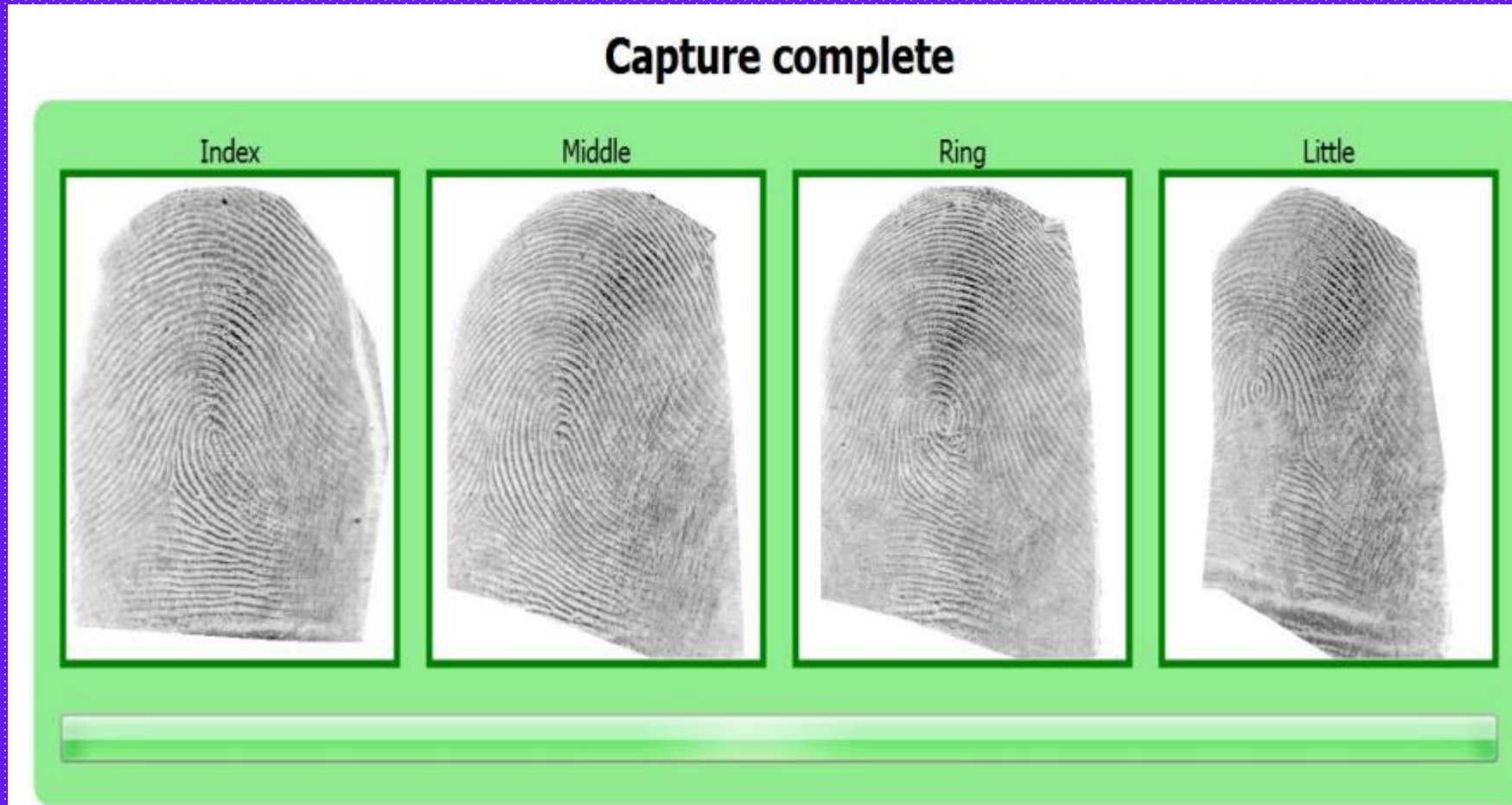
# USER MANAGEMENT

CLICK ON THE FLASHING HANDS TO START CAPTURING



# USER MANAGEMENT

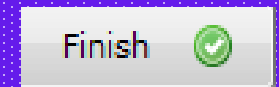
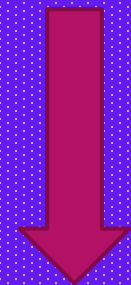
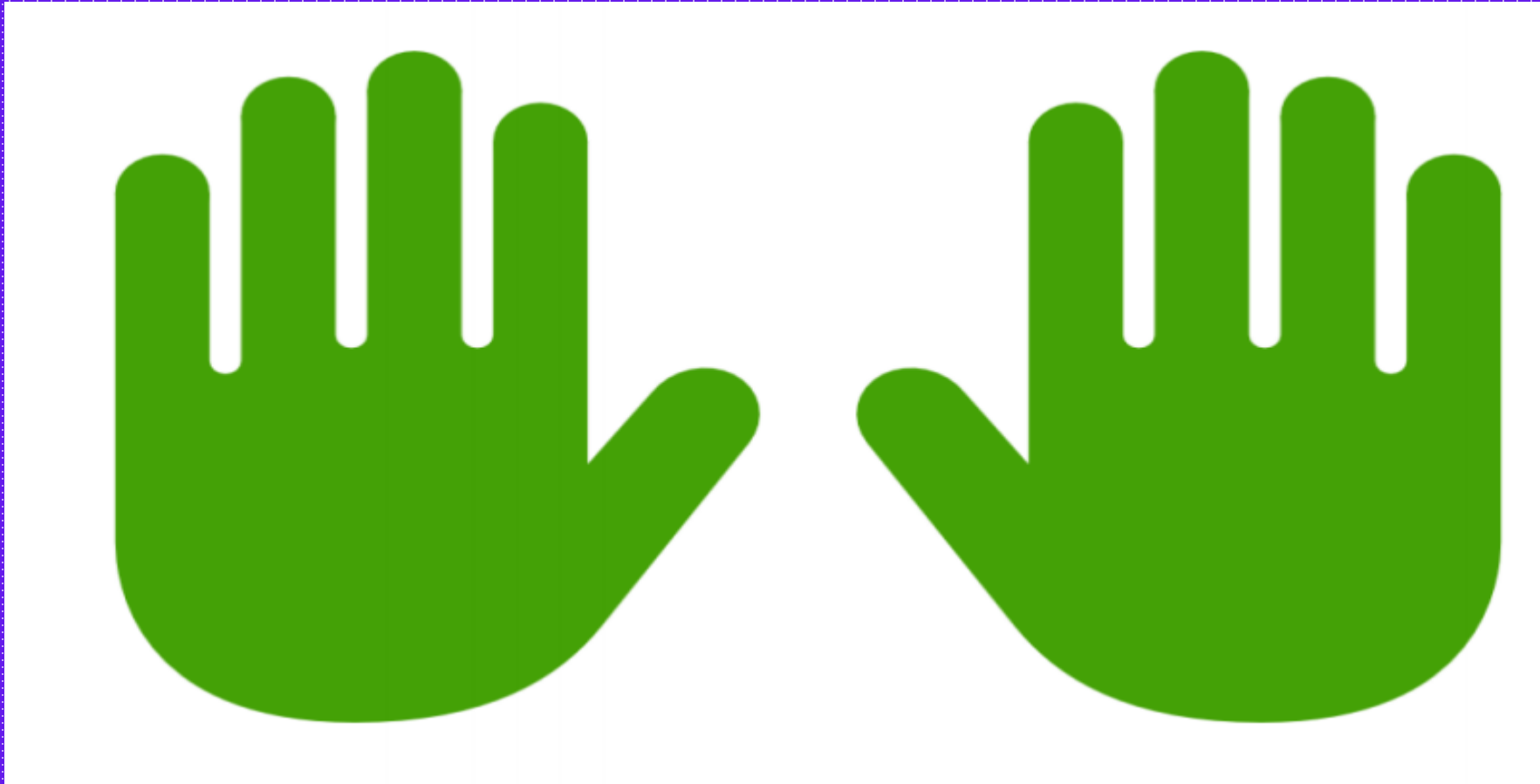
FOLLOW THE PROMPTS ON THE MWC SCREEN





# USER MANAGEMENT

WHEN COMPLETE YOU SHOULD HAVE TWO GREEN HANDS



# FINAL RESOLUTION

ONE **USER AUTHENTICATION MODE** NEEDS TO BE CREATED

ONE USER POLICY NEED TO BE CREATED AND ASSIGN TO THE UAM

BIOMETRIC DEVICE PROFILE NEEDS TO BE CONFIGURED TO READ SEOS CARDS

IF YOUR SEOS CARDS 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

# WEBSITE

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