

# HAND AND PIN WITH MWC



**and**



# 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

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:

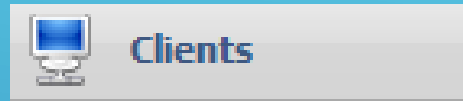
Change User Onsite / Offsite Status:

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:

None

Morpho 3D Face enrollment biometric device:

Search

### Contact Enrollment

Morpho Finger biometric enrollment:

Any MorphoSmart

Morpho Finger enrollment MorphoAccess:

Search

### Contactless Enrollment

Morpho Contactless Finger biometric enrollment:

MorphoWave Compact (IP)

Morpho Contactless Finger enrollment MorphoAccess:

MorphoWave Compact

Search

### Smartcard Encoding

Morpho Smartcard encoding:

Any PC/SC Smartcard reader

Morpho Smartcard encoding PC/SC device:

Morpho Smartcard encoding MorphoAccess:

Search

### Keys

Key Policy:

Default

Finish



# 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:

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.



**WIEGAND PROFILE: THIS VALUE WILL BE SENT BACK TO YOUR ACP**

# BIOMETRIC DEVICE PROFILE

**Multi-Factor Mode Settings**

Multi-Factor Mode:  

Contactless Smart Card Mode:

**Morpho 3D Face Multi-Factor Mode**

Mode:

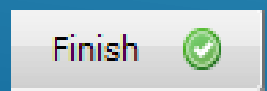
**MA 100, MA J, MA 500, MA VP Multi-Factor Mode**

Mode:

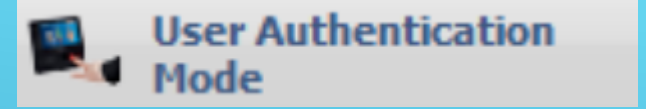
**MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme, MA VP MD and MorphoWave Multi-Factor Modes**

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

SET THE MULTI-FACTOR MODE SETTINGS AS EXACTLY AS SHOWN



# 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

- 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 VP MD, 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:

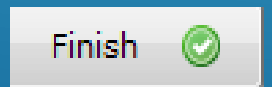
Allow Start By Wiegand In:

Require Pin:  ←

Require Template Match:



**FOLLOW THIS SETTINGS EXACTLY AS SHOWN**





# 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

The screenshot shows a web interface for creating a user policy. On the left is a sidebar with menu items: Operator, Key Policy, Biometric Device Profile, Biometric Device, Wiegand Profiles, User Policy (highlighted with a blue arrow), Access Schedules, User Distribution Group, and User Authentication Mode. The main area is titled 'Enter the details for this User Policy' and contains the following fields:

- Name: Hand and Pin (with a blue arrow pointing to the text)
- Description: (empty text box)
- Access Mode: All Biometric Devices and Clients (dropdown menu)
- Allow MA 500 database selection during user enrollment
- Access Schedule: 24 hours, 7 days a week (dropdown menu)
- Extended User Details:  Display extended user details (with a blue arrow pointing to the checkbox)
- Wiegand Profile: Standard 26 bit (dropdown menu, with a blue arrow pointing to the text)
- User Authentication Mode: Hand and Pin (dropdown menu, with a blue arrow pointing to the text)
- Show Photo Capture Page:

At the bottom right, there is a 'Next' button with a right-pointing arrow, and a large blue arrow points down towards it.

**WIEGAND PROFILE WILL BE WHAT ASSIGN TO THIS USER  
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

 Home

 Administration

 User Management

CREATE A NEW USER WITH THE USER POLICY CREATED EARLIER

Enter details for this User

User Policy:

Hand and Pin

Enabled:



First Name:

Billy

Middle Name:

Last Name:

Smith

Date of Birth:

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

Next

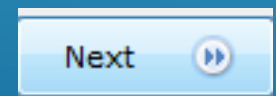


# USER MANAGEMENT

USER ID IS WHAT ASSOCIATED WITH THE USER HAND

Wiegand Values

User ID	12345
---------	-------



# USER MANAGEMENT


PUT IN THE PIN CODE FOR THAT USER

Enter and confirm the PIN

PIN:

Confirm PIN

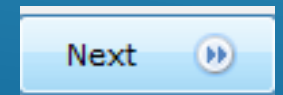
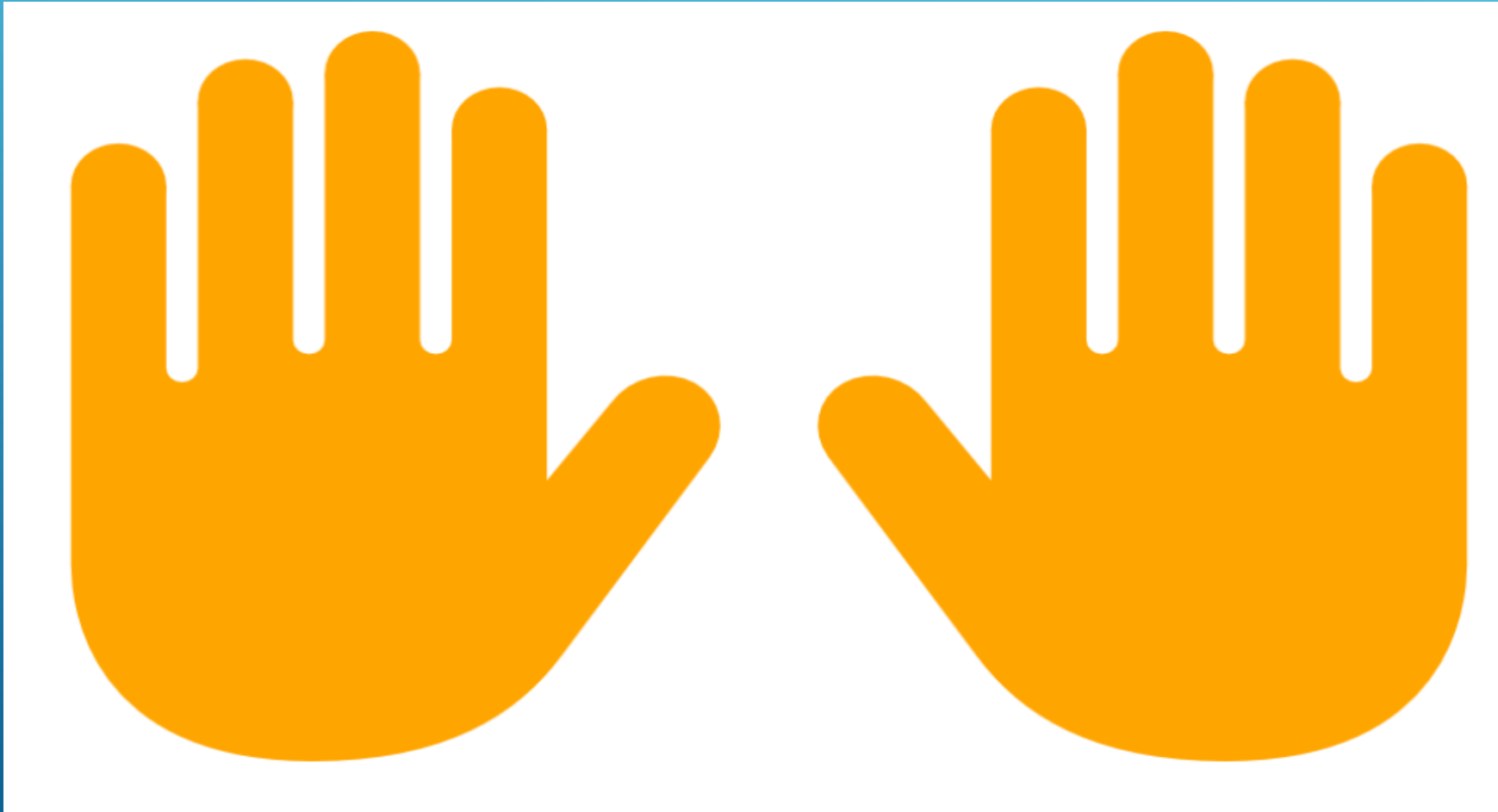


Next 



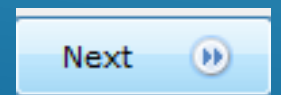
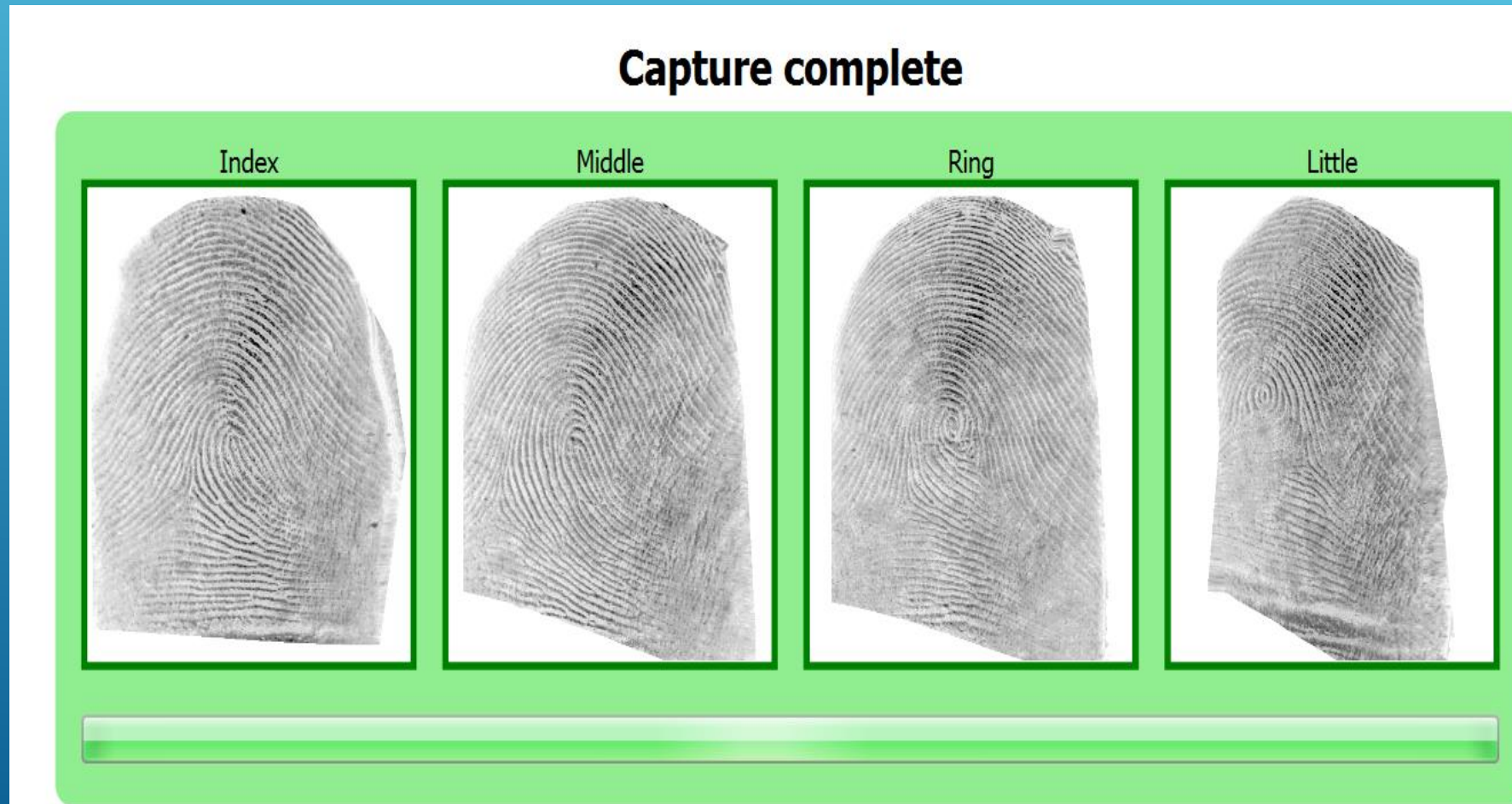
# USER MANAGEMENT

CLICK ON THE FLASHING HANDS TO START CAPTURING



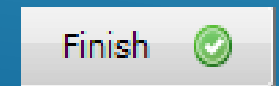
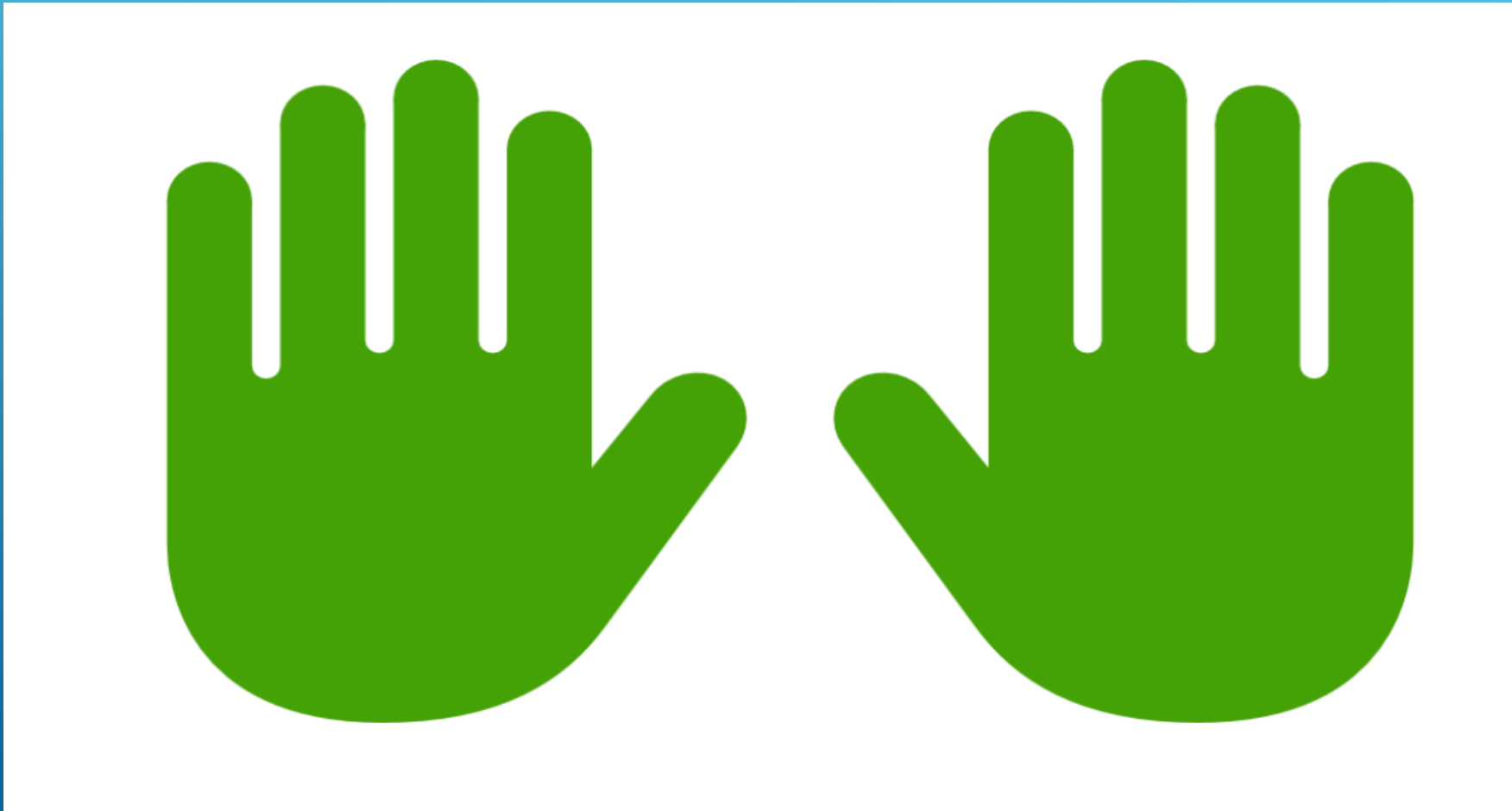
# USER MANAGEMENT

FOLLOW THE PROMPTS ON THE MWC SCREEN



# USER MANAGEMENT

WHEN COMPLETE YOU SHOULD HAVE TWO GREEN HANDS



# END RESULT

User swipes there hand then puts  
in there Pin code for access

\*the User ID gets sent to the ACP not the Pin code

# WEBSITE

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