How to use a Finger Then Keypad access

- Design for: Sigma and Sigma Lite +
- For Users to use a Finger AND Keyboard access
Software Screen shots

Some screen shots might differ slightly from your version of Software
Requirements

- Software
- Morpho Manager

- Get the software from
  - \url{http://service.morphotrak.com/software-links.html}

- You would need a MSO to capture fingerprint enrollments
- You could use *one access reader* to capture fingerprints if you did not have a MSO (*only Sigma and Sigma Lite products*)

- MSO300
Before we begin......
No MSO to capture fingerprints?

Use a Sigma Or a Sigma Lite for enrollment (this option only available Morpho Manager 7.X.X and higher)

Follow the next few steps for configuration
To use a Sigma product to capture fingerprints

- Path > Administration > Client > click (This computer) and Edit
To use a Sigma product to capture fingerprints

- Click next to where it says Enrollment Devices
To use a Sigma product to capture fingerprints

**This is if you want to use a Sigma Family to capture fingerprints

Change Morpho Finger Biometric enrollment >MorphoAccess and Search for your device that you want to use to capture fingerprints

Click Finish
1. **User Authentication Mode**

- **Step One**
1. **User Authentication Mode**

- Create a User Authentication
- Path > Administration > User Authentication Mode
- Designate the authentication mode you wish to utilize for user placed into this User Policy.
1. **User Authentication Mode**

Adding User Authentication Mode

Enter details for this User Authentication Mode

- **Name:** Finger then Keypad
- **Description:**
- **MA 100, MA J, MA 500, and MA VP Mode:** None
- **Morpho 3D Face Mode:** None

⚠️ Smartcard encoding will prefer the MA Sigma settings over MA 100, MA J, MA 500, and MA VP mode settings.
1. **User Authentication Mode**

![User Authentication Mode Diagram](diagram.png)

- **Enable User Authentication Mode**: Check
- **Download Identifier To Device**: Enabled
- **Encode To Smartcard Mode**: None
- **Template Location**: Downloaded To Device
- **Pin Location**: Downloaded To Device
- **Allow Start By Biometric**: Check
- **Allow Start By Contactless Card**: Uncheck
- **Allow Start By Keyboard**: Uncheck
- **Allow Start By Wiegand In**: Uncheck
- **Require Pin**: Check
- **Require Template Match**: Check

**Click Finish**
2. **User Policy**

- Step Two
2. **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.
2. **User Policy**

- **Name:** Enter the name for the User Policy, e.g., *Finger then Keypad*.
- **Description:** Optional field for additional notes.
- **Access Mode:** Select from the dropdown menu, e.g., *All Biometric Devices and Clients*.
- **Access Schedule:** Choose the schedule for the access, e.g., *24 hours, 7 days a week*.
- **Extended User Details:** Optional field for detailed user information.
- **Wiegand Profile:** Select the profile that is associated with your Access Control Panel, e.g., *Standard 26 bit*.
- **User Authentication Mode:** Select the mode you created earlier, e.g., *Finger then Keypad*.
- **Show Photo Capture Page:** Enable for photo capture.

**Click Finish**

- Use the **Authentication Mode** you created earlier.
- Use the **Wiegand format** that is associated with your Access Control Panel (if using ACP).
3. **Biometric Device Profile**

➤ Step Three
3. **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.

- Also called BDP
3. **Biometric Device Profile**

**Enter details for the Biometric Device Profile**

- **Name:** Finger then Keypad
- **Description:**
- **Configuration Mode:** Express
- **Realtime logging enabled:**
- **Log Retrieval Enabled:**
- **Log retrieval interval:** 300 seconds
- **Display name encoding code page:** Western Europe (Default) (ISO-8859-1) (Applicable to MA500 series only)
- **Duplicate check on biometrics:**
- **MorphoAccess heartbeat interval:** 30 seconds
- **Key Policy:** Default original

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

- **Allow Remote Enrollment:**
- **Default User Policy for Remote Enrollment:** 37
3. **Biometric Device Profile**

**Wiegand Profile:** Use the Wiegand format that is associated with your Access Control Panel (if using ACP).

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.
3. Biometric Device Profile

Click Finish
4. **Biometric Device**

- Step Four
4. **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 +, the Morpho 3D Face, the Morph Wave, and the Morpho Tablet Terminal.

- The IP Address on each device must be manually assigned and must be within the IP range of the network. The IP address must not be used by any other device on the network.
4. **Biometric Device**

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

**Adding Biometric Device**

Enter the details for this Biometric Device

- **Name:** Finger then Keypad [Name it]
- **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+ [Assign the BDP you created earlier]
- **Serial Number:**
- **Hostname/IP Address:** 10.1.1.1 [Assign its IP address]
- **Port:** 11010
- **Biometric Device Profile:** Finger then Keypad
- **Include in Time & Attendance Exports:**
- **Change User Onsite/Offsite Status:**
- **Onsite Key:** No Key [Choose a key]
- **Offsite Key:** No Key [Choose a key]

**Click Finish**
5. **User Management**

- Step Five
5. **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.
5. **User Management**

Assign User Policy you created earlier
5. **User Management**

The User ID will be sent to your Access Control Panel (if using ACP)
5. **User Management**

Add the Pin code for this User

*Pin code is the extra authentication that is associated with the User ID*
5. **User Management**

- Capture your fingerprints (two fingers mandatory) Use a MSO 300, MSO1300, MSO VP or a Sigma Reader

Click Finish
Website

- Please visit our website, Service.morphotrak.com for software, firmware, videos and PDF’s.