

MorphoManager

version: 11.2.0

User Manual



Contents

Introduction	6
Support	6
Overview	7
What is a client?	7
What is a server?	7
What is a fingerprint enrollment device?	7
What is a Biometric Device?	8
Setting up MorphoManager	9
Computer hardware requirements:	9
Supported Operating Systems:	9
Installation of MorphoManager software	9
Setting up MorphoManager on a single PC	10
Server and Client Installation	11
Product Registration	12
Procedure for registration	12
Activate Online	13
Activate Offline	15
Advanced Client Configuration	16
Advanced Server Configuration	18
Server Manager	20
Running MorphoManager Login	20
Home Screen	21
Administration	22
Operator	22
Creating a new Operator	22
Screen 1 – Operator Details	22
Screen 2 – Operator Roles	23
Key Policy	24
Creating a new Key Policy	24
Screen 1 – Key Policy Details	24
Screen 2 – MIFARE Classic Key Settings	24
Screen 3 – MIFARE DESFire Key Settings	25
Screen 4 – iClass Key Settings	25
Screen 5 – Bioscrypt 4G Site Keys	25
Screen 6 – Certification Management	26
Lock & Unlock	27
Biometric Device Profile	28
Creating a new Biometric Device Profile (Express)	28
Screen 1 – Configuration Details	28
Screen 2– Biometric Device Settings	29
Screen 3 - Multi-Factor Mode Settings	31
Screen 4 – Access Control Mode Settings	33
Screen 5 – Function Key Mode for MA 100, J, 500, and VP Family	34
Screen 6 – MA 100, MA J, MA 500 and MA VP Settings	35
Screen 7 – MA Sigma, Sigma Lite, Sigma Lite +, & MorphoWave Settings	36
Screen 8 – MA Sigma, Sigma Lite, Sigma Lite +, & MorphoWave Settings (continued)	37
Screen 9– MA Sigma, Sigma Lite, Sigma Lite +, & MorphoWave Settings (continued)	38
Screen 10 – Function Key Mode for MA Sigma, MA Sigma Lite, MA Sigma Lite+ and Morpho Wave Key Mode Settings	39
Screen 11 – MA Sigma, MA sigma Lite+, and MorphoWave Custom Media Files	39
Screen 12 – MA Sigma Custom Parameters	40
Screen 13 – Morpho 3D Face Settings	41
Screen 14 – Video Phone Server Settings	41
Creating a new Biometric Device Profile (Advanced)	43
Screen 2- Wiegand Profile for User ID Conversion	43
Screen 3 - MA 100, MA J, MA 500 and MA VP Advanced Settings	43
Screen 4 – MA Sigma Advanced Settings	44

Screen 5 –MA Sigma Lite Advanced Settings	44
Screen 6 –MA Sigma Lite+ Advanced Settings	45
Screen 7 – MorphoWave Advanced Settings	45
Screen 8 – MA Sigma Extreme Advanced Settings	46
Screen 14 – Morpho 3D Face Settings	47
Creating a new Biometric Device Profile (External).....	47
Biometric Device	48
Create a Biometric Device.....	48
Modify a Biometric Device.....	50
Delete a Biometric Device.....	50
Biometric Device Status and Tasks.....	50
Troubleshooting and Maintenance.....	51
Toolbar Functionality.....	51
Get Logs.....	51
Set Date/Time.....	51
Rebuild.....	51
Set Online	51
Wiegand Profiles	52
Create a Wiegand Profile.....	52
Screen 1 – Configuration Details.....	52
Screen 2 – Wiegand Profile Elements	53
User Policy.....	55
Create a new User Policy	55
Screen 1 – Details	55
Screen 2 – Details for Finger Biometric Options	56
Screen 3 – Details for Wave Biometric Options	58
Access Schedules.....	59
Create an Access Schedule.....	59
Screen 1 – Details	59
Screen 2 – MA Sigma, Sigma Lite, Sigma Lite+ and Morpho Wave access schedules.....	59
Screen 3 – MA 100, MA J, MA 500 and MA VP access schedules.....	60
User Distribution Group	61
Create a User Distribution Group	61
Screen 1 – Details	61
Screen 2 – Select Biometric Device Access	61
Screen 3 – Select MorphoManager Client Access.....	61
User Authentication Mode.....	62
Create a new User Authentication Mode	62
Screen 1 – Details, MA 2G Family Mode, and 3D Face Mode	62
Screen 2 – Details for MA Sigma, MA Sigma lite, MA Sigma Lite +, and Morpho Wave Modes for this User	64
Operator Role.....	66
Notifications	67
Create a new Notification	67
Screen 1 – Details	67
Screen 2 – Select Biometric Devices	68
Screen 3 – Email List	69
Clients.....	69
Screen 1 – Enter the details for this Client.....	69
Screen 2 – Select the tabs displayed on this Client	69
Screen 3 - Camera Configuration	70
Screen 4 - Finger Template Capture Options	70
Screen 5 – Card Template Priority	71
Screen 6 - Enrollment Devices	71
Screen 7 – MSO Identification Configuration Settings	72
Screen 8 – Morpho Wave Identification Configuration Settings	73
Scheduled Reports	75
Card Template	77
Card Encoding Log.....	78
Event Logs	78
Exception Logs.....	78
System Configuration	79
Section 1 – Time and Attendance	79
Section 2 – Communications Engine.....	80

Section 3 – System Functionality	81
Section 4 – System Management.....	82
Section 5 – Gateways.....	83
Section 6 – Connector Service	83
Section 7 – BioBridge	84
Section 8 - Privacy Mode	86
Section 9 – Password Rules.....	86
Section 10 – MorphoTablet	86
Section 11 – Biometric Device Template Priority.....	86
Section 12 – Display Options	87
Section 13 – MorphoWave	88
User Management	89
User Details	89
Creation and enrollment of a User	90
Screen 1 – User Details	90
Screen 2 – Additional Details	91
Screen 3 – Contact Details	92
Screen 4 – User Defined Fields	92
Screen 5 – Biometric Device Override Details (If a Wiegand Profile is set)	92
Screen 6 – User Distribution Groups.....	93
Screen 7 – Photo Capture	93
Screen 8 – PIN Code.....	94
Screen 9 – 3D Face.....	95
Screen 10 – Wave Enrollment.....	96
Screen 10 – Fingerprint Capture	100
User Actions	105
Filtering	105
MSO Identification	106
MorphoWave Identification.....	107
Onsite/Offsite.....	109
Access Logs.....	110
Reports.....	111
User Activity Report	111
Biometric Device Activity Report.....	112
User Policy Activity Report	112
All Activity (included all users and Biometric Device).....	112
Inactivity Report	112
List Report	112
User Policy Members Report.....	112
Permissible Report	112
Tools and Utilities.....	113
Database Management.....	113
Database Backup Tool	113
Database Copy Tool.....	113
Copying a database.....	113
Biometric Device Setup	116
Biometric Device IP Address Configuration	116
Biometric Device Profile Creation Tool	117
MEMS Migrator.....	118
SecureAdmin / SecureAdmin Lite Migrator	119
MA Sigma Firmware Update Tool	120
Create a Firmware Update job	120
Screen 1	120
Screen 2	121
Screen 3	121
Biometric Device Wiring.....	123
MA 500 / MA 500+ Series: New Block board wiring	123
MA 500 Series: Old block board wiring	124
MA Sigma Series: Cabling Diagram	125
MA Sigma Lite Series: Cabling Diagram.....	126

Ethernet Interface (LAN 10 Mbps)	127
T568B and T568A RJ45 Wire Positions.....	127
Biometric Device TCP/IP Ethernet Wiring	128
Power Supply source	128
Wiegand output wiring.....	129
Wiegand input wiring	129
Output relay and Tamper-Switch	129

Introduction

MorphoManager is the latest generation of biometrically powered Access Control and Time & Attendance capture software. The software works with Biometric Device hardware to capture user's finger prints, photos, and personal details. The fingerprint information is sent to specified Biometric Devices where access control is required and where users clock on and off throughout the day. MorphoManager also works with Morpho 3D Face Readers to capture user's facial traits.

Support

Please contact your installer for additional support.

Overview

A MorphoManager system consists of four components:

- A MorphoManager Server
- At least one MorphoManager Client
- A fingerprint/finger vein/hand/3D Face enrollment device.
- At least one Biometric Device.

What is a client?

A client is a computer that has the **MorphoManager Client** software installed. There can be more than one client in a MorphoManager system.

The client application provides the management of access points, enrolling of personnel, and reporting. A PC that has the enrollment scanner connected and is used as the user registration PC. A client PC may be used to view data and not have an enrollment device connected.

What is a server?

A server is a computer that has the **MorphoManager Server** software installed.

The server manages the communication between the Biometric Device and the PC and interacts with the database. It also handles requests from clients.

What is a fingerprint enrollment device?

A fingerprint enrollment device captures an image of a user's fingerprint, extracts the features and sends it to the MorphoManager software. This information is sent to a Biometric Device for user authentication. There are currently three types of fingerprint enrollment devices:



MorphoSmart 300
USB Fingerprint
Reader



MorphoSmart 1300
USB Fingerprint Reader



MorphoSmart FVP
USB Fingerprint and Vein
Reader



MorphoWave
USB Hand
Reader

The readers are connected to a computer that is running MorphoManager Client software. All enrollment of personnel is performed using MorphoManager software. Device drivers for this hardware are automatically installed when MorphoManager Client software is installed.

What is a Biometric Device?



**MorphoAccess
500+
(MA 500+)**



**MorphoAccess
OMA 520
(OMA 520)**



**MorphoAccess
VP
(MA-VP)**



**MorphoAccess
J-Series
(MA-J)**



**MorphoAccess
Sigma
(MA-Sigma)**



**MorphoAccess
Extreme
(MA-Extreme)**



**MorphoAccess
Lite+
(MA-Lite+)**



**MorphoAccess
Lite
(MA-Lite)**

A Biometric Device such as the MorphoAccess units above are used to authenticate users and allow access to doors. They record a log of every presentation. MorphoManager is used to manage user's access to a Biometric Device.



Morpho 3D Face Reader



MorphoWave

Like the Biometric Devices above, a Morpho 3D Face Reader is a Biometric Device used to authenticate users while recording a log of every presentation. While they are also managed by MorphoManager, they follow a different method when authenticating users. The Morpho Wave is another Biometric Device, but uses the biometrics of an entire hand (three or four fingers by default) that is swiped / waved quickly through the device.

Setting up MorphoManager

This section outlines the requirements for MorphoManager systems.

Computer hardware requirements:

Processor:	Dual Core CPU
RAM:	4 GB
Ports:	Three USB ports
Network:	100Mbps Ethernet port required for client/server connections.
Internet Access:	Required for updates. (If no internet access is available, updates can be installed via USB memory stick or CD Rom)

Supported Operating Systems:

MorphoManager Server:

- Microsoft Windows 7 64-bit
- Microsoft Windows 8.1 64-bit
- Windows Server 2008 R2 64-bit
- Windows Server 2012 64-bit
- Windows Server 2012 R2 64-bit
- Windows Server 2016 64-bit
- Windows 10 64-bit

MorphoManager Client:

- Microsoft Windows 7 32-bit / 64-bit
- Microsoft Windows 8.1 32-bit / 64-bit
- Windows Server 2008 R2 64-bit
- Windows Server 2012 64-bit
- Windows Server 2012 R2 64-bit
- Windows Server 2016 64-bit
- Windows 10 32-bit / 64-bit

Installation of MorphoManager software

There are two configurations for MorphoManager:

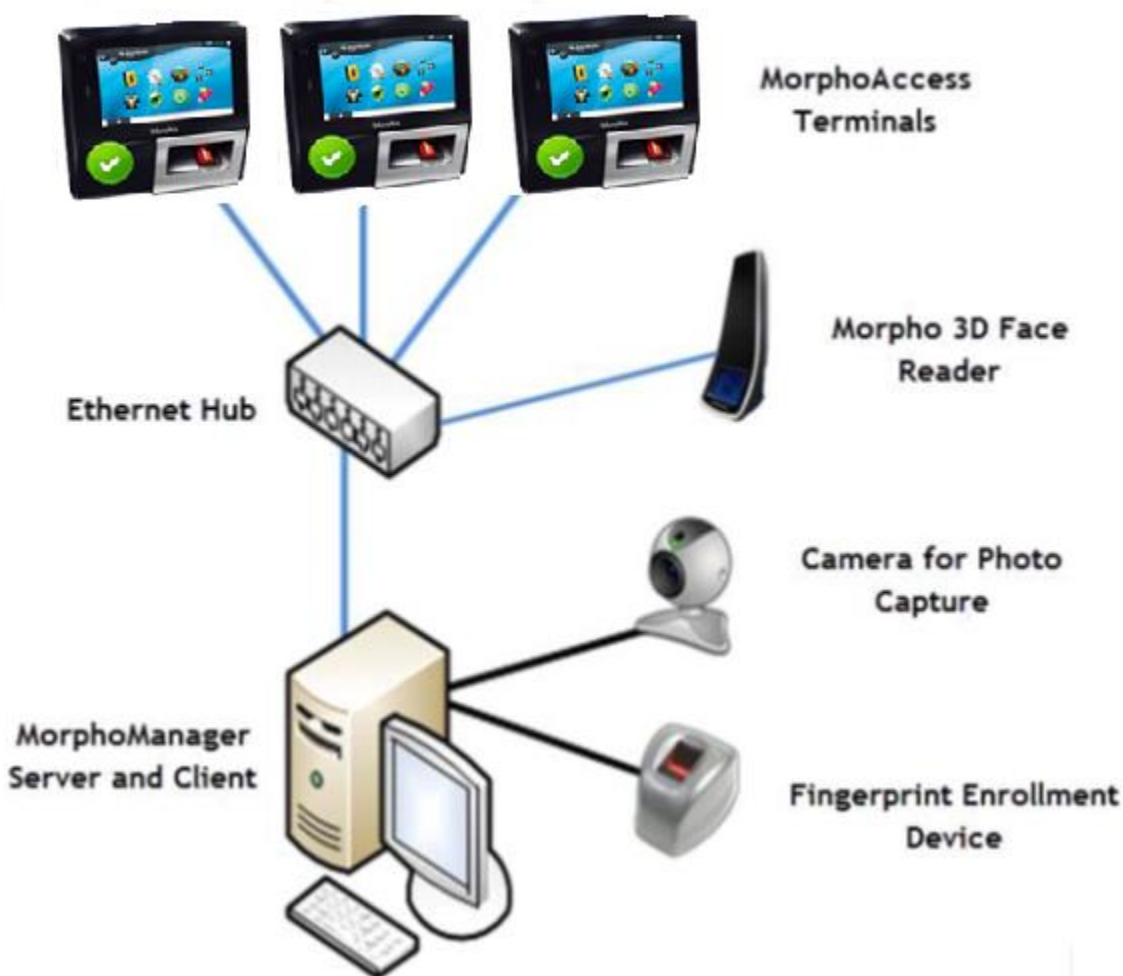
- Client and Server on the same PC
A PC can have both the client and server software installed. The server software needs to be installed first.
- Server PC and Client PCs
The server software needs to be installed on the server PC and the client software needs to be installed on each client PC that will connect to the server PC over a LAN or VPN connection.
The server software needs to be installed first.

Updates for MorphoManager can be obtained by visiting: <http://support.morphomanager.com/>

Setting up MorphoManager on a single PC

Both the client and the server applications can be installed on one computer.

- Locate and select the link to install the MorphoManager Server.
- After the server is installed, install the client.
- Once the client is installed reboot the computer.
- Connect the MSO 300 enrollment device to the PC.
- Ensure the Biometric Devices are on the same network as the MorphoManager Server/Client PC and are in the same IP range.
- Start MorphoManager – double click on the icon on the desktop.
- When logging in for the first time the following details are used.
 - Username: **administrator**
 - Password: **password**
- It is recommended the Administrator password is changed immediately. This can be done by clicking on the **Change Password** icon on the status bar.

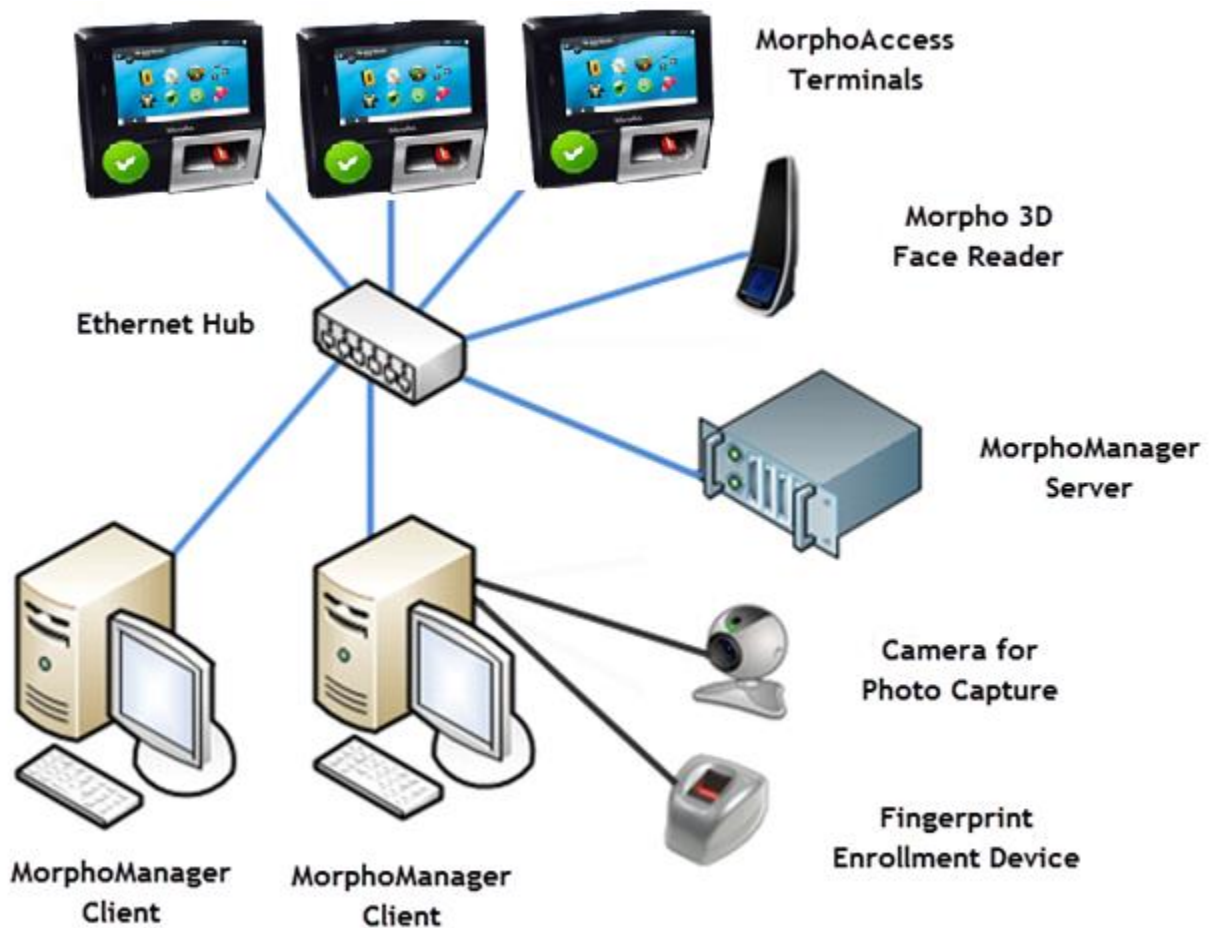


For added security, many businesses and departments have chosen to dedicate a PC for MorphoManager and often use a dedicated hub to which only the MorphoManager PC's and Biometric Devices connected.

Alternatively, an existing hub can be used, but it is recommended that the IP range of the MorphoManager PC and Biometric Devices are different from the corporate PC's.

Server and Client Installation

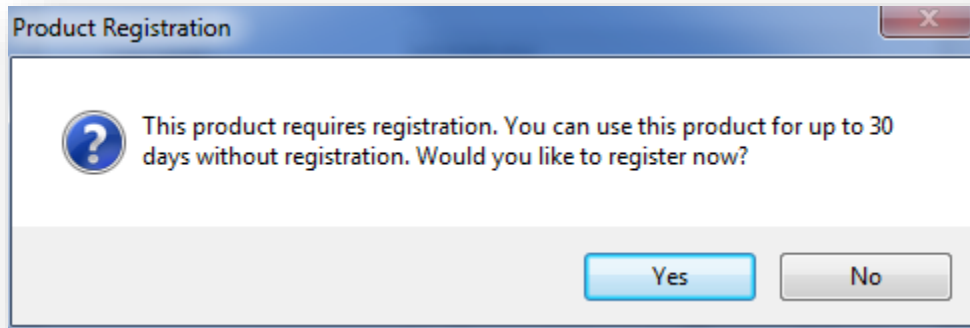
This configuration can be used with an existing corporate network that already has a server. The MorphoManager client application can be installed on any PC that is attached to the server.



The MorphoManager server application can be installed on a separate PC which may or may not be a dedicated server.

Product Registration

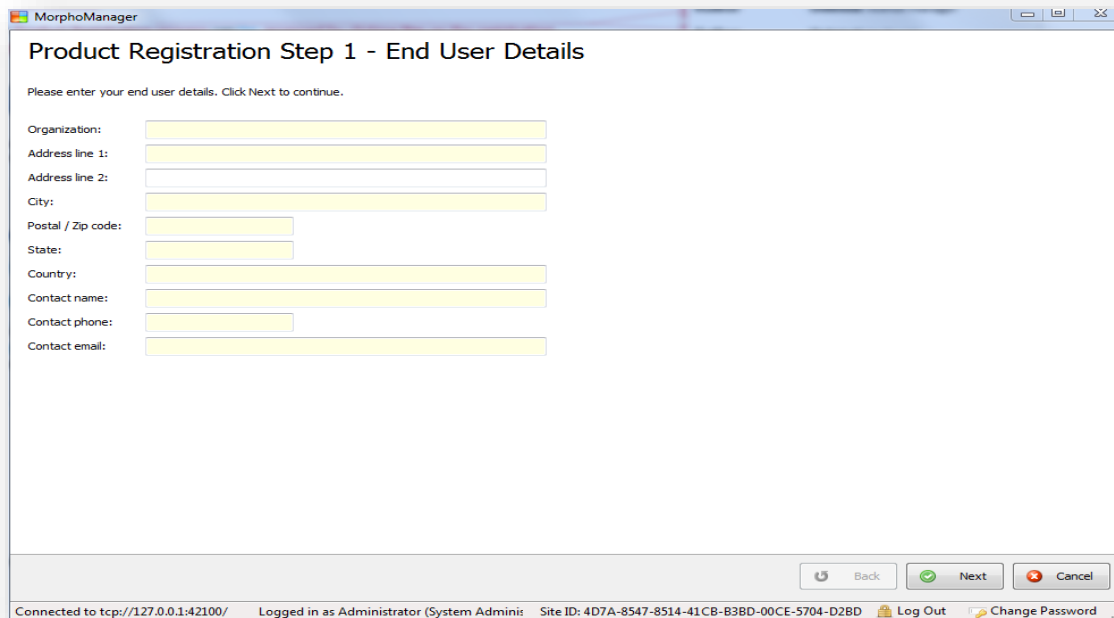
The MorphoManager Product Registration process can be accessed by clicking **Yes** on the registration prompt after logging into Morpho Manager.



If the product is not registered, MorphoManager will run for 30 days in trial mode.

Procedure for registration

MorphoManager can be registered either online or offline. On the first step of the registration wizard enter the end user details and click **Next**.

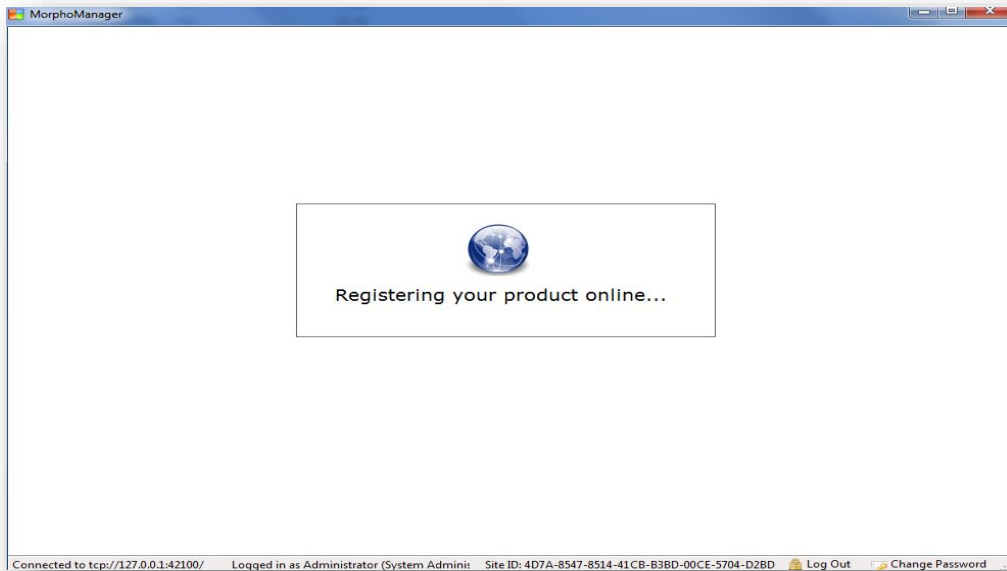


On the following screen enter the installer details and click **Next**.

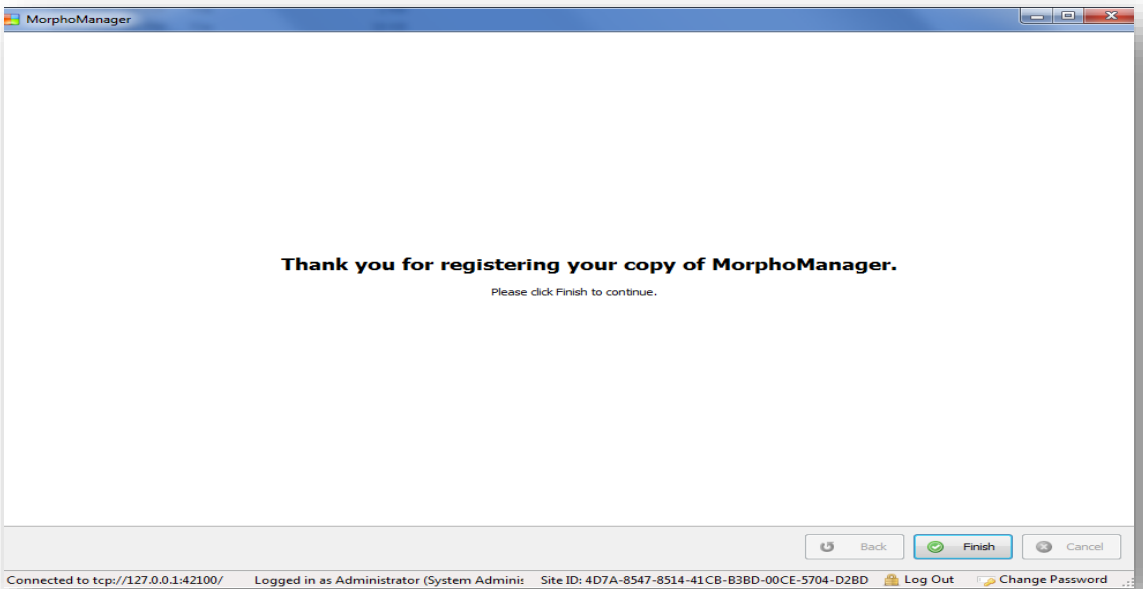
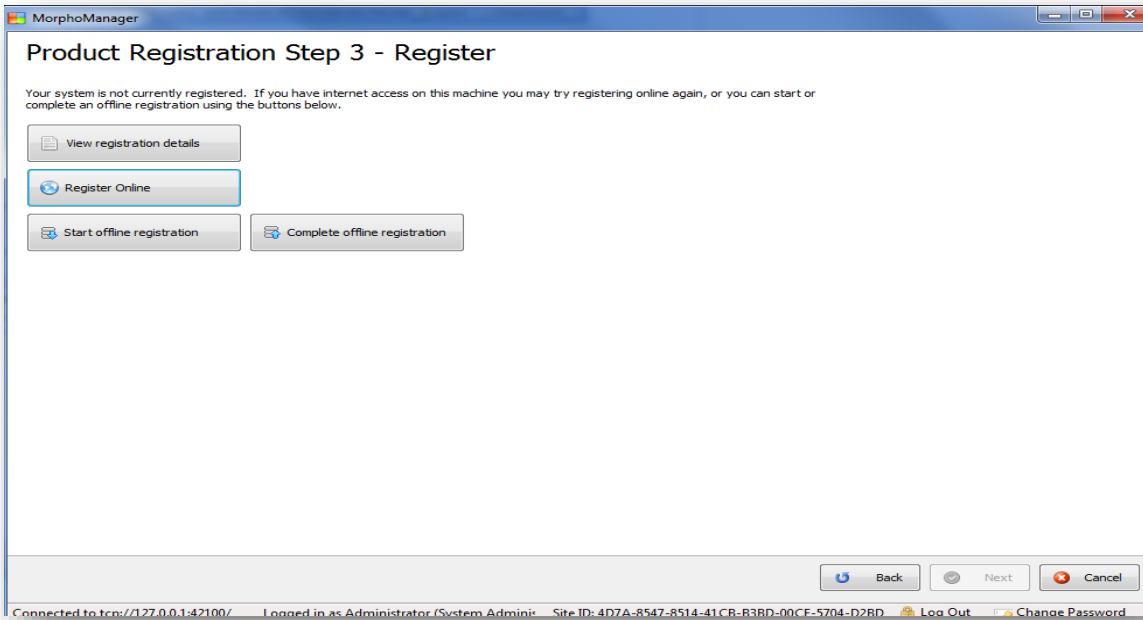
The screenshot shows a window titled "MorphoManager" with the subtitle "Product Registration Step 2 - Installer Details". Below the subtitle, it says "Please enter your installer details. Click Next to continue." There is a checkbox labeled "Installer details are the same as end user details". Below this are several input fields for: Organization, Address line 1, Address line 2, City, Postal / Zip code, State, Country, Contact name, Contact phone, and Contact email. At the bottom right, there are three buttons: "Back", "Next", and "Cancel". At the bottom of the window, there is a status bar with the following text: "Connected to tcp://127.0.0.1:42100/ Logged in as Administrator (System Adminis Site ID: 4D7A-8547-8514-41CB-B3BD-00CE-5704-D2BD Log Out Change Password".

Activate Online

If you are connected to the internet you will be activated online after clicking **Next** on the Step 2 wizard screen. The following screen should appear:



When the process is complete the following screen will appear. Morpho Manager is now registered. After clicking **Finish** you will be taken to the MorphoManager Home Screen.



Activate Offline

If you do not have the internet, you will be shown the following screen after Step 2 mentioned in the beginning of this registration section. From here you can click **Start offline registration**.

The system will prompt you to save a registration file. Choose a location, give the file a name, and click **Save**.

In the Americas email the file for registration processing to cscenter@morpho.com. For the rest of the world, please email the file to hotline.biometrics@morpho.com. Once it has been completed it will be emailed back to you. Save it where it is accessible to MorphoManager and reopen the registration process by clicking **Yes** to the registration prompt you receive when logging in to MorphoManager. You can now click the **Complete offline registration** button. Find the file and click **Open**. This will complete the offline registration process.

Advanced Client Configuration

The MorphoManager **Advanced Client Configuration** can be found by clicking on the start menu, then selecting “MorphoManager” and then “MorphoManager Advanced Client Configuration”.

The screenshot shows the 'Advanced Client Configuration' window. It is organized into three main sections:

- Server connection:**
 - Server connection type: Local computer only (dropdown)
 - Broadcast port: 43100 (text box)
 - Hostname: (empty text box)
 - Port: 42100 (text box)
 - Remoting channel type: TCP (dropdown, with note '(Must match server setting)')
 - A button: 'Manage high availability server list'
- Automatic login:**
 - Enable automatic login:
 - Username: (empty text box)
 - Password: (empty text box)
- Server connection test:**
 - Instruction: 'Click the test button below to discover servers'
 - Table with columns: Product, Version, Server connection point, Server uptime
 - Buttons: 'Test', 'View errors'

At the bottom of the window are three buttons: 'Apply changes', 'Revert changes', and 'Close'.

Server Connection Type:

Local Computer Only: Use this setting when the client and server are installed on the same PC.

Manually Specified: The server is installed on a different PC to the client. Enter the hostname or IP address of the server in the hostname box. The port must be the same as the remoting port specified on the server configuration. The port values should only be changed if the default ports are being used by another application.

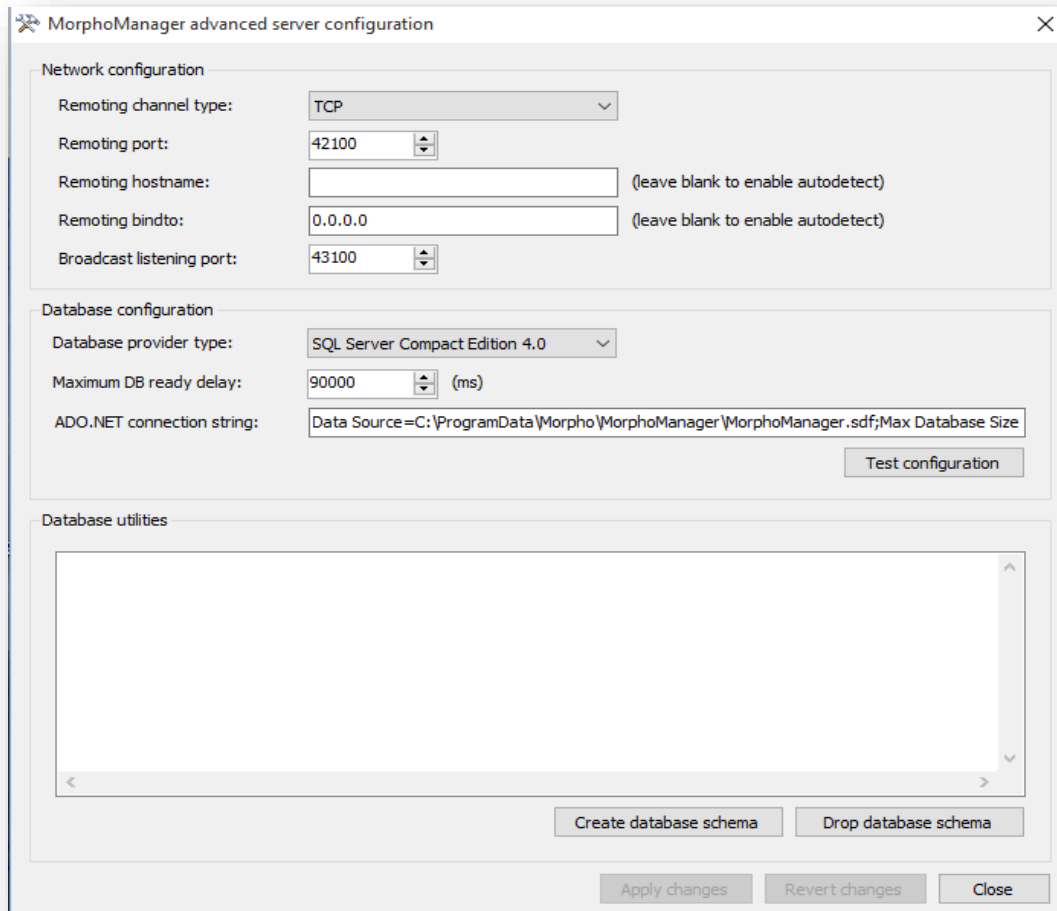
Automatic Discovery: Used when the server is installed on a different PC to the client. The application will attempt to automatically find a MorphoManager server on the network. If there is a problem with Automatic Discovery use manually specified instead. The broadcast port must be the same as the broadcast listening port specified on the server

	configuration. The port values should only be changed if the default ports are being used by another application.
Port:	Specifies the server port that the MorphoManager Server is accepting client connections on. The default port is: 42100.
Remoting channel type:	Specifies whether the client/server communication should be unencrypted (TCP) or encrypted (Encrypted TCP). This setting must match the setting on the MorphoManager Server. The default is unencrypted (TCP).
Enable Automatic Login:	When enabled, the MorphoManager client will use the username and password entered here to login automatically. This can be a security problem, and should be used on clients that are secured by other means or have only one user. It is primarily used for convenience so the user does not have to enter their user name and password if it is unnecessary.

Apply the settings required and click on **Apply changes** and then **Close**.

Advanced Server Configuration

The MorphoManager Advanced Server Configuration can be found by clicking on the start menu, then selecting “MorphoManager”, followed by “Server”, and then “Advanced Server Configuration”.



Remoting Channel Type: Specifies whether client/server communication is to be encrypted. Default setting is unencrypted (TCP). This setting must be applied at all clients.

Remoting Port: This is the port that the client will communicate with the server on. It must be the same as the one specified in the client configuration.

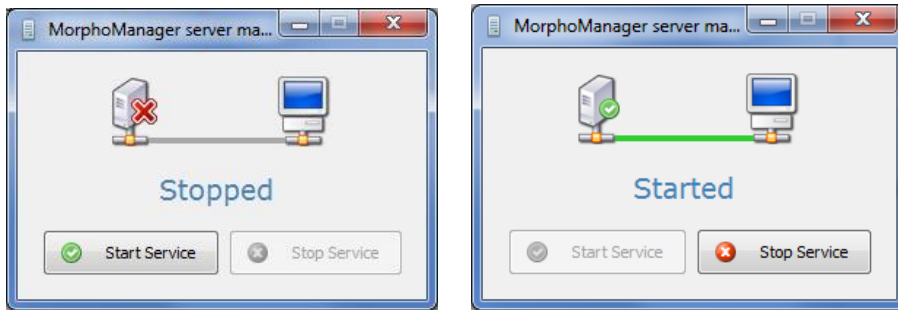
Remoting Hostname: This is the hostname that the client will connect to. This must be the same as the hostname specified in the client configuration. This should be left blank by default.

Remoting Bindto:	If you have more than one IP address on your PC, and you want to force MorphoManager to use a specific IP, please enter it here (Advanced users only).
Broadcast Listening Port:	This is the port that the auto detection of servers operates on. It must be the same as the port specified in the client configuration.
Database Provider Type:	<p>There are two database provider types:</p> <ul style="list-style-type: none">• SQL Server (2005 or later)• SQL Server Compact Edition 4.0 <p>SQL server Compact Edition 4.0 is selected by default and is the preferred option for smaller installations. The SQL Server 2005 or later edition is used on larger installations, or where an existing SQL Server is already available.</p>
Maximum DB Ready Delay:	Maximum amount of time to wait for the database to be available.
ADO.Net Connection String:	This is the connection string that will be used to connect to the database. Enter the connection string and click Test Connection . Ensure the connection is successful before applying changes.
Drop Database Schema:	Dropping a database schema will remove all tables and all data from the database. This is a non-recoverable operation and cannot be undone. Revert changes will not undo this operation. A prompt will be displayed confirming this action.
Create Database Schema:	Creating a database schema should only be performed on a new empty database or an existing database that has had a drop schema operation performed on it. This operation will set up a database and create all the tables and default data for MorphoManager.
Apply Changes:	When all the settings are correct click Apply Changes to save the changes.
Revert Changes:	Reverts all changes back to their last saved state. A drop database schema <u>cannot</u> be reverted.

Server Manager

The MorphoManager Server Manager can be found by clicking on the start menu, then selecting “MorphoManager”, followed by “Server” and then “Server Manager”.

The server manager is used to start and stop the MorphoManager server. Stopping the server will stop all clients from operating. This should only be performed if instructed by the support staff.



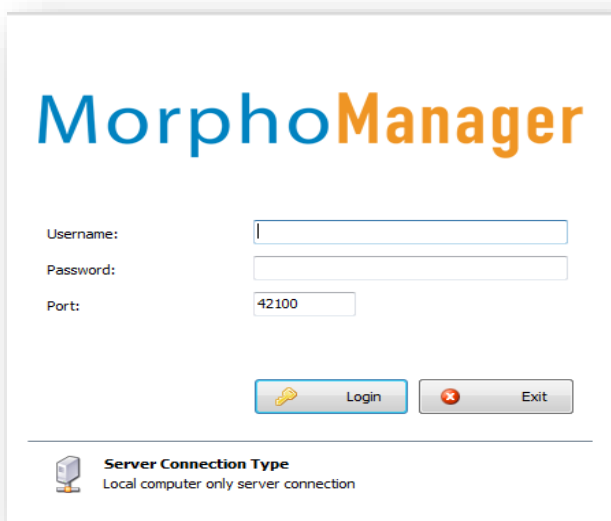
Running MorphoManager Login

MorphoManager Client software requires a username and password to be entered before starting.



By default, the username is **administrator** and the Password is **password**.

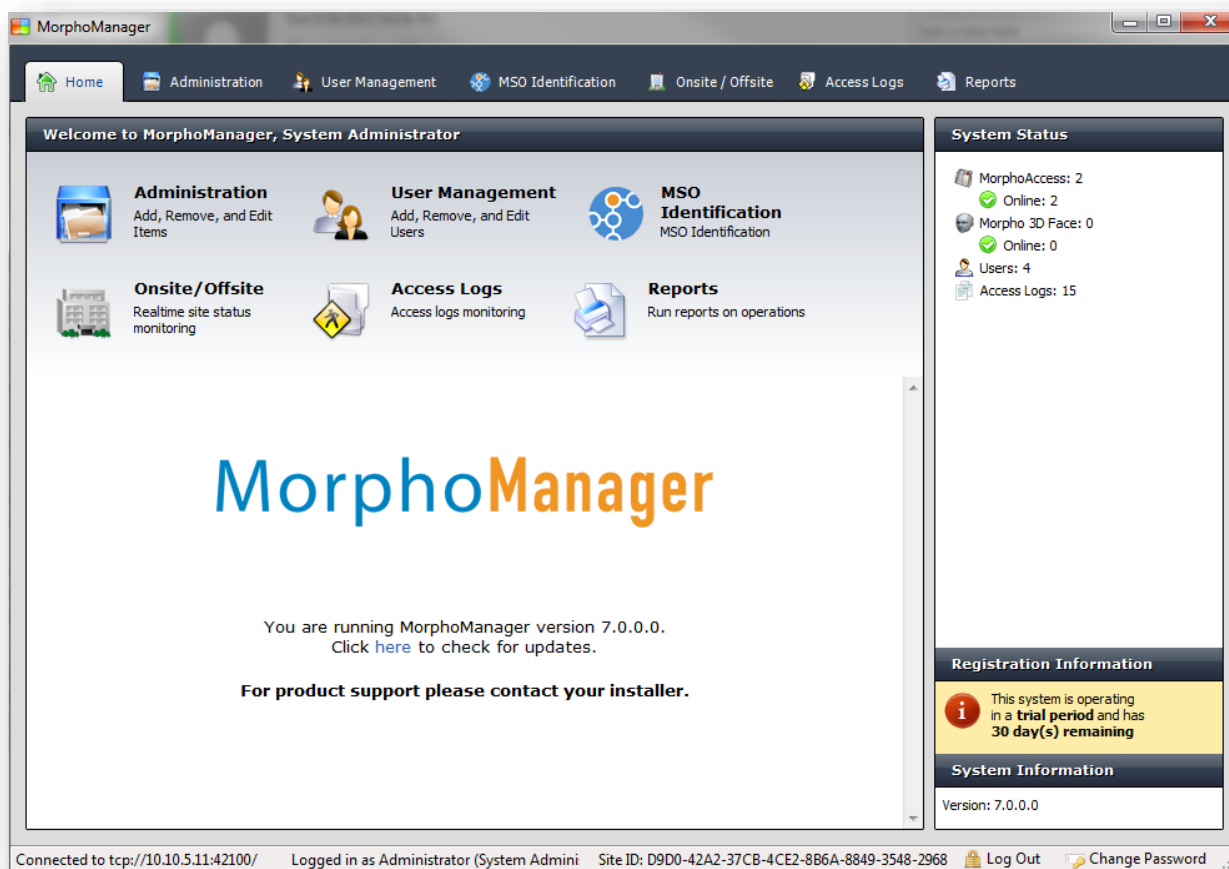
Once you have entered the correct username & password, click **Login** to login.



Home Screen

At the top of the home screen, there is a set of tabs (**Home, Administration, User Management, MSO Identification, Onsite/Offsite, Access Logs, and Reports**) and a set of buttons on the home screen. Select an item to enter that section.

At the bottom of the home screen is a link to MorphoManager updates. If you have access to the internet, you will be directed to this area which will be updated with news and information regarding MorphoManager patches and important messages.



The right hand side of the screen displays the system status and system information. System status contains a count of the total number of Biometric Devices and their current status. It also contains a count of the total number of users within the system and the total number of access logs. System Information contains the installed version number, and your server serial code.

Administration

The administration section is used to configure and setup MorphoManager. Error and event logs are also viewable in this section.



When creating or editing an item, a coloured text entry box means the information is required and must be filled in before the item can be finished and saved.

Operator

An operator is a person who uses the MorphoManager Client software. Operators are the only people who can login to the MorphoManager application. The Administrator operator has full access to all functions. Other operators with limited rights can be created.



In the panel to the right, you will see that a default Operator has been created as the System Administrator. This operator cannot be deleted or modified. This operator has access to every part of Bio Manager and so keeping the password for this user secure is essential.

Creating a new Operator

Select the **Operator** section on the left and click **Add**

Screen 1 – Operator Details

Enter the details for this Operator

Username:

First name:

Middle name:

Last name:

Job title:

Authentication method: Native username\password

Administrator: (Check to set full privilege)

Reset password: (Check to reset password)

Password:

Confirm password:

Active directory domain:

Back Next Finish Cancel

Username:

This will be entered at the login screen (must be greater than 4 characters).

- First / Middle / Last Name:** The first, middle and last name of the operator being added (First and Last names are mandatory fields).
- Job Title:** The job function that this operator performs.
- Authentication Method:** There are two methods for password authentication.
- Native Username / Password:** This method uses the username and password entered in this screen.
- Active Directory Integration:** This method uses the Windows Active directory to authenticate passwords. The username must match an existing user in the active directory. The active directory domain must be specified to use this option.
- Administrator:** Select this option to provide full administrator rights to this user (not recommended).

Screen 2 – Operator Roles

Select the Operator Roles this operator will be allowed to perform. More than one Operator Role can be selected and the Operator will have access to all of the functions that the roles allow.

Operator role	Grant
Access Logs Monitor Operator	<input type="checkbox"/>
BioBridge Enrollment Operator	<input type="checkbox"/>
MSO Identification Operator	<input type="checkbox"/>
Onsite/Offsite Monitor Operator	<input type="checkbox"/>
Reports Operator	<input type="checkbox"/>
User Management Operator	<input type="checkbox"/>

Navigation buttons: Back, Next, Finish, Cancel

Key Policy

This section allows the setting of Contactless Card keys and whether they are stored in an encrypted or unencrypted format.

Creating a new Key Policy

Select the **Key Policy** section of Administration and click **Add**.

Screen 1 – Key Policy Details

Enter details for the Key Policy

Name:

Description:

Security Mode:

- Name:** Name the policy anything up to fifty characters.
- Description:** Give the policy a description of up to one hundred characters.
- Security Mode:** Can be either Recommended or Extreme. Recommended is set by default. Recommended mode uses a known key and is unencrypted. Extreme mode is encrypted, uses a user defined key, and is not recoverable if it is forgotten.

Screen 2 – MIFARE Classic Key Settings

Set the keys for MIFARE Classic on this screen.

MIFARE Classic Key Settings

Start Write Sector:

Read/Write Keys:

Sector Number	Key A	Key B
0	FFFFFFFFFFFF	FFFFFFFFFFFF
1	FFFFFFFFFFFF	FFFFFFFFFFFF
2	FFFFFFFFFFFF	FFFFFFFFFFFF
3	FFFFFFFFFFFF	FFFFFFFFFFFF
4	FFFFFFFFFFFF	FFFFFFFFFFFF
5	FFFFFFFFFFFF	FFFFFFFFFFFF
6	FFFFFFFFFFFF	FFFFFFFFFFFF
7	FFFFFFFFFFFF	FFFFFFFFFFFF

Screen 3 – MIFARE DESFire Key Settings

Set the keys for MIFARE DESFire on this screen.

MIFARE DESFire Key Settings

Mifare DESFire (3DES)

Master Key: (as hex values)

Application Key: (as hex values)

Read Key: (as hex values)

Mifare DESFire EV1 (AES)

Master Key: (as hex values)

Application Key: (as hex values)

Read Key: (as hex values)

- Disable Morpho Key Derivation on Master Key:
- Disable Morpho Key Derivation on Application Key (Only Available for SIGMA, SIGMA Lite, and SIGMA Lite+)
- Do Not Authenticate With Master Key:

Screen 4 – iClass Key Settings

Set the keys for iClass on this screen.

iClass Key Settings

Start reading from block: (for 16K/2 cards)

Start reading from page: (for 16K/16 cards)

- Use HID iClass Factory Keys

Screen 5 – Bioscrypt 4G Site Keys

Bioscrypt 4G Site Keys

You can allow smart cards (MIFARE / iClass) encoded with SecureAdmin or SecureAdmin Lite to be read by MorphoAccess SIGMA family devices by specifying the Primary and Secondary Site Keys. You can choose to enter the keys manually below, or click "Import" to load the keys from a Site Key file generated by SecureAdmin or SecureAdmin Lite.

Primary site key:

Secondary site key:

Enable hashing

DESFire AID:

DESFire FID:

iClass Page Offset:

iClass Book Number:

iClass Page Layout:

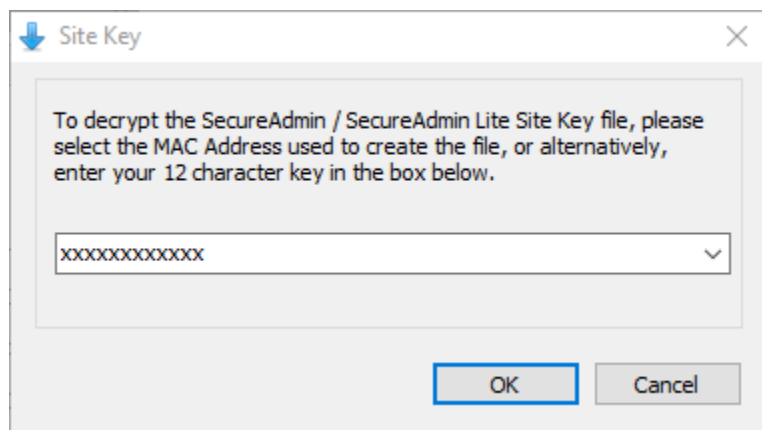
MiFare Kb Number:

MiFare Key Policy:

You can allow smart cards (MiFare/iClass) that have been encoded with Secure Admin or Secure Admin Lite to be read by the MA Sigma family of devices. You can enter the site keys manually, if they are known, or you can import the site key file that was generated in Secure Admin or Secure Admin Lite.

The device parameters on this screen will be overwritten when you use an Advanced Biometric Device Profile.

When importing a site key file, you will need to specify a “code” to unlock the site key file. Generally Secure Admin uses the MAC address of the PC to lock this file. You can either select your MAC address from the dropdown list or enter the 12-character key that was used during the creation of the file. This 12-character “code” needs to match the code used during the file creation.



“Allow Secure Admin Cards” needs to be turned on/off in the Biometric Device Profile.

Screen 6 – Certification Management

The Certificate Management page allows viewing and managing certificates bound to the Key Policy. It allows for adding new certificates or deleting existing ones.

Add a Certificate:

Add a Certificate

Certificate File:	<input type="text"/>	<input type="button" value="Browse"/>
Certificate Type:	<input type="text" value="PC"/>	<input type="button" value="v"/>
Certificate Password:	<input type="text"/>	

After clicking **Add** on the main Certification Management screen, the screen above will appear. Click **Browse** and find the Certification File to be utilized. Next, choose the Certificate Type (either PC or MA) to be utilized. Lastly, enter the mandatory Certificate Password. Click **Next** to return to the management page.



Only ONE PC certificate is allowed to be stored on the Key Policy. Any number of MA certificates can be stored on the Key Policy.

Lock & Unlock

The Lock & Unlock functions in Key Policy will only apply to Key Policies that have a Security Mode of “Extreme”. If the Status is Locked, the Unlock operation will be enabled. This will allow the ability to specify the user defined key. Which will be sent back to the Server to decrypt the Key Policy data for that Key Policy. If the data can be successfully decrypted, the status will be returned as Unlocked.

If the status is Unlocked, the Lock operation will be enabled. This will prompt for the user defined key, which once given will be sent to the Server to lock the Key Policy. The user defined key will be qualified to ensure it's a valid key. If it is, it will clear unencrypted data from the Server. The Key Policy cannot be read again until the Key Policy is unlocked.

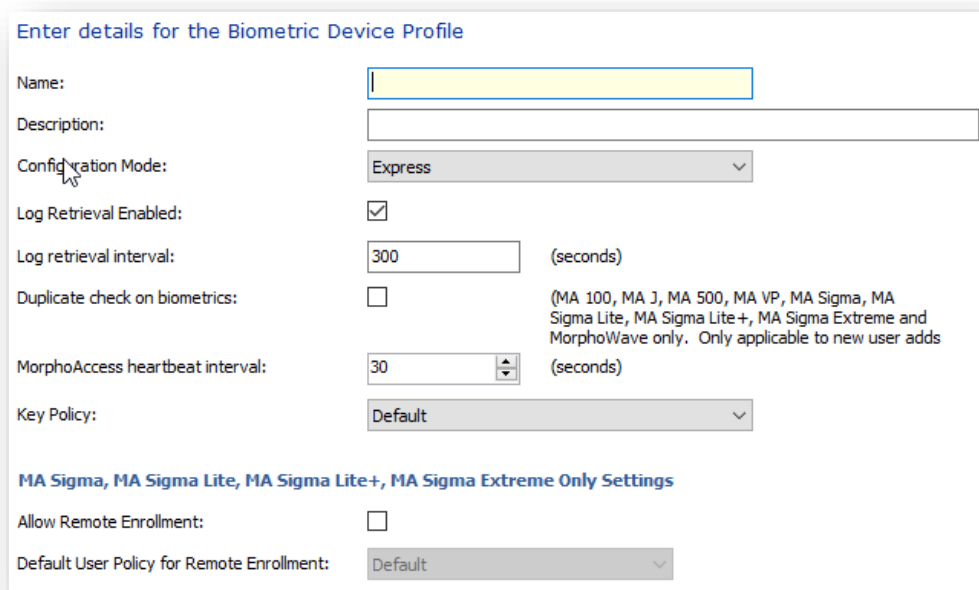
Biometric Device Profile

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.

Creating a new Biometric Device Profile (Express)

Select the **Biometric Device Profile** section of Administration and click **Add**.

Screen 1 – Configuration Details



Enter details for the Biometric Device Profile

Name:

Description:

Configuration Mode: Express

Log Retrieval Enabled:

Log retrieval interval: 300 (seconds)

Duplicate check on biometrics: (MA 100, MA J, MA 500, MA VP, MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme and MorphoWave only. Only applicable to new user adds)

MorphoAccess heartbeat interval: 30 (seconds)

Key Policy: Default

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

Allow Remote Enrollment:

Default User Policy for Remote Enrollment: Default

Name: Name the profile anything up to fifty characters.

Description: Give the profile a description of up to one hundred characters.

Configuration Mode: Can be either Express, Advanced, or External, but in this example **Express** is selected.

Note: It is possible to create a BDP in Express mode, then convert it to Advanced mode: all settings from Express mode are maintained. You may need to set additional parameters available in Advanced mode.

Log Retrieval Enabled: When this option is selected downloading logs from individual biometric devices is supported. This is the default functionality. If not selected, retrieving logs from devices is disabled which allows for third party products to retrieve device logs rather than MorphoManager. Realtime logging is not affected.

Log Retrieval Interval: Each Biometric Device is periodically polled to collect any new data and remove stored data from memory. This is the amount of time between each polling sequence. The default is 300 seconds.

Duplicate Check on Biometrics: When turned on this will check users when being enrolled for duplicate fingerprints in the system.

Morpho Access Heartbeat Interval: This will determine how often the system checks to see if the Biometric Devices are online.

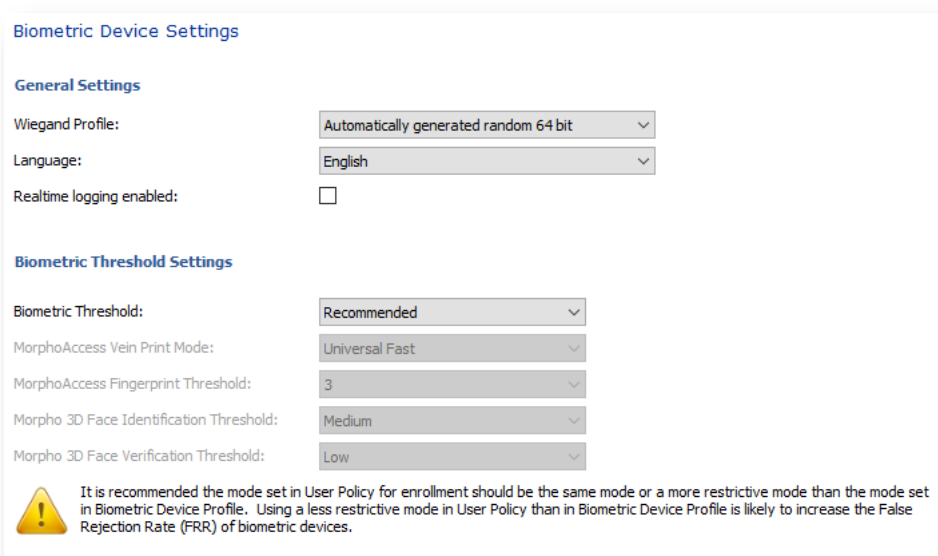
Key Policy: Select the Key Policy to be utilized on the Biometric Device.

Allow Remote Enrollment: Allows users to be enrolled on selected MA Sigma. Once a user is enrolled on a device, the software will retrieve the user from the device, be inserted into the MorphoManager database, and then distributed to any other Sigma's as per User Policy settings.

Default User Group For Remote Enrollment: Remotely enrolled users will be placed in the User Policy selected.

Screen 2– Biometric Device Settings

These values determine the cut off point for a biometric presentation to match with a stored template. A higher value will lead to more false rejections for people with lower quality fingerprints. Lowering the value allows people with lower quality fingerprints to be authenticated, but if the value is too low there is a possibility of a false acceptance. This is only enabled when the Biometric Device type has been detected.



General Settings:

Wiegand Profile: Select the Wiegand Profile to be utilized on the Biometric Device.



If you are utilizing the Wiegand output on the Biometric Devices, you will need to set the Wiegand Profile for the Biometric Device(s) here. The Wiegand Profile you choose for your devices should match the one being utilized for your users which is set in the User Policy section of this manual.

Language: Choose the language you wish to use on your Biometric Device display screen.

Realtime Logging Enabled: Enable this check box to have access logs sent from the biometric device to MorphoMnanager in real time. Logs are sent instantly for every finger presentation. By default, this setting will be disabled. It can be enabled only after configuring the settings in System Configuration.

*The port used as the server listening port will need to be opened in your firewall settings.

Biometric Threshold: The default is Recommended. However, it can be set to Low, High, Very High, and Custom. Choosing the Custom setting will allow you to set individual threshold properties for the four device types greyed out in the screenshot above. For further detail on the Vein/ Print mode options please see the User Policy – Screen 2 section of the manual..



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 Policy. 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.

Screen 3 - Multi-Factor Mode Settings

Multi-Factor Mode Settings

Multi-Factor Mode:

Contactless Smart Card Mode:

Morpho 3D Face Multi-Factor Mode

Mode:

MorphoAccess 100, 500, J, VP Multi-Factor Mode

Mode:

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

Biometric:	<input checked="" type="checkbox"/>	Mifare Classic:	<input type="checkbox"/>
Proximity Card:	<input type="checkbox"/>	Mifare DESFire:	<input type="checkbox"/>
Wiegand In:	<input type="checkbox"/>	Mifare DESFire EV1:	<input type="checkbox"/>
Keypad:	<input type="checkbox"/>		
HID iClass:	<input type="checkbox"/>		
HID iClass-SE PACS Data:	<input type="checkbox"/>		
HID iClass-SEOS PACS Data:	<input type="checkbox"/>		
Smart Card Serial Number:	<input type="checkbox"/>		

This area dictates the matching mode used by the Biometric Devices. This is only enabled when the Biometric Device type has been detected.

Multi-Factor Mode:

There are ten individual options and the ability to do a custom selection for each hardware family. The options are as follows:

- **Biometric Only** – Select this option if the Biometric Device is used for identification by biometrics only. With this option, a person does not have to provide any input other than the biometric utilized by that device for identification.
- **Wiegand In** – This option authenticates Wiegand Input to match against a biometric template.
- **Keypad** – This option allows the user to enter a user code or a pin number via the terminal keypad to match against a biometric template.
- **Proximity Card** – This option allows Proximity Cards to be utilized with a Proximity card capable device. Fingerprints will be stored on the device instead of card.
- **HID iClass** – This option allows HID iClass Cards to be utilized with an HID iClass card capable device.
- **Mifare Classic** – This option allows Mifare Classic Cards to be utilized on a Mifare Classic capable device

- **Mifare DESFire** – This option allows Mifare DESFire Cards to be utilized on a Mifare DESFire capable device.
- **Mifare DESFire EV1** – This option allows Mifare DESFire Cards to be utilized on a Mifare DESFire EV1 capable device. This can only be utilized on MA Sigma level devices.
- **Custom** – The Custom setting will allow you to set individual properties for each of the three hardware families (The Morpho 3D Face, MorphoAccess 100, 500, J, VP, MA SIGMA, MA SIGMA Lite and MA Sigma Lite +) which are greyed out in the screenshot above.
- **HID iClass SEPACS Data** – Users may be identified/authenticated using the pre-programmed HID PACS data of a HID iClass / iClass SE contactless card and a HID iClass / iClass SE compatible biometric device.
- **HID iClass SEOSPACS Data** – Users may be identified/authenticated using the pre-programmed HID PACS data of a HID iClass Seos contactless card and a HID iClass Seos compatible biometric device.
- **Smart Card Serial Number** – Users may be identified/authenticated using the pre-programmed card serial number on a contactless smartcard and a biometric device capable of reading smart contactless cards (MIFARE/DESFire/iClass/etc.).



It is always recommended to use Biometric Only mode. However, depending on how the MorphoAccess will be used any of the above options can be selected.

Screen 4 – Access Control Mode Settings

Access Control Mode Settings

Access Control Mode: Integrated

Wiegand Out Enabled:

Panel Feedback Mode: None

Panel Feedback No Response Timeout: 3000

Relay Enabled:

Relay Duration: 3000

Push To Exit Enabled:

Push To Exit Duration: 3000

Duress Wiegand Mode: Reversed

Duress Wiegand Profile: Automatically generated random 64

Back Next Finish Cancel

This area sets the properties for Access Control on your Biometric Devices.

Access Control Mode: There are four modes available, None, Integrated, Stand-alone, and Custom. The default here is Integrated, in Integrated you can set the Panel Feedback Mode and Panel Feedback No Response Timeout properties. In Stand-alone mode you can set the properties on Relay Enabled, Relay Duration, Push to Exit Enabled, and Push to Exit Duration. And, lastly in Custom mode you can set all properties.

Wiegand Out Enabled: This will determine whether or not your biometric device will output a Wiegand value.

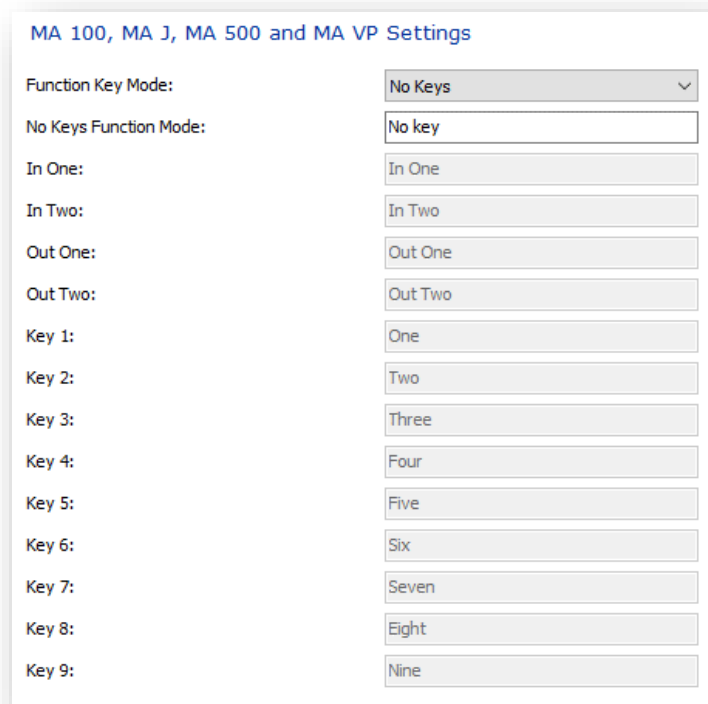
Panel Feedback Mode: Allows you to choose between LEDIN and RS485.

Panel Feedback No Response Timeout: This value will determine the length of response time allowed from the Access Control Panel.

Relay Enabled: Each Biometric Device has an on board relay that can be used to control an external device on successful presentation of a fingerprint. Use this option to activate the relay when a user is authenticated.

- Relay Duration:** If the relay is activated, this value will determine the length of activation time.
- Push To Exit Enabled:** This allows the Access Panel to open a door even though the user is not identified on device.
- Push to Exit Duration:** This sets the length of time the door will remain open if Push to Exit is enabled.
- Duress Wiegand Mode:** This determines whether the use of Wiegand for duress finger is Disabled, Reversed, or Custom.
- Duress Wiegand Profile:** If the Duress Wiegand Mode is Custom, this will set the Wiegand Profile to be used during presentation of a duress finger.

Screen 5 – Function Key Mode for MA 100, J, 500, and VP Family



- Function Key Mode:** This area determines what function keys, if any, will be available on a device (where applicable). Options in this drop down are No Keys, Two Keys, Four Keys, or Nine Keys to be displayed on device. Each key enabled in the list of keys can be renamed to meet individual needs for events in Time & Attendance and Access Log records.

Screen 6 – MA 100, MA J, MA 500 and MA VP Settings

MA 100, MA J, MA 500 and MA VP Settings

MA500 Multi Database Enabled: (Requires Xtended Licenses)

Display name encoding code page: Western Europe (Default) (ISO-8859-1) v (Applicable to MA500 series only)

Enable MA 500

Multi-database Mode:

This will allow you to enable the Multi-database mode on this family of devices if they have the proper license installed.

Display Name

Encoding Code Page:

This section allows you to set encoding for the display name for downloading to MA2G devices. Your choices will be:

- Western Europe (Default) (ISO-8859-1)
- Central Europe (ISO-8859-2)
- Southern Europe (ISO-8859-3)
- Baltic (ISO-8859-4)
- Cyrillic (ISO-8859-5)
- Arabic (ISO-8859-6)
- Greek (ISO-8859-7)
- Hebrew (ISO-8859-8)
- Turkish (ISO-8859-9)
- Latin 9 (ISO-8859-15)

Screen 7 – MA Sigma, Sigma Lite, Sigma Lite +, & MorphoWave Settings

MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme, MorphoWave Settings

Face Detection Settings

Face Detection Mode: Disabled

Face Logging Mode: Rejected Only

User Experience

Volume: 70

Enable idle timeout

Start video playback after: 120 (seconds)

Turn off screen

Turn off screen after: 120 (seconds)

Turn off fingerprint sensor when screen turns off

Keyboard Mode: QWERTY

Show Administration Menu:

Show Date and Time:

Face Detection Mode: Allows you to set the Sigma units to capture a photo when someone is presenting to the device (this works in conjunction with the Face Logging Mode). There are four individual options:

- **Disabled** – Use this option if you want to completely turn off Face Detection photo capture.
- **None** – Will take a 1 photo for the log whether or not a face is detected.
- **Optional** – Takes a series of pictures and chooses the best face it detects out of them for the log. However, if the user is rejected (biometric mismatch) AND it doesn't detect a face, no photo will be used.
- **Mandatory** – Takes a picture in all scenarios (rejected or accepted presentation).

Face Logging Mode: This determines whether or not Rejected, Accepted, or Rejected and Accepted presentations to the Sigma are logged. This works in conjunction with Face Detection Mode.

Volume: Set the device volume level to anything from 0-100 for all Sigma family of devices and the Morpho Wave.

Enable idle timeout: Allows the following to be set on the Sigma and Morpho Wave devices (video capacity does not exist for the Lite+):

- **Start video playback after** – Set the amount of time the device is idle before the designated video on the device for idle time starts.
- **Turn off screen** – When enabled it sets the amount of time that the video will run before the screen will go blank. If disabled, the video will continue to run.
- **Turn off fingerprint sensor when screen turns off** – When enabled it will turn off the fingerprint sensor on the device at the same time the screen is turned off. If disabled, the fingerprint sensor will continue to remain lit.

Keyboard Mode: Select whether a QWERTY or AZERTY keyboard will be used on the device(s).

Screen 8 – MA Sigma, Sigma Lite, Sigma Lite +, & MorphoWave Settings (continued)



SecureAdmin Cards: When enabled, you will be able to use smart cards that have been encoded in Secure Admin or Secure Admin Lite. This setting only pertains to the Sigma family of devices. You will need to set the Secure Admin Site Keys in the Key Policy menu.

Enable Finger Authentication Rule: Enables the ucc.finger_bio_auth.rule Sigma parameter. When enabled, the user will be prompted to present a fingerprint as verification.

Access Schedules: When enabled, the access schedule functionality will be switched on for MA Sigma, Sigma Lite, Sigma Lite+ and Morpho Wave.



If this system is an upgrade from MorphoManager 9.6.4 or lower, you will need to manually rebuild all MA Sigma devices after enabling the Access Schedules option.

Screen 9– MA Sigma, Sigma Lite, Sigma Lite +, & MorphoWave Settings (continued)

MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme, MorphoWave Settings

Device Password

Enable Managing Device Password

Device Password:

Secure Communications Mode

Secure Communications Mode: Selecting this option will instruct MorphoManager to attempt to connect to MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme and MorphoWave devices assigned this Biometric Device Profile using SSL/TLS. If each device is not configured correctly with the proper certificates present in the Key Policy, MorphoManager will not be able to connect to those devices.

Device Password: When enabled a numeric non-default password can be set for the device(s). The password can be between four to eight digits long. Once the non-default password has been set, the default password will need to be manually re-entered here to reverse the change.

Secure Communications Mode: Turn this on to use SSL communications between the Biometric Device and the MorphoManager Server.



When using SSL Communications, the port on the Biometric Device will need to be changed from the default which does not use SSL. This can be edited in Biometric Device.

Screen 10 – Function Key Mode for MA Sigma, MA Sigma Lite, MA Sigma Lite+ and Morpho Wave Key Mode Settings

MA Sigma, MA Sigma Lite+, MA Sigma Extreme, MorphoWave Key Mode Settings

Function Key Mode: v

No Keys Function Mode:

Key 1: <input style="border: none; background-color: #ccc; width: 100%;" type="text" value="IN"/>	Key 9: <input style="border: none; background-color: #ccc; width: 100%;" type="text" value="Nine"/>
Key 2: <input style="border: none; background-color: #ccc; width: 100%;" type="text" value="OUT"/>	Key 10: <input style="border: none; background-color: #ccc; width: 100%;" type="text" value="Ten"/>
Key 3: <input style="border: none; background-color: #ccc; width: 100%;" type="text" value="IN DUTY"/>	Key 11: <input style="border: none; background-color: #ccc; width: 100%;" type="text" value="Eleven"/>
Key 4: <input style="border: none; background-color: #ccc; width: 100%;" type="text" value="OUT DUTY"/>	Key 12: <input style="border: none; background-color: #ccc; width: 100%;" type="text" value="Twelve"/>
Key 5: <input style="border: none; background-color: #ccc; width: 100%;" type="text" value="Five"/>	Key 13: <input style="border: none; background-color: #ccc; width: 100%;" type="text" value="Thirteen"/>
Key 6: <input style="border: none; background-color: #ccc; width: 100%;" type="text" value="Six"/>	Key 14: <input style="border: none; background-color: #ccc; width: 100%;" type="text" value="Fourteen"/>
Key 7: <input style="border: none; background-color: #ccc; width: 100%;" type="text" value="Seven"/>	Key 15: <input style="border: none; background-color: #ccc; width: 100%;" type="text" value="Fifteen"/>
Key 8: <input style="border: none; background-color: #ccc; width: 100%;" type="text" value="Eight"/>	Key 16: <input style="border: none; background-color: #ccc; width: 100%;" type="text" value="Sixteen"/>

Function Key Mode: This area determines what function keys, if any, will be available on a MA Sigma, MA Sigma Lite and MA Sigma Lite +, and Morpho Wave Key Mode Settings. Options in this drop down are No Keys, Four Keys, or Sixteen Keys to be displayed on device. Each key enabled in the list of keys can be renamed to meet individual needs for events in Time & Attendance and Access Log records. In Sixteen Keys mode any key name field left blank will not show as a button on the device screen.

Screen 11 – MA Sigma, MA sigma Lite+, and MorphoWave Custom Media Files

MA Sigma, MA Sigma Lite+, MA Sigma Extreme, MorphoWave Custom Media Files

Custom media files

Add
 Edit
 Delete

File Type	Sub type
Picture	None

This wizard screen allows the addition of custom Video, Picture, and Audio files to be used on an MA Sigma and MA Sigma Lite + Custom Media Files. Applying the Biometric Device Profile containing these files to the Biometric Device will place the files onto that device.


Screen 12 – MA Sigma Custom Parameters

MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme, MorphoWave Custom Parameters

Custom Parameters

Add Edit Delete

Name	Value
audio.volume	25

 The parameters on this page are not validated and sent directly to all MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme and MorphoWave devices assigned this Biometric Device Profile, as is.

Clear All

The MA Sigma Custom Parameters screen allows the user to specify parameters to be sent directly to any MA5G device associated to the Biometric Device Profile. The parameters are not verified prior to being sent to the device and will override default parameters.

To enter a custom parameter click the Add button then provide the parameter name and its value and click Next.

MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme, MorphoWave Custom Parameter

Name:

Value:

Individual parameters can be edited or deleted by selecting the appropriate button. To remove all existing parameters select the Clear All button.

Screen 13 – Morpho 3D Face Settings

Morpho 3D Face Settings

Capture Settings

Enrollment capture timeout: 30 (seconds)

Authentication capture timeout: 15 (seconds)

Preview image type: Color Image

Misc Settings

Onscreen message timeout: 5 (seconds)

Enrollment Capture Timeout: Time the device will attempt to capture a 3D Face during enrollment (default 30 seconds).

Authentication Capture Timeout: The maximum time the device will attempt to authenticate/verify a user in verification mode.

Preview Image Type: Specifies whether to show the enrollment preview image in color or 3D face surface mode.

Onscreen Message Timeout: The amount of time that an on screen messages will be shown to the user.

Screen 14 – Video Phone Server Settings

To utilize the Video Phone features of the MA Sigma only, you will need to add your server here. Adding a Video Phone Server is not mandatory for creating a Biometric Device Profile and you can click **Finish** on this screen with or without adding the Video Phone Server.

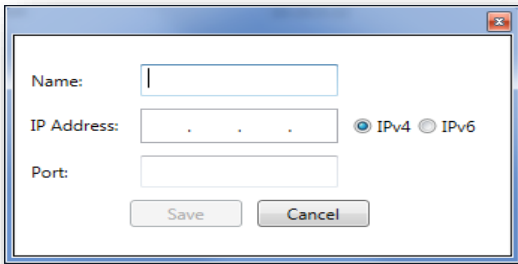
Video Phone Server Settings

Video Phone Servers

Add Edit Delete

Name	IP Address	Port
Front Desk	10.10.5.12	5060

Click **Add** to add the Name, IP Address and Port of your Video Phone Server.



A screenshot of a configuration dialog box. The dialog has a title bar with a close button. It contains three input fields: 'Name' with a single character, 'IP Address' with three dots and radio buttons for 'IPv4' (selected) and 'IPv6', and 'Port' which is empty. At the bottom are 'Save' and 'Cancel' buttons.

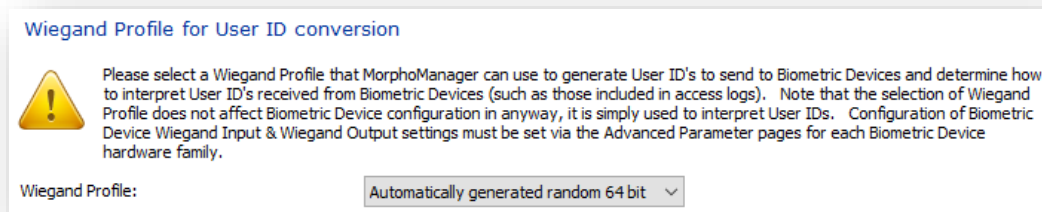
Click **Save** when finished.

Creating a new Biometric Device Profile (Advanced)

Select the **Biometric Device Profile** section of Administration and click **Add**. On Screen 1 you will select **Advanced** from the “Configuration Mode” drop down.

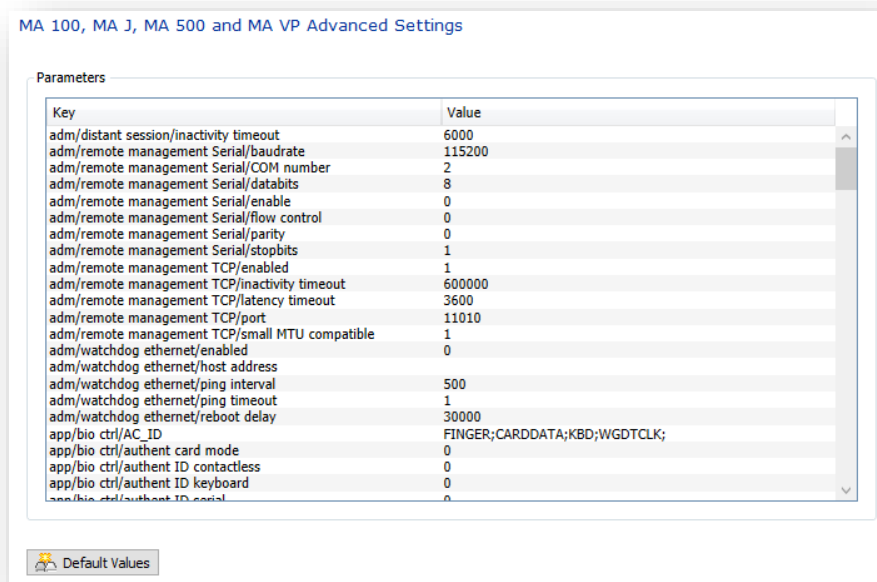
The Advanced Profile Screen 2 allows you to configure the various parameters for the Morpho Access 100, 500, J, and VP.

Screen 2- Wiegand Profile for User ID Conversion



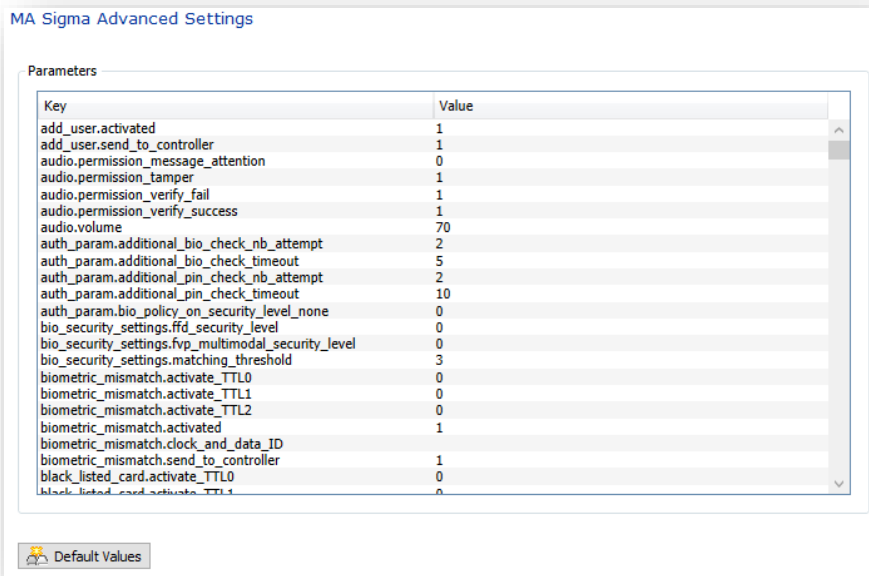
Select the Wiegand Profile to be utilized on the Biometric Device.

Screen 3 - MA 100, MA J, MA 500 and MA VP Advanced Settings



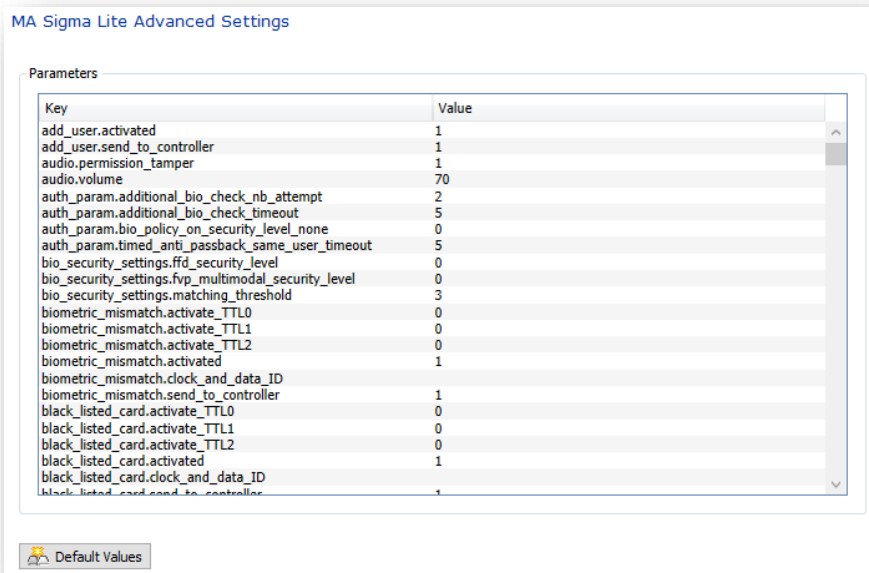
Parameters available for MA2G devices. If you have made changes to the parameters and wish to return to the original defaults on this screen, you can simply click the **Default Values** button.

Screen 4 – MA Sigma Advanced Settings



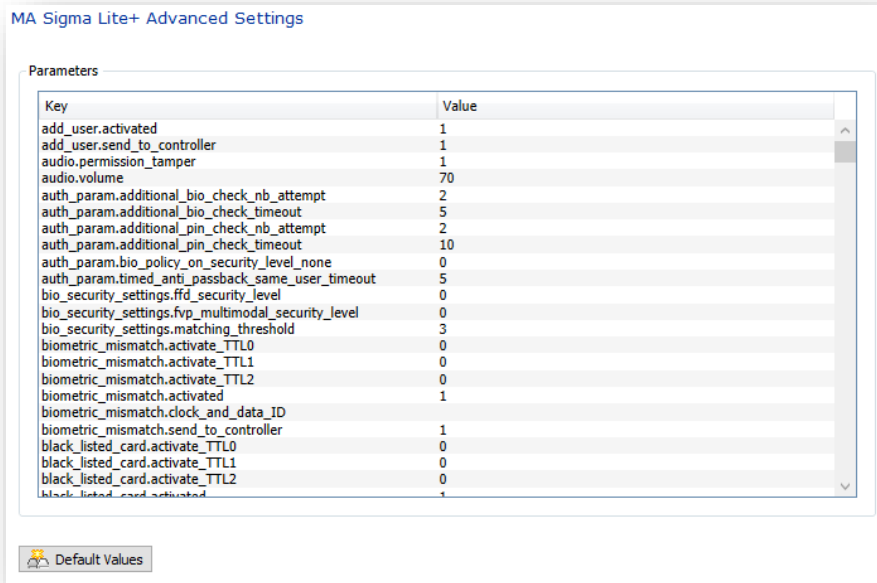
Parameters available for MA Sigma devices. If you have made changes to the parameters and wish to return to the original defaults on this screen, you can simply click the **Default Values** button.

Screen 5 –MA Sigma Lite Advanced Settings



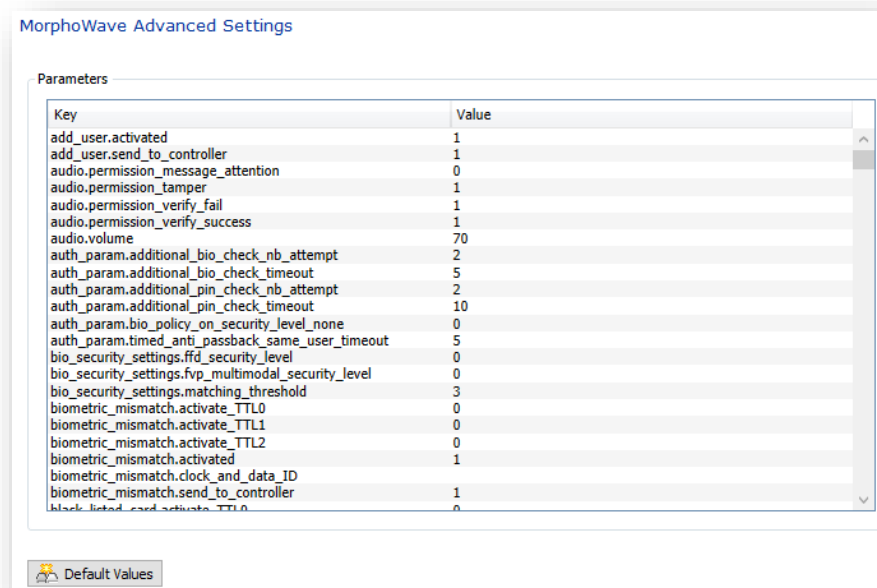
Parameters available for MA Sigma Lite devices. If you have made changes to the parameters and wish to return to the original defaults on this screen, you can simply click the **Default Values** button.

Screen 6 –MA Sigma Lite+ Advanced Settings



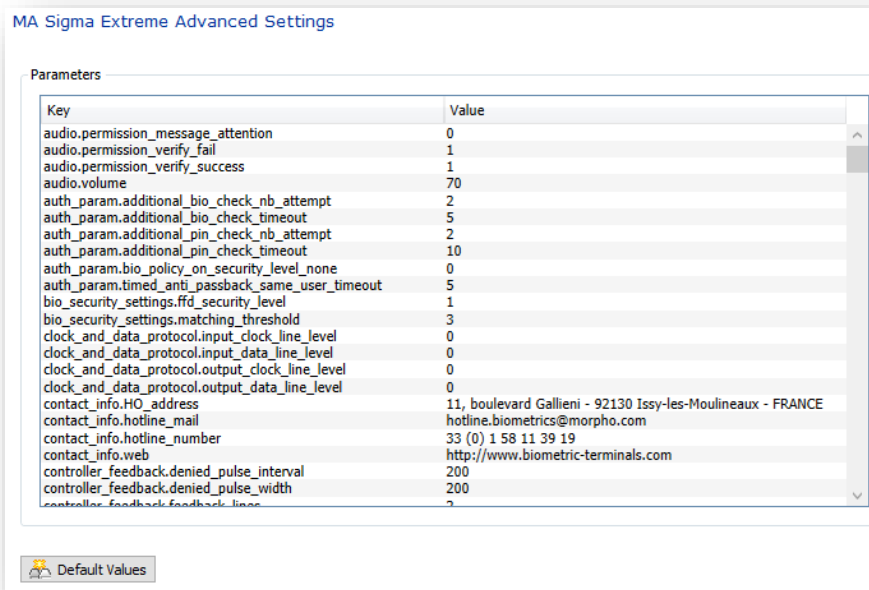
Parameters available for MA Sigma Lite+ devices. If you have made changes to the parameters and wish to return to the original defaults on this screen, you can simply click the **Default Values** button.

Screen 7 – MorphoWave Advanced Settings



Parameters available for MorphoWave. If you have made changes to the parameters and wish to return to the original defaults on this screen, you can simply click the **Default Values** button.

Screen 8 – MA Sigma Extreme Advanced Settings



Parameters available for MA Sigma Extreme. If you have made changes to the parameters and wish to return to the original defaults on this screen, you can simply click the **Default Values** button.



Information for the wizard screens 9 – 13 can be found in the section for **Creating a new Biometric Device Profile (Express)**.

Screen 14 – Morpho 3D Face Settings

Morpho 3D Face Settings

Capture Settings

Enrollment capture timeout: 30 (seconds)

Authentication capture timeout: 15 (seconds)

Preview image type: Color Image

Threshold Settings

Morpho 3D Face Identification Threshold: Medium

Morpho 3D Face Verification Threshold: Low

Misc Settings

Onscreen message timeout: 5 (seconds)

In Advanced mode, Morpho 3D Face includes Threshold Settings which are available on this screen.

Creating a new Biometric Device Profile (External)

Enter details for the Biometric Device Profile

Name: Advanced

Description:

Configuration Mode: External

Realtime logging enabled:

Log retrieval interval: 300 (seconds)

Language: English

Selecting External for your Configuration Mode allows you to set all parameters on device or via external software that interfaces with the Biometric Device parameters. When selecting External mode this will be the only wizard screen you will utilize.

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 Morpho Wave, and the Morpho Tablet Terminal.

Create a Biometric Device

Select the **Biometric Device** section of Administration and then click **Add** in the toolbar.

Enter the details for this Biometric Device

Name: MA Sigma Exteme

Description:

Location:

Asset ID:

Export Value:

Time Zone: (UTC-05:00) Eastern Time (US & Canada) ▾

Hardware Family: MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extren ▾

Serial Number:

Hostname \IP Address: 100.100.100.100

Port: 11010

Biometric Device Profile: Default ▾

Include in Time & Attendance Exports:

Change User Onsite / Offsite Status:

Onsite Key: No Key ▾

Offsite Key: No Key ▾

Name: The name of the Biometric Device.

Description: A description of the Biometric Device.

Location: The installed location of the Biometric Device.

Export Value: This value is typically used for Access log exporting when the MorphoManager data needs to be exported to a third-party payroll package. It can have a maximum of 20 characters. When the access logs are exported, the value specified here will be used as the Biometric Device name in the output exported file. This again depends on the particular requirements of the payroll package and the access log exporter that is configured in the System configuration under T&A General settings.

Time Zone: It is important that this field is entered correctly as it will affect the time displayed on the Biometric Device and in which time zone access logs are recorded.

Hardware Family: Corresponds to the model of the Biometric. As mentioned above 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, Sigma Lite, MA Sigma Lite + and MA Sigma Extreme family, the Morpho 3D Face, the MorphWave, and the Morpho Tablet Terminal.

Serial Number: This field is required for the Morpho Tablet Terminal device, but not needed for the other hardware families. The serial number can be found on the device under Settings>About Tablet>Status.

Hostname \ IP address: This value is critical. Enter the IP address of the selected Biometric Device.



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. An IP Address is not needed for the Morpho Tablet Terminal hardware family.

Port: This is the default that MorphoManager software is expecting.

Biometric Device Profile: This will allow a common settings and parameters profile to be set for the device added. The profile itself is created in the Biometric Device Profile section of Administration.

Include in Time & Attendance Exports: Enable if the gathered data is to be sent to a Payroll or Rostering package.

Change User Onsite/Offsite Status: Enable if Onsite/Offsite events are to be recorded.

Onsite Key: Determines which function key on the device will be utilized to set a user Onsite.

Offsite Key: Determines which function key on the device will be utilized to set a user Offsite.

After all information has been entered click **Finish** to save the changes or **Cancel** to discard the changes. You will now see the new Biometric Device in the window and its status will be Online, provided the PC and device are correctly connected and configured. The Tasks column shows the count of the queued or the failed tasks.

Modify a Biometric Device

To modify a Biometric Device, left click on a device and click **Edit** on the toolbar. A wizard will open showing the information entered when the Biometric Device was created. Change any of the values required and click **Finish** to save changes or **Cancel** to discard changes.

Delete a Biometric Device

Select the device to delete and click **Delete** on the toolbar. To delete a Biometric Device, you must remove ALL user policy and user access. A Biometric Device cannot be deleted if any user still has access. This ensures that all user access has been correctly revoked.

Biometric Device Status and Tasks

When viewing a list of Biometric Devices, the status column indicates the current status of each Biometric Device. Online means the Biometric Device is responding to communication requests. Offline means that the Biometric Device is not responding to communication requests. A new status, Never Connected, has been added in MorphoManager version 11 to indicate the device has never been online.

The tasks column indicates the number of tasks remaining for the Biometric Device to process. Clicking on the **Queued Tasks** and **Failed Tasks** tab in the details section allows these tasks to be reviewed. Clicking on **Logs** allows review of access logs retrieved from that Biometric Device, if this functionality is enabled.

The screenshot displays the MorphoManager web interface. The main window shows a list of Biometric Devices with the following data:

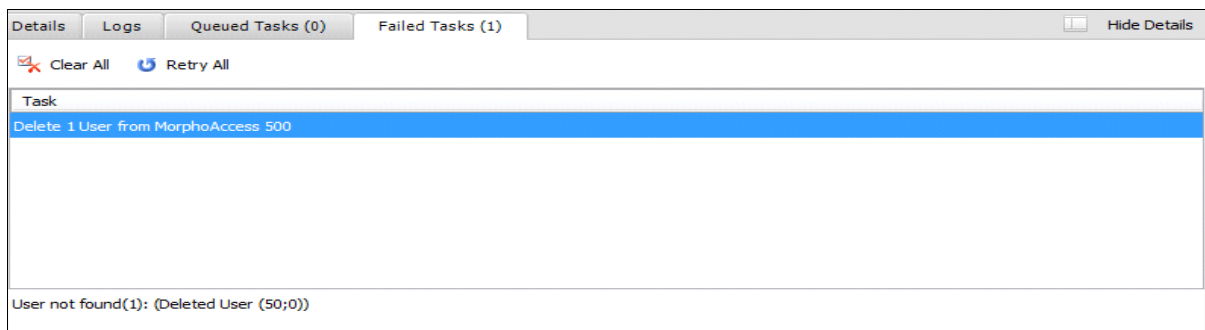
Name	Description	Location	Biometric D...	Status	Tasks
MAVP-Dual			Default	Online	1
Sigma			Default	Online	1
SigmaLite			Default	Never Connected	7

The details section for the selected 'Sigma' device shows the following information:

- Description:** MA SIGMA iClass WR
- Hardware Type:** 1431SMS0002267
- Serial Number:** 3.3.1
- Firmware version:** 10.10.214.1:11010
- Hostname\IP Address:** 1000 / 100000
- Time Zone:** (UTC-05:00) Eastern Time (US_Canada)
- Device Status:** Online

The interface also includes a navigation menu on the left with options like Operator, Key Policy, Biometric Device Profile, and a toolbar at the top with actions like Add, Edit, Delete, Refresh, Get Logs, Set Date/Time, Rebuild, Reboot, and Set Offline. The status bar at the bottom indicates the user is logged in as Administrator and provides site ID and login options.

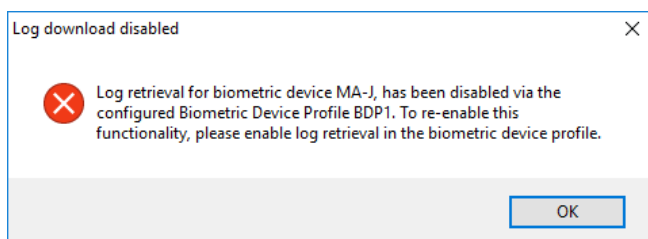
Troubleshooting and Maintenance



In the example screen above, the “Delete User” task failed. The message below explains the reason for the failed task.

Toolbar Functionality

Get Logs – This functionality is enabled by default and allows currently stored transactions from the biometric device to be downloaded into MorphoManager. Automatic retrieval occurs every 5 minutes, by default. If this functionality is disabled in the Biometric Device Profile the following message is displayed if Get Logs is clicked:









Set Date/Time – Updates the Biometric Device’s clock to the time on the server. This command is run automatically once a day at the time specified in the system configuration.

Rebuild – The rebuild function will remove all users from a Biometric Device and upload the users who are permitted access. This function should only be used if the device is not operating as expected. Unexpected behavior could occur if a device was moved from another site and contained existing users from that site. During normal operation any users who are added or deleted through user management are updated on the Biometric Device in real time.

Set Online – MorphoManager monitors and displays the status of every Biometric Device. If a device has gone offline, clicking **Set Online** will attempt to connect to the device and go online. The status of the Biometric Device will change to “Pending Online” while the connection is occurring. If there is a problem connecting to the Biometric Device the status will revert to “Offline”.

Wiegand Profiles

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 Profiles					
     					
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	

Create a Wiegand Profile

Screen 1 – Configuration Details

Enter details for this Wiegand profile

Name:

Description:

Bit Length:

Name: Name the profile anything up to fifty characters.

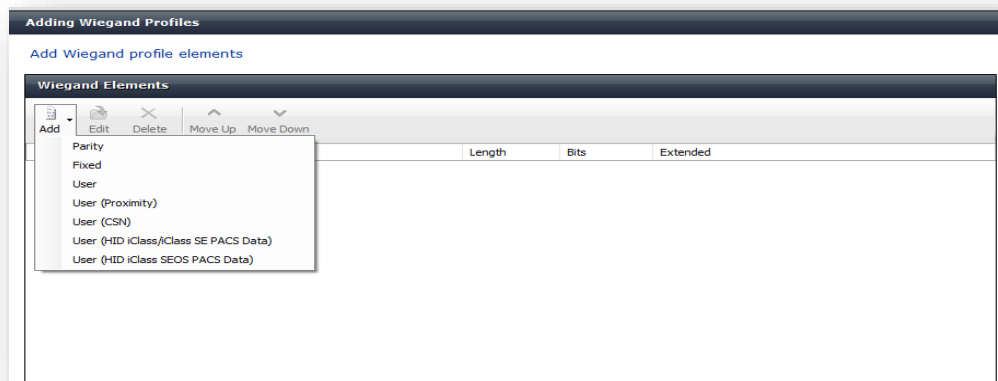
Description: Give the profile a description of up to one hundred characters.

Bit Length: Designate the overall bit length needed for your profile.

Screen 2 – Wiegand Profile Elements

On Screen 2 you will be able to add the elements needed to make up your Wiegand Profile. Click **Add** to select the element needed from the drop down. There are five element types that can be used to construct a Wiegand Profile:

- **Parity:** Indicates a single bit that is typically used for error detection. Parity is calculated over one or more bits within the entire profile and can be Even or Odd.
- **Fixed:** Indicates a value that is common to all users of this Wiegand Profile. Typical examples of fixed values are Facility/Site codes. This value is set once in the Wiegand Profile and will then be used by all users of this Wiegand Profile.
- **User:** A value that can be entered during enrollment for each user. A typical example of a User value is a User ID.
- **User (Proximity):** Similar to the User value, this value is defined during enrollment, but is read from a connected proximity card.
- **User (CSN):** Similar to the User value, this value is defined during enrollment, but is read from an ISO/IEC 14443 smart card's serial number.
- **User (HID iClass/iClass SE PACS Data):** Similar to the User value, this value is defined during enrollment, but is read from the HID iClass/iClass SE PACS (Physical Access Control System) information on the card.
- **User (HID iClass SEOS PACS Data):** Similar to the User value, this value is defined during enrollment, but is read from the HID iClass/iClass SEOS PACS (Physical Access Control System) information on the card.



Once the element has been selected the details screen for that element can be populated as in the example below. Once the screen is populated click **Next**.

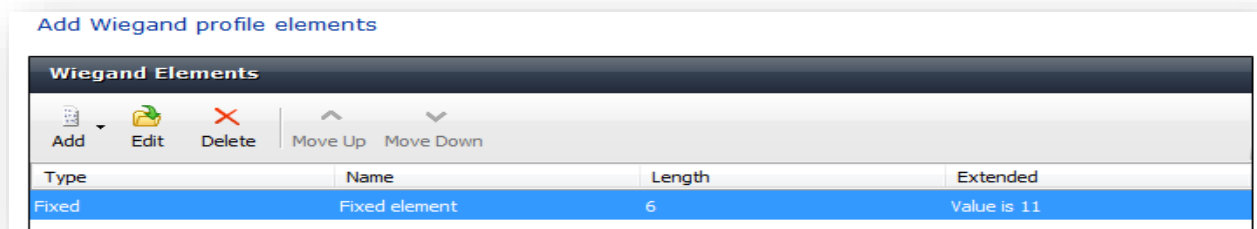
Fixed element details

Name:

Length:

Value:

You will be taken back to the Wiegand Profile element screen (below) and it will now be populated with the element you just added.



Once you have built out all of the elements needed to make up your Wiegand Profile, you can click FINISH.

User Policy

User policies are used to apply access rights and rules to all members of the group.



Users cannot exist in the database without being assigned to a User Policy. However, a User Policy can exist without having access to any Biometric Device. This can be useful for segregating users who, for security or other reasons, should not be stored on a device.

Create a new User Policy

Screen 1 – Details

Enter the details for this User Policy

Name:	<input type="text" value="Default"/>
Description:	<input type="text"/>
Access Mode:	<input type="text" value="All Biometric Devices and Clients"/>
	<input checked="" type="checkbox"/> Allow MA 500 database selection during user enrollment
Access Schedule:	<input type="text" value="24 hours, 7 days a week"/>
Extended User Details:	<input type="checkbox"/> Display extended user details
Wiegand Profile:	<input type="text" value="Automatically generated random 64 t"/>
User Authentication Mode:	<input type="text" value="Biometric (1:Many)"/>
Show Photo Capture Page:	<input checked="" type="checkbox"/>

Name:

Name of the user policy.

Description:

Description of the purpose of the user policy.

Access Mode:

This value determines the access to Biometric Devices that users in this policy will have.

All Biometric Devices and Clients: Users in this policy have access to all Biometric Devices and all Clients for MSO Identification.

Per User: Users in this policy will have access to the Biometric Device(s) specified in the User Distribution Groups selected for them in User Management and cannot be overridden. The same will take place for Clients when using MSO Identification.


Checking the Allow MA 500 database selection during user enrollment allows you to choose the section of an MA 500 where you want to add your user. The MA 500 must have an extended license for 50k users. When adding a new user, you will have a drop down menu of zero to four. This is where you decide which of the five sections of the database you want to add the user to.

Access Schedule: Any Access schedules that have been created in the Access Schedule menu (Administration / Access Schedules) will appear in this dropdown menu.

Access times will be restricted/permitted as set up in the Access Schedules menu.

Extended User Details: If enabled, additional user information such as Phone Number(s), Email, and Address can be entered for a user.

Wiegand Profile: Select the Wiegand Profile you wish to use for users in this User Policy.



The Wiegand Profile you choose for your users should match the one you utilize for your biometric access devices set in the Biometric Device Profile section of this manual.

User Authentication Mode: Designate the authentication mode you wish to utilize for user placed into this User Policy.

Show Photo Capture Page: If enabled, the Photo Capture wizard screen will be shown in User Management when adding or editing users.

Screen 2 – Details for Finger Biometric Options

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	▼
Show Finger Biometric Capture Page:	<input checked="" type="checkbox"/>	(User Authentication Mode requires templates)



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 Policy. 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.

Finger Biometric Enrollment Minimum Fingers:

Designate the minimum number of fingers that will be captured during user enrollment. Options are None, One, Two, Three, (with third as the Duress Finger), and Ten. **Please note that MA 100, MA J, MA 500, MA VP devices require a minimum of two enrolled fingers.**

Preferred Finger One:

Designate the first preferred finger for capture on the Finger Biometric Enrollment wizard screen of User Management.

Preferred Finger Two: Designate the second preferred finger for capture on the Finger Biometric Enrollment wizard screen of User Management.

Preferred Duress Finger: Designate the Duress Finger to be captured on the Finger Biometric Enrollment wizard screen of User Management.



Duress Finger can only be utilized on the Morpho Sigma, MA Sigma Lite, and MA Sigma Lite + of readers.

Vein / Print Mode: Designate the mode to be utilized during enrollment with an MSO VP. This mode must align with the Biometric Threshold settings set in the Biometric Device Profile for MorphoAccess Fingerprint Threshold. The following modes are available:

Universal Fast: Universal fast is the recommended vein/print mode. Universal fast provides the fastest biometric capture and is an excellent trade-off between security, biometric spoofing and ease of use. This mode offers the lowest failure to enroll rate. It is likely that users who experience difficulties enrolling on fingerprint only devices can be successfully enrolled on vein/print devices configured to this mode.

Universal accurate: Universal accurate is very similar to universal fast profile but with more time allowed for biometric data capture during enrollment and matching. This mode is recommended only when the biometrics of a significant number of users are difficult to enroll due to extreme conditions, such as very cold temperature and/or highly damaged fingerprints.

Anti-spoofing: Anti-spoofing provides a very high level of biometric spoofing detection. Anti-spoofing is more restrictive than universal fast and universal accurate. This mode is recommended when detection of a physical live finger is desired. This mode requires that vein network biometric data must be found under the skin of the finger. This mode is recommended when a lower False Acceptance Rate (FAR) is more important than a low Failure To Enroll (FTE) rate.

Full multimodal: Full multi-modal provides the highest level of security during biometric capture and biometric matching. Full multi-modal is the most restrictive mode. This mode requires that vein network biometric data must be found under the skin of the finger. This mode is recommended when the lowest False Acceptance Rate (FAR) is more important than a low Failure To Enroll (FTE) rate.



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 Policy. 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

Show Finger Biometric Capture Page: If enabled, the Finger Biometric Capture wizard screen will be shown in User Management when adding or editing users. It can only be disabled if the Finger Biometric Enrollment Minimum Fingers is set to None and the User Authentication Mode is not for finger biometrics.

Screen 3 – Details for Wave Biometric Options

Enter the details for wave biometric options

Wave Enrollment Minimum Hands:	<input type="text" value="None"/>
Show Wave Biometric Capture Page:	<input type="checkbox"/>

Wave Enrollment Minimum Hands: Designate the minimum number of hands that will be captured during user enrollment. Options are None, One, or Two.

Show Wave Biometric Capture Page: If enabled, the Wave Biometric Capture wizard screen will be shown in User Management when adding or editing users. It can only be disabled if the Wave Enrollment Minimum Hands is set to None.

Access Schedules

Access Schedules allow access times to be set for the Biometric Devices. Up to 58 individual Access Schedules can be created. The Access Schedules are applied to users via the User Policy section of MorphoManager. Thus, a user’s access via the Sigma family of devices will be governed by the Access Schedule set on their User Policy.

Create an Access Schedule

Screen 1 – Details

Adding Access Schedules

Enter details for the MA Sigma Access Schedule

Name:

Description:

Name: Name of the Access Schedule

Description: Description of the Access Schedule

Screen 2 – MA Sigma, Sigma Lite, Sigma Lite+ and Morpho Wave access schedules

This section will create Access Schedules pertaining to the MA Sigma, Sigma Lite, Sigma Lite+ and Morpho Wave devices. They allow for one or two time periods of access to be set per day on the devices. Each time period per day can be set up in increments of fifteen minutes.

From this screen set the times needed in fifteen minute increments. If a day is not set (left blank), no access will be allowed for users of the Access Schedule on that day.

The [Access Schedules setting](#) (page 38) needs to be enabled in the Biometric Device Profile menu for Sigma, Sigma Lite, Sigma Lite+ and Morpho Wave devices. If the setting is disabled, the access schedules will not be applied to these devices.

Adding Access Schedules

Select time slots for the MA Sigma Access Schedule

	Period 1		Period 2		
Sunday	<input style="width: 60px;" type="text"/>	- <input style="width: 60px;" type="text"/>	<input style="width: 60px;" type="text"/>	- <input style="width: 60px;" type="text"/>	Clear
Monday	06:00	- 13:00	14:00	- 23:00	Clear
Tuesday	<input style="width: 60px;" type="text"/>	- <input style="width: 60px;" type="text"/>	<input style="width: 60px;" type="text"/>	- <input style="width: 60px;" type="text"/>	Clear
Wednesday	<input style="width: 60px;" type="text"/>	- <input style="width: 60px;" type="text"/>	<input style="width: 60px;" type="text"/>	- <input style="width: 60px;" type="text"/>	Clear
Thursday	<input style="width: 60px;" type="text"/>	- <input style="width: 60px;" type="text"/>	<input style="width: 60px;" type="text"/>	- <input style="width: 60px;" type="text"/>	Clear
Friday	<input style="width: 60px;" type="text"/>	- <input style="width: 60px;" type="text"/>	<input style="width: 60px;" type="text"/>	- <input style="width: 60px;" type="text"/>	Clear
Saturday	<input style="width: 60px;" type="text"/>	- <input style="width: 60px;" type="text"/>	<input style="width: 60px;" type="text"/>	- <input style="width: 60px;" type="text"/>	Clear

Screen 3 – MA 100, MA J, MA 500 and MA VP access schedules


This screen allows you to create access times by selecting from the table with fifteen minute steps across 24 hours for each day of the week. Click and drag the mouse over the required areas to select and deselect times. The time area in blue indicates access is allowed. White indicates access is denied. The buttons “Allow All Access” and “Deny All Access” can be used to clear or set access for all days and times.

[Enter Time Mask Details](#)

Time Mask

	12AM	2AM	4AM	6AM	8AM	10AM	12PM	2PM	4PM	6PM	8PM	10PM	12AM
Sunday	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
Monday	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
Tuesday	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
Wednesday	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
Thursday	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
Friday	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
Saturday	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue

12AM 2AM 4AM 6AM 8AM 10AM 12PM 2PM 4PM 6PM 8PM 10PM 12AM

Allow All Access Deny All Access 

User Distribution Group

User Distribution Groups are designed to distribute users onto groups of MA readers or MorphoManager Clients. In order to be utilized the user must be in a User Policy that has its Access Mode set to “Per User”. Then the User Distribution Groups will be selectable when creating (or editing) a user.

Create a User Distribution Group

Screen 1 – Details

Name: Name of the User Distribution Group

Description: Description of the purpose of the group.

Screen 2 – Select Biometric Device Access

Select the Biometric Device(s) that this group will have access to. The “Select All” button will allow access to all Biometric Devices. The “Clear All” button will remove access to all devices.

Name	Description	Location	Model
<input checked="" type="checkbox"/> MA 500	MA 100, MA J, MA 500 and MA VP	MA Sigma	
<input type="checkbox"/> Prox	MA Sigma		

Screen 3 – Select MorphoManager Client Access

Select the MorphoManager Client(s) that this group will have access to.

Name	Description	Location
<input type="checkbox"/> WIN-1BICEVCR2VG		
<input checked="" type="checkbox"/> AMAHON-WIN7		

If using MSO Identification, this will limit the MSO device on the selected client to the number of users in this User Distribution Group. Please note, the capacity of MSO Identification is 500 user per device. This can be expanded with Safran Morpho licensing.

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.

There are four automatically generated User Authentication Modes:

Name	Description
Biometric (1:Many)	Biometric (1:Many)
Contactless Card ID + Biometric (1:1)	Contactless Card ID + Biometric (1:1)
Encoded Smartcard + Biometric (1:1)	Encoded Smartcard + Biometric (1:1)
Wiegand In + Biometric (1:1)	Wiegand In + Biometric (1:1)

Create a new User Authentication Mode

Screen 1 – Details, MA 2G Family Mode, and 3D Face Mode

Adding 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:

Name: Name of the User Authentication Mode.

Description: Description of the purpose of the mode.

MA 100, MA J, MA 500, and MA VP Mode: Select None or the desired authentication mode from the dropdown menu.

Identifier Template Downloaded to Device: The user is authenticated by presenting their finger at a Biometric Device and matching with fingerprint data stored on the Biometric Device. Or, they can key in their authentication identifier at the device and then present their finger.

Identifier Template Encoded to Smartcard: The user carries a card with a Wiegand code on it and touches it on the Biometric Device. If the code read from the card is in the list of accepted Wiegand codes stored on the Biometric Device the fingerprint scanner is activated. The user is authenticated by presenting their finger at the Biometric Device and matching with fingerprint data stored on the card.

Identifier PIN Encoded to Smartcard: The user carries a card with a Wiegand code on it and touches it on the Biometric Device. If the code read from the card is in the list of accepted Wiegand codes stored on the Biometric Device the keypad is activated. The user is authenticated if the PIN code entered matches the stored PIN code.

Identifier Template PIN Encoded to Smartcard: The user carries a card with a Wiegand code on it and touches it on the Biometric Device. If the code read from the card is in the list of accepted Wiegand codes stored on the Biometric Device the keypad is activated. If the PIN code entered matches the stored PIN code the fingerprint scanner is activated. The user is authenticated by presenting their finger at the Biometric Device and matching with fingerprint data stored on the Biometric Device.

Identifier Encoded to Smartcard: The user carries a card with a Wiegand code on it and touches it on the Biometric Device. The user is authenticated if the code read from the card is in the list of accepted Wiegand codes stored on the Biometric Device.

Identifier Encoded to Smartcard Identifier Template Downloaded to Device: The user carries a card with a Wiegand code on it and touches it on the Biometric Device. If the code read from the card is in the list of accepted Wiegand codes stored on the Biometric Device the fingerprint scanner is activated. The user is authenticated by presenting their finger at the Biometric Device and matching with fingerprint data stored on the device.

Identifier from Smartcard Identifier Template Downloaded to Device: The user carries a card with a Card Serial Number (CSN) Wiegand code on it and touches it on the Biometric Device. If the code read from the card is in the list of accepted Wiegand codes stored on the Biometric Device the fingerprint scanner is activated. The user is authenticated by presenting their finger at the Biometric Device and matching with fingerprint data stored on the device

Morpho 3D Face Mode:

Identifier Template Download to Device: The user is authenticated by presenting their face at a 3D Face Reader Biometric Device and matching with 3D Face data stored on the Biometric Device.

Screen 2 – Details for MA Sigma, MA Sigma lite, MA Sigma Lite +, and Morpho Wave Modes for this User

MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme and 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:

MA Sigma, MA Sigma Lite, MA Sigma lite +, MA Sigma Extreme and MorphoWave Mode:

Can be left as None if you are not utilizing MA Sigma devices.

Download Identifier To Device:

Will download the users Wiegand Code to the MA Sigma.

Encode to Smartcard Mode:

Allow: Will allow smartcard coding for a user, but will not prompt during user creation.

Allow and Prompt: Will allow smartcard encoding for a user and will prompt to encode the card during user creation.

Template Location:

Download to Device: Will download users biometric template onto the MA Sigma.

Encoded to Smartcard: Will encode user's biometric template onto a smartcard.

Download to Device and Encode to Smartcard: Will download users template onto the MA Sigma and encode users' biometrics template onto a smartcard.

PIN Location:

Downloaded to Device: Will download users PIN onto the MA Sigma.

Encoded to Smartcard: Select when you want to encode the user's PIN onto a smartcard.

Allow Start by Biometric:

Allow the trigger for authentication to be started by presenting the user's finger to the Sigma.

Allow Start by Contactless Card:

Allow the trigger for authentication to be started by presenting the user's smartcard to the Sigma.

Allow Start by Keyboard:

Allow the trigger for authentication to be started by touching the keyboard screen icon on the Sigma.

Allow Start by Wiegand In:

Allow the trigger for authentication to be started by receiving a Wiegand In signal to the Sigma.

Require PIN:

Makes using a PIN mandatory for authentication.

Require Template Match:

Makes using correct biometric template for user authentication.

Operator Role

Creating and modifying Operator roles is an advanced feature that should only be used by experienced operators.

Screen 1 – Operator Roles Details

Enter the name for this operator role.

Screen 2 – Custom Commands

Select the custom commands this operator role will allow access to.

Select the custom commands available to this operator role

Custom command access set	Execute
BI.ESP4.BioMatch90.AccessLogEntity+AccessLogGetAccessLogsByCreatedDateTimeRangeCustomCommand	<input type="checkbox"/>
BI.ESP4.BioMatch90.AccessLogEntity+AccessLogGetAccessLogsByDateRangeCustomCommand	<input type="checkbox"/>
BI.ESP4.BioMatch90.AccessLogEntity+AccessLogGetMaxAccessLogCreatedDateTimeCustomCommand	<input type="checkbox"/>
BI.ESP4.BioMatch90.AccessLogEntity+AccessLogGetPictureCapturedCustomCommand	<input type="checkbox"/>
BI.ESP4.BioMatch90.TaskEntity+TaskRetryCustomCommand	<input checked="" type="checkbox"/>

Screen 3 – Entity Access

Select the entities this operator role will have access to and the type of access (view, add, edit, delete, import, export).

Select the entity actions available to this operator role

Entity access set	View	Add	Edit	Delete	Import	Export
BI.ESP4.ServerEntity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BI.ESP4.OperatorRoleEntity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BI.ESP4.OperatorEntity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BI.ESP4.SystemExceptionLogEntity	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BI.ESP4.SystemEventLogEntity	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BI.ESP4.ConfigurationEntity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BI.ESP4.LicenseEntity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ID1.ESP4.MM.BiometricDeviceProfileEntity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BI.ESP4.BioMatch90.BiometricDeviceEntity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BI.ESP4.BioMatch90.TaskEntity	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BI.ESP4.BioMatch90.User_Entity	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

NOTE: This screen allows you to restrict or grant operators the ability to import / export users.

Screen 4 – Report Access

Select the reports this operator role will have access to.

Screen 5 – User Interface Access Set

Select the user interface elements this operator will have access to.

Select the user interface elements available to this operator role

User interface guide access set	Display
User Management	<input checked="" type="checkbox"/>
Onsite/Offsite Monitor	<input type="checkbox"/>
Reports	<input type="checkbox"/>
Access Logs Monitor	<input type="checkbox"/>
BioBridge Enrollment Client	<input type="checkbox"/>
MSO Identification Management	<input type="checkbox"/>
MorphoWave Identification Management	<input type="checkbox"/>
Administration	<input type="checkbox"/>

Notifications

Setting up a Notification event will allow specific notifications to be sent when a certain condition is met. For example, a notification when a biometric device has gone offline.



Notifications will only be emailed if the Gateways section of System Configuration is correctly set.

Create a new Notification

Screen 1 – Details

User Management MSO Identification Onsite / Offsite Access Logs Reports

Adding Notifications

Enter details for this Notification

Name:

Description:

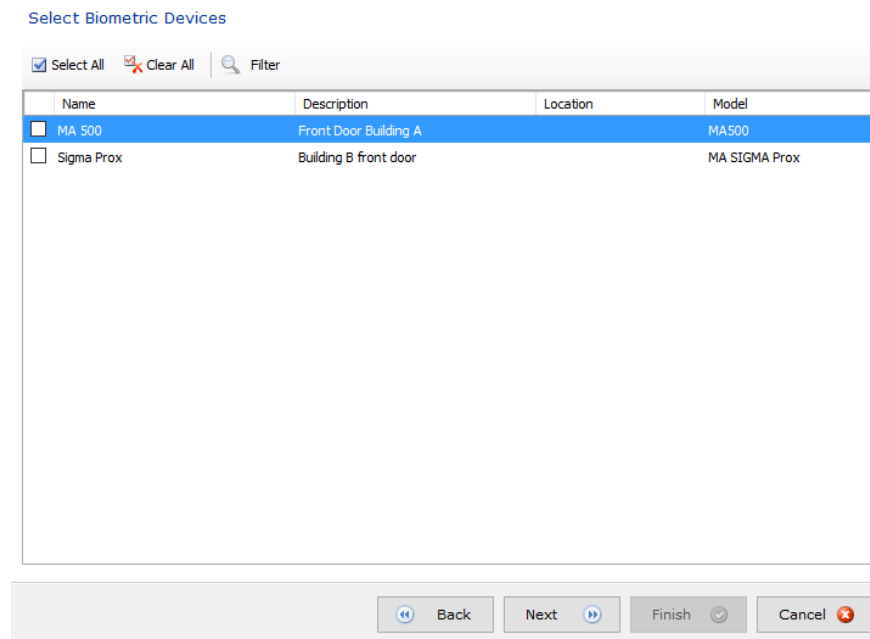
Trigger Type:

Notification Type:

« Back Next » Finish ✓ Cancel ✕

- Name:** Name of the Notification.
- Description:** Description of the Notification's purpose.
- Access Mode:** Determines what event will trigger the Notification being generated and sent.
- Notification Type:** Determines how the Notification will be sent.

Screen 2 – Select Biometric Devices



Select the Biometric Devices that will be monitored for the trigger type selected on Screen 1. The Filter option in the toolbar can be used to narrow down the devices which appear on the list.

Screen 3 – Email List

Email List

Email Subject:

Notification Email List

Email Address
dw@outlook.com
OG@gmail.com

The Email List screen will allow for configuring what the emails subject line will be and to whom it will be sent. Email addresses can be Added, Edited, and Deleted. At least one recipient must be present to click **Finish**.

Clients

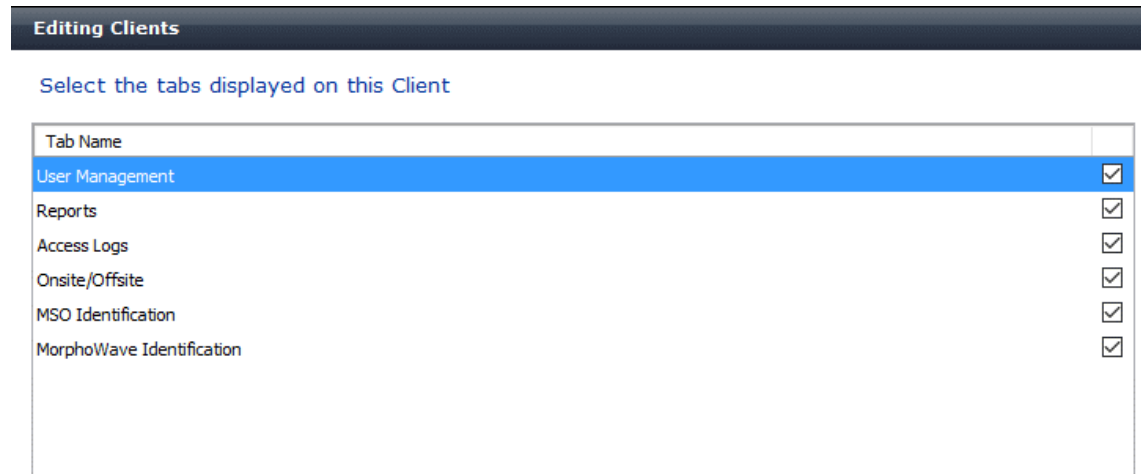
Clients are computers that have the MorphoManager Client software installed and communicate with a MorphoManager server.

Screen 1 – Enter the details for this Client

- Name:** Name of the computer the client is installed on.
Description: A description of the purpose of the client.
Location: The physical location of the client computer.

Screen 2 – Select the tabs displayed on this Client

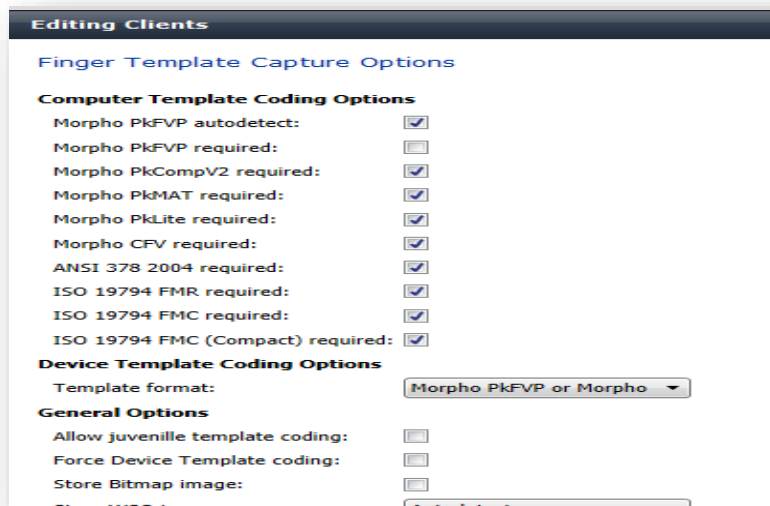
Select the tabs that are displayed on this client. MorphoManager will need to be closed and restarted for the changes to take effect.



Screen 3 - Camera Configuration

Setup the camera that is connected to this client. If the camera is configured here, then the settings are visible in “Capture Photo” in the User Management when enrolling the User. And if a Camera is Configured in “Capture Photo” in the User Management then the settings are visible in the Camera Configuration of the Client.

Screen 4 - Finger Template Capture Options



Computer Template Coding Options: Configures the template formats that will be coded when an enrollment is performed using MorphoKit.

Device Template Coding Options: configures the (single) template format that will be coded when an enrollment is performed using MorphoSmart.

Screen 5 – Card Template Priority

Card Template Priority

The following order will be used to determine which captured template coding will be encoded to a contactless card.

Morpho PkFVP	Move up
Morpho PkCompV2	
Morpho PkMAT	Move down
ANSI 378 (2004)	
MINEX A	
ISO 19794 FMR	
ISO 19794 FMC	
ISO 19794 FMC (Compact)	
Morpho PKLite	
ISO 19794 FMC (Compact - Ascending Angle)	
DIN V66400 (Compact)	
DIN V66400 (Compact - Ascending Angle)	

Encode duress finger to card (MA Sigma family devices only)

This page allows setting of card template encoding priority and allows the enabling of duress finger to be encoded on cards for the MA Sigma family of devices.

Screen 6 - Enrollment Devices

Select the Enrollment Devices you wish to utilize in MorphoManager during User enrollment. You can specify any MorphoSmart device to use the first detected MorphoSmart for finger enrollment, or alternatively select a specific device (if more than one is attached to this PC) or use a selected MorphoAccess Sigma device for enrollment.

For card encoding, you can select any PC/SC device to utilize the first detected device, a specific PC/SC device (if more than one is present) or elect to use a selected MorphoAccess Sigma for card encoding (only on MA Sigma Multi, MA Sigma Lite and MA Sigma iClass).

Key Policy can be selected to determine the keys utilized to encode contactless cards.

Enrollment Devices

Morpho 3D Face enrollment:	None	▼
Morpho 3D Face enrollment biometric device:		Search
Morpho Finger biometric enrollment:	Any MorphoSmart	▼
Morpho Finger enrollment MorphoAccess:		Search
Morpho Smartcard encoding:	Any PC/SC Smartcard reader	▼
Morpho Smartcard encoding PC/SC device:		▼
Morpho Smartcard encoding MorphoAccess:		Search
Key Policy:	Default	▼

Screen 7 – MSO Identification Configuration Settings

MSO Identification Configuration Settings

Unsecure MSO Identification Threshold:

Secure MSO Identification Threshold:

Identification Auto Reset: Enabled
 (Seconds)

Not Identified Auto Reset: Enabled
 (Seconds)

Identification Sound: Enabled

Not Identified Sound: Enabled

Unsecure MSO

Identification Threshold: This value specifies the threshold score for positive identification on Unsecured MSO devices. By default, the score should be set to 4000. Lowering the score will reduce the security, but allow users with lower quality fingerprints to be identified. Raising the score will increase security, but users with lower quality fingerprints may not be identified.

Secure MSO

Identification Threshold: This value determines the identification threshold for Secured MSO devices. The default value for this setting is 4 (1-10). Lowering the score will reduce the security, but allow users with lower quality fingerprints to be identified. Raising the score will increase security, but users with lower quality fingerprints may not be identified.

Identification Auto Reset: If enabled, specifies the amount of time (in seconds) to display the “Identified” screen prior to returning to presentation mode.

- Not Identified Auto Reset:** If enabled, specifies the amount of time (in seconds) to display the “Not Identified” screen prior to returning to presentation mode.
- Identification Sound:** If enabled, a sound will be played via the computer’s speakers indicating a positive identification has occurred.
- Not Identified Sound:** If enabled, a sound will be played via the computer’s speakers indicating a not identified event has occurred.

Screen 8 – Morpho Wave Identification Configuration Settings

MorphoWave Identification Configuration Settings

MorphoWave Identification Threshold:	<input type="text" value="3500"/>
Identification Auto Reset:	<input checked="" type="checkbox"/> Enabled
	<input type="text" value="2000"/> (Seconds)
Not Identified Auto Reset:	<input checked="" type="checkbox"/> Enabled
	<input type="text" value="2000"/> (Seconds)
Identification Sound:	<input type="checkbox"/> Enabled
Not Identified Sound:	<input type="checkbox"/> Enabled

Unsecure Morpho Wave Identification Threshold:

This value specifies the threshold score for positive identification on Unsecured Morpho Wave devices. By default, the score should be set to 4000. Lowering the score will reduce the security, but allow users with lower quality fingerprints to be identified. Raising the score will increase security, but users with lower quality fingerprints may not be identified.

Secure Morpho Wave Identification Threshold:

This value determines the identification threshold for Secured Morpho Wave devices. The default value for this setting is 4 (1-10). Lowering the score will reduce the security, but allow users with lower quality fingerprints to be identified. Raising the score will increase security, but users with lower quality fingerprints may not be identified.

Identification Auto Reset: If enabled, specifies the amount of time (in seconds) to display the “Identified” screen prior to returning to presentation mode.

Not Identified Auto Reset: If enabled, specifies the amount of time (in seconds) to display the “Not Identified” screen prior to returning to presentation mode.

Identification Sound: If enabled, a sound will be played via the computer's speakers indicating a positive identification has occurred.

Not Identified Sound: If enabled, a sound will be played via the computer's speakers indicating a not identified event has occurred.

Scheduled Reports

Scheduled reports enable the periodic generation and delivery of reports based on a predefined set of criteria.



SMTP Settings must be configured in system configuration before a scheduled report can be created.

To add a new scheduled report, click the **Add** button.

Fill in the details for the scheduled report and click **Next**.

The 'Enter Details' form contains the following fields:

- Name: [Empty text box with a red information icon]
- Description: [Empty text box]
- Schedule: [Monthly (dropdown menu)]
- Scheduled Time of Day: [7:00:00 PM (time picker)]
- Scheduled Start Date: [07/01/2014 (calendar icon)]
- No End Date: [checkbox]
- Scheduled End Date: [07/01/2015 (calendar icon)]

Select the format of the scheduled report. Options are pdf, word document, or excel spread sheet.

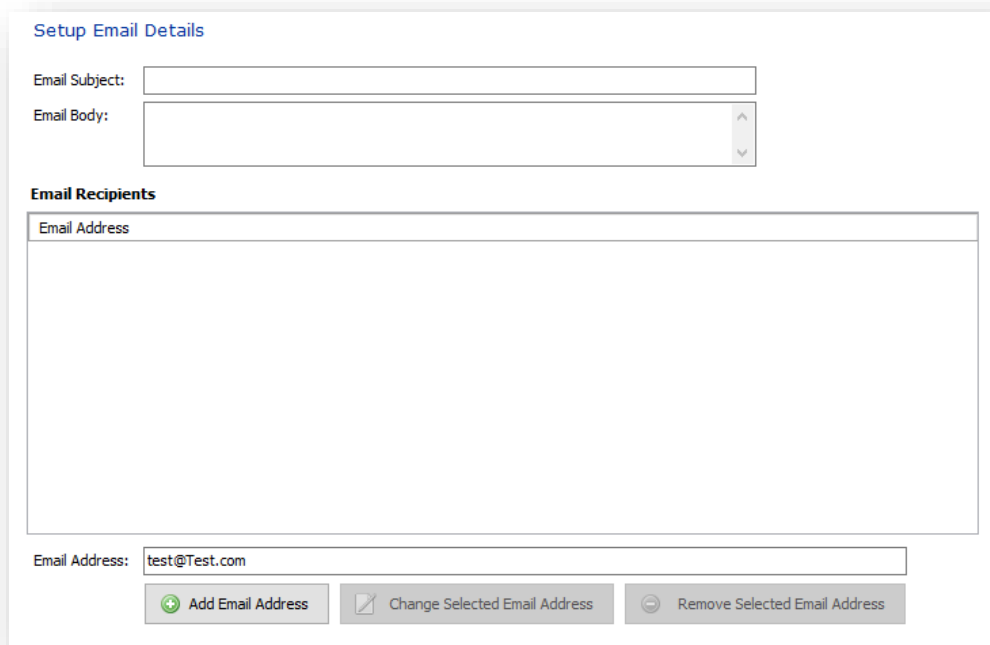
The 'Setup Report' form contains the following fields:

- Report Format: [Pdf (dropdown menu)]
- Report: [All Activity Report (dropdown menu)]
- Report Input:
 - From Scheduled Time Offset: [7] Days [0] Hours [0] Minutes
 - To Scheduled Time Offset: [0] Days [0] Hours [0] Minutes
- Report Columns: [Section header]

Select the type of report that will be generated and enter the details for that report type. The scheduled report will use those details each time it automatically generates a scheduled report. Some report types

allow for an offset to be entered. This allows reports to be generated for a specific date range relative to the current date e.g. A report can be set to run every week for the last seven days.

Click **Next** to go to the next page when the details are correct.



Setup Email Details

Email Subject:

Email Body:

Email Recipients

Email Address

Email Address:

Enter the email subject, body of the email and the recipients.

To add a recipient, type the email address in the text box and click **Add Email Address**. To edit an existing email address, select the address to change, type in the new address and click **Change Selected Email Address**. To remove a recipient, select the email address and click **Remove Selected Email Address**. This information will be used whenever this scheduled report is generated. Click **Finish** to save the scheduled report.

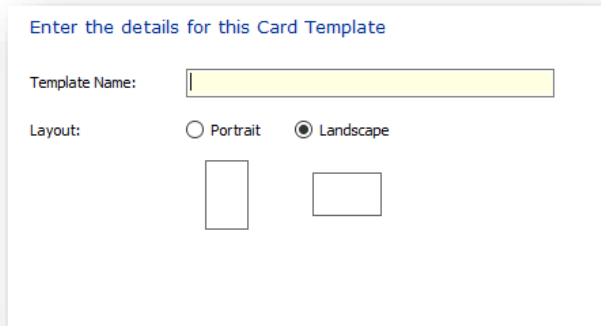
To change the details of the selected scheduled report, click on **Edit** in the toolbar. To remove the selected scheduled report, click on **Delete**. To generate the selected scheduled report now instead of waiting for the predefined generation interval, click on **Run Report Now**.

Card Template

A card template is used to print ID cards for enrolled personnel.

Screen 1 - Details

Enter a name for the template and select the layout of the card.



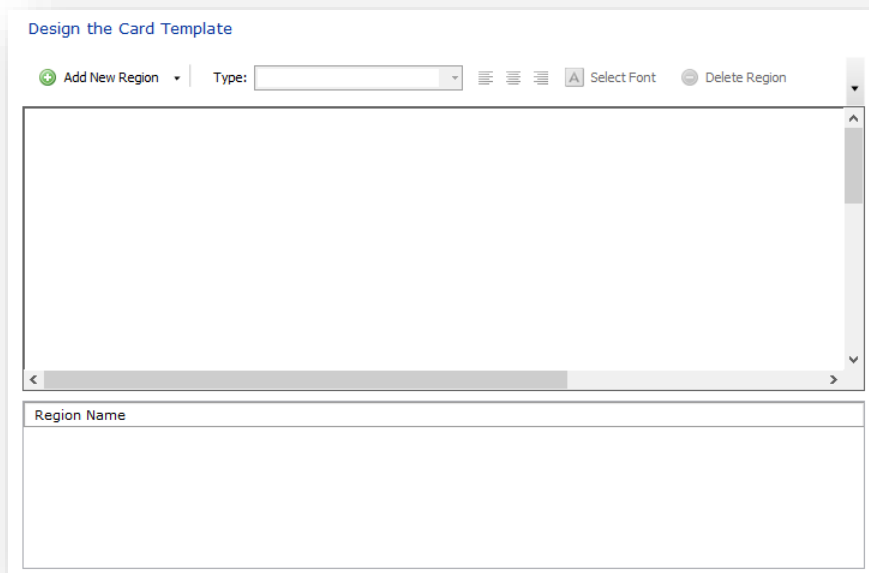
Enter the details for this Card Template

Template Name:

Layout: Portrait Landscape

Screen 2 - Design

Use this screen to design the layout of the card. A region is an item that can be moved around and will be replaced by the actual data when the card is printed (e.g. First Name). A background image can also be added for logos or artwork that is required on the card. To edit a region, click on it or select it from the list below, and change the options using the toolbar items. The region's alignment (left, center or right), font and type can be changed. The size of the region can be changed by dragging the boxes on the edges of the region. To change a background image region, select the region and click **Load Image**. To remove a region, select it and click **Delete Region**.



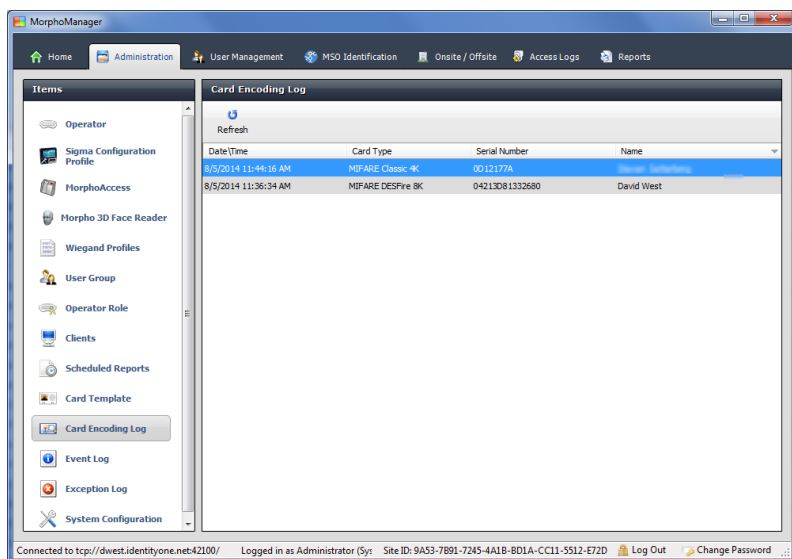
Design the Card Template

Type:

Region Name

Card Encoding Log

This area is designed to store a log of all smartcards encoded via MorphoManager. Information will include the Date\Time stamp, the Card Type, Serial Number, and user name. The user name will be shown as Unknown if the user has been deleted from the system.



Event Logs

Here you will find the history of internal actions performed by MorphoManager. A common error is a failed attempt by MorphoManager to communicate with the Biometric Device. This situation will occur if, for example, there is more than one Biometric Device and all are in error – this may well point to the network hub being switched off or if power to all Biometric Device has been interrupted.

A **Send to Support** button is available when discussing an error with the support team. You may be asked about the information on the screen and also asked that the log be emailed to support for further analysis. When clicked, the log file is automatically attached to a new email using the default email client on the PC. Where it can be examined by support staff to help determine the process needed to rectify any fault conditions.

The “export logs” action is useful for a situation where the MorphoManager PC is not connected to the Internet, allowing the file to be saved in a location for future reference. To export event logs, click on **Save to Disk** button and save it in the location needed. The last selection allows for the start and end date and times to be selected. Select the destination for the file and click **Save**.

Exception Logs

Exception logs store messages that are created by MorphoManager in the event of an internal action not producing the expected results.

The Export Logs and Email Logs to Support icons provide the same functionality as previously outlined in event logs.

System Configuration

Section 1 – Time and Attendance

The screenshot shows a configuration window with the following settings:

- Export profiles**
 - Access log exporter: (none) [Configure]
 - Access log exporter date time mode: MorphoAccess Local Time
- Automatic access log exporter**
 - Automatic Export: Automatically export access log information
 - Export to directory: C:\Users\damien.crabtree
 - Export filename: transactions.csv
 - Export access log data every: 60 (minutes)
 - Export will start from: 1/01/2006 12:00:00 AM (last export occurred)

Access Log Exporter

These settings are used for manual and automatic access log exporting to a Payroll or Rostering software package. You need to select the format you want the exported data to comply with. You may choose from ASTROW, Commac, Preceda, Timeminder, Powerforce, RosterOn, MYOB, MorphoManager Standard, Kronos, Pay Global (Employee ID/Wiegand Usercode), Sodsb and TimeAmerica.

Automatic Access Log Exporter

Click on the check box for **Automatic export access log information** and select a destination for the exported file.

Enter the default file name and destination for the file. The directory **MUST** exist on the server computer as the file will be saved to the server's hard drive.

The file will be exported at the interval specified at **Export access log data every**.

Section 2 – Communications Engine

Communications Engine Settings

Maximum active communication channels:

MASG User Batch Size :

Number of concurrent tasks that can execute per physical core: (2 physical cores detected on server)

Disable device events and error logging:

System Event Log

Write information to the system event log:

Write warnings to the system event log:

Write errors to the system event log:

Realtime Access Log Recording Settings

Server listening IP address:

Server listening port number:

MorphoAccess notification timeout: (milliseconds)

Enable Realtime Access Log Relay

Host	Port
------	------

- Maximum Active Communication Channels:** The maximum number of active communication channels.
- MASG User Batch Size:** Sets the batch size of users to be sent to a device.
- Number of concurrent tasks per CPU core:** Limits the number of concurrent tasks per CPU core to improve system performance.
- System Event Log:** Select the types of information to write to the system event log.
- Realtime Access Log Recording Settings*:** These settings are to be configured to use the Realtime Access logs for a Biometric Device.
*The port used as the server listening port will need to be opened in your firewall settings

Section 3 – System Functionality

BioBridge	Privacy Mode	Morpho Tablet	Password Rules	Biometric Device Template Priority	Display Options
Time & Attendance	Communications Engine	System Functionality	System Management	Gateways	Connector Service

Default Tab

Home

User Management

Show all users when total user count is less than: 10000

System Reporting

Send error and usage statistics

User Onsite/Offsite

User Onsite/Offsite update status enabled will automatically set users Onsite or Offsite when Access Logs are retrieved

User Onsite/Offsite update status enabled

Default Tab

This defines the tab selected by default when MorphoManager starts.

User Management

This allows you to control how many users will appear on your User Management screen. If you have more than the amount in the value filed, you can use filtering to find the additional users.

User Onsite/Offsite

This will be turned off by default. When turned on Biometric Devices that are set to use their Onsite/Offsite functionality will set the users to either Onsite or Offsite in the Onsite/Offsite section of MorphoManager. The users Onsite or Offsite status is recorded during the Get Logs task. If this is left disabled no recording of Onsite/Offsite change is populated in the Onsite/Offsite section during the Get Logs.

Section 4 – System Management

The screenshot displays the 'Log Management' section with four input fields: 'Maximum system error logs' (500), 'Maximum system event logs' (500), 'Maximum access logs' (10000), and 'Maximum access log age (Days)' (1095). Below this is the 'Disabled User Management' section, which includes a descriptive sentence and three radio button options: 'Never Delete', 'Delete Immediately', and 'Delete After:'. The 'Delete After' option is selected, with a dropdown menu showing '90' and '(days)'.

Log Management

These settings are in place to prevent any log files from becoming unmanageable due to their size. The above values are the default values. When the log count reaches these values the oldest logs are deleted until they are within the values specified.

Disabled User Management

Users who are disabled in User Management will be governed by the following options:

- Never Delete:** This is the system default. Users who are disabled will never be deleted from MorphoManager.
- Delete Immediately:** Users will be deleted immediately from MorphoManager when disabled.
- Delete After:** Users will be deleted from MorphoManager after the assigned amount of day set here when disabled.

Section 5 – Gateways

Gateway Settings - Email

SMTP Server Hostname:	<input type="text"/>
SMTP Port Number:	<input type="text" value="25"/>
SMTP Server Authentication:	<input type="checkbox"/> Server Requires Authentication
SMTP Username:	<input type="text"/>
SMTP Password:	<input type="password"/> <input type="checkbox"/> Reset Password
SMTP Requires SSL:	<input type="checkbox"/> Server requires SSL
From Email Address:	<input type="text"/>
Reply To Email Address:	<input type="text"/>

The Gateway settings are used to receive emails for Scheduled Reports. These settings are specific to the Mail server. For further assistance, to configure the gateway settings, please refer to your IT support.
Automatic Certificate Binding Mode.

Section 6 – Connector Service

Enter the settings for the connector service.

Connector Service

Certificate binding mode:	<input checked="" type="radio"/> Automatic <input type="radio"/> Manual
P6 integration key:	<input type="text" value="8E690F673157E9B6D733987CC72B2BA2"/>
Allow creation of self-signed certificates:	<input checked="" type="checkbox"/>
Allow use of expired or not yet valid certificates:	<input type="checkbox"/>
Hostname binding option:	<input checked="" type="radio"/> Automatic <input type="radio"/> Manual
Hostname:	<input type="text"/>
Automatic binding port:	<input type="text" value="443"/>
Certificate thumbprint:	<input type="text"/>
Manual binding port:	<input type="text" value="443"/>

Section 7 – BioBridge

Completely optional, BioBridge allows you to extract user data from compatible third-party systems. User/grouping Information can be “synced” by the BioBridge Enrollment Client when you set the configurations for the respective third-party system. You can set “rules” for when data is synced between both parties.

System Configuration

Time & Attendance | Communications Engine | System Functionality | System Management | Gateways | Connector Service | **BioBridge** | Privacy Mode | Morpho Tablet | Password R

MorphoManager BioBridge Settings

System:

Wiegand Profile:

Grouping Mode:

Enable Forced User Policy: Enabled

Forced User Policy:

User Synchronization Start Time:

User Synchronization End Time:

Delay Between Each User Synchronization (ms):

Allow User Sync While User Cache Is Refreshing: Enabled

User Cache Schedule:

Sunday Monday Tuesday Wednesday Thursday Friday Saturday

0:00 1:00 2:00 3:00 4:00 5:00
 6:00 7:00 8:00 9:00 10:00 11:00
 12:00 13:00 14:00 15:00 16:00 17:00
 18:00 19:00 20:00 21:00 22:00 23:00

User Distribution Group Mappings:

Access Groups	User Distribution Group

System

Choose your BioBridge compatible system from the drop down menu.

Configure connection

Connection credentials for the third-party software.

BioBridge Logon Details Connection

Logon details

Please enter the **Third Party** logon credentials below.

Server:

Username:

Password:

Wiegand Profile

Most (but not all) BioBridge compatible systems use a specific Wiegand format to identify users/cardholders. This can be specified on Cards, Card Types or can be specified as a “Wiegand Format”. Please select the Wiegand format in use from the drop down menu.

Grouping Mode

This setting determines how MorphoManager should map BioBridge users into MorphoManager User Distribution Groups. This can be done by either automatically trying to map based on the names (Automatic), or by manually selecting which BioBridge Access Level maps to which MorphoManager User Distribution Group.

Enable Forced User Policy

By activating this feature, you can select a User Policy from the drop down menu. The 3rd party user will automatically be placed in this User Policy during the enrollment process started in the BioBridge Enrollment Client. The User Policy selected here must be a “Per User” access mode policy.

User Synchronization Start Time and End Time

The user synchronization engine will only be permitted to run in this time frame.

Delay between Each User Synchronization

The duration that the User Synchronization Engine will sleep between each user sync. Increase the delay time to use less system resources, but this will also extend the time it takes for all the users to be updated.

Allow User Sync While User Cached Is Refreshing

When enabled, the User Synchronization engine will run in parallel to the User Cache Refresh. This is very taxing on system resources. It is recommended to disable this setting when using large databases.

User Cache Refresh Schedule

The specified times when the user cache refresh may start. The ideal schedule would be 24/7, but this is not always possible with large databases.

User Distribution Group Mappings

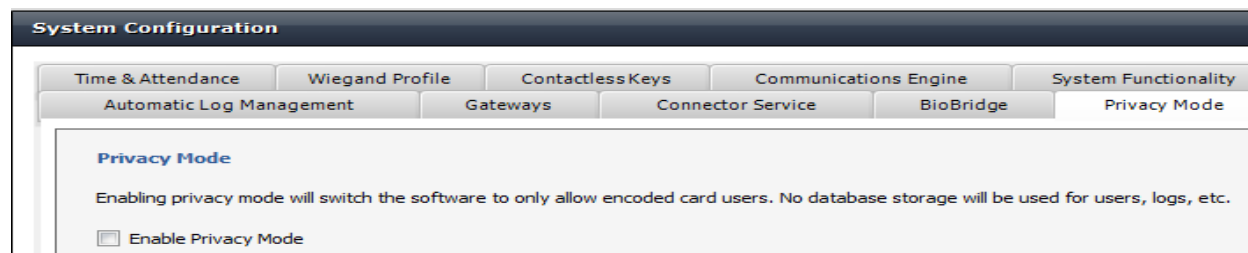
This displays and allows for modification of how the BioBridge groups map to MorphoManager User Distribution Groups (if using Manual Grouping Mode). If no MorphoManager User Distribution Group is selected for a particular BioBridge Grouping, those users will not be available for enrollment into MorphoManager.



For vendor specific details, please refer to the separate BioBridge Quick Start Guide manuals.

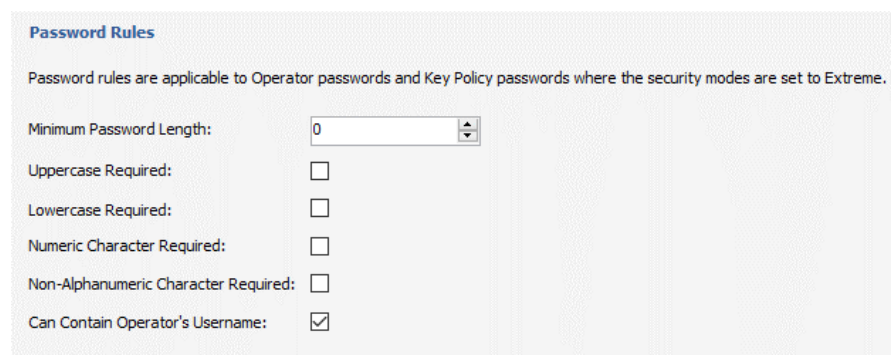
Section 8 - Privacy Mode

This mode will allow customers to enroll card-only users (i.e. Card-only, Card + PIN, Card + Fingerprints, Card + Fingerprints + PIN) without saving their details to the MorphoManager database. This mode will apply to all User Policies, and will only apply to **new** enrolments. Users who are enrolled in this mode will not appear in User Management. Additionally, if Privacy Mode is enabled log retrieval will be disabled.



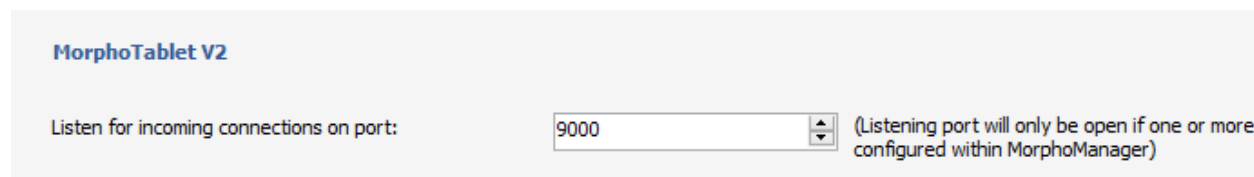
Section 9 – Password Rules

Password Rules allow setting of password complexity for Operators on the system and for Key Policies in Extreme mode. By default, there are no password complexity rules enforced, but that can be configured here.



Section 10 – MorphoTablet

Enter the port the tablet will communicate with the MorphoManager Server.



Section 11 – Biometric Device Template Priority

This section will allow you to set the order of template types to be distributed to different families of Biometric Devices. The order of template types will be used to determine what type of template will be downloaded to a biometric device, based on the available template types present on each user enrolled.

Biometric Device Template Priority

The following determines the template priority to be downloaded to the device families. The first item on the list will have highest priority.

MorphoAccess Template Priority (MA-J, MA 500, MA FVP)

- Morpho PkFVP
- Morpho PkCompV2
- Morpho PkMAT
- ANSI 378 (2004)
- MINEX A
- ISO 19794 FMR
- ISO 19794 FMC
- ISO 19794 FMC (Compact)

MorphoAccess Sigma Template Priority (MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme and MorphoWave)

- Morpho PkLite
- Morpho PkFVP
- Morpho PkCompV2
- Morpho PkMAT
- ANSI 378 (2004)
- MINEX A
- ISO 19794 FMR
- ISO 19794 FMC
- ISO 19794 FMC (Compact)
- ISO 19794 FMC (Compact - Ascending ...)
- DIN V66400 (Compact)
- DIN V66400 (Compact - Ascending Angle)
- BLUR
- VIIR

Section 12 – Display Options

User Wizard Display Options

Display	Mandatory	DisplayName
<input checked="" type="checkbox"/>	<input type="checkbox"/>	User defined field 1
<input type="checkbox"/>	<input checked="" type="checkbox"/>	User defined field 2
<input type="checkbox"/>	<input type="checkbox"/>	User defined field 3
<input type="checkbox"/>	<input type="checkbox"/>	User defined field 4
<input type="checkbox"/>	<input type="checkbox"/>	User defined field 5
<input type="checkbox"/>	<input type="checkbox"/>	User defined field 6
<input type="checkbox"/>	<input type="checkbox"/>	User defined field 7
<input type="checkbox"/>	<input type="checkbox"/>	User defined field 8
<input type="checkbox"/>	<input type="checkbox"/>	User defined field 9
<input type="checkbox"/>	<input type="checkbox"/>	User defined field 10

Selecting to display user defined fields will show another page in the user wizard that collects the information as set in these fields. Select the fields to display, whether or not information is mandatory, and assign names for the fields.

Section 13 – MorphoWave

The screenshot displays a configuration window with three main sections:

- MorphoWave Unlock:** Shows a challenge code of 0322 6270, an empty input field for the Morpho response code, and an 'Unlock' button.
- User Management:** Includes a message: 'To use the Enhanced MorphoWave enrollment requires unlocking. Please contact Morpho support with your challenge code to unlock.' Below this is a dropdown menu for 'Enrollment Method' currently set to 'Enrollment 1'.
- MorphoWave Identification:** Contains the text: 'Enabling this feature will load all MorphoWave enrolled users at server start up. This may slow down performance in the case of a large user' and a checked checkbox labeled 'Enable On Server Startup'.

MorphoWave Unlock

Currently not supported.

User Management

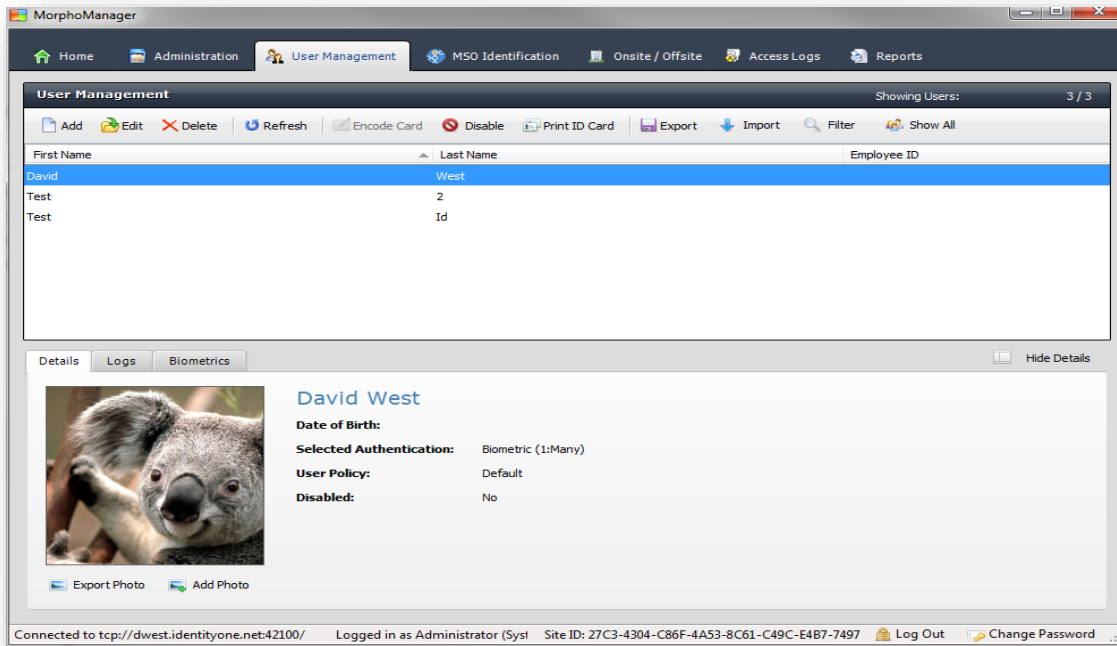
Currently not supported.

MorphoWave Identification

Enabling this feature will load MorphoWave enrolled users into cache when the MorphoManager Server is started. If this feature is not selected only users who are edited will be loaded into cache.

User Management

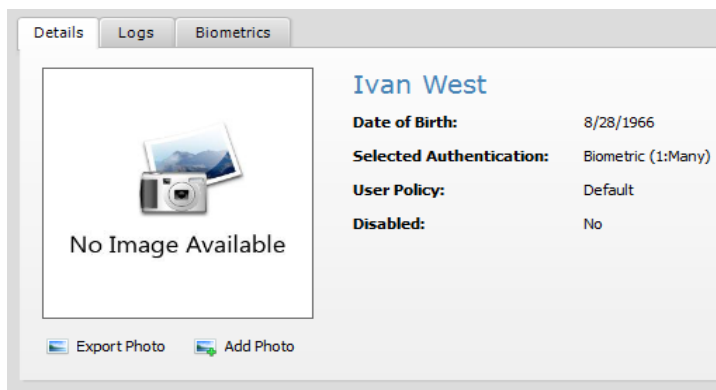
Users are people who will have their biometric data (or minutia) sent to the selected Biometric Device for identification purposes for either access control or time and attendance. Select the user management tab to access this area.



User Details

Information about a user's Details, Logs, and Biometrics is available when a user is highlighted in the list of users.

Details:



If a user has been Disabled, their disabled date and the Operator who disabled them will appear on the Details tab.

Logs:

Accessed On	MorphoAccess	Key
11/3/2015 1:13:34 PM	Sigma Prox	No key
11/3/2015 1:13:30 PM	MA 500	No key

Biometrics:

Biometric Type	Format	Quality	Capture Date/Time	Coding	Device
Left index finger	Morpho PKCOMPV2	96	11/3/2015 1:07:30 PM	PC	MSO300
Left index finger	Morpho PKMAT	96	11/3/2015 1:07:30 PM	PC	MSO300
Left index finger	Morpho CFV	96	11/3/2015 1:07:30 PM	PC	MSO300
Left index finger	Morpho PKLite	96	11/3/2015 1:07:30 PM	PC	MSO300
Left index finger	ANSI 378	96	11/3/2015 1:07:30 PM	PC	MSO300
Left index finger	ISO 19794 FMR	96	11/3/2015 1:07:30 PM	PC	MSO300
Left index finger	ISO 19794 FMC (Compact)	96	11/3/2015 1:07:30 PM	PC	MSO300
Left index finger	ISO 19794 FMC	96	11/3/2015 1:07:30 PM	PC	MSO300

The templates captured for the user will be shown. Templates for the user can be Exported and Imported from this screen.

Creation and enrollment of a User

To create a new user, select the click the **Add** button on the Toolbar. This will display the User Wizard.

Screen 1 – User Details

Enter the details for the new user.

- 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.
- First Name:** User's first Name **(Required)**
- Middle Name:** User's Middle Name
- Last Name:** User's Last Name **(Required)**
- Date of Birth:** Enter the date of birth of the user. This can be entered in several different ways. E.g. 30th May 1975 could be entered in the following ways 30/5/75, 30-5-75, 30 May 1975, 30 5 1975.

Screen 2 – Additional Details

Enter additional details for this user

Job title:

Employee ID:

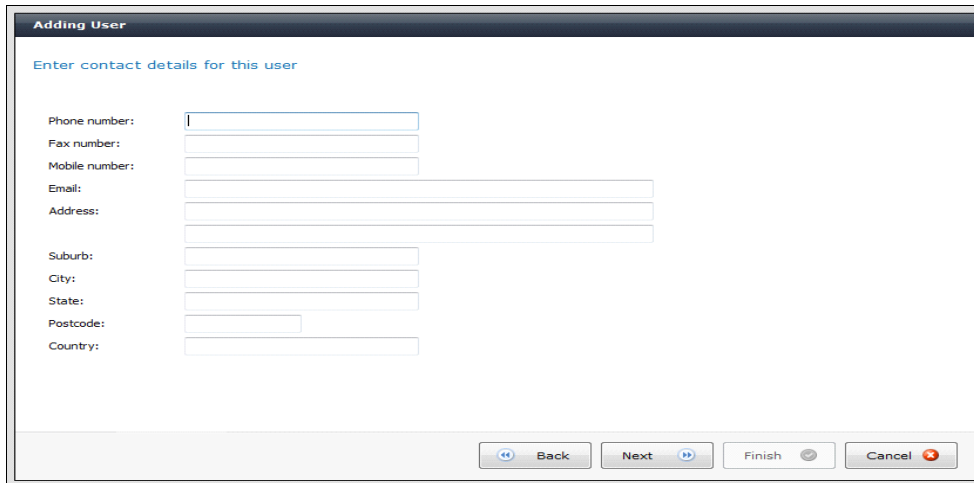
Biometric device display name:

Comments:

MorphoAccess Database: (Only applicable for MA 500 with Xtended Licenses)

- Job Title:** The user's job title.
- Employee ID:** A company specific code that may be assigned to a user. If used for "Time and Attendance", this field should match the employee number from the Payroll or Rostering software.
- Biometric Device Display Name:** The information displayed upon acceptance by the Biometric Device and defaults to the First and last name of the user.
- Comments:** Any additional information that is relevant to that person.

Screen 3 – Contact Details



The screenshot shows a window titled "Adding User" with a subtitle "Enter contact details for this user". The form contains the following fields:

- Phone number:
- Fax number:
- Mobile number:
- Email:
- Address:
- Suburb:
- City:
- State:
- Postcode:
- Country:

At the bottom of the form are four buttons: "Back" (with a left arrow), "Next" (with a right arrow), "Finish" (with a checkmark), and "Cancel" (with a red X).

This page and the User Defined Fields page to follow are only visible if “Display Extended user policy details” has been enabled on the selected User Policy. If so, enter the details for the selected user.

Screen 4 – User Defined Fields

Enter custom details for this User

Department:

Field2:

These fields are set in System Configuration>Display Options. Up to ten fields can be named and set as mandatory.

Screen 5 – Biometric Device Override Details (If a Wiegand Profile is set)

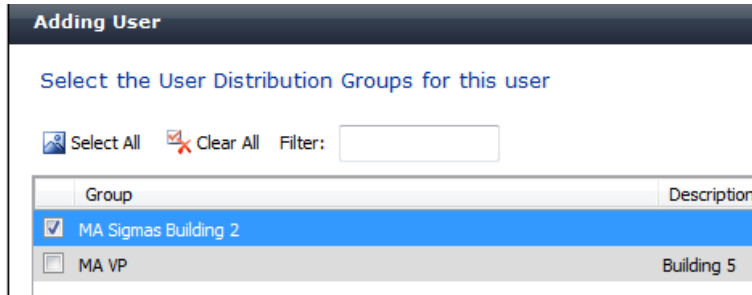
Wiegand Values

User ID

The User ID can be put in manually or by utilizing the Randomize button. This screen is only available if you have changed the User Policy to have a particular Wiegand Profile set, rather than leaving the default setting of “Automatically generated random 64 bit”. Additionally, a Read Card Serial Number button will be present if you utilize one of the Wiegand Profiles referencing Card Serial Numbers.

Screen 6 – User Distribution Groups

If your User Policy is a Per User access mode, you will be able to select the group of biometric devices you want to place the user on.



Screen 7 – Photo Capture



Position the person in front of a plain background so that all of their face is visible in the picture, similar to a passport photo. Once the user is positioned correctly click **Capture Photo**. Click on the image in the top left corner and drag towards the bottom right drawing a square around the part of the photo to keep. This can be done many times until the correct area is selected. Click **Accept Changes** to accept the changes if no camera is connected just click **Next**.

If the person is not available to have their photo taken, click **Person not at Camera**, to skip photo capture.



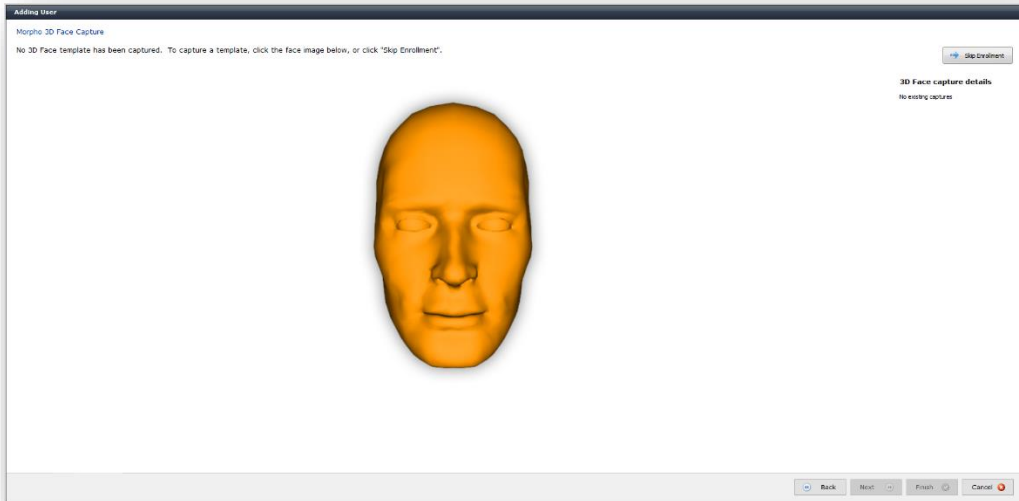
If the photo is not acceptable, click **Update Photo** to recapture the photo. Photos can be imported and exported using the corresponding buttons. Additional configuration options for the camera can be changed by clicking on **Configure Camera**.

Screen 8 – PIN Code

A screenshot of a software interface titled "Adding User". Below the title, there is a blue instruction: "Enter and confirm the PIN". Below this instruction are two input fields. The first is labeled "PIN:" and the second is labeled "Confirm PIN:". Both input fields are empty and have a light yellow background.

PIN Code: Will be utilized and appear on screen when the authentication mode is set to one including PIN. Ex. Smartcard + PIN.

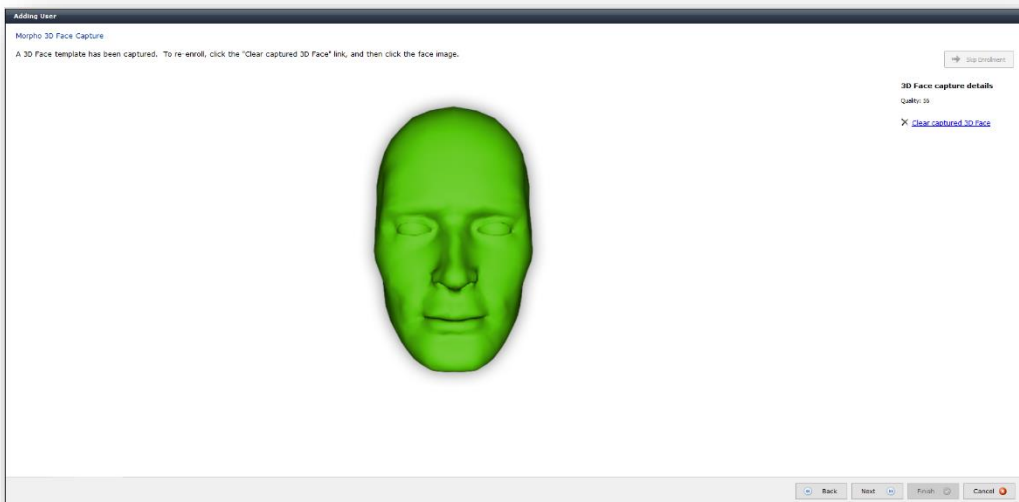
Screen 9 – 3D Face



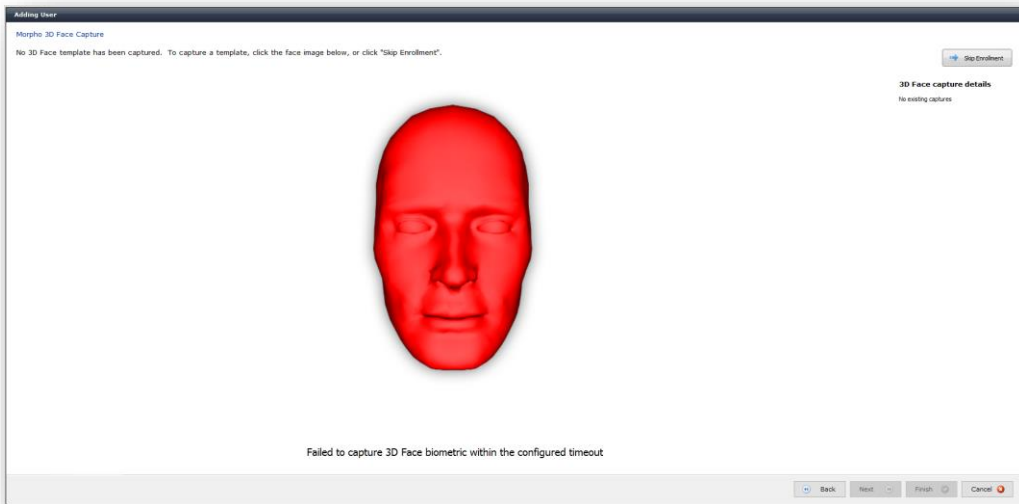
The 3D Face reader will scan a user’s face and capture a 3D rendering of the image. To scan a user’s face align the face on the device until the device indicates the face has been recognized.

Once the face is recognized the message on the device will change to “Look here and center your image.” Once the face is centered and the scanning process begins the message on the device will change to “Face detected Do not move.” A progress bar is shown on the device showing the user being scanned the status of the scan. Once complete the message “Enroll Success” will be displayed on the device.

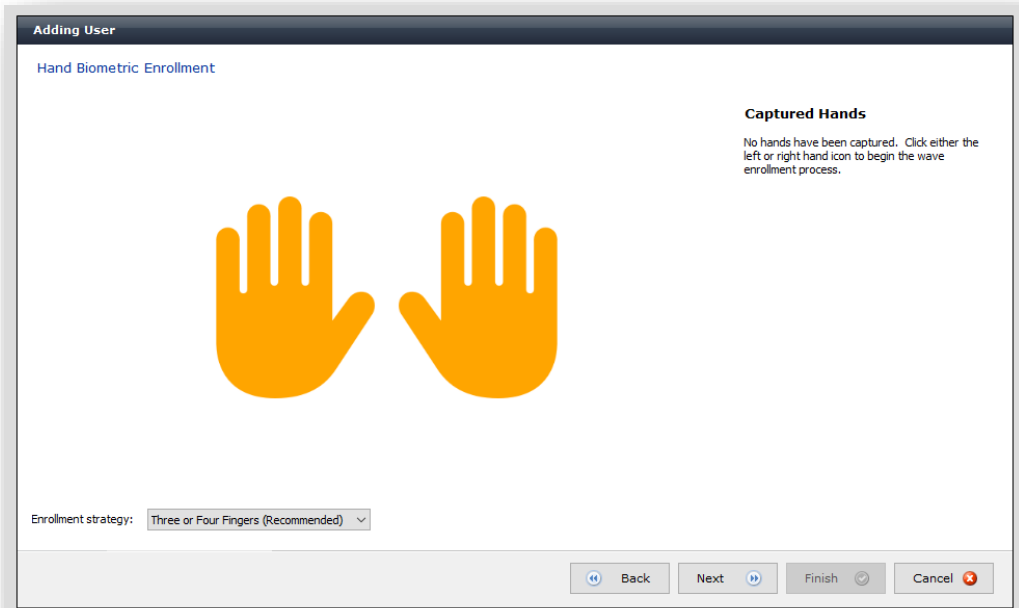
When a scan is successful the image below is seen.



If the face was not able to be scanned the image below will be seen and the face capture process will need to be performed again. When this occurs, it is most often because the user moved during the scanning process.



Screen 10 – Wave Enrollment

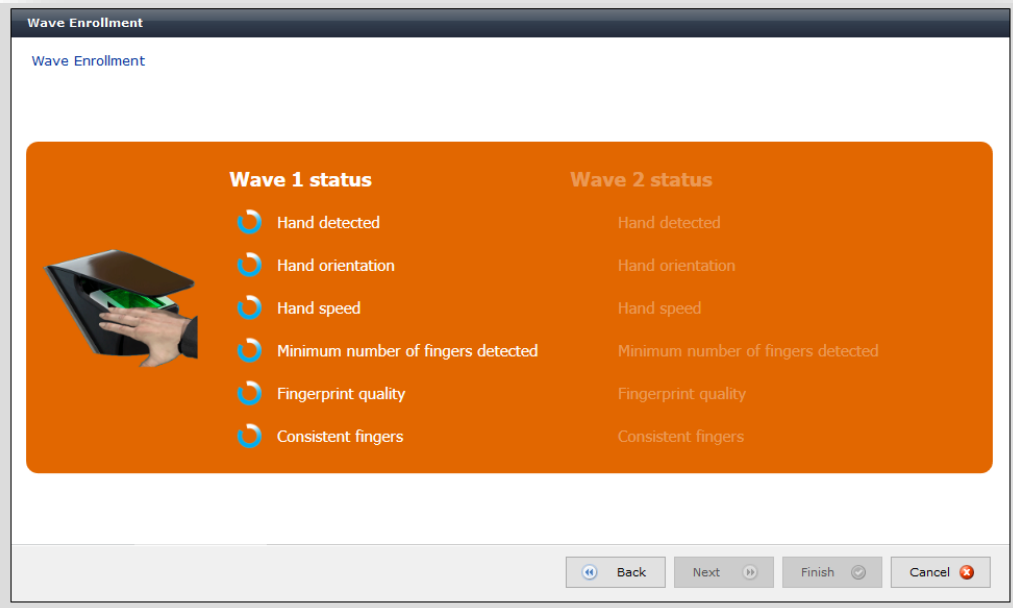


The number of hands required for full enrollment of the user is dictated by that setting in User Policy. In order to start the captures, click on one of the hands.

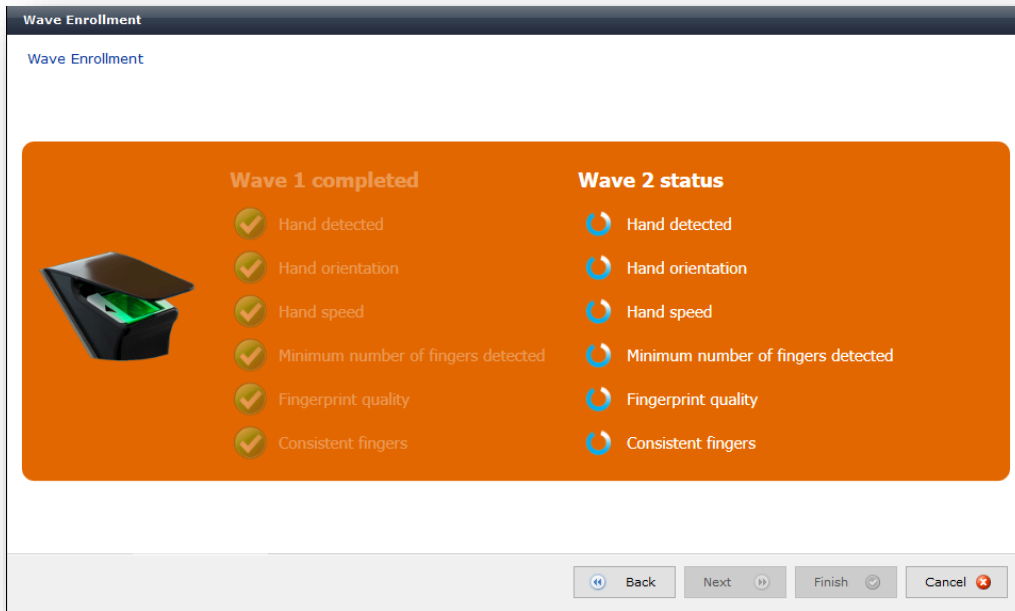
If either of the following conditions occurs a “No Device” message box will be displayed when you select a finger to enroll:

- There is no fingerprint reader connected
- The correct licensing is not in place for the device.

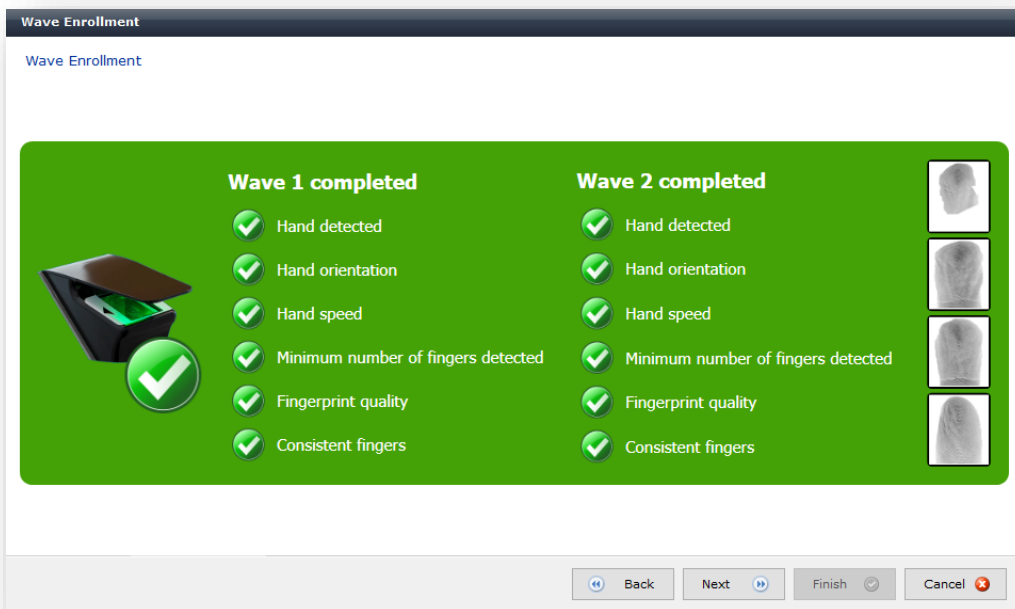
If the reader is connected correctly the following screen below will be displayed.



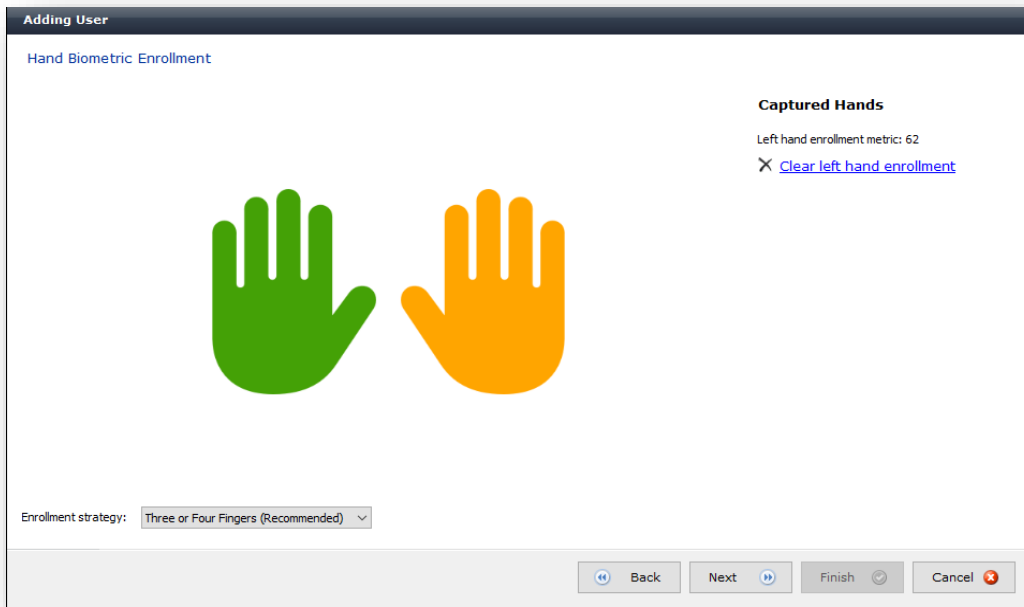
Move your hand through the Wave sensor which should now be illuminated. You will then see the results of Wave 1 appear on screen. If it is successful, you will then be prompted to present for Wave 2. If it is not successful, you will see a red X in the elements of Wave 1 that were not successful. Move your hand through the sensor again until Wave 1 is completed.



Upon successful completion of both Wave 1 and Wave 2, the following screen will appear.

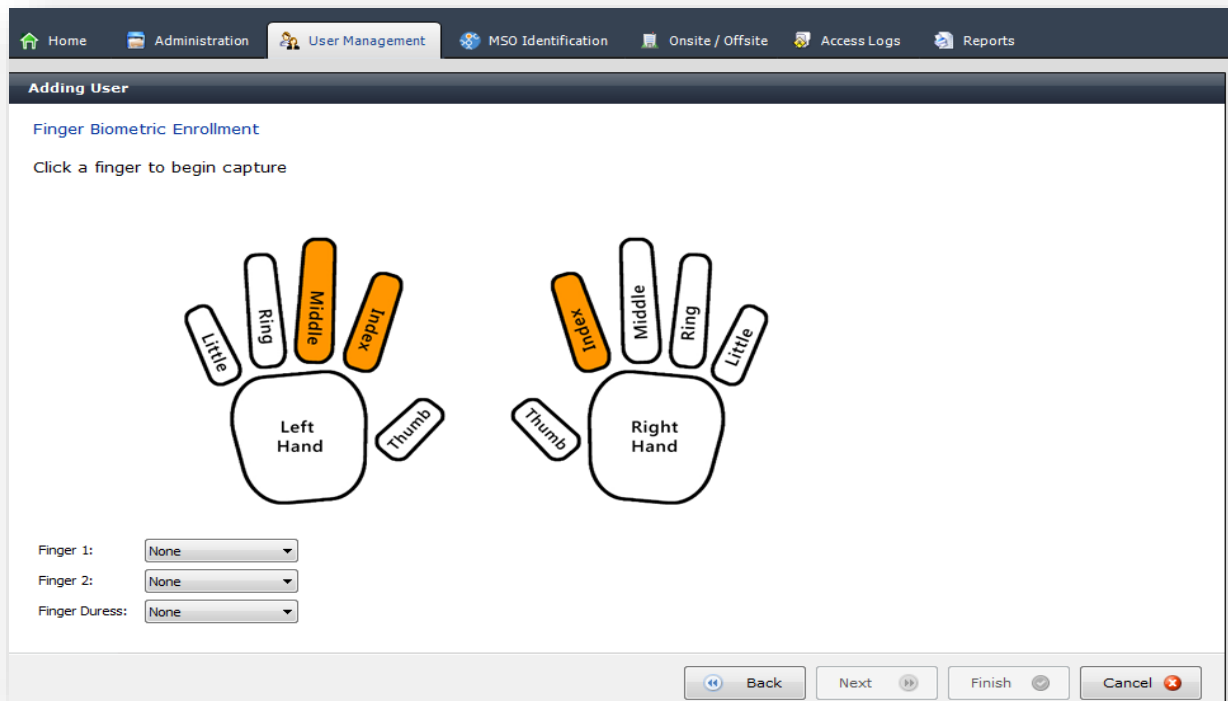


Once the enrollment is complete for Wave 1 and 2, click **Next**. The screen below will appear showing captured hand and quality displayed on the right. In the event a user is not being recognized at any Morpho Wave Device, click **Clear <enrolled finger> finger enrollment** to allow re-enrollment.



Positive Identification and general performance of MorphoManager is maximized by the quality of the fingerprint captured during enrollment. MorphoManager has been designed to reject poor quality fingerprints; however, it is still possible they may slip through.

Screen 10 – Fingerprint Capture

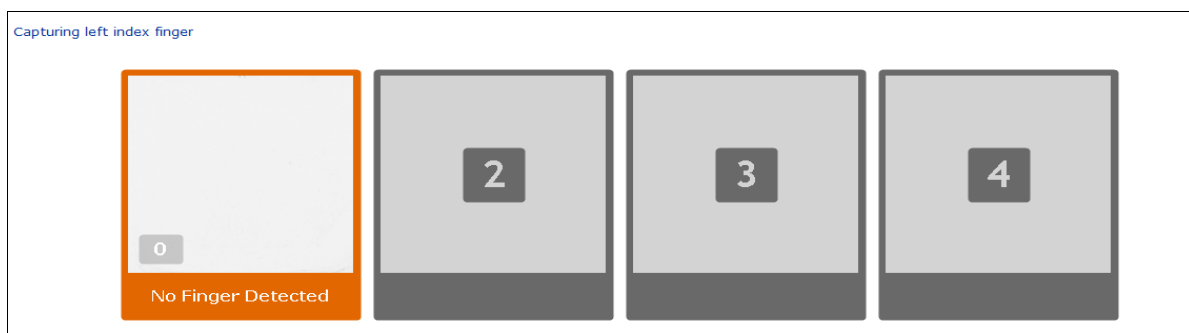


The default fingers that the system suggests you to enroll are set at the User Group level and are flashing orange. **You do not need to use these fingers as you can click on others. However, you will need to set at least Finger 1 from the respective drop down list after fingerprint capture.**

If either of the following conditions occurs a “No Device” message box will be displayed when you select a finger to enroll:

- There is no fingerprint reader connected
- The fingerprint reader connected is the wrong model for the software.

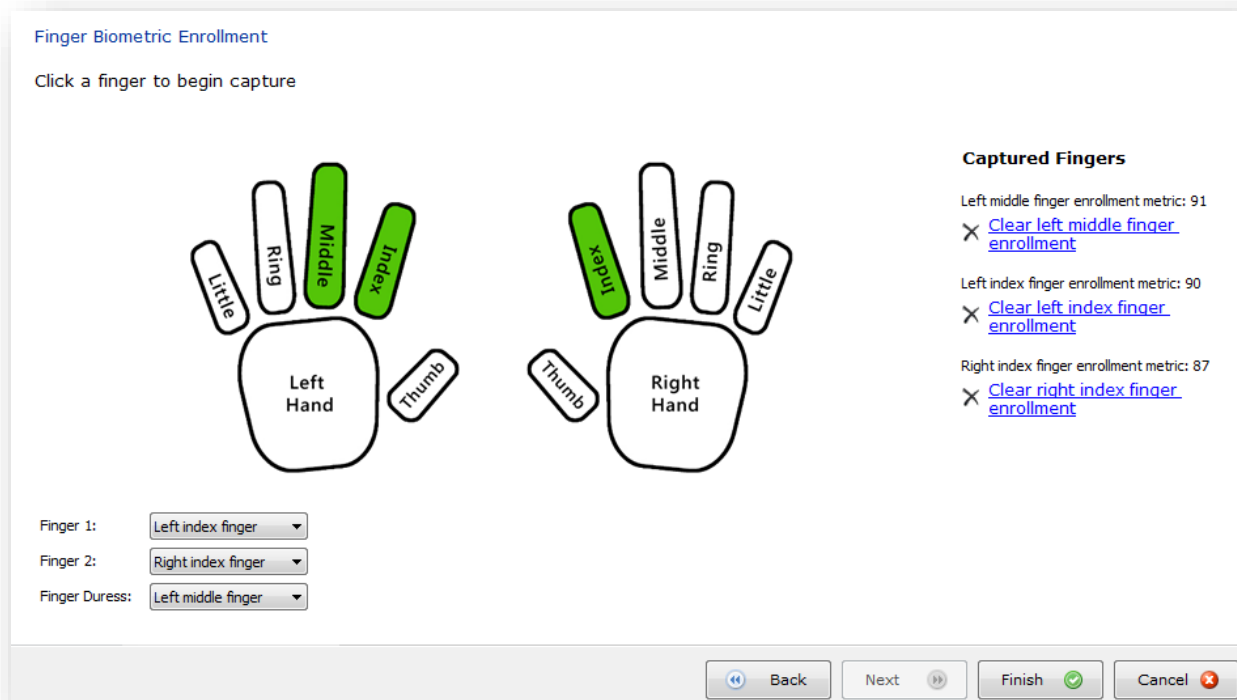
If the reader is connected correctly the following screen below will be displayed.



Click on a finger and have the user place their finger in the center of the scanner glass. You will then see the print appear on screen. There are four scans performed on each finger; the first three are used to create the biometric template. The system selects the best elements of each print and consolidates those features, allowing a greater range of presentations to be recognized. The fourth print is used for verification purposes. Below each enrollment image a color bar will be displayed indicating the quality of the print as it is being captured. Green indicates quality is above recommended quality. Orange indicates the quality is above the minimum but below the recommended quality. Operators with administrative rights are permitted to accept fingerprints of this quality. Red indicates the quality is below the minimum, the user must re-enroll.

Follow the instructions on screen. Green indicates ready to capture. Orange indicates that a finger is presented but the capture has not finished yet. Check the instructions to ensure the finger is placed correctly. When the border is red, the current finger capture is finished. Continue until all boxes are filled.

Once the enrollment is complete, you will see the screen below (this example is utilizing a Duress Finger). Captured finger quality is displayed on the right. In the event a user is not being recognized at any Biometric Device with enrolled fingers, click **Clear <enrolled finger> finger enrollment** to allow re-enrollment.





Positive Identification and general performance of MorphoManager is maximized by the quality of the fingerprint captured during enrollment. MorphoManager has been designed to reject poor quality fingerprints; however, it is still possible they may slip through.

The key to capturing a high quality fingerprint is to visually look for a clearly presented pattern that is centered and square with the right amount of pressure. Don't hesitate to retry the capture if you are unsatisfied. For assistance refer to the fingerprint capture guide. Click **Finish** to save the user or cancel to discard changes.

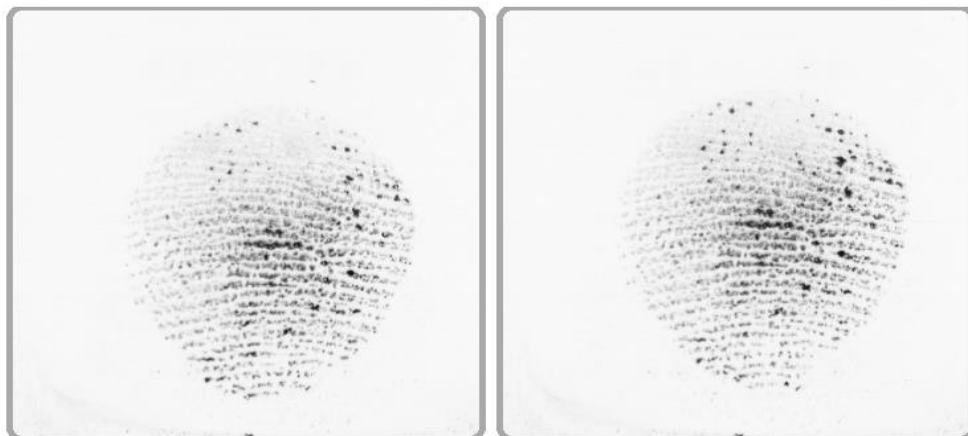
To get the best performance from your MorphoManager software and Biometric Device hardware, care must be taken with enrollment of users into the system. Below are examples of fingerprint capture which could result in either false acceptance or false rejection of users at your Biometric Device. We also suggest that the Biometric Device be mounted at a height of approximately 1 meter from the ground. Mounting the Biometric Device at this height will facilitate full finger presentation when using the Biometric Device. Mounting the Biometric Device significantly higher or lower on the wall makes presentation of a full fingertip much more difficult.

Figure 1



This is an example of a finger that has been cleaned of oil by methylate spirit. Very little information is shown on the print to develop the algorithm. This can happen if you use hand wipes or hand cleaners prior to using the Biometric Device. If the hand cleaners are used for infection control or similar requirements, either use the hand cleaner after using the Biometric Device or provide a hand cream solution to replace the natural body oils stripped from the hands.

Figure 2



This is an example of a print where the person being enrolled has used only light pressure and partial presentation of the tip of the finger. The user will have difficulty presenting the same portion of the finger when clocking “On” or “Off” if this is allowed during enrollment. This type of enrollment could also lead to a significant number of false acceptances which is where a user is identified incorrectly. This is because there is little information in this portion of a fingerprint to develop a good algorithm.

Figure 3



Figure 3 shows the finger being presented in two different places on the enrollment device. The MSO300 or 1300 will actually discard any non-matching prints and average those remaining out of the three presentations. If the third print was in a different place again, the software would either accept one as being a match and use that or reject the enrollment. However, matching on two prints isn't as good as three identical prints

Figure 4



In this example the captured finger has a large amount of oil on it and pressure was quite high on the reader lens. This will probably work okay but is not ideal. A user needs well defined ridges and troughs as well as intersection points in the print. These sites are the matching points used to develop the algorithm which is the finger template that subsequent finger presentations are matched against at the Biometric Device.

Figure 5



This is an example of the presentation required for the best possible enrollment by a user. This example has good information like visible ridges and intersection points for development of the algorithm by the enrollment device. A full print is presented to the window and even pressure from the finger. The print should use as much of the finger phalange as possible.

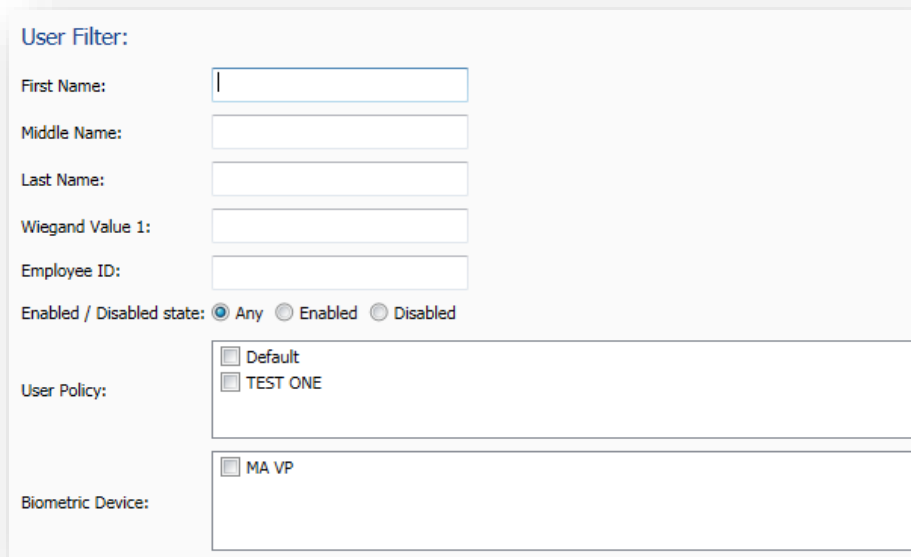
User Actions

There are several additional functions available for user management.

- Edit:** Opens the already saved user details for viewing or editing.
- Delete:** Use with caution as the user's details will be permanently deleted. This operation cannot be undone.
- Refresh:** Refreshes the user list from the database. This will update the display with the most current data.
- Disable User:** When a user is disabled they no longer have access to any Biometric Device. All access logs and user information is retained for reporting. Disabled users can be enabled at any time.
- Export Photo:** The photo stored in the User record can be saved to disk.
- Add Photo:** A photo from disk can be used as the user's photo. This is useful if a camera is not connected to the PC.

Filtering

The display of users can be filtered by clicking the **Filter** button. Select the required items and click **Ok**. The list of users will automatically be updated using the new filter information. To return the filters to their original state click **Reset Filters**. To display all users click **Show All**.

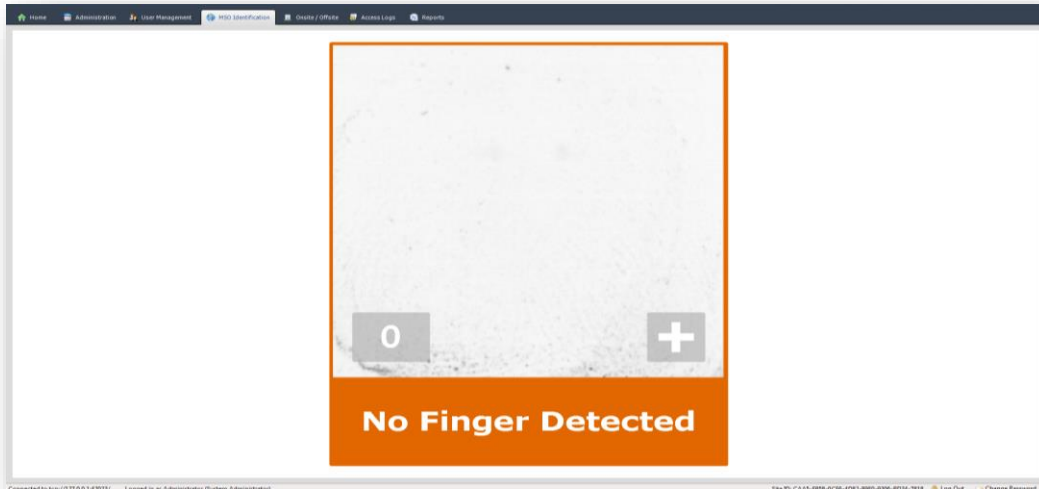


The screenshot shows a 'User Filter' dialog box with the following fields and options:

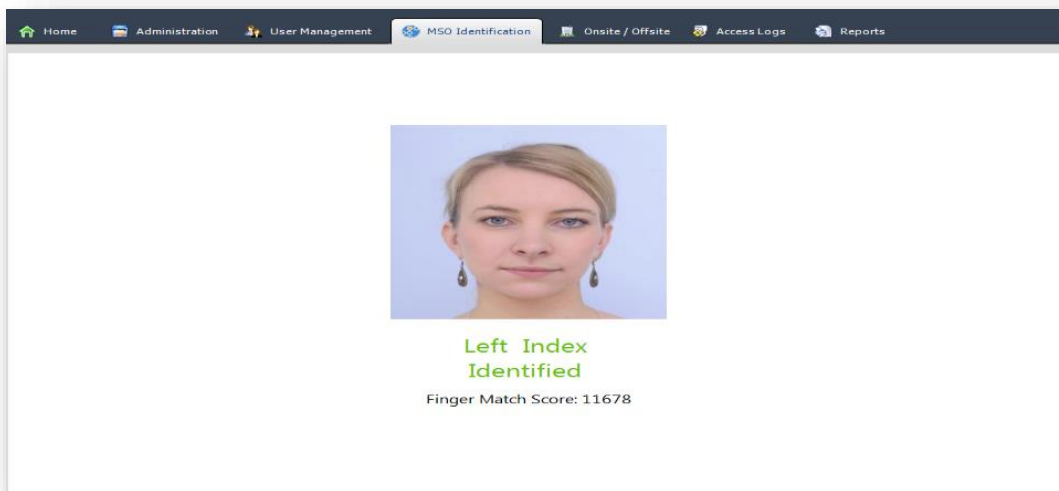
- First Name:** Text input field.
- Middle Name:** Text input field.
- Last Name:** Text input field.
- Wiegand Value 1:** Text input field.
- Employee ID:** Text input field.
- Enabled / Disabled state:** Radio buttons for Any, Enabled, and Disabled.
- User Policy:** A list box containing Default and TEST ONE.
- Biometric Device:** A list box containing MA VP.

MSO Identification

The MSO Identification section allows for users fingerprints to be identified using the configured MorphoSmart device.

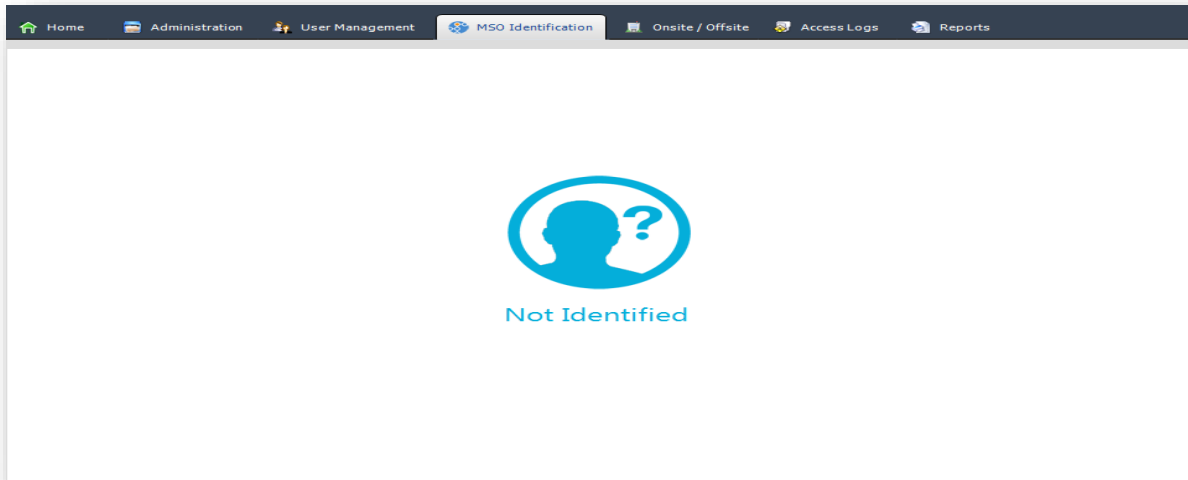


Once the user presents their fingerprint to the MSO device an “Identified” or “Not Identified” screen will be shown.



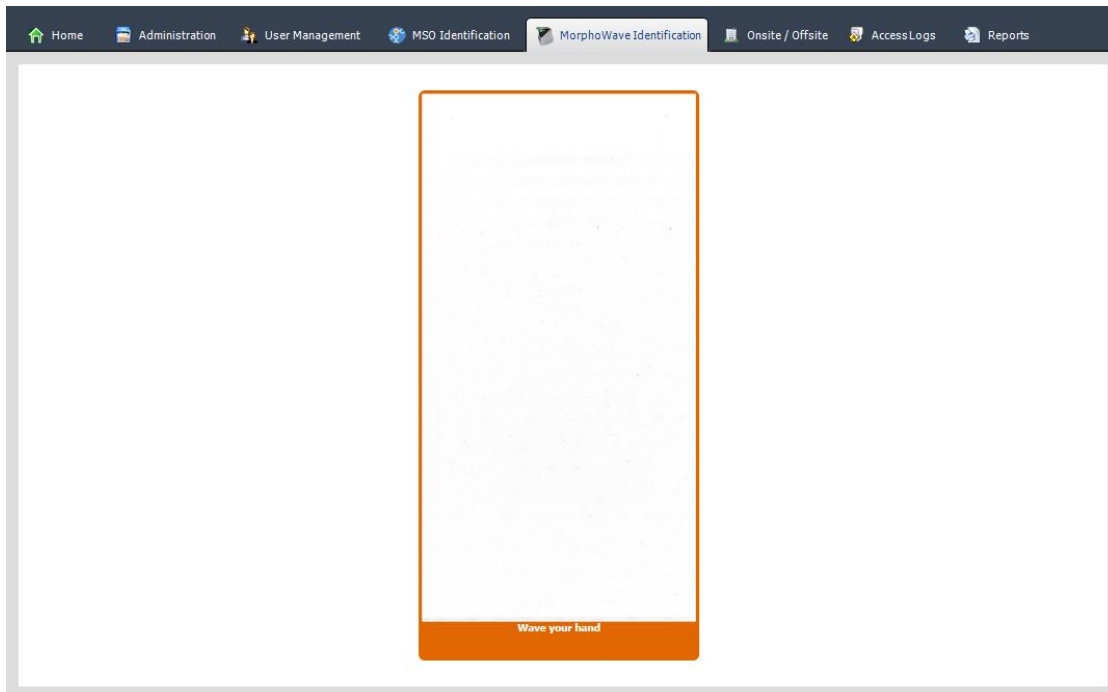
Identified: The identified user’s name, photo and identification score (if using an unsecured MSO device) will be displayed.

Not Identified: If the captured fingerprint is not matched against a previously enrolled finger, the “Not Identified” screen will be shown.

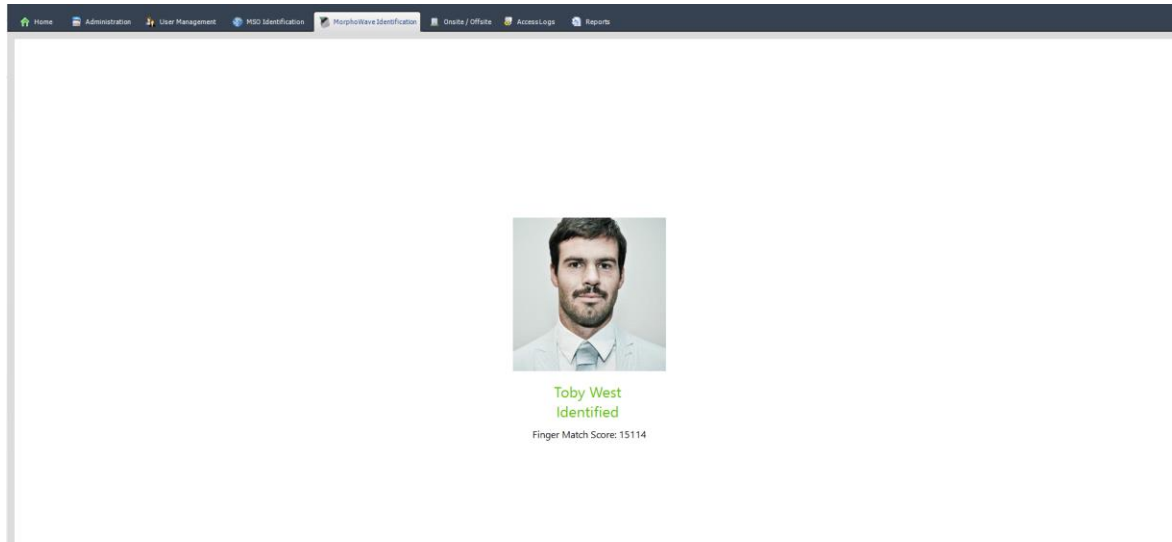


MorphoWave Identification

The MSO Wave Identification section allows for user's hands to be identified using the configured Morpho Wave device.

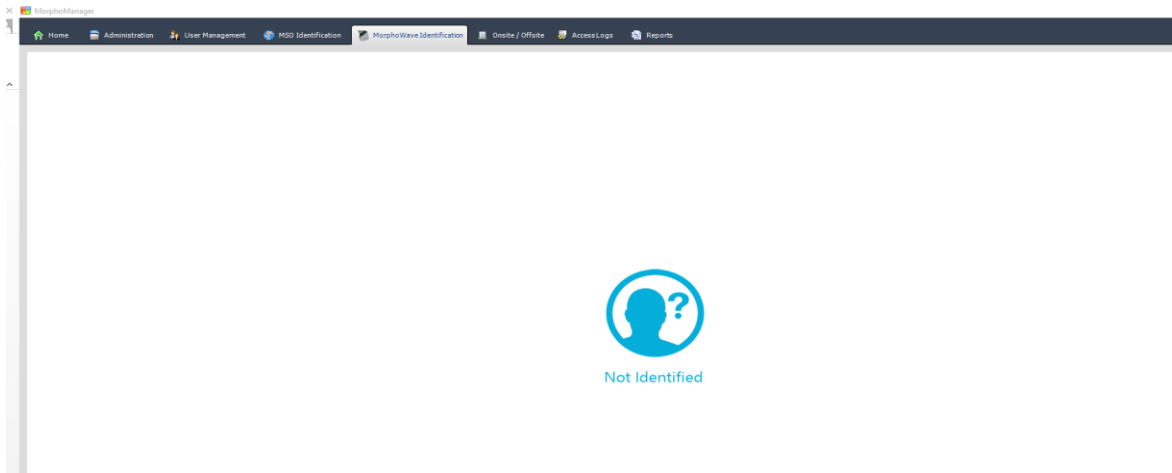


Once the user presents their hand to the Morpho Wave device an “Identified” or “Not Identified” screen will be shown.



Identified: The identified user’s name, photo and identification score will be displayed.

Not Identified: If the captured hand is not matched against a previously enrolled hand, the “Not Identified” screen will be shown.



Onsite/Offsite



The Onsite/Offsite tab is hidden by default. In order to access this section it will need to be turned on in the Clients section of Administration. Once it has been checked, log out and back into MorphoManager. Additionally, it's functionality to record Onsite and Offsite movement needs to be enabled via the User Onsite/Offsite section on the System Configuration>System Functionality tab.

The Onsite section is used to show which users are currently onsite or offsite. The Onsite and Offsite items in the tree view on the left can be expanded to show user groups.

User Name	User Policy	Last Presented
First_000010 Last_000010	MW 1	5/9/2017 1:46:55 PM
First_000011 Last_000011	Default	5/9/2017 1:46:55 PM
First_000012 Last_000012	Default	5/9/2017 1:46:55 PM
First_000013 Last_000013	Default	5/9/2017 1:46:55 PM
First_000014 Last_000014	Default	5/9/2017 1:46:55 PM
First_000015 Last_000015	MW 1	5/9/2017 1:46:55 PM
First_000016 Last_000016	Default	5/9/2017 1:46:55 PM
First_000017 Last_000017	MW 1	5/9/2017 1:46:55 PM
First_000018 Last_000018	MW 1	5/9/2017 1:46:55 PM
First_000019 Last_000019	MW 1	5/9/2017 1:46:55 PM
First_000020 Last_000020	Default	5/9/2017 1:46:55 PM
First_000021 Last_000021	MW 1	5/9/2017 1:46:55 PM

Selected User

First_000016 Last_000016

Status: On Site
Time On Site: 00 hr, 01 min
Last Activity: 5/9/2017 1:46:55 PM

Set User Off-Site

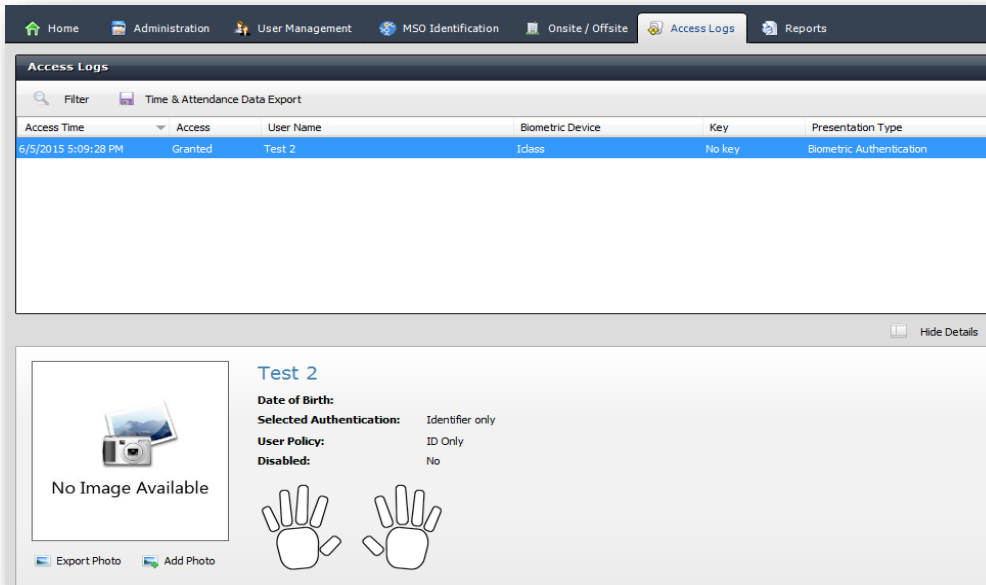
NOTE:

To manually set a user onsite/offsite, click on the User in the Main screen and click on **Set User Off-Site** or **Set User On-Site**.

Depending on the Biometric Device Onsite mode that has been set, the users will be shown in onsite or offsite.

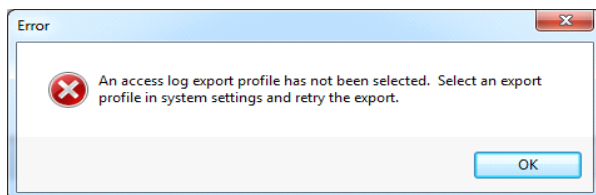
Access Logs

An access log is a record of transactions recorded by the system.



To filter the display of access logs, click **Filter**. Enter or select the details for filtering and click **Ok**. To reset the filters to their original state, click **Reset Filters**.

Before the access log can be exported, you need to create an Export profile. This is an initial setup procedure and is performed only once unless you need to export to another type of time and attendance application. The following error will be displayed if the profile has not been created.

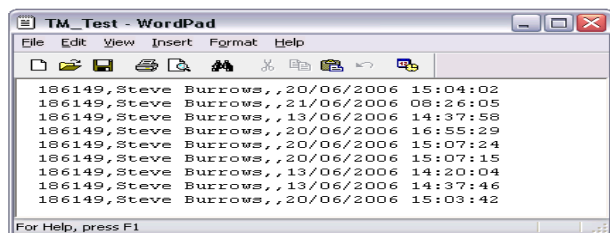


Refer to the system configuration section for instructions on configuring an access log export profile.

Once an access log exporter has been set-up, click on **Export Access logs** and you are presented with a window showing the destination of the file. Enter a file name with its extension and click on **Save**.

Note: Employee ID and Export value must be present to be exported into the logs. Biometric Device name and User ID are NOT exported.

The following is an example of Exported Access logs.



Reports

The reports center has a variety of reporting options for displaying information about user activity.

- List Report:** Displays a list of all items in the selected category (Biometric Device, Operators and Users)
- User Policy Members Report:** Displays a list of all users that are members of the selected user policy.
- Activity Reports:** These reports will show all activity for the selected item type.

User Activity Report

- Select the desired date range. The default **Date Range** date and time is one week previous.
- Select the User. Enter the first few characters of both the first and last name. Select Search. Once the user is on the screen, select the user and click **Generate Report**.

Biometric Device Activity Report

- Select the desired Date Range. The default **Date Range** date and time is one week previous.
- Select the Biometric Device. Enter the first few characters of the name of the Biometric Device. Select Search. Once the Biometric Device is on the screen, select the Biometric Device and click **Generate Report**. If you are not sure of the name or spelling of the Biometric Device, click on **Search** with an empty search box and all the Biometric Device will appear.

User Policy Activity Report

- Select the desired Date Range. The default **Date Range** date and time is one week previous.
- Select the User Policy. Enter the first few characters of the name of the policy. Select Search. Once the policy is on the screen, select it and click **Generate Report**. If you are not sure of the name or spelling of the policy, click on **Search** with an empty search box and all the user policies will appear.

All Activity (included all users and Biometric Device).

- Select the desired Date Range. The default **Date Range** date and time is one week previous.
- Click **Generate Report**.

Inactivity Report

- Select the desired Date Range. The default **Date Range** is one week previous.
- Select the User Policy. Enter the first few characters of the name of the user policy. Select Search. Once the user policy is on the screen, select the user policy and click **Generate Report**.

List Report

- Select the Report type from the options Biometric Device, Operator, User and User Policy.
- Click **Generate Report**.

User Policy Members Report

- Search and select the User Policy and click on **Generate Report**.

Permissible Report

- Select the Report type (Biometric Device or User).
- Search for the Biometric Device name or the user name and click on **Generate Report**.

Tools and Utilities

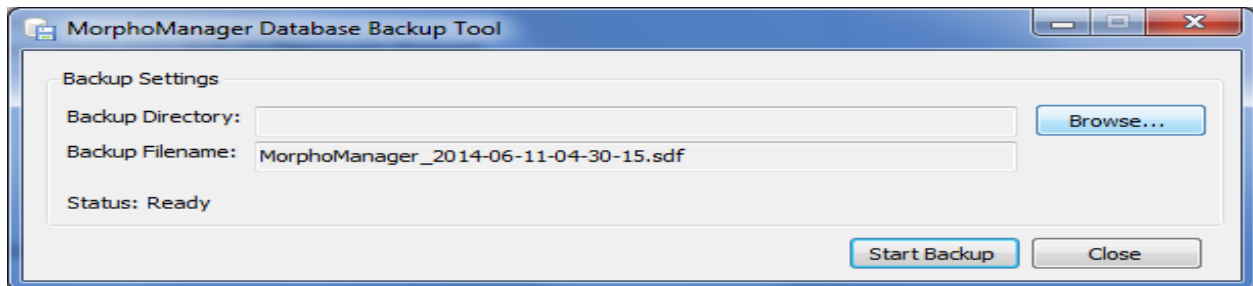
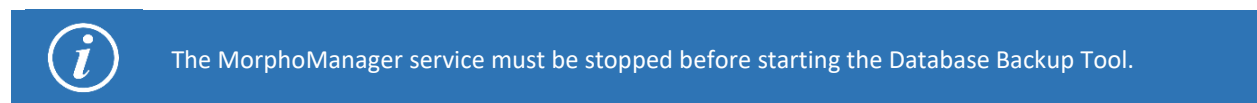
The following tools and utilities can be found in the Windows Start Menu under the MorphoManager folder.

Database Management

Database Backup Tool

The Backup Tool allows for the backup of SQLCE database. Systems running SQL Server will need to contact Microsoft for backup information.

When you start the Database Backup Tool, you will be prompted for backup directory. Select the directory you want to back up the database to.



Browse

Click Browse to change the backup directory

Start Backup

Starts the backup process.

Database Copy Tool

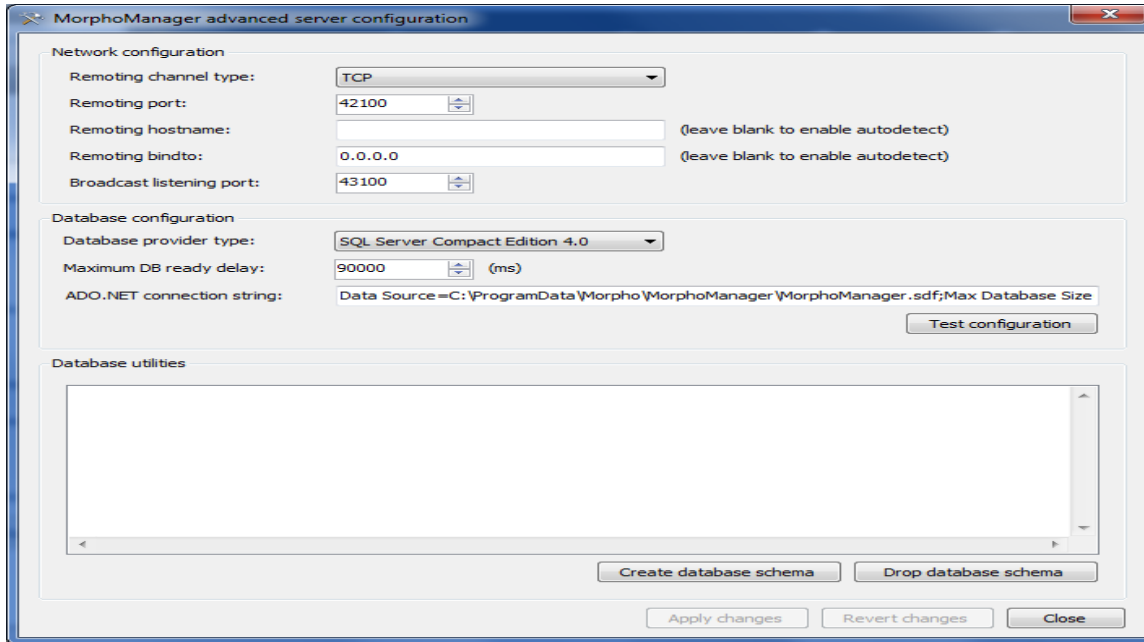
The Database Copy Tool copies a databases table schema and data from one database to another. This allows for easy upgrading from the default SQL CE database to Microsoft SQL server when the system grows beyond the limits of SQL CE.

For customer support on Microsoft SQL Server, please contact [Microsoft SQL Server TechCenter](#).

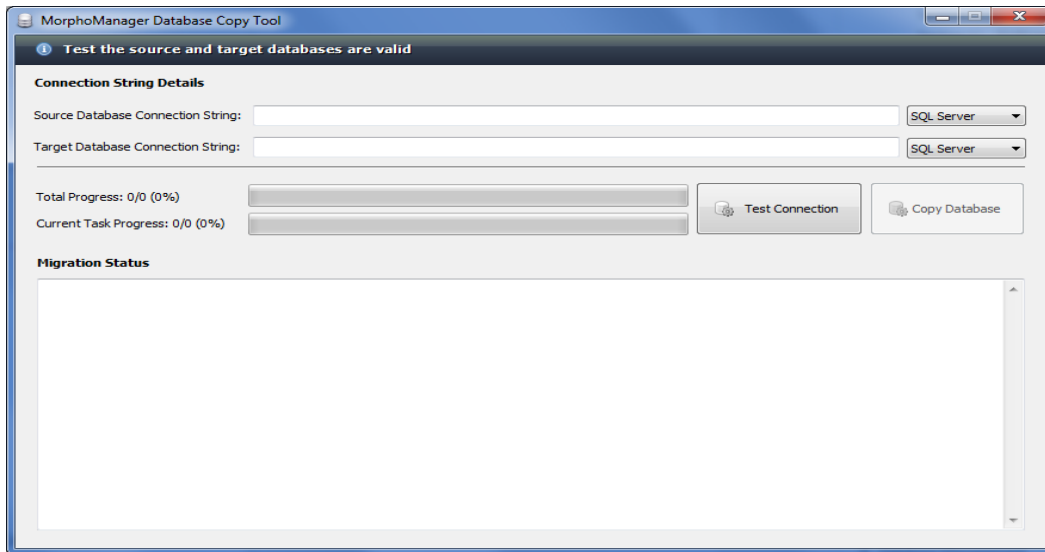
Copying a database

The following instructions are for upgrading the default SQL CE database to Microsoft SQL Server.

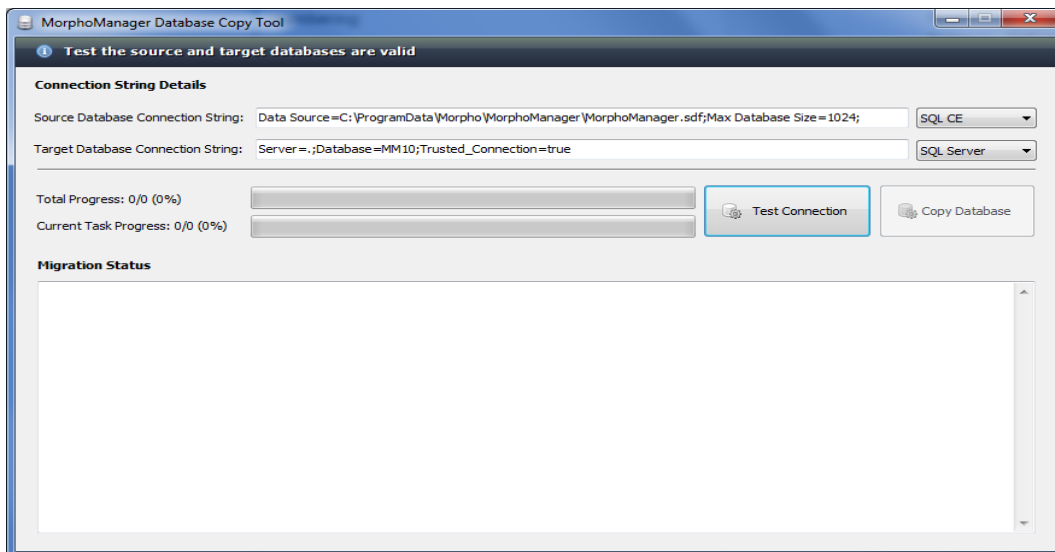
- **BACKUP YOUR CURRENT DATABASE.**
- Install and configure Microsoft SQL Server.
- Create a new database (MorphoManager)
- Stop MorphoManager Server
- Start Advanced server configuration



- Set Database provider type to SQL Server 2005 or later
- Set the ADO.Net connection string for the database you created. Save the existing ADO.NET connection string for later use.
- Apply changes
- Test configuration
- Create the database schema in the new database
- Start Database Copy Tool
- Connect String Details



- Enter the ADO.NET connection string saved from 5.2 into the Source Database Connection String field.
- Set the correct database type using the dropdown lists.
- Test Connections
- Copy Database



- Verify your source and target database connection strings
- Click **Copy Database** button

All data within the target database will be erased.

Review the migration status to ensure no errors were encountered.

Biometric Device Setup

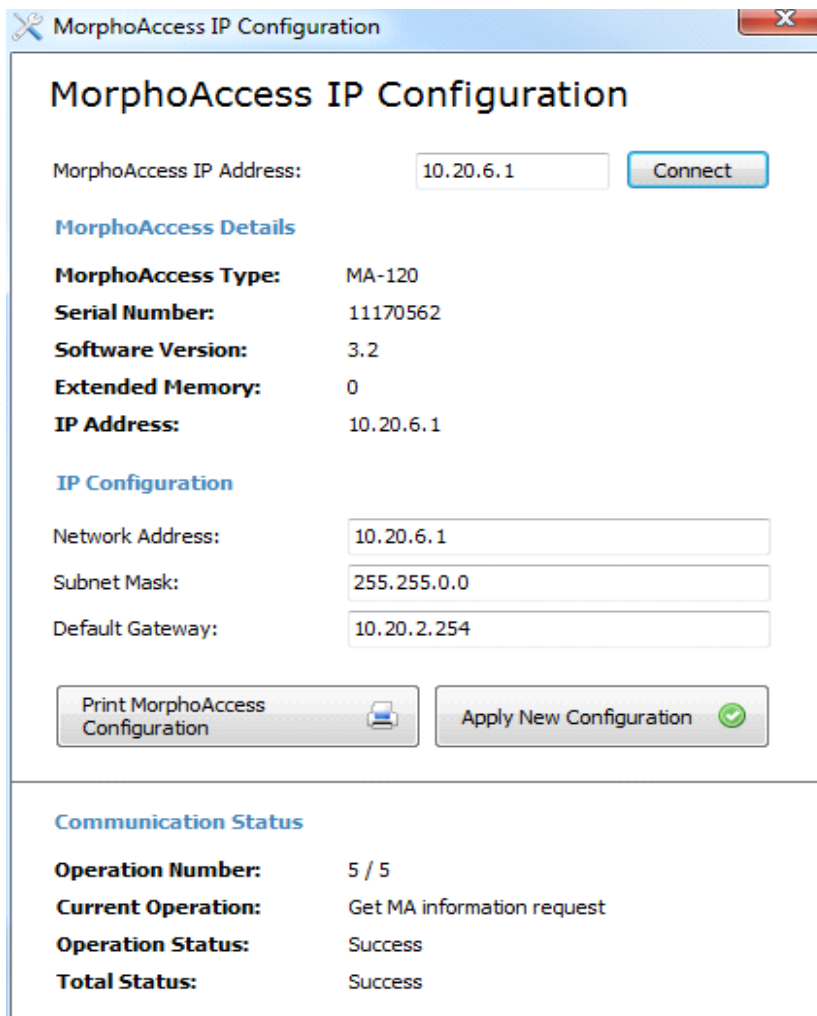
Biometric Device IP Address Configuration

By default, all MA2G biometric devices shipped from Safran are set to a default configuration.

IP Address: 134.1.32.214
Subnet Mask: 255.255.0.0
Default Route: 134.1.6.1

Use the Biometric Device IP Address Configuration Tool to change it.

The tool is located on the server installation in the program files menu.



The screenshot shows the 'MorphoAccess IP Configuration' window. At the top, there is a title bar with a wrench icon and the text 'MorphoAccess IP Configuration'. The main content area is titled 'MorphoAccess IP Configuration' and contains several sections:

- MorphoAccess IP Address:** A text box containing '10.20.6.1' and a 'Connect' button.
- MorphoAccess Details:** A section with the following fields:
 - MorphoAccess Type:** MA-120
 - Serial Number:** 11170562
 - Software Version:** 3.2
 - Extended Memory:** 0
 - IP Address:** 10.20.6.1
- IP Configuration:** A section with the following fields:
 - Network Address:** 10.20.6.1
 - Subnet Mask:** 255.255.0.0
 - Default Gateway:** 10.20.2.254
- Buttons:** Two buttons are located at the bottom of the configuration section: 'Print MorphoAccess Configuration' (with a printer icon) and 'Apply New Configuration' (with a green checkmark icon).
- Communication Status:** A section at the bottom with the following fields:
 - Operation Number:** 5 / 5
 - Current Operation:** Get MA information request
 - Operation Status:** Success
 - Total Status:** Success

Enter the existing IP address of the Biometric Device and click **Connect**.

Enter the new configuration and click **Apply New Configuration**.

Biometric Device Profile Creation Tool

This tool will allow you to generate a Biometric Device Profile from MA2G or MA5G family parameters that are set on a device. The data will be collected and a file created that can be imported into MorphoManager to utilize as an advanced BDP.

The Tool can be accessed by clicking on the start menu, then selecting “MorphoManager”, followed by “MorphoManager Biometric Device Profile Creation Tool”.

IP/Hostname: IP/Hostname of the device that is intended to be used.

Port: Default

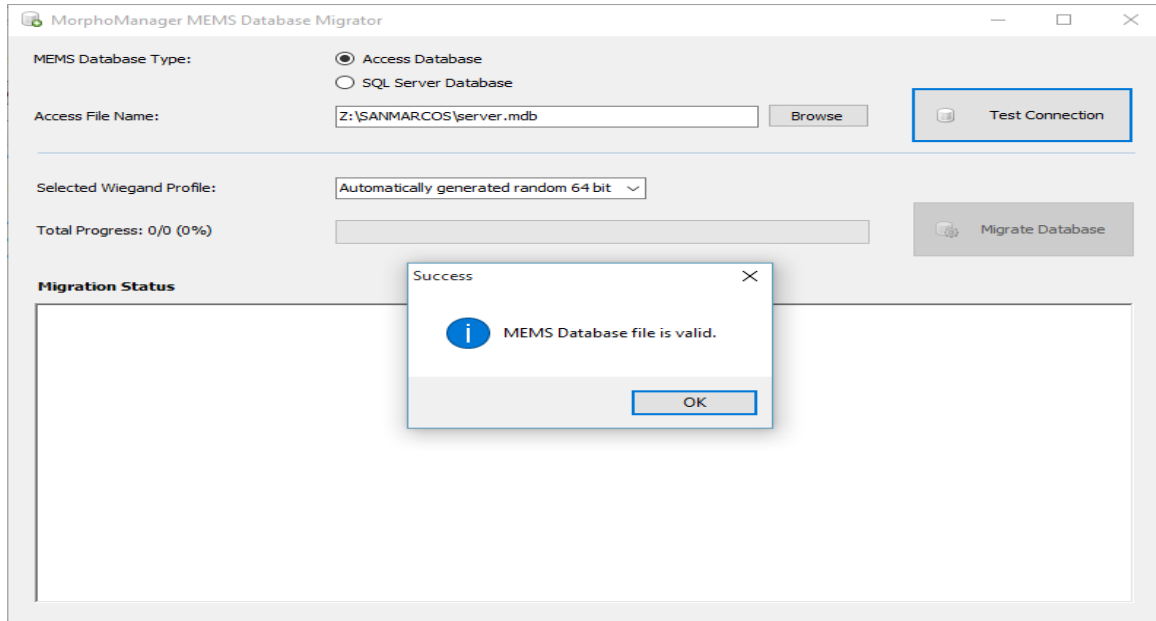
Hardware Family: There are two options in the drop down.
MA 100, MA J, MA 500 or MA VP
MA Sigma



The screenshot shows a window titled "Biometric Device Profile Creation Tool" with the MorphoManager logo. Below the logo, the title "Biometric Device Profile Creation Tool" is repeated. A descriptive paragraph states: "This tool allows you to create a MorphoManager Biometric Device Profile based off the current settings of a MorphoAccess device. Simply enter the device's IP or hostname, select the appropriate hardware type and click Create." The form includes three input fields: "IP/Hostname:" (empty), "Port:" (containing "11010"), and "Hardware family:" (a dropdown menu with "MA 100, MA J, MA 500" selected). A "Create" button is positioned below these fields. At the bottom of the window, there is a "Status:" label above a large empty text area and a "Close" button.

MEMS Migrator

The MEMS Migrator tool will migrate users from the MEMS database selected into MorphoManager. MEMS users and their groups will be migrated to User Policies and User Distribution Groups in MorphoManager. An empty User Distribution Group will be created for every MEMS Group migrated. Biometric Devices can then be added to the User Distribution Groups to mimic the MA(s) used in the MEMS groups.



- Select the MEMS database type and file to migrate
- Click **Test Connection** to see if it is valid (see screen shot above).
- If valid, select the Wiegand Profile to use for migrated users.
- Click **Migrate Database**.
- When the Migration Status panel shows a successful migration, the migration process is finished.

SecureAdmin / SecureAdmin Lite Migrator

The SecureAdmin Migrator tool will migrate users from a SecureAdmin or Secure Admin Lite database in either SQL or Oracle platforms into MorphoManager. SecureAdmin users' demographics & biometrics are migrated. The migration tool allows the user to specify which SecureAdmin user group(s) and biometric template type(s) are migrated to the specified MorphoManager user policy. The tool is intended to be installed on the same PC as the SecureAdmin / SecureAdmin Lite server and will auto-detect the SecureAdmin / SecureAdmin Lite database to simplify the migration process. A manual connection string can also be entered. The SecureAdmin Migrator tool is available from your Morpho support representative.

The tool will step the user through a series of screens filtering how data is to be migrated.

Below is a summary of the SecureAdmin Migrator tool screens.

- 1) SecureAdmin Database Type & Connection String: Auto-detects (manual connection also available) and tests the connection to the SecureAdmin database to be migrated into MorphoManager
- 2) Template Types to Migrate: Template types to migrate can be selected or omitted on this screen
- 3) User Migration Options: User can select SecureAdmin User Groups and/or individual template types to map to MorphoManager User Policy (shown below)
- 4) Confirmation Dialog: A dialog will be displayed indicating that continuing the migration process will overwrite previously migrated data in the MorphoManager database with the exception of newly captured Morpho biometric templates
- 5) Migration Progress: A status bar will provide the status on the migration process
- 6) Summary: A summary of successfully migrated users, failed users and a total of all users. The option to export lists for both successful and failed users is also available.

SecureAdmin & SecureAdmin Lite Database Migrator

Secure Admin ,Secure Admin Lite Migrator

User migration options

Please select whether SecureAdmin User Groups should be migrated as MorphoManager User Policies.
You may also select whether to migrate additional user information from SecureAdmin, including address, phone, etc.

SecureAdmin User Group	Template Type	MorphoManager User Policy
TEM_Group	TEM	TEM_Group
VUR_Group	VUR	VUR_Group
BUR_Group	BUR	TEM_Group
▶▶		

If there are users not covered by the mappings above migrate them to MorphoManager User Policy: Default

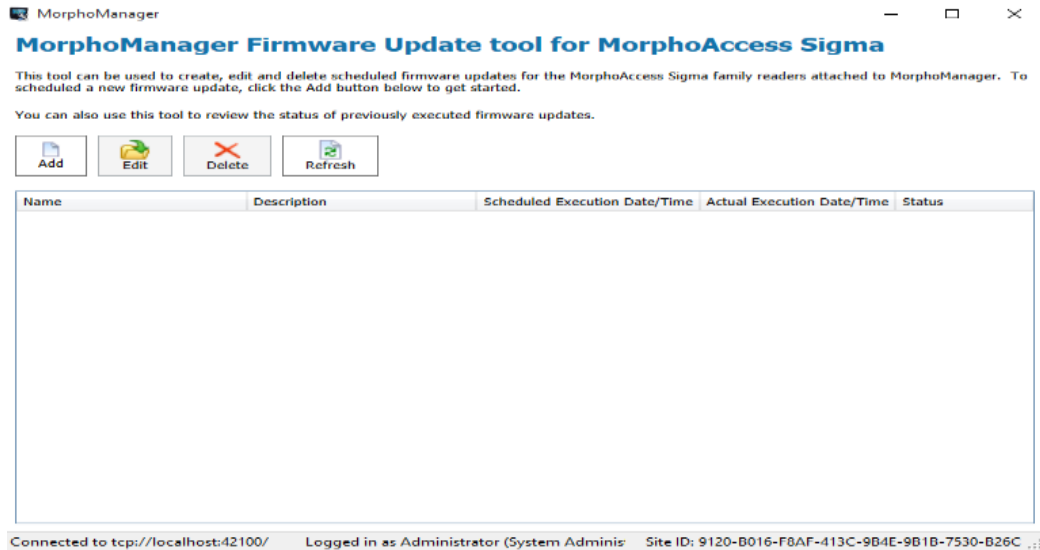
Migrate user address fields
 Migrate user phone numbers

Back Next Finish Cancel

Connected to tcp://127.0.0.1:42100/ Logged in as Administrator (System Administrat Site ID: B3EB-ECD5-E0AA-4A03-ADD4-EB3E-43B0-4253

MA Sigma Firmware Update Tool

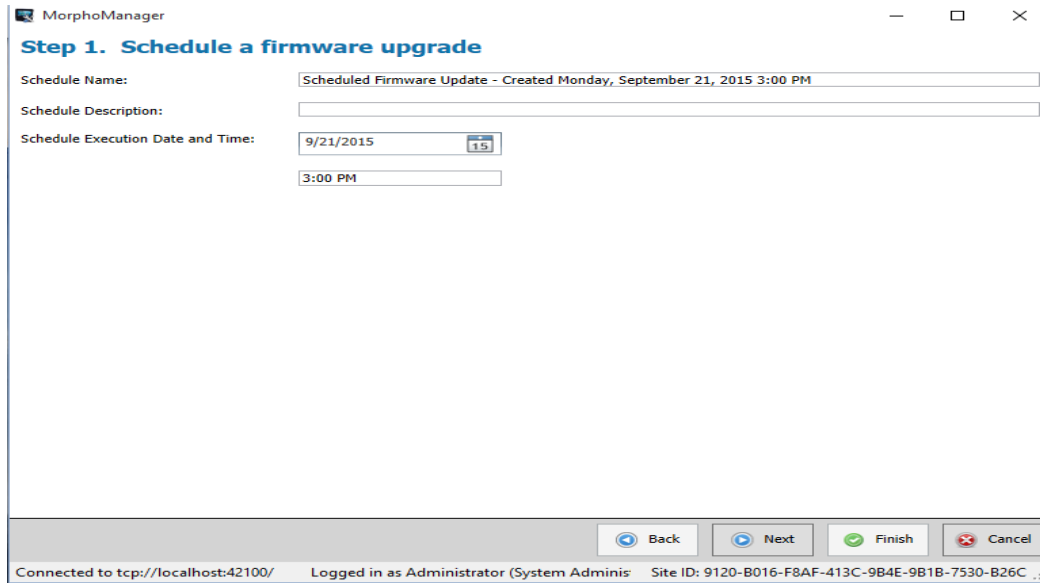
The Firmware Update Tool is designed to be used only for the Sigma Family of hardware (5G).



Create a Firmware Update job

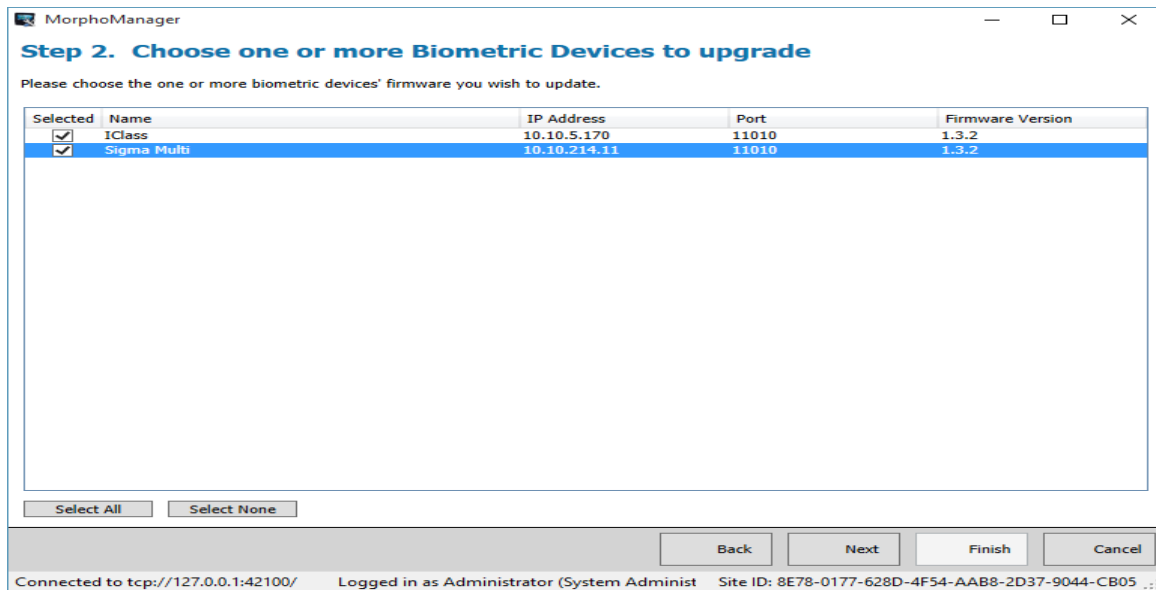
From the home screen above click **Add** to create a Firmware Update job to be executed.

Screen 1



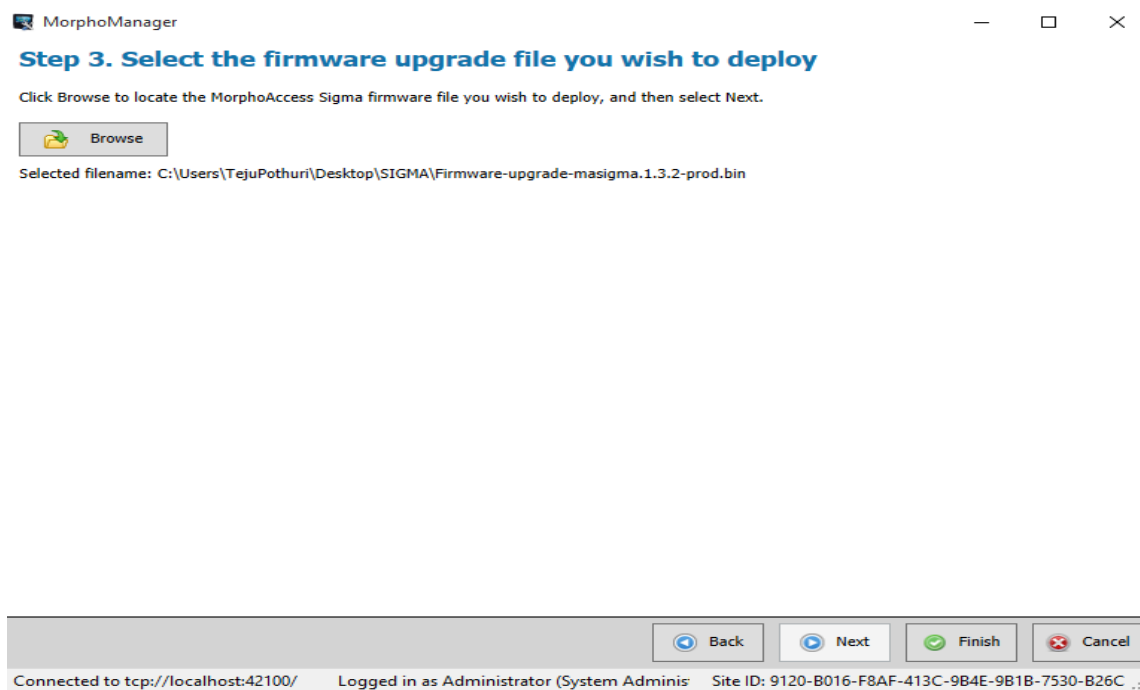
Set the date and time to run the firmware update job. By default, it will run immediately. However, this can be scheduled to run at a future date and time. Click **Next**.

Screen 2

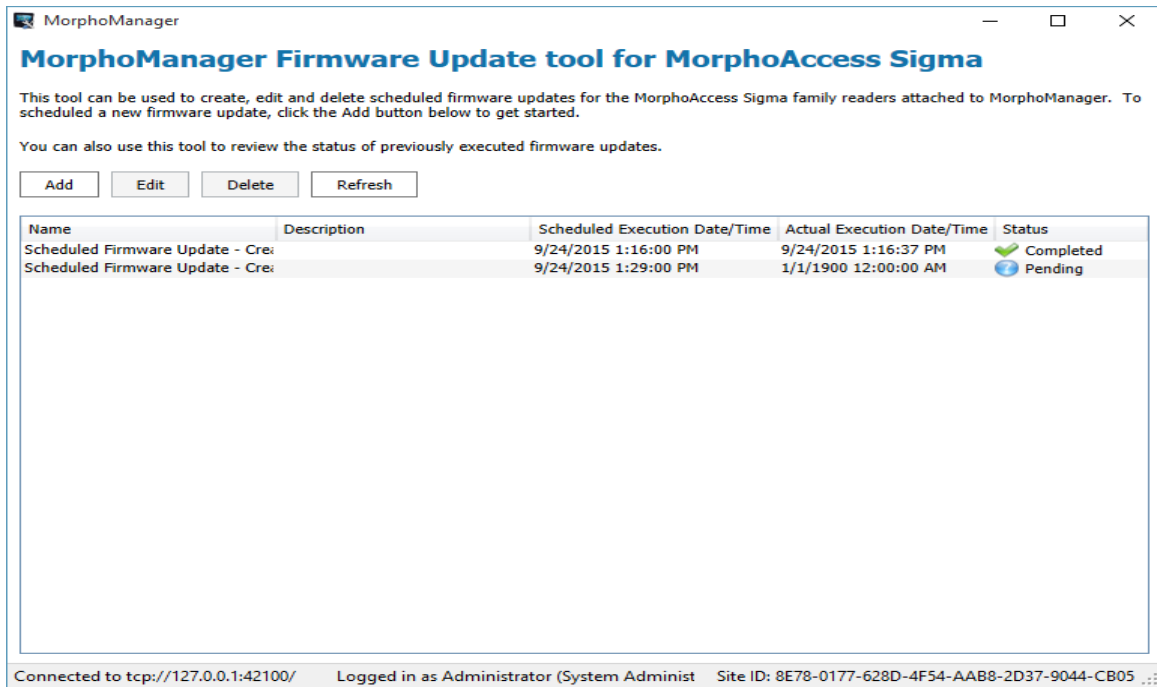


Select the Biometric Device(s) connected to MorphoManager that will be included in this Firmware Update. Click **Next**.

Screen 3



Browse and select the firmware update version file to be applied to the Biometric Devices selected on Screen 2. Click **Finish**. The tool will return to the main screen below.



The Firmware Update jobs generated will be listed on the main screen with their execution status, date and time. Unexecuted jobs can be edited or deleted. Completed ones can be deleted. If the job status shows it has failed, further detail can be found in MorphoManager’s Event Log.

MA 500 Series: Old block board wiring

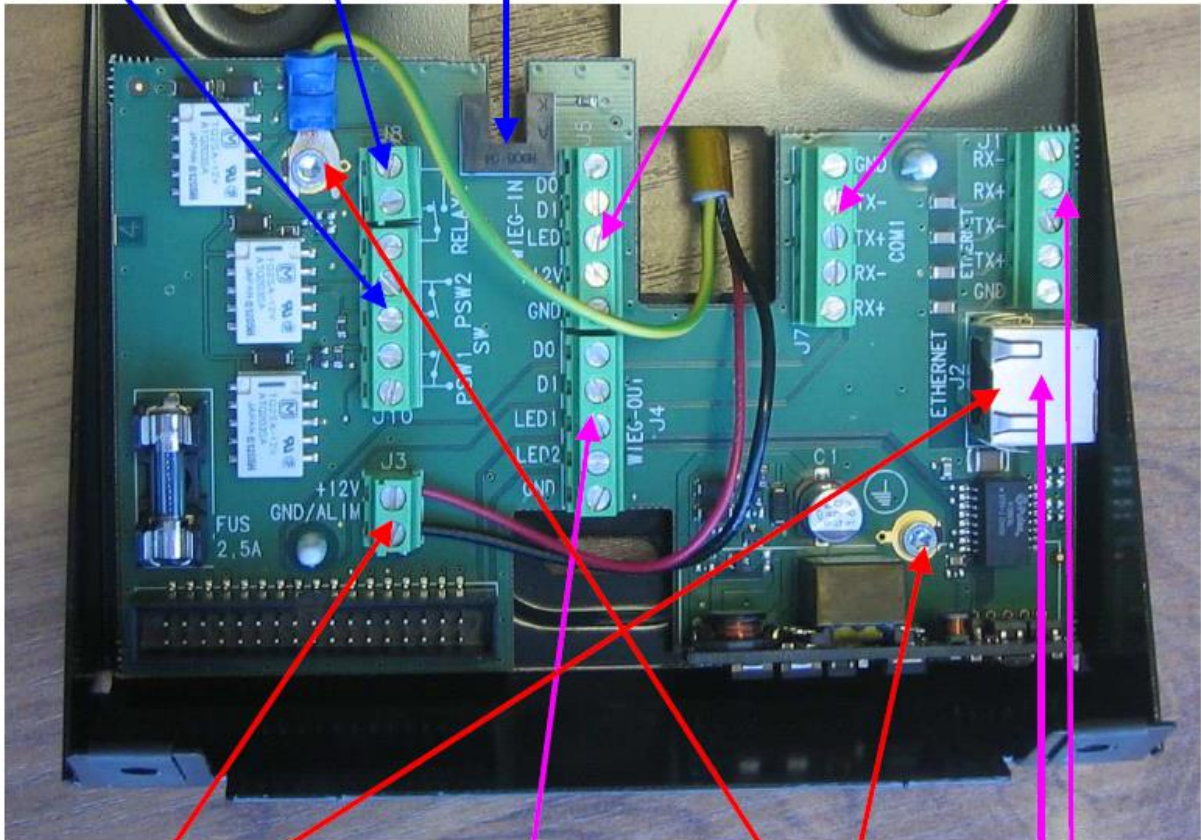
Tamper switch
Anti theft switch

Relay

Anti theft opto

Wiegand IN
Dataclock IN

COM
RS422 / RS485



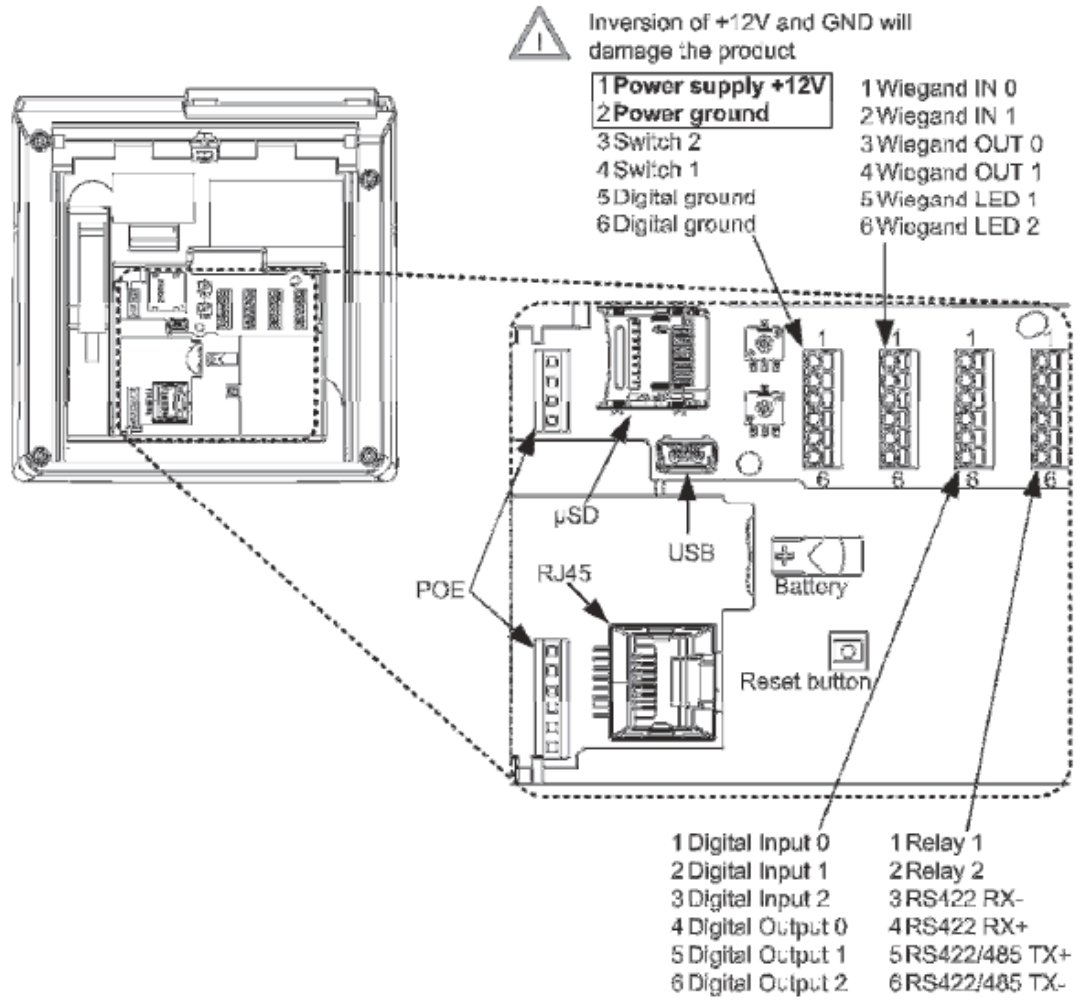
Power supply source
External +12V DC
or
Power Over Ethernet

Wiegand OUT
Dataclock OUT

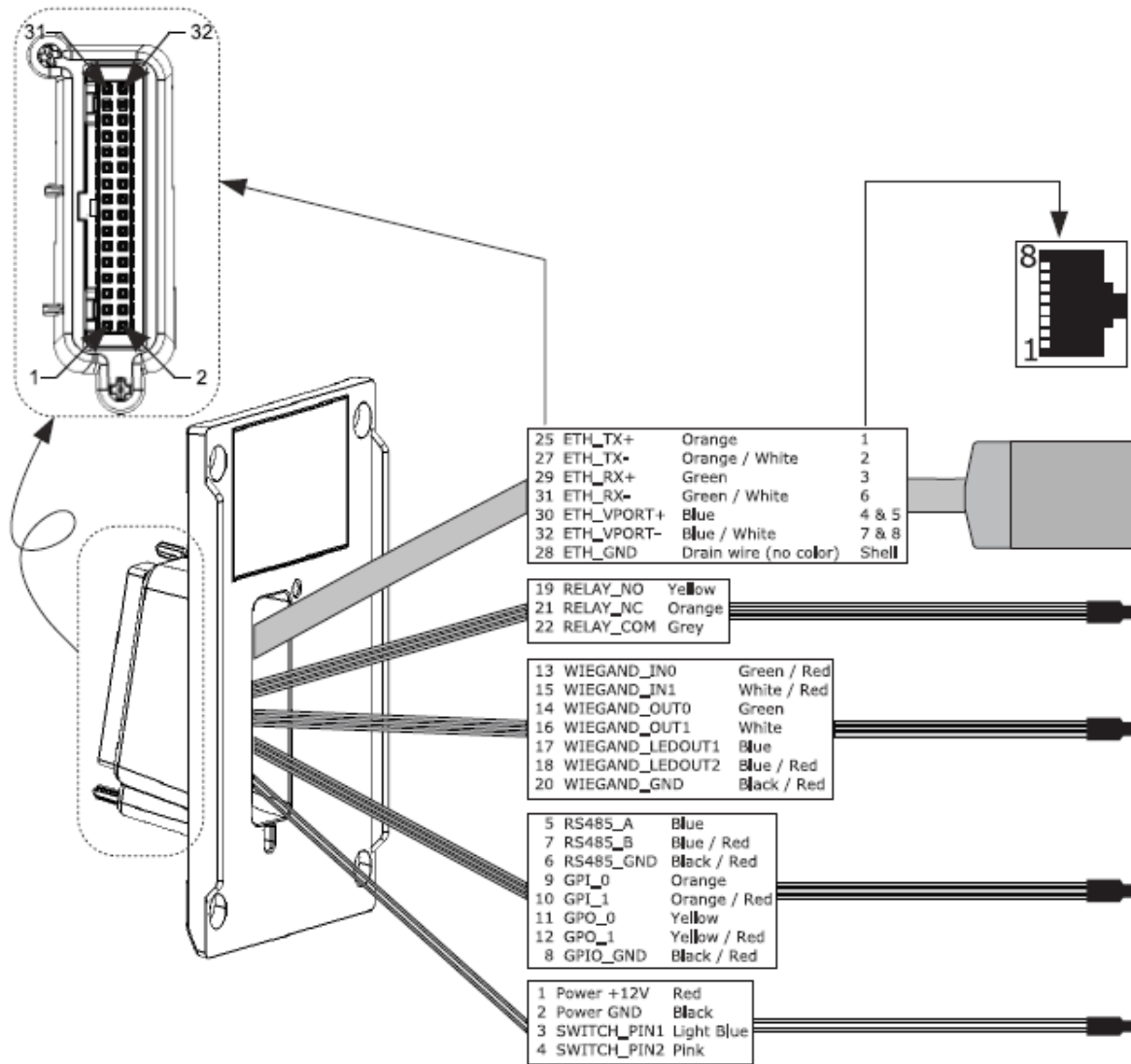
Ground
security
reference

Ethernet
Terminal block
or
RJ45

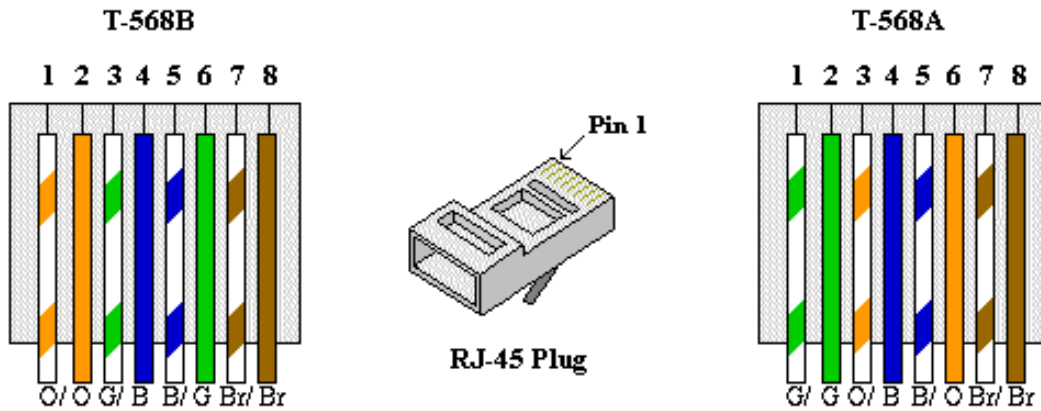
MA Sigma Series: Cabling Diagram



MA Sigma Lite Series: Cabling Diagram

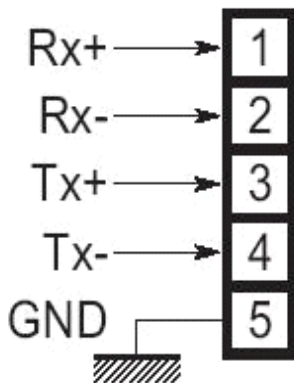


Ethernet Interface (LAN 10 Mbps)



T568B and T568A RJ45 Wire Positions

Pin	Signal	T568B Connection	T568A Connection
1	Tx (+) (Transmit Data +)	White Orange	White Green
2	Tx (-) (Transmit Data -)	Orange	Green
3	Rx (+) (Receive Data +)	White Green	White Orange
4	No Connection	Blue	Blue
5	No Connection	White Blue	White Blue
6	Rx (-) (Receive Data -)	Green	Orange
7	No Connection	White Brown	White Brown
8	No Connection	Brown	Brown



Biometric Device TCP\IP Ethernet Wiring

Create a straight-through connection when connecting the Biometric Device into a Hub/Switch

Create a cross-over connection when connecting the Biometric Device directly into a computer.

RJ45 Wire Positions	Biometric Device Wiring	Result
T568B	T568B	Straight-through
T568B	T568A	Cross-over
T568A	T568A	Straight-through
T568A	T568B	Cross-over

For a straight-through connection match the T568B RJ45 Wire Positions to the T568B Biometric Device TCP\IP Ethernet Wiring.

For a cross-over connection, match the T568A RJ45 Wire Positions to the T568B Biometric Device TCP\IP Ethernet Wiring.

For a straight-through connection match the T568A RJ45 Wire Positions to the T568A Biometric Device TCP\IP Ethernet Wiring.

For a cross-over connection, match the T568A RJ45 Wire Positions to the T568B Biometric Device TCP\IP Ethernet Wiring.

Power Supply source

			MA 500 / MA 500+ Series OMA	500 Series
1	+12V	In	Positive 12 Volts, power supply	Red
2	GND/ALIM	In	Ground power supply	Black
	Ground	In	Ground security reference	Yellow/green

External power supply: Must conform to CEE/EEC EN60950 standard 9V to 16 Volts \pm 5% (regulated) 1.5 Amp minimum (peak) Power may come from a 12Volt Wiegand power supply, conforming to the Security Industry Association's Wiegand standard March 1995, able to deliver 9 Watts.

In standard operating activity, typical power consumption is 4.5 Watts. In extreme temperature conditions, with all options (USB Flash drive, 12V output for Wiegand in), maximum power consumption is up to 9 Watts. These Biometric Device make use of POE functionality; if Ethernet network is POE compatible, power supply may come from Ethernet wiring.

Wiegand output wiring

MA 500 / MA 500+ Series				OMA 500 Series
1	D0	Out	Wiegand D0	Wiegand Dataclock cable Green
2	D1	Out	Wiegand D1	White
3	LED1	In	Wiegand LED In 1 (Option)	Brown
4	LED2	In	Wiegand LED In 2 (Option)	Gray
5	GND		Ground for Wiegand	Black

Wiegand input wiring

MA 500 / MA 500+ Series				OMA 500 Series
1	D0	In	Wiegand D0	Wiegand Blue
2	D1	In	Wiegand D1	Yellow
3	LED	Out	Wiegand LED Out 1 (Option)	Orange
4	+12V	Out	12 Volts Power output (150mA max)	Red
5	GND		Ground for Wiegand	Black

Output relay and Tamper-Switch

MA 500 / MA 500+ Series				OMA 500 Series
1	CRO		Contact relay normally open	Switch/relay cable Red
2	CRC		Contact relay normally closed	Orange
3	CR		Contact relay common	Yellow
4	TSW2_1		Tamper switch Contact 1	White
5	TSW2-0		Tamper switch Contact 0	Green
6	ATSW1_1		Anti theft switch Contact 1	Not available
7	ASTW1_0		Anti-theft switch Contact 0	Not available
	Ground		Not connected	Black