# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Support</td>
<td>5</td>
</tr>
<tr>
<td>Overview</td>
<td>6</td>
</tr>
<tr>
<td>What is a client?</td>
<td>6</td>
</tr>
<tr>
<td>What is a server?</td>
<td>6</td>
</tr>
<tr>
<td>What is a fingerprint enrollment device?</td>
<td>6</td>
</tr>
<tr>
<td>What is a Biometric Device?</td>
<td>7</td>
</tr>
<tr>
<td>Setting up MorphoManager</td>
<td>7</td>
</tr>
<tr>
<td>Computer hardware requirements</td>
<td>7</td>
</tr>
<tr>
<td>Supported Operating Systems</td>
<td>7</td>
</tr>
<tr>
<td>Supported USB Enrollment Devices</td>
<td>7</td>
</tr>
<tr>
<td>Supported Biometric devices</td>
<td>8</td>
</tr>
<tr>
<td>Supported Card Reader / Encoders</td>
<td>10</td>
</tr>
<tr>
<td>Biometric Device Capacity</td>
<td>11</td>
</tr>
<tr>
<td>Biometric Device supported firmware</td>
<td>11</td>
</tr>
<tr>
<td>Installation of MorphoManager software</td>
<td>12</td>
</tr>
<tr>
<td>Updating to MorphoManager 15.0.0</td>
<td>12</td>
</tr>
<tr>
<td>Setting up MorphoManager on a single PC</td>
<td>13</td>
</tr>
<tr>
<td>Server and Client Installation</td>
<td>14</td>
</tr>
<tr>
<td>MorphoManager Client Configuration</td>
<td>15</td>
</tr>
<tr>
<td>Basic</td>
<td>15</td>
</tr>
<tr>
<td>Advanced</td>
<td>16</td>
</tr>
<tr>
<td>Login Options</td>
<td>18</td>
</tr>
<tr>
<td>MorphoManager Server Manager</td>
<td>19</td>
</tr>
<tr>
<td>Home</td>
<td>19</td>
</tr>
<tr>
<td>Database Configuration</td>
<td>19</td>
</tr>
<tr>
<td>Advanced Configuration</td>
<td>20</td>
</tr>
<tr>
<td>Running MorphoManager</td>
<td>23</td>
</tr>
<tr>
<td>Login</td>
<td>23</td>
</tr>
<tr>
<td>Product Registration</td>
<td>23</td>
</tr>
<tr>
<td>Procedure for registration</td>
<td>24</td>
</tr>
<tr>
<td>Activate Online</td>
<td>24</td>
</tr>
<tr>
<td>Activate Offline</td>
<td>26</td>
</tr>
<tr>
<td>Express Configuration</td>
<td>27</td>
</tr>
<tr>
<td>Device discovery</td>
<td>27</td>
</tr>
<tr>
<td>Authentication modes</td>
<td>28</td>
</tr>
<tr>
<td>Card selection</td>
<td>29</td>
</tr>
<tr>
<td>Home Screen</td>
<td>31</td>
</tr>
<tr>
<td>Administration</td>
<td>32</td>
</tr>
<tr>
<td>Operator</td>
<td>32</td>
</tr>
<tr>
<td>Creating a new Operator</td>
<td>32</td>
</tr>
<tr>
<td>Key Policy</td>
<td>35</td>
</tr>
<tr>
<td>Creating a new Key Policy</td>
<td>35</td>
</tr>
<tr>
<td>Lock &amp; Unlock</td>
<td>43</td>
</tr>
<tr>
<td>Biometric Device Configuration</td>
<td>44</td>
</tr>
<tr>
<td>Creating a new Biometric Device Configuration (Express)</td>
<td>44</td>
</tr>
<tr>
<td>Creating a new Biometric Device Configuration (Advanced)</td>
<td>60</td>
</tr>
<tr>
<td>Creating a new Biometric Device Configuration (External)</td>
<td>64</td>
</tr>
<tr>
<td>Biometric Device</td>
<td>65</td>
</tr>
<tr>
<td>Create a Biometric Device</td>
<td>65</td>
</tr>
<tr>
<td>Modify a Biometric Device</td>
<td>66</td>
</tr>
<tr>
<td>Delete a Biometric Device</td>
<td>67</td>
</tr>
<tr>
<td>Biometric Device Status and Tasks</td>
<td>67</td>
</tr>
<tr>
<td>Troubleshooting and Maintenance</td>
<td>68</td>
</tr>
<tr>
<td>Toolbar Functions</td>
<td>68</td>
</tr>
<tr>
<td>Refresh</td>
<td>68</td>
</tr>
<tr>
<td>Synchronize</td>
<td>68</td>
</tr>
<tr>
<td>Get Logs</td>
<td>68</td>
</tr>
</tbody>
</table>
MorphoManager User Manual

View Sync Log ........................................................................................................68
Set Date/Time ........................................................................................................69
Rebuild ..................................................................................................................69
Set Online .............................................................................................................69
Wiegand Profiles ..................................................................................................70
Create a Wiegand Profile .......................................................................................70
User Configuration ...............................................................................................73
Create a new User Configuration ........................................................................73
Access Schedules ..................................................................................................77
Create an Access Schedule ..................................................................................77
User Distribution Group .......................................................................................79
Create a User Distribution Group .......................................................................79
User Authentication Mode ....................................................................................80
Create a new User Authentication Mode .............................................................80
Operator Role .......................................................................................................84
Notifications .........................................................................................................86
Create a new Notification ......................................................................................86
Clients ..................................................................................................................88
Screen 1 – Enter the details for this Client .........................................................88
Screen 2 – Select the tabs displayed on this Client ..............................................89
Screen 3 - Camera Configuration .........................................................................90
Screen 4 – Key Policy ............................................................................................91
Screen 5 - Enrollment Devices .............................................................................91
Scheduled Reports ..............................................................................................92
Card Template ......................................................................................................95
Card Encoding Log ...............................................................................................96
Event Logs ............................................................................................................96
Exception Logs .....................................................................................................96
System Configuration .........................................................................................96
Time and Attendance ..........................................................................................96
Communications Engine ....................................................................................99
System Functionality .........................................................................................100
System Management .........................................................................................101
Gateways .............................................................................................................102
BioBridge .............................................................................................................103
Privacy Mode .......................................................................................................105
MorphoTablet ......................................................................................................105
Card Template Management .............................................................................105
Finger Template Capture Options .......................................................................107
Display Options ...................................................................................................108
MorphoWave .......................................................................................................108
Duplication Control ............................................................................................109
User Management ...............................................................................................112
User Details .........................................................................................................112
Creation and enrollment of a User ......................................................................114
Screen 1 – User Details .......................................................................................114
Screen 2 – Additional Details ..............................................................................115
Screen 3 – Contact Details ..................................................................................116
Screen 4 – User Defined Fields ..........................................................................116
Screen 5 – Wiegand Values (If a Wiegand Profile is set) .....................................116
Screen 6 – User Distribution Groups ..................................................................117
Screen 7 – Photo Capture .....................................................................................117
Screen 8 – PIN Code ............................................................................................118
Screen 9 – 3D Face ...............................................................................................119
Screen 10 – Wave Enrollment ............................................................................120
Screen 11 – Fingerprint Capture .........................................................................123
User Management Toolbar ................................................................................127
Edit .......................................................................................................................127
Delete ..................................................................................................................127
Refresh ...............................................................................................................127
Disable User .......................................................................................................127
Import ..................................................................................................................127
Verification - Database .......................................................................................128
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Photo</td>
<td>128</td>
</tr>
<tr>
<td>Add Photo</td>
<td>129</td>
</tr>
<tr>
<td>Filter</td>
<td>129</td>
</tr>
<tr>
<td>Biometric Identification</td>
<td>130</td>
</tr>
<tr>
<td>Contact Fingerprint Identification</td>
<td>130</td>
</tr>
<tr>
<td>Contactless Fingerprint Identification</td>
<td>131</td>
</tr>
<tr>
<td>Onsite/Offsite</td>
<td>132</td>
</tr>
<tr>
<td>Transaction Logs</td>
<td>133</td>
</tr>
<tr>
<td>Reports</td>
<td>135</td>
</tr>
<tr>
<td>User Activity Report</td>
<td>135</td>
</tr>
<tr>
<td>Biometric Device Activity Report</td>
<td>135</td>
</tr>
<tr>
<td>User Configuration Activity Report</td>
<td>135</td>
</tr>
<tr>
<td>All Activity (included all users and Biometric Device)</td>
<td>135</td>
</tr>
<tr>
<td>Inactivity Report</td>
<td>135</td>
</tr>
<tr>
<td>List Report</td>
<td>135</td>
</tr>
<tr>
<td>User Configuration Members Report</td>
<td>136</td>
</tr>
<tr>
<td>Permissible Report</td>
<td>136</td>
</tr>
<tr>
<td>User ID duplicate report</td>
<td>136</td>
</tr>
<tr>
<td>Fingerprint Biometric duplicate report</td>
<td>136</td>
</tr>
<tr>
<td>Windows Certificate Store</td>
<td>136</td>
</tr>
<tr>
<td>Importing a Certificate to the Store</td>
<td>136</td>
</tr>
<tr>
<td>Checking the Certificate Store</td>
<td>140</td>
</tr>
<tr>
<td>Tools and Utilities</td>
<td>141</td>
</tr>
<tr>
<td>Database Management</td>
<td>141</td>
</tr>
<tr>
<td>Database Backup Tool</td>
<td>141</td>
</tr>
<tr>
<td>SQL Compact to SQL Server Database Migrator</td>
<td>141</td>
</tr>
<tr>
<td>Migrating a database</td>
<td>141</td>
</tr>
<tr>
<td>Biometric Device Configuration Creation Tool</td>
<td>143</td>
</tr>
<tr>
<td>MA Sigma Firmware Update Tool</td>
<td>144</td>
</tr>
<tr>
<td>Create a Firmware Update job</td>
<td>144</td>
</tr>
<tr>
<td>Screen 1</td>
<td>144</td>
</tr>
<tr>
<td>Screen 2</td>
<td>145</td>
</tr>
<tr>
<td>Screen 3</td>
<td>145</td>
</tr>
</tbody>
</table>
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 users’ fingerprints, 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 four types of fingerprint enrollment devices:

- **MorphoSmart 300**
  USB Fingerprint Reader

- **MorphoSmart 1300**
  USB Fingerprint Reader

- **MorphoSmart FVP**
  USB Fingerprint and Vein Reader

- **MorphoWave Desktop**
  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?
A Biometric Device is 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.

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: 100Mbs 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)
Screen Resolution: 1080p

Supported Operating Systems
MorphoManager Server:
- Microsoft Windows 7 SP1 64-bit - KB4019990 update installed
- Microsoft Windows 8.1 64-bit - KB4019990 update installed
- Microsoft Windows 10 64-bit (Anniversary update or later)
- Windows Server 2008 R2 SP1 64-bit - KB4019990 update installed
- Windows Server 2012 64-bit - KB4019990 update installed
- Windows Server 2012 R2 64-bit - KB2919355 update installed

MorphoManager Client:
- Microsoft Windows 7 SP1 32-bit / 64-bit - KB4019990 update installed
- Microsoft Windows 8.1 32-bit / 64-bit - KB4019990 update installed
- Microsoft Windows 10 32-bit / 64-bit (Anniversary update or later)
- Windows Server 2008 R2 SP1 64-bit - KB4019990 update installed
- Windows Server 2012 64-bit - KB4019990 update installed
- Windows Server 2012 R2 64-bit - KB2919355 update installed

Database server:
- SQL Server 2014 SP3 or newer

Supported USB Enrollment Devices
- MSO 300
- MSO 1300 E2
- MSO 1300 E3
- MSO 1350
- MSO 1350 E
- MSO 1350 E2
- MSO VP
- MorphoWave Desktop

**Supported Biometric devices**

<table>
<thead>
<tr>
<th>MorphoAccess 500+</th>
<th>MorphoAccess OMA 520</th>
</tr>
</thead>
<tbody>
<tr>
<td>MorphoAccess VP / MA VP MD</td>
<td>MorphoAccess J-Series</td>
</tr>
<tr>
<td>MorphoAccess Sigma</td>
<td>MorphoAccess Sigma Extreme</td>
</tr>
<tr>
<td>MorphoAccess Sigma Lite+</td>
<td>MorphoAccess Sigma Lite</td>
</tr>
<tr>
<td>Morpho 3D Face</td>
<td>MorphoWave Compact</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------</td>
</tr>
<tr>
<td><img src="image1" alt="Morpho 3D Face" /></td>
<td><img src="image2" alt="MorphoWave Compact" /></td>
</tr>
<tr>
<td>MorphoWave Tower</td>
<td>VisionPass</td>
</tr>
<tr>
<td><img src="image3" alt="MorphoWave Tower" /></td>
<td><img src="image4" alt="VisionPass" /></td>
</tr>
</tbody>
</table>
## Supported Card Reader / Encoders

### Supported Card Types and Card Readers

<table>
<thead>
<tr>
<th>Card Family</th>
<th>HID Prox</th>
<th>HID iClass</th>
<th>HID iClass Seos</th>
<th>MIFARE Classic</th>
<th>MIFARE DESFire EV0</th>
<th>MIFARE DESFire EV1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Variant</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HID® OMNIKEY® 5427CK</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>HID® OMNIKEY® 5427G2</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>HID® OMNIKEY® 5025CL</td>
<td>✔</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Identiv uTrust 3700F</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
</tr>
</tbody>
</table>

### Supported Card Capabilities

<table>
<thead>
<tr>
<th>Card Family</th>
<th>HID Prox</th>
<th>HID iClass</th>
<th>HID iClass Seos</th>
<th>MIFARE Classic</th>
<th>MIFARE DESFire EV0</th>
<th>MIFARE DESFire EV1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Card Variant</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read CSN/ID</td>
<td>✔</td>
<td>✔</td>
<td></td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Encode to Card</td>
<td>X</td>
<td>✔</td>
<td>✔</td>
<td>**</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Read PACS Data</td>
<td>X</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

* Encoding is not supported for HID iClass® 2K/2
** Encoding to HID® iClass® Seos® cards requires the application already exists on the card due to the hardware limitation with the HID® OMNIKEY® 5427 CK/G2
Biometric Device Capacity
MorphoManager is limited to a capacity of 5000 total biometric devices. Below are the maximum number of devices that can be added to MorphoManager for each device family.

<table>
<thead>
<tr>
<th>Hardware Family</th>
<th>Device Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of devices</td>
<td>Up to 5000 total devices</td>
</tr>
<tr>
<td>2G</td>
<td>Up to 500</td>
</tr>
<tr>
<td>All other devices</td>
<td>Up to 5000</td>
</tr>
</tbody>
</table>

If an attempt is made to add more devices from a family than MorphoManager Supports, that device will not be added to the system.

Biometric Device supported firmware
Below are the firmware versions that have been tested and validated to work with MorphoManager.

<table>
<thead>
<tr>
<th>Device Series</th>
<th>Supported firmware version</th>
</tr>
</thead>
<tbody>
<tr>
<td>MorphoAccess 100 Series</td>
<td>3.2.10</td>
</tr>
<tr>
<td>MorphoAccess 500 Series</td>
<td>3.9.0</td>
</tr>
<tr>
<td>Outdoor MorphoAccess 500 Series</td>
<td>3.9.0</td>
</tr>
<tr>
<td>MorphoAccess J Series</td>
<td>3.8.0</td>
</tr>
<tr>
<td>MorphoAccess VP Series</td>
<td>3.11.0</td>
</tr>
<tr>
<td>MorphoAccess Sigma Series</td>
<td>4.6.0</td>
</tr>
<tr>
<td>MorphoAccess VP MD Series</td>
<td>4.7.3</td>
</tr>
<tr>
<td>MorphoWave Tower</td>
<td>2.3.0</td>
</tr>
<tr>
<td>MorphoWave Compact Series</td>
<td>1.5.3</td>
</tr>
<tr>
<td>VisionPass</td>
<td>2.4.0</td>
</tr>
<tr>
<td>Morpho 3D Face Reader</td>
<td>4.8.2.0.0.0.0.0</td>
</tr>
</tbody>
</table>

Devices with a firmware version lower than the supported version will remain offline. The status of these devices will change to Online only once the devices are updated to the minimum firmware version or higher.
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://www.morphomanager.net/](http://www.morphomanager.net/)

Updating to MorphoManager 15.0.0

MorphoManager 14.6.x is required to update to MorphoManager 15.0.0

It is not possible to update to MorphoManager 15 from any other version than 14.6.x
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 enrollment device to the PC.
- Ensure the Biometric Devices are on the same network as the MorphoManager Server and are in the same IP range.
- Start MorphoManager Client – 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 connect.

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.
MorphoManager Client Configuration

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

### Basic

Server connection details

- **Hostname**: By default, it will be localhost. Use this setting when the client and server are installed on the same PC.
  - If the server is installed on a different PC to the client. Enter the hostname or IP address of the server in the hostname box.

- **Port**: Specifies the server port that the MorphoManager Server is accepting client connections on. The default port is: 42100. 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.
**Client protocol settings:** This is the protocol the client will use to connect to the MorphoManager Server. This value should be SOAP 1.2 Binary, unless instructed to change this by customer support.

**TLS Mode – Transport:** The communication between server and client will be encrypted. This mode does not validate the authenticity of the MorphoManager Server.

**TLS Mode – Transport and Mutual Authentication:** The communication between server and client will be encrypted. This mode will also validate the authenticity of the MorphoManager Server.

**Client Certificate thumbprint:** Used to specify the thumbprint of the client certificate. This thumbprint will then be used to find, validate, and return the certificate from the certificate store. MorphoManager will use this certificate to encrypt communications between client and server.

The following is required of the certificate to pass validation:
• The certificate exists in either the Personal or Trusted Root Certification Authorities collection store
• The certificate contains a private key
• The certificate’s Key Usage Extension contains a Key Encipherment or Data Encipherment flag
• The certificate’s Enchased Key Usage Extension contains a valid Server Authentication value (1.3.6.1.5.5.7.3.1)

Server certificate Authentication mode:

If **Disabled** is selected, MorphoManager will perform no further validation on the certificate.

When **Client Server Certificate Common Issuer** is selected, the server certificate and client certificate must have the same issuer.

When **Server Certificate thumbprint** is selected, the operator must specify the server certificate thumbprint. If the server’s certificate thumbprint does not match the thumbprint specified here, the connection will be refused, because the server authentication failed.

When **Server Certificate issuer thumbprint** is selected, the operator must specify the server certificate issuer thumbprint. If the server’s certificate issuer thumbprint does not match the thumbprint specified here, the connection will be refused, because the server authentication failed.
Login Options

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 username and password if it is unnecessary.

Operator override:
The operator will be able to change the advanced settings before logging in.
MorphoManager Server Manager
The MorphoManager Server Manager can be found by clicking on the start menu, then selecting “MorphoManager” and “MorphoManager Server Manager”.

Home
The server control is used to start and stop the MorphoManager server. Stopping the server should only be performed if instructed by the support staff. To start or stop the server, click the Power icon.

Database Configuration
Database Connection
Database Type: There are two database provider types:

- SQL Server (2014 SP3 or later)
- SQL Server Compact Edition 4.0

SQL server Compact Edition 4.0 is selected by default and is the option for smaller installations. The SQL Server 2014 SP3 or later
edition is used on larger installations, or where an existing SQL Server is already available. It is recommended to use SQL Server for any live production environment.

**Database Connection String:**

This is the connection string that will be used to connect to the database. Enter the connection string and click Test Configuration. Ensure the connection is successful before saving changes.

**Database Schema Management**

**Delete Database Schema:**

Deleting a database schema will remove all tables and all data from the database. This is a non-recoverable operation and cannot be undone. **A drop database schema cannot be reverted.** A prompt will be displayed confirming this action.

**Create Database Schema:**

Creating a database schema can only be performed on a new, empty database. This operation will set up a database and create all the tables and default data for MorphoManager.

**Validate Database Schema:**

Validating a database schema will reveal if there are any errors or issues in the current database schema.

**Advanced Configuration**

**Basic**

**Listening 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.

**TLS Settings (Advanced)**

**TLS Mode – Transport:**

The communication between server and client will be encrypted. This mode does not validate the authenticity of the MorphoManager Server.

**TLS Mode – Transport and Mutual Authentication:**

The communication between server and client will be encrypted. This mode will also validate the authenticity of the MorphoManager Server.

**Server Certificate Discovery Mode:**

**Search and create self-signed certificate if discovery fails** will first search the Windows certificate store to determine if the server certificate already exists. The certificate is searched by Hostname as the Common Name. If no certificate is found by the hostname,
MorphoManager User Manual

MorphoManager Server will create a new self-signed server certificate.

**Search** will search the Windows certificate store to determine if the server certificate already exists. No certificate will be created if the certificate is not found.

**Thumbprint** lets the operator specify the server certificate thumbprint that should be used by the MorphoManager Server. The certificate needs to exist in the Windows Certificate store.

**Hostname Mode:**

*Automatically detected* can detect the hostname of the server and will use this detected hostname to search and/or create the server certificate.

**Hostname:**

The hostname of the MorphoManager server. This is the hostname that the client will connect to. This must be the same as the hostname specified in the client configuration.

**Server Certificate Thumbprint:**

Used to specify the thumbprint of the server certificate. This thumbprint will then be used to find, validate, and return the certificate from the certificate store. MorphoManager will use this certificate to encrypt communications between client and server.

The following is required of the certificate to pass validation:

- The certificate exists in either the Personal or Trusted Root Certification Authorities collection store
- The certificate contains a private key
- The certificate’s Key Usage Extension contains a Key Encipherment or Data Encipherment flag
- The certificate’s Encased Key Usage Extension contains a valid Server Authentication value (1.3.6.1.5.5.7.3.1)

**Client Certificate Authentication Mode:**

When **Client Server Certificate Common Issuer** is selected, the server certificate and client certificate must have the same issuer.

When **Client Certificate issuer thumbprint** is selected, the operator must specify the client certificate issuer thumbprint. If the client’s certificate issuer thumbprint does not match the thumbprint specified here, the connection will be refused, because the client authentication failed.

**Client Certificate Issuer**
Thumbprint: The operator must specify the client certificate issuer thumbprint. If the client’s certificate issuer thumbprint does not match the thumbprint specified here, the connection will be refused, because the server authentication failed.
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.

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 7 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.

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 internet, you will be prompted to **Start offline registration**.

Save the offline registration file to a known location.

In a web browser, navigate to [www.morphomanager.net](http://www.morphomanager.net) and follow the link for offline registrations. Follow the on-screen prompts. When done successfully, a “response” file will be generated. Download the response file to a known location.

Close and re-open the MorphoManager client. When prompted, select the option to complete an offline registration. Find and select the “response” file.

Once the file is loaded you will see a success message, indicating that MorphoManager is now registered.

If you experience difficulties during this process you may contact support. In the Americas email the file for registration processing to support.bioterminals.us@idemia.com. For the rest of the world, please email the file to support.bioterminals@idemia.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.
Express Configuration

Express Configuration will allow MorphoManager to be configured based on a series of wizard screens and prompts. For example, will the system be using biometric only, or will contactless cards be involved?

Once Express Configuration is created, MorphoManager will have a corresponding User Authentication Mode, User Configuration, and Biometric Device Configuration set as a default in MorphoManager. Therefore, when a Biometric Device is added to the system, the default Biometric Device Configuration for that terminal will be set to the one created by the first Express Configuration. The same will happen when creating a user and their default User Configuration. The system defaults for these items can be managed in System Configuration> System Functionality. Further details can be found in the System Configuration portion of the manual.

At the initial login to MorphoManager the Express Configuration creation wizard will launch automatically.

Follow the wizard prompts and answer the questions based on how the site installation will function.

Express Configuration does not support the configuration of 2G devices.

Device discovery

The second screen of the Express Configuration Wizard will detect devices. MorphoManager uses User Datagram Protocol (UDP) to discover devices.

If you have multiple network adapters, you will need to disable all but one that is used for network communications before starting the device discovery.
All detected devices will be displayed in the grid. Devices that did not respond within the timeout, will not be displayed.

It is only possible to discover devices with IPv4 addresses.

In this grid you can alter the **Name** and **Description** to suit your needs.

Mark all the devices you would like to add to MorphoManager by marking the checkbox in the Add column.

Devices that are already in MorphoManager will be marked in gray with a checkmark in the “Already in System” column.

MorphoManager Automatic Device discovery Firewall rules are created during MorphoManager installation.

- Inbound rule: UDP port 32002
- Outbound rule: UDP 32001

**Authentication modes**

The following authentication modes are supported for Express Configuration:

1. **Biometric Only**
   
   A user is authenticated by biometrics only. E.g. the user places the enrolled fingerprint on the biometric device, and they are granted access.

2. **Card Only**
   
   A user is authenticated by a card only. E.g. the user presents their card to the device and they are granted access. No Biometrics required.

3. **Card and Biometric**
A user is authenticated by a card and a biometric. Each user requires a card and a biometric. E.g. the user presents their card to the device, the device prompts them for their fingerprint, after the fingerprint is placed, the user is granted access.

4. **Card or Biometric**
   A user is authenticated by a card or a biometric. A user requires only a Biometric, or only a card. E.g. user A places their enrolled fingerprint on the biometric device to gain access. User A is not furnished with a card. User B presents their card to the device to gain access. User B does not have any fingerprints enrolled.
   It is also possible to furnish user A with a card, and User A will be able to gain access with a card only or with fingerprints only.

5. **Card and PIN**
   A user is authenticated by a card plus a PIN. E.g. the user presents their card to the MA device, they are prompted to enter a PIN. Access is granted if the PIN matches.

6. **Card and Biometric and PIN**
   A user is authenticated by a card, a biometric and a PIN. They are required to have all three. E.g. the user presents their card to the MA device, they are prompted to present their fingerprint, they are prompted to enter their PIN. Only if all three matches will access be granted.

7. **Wiegand in and Biometric**
   This mode is used in conjunction with another device that is connected to the MA device’s wiegand input connecters. E.g. the User presents their card to a separate card reader. This card reader is connected via wiegand to the MA. After the card was presented, the user is prompted to place their fingerprint on the MA device. Access is granted if the fingerprint is verified.

For each of the Authentication modes that include a biometric, the administrator can configure whether Contact templates, Contactless templates, or Face templates are required. For the Card Only and Card+ PIN authentication modes, Biometrics are not configurable and will never be required.

**Card selection**
On the card selection page, you can decide to manually select the cards you will use, or to automatically detect the cards that you have.

A supported USB Card reader must be attached to the Client if you wish to use the Automatic Card detection Mode:

1. Select the Automatic radio button
2. Select your card reader in the drop-down menu
3. Click the Read Card button
4. Place your card on the card reader and wait for the operation to complete
After the Express Configuration wizard is completed, the following items will be created in MorphoManager:

- Biometric Device Configuration
- User Configuration
- User Authentication Mode
- Set the defaults in System Configuration

These items will be given the same name as the Express Configuration they were created from. For further details on those items please see the corresponding section(s) of this manual.

The Express Configuration Wizard can also be launched at any time after the initial login to MorphoManager from an icon on the Home Tab.
Home Screen

At the top of the home screen, there is a set of tabs:

- Home
- Administration
- User Management
- Biometric Identification
- Access Logs
- 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 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 colored 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.

The System Administrator operator cannot be deleted or modified. This operator has access to every part of MorphoManager 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
Username: Enter a Username that will be used to log in to MorphoManager Client. When using Active Directory, it is necessary to enter the Username including the domain. Two formats may be used:
- Username@Domain
- Domain\Username

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.
- MorphoManager Username and Password: The Username and Password is stored in the MorphoManager database and is managed by MorphoManager
- Active directory: The password and account state are managed by Active Directory.

Administrator: Select this option to provide full administrator rights to this user (not recommended).

Password: To meet the password complexity rules, the password must be between 8 and 64 characters long. In addition, the password must contain at least 1 of the following criteria:
- At least one uppercase letter.
- At least one number.
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 the functions that the roles allow.
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

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.

Require password: Select this option to secure the Key Policy with a password. The gets set on the next page. Securing the Key Policy with a password adds an extra layer of security to MorphoManager. An operator will need to enter the password to view the card keys. This password is not required during card encoding.
Screen 2 – MIFARE Classic Key Settings
Set the keys for MIFARE Classic on this screen.

Contact Fingerprints:
- **Start write sector:** Sets the card write sector from where the encoding/reading should start for contact fingerprints.
- **Start write block:** Sets the block within the sector where the encoding/reading should start contact fingerprints.
- **Absolute block number:** This value correlates directly to the sc_tlv_mifare.start_block parameter for 5G devices. It is the overall block number of the card layout.

Contactless Fingerprints:
- **Start write sector:** Sets the card write sector from where the encoding/reading should start contactless fingerprints.
- **Start write block:** Sets the block within the sector where the encoding/reading should start contactless fingerprints.
- **Absolute block number:** This value correlates directly to the sc_tlv_mifare.start_block parameter for 5G devices. It is the overall block number of the card layout.
Screen 3 – MIFARE DESFire Key Settings
Set the keys for MIFARE DESFire on this screen.

**DESFire FID:** The File ID that should be used to read and write to the DESFire card.

**Set DESFire AID:** This button leads to the page where Application ID can be set. The DesFire AID may be entered in ASCII or in HEX by choosing the relevant radio button.
Screen 4 – iClass Encoding Settings
Set the encode/reading properties for iClass cards. This page also sets the Application ID and DO tag for Seos cards.

Start Reading from block setting applies only to 16K/2 cards.
Start Reading from page setting applies only to 16K/16 cards.
Start reading from book setting applies only to 32K cards. When using 32K cards, the block and page settings will be considered for Book 0.
Screen 5 – iClass Key Settings
Set the key type, default, or non-default, for iClass on this screen.

Unchecking the “Use HID iClass factory Keys” checkbox, will open further settings where custom iClass keys may be set.
Screen 6 – SEOS Keys

This page is used to set the Transport keys for iClass Seos cards. When the operator uses default keys, the details will be hidden.

When using the default keys, it is necessary to load the default transport keys into the 5G terminal with a configuration card.
Screen 7 – Omnikey Reader Keys

The operator may set the Omnikey reader keys on this screen. These settings only apply to the Omnikey 5022 and 5427. An Omnikey 5x21 will not be affected by these settings.
Screen 8 – Bioscrypt 4G Site Keys

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.

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

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

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. These 12 characters need to match the code used during the file creation.
Screen 9 – 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:

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 can 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 is 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 Configuration
The Biometric Device Configuration 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 Configuration (Express)
Select the Biometric Device Configuration section of Administration and click Add.

Screen 1 – Configuration Details

![Configuration Screen]

- **Name:** Name the configuration 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, users will be checked for duplicates as they are added to devices. The device can only check new users added. This check is performed by the device and NOT MorphoManager. This feature severely impacts the performance of the “Add User” task. It should only be enabled when absolutely necessary. When enabling duplicate checking on the device, it is necessary to reduce the MA5G User batch Size to no greater than 100.

Morpho Access
Heartbeat Interval: The interval to ping MorphoAccess terminals. If the terminal does not respond to the ping, the device status will be updated to Offline.

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 Configuration settings.

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

It is recommended the mode set in User Policy for enrollment should be the same mode or a more restrictive mode than the mode set in Biometric Device Profile. Using a less restrictive mode in User Policy than in Biometric Device Profile is likely to increase the False Rejection Rate (FRR) of biometric devices.

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 Configuration 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 MorphoManager 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 Configuration – Screen 2 section of the manual.

It is recommended the threshold mode set in User Configuration for enrollment should be the same threshold mode or a more restrictive mode than the mode set in Biometric Device Policy. Using a less restrictive mode in User Configuration than in Biometric Device Configuration is likely to increase the False Rejection Rate (FRR) of biometric devices.
Screen 3 - Multi-Factor Mode Settings

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 a HID iClass card capable device.
- **Mifare Classic** – This option allows Mifare Classic Cards to be utilized on a Mifare Classic capable device.
- **Mifare DESFire 3DES** – This option allows Mifare DESFire Cards to be utilized on a Mifare DESFire capable device.
- **Mifare DESFire AES** – This option allows Mifare DESFire Cards to be utilized on a Mifare DESFire EV1 capable device.
- **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.

- **Clock and Data In** – This option sets DataClock Input as the trigger event. If selected the Biometric Device will be configured to allow a DataClock Input and verify a user’s fingerprint. This is only supported for 5G devices.
- **HID iClass SEOS** – Allows HID iClass Cards to be utilized with a HID iClass SEOS card capable device.

## Screen 4 – Access Control Mode Settings

The Access Control Mode Settings are used to configure how the biometric device will integrate with an Access Control Panel.

### Access Control Mode Settings

- **Access Control Mode:**
  - None
  - Integrated by Wiegand / Panel Feedback
  - Integrated by OSDP
  - Stand-alone

- **Wiiegand Out Enabled:**
  - Enabled

- **Clock and Data Out Enabled:**
  - Disabled

- **Panel Feedback Mode:**
  - None

- **Panel Feedback No Response Timeout:**
  - 3000 milliseconds

- **Relay Enabled:**
  - Enabled

- **Relay Duration:**
  - 1000 milliseconds

- **Push To Exit Enabled:**
  - Disabled

- **Request to Exit Egress Timeout:**
  - 25000 milliseconds

- **OSDP Device Address:**
  - 127

- **OSDP Secure Channel:**
  - Disabled

- **Duress Wiegand Mode:**
  - Reversed

- **Duress Wiegand Profile:**
  - Automatically generated random 64 bit

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

### Access Control Mode:

- **Controls how the Biometric Device will integrate with an Access Control Panel**
  - None – All parameters will be disabled related to Access Control Mode
  - Integrated by Wiegand / Panel Feedback – Used when the biometric device will communicate with an access control panel via wiegand and/or Panel feedback
  - Integrated by OSDP - Used when the biometric device will communicate with an access control panel via ISDP
  - Stand-alone – Used when the biometric device is not connected to an access control panel
- **Custom** – Allows the operator to set all the available options for a custom configuration.

**Wiegand Out Enabled:** This will determine if 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

<table>
<thead>
<tr>
<th>Function Key Mode:</th>
<th>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 &amp; Attendance and Access Log records.</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Keys Function Mode:</td>
<td>No key</td>
</tr>
<tr>
<td>In One:</td>
<td>In One</td>
</tr>
<tr>
<td>In Two:</td>
<td>In Two</td>
</tr>
<tr>
<td>Out One:</td>
<td>Out One</td>
</tr>
<tr>
<td>Out Two:</td>
<td>Out Two</td>
</tr>
<tr>
<td>Key 1:</td>
<td>One</td>
</tr>
<tr>
<td>Key 2:</td>
<td>Two</td>
</tr>
<tr>
<td>Key 3:</td>
<td>Three</td>
</tr>
<tr>
<td>Key 4:</td>
<td>Four</td>
</tr>
<tr>
<td>Key 5:</td>
<td>Five</td>
</tr>
<tr>
<td>Key 6:</td>
<td>Six</td>
</tr>
<tr>
<td>Key 7:</td>
<td>Seven</td>
</tr>
<tr>
<td>Key 8:</td>
<td>Eight</td>
</tr>
<tr>
<td>Key 9:</td>
<td>Nine</td>
</tr>
</tbody>
</table>
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 +, Sigma Extreme, MA VP MD, & MorphoWave Settings

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 a face is detected or not.
- **Optional** – Takes a series of pictures and choses the best face it detects out of them for the log. However, if the user is rejected (biometric mismatch) AND it does not detect a face, no photo will be used.
- **Mandatory** – Takes a picture in all scenarios (rejected or accepted presentation).

Face Logging Mode: This works in conjunction with Face Detection Mode. Which transactions require a face capture to occur.

Face logs are saved to the MorphoManager database. It is not recommended to use the face logging functionality with a SQL CE database due to the file size limitation.

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

Enable idle timeout: Allows the following to be set on the Sigma and MorphoWave devices (video capacity does not exist for the Lite+ and MA VP MD):
- **Start video playback after** – Parameter to set the idle duration. If no action is performed during this duration, the screen will go into Idle mode. A value between 60s and 3600s.
- **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 utilized.

**Show Administration Menu:**
Select to allow the Administration Menu to be accessible on the device. If not checked the Administration Menu icon will remain on the screen but access will be disabled. This is selected by default.

**Show date and time:**
Select to display the date and time at the bottom of the device LCD screen. This is selected by default.

**i**
The *Show Administration Menu & Show Date and Time* feature is applicable only on devices with an LCD display.
Screen 8 – MA Sigma, Sigma Lite, Sigma Lite+, Sigma Extreme, MA VP MD & 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 MorphoWave.

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+, Sigma Extreme, MA VP MD & MorphoWave
Settings (continued)
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 TLS communications between the Biometric Device and the MorphoManager Server.

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

Enforce Certificate Validation: When this checkbox is selected the certificate on the device must match the certificate associated to the Key Policy assigned to this Biometric Device Configuration. If the certificates do not match, a connection to the device will not be established.

Incoming Connection Timeout: This will set the amount of time that MorphoManager will wait for devices to connect to the server when they are in a device-to-server communications mode.

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

<table>
<thead>
<tr>
<th>Function Key Mode:</th>
<th>No Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Keys Function Mode:</td>
<td>No key</td>
</tr>
<tr>
<td>Key 1:</td>
<td>IN</td>
</tr>
<tr>
<td>Key 2:</td>
<td>OUT</td>
</tr>
<tr>
<td>Key 3:</td>
<td>IN DUTY</td>
</tr>
<tr>
<td>Key 4:</td>
<td>OUT DUTY</td>
</tr>
<tr>
<td>Key 5:</td>
<td>Five</td>
</tr>
<tr>
<td>Key 6:</td>
<td>Six</td>
</tr>
<tr>
<td>Key 7:</td>
<td>Seven</td>
</tr>
<tr>
<td>Key 8:</td>
<td>Eight</td>
</tr>
<tr>
<td>Key 9:</td>
<td>Nine</td>
</tr>
<tr>
<td>Key 10:</td>
<td>Ten</td>
</tr>
<tr>
<td>Key 11:</td>
<td>Eleven</td>
</tr>
<tr>
<td>Key 12:</td>
<td>Twelve</td>
</tr>
<tr>
<td>Key 13:</td>
<td>Thirteen</td>
</tr>
<tr>
<td>Key 14:</td>
<td>Fourteen</td>
</tr>
<tr>
<td>Key 15:</td>
<td>Fifteen</td>
</tr>
<tr>
<td>Key 16:</td>
<td>Sixteen</td>
</tr>
</tbody>
</table>
**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 MorphoWave 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 – Biometric Device Database Synchronization**

MorphoManager supports automatic & manual Biometric Device database synchronization. This process allows MorphoManager to periodically poll selected devices to retrieve its user database and compare against the Server’s database and determine if there are any inconsistencies. If inconsistencies are detected, these will be logged for operator review, or can be optionally configured to be automatically resolved without operator interaction.

**Synchronization mode:**

- **Disabled** – the synchronization functionality is disabled.
- **Manual** – Synchronization must be initiated manually through the Biometric Device menu.
- **Automatic** – This is the default synchronization mode. Synchronization will initiate at the scheduled time automatically.

**Resolution mode:**

- Inconsistencies found during synchronization can be resolved by adding missing users to the device, or by removing unknown users from the device. The MorphoManager database is used as the reference point.
- **Manual** – Operator review, and interaction is required to resolve any inconsistencies found during synchronization.
Automatic – This is the default resolution mode. Any inconsistencies found will be resolved automatically. No operator interaction is required.

**Synchronization schedule:**   This schedule applies to the Automatic Synchronization Mode. It used to determine the days on which the synchronization task should run.

**Time of day to Synchronize:**  This only applies to the Automatic Synchronization Mode. Time of day when the synchronization task will start.

Screen 12 – MA Sigma, MA sigma Lite+, and MorphoWave Custom Media Files

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 Configuration containing these files to the Biometric Device will place the files onto that device.

Screen 13 – MA Sigma Custom Parameters

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 Configuration. 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, MA Sigma VP, MorphiWave Custom**

Name: audio.volume  
Value: 5

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

**Screen 14 – Morpho 3D Face Settings**

![Morpho 3D Face Settings](image)

- **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 on-screen messages will be shown to the user.
Screen 15 – 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 Configuration and you can click Finish on this screen with or without adding the Video Phone Server.

Video Phone Server Settings

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

Click Save when finished.
Creating a new Biometric Device Configuration (Advanced)
Select the **Biometric Device Configuration** 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.
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 Tower Advanced Settings

Parameters available for MorphoWave Tower. 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 – MorphoWave Compact Advanced Settings

Parameters available for MorphoWave Compact. 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 9 – 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.
Parameters available for MA VP MD. 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 11 – 16 can be found in the section for Creating a new Biometric Device Configuration (Express).

Creating a new Biometric Device Configuration (External)

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 five different hardware families can be added here; the MA 100, MA J, MA 500, and MA VP family, the MA Sigma, MA Sigma Lite, MA Sigma Lite +, MA Sigma Extreme, MA VP MD, the Morpho 3D Face, the MorphoWave Tower, MorphoWave Compact, 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name:</strong></td>
<td>The name of the Biometric Device.</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td>A description of the Biometric Device.</td>
</tr>
<tr>
<td><strong>Location:</strong></td>
<td>The installed location of the Biometric Device.</td>
</tr>
<tr>
<td><strong>Export Value:</strong></td>
<td>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 requirements of the payroll package and the access log exporter that is configured in the System configuration under T&amp;A General settings.</td>
</tr>
<tr>
<td><strong>Time Zone:</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
**Hardware Family:** Corresponds to the model of the Biometric Devices. 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 +, MA Sigma Extreme, and MA VP MD family, the Morpho 3D Face, the MorphoWave Tower and MorphoWave Compact family, 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:** Port number that the device is configured to use.

**Biometric Device Configuration:** 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 Configuration 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 Configuration 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 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.
Troubleshooting and Maintenance

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

Toolbar Functions

Refresh
This does not get the latest status from the devices. The refresh button gets the last known status from the MorphoManager server and refreshes the view of the MorphoManager Client.

Synchronize
Initiates the Synchronize task if it is enabled in the Biometric Device Configuration.

Get Logs
This functionality is enabled by default and allows currently stored transaction logs 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 Configuration a warning message is displayed if Get Logs is clicked.

The Get Logs function will download 100 logs from the biometric terminal every time the task is executed.

View Sync Log
This button will be enabled when inconsistencies have been detected that need to be resolved manually. When no inconsistencies exist, this button will be disabled.
From the Synchronization log, you can choose to add the missing user to the device. Likewise, when an unknown user exists on the device, the operator can choose to remove that user from the device.

**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 tasks in the queue and create new tasks to configure the device. The following tasks are created when rebuilding a device:

- **Get logs** – Gets all the access logs from the device, and clears the device access logs after retrieval
- **Set date and time** – Sets the date and time based on the MorphoManager Server time and device time zone
- **Reset media files** – Removes all existing media files
- **Delete existing access schedules** – All access schedules on the device are removed
- **Set configuration** – Applies the Biometric Device Configuration to the device
- **Delete all users** – This is an optional task. Removes all users from the device
- **Add users** – This is an optional task. All the users, that are eligible for upload, are sent to the device.

This function should only be used if the device is not operating as expected. Unexpected behavior could occur if a device were 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.

Create a Wiegand Profile
Screen 1 – Configuration Details

Enter details for this Wiegand profile

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 many 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)**: Like the User value, this value is defined during enrollment, but is read from a connected proximity card.
- **User (CSN)**: Like 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)**: Like 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)**: Like 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.
- **Clock and Data**: A unique value that will be used as a user’s identifier. The difference between the “User” element type and “Clock and Data” element type is the latter will save the value as a string value. This means that an ID of 01 will be different than 001. Both these values are unique when using this element type. This wiegand element is only supported for 5G devices.

![Adding Wiegand Profiles](image)

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**.
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 the elements needed to make up your Wiegand Profile, you can click FINISH.
**User Configuration**

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 Configuration. However, a User Configuration 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 Configuration

**Screen 1 – Details**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the User Configuration.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the purpose of the User Configuration.</td>
</tr>
<tr>
<td>Access Mode: All</td>
<td>This value determines the access to Biometric Devices that users in this policy will have.</td>
</tr>
<tr>
<td>Access Mode: Per User</td>
<td>This value determines the access to Biometric Devices that users in this policy will have.</td>
</tr>
</tbody>
</table>

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 Configuration.

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

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

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: 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.
**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 Configuration 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 Configuration for enrollment should be the same mode or a more restrictive mode then the mode set in Biometric Device Policy. Using a less restrictive mode in User Configuration than in Biometric Device Configuration is likely to increase the False Rejection Rate (FRR) of biometric devices.
Screen 3 – Details for Wave Biometric Options

Enter the details for wave biometric options

Wave Enrollment Minimum Hands:  
- 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 Configuration 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 Configuration.

Create an Access Schedule
Screen 1 – Details

<table>
<thead>
<tr>
<th>Name:</th>
<th>Name of the Access Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td>Description of the Access Schedule</td>
</tr>
</tbody>
</table>

Screen 2 – MA Sigma, Sigma Lite, Sigma Lite+, Sigma Extreme, MA VP MD, and MorphoWave access schedules
This section will create Access Schedules pertaining to the MA Sigma, Sigma Lite, Sigma Lite+, Sigma Extreme, MA VP MD, and MorphoWave devices. They allow for up to two periods of access to be set per day on the devices. Each 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 Configuration menu for Sigma, Sigma Lite, Sigma Lite+, Sigma Extreme, MA VP MD, and MorphoWave devices. If the setting is disabled, the access schedules will not be applied to these devices.
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.

Screen 4 – MorphoWave Tower
This section will create Access Schedules pertaining to MorphoWave Tower. They allow for up to two periods of access to be set per day on the devices. Each 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.
User Distribution Group

User Distribution Groups are designed to distribute users onto groups of MA readers or MorphoManager Clients. To be utilized the user must be in a User Configuration 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

![Adding User Distribution Group]

**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.
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 Configuration. Users added to the system will have their authentication triggers governed by the User Authentication Mode portion of the User Configuration they are placed in.

There are four automatically generated User Authentication Modes:

Create a new User Authentication Mode
Screen 1 – Details, MA 2G Family Mode, and 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 +, MA Sigma Extreme, MA VP MD, and MorphoWave Modes for this User

**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.

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).

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.
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

Name: Name of the Notification.

Description: Description of the Notification’s purpose.

Trigger type: Determines what event will trigger the Notification.

Delay notifications by: The number of missed heartbeats before triggering the notification. E.g. when this is set to 10, an offline notification will only be sent after 10 heartbeats failed. This option is only available for the “Device Offline” trigger type.

Notify when online: Send a notification when terminals in this notification group are back online.
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

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 – Key Policy**

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

![Screen 4 - Key Policy](image)

**Screen 5 - 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:

1. any PC/SC device to utilize the first detected device (not recommended)
2. a specific PC/SC device (Recommended setting)
3. a selected MorphoAccess for card encoding.
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**.

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

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.
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.

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.
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 username. The username 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.

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
Time and Attendance
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:

- Comacc
- Preceda
- Timeminder
- PowerForce
- RosterOn
- MYOB Enterprise
- MorphoManager Standard*
- Kronos
- Pay Global (Employee ID/Wiegand Usercode)
- SDb
- TimeAmerica
- ASTROW
- TimeKeeper
- MorphoManager Standard with GPS Coordinates**

**MorphoManager Standard with GPS

This format will include GPS coordinates, obtained from the MorphoTablet V2, in the exported Time & Attendance report. The MorphoTablet V2 is the only device that supports GPS coordinate logging.

*MorphoManager Standard Export Format

The MorphoManager Standard format will be exported as a comma-separated file (*.csv) with the following layout:
Date & Time, Device Export Value, Employee ID, First Name, Last Name, Time & Attendance Key

e.g.
20171229152619,Front Door,0023,John,Doe,IN

The MorphoManager Standard with GPS format will be exported as a comma-separated file (*.csv) with the following layout:

Date & Time, Device Export Value, Employee ID, First Name, Last Name, Time & Attendance Key, GPS Latitude, GPS Longitude, 0

e.g.
20171229152619,Front Door,0023,John,Doe,OUT,N 33° 50" 14',W 84° 22" 21',0

For logs to show in the Time & Attendance report, it is necessary to enable the option - Include in Time & Attendance Exports - in the Biometric Device menu.

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.
### Communications Engine

**Communications Engine Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum active communication channels:</td>
<td>50</td>
</tr>
<tr>
<td>MA5G User Batch Size:</td>
<td>1000</td>
</tr>
<tr>
<td>Number of concurrent tasks that can execute per physical core:</td>
<td>50 (2 physical cores detected on server)</td>
</tr>
<tr>
<td>Disable device events and error logging:</td>
<td>☑</td>
</tr>
<tr>
<td>System Event Log:</td>
<td></td>
</tr>
<tr>
<td>Write information to the system event log:</td>
<td>☑</td>
</tr>
<tr>
<td>Write warnings to the system event log:</td>
<td>☑</td>
</tr>
<tr>
<td>Write errors to the system event log:</td>
<td>☑</td>
</tr>
<tr>
<td>Realtime Access Log Recording Settings*</td>
<td></td>
</tr>
<tr>
<td>Server listening IP address:</td>
<td></td>
</tr>
<tr>
<td>Server listening port number:</td>
<td>11020</td>
</tr>
<tr>
<td>MorphoAccess notification timeout:</td>
<td>5000    (milliseconds)</td>
</tr>
<tr>
<td>Enable Realtime Access Log Relay:</td>
<td>☑</td>
</tr>
<tr>
<td>Host</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td></td>
</tr>
</tbody>
</table>

**Maximum Active Communication Channels**: The maximum number of active communication channels.

**MA5G 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.
System Functionality

Default Tab
This defines the tab selected by default when MorphoManager starts.

Default User Configuration
This defines the User Configuration that will be used as default when creating a user to the system.

Default Biometric Device Configuration
This defines the Biometric Device Configuration that will be used as default when adding a Biometric Device to the system.

Default Wiegand Profile
This defines the Wiegand Profile that will be used as default when adding a User Configuration and Biometric Device Configuration to the system.

Default User Authentication Mode
This defines the User Authentication Profile that will be used as default when adding a User Configuration to the system.
**Default Key Policy**
This defines the Key Policy that will be used as default when adding a Biometric Device Configuration to the system.

**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.

**System Management**

<table>
<thead>
<tr>
<th>Log Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum system error logs: 500</td>
</tr>
<tr>
<td>Maximum system event logs: 900</td>
</tr>
<tr>
<td>Maximum access logs: 10000</td>
</tr>
<tr>
<td>Maximum access log age (Days): 1095</td>
</tr>
</tbody>
</table>

**Disabled User Management**
Users that are disabled through User Management and through a configured BoBridge system will follow the selected rule.

- **Never Delete**
- **Delete Immediately**
- **Delete After:** 90 (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.

Gateways

<table>
<thead>
<tr>
<th>Gateway Settings - Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server Hostname:</td>
</tr>
<tr>
<td>SMTP Port Number: 25</td>
</tr>
<tr>
<td>SMTP Server Authentication:</td>
</tr>
<tr>
<td>Server Requires Authentication</td>
</tr>
<tr>
<td>SMTP Username:</td>
</tr>
<tr>
<td>SMTP Password:</td>
</tr>
<tr>
<td>SMTP Requires SSL:</td>
</tr>
<tr>
<td>Server requires SSL</td>
</tr>
<tr>
<td>From Email Address:</td>
</tr>
<tr>
<td>Reply To Email Address:</td>
</tr>
</tbody>
</table>

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.**
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

Choose your BioBridge compatible system from the drop-down menu.

Configure connection

Connection credentials for the third-party software.
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 Configuration
By activating this feature, you can select a User Configuration from the drop-down menu. The 3rd party user will automatically be placed in this User Configuration during the enrollment process started in the BioBridge Enrollment Client. The User Configuration 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
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 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.
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.

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

Card Template Management
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.

Card Encoding Template Management
These options will allow for 2 (or 3 w/Duress) contact templates to be encoded to the card.

- Enable Contact Fingerprint Encoding
- Encode duress finger to card (MA Sigma family devices only)

Choose one of the following options to determine which captured template format will be encoded to a contactless card. To unlock Standard Template, please complete the challenge code process in the Finger Template Capture Options tab. Standard Templates will be included in the other options when unlocked.

- Fingerprint Templates
- Fingervein Templates
- Standard Templates

Contactless Template Management
Select the number of contactless fingerprints to encode

- Disabled
- Disable the ability to encode contactless templates to card

Face Template Management
These options will allow face templates to be encoded to the card.

- Enable face template encoding
Enable Contact Fingerprint Encoding
When disabled, the system will not encode fingerprint templates to smartcards.

Encode duress finger to card
When enabled, the system will encode a third fingerprint, the duress finger, to the card, if it is enrolled. Only the Sigma family devices support a duress finger.

Card encoding template priority
This section determines which template types to encode to a card. The default setting is “Fingerprint Templates” and this will provide the optimum performance. If you are using any FVP devices, select the “Finger-vein Templates” radio button to ensure that the FVP templates get encoded to the card. The last option, “Standard Templates”, is only for advanced users. This option is locked, but may be unlocked on the Finger Template Capture options tab.

Number of contactless fingerprints to encode
Determines how many fingerprints, overall, will be encoded to the card.
- Disabled: Contactless fingerprints will not be encoded to cards
- 2 Fingers: one finger per hand will be encoded to the card. If the user has just one hand enrolled, two fingers from the one hand will be encoded to the card.
- 4 Fingers: four fingers from one hand will be encoded. Right-hand is the preferred hand.
- 8 Fingers: four fingers per hand will be encoded to the card

A VERIF license on the MorphoManager server is required to encode contactless fingerprints to a smartcard
Finger Template Capture Options

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

ANSI/ISO template Unlock code: If you wish to use ANSI or ISO templates, you need to contact Morpho Support to unlock these template types

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

Allow juvenile template coding: Used when capturing fingerprints of a young person

Force Device Template coding: This option will override any license present and use the configuration for “Device Template Coding Options”

Store WSQ image: Stores the WSQ image of the fingerprint. A license is required for this option.
Display Options

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, if information is mandatory, and assign names for the fields.

MorphoWave

MorphoWave Unlock

There is an alternative Wave Desktop Enrollment available that may be used in advanced cases. Please contact Morrho support to unlock Enrollment 2 for MorphoWave Desktop.

User Management

This setting can only be unlocked with an unlock code obtained from Morrho support.
Duplication Control

ID Duplication

Check if user’s ID is unique
During user add and edit, the current user’s ID will be checked against the existing database of users to determine if this current user has a unique ID. This option is disabled by default.

Allow users with duplicate IDs
This is a sub-setting of Unique User ID Check. When enabled, the operator will be presented with a warning that a duplicate ID was detected. The operator may continue with this duplicate ID or amend the ID before continuing the enrollment process for the user.
When disabled, the operator will be presented with a pop-up message that a duplicate ID has been detected. Only once the duplicate ID has been resolved will it be possible to save the user.

Leading zeroes are significant and MorphoManager takes leading zeroes into account when determining if the ID is unique. E.g. ID 001 is not the same as ID 0001. Excluding leading zeroes in the Wiegand ID fields is best practice.

User Fingerprint Duplication

To prevent an operator from enrolling duplicate fingerprints when users are added to the system.

Prevent duplicate fingerprints within a user record
During user enrollment a verification will be performed to verify the presented fingerprint is only enrolled once. This setting only checks for duplicates within a user’s own record during the enrollment process.

A VERIF license on the MorphoManager client is required to prevent duplicate fingerprints within a user record
Prevent duplicate fingerprints between user records

After saving a user enrollment, the fingerprint uniqueness is determined against existing users in the MorphoManager database. This setting will prevent enrolling a user more than once. This functionality works in conjunction with the matcher settings.

It is important to note that this check can only occur when the matcher status is “Ready”.

Only new template enrollments will be checked for duplicates. Editing a user, without changing the templates, will not be checked for duplicates against the database.

System Fingerprint Duplication

A system-wide fingerprint duplicate search will occur based on the schedule defined in this section. This search collects and stores the results to view in a report. The search can be CPU intensive, therefore the search should be scheduled during off-peak times.

The system-wide fingerprint duplicate search details can be viewed in the Matcher Settings.

Results of the search can be viewed in the Fingerprint Duplicate Report.

Run fingerprint duplication check

This button will launch the system-wide duplicate fingerprint search. The button is only enabled when the matcher status is “Ready”. This search may take many hours before the results can be viewed in the Duplicate fingerprint report.
Matcher settings and information

MorphoManager runs a matching engine to determine if fingerprints are unique and to search for duplicates in the database.

Identification threshold
A higher setting translates to more minutiae points that need to match before a duplicate can be confirmed. A higher setting may lead to less duplicates being detected and potentially not find duplicates that do exist

A lower setting translates to less minutiae points that need to match before a duplicate can be confirmed. A lower setting may lead to more duplicates being detected and potentially falsely flag two fingerprints as duplicates.

Current matcher status
The Current status of the matcher.

- Initializing: The matcher is starting up
- Available: The matcher has completed its last system-wide search and is ready to run again. This also means the matcher is ready to be used for the duplicate detection between user records.
- Running Report: A system-wide duplicate search is currently processing
- Unknown: The status of the matcher is not known
- Inadequate license: An IDENT license has not been detected on the MorphoManager server.

Last execution date/time
The last time the system-wide search started.

Last execution status
The status of the last system-wide duplicate search.
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:**

![Logs Image]

**Biometrics:**

![Biometrics Image]

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 Details Screen](image)

**User Configuration:** Select the User Configuration 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

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

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

Screen 4 – User Defined Fields

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

Screen 5 – Wiegand Values (If a Wiegand Profile is set)

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

![Adding User](image)

Screen 7 – Photo Capture

Position the person in front of a plain background so that all their face is visible in the picture, like 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**

**Adding User**

Enter and confirm the PIN

**PIN:**

**Confirm PIN:**

**PIN Code:** Will be utilized and appear on screen when the authentication mode is set to one including PIN. Ex. Smartcard + PIN.
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 Configuration. 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 MorphoWave Device, click **Clear <enrolled finger> finger enrollment** to allow re-enrollment.
Screen 11 – Fingerprint Capture

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 default fingers that the system suggests you 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.

![Capturing left index finger](image)
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. Do not 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 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 is not 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.
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 Management Toolbar
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 will be retained for reporting. Disabled users can be enabled at any time. Disabled users are considered when checking for duplicate ID’s and biometrics.

Import
Individual or Multiple users can have their information imported into MorphoManager via the Import feature. Individual users can have their demographic data and biometric templates imported. However,
Multiple users will only have the demographic data for those users. Biometric template capture for the users can then be done later.

For more information about the importing of multiple users, please refer to the Import Users from CSV File Guide.

**Verification - Database**

> A VERIF license is required on the MorphoManager Client Computer to perform biometric authentication

Verifies a presented fingerprint against the fingerprint stored in the MorphoManager database. If the fingerprints match, a “Verification Successful” message is displayed along with the verification score. If the fingerprints do not match, a “Verification Failed” message is displayed.

Verification can verify contact and contactless fingerprints. The current selected tab will determine which fingerprint type will be verified.

The device that will be used for verification is set in the Clients menu and is the same device as the enrollment device.

**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.

Filter
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.
Biometric Identification
Used to identify a user by their fingerprints. It is possible to do an identification on contact templates and contactless templates.

An IDENT and VERIF license, on the MorphoManager server, is required to run the matcher which performs the identification.

Contact Fingerprint Identification
Select the Contact Identification tab to identify a user by their fingerprints using the configured Contact Enrollment device.

Once the user presents their fingerprint to the 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 fingerprint is not matched against a previously enrolled finger, the “Not Identified” screen will be shown.
Contactless Fingerprint Identification
Select the Contactless Identification tab to identify a user by their hand using the configured Contactless Enrollment device.

Once the user presents their hand to the MorphoWave 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. 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, its 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.

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.
Transaction 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 Configuration Members Report:** Displays a list of all users that are members of the selected User Configuration.

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

**List Report**
- Select the Report type from the options Biometric Device, Operator, User and User Configuration.
- Click **Generate Report**.
User Configuration Members Report
• Search and select the User Configuration and click on Generate Report.

Permissible Report
• Select the Report type (Biometric Device or User).
• Search for the Biometric Device name or the username and click on Generate Report.

User ID duplicate report
This report launches a search for duplicate wiegand ID’s. If any duplicate ID’s are found, they will be listed in this report.

Fingerprint Biometric duplicate report
This report will display the results of the system-wide duplicate fingerprint search. The search is not launched each time this report runs. The report will only display the data from the last system-wide duplicate fingerprint search. If any users are found to have duplicate fingerprints, they will be listed in this report.

Windows Certificate Store
Importing a Certificate to the Store
Begin by locating the certificate to be placed in the certificate store. Right click on the certificate and choose the Install PFX option.
A Certificate Import Wizard will appear. Under the Store Location option, select Local Machine and click Next.

The next page will allow you to specify the file to import. The location of your certificate should already be provided in the File Name field space.
Next, enter the certificate’s password. This is the password that should already be associated with the certificate, not a new one. Check any additional import options that may be applicable.

The next page allows you to select which store the certificate will be imported to. You can choose to have the store automatically selected, however, since MorphoManager will be expecting the certificate to reside in either the Personal store or the Trusted Root Certification Authorities store, select the
option that allows you to place the certificate to the store of your choosing and browse to the store’s location.

Finally, ensure that the information provided on the last screen is correct and click the Finish button to begin the import process. Once complete a prompt will appear informing you that the import was successful.
Checking the Certificate Store

To check that the certificate has been imported to the store, begin by typing ‘certificates’ until you see the Manage computer certificates option appear. Click to open.

Once the certificate store opens, locate the folder that was specified during the import process. You should see your new certificate. It may be hard to tell which one is newly imported, so you may want to take note of which ones where there before hand. Additionally, multiple may have been imported from what appeared to be one.
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 SQL CE database. Systems running SQL Server will need to contact your DBA or 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.

The MorphoManager service must be stopped before starting the Database Backup Tool.

Browse
Click Browse to change the backup directory

Start Backup
Starts the backup process.

SQL Compact to SQL Server Database Migrator
This tool copies a SQL CE database’s table schema and data to a designated Microsoft SQL server database when the system grows beyond the limits of SQL CE. It utilizes the SQL CE database in use by MorphoManager by default.

For customer support on Microsoft SQL Server, please contact Microsoft SQL Server TechCenter.

Migrating 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) in SQL Server.
- Stop MorphoManager Server
- Start the SQL Compact to SQL Server Database Migrator tool.
- **Connection String Details** (the source is automatically filled)

![Connection String Details](image)

- Enter the Target SQL Server connection string for the SQL Server database that was created.
- Test Connection. Once this is successful, move to the next step.

![Connection String Details](image)

- Click **Migrate Database**.
- Confirm the migration of data.
- Once complete, confirm that MorphoManager will now use this new SQL Server database.
Biometric Device Configuration Creation Tool

This tool will allow you to generate a Biometric Device Configuration 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 Configuration 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
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.
Firmware updates are performed over TCP port 11001.

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.