MORPHO MANAGER

User Manual

Last Update: 17.4.0

IDEMIA PUBLIC SECURITY

Contents

Contents 2
Introduction 5
Overview 5
What is a client? 5
What is a server? 5
What is a biometric enrollment scanner? 5
What is a Biometric Device? 6
Setting up MorphoManager 7
Computer hardware requirements 7
Software requirements 7
Supported USB enrollment scanners 7
Supported Biometric Devices 8
Discontinued Biometric devices 9
Supported Card Reader / Encoders 10
Biometric Device Capacity 11
Biometric Device supported firmware 11
Installation of MorphoManager software 12
Updating to MorphoManager 16.x 12
System architecture 13
Installation process overview 14
Windows Service Account For MorphoManager Server 14
SQL database installation 17
Troubleshooting MorphoManager Server Installation 18
Password Management for Default Operator 20
MorphoManager Client Configuration 21
Basic 21
Advanced 23
Login Options 25
MorphoManager Server Manager 26
Home 26
Database Configuration 27
Advanced Configuration 28
Certificate Management 30
Product Activation and License management 31
Procedure for License request 31
Procedure for License upload 32
License Protected Features 36
Express Configuration 36
Secure Communication Policy 36
Device discovery 36
Authentication modes 38
Card selection 39
Home Screen 40
Secure Communication Policy 41
Overall guideline 41
Enforced security, self-generated certificates 41
Enforced security, imported certificates 41
On-demand security 42
Administration 42
Operator 42
Creating a new Operator 43
Key Policy 45
Creating a new Key Policy 45
Lock & Unlock 54
Biometric Device Configuration 55
Creating a new Biometric Device Configuration (Express) 55
Creating a new Biometric Device Configuration (Advanced) 74
Creating a new Biometric Device Configuration (External) 80
Biometric Device 81

Create a Biometric Device....81
Modify a Biometric Device....83
Delete a Biometric Device....83
Biometric Device Status and Tasks....83
Allow Card Encoding....83
Troubleshooting and Maintenance....85
Toolbar Functions Refresh....85
Synchronize....85
Get Logs....85
View Sync Log....86
Set Date/Time....86
Rebuild....86
Set Online....87
Secure State....87
Actions for multiple Devices....88
Wiegand Profiles....89
Create a Wiegand Profile....89
User Configuration....92
Create a new User Configuration....92
Access Schedules....96
Create an Access Schedule....96
User Distribution Group....98
Create a User Distribution Group....98
User Authentication Mode....99
Create a new User Authentication Mode....100
Operator Role....104
Notifications....108
Create a new Notification....108
Clients....110
Screen 1 – Enter the details for this Client....110
Screen 2 – Select the tabs displayed on this Client....111
Screen 3 - Camera Configuration....112
Screen 4 – Key Policy....113
Screen 5 - Enrollment Devices....113
Scheduled Reports....116
Card Template....118
Card Encoding Log....119
Event Logs....119
Exception Logs....119
System Configuration....119
Time and Attendance....119
Communications Engine....122
System Functionality....123
System Management....124
Gateways....125
BioBridge....125
Privacy Mode....128
Card Template Management....128
Biometric Template Capture....129
Display Options....131
MorphoWave....131
Duplication Control....132
Password Rules....135
User Management....137
User Details....137
Creation and enrollment of a User....139
Screen 1 – User Details....139
Screen 2 – Additional Details....140
Screen 3 – Contact Details....141
Screen 4 – User Defined Fields....141
Screen 5 – Wiegand Values (If a Wiegand Profile is set)....141
Screen 6 – User Distribution Groups....142
Screen 7 – Photo Capture....142
Screen 8 – PIN Code....143
Screen 9 – 3D Face....144
Screen 10 – Wave Enrollment....145
Screen 11 – Fingerprint Capture....148

User Management Toolbar 153
Edit 153
Delete 153
Refresh 153
Encode Card 153
Delete Encoding 153
Disable User 154
Import 154
Verification - Database 155
Export Photo 155
Add Photo 155
Filter 155
Actions on multiple users 157
Biometric Identification 159
Contact Fingerprint Identification 159
Contactless Fingerprint Identification 160
Onsite/Offsite 161
Transaction Logs 163
Reports 165
User Activity Report 165
Biometric Device Activity Report 165
User Configuration Activity Report 165
All Activity (included all users and Biometric Device) 165
Inactivity Report 165
List Report 165
User Configuration Members Report 166
Permissible Report 166
User ID duplication report 166
Fingerprint Biometric duplication report 166
Windows Certificate Store 166
Importing a Certificate to the Store 166
Checking the Certificate Store 171
Tools and Utilities 172
Export and Import 172
Biometric Device Configuration Creation Tool 173
Biometric Terminal UpgradeTool 174
Create a Firmware Update job 174
Compatibility Check Utility 177
Server Analytics Report 178
Technical Healthcare Monitoring 179
Resilience 179

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' biometric data, photos, and personal details. The biometric information is sent to specified Biometric Devices where access control is required and where users clock on and off throughout the day.

Overview

A MorphoManager system consists of four components:

- A MorphoManager Server
- At least one MorphoManager Client
- At least one biometric enrollment scanner
- 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 biometric enrollment scanner?

An enrollment device captures a user's biometric sample, extracts the features, and sends it to the MorphoManager software. This information is sent to a Biometric Device for user authentication.

The following scanners can be used for fingerprint enrollment:

MorphoSmart 300
USB Fingerprint Scanner

MorphoSmart 1300
USB Fingerprint Scanner

MorphoSmart 330
USB Fingerprint Scanner

The scanners 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.

For contactless fingerprints (MorphoWave range) and face (VisionPass range), a Biometric Device itself is used as the enrollment scanner.

What is a Biometric Device?

Biometric Devices are used to authenticate users and allow access to doors. They record a log of every presentation. MorphoManager is used to manage user's access to a Biometric Device.

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
Ethernet:	100Mbs port required for client/server connections.
Network:	Specific network dedicated to the access control system, different from the corporate network and not connected to the Internet
Screen Resolution:	1080p

Software requirements

Operating System for MorphoManager Server**:**

- Microsoft Windows 10 64-bit (Anniversary update or later)
- Windows Server 2016 64-bit
- Windows Server 2019 64-bit
- Windows Server 2022 64-bit
- Windows Server 2025 64-bit
- Windows 11 64-bit

Operating System for MorphoManager Client:

- Microsoft Windows 10 64-bit (Anniversary update or later)
- Windows Server 2016 64-bit
- Windows Server 2019 64-bit
- Windows Server 2022 64-bit
- Windows Server 2025 64-bit
- Windows 11 64-bit

Antivirus: running for both MorphoManager Server and Client, and constantly updated

Database server:

- SQL Server 2017
- SQL Server 2019
- SQL Server 2022

Supported USB enrollment scanners

- MSO 300
- MSO 330
- MSO 1300 E3
- MSO 1300 E4

MSO 1300 E2, MSO 1350 series are deprecated one.

Supported Biometric Devices

SIGMA Wide

SIGMA Extreme

SIGMA Lite

SIGMA Lite+

MorphoWave Compact / XP

MorphoWave XP 2

MorphoWave SP

VisionPass

VisionPass SP,
possibly with
Fingerscan accessory

Discontinued Biometric devices

The following terminals are discontinued and not supported any more. IDEMIA strongly recommends to replace them to more recent products as soon as possible.
They are currently available in MorphoManager interface for the sole purpose of enabling migration, without guarantee they work properly. They will be removed in a future release.

Morpho 3D Face

MorphoAccess VP

MorphoAccess J Series

MorphoAccess 500+ Series

OMA 520 Series

MorphoSmart Finger VP

MorphoWave Tower

Supported Card Reader / Encoders

Supported Card Types and Card Readers

Card Family	HID Prox	HID iClass	HID iClass Seos	MIFARE Classic	MIFARE DESFire EV0	MIFARE DESFire EV1
Card Variant	Prox	2K/2 16K/2 16K/16 32K (16K/2+16K/1) 32K (16K/16+16K/1)	Seos®	1K 4-byte NUID 1K 7-byte UID 4K 4-byte NUID 4K 7-byte UID	2K 4K 8K	2K 4K 8K
HID® OMNIKEY® 5427CK	✓	✓	✓	✓	✓	✓
HID® OMNIKEY® 5427G2	✓	✓	✓	✓	✓	✓
HID® OMNIKEY® 5025CL	✓	X	X	X	X	X
Identiv uTrust 3700F	X	X	X	✓	✓	✓

Supported Card Capabilities

Card Family	HID Prox	HID iClass	HID iClass Seos	MIFARE Classic	MIFARE DESFire EV0	MIFARE DESFire EV1
Card Variant	Prox	2K/2 16K/2 16K/16 32K (16K/2+16K/1) 32K (16K/16+16K/1)	Seos®	1K 4-byte NUID 1K 7-byte UID 4K 4-byte NUID 4K 7-byte UID	2K 4K 8K	2K 4K 8K
Read CSN/ID	✓	✓	✓	✓	✓	✓
Encode to Card	X	✓*	✓**	✓	✓	✓
Read PACS Data	X	✓	✓	X	X	X

* 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

Supported Template Types

Card Family	HID Prox	HID iClass	HID iClass Seos	MIFARE Classic	MIFARE DESFire EV0	MIFARE DESFire EV1
HID® OMNIKEY® 5427G2	X	ALL*	ALL*	ALL*	ALL*	ALL*
HID® OMNIKEY® 5025CL	X	X	X	X	X	X

* MorphoManager is capable to encode all type of biometric templates (Including Finger, Hand and Face) available in Morpho Manager database inside contactless card with the help of above-mentioned encoder. Type of template will be:

- Finger: PkCOMPv2
- Hand: MorphoWave Hand
- Face: Face V2 Light Comp/Face V3(if Face V2 Light Comp not available)

Biometric Device Capacity

MorphoManager is limited to a capacity of 5 000 total biometric devices.

If an attempt is made to add more devices, 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.

Device Series	Supported firmware version
MorphoAccess Sigma Series	4.12.0
MorphoWave Compact / XP Series	2.10.7
MorphoWave XP 2 Series	3.0.0
MorphoWave SP	1.1.1
VisionPass	2.10.7
VisionPass SP	2.0.0 3.0.0 for support of Fingerscan accessory

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

- Please refer to the ‘Conditions for a secure installation’ dedicated document.
- Please make sure your MorphoManager is always up to date with security.

Updating to MorphoManager 16.x

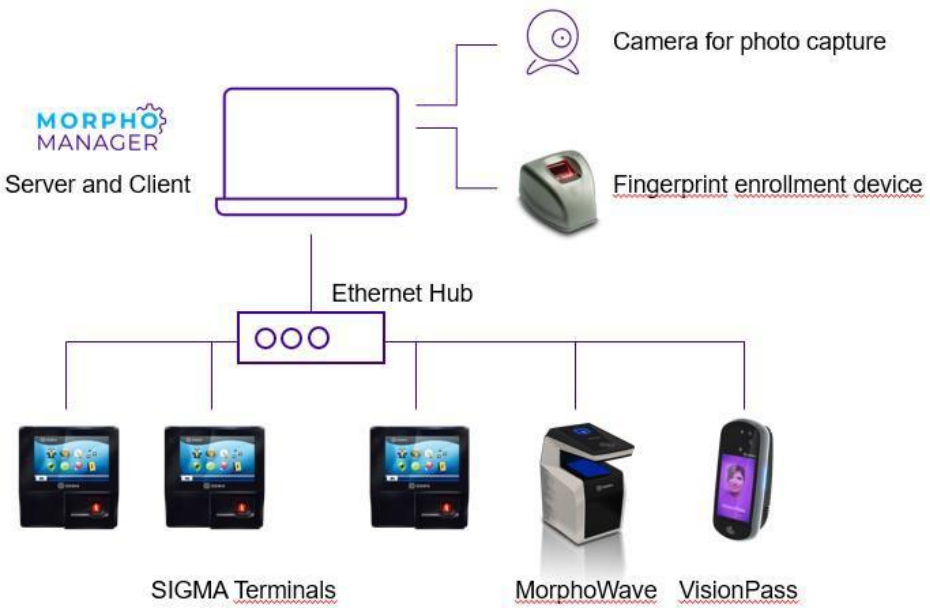
It is not possible to update to MorphoManager 16.x from a version earlier than 14.6.1.

In all cases, if you have an existing installation, it is advised to run Compatibility Check Utility before upgrading your copy of MorphoManager.

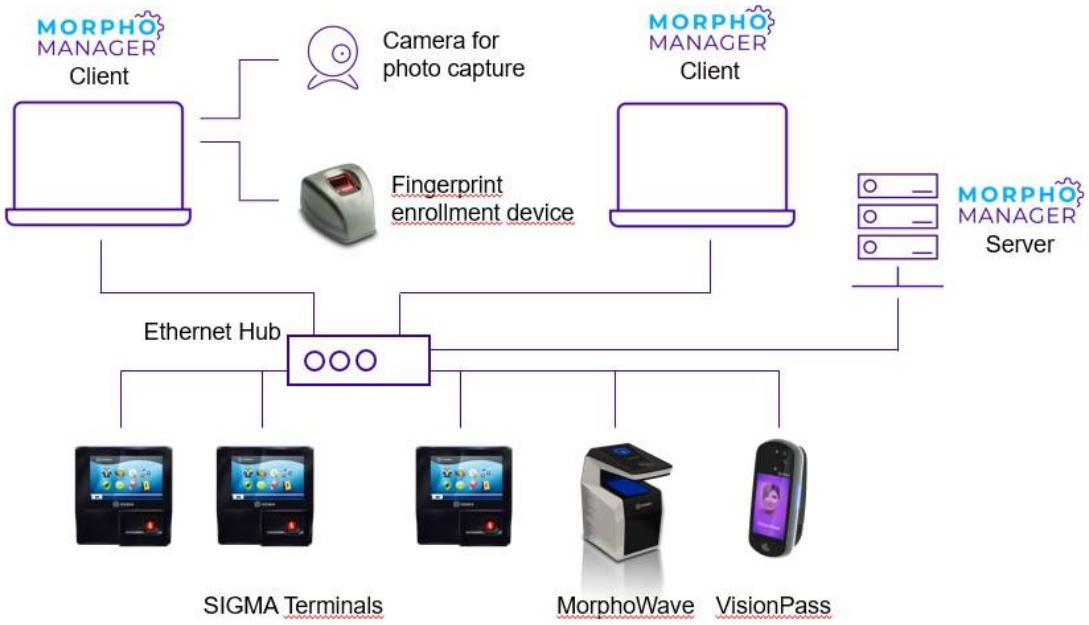
Version 16 introduced the Secure Communication Policy. Please refer to the dedicated section below.

System architecture

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



Alternately, the MorphoManager Server application can be installed on a separate PC which may or may not be a dedicated server. This configuration can be used with an existing corporate network that already has a server. In this case, the MorphoManager Client application is to be installed on each client PC that will connect to the MorphoManager Server machine over a LAN or VPN connection.



MorphoManager is not designed to be virtualized. Virtualization solutions may have unexpected consequences and are not supported by IDEMIA.

Installation process overview

- *[Optional] Install and configure SQL Server.*
- Install the MorphoManager Server.
- *[Optional] Reboot MorphoManager Server machine (not needed if MorphoManager Client is to be installed on the same machine)*
- After the server is installed, install the MorphoManager Client and reboot.
- Ensure the Biometric Devices are on the same network as the MorphoManager Server and are in the same IP range.
- Start the MorphoManager Client – double click on the icon on the desktop.
- Activate the product.

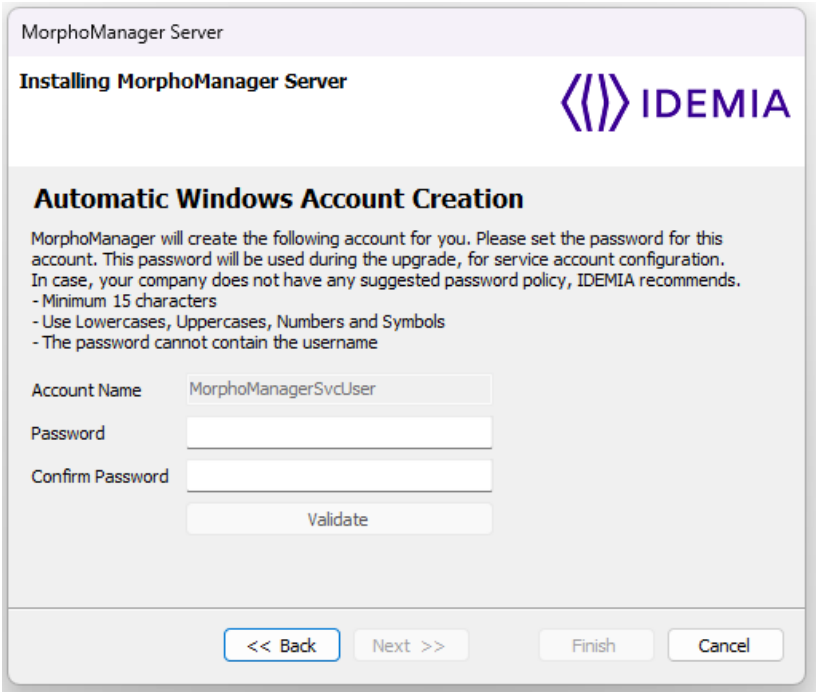
Note: MorphoManager is not compatible with the "FIPS compliant algorithm" Windows setting. In case this setting is enabled, please follow the below procedure to disable it:

- Navigate to Control Panel \ System and Security \ Administrative Tools \ Local Security Policy
- Expand Local Policies from left panel and select Security Options
- Find the Policy called "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing"
- Set it to Disabled.

Windows Service Account For MorphoManager Server

For security reasons, IDEMIA recommends to run MorphoManager Server with a dedicated Windows account having limited privileges.

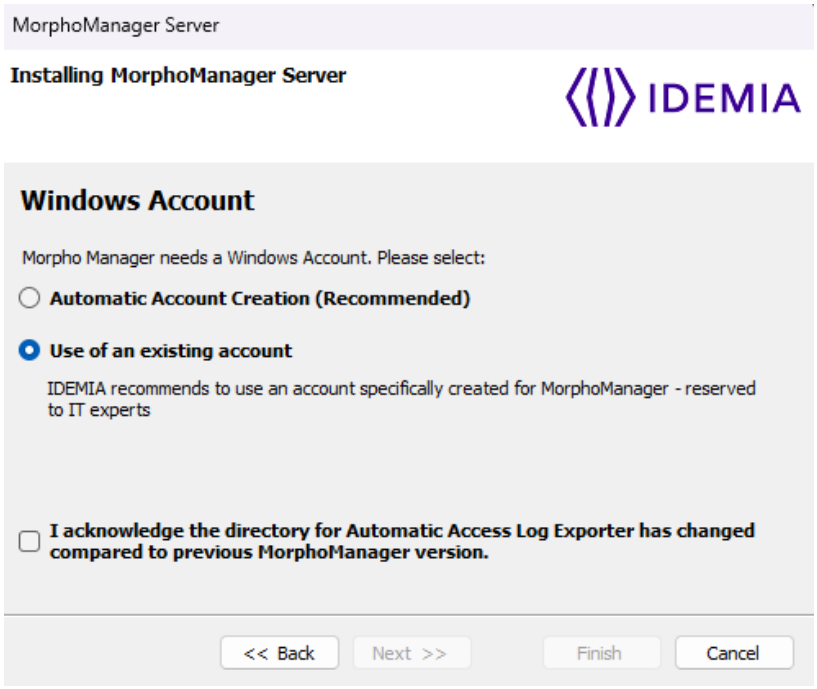
The installation wizard offers the option of creating it.



Please define a password. The 'Validate' button checks 'Password' and 'Confirm Password' match.

This password will not be needed to operate MorphoManager, but will be requested to update to a later version. Please keep it safely.

In case the Windows account was previously created, please leverage the 'Use of an existing account' option.

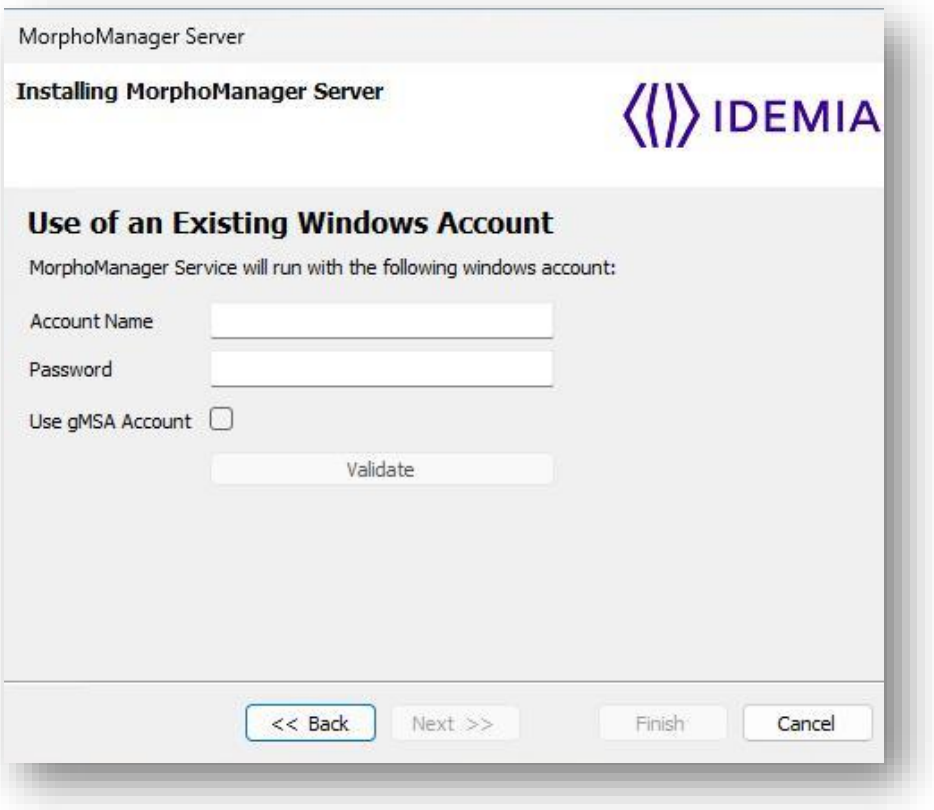


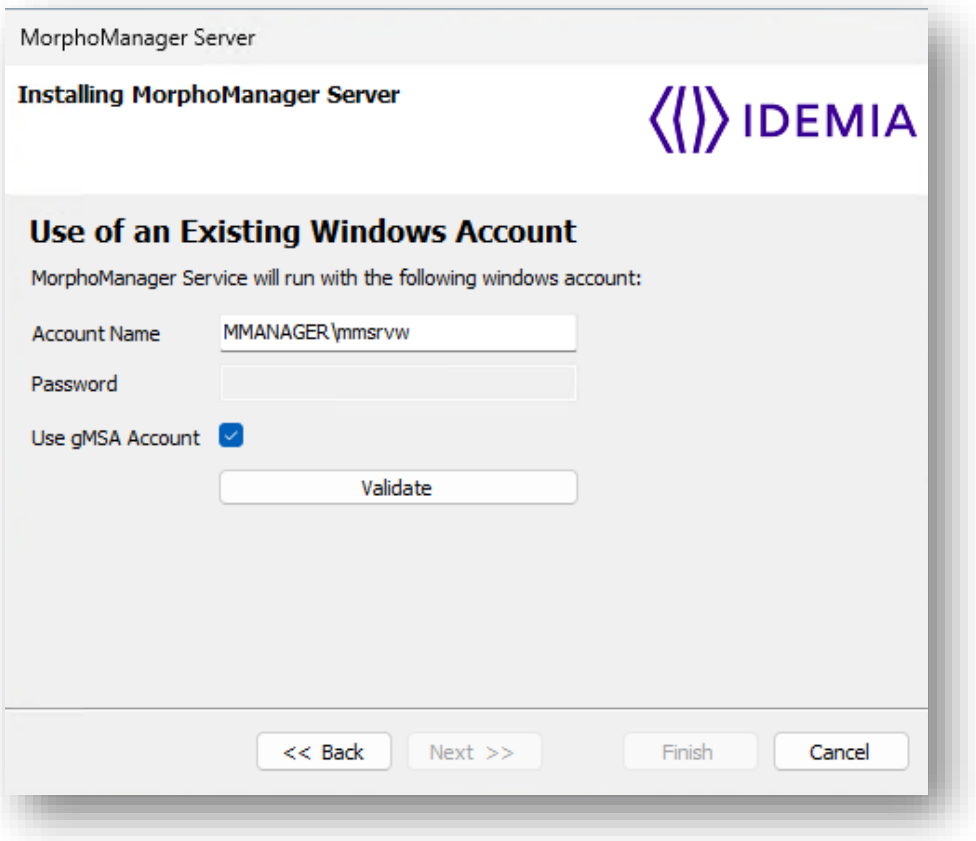
If the creation was done by the 'Automatic Windows Account Creation' of MorphoManager installation wizard,

please use MorphoManagerSvcUser as Account Name and the password you defined.

The gMSA option allows to use a pre-defined account without password (reserved to IT experts). To use a gMSA account, the domain name must be input before the account name in one of the below formats: DOMAIN\gMSA or DOMAIN\gMSA$. Please note that the operating system shall be logged in with an Active Directory (AD) account when using gMSA (including for the setup).

IDEMIA strongly recommends to use an Active Directory account with local administrator rights to install MorphoManager, which is required when using a gMSA account with this version. Please refer your IT Administrator for more details.





IDEMIA strongly recommends to use an account specifically created for MorphoManager (reserved to IT experts) only in case of 'Use of an existing account' option.

To change the configured Service account outside the installation process, please follow the below steps:

- Add the user to be configured to the database (if not already present)
- Open services.msc (in admin mode) and modify the logged in as account name with the another existing account.
- Open server manager and save the TLS configurations (Do not skip this step)
- Restart the Server

SQL database installation

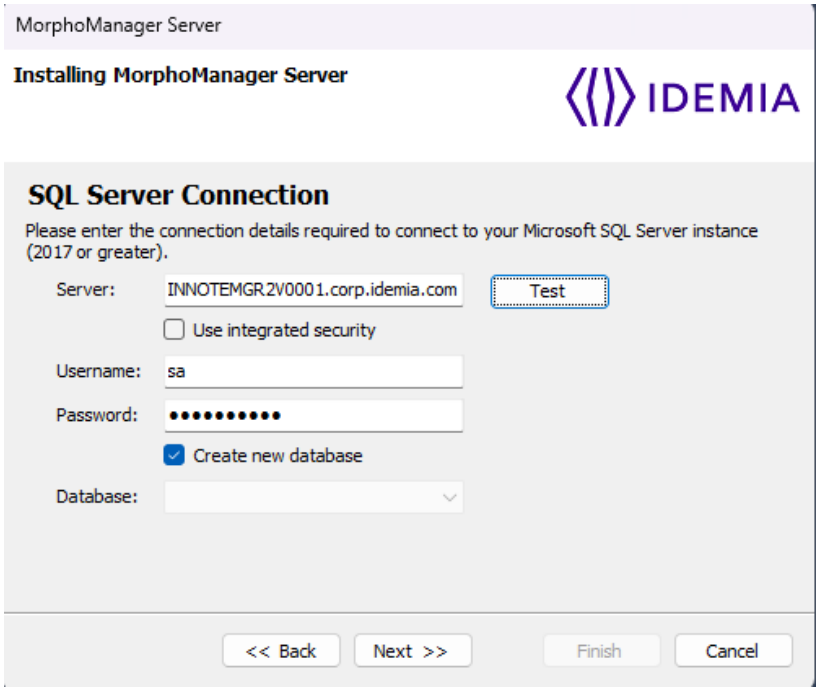
MorphoManager Server requires a SQL Server database. In any case, please make sure:

- Not to manipulate the MorphoManager SQL database – this may create incompatibilities and is not supported by IDEMIA.
- The SQL database it is protected with a state-of-the-art security solution – it will store sensitive information for the security of the system and for users' privacy.

The MorphoManager Server installation wizard proposes the option of installing and configuring SQL Server

automatically.

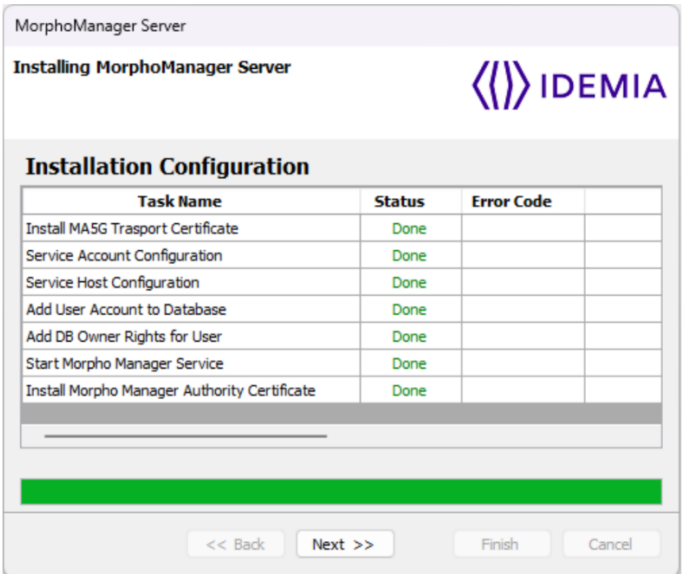
Alternately, an existing SQL Server database can be used. The connection information is to be provided during the MorphoManager Server installation:



In case the “integrated security” option is enabled, the SQL user shall have been properly configured in the SQL database, with associated Database owner rights.

Troubleshooting MorphoManager Server Installation

At the end of the installation wizard for MorphoManager Server, configuration of the machine is processed.



In case of failure, an error code is displayed.

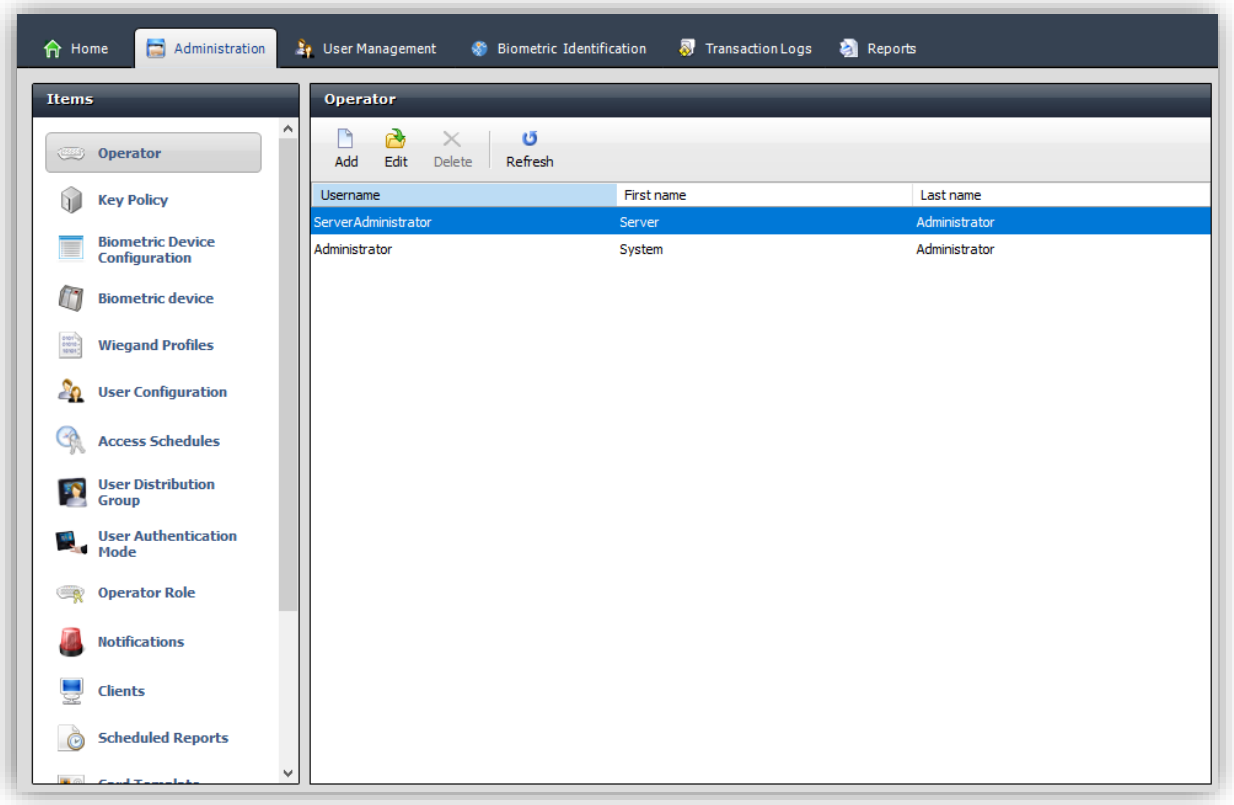
Error code	Error
100	Generic Error
101	Process Error
102	File Read Write Error
103	Serialization Error
200	Service host configuration error
201	Service host get certificate error
300	Authority Certificate Install Error
500	Audit Log Certificate Install Failure
501	Audit Log Certificate File Not Found Failure
510	Audit Log Certificate Renew Failure
511	Audit log Certificate Validation Failure
2000	User not found
3000	Authority Certificate Generic Error
3001	Authority certificate not found error
4000	Service Account Configuration Generic Error
4001	Service Account Configuration Not Supported Error
4002	Service Account Configuration Access Denied error
4003	Service Account Configuration Dependent Services Running Error
4007	Service Account Configuration Service Request Timeout Error
4008	Service Account Configuration Unknown Failure
4011	Service Account Configuration User Account Not Available
4015	Service Account Configuration Service Logon Failed
5000	Service Host Configuration Generic Error
6000	Database configuration generic exception
6001	Invalid Connection String
6002	Database Connection Failure
6003	Database user does not exists error
6004	Database sql error
6100	Add User to db generic error
6101	Add User Account create login error
6102	Add User Account create user error
6200	Add Database owner rights generic error
6201	Add Database owner rights error
7000	Service Start generic exception
7001	Morpho Manager Service Logon Failure
7002	Service Start timeout error
8000	Certificate Install error
9000	Grant Folder Permissions Generic error
9001	Grant Folder Permissions Directory Not found error
10000	Generic exception related to Audit Log Start Verification.
10001	Audit Log Start Verification Failed. As Audit Log is already configured, a manual restart of MorphoManager Server required from ServerManager application.

Please refer to the '*MorphoManager Audit Trail*' dedicated document for audit log feature specific details.

Password Management for Default Operator

By default, below two operators will be available in system for managing or accessing MorphoManager Server and Client application:

- Server Administrator (to technically administrate MorphoManager Server)
- Administrator (for the MorphoManager system administration)



Server Technical Administrator allowed to access full server privilege with the below mentioned credentials:

- Username: **serveradministrator**
- Password: **password**

System Administrator allowed to access full client privilege with the below mentioned credentials:

- Username: **administrator**
- Password: **password**

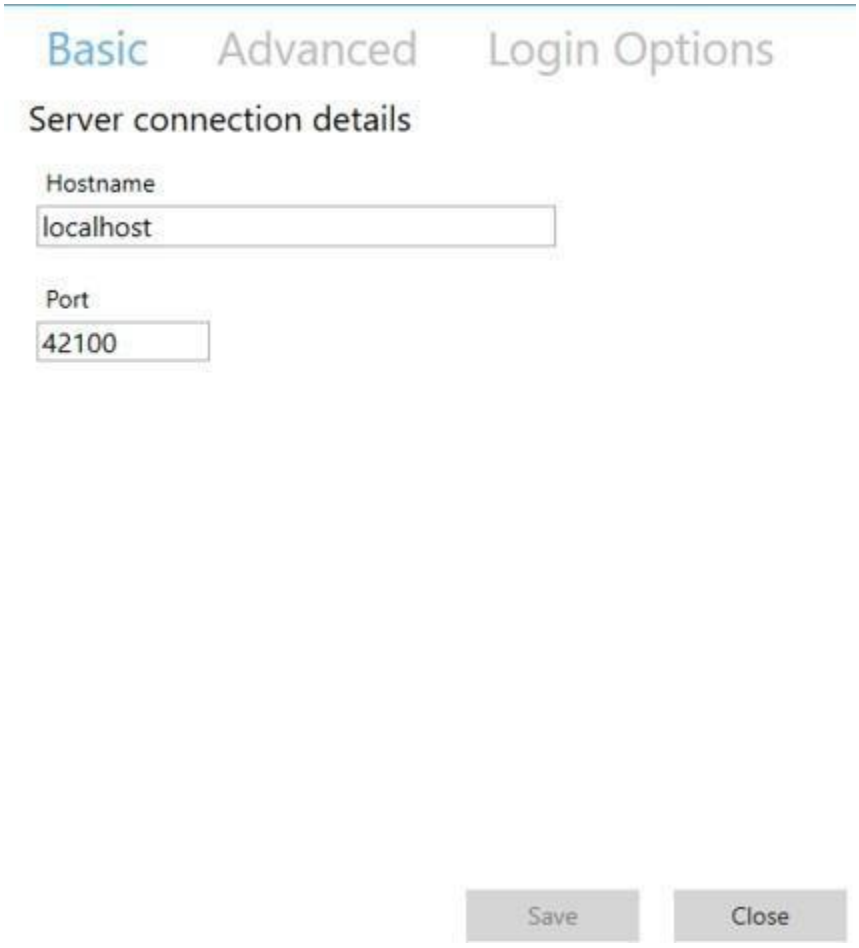
Password reset is requested at first login.

The client session automatically logs out after 20 minutes of inactivity on machine.

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

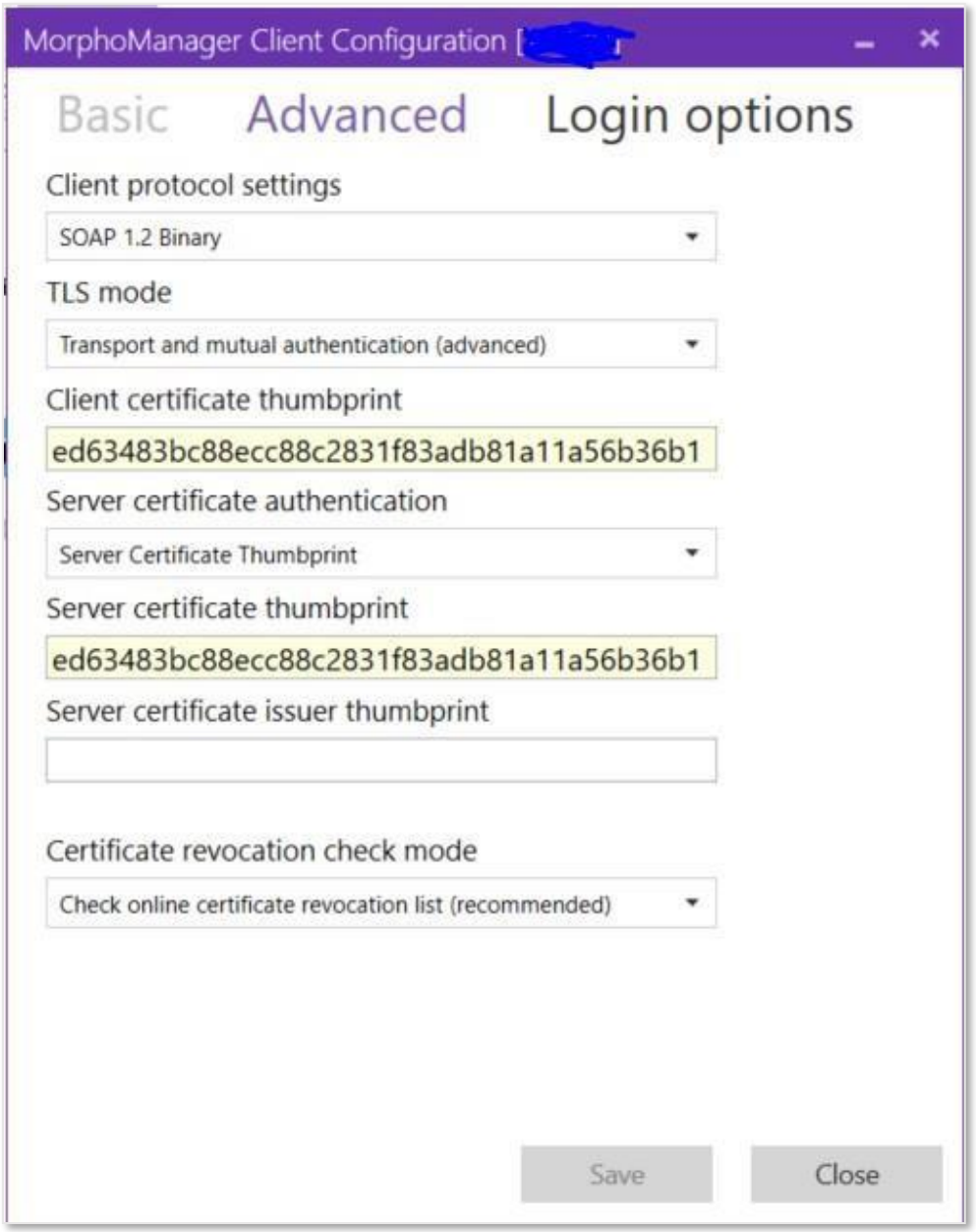


Server Connection Details

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.

Advanced



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.

IDEMIA recommends not to use self-signed certificates for production environments. Please refer to the TLS configuration Manual.

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:

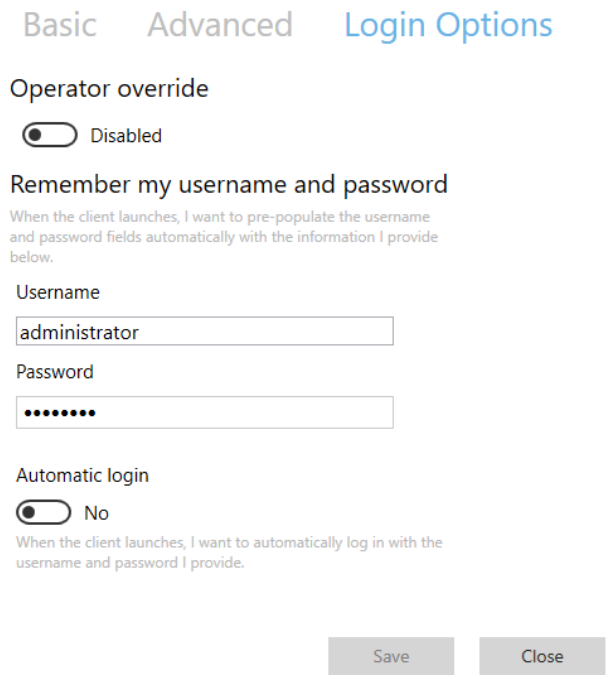
If **Disabled** is selected, MorphoManager will perform no further validation on the certificate.

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.

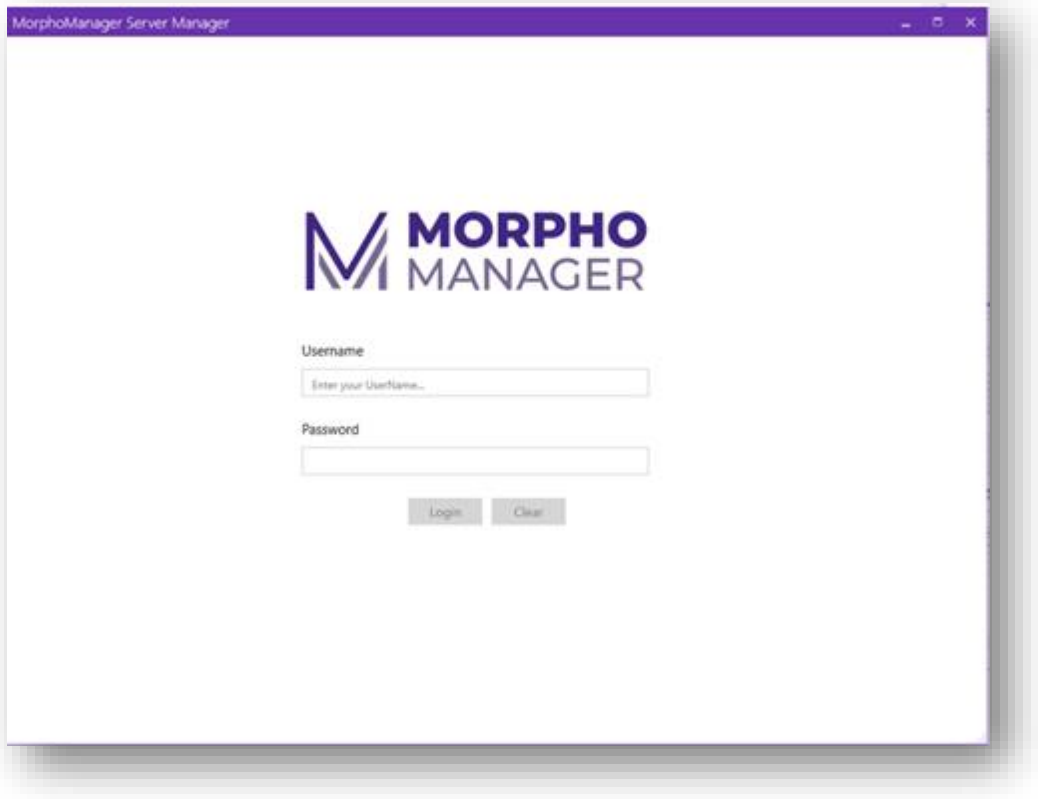
Operator override: The operator will be able to change the advanced settings before logging in.

Passwords for operators to login to MorphoManager Client follow a defined policy for renewal. In case *automatic login* is configured for an account to login to MorphoManager Client Configuration tool, do not forget to update the password inside Client Configuration tool for automatic login.

MorphoManager Server Manager

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

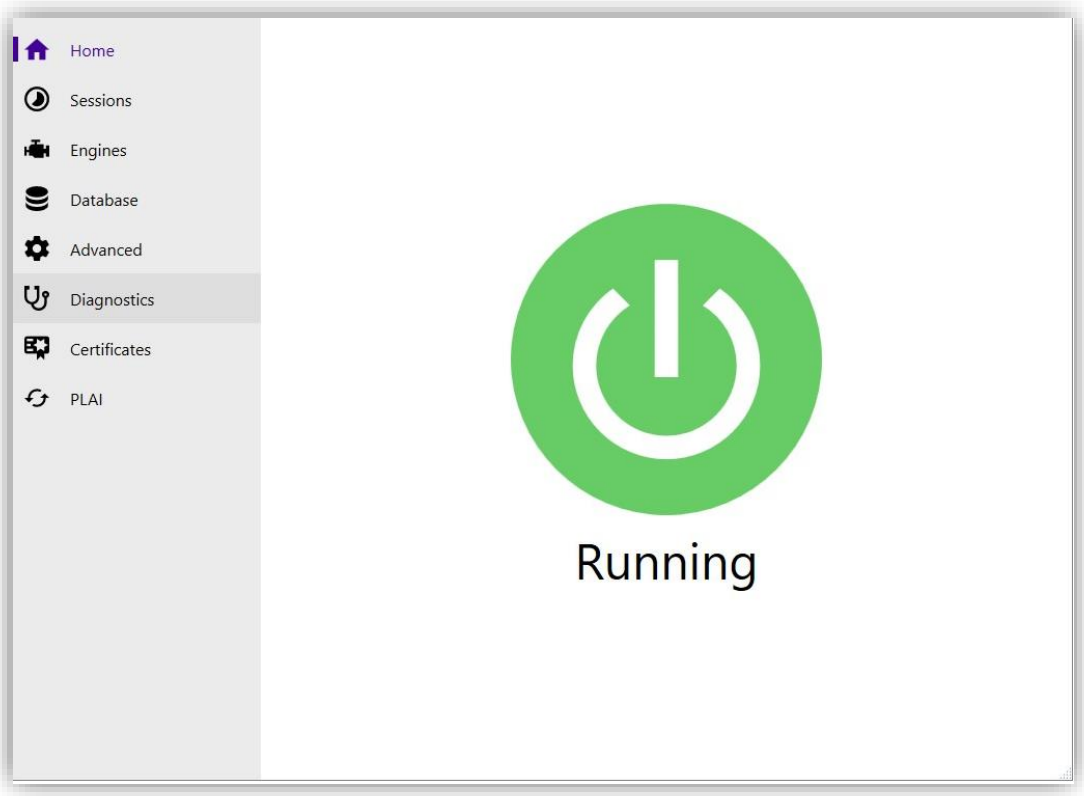
Launch MorphoManager Server Manager, the screen will appear to enter user credentials for login purpose.



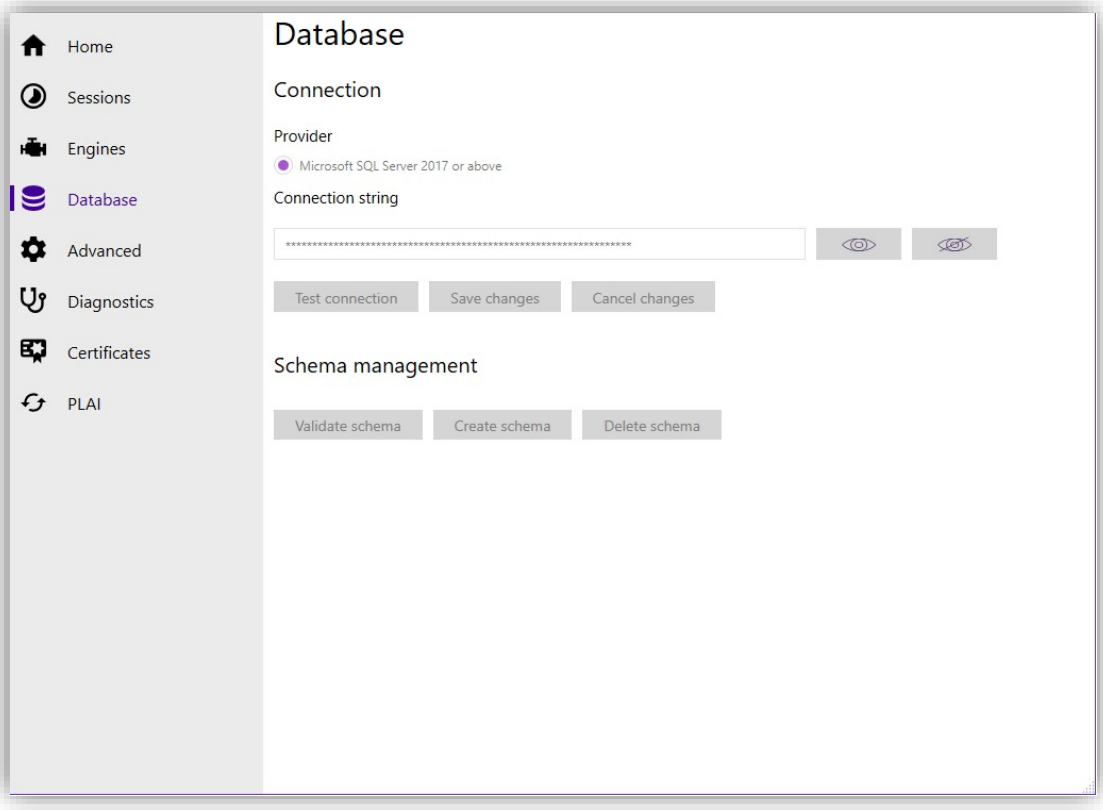
Login to Server Manager by entering valid credentials with Server Technical Administrator operator.

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: SQL Server is the database provider type.

From 16.4 version of MorphoManager, support of SQL CE has been removed and not supported anymore by IDEMIA.

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.

From 16.4 version of MorphoManager, the connection string with SQL Server is hidden by default.

- Click on Eye button to show the connection string
- Click on Cross Eye button to hide it back

NOTE: This can only be accessible to authorized accounts.

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.

IDEMIA recommends not to use self-signed certificates for production environments. Please refer to the TLS configuration Manual.

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 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.

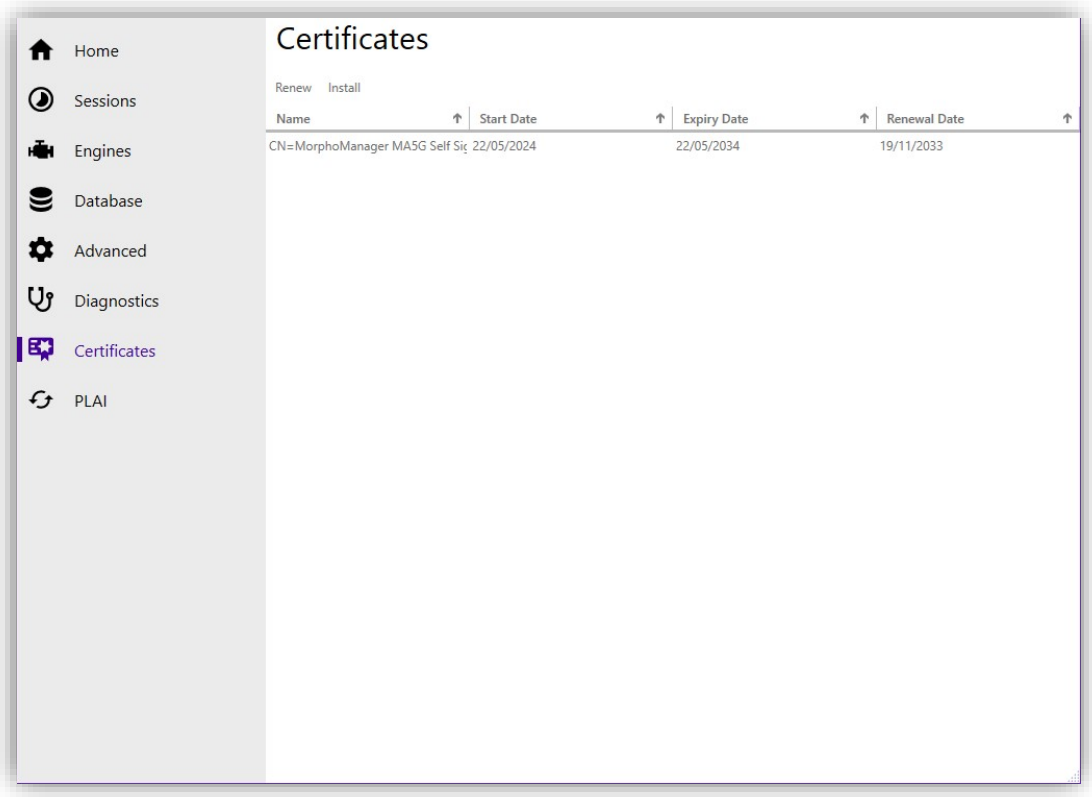
The following is required of the certificate to pass validation:

- 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 Enchased 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.

Certificate Management

This tab is used to display details related to authority certificates that installed into the system at time of server installation process.



Here we will be having name of installed authority certificate, its start date, expiry date and date of renewal. Expiration date is 10 years after start date. Renewal period starts 6 months prior to expiration date.

Renew	to be used before the expiration date of the existing Certificate Authority
Install	to re-install the authority certificate in one of the following cases:

- After a delete / create of the database schema (creating a schema adds a new authority certificate to the database, but installing it in the certificate store requires the Install button to be triggered)
- After restoring a backup.

NOTE: 'Renew' and 'Install' operations require Windows administration rights.

Product Activation and License management

Starting from version 16.7, MorphoManager Client software requires a specific license to unlock features such as device management, user management, and BioBridge management.

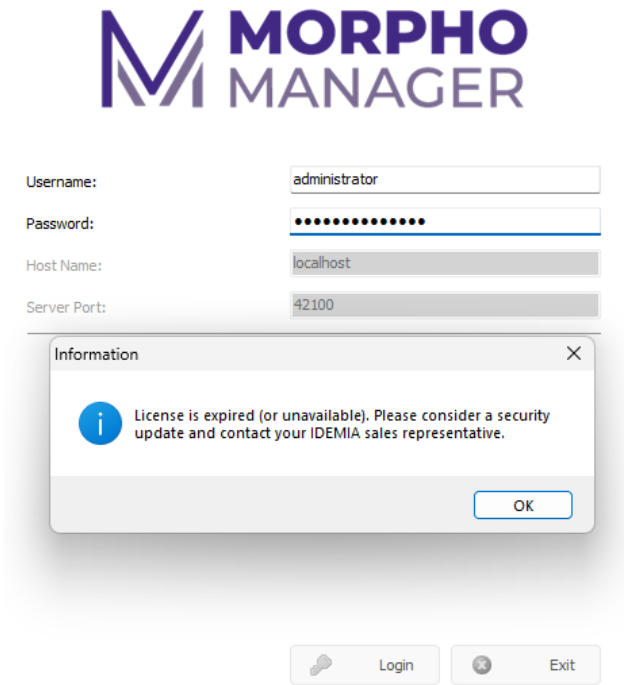
Below is the list of available licenses:

License Type	License Name	Description
Device and User Management	MM_5_TERMINALS	Supports 0 to 5 biometric devices, up to 20K users
	MM_10_TERMINALS	Supports 0 to 10 biometric devices, up to 20K users
	MM_25_TERMINALS	Supports 0 to 25 biometric devices, up to 20K users
	MM_50_TERMINALS	Supports 0 to 50 biometric devices, up to 20K users
	MM_100_TERMINALS	Supports 0 to 100 biometric devices, up to 20K users
	MM_ENTERPRISE	Supports 0 to 5000 biometric devices, up to 100K users, Includes Single Sign-On (SSO)
BioBridge Management	MM_EXTRA_BIOBRIDGE	Required for Lenel OnGuard BioBridge and CCure 9000 BioBridge
Audit Log	MM_AUDIT	Enables audit log functionality

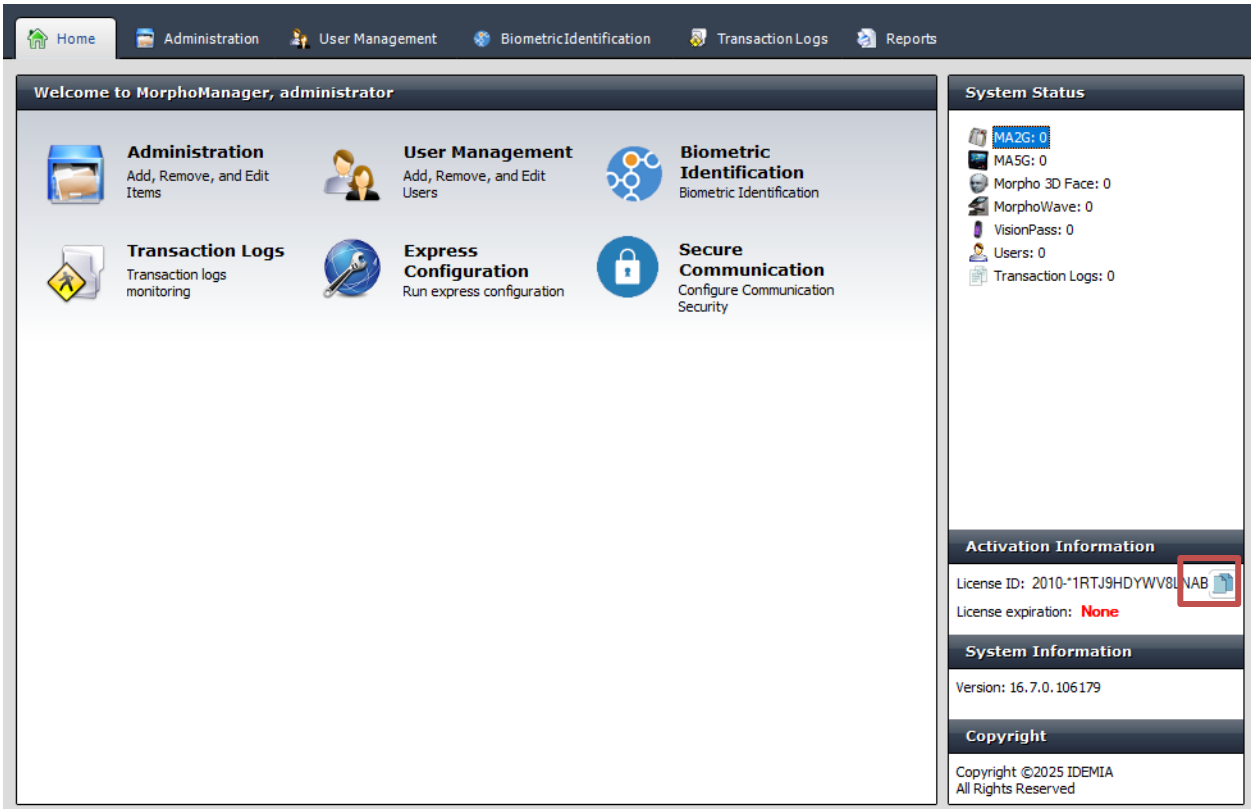
NOTE : previous *MM_Activation* license is no longer required to activate the MorphoManager software.

Procedure for License request

1. Launch and login MorphoManager Client 16.7.0 or above with default operator credentials.



2. On the information window about unavailability of a license, click OK and proceed with Client login.
3. Copy license ID from 'Activation Information' section of Homepage.



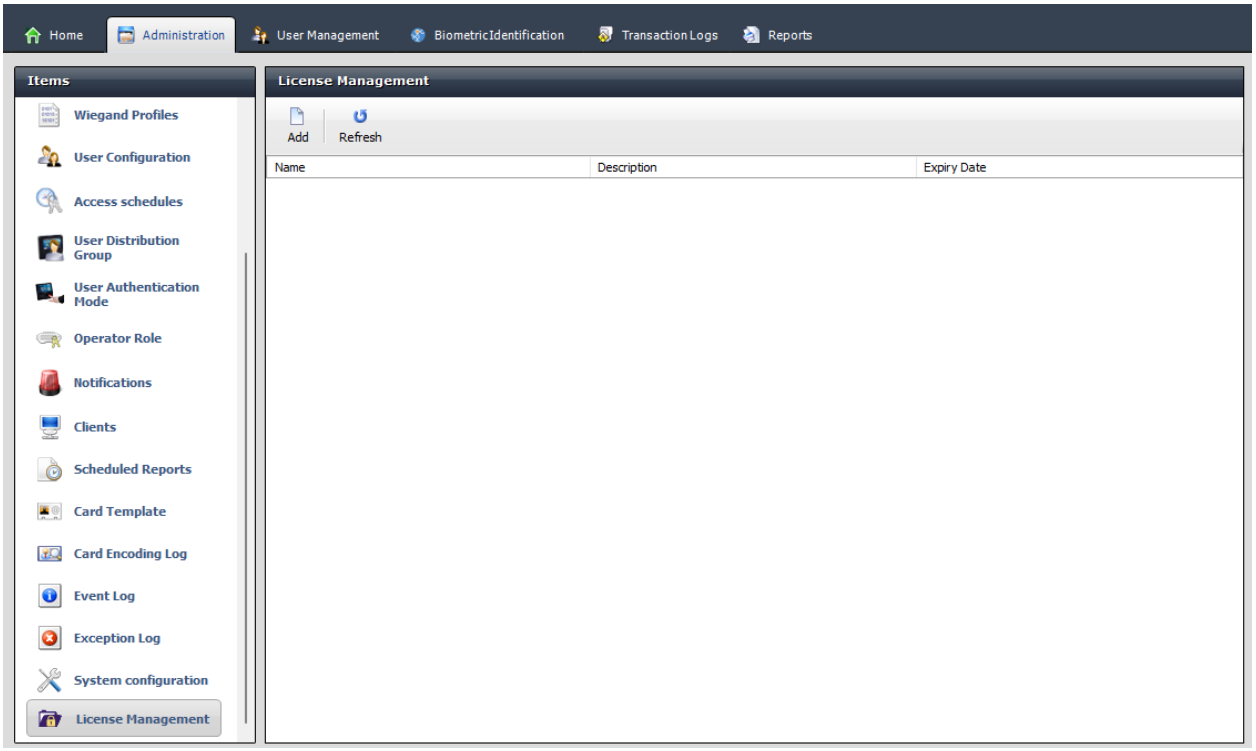
4. Request a license via your IDEMIA sales representative or check https://biometricdevices.idemia.com/s/morphomanager
5. Receive the license file by email.

Please note, in case you back-up and restore your Machine, a new license will be required.

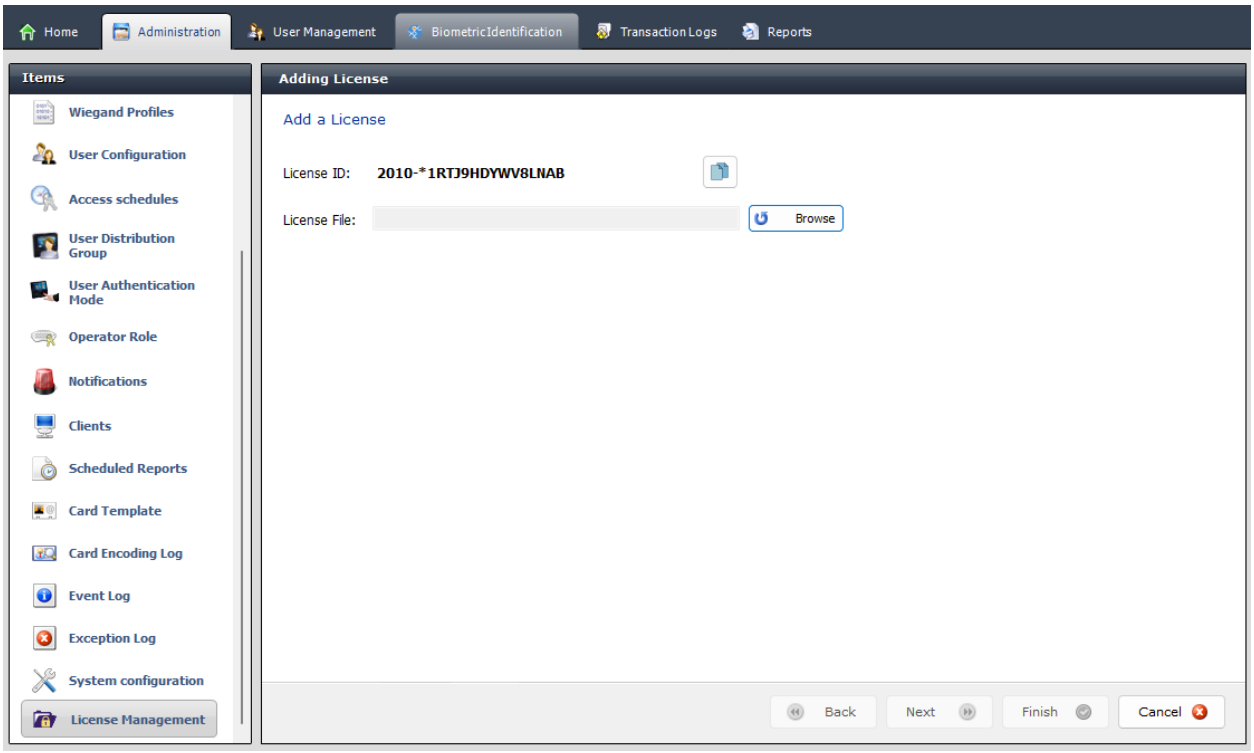
Procedure for License upload

MorphoManager does not need direct Internet connection to proceed to license activation.

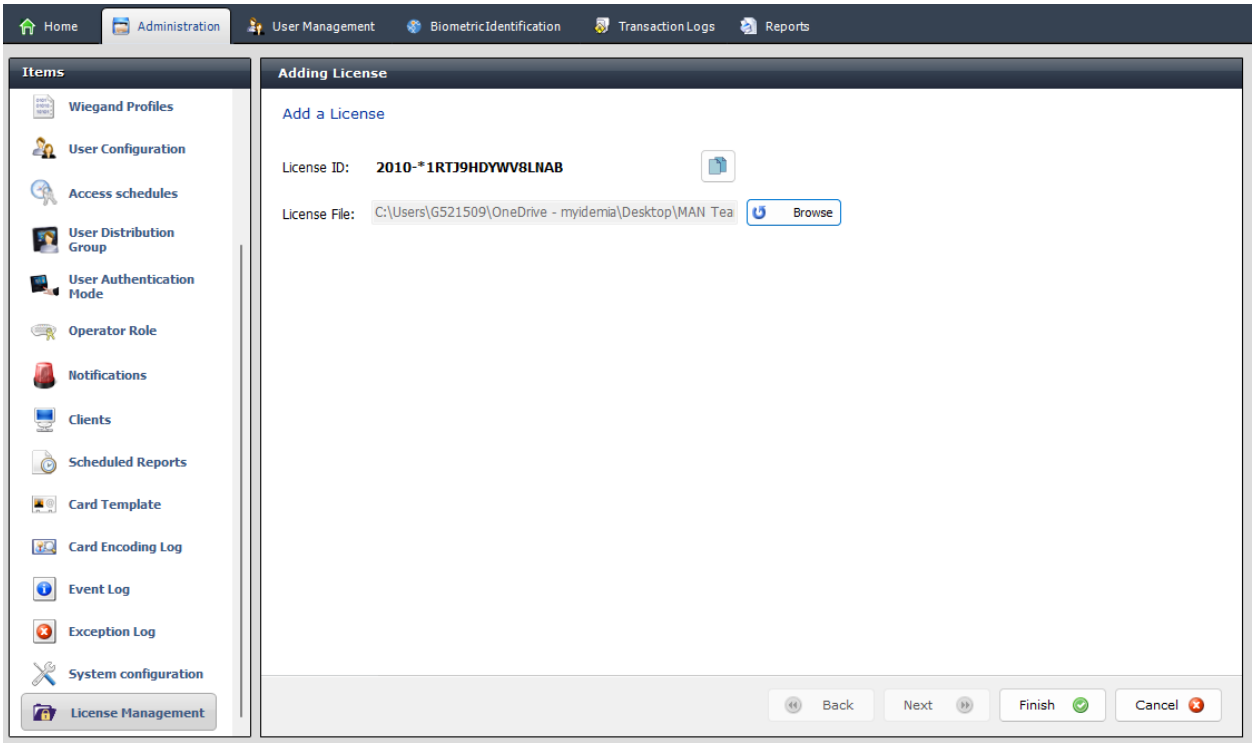
Once your License file is available on your computer (or on any portable device connected to your computer), then upload it on MorphoManager.



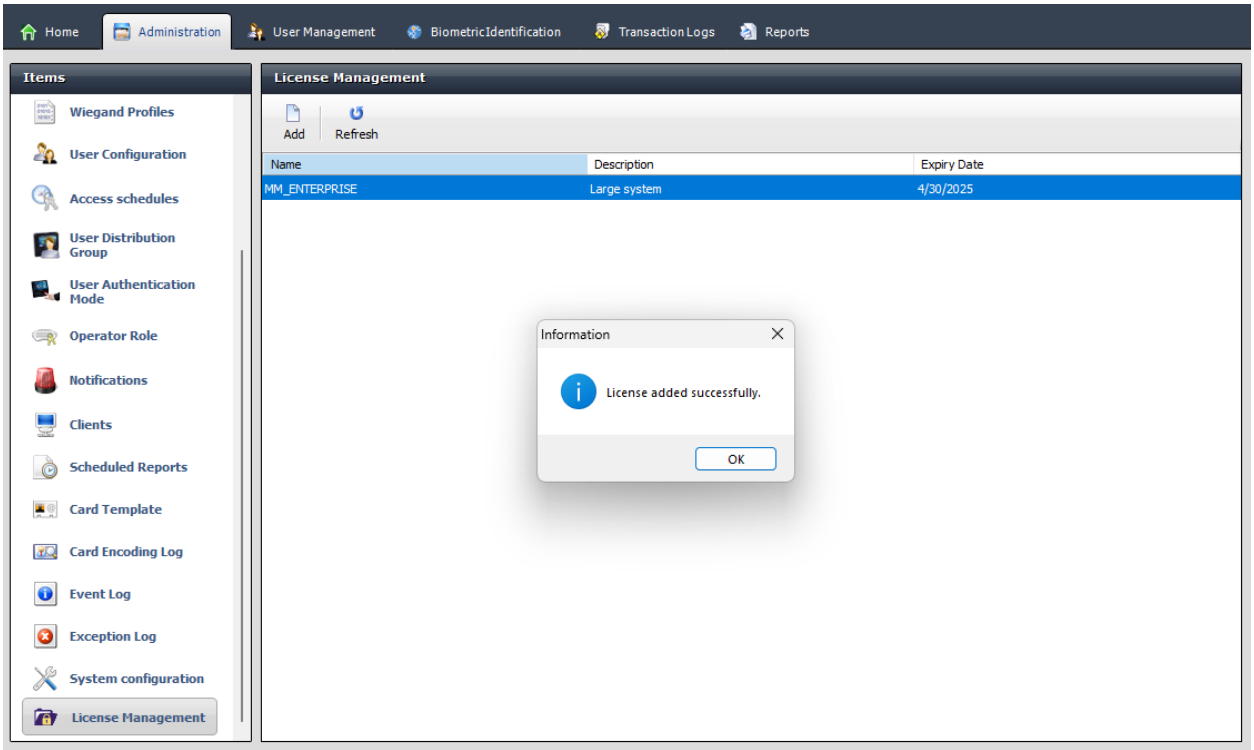
1. In the License Management section of Administration, click **Add**



2. **Browse** and upload the license file.

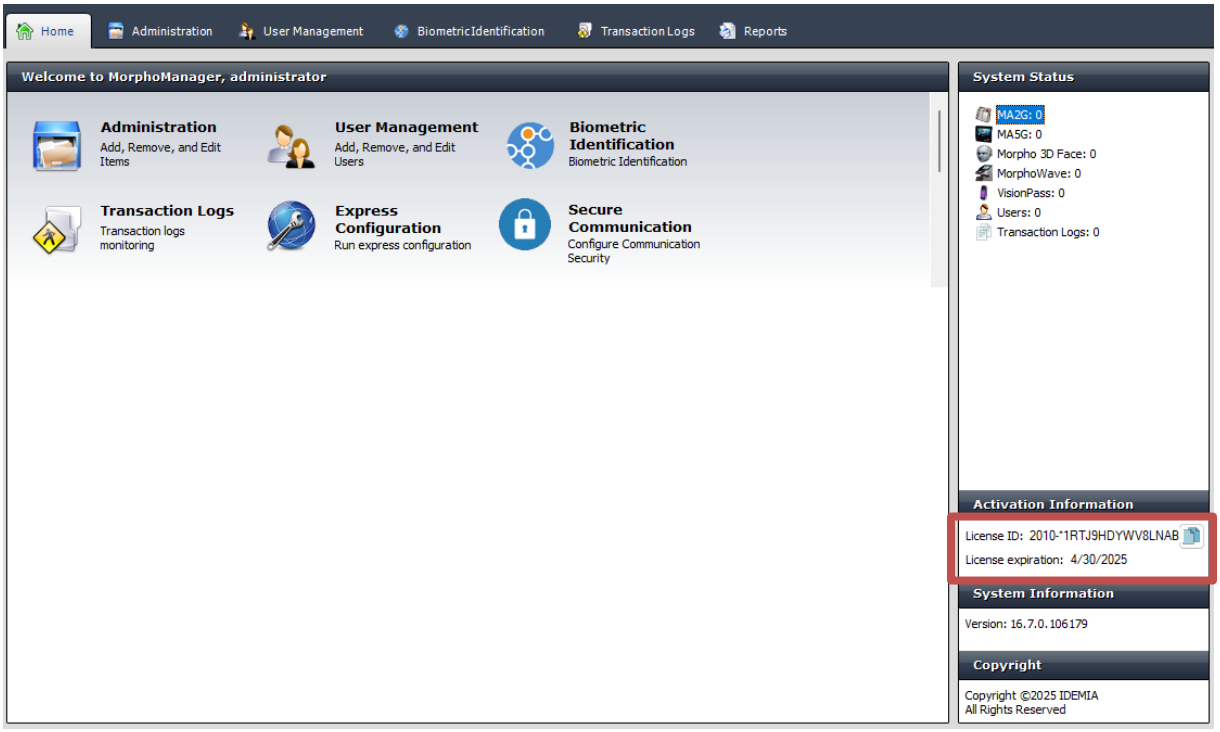


3. Click on **Finish**.



After successful upload, the Activation Information of the MorphoManager Client homepage will display the closest expiry date among all valid licenses available in the system.

NOTE: a restart of the machine hosting MorphoManager Server may be required to reflect the expiry date of a newly uploaded license.



NOTE : Other IDEMIA licenses (for instance, VERIF or IDENT) can be added through MorphoManager License Management. However, they will not appear in the License Management interface: only licenses listed above will be displayed there.

The license activation procedure must be renewed before the license expiration. Upon starting MorphoManager Client or BioBridge Enrollment Client, a notification will alert the operator **3 months before the license expiration date**.

License Protected Features

License Type	Restricted Actions (If No Valid License or Expired)
Device and User Management (MM_XX_TERMINALS or MM_ENTERPRISE)	Cannot add or edit biometric devices in the Biometric Device section.
	Cannot add devices using Express Configuration.
	Cannot add, edit, or import users in User Management. Action buttons like Add Photo and Import Template will be disabled.
	Restricts user and device management if SSO enabled but no valid MM_ENTERPRISE license is available or expired.
	Restricts user and device management if audit log feature is enabled but no valid MM_AUDIT license is available or expired.
BioBridge Management (MM_EXTRA_BIOBRIDGE)	Restricts the usage of "Configure Connection" button in the BioBridge tab for Lenel or CCURE 9000 without a valid MM_EXTRA_BIOBRIDGE license.
	Prevents BioBridge Enrollment Client from starting if the license is invalid, expired, unavailable, or user capacity is reached.
	Prevents enrolling, editing, importing templates, or adding photos in Enrollment Client if user capacity is reached.
	Restricts BioBridge Enrollment Client if BioBridge is configured for Lenel or CCURE 9000 and the related MM_EXTRA_BIOBRIDGE license has expired.
	Blocks Embedded Enrollment in C_CURE and ONGUARD if MM_EXTRA_BIOBRIDGE license is unavailable or User Capacity is reached.
	Restricts BioBridge Enrollment Client usage if a valid MM_EXTRA_BIOBRIDGE license exists but other necessary licenses (MM_XX_TERMINALS or MM_ENTERPRISE) do not exist or have expired.
	Prevents BioBridge Enrollment Client from starting if SSO is enabled but no valid MM_ENTERPRISE license is available or expired.
Audit Log (MM_AUDIT)	Prevents BioBridge Enrollment Client from starting if Audit Log is enabled but no valid MM_AUDIT license is available or expired.

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.

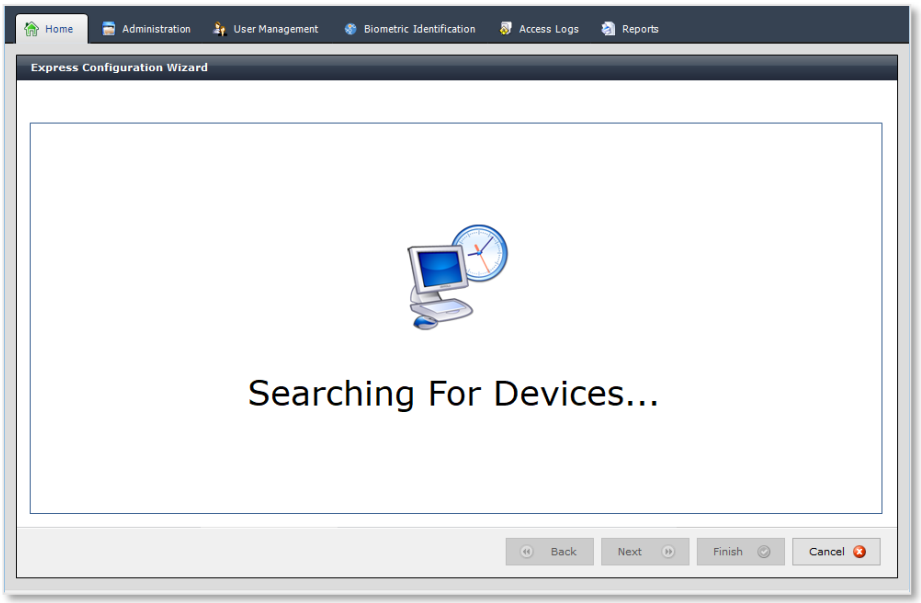
Secure Communication Policy

Please select the recommended “Enforced Security – Self-generated Certificates” value, or refer to the dedicated section below.

Device discovery

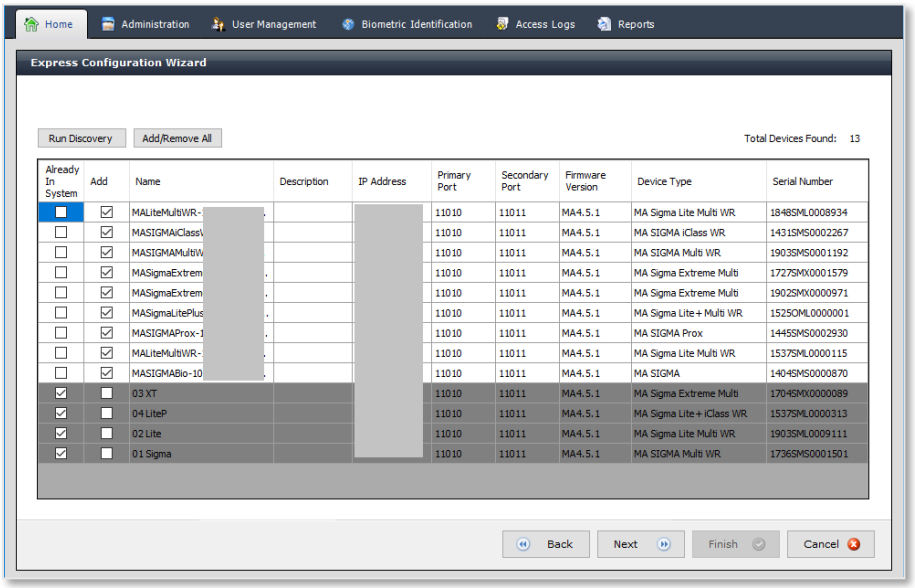
The second screen of the Express Configuration Wizard will detect devices. MorphoManager uses User Datagram Protocol (UDP) to discover devices.

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.

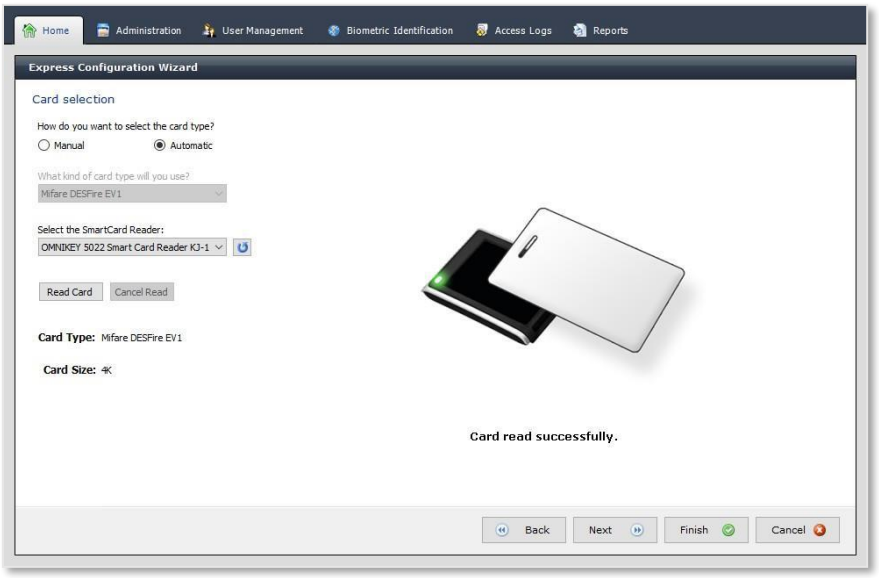
For each of the Authentication modes that include a biometric, the administrator can configure whether Contact templates, Contactless templates, or Face templates are required. For the Card Only and Card+ PIN authentication modes, Biometrics are not configurable and will never be required.

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 Screen.

Home Screen

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

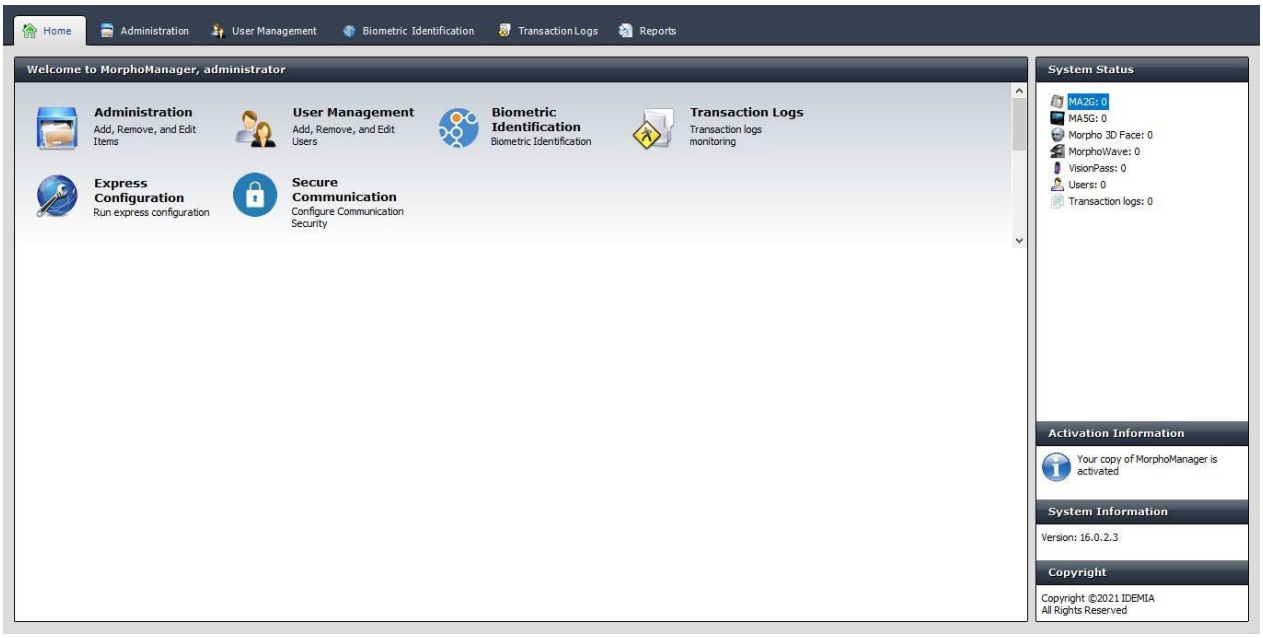
- Home
- Administration
- User Management
- Biometric Identification
- Transaction Logs
- Reports

And a set of buttons on the home screen. New button “Secure Communication” added for selecting one of the below mentioned Secure Communication Policy :

- Enforced Security Self-Generated Certificate
- Enforced Security Imported Certificate
- On-Demand Security

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.

Secure Communication Policy

The Secure Communication Policy defines the security modality for the communication with the biometric terminals.

Overall guideline

The Secure Communication Policy can be either Enforced Security, or On-demand security. Selecting one value is a mandatory step after installation. Enforced Security shall be used for a secure system, and is recommended by IDEMIA. If the pre-requisites of Enforced Security are not met, On-Demand security is available as a temporary phase.

- Pre-requisites of Enforced Security Secure Communication Policy : The system has no other biometric terminal as:
  - MorphoWave Compact / XP
  - MorphoWave SP
  - VisionPass
  - VisionPass SP
  - SIGMA Lite and Lite+
  - SIGMA Wide
  - SIGMA Extreme
- All biometric terminals have an Enforced Security status.

Please refer to:

- The dedicated Technical Bulletin for an overview of Enforced Security configuration.
- The Knowledge Base, available on IDEMIA portal, for a “How to” guideline depending on your use case.

Enforced security, self-generated certificates

This Secure Communication Policy:

- Ensures the biometric terminals in the Enforced Security status.
- Secures the communication between MorphoManager Server and the biometric terminals with TLS
- Automatically generates the required TLS certificates.
- Automatically incorporates the generated TLS certificates in all Key Policies of the MorphoManager installation.
- Is recommended by default.

Enforced security, imported certificates

This Secure Communication Policy:

- Ensures the biometric terminals in the Enforced Security status.
- Secures the communication between MorphoManager Server and the biometric terminals with TLS
- Is reserved to TLS experts and / or installations with an existing PKI (Public Key Infrastructure)

The TLS certificates are to be generated outside MorphoManager and imported

- in all Key Policies
- in all Biometric Devices

On-demand security

In this policy, TLS secure communication with the terminals is not enforced, but can be used on a case by case basis.

Administration

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

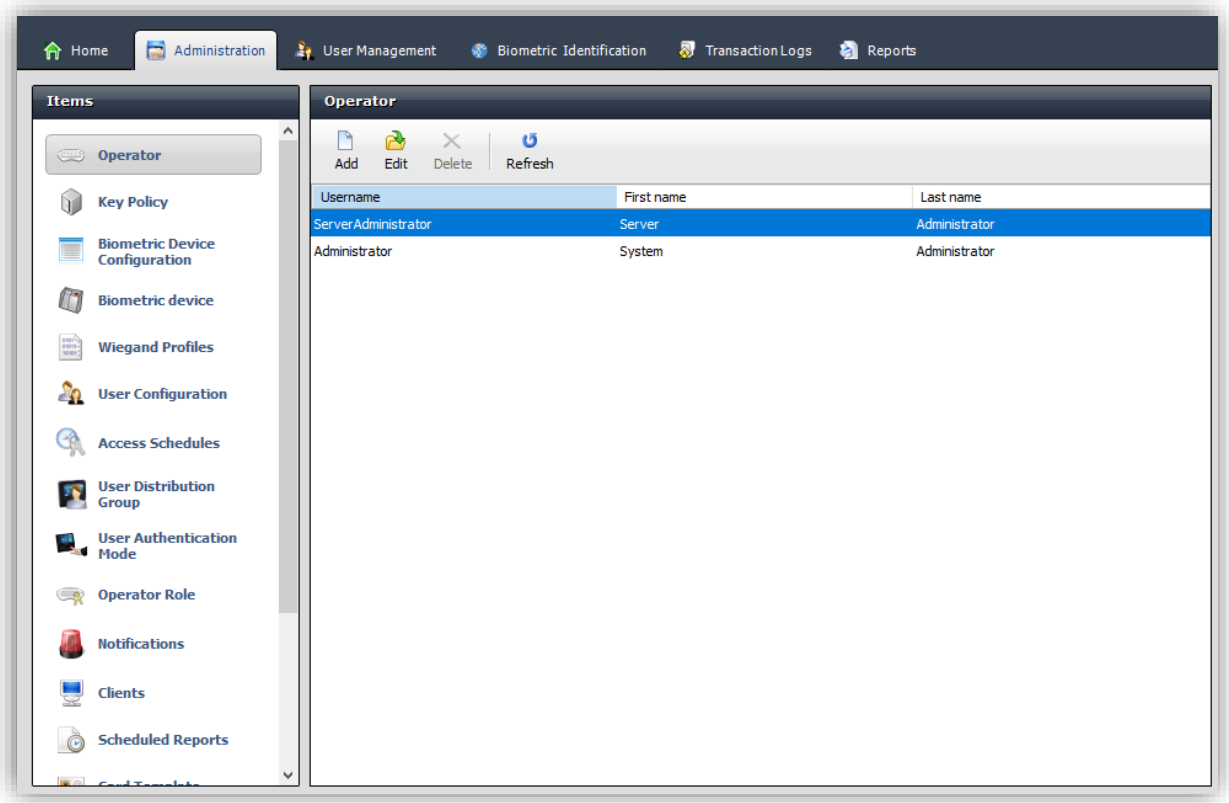
> When creating or editing an item, a colored text entry box means the information is required and must be filled in before the item can be finished and saved.

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.

By default, below two operator will be available in system for managing or accessing MorphoManager Server and Client application:

- Server Technical Administrator: Having full access to Server application
- System Administrator: Having full access to Client application

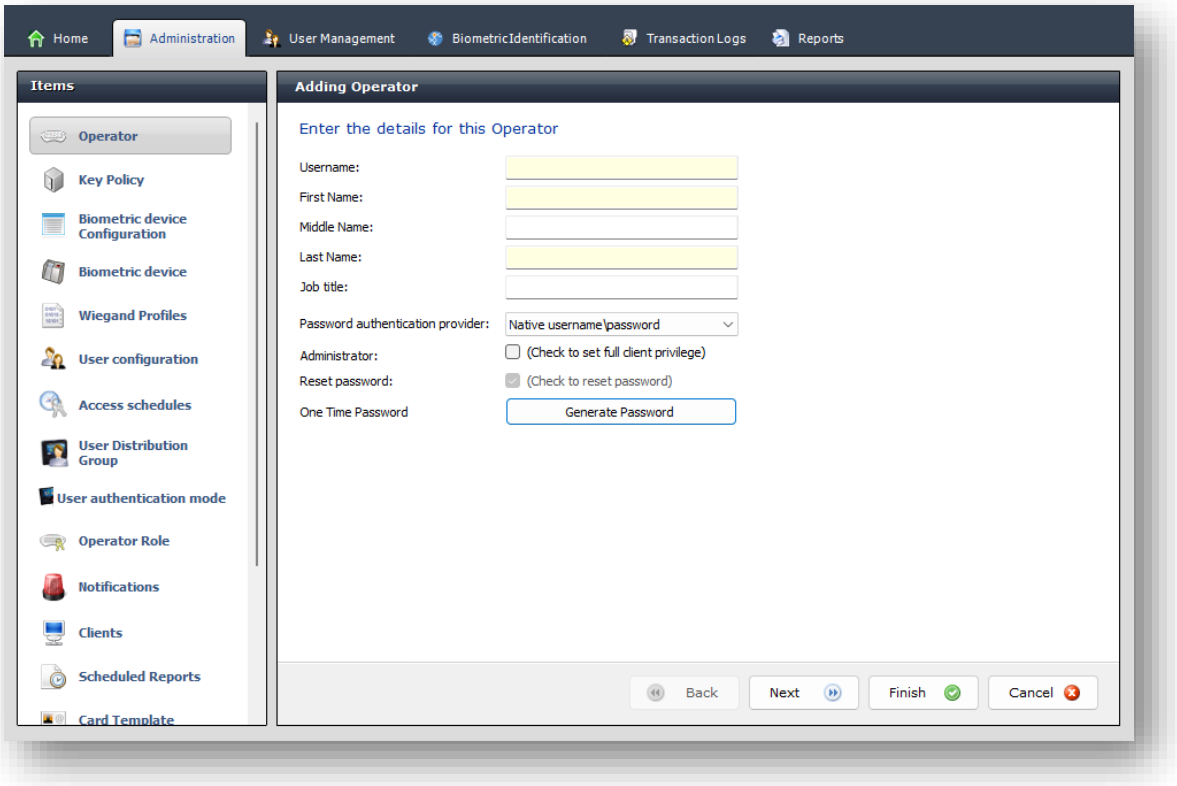


Both Administrator operators cannot be deleted or modified. Keeping the password secure for them is essential.

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:

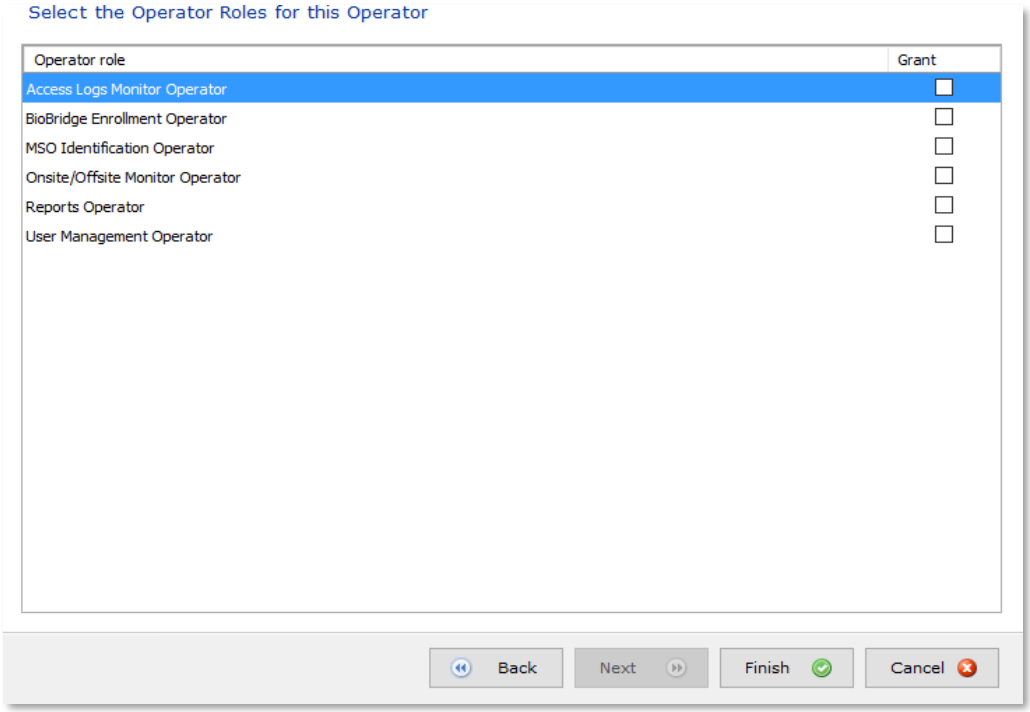
	The Username and Password is stored in the MorphoManager database and is managed by MorphoManager **Active directory:** The password and account state are managed by Active Directory.
Administrator:	Select this option to provide full administrator rights to this user (not recommended).
One Time Password:	Generate random password (can be copied from the MorphoManager Graphical User Interface) which will be required at first login, and after the operator will be requested to modify the password.

If the Operator has not logged in one (1) week time after the account creation, the account will be disabled. A disabled Operator shall contact an Administrator to for account reset and request to generate new One Time Password.

After a MorphoManager upgrade from any previous version to a version enforcing One Time Password, all operators will be required to change their password at first login.

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.



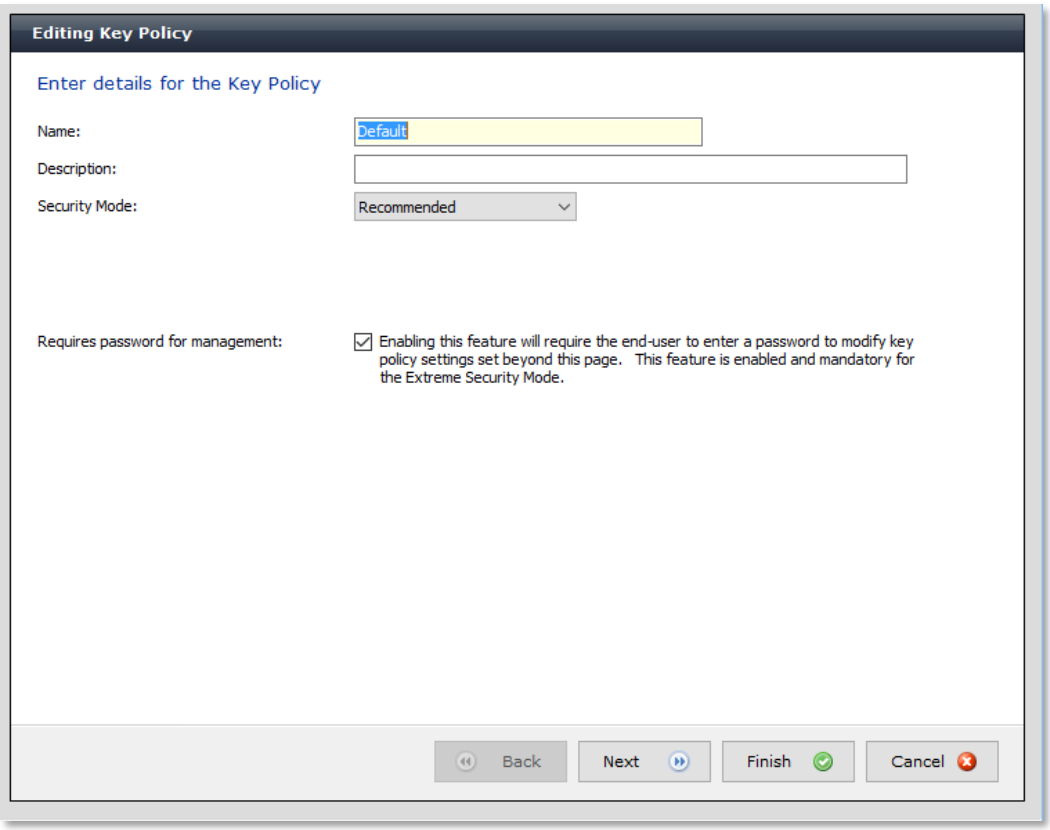
Key Policy

This section allows the setting of Contactless Card keys and TLS certificates for the communication with the Biometric Terminals. Once a Key Policy is configured, please assign it to the associated clients (for card encoding) and Biometric Device Configurations.

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. When in Extreme mode, the Key Policy:

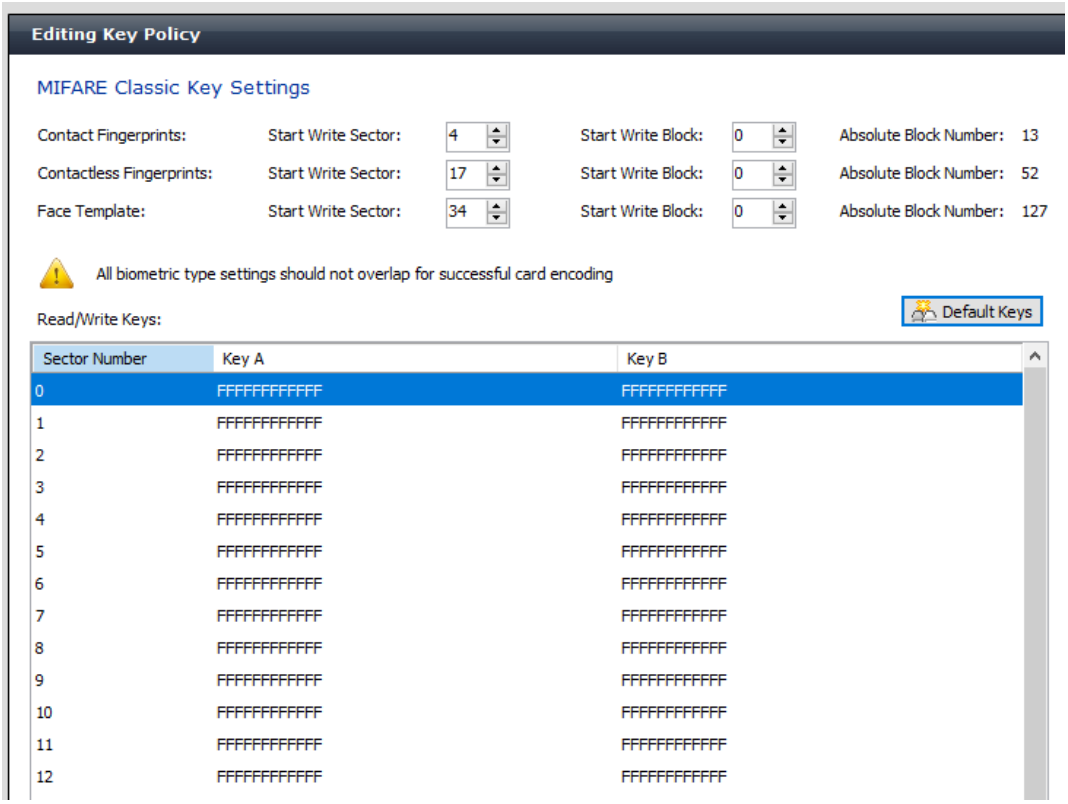
- is mandatorily secured with a password (see below), ,
- can be locked / unlocked by providing valid password .

Require password: When in Recommended mode, select this option to secure the Key Policy with a password (to be filled in on the next page). Securing the Key Policy with a password adds an extra layer of security: an operator will need to enter the password to view the card keys. This password is

not required during card encoding. The password can be recovered if it is forgotten.

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.

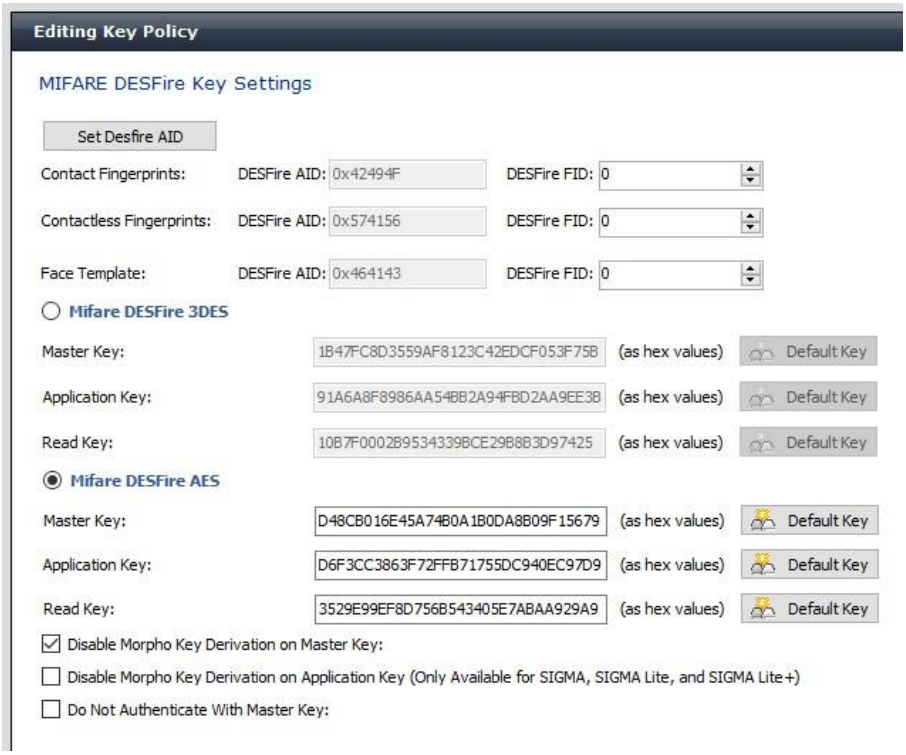
Start write block: Sets the block within the sector where the encoding/reading should start contactless fingerprints.

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.

The default value of Mifare Classic key settings in MorphoManager Key Policy differs from the terminal default value.

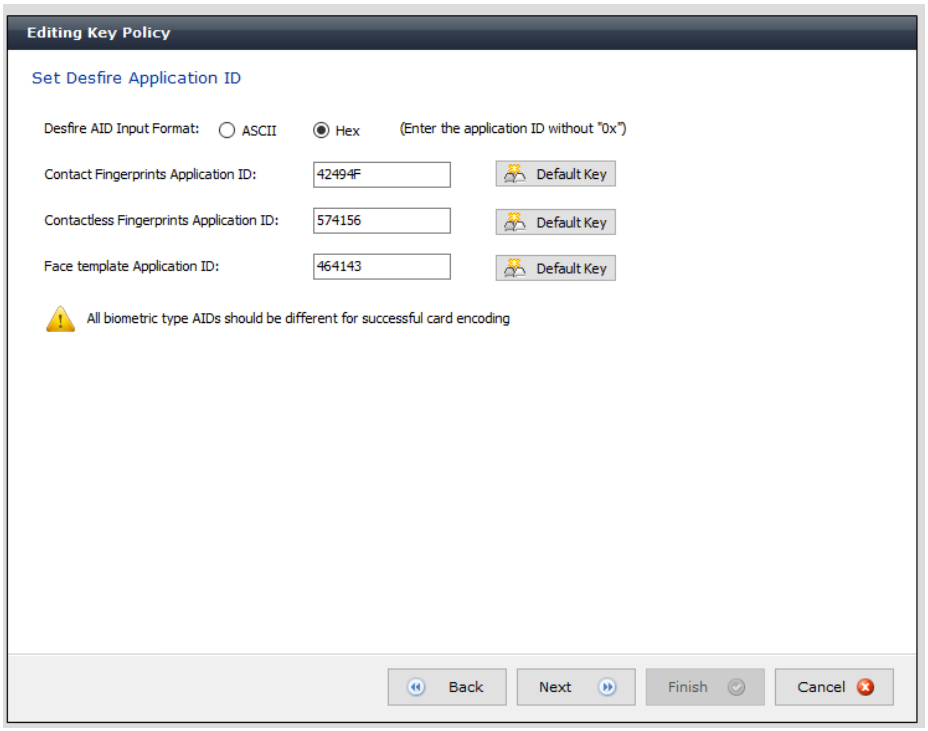
Screen 3 – MIFARE DESFire Key Settings

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.

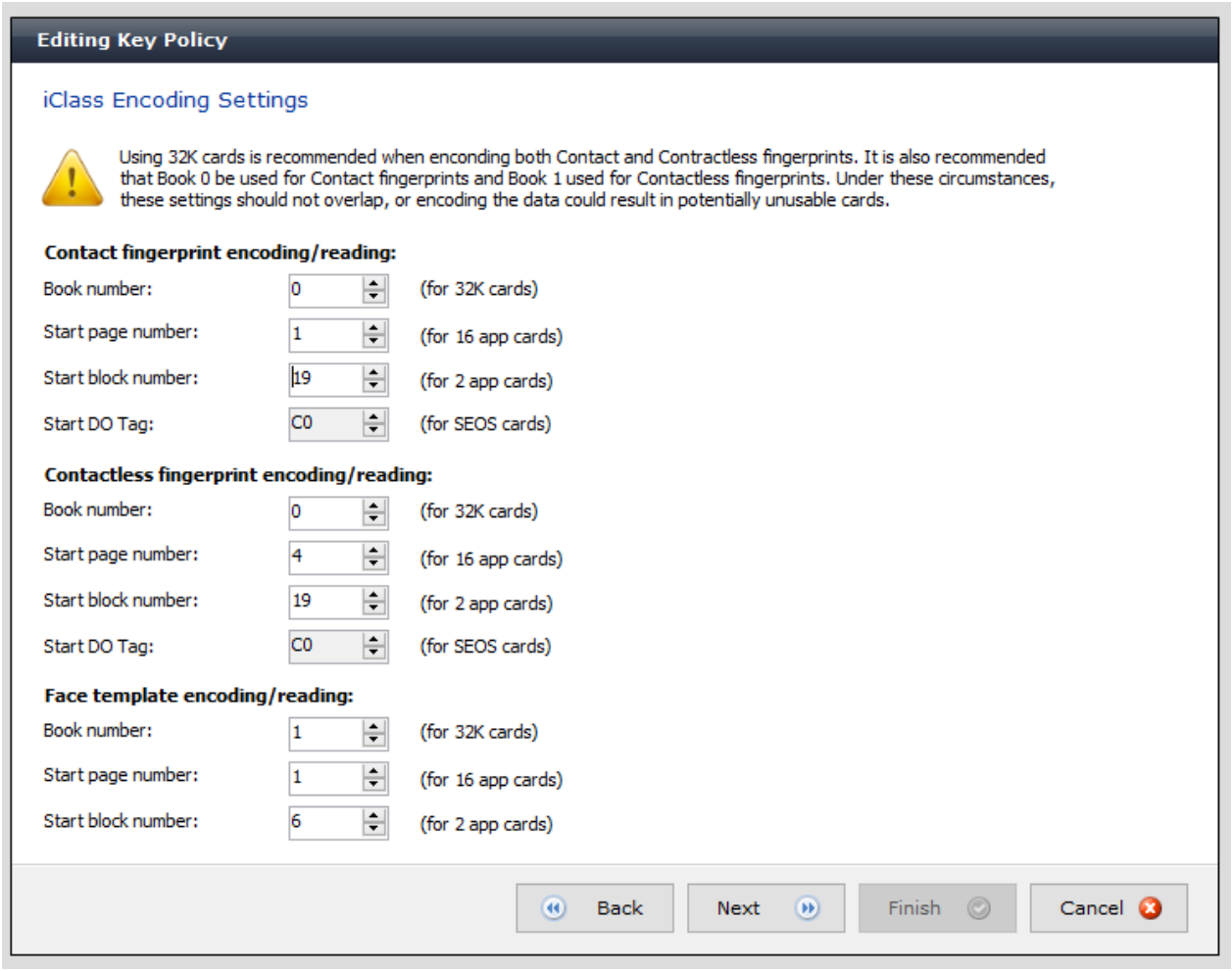
Set DESFire AID: This button leads to the page where Application ID can be set. The DesFire AID may be entered in ASCII or in HEX by choosing the relevant radio button.



The default value of Mifare DESFire key settings in MorphoManager Key Policy differs from the terminal default value.

Screen 4 – iClass Encoding Settings

Set the encode/reading properties for iClass cards. This page also sets the Application ID and D0 tag for Seos cards.



Start Reading from block setting applies only to 16K/2 cards.

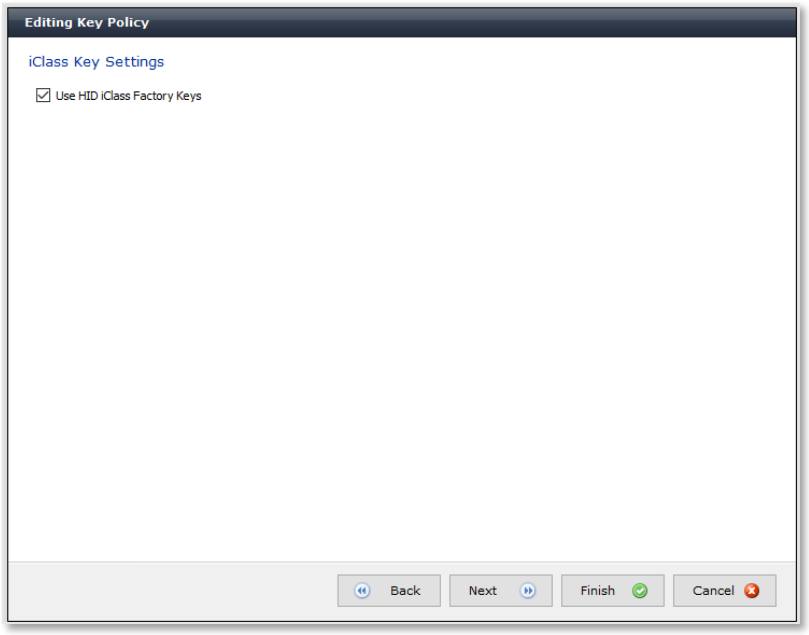
Start Reading from page setting applies only to 16K/16 cards.

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.

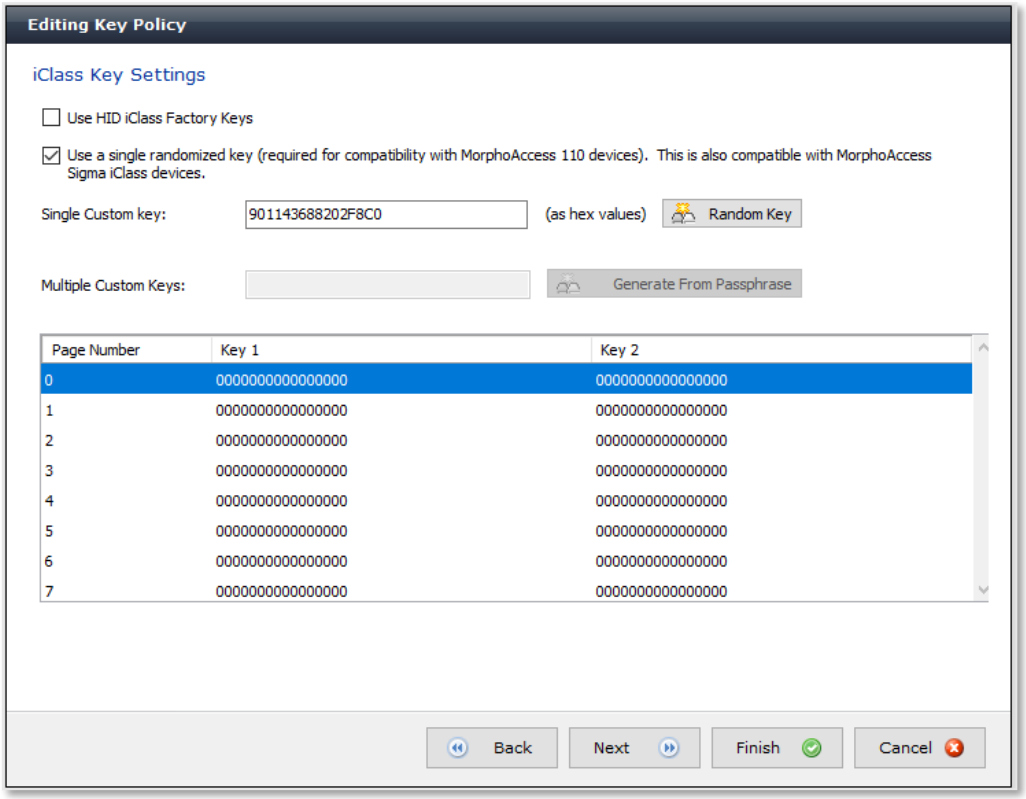
The default value of iClass Encoding key settings in MorphoManager Key Policy differs from the terminal default value .

Screen 5 – iClass Key Settings

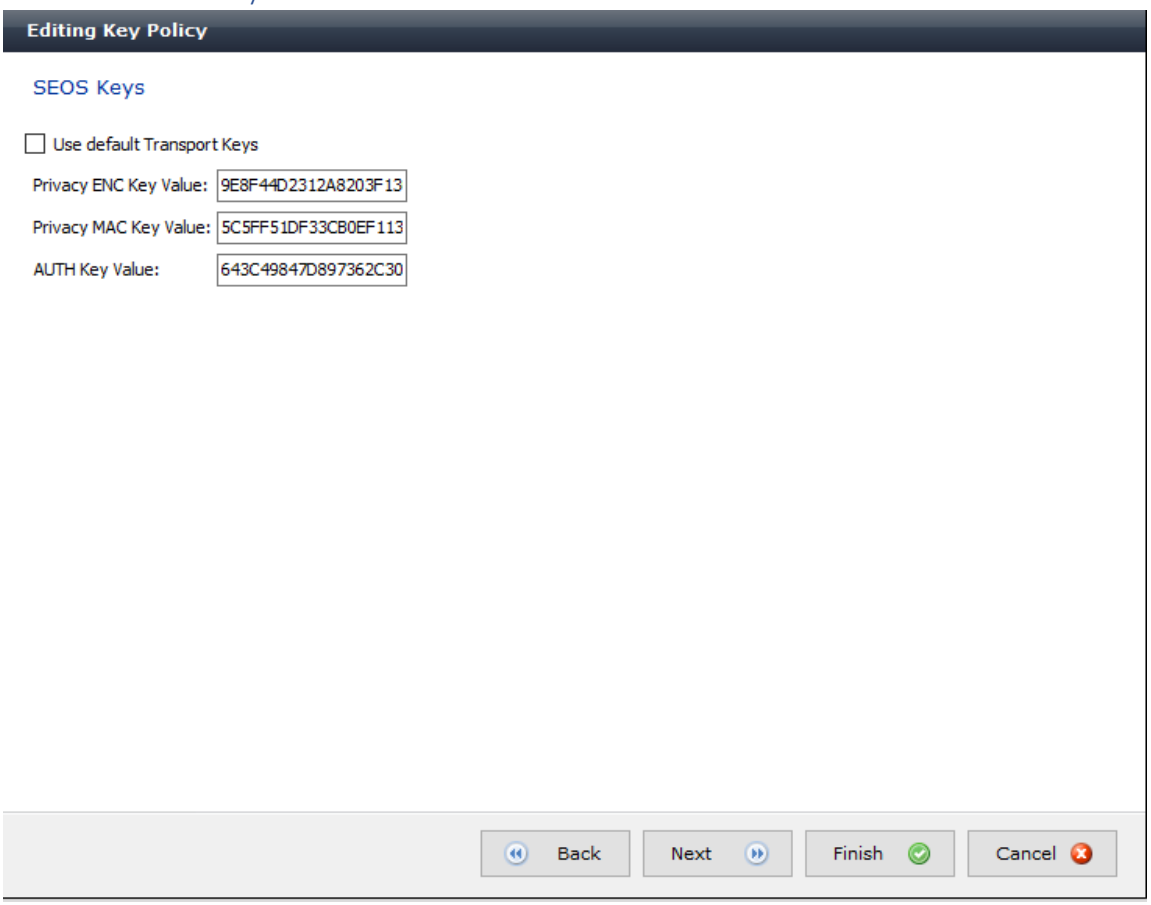
Set the key type, default, or non-default, for iClass on this screen.



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



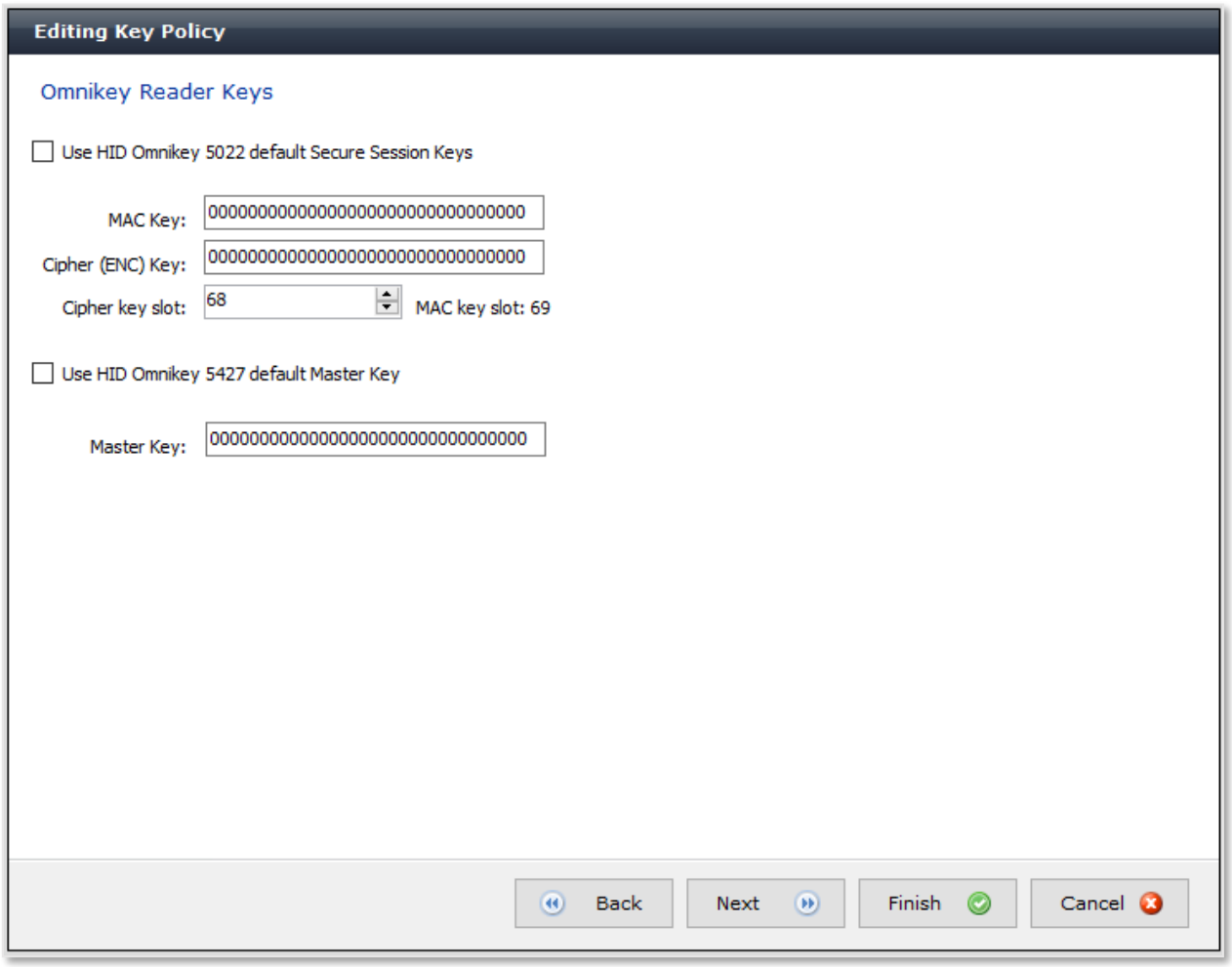
Screen 6 – SEOS Keys



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.

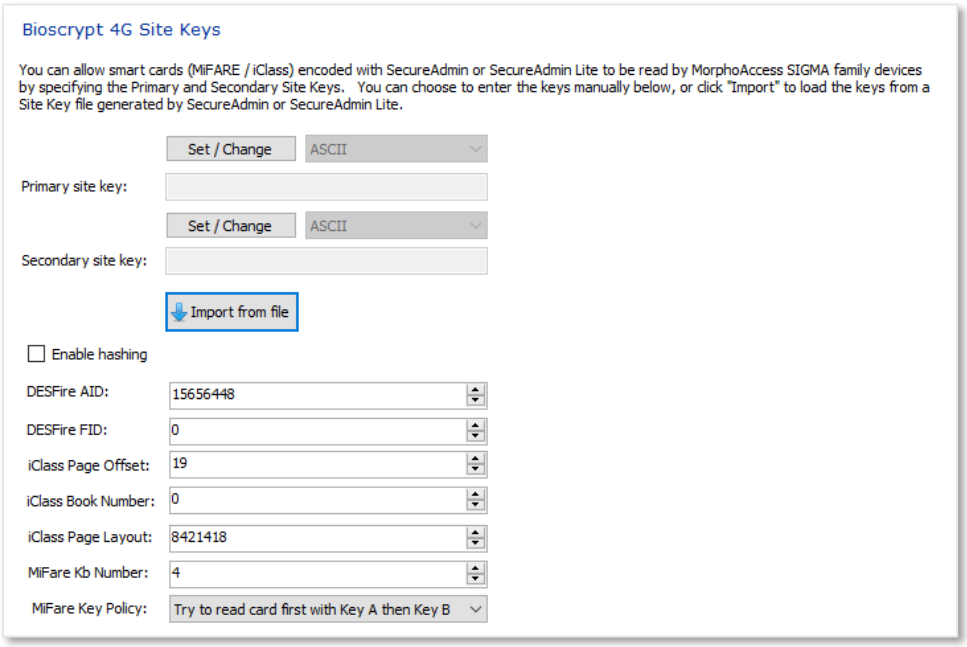
Screen 7 – Omnikey Reader Keys



The operator may set the Omnikey reader keys on this screen. These settings only apply to the Omnikey 5427. An Omnikey 5x21 will not be affected by these settings.

Omnikey 5021 & 5022 is not supported anymore and will be removed in a future release.

Screen 8 – Bioscrypt 4G Site Keys

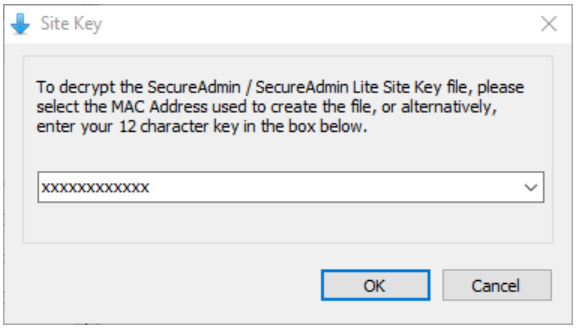


You can allow smart cards (MiFare/iClass) that have been encoded with Secure Admin or Secure Admin Lite to be read by the MA Sigma family of devices. You can enter the site keys manually, if they are known, or you can import the site key file that was generated in Secure Admin or Secure Admin Lite.

"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.

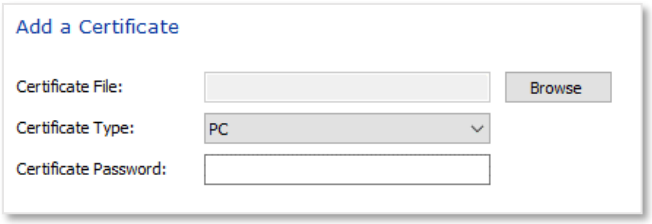
When importing a site key file, you will need to specify a "code" to unlock the site key file. Generally Secure Admin uses the MAC address of the PC to lock this file. You can either select your MAC address from the dropdown list or enter the 12-character key that was used during the creation of the 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 TLS 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 per Key Policy. Any number of terminals (biometric devices) certificates can be stored on the Key Policy.

If you have selected Enforced Security – Self-generated Certificates for the Secure Communication Policy, "Add" button will be disabled as each of the key policies loaded automatically with TLS certificates for the communication with the biometric terminals.

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.

To associate a Key Policy to either a client or a biometric device configuration, the Status shall be Unlocked.

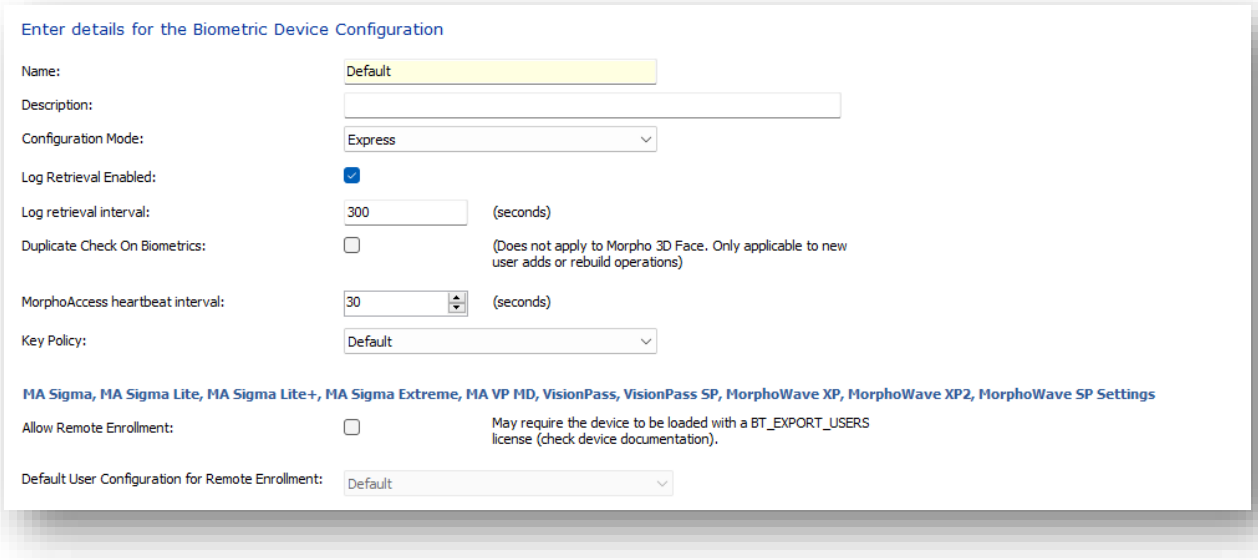
Biometric Device Configuration

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



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.

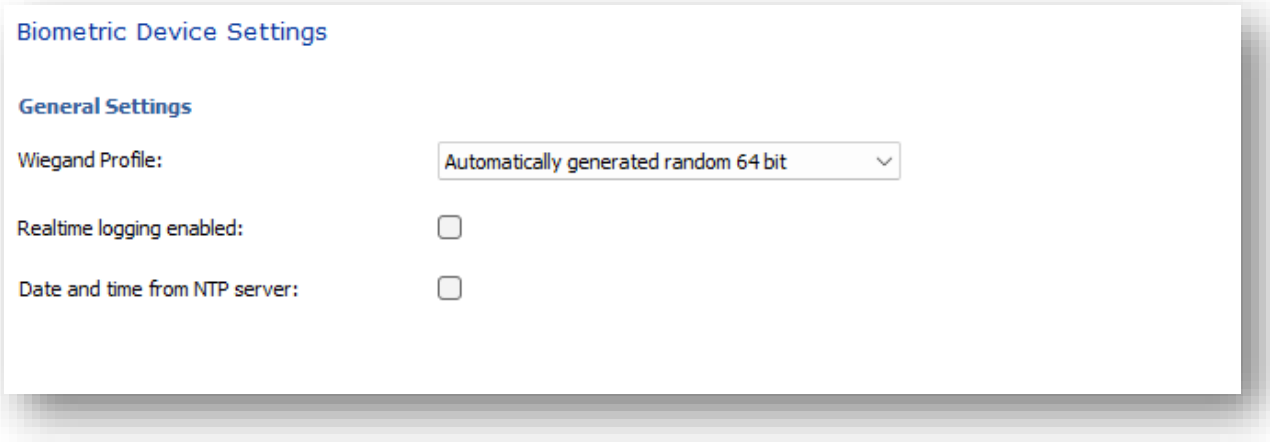
Morpho Access Heartbeat Interval: The interval to ping MorphoAccess terminals. If the terminal does not respond to the ping, the device status will be updated to Offline.

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



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.

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.

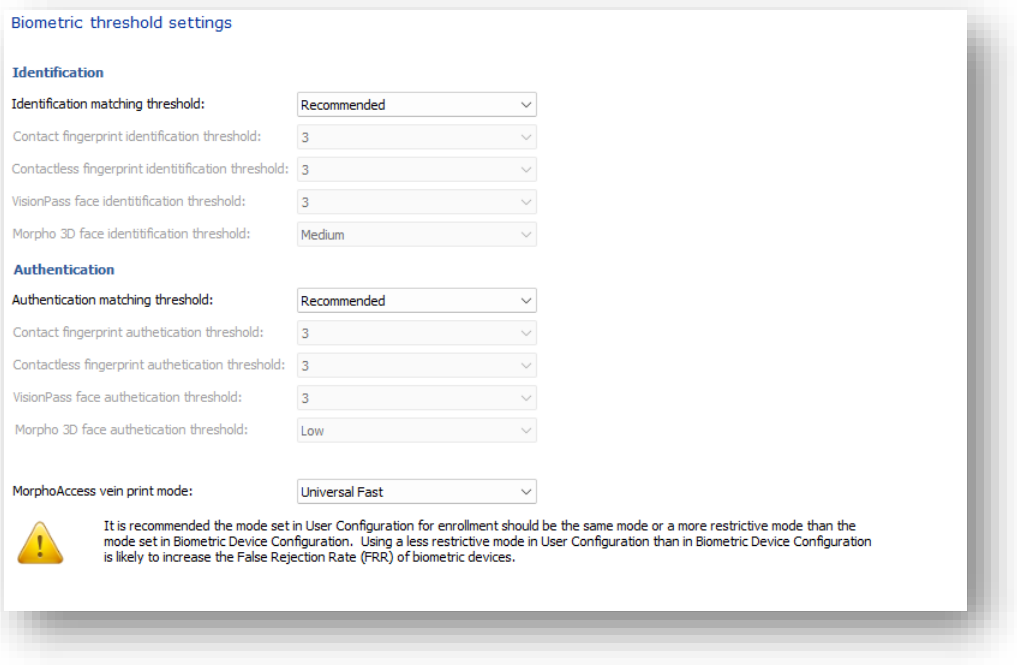
Date And Time From NTP Server: Enable this check box to set the biometric device to receive date and time from NTP (Primary or secondary NTP Server address). SetDateTime will not be possible from MorphoManager after enabling this configuration.

A manual execution of the SetDateTime task is required after disabling NTP Configuration from the Biometric Device Configuration screen to update the device time.

The **NTP Configuration** checkbox is available in the **Express Biometric Device Configuration**. For **Advanced Biometric Device Configuration**, NTP configuration shall be performed using the **Advanced Settings** section.

Screen 3 – Biometric Threshold 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.

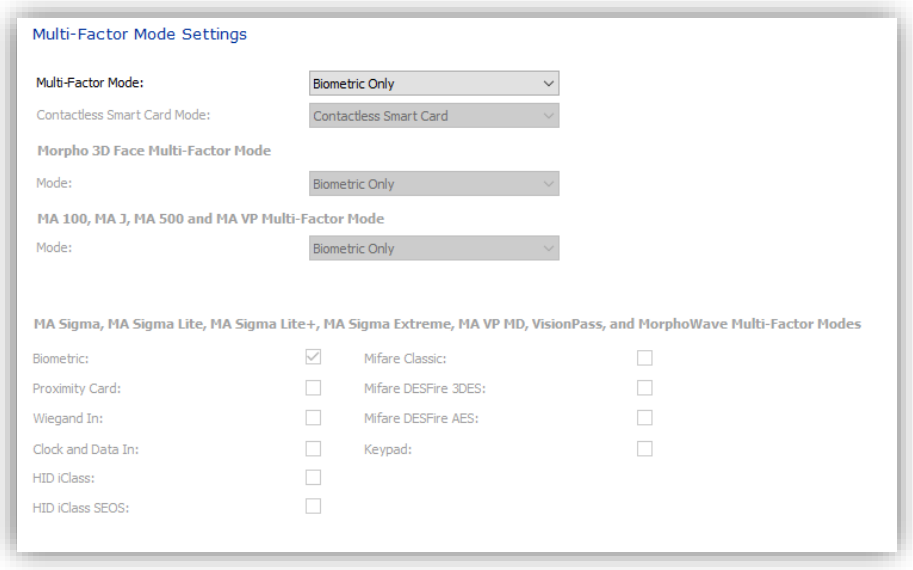


Biometric Threshold: The default is Recommended. However, it can be set to Low, High, Very High, and Custom. Choosing the Custom setting will allow you to set individual threshold properties for the four device types greyed out in the screenshot above. For further detail on the Vein/ Print mode options 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 4 - 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.

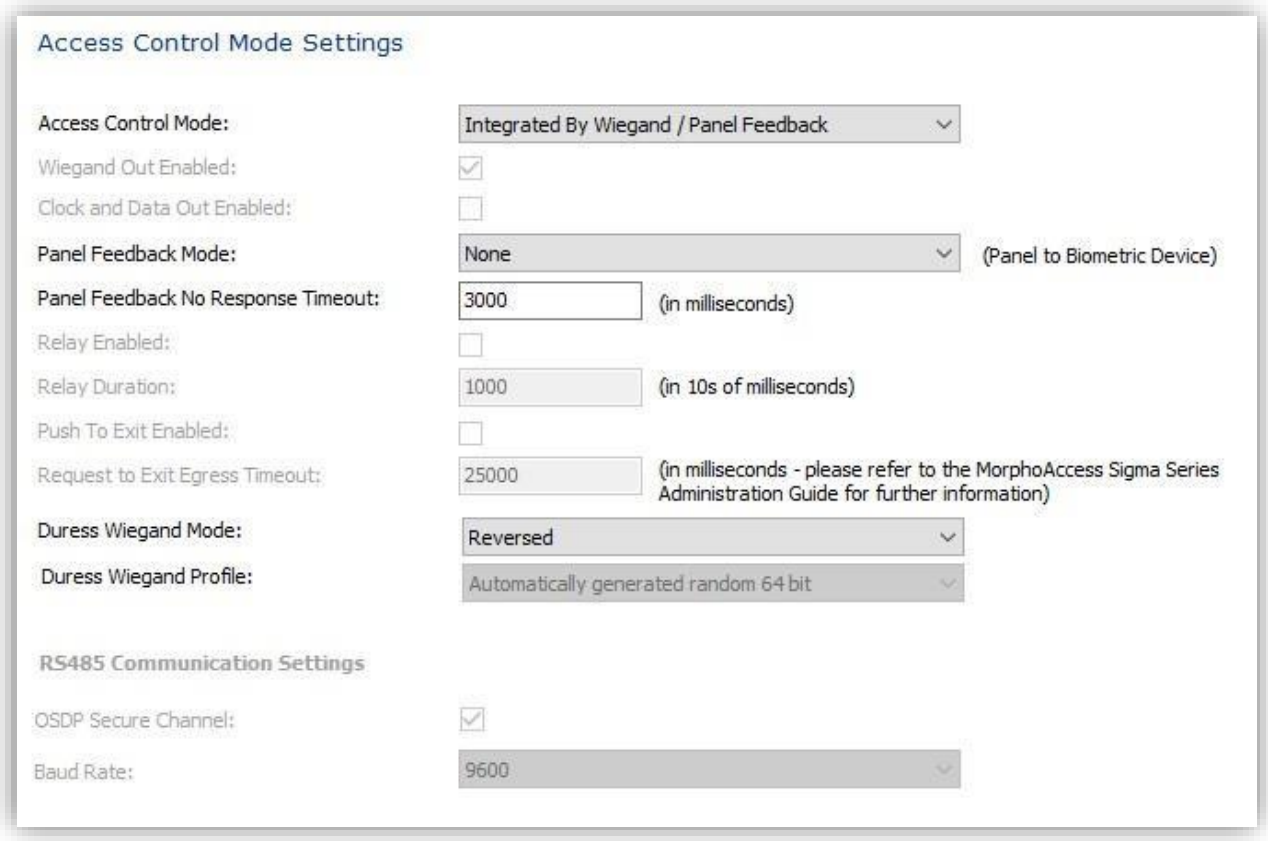
Multi-Factor Mode: There are ten individual options and the ability to do a custom selection for each hardware family. The options are as follows:

- **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 5 – Access Control Mode Settings



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 OSDP

- **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.

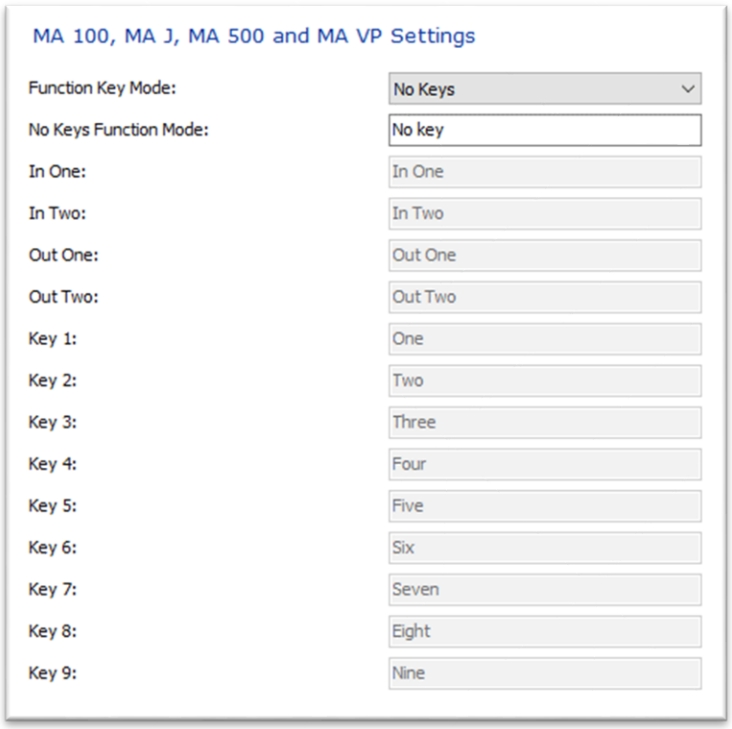
Push to Exit Duration: This sets the length of time the door will remain open if Push to Exit is enabled.

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.

Baud Rate: Allows you to set the baud rate for any RS485 communication.

Screen 6 – Function Key Mode for MA 100, J, 500, and VP Family



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

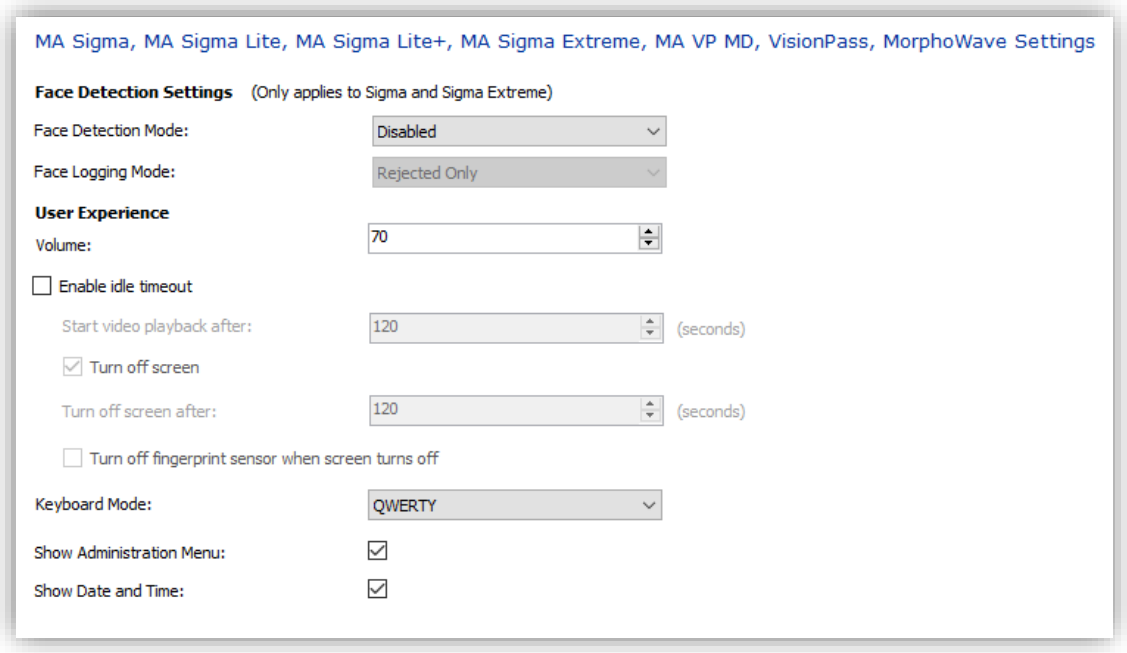
Screen 7 – MA 100, MA J, MA 500, and MA VP Settings

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 8 – MA Sigma, Sigma Lite, Sigma Lite +, Sigma Extreme, MA VP MD, VisionPass & 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.

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.

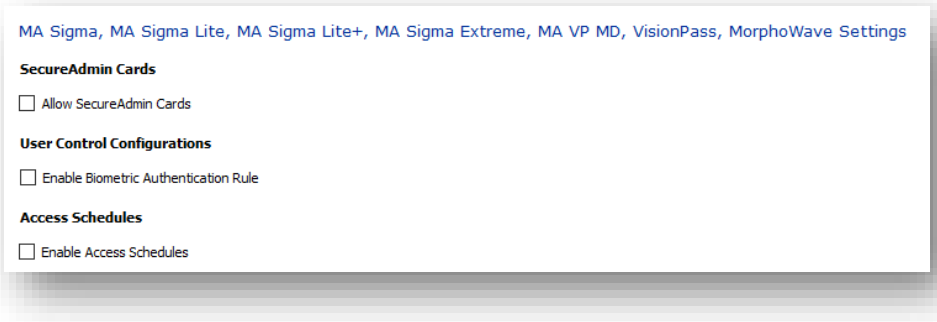
Keyboard Mode: Select whether a QWERTY or AZERTY keyboard will be utilized.

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.

The *Show Administration Menu & Show Date and Time* feature is applicable only on devices with an LCD display.

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



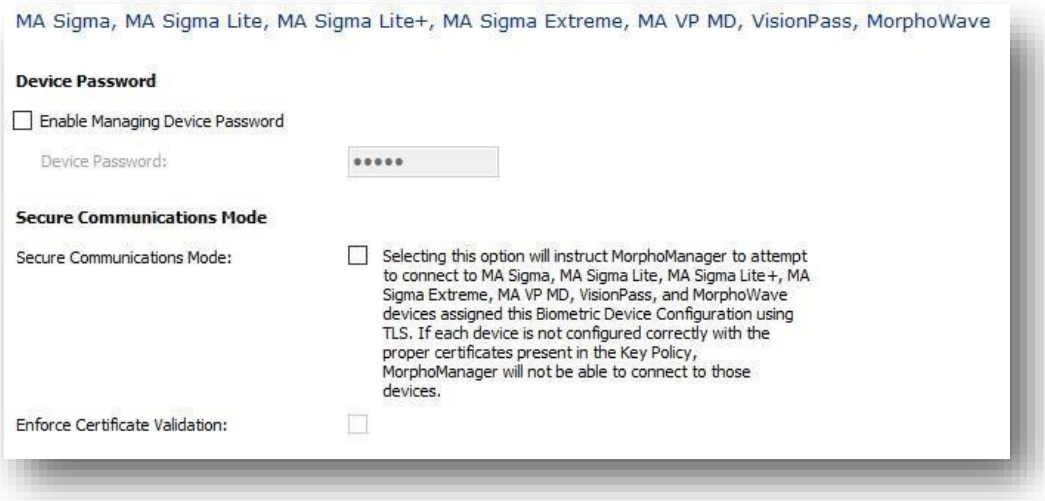
SecureAdmin Cards: When enabled, you will be able to use smart cards that have been encoded in Secure Admin or Secure Admin Lite. This setting only pertains to the Sigma family of devices. You will need to set the Secure Admin Site Keys in the Key Policy menu.

Enable Biometric Authentication Rule: Enables the ucc.finger_bio_auth.rule in Sigma family devices and ucc.biometric_auth_rule in MWC and VIP devices . When enabled, the user will be prompted to present a biometric as verification.

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

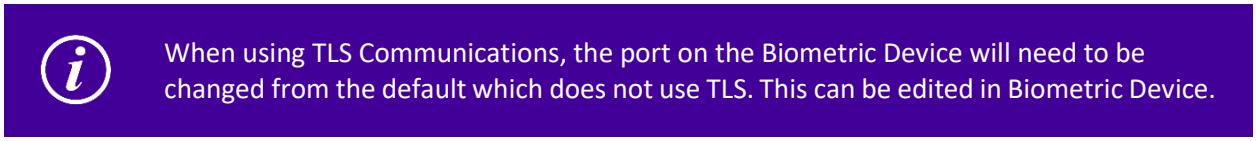
If this system is an upgrade from MorphoManager 9.6.4 or lower, you will need to manually rebuild all MA Sigma devices after enabling the Access Schedules option.

Screen 10 – 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.

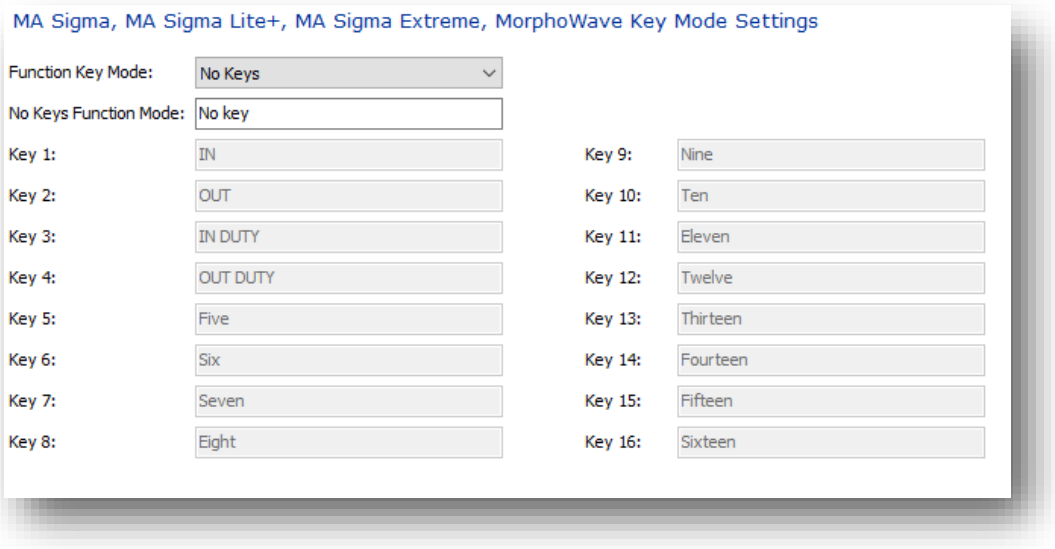
Secure Communications Mode: Turn this on to use TLS communications between the Biometric Device and the MorphoManager Server.



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.

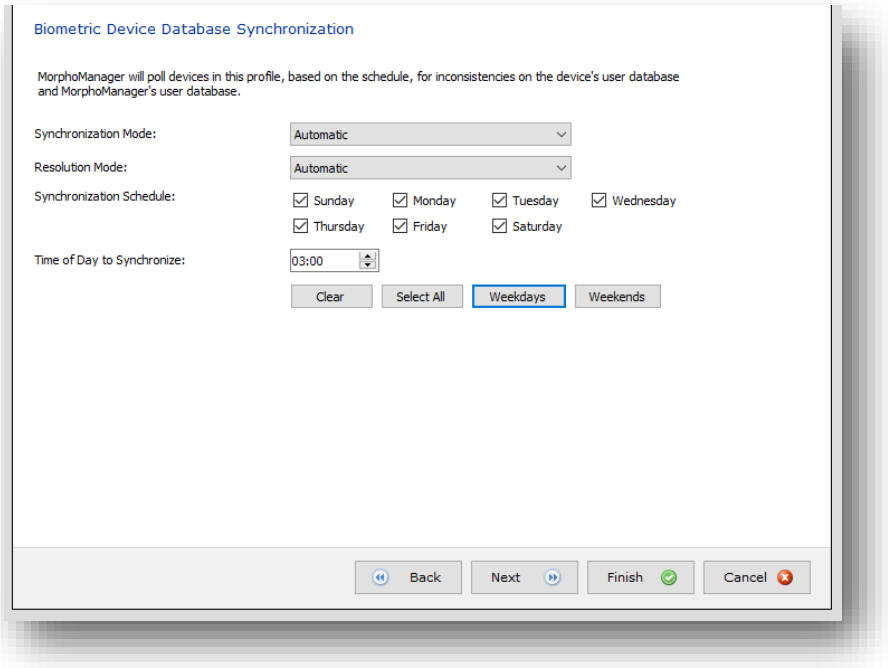
Screen 11 – Function Key Mode for MA Sigma, MA Sigma Lite+ and MorphoWave Key Mode Settings



Function Key Mode: This area determines what function keys, if any, will be available on a MA Sigma, MA Sigma Lite ,MA Sigma Lite +, MA Sigma Extreme, VisionPass 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 12 – 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.

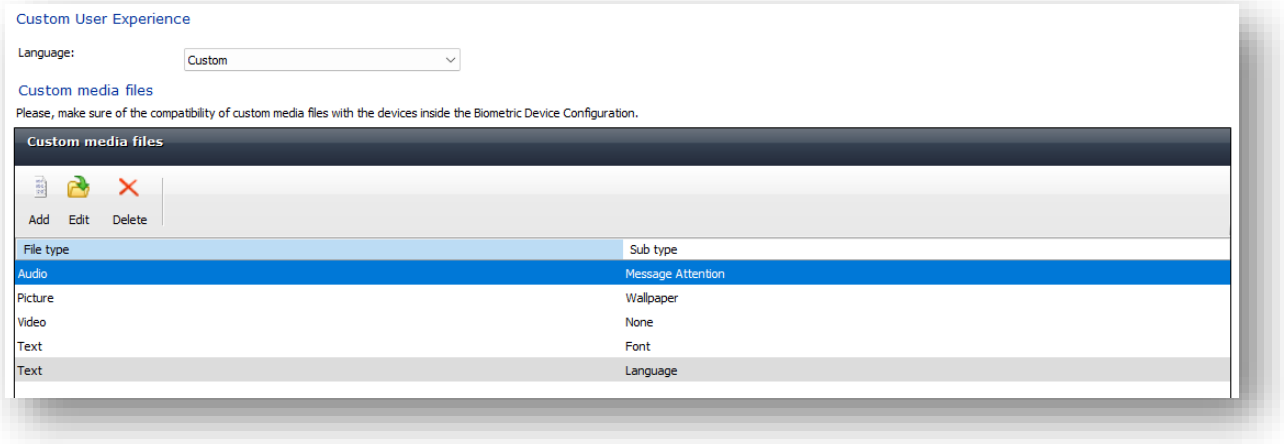
Manual – Operator review, and interaction is required to resolve any inconsistencies found during synchronization.

Automatic – This is the default resolution mode. Any inconsistencies found will be resolved automatically. No operator interaction is required.

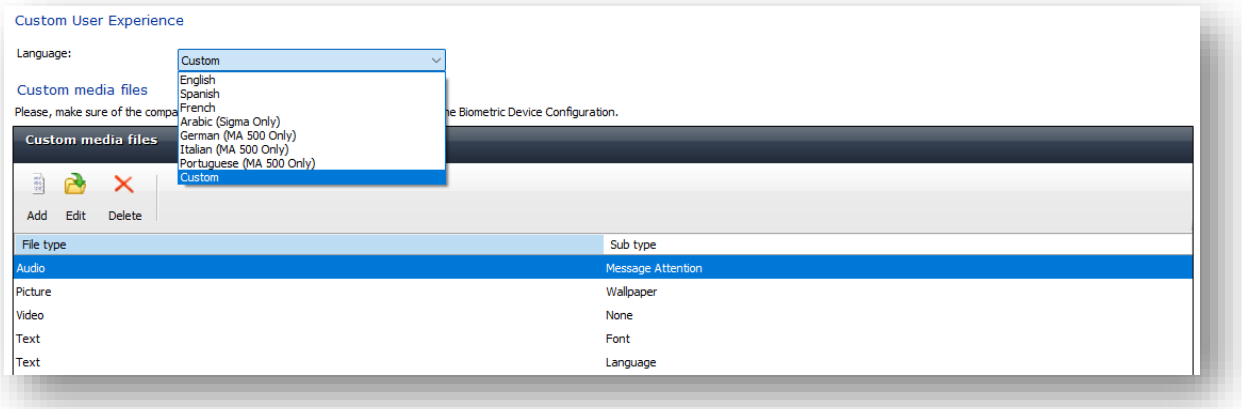
Synchronization schedule: This schedule applies to the Automatic Synchronization Mode. It used to determine the days on which the synchronization task should run.

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

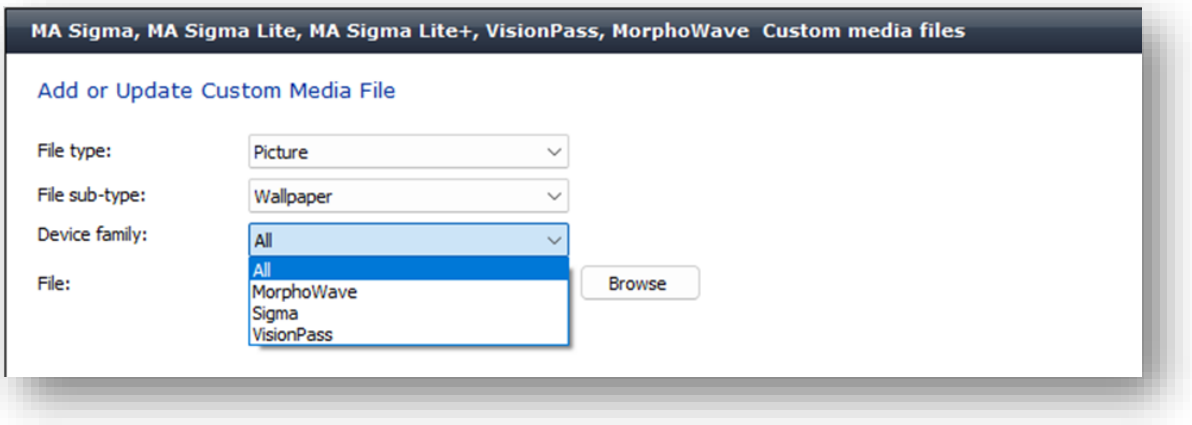
Screen 13 – MA Sigma, MA Sigma Lite+, MA Sigma Extreme, VisionPass and MorphoWave Custom Media Files



This wizard screen allows the addition of custom Video, Picture, Audio and Text files to be used on biometric devices as Custom Media Files. Applying the Biometric Device Configuration containing these files to the Biometric Device will place the files onto that device.



Language from '*Custom User Experience'* will be used to select type of language you wish to use on your Biometric Device display screen. By selecting *'Custom'* value, default messages on biometric device will be customized with selected language (not supported by default by the terminal) from '*Custom media files'*.



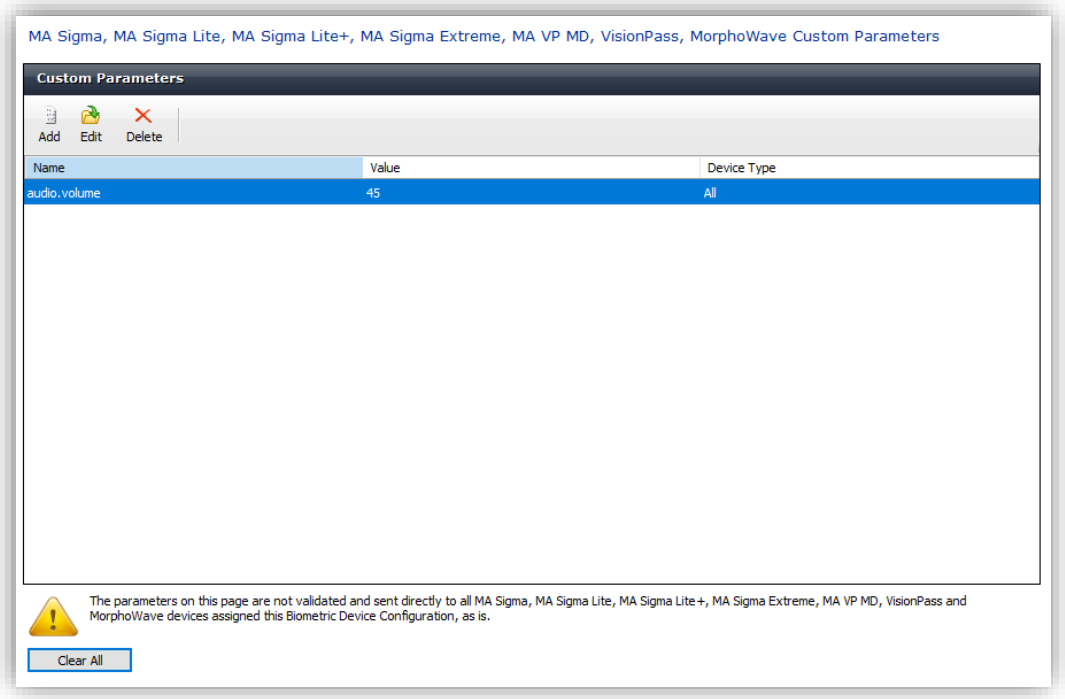
Different wallpapers can be used to upload on different devices according to the s '*Device family*'.

Please, make sure of the compatibility of custom media files with the devices inside the Biometric Device Configuration according to the below matrix.

			SIGMA				MorphoWave			VisionPass	
File type	File sub-type	Device family	Lite	Lite+	Wide	Extreme	SP	XP	XP2		SP
Audio	Message attention	-	N	N	Y	Y	N	Y	Y	Y	N
	Tamper	-	N	N	Y	Y	N	Y	Y	Y	N
	Test	-	N	N	Y	Y	N	Y	Y	Y	N
	Verification failed	-	N	N	Y	Y	N	Y	Y	Y	N
	Verification succeeded	-	N	N	Y	Y	N	Y	Y	Y	N
Picture	Wallpaper	All	N	Y	Y	Y	N	Y	Y	Y	Y
		SIGMA	N	Y	Y	Y	N	N	N	N	N
		MorphoWave	N	N	N	N	N	Y	Y	N	N
		VisionPass	N	N	N	N	N	N	N	Y	Y
	Biometric animation	-	N	N	Y	Y	N	Y	Y	N	N
	Bio QR animation	-	N	N	N	N	N	Y	Y	N	N
	Card animation	-	N	N	Y	Y	N	Y	Y	N	N
	Card bio animation	-	N	N	Y	Y	N	Y	Y	N	N
	Card bio QR animation	-	N	N	N	N	N	Y	Y	N	N
	Card QR animation	-	N	N	N	N	N	Y	Y	N	N
	QR code animation	-	N	N	N	N	N	Y	Y	N	N
Video	-	-	N	N	Y	Y	N	Y	N	Y	N
Text	Font	-	N	N	Y	Y	N	Y	Y	Y	Y
	Language	-	N	N	Y	Y	N	Y	Y	Y	Y

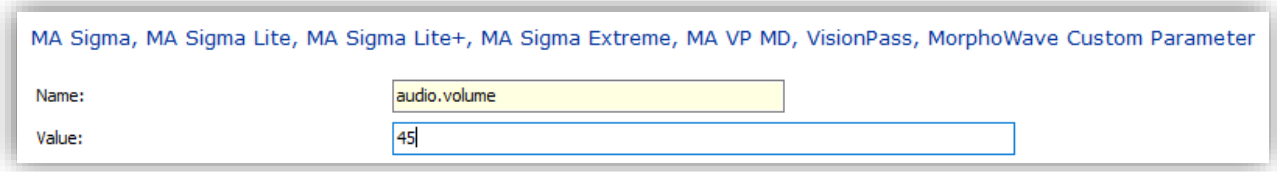
Compatibility matrix between Custom Media File and Biometric Device

Screen 14 – 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.

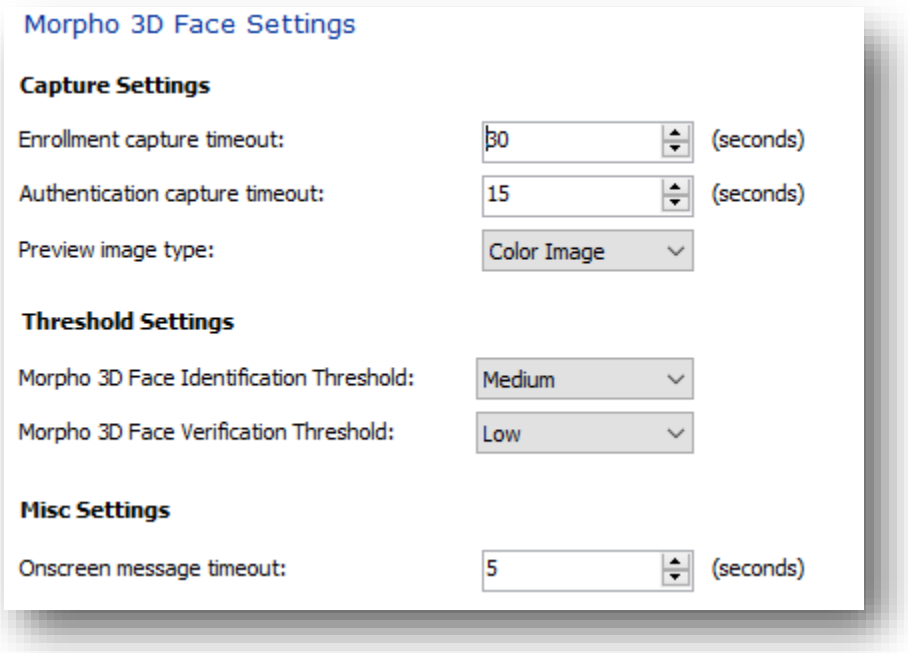
To enter a custom parameter, click the Add button then provide the parameter name and its value and click Next.



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

NTP configuration cannot be performed via custom parameters. Attempting to do so will result in a failed task related to the SetDateTime operation.

Screen 15 – Morpho 3D Face Settings



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

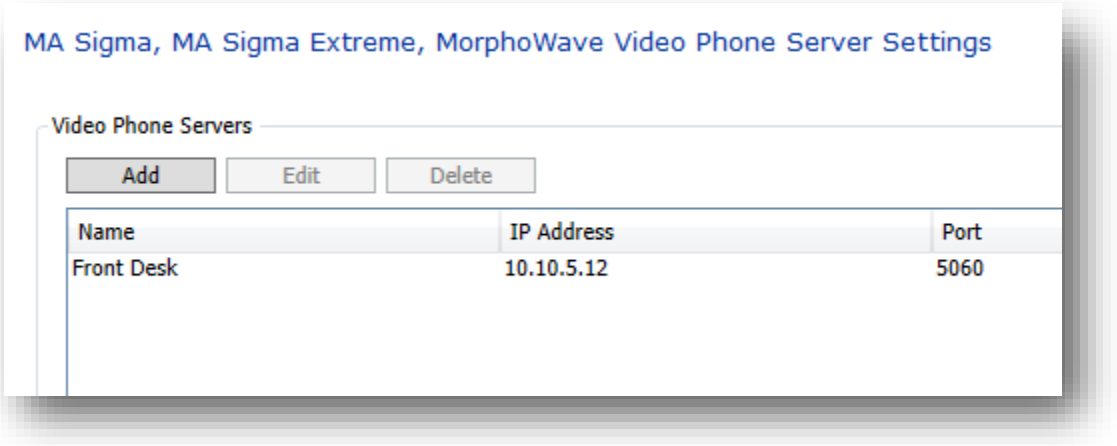
Authentication Capture Timeout: The maximum time the device will attempt to authenticate/verify a user in verification mode.

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

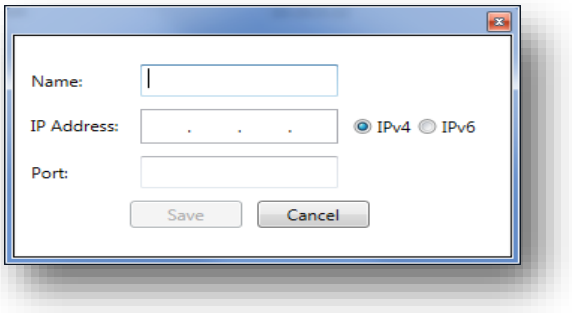
Onscreen Message Timeout: The amount of time that on-screen messages will be shown to the user.

Screen 16 – 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.



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



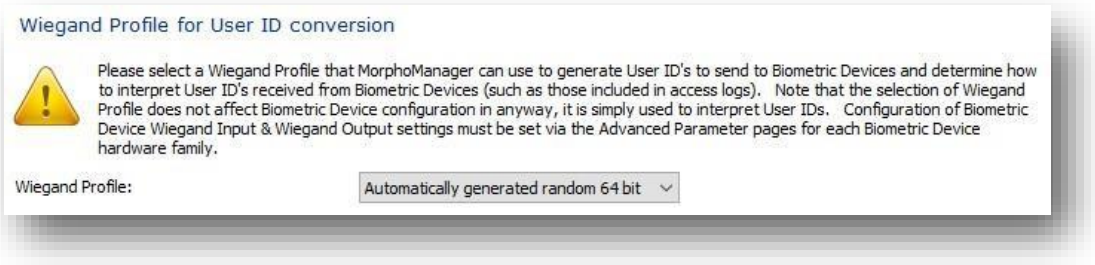
Click **Save** when finished.

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.

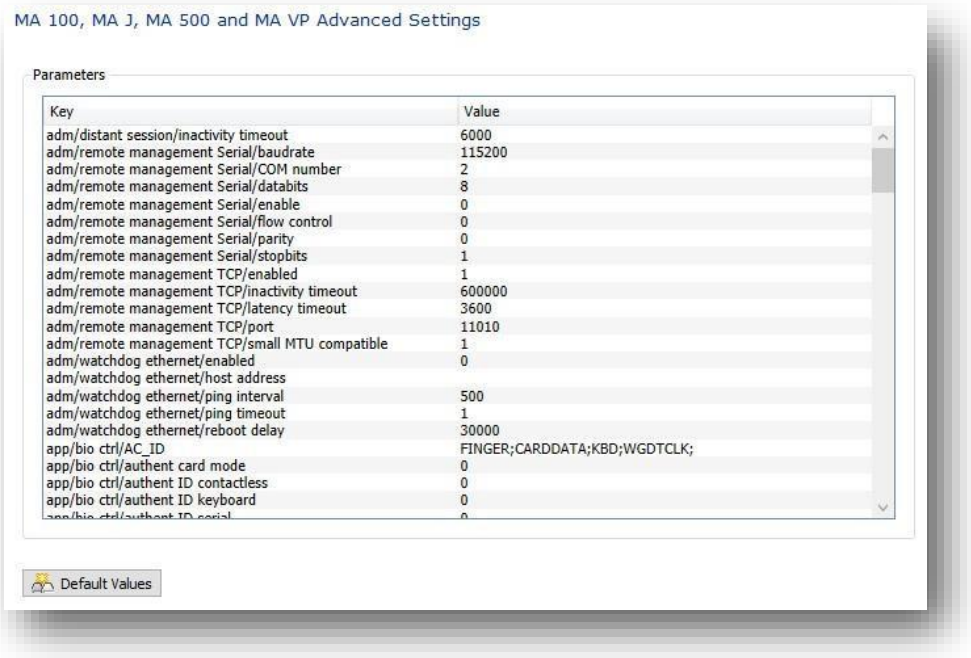
The Advanced Profile Screen 2 allows you to configure the various parameters for the Morpho Access 100, 500, J, and VP.

Screen 2- Wiegand Profile for User ID Conversion



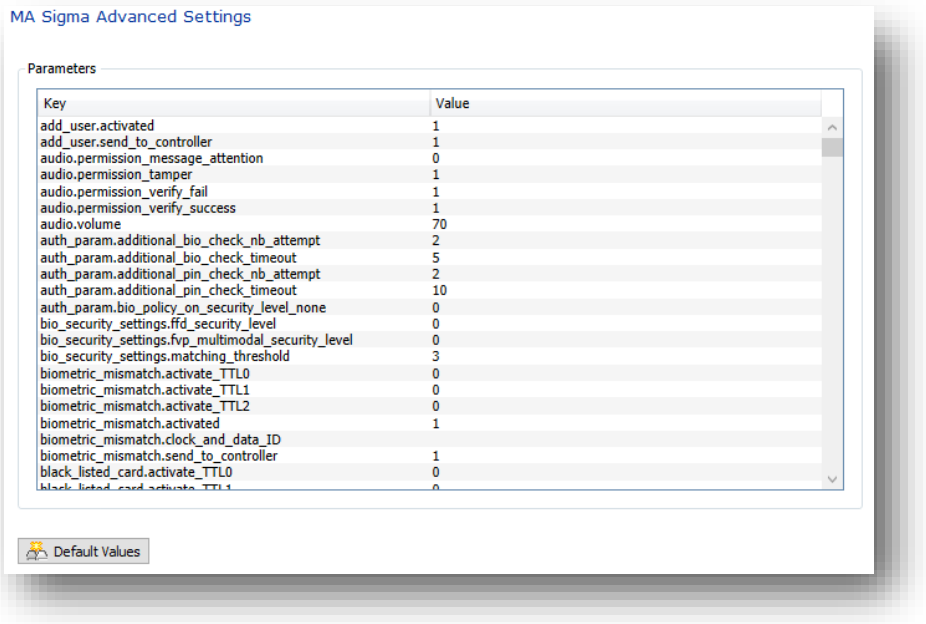
Select the Wiegand Profile to be utilized on the Biometric Device.

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



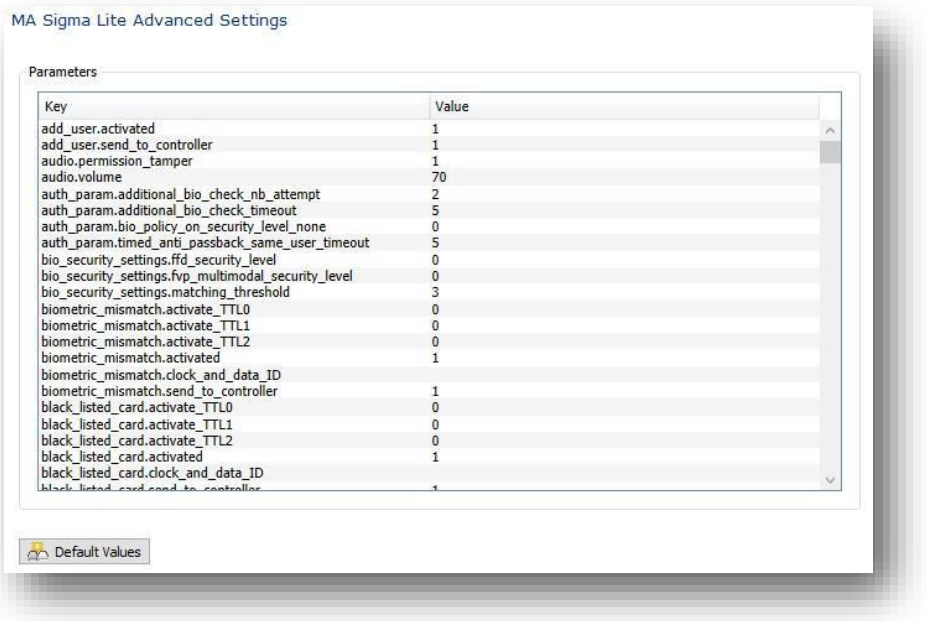
Parameters available for MA2G devices. If you have made changes to the parameters and wish to return to the original defaults on this screen, you can simply click the **Default Values** button.

Screen 4 – MA Sigma Advanced Settings



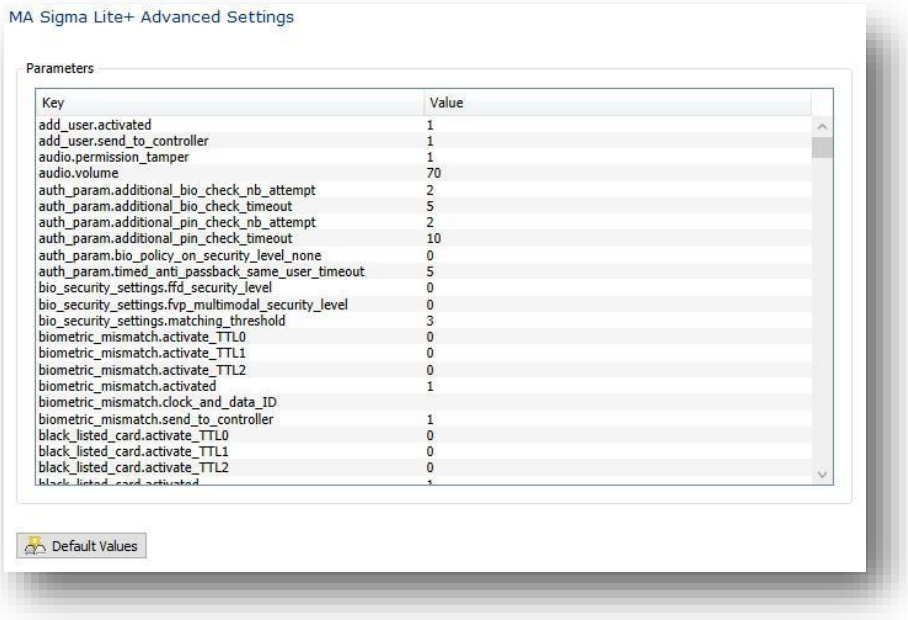
Parameters available for MA Sigma devices. If you have made changes to the parameters and wish to return to the original defaults on this screen, you can simply click the **Default Values** button.

Screen 5 –MA Sigma Lite Advanced Settings



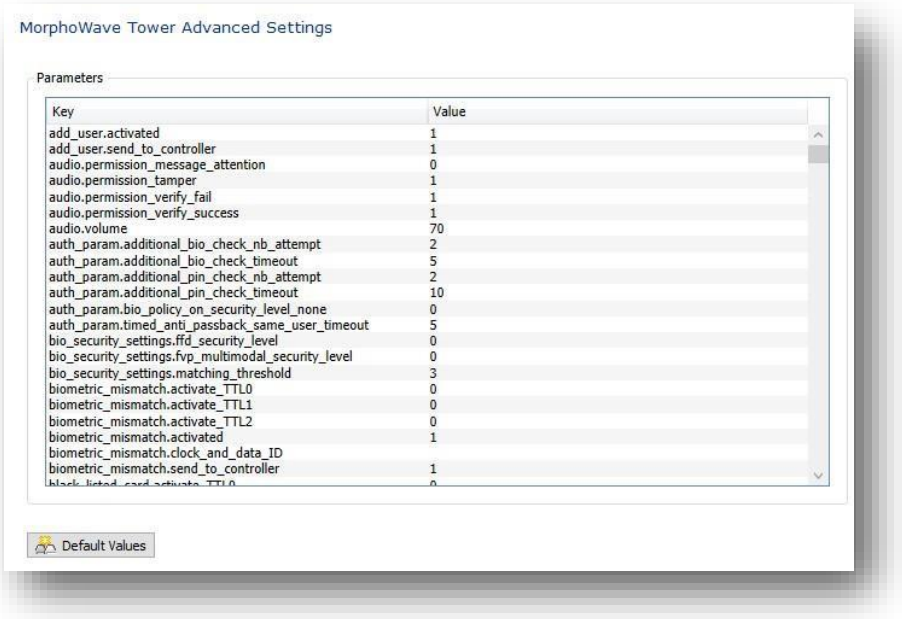
Parameters available for MA Sigma Lite devices. If you have made changes to the parameters and wish to return to the original defaults on this screen, you can simply click the **Default Values** button.

Screen 6 –MA Sigma Lite+ Advanced Settings



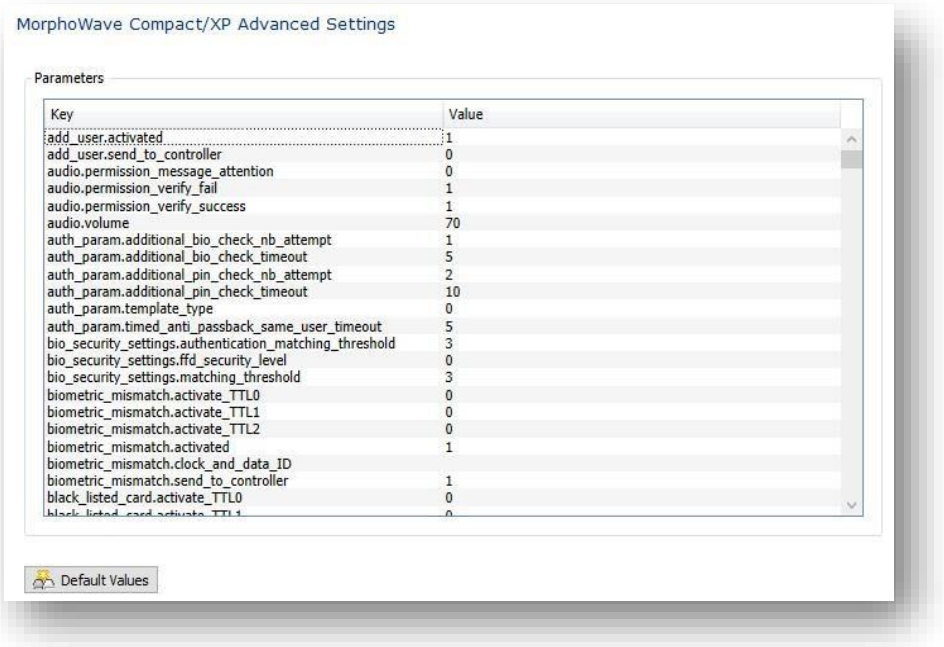
Parameters available for MA Sigma Lite+ devices. If you have made changes to the parameters and wish to return to the original defaults on this screen, you can simply click the **Default Values** button.

Screen 7 – MorphoWave Tower Advanced Settings



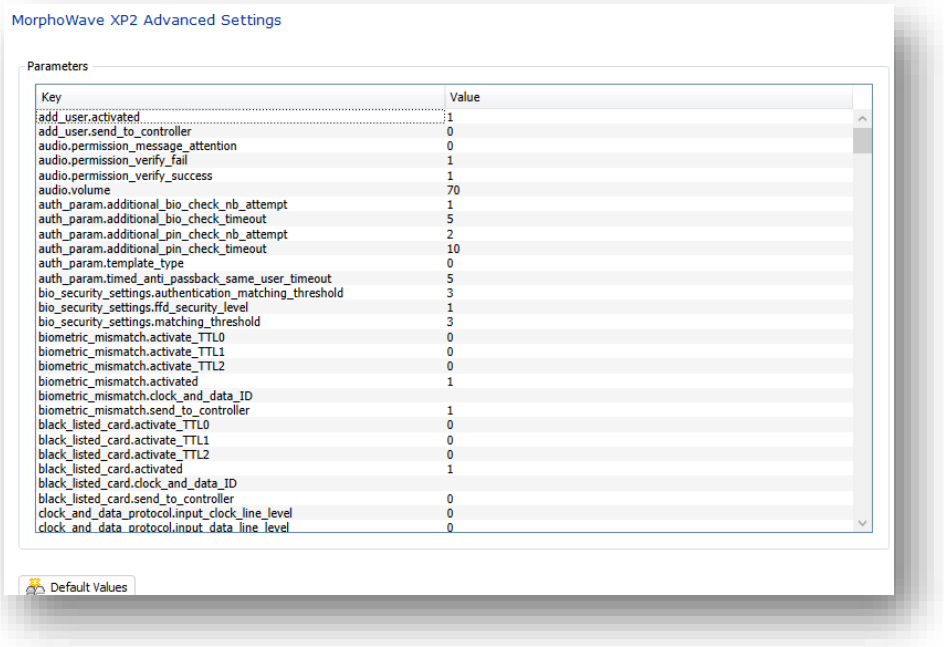
Parameters available for MorphoWave Tower. If you have made changes to the parameters and wish to return to the original defaults on this screen, you can simply click the **Default Values** button.

Screen 8 – MorphoWave Compact / XP Advanced Settings



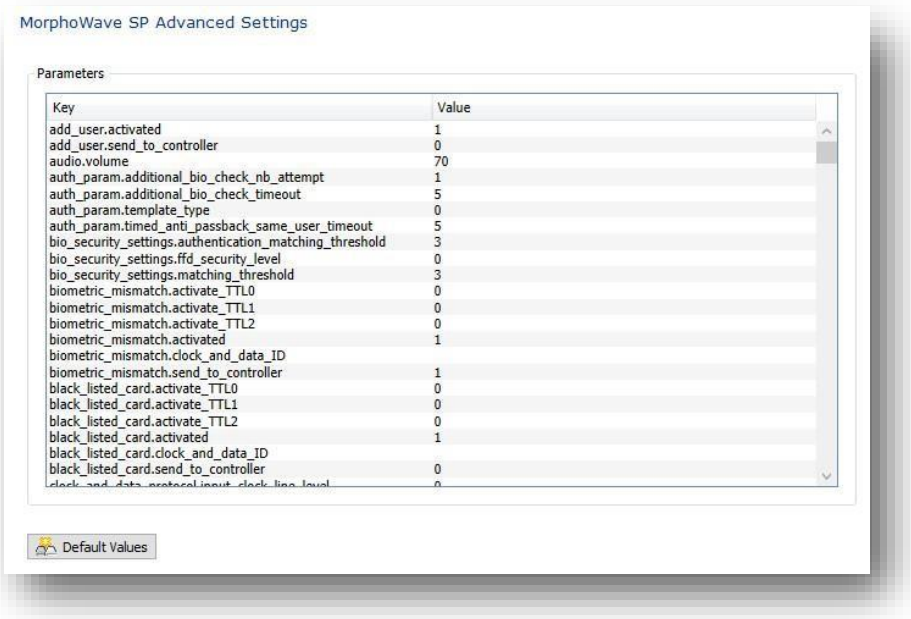
Parameters available for MorphoWave Compact / XP. If you have made changes to the parameters and wish to return to the original defaults on this screen, you can simply click the **Default Values** button.

Screen 9 – MorphoWave Compact / XP 2 Advanced Settings



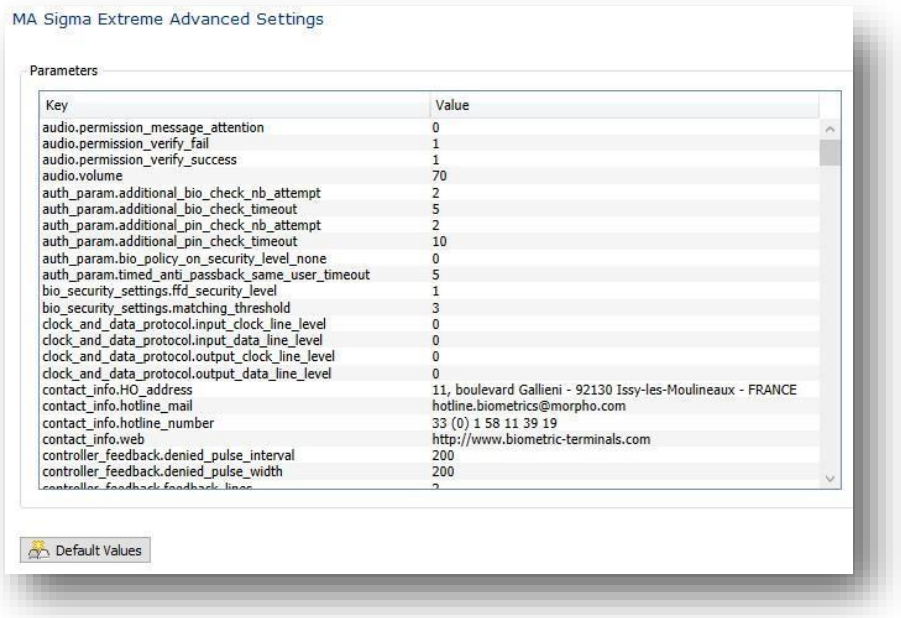
Parameters available for MorphoWave Compact / XP 2. If you have made changes to the parameters and wish to return to the original defaults on this screen, you can simply click the **Default Values** button.

Screen 10 – MorphoWave SP Advanced Settings



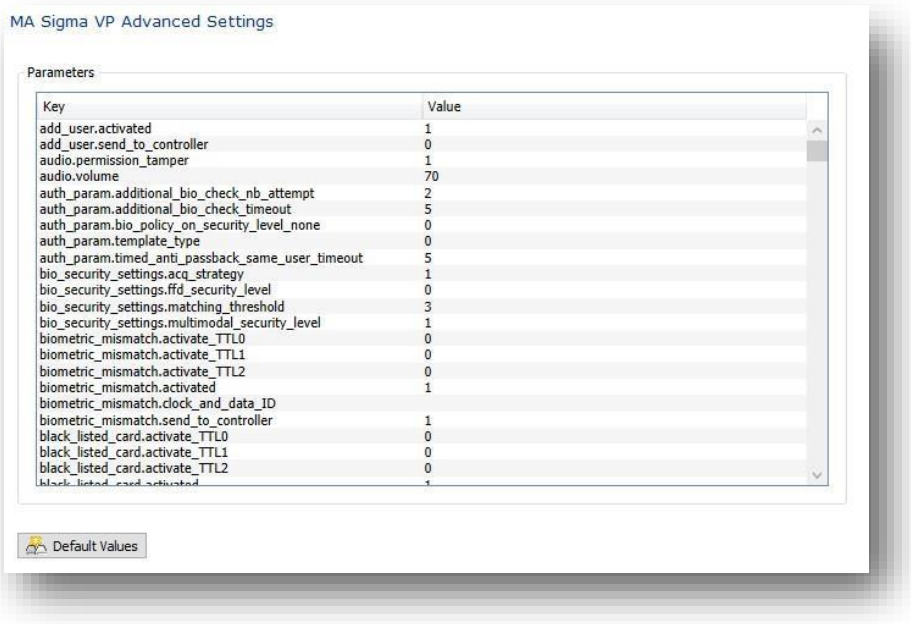
Parameters available for MorphoWave SP. If you have made changes to the parameters and wish to return to the original defaults on this screen, you can simply click the **Default Values** button.

Screen 11 – MA Sigma Extreme Advanced Settings



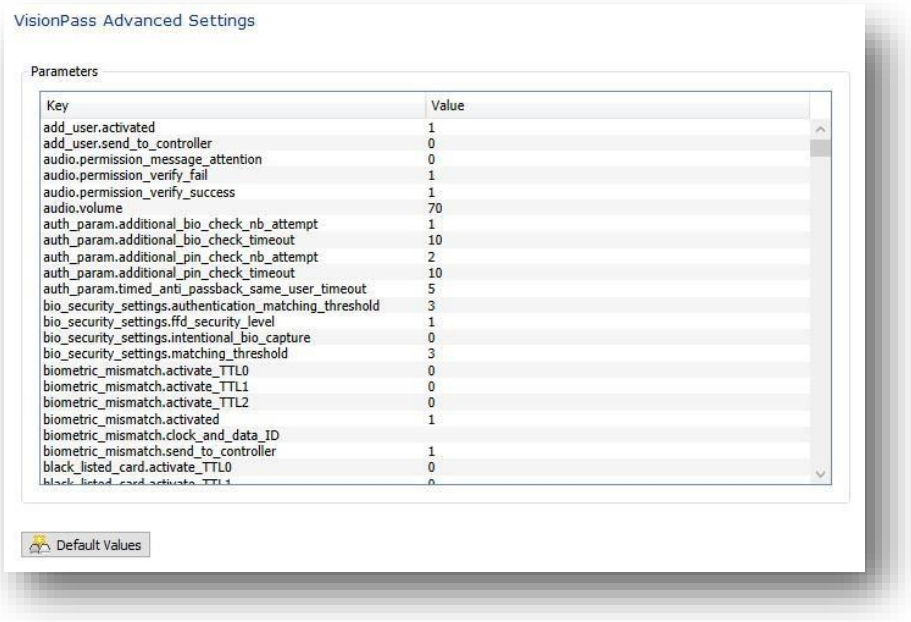
Parameters available for MA Sigma Extreme. If you have made changes to the parameters and wish to return to the original defaults on this screen, you can simply click the **Default Values** button.

Screen 12 – MA VP MD Advanced Settings



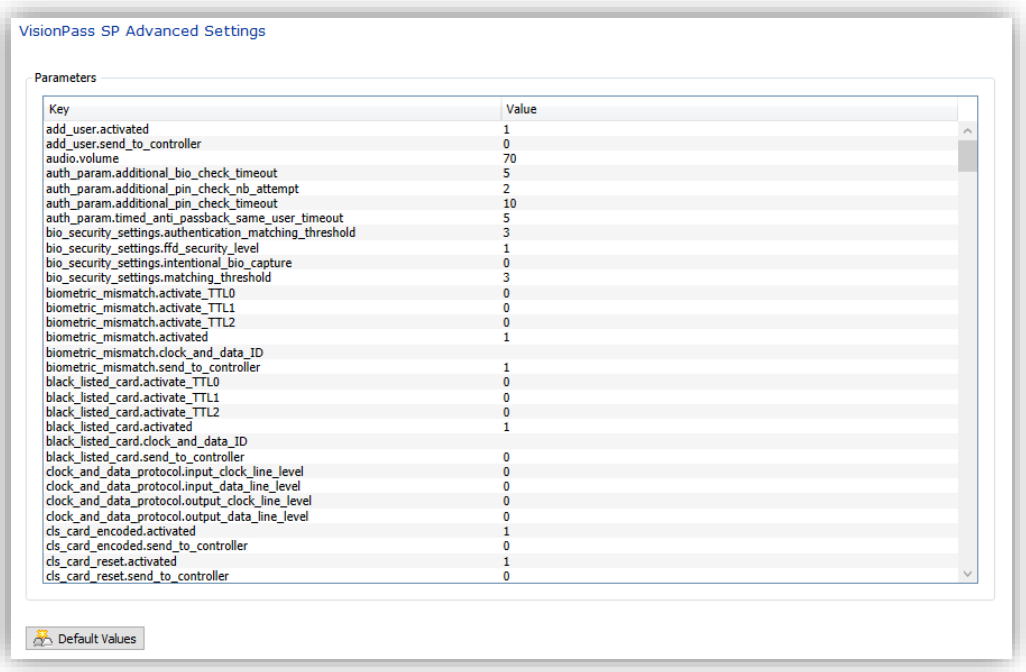
Parameters available for MA VP MD. If you have made changes to the parameters and wish to return to the original defaults on this screen, you can simply click the **Default Values** button.

Screen 13 – VisionPass Advanced Settings



Parameters available for VisionPass. 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.

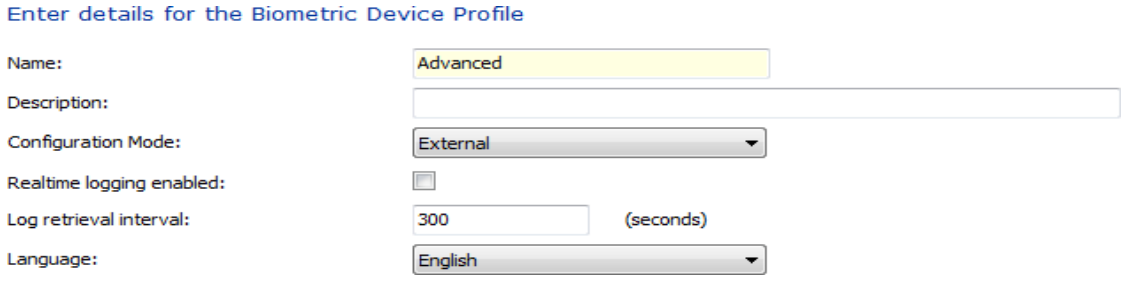
Screen 14 – VisionPass SP Advanced Settings



Parameters available for VisionPass SP. 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 13 – 19 can be found in the section for **Creating a new Biometric Device Configuration (Express).**

Creating a new Biometric Device Configuration (External)



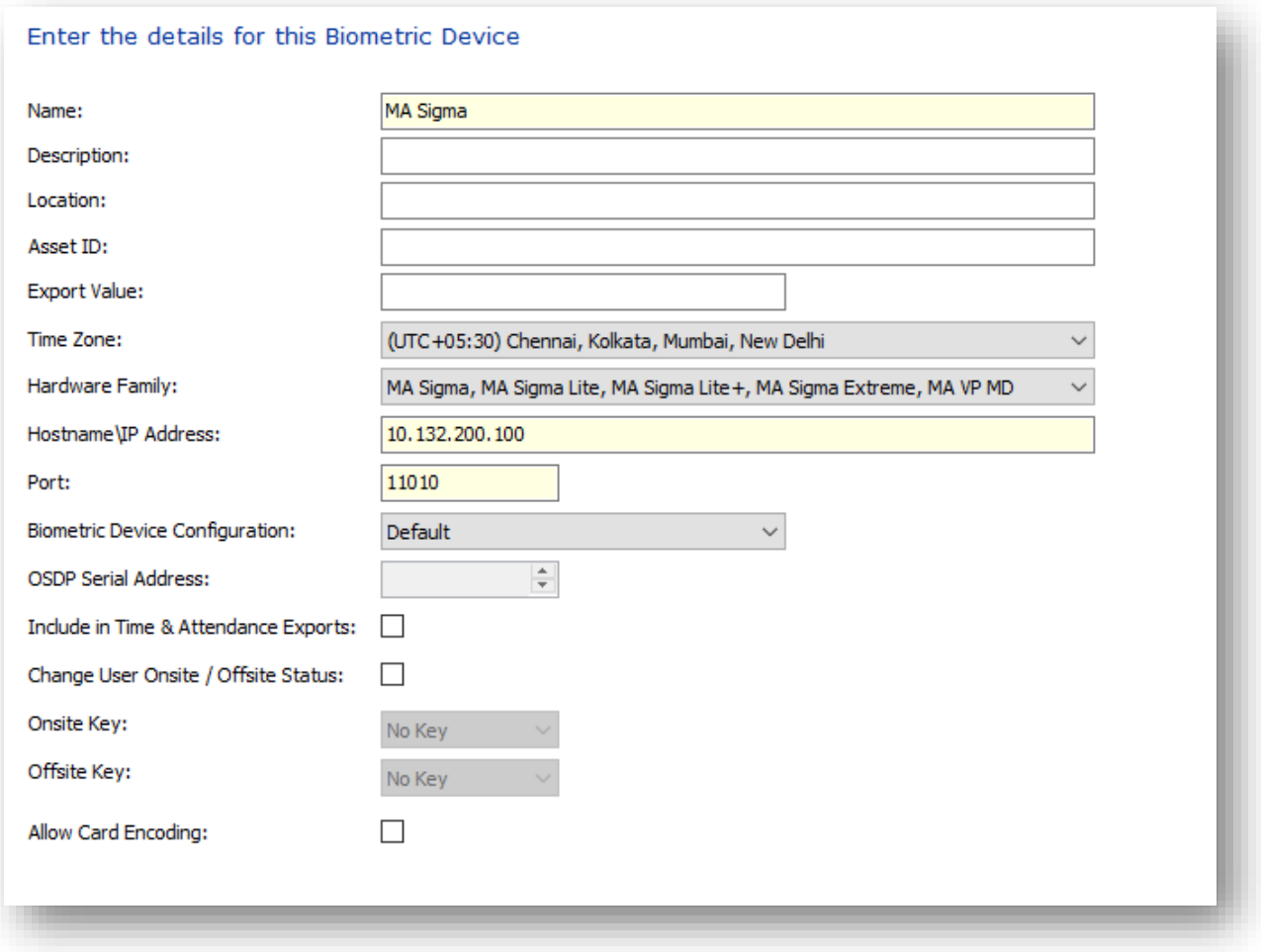
Selecting External for your Configuration Mode allows you to set all parameters on device or via external software that interfaces with the Biometric Device parameters. When selecting External mode this will be the only wizard screen you will utilize.

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 / XP, MorphoWave SP and the VisionPass and VisionPass SP

Create a Biometric Device

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



Name: The name of the Biometric Device.

Description: A description of the Biometric Device.

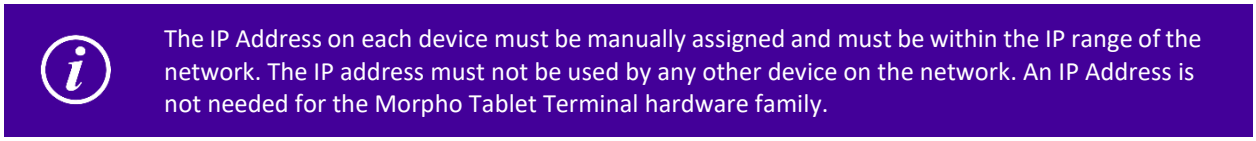
Location: The installed location of the Biometric Device.

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

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

Hardware Family: Corresponds to the model of the Biometric. As mentioned above Biometric Devices from three different hardware families can be added here; the MA 100, MA J, MA 500, and MA VP family, the MA Sigma, Sigma Lite, MA Sigma Lite + ,MA Sigma Extreme, and MA VP MD family, the Morpho 3D Face, the MorphoWave Tower and MorphoWave Compact / XP, MorphoWave SP and the VisionPass and VisionPass SP.

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



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.

OSDP Serial Address: Enabled if the selected Biometric Device Configuration is set to communicate via OSDP. This field is applicable only for the MA Sigma, Sigma Lite, MA Sigma Lite +, MA Sigma Extreme, and MA VP MD family and MorphoWave Compact / XP, MorphoWave SP and the VisionPass.

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.
Allow Card Encoding:	Cryptographic keys to encode Mifare or DESFire cards will not be sent to the device unless this option is selected.

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, click on **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 related to this device. 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

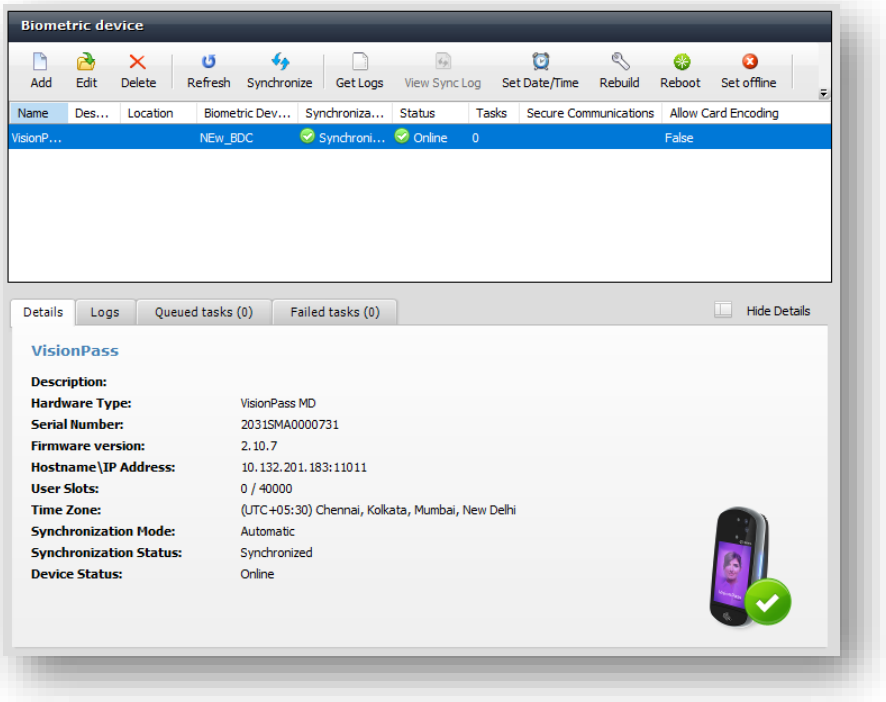
When viewing a list of Biometric Devices, the status column indicates the status of each Biometric Device. Online means the Biometric Device is responding to communication requests. Offline means that the Biometric Device is not responding to communication requests. A new status, Never Connected, has 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.

Allow Card Encoding

The value “True” indicates that added device can be used as encoder by sending cryptographic keys to encode Mifare or DESFire cards.
The value “False” indicate that added device cannot be used as encoder.

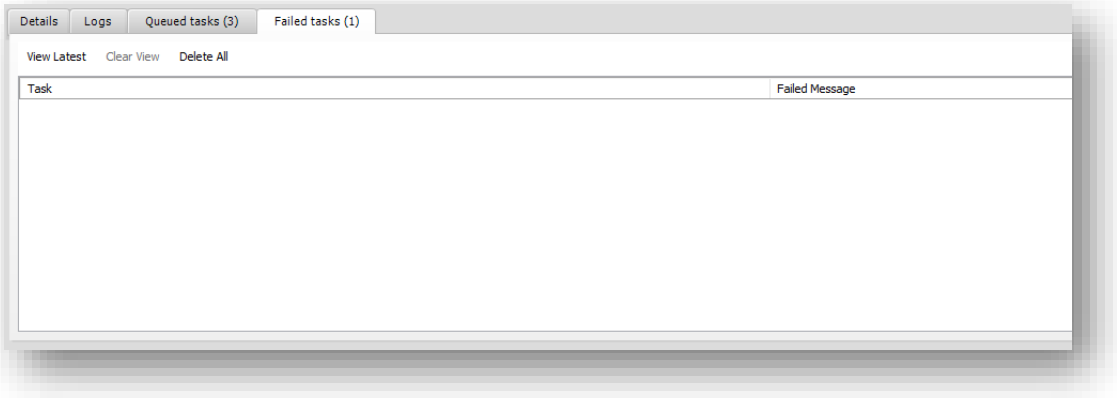
This option is introduced in version 16.3. When upgrading from a previous version, MorphoManager will automatically delete the keys from all connected devices during the upgrade; to restore the encoding capability for these devices, this option shall be used.



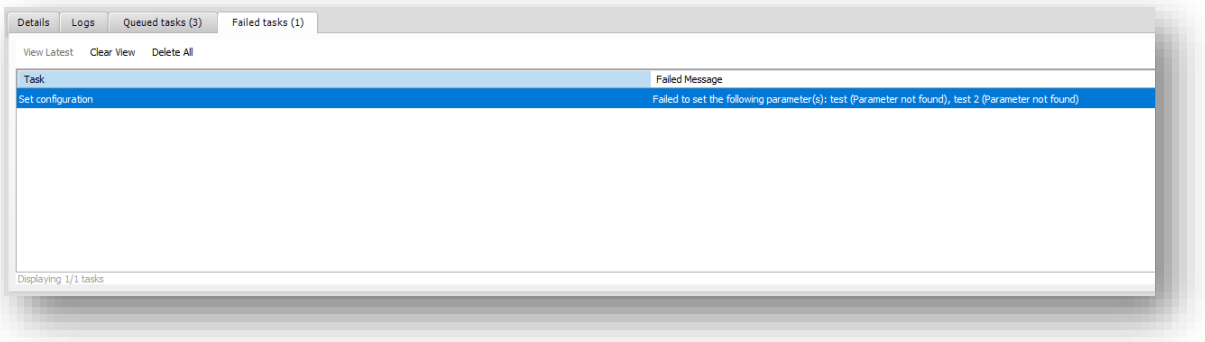
The icon displayed on the administration page of Biometric Devices can have various meanings, as explained in the below table :

Device Status	Icon	Meaning
Online		Device accessible by MorphoManager application and no further action required from the operator.
Online Pending		MorphoManager trying to connect to the biometric device to verify its accessibility.
OnlineWithError		Device accessible by MorphoManager application but an error was encountered during a task execution that could affect the device behavior.
Offline		Device not accessible by MorphoManager application therefore, an appropriate action required by the operator (network issue, device down, etc.).
ManuallyOffline		The operator either requested to stop the interactions between MorphoManager application and the device or the device is used by MorphoManager application for another purpose (like enrollment, encoding...)
SecurityIssue		Device accessible by Morpho Manager application but the security of the communication is not correctly set. Therefore an action is required from the operator.
Unsupported		The firmware detected during connection with device is not compatible with the current version of Morpho Manager application (the condition on minimal version is not met).
NeverConnected		Morpho Manager application has never been able / never tried to connect to this device.

Troubleshooting and Maintenance



- View Latest : Fetch and display up up to 500 failed tasks from database for selected device.
- Clear View : Remove fetched failed tasks from display.
- Delete All : Remove all failed tasks from display and database. It will not be possible to retrieve them afterwards.



In the example screen above, the “Set Configuration” task failed. The message in front 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

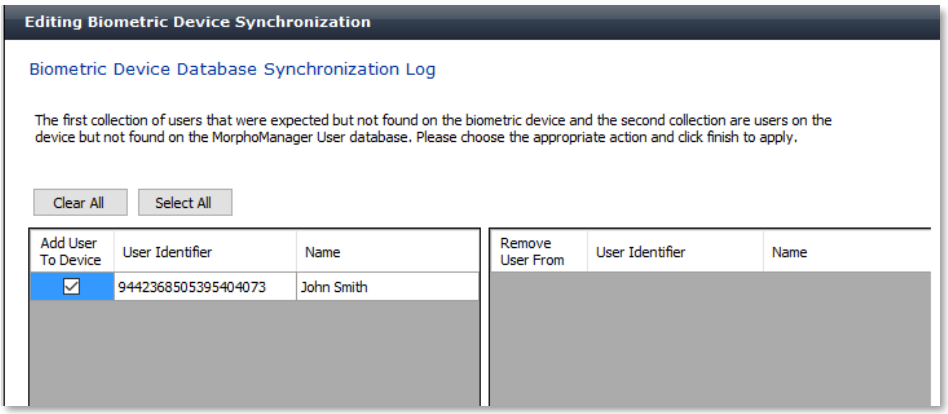
This functionality is enabled by default and allows currently stored transaction logs from the biometric device to be downloaded into MorphoManager. Automatic retrieval occurs every 5 minutes, by default.

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 on server start or once a day (or after every 24 hour) in case if server not started.

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

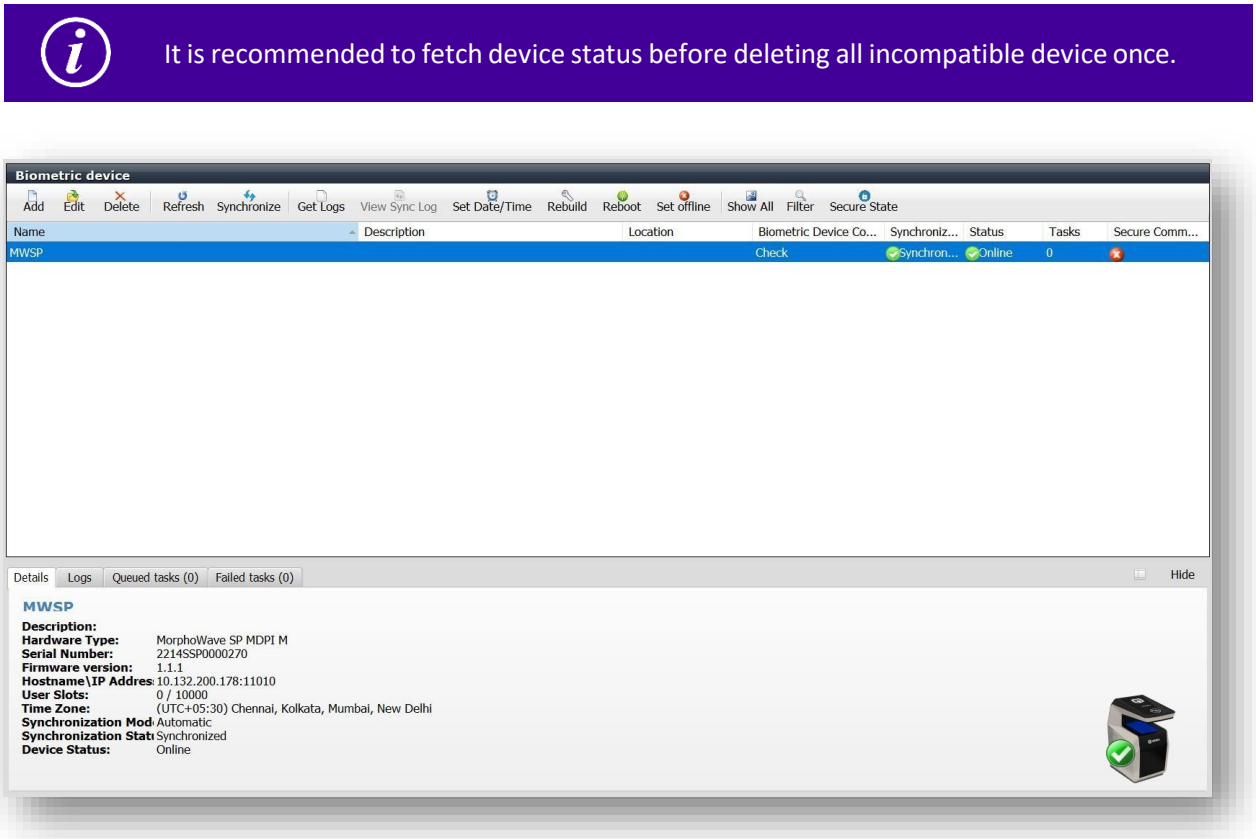
normal operation, any users who are added or deleted through user management are updated on the Biometric Device in real time.

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”.

Secure State

MorphoManager fetch and displays the secure state status of every connected Biometric Device. The secure state status of the Biometric Device will not be updated in case if any of the task is ongoing on MorphoManager side. So it is recommended to fetch the status of device when there is no pending task left in queue.

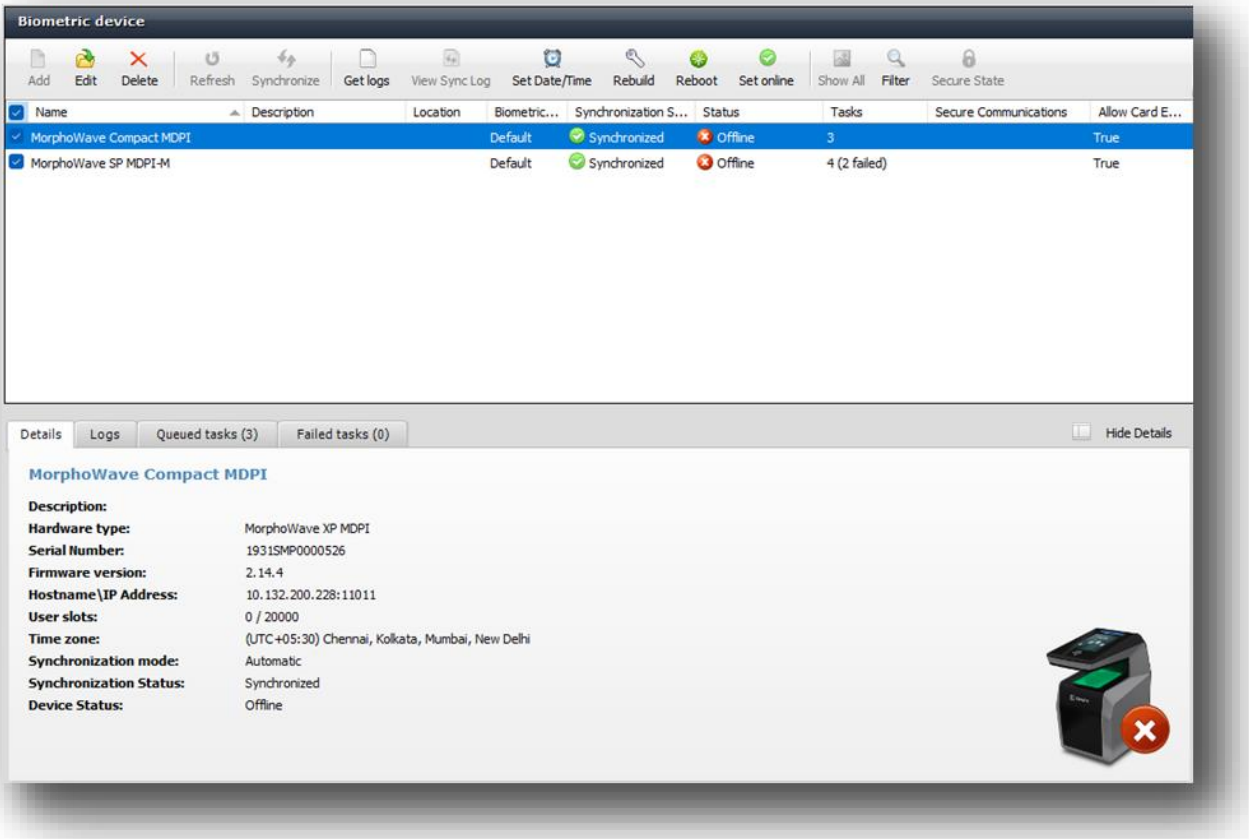


Actions for multiple Devices

Below is the list of operations that can be done simultaneously on multiple devices:

- Edit
- Delete
- Get Logs
- Set Date/Time
- Rebuild
- Reboot
- Set Online/Offline
- Filter

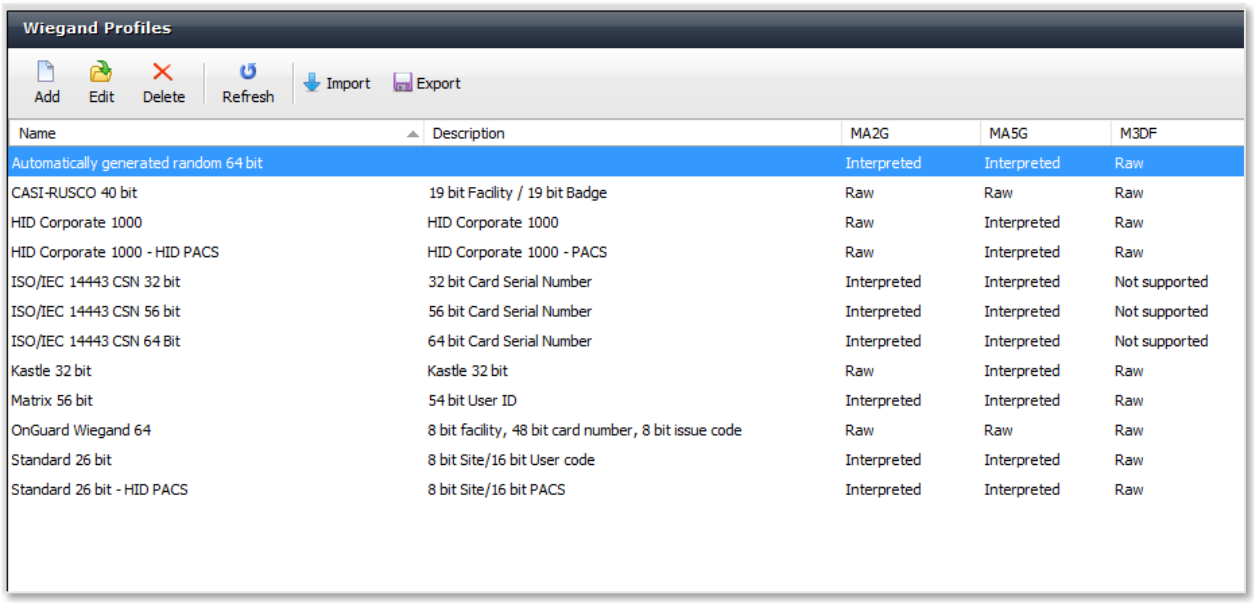
To select multiple devices, use the tick box on the left-hand side of the panel. The top tick-box allows to select all devices.



Actions on multiple devices may require significant processing and time. IDEMIA recommends performing them during idle periods of the system.

Wiegand Profiles

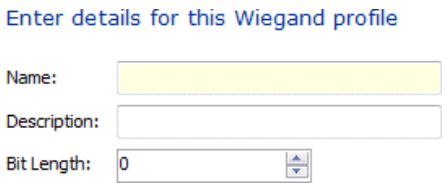
This section allows you to view, add, edit & delete Wiegand Profiles in MorphoManager. Wiegand Profiles define what information is output over the Wiegand Out interface of the Morpho Biometric Devices when a user is identified. This is most typically used in conjunction with an Access Control System.



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

Create a Wiegand Profile

Screen 1 – Configuration Details



Name: Name the profile anything up to fifty characters.

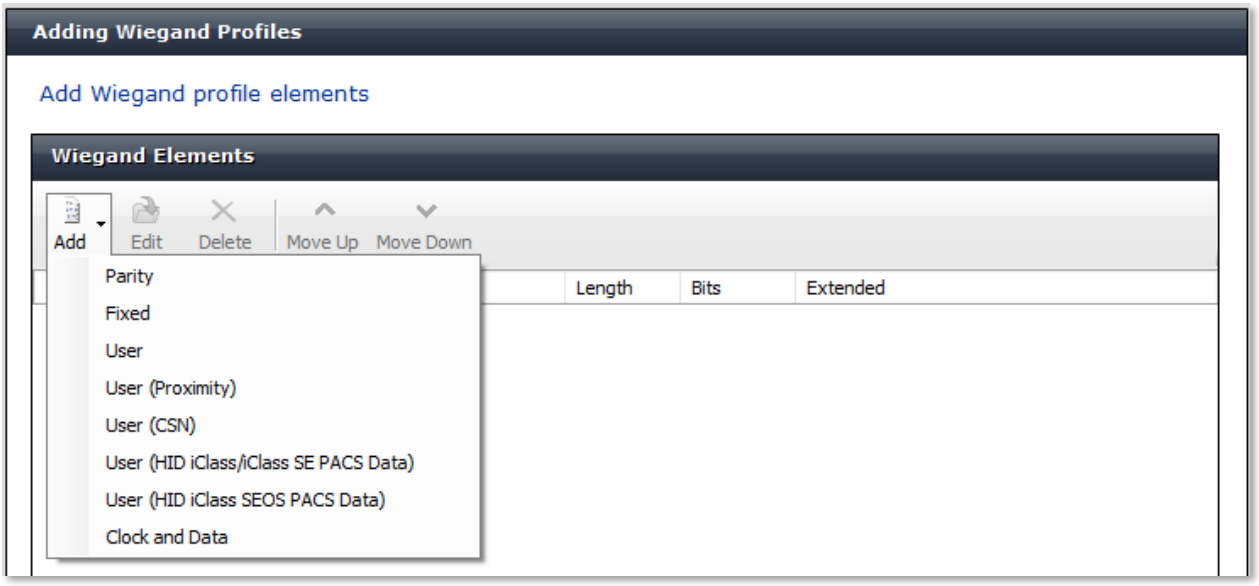
Description: Give the profile a description of up to one hundred characters.

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

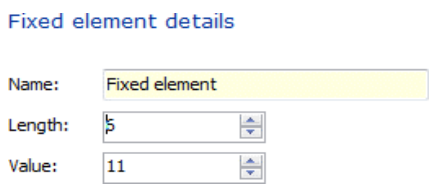
Screen 2 – Wiegand Profile Elements

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:

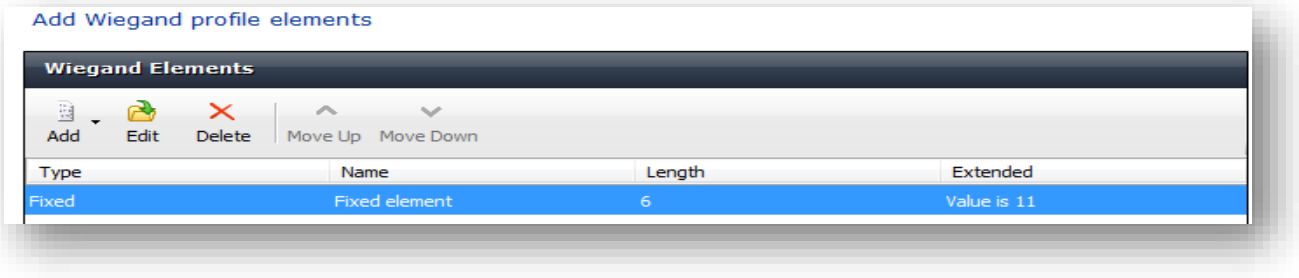
- **Parity:** Indicates a single bit that is typically used for error detection. Parity is calculated over one or more bits within the entire profile and can be Even or Odd.
- **Fixed:** Indicates a value that is common to all users of this Wiegand Profile. Typical examples of fixed values are Facility/Site 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.



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.

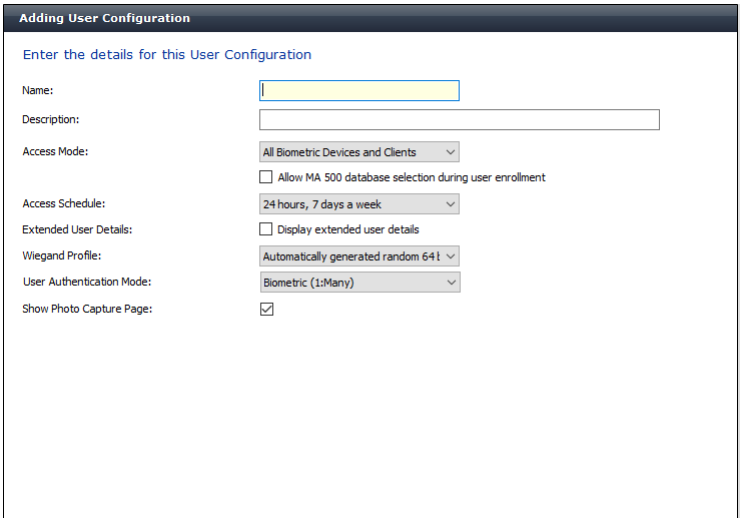
User Configuration

User polices 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



Name: Name of the User Configuration.

Description: Description of the purpose of the User Configuration.

Access Mode: This value determines the access to Biometric Devices that users in this policy will have.
All Biometric Devices and Clients: Users in this policy have access to all Biometric Devices.
Per User: Users in this policy will have access to the Biometric Device(s) specified in the User Distribution Groups selected for them in User Management and cannot be overridden.

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.

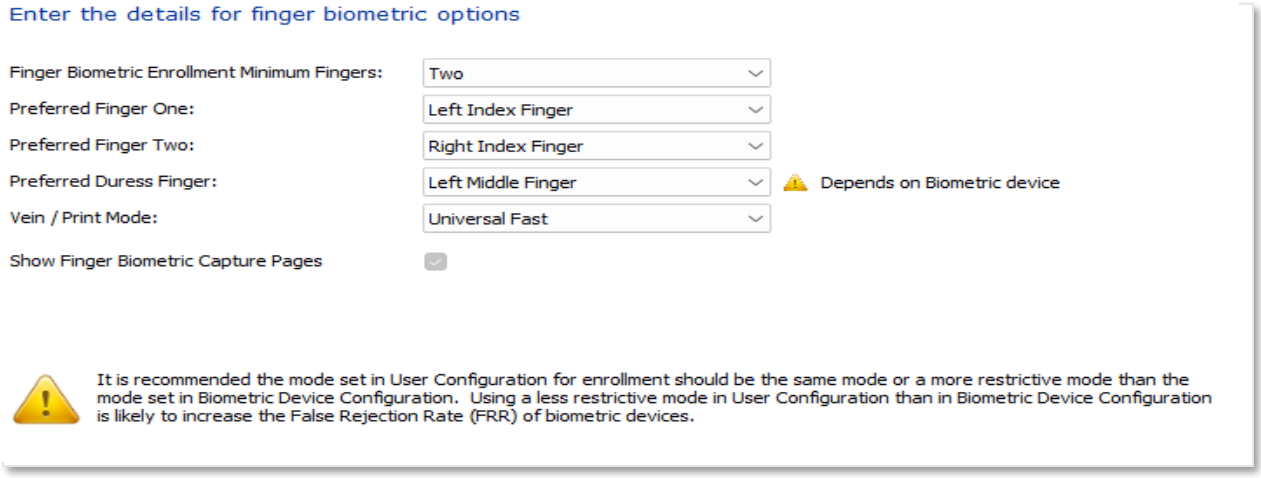
Wiegand Profile: Select the Wiegand Profile you wish to use for users in this User Configuration.

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



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

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

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

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

Duress Finger can only be utilized on the Sigma, Sigma Lite, and Sigma Lite + of readers (excluding Fingerscan and MorphoWave).

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.

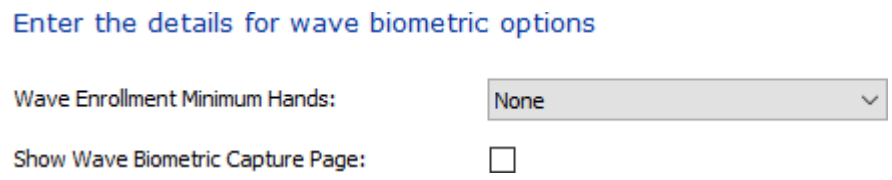
Universal accurate: Universal accurate is very similar to universal fast profile but with more time allowed for biometric data capture during enrollment and matching. This mode is recommended only when the biometrics of a significant number of users are difficult to enroll due to extreme conditions,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

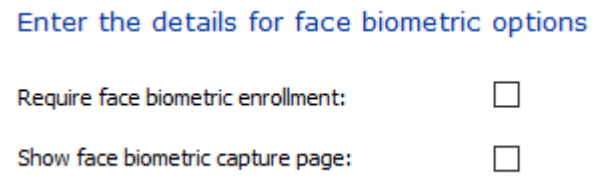
Screen 3 – Details for Wave Biometric Options



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

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

Screen 4 – Details for Face Biometric Options



Require face biometric enrollment: If enabled, enrollment with face biometric template will performed.

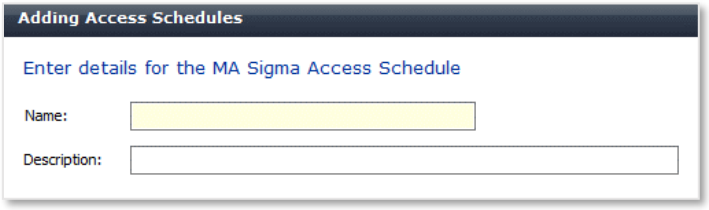
Show face biometric capture page: If enabled, the face biometric capture wizard screen will be shown in User Management when adding or editing users.

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



Name: Name of the Access Schedule

Description: Description of the Access Schedule

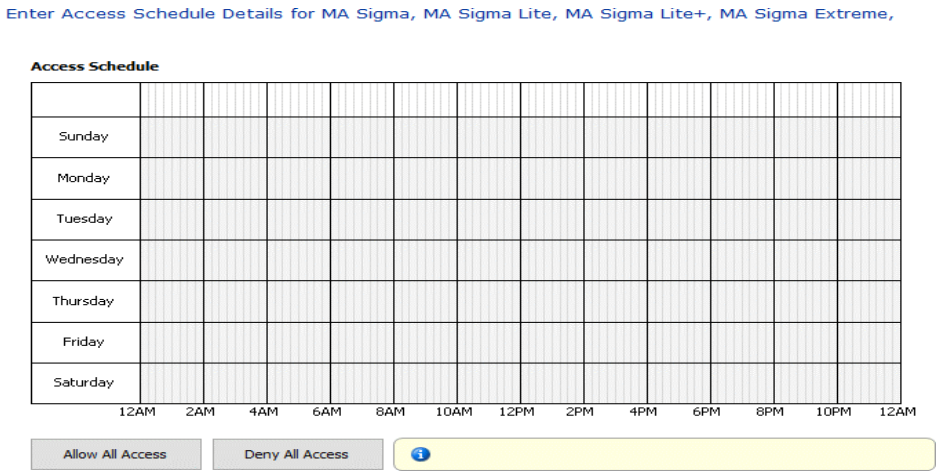
You can enter a maximum of 50 characters (all characters are allowed) for Access Schedule Name.

Screen 2 – MA Sigma, Sigma Lite. Sigma Lite+ 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.

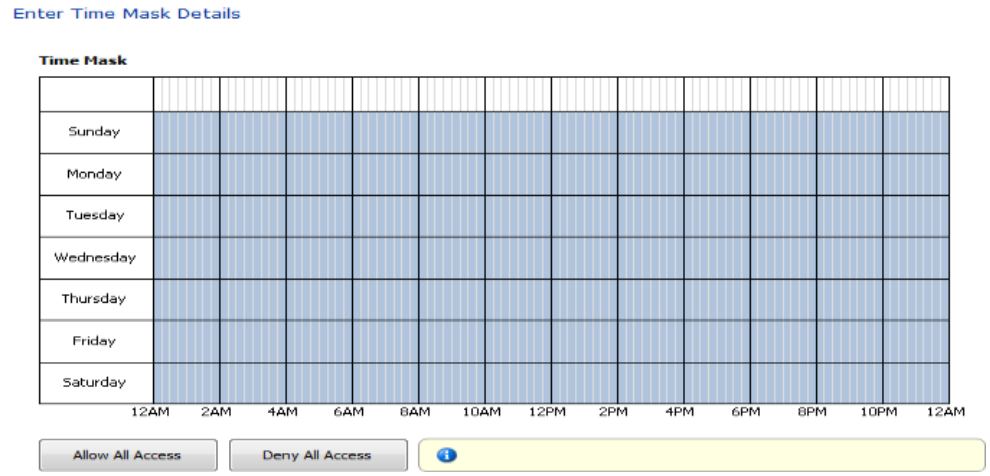
From this screen set the times needed in fifteen-minute increments. If a day is not set (left blank), no access will be allowed for users of the Access Schedule on that day.

The Access Schedules setting needs to be enabled in the Biometric Device Configuration menu for Sigma, Sigma Lite, Sigma Lite+, Sigma Extreme, 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

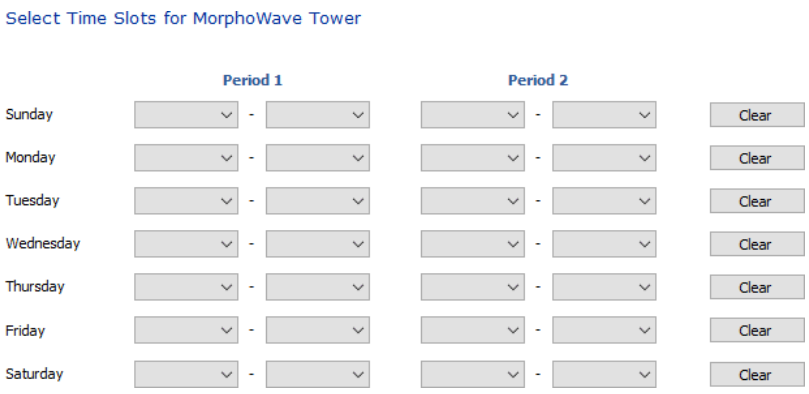
This screen allows you to create access times by selecting from the table with fifteen-minute steps across 24 hours for each day of the week. Click and drag the mouse over the required areas to select and deselect times. The time area in blue indicates access is allowed. White indicates access is denied. 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

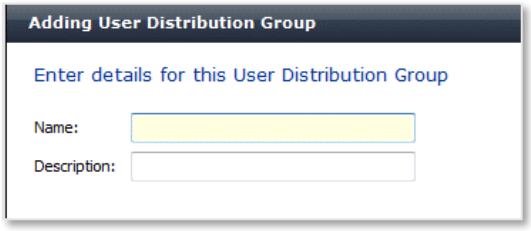
User Distribution Groups are designed to distribute users onto groups of MA readers or MorphoManager Clients. To be utilized the user must be in a User Configuration that has its Access Mode set to “Per User”. Then the User Distribution Groups will be selectable when creating (or editing) a user.

Part of the users data that are distributed via User Distribution Groups are biometric templates.

Please note, if a Fingerscan accessory is removed from a VisionPass SP, the fingerprint templates will not automatically be removed from the device by MorphoManager. This will require a Rebuild of the device.

Create a User Distribution Group

Screen 1 – Details

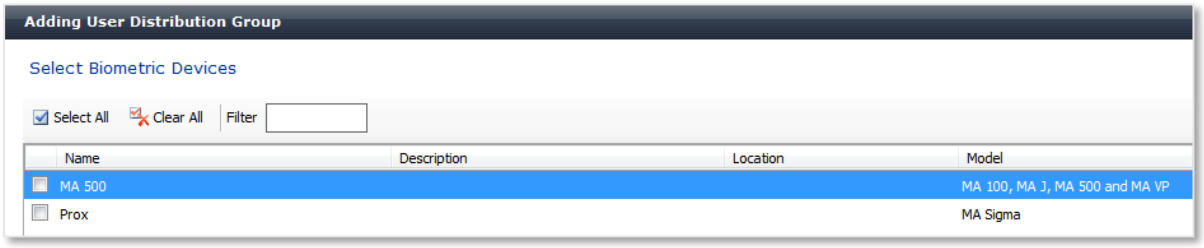


Name: Name of the User Distribution Group

Description: Description of the purpose of the group.

Screen 2 – Select Biometric Device Access

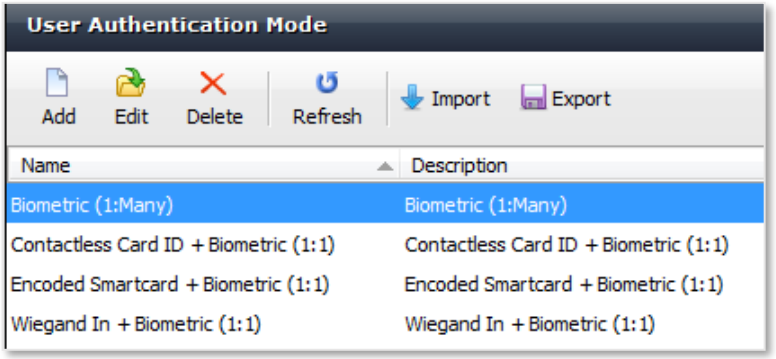
Select the Biometric Device(s) that this group will have access to. The “Select All” button will allow access to all Biometric Devices. The “Clear All” button will remove access to all devices.



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.

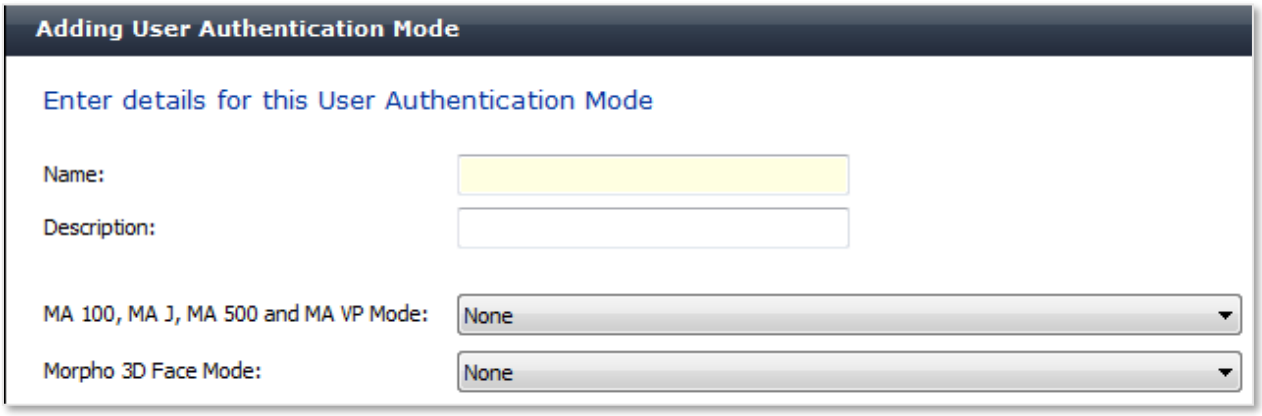
There are four automatically generated User Authentication Modes:



Card + Biometric is not supported by Fingerscan accessory.

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.

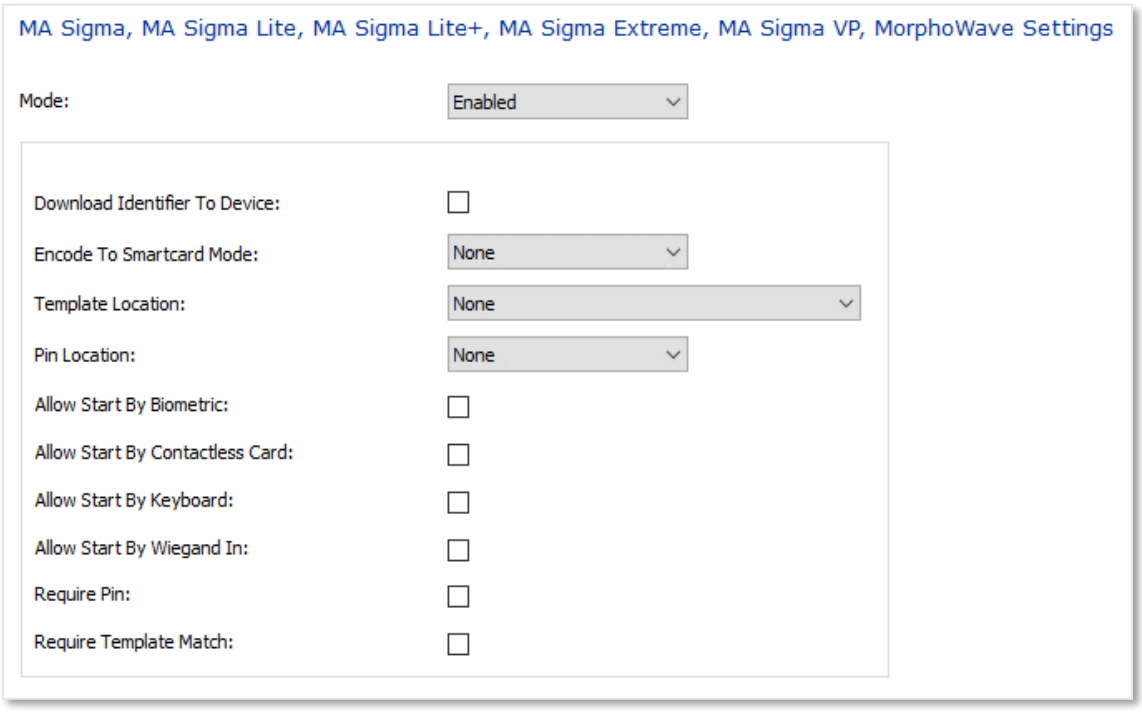
Identifier Encoded to Smartcard Identifier Template Downloaded to Device: The user carries a card with a Wiegand code on it and touches it on the Biometric Device. If the code read from the card is in the list of accepted Wiegand codes stored on the Biometric Device the fingerprint scanner is activated. 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.
In case of Face template, the template encoded in the card is Face_V2_Light_Comp, or Face_V3 if Face_V2_Light_Comp is not available.

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.

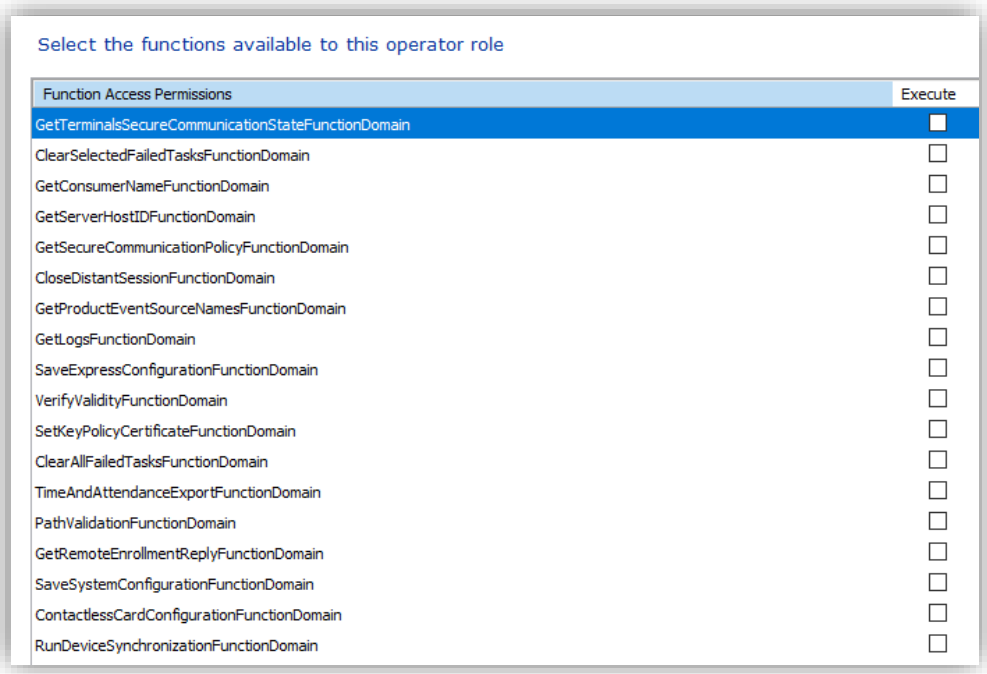
Role	Description	Documentation
BioBridge Enrollment Operator	Access to the BioBridge enrollment client to enroll new users in the system	BioBridge Quick start guide
Biometric Identification Operator	Access to the Biometric Identification feature of MorphoManager Client	MorphoManager User Manual – 'Biometric Identification' section
Onsite / Offsite Monitor Operator	Access to the Onsite / Offsite feature of MorphoManager Client	MorphoManager User Manual – 'Onsite / Offsite' section
Reports Operator	Access to the Reports feature of MorphoManager Client	MorphoManager User Manual – 'Reports' section
Transaction Logs Monitor Operator	Access to the Transaction Logs feature of MorphoManager Client	MorphoManager User Manual – 'Transaction Logs' section
User Management Operator	Access to the User Management feature of MorphoManager Client	MorphoManager User Manual – 'User Management' section

Screen 1 – Operator Roles Details

Enter the name for this operator role.

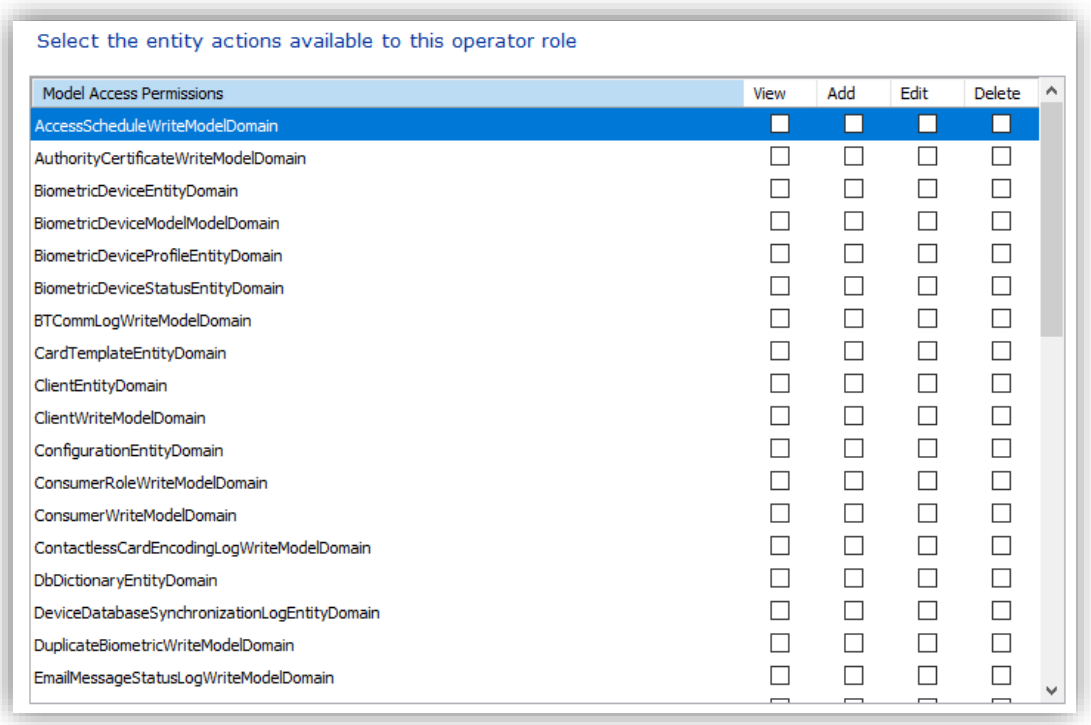
Screen 2 – Function Access Permissions

Select the functions, this operator role will allow access to.



Screen 3 – Entity Access

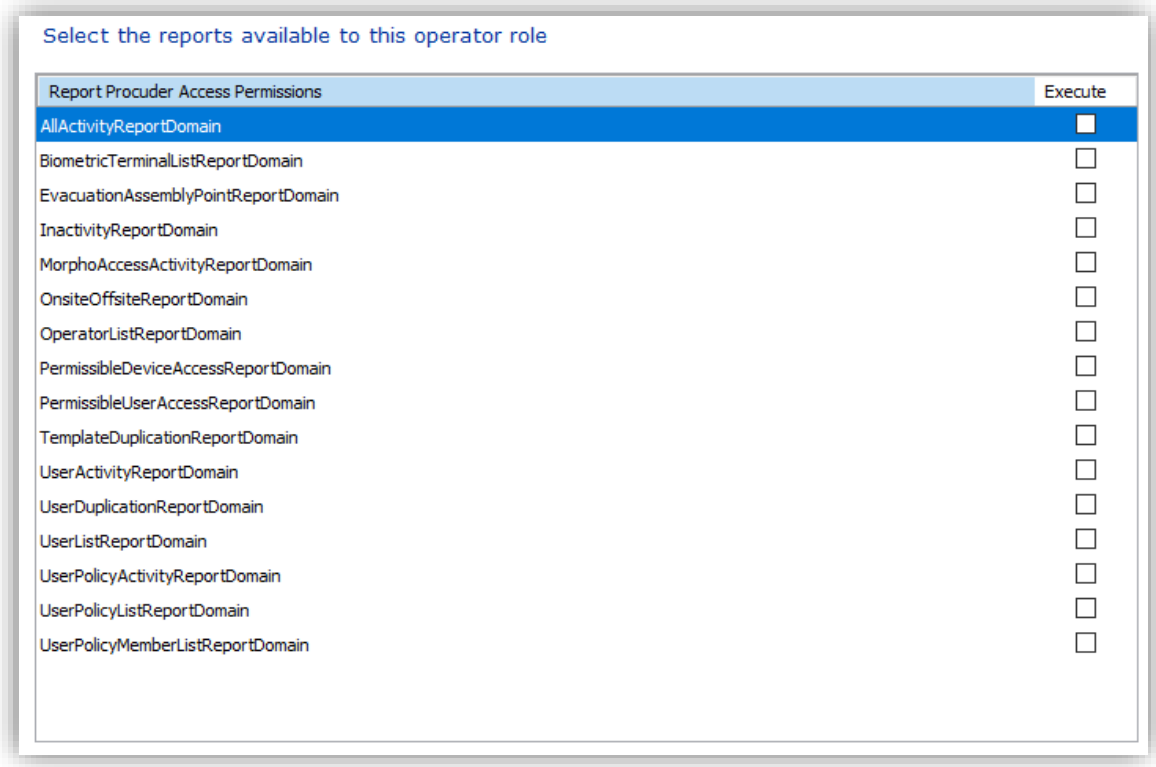
Select the entities this operator role will have access to and the type of access (view, add, edit, delete).



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

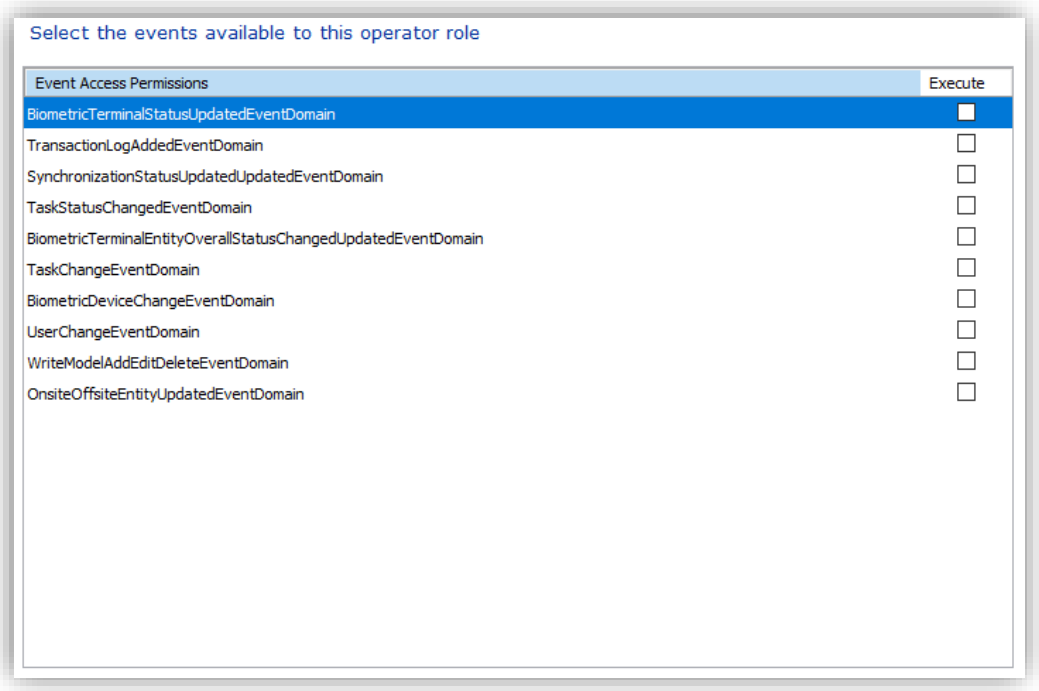
Screen 4 – Report Access

Select the reports this operator role will have access to.



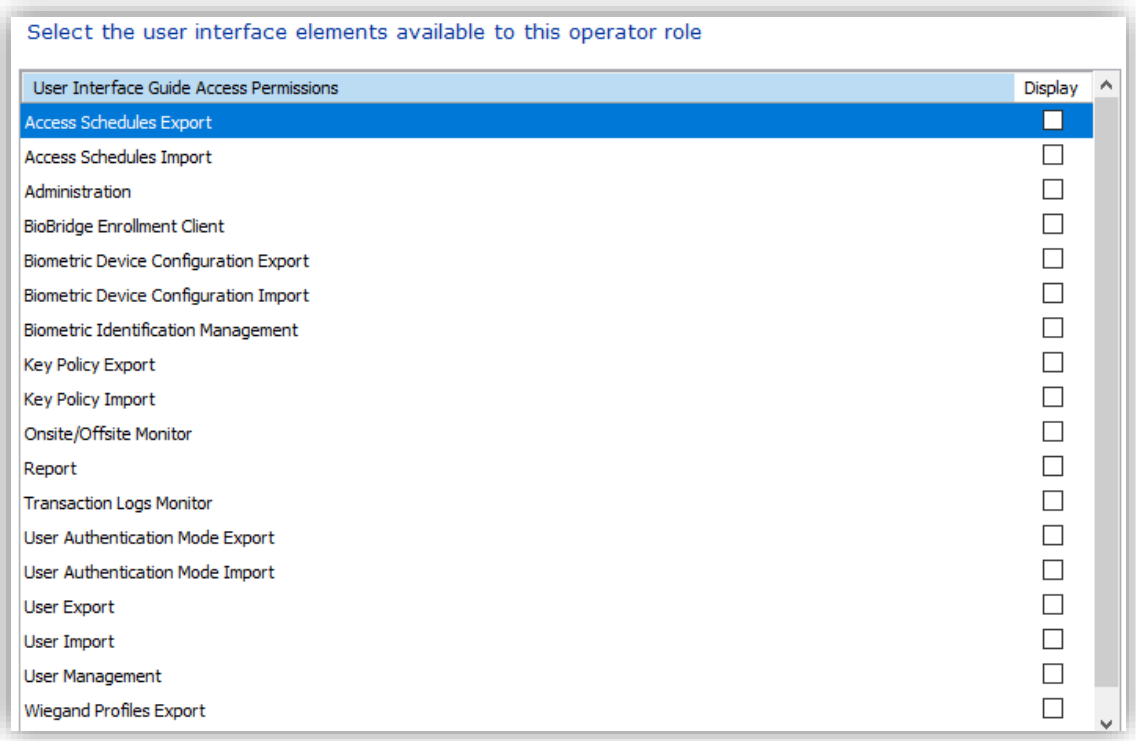
Screen 5 – Event Access Permissions

Select the events, this operator will have access to.



Screen 6 – User Interface Access Set

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



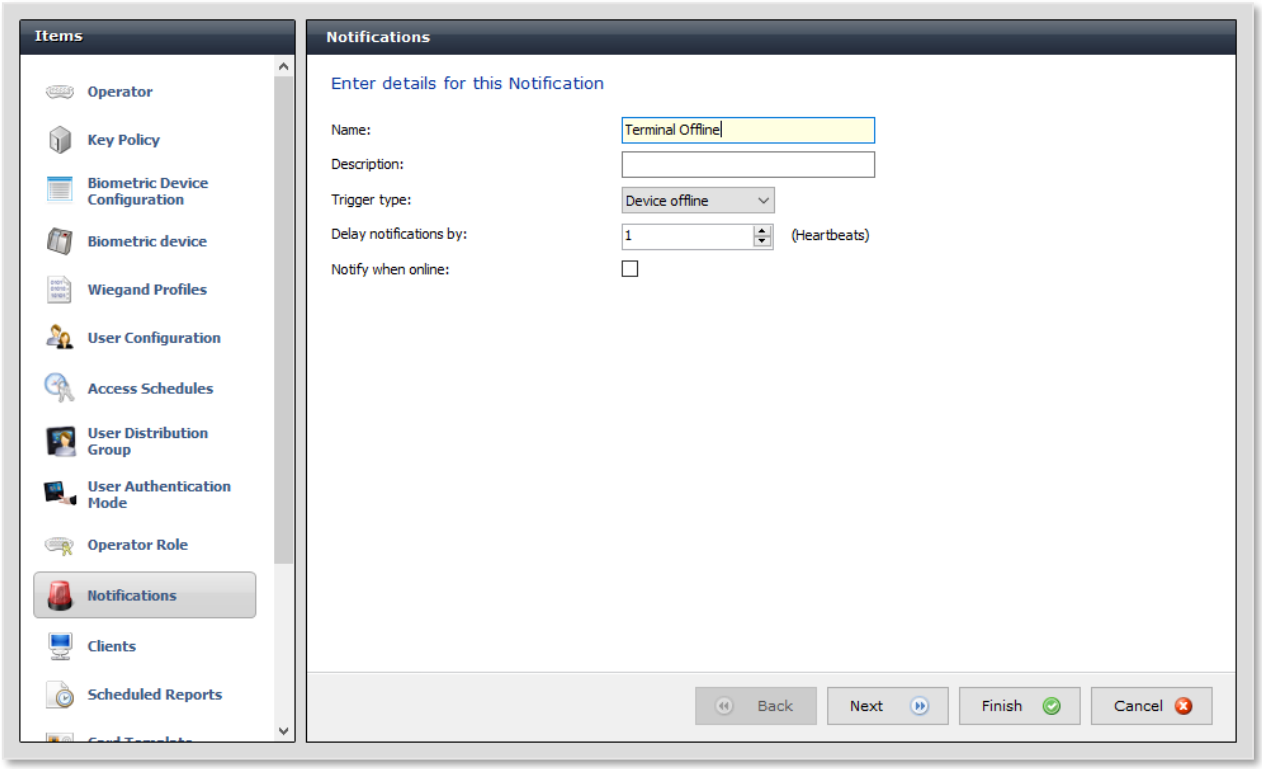
Notifications

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.

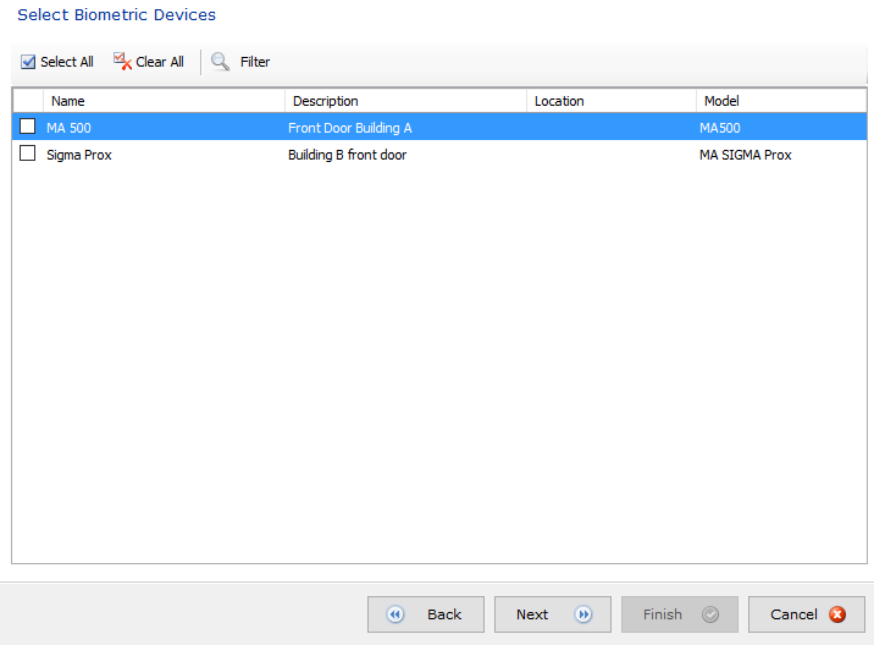
Description: Description of the Notification's purpose.

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.

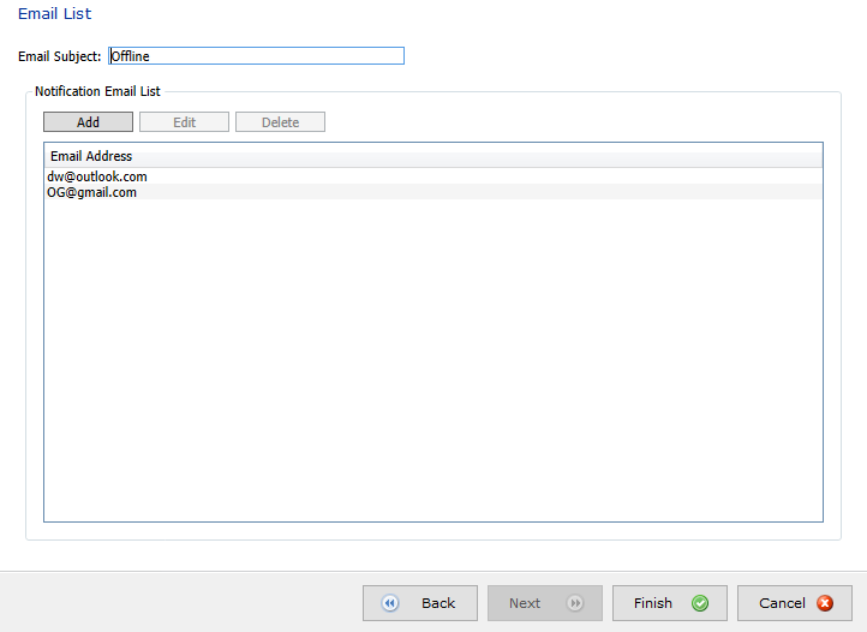
Notify when online: Send a notification when terminals in this notification group are back online

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



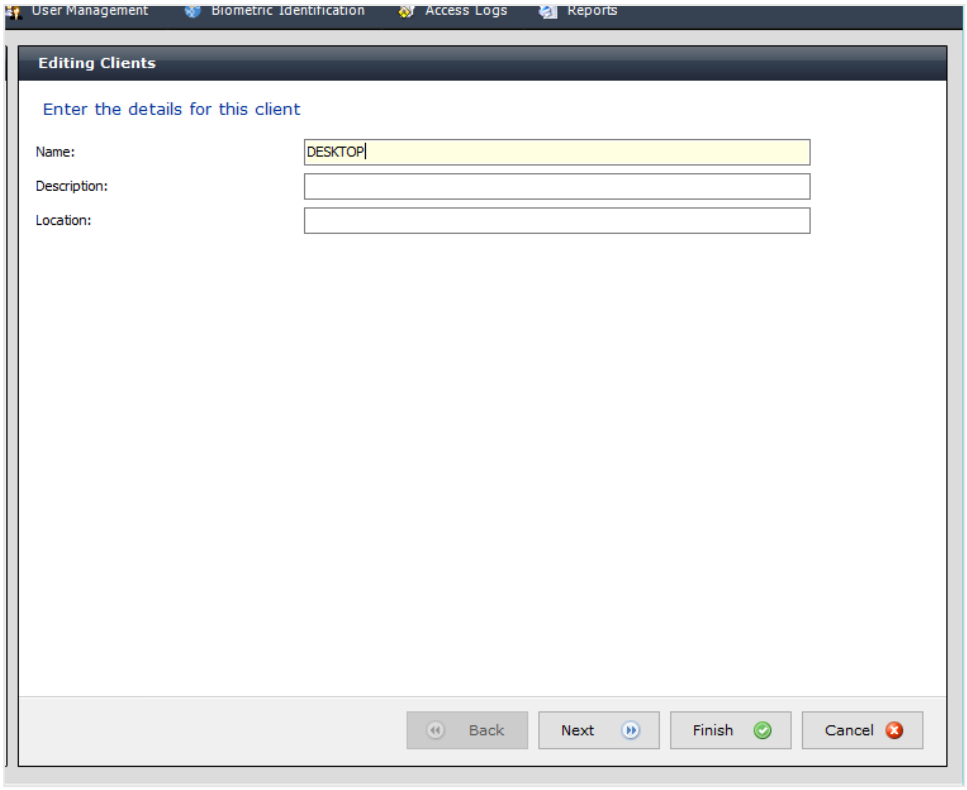
The Email List screen will allow for configuring what the emails subject line will be and to whom it will be sent. Email addresses can be Added, Edited, and Deleted. At least one recipient must be present to click **Finish**.

Clients

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

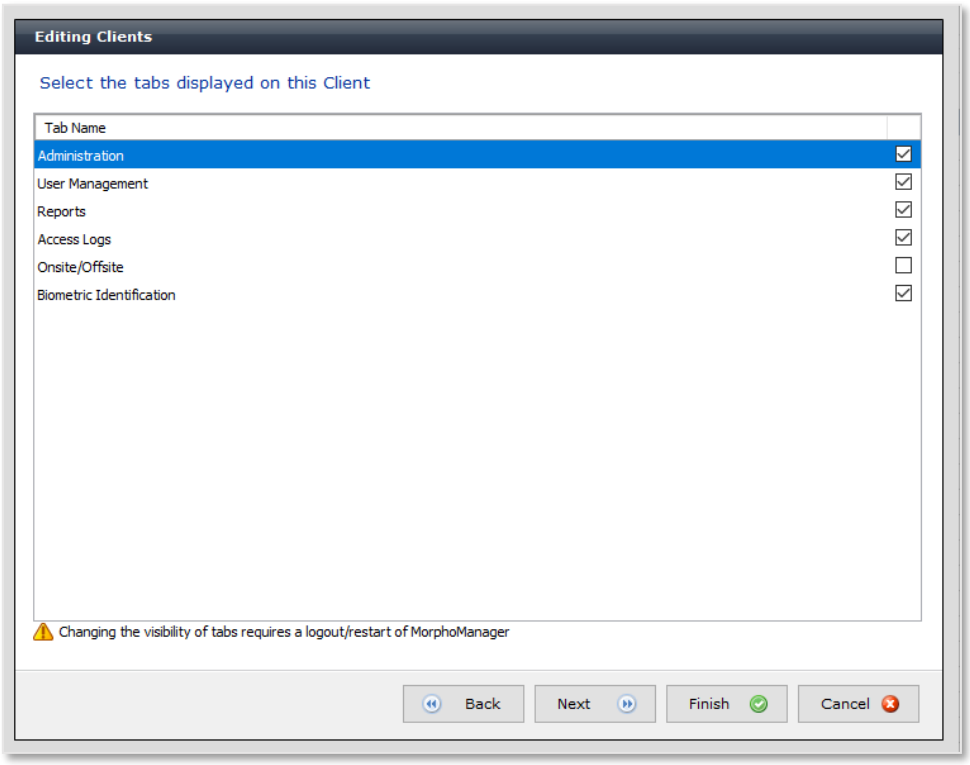
Screen 1 – Enter the details for this Client

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.



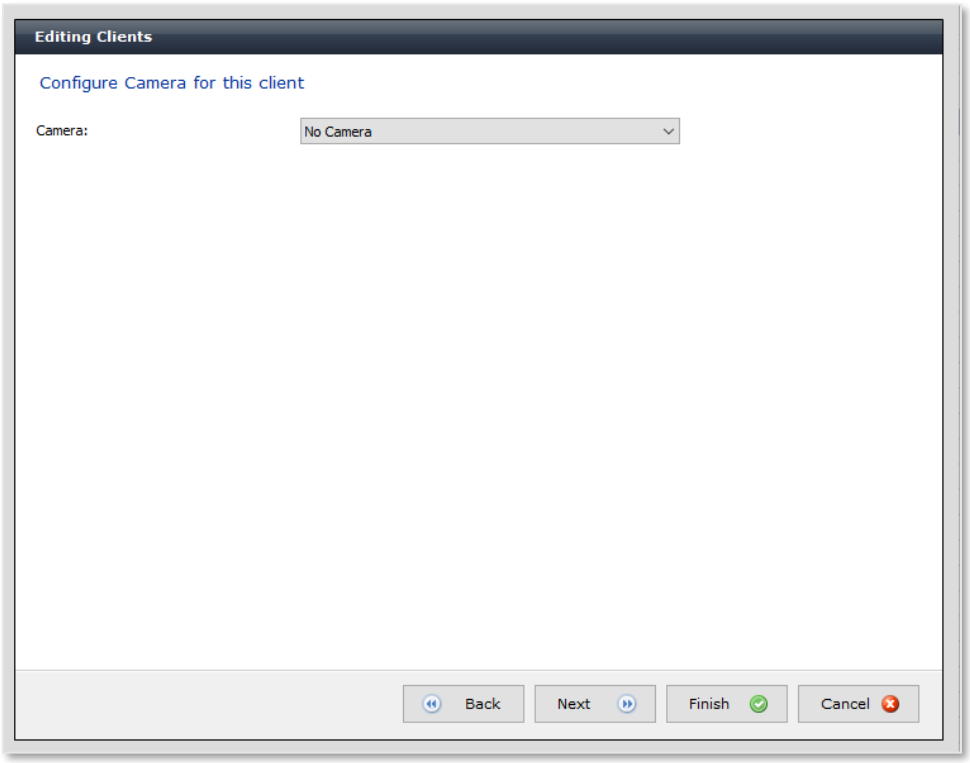
Screen 2 – Select the tabs displayed on this Client

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



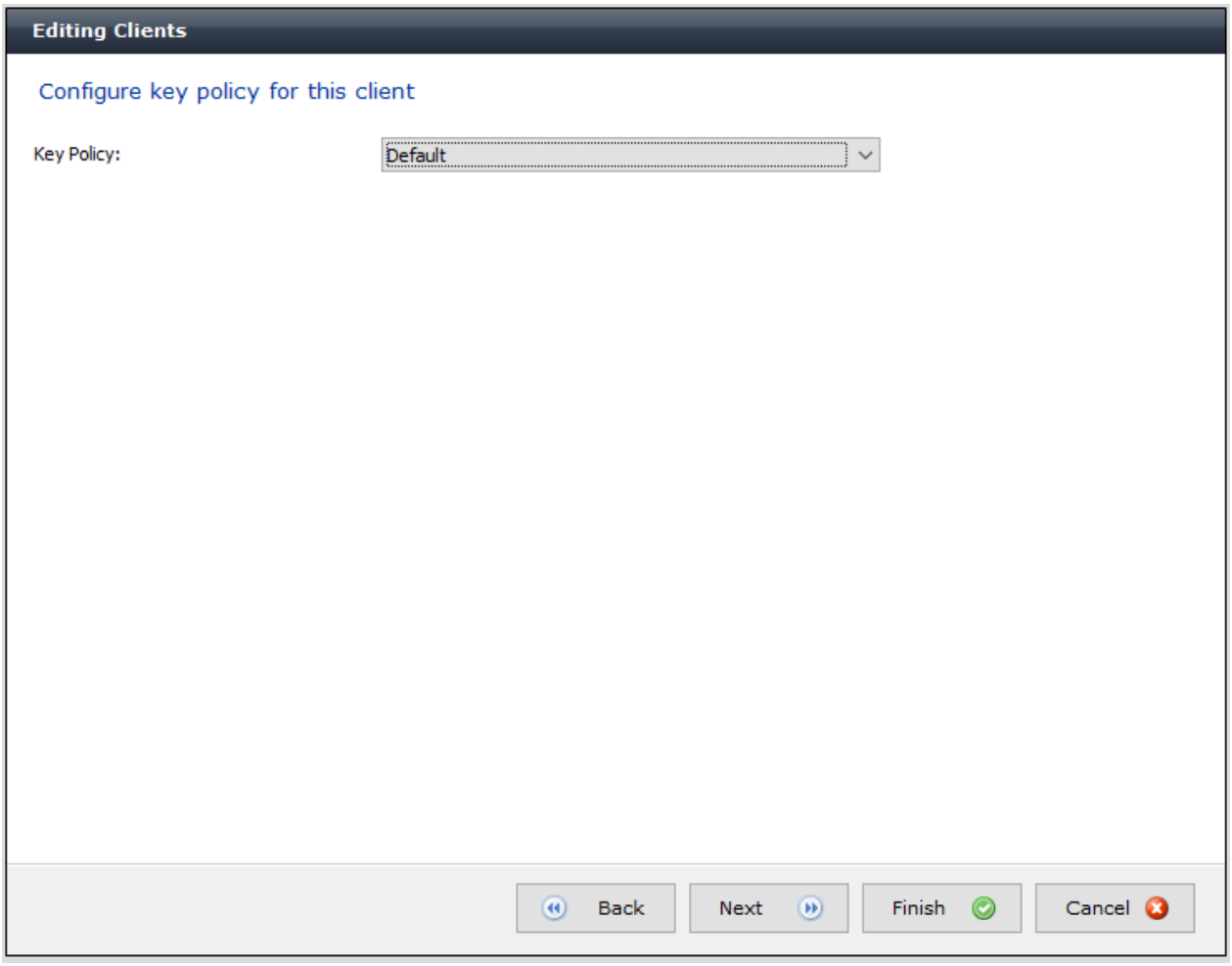
Screen 3 - Camera Configuration

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

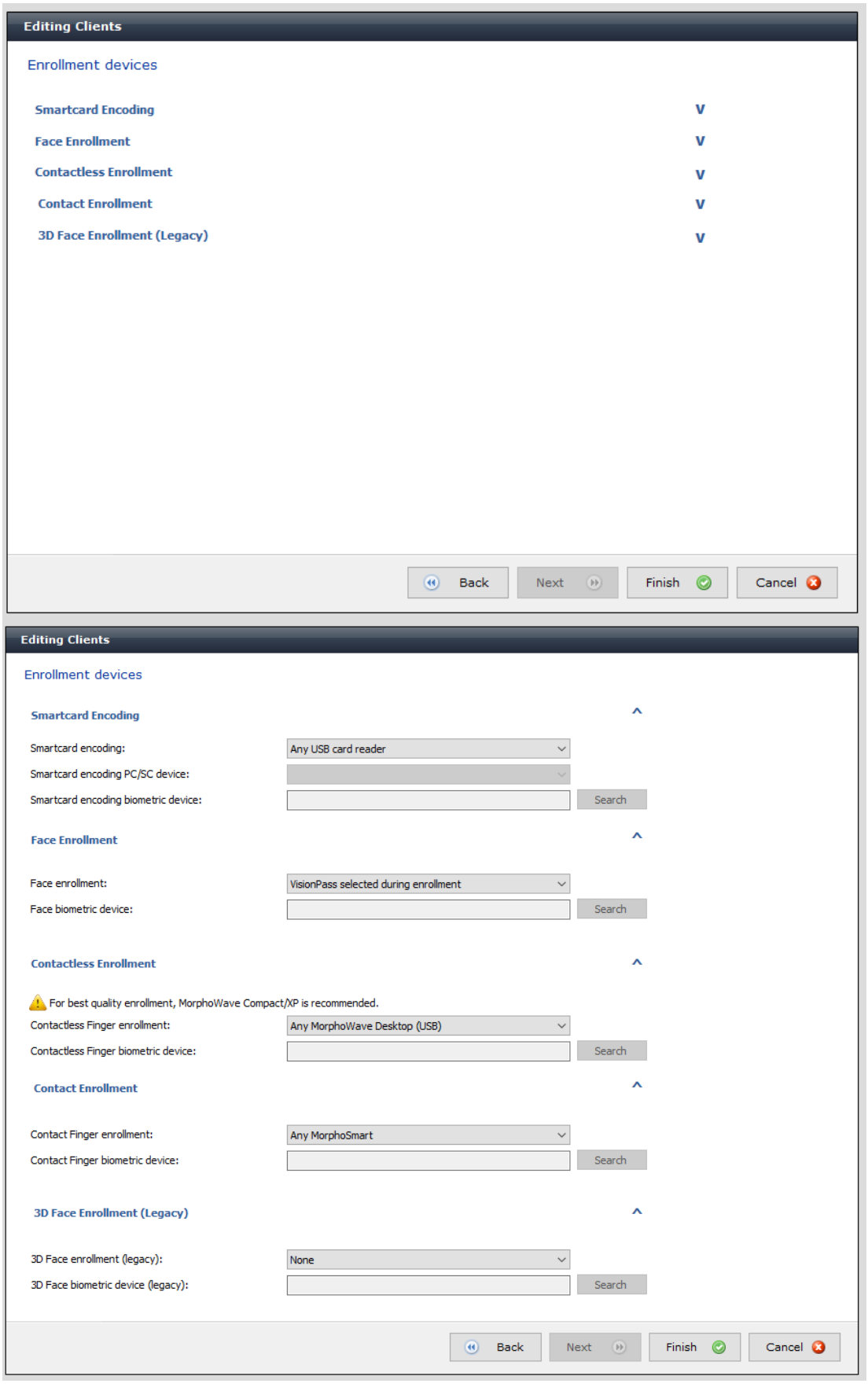
If the Client is aimed at encoding contactless cards, the Key Policy is to be selected (please refer to the dedicated section for details about the Key Policy).



Screen 5 - Enrollment Devices

Select the Enrollment Devices you wish to use in MorphoManager during User enrollment. For majority of terminals, you can choose between:

- Any Biometric Device: MorphoManager will select the first terminal detected on your system.
- Selected Biometric Device: You choose now which Biometric Device will be used for all the enrollment on this Client.
- Biometric Device selected during enrollment: the Biometric Device will be chosen by the Operator during the process of User Enrollment.



The SIGMA device must be accessible from the MorphoManager Client for the purposes of contact enrollments. The MorphoManager Client will make a connection directly to the device and will not route the traffic through the MorphoManager Server.

For contactless enrollments it requires the biometric device to be accessible from the MorphoManager Server. The MorphoManager Server will make a connection directly to the device and will not route the traffic through the MorphoManager Client.

For contactless enrollments: Enrollment can be done either using MorphoWave SP or MorphoWave XP/XP 2 products, however, it is recommended to use XP/XP 2 product to maximize the performances. Moreover this level of interoperability between XP/XP 2 (enrollment) and SP (verification) is met only if the enrolment has been done using a MorphoWave XP/XP 2 firmware later than version 1.5.0, and with pklite templates.

Fingerscan accessory for VisionPass SP cannot be used as an enrollment device.

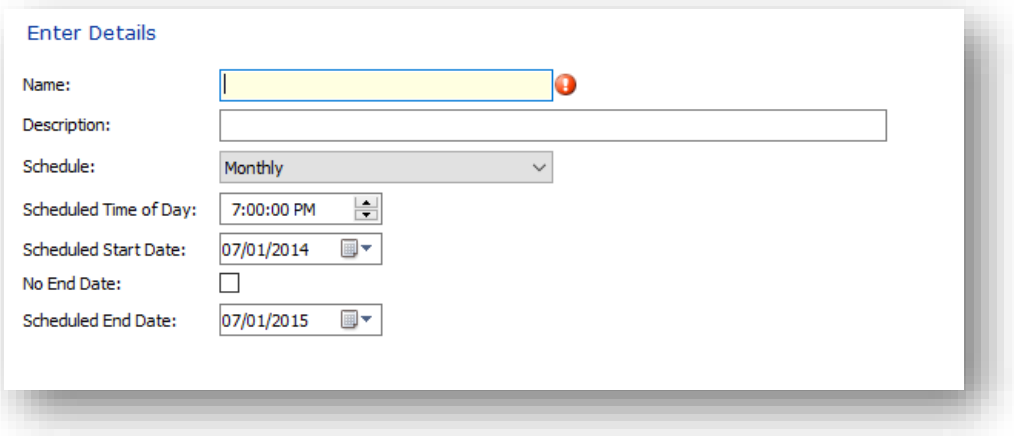
Scheduled Reports

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

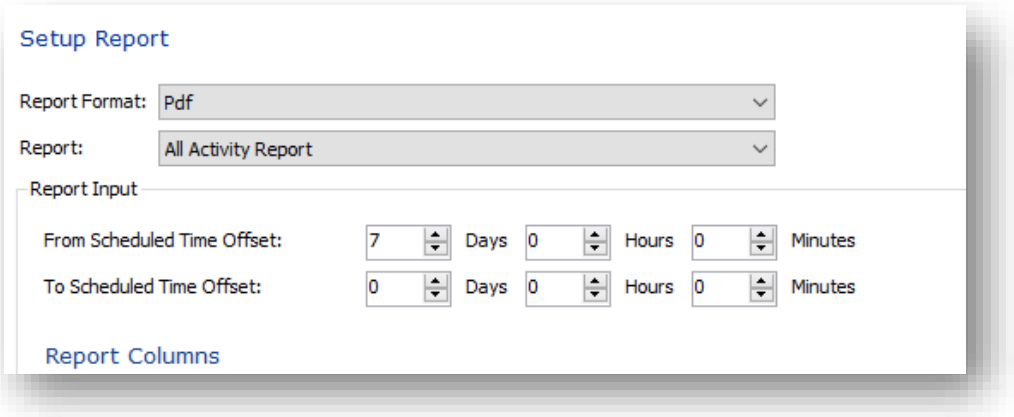
SMTP Settings must be configured in system configuration before a scheduled report can be created.

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

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

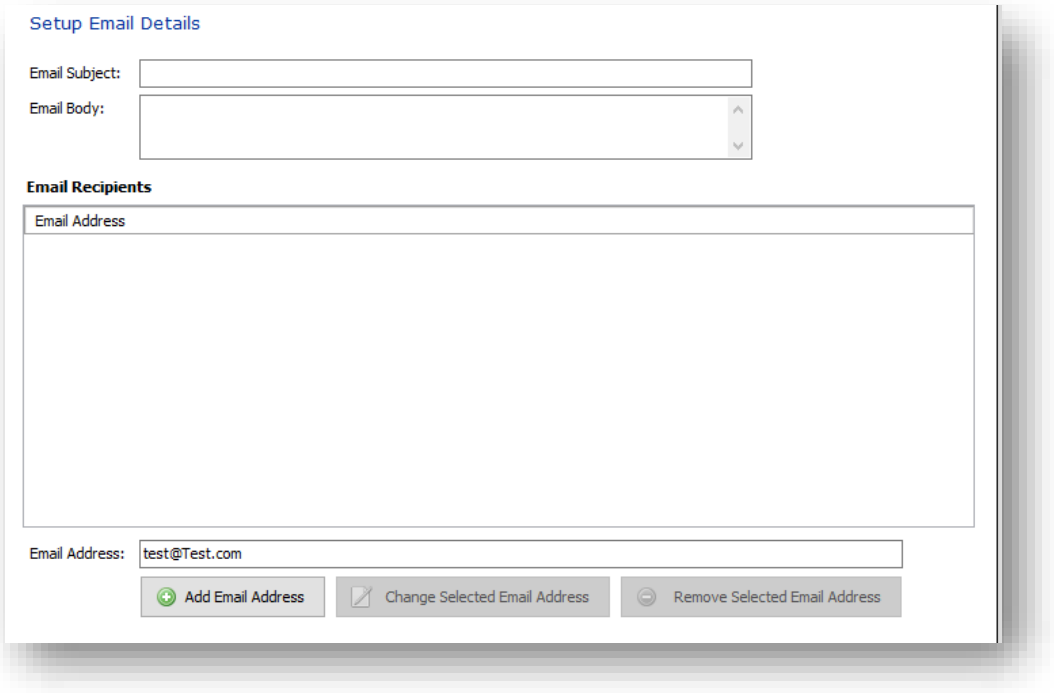


Select the format of the scheduled report. Options are pdf, word document, or excel spread sheet.



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.

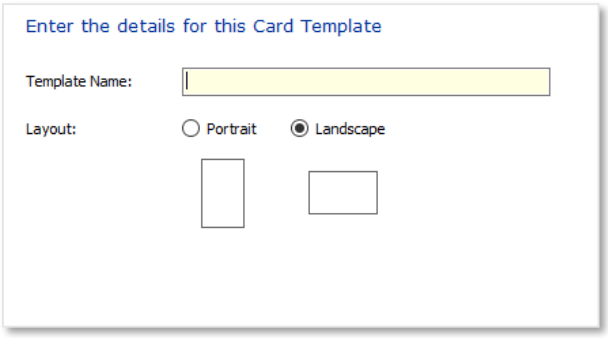
To change the details of the selected scheduled report, click on **Edit** in the toolbar. To remove the selected scheduled report, click on **Delete**. To generate the selected scheduled report now instead of waiting for the predefined generation interval, click on **Run Report Now**.

Card Template

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

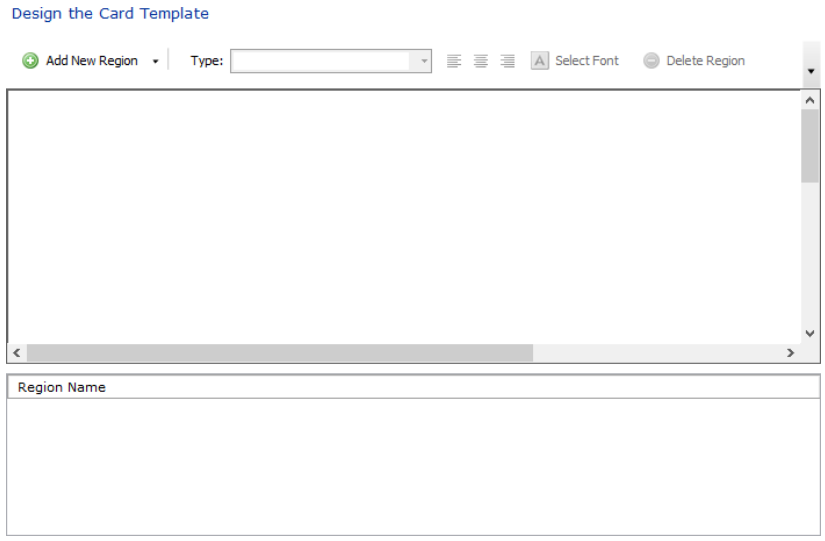
Screen 1 - Details

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



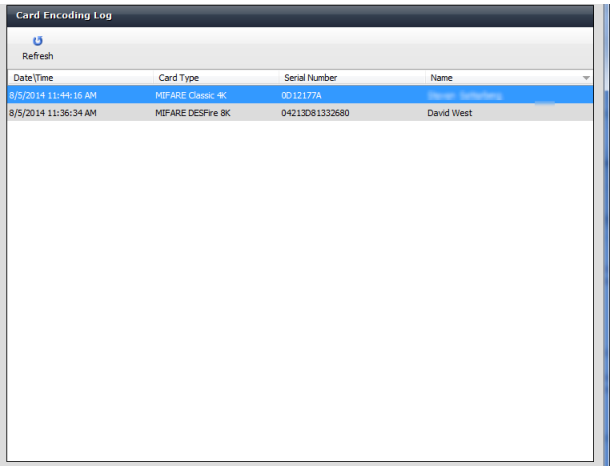
Screen 2 - Design

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.

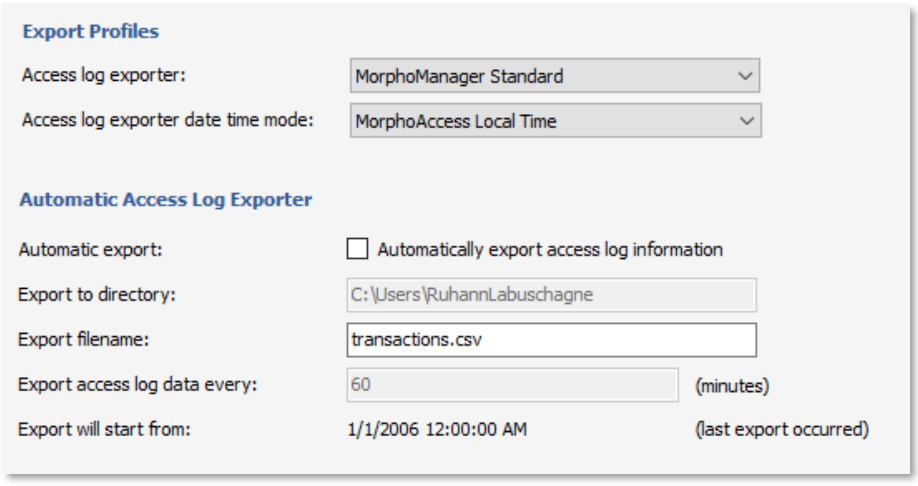
Exception Logs

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 setting 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)
- SOdb
- TimeAmerica.
- ASTROW
- TimeKeeper
- MorphoManager Standard **

****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

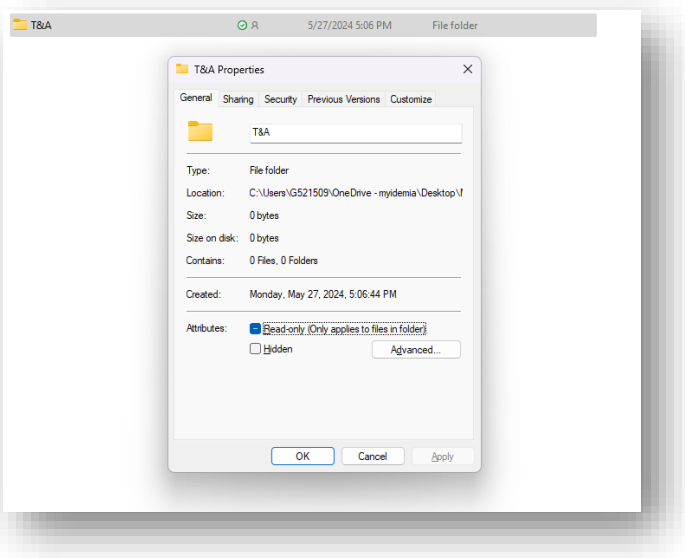
Automatic Access Log Exporter

Click on the check box for **Automatic export access log information**. The file will be exported at the interval specified at **Export access log data every**.

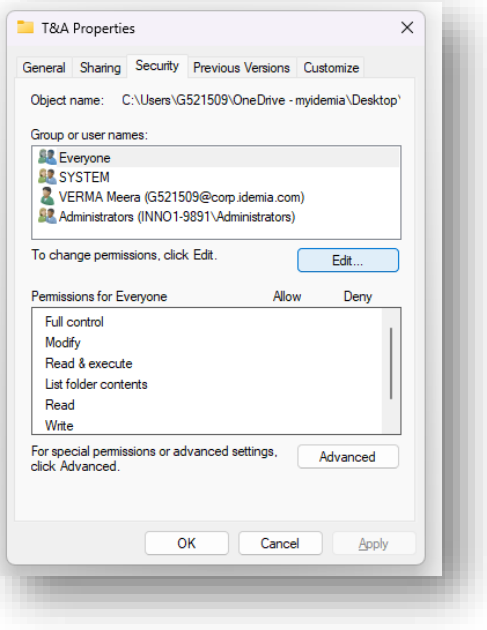
Enter the file name and destination for the file. The directory MUST exist on the server computer as the file will be saved to the server's hard drive.

If you change the default directory, please make sure MorphoManager (Service account user) will have writing access rights to this directory, for instance following the below procedure :

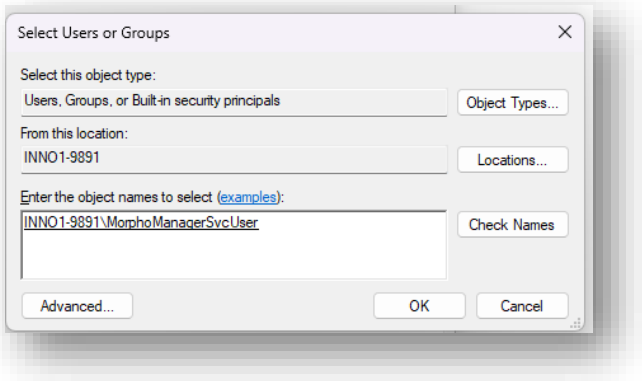
- Navigate to specific directory > Right click on folder and 'open Properties'



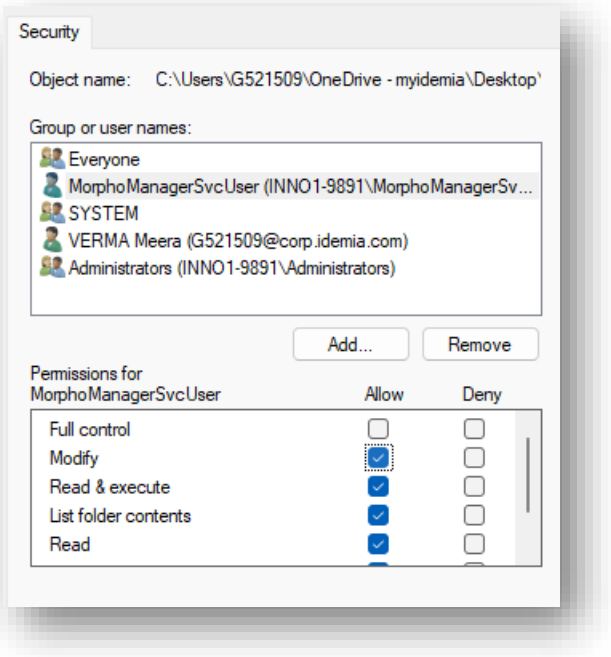
- Switch to Security tab and click on Edit button of 'Group or user names:'



- Add related user account mapped with MorphoManager Service

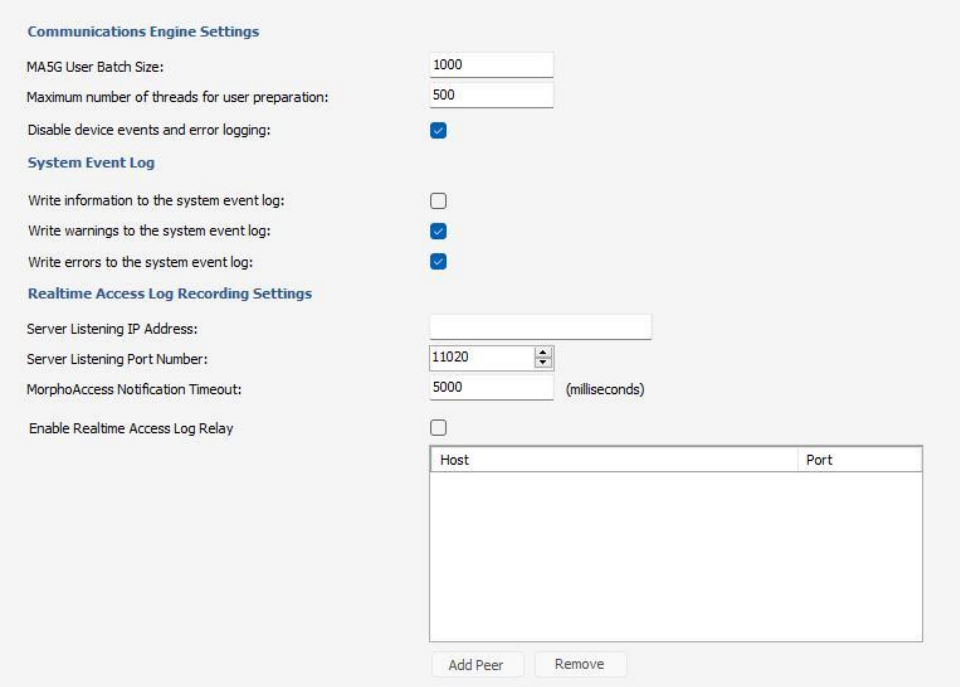


- Provide Modify/Write access rights to same user account.



- Click on Apply and Ok button for providing the access rights.

Communications Engine



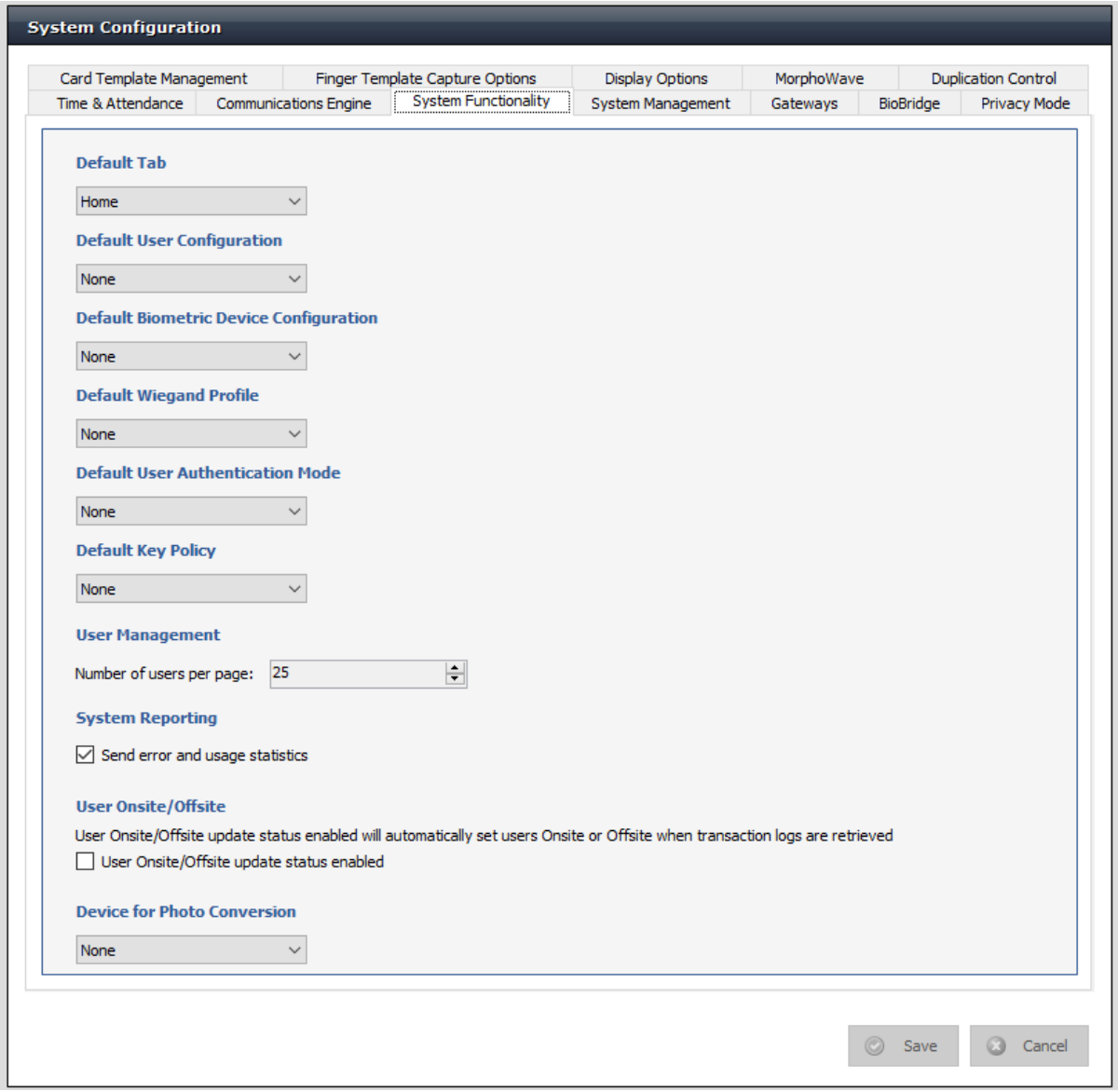
MA5G User Batch Size: Sets the batch size of users to be sent to a device.

Maximum number of threads for user preparation: Reserved for Idemia Support.

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.

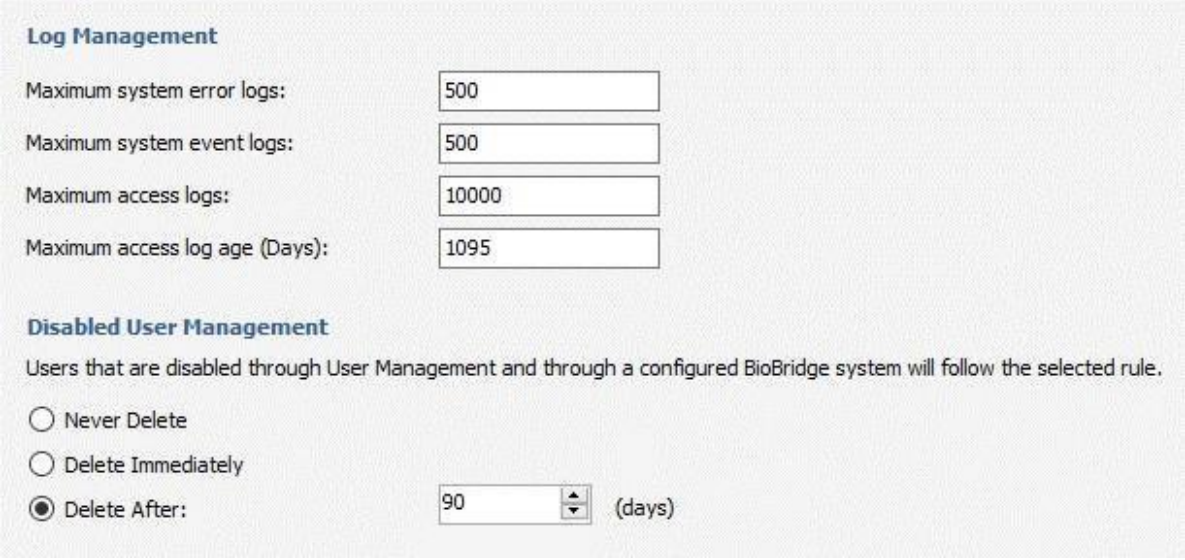
Default User Authentication Mode
This defines the User Authentication Profile that will be used as default when adding a User Configuration to the system.

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 on one page will appear on your User Management screen. By default, the value of this field will be 25 (which is the minimum value) and its maximum value will be 250.

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



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.

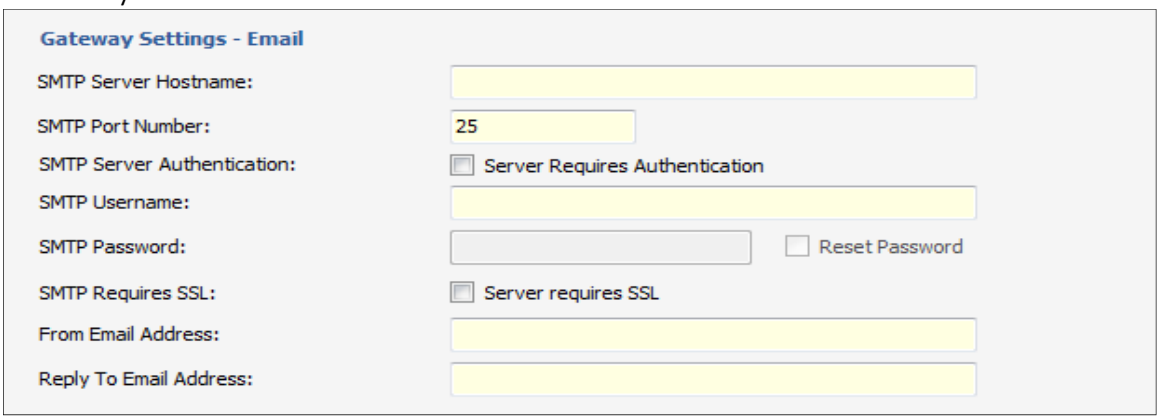
Disabled User Management
Users who are disabled in User Management will be governed by the following options:

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.

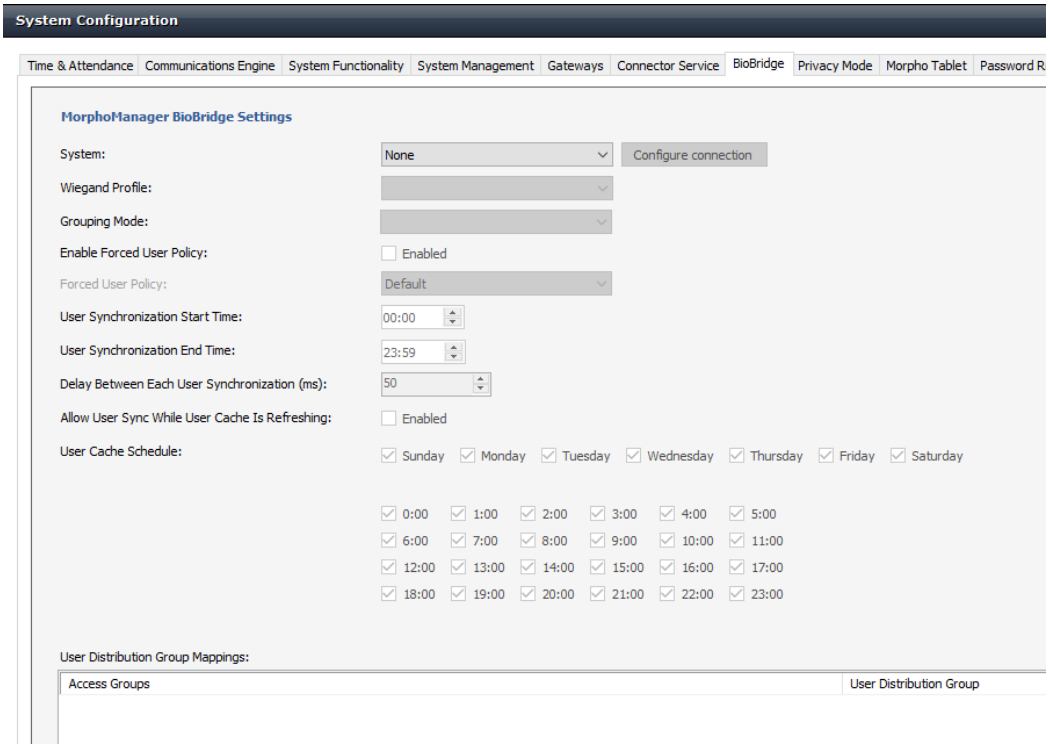
Gateways



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.

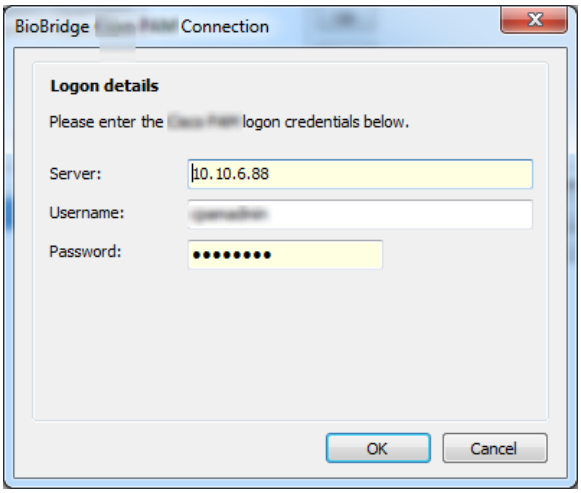
BioBridge

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.

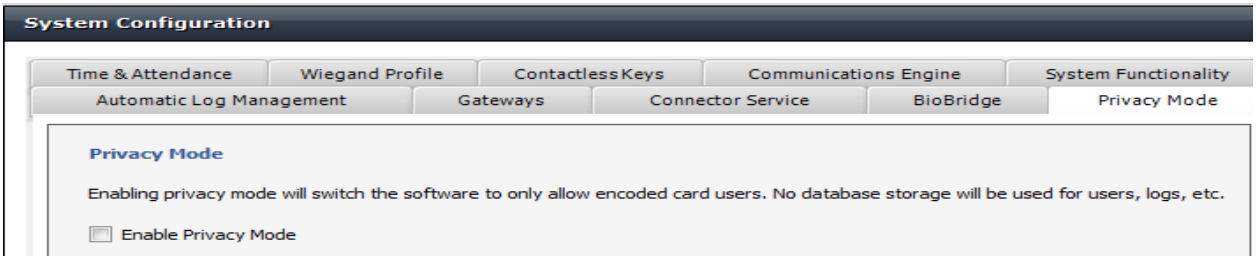
User Cache Refresh Schedule need to be selected on hourly basis in case when system selected as CCURE

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

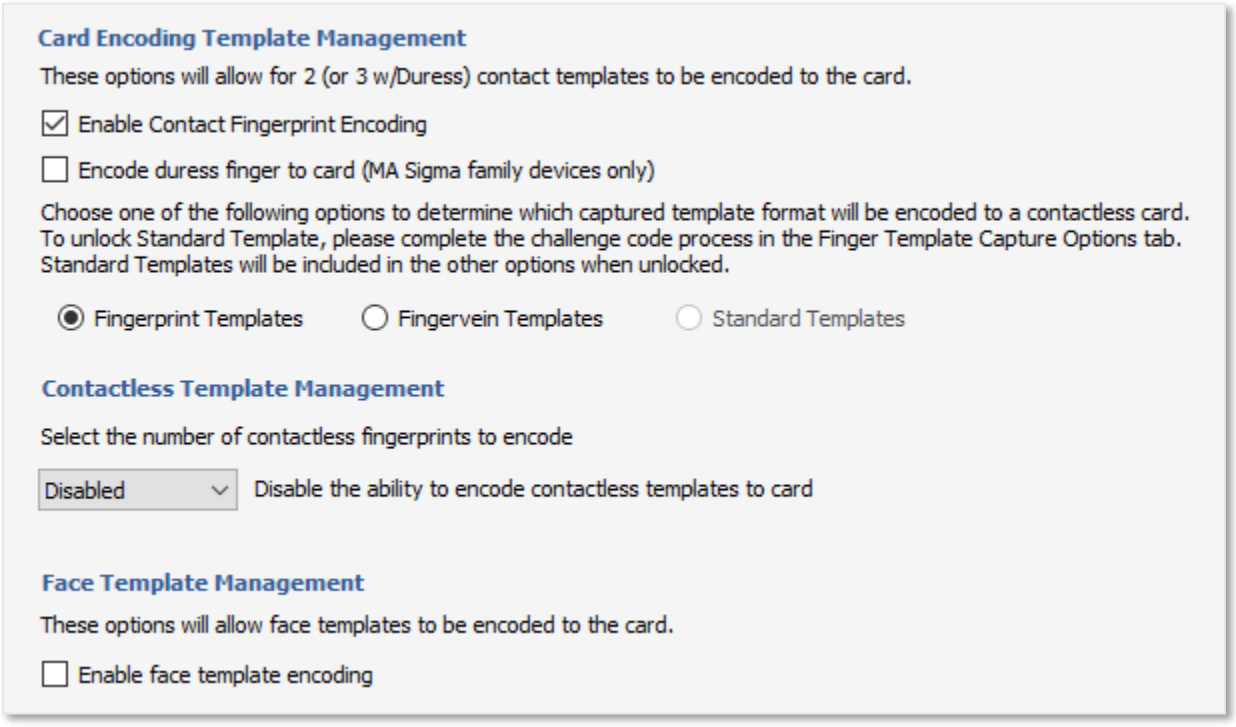
This mode will allow customers to enroll card-only users (i.e. Card-only, Card + PIN, Card + Fingerprints, Card + Fingerprints + PIN) without saving their details to the MorphoManager database. This mode will apply to all User Policies and will only apply to **new** enrolments. Users who are enrolled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



Privacy Mode is not compatible with multiple user import.

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.



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.

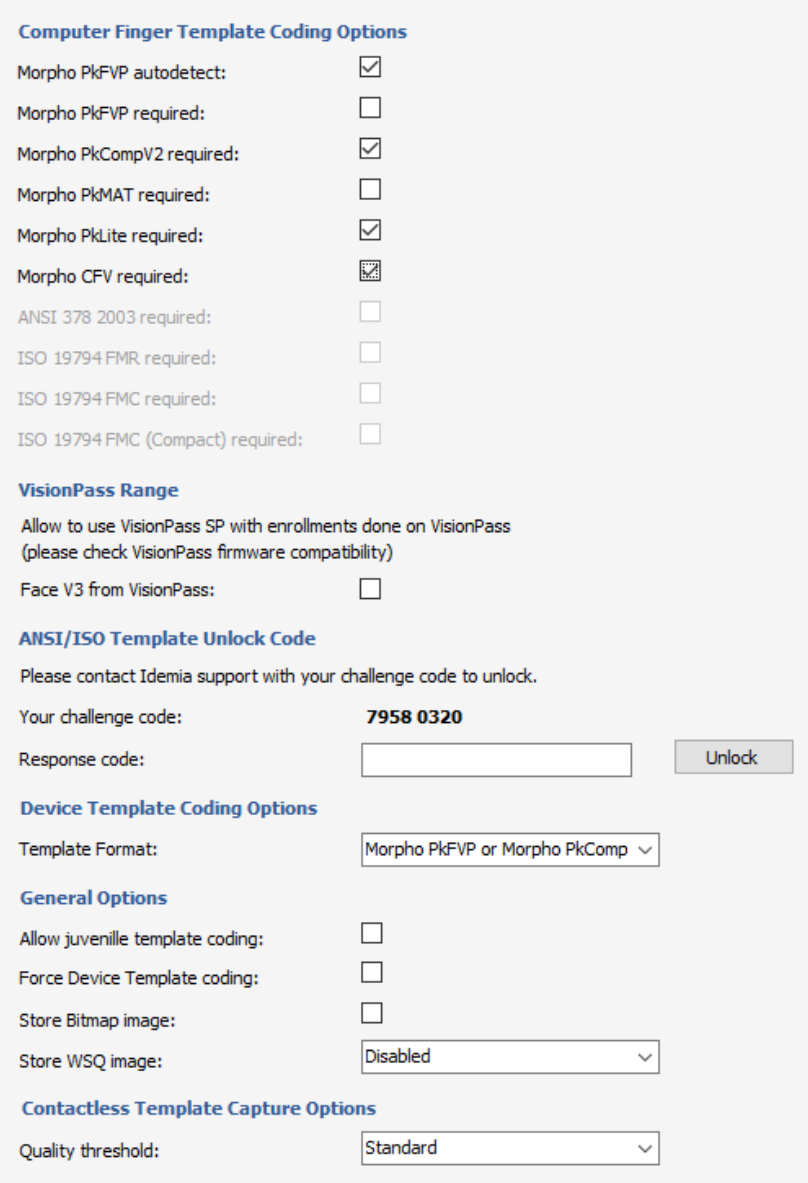
Card encoding template priority
This section determines which template types to encode to a card. The default setting is “Fingerprint Templates” and this will provide the optimum performance. If you are using any FVP devices, select the “Finger-vein Templates” radio button to ensure that the FVP templates 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 client is required to encode contactless fingerprints to a smartcard

Biometric Template Capture



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

VisionPass Range: Enables generation of V3 template format from the VisionPass device during enrollment if firmware allows. Requires extra time for enrollment.

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

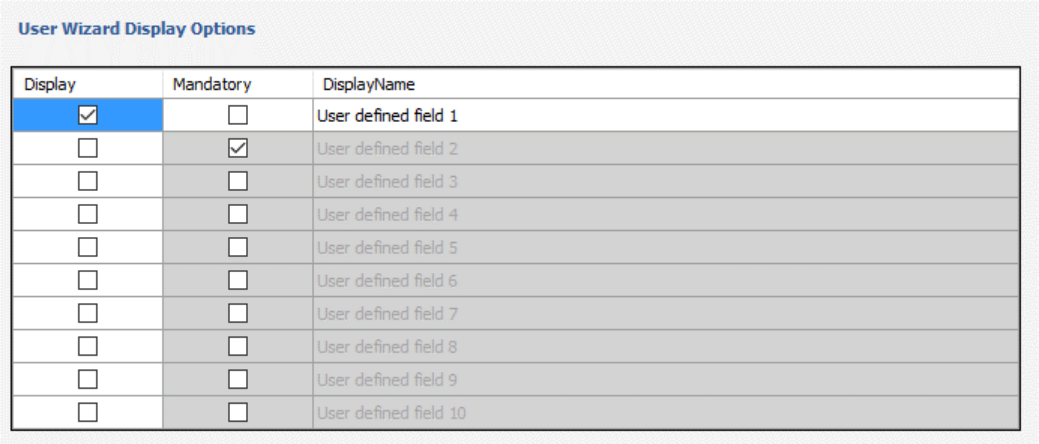
Device Template Coding Options: configures the (single) template format that will be coded when an enrollment is performed using MorphoSmart.

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”

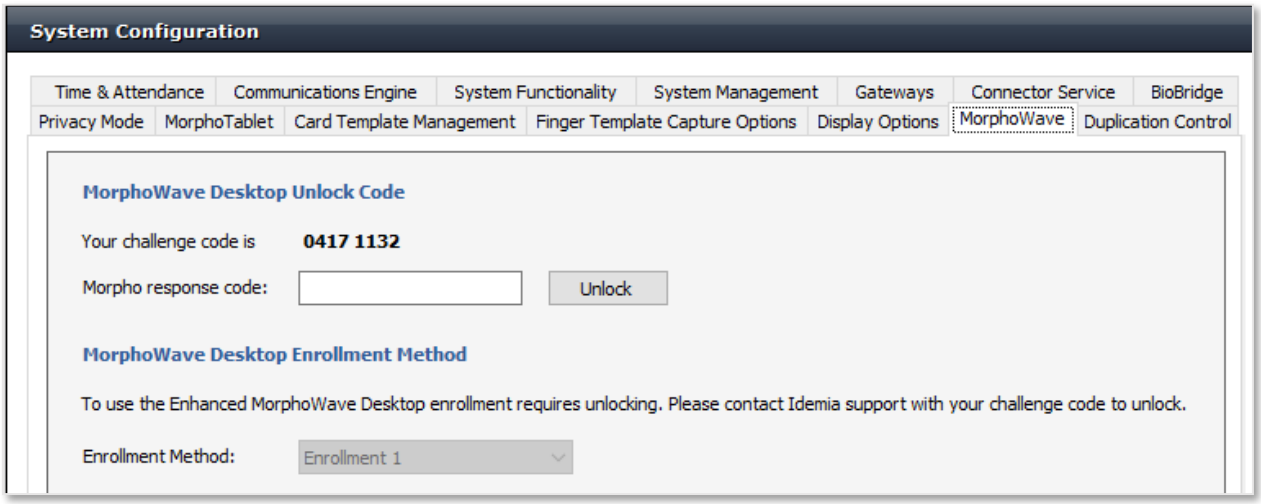
Store WSQ image: Stores the WSQ image of the fingerprint in case it was captured from a MSO USB enrollment device. A license is required for this option.

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



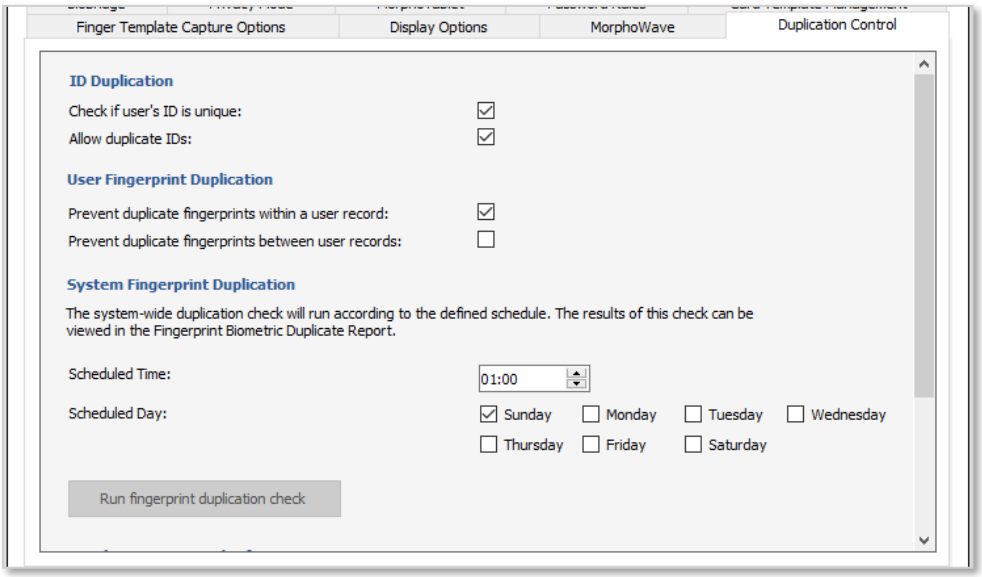
MorphoWave Unlock

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

User Management

This setting can only be unlocked with an unlock code obtained from Morpho 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.

An IDENT and VERIF license, on the MorphoManager server, is required to prevent duplicate fingerprints between user records.

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.

An IDENT and VERIF license, on the MorphoManager server, is required to prevent duplicate fingerprints between user records

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.

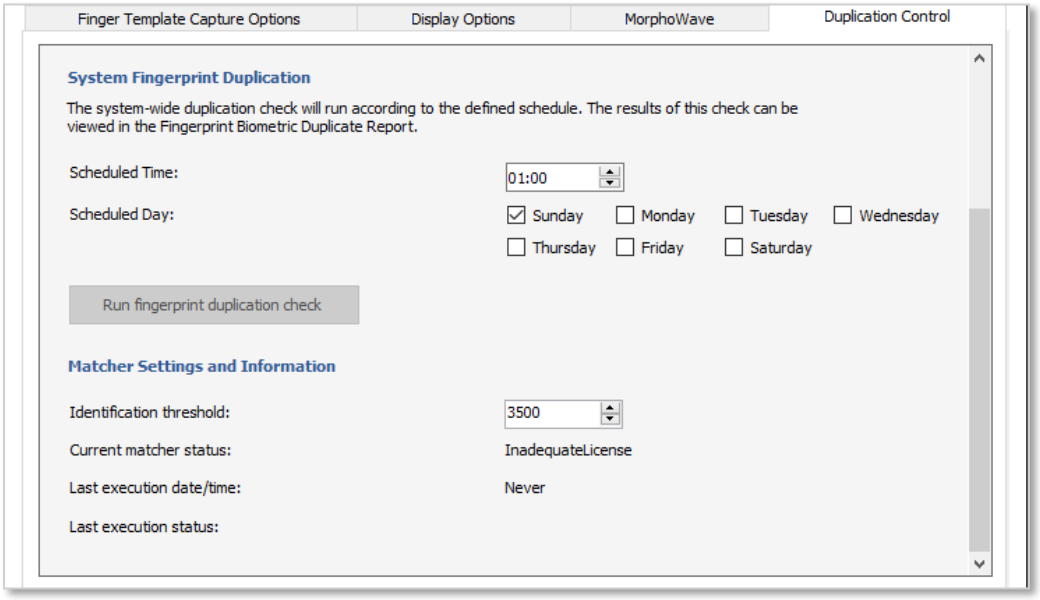
Results of the search can be viewed in the Fingerprint Duplicate Report.

An IDENT and VERIF license, on the MorphoManager server, is required to run the matcher (duplicate search).

De-duplication with face templates is not available.

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.

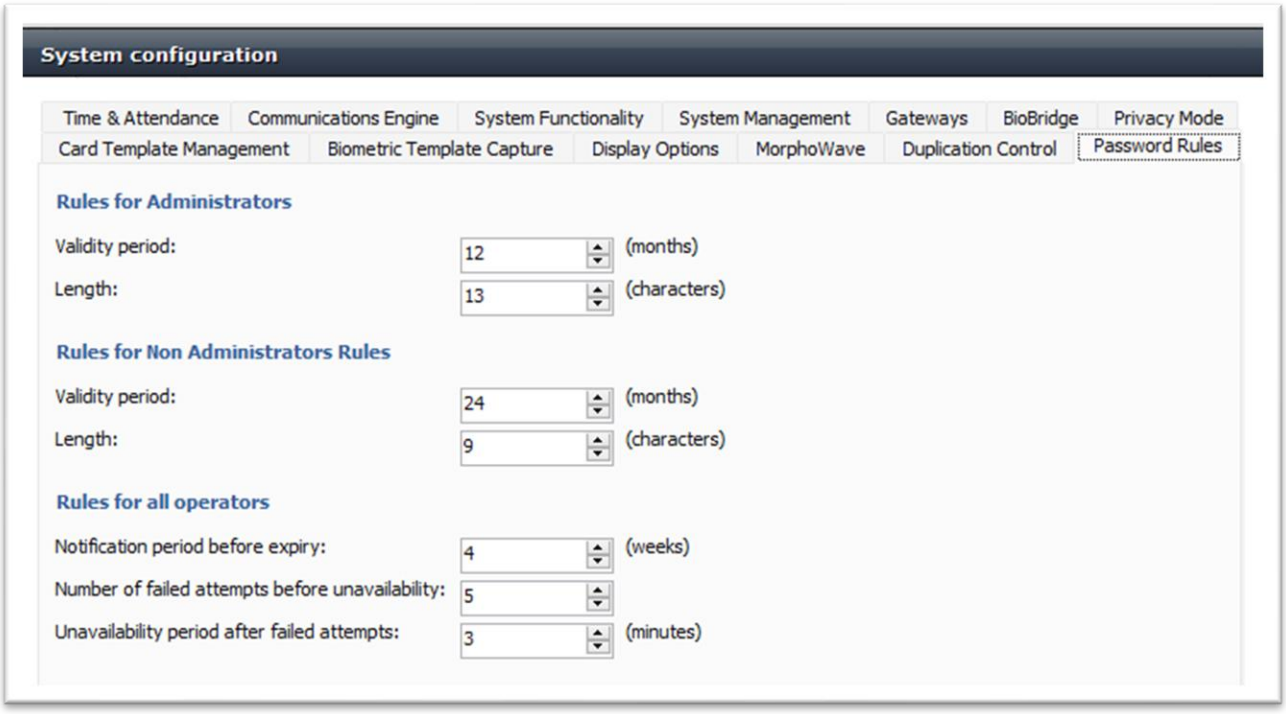
Current matcher status
The Current status of the matcher.

- **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.

Password Rules



Rules for Administrators
These settings are in place to configure rules for administrator accounts with respect to password validity and length.
Password validity range from 1 month to 36 months. The default value of password validity is 12 months.
Password length range from 9 to 256 characters. The default value of password length is 13 characters.

Rules for Non Administrators
These settings are in place to configure rules for non-administrator accounts with respect to password validity and length.
Password validity range from 1 month to 36 months. The default value of password validity is 24 months.
Password length range from 9 to 256 characters. The default value of password length is 9 characters.

Rules for all operators
These settings are in place to configure generic rules for all operators with respect to :

- Notification period before expiry : Configuration for password renewal notification. Range from 1 week to 3 months (default value will be 4 weeks)
- Number of failed attempts before unavailability : Configuration for number of failed attempts before account locked. Range from 1 to 10 (default will be 5)
- Unavailability period after failed attempts : Configuration for setting time period for which account will be unavailable. Range from 3 to 15 minutes (default will be 3 min)

The password must contain Uppercases, Lowercases, Numbers and Symbols. Username cannot be used as a password.

Password Renewal

All MorphoManager operators shall be required to change their password after a certain period of time which can be configured with the help of validity period. For this purpose, they will be prompted with a renewal notification.

If the password is not renewed one week after the expiration, the account is disabled and shall be re-enabled by an administrator.

Note: passwords can be renewed or reset (by and administrator) at any time.

From version 16.5, below mentioned additional messages will be displayed in case of :

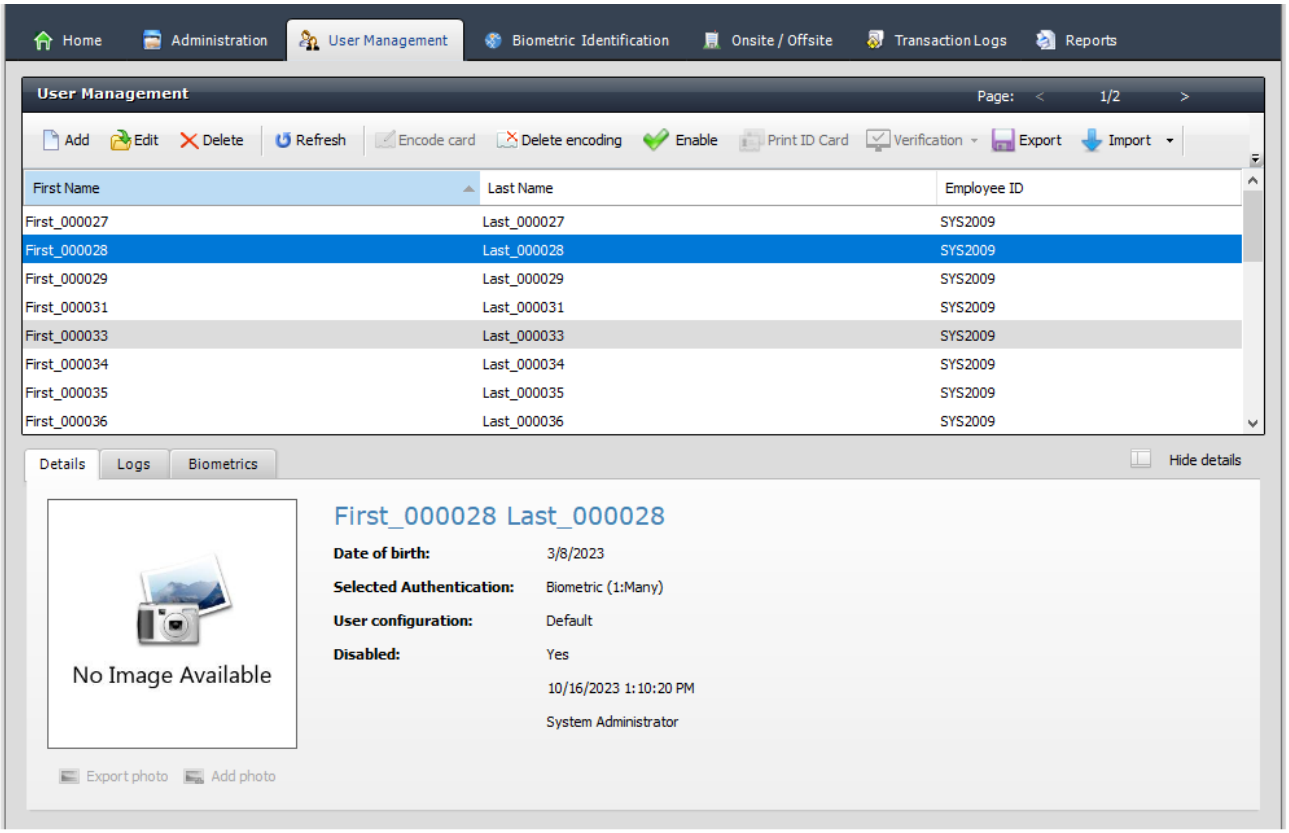
- *Inactive account* : Your account is inactive, please contact administrator or support team.
- *Entered Incorrect password* : Invalid password, 'X' attempts remaining.
- *Locked account* : Your account is unavailable for 'X' minutes. Please wait.
- *Automatic Login* : Don't forget to update the password inside Client Configuration tool for automatic login

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.

MorphoManager supports up to 100,000 users.

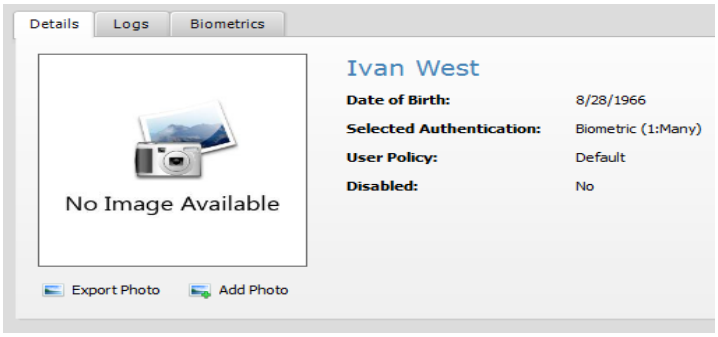
25 users are displayed by default in the User Management list. To increase this default value up to 250, please change the configuration in System Configuration > System > User Management.



User Details

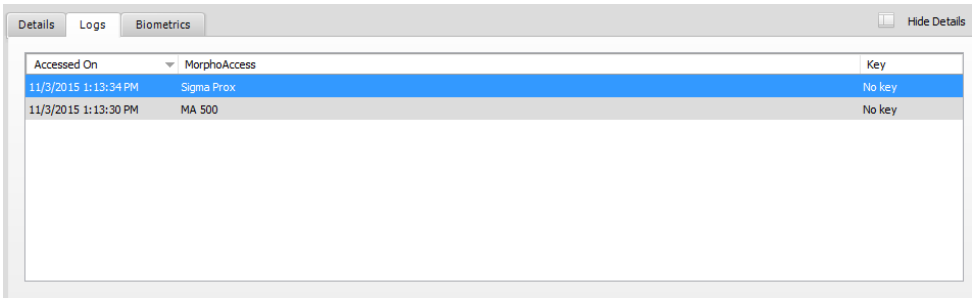
Information about a user's Details, Logs, and Biometrics is available when a user is highlighted in the list of users.

Details:

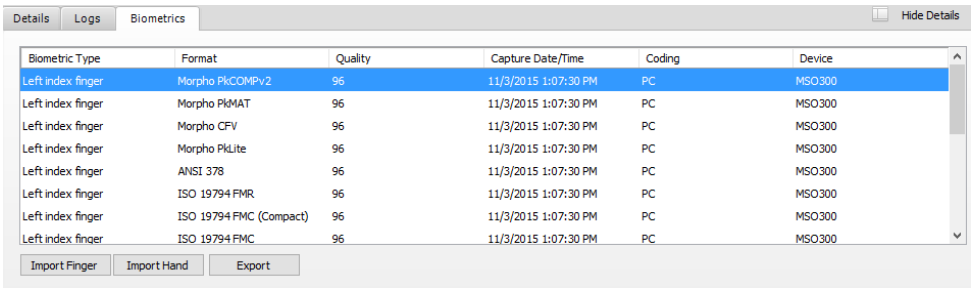


If a user has been Disabled, their disabled date and the Operator who disabled them will appear on the Details tab.

Logs:



Biometrics:



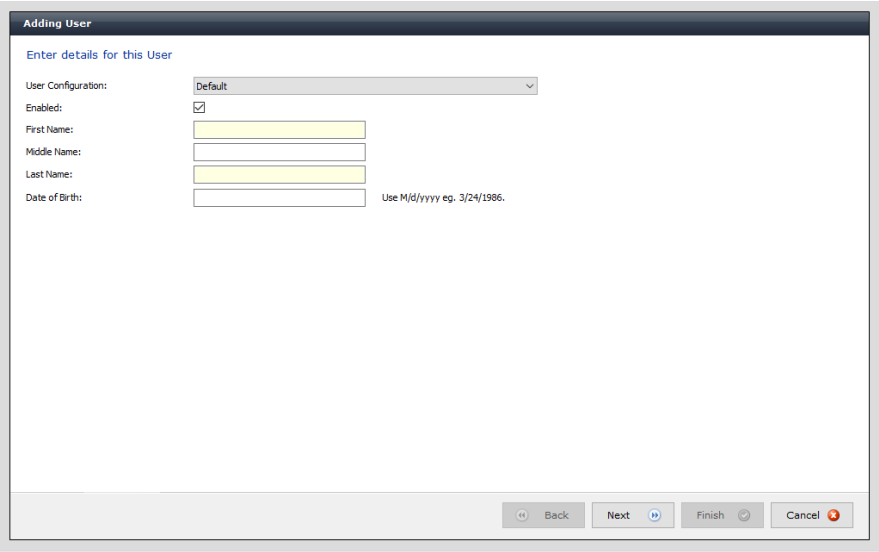
The templates captured for the user will be shown. Templates for the user can be Exported and Imported from this screen.

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 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.

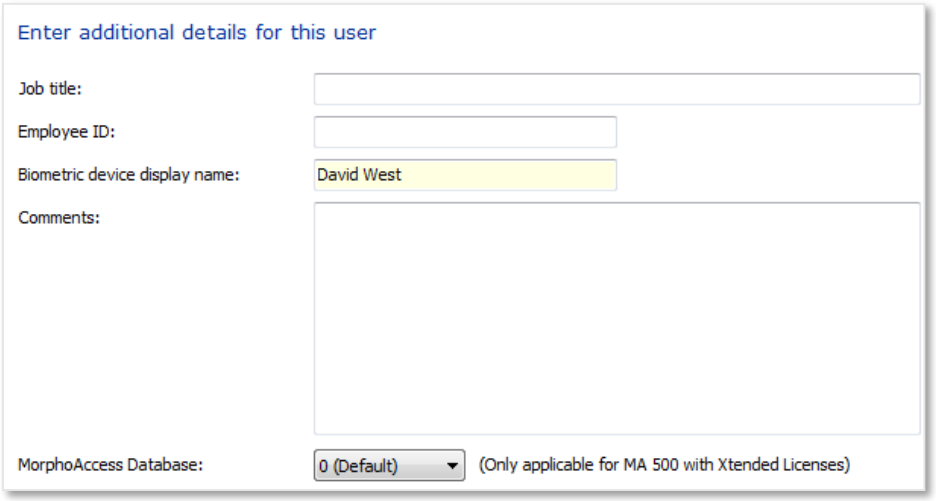
First Name: User's first Name **(Required)**

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



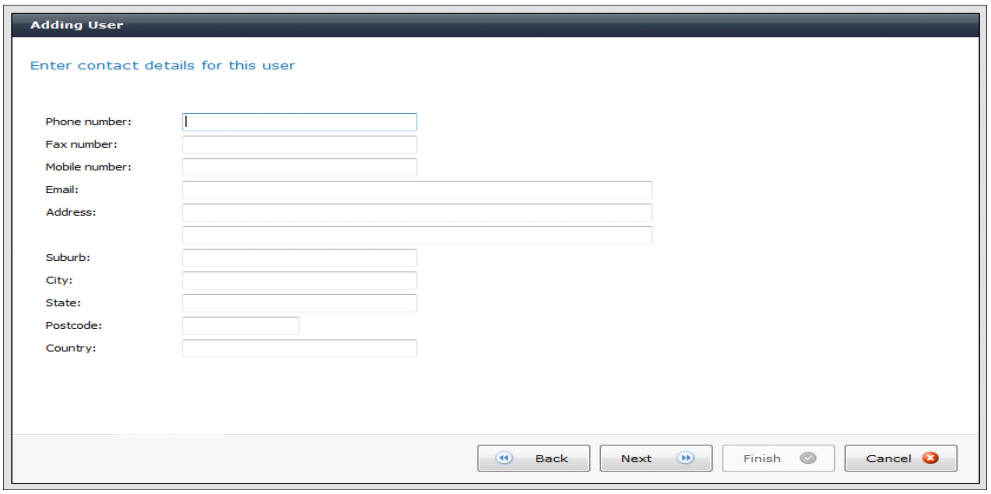
Job Title: The user's job title.

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

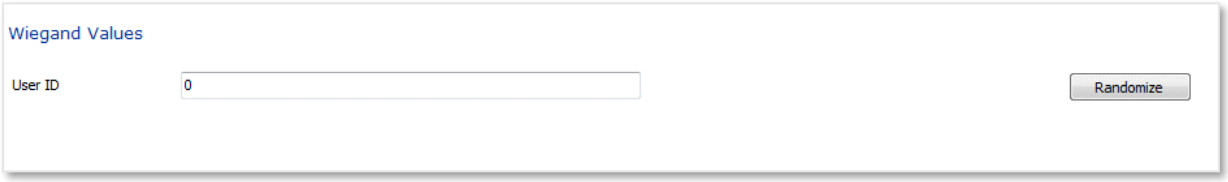


This page and the User Defined Fields page to follow are only visible if "Display Extended User Configuration details" has been enabled on the selected User Configuration. If so, enter the details for the selected user.

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.

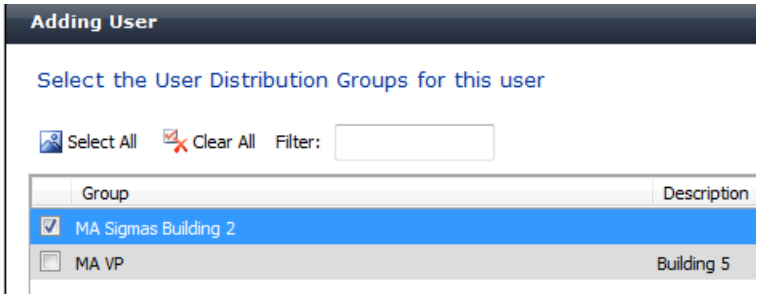
Screen 5 – Wiegand Values (If a Wiegand Profile is set)



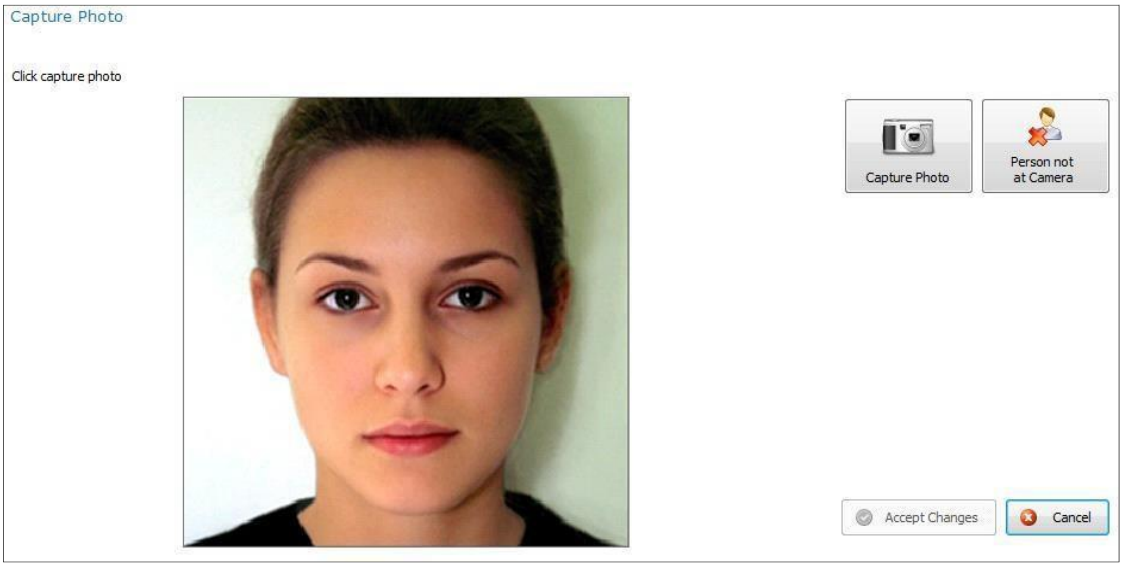
The User ID can be put in manually or by utilizing the Randomize button. This screen is only available if you have changed the User Configuration to have a Wiegand Profile set, rather than leaving the default setting of "Automatically generated random 64 bit". Additionally, a Read Card Serial Number 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.



Screen 7 – Photo Capture

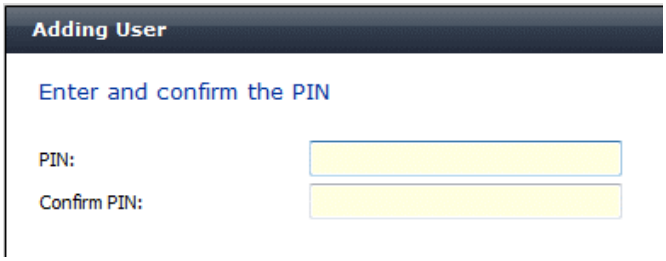


Position the person in front of a plain background so that all their face is visible in the picture, like a passport photo. Once the user is positioned correctly click **Capture Photo**. Click on the image in the top left corner and drag towards the bottom right drawing a square around the part of the 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.

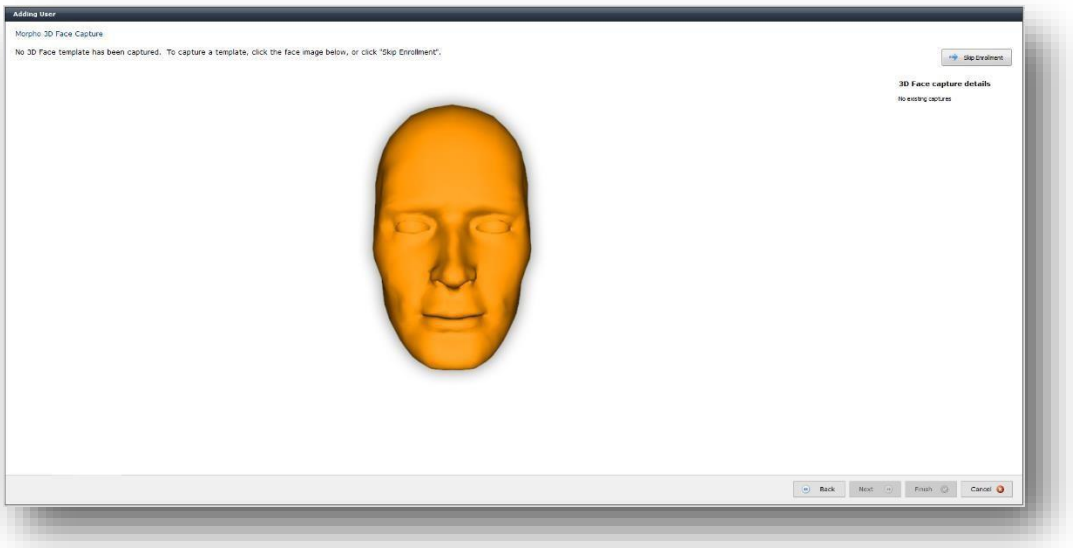
If the photo is not acceptable, click **Update Photo** to recapture the photo. Photos can be imported and exported using the corresponding buttons. Additional configuration options for the camera can be changed by clicking on **Configure Camera**.

Screen 8 – PIN Code



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

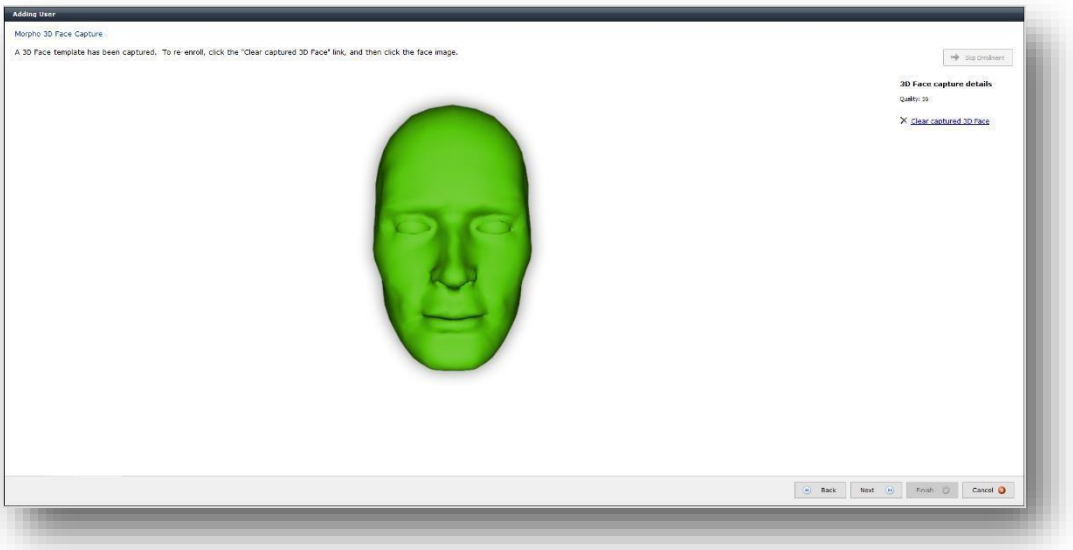
Screen 9 – 3D Face



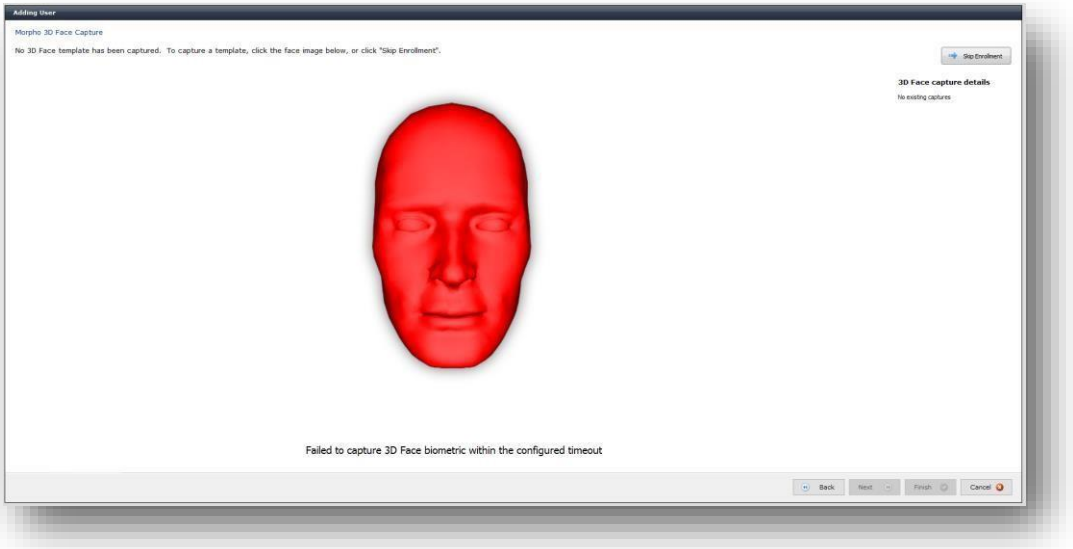
The 3D Face reader will scan a user's face and capture a 3D rendering of the image. To scan a user's face, align the face on the device until the device indicates the face has been recognized.

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

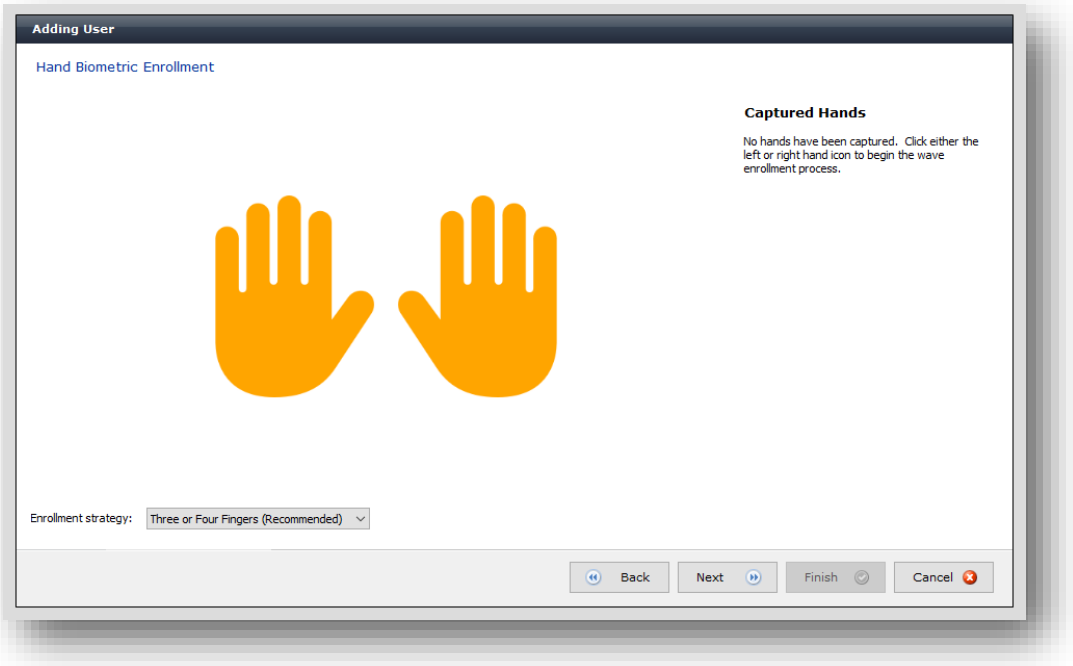
When a scan is successful the image below is seen.



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



Screen 10 – Wave Enrollment

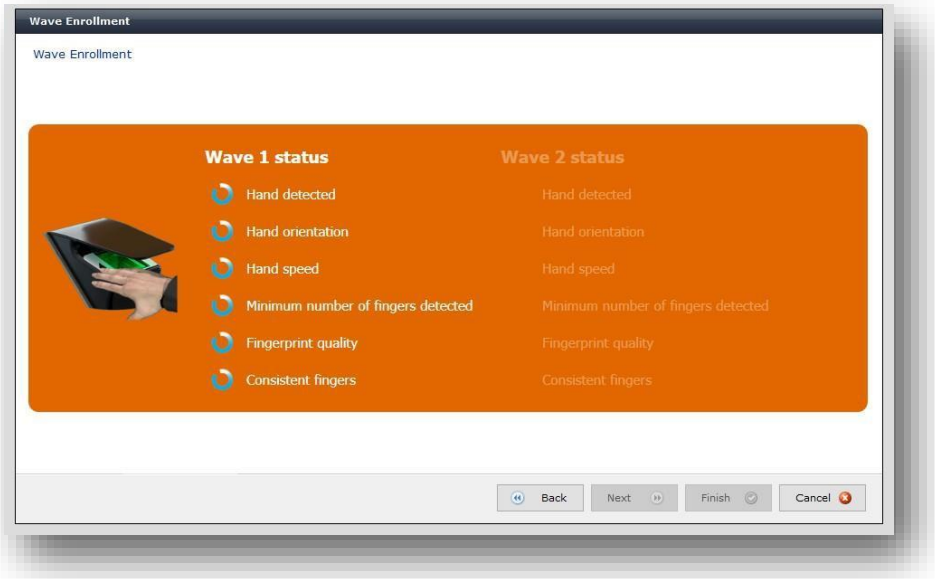


The number of hands required for full enrollment of the user is dictated by that setting in User Configuration. To start the captures, click on one of the hands.

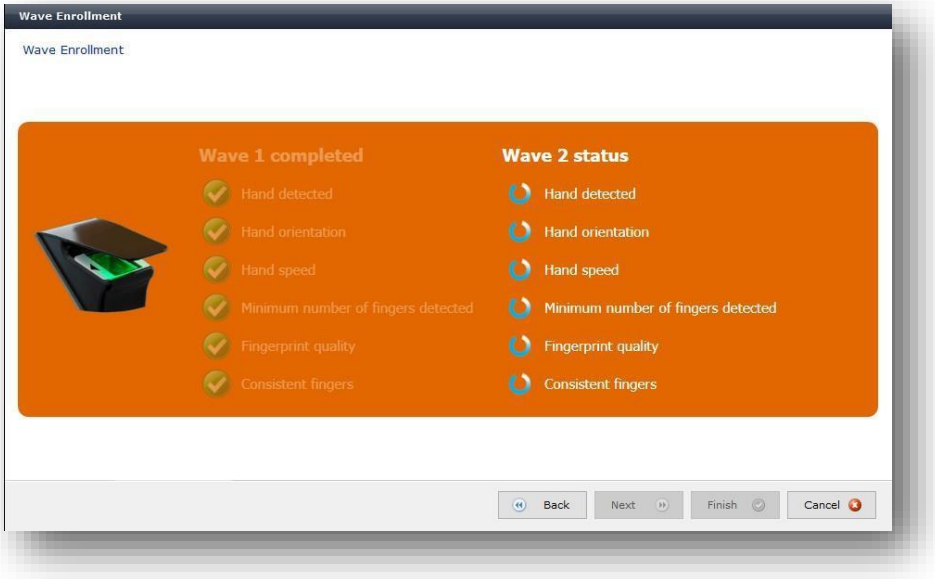
If either of the following conditions occurs a “No Device” message box will be displayed when you select a finger to enroll:

- 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.

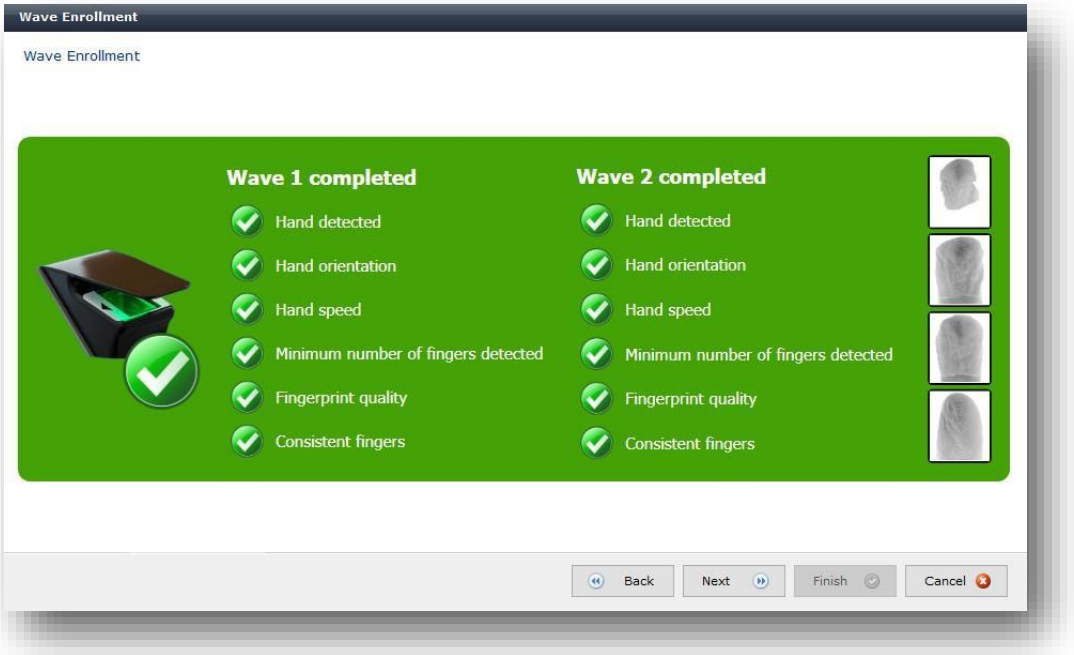


Move your hand through the Wave sensor which should now be illuminated. You will then see the results of Wave 1 appear on screen. If it is successful, you will then be prompted to present for Wave 2.

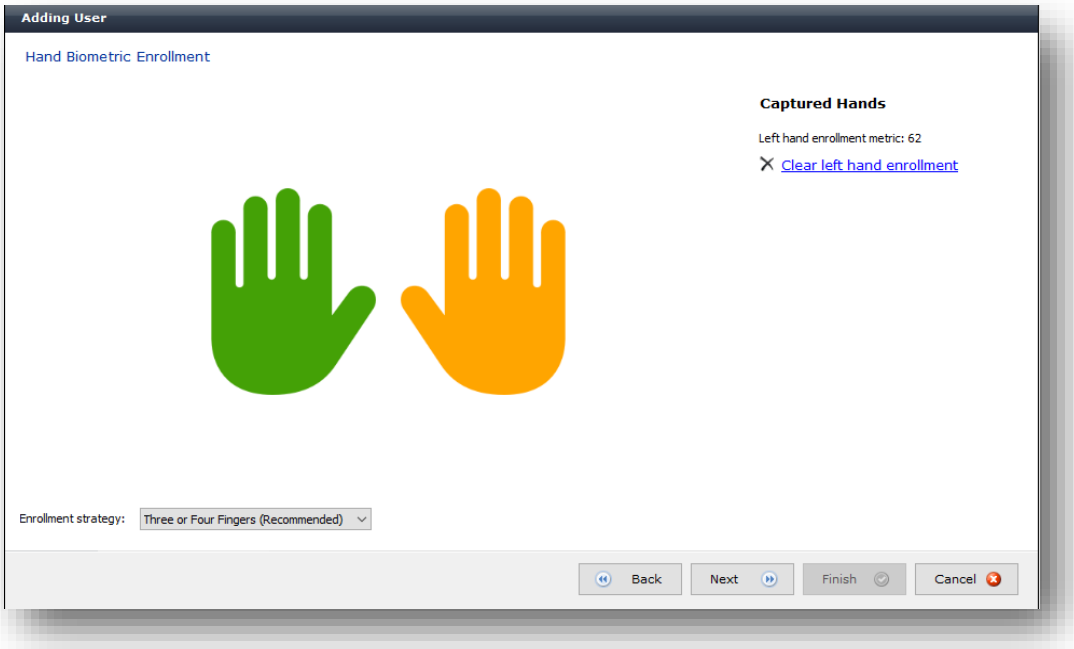


If it is not successful, you will see a red X in the elements of Wave 1 that were not successful. Move your hand through the sensor again until Wave 1 is completed.

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

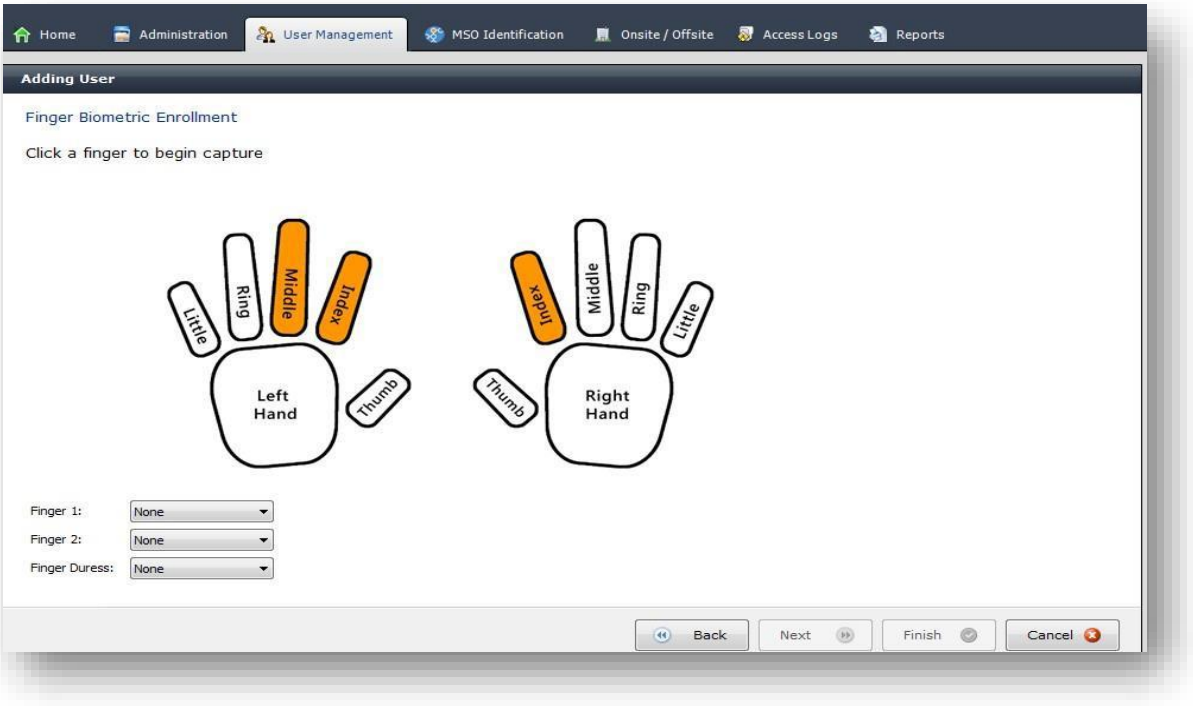


Once the enrollment is complete for Wave 1 and 2, click **Next**. The screen below will appear showing captured hand and quality displayed on the right. In the event a user is not being recognized at any MorphoWave Device, click **Clear <*enrolled finger*> finger enrollment** to allow re-enrollment.



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.

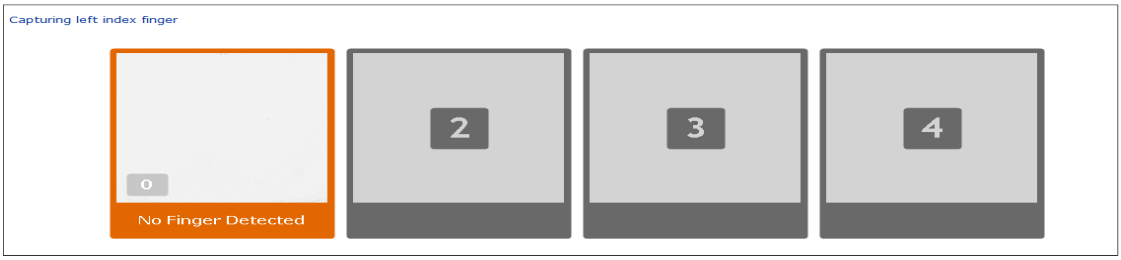


The default fingers that the system suggests you enroll are set at the User Group level and are flashing orange. You do not need to use these fingers as you can click on others. However, you will need to set at least Finger 1 from the respective drop-down list after fingerprint capture.

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.

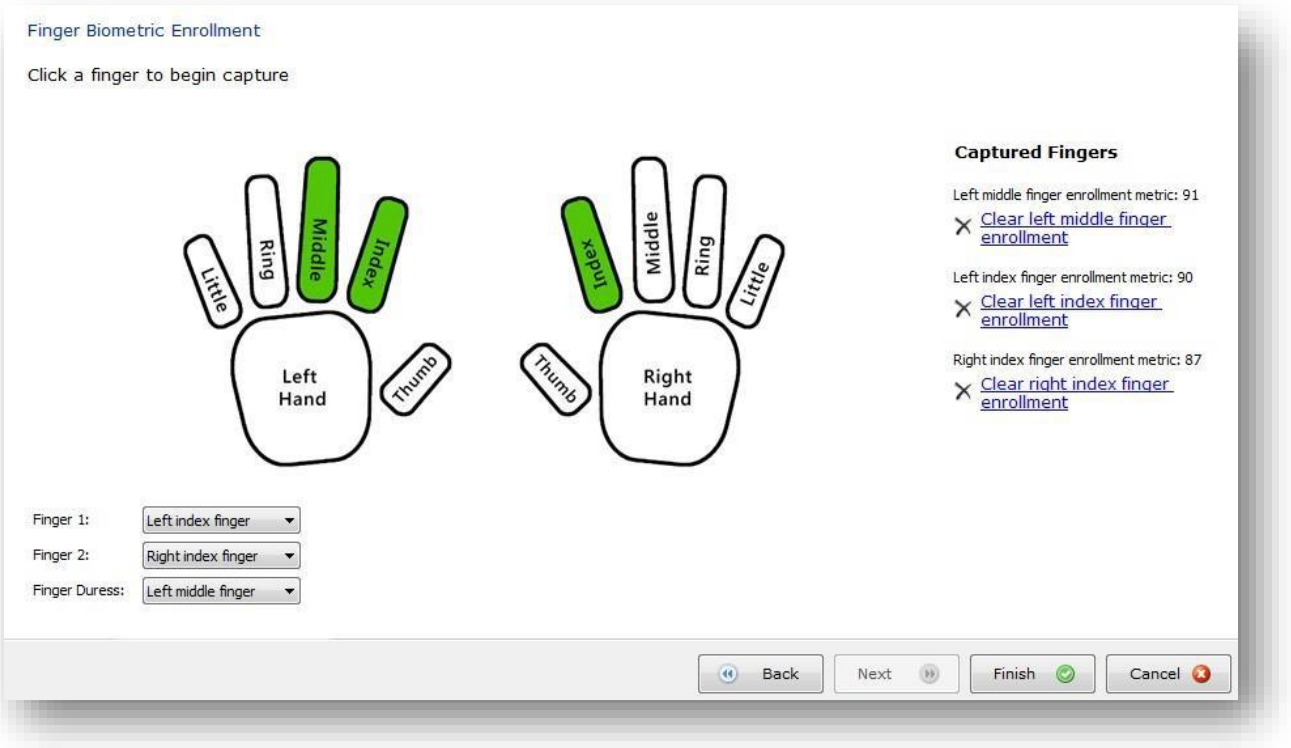


Click on a finger and have the user place their finger in the center of the scanner glass. You will then see the print appear on screen. There are four scans performed on each finger; the first three are used to create the biometric template. The system selects the best elements of each print and consolidates 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.

The real fingerprints as acquired by the MorphoWave device during enrollment can be hidden from screen. Use this feature with care, as bypassing the visual inspection of enrolled fingerprints may reduce the biometric performance of the system. It is enabled by adding the below parameter in the Server configuration file:
<ShowPrints>false</ShowPrints>

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

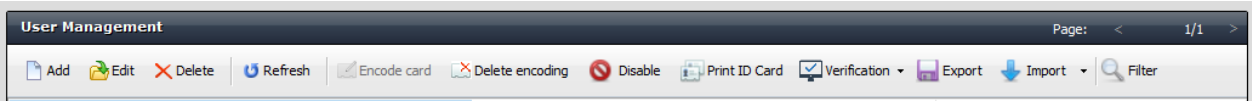
In this example the captured finger has a large amount of oil on it and pressure was quite high on the reader lens. This will probably work okay but is not ideal. A user needs well defined ridges and troughs as well as intersection points in the print. These sites are the matching points used to develop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

Figure 5

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

User 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.

Encode Card

Use to encode presented smartcard with user data.

Delete Encoding

Use to remove encoded data from smartcard and available with below 2 options:

- Reset Card: Delete all data written by MorphoManager and reset all configuration modified by MorphoManager on detected card.
- Erase User Data: Erase all user data (demographic and biometric data) written by MorphoManager on detected card – for MiFare DESFire cards only.

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.

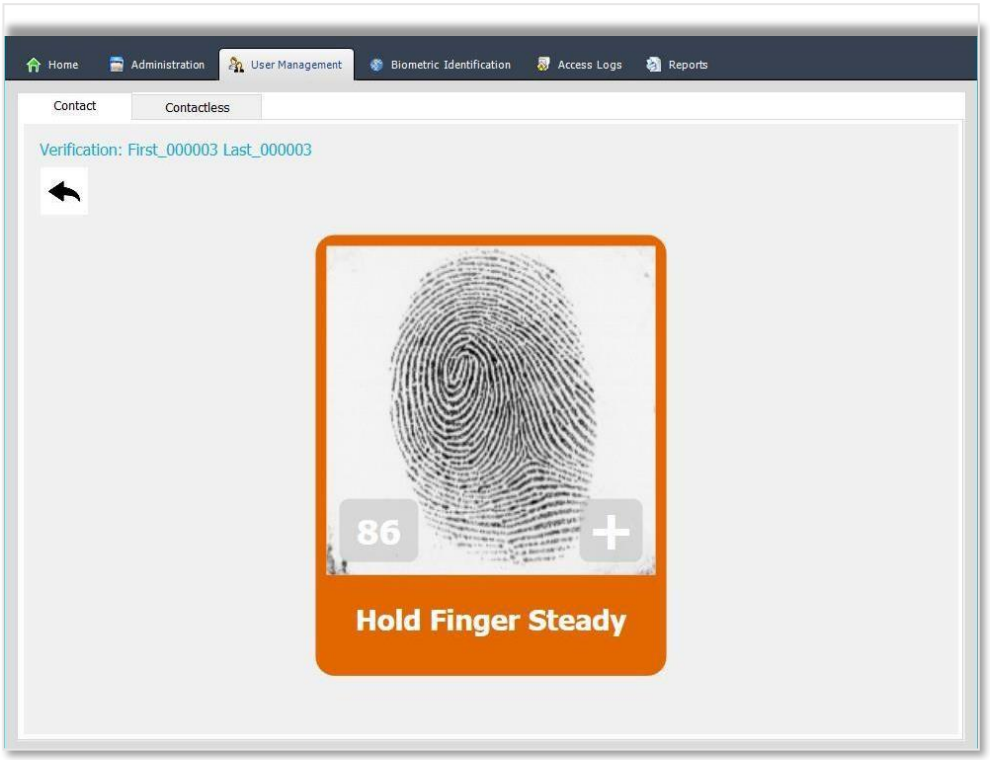
Verification - Database

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**.

The number of users displayed cannot exceed the valued defined as "Numbers of users per page" in the System configuration menu.

Filter inside User Management tab is used to filter out users on the basis of User Configuration Access Mode and its respective User Distribution Group.

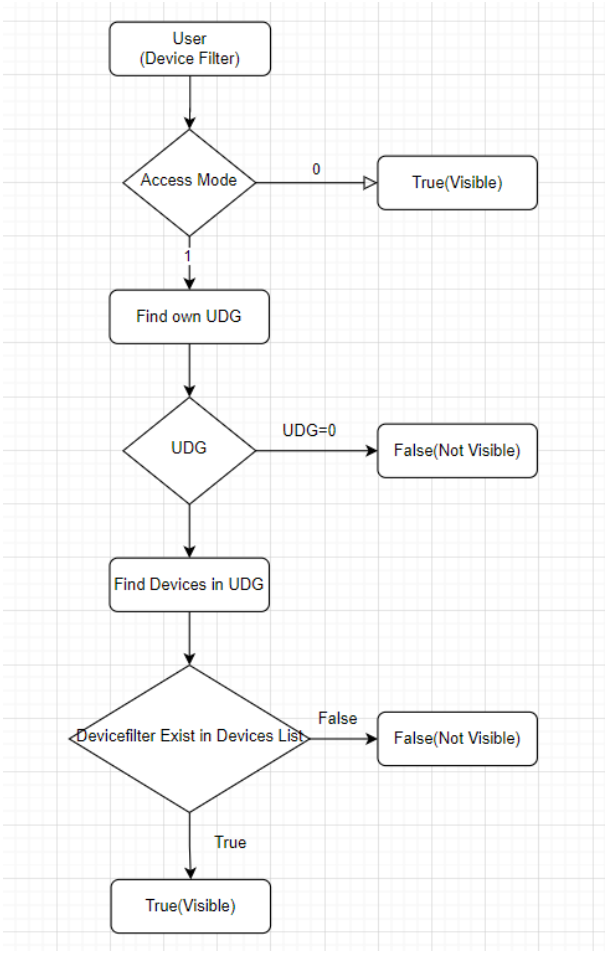
User will be filtered out on the basis of below checks :

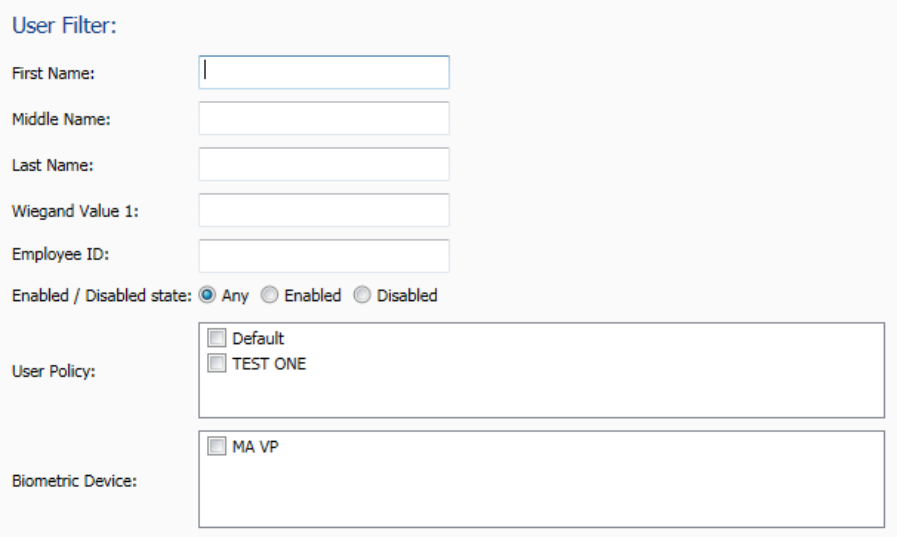
- User configuration access mode
- User Distribution Group

Steps for filtering users based on *"Biometric Device"* Filter:

- Step 1 : Validate whether User Configuration Access Mode is
  - 0 : All Biometric Device and Clients
  - 1 : Per User
- In case,
  - if Access Mode is '0' then it will show related User without checking for further validations
  - if Access Mode is '1' then it will go for further validations and check for User Distribution Group
- Step 2 : Validate whether User Distribution Group is mapped with that user or not
  - If UDG is not mapped, then it will not show the related User
  - If UDG is mapped, then it will go for further validations and check for selected biometric device
- Step 3 : Validate whether selected biometric device from filter is available in that specific UDG or not
  - If device not exist in UDG, then it will not show the related User
  - If device exist in UDG, then it will show the related User

Flow Diagram:





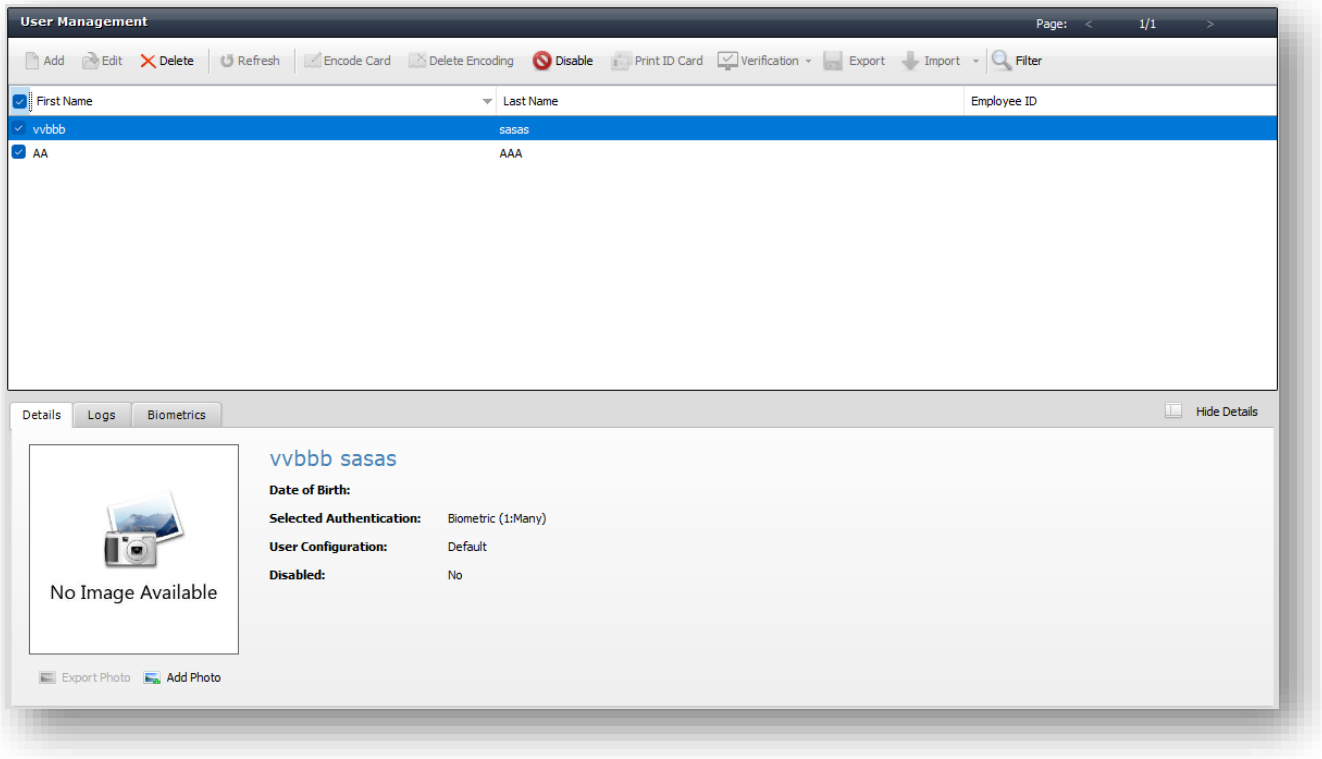
Actions on multiple users

Below is the list of operations that can be done simultaneously on multiple users:

- Delete

- Disable/Enable
- Filter

To select multiple users, use the tick box on the left-hand side of the panel. The top tick-box allows to select all users.



Actions on multiple users may require significant processing and time. IDEMIA recommends performing them during idle periods of the system.

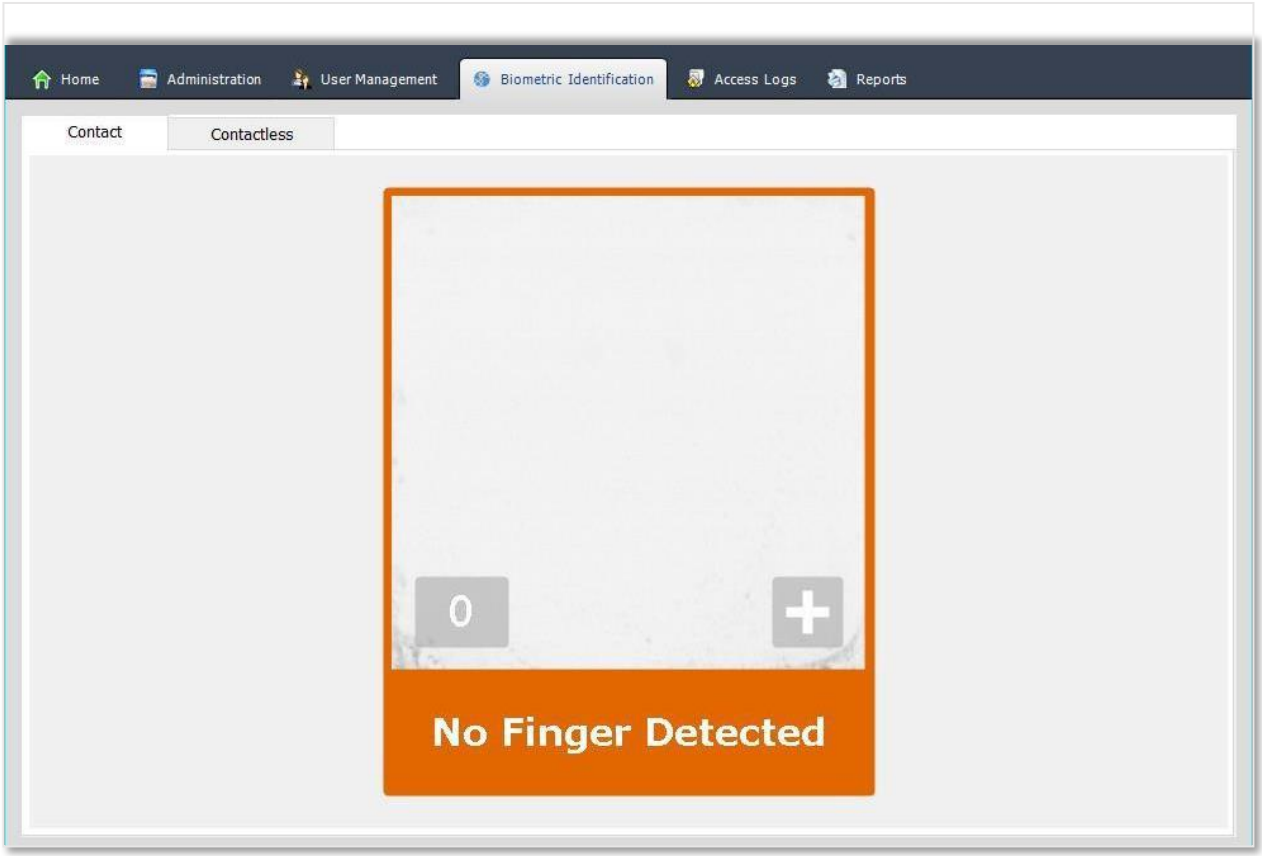
Biometric Identification

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.

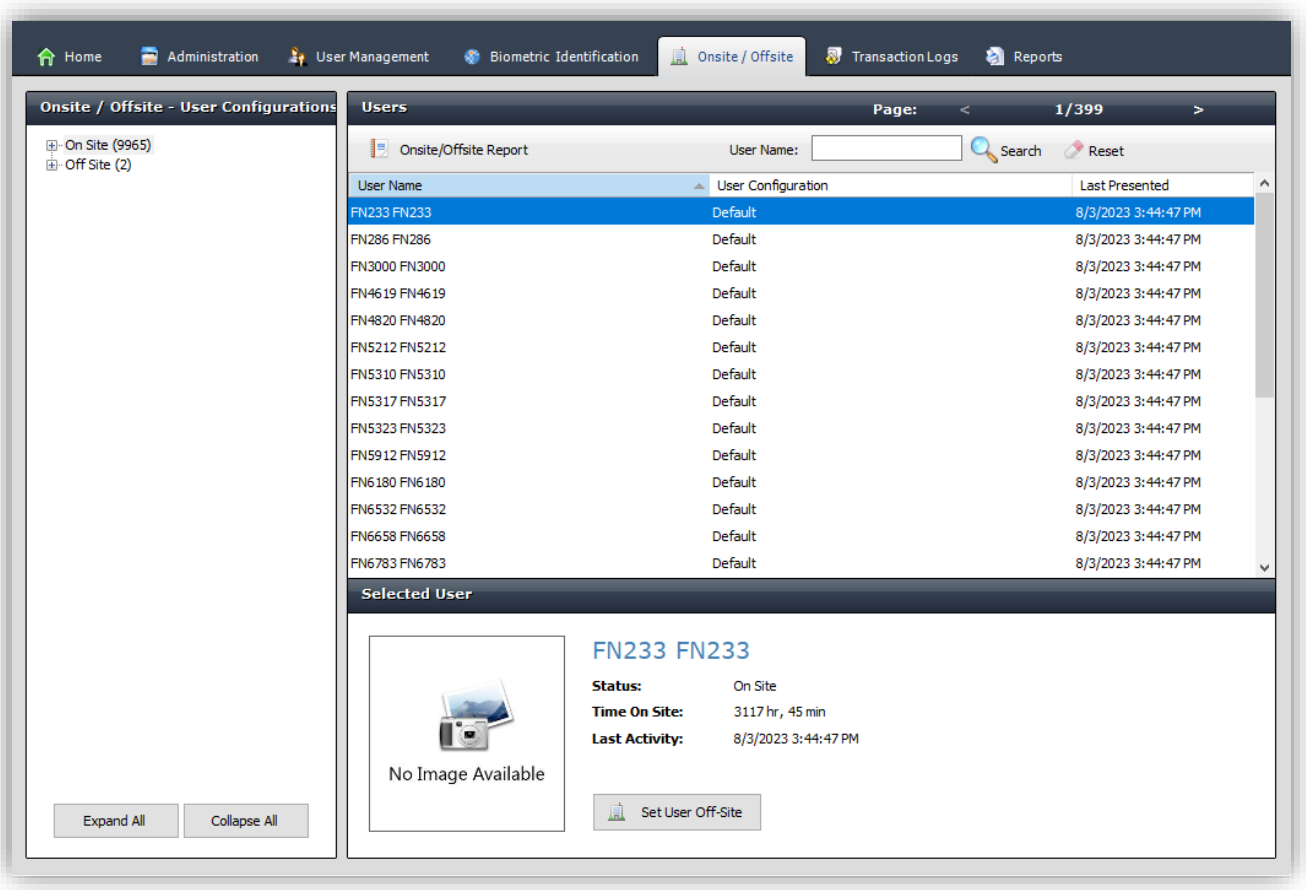
Onsite/Offsite

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.

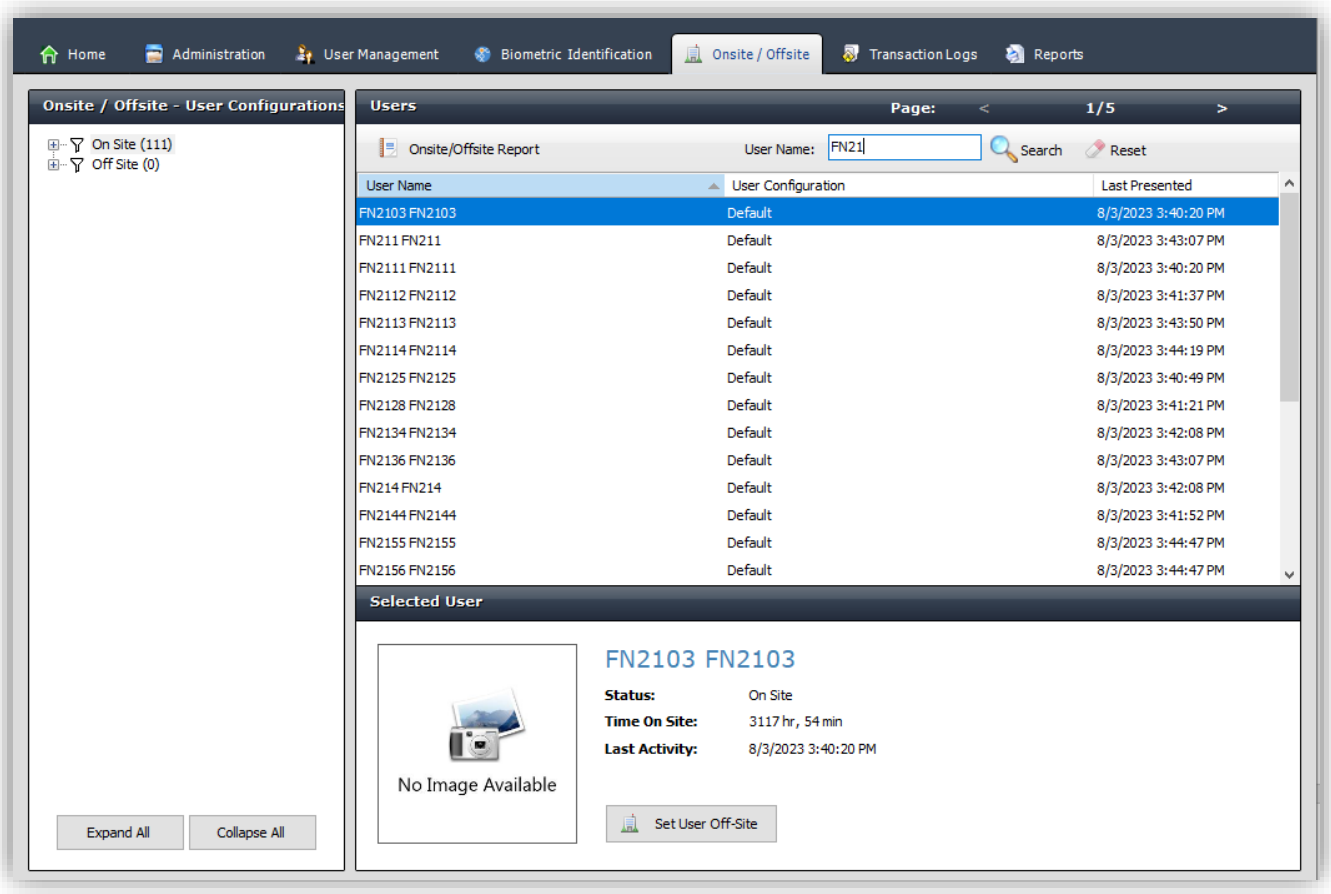
The Onsite section is used to show which users are currently onsite or offsite. The Onsite and Offsite items in the tree view on the left can be expanded to show user groups.

By default, total of number of user count visible inside the tree view of OnSite/OffSite parent nodes and Onsite parent node will be selected and its related user display according to page size configuration.

25 users are displayed by default in the Onsite/Offsite display grid. To increase this default value up to 250, please change the configuration in System Configuration > System Functionality> User Management.



User can be filter with the help of Search button and the same filtered user value will be reflected on tree view with filter icon as shown :



Filter can be removed with the help of Reset button.

Reports of Onsite/Offsite users can be fetched anytime with the help of “Onsite/Offsite Report” button.

NOTE:

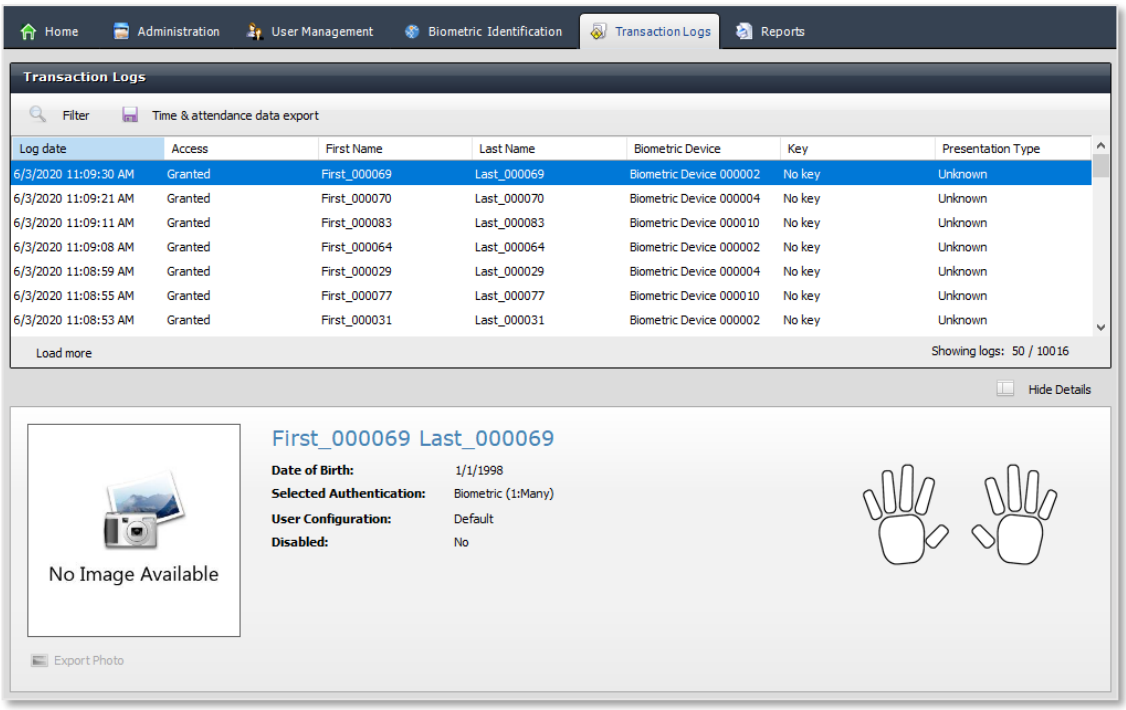
To manually set a user onsite/offsite, click on the User in the Main screen and click on **Set User Off-Site** or **Set User On-Site**.

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

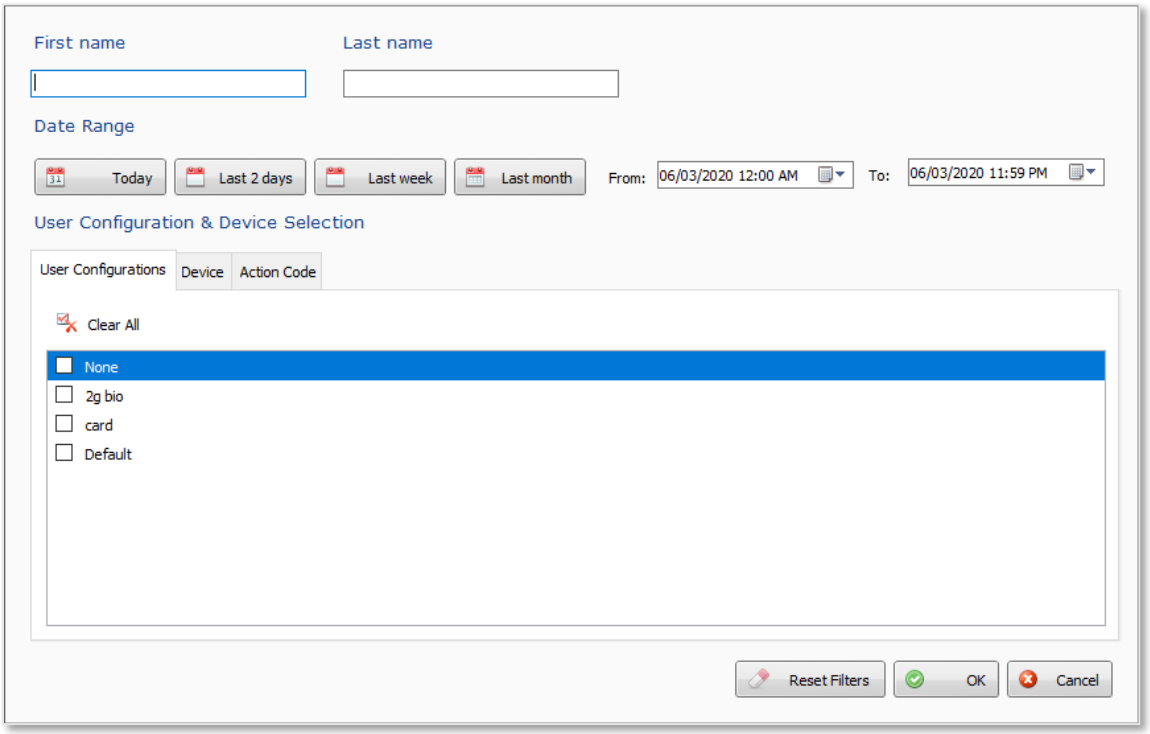
Status of users inside Onsite/Offsite tab will be updated as per the identification done with related function key.
In case, if TNA mode and its respected function keys are not configured inside BDC then user identified with biometric device will fall directly in Offsite state/mode.
But in case if TNA mode and its respected function keys are configured inside BDC then user identified with biometric device will fall in Onsite or Offsite as per selection of entry or exit function keys.
For example, if entry function key selected then user fall in category of Onsite and if exit function key selected then user fall in category of Offsite.

Transaction Logs

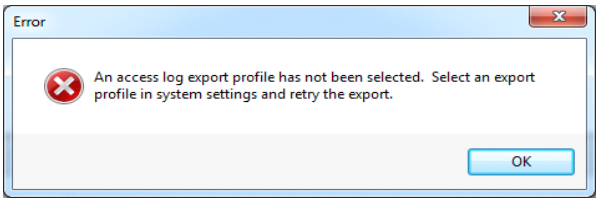
An access log is a record of transactions recorded by the system.



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.

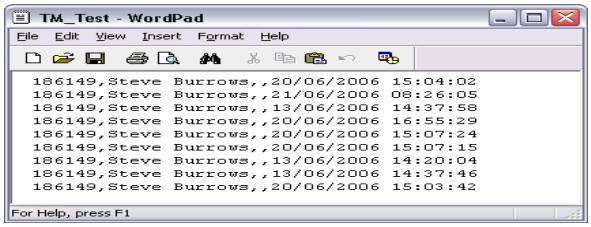


Refer to the system configuration section for instructions on configuring an access log export profile.

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 duplication 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 duplication 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.

NOTE : Please note that the "Fingerprint Biometric Duplication Report' feature will be removed in a future MorphoManager version.

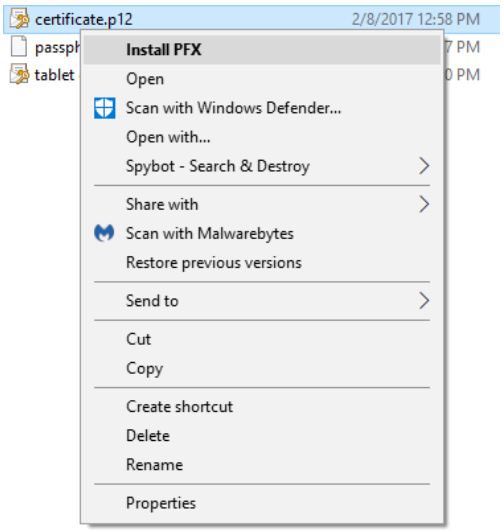
Windows Certificate Store

Please note, this section will be only required for below mentioned use cases :

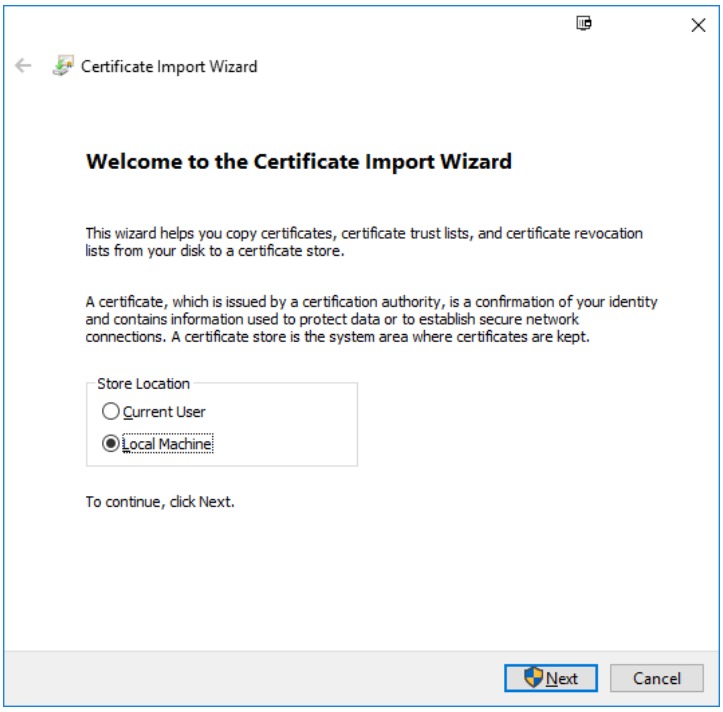
- MorphoManager – Upgrade to Enforced Security – Imported Certificate (without TLS)
- MorphoManager – Install Enforced Security – Imported Certificate

Importing a Certificate to the Store

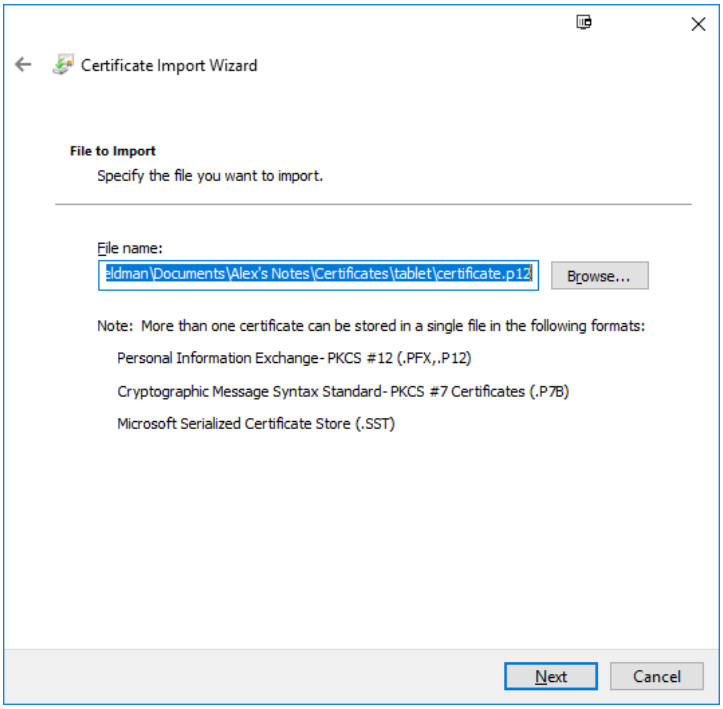
Begin by locating the certificate to be placed in the certificate store. Right click on the certificate and choose the **Install PFX** option.



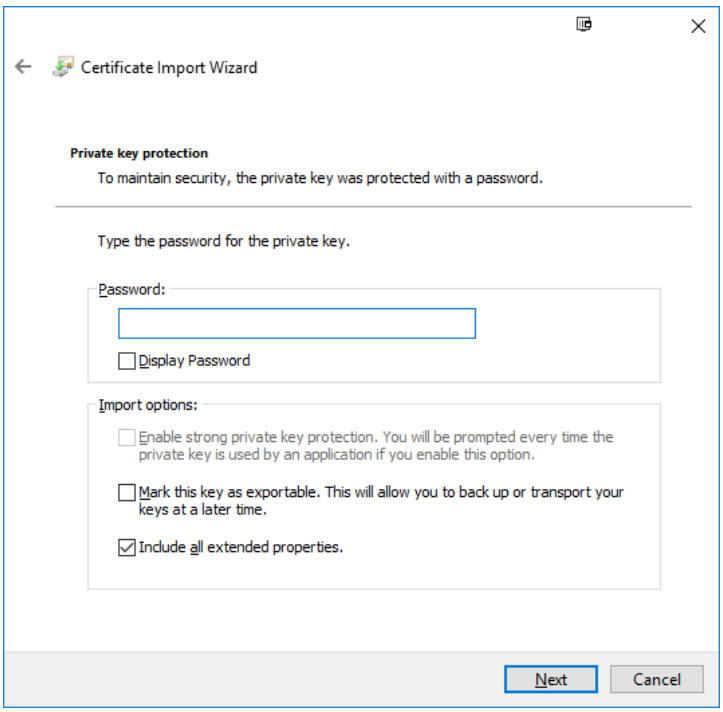
A Certificate Import Wizard will appear. Under the Store Location option, select Local Machine and click Next.



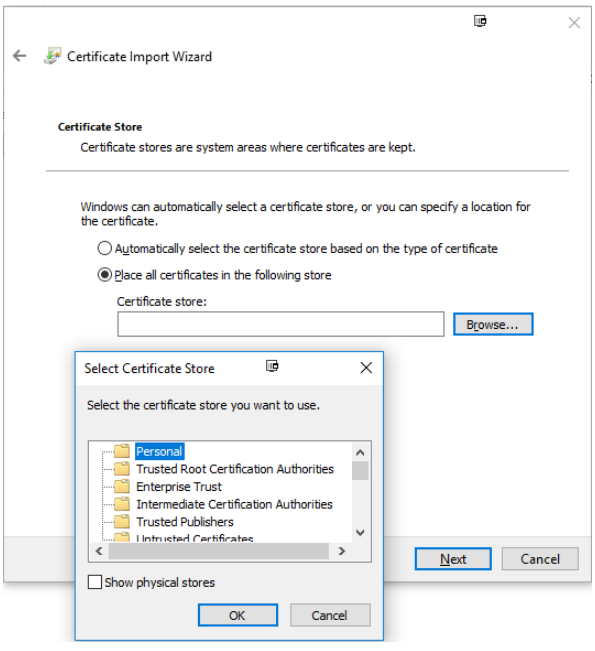
The next page will allow you to specify the file to import. The location of you certificate should already be provided in the File Name field space.



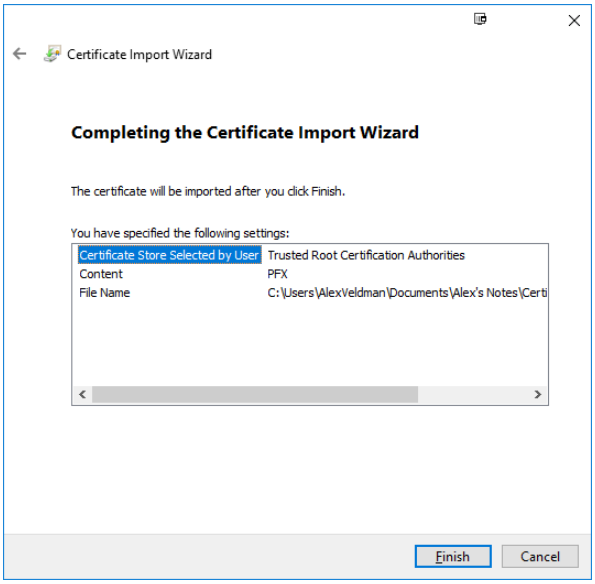
Next, enter the certificate's password. This is the password that should already be associated with the certificate, not a new one. Check any additional import options that may be applicable.



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.

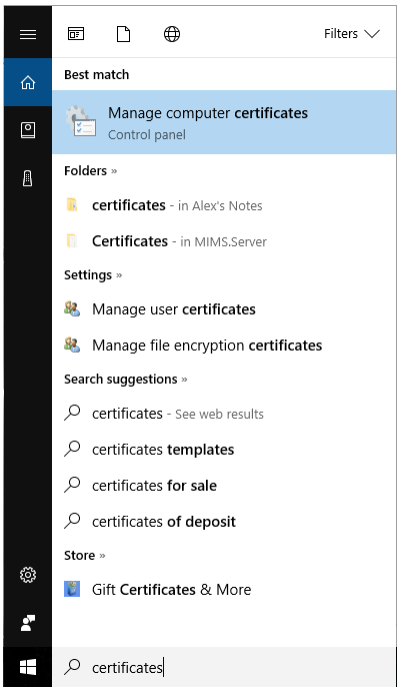


Finally, ensure that the information provided on the last screen is correct and click the Finish button to begin the import process. Once complete a prompt will appear informing you that the import was successful.

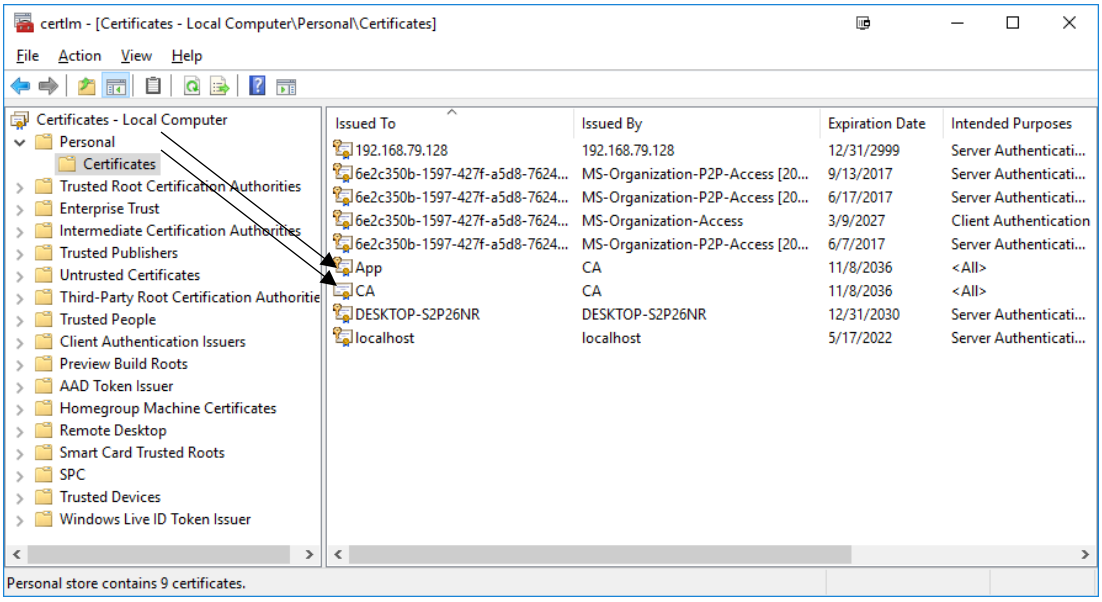


Checking the Certificate Store

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, except Import and Export functionality, which are built in the MorphoManager Graphical User Interface.

Export and Import

MorphoManager can export various types of data:

- Key Policy
- Biometric Device Configuration
- Wiegand Profiles
- Access Schedule
- User Authentication Mode
- User Management

These data can then be imported into another MorphoManager installation.

Data exported from a version (e.g 14.6.0) of MorphoManager cannot be imported into another version (e.g 15.X) of MorphoManager.

If you need, for instance, to transfer data from a production installation with version X to another production installation with version Y, the recommended path is the following:

- Export data from the production installation with version X
- Install a test system with version X
- Import data in the test system
- Upgrade the test system to version Y
- Export data from the test system
- Import data in the production installation with version Y

1. When exporting a Biometric Device Configuration, the export file may contain confidential data like a password. Please make sure to protect confidential data appropriately.
2. Only Custom defined Access Schedules can be exported. The system defined Access Schedules i.e “No Allowed Time” and “24hours,7 days a week” cannot be exported.
3. Users can be imported in xml (for single) or csv (for multiple) format.

Biometric Device Configuration Creation Tool

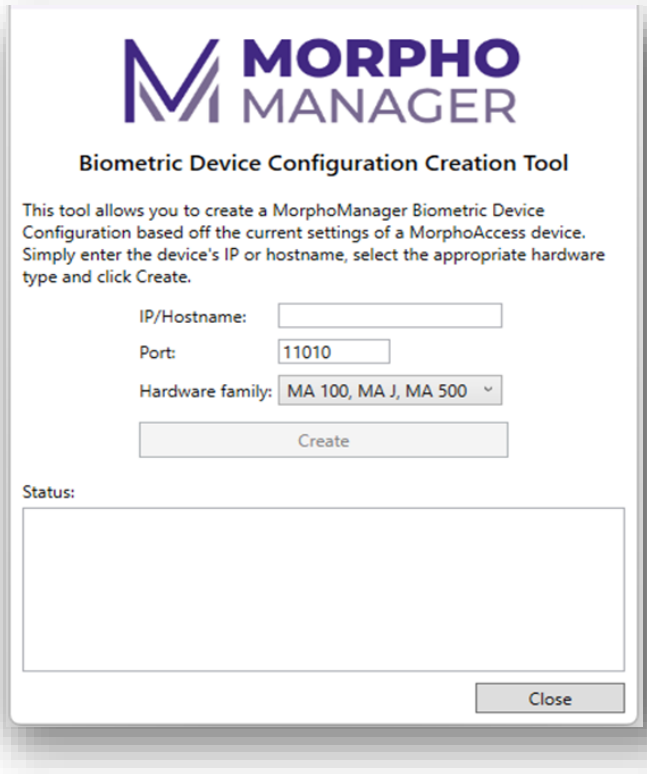
This tool will allow you to generate a Biometric Device Configuration from MA2G or MA5G family parameters that are set on a device. The data will be collected, and a file created that can be imported into MorphoManager to utilize as an advanced BDP.

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

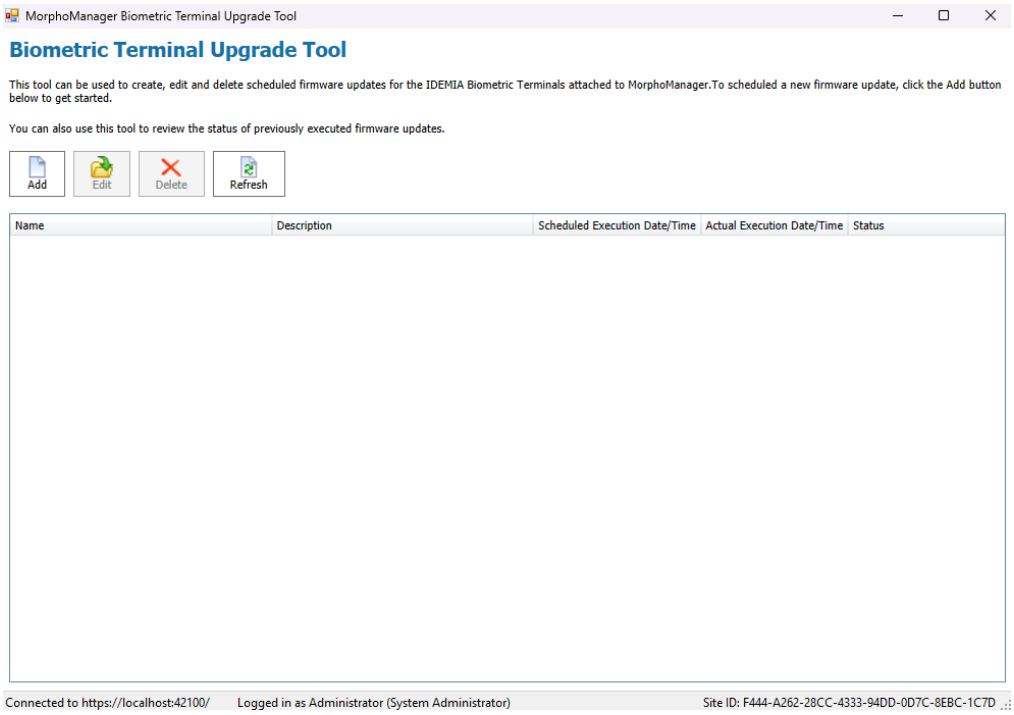
Hardware Family: There are two options in the drop down.
MA 100, MA J, MA 500, or MA VP
MA Sigma



Biometric Terminal UpgradeTool

The Firmware Upgrade Tool is designed to be used for the following biometric terminals: SIGMA Range (5G), MorphoWave Compact / XP, MorphoWave SP, VisionPass and VisionPass SP.

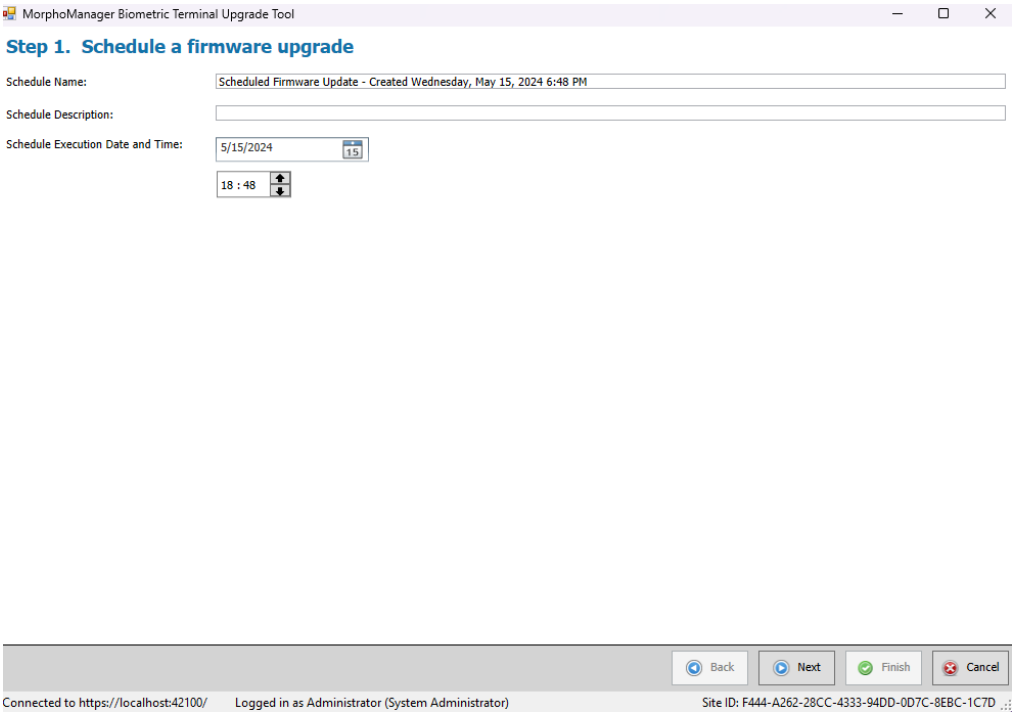
From version 16.5, sufficient access rights (read/write access) will be required by corresponding Windows service account for accessing MorphoManager Server installation folder.



Create a Firmware Update job

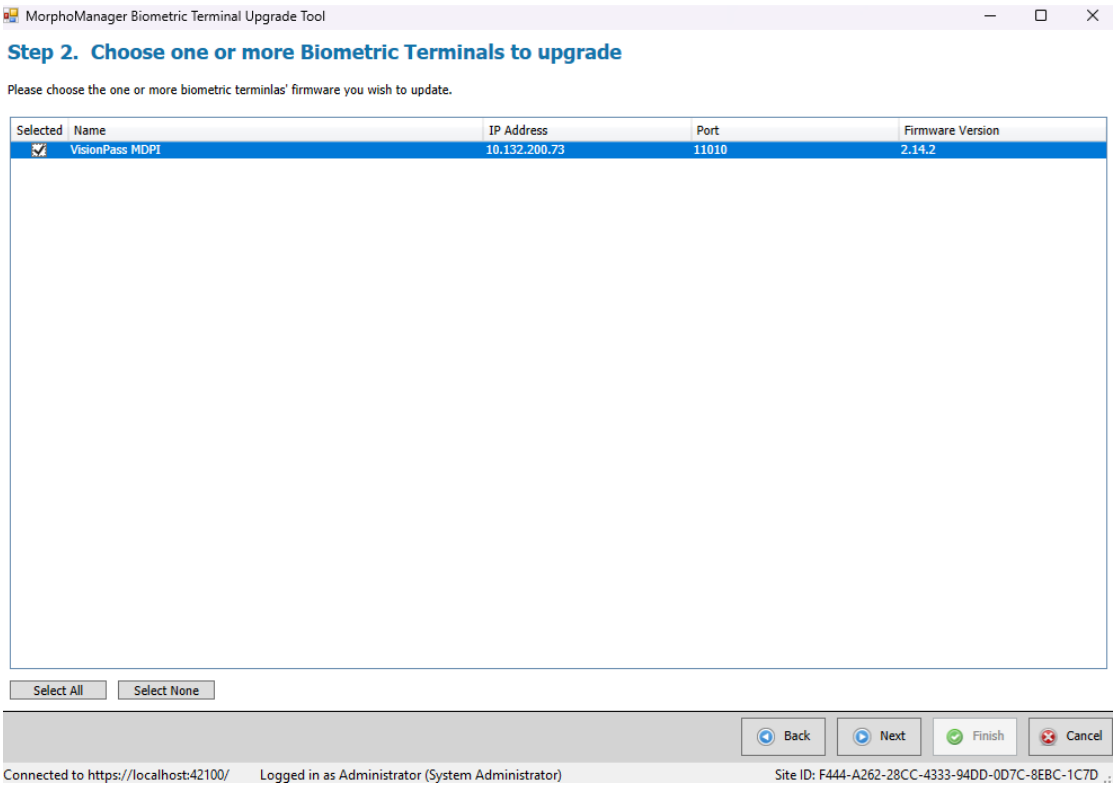
From the home screen above click **Add** to create a Firmware Update job to be executed.

Screen 1



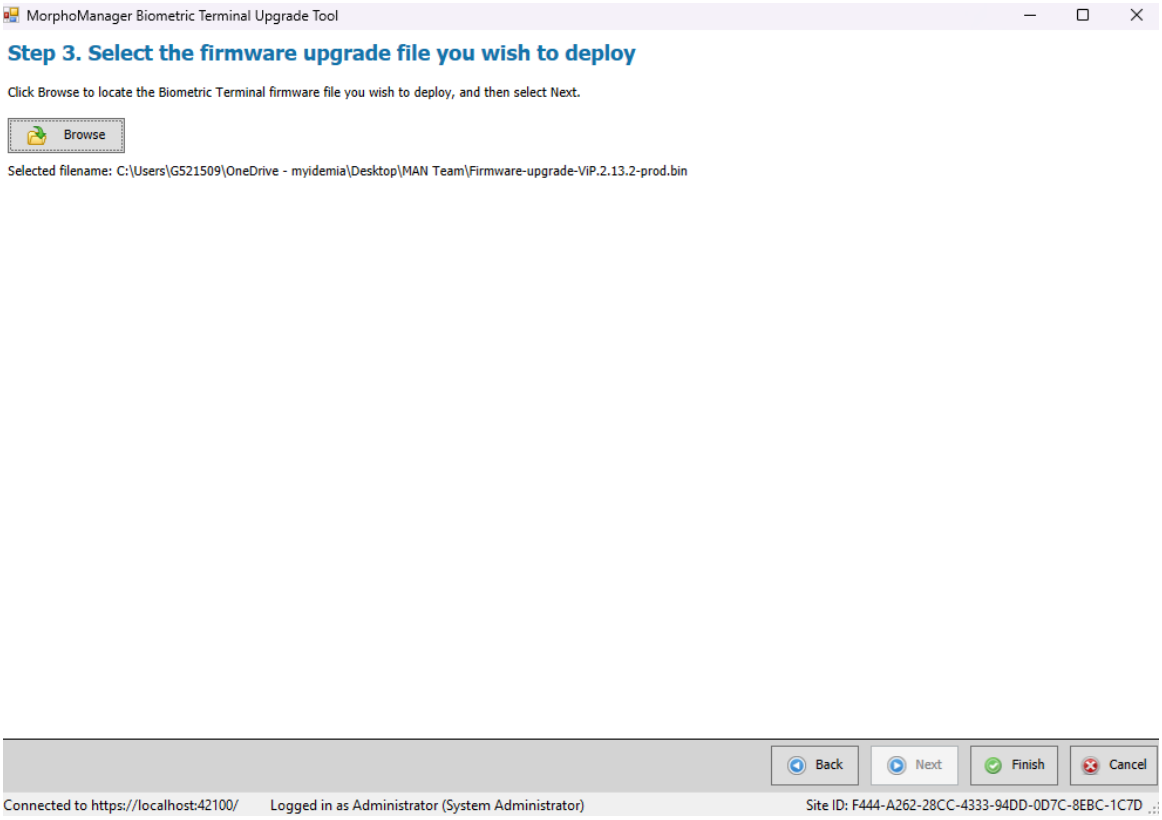
Set the date and time to run the firmware update job. By default, it will run immediately. However, this can be scheduled to run at a future date and time. Click **Next**.

Screen 2

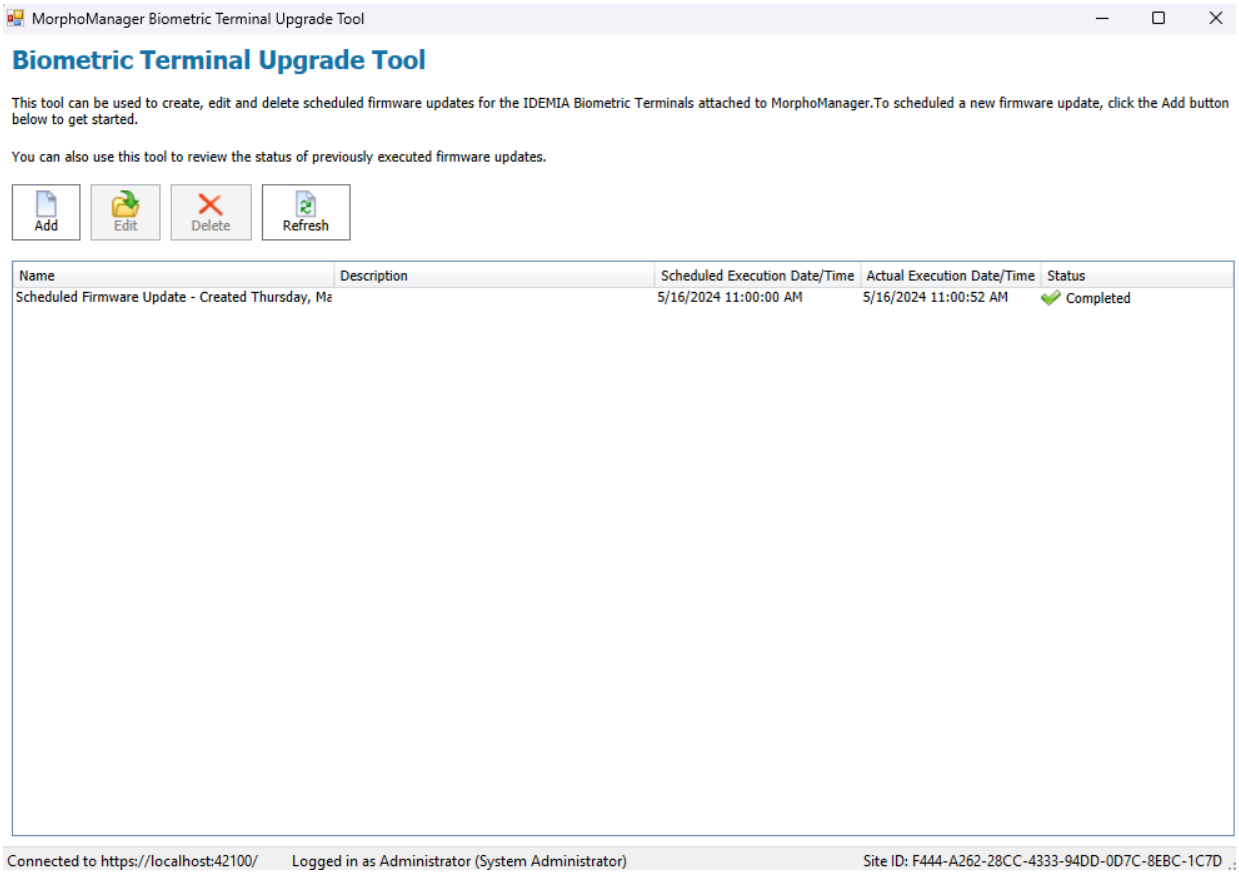


Select the Biometric Terminal(s) connected to MorphoManager that will be included in this Firmware Update. Click **Next**.

Screen 3



Browse and select the firmware update version file to be applied to the Biometric Terminals 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 and Exception Log.

Compatibility Check Utility

The purpose of this utility is to the check the compatibility of the existing MorphoManager database with the new version. It is advised to run this utility before upgrading MorphoManager from 14.6.0 or above versions.

This utility could be located within the MorphoManager package under "Compatibility Check Utility/ CompatibilityCheck.exe". Double click the file to launch the utility.

Please refer Readme.txt for more information.

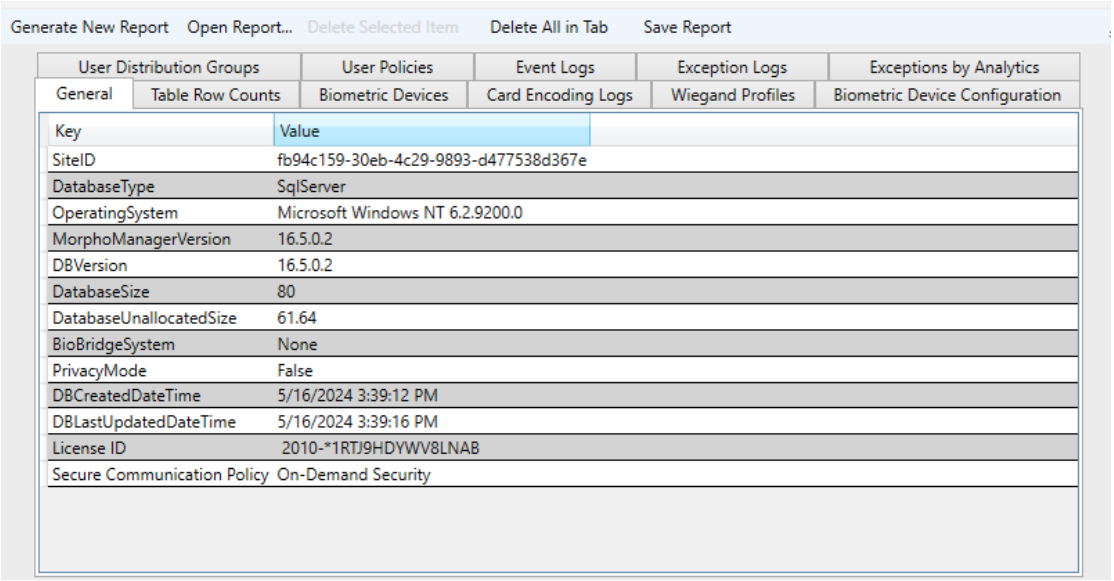
The result of the utility could be located at "Compatibility Check Utility/CompatibilityCheck.txt".

There are two possible results:

1. SUCCESS: Database is compatible with the new version. Please continue with upgrade.
2. FAILED: Database is not compatible with the new version. Please contact Idemia support for

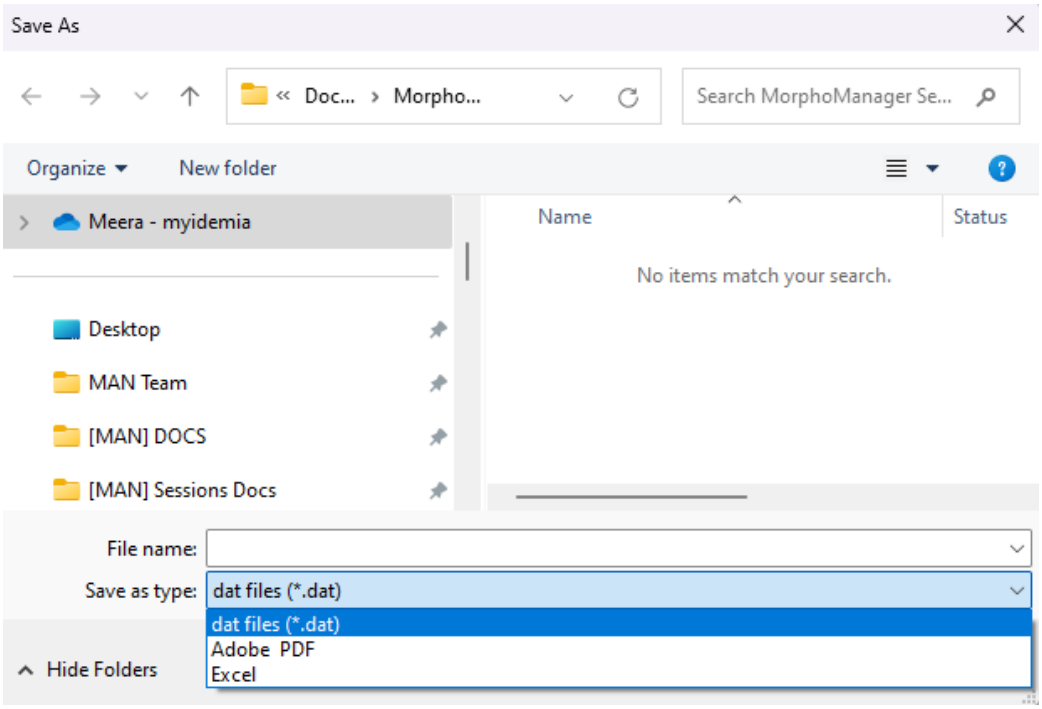
further assistance.

Server Analytics Report



The purpose of this utility is to generate and save a report needed for IDEMIA support team. Report can be exported in the following formats:

- XLSX for support process
- DAT for support process
- PDF for information only (visibility may be limited depending on size of data field)



Technical Healthcare Monitoring

This section describes the tools that have been implemented to monitor specific actions in MorphoManager.

Resilience

This feature is available for user adding and logs retrieval from version 15.3.1 and consists in an automatic retry of these both requests in case of transient failure.

Currently we implemented a retry of ten times each 5 seconds.

This feature will become configurable in a future version.