Building Integration System

Integrating IDEMIA Biometrics with ACE

en Configuration Guide

Table of contents

1 Introduction

This document describes the configuration of IDEMIA biometric devices to work with Bosch access control systems through **MorphoManager** and **BioBridge**.

In order to keep the document at a manageable size, only a few relevant aspects of the very comprehensive MorphoManager software are described here. For details, please consult IDEMIA documentation at https://service.morphotrak.com/documentation.html

Intended audience

System architects, installers and configurators who want to add IDEMIA biometric readers to Bosch access control systems.

2 System overview

The following non-Bosch components are involved:

- **IDEMIA** (formerly **Morpho**) is a multinational company specializing in security and identity solutions.
- **MorphoManager** is a biometric access control application from the IDEMIA company. The application works with biometric devices to capture fingerprints and other biometric data. The biometric information is associated with cardholder data in a database. When cardholders present themselves at an IDEMIA biometric access reader, and their biometric data matches a card number in the database, the reader sends the associated card data to the local access controller, such as an AMC2 device, which then makes the decision to grant or deny access.
- **BioBridge** is the interface software connecting **MorphoManager** with Bosch access control systems and others.

3 Configuring IDEMIA Universal BioBridge

This section describes the configuration of IDEMIA biometric devices to work with Bosch access control systems through **MorphoManager** and **BioBridge**.
The subsections cover the configuration tasks necessary in the following areas:

- The Bosch access control system
- MorphoManager
- The BioBridge enrollment client in MorphoManager
- Adaptations for various card technologies and formats

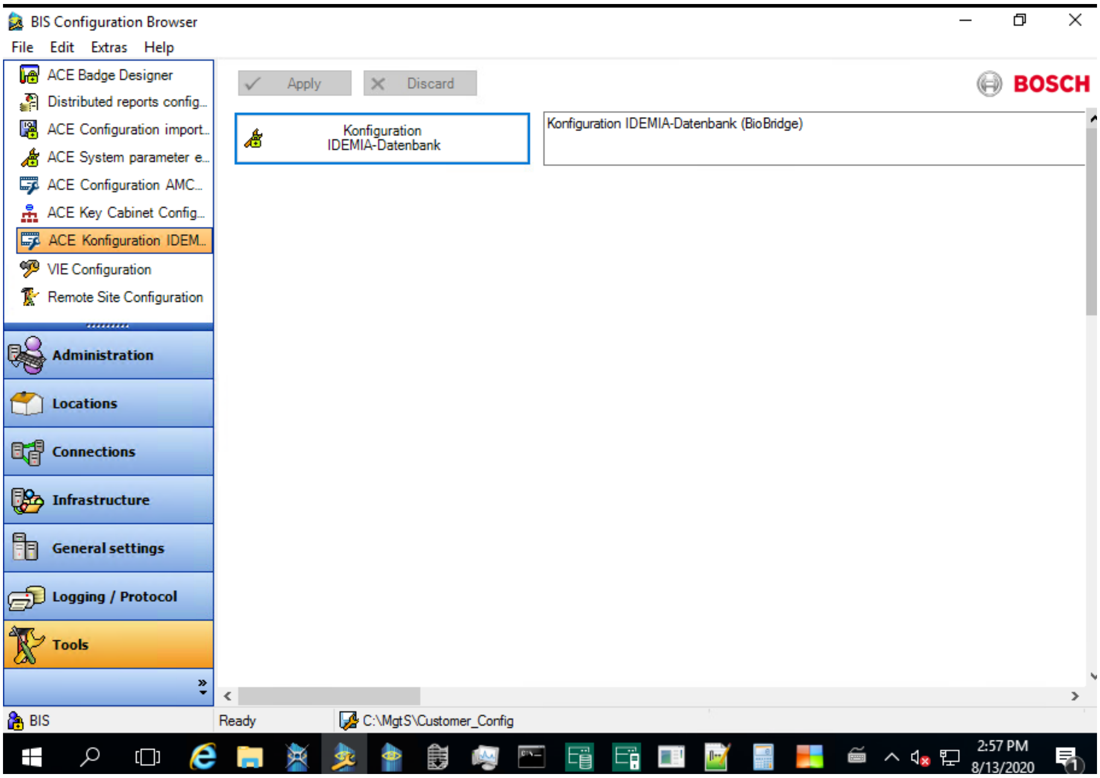
3.1 Setting up BioBridge in the Bosch access control system

The following steps are performed in ACE to create the database that links IDEMIA biometric devices to the Bosch access control system. The database maps the following database entities to each other:

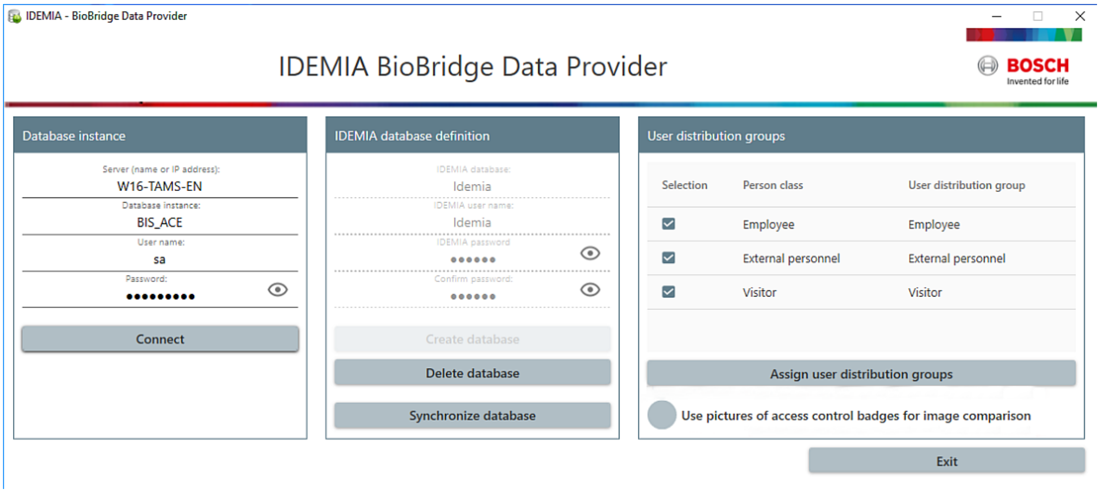
- **Person class** (Bosch) and
- **User distribution group** (IDEMIA).

Dialog path

- **BIS Configuration Browser** > **Tools** > **ACE configuration IDEMIA database**


BIS Configuration Browser
File Edit Extras Help
ACE Badge Designer
Distributed reports config...
ACE Configuration import...
ACE System parameter e...
ACE Configuration AMC...
ACE Key Cabinet Config...
ACE Konfiguration IDEM...
VIE Configuration
Remote Site Configuration
Administration
Locations
Connections
Infrastructure
General settings
Logging / Protocol
Tools
Apply
Discard
BOSCH
Konfiguration IDEMIA-Datenbank
Konfiguration IDEMIA-Datenbank (BioBridge)
BIS
Ready
C:\MgtS\Customer_Config
2:57 PM
8/13/2020

1. Click **Configuration IDEMIA database**
   The **IDEMIA BioBridge Data Provider** dialog appears.



Server (name or IP address): W16-TAMS-EN
Database instance: BIS_ACE
User name: sa
Password: ●●●●●●●●●

IDEMIA database: Idemia
IDEMIA user name: Idemia
IDEMIA password: ●●●●●●
Confirm password: ●●●●●●

Selection	Person class	User distribution group
☑	Employee	Employee
☑	External personnel	External personnel
☑	Visitor	Visitor

○ Use pictures of access control badges for image comparison

2. In the **Database instance** pane, enter the following information:

- **Server**: The hostname or IP address of the computer where the BIS_ACE SQL Server database instance is running. This may be the local hostname, if the SQL Server is running locally.
- **Database Instance**: The instance of the ACE database (default *BIS_ACE*).
- **Username**: The name of administrator account of the ACE database instance (default: *sa*)
- **Password**: The password of the administrator account, as configured during the installation of ACE

In the IDEMIA database definition pane

The first two fields are read-only:

- **Idemia database**: the name of the database that joins Bosch and IDEMIA data.
- **Idemia username**: the name of the database user in whose name the software executes commands in the database.

1. Enter and confirm a strong password for **Idemia username**.
2. Carefully note the password. It will be required in future configuration tasks, and cannot be restored if lost.
3. Click **Create database**.
   A message box will confirm if the creation was successful. Click **OK**
4. Click **Connect** to test the database connection.
5. When tests are successfully completed, click **Exit** to close the dialog.

In the User distribution groups pane

User Distribution Groups are MorphoManager objects that map users (credential holders) to groups of biometric readers or MorphoManager clients. We map them to the **Person Classes** of Bosch access control systems.

1. In the Select column, select the check box of each ACE **Person Class** that your installation uses.
2. For each line you have selected, copy the name of that Person class to the corresponding cell in the **User distribution group** column.
3. When your mapping is complete, click **Assign user distribution groups**.

Providing ID photos for VisionPass face recognition

To allow IDEMIA readers to perform VisionPass face recognition using cardholders' ID photos from the ACE database:

- Click **Use pictures of access control badges for image comparison**
  The **IDEMIA BioBridge Data Provider** window confirms that synchronization is in progress.
  Note that, depending on the amount of image data involved, the transfer may take considerable time.

3.2 Setting up BioBridge in MorphoManager

Prerequisites

MorphoManager is installed on a MorphoManager server in your network. See the MorphoManager's own installation guide and online help.

Overview

To use the BioBridge interface between Bosch access control systems and Morphomanager, you need to configure the following in MorphoManager:

- Wiegand Profiles
- Biometric Device Profiles
- Biometric Device
- User Policy
- User Distribution Group
- BioBridge System Configuration

In addition, Open Database Connectivity (ODBC) must be set up for communication between Morphomanager BioBridge and the database it shares with ACE .

All these configuration tasks are described in the following sections.

3.2.1 Wiegand Profiles

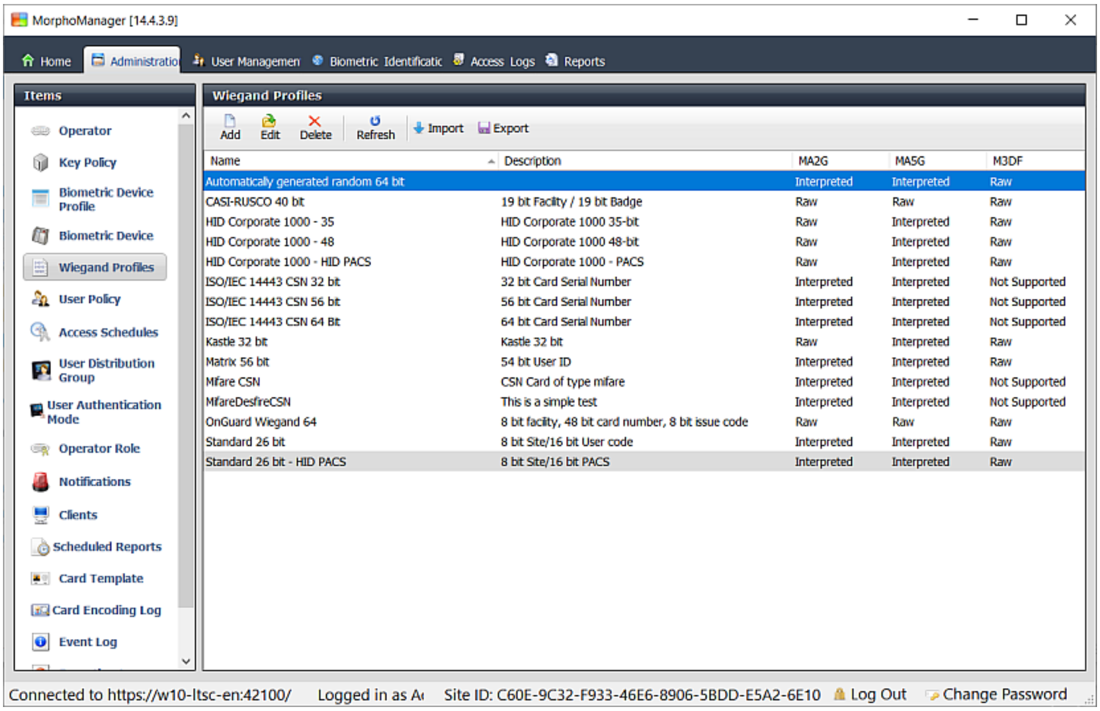
Notice!

Despite the name, Wiegand Profiles apply to all reader types, including OSDP readers.

Wiegand Profiles define what information the biometric devices output via their Wiegand Out interface, when they identify a user. This information goes to the Bosch access control system, which uses it to make an access decision.

Procedure:

1. In MorphoManager navigate to **Administration** > **Wiegand Profile**.
2. Select one of the predefined Wiegand profiles or click **Add** to create a custom profile.
   In general, all CSN profiles are suitable for use with Bosch access control systems, plus the standard 26 bit profiles. If your installer has provided a profile for your system, click **Import** to locate and import the file provided, and select it from the list.



Name	Description	MA2G	MA5G	M3DF
Automaticaly generated random 64 bit		Interpreted	Interpreted	Raw
CASI-RUSCO 40 bit	19 bit Facilty / 19 bit Badge	Raw	Raw	Raw
HID Corporate 1000 - 35	HID Corporate 1000 35-bit	Raw	Interpreted	Raw
HID Corporate 1000 - 48	HID Corporate 1000 48-bit	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
Mifare CSN	CSN Card of type mifare	Interpreted	Interpreted	Not Supported
MifareDesfireCSN	This is a simple test	Interpreted	Interpreted	Not Supported
OnGuard Wiegand 64	8 bit facilty, 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

3. In the dialog, enter the information that your access control system requires from the biometric devices.
4. Carefully note the name of the Wiegand profile that you select or create here. You must reference it in the MorphoManager configurations of **User Policy** and **Biometric Device Profile**.

3.2.2 Biometric Device Profile

The Biometric Device Profile defines common settings and parameters for one or more biometric devices. When you add biometric devices to the system later in the **Biometric Device** section of **Administration**, you apply a Biometric Device Profile to them.
The following procedure assumes that you are deploying biometric readers from IDEMIA with additional card-reading technology.

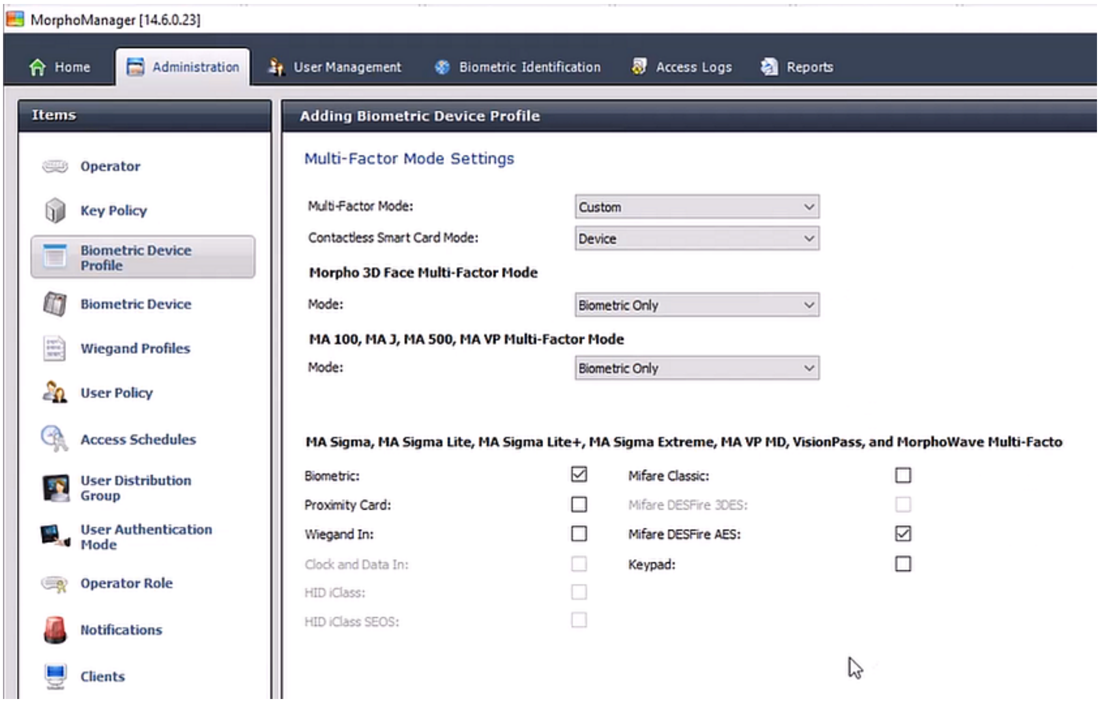
Procedure:

1. In MorphoManager navigate to **Administration** > **Biometric Device Profile**.
2. Click **Add** to create a new biometric device profile.
3. On the next screen, enter a name for the profile and a description (optional). If you do not use the description field, we recommend a name that describes the type and the identification modes (biometry and/or card) of the group of readers.
4. Click **Next** until you arrive at the **Biometric Device Settings**

– Select the Wiegand profile that you created previously for your installation.

5. Click **Next** until you arrive at **Multi-Factor Mode Settings**

– For **Multi-Factor Mode**: that is, a combination of biometric and access card reading capability, select `Custom` from the list.
– For **Contactless Smart Card Mode**: select `Device` from the list.



Adding Biometric Device Profile

Multi-Factor Mode Settings

Multi-Factor Mode: Custom
Contactless Smart Card Mode: Device

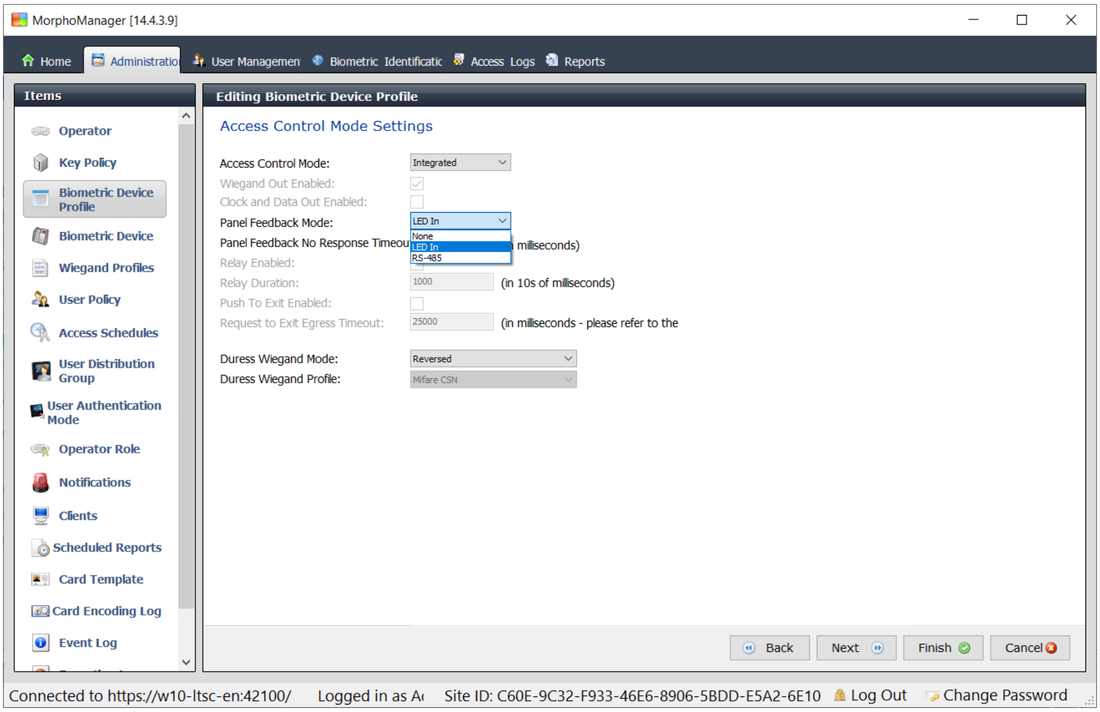
Morpho 3D Face Multi-Factor Mode
Mode: Biometric Only

MA 100, MA J, MA 500, MA VP Multi-Factor Mode
Mode: Biometric Only

MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme, MA VP MD, VisionPass, and MorphoWave Multi-Facto

Biometric: ☑ Mifare Classic: □
Proximity Card: □ Mifare DESFire 3DES: □
Wiegand In: □ Mifare DESFire AES: ☑
Clock and Data In: □ Keypad: □
HID iClass: □
HID iClass SEOS: □

6. Click **Next** until you arrive at the **Access Control Mode Settings** page.



Editing Biometric Device Profile

Access Control Mode Settings

Access Control Mode: Integrated
Wiegand Out Enabled: ☑
Clock and Data Out Enabled: □
Panel Feedback Mode: LED In (None / LED In / RS-485)
Panel Feedback No Response Timeou … milliseconds)
Relay Enabled: □
Relay Duration: 1000 (in 10s of milliseconds)
Push To Exit Enabled: □
Request to Exit Egress Timeout: 25000 (in milliseconds - please refer to the

Duress Wiegand Mode: Reversed
Duress Wiegand Profile: Mifare CSN

Connected to https://w10-ltsc-en:42100/ Logged in as A‹ Site ID: C60E-9C32-F933-46E6-8906-5BDD-E5A2-6E10 Log Out Change Password

At this point, the procedures for Wiegand and OSDP AMCs diverge. Follow the procedure that corresponds to your AMC controller type:

For Wiegand AMCs

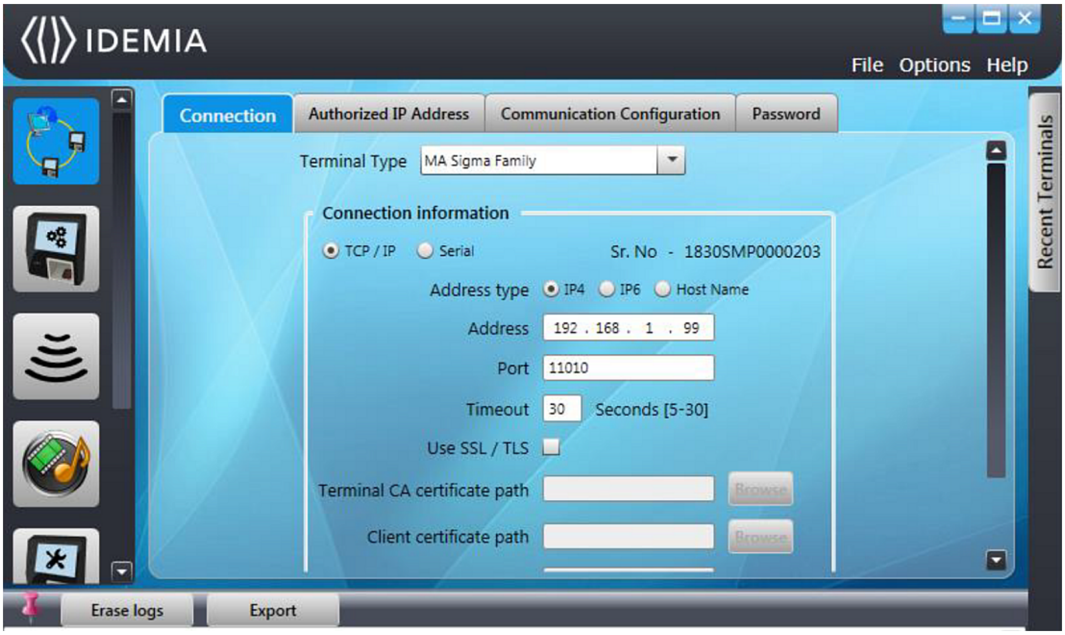
1. Set **Access Control Mode** to *`Integrated`*
2. Set **Panel feedback Mode** to *`LED In`*
3. Click **Finish**

For OSDP AMCs

1. Set **Access Control Mode** to `Integrated`
2. Set **Panel feedback Mode** to `LED In`
3. Click **Next** until you reach the **Custom Parameters** page
4. Click **Add** and add four custom parameters and set their values as follows:

- `Comm_channels_state.serial =1` (Enable communications channels)
- `OSDP.channel=1` (Enable OSDP)
- `OSDP.device_serial_address = <value>` (Set `<value>` to the bus address of the reader)
- `OSDP.secure_connection=1` (Enable secure channel)

5. Click **Finish**
6. Start the separate **MorphoBioToolBox (MBTB)** program
7. On the **Connection** tab, set the IP address of the biometric reader



Terminal Type: MA Sigma Family

Connection information

● TCP / IP ○ Serial

Sr. No - 1830SMP0000203

Address type ● IP4 ○ IP6 ○ Host Name

Address 192 . 168 . 1 . 99

Port 11010

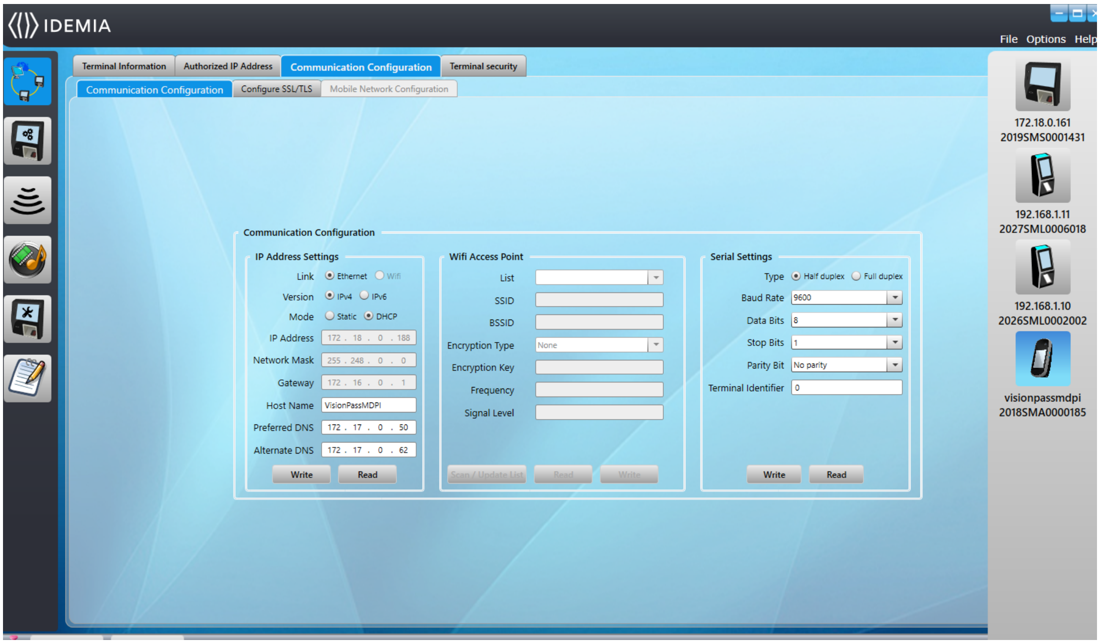
Timeout 30 Seconds [5-30]

Use SSL / TLS □

Terminal CA certificate path

Client certificate path

1. In the MorphoBioToolBox program, go to **Network & Secure Communication** > tab: **Communication Configuration**



Communication Configuration

IP Address Settings

Link ● Ethernet ○ Wifi
Version ● IPv4 ○ IPv6
Mode ○ Static ● DHCP
IP Address 172 . 18 . 0 . 188
Network Mask 255 . 248 . 0 . 0
Gateway 172 . 16 . 0 . 1
Host Name VisionPassMDPI
Preferred DNS 172 . 17 . 0 . 50
Alternate DNS 172 . 17 . 0 . 62
Write Read

Wifi Access Point

List
SSID
BSSID
Encryption Type None
Encryption Key
Frequency
Signal Level

Serial Settings

Type ● Half duplex ○ Full duplex
Baud Rate 9600
Data Bits 8
Stop Bits 1
Parity Bit No parity
Terminal Identifier 0
Write Read

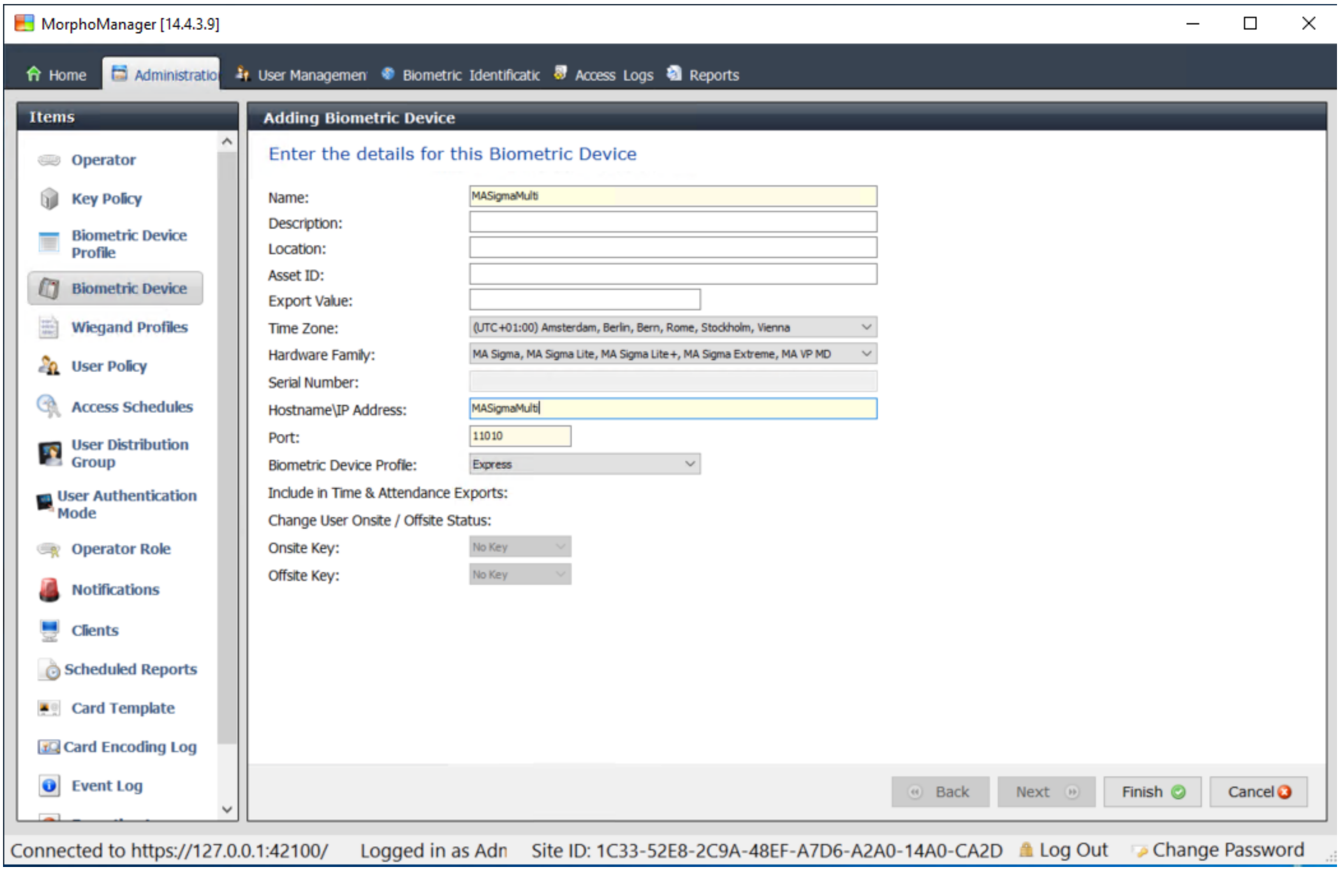
1. Make the following settings in the **Serial Settings** pane:
   - **Type**: `Half Duplex`
   - **Baud** Rate: `9600`
   - **Data Bits**: `8`
   - **Stop Bits**: `1`
   - **Parity Bit**: `No parity`
   - **Terminal identifier**: `0`.
2. If you change any of the values, click **Write** to send the changes to the device.

3.2.3 Biometric Device(s)

The biometric devices test whether the biometric credentials that they read match records in the database. They also keep a log of every usage event.

Procedure:

1. In MorphoManager navigate to **Administration** > **Biometric Device**.
2. Click **Add** to create a new Biometric Device.
3. Enter at least the essential details for the device:
   - (from the list) **Hardware Family**
   - **Hostname\IP address**
   - (from the list) the **Biometric Device Profile** that you have defined earler
4. Click **Finish**



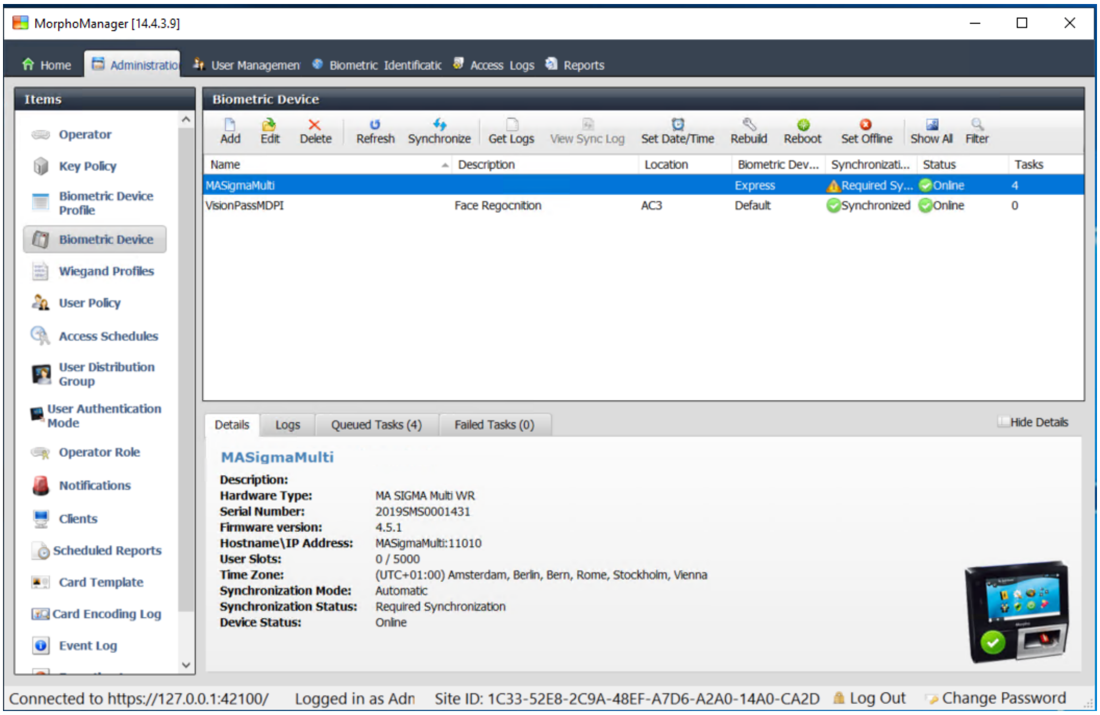
Adding Biometric Device

Enter the details for this Biometric Device

Name:	MASigmaMulti
Description:	
Location:	
Asset ID:	
Export Value:	
Time Zone:	(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Hardware Family:	MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme, MA VP MD
Serial Number:	
Hostname\IP Address:	MASigmaMulti
Port:	11010
Biometric Device Profile:	Express
Include in Time & Attendance Exports:	
Change User Onsite / Offsite Status:	
Onsite Key:	No Key
Offsite Key:	No Key

Connected to https://127.0.0.1:42100/ Logged in as Adn Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D Log Out Change Password

The Biometric Device dialog now lists devices that are already configured:



Biometric Device

Name	Description	Location	Biometric Dev...	Synchronizati...	Status	Tasks
MASigmaMulti			Express	⚠Required Sy...	✓Online	4
VisionPassMDPI	Face Regocnition	AC3	Default	✓Synchronized	✓Online	0

MASigmaMulti

Description:	
Hardware Type:	MA SIGMA Multi WR
Serial Number:	2019SMS0001431
Firmware version:	4.5.1
Hostname\IP Address:	MASigmaMulti:11010
User Slots:	0 / 5000
Time Zone:	(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Synchronization Mode:	Automatic
Synchronization Status:	Required Synchronization
Device Status:	Online

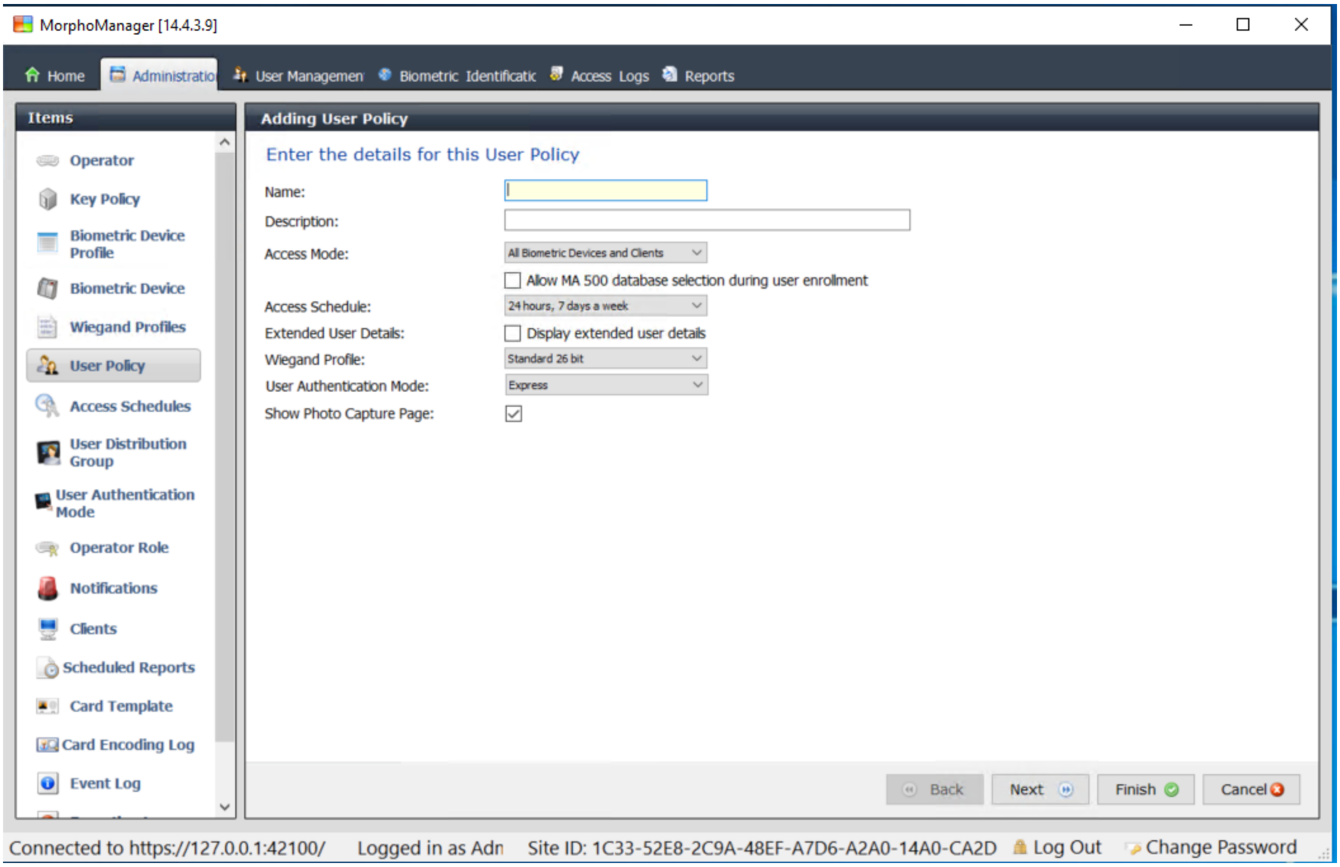
Connected to https://127.0.0.1:42100/ Logged in as Adn Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D Log Out Change Password

3.2.4 User Policy

User polices are bundles of access rights that you assign to users who have the same access requirements, that is, which biometric devices they are permitted to use in which modes and at what times.

Procedure:

1. In MorphoManager navigate to **Administration** > **User Policy**
2. Click **Add** to create a new user policy.



Adding User Policy

Enter the details for this User Policy

Name:

Description:

Access Mode: All Biometric Devices and Clients

□ Allow MA 500 database selection during user enrolment

Access Schedule: 24 hours, 7 days a week

Extended User Details: □ Display extended user details

Wiegand Profile: Standard 26 bit

User Authentication Mode: Express

Show Photo Capture Page: ☑

Connected to https://127.0.0.1:42100/ Logged in as Adn Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D

3. In the **Adding User Policy** dialog enter the following:
   - A **Name** for the User Policy and (optionally) a description
   - The **Access Mode** `Per User`
   - An **Access Schedule** governing the days and times when access is permitted
   - The same **Wiegand Profile** that you defined and used for the **Biometric Device Profile**.
   - A **User Authentication Mode**, depending on the ways in which the device users will use the devices (by fingerprint, finger, face, cards etc.). See the MorphoManager User Manual for details.
4. Click **Finish**

The default User Policy will have a User Authentication mode of `(1: Many)`. To utilize other authentication modes, create additional User Policies. Consult the MorphoManager User Manual for more detail on all the various properties that can be assigned to a User Policy.

3.2.5 User Distribution Groups

User Distribution Groups map users to groups of biometric readers or MorphoManager clients.

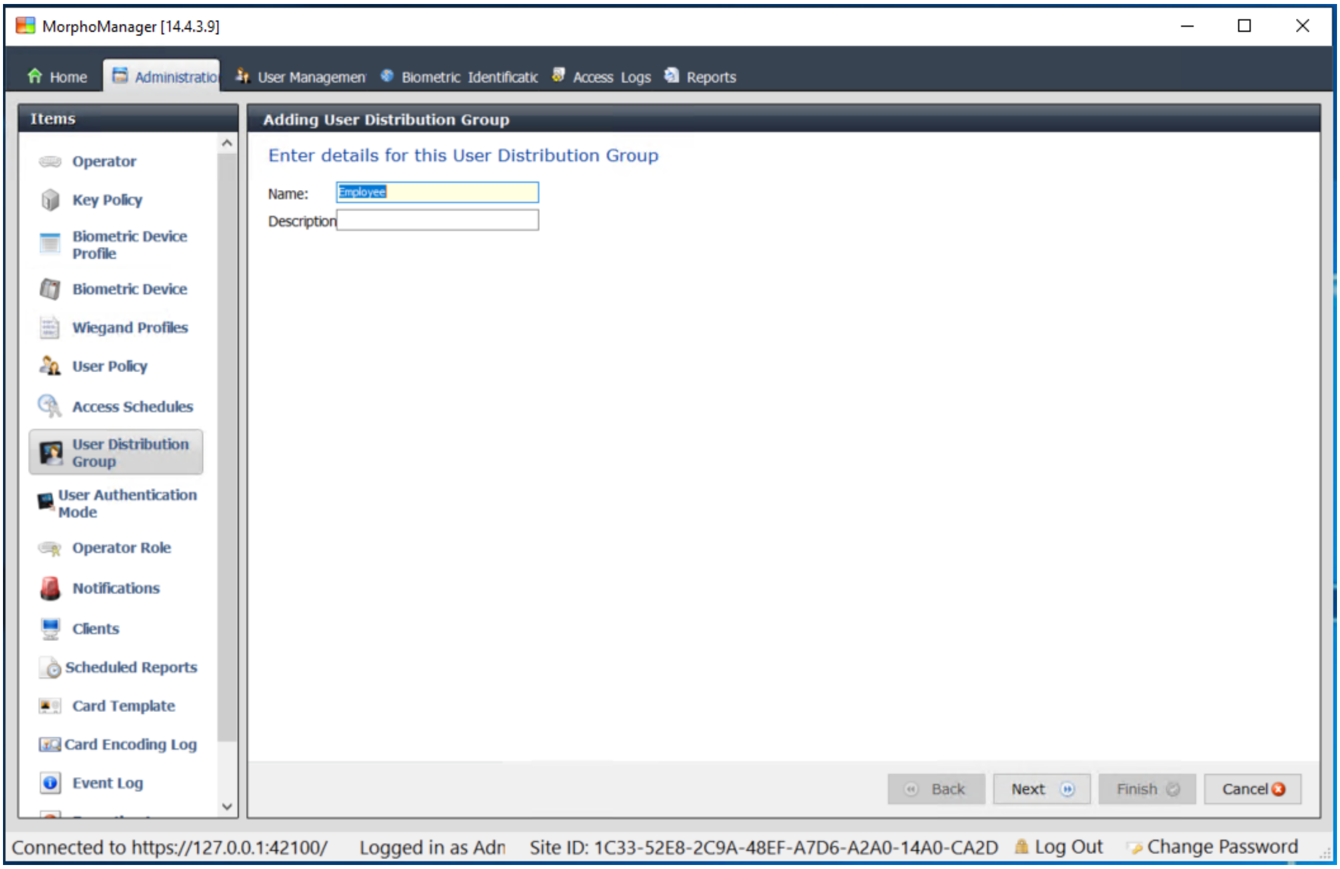
Prerequisites:

Users in User Distribution Groups must have a User Policy where **Access Mode** is set to `Per User`.

Each User Distribution Group must be mapped to at least one Person Class in ACE . Therefore create at least one User Distribution Group for each Person Class that you use.

Procedure:

1. In MorphoManager navigate to **Administration** > **User Distribution Group**.
2. Click **Add** to create a new User Distribution Group.



Adding User Distribution Group

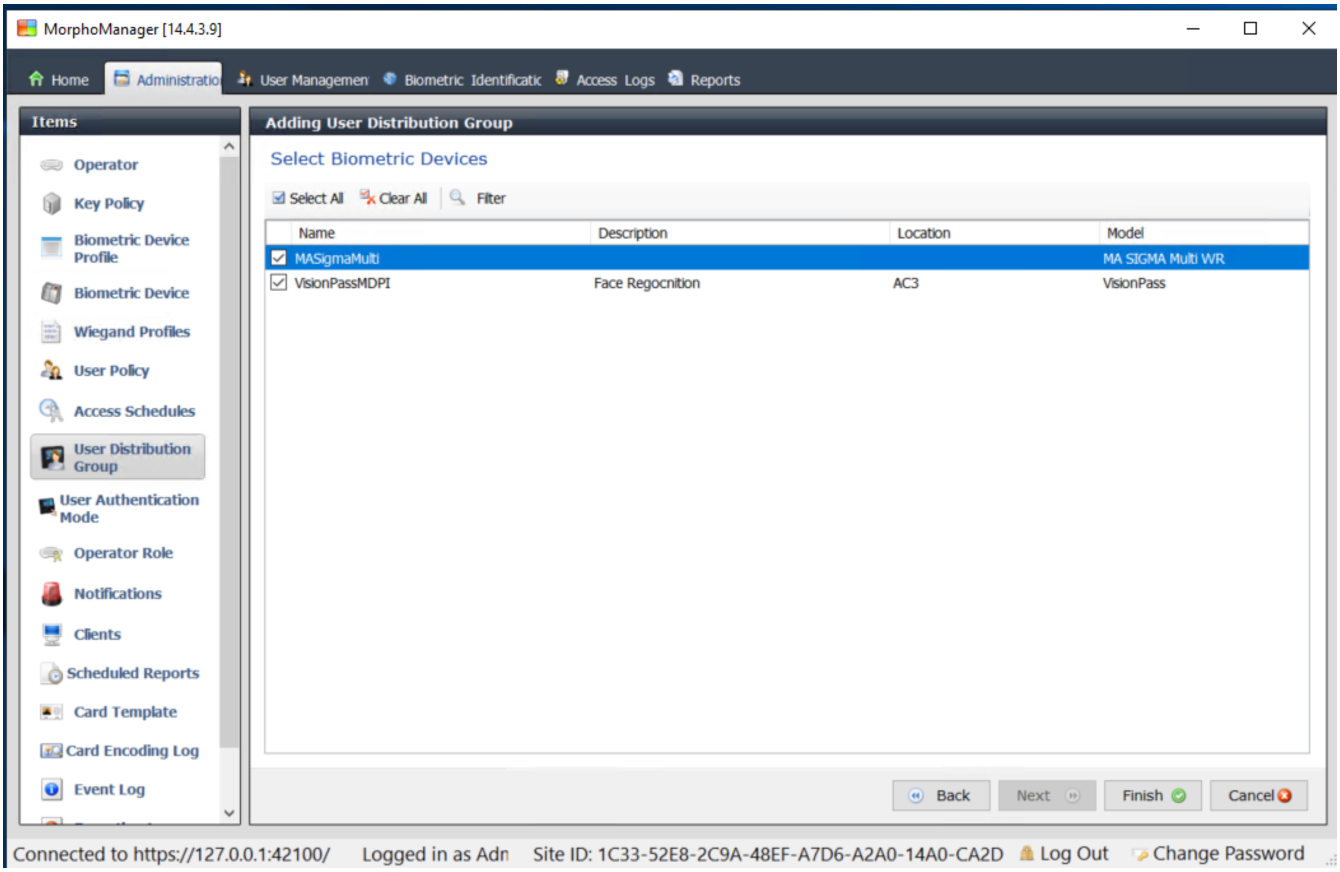
Enter details for this User Distribution Group

Name: Employee

Description

Connected to https://127.0.0.1:42100/ Logged in as Adn Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D

3. Click **Next** until you reach the page titled **Select Biometric Devices**.
4. Select the check boxes of those biometric devices that the persons of this User Distribution Group are to use.



	Name	Description	Location	Model
☑	MASigmaMulti			MA SIGMA Multi WR
☑	VisionPassMDPI	Face Regocnition	AC3	VisionPass

5. Click **Finish**

3.2.6 Setting up ODBC for BioBridge

Introduction

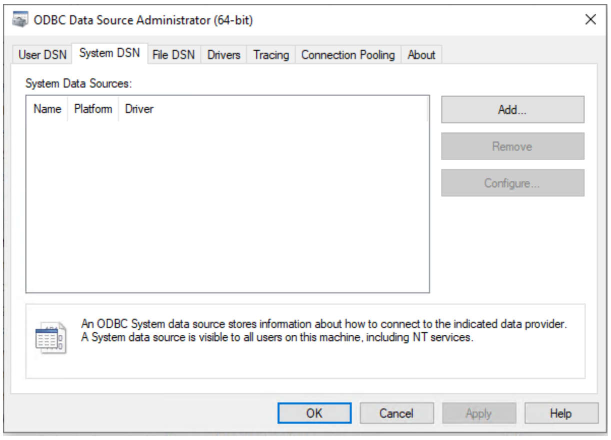
Open Database Connectivity (ODBC) is a prerequisite for use of MorphoManager BioBridge. ODBC is a standardized programming interface for accessing different databases. The recommended driver is *`OdbCDriver17SQLServer`*, which you can find on the BIS installation media at

`BIS\3rd_Party\OdbCDriver17SQLServer`

Creating a Data Source

Creating a Data Source name (DSN) for ODBC

1. In the Windows Control Panel select **Administrative Tools**.
2. Select *`ODBC Data Sources (64-bit)`* from the list.
3. Select the **System DSN** tab.

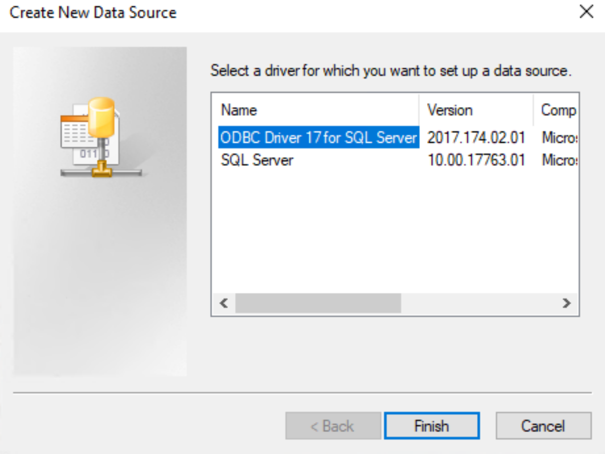


System Data Sources:

Name	Platform	Driver

An ODBC System data source stores information about how to connect to the indicated data provider. A System data source is visible to all users on this machine, including NT services.

4. Click **Add** to select a driver.
5. Select *`ODBC Driver 17 for SQL Server`* as the driver, and click **Finish**.



Select a driver for which you want to set up a data source.

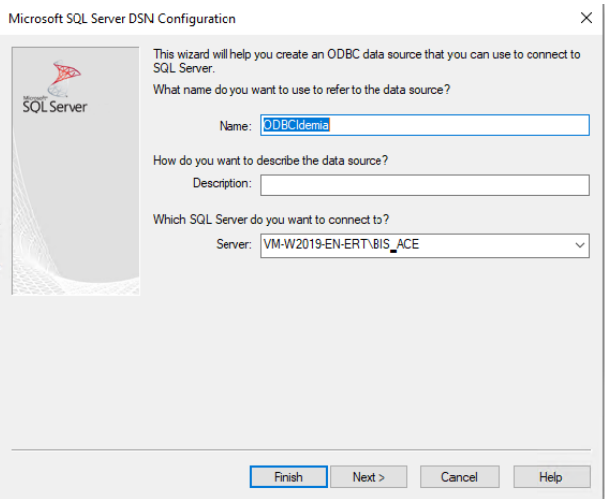
Name	Version	Comp
ODBC Driver 17 for SQL Server	2017.174.02.01	Micro:
SQL Server	10.00.17763.01	Micro:

6. Enter the following details for the Data Source.

– **Name**: a name for the data source

– **Description** (optional)

– **Server**: the name of the computer where the ACE database is installed, and the name of the database (default: <MyACEserver>*`BIS_ACE`*)



This wizard will help you create an ODBC data source that you can use to connect to SQL Server.

What name do you want to use to refer to the data source?

Name: ODBCIdemia

How do you want to describe the data source?

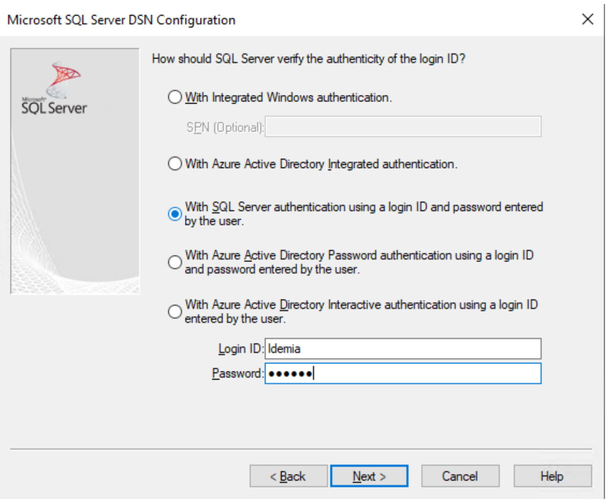
Description:

Which SQL Server do you want to connect to?

Server: VM-W2019-EN-ERT\BIS_ACE

7. Click **Next >**

A dialog appears to collect login information



Microsoft SQL Server DSN Configuration

How should SQL Server verify the authenticity of the login ID?

○ With Integrated Windows authentication.

SPN (Optional):

○ With Azure Active Directory Integrated authentication.

● With SQL Server authentication using a login ID and password entered by the user.

○ With Azure Active Directory Password authentication using a login ID and password entered by the user.

○ With Azure Active Directory Interactive authentication using a login ID entered by the user.

Login ID: Idemia

Password: ••••••

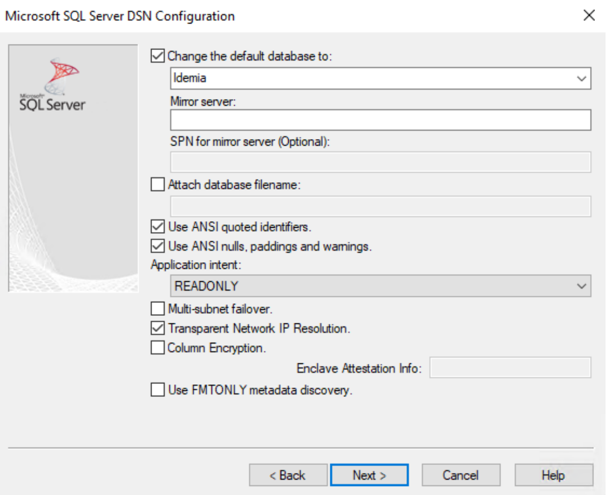
8. Select **With SQL Server authentication using a login ID...**
9. Enter the following information:

- **Login ID**: The user name of the Idemia database user as configured in ACE . This is always `Idemia`.
- **Password**: The password that was set for the Idemia database user, when it was configured in ACE

10. Click **Next >**
11. In the next dialog, select the check boxes:

- **Change the default database to:** and select `Idemia`
- **Use ANSI quoted identifiers**
- **Use ANSI nulls, paddings and warnings**
- **Transparent Network IP Resolution**

12. Set **Application intent** to `READONLY`



Microsoft SQL Server DSN Configuration

☑ Change the default database to:

Idemia

Mirror server:

SPN for mirror server (Optional):

☐ Attach database filename:

☑ Use ANSI quoted identifiers.

☑ Use ANSI nulls, paddings and warnings.

Application intent:

READONLY

☐ Multi-subnet failover.

☑ Transparent Network IP Resolution.

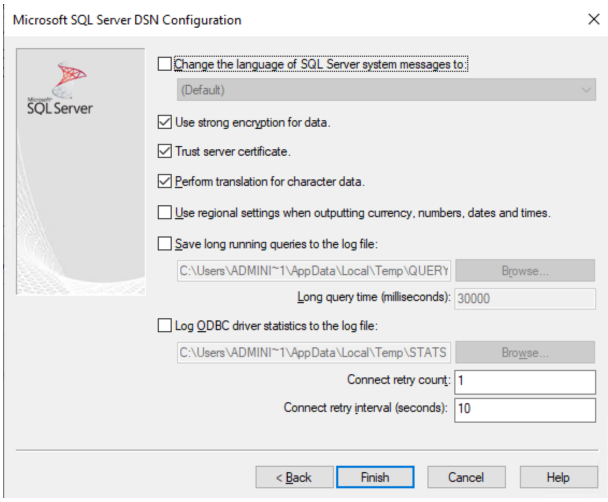
☐ Column Encryption.

Enclave Attestation Info:

☐ Use FMTONLY metadata discovery.

13. Click **Next >**
14. In the next dialog, select the check boxes

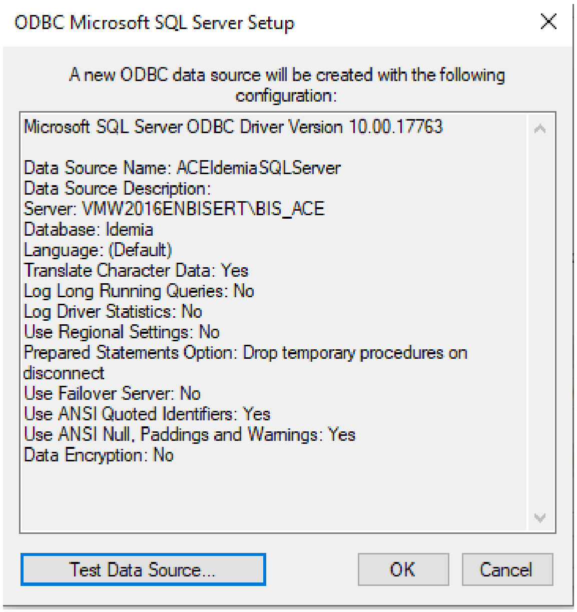
- **Use strong encryption for data**
- **Perform translation for character data**
- **Trust server certificate**



□ Change the language of SQL Server system messages to:
(Default)
☑ Use strong encryption for data.
☑ Trust server certificate.
☑ Perform translation for character data.
□ Use regional settings when outputting currency, numbers, dates and times.
□ Save long running queries to the log file:
C:\Users\ADMINI~1\AppData\Local\Temp\QUERY Browse...
Long query time (milliseconds): 30000
□ Log ODBC driver statistics to the log file:
C:\Users\ADMINI~1\AppData\Local\Temp\STATS Browse...
Connect retry count: 1
Connect retry interval (seconds): 10

15. Click **Finish**

16. In the next dialog, review the summary data

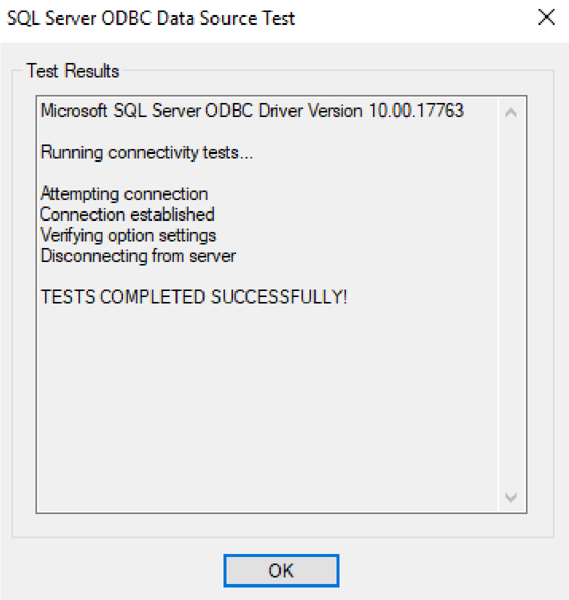


A new ODBC data source will be created with the following configuration:

```
Microsoft SQL Server ODBC Driver Version 10.00.17763

Data Source Name: ACEIdemiaSQLServer
Data Source Description:
Server: VMW2016ENBISERT\BIS_ACE
Database: Idemia
Language: (Default)
Translate Character Data: Yes
Log Long Running Queries: No
Log Driver Statistics: No
Use Regional Settings: No
Prepared Statements Option: Drop temporary procedures on
disconnect
Use Failover Server: No
Use ANSI Quoted Identifiers: Yes
Use ANSI Null, Paddings and Warnings: Yes
Data Encryption: No
```

17. Click **Test Data Source...** and ensure that the tests complete successfully



```
Microsoft SQL Server ODBC Driver Version 10.00.17763

Running connectivity tests...

Attempting connection
Connection established
Verifying option settings
Disconnecting from server

TESTS COMPLETED SUCCESSFULLY!
```

18. Save all changes and exit the ODBC setup wizard.

3.2.7 BioBridge System Configuration

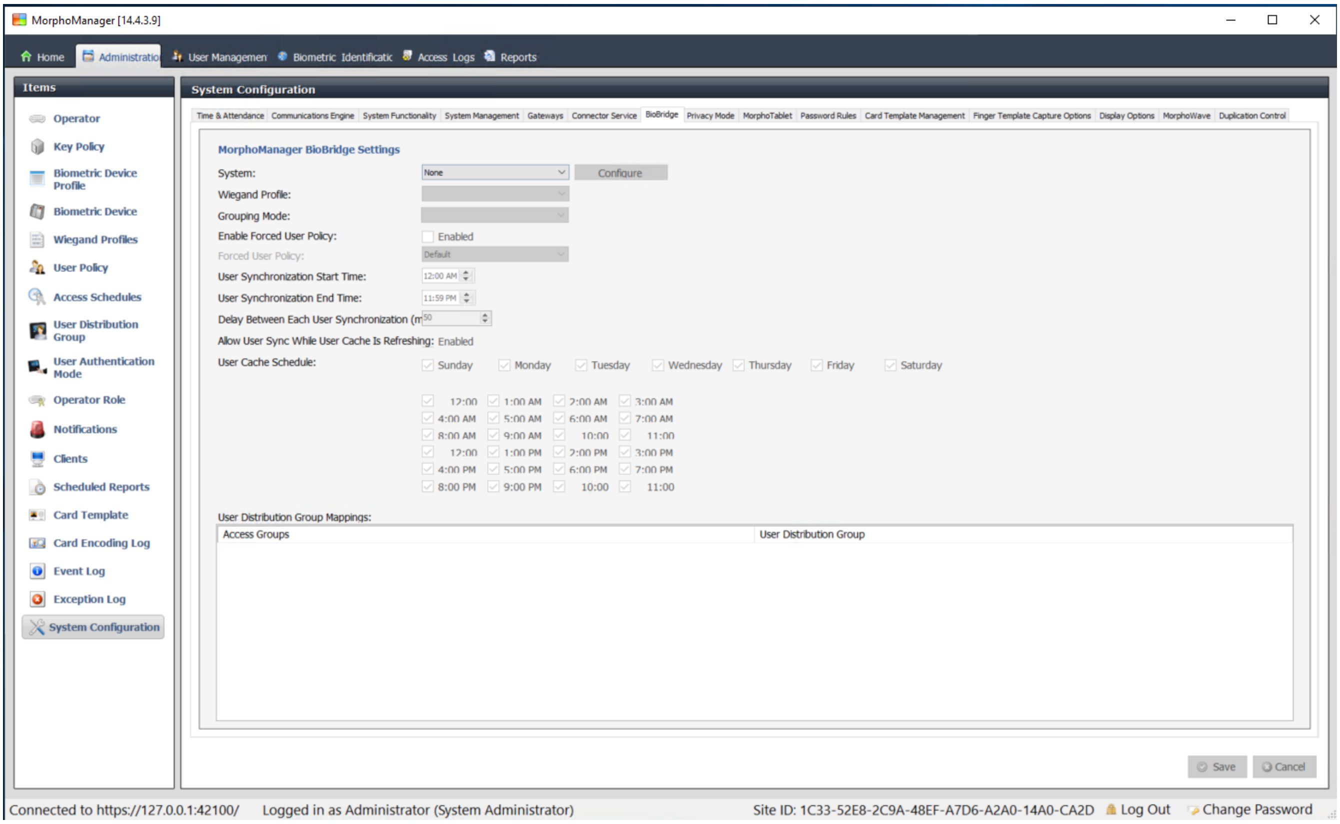
This section describe the remaining settings required for access control systems to use the BioBridge interface.

Prerequisite

ODBC is set up for BioBridge. See *Setting up ODBC for BioBridge, page 16*

Procedure:

1. In MorphoManager navigate to **Administration** > **System Configuration**.
2. Select the **BioBridge** tab



System Configuration

MorphoManager BioBridge Settings

System: None

Wiegand Profile:

Grouping Mode:

Enable Forced User Policy: □ Enabled

Forced User Policy: Default

User Synchronization Start Time: 12:00 AM

User Synchronization End Time: 11:59 PM

Delay Between Each User Synchronization (m 50

Allow User Sync While User Cache Is Refreshing: Enabled

User Cache Schedule: ☑ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday

☑ 12:00 ☑ 1:00 AM ☑ 2:00 AM ☑ 3:00 AM
☑ 4:00 AM ☑ 5:00 AM ☑ 6:00 AM ☑ 7:00 AM
☑ 8:00 AM ☑ 9:00 AM ☑ 10:00 ☑ 11:00
☑ 12:00 ☑ 1:00 PM ☑ 2:00 PM ☑ 3:00 PM
☑ 4:00 PM ☑ 5:00 PM ☑ 6:00 PM ☑ 7:00 PM
☑ 8:00 PM ☑ 9:00 PM ☑ 10:00 ☑ 11:00

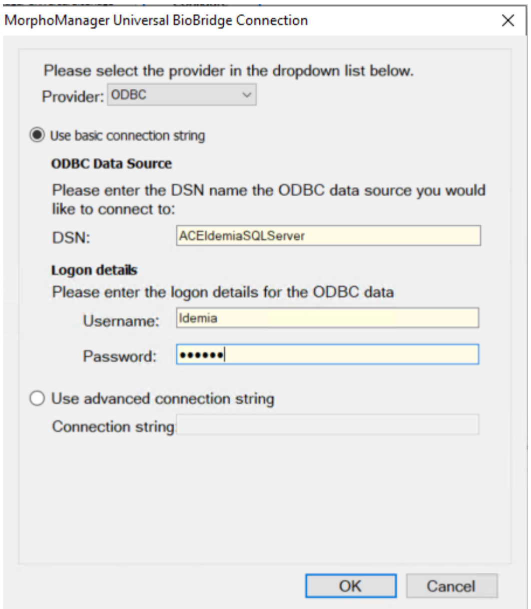
User Distribution Group Mappings:

Access Groups	User Distribution Group

Connected to https://127.0.0.1:42100/ Logged in as Administrator (System Administrator) Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D

3. In the **System** drop-down list, select `MorphoManager Universal BioBridge`
4. Click **Configure**

   A popup dialog appears.



Please select the provider in the dropdown list below.

Provider: ODBC

● Use basic connection string

ODBC Data Source

Please enter the DSN name the ODBC data source you would like to connect to:

DSN: ACEIdemiaSQLServer

Logon details

Please enter the logon details for the ODBC data

Username: Idemia

Password: ••••••

○ Use advanced connection string

Connection string

In the popup window

1. In the **Provider** drop-down list, select *ODBC*
2. Enter the DSN (Data Source Name) from the ODBC setup.
3. Under **Logon details**, enter the username (*Idemia*) and password as defined in the ODBC setup.
4. Click **OK** to return to the **System Configuration** dialog.

In the **System Configuration** dialog

1. For **Wiegand Profile**: select from the list the Wiegand profile that you defined earlier.

Grouping mode:

This setting determines how MorphoManager should map MM Universal BioBridge users to MorphoManager User Distribution Groups. Select one of the following:

- **Automatic**: This mode will automatically match **Access Level groups** from MM Universal BioBridge to MorphoManager **User Distribution Groups**, if they have the same naming convention.
- **Manual**: If the **Access Level groups** of MM Universal BioBridge and the **User Distribution Group(s)** of MorphoManager are not the same, then you can perform the mapping manually in **User Policy Mappings**.

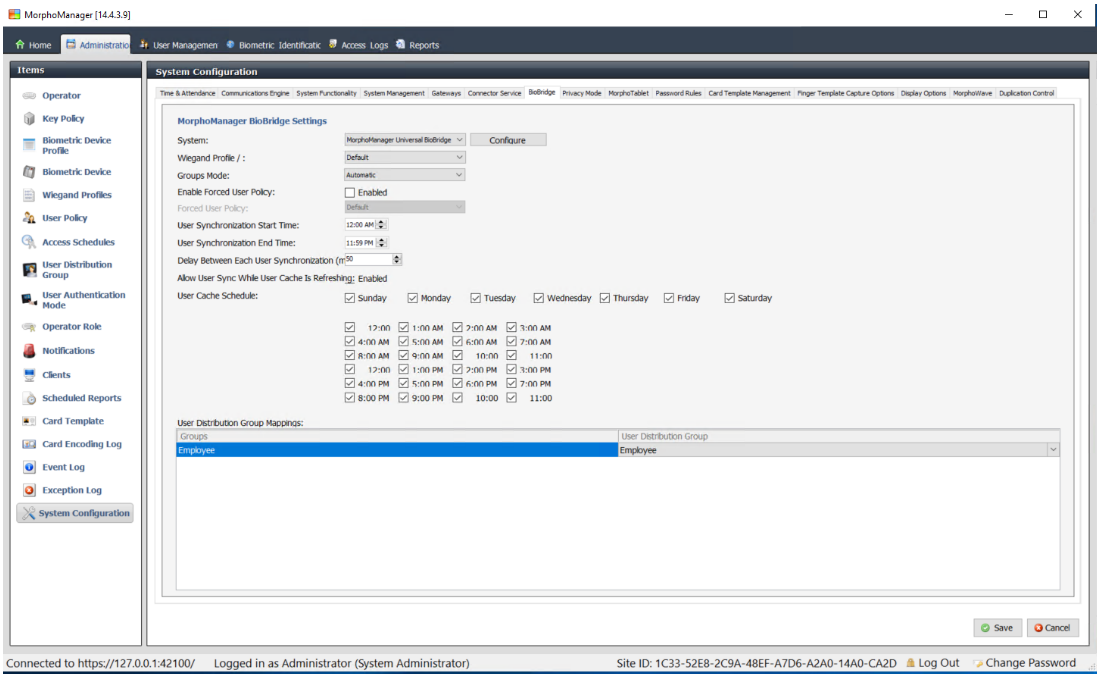
Other settings

In most cases the following settings can be left at their default values:

Enable Forced User Policy	When selected, all users that are enrolled in the BioBridge enrollment client will receive the User Policy that is selected from the adjacent list. If you select this check box, always use the User policy named `Per User`
User Synchronization Start Time and End Time	The user synchronization engine will only be permitted to run between these two times.
Delay between Each User Synchronization	The time interval between user synchronizations. Increasing the delay will save system resources, but increase the time for all the users to be updated.
Allow User Sync While User Cache 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 that you disable this setting when using large databases.
User Cache Refresh Schedule	The days and times when the user cache may be refreshed. For the highest accuracy, this should be at all times, but for the performance of systems with large databases, a compromise is required.

User Distribution Group mappings

- In the mappings table, ensure that all **Groups** (**Personnel classes** defined in ACE) are mapped to **User Distribution groups** (defined MorphoManager).



System Configuration

MorphoManager BioBridge Settings

System: MorphoManager Universal BioBridge
Wiegand Profile / : Default
Groups Mode: Automatic
Enable Forced User Policy: □ Enabled
Forced User Policy: Default
User Synchronization Start Time: 12:00 AM
User Synchronization End Time: 11:59 PM
Delay Between Each User Synchronization (m 50
Allow User Sync While User Cache Is Refreshing: Enabled
User Cache Schedule: ☑ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday

☑ 12:00 ☑ 1:00 AM ☑ 2:00 AM ☑ 3:00 AM
☑ 4:00 AM ☑ 5:00 AM ☑ 6:00 AM ☑ 7:00 AM
☑ 8:00 AM ☑ 9:00 AM ☑ 10:00 ☑ 11:00
☑ 12:00 ☑ 1:00 PM ☑ 2:00 PM ☑ 3:00 PM
☑ 4:00 PM ☑ 5:00 PM ☑ 6:00 PM ☑ 7:00 PM
☑ 8:00 PM ☑ 9:00 PM ☑ 10:00 ☑ 11:00

User Distribution Group Mappings:

Groups	User Distribution Group
Employee	Employee

Connected to https://127.0.0.1:42100/ Logged in as Administrator (System Administrator) Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D

3.3 Configuring the BioBridge Enrollment Client

Introduction

A BioBridge enrollment client is a computer at which you can create biometric records for users of the access control system. The setup of a BioBridge enrollment client has 3 parts:

- Adding an enrollment operator to MorphoManager
- Configuring the MorphoManager client computers for enrollment tasks
- Testing the enrollment client

Prerequisites

MorphoManager BioBridge is installed on every ACE workstation from which you perform biometric enrollment for IDEMIA systems.

3.3.1 Adding an enrollment operator to Morpho Manager

Procedure

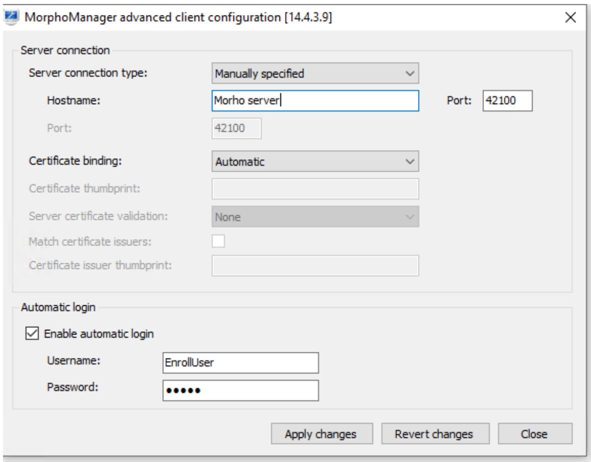
Follow the instructions in the MorphoManager client installation guide.
Note: for security reasons, Active Directory user accounts are recommended.

3.3.2 Configuring the MorphoManager client computers for enrollment tasks

Perform this procedure on each computer that you wish to use for biometric enrollment.

Procedure

1. In the MorphoManager installation directory (default: `C:\Program,Files(x86)\Morpho\MorphoManager\Client\`)
   execute the file `ID1.ECP4.MorphoManager.AdvancedClientConfig.exe` as administrator



MorphoManager advanced client configuration [14.4.3.9]

Server connection

Server connection type: Manually specified

Hostname: Morho server

Port: 42100

Port: 42100

Certificate binding: Automatic

Certificate thumbprint:

Server certificate validation: None

Match certificate issuers: □

Certificate issuer thumbprint:

Automatic login

☑ Enable automatic login

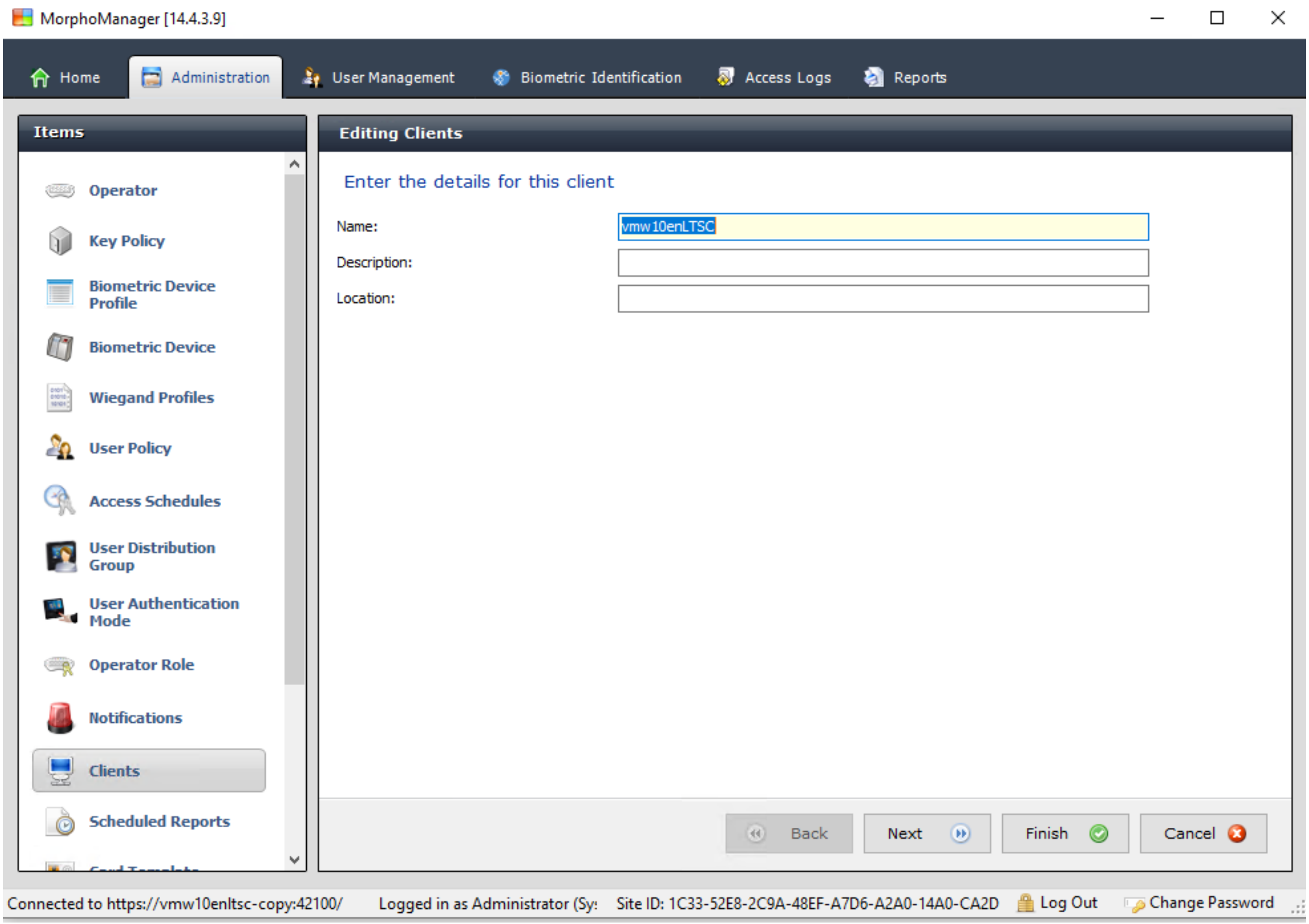
Username: EnrollUser

Password: •••••

2. Enter the Hostname of the Morpho server under **Hostname**
3. Under **Automatic login**

- Select the check box Enable Automatic login
- Enter the username and password that you entered for the enrollment operator in the previous section

1. In the MorphoManager installation directory (default: `C:\Program Files(x86)\Morpho\MorphoManager\Client\`)
   execute the file `Start ID1.ECP4.MorphoManager.Client.exe` as Administrator
2. Navigate to **Administration** > **Clients**
3. Select a client computer
4. Click **Edit**



Enter the details for this client

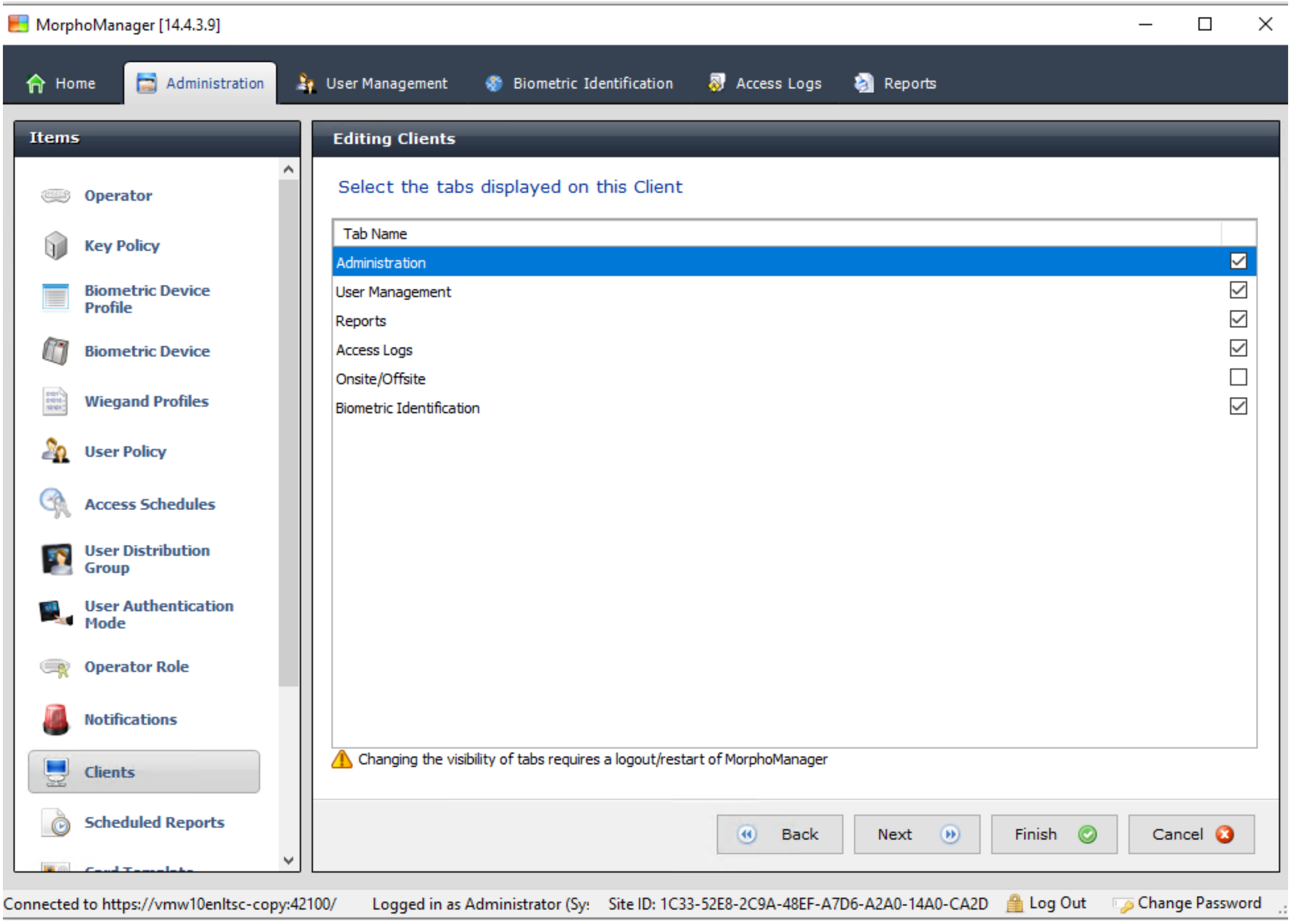
Name: vmw10enLTSC

Description:

Location:

Connected to https://vmw10enltsc-copy:42100/ Logged in as Administrator (Sy: Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D

5. Enter the name of the intended enrollment client, and optionally the location and a description
6. Click **Next**



Editing Clients

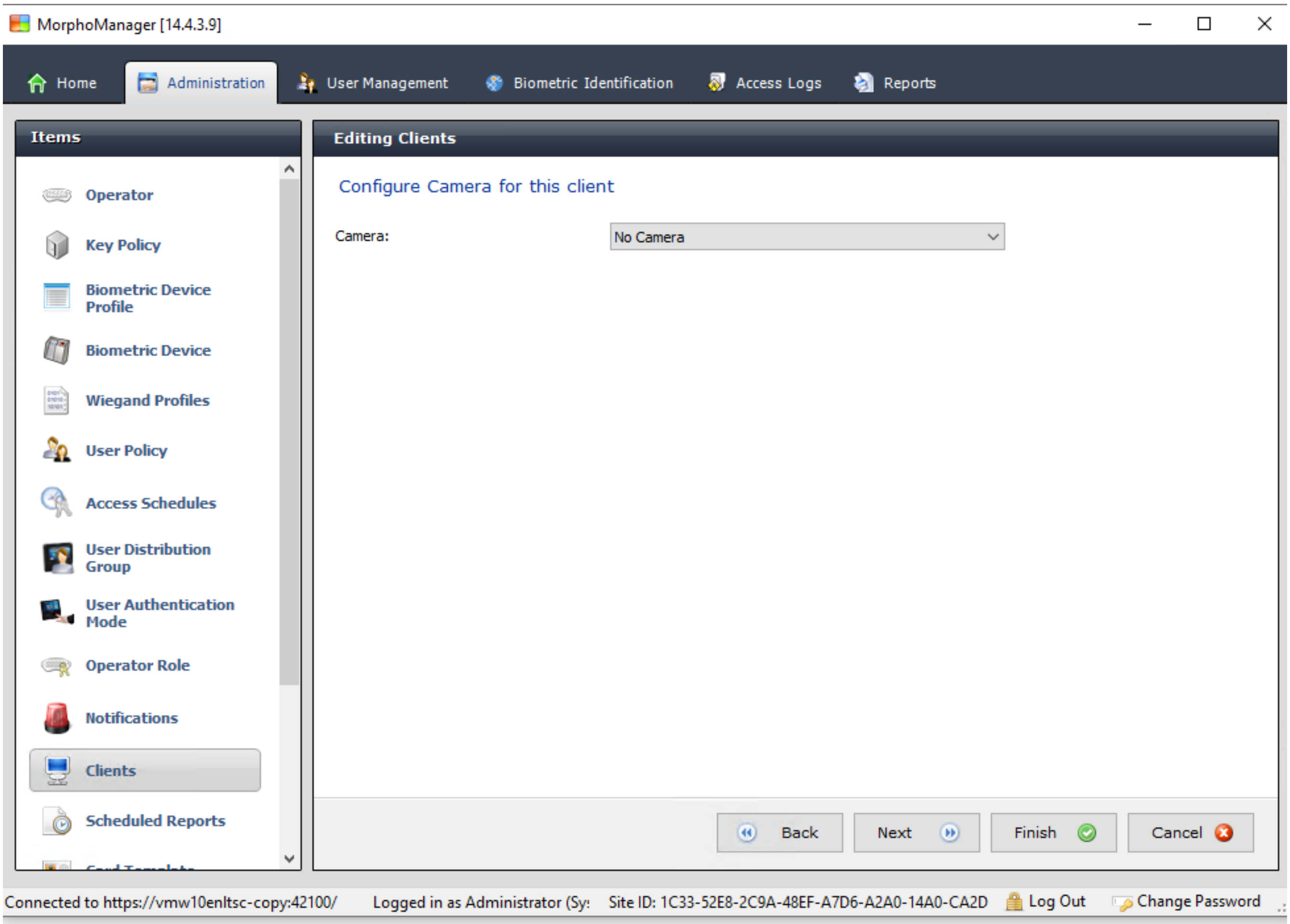
Select the tabs displayed on this Client

Tab Name	
Administration	☑
User Management	☑
Reports	☑
Access Logs	☑
Onsite/Offsite	□
Biometric Identification	☑

Changing the visibility of tabs requires a logout/restart of MorphoManager

Connected to https://vmw10enltsc-copy:42100/ Logged in as Administrator (Sy: Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D

7. Select the check boxes of the tabs that you want to display on the enrollment client:
   - **Administration,**
   - **User Management,**
   - **Reports,**
   - **Access Logs,**
   - **Biometric Identification**
8. Click **Next**

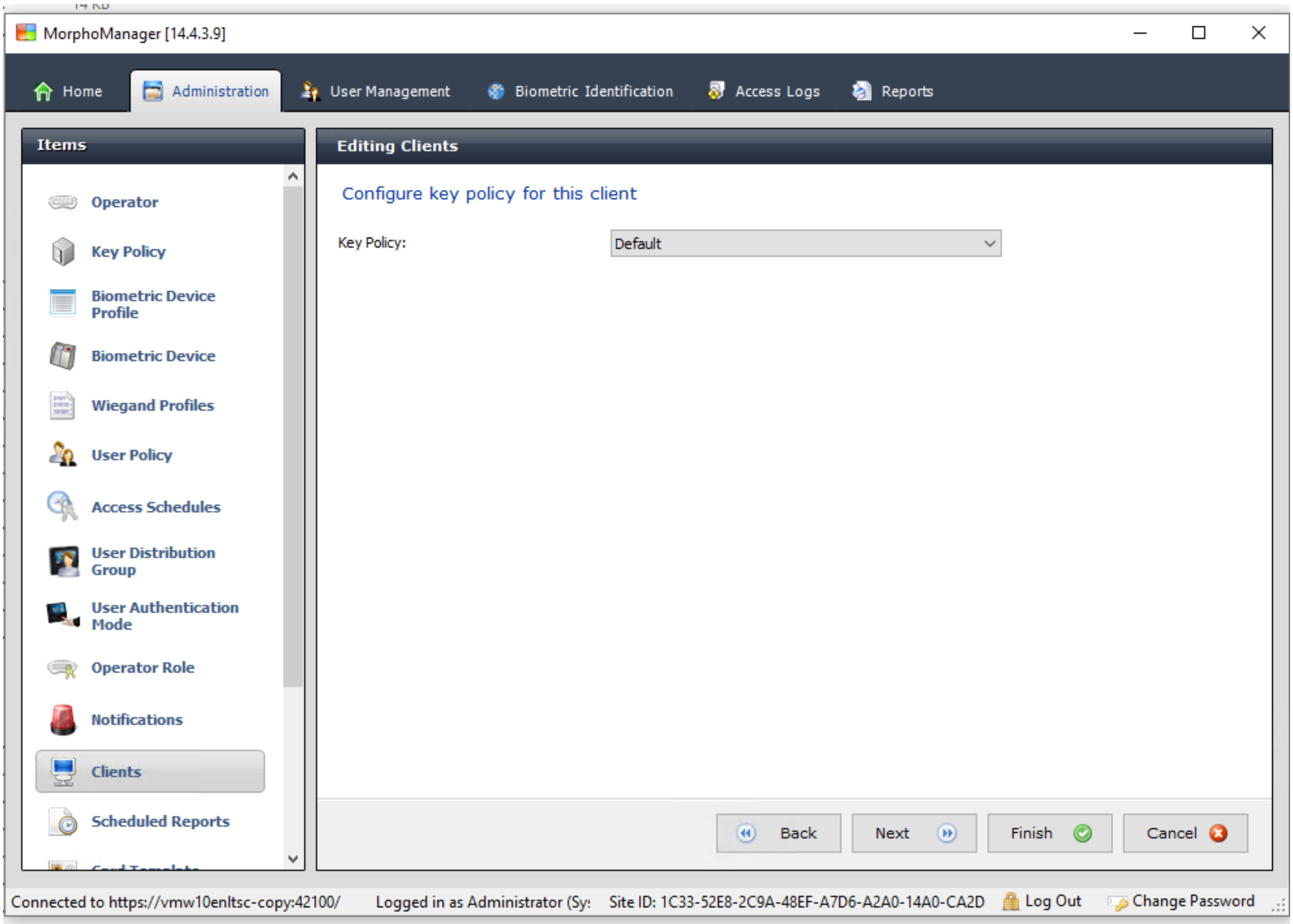


Configure Camera for this client

Camera: No Camera

Connected to https://vmw10enltsc-copy:42100/ Logged in as Administrator (Sy: Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D

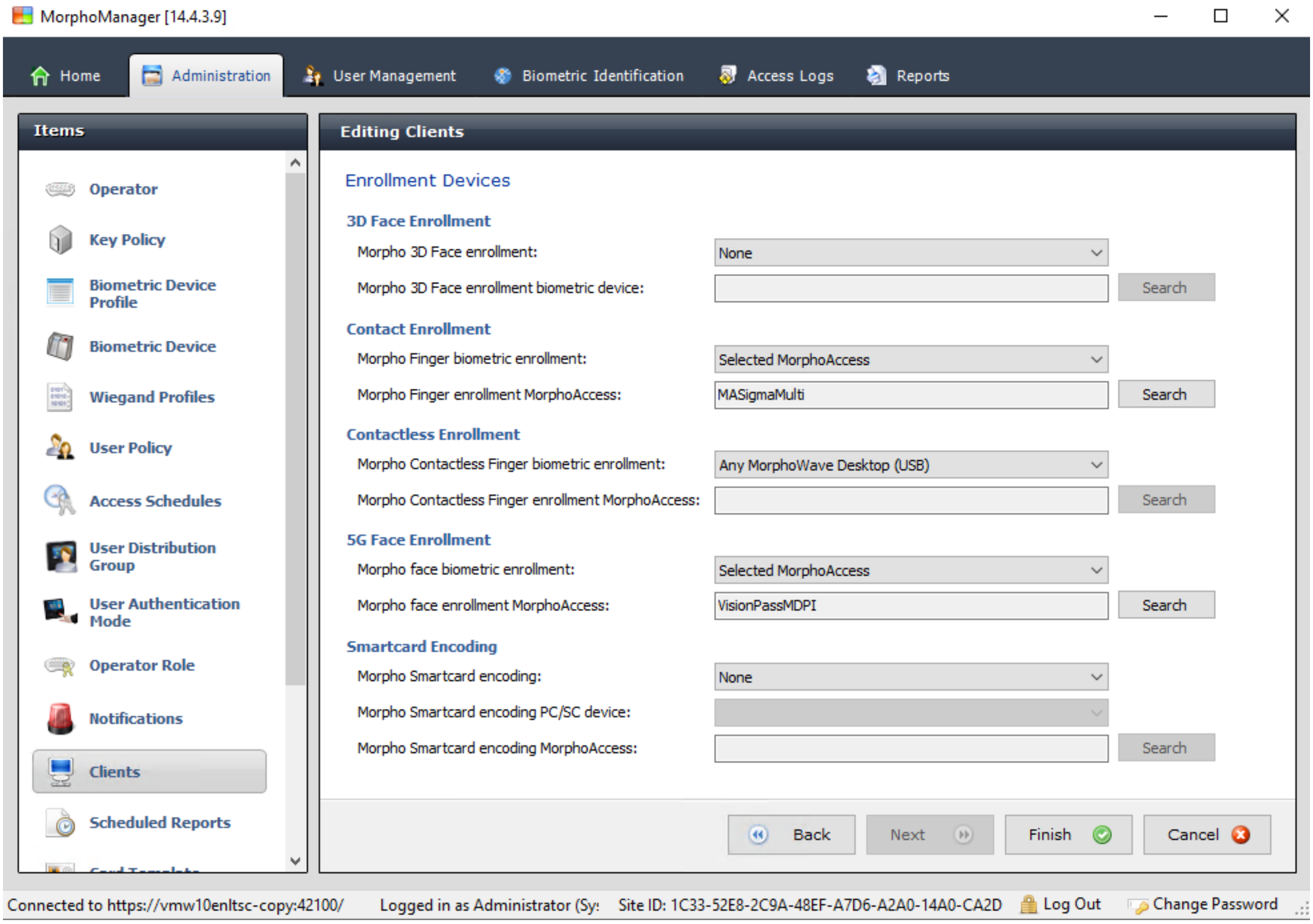
9. For **Camera:** select `No camera` from the list
10. Click **Next**



Configure key policy for this client

Key Policy: Default

11. For **Key Policy** select `Default` from the list
12. Click **Next**



Editing Clients

Enrollment Devices

3D Face Enrollment

Morpho 3D Face enrollment:	None	
Morpho 3D Face enrollment biometric device:		Search

Contact Enrollment

Morpho Finger biometric enrollment:	Selected MorphoAccess	
Morpho Finger enrollment MorphoAccess:	MASigmaMulti	Search

Contactless Enrollment

Morpho Contactless Finger biometric enrollment:	Any MorphoWave Desktop (USB)	
Morpho Contactless Finger enrollment MorphoAccess:		Search

5G Face Enrollment

Morpho face biometric enrollment:	Selected MorphoAccess	
Morpho face enrollment MorphoAccess:	VisionPassMDPI	Search

Smartcard Encoding

Morpho Smartcard encoding:	None	
Morpho Smartcard encoding PC/SC device:		
Morpho Smartcard encoding MorphoAccess:		Search

Connected to https://vmw10enltsc-copy:42100/ Logged in as Administrator (Sy: Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D

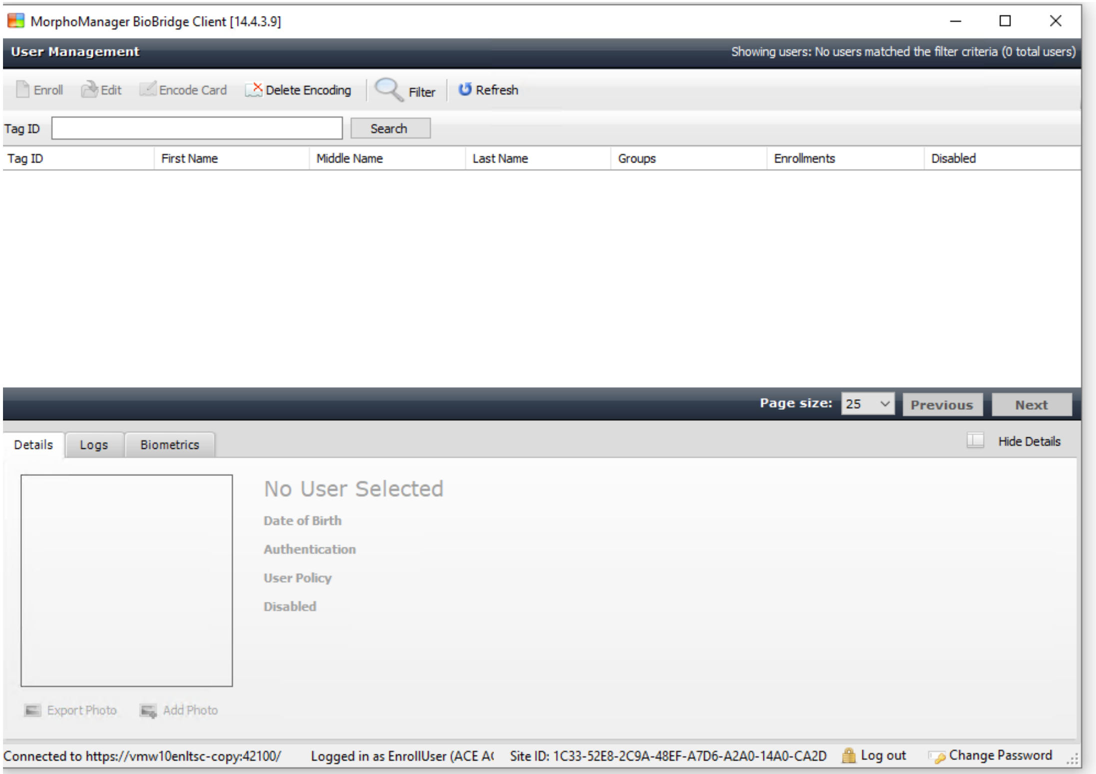
13. Select the biometric enrollment reader that you want to use on the enrollment workstation
14. Click **Finish**
15. Close the MorphoManager application

Refer to

– *Configuring the BioBridge Enrollment Client, page 23*

3.3.3 Testing the enrollment client

1. In the MorphoManager installation directory (default: *`C:\Program,Files(x86)\Morpho\MorphoManager\Client\`*)
   execute the file *`ID1.ECP4.MorphoManager.BioBridgeEnrollmentClient.exe`*



Showing users: No users matched the filter criteria (0 total users)

Page size: 25

No User Selected

Connected to https://vmw10enltsc-copy:42100/ Logged in as EnrollUser (ACE A(Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D

1. Make sure that you can invoke the enrollment screen without having to enter the username and password of the enrollment operator.

3.4 Supporting different card technologies and formats

In order for the MAC to interpret your access cards correctly, you must ensure that the Wiegand profile (or profiles) that you have defined in MorphoManager include the format (or formats) of those access cards:

General procedure

1. In MorphoManager navigate to **Administration** > **Wiegand Profile**
2. Click **Add** to create a custom Wiegand profile
3. In the related dialogs, enter the formatting information and the card technology that your system uses
4. In order to use your newly-defined Wiegand profile in the system, enter its name in the **Wiegand Profile** field of the following MorphoManager dialogs:

- **Administration > Biometric Device profile**
- **Administration > User policy**

Mifare Classic CSN

1. Add Wiegand Element `User CSN Element` and enter the following details

- **Name**: `CSN` (for example)
- **Length** `32`
- **Transformation mode:** `Reversed`

2. **Under Administration > Biometric Device profile**, on the **Multi-Factor Mode Settings** page, select the check box **MIFARE Classic**

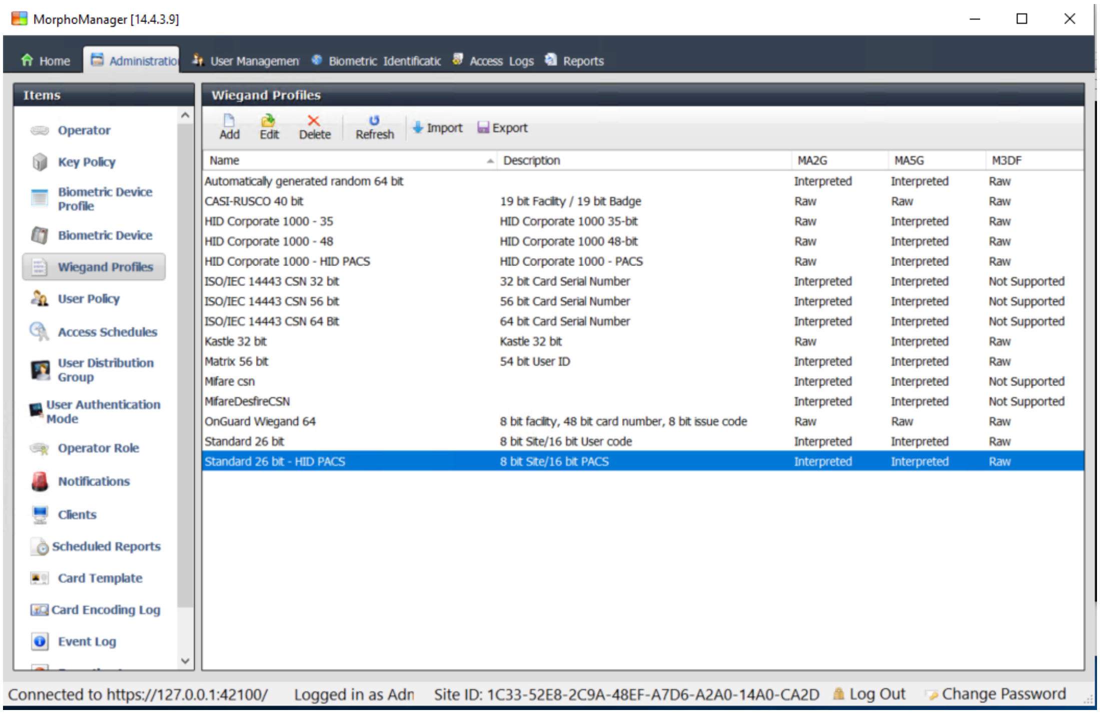
Mifare DESFire CSN

The configuration is identical to Mifare Classic except for the following details:

- **Length:** `56`
- Add **Wiegand Element User CSN Element**
  - Enter a name under **Name:**
  - For **Length** enter 56
  - For **Transformation mode:** enter `Reversed`
- **Under Administration > Biometric Device profile**, on the **Multi-Factor Mode Settings** page, select the check box **Mifare DESFire 3DES**

iClass 26 BIT

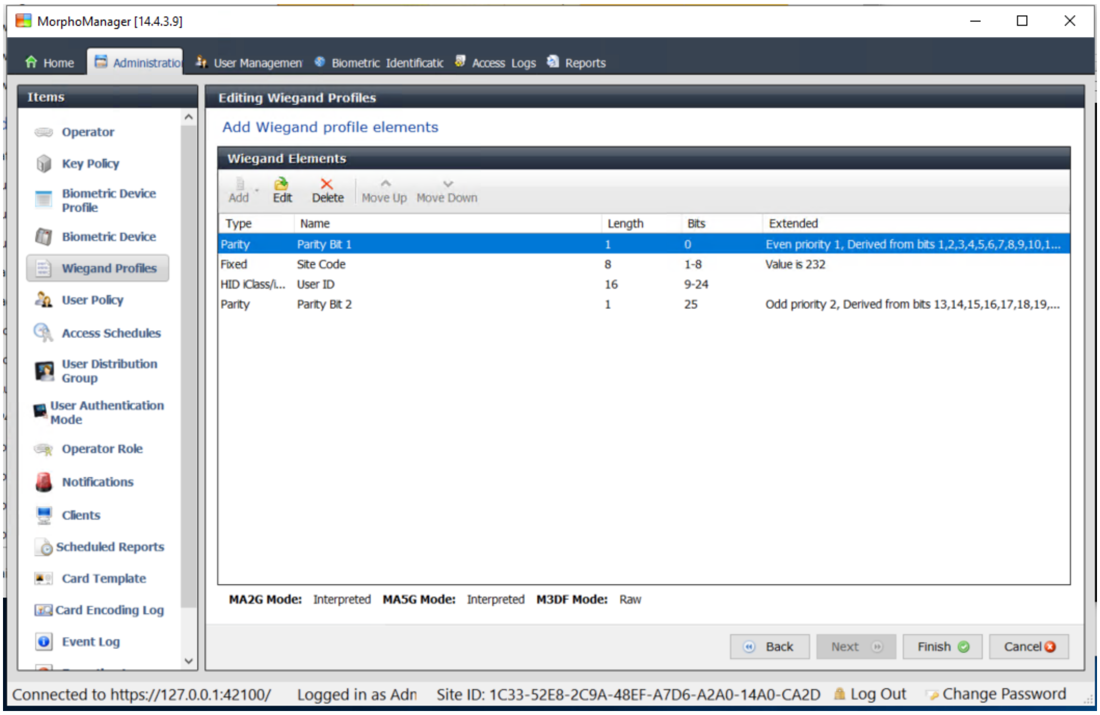
1. Select the predefined profile `Standard 26 bit-HID PACS`



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 - 35	HID Corporate 1000 35-bit	Raw	Interpreted	Raw
HID Corporate 1000 - 48	HID Corporate 1000 48-bit	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
Mifare csn		Interpreted	Interpreted	Not Supported
MifareDesfireCSN		Interpreted	Interpreted	Not Supported
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

Connected to https://127.0.0.1:42100/ Logged in as Adn Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D

2. Click **Edit**
3. Click **Next**



Editing Wiegand Profiles

Add Wiegand profile elements

Wiegand Elements

Type	Name	Length	Bits	Extended
Parity	Parity Bit 1	1	0	Even priority 1, Derived from bits 1,2,3,4,5,6,7,8,9,10,1...
Fixed	Site Code	8	1-8	Value is 232
HID iClass/i...	User ID	16	9-24	
Parity	Parity Bit 2	1	25	Odd priority 2, Derived from bits 13,14,15,16,17,18,19,...

MA2G Mode: Interpreted MA5G Mode: Interpreted M3DF Mode: Raw

Connected to https://127.0.0.1:42100/ Logged in as Adn Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D

4. Click **Edit**
5. Delete the line `Fixed Facility Code`
6. Select the line `HID iClass SEP User ID`
7. Click **Edit**
8. Change the length of the User ID from *1..16* to *1..24*
9. **Under Administration > Biometric Device profile**, on the Biometric Device Settings page, for Wiegand Profile select `Standard 26 BIT-HID-PACS`
10. **Under Administration > Biometric Device profile**, on the **Multi-Factor Mode Settings** page, select the check box `HID iClass`
11. Click Next until you reach the page **Custom Parameters**
12. Click **Add**
13. Add custom parameter (case-sensitive) Wiegand.site_code_propagation
14. Set its value to *1*
15. Click **Finish**.
16. Enter this completed Wiegand profile under **Administration > User policy**

iClass 35 BIT

1. Select the predefined profile `HID Corporate 1000 35 BIT`
2. Click **Edit**
3. Click **Next**
4. Select and delete the element line `Fixed Company ID`
5. Select and delete the element line `User Card ID Number`
6. Add the element line `HID iClass/iClass SE PACS Data` and in its element details, set the following:

- Name: `Card ID Number`
- Length: *32*
- **Under Administration > Biometric Device profile**, on the **Multi-Factor Mode Settings** page, select the check box `HID iClass`
- Click **Next** until you reach the page **Custom Parameters**
- Click **Add**

- Add custom parameter (case-sensitive) Wiegand.site_code_propagation
- Set its value to `1`
- Click **Finish**.
- Enter this completed Wiegand profile under **Administration > User policy**

iClass 37 BIT

- **Length** `37`

1. Add element Parity:

- **Name**: (for example) `EvenParityBit 1`
- **Priority**: `1`
- **Length**: `18`
- **Mode**: `Even`
- **Basis bits**: `1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18`

2. Add element `User HID iClass/iClass`

- **Name**: (for example): `Parity Bits 2`
- **Priority**: `2`
- **Length**: `19`
- **Mode**: `Odd`
- **Basis bits**: `19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37`
- **Under Administration > Biometric Device profile**, on the **Multi-Factor Mode Settings** page, select the check box `HID iClass`
- Click **Next** until you reach the page **Custom Parameters**
- Click **Add**
- Add custom parameter (case-sensitive) Wiegand.site_code_propagation
- Set its value to `1`
- Click **Finish**.
- Enter this completed Wiegand profile under **Administration > User policy**

iClass 48BIT

1. Select the predefined profile `HID Corporate 1000 48 BIT`
2. Click **Edit**
3. Click **Next**
4. Select and delete the element line `Fixed Company ID`
5. Select and delete the element line `User Card ID Number`
6. Add the element line `HID iClass/iClass SE PACS Data` and in its element details, set the following:

- Name: `User`
- Length: `45`

7. **Under Administration > Biometric Device profile**, on the **Multi-Factor Mode Settings** page, select the check box `HID iClass`
8. Click **Next** until you reach the page **Custom Parameters**
9. Click **Add**
10. Add custom parameter (case-sensitive) `Wiegand.site_code_propagation`

- Set its value to `1`

11. Click **Finish**.
12. Enter this completed Wiegand profile under **Administration** > **User policy**

HID Prox

1. Select the predefined profile *Standard 26 BIT*
2. Click **Edit**
3. Click **Next**
4. Delete the line *Fixed Facility Code*
5. Click **Edit**
6. Change the length of the User ID from *1..16* to *1..24*
7. **Under Administration > Biometric Device profile**, on the Biometric Device Settings page, for Wiegand Profile select *Standard 26 BIT*
8. **Under Administration > Biometric Device profile**, on the **Multi-Factor Mode Settings** page, select the check boxes:
   - **Biometry**
   - **Proximity card**
9. Click **Next** until you reach the page **Custom Parameters**
10. Click **Add**
11. Add custom parameter (case-sensitive) *Wiegand.site_code_propagation*
    - Set its value to *1*
12. Click **Finish**.
13. Enter this completed Wiegand profile under **Administration** > **User policy**

3.5 Identification modes at biometric devices

Introduction

Biometric readers can identify credential holders in different ways, known as identification modes.

- By **Card OR Biometry**, depending on what the credential holder presents to the reader
- By **Card AND Biometry**, that is the user must verify through biometric credentials that they are the true owners of the card.
- By **Biometry only**

This section describes how to set configure these modes in MorphoManager.

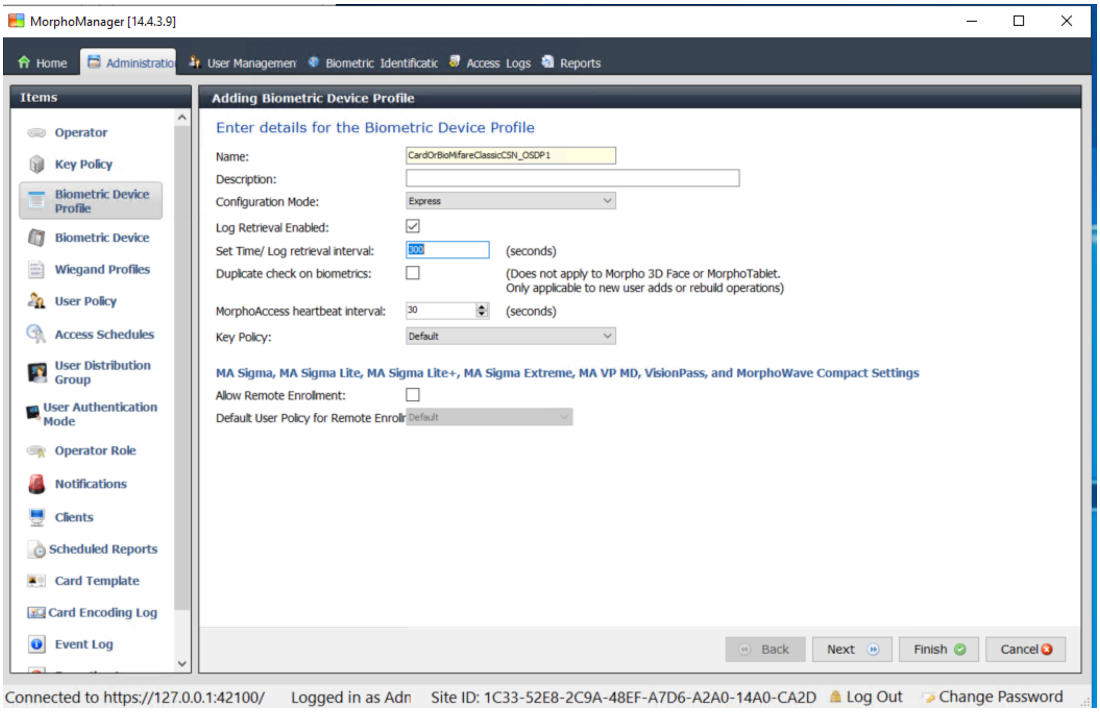
Dialog path

In MorphoManager **Administration** tab

3.5.1 Card OR Biometry

Make the following settings if users are to identify themselves EITHER by card OR by biometric credentials.

1. In MorphoManager, go to **Administration** > **Biometric Device Profile**



Adding Biometric Device Profile

Enter details for the Biometric Device Profile

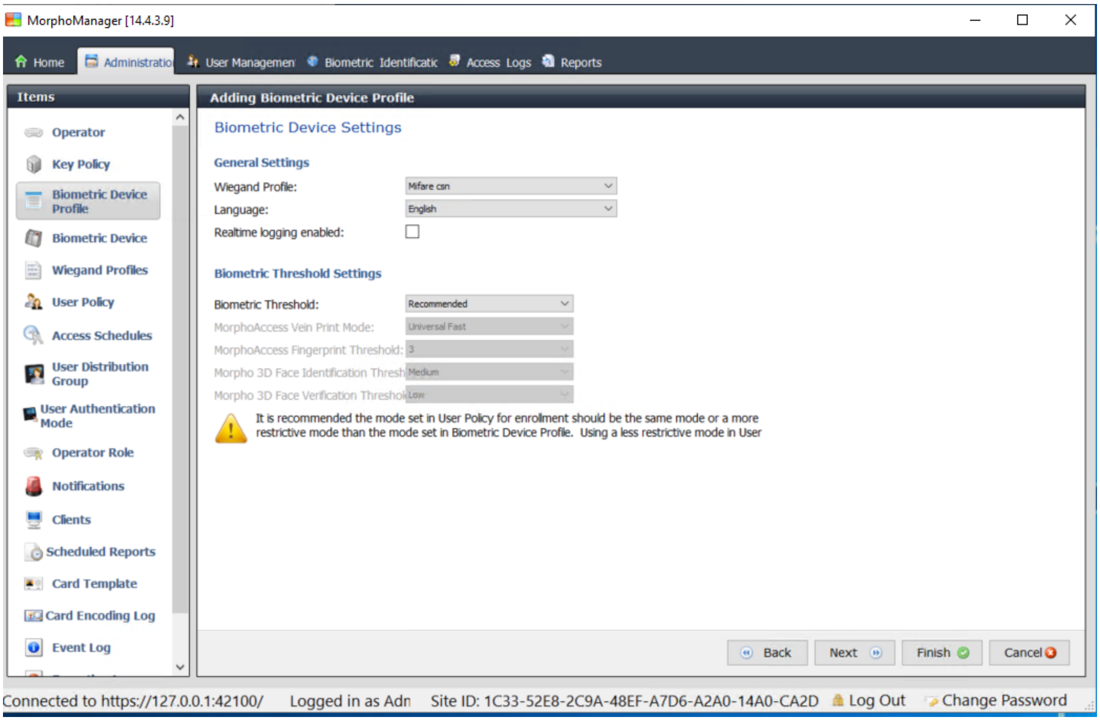
Name: CardOrBioMifareClassicCSN_OSDP1
Description:
Configuration Mode: Express
Log Retrieval Enabled: ☑
Set Time/ Log retrieval interval: 300 (seconds)
Duplicate check on biometrics: □ (Does not apply to Morpho 3D Face or MorphoTablet. Only applicable to new user adds or rebuild operations)
MorphoAccess heartbeat interval: 30 (seconds)
Key Policy: Default

MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme, MA VP MD, VisionPass, and MorphoWave Compact Settings

Allow Remote Enrolment: □
Default User Policy for Remote Enrolr Default

Connected to https://127.0.0.1:42100/ Logged in as Adn Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D Log Out Change Password

2. Click **Next** until you reach the page titled **Biometric Device Settings**



Adding Biometric Device Profile

Biometric Device Settings

General Settings

Wiegand Profile: Mifare csn
Language: English
Realtime logging enabled: □

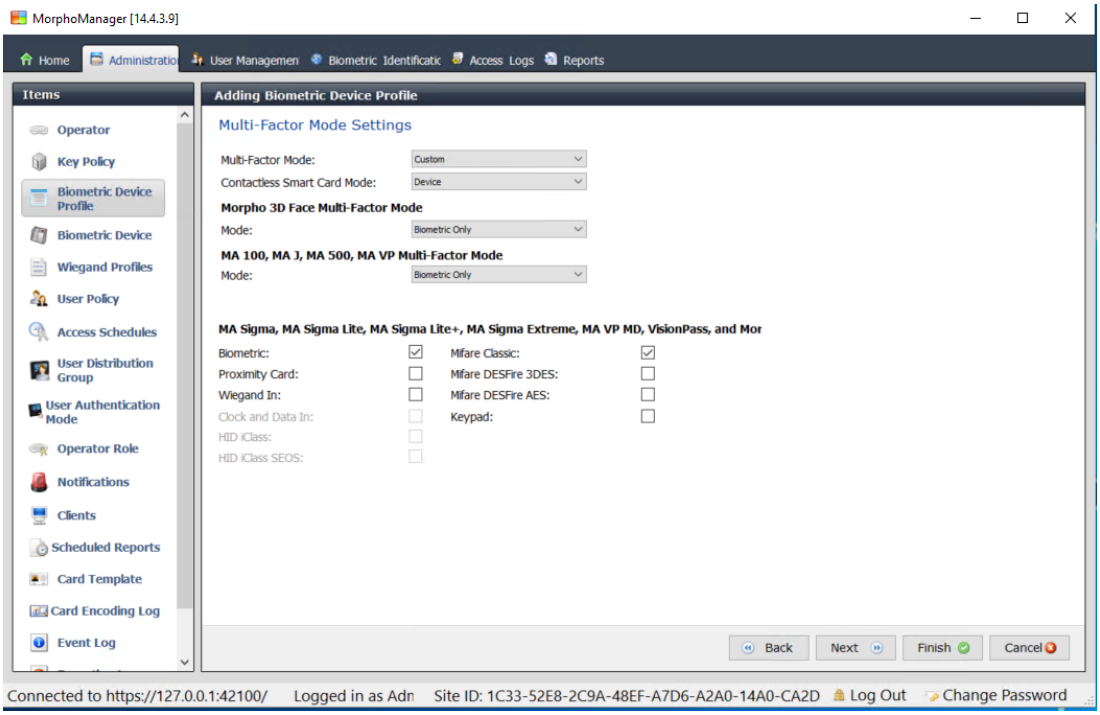
Biometric Threshold Settings

Biometric Threshold: Recommended
MorphoAccess Vein Print Mode: Universal Fast
MorphoAccess Fingerprint Threshold: 3
Morpho 3D Face Identification Thresh Medium
Morpho 3D Face Verification Threshol Low

It is recommended the mode set in User Policy for enrolment should be the same mode or a more restrictive mode than the mode set in Biometric Device Profile. Using a less restrictive mode in User

Connected to https://127.0.0.1:42100/ Logged in as Adn Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D Log Out Change Password

3. For **Wiegand Profile**, select the same profile that you defined for your biometric devices when setting up BioBridge.



Adding Biometric Device Profile

Multi-Factor Mode Settings

Multi-Factor Mode: Custom

Contactless Smart Card Mode: Device

Morpho 3D Face Multi-Factor Mode

Mode: Biometric Only

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

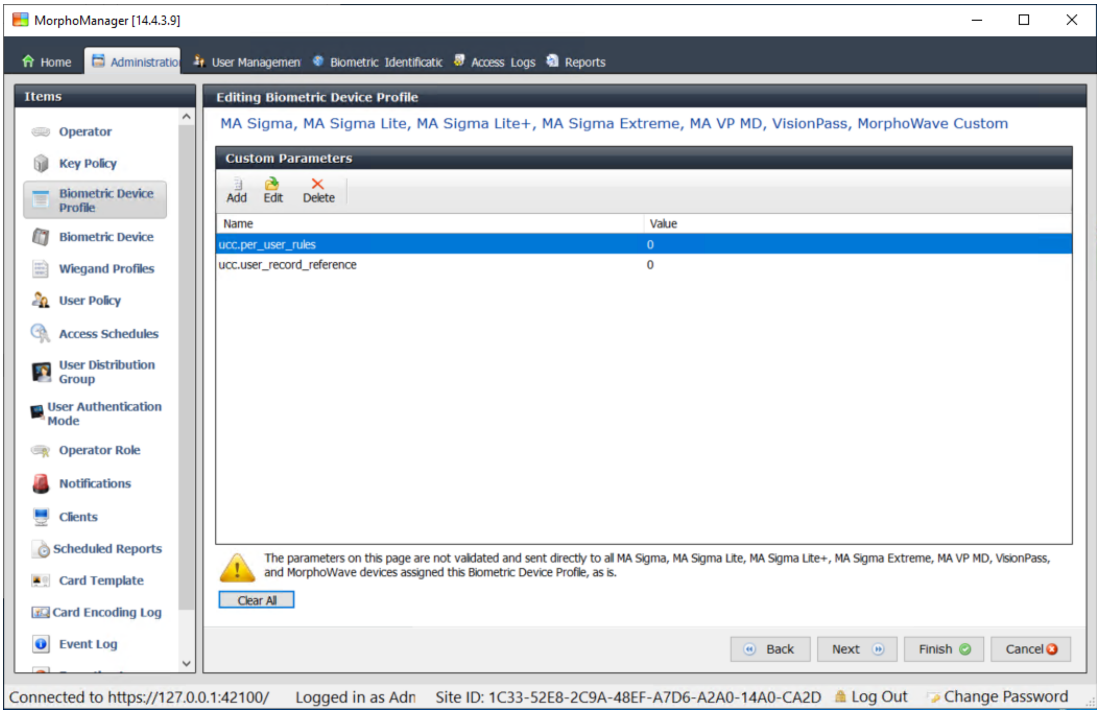
Mode: Biometric Only

MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme, MA VP MD, VisionPass, and Mor

Biometric:	☑	Mifare Classic:	☑
Proximity Card:	□	Mifare DESFire 3DES:	□
Wiegand In:	□	Mifare DESFire AES:	□
Clock and Data In:	□	Keypad:	□
HID iClass:	□		
HID iClass SEOS:	□		

Connected to https://127.0.0.1:42100/ Logged in as Adn Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D

4. Select the **Biometric** check box, plus the check box of the card technology that your installation uses.
5. Click **Next** until you reach the **Custom Parameters** screen



Editing Biometric Device Profile

MA Sigma, MA Sigma Lite, MA Sigma Lite+, MA Sigma Extreme, MA VP MD, VisionPass, MorphoWave Custom

Custom Parameters

Name	Value
ucc.per_user_rules	0
ucc.user_record_reference	0

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

Connected to https://127.0.0.1:42100/ Logged in as Adn Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D

6. Click **Add** to add two custom parameters.
   Note: If these two parameters are set, the reader sends the card data directly to the AMC. The user does need not be enrolled on the IDEMIA reader.

– *ucc.per_user_rules*

– *ucc.user_record_reference*

7. Click **Finish**

Assign this user policy to the users

1. In MorphoManager, go to **Administration** > **User Policy**
2. Set the following attributes for **User Authentication Mode:**

- Enable **Allow Start By Biometric**
- Enable **Allow Start By Contactless Card**
- Disable **Require Template Match**

3. Click **Finish**

3.5.2 Card AND Biometry

Make the following settings if users must use a card AND biometric credentials, to verify that they are the owners of the card.

1. In MorphoManager, go to **Administration** > **Biometric Device Profile**
2. Click **Next** until you reach the page titled **Biometric Device Settings**
3. For **Wiegand Profile**, select the same profile that you defined for your biometric devices when setting up BioBridge.
4. Click **Next** until you reach the page titled **Multi-Factor Mode Settings**
5. Select the check box of the card technology that your installation uses.
6. Click **Finish**

Assign this user policy to the users

1. In MorphoManager, go to **Administration** > **User Policy**
2. For **User Authentication Mode** select *`Contactless Card ID + Biometric`* from the list.
3. Click **Finish.**

3.5.3 Biometry only

Make the following settings if users are to identify themselves by biometric credentials only.

1. In MorphoManager, go to **Administration** > **Biometric Device Profile**
2. Click **Next** until you reach the page titled **Biometric Device Settings**
3. For **Wiegand Profile**, select the same profile that you defined for your biometric devices when setting up BioBridge
4. Click **Next** until you reach the page titled **Multi-Factor Mode Settings**
5. For **Multi-Factor Mode** select *`Biometry only`* from the list
6. Click **Finish**

Assign this user policy to the users

1. In MorphoManager, go to **Administration** > **User Policy**
2. For **User Authentication Mode** select *`Biometric(1:many)`* from the list.
3. Click **Finish.**

3.6 Technical notes and limits

Officially supported windows operating systems

IDEMIA supports the same Windows 10 versions as ACE .

Officially supported version of Microsoft SQL Server

The support version is SQL Server 2017

One IDEMIA system per Access System

A Bosch access control system can support only one IDEMIA system.

One IDEMIA card per cardholder.

Bosch access control systems support multiple cards per cardholder, but IDEMIA supports only one. Therefore, upon enrollment, and when synchronizing with BIS, the first valid card (that is, where status=1) of type “Access”, “Temporary” or “Parking” is assigned to IDEMIA. If the card is later blocked, its number is still transmitted and recorded in the event log.

Maximum number of IDEMIA cardholders

The BioBridge MorphoManager can handle up to 100,000 cardholders.

Maximum number of access groups

IDEMIA supports up to 5000 access groups (user distribution groups). These are mapped to **Person classes** in the Bosch access control system.

Performance of templates download

- 1000 templates to 1 device: Download takes under 1 minute.
- 1000 templates to 100 devices: Download in some minutes.

IDEMIA does not support BIS-ACE Divisions

Where an IDEMIA system is integrated, an ACE system is not able to screen the cardholders of one Division reliably from the access control operators of another Division. If absolute privacy is mandatory between Divisions, do not integrate an IDEMIA system.

Virtual Cards / Access by PIN code alone.

IDEMIA does not support access by PIN code alone. A physical card is required.

IDEMIA duress-finger functionality

The IDEMIA duress finger functionality is currently not supported by AMC controllers.

Minimum set of identification criteria.

Enrollment in the IDEMIA system requires at least the following identification criteria:

- First name,
- Last name,
- Person class
- One physical card assigned to the cardholder.

States displayed on the readers

No reader state (e.g. device blocked) is displayed on Wiegand and OSDP readers.

Backup and Restore

Before restoring a backup of a Backup of an ACE system with IDEMIA, delete and recreate the IDEMIA database using the IDEMIA DataBridge provider tool.

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com