



BOSCH

Building Integration System

Integrating IDEMIA Biometrics with ACE

en

Configuration Guide

Table of contents

1	Introduction	4
2	System overview	5
3	Configuring IDEMIA Universal BioBridge	6
3.1	Setting up BioBridge in the Bosch access control system	6
3.2	Setting up BioBridge in MorphoManager	8
3.2.1	Wiegand Profiles	8
3.2.2	Biometric Device Profile	9
3.2.3	Biometric Device(s)	12
3.2.4	User Policy	14
3.2.5	User Distribution Groups	14
3.2.6	Setting up ODBC for BioBridge	16
3.2.7	BioBridge System Configuration	20
3.3	Configuring the BioBridge Enrollment Client	23
3.3.1	Adding an enrollment operator to Morpho Manager	23
3.3.2	Configuring the MorphoManager client computers for enrollment tasks	23
3.3.3	Testing the enrollment client	29
3.4	Supporting different card technologies and formats	30
3.5	Identification modes at biometric devices	34
3.5.1	Card OR Biometry	34
3.5.2	Card AND Biometry	37
3.5.3	Biometry only	37
3.6	Technical notes and limits	37

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

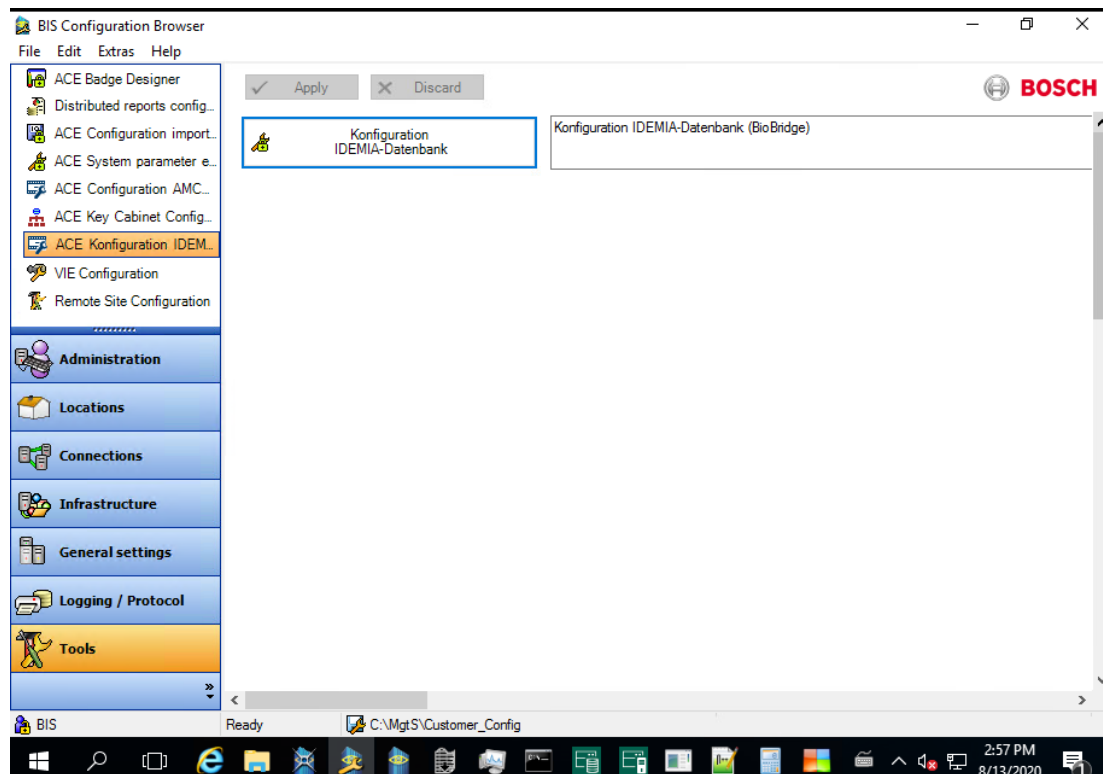
3.1 Setting up BioBridge in the Bosch access control system

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**



1. Click **Configuration IDEMIA database**

The **IDEMIA BioBridge Data Provider** dialog appears.



IDEMIA BioBridge Data Provider

Database instance

Server (name or IP address):

Database instance:

User name:

Password:

IDEMIA database definition

IDEMIA database:

IDEMIA user name:

IDEMIA password:

Confirm password:

User distribution groups

Select	Person class	User distribution group	
<input checked="" type="checkbox"/>	Employee	Employee	
<input checked="" type="checkbox"/>	External personnel	External personnel	
<input type="checkbox"/>	Visitor	Visitor	

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**.

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



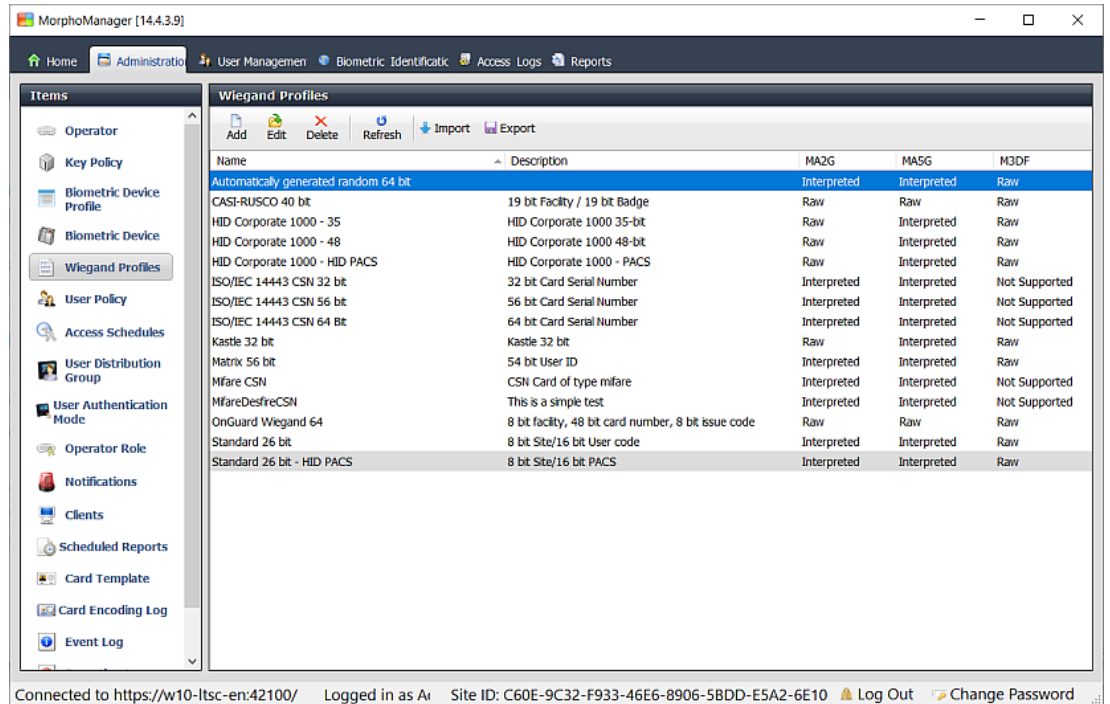
Notice!

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.



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

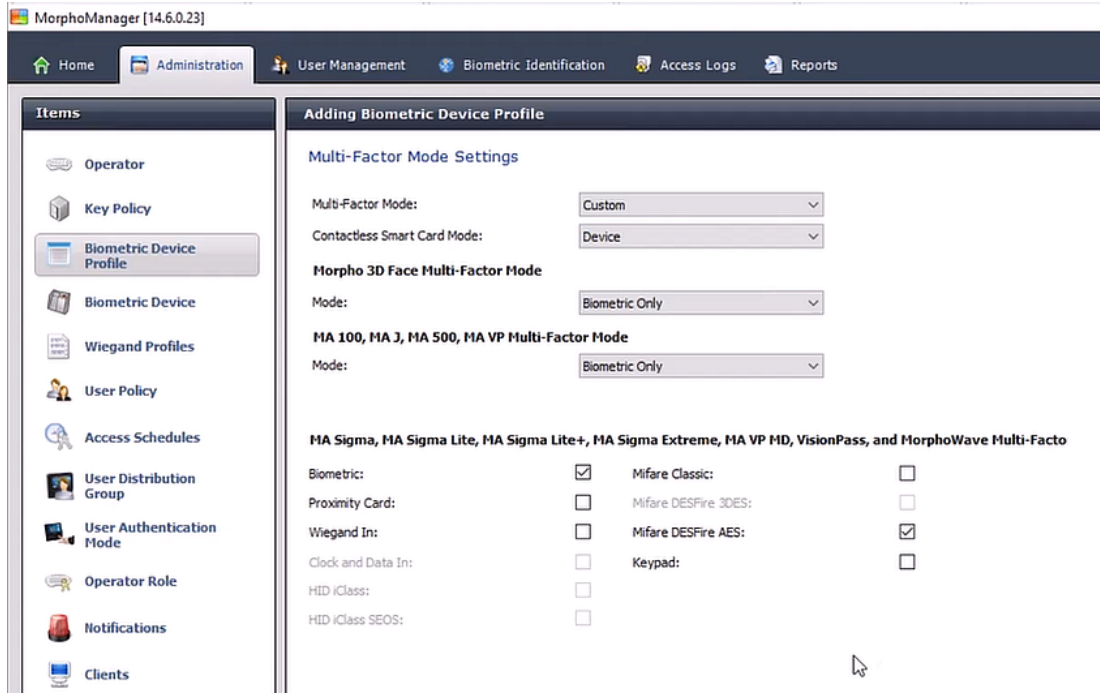
Biometric Device Profile

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.

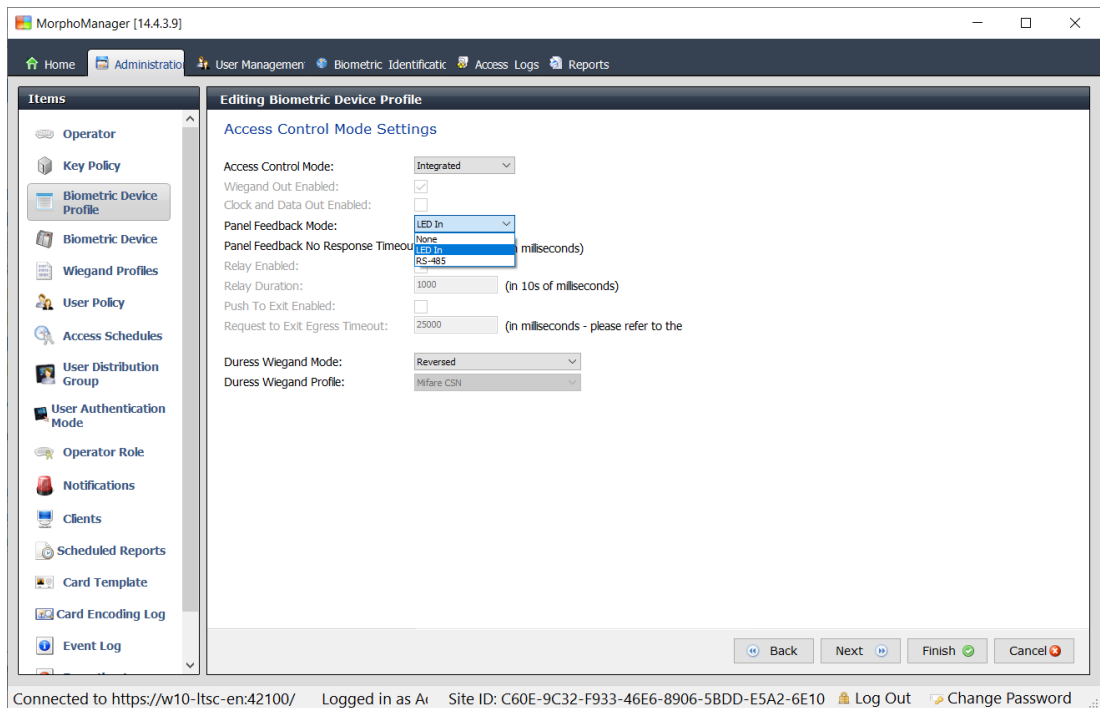
The following procedure assumes that you are deploying biometric readers from IDEMIA with additional card-reading technology.

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.



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



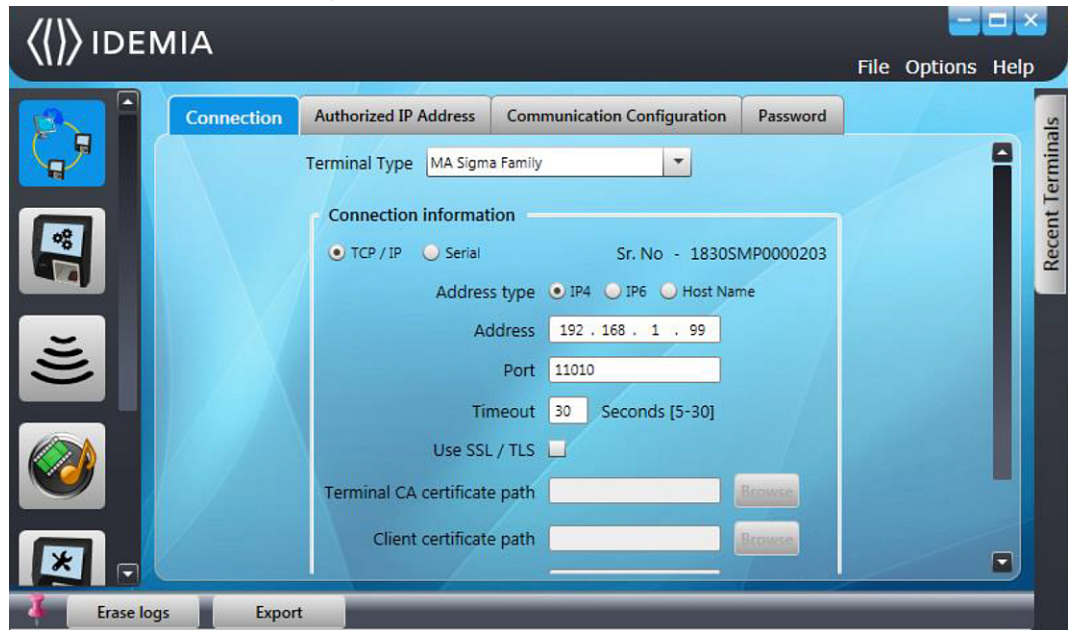
At this point, the procedures for Wiegand and OSDP AMCs diverge. Follow the procedure that corresponds to your AMC controller type:

For Wiegand AMCs

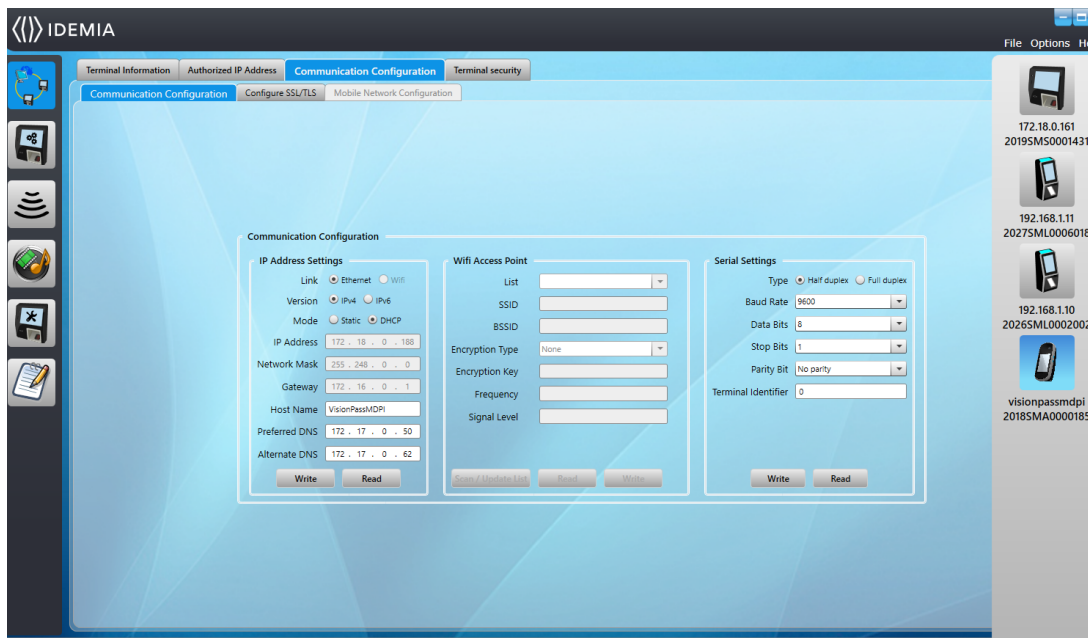
1. Set **Access Control Mode** to *Integrated*
2. Set **Panel feedback Mode** to *LED In*
3. Click **Finish**

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



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



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.

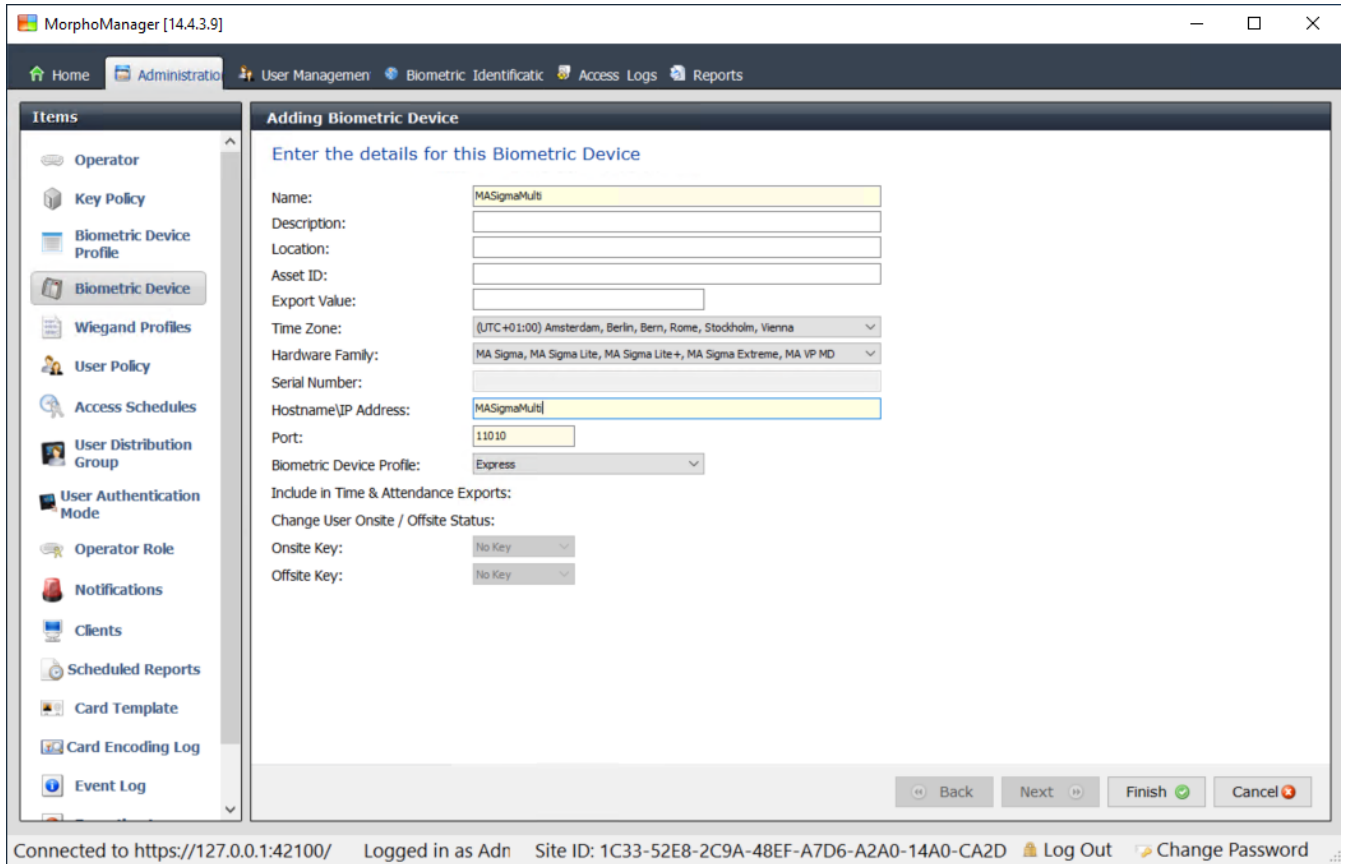
3.2.3

Biometric Device(s)

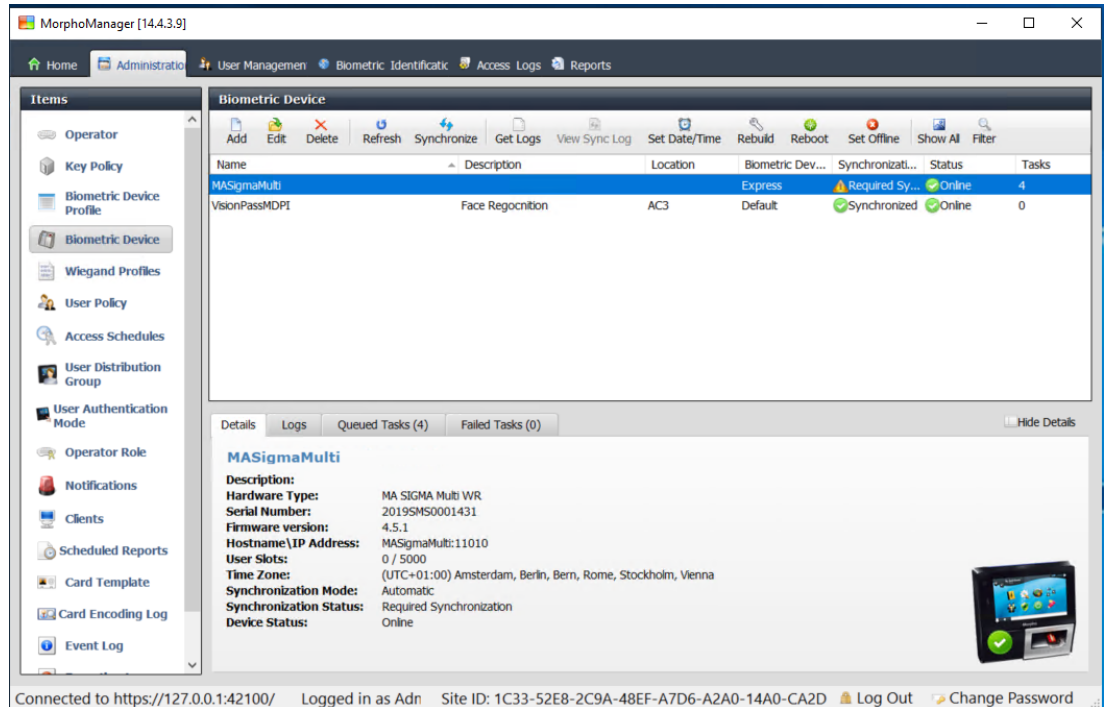
The biometric devices test whether the biometric credentials that they read match records in the database. They also keep a log of every usage event.

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 earlier
4. Click **Finish**



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



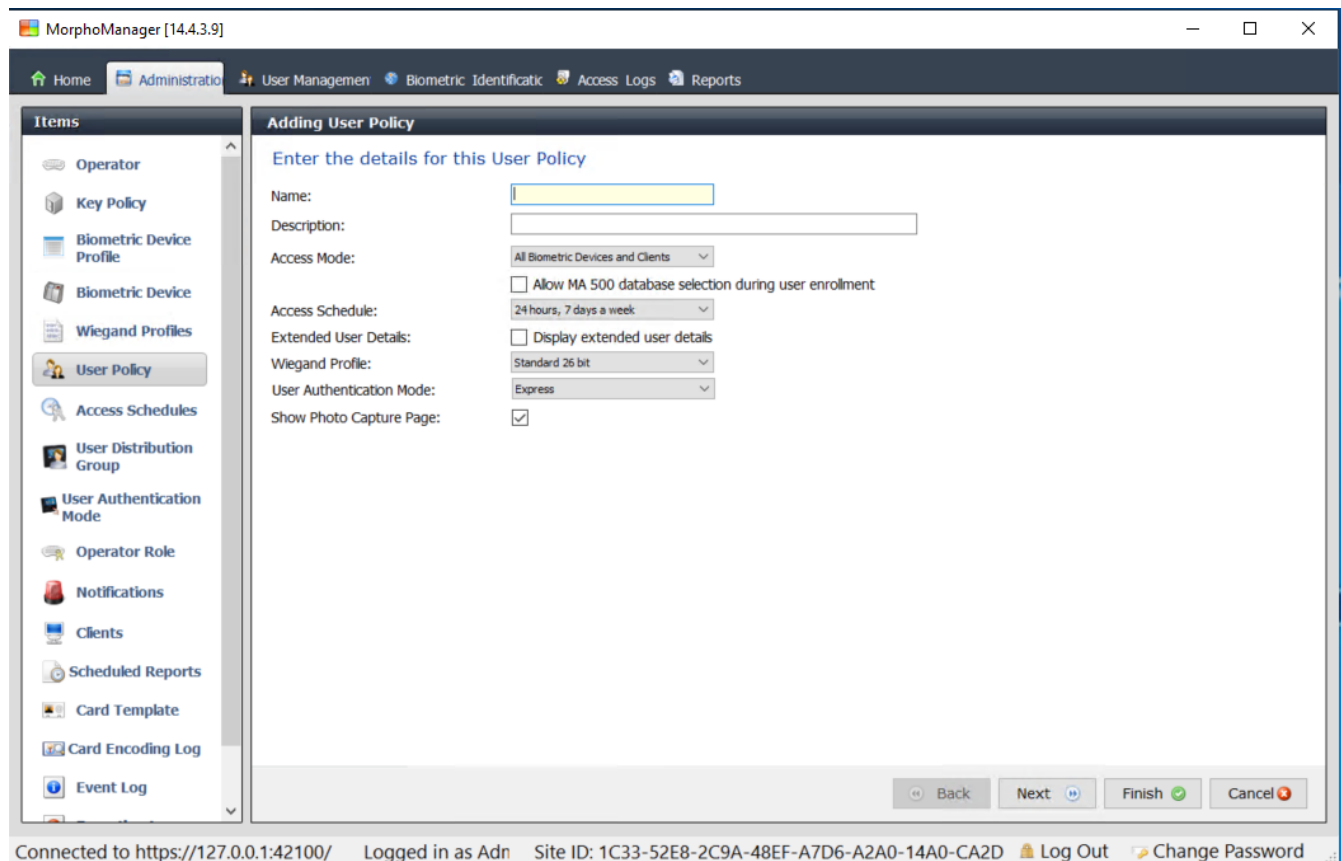
3.2.4

User Policy

User policies 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.



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.

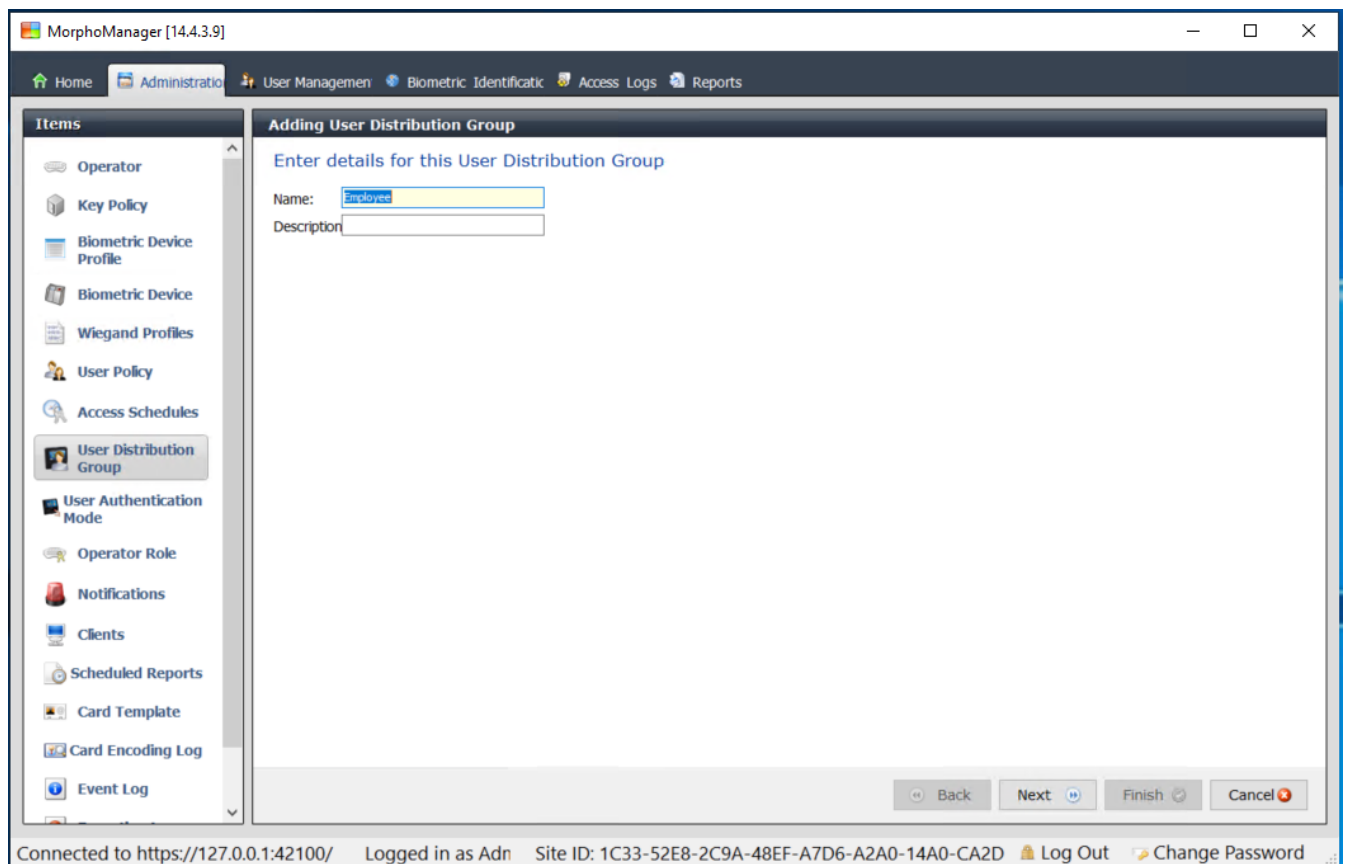
Prerequisites:

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

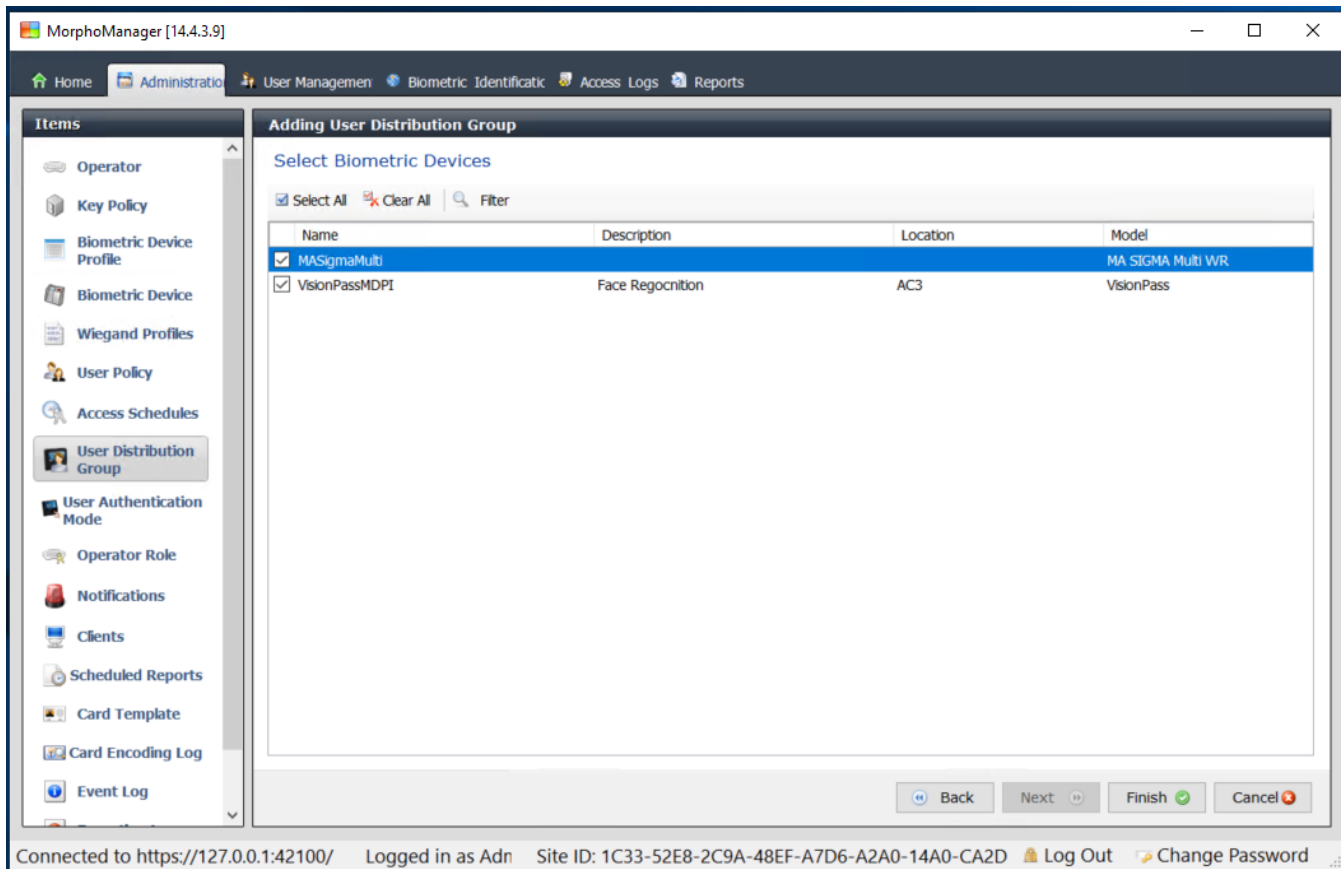
Each User Distribution Group must be mapped to at least one Person Class in ACE . Therefore create at least one User Distribution Group for each Person Class that you use.

Procedure:

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



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.



5. Click **Finish**

3.2.6 Setting up ODBC for BioBridge

Introduction

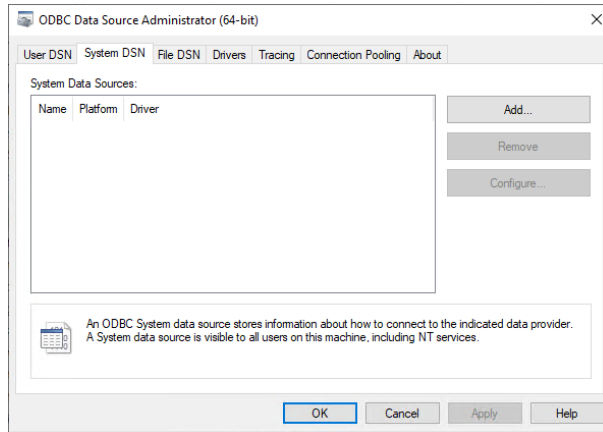
Open Database Connectivity (ODBC) is a prerequisite for use of MorphoManager BioBridge. ODBC is a standardized programming interface for accessing different databases. The recommended driver is *OdbcDriver17SQLServer*, which you can find on the BIS installation media at

BIS\3rd_Party\OdbcDriver17SQLServer

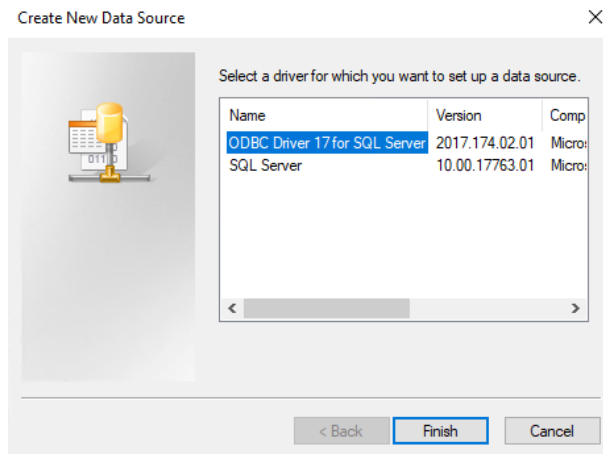
Creating a Data Source

Creating a Data Source name (DSN) for ODBC

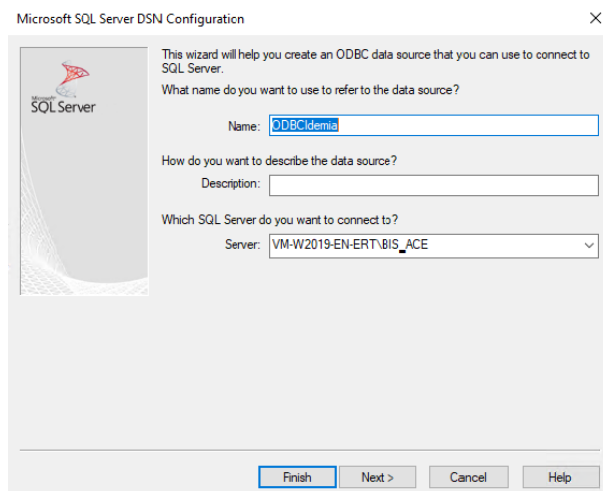
1. In the Windows Control Panel select **Administrative Tools**.
2. Select *ODBC Data Sources (64-bit)* from the list.
3. Select the **System DSN** tab.



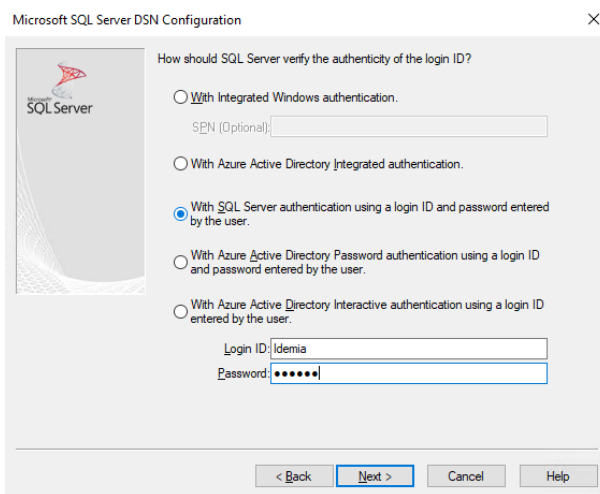
- 4. Click **Add** to select a driver.
- 5. Select *ODBC Driver 17 for SQL Server* as the driver, and click **Finish**.



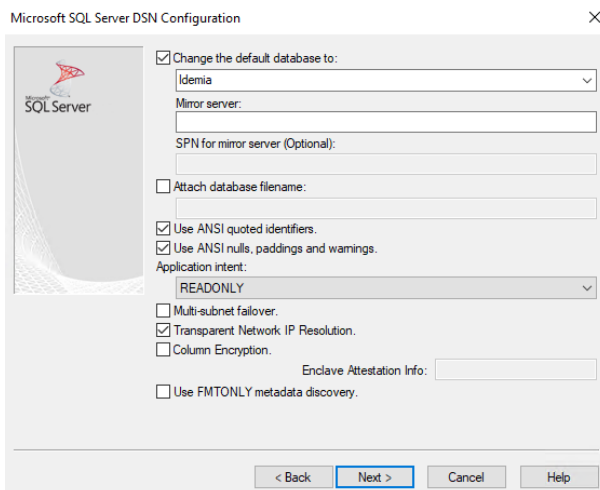
- 6. Enter the following details for the Data Source.
 - **Name:** a name for the data source
 - **Description** (optional)
 - **Server:** the name of the computer where the ACE database is installed, and the name of the database (default: <MyACEserver>\BIS_ACE)



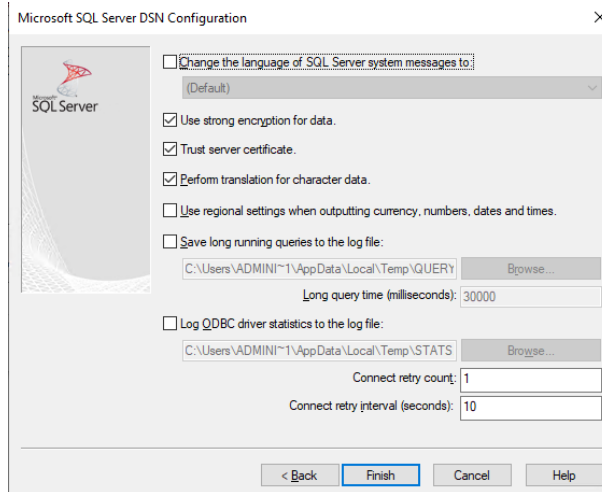
- 7. Click **Next >**
A dialog appears to collect login information



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*

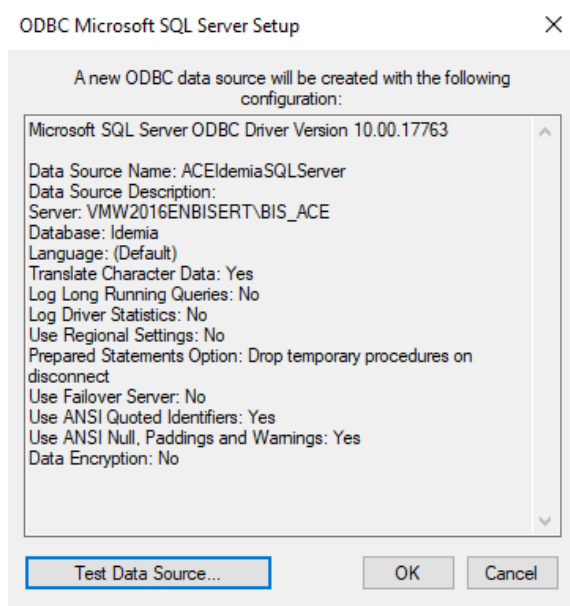


13. Click **Next >**
14. In the next dialog, select the check boxes
 - **Use strong encryption for data**
 - **Perform translation for character data**
 - **Trust server certificate**

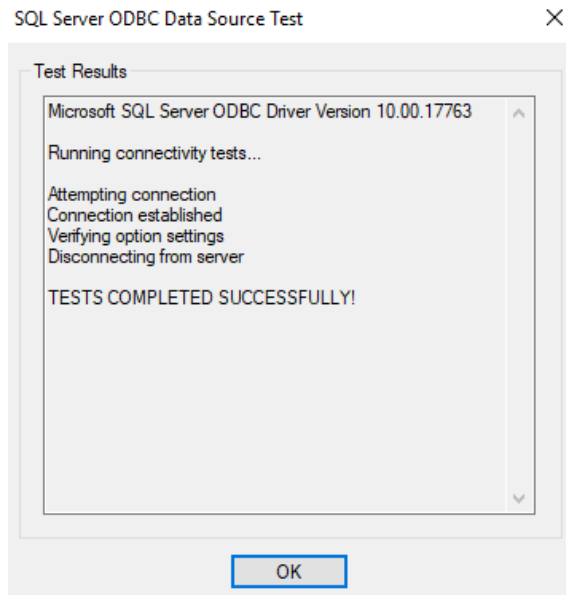


15. Click **Finish**

16. In the next dialog, review the summary data



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



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

3.2.7

BioBridge System Configuration

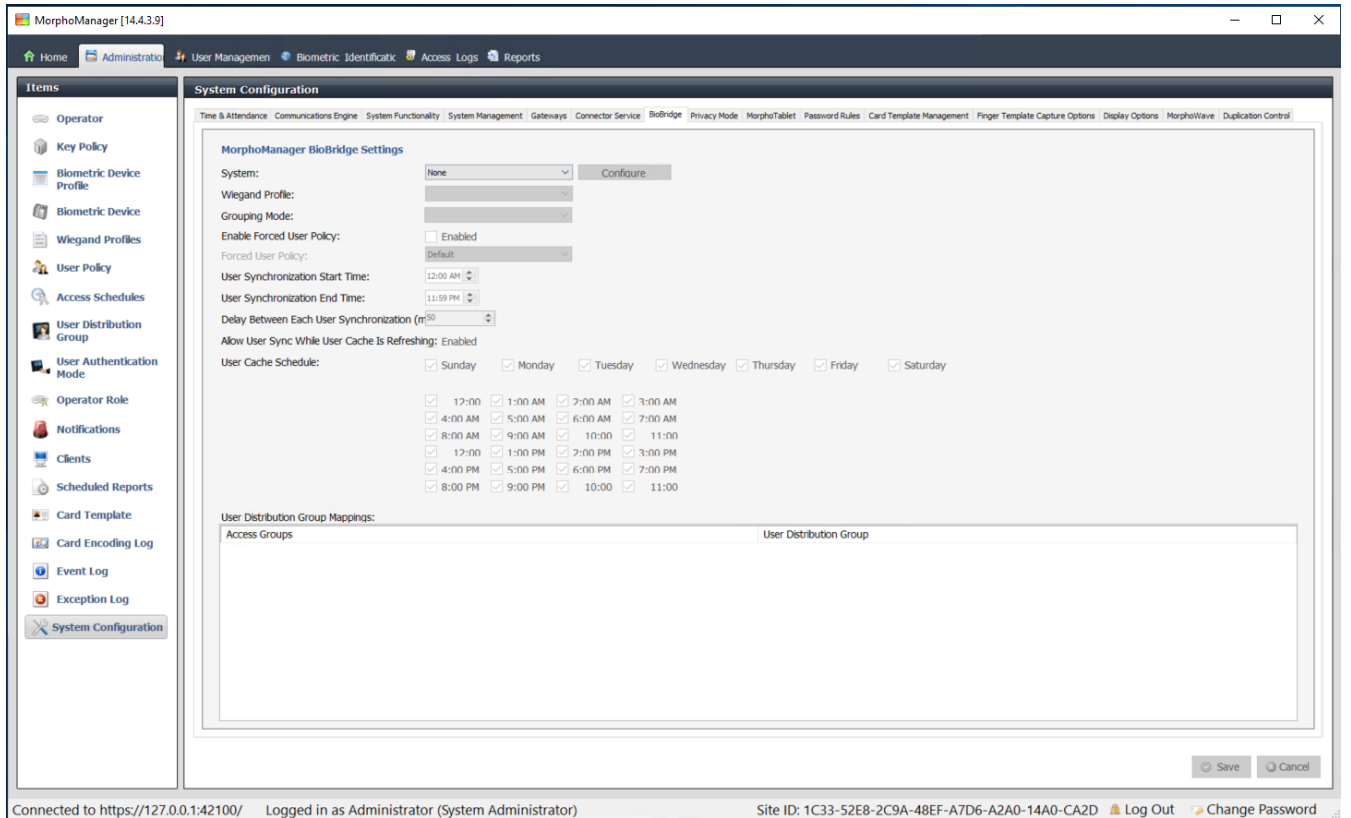
This section describe the remaining settings required for access control systems to use the BioBridge interface.

Prerequisite

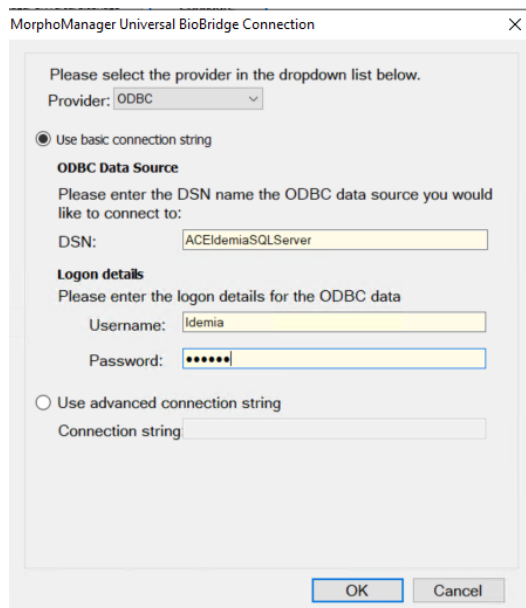
ODBC is set up for BioBridge. See *Setting up ODBC for BioBridge*, page 16

Procedure:

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



3. In the **System** drop-down list, select *MorphoManager Universal BioBridge*
4. Click **Configure**
A popup dialog appears.



- 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**.

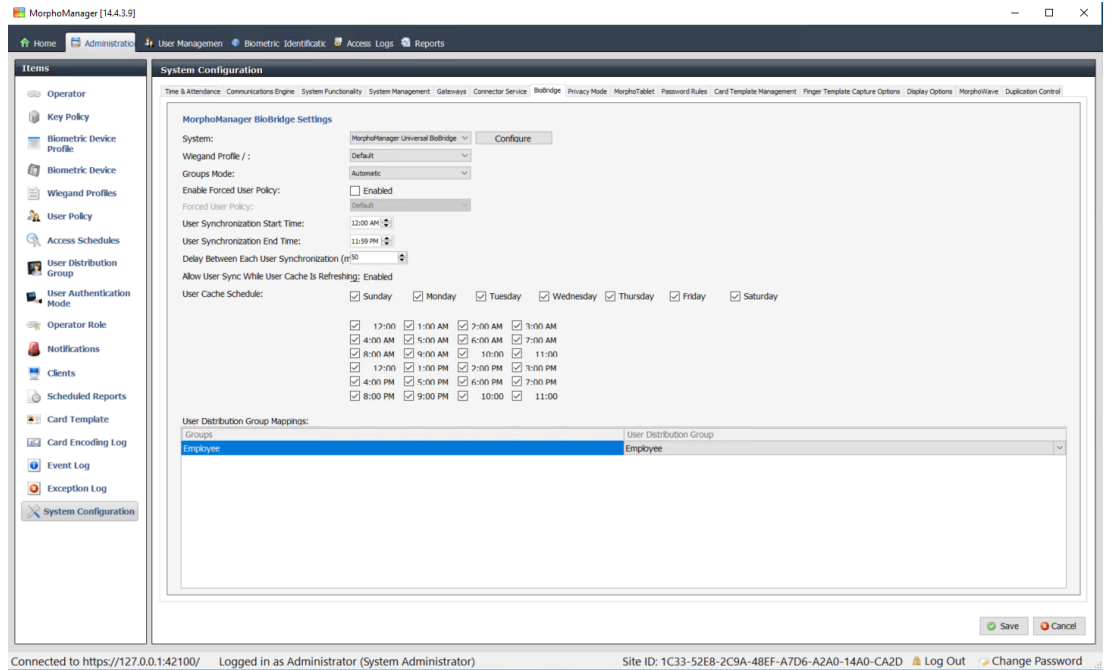
Other settings

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 <i>Per User</i>
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).



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.

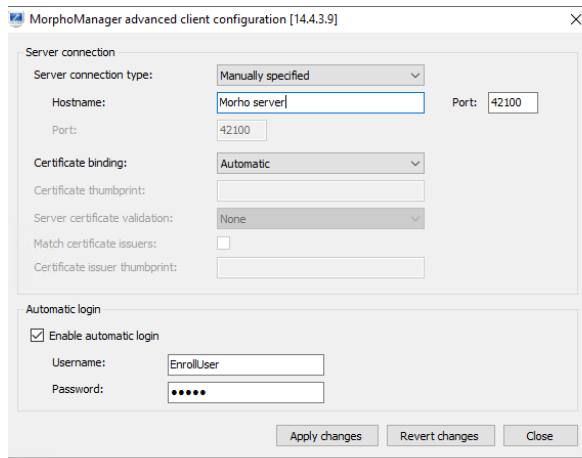
Note: for security reasons, Active Directory user accounts are recommended.

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

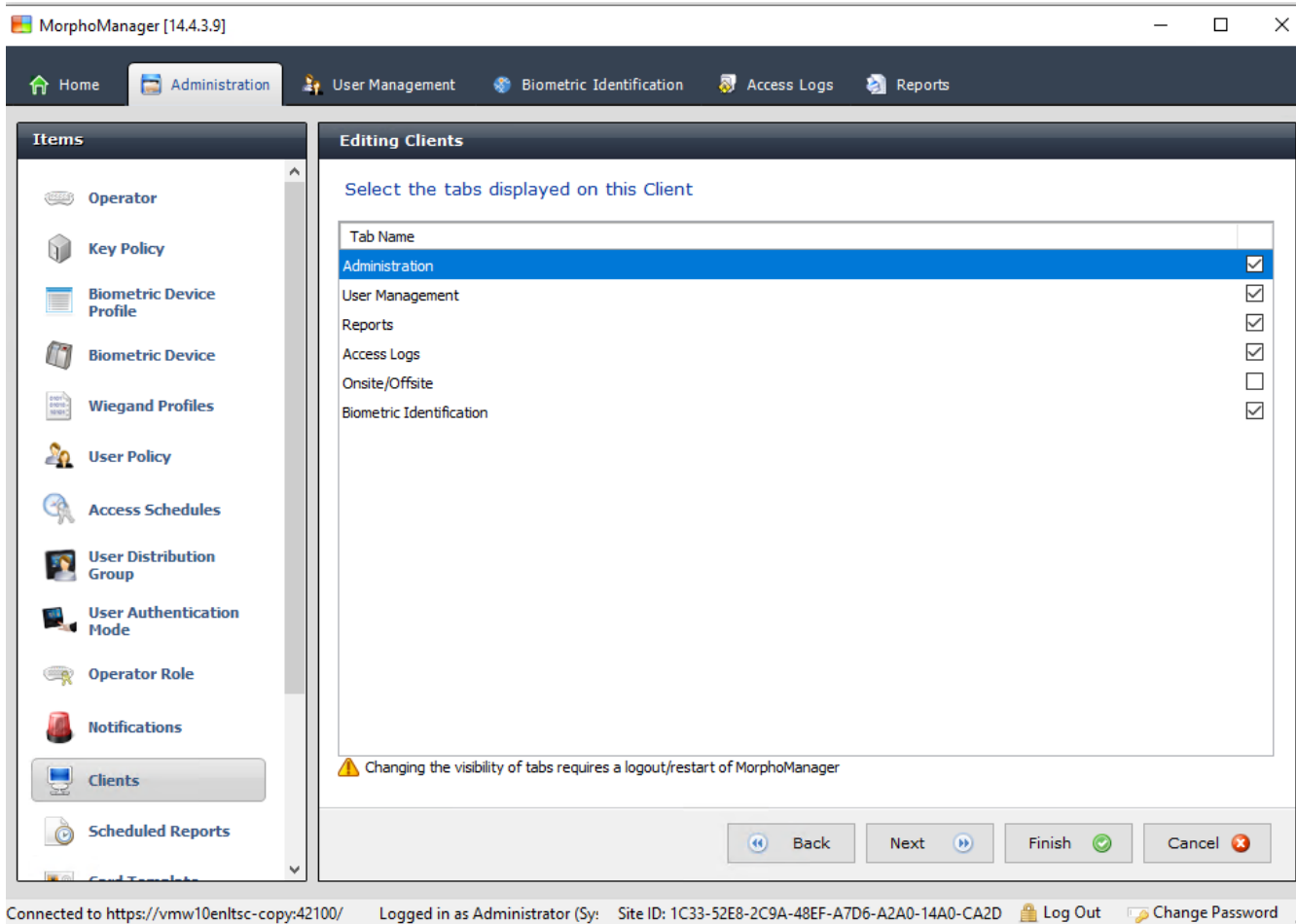
1. In the MorphoManager installation directory (default: *C:\Program Files (x86)\Morpho\MorphoManager\Client*) execute the file *ID1.ECP4.MorphoManager.AdvancedClientConfig.exe* as administrator



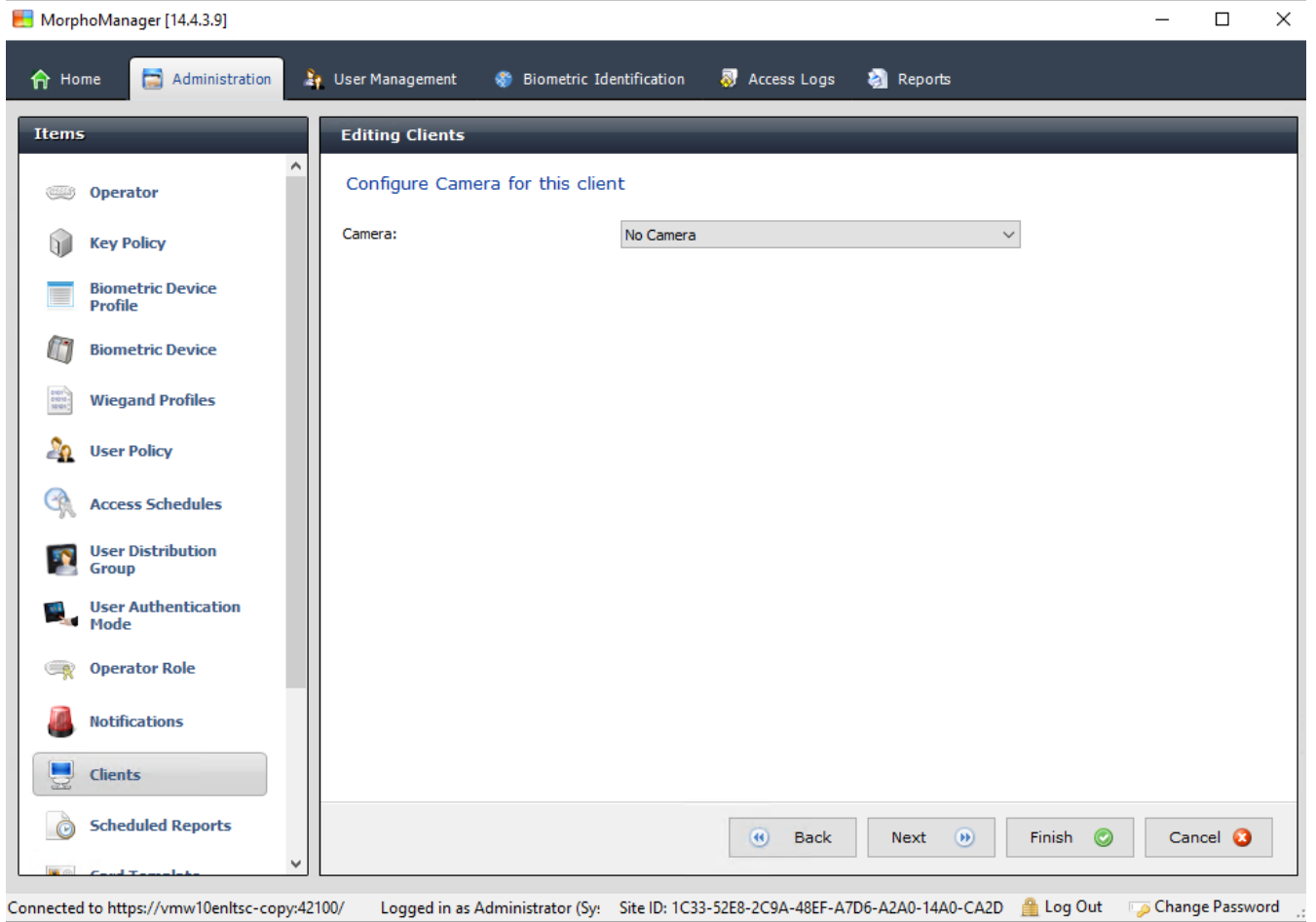
2. Enter the Hostname of the Morpho server under **Hostname**
3. Under **Automatic login**
 - Select the check box Enable Automatic login
 - Enter the username and password that you entered for the enrollment operator in the previous section
1. In the MorphoManager installation directory (default: *C:\Program 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**

The screenshot shows the MorphoManager [14.4.3.9] Administration interface. The main navigation bar includes Home, Administration, User Management, Biometric Identification, Access Logs, and Reports. The left sidebar lists various configuration items, with 'Clients' highlighted. The main content area is titled 'Editing Clients' and contains the instruction 'Enter the details for this client'. Below this instruction are three input fields: 'Name' (containing 'vmw10enLTSC'), 'Description', and 'Location'. At the bottom of the form are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'. The status bar at the bottom indicates the user is logged in as Administrator and provides site ID and options for logging out or changing the password.

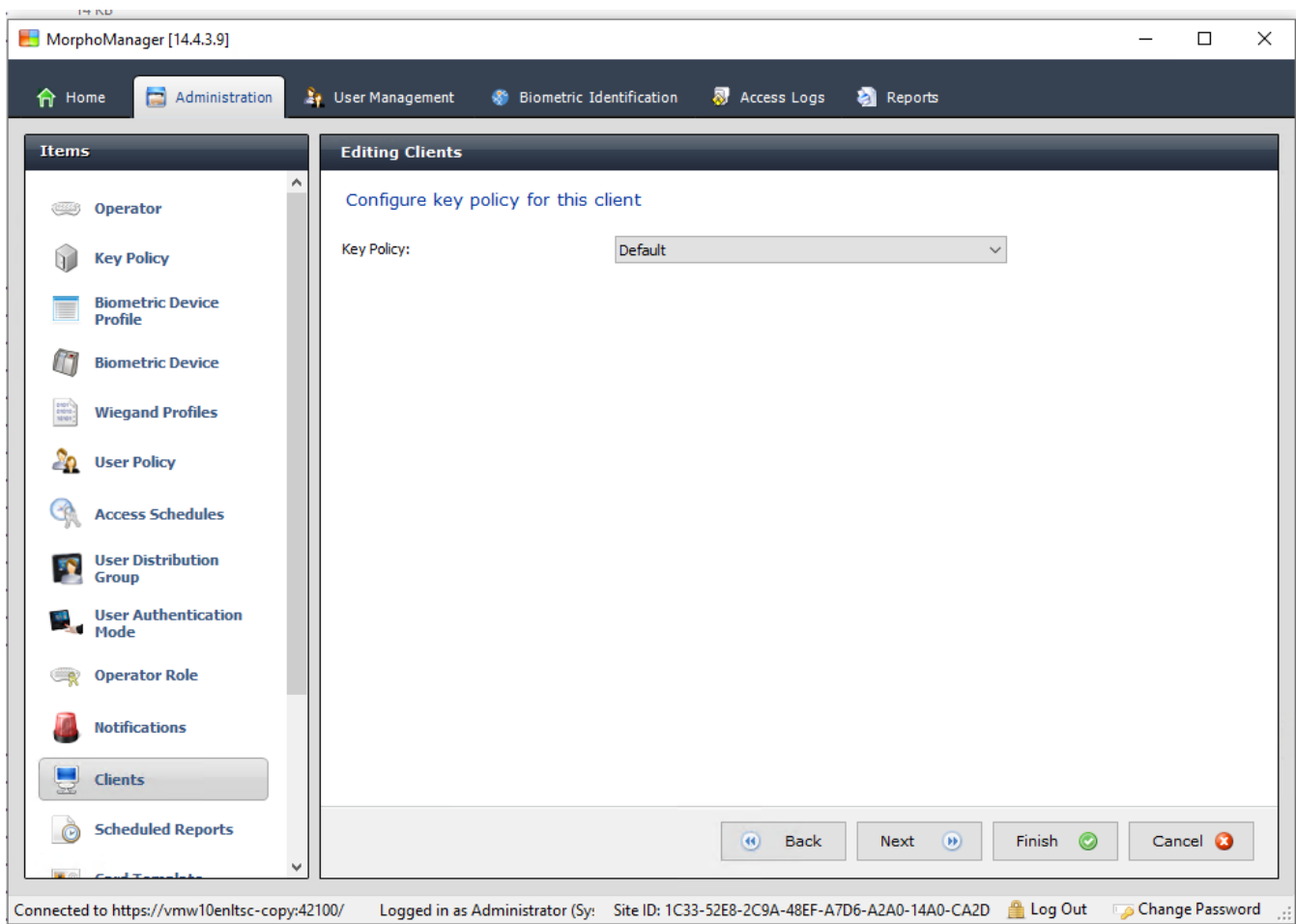
5. Enter the name of the intended enrollment client, and optionally the location and a description
6. Click **Next**



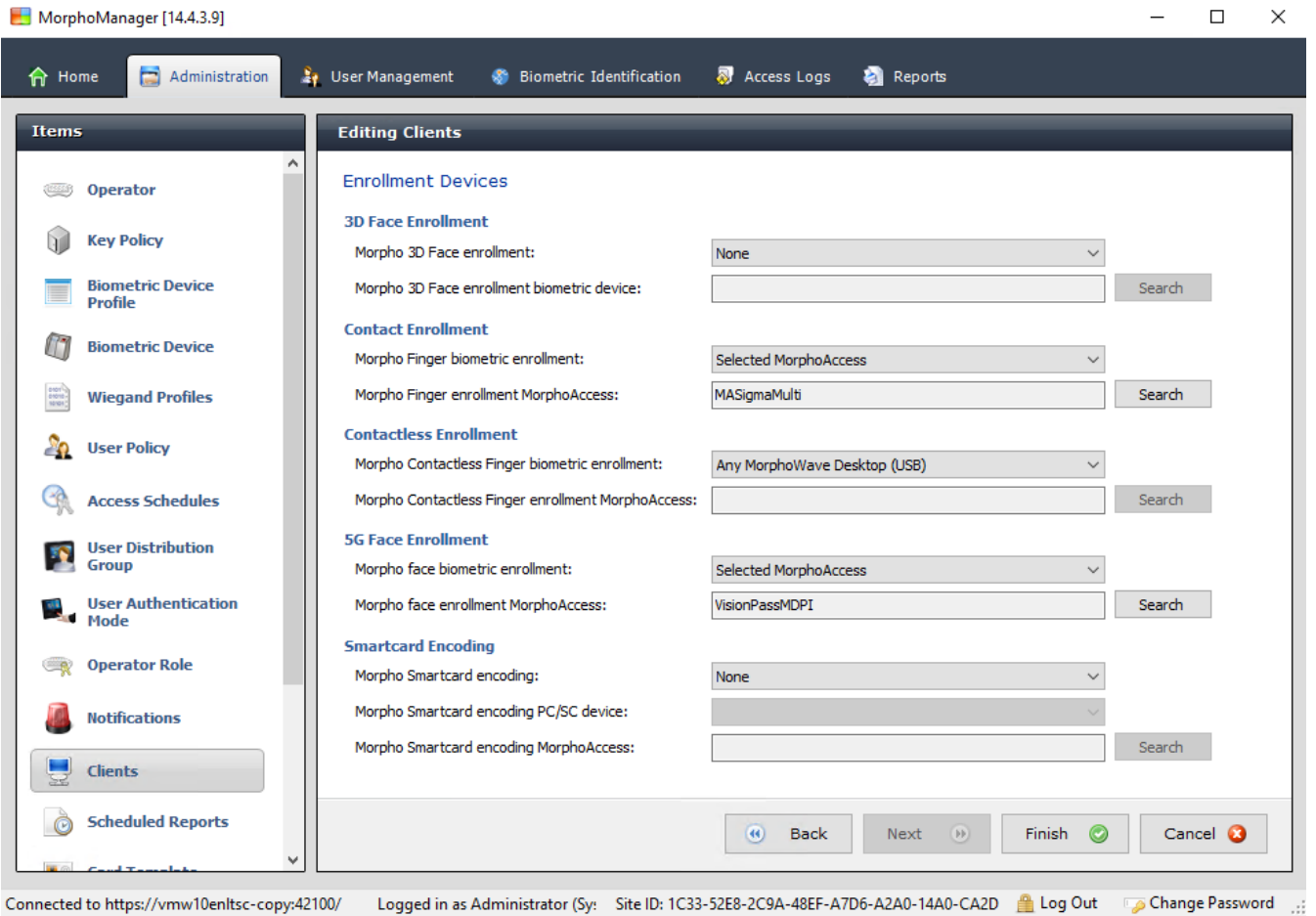
7. Select the check boxes of the tabs that you want to display on the enrollment client:
 - **Administration,**
 - **User Management,**
 - **Reports,**
 - **Access Logs,**
 - **Biometric Identification**
8. Click **Next**



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



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



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

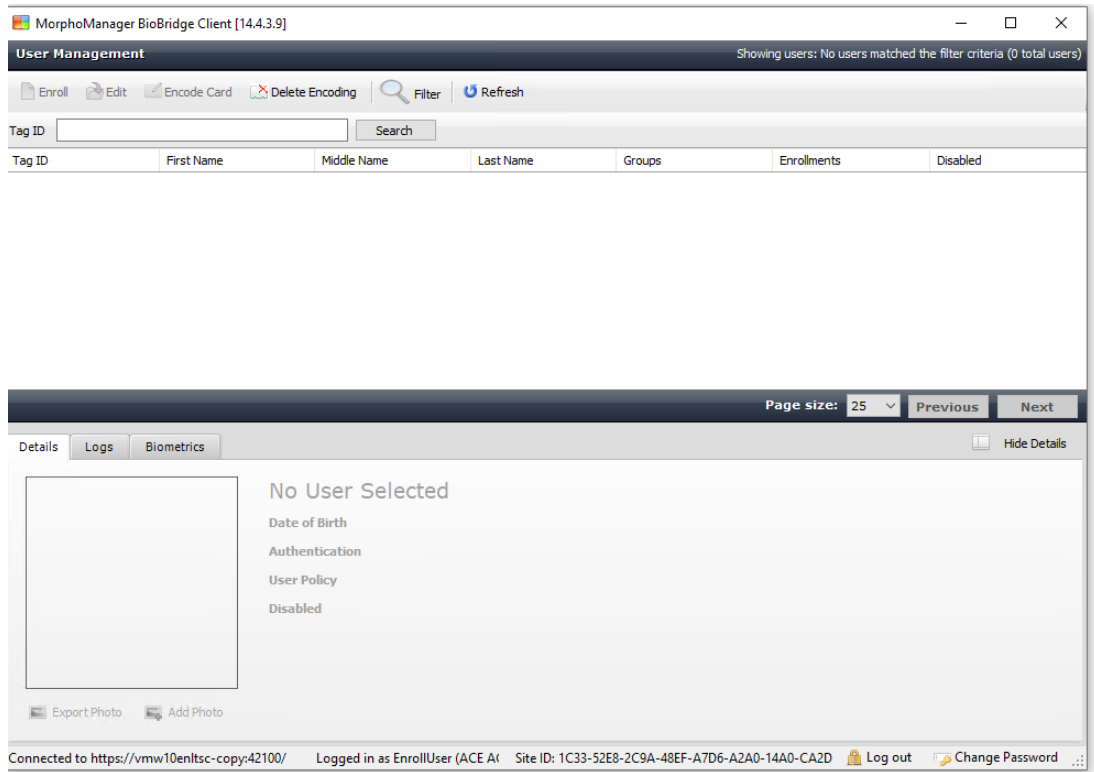
Refer to

– *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`



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**

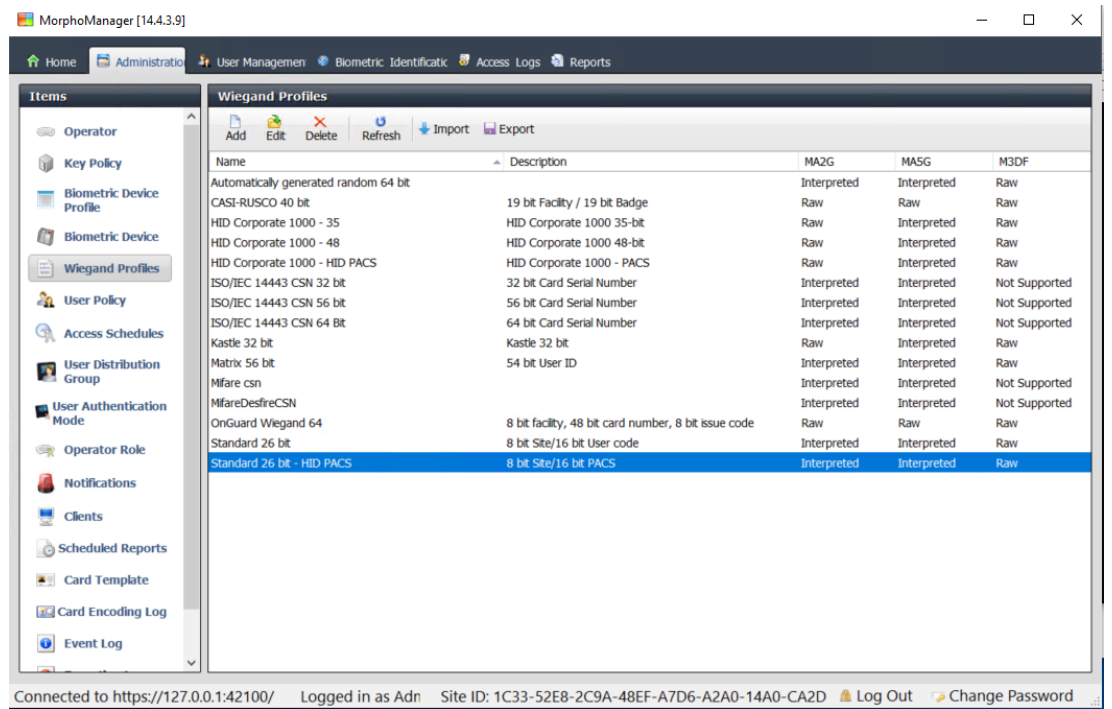
Mifare DESFire CSN

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

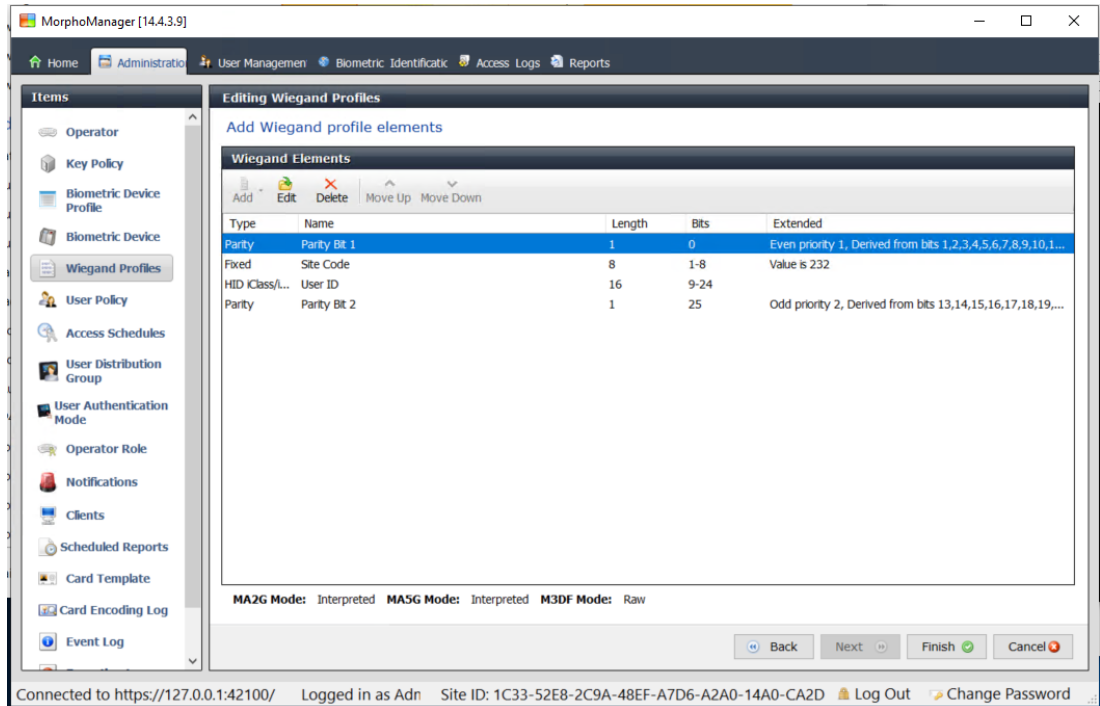
- **Length:** 56
- Add **Wiegand Element User CSN Element**
 - Enter a name under **Name:**
 - For **Length** enter 56
 - For **Transformation mode:** enter *Reversed*
- **Under Administration > Biometric Device profile,** on the **Multi-Factor Mode Settings** page, select the check box **Mifare DESFire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

iClass 26 BIT

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



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



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

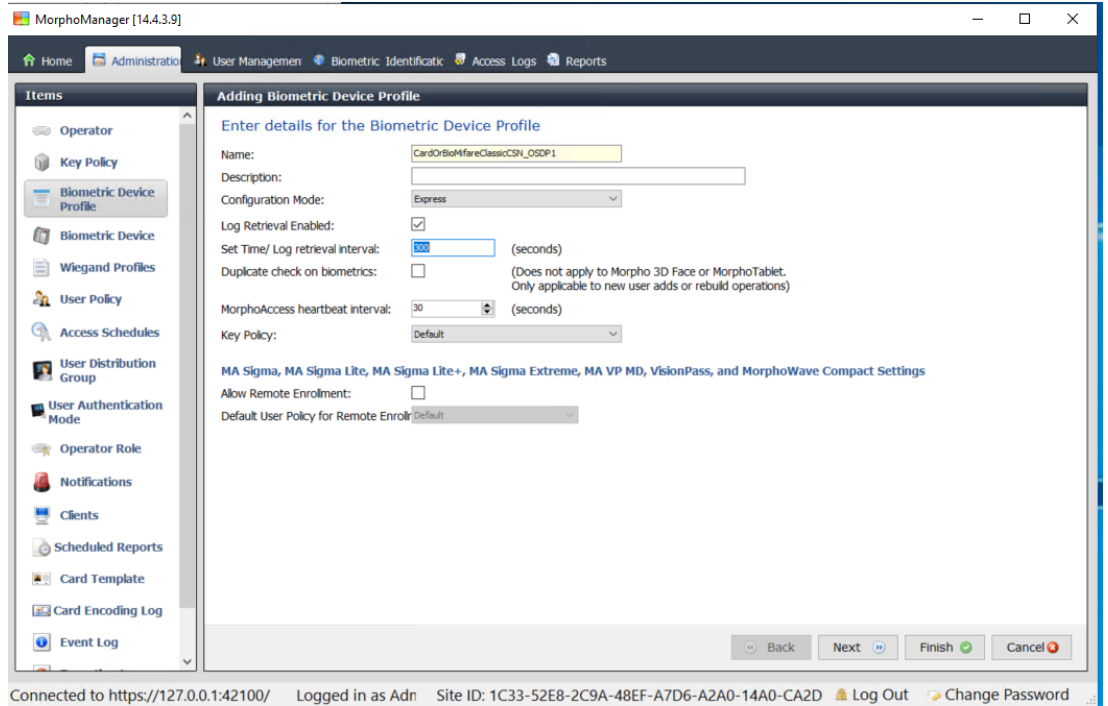
In MorphoManager **Administration** tab

3.5.1

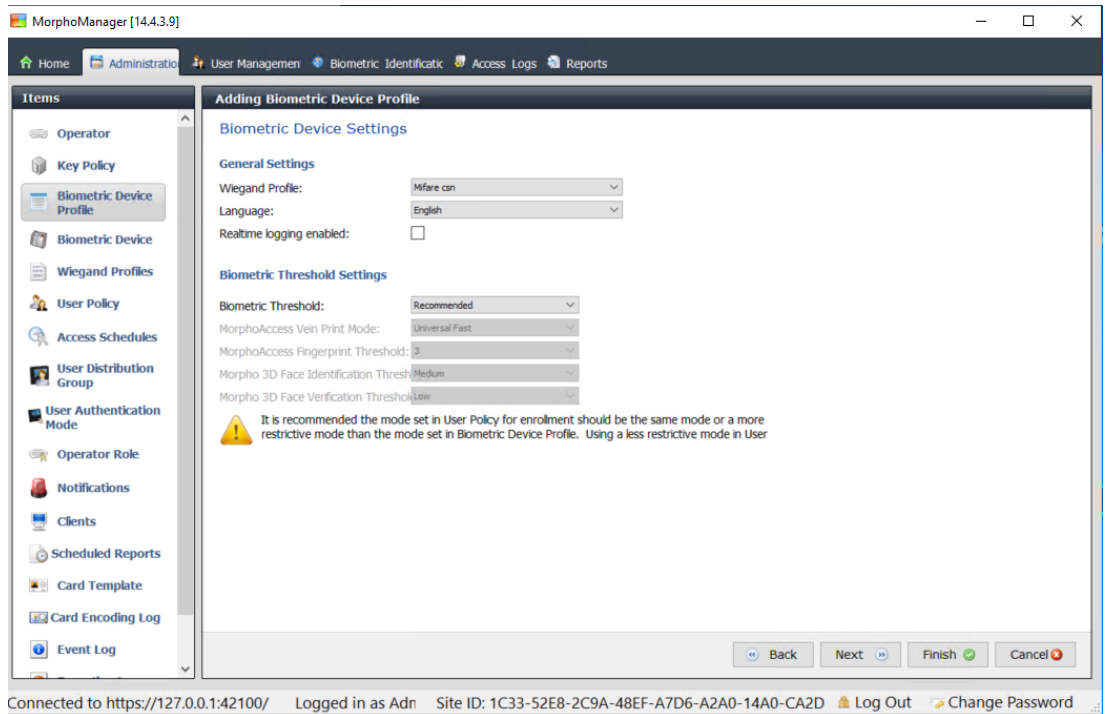
Card OR Biometry

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

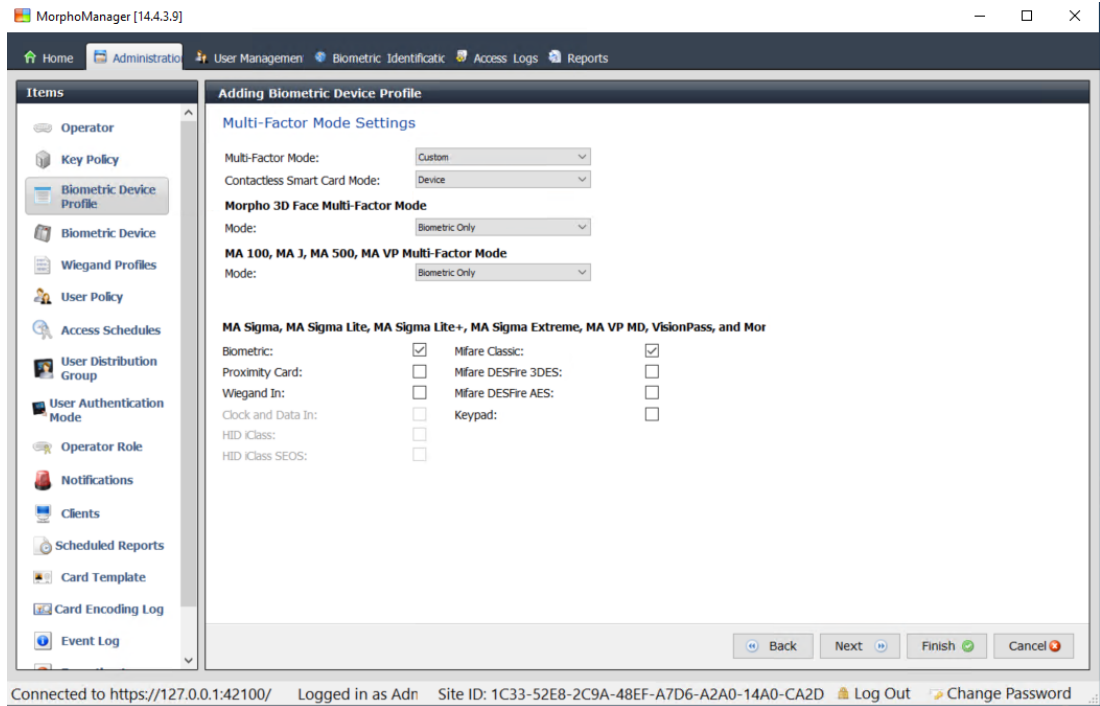
1. In MorphoManager, go to **Administration > Biometric Device Profile**



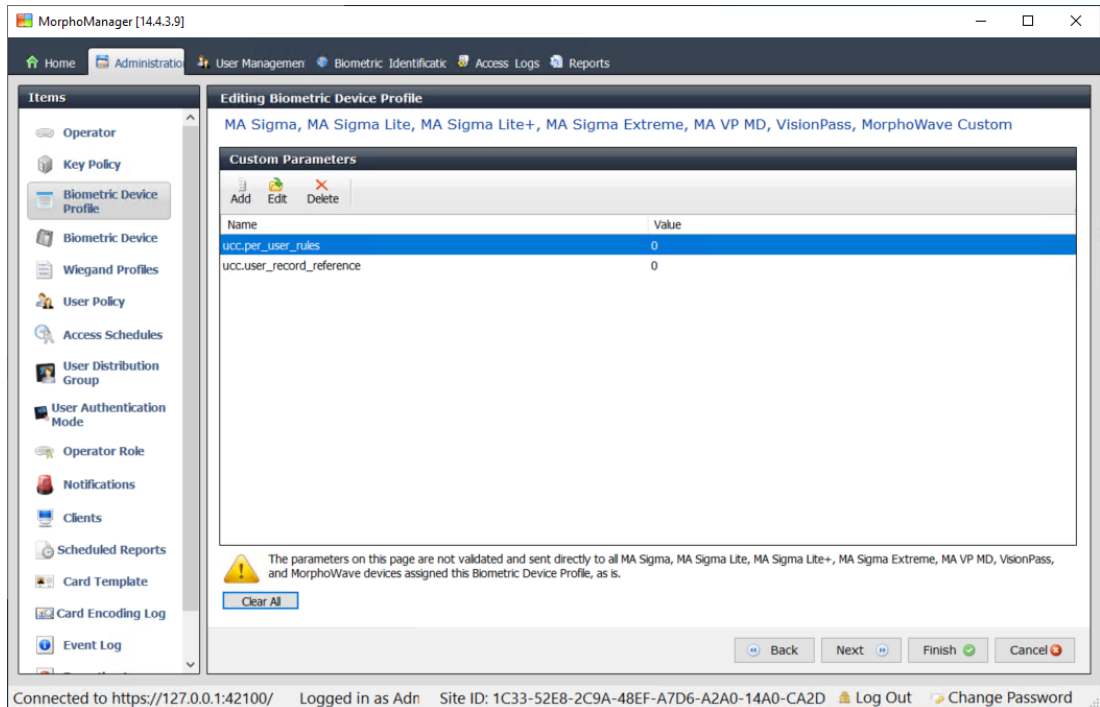
2. Click **Next** until you reach the page titled **Biometric Device Settings**



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



4. 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



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 not need to 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

© Bosch Sicherheitssysteme GmbH, 2020