MorphoManager

BioBridge

Lenel OnGuard OpenAccess

Quick Start Guide

IDEMIA
augmented identity

Table of Contents

Introduction 3
Support 3
Setting up BioBridge 4
Biometric Device Profile 5
Biometric Device(s) 6
User Policy 7
User Distribution Groups 8
BioBridge System Configuration 9
Using the BioBridge Enrollment Client 14
Toolbar 14
Enroll 15
Edit 15
Encode Card 15
Filter 15
Refresh 16
Search Field 16
Data Grid 16
Embedded Enrollment 17
Pre-requisites 17
Biometric Capture 18

Introduction

BioBridge is an enrollment and synchronization middleware that overlays enrollment and demographic synchronization between MorphoManager and third-party data sources. The infrastructure is extensible and supports interfacing to multiple third-party systems (one at a time) by the implementation of an interface. BioBridge is not dependent on the underlying technology platform required for integration.

BioBridge supports the following versions of Lenel OnGuard with OpenAccess:

- 7.3
- 7.4
- 7.5

Support

Please contact your installer for additional support.

Setting up BioBridge

The following areas of MorphoManager need to be configured as part of the Lenel OnGuard BioBridge setup:

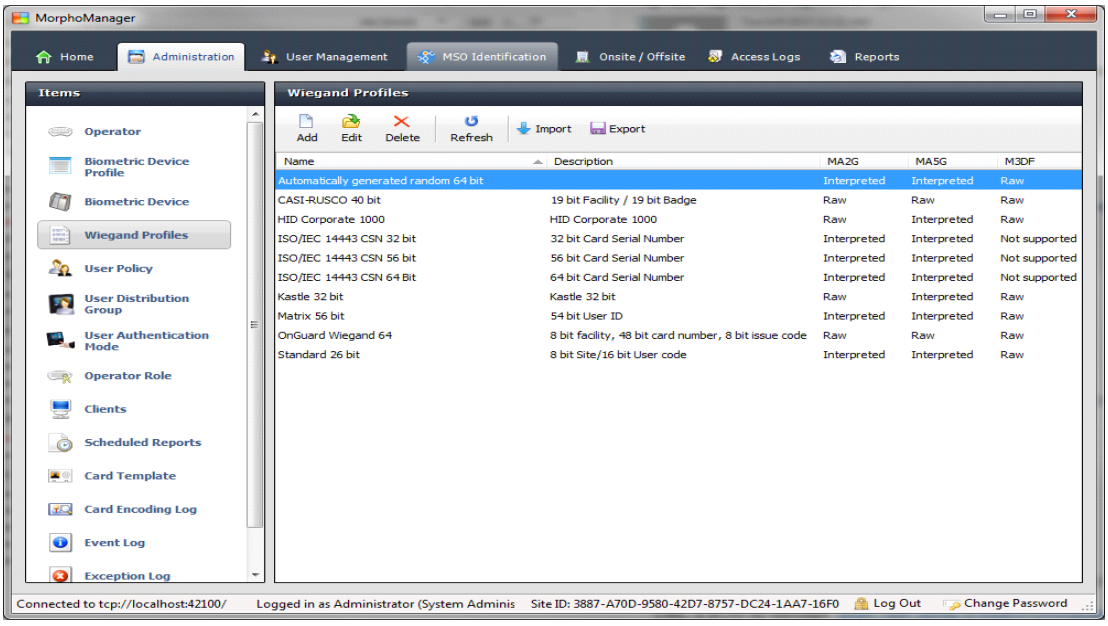
- Wiegand Profiles
- Biometric Device Profiles
- Biometric Device
- User Policy
- User Distribution Group
- BioBridge System Configuration

Wiegand Profiles

Wiegand Profiles define what information is output over the Wiegand Out interface of the Morpho Biometric Devices when a user is identified. This is most typically used in conjunction with an Access Control System.

- From Administration tab select Wiegand Profile.
- Click **Add** button to create a custom Wiegand profile.

The Wiegand formatting used can vary from system to system, but some common formats are listed below.

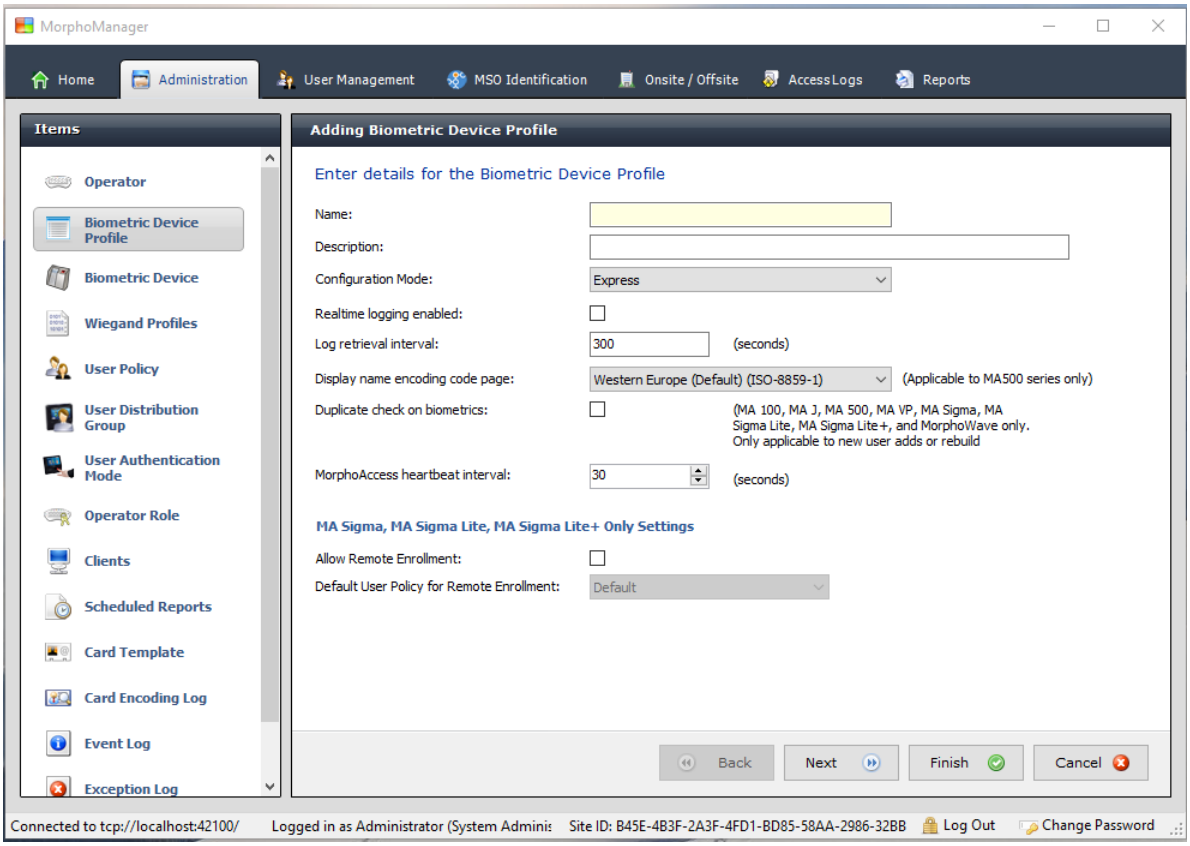


The actual setting of the Wiegand Profile from this list will be done at the User Policy and Biometric Device Profile Level. Please refer to those sections for further details.

Biometric Device Profile

The Biometric Device Profile will define common settings and parameters for one or more biometric devices. This profile can be applied when adding units into the system from the Biometric Device section of Administration.

- From Administration tab select Biometric Device Profile.
- Click **Add** button to create a new Biometric Device Profile.



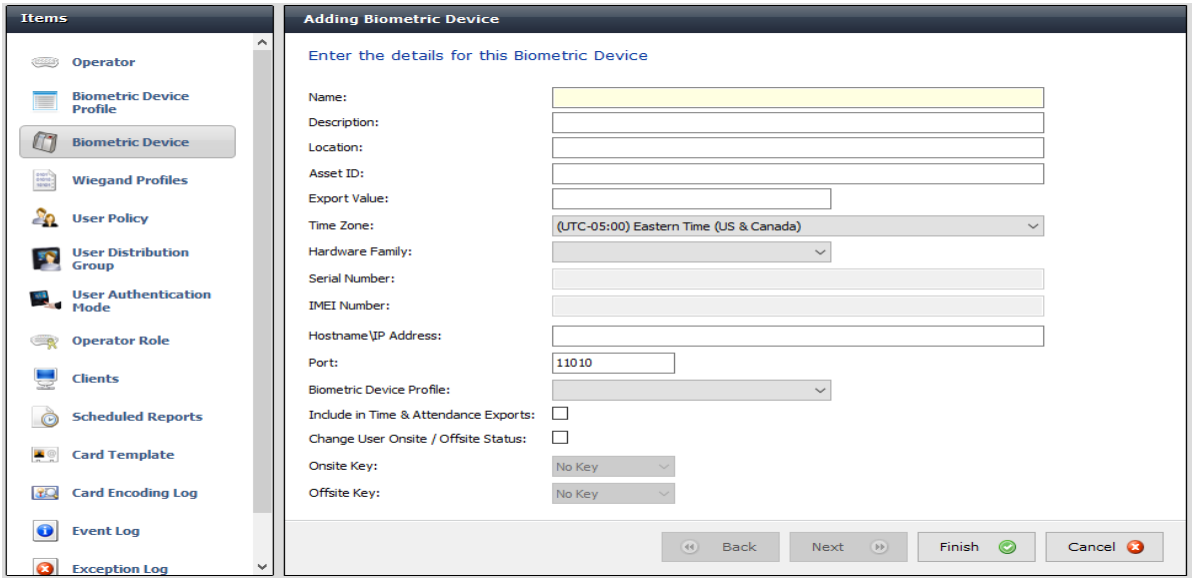
In order to create the most basic profile utilizing biometrics stored on the devices that can be used, simply give the profile a name and click **Finish**. Please reference the MorphoManager User Manual for more detail on all the various properties that can be assigned to a Biometric Device Profile including the use of smartcards.

If you plan on using a Wiegand Profile, you will need to set the Wiegand Profile for the Biometric Device(s) here. The Wiegand Profile you choose for your devices must marry to the one being utilized for your users set in the User Policy section of this guide.

Biometric Device(s)

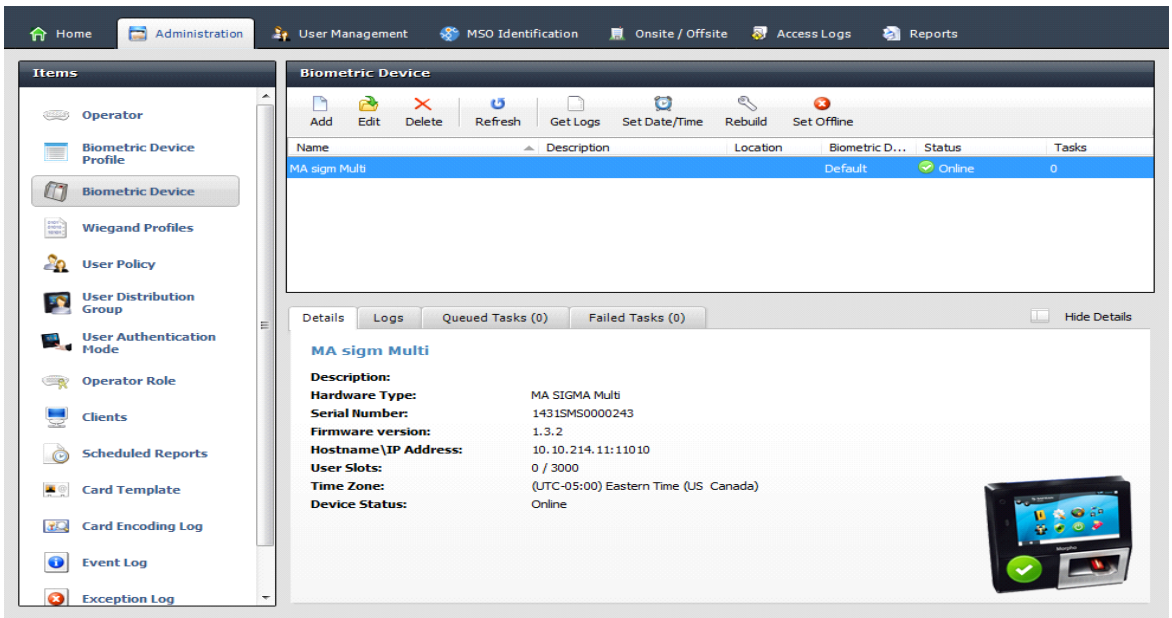
A Biometric Device is the device used to verify users and allow access to doors. They record a log of every attempt to gain access. MorphoManager is used to manage user's access to Biometric Devices.

- From Administration tab select Biometric Device.
- Click **Add** button to create a new Biometric Device.
- Enter the details for the device including the Hardware Family the device falls into, the IP address, and the Biometric Device Profile.



- Once the required details are entered click **Finish**.

Below is a screenshot of how the Biometric Device Screen looks after the configuration and the devices are online.

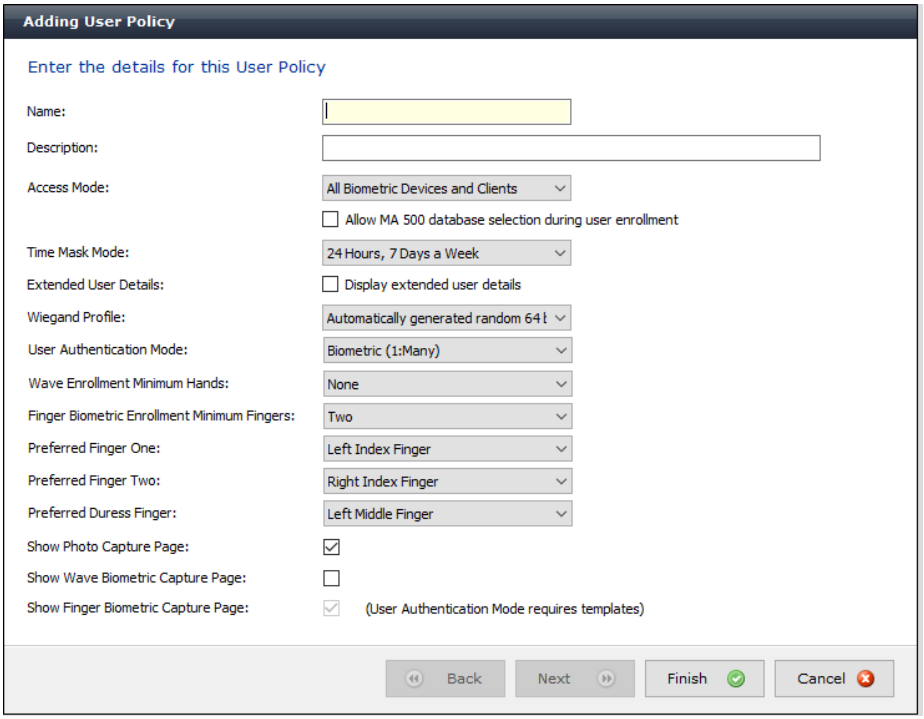


User Policy

User polices are used to apply access rights and rules to all members of the group.
To Configure BioBridge, MorphoManager's UserPolicy with an Access Mode "**Per User**" must be selected.

This will create User Distribution Groups (groups of Biometric Devices) that can place the enrolled user into specific devices

- From Administration tab select User Policy.
- Click **Add** button to create a new User Policy.



If you plan on using a Wiegand Profile, you will need to set it here in order for the users enrolled in this User Policy to have a particular Wiegand Profile. The Wiegand Profile you choose for your users must marry to the one you utilize for your biometric access devices set in the Biometric Device Profile section of this guide.

The default User Policy will be set to utilize an authentication mode of Biometric (1: Many). To utilize another authentication mode (such as encoding smartcards) additional User Policies can be created.

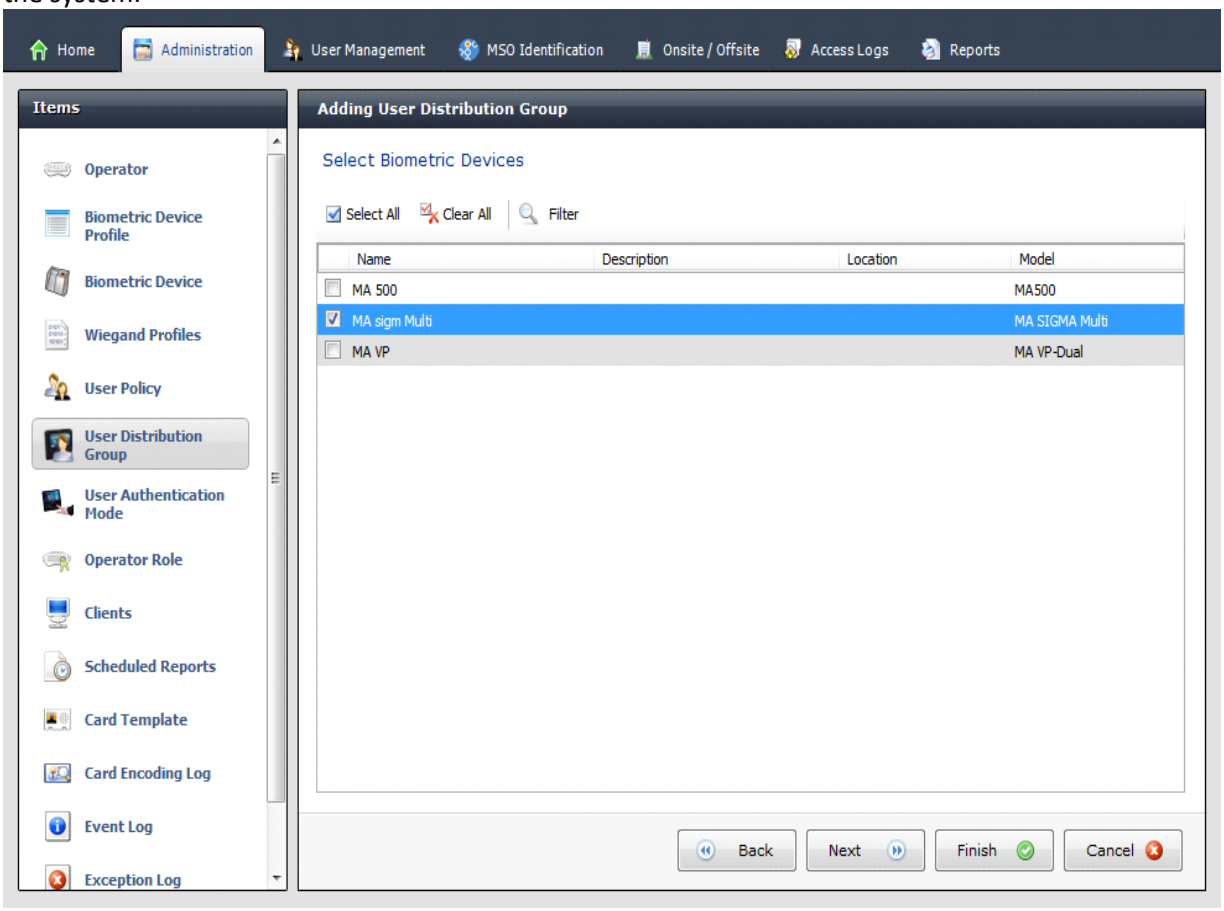
Please reference the MorphoManager User Manual for more detail on all the various properties that can be assigned to a User Policy including Wiegand Profile, Finger Biometric Enrollment Minimum, Fingers, Access Modes and User Authentication Modes.

User Distribution Groups

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

- From Administration tab select User Distribution Group.
- Click **Add** button to create a new User Distribution Group.

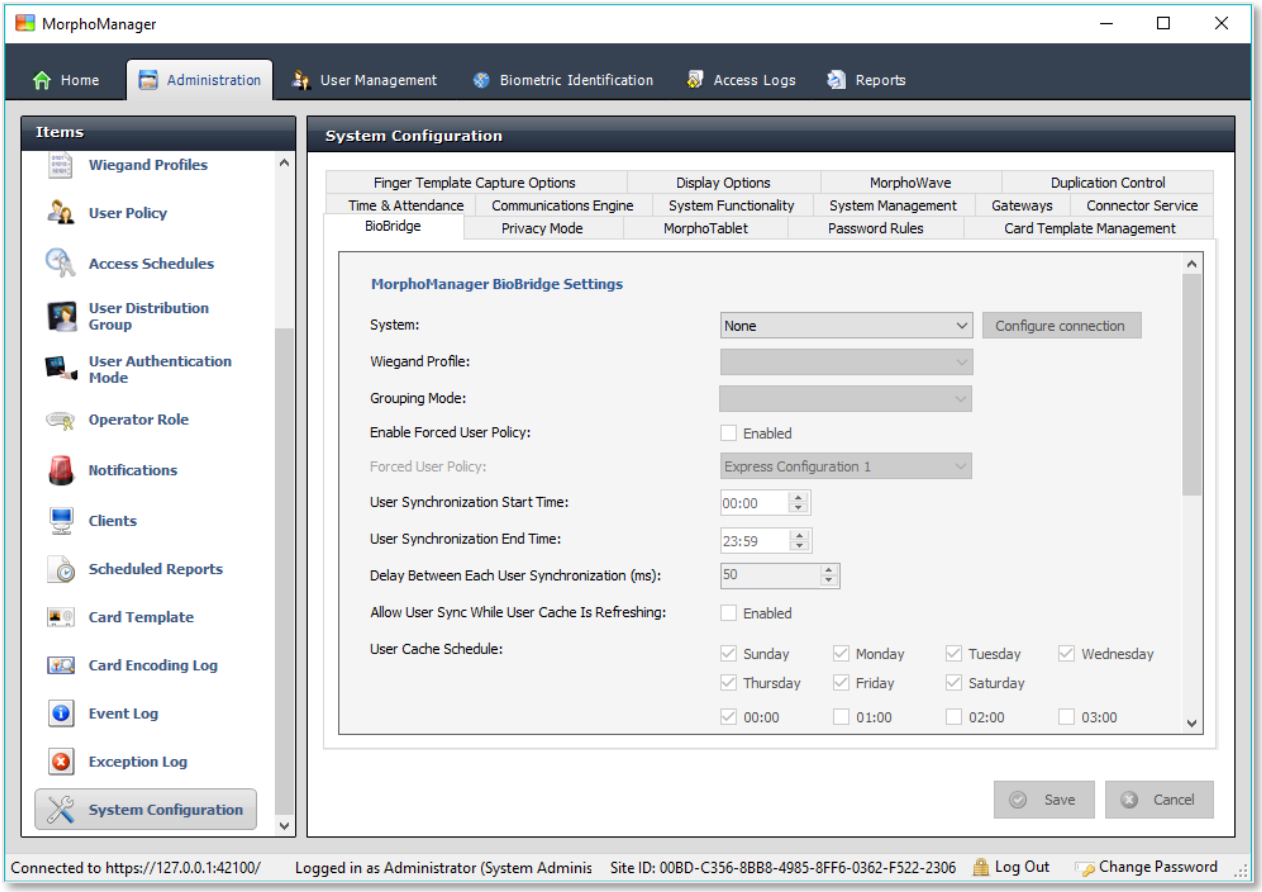
Below is the screenshot where group will only be placing users on one of the three devices installed on the system.



BioBridge System Configuration

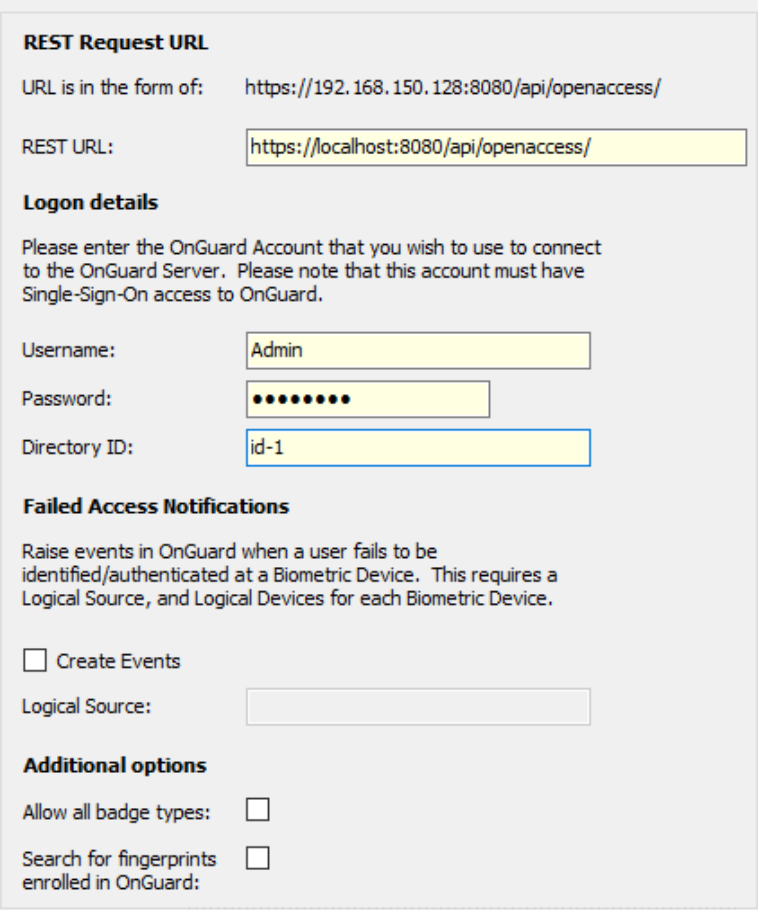
The last step in the process is to configure BioBridge specifications to OnGuard.

From Administration, select System Configuration.
Select the BioBridge Tab in System Configuration.



System: From the System drop down menu choose OnGuard 7.4 & 7.5 and click the **Configure connection** button. A BioBridge connection box window will pop up.

If you wish to use WMI with OnGuard 7.4 you need to select the “Lenel OnGuard” option in the System Dropdown. Use the “Lenel OnGuard” quick start guide to set up a WMI connection.



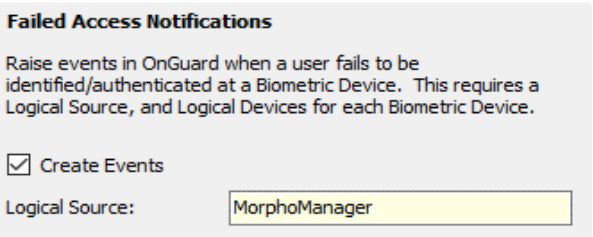
Rest URL: The URL of OnGuard server's restful API

Username: OnGuard username

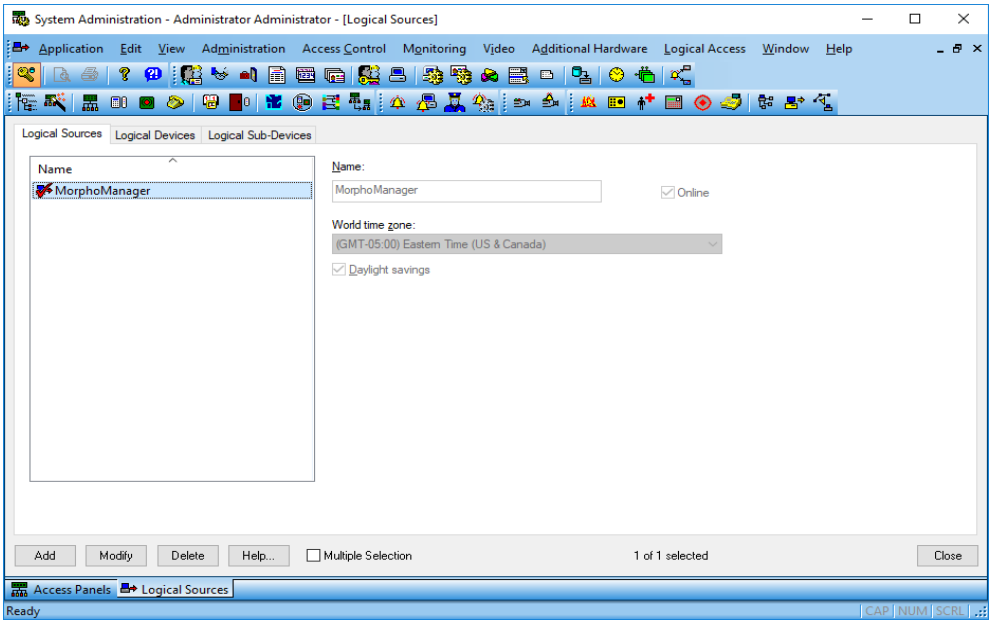
Password: Password that matches the OnGuard username

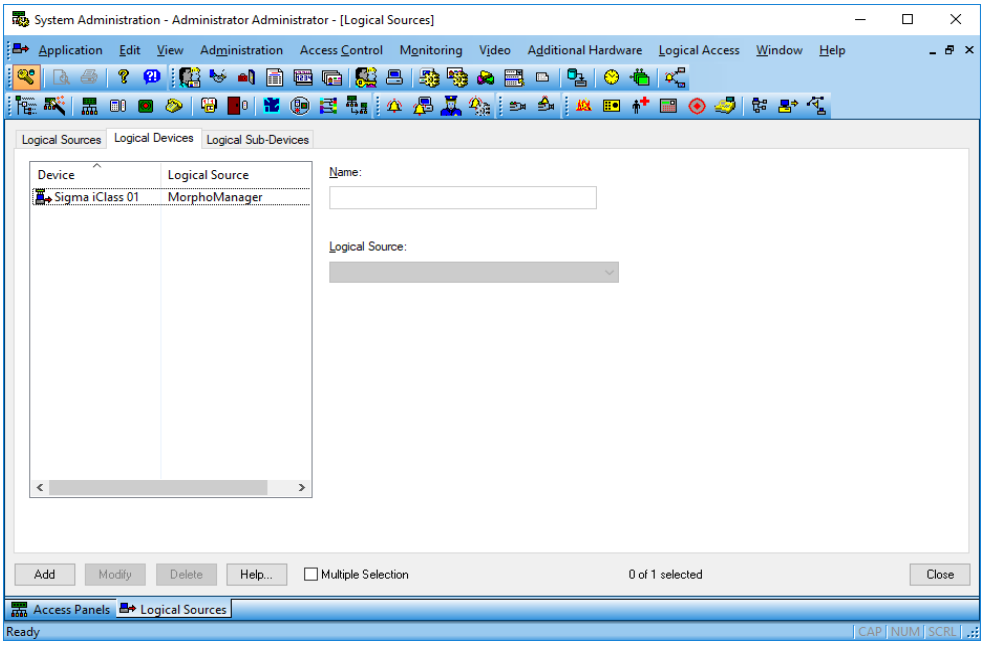
Directory ID: The OnGuard Directory ID being utilized for Open Access. Entering the following in a web browser address on the machine running Open Access will give you the information: https://localhost:8080/api/access/onguard/openaccess/directories?version=1.0

Failed Access Notifications: The Logical Data Source can be set up in Lenel's System Administration > Additional Hardware > Logical Sources. This will allow failed access attempt events to be reported in OnGuard.



Both, the Logical Source and Logical Device must be configured in Lenel. The naming of the devices will need to marry to the exact name of the Biometric Device devices in MorphoManager. (See screenshots below for this area of OnGuard).





Additional options:

Allow all badge types: When enabled, MorphoManager will ignore the wiegand profile/badge type setting on the BioBridge tab. MorphoManager can see all badge types in OnGuard.

Search for fingerprints enrolled in OnGuard: When enabled, users who have had their finger biometrics captured in OnGuard will have that data brought over automatically to

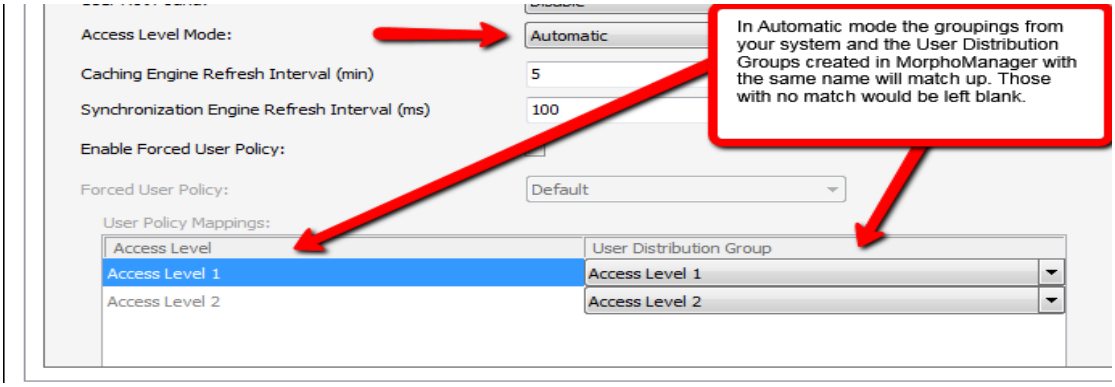
MorphoManager with the user. There will be no need to enrol these users and capture their fingerprint data in the BioBridge Enrolment Client.

When finished with the configuration, click OK and the system will return to the main MorphoManager BioBridge Settings screen. Complete the other fields as described.

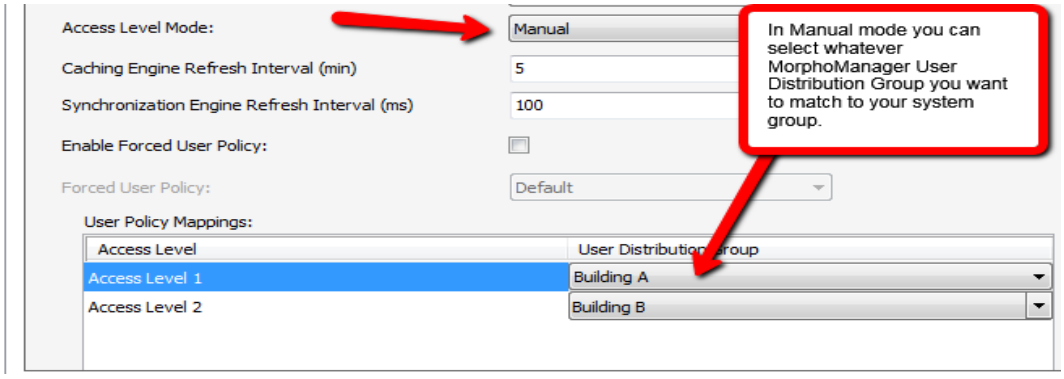
Wiegand Profile: Select the Wiegand format in use from the drop down menu.

Grouping Level Mode: This setting determines how MorphoManager should map OnGuard users into MorphoManager User Distribution Groups.

Automatic: This mode will automatically match Access Level groups from OnGuard to the ones created in MorphoManager User Distribution Group if they have the same naming convention.



Manual: If the Access Level grouping names of OnGuard and the User Distribution Group(s) created in MorphoManager are not the same, then selecting which OnGuard Access Level maps to which MorphoManager User Distribution Group can be done manually in the User Policy Mappings.



For basic setups, the following settings do not require any changes:

Enable Forced User Policy
By activating this feature, you can select a User Policy from the drop-down menu. The 3rd party user will automatically be placed in this User Policy during the enrollment process started in the

BioBridge Enrollment Client. The User Policy selected here must be a “Per User” access mode policy.

User Synchronization Start Time and End Time
The user synchronization engine will only be permitted to run in this time frame.

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

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

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

Using the BioBridge Enrollment Client

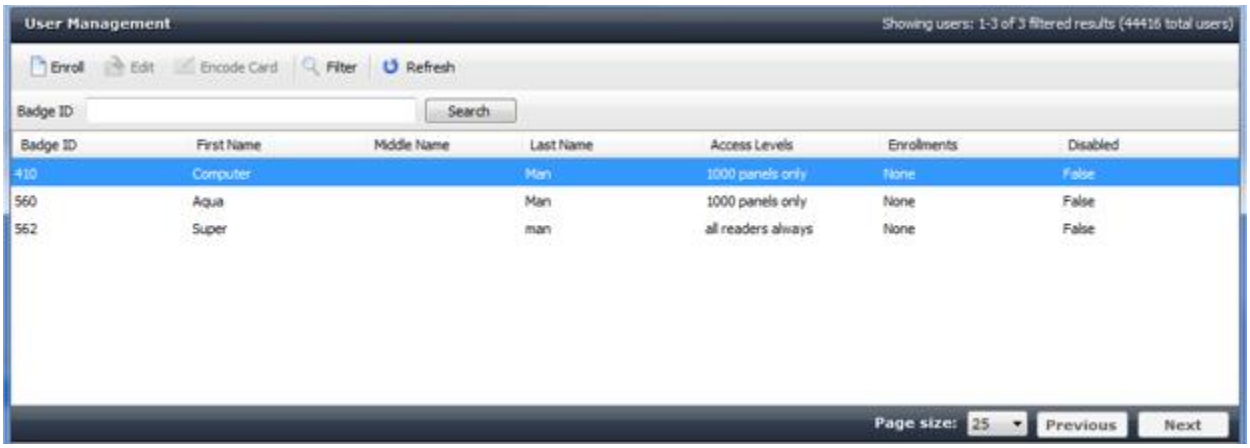
After configuring BioBridge you will now utilize the BioBridge Enrollment Client. This client will check if BioBridge Integration has been enabled and configured. If it has not been configures, the application will display the message “BioBridge integration has not been enabled and configured” and you will need to go back to MorphoManager/Administration/System Configuration/BioBridge to configure it properly.

If BioBridge integration is configured the application will display a user management screen. The screen will consist of a toolbar and a data grid.

Toolbar

The toolbar will have the following items:

- Enroll
- Edit
- Encode Card
- Filter
- Refresh
- Search Field



Enroll

Enroll will start the enrollment of the selected user. The enrollment process will be derived from the standard MorphoManager user add/edit wizard with the following pages (For details on the enrollment process please see the User Management section of the MorphoManager User Manual):

- Authentication Type (Only if more than one mode is configured)
- 3D Face Selection
- 3D Face Enrollment
- Finger Selection
- Finger Enrollment

If a card-based authentication method is configured the operator will be prompted if they want to encode a card.

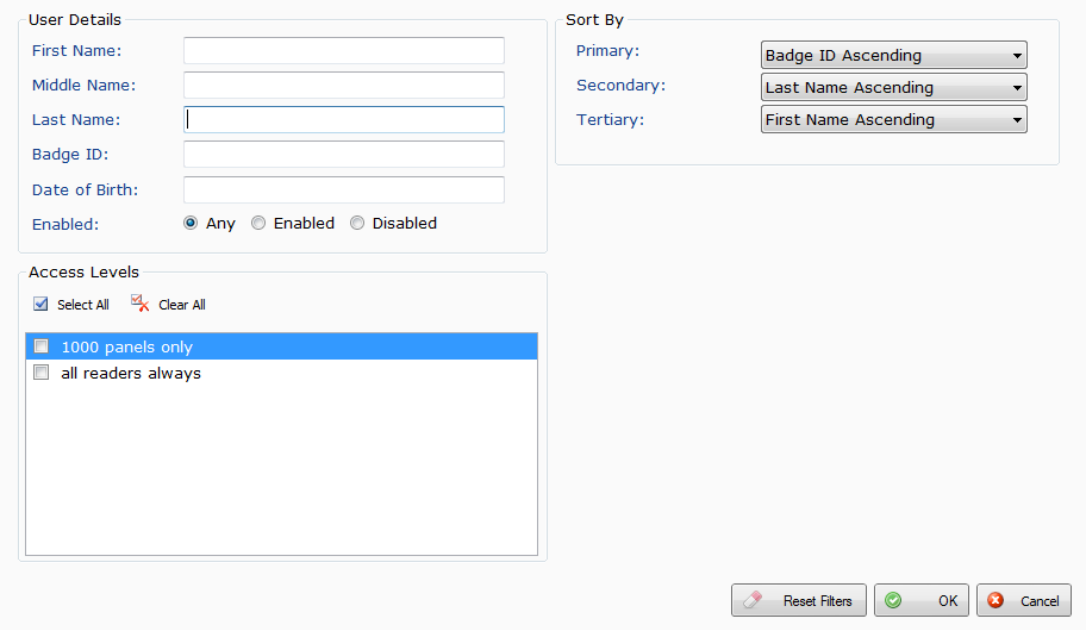
Edit

Opens the already enrolled user details for viewing or editing.

Encode Card

Encode card will display an animation of the card being presented to a SDI 011 and wait for the card encoding to complete or be cancelled.

Filter



Filter will show a popup inline form that allows filtering on the following items:

- First Name
- Middle Name

- Last Name
- Badge ID
- Date of Birth
- Enabled/Disabled
- Access Levels

Refresh

Refresh will update the data currently being shown using the currently set filter conditions.

Search Field

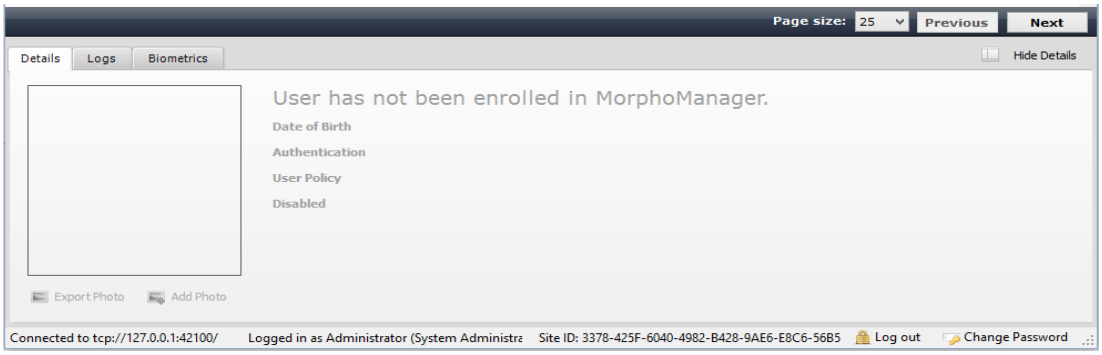
The Search Field can be used to find individual users quickly and/or to migrate users from Lenel On Guard to the BioBridge Enrollment Client without waiting for a cache refresh.

Data Grid

The data shown in the data grid is a combination of your system and MorphoManager. Only users that exist in your system will be shown. A MorphoManager user does not exist until the user is enrolled. By default, pagination is set for the first 25 BioBridge users to be shown. Operators may change the pagination to 25, 50, 100 & 250.

The data grid will have the following columns:

- Badge ID
- First name
- Middle name
- Last name
- Access Levels – (Comma separated values if more than one)
- Enrollments (None, Finger, Finger & 3D Face, 3D Face) (Derived from linked MorphoManager User)
- Disabled- A value of either True or False will be present.



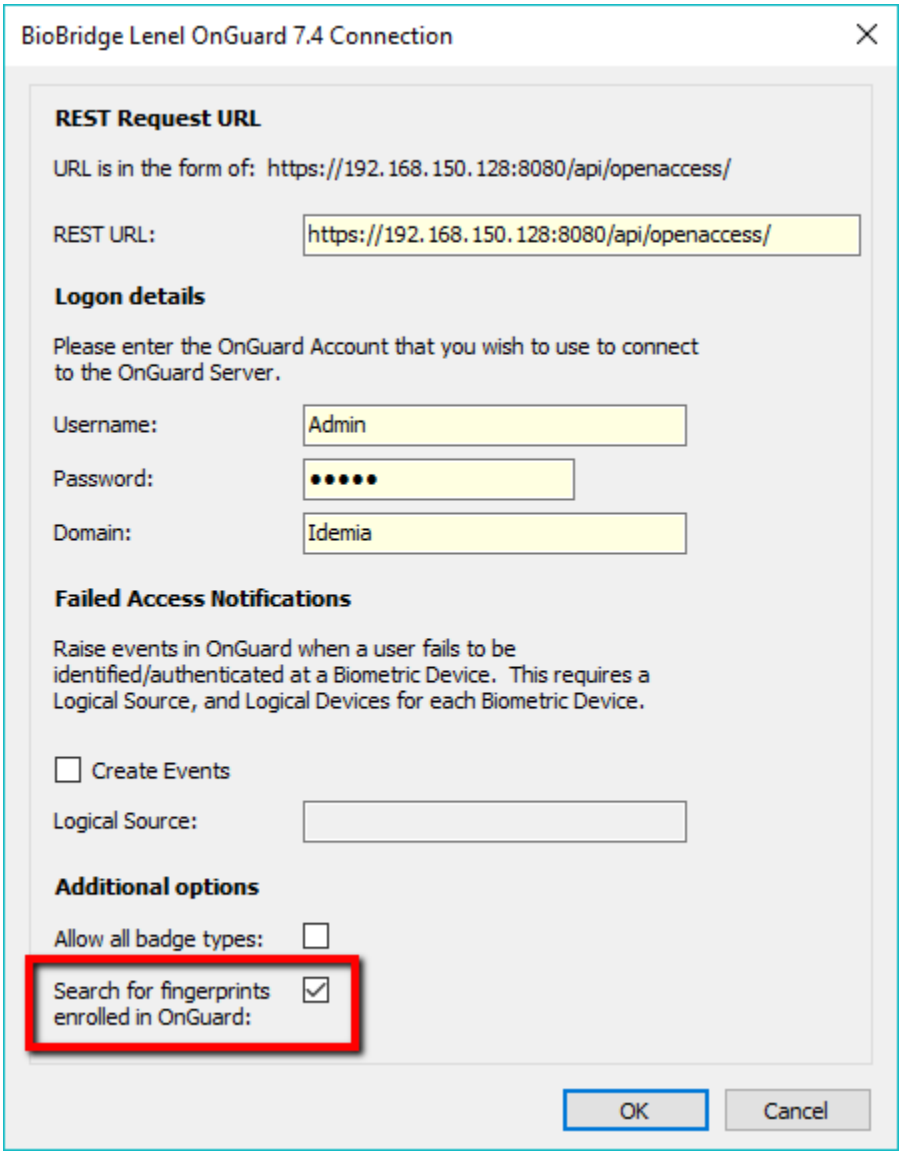
Enrolled user will show their MorphoManager details in the “Show Details” panel below the data grid. This area will be blank if the user has not been enrolled.

Embedded Enrollment

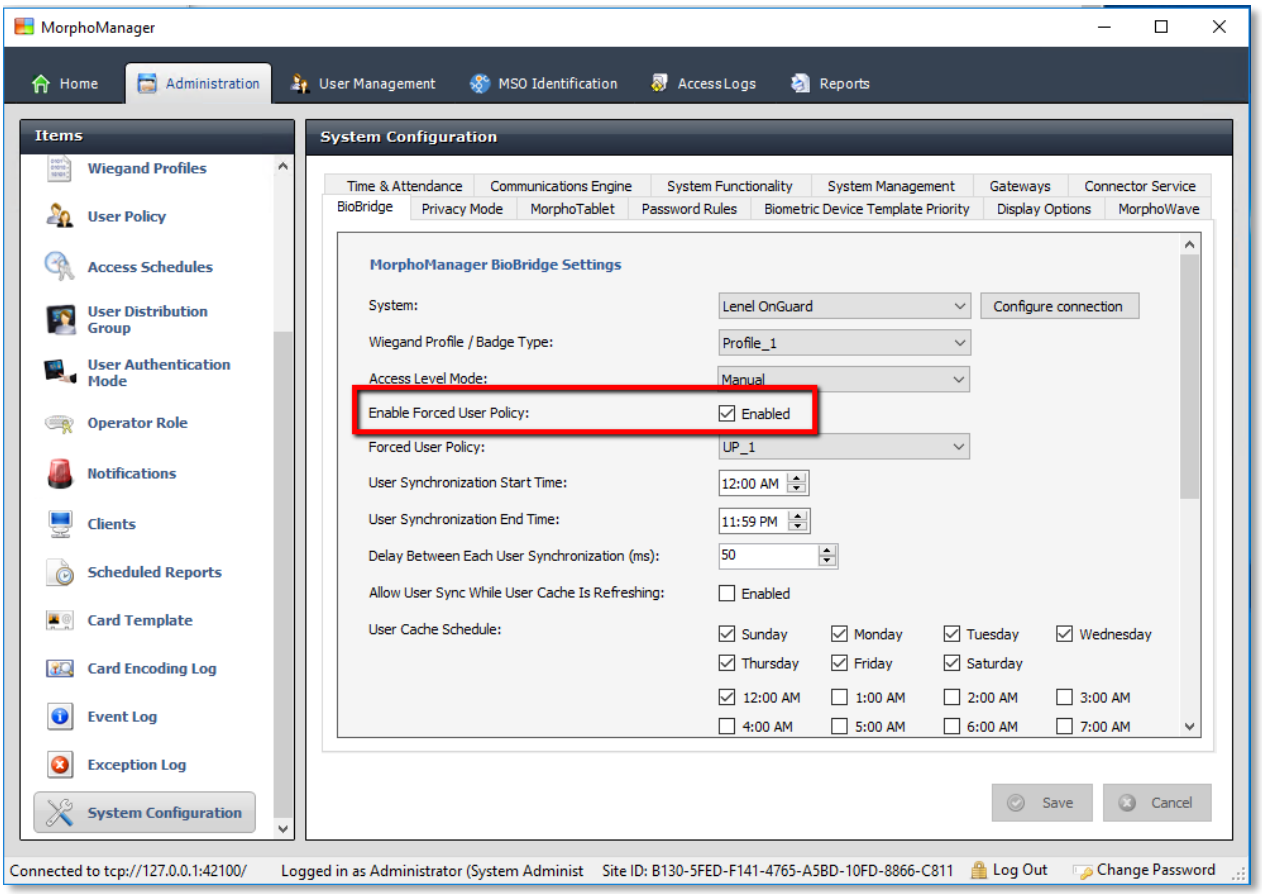
In order to have Cardholders in Lenel automatically enrolled in MorphoManager the following steps will need to be completed in Lenel after completing the “Setting up Biobridge” section of this guide.

Pre-requisites

1. In the BioBridge System Configuration section enable the “Search for fingerprints enrolled in OnGuard” option.

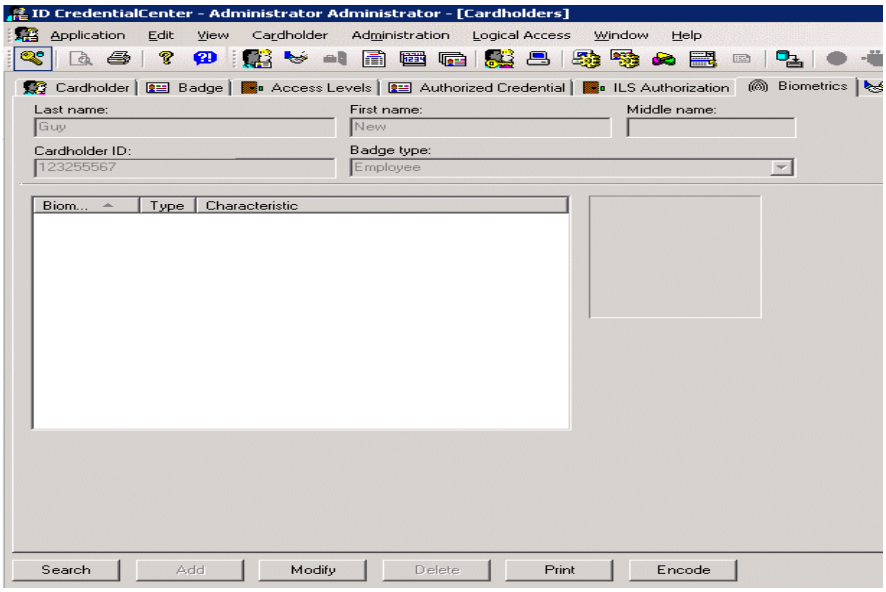


2. Enable the “Forced User Policy” setting.



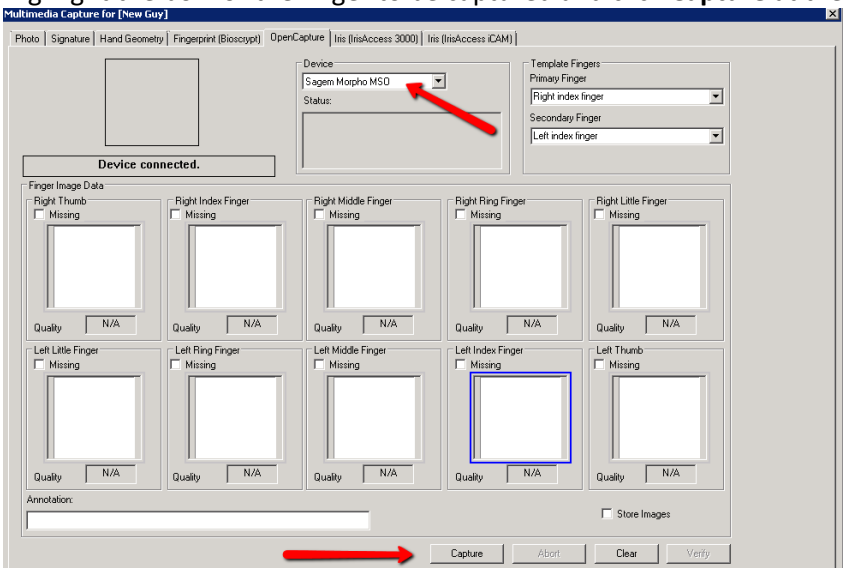
Biometric Capture

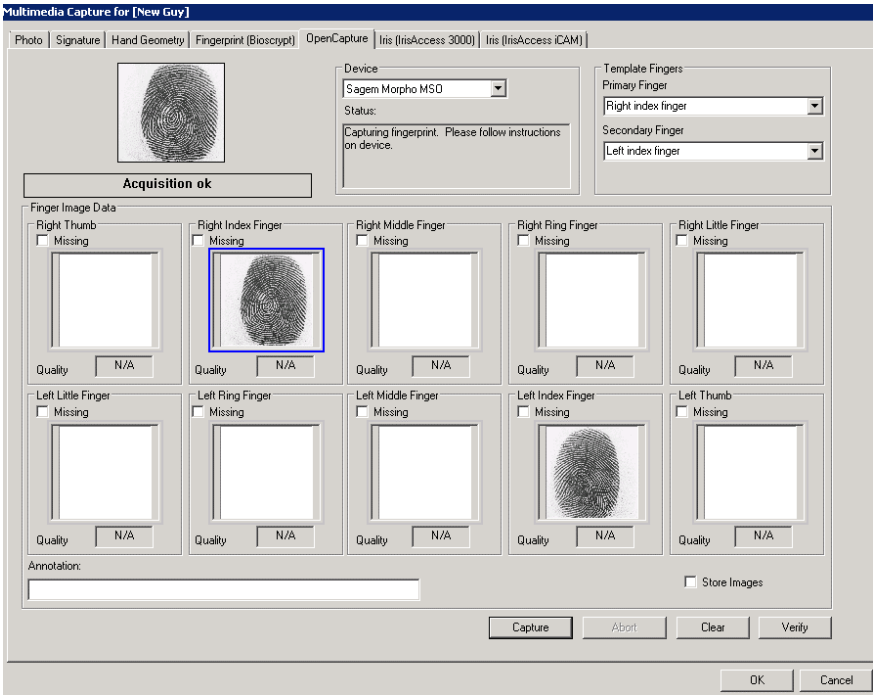
On the Cardholder select the Biometrics tab and click **Modify**.



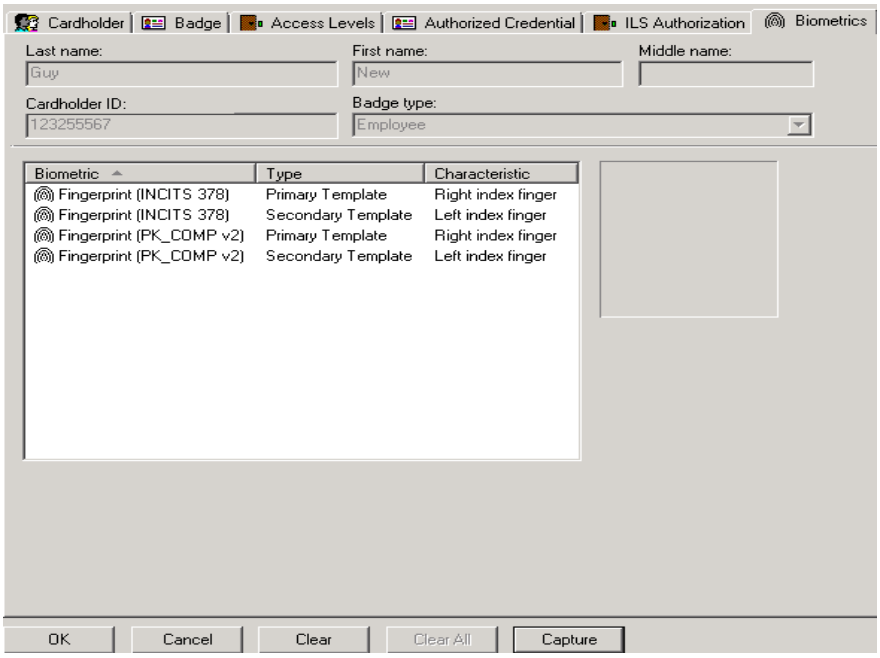
Now click **Capture** on that screen. On the Multimedia Capture screen that appears next select the Open Capture tab. Once this screen appears select the biometic capture device you have connected to Lenel. In this example a Sagem Morpho MSO is used. The device should show as connected.

Highlight the box for the finger to be captured and click **Capture** at the bottom of the screen.





Once the needed biometrics have been captured click **OK.** The screen below will appear. Click **OK** again to finish the process.



Cardholders who have completed the capture of their biometrics and meet the configuration properties set up on MorphoManager will automatically be enrolled in MorphoManager.