

MorphoManager

BioBridge

Controlsoft Identity Access

Quick Start Guide



Table of Contents

Introduction.....	3
Support	3
Setting up BioBridge	4
Wiegand Profiles.....	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	12
Toolbar.....	12
Enroll.....	12
Edit.....	13
Encode Card.....	13
Filter.....	13
Refresh.....	13
Search Field.....	14
Data Grid.....	14
Embedded enrollment.....	14

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 version of Controlsoft Identity Access:

- 2016.1

Support

Please contact your installer for additional support.

Setting up BioBridge

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

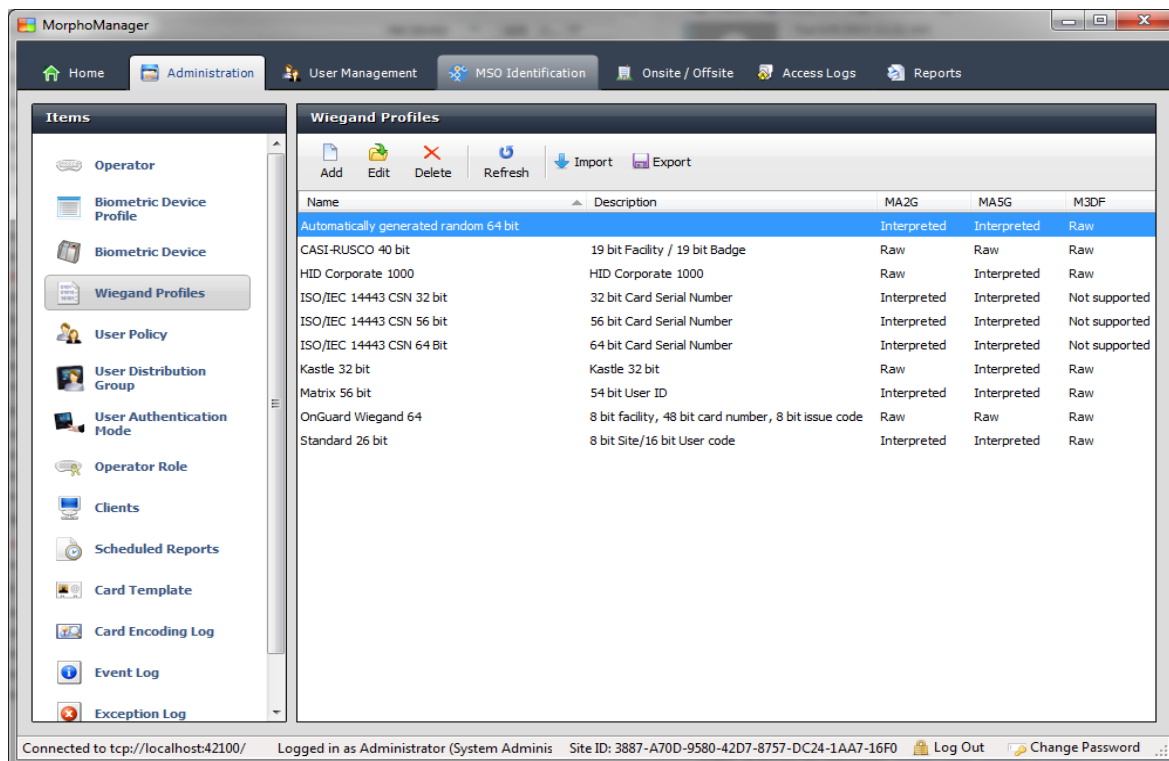
1. Wiegand Profiles
2. Biometric Device Profiles
3. Biometric Device
4. User Policy
5. User Distribution Group
6. BioBridge System Configuration

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.

The screenshot displays the MorphoManager web application interface. The top navigation bar includes 'Home', 'Administration', 'User Management', 'MSO Identification', 'Onsite / Offsite', 'AccessLogs', and 'Reports'. The left sidebar lists various system components, with 'Biometric Device Profile' highlighted. The main content area is titled 'Adding Biometric Device Profile' and contains the following fields and options:

- Name:** A text input field.
- Description:** A text input field.
- Configuration Mode:** A dropdown menu set to 'Express'.
- Realtime logging enabled:** A checkbox, currently unchecked.
- Log retrieval interval:** A numeric input field set to '300' with '(seconds)' next to it.
- Display name encoding code page:** A dropdown menu set to 'Western Europe (Default) (ISO-8859-1)', with a note '(Applicable to MA500 series only)'.
- Duplicate check on biometrics:** A checkbox, currently unchecked, with a note '(MA 100, MA 1, MA 500, MA VP, MA Sigma, MA Sigma Lite, MA Sigma Lite+, and MorphoWave only. Only applicable to new user adds or rebuild)'.
MorphoAccess heartbeat interval: A numeric input field set to '30' with '(seconds)' next to it.
- MA Sigma, MA Sigma Lite, MA Sigma Lite+ Only Settings:**
 - Allow Remote Enrollment:** A checkbox, currently unchecked.
 - Default User Policy for Remote Enrollment:** A dropdown menu set to 'Default'.

At the bottom of the form are navigation buttons: 'Back', 'Next', 'Finish' (with a green checkmark), and 'Cancel' (with a red X).

The status bar at the bottom of the window shows: 'Connected to tcp://localhost:42100/ Logged in as Administrator (System Adminis Site ID: B45E-4B3F-2A3F-4FD1-BD85-58AA-2986-32BB Log Out Change Password

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 Group 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.

The screenshot shows the 'Adding Biometric Device' configuration window. On the left is a navigation pane with 'Biometric Device' selected. The main area contains the following fields:

- Name: (text input)
- Description: (text input)
- Location: (text input)
- Asset ID: (text input)
- Export Value: (text input)
- Time Zone: (dropdown menu, currently set to '(UTC-05:00) Eastern Time (US & Canada)')
- Hardware Family: (dropdown menu)
- Serial Number: (text input)
- IMEI Number: (text input)
- Hostname/IP Address: (text input)
- Port: (text input, value: 11010)
- Biometric Device Profile: (dropdown menu)
- Include in Time & Attendance Exports: (checkbox)
- Change User Onsite / Offsite Status: (checkbox)
- Onsite Key: (dropdown menu, value: No Key)
- Offsite Key: (dropdown menu, value: No Key)

At the bottom right are buttons for 'Back', 'Next', 'Finish', and 'Cancel'.

- 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.

The screenshot shows the 'Biometric Device' management screen. At the top, there is a toolbar with buttons: Add, Edit, Delete, Refresh, Get Logs, Set Date/Time, Rebuild, and Set Offline. Below the toolbar is a table with the following data:

Name	Description	Location	Biometric D...	Status	Tasks
MA sigm Multi			Default	Online	0

Below the table are tabs for 'Details', 'Logs', 'Queued Tasks (0)', and 'Failed Tasks (0)'. The 'Details' tab is active, showing the following information for the 'MA sigm Multi' device:

- Description: MA SIGMA Multi
- Hardware Type: 1431SMS0000243
- Serial Number: 1.3.2
- Firmware version: 10.10.214.11:11010
- Hostname/IP Address: 0 / 3000
- Time Zone: (UTC-05:00) Eastern Time (US Canada)
- Device Status: Online

A small image of the biometric device is shown in the bottom right corner.

User Policy

User policies 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.

The screenshot shows a dialog box titled "Adding User Policy" with the instruction "Enter the details for this User Policy". The form includes the following fields and options:

- Name: [Text input field]
- Description: [Text input field]
- Access Mode: [Dropdown menu: All Biometric Devices and Clients]
- Allow MA 500 database selection during user enrollment
- Time Mask Mode: [Dropdown menu: 24 Hours, 7 Days a Week]
- Extended User Details: Display extended user details
- Wiegand Profile: [Dropdown menu: Automatically generated random 64]
- User Authentication Mode: [Dropdown menu: Biometric (1:Many)]
- Wave Enrollment Minimum Hands: [Dropdown menu: None]
- Finger Biometric Enrollment Minimum Fingers: [Dropdown menu: Two]
- Preferred Finger One: [Dropdown menu: Left Index Finger]
- Preferred Finger Two: [Dropdown menu: Right Index Finger]
- Preferred Duress Finger: [Dropdown menu: Left Middle Finger]
- Show Photo Capture Page:
- Show Wave Biometric Capture Page:
- Show Finger Biometric Capture Page: (User Authentication Mode requires templates)

At the bottom, there are four buttons: "Back", "Next", "Finish" (with a green checkmark), and "Cancel" (with a red X).



If you plan on using a Wiegand Profile, you will need to set it here in order for the users enrolled in this User Group 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.

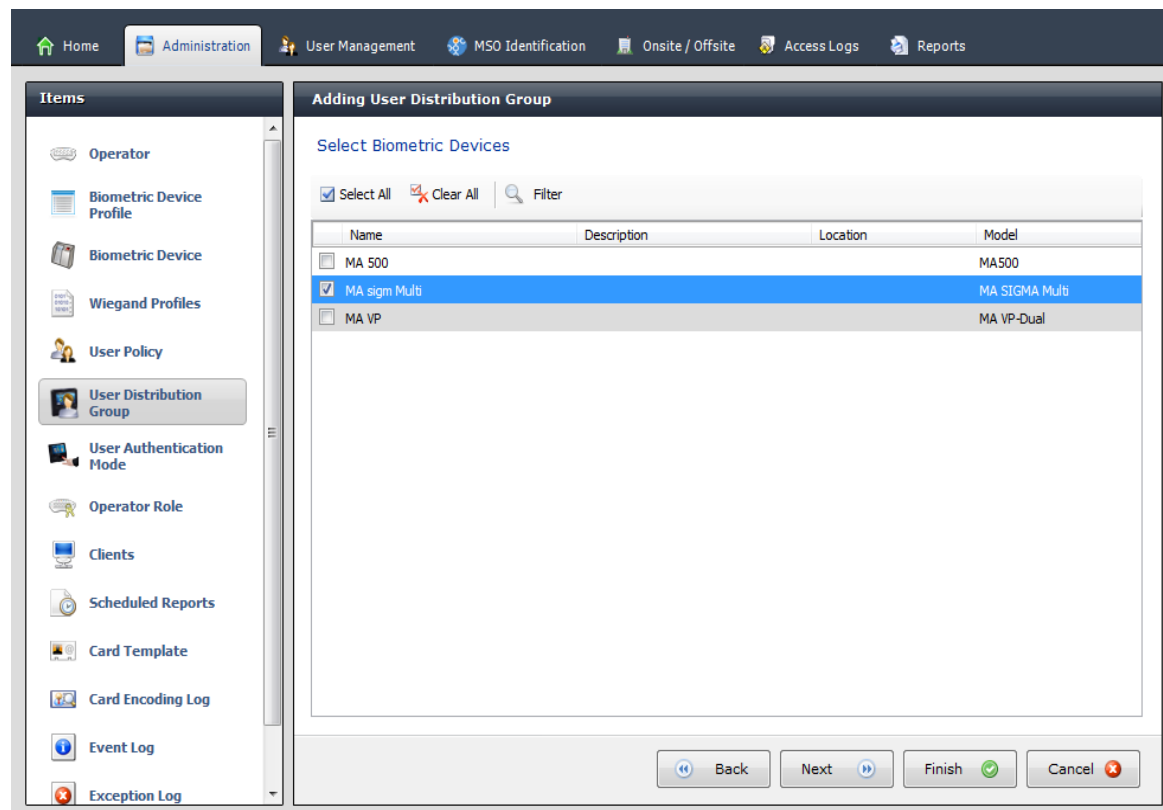
Please reference the MorphoManager User Manual for more detail on all the various properties that can be assigned to a User Policy including Wiegand Profile, Finger Biometric Enrollment Minimum, Fingers, Access Modes and User Authentication Modes.

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 Controlsoft Identity Access.

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

The screenshot shows the 'System Configuration' interface with the 'BioBridge' tab selected. The page title is 'MorphoManager BioBridge Settings'. The configuration options are as follows:

- System: None (dropdown menu) with a 'Configure connection' button.
- Wiegand Profile: (dropdown menu)
- Grouping Mode: (dropdown menu)
- Enable Forced User Policy: Enabled
- Forced User Policy: Default (dropdown menu)
- User Synchronization Start Time: 00:00 (time picker)
- User Synchronization End Time: 23:59 (time picker)
- Delay Between Each User Synchronization (ms): 50 (numeric input)
- Allow User Sync While User Cache Is Refreshing: Enabled
- User Cache Schedule: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday

Below the schedule, there is a grid of checkboxes for hourly intervals from 0:00 to 23:00, all of which are checked.

At the bottom, there is a section for 'User Distribution Group Mappings' with a table:

Access Groups	User Distribution Group

System: From the System drop down menu choose Controlsoft Identity Access and click the **Configure connection** button. A BioBridge connection box window will pop up. Fill in all the required fields and click OK.

Use basic connection string

Server / Instance

Please enter the hostname/address and instance name (if applicable) of the SQL Server you would like to connect to:

SQL Server:

Database:

Logon details

Please select the authentication mechanism to use to connect to the SQL Instance:

Use Windows Integrated Security

Use SQL Server User & Password

Username:

Password:

Use advanced connection string

Connection string:

OK Cancel

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

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

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

Access Level Mode: Automatic

Caching Engine Refresh Interval (min):

Synchronization Engine Refresh Interval (ms):

Enable Forced User Policy:

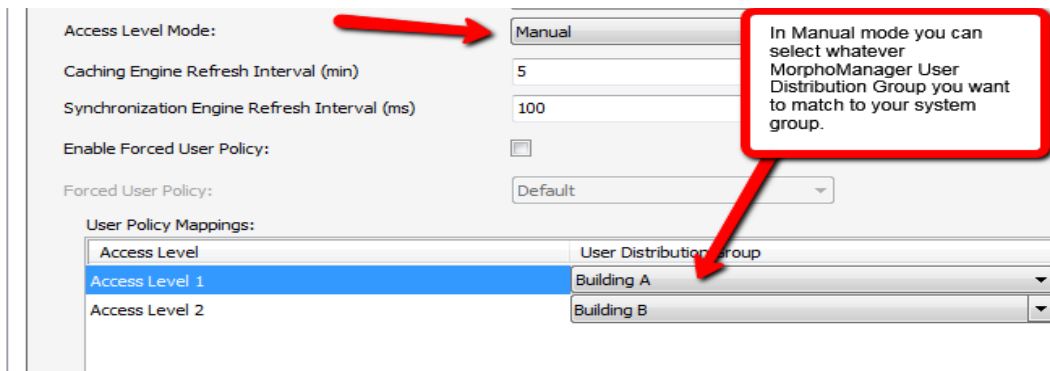
Forced User Policy:

User Policy Mappings:

Access Level	User Distribution Group
Access Level 1	Access Level 1
Access Level 2	Access Level 2

In Automatic mode the groupings from your system and the User Distribution Groups created in MorphoManager with the same name will match up. Those with no match would be left blank.

Manual: If the Access Level grouping names of Controlsoft Identity Access and the User Distribution Group(s) created in MorphoManager are not the same, then selecting which Controlsoft Identity Access 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

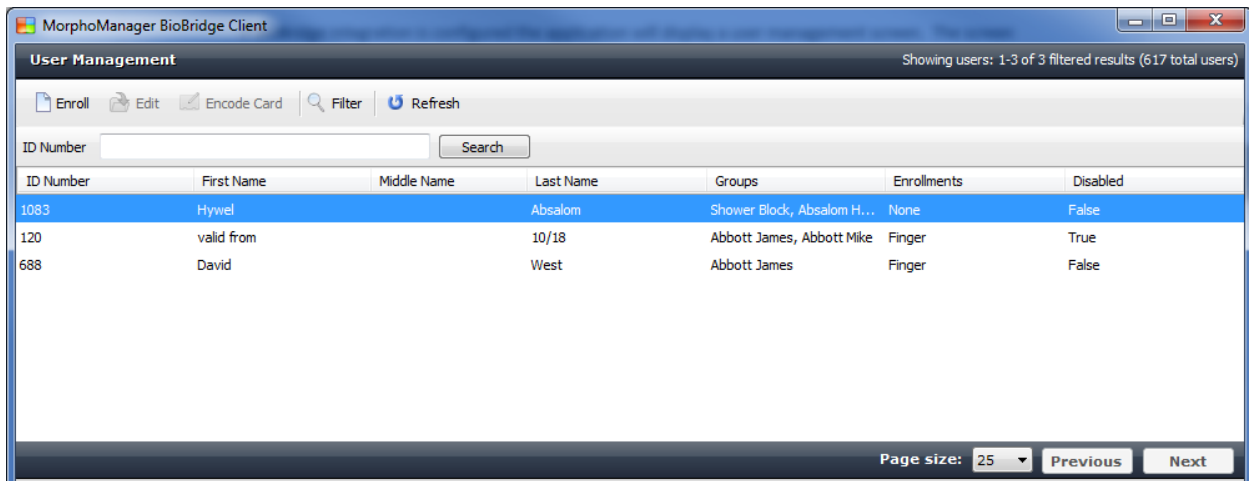
After configuring BioBridge you will now utilize the BioBridge Enrollment Client. This client will check if BioBridge Integration has been enabled and configured. If it is has not, the application will display the message “BioBridge integration has not been enabled and configured” and you will need to 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

The screenshot displays a user management interface with several sections:

- User Details:** Includes input fields for First Name, Middle Name, Last Name, ID Number, and Date of Birth. Below these is an 'Enabled' section with radio buttons for 'Any' (selected), 'Enabled', and 'Disabled'.
- User Wiegand values:** A section with the text 'Not Applicable' and an empty input field.
- Groups:** A list of groups with checkboxes for selection. The groups are: Abbott James (checked), Abbott Mike (checked), Absalom Hywel (checked), Acheson Kenneth (checked), Adam Jonathan (checked), and Adams Kerry (checked). Above the list are 'Select All' and 'Clear All' options.
- Sort By:** Three dropdown menus for sorting: Primary (ID Number Ascending), Secondary (Last Name Ascending), and Tertiary (First Name Ascending).

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

- First Name
- Last Name
- ID Number
- Enabled/Disabled
- Group

Refresh

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

Search Field

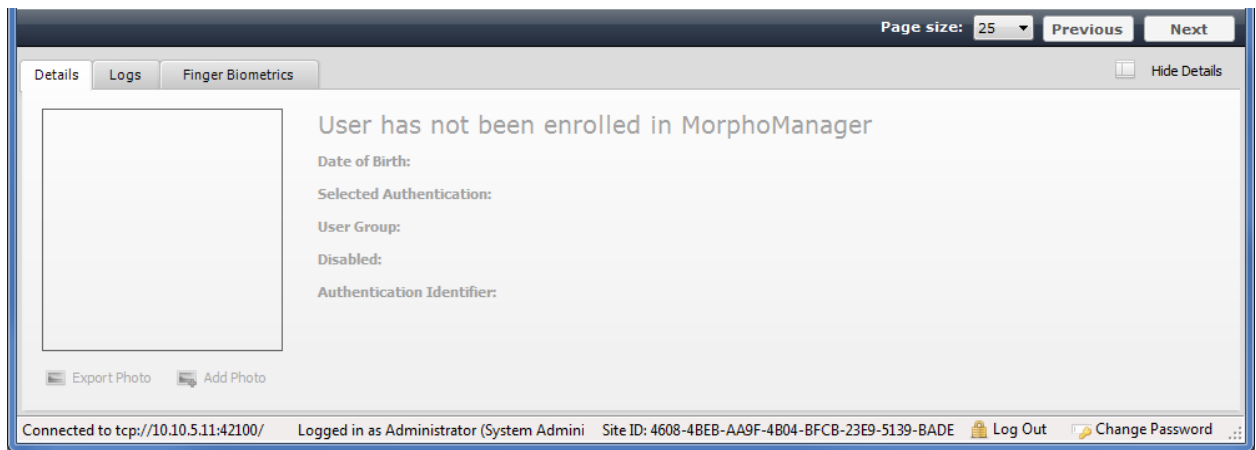
The Search Field can be used to find individual users quickly and/or to migrate users from Controlsoft to the BioBridge Enrollment Client without waiting for a cache refresh.

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:

- ID Number
- First name
- Last name
- Groups – All of the groups that your user is a member of in your system.(Comma separated values)
- 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

Embedded enrollment is not supported for Controlsoft Identity Access.