

# BioConnect ID Enterprise v4.2

---

## Software Configuration Guide

Revision 1.0

## Table of Contents

1. Support .....	3
2. Software Configuration .....	4
2.1 Root Account Login .....	4
2.2 Configuration Options .....	4
2.2.1 BioConnect ID Enterprise Configuration .....	5
2.2.2 BioConnect ID Enterprise Reporting Configuration .....	6
2.2.3 Licensing Configuration .....	7
3. Client Navigation .....	8
4. User Management .....	10
4.1 Credentials Tab .....	10
4.2 Administration Tab .....	11
4.2.1 Username and Password .....	11
4.2.2 Active Directory .....	12
5. Quick Enrollment .....	14
5.1 Fingerprint Enrollments .....	14
5.2 Encode to Card (Template on a Card) .....	16
5.3 User Credentials .....	17
5.4 Face Enrollment (FaceStation) .....	17
6. Device Management .....	18
6.1 Adding a Device .....	18
6.2 Recommended: Adding a Device in DHCP .....	18
6.3 Advanced: Adding a Device using BioStar Config .....	20
6.4 Reader Setting Definitions (Device Management) .....	21
6.4.1 Details Tab .....	21
6.4.2 General Information Tab .....	23
6.4.3 Network Details Tab .....	24
6.4.4 Wiegand Details Tab .....	24
7. Synchronization .....	26
8. Advanced: BioStar Configuration Software .....	27
9. Additional Assistance .....	28
Appendix A: Dashboard Quick Review .....	29

## 1. Support

Telephone support is available Monday - Friday from 8:30 AM to 8:30 PM Eastern to assist with installing, configuring and troubleshooting the BioConnect ID Enterprise. The technical support team is well versed to assist integrators both during the planning or post sales stages.

The goal of the BioConnect team is to make the software as easy as possible to install and configure. If an unexpected problem occurs or if you would like some guidance, please don't hesitate to reach out using one of the contact methods listed below:

### Support Website:

<http://www.bioconnect.com/support/>

### Telephone:



Toll-Free 1-855-ENTERID (368-3743)

### Email:

[support@bioconnect.com](mailto:support@bioconnect.com)

## 2. Software Configuration

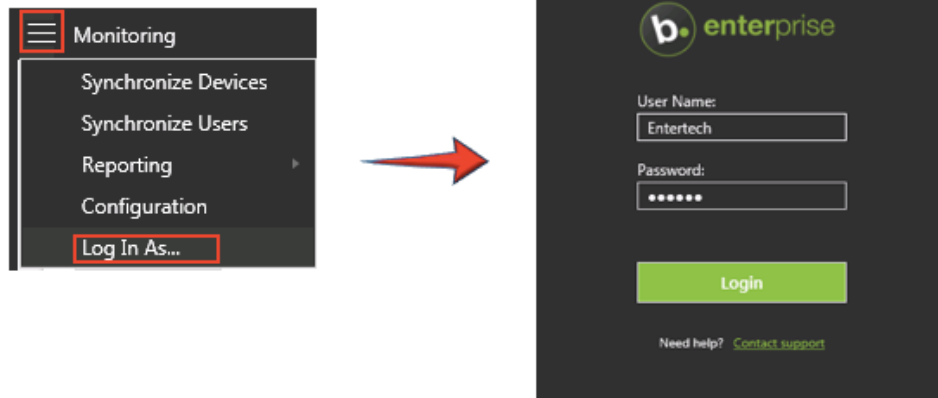
### 2.1 Root Account Login

The default “root” level account is (case sensitive):


Username: Entertech

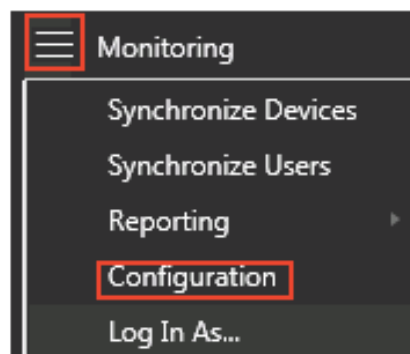
Password: Bobcat

This account’s password can be changed within the configuration window.



### 2.2 Configuration Options

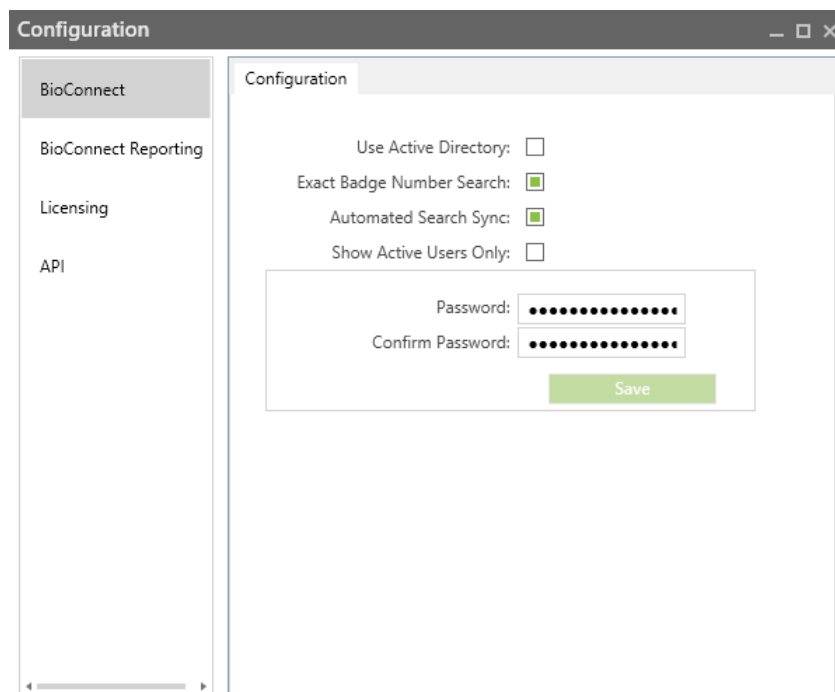
To open, click [Menu]  > [Configuration].



You will see three configuration tabs on the left pane: BioConnect, BioConnect Reporting, Licensing. (For more details see section 2.2.1)

### 2.2.1 BioConnect ID Enterprise Configuration

This section of the software is primarily used by the root level Administrator account “Entertech”. This allows you to turn on/off Active Directory, set the root account password, check the status of your license or update the existing license.



#### Use Active Directory

If you enable the Use Active Directory option, all Username and Passwords will no longer be able to login to the software with the exception of the root level administrator account. Only accounts that are registered on the domain and linked to a cardholder within BioConnect ID Enterprise will be able to access the software. To add Active Directory accounts, go to the cardholder’s profile within User Management (See [section 4.2](#))

#### Exact Badge Number Search

This option requires that you type the exact credential number of the cardholder you are searching for instead of a portion of the credential number. For example, if you are searching for the card “18273”, with this checkbox left unchecked, you will get the record with the card “18273”, but you also get “182731323, 123182732, 918273”

because all of these cards consist of the 18273 digits. To protect against this, you can choose to only bring results for the exact number you searched for.

### **Automated Search Sync**

This option allows you to enable or disable the automatic database sync that occurs every time you press the [Search] button or open Quick Enrollment or User Management. In large systems, this can improve the speed of the software and will result in the software only synchronizing every 5 minutes, or anytime a manual synchronize is triggered from the software menu.

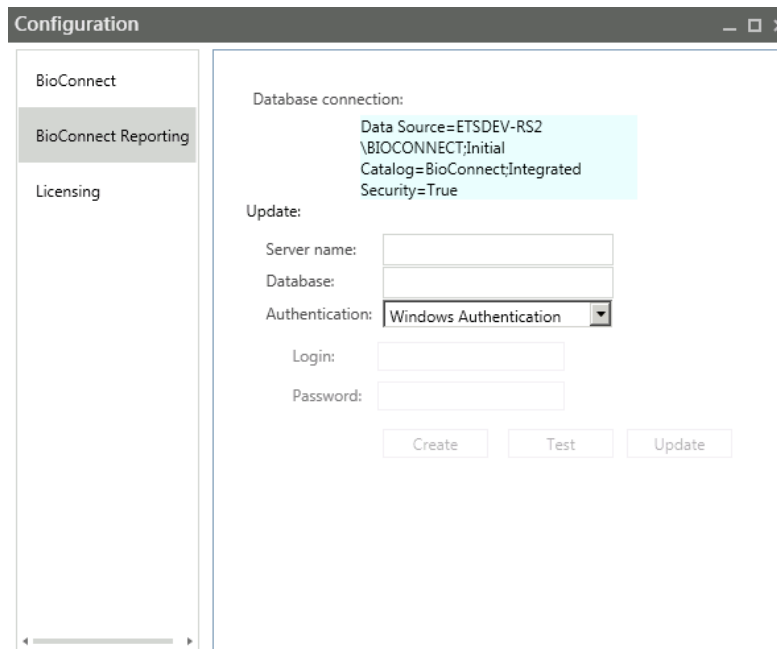
### **Show Active Users Only**

This option allows you to filter the BioConnect ID Enterprise user list to display only active users from the ACM. The default setting is to show all users synchronized from the ACM, both active and inactive.

## **2.2.2 BioConnect ID Enterprise Reporting Configuration**

The 'Reporting' section of BioConnect ID Enterprise allows you to take the system's event data, sort it, and export customized reports based on your specifications.

Before using the reporting section itself, you'll need to enter connection details for the database which is storing your event logs. This is generally the same database used to install / setup BioConnect ID Enterprise, so use those connection settings if you're unsure. By default, the Reporting connection setting will match your existing BioConnect ID Enterprise database. See below:



**Configuration**

BioConnect

BioConnect Reporting

Licensing

Database connection:

Data Source=ETSDEV-RS2  
 \BIOCONNECT;Initial  
 Catalog=BioConnect;Integrated  
 Security=True

Update:

Server name:

Database:

Authentication:

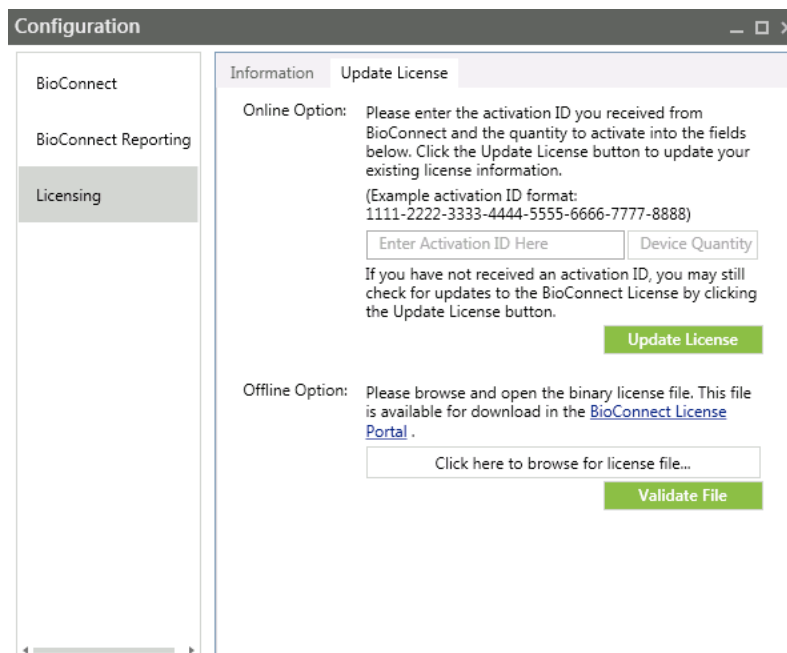
Login:

Password:

The [Test] button will confirm whether your settings established a proper connection to the database. Once you've tested the connection, click [Update] to save those settings.

### 2.2.3 Licensing Configuration

After setting up your initial trial or license, you can always update an existing license by going to **Menu -> Configuration -> Licensing** from the BioConnect ID Enterprise application.



**Configuration**

BioConnect

BioConnect Reporting

Licensing

Information Update License

Online Option: Please enter the activation ID you received from BioConnect and the quantity to activate into the fields below. Click the Update License button to update your existing license information.  
 (Example activation ID format: 1111-2222-3333-4444-5555-6666-7777-8888)

If you have not received an activation ID, you may still check for updates to the BioConnect License by clicking the Update License button.

Offline Option: Please browse and open the binary license file. This file is available for download in the [BioConnect License Portal](#).

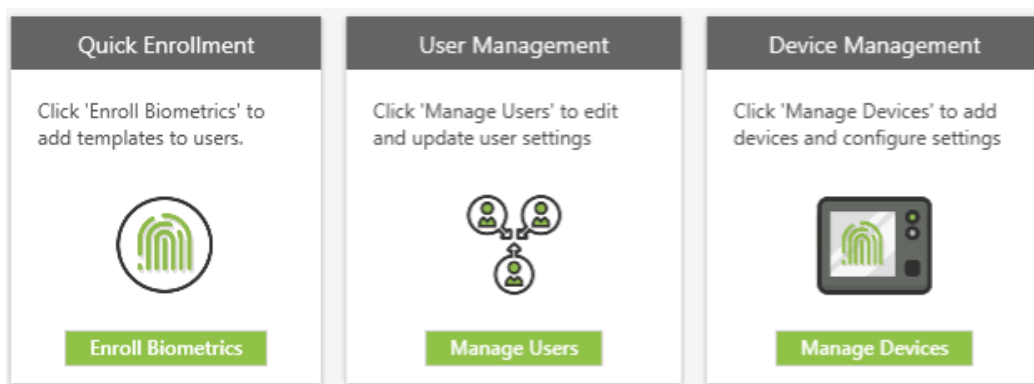
### 3. Client Navigation

This is the BioConnect ID Enterprise home screen. Here you have 3 options to choose from:

**Quick Enrollment:** This is where you conduct all biometric enrollments or Template on a Card encoding. (See Chapter 5 for more information.)

**User Management:** Here you can see all of the users that have synchronized over from the access control software. (See Chapter 4 for more information.)

**Device Management:** Here you can check the status of the readers or complete tasks such as firmware updates, add new devices, or configure reader settings. (See Chapter 6 for more information.)



**Menu:** This Menu consists of the Synchronization tools (Synchronize with Devices or Access Control Software), as well as software configuration options.

**Monitoring:** This feature allows you to view system events including reader status messages, or BioConnect ID Enterprise user account login/activity data.

**Support:** This will direct you to BioConnect ID technical support website.

**About:** This will show you the software version of your client and server, technical support contact information and the software expiry date.

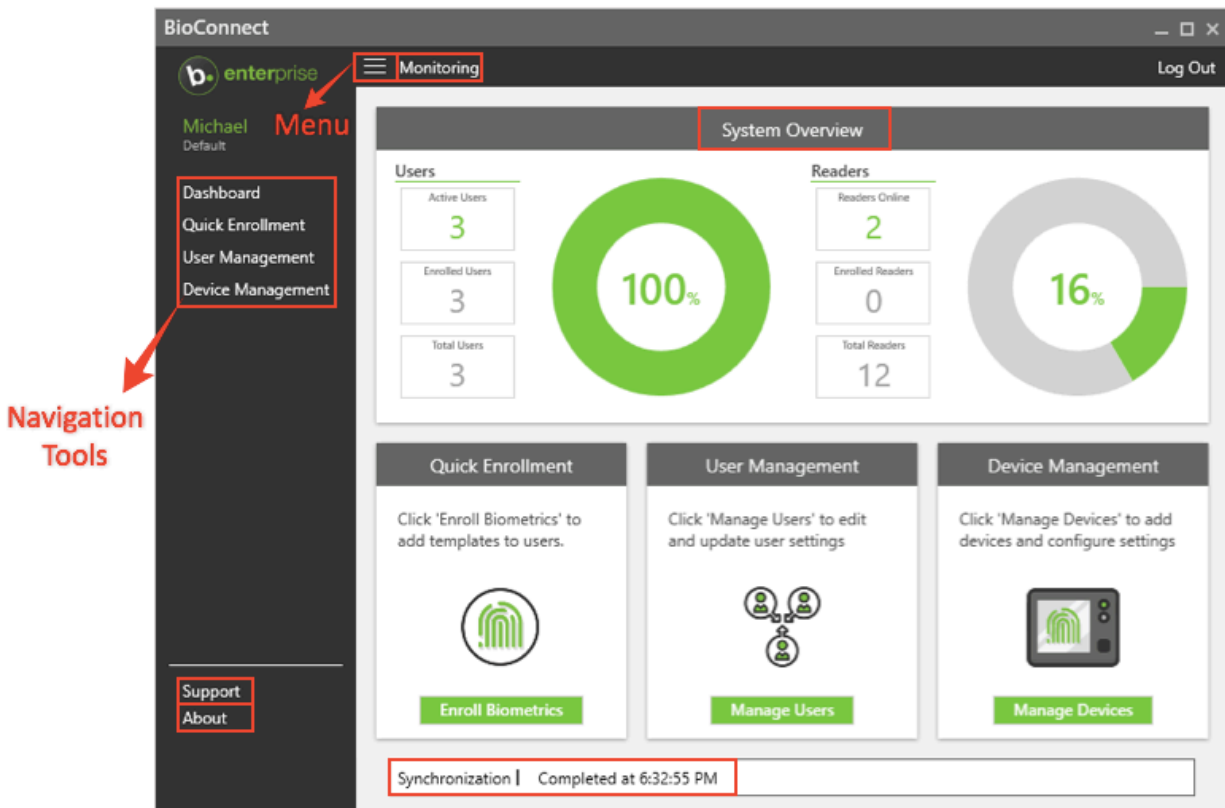
**System Overview:** This feature allows you to view the user and reader onboarding status by showing number of users (by active users, enrolled users, total users),



number of readers (by readers online, enrolled readers, total readers) as well as the percentages of active users and readers online.

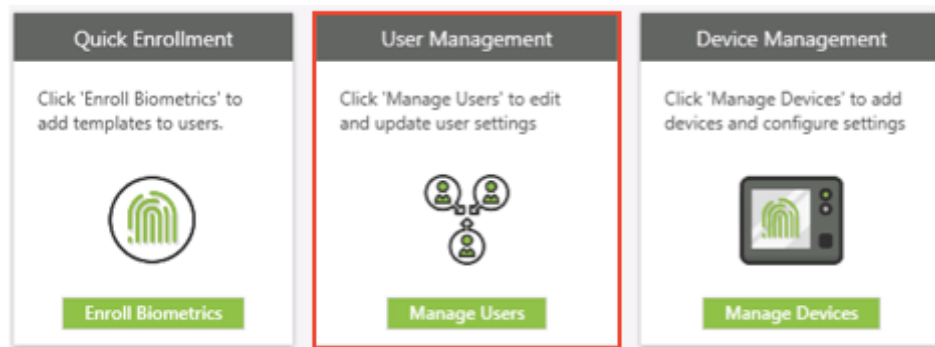
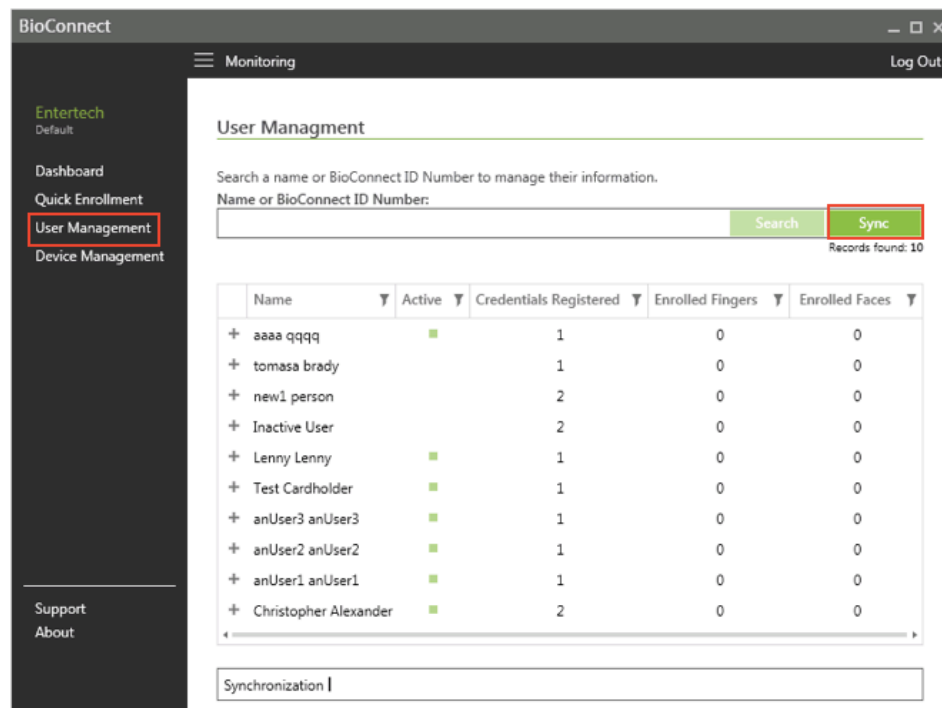
**Navigation Tools:** There are shortcuts available in each section to assist you with navigating throughout the software.

**Synchronization Status:** Data displayed here will inform you of the current status of the synchronization between your access control software and BioConnect.



## 4. User Management

The User Management section of the software allows you to view all of the users who have been synchronized from your access control software. You can sort/filter the users to see details such as who has been enrolled. Click [Sync] at any time to re-sync the data in the list.

The screenshot shows the BioConnect User Management interface. On the left is a sidebar with navigation links: Entertech Default, Dashboard, Quick Enrollment, User Management (highlighted with a red box), and Device Management. Below these are links for Support and About. The main area is titled 'User Management' and contains a search bar with the text 'Search a name or BioConnect ID Number to manage their information.' and a 'Sync' button (highlighted with a red box). Below the search bar is a table with 10 records found. The table has columns: Name, Active, Credentials Registered, Enrolled Fingers, and Enrolled Faces. The records are as follows:

Name	Active	Credentials Registered	Enrolled Fingers	Enrolled Faces
+ aaa qqq	■	1	0	0
+ tomasa brady		1	0	0
+ new1 person		2	0	0
+ Inactive User		2	0	0
+ Lenny Lenny	■	1	0	0
+ Test Cardholder	■	1	0	0
+ anUser3 anUser3	■	1	0	0
+ anUser2 anUser2	■	1	0	0
+ anUser1 anUser1	■	1	0	0
+ Christopher Alexander	■	2	0	0

At the bottom of the interface is a 'Synchronization' section with a button.

### 4.1 Credentials Tab

All badges are listed under the Credentials tab of the user profile.

1. **Active Checkbox:** The cardholder must have an active credential within the access control software to appear “active” within BioConnect ID Enterprise. If there are no active credentials, the user will appear inactive within BioConnect ID Enterprise. Please see below for some definitions of the various options:
2. **Biometric Card Checkbox:** This option allows you to choose which card is sent to the access control panel in the event of a Biometric-Only identification. If no card is selected, the system will assume the first card listed. This is only necessary when a cardholder has multiple credentials.
3. **Card Only Checkbox:** This checkbox allows the selected card to be accepted by the reader without a biometric verification. If the reader is configured for Card + Finger, this will allow the card to gain access immediately without a biometric verification. This is a useful feature for people who are not going to be enrolled, or people who have not enrolled yet but still need access.

Name ▼	Active ▼	Credentials Registered ▼	Enrolled Fingers ▼	Enrolled Faces
Test Cardholder	<input checked="" type="checkbox"/>	1	0	0
<div> Details Biometrics <b>Credentials</b> Device Sync Administration </div>				
Badge Number ▼	Active	Biometric Card	Card Only	
312323	<input checked="" type="checkbox"/>			

## 4.2 Administration Tab

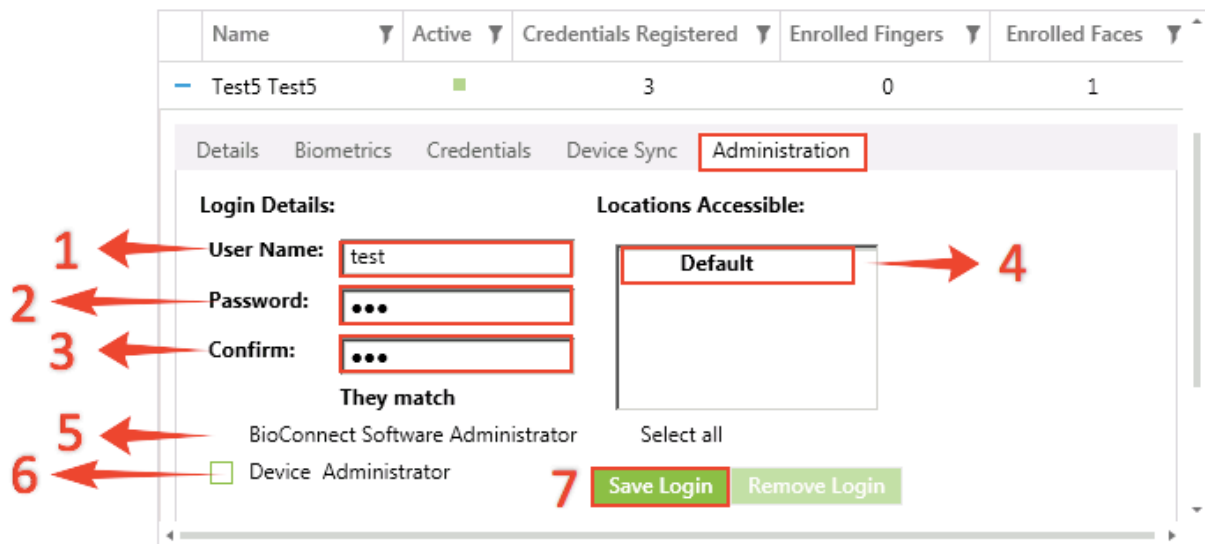
The Administration tab allows you to give access to the BioConnect ID Enterprise. This can be done using a Username and Password, or by using Active Directory. Cardholders are linked to Usernames or Windows Credentials to gain access to the BioConnect ID Enterprise to conduct enrollments.

### 4.2.1 Username and Password

To provide access using Username and Password, Active Directory must be turned off. This can be turned off within the Configuration section of the software.

1. Enter the username into the text field that you would like to provide access to. In the example below, the username is ‘test’.

2. Enter a value into the password field (For example, “123”).
3. Retype the password in the text field to confirm it.
4. Choose a location(s) that the person will be working from. This will allow them to see the enrollment readers that are at that specific location.
5. Decide if the user is going to be an Administrator or Standard User. Admins can access the entire software including device management, as well as providing other cardholders access to the software. Standard Users can only login to the software to conduct enrollments.
6. Decide if the user is a Device Administrator. Device Admins are able to login to the on-screen menus of devices that have LCDs. This level of access should be restricted to network administrators.
7. Click [Save Login]



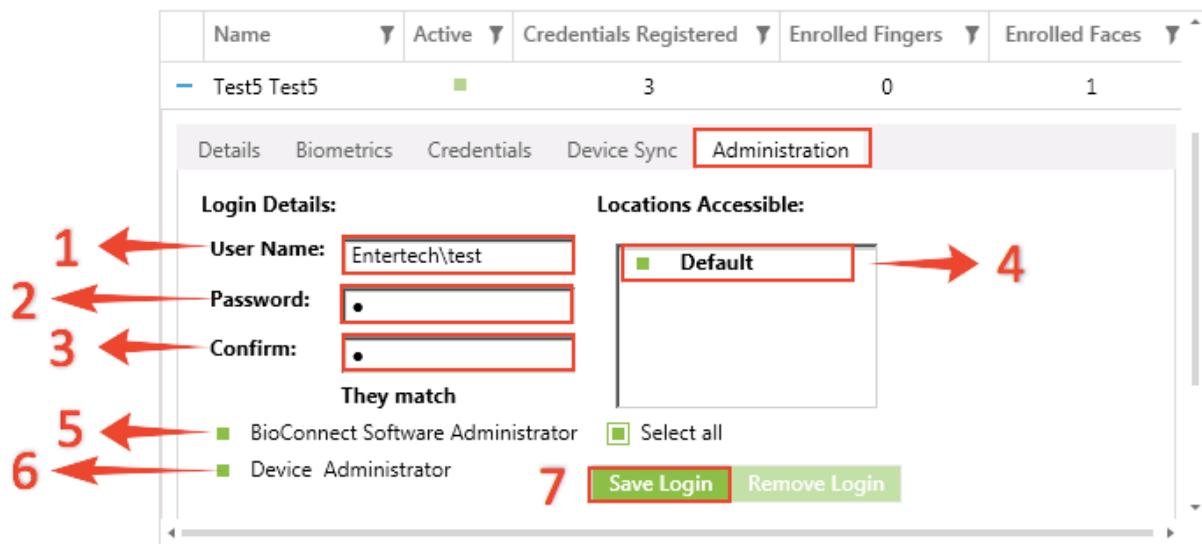
The screenshot shows a user management interface for 'Test5 Test5'. At the top, a table lists user statistics: Name, Active, Credentials Registered (3), Enrolled Fingers (0), and Enrolled Faces (1). Below this is a tabbed interface with 'Administration' selected. The 'Login Details' section contains three input fields: 'User Name' (containing 'test'), 'Password' (masked with dots), and 'Confirm' (masked with dots). Red callout 1 points to the User Name field, 2 to the Password field, and 3 to the Confirm field. Below these fields, a message states 'They match'. To the right, the 'Locations Accessible' section shows a dropdown menu with 'Default' selected, indicated by red callout 4. Below the login details, there are two checkboxes: 'BioConnect Software Administrator' (checked) and 'Device Administrator' (unchecked), with red callouts 5 and 6 respectively. At the bottom right, there are two buttons: 'Save Login' (highlighted with a red box and callout 7) and 'Remove Login'.

#### 4.2.2 Active Directory

To provide access using Active Directory, the option must be enabled within the Configuration section of the software. Once this is enabled, the only user who can access the software using a Username and Password is the root level administrator “Entertech”.

1. Enter the “DOMAIN\username” into the username field that you would like to provide access to. In the example below, the domain is ‘Entertech’ and the Windows Account username is ‘test’.
2. Enter a value into the password field (For example, “1”). This will not be able to be used for access to the software, it is simply a placeholder. You do not need to use the person’s actual Active Directory password.

3. Retype the password in the text field to confirm it.
4. Choose a location(s) that the person will be working from. This will allow them to see the enrollment readers that are at that specific location.
5. Decide if the user is going to be an Administrator or Standard User. Admins can access the entire software including device management, as well as providing other cardholders access to the software. Standard Users can only login to the software to conduct enrollments.
6. Decide if the user is a Device Administrator. Device Admins are able to login to the on-screen menus of devices that have LCDs. This level of access should be restricted to network administrators.
7. Click [Save Login]



The screenshot shows the 'Administration' tab of the BioConnect Software interface. The interface includes a table at the top with columns: Name, Active, Credentials Registered, Enrolled Fingers, and Enrolled Faces. Below the table is a form with two main sections: 'Login Details' and 'Locations Accessible'.

**Step 1:** Points to the 'User Name' field, which contains 'Entertech\test'.

**Step 2:** Points to the 'Password' field, which is masked with dots.

**Step 3:** Points to the 'Confirm' field, which is also masked with dots.

**Step 4:** Points to the 'Locations Accessible' dropdown menu, which currently shows 'Default'.

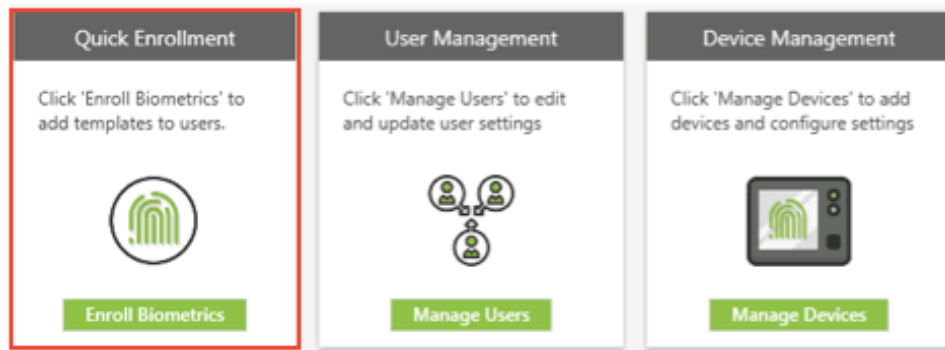
**Step 5:** Points to the 'BioConnect Software Administrator' checkbox, which is checked.

**Step 6:** Points to the 'Device Administrator' checkbox, which is checked.

**Step 7:** Points to the 'Save Login' button.

Other visible elements include the 'Details', 'Biometrics', 'Credentials', 'Device Sync', and 'Administration' tabs. The 'Login Details' section also shows a 'They match' confirmation message. The 'Locations Accessible' section has a 'Select all' checkbox.

## 5. Quick Enrollment



### 5.1 Fingerprint Enrollments

**Quick Enrollment**


Search a name or BioConnect ID Number and select a reader to enroll a user.

Name or BioConnect ID Number:

Reader Name:

Finger Enrollment   Encode To Card   User Credentials   Face Enrollment

Select a Finger:  Minimum Quality:



The Quick Enrollment section of the software is where all biometrics are captured. To enroll a fingerprint:

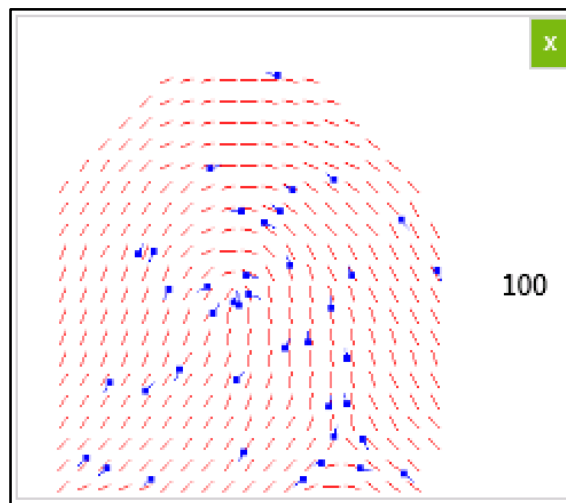
1. Search for the user you would like to enroll.
2. Choose which reader you would like to enroll from (For BioMini USB scanner enrollments, you will see the device listed within this list when it is connected to your PC).
3. Choose which finger you would like to enroll.
4. Click [Enroll]

The enrollment process will ask you to place your finger 3 times. Ensure that you lift your finger up off of the scanner between each scan. Doing this allows for more unique data points to be captured and creates a higher quality enrollment.

**NOTE:** If you do not see the device in the list that you are looking for, please see section 6.4 to enable the device as an enrollment reader.

The [Sync] button performs a check on the Access Control database for any changes to cardholder information.

It is critical for the success of the system that good enrollments are captured. Below is an example of a good enrollment:



In the above example, you can see that the **middle** of the finger is placed in the middle of the scanner. You can clearly see the ridges of the fingerprint and the quality score is at 100% (Quality scores are only available when enrolling from the BioMini USB scanner).

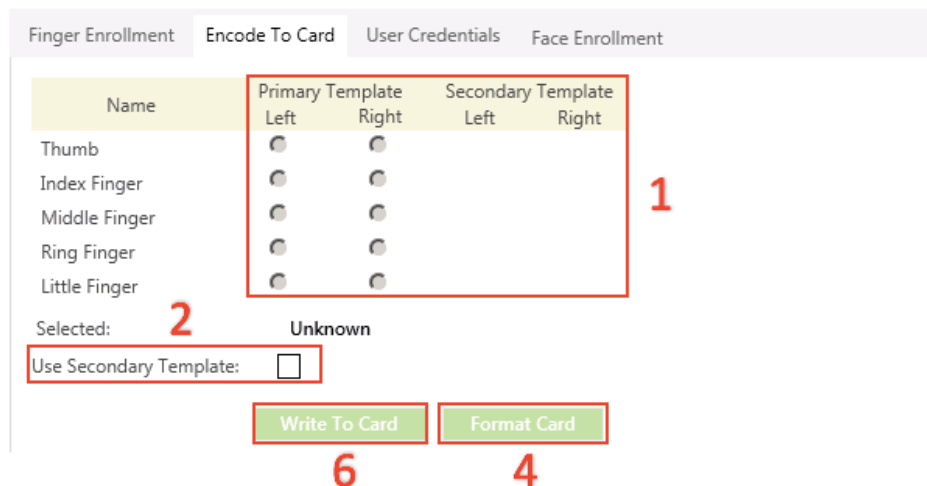
**WARNING:** Placing your fingers too low on the scanner, or not placing the finger flat create poor enrollments. These will lead to low success rates and could also increase the possibility of a False Accept (Having a fingerprint show up as another cardholder). Although this is extremely unlikely, having a high volume of poor fingerprints (Fingertips) in the software can lead to issues as fingertips do not have as much unique data as the middle of the finger. **Always ensure that you are capturing the best fingerprints possible during the enrollment phase.** These enrollments are going to be the basis for all fingerprint matching going forward.

## 5.2 Encode to Card (Template on a Card)

When working with Mifare or iClass smartcards, you have the option of encoding two templates onto the card itself for verification. This allows you to carry your templates with you to the reader instead of having the reader use the Server as it's matching database. This is common in locations where networking is difficult.

To encode templates onto the card:

1. Choose a template for your primary and secondary template.
2. If you prefer to only write one template, you can uncheck "Use Secondary Template".
3. Choose a reader that is smart card compatible (iClass or Mifare) as your enrollment device.
4. Click [Format Card].
5. Hold the Smart Card up against the front of the reader until you hear a "success" chime.
6. Click [Write Card].
7. Hold the card up against the front of the reader until you hear a "success" chime.



Name	Primary Template		Secondary Template	
	Left	Right	Left	Right
Thumb	<input type="radio"/>	<input type="radio"/>		
Index Finger	<input type="radio"/>	<input type="radio"/>		
Middle Finger	<input type="radio"/>	<input type="radio"/>		
Ring Finger	<input type="radio"/>	<input type="radio"/>		
Little Finger	<input type="radio"/>	<input type="radio"/>		

Selected: Unknown

Use Secondary Template: ☐

Write To Card Format Card

Once this completes, the template is now located on the internal memory of the card. You will need to configure the readers to accept Template on a Card using the BioStar Configuration Software. For more details on this software, see the Chapter 8 in this guide for BioStar Configuration Software.

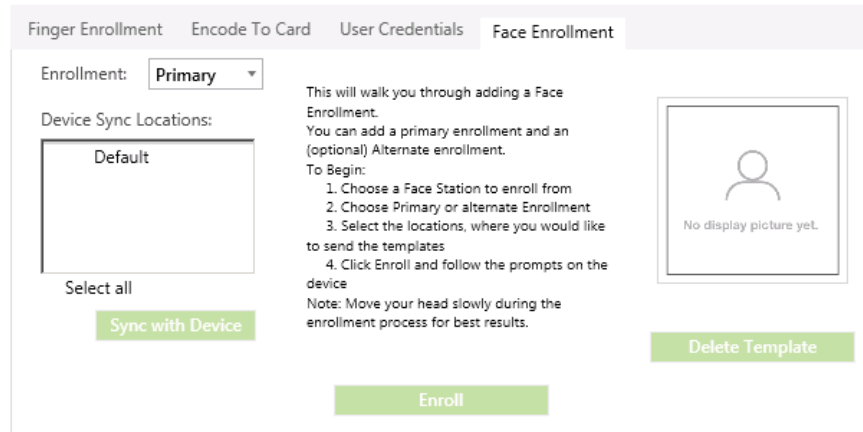


## 5.3 User Credentials

For details on User Credentials – Please see section 4.1 [Credentials Tab](#).

## 5.4 Face Enrollment (FaceStation)

To enroll a Face, you must have a FaceStation device added to BioConnect ID Enterprise with the “Enrollment” option applied within the device settings.



Face templates are sent to devices in groups. You can choose which location groups to send the templates to – This will send the templates to all of the devices listed under that specific location group.

The maximum number of face templates that should be sent to a device for 1:N matching (Matching with only your face/biometric only) is 1,000. To use more than 1,000 faces in a given location group, a 1:1 verification should be used (Either typing the BioConnect ID into the device before verifying your face, or by presenting a card to the device before verification).

You can enroll two face templates per user (Not required). If a user occasionally wears glasses, it is best to enroll them both with and without glasses.

**Delete Templates:** Clicking [Delete Templates] will remove all of the user’s templates from the system and devices. Once the templates are deleted, the user will have to re-enroll before using the system again.

**Sync with Device:** Using the Sync with Devices function will re-send the templates to the appropriate location device groups. If you want to change the device sync locations after the enrollment process has been completed, make the location changes and click [Sync with Device].

## 6. Device Management

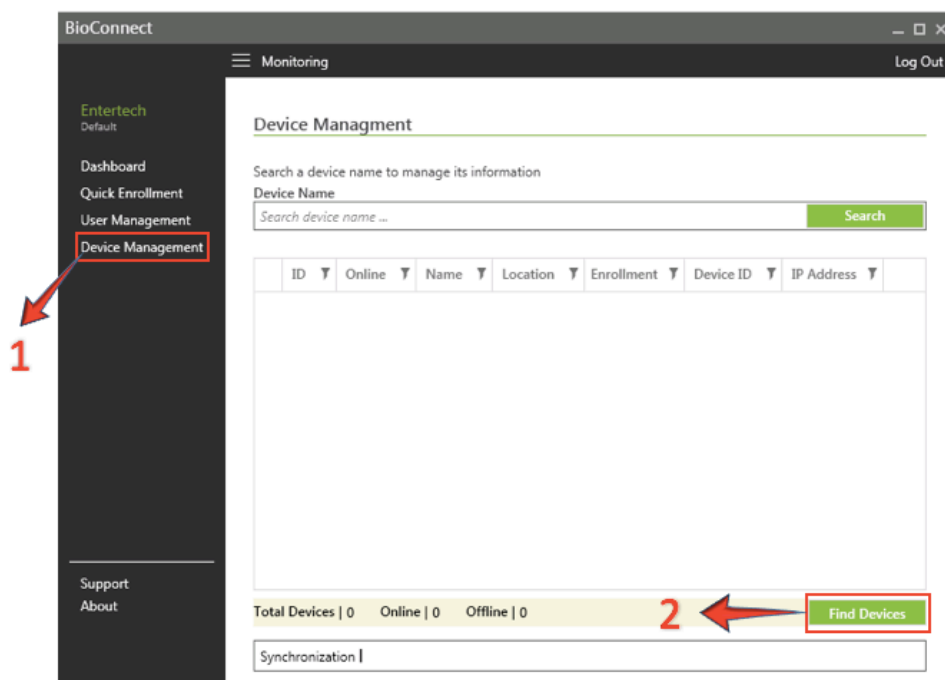
### 6.1 Adding a Device

The easiest way to configure and network Suprema readers is to connect them into a router. All Suprema readers come in DHCP mode out of the box. To network them, simply connect them into a network that supports DHCP. If you connect the device directly to a standalone “dumb” switch or directly to your PC, you won’t acquire an address. You can reset the devices back to a default IP address of 192.168.0.1 - To do this, please see the User Manual for the specific device type, included with the BioConnect ID Enterprise Install Package.

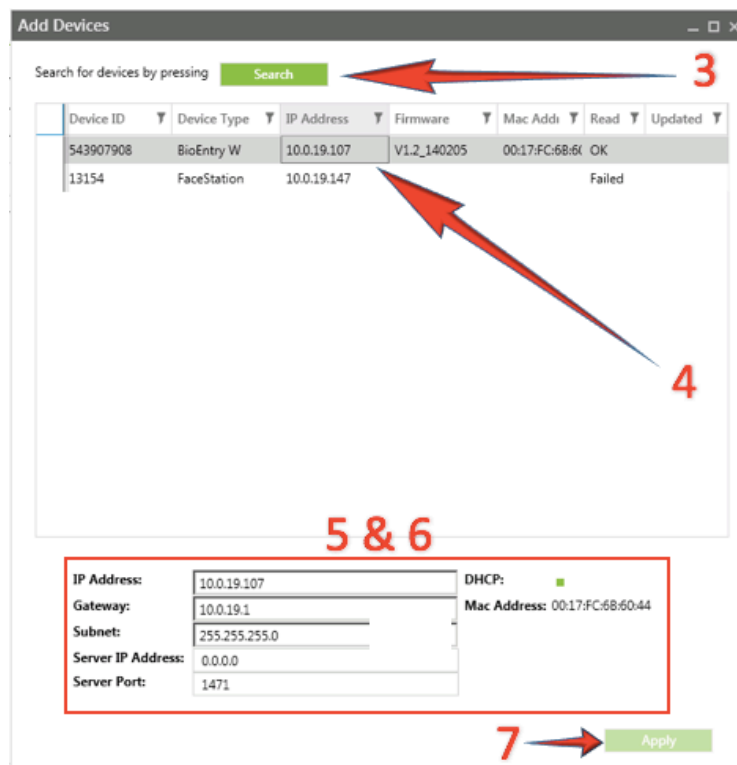
### 6.2 Recommended: Adding a Device in DHCP

**NOTE:** Your device must be on the same network as your BioConnect ID Enterprise Client software. This means, the client should be installed on a local PC or laptop, acquiring an IP address in the same range/subnet as the readers and connected back to the BioConnect server.

1. Go to **Device Management**
2. Click [Find Devices]



3. Click the [Search] button to find readers on the network
4. Choose your reader - If the “Read” column says OK, the software connected to the device successfully. If it says “FAIL”, this means that the connection was not successful. The device may already be connected to a server or at an unreachable IP address.
5. Choose to either use DHCP, or statically set the IP Address, Subnet and Gateway.
6. Enter the IP Address of the server that you want the device to connect to with a Server Port of 8001 (Generation 1 Device) or 51212 (Generation 2 Device).
7. Click [Apply]
8. The device will automatically show up within the Device Management window within about 30 seconds. If the device does not show up, ensure that you have no firewalls blocking TCP Port 8001/51212.



The screenshot shows the 'Add Devices' window. At the top, there is a search bar with a green 'Search' button, indicated by a red arrow and the number 3. Below the search bar is a table with columns: Device ID, Device Type, IP Address, Firmware, Mac Address, Read, and Updated. The table contains two rows: one for 'BioEntry W' with IP 10.0.19.107 and 'Read' status 'OK', and another for 'FaceStation' with IP 10.0.19.147 and 'Read' status 'Failed'. A red arrow points to the 'BioEntry W' row, labeled with the number 4. Below the table, there is a section for configuration, indicated by a red box and the numbers 5 & 6. This section includes fields for IP Address (10.0.19.107), Gateway (10.0.19.1), Subnet (255.255.255.0), Server IP Address (0.0.0.0), and Server Port (1471). To the right of these fields are checkboxes for DHCP (checked) and Mac Address (00:17:FC:68:60:44). At the bottom right, there is a green 'Apply' button, indicated by a red arrow and the number 7.

Device ID	Device Type	IP Address	Firmware	Mac Address	Read	Updated
543907908	BioEntry W	10.0.19.107	V1.2_140205	00:17:FC:68:60:44	OK	
13154	FaceStation	10.0.19.147			Failed	

IP Address: 10.0.19.107  
Gateway: 10.0.19.1  
Subnet: 255.255.255.0  
Server IP Address: 0.0.0.0  
Server Port: 1471

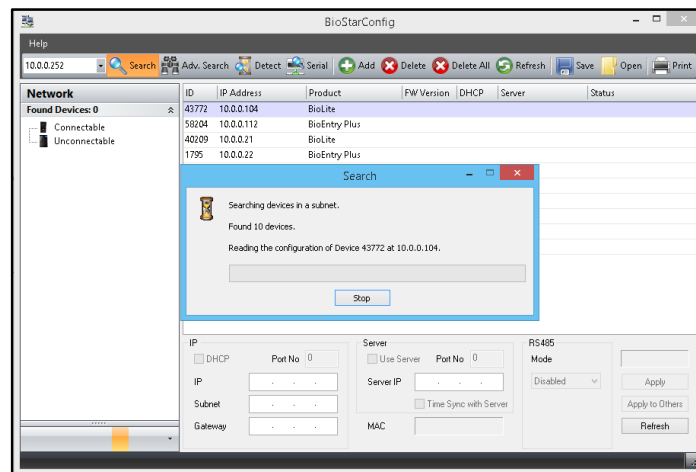
DHCP: ☒  
Mac Address: 00:17:FC:68:60:44

Apply

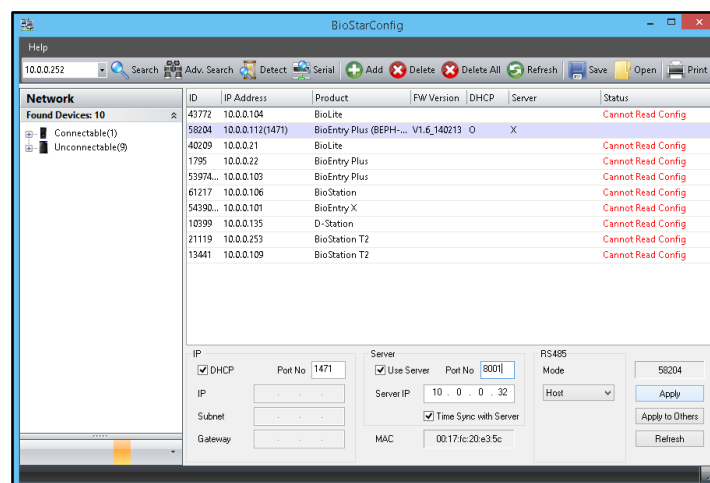
### 6.3 Advanced: Adding a Device using BioStar Config

BioStar Config is an IP Network utility included with BioConnect ID Enterprise that can help search for hard to detect devices. You can find the executable file on the Server at C:\Program Files(x86)\Entertech Systems\BioConnect\BioConnect Service\Utilities\BioStarConfig.exe. This file can be copied onto a laptop for convenience.

1. Open BioStar Config
2. Click the [Search] button



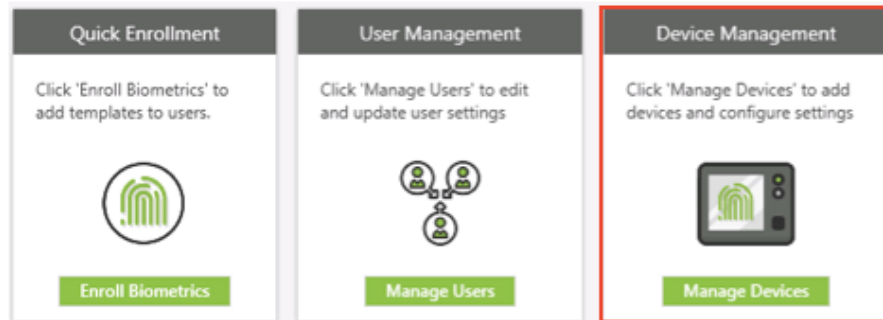
3. If your reader appears, click on the device and enter the desired network/server details at the bottom and click [Apply].



4. If you cannot find your device using the standard search, click [Advanced Search]. You may have to install a third party network search tool called

WinPcap. This is also included in the same directory as BioStar Config on the server.

## 6.4 Reader Setting Definitions (Device Management)



### 6.4.1 Details Tab

Details	General Information	Network Details	Wiegand Details
<b>Name:</b> <b>Location:</b> <b>Enrollment Reader:</b> <b>Profile:</b> <b>Online:</b> <b>Device ID:</b> <b>Operation Mode:</b>	<input type="text" value="Unknown - 00-1"/> <input type="text" value="Default"/> <input type="text" value="Default"/> <input type="text" value="Default"/> <input type="text" value="547732411"/> <input type="text" value="No Change"/>		
<input type="button" value="Update Firmware"/> <input type="button" value="Save"/> <input type="button" value="Delete"/>			

**Name:** The name you would like to give the reader. It is recommended to keep this consistent with the name you give the reader within the access control software.

**Location:** This is the location/region of the reader. This location is used throughout the software primarily to limit which enrollment readers are available for use by the people performing enrollments. For example, you may not want people in New York having to filter through enrollment devices across the country to find the one nearest to them. You can limit which locations a user has access to in the User Management section of the software.

**Enrollment Reader:** This option allows you to designate the reader as a possible enrollment reader. Readers with this enabled can still operate as a production reader, but will be available within the Device list during the enrollment process.

**Profile:** This feature is for custom applications only. If a reader preset has been incorporated into the software license for your organization, you can use this feature to push down the specific configuration to the reader.

**Online:** This box will become active when the device is online.

**Device ID:** The device's serial number.

**Operation Mode:** The authentication mode of the reader. Possible presets are Card + Finger/Finger Only, Card + Finger, or Card Only. Below are some descriptions:

*Card + Finger/Finger Only:*

This mode will allow either Card + Finger OR Fingerprint Only to gain access to the reader. You can also enable “Card Only” within cardholders User Profiles within the User Management section of the software to achieve a Card OR Finger authentication mode using this option.

*Card + Finger:*

This option requires Card + Finger for authentication.

*Card Only:*

This option will only allow cards to be used at the doors, no fingerprints.

Various operations modes which support PINs, such as 3-factor authentication (Card + Finger + PIN), are also included for supporting devices.

**NOTE:** If your preferred authentication mode is not listed, you will use the BioStar configuration software to configure these custom settings in the reader. Please see Chapter 8 of this guide on the [BioStar Configuration Software](#) for more details.

## 6.4.2 General Information Tab

Details	General Information	Network Details	Wiegand Details
<b>Reader Type:</b>	BioStation 2		
<b>Product Name:</b>	BioStation 2		
<b>Firmware Version:</b>	1.2.0 (Rev : 2016/02/04 08:38:40)		
<b>Kernel Version:</b>	1.0.1 (Rev : 2015/10/02 08:02:28)		
<b>Template Type:</b>	Suprema		

Restart
Update Firm
Save
Delete

**Reader Type:** This is the product version.

**Product Name:** The product code for the reader.

BioConnect ID Enterprise supports multiple biometric hardware options. Customer can choose from a wide range of multi-factor readers such as face, fingerprint, card and PIN.

Currently following devices can be enabled by BioConnect ID Enterprise:

- Suprema Gen 1:
  - BioEntry Plus
  - BioEntry W
  - BioLite Net
  - FaceStation
  - BioMinis
- Suprema Gen 2:
  - BioStation 2
  - BioEntry W2
- CabinetShield

**Firmware/Kernel Version:** The current firmware/kernel installed on the reader. Note that firmware updates can be installed through the software, but Kernel updates **must** be upgraded at the reader itself using the onboard USB port.

**Template Type:** The current fingerprint template (Suprema or ISO) used by the reader.

### 6.4.3 Network Details Tab

The IP Address, Subnet and Gateway of the reader. Having DHCP enabled will cause the reader to look to the network for an IP address assignment. With it disabled, you can assign it your own address.

**Server IP Address:** The IP address of the server which you would like to have the device connect into. This should be the server where the BioConnect ID Enterprise services are installed. The server **must** have a static IP address.

**Server Port:** The default port for the BioConnect ID Enterprise server to listen on is either 8001 (Generation 1 Device) or 51212 (Generation 2 Device). Be sure that this is not blocked by your firewall.

Details	General Information	Network Details	Wiegand Details
IP Address:	10.0.19.119		DHCP: <input checked="" type="checkbox"/>
Gateway:	10.0.19.1		Mac Address:
Subnet:	255.255.255.0		
Server IP Address:	10.0.19.48		
Server Port:	51212		

Restart
Update Firm
Save
Delete

### 6.4.4 Wiegand Details Tab

**Facility Code:** This is the facility code that will be sent to the panel (along with the matching card number) when a fingerprint is authenticated.

**Card Format:** The card format you want to use on the reader. Suprema readers are limited to 1 card format per reader. For your convenience, some of the most popular card formats are included within BioConnect ID Enterprise:

- Standard 26 bit Wiegand
- 35 bit Corporate 1000
- 37 bit H10304
- 48 bit Corporate 1000



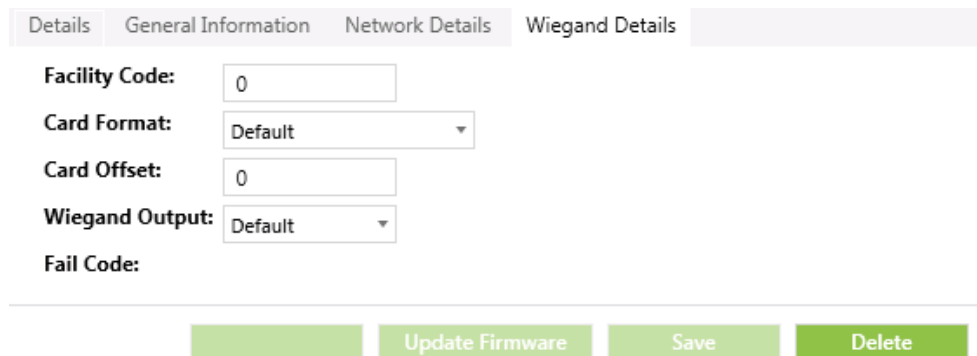
**NOTE:** You can set custom formats as well. Suprema readers are compatible with up to 64 bit cards, with a maximum of 32 ID bits. This can be customized by using the BioStar Configuration Software (Refer to Chapter 8 for more information.)

**Card Offset:** The card offset is used by some Access Control systems when they have duplicate card numbers across different card formats within their system. This feature adjusts for the card offset set within the access control software. If you are not using an offset, leave this value as 0.

**Wiegand Output:** This option allows you to send the User ID field instead of the card number to the panel after a successful card or finger authentication at the reader. It is recommended that unless in rare cases, you should leave this option set to “Card #”.

**Fail Code:** The fail code will send the largest possible number within your card format when a failure occurs at the reader. For example, with 26 bit Wiegand the largest number would be 65535. Failures include rejected fingerprint or card reads.

**Delete Button:** The [delete] button within the Device Configuration tabs allows you to remove a device that is no longer online or used within your system.



The screenshot displays the 'Wiegand Details' configuration tab in the BioStar Configuration Software. The interface includes a top navigation bar with tabs for 'Details', 'General Information', 'Network Details', and 'Wiegand Details'. The 'Wiegand Details' tab is currently selected. Below the navigation bar, the configuration fields are as follows:

- Facility Code:** A text input field containing the value '0'.
- Card Format:** A dropdown menu with 'Default' selected.
- Card Offset:** A text input field containing the value '0'.
- Wiegand Output:** A dropdown menu with 'Default' selected.
- Fail Code:** A text input field that is currently empty.

At the bottom of the configuration area, there are four green buttons: 'Update Firmware', 'Save', and 'Delete'. A fourth button, which is partially obscured, is likely 'Cancel'.


## 7. Synchronization

BioConnect ID Enterprise is designed to make synchronization simple requiring no interaction from the user. There are three types of synchronizations that occur:


### **Automatic Sync:**

The automatic synchronize occurs automatically every 5 minutes in the background. It is also triggered whenever you open the User Management section of the client, or do a search. This means that you do not have to wait 5 minutes for the data to synchronize if you need it immediately.

### **Manual User Sync:**

The manual user synchronize feature can be activated at any time within the BioConnect ID Enterprise client by clicking [Menu]  > [Synchronize Users]. During normal use, this feature will not be required. Choose a date that you would like to synchronize from (The date will pull all changes that have occurred since that date). This is a helpful feature if a cardholder does not appear to have the most up to date information.

### **Manual Device Sync:**

The manual device synchronize can be activated at any time within the BioConnect ID Enterprise client by clicking [Menu]  > [Synchronize Devices]. During normal use, this feature will not be required. Purpose of this synchronization is to push the user info and templates to the internal memory of the reader.

**NOTE:** The software also does a full re-synchronize each night. This helps by providing redundancy to ensure that all data was properly updated within the BioConnect ID Enterprise.

## 8. Advanced: BioStar Configuration Software

**IMPORTANT NOTE:** This section is for Suprema Generation 1.0 devices. If you're using the BioStation 2 (Suprema Generation 2.0), please consult our Support Portal (<http://www.bioconnect.com/support/>) for resources on using BioStar 2.

The BioStar software by Suprema is required for some reader configuration that is not available within the BioConnect ID Enterprise. Some examples include:

- You are using a card wiegand format that is not included as a preset
- The Authentication Mode that you want to use is not included as a preset (For example: Card + Finger OR PIN)

BioStar is included within every BioConnect ID Enterprise Installation Package. This software can be installed on the same server that is running BioConnect ID Enterprise, and uses a different server port for communication.

For your reference:

BioConnect ID Enterprise Server Port: 8001  
BioStar Server Port: 1480

When a device is configured, you point it to a Server IP address and a port. The port that you choose will determine which software it connects into. To switch a reader from BioConnect ID Enterprise to BioStar, simply change the Server Port within its network settings in the Device Management section of the software.

The BioStar-specific documentation is also available within the BioConnect ID Enterprise Install Package. Please note that although the BioStar software is a fully functional access control software, we are using it primarily for its reader configuration setting options.

Please see the BioStar manual and Reader-Specific documentation for more details.

## 9. Additional Assistance

If you encounter issues during the BioConnect ID Enterprise installation that were not covered here, please don't hesitate to reach out to us or visit our support website.

Telephone support is available **Monday - Friday from 8:30 AM to 8:30 PM Eastern** to assist with installing, configuring and troubleshooting the BioConnect ID Enterprise. The technical support team is well versed to assist integrators both during the planning or post sales stages.

### Support Website:

<http://www.bioconnect.com/support/>

### Telephone:



Toll-Free 1-855-ENTERID (368-3743)

### Email:

[support@bioconnect.com](mailto:support@bioconnect.com)

## Appendix A: Dashboard Quick Review

