

Overview:

- Minimum supported version of Biostar 2 is V2.8.15.12. With every new release of Biostar 2, the integration will be tested internally.
- There is no annual charge for the integration, the only thing that is required is an upgrade to 2023. There is no connection fee per device, but the license engine allows us to control how many devices can be connected. This is so customers can't add devices to the system as they like without us knowing. We can also control the type of devices, whether it be Access Control or Attendance. An example could be you asking for a license that allows 3 Access Control devices and 5 Attendance devices. If any more devices are added, then a new license will be required.
- Suprema licensing structure still applies to the integration. Noticeable points are below, for full details, please see <https://www.supremainc.com/en/platform/hybrid-security-platform-biostar-2.asp>
 - Free version has a maximum of 5 doors (attendance only units are still classed as doors)
 - Basic version has a maximum of 20 doors (attendance only units are still classed as doors)
 - Standard version has a maximum of 50 doors (attendance only units are still classed as doors)
 - Advanced version has a maximum of 100 doors (attendance only units are still classed as doors)
 - Anti-pass back/repeat swipe duration is reader specific for free and basic licenses. From the standard license upwards, it is global. An example could be a server room with two doors. On the free and basic licenses, you could gain access to door "A", pass your card to an employee, and they could gain access through door "b". If this was using the global anti-pass back, you would be denied access at door "b" until you had "exited" through one of the doors first.
 - Fire alarm triggers are from Standard license upwards. This is because we make use of the zones section in Biostar.

Installation:

- Requirements
 - Biostar 2 software <https://www.supremainc.com/en/support/biostar-2-package.asp>
 - Please check Suprema's minimum spec documentation for the requirements for Biostar.
 - timeware® 2023 (23.1.2 or greater)
 - .NET Runtime 7.0.X <https://dotnet.microsoft.com/en-us/download/dotnet/7.0>
- Run the installer as admin. Make a note of the password created for the "admin" account as we will need this later. The 2nd page when you are setting a password for "root", make a note of the password but we don't need this specifically for the integration. "Express installation" option is no longer recommended, we want to choose "custom installation" so we can change the database structure to be SQL rather than MariaDB.

NMD³

Hosting

- On the next screen, change "DB Type" to MS-SQL and point it to your SQL instance. This can be a separate instance purely for Biostar DB's, or you can have them hosted on the same instance as the timeware® databases. The server port can be found in SQL Configuration manager app. We have decided on a standard of "biostar2_ac", "biostar2_ta" and "biostar2_ve" for the database names. The Username and Password is the same details which you use to connect to your instance. Depending on SQL version you may need to manually create the databases yourself from within SSMS. To do this just right click on your instance->new database. Make sure "Generate the database tables" is ticked.

Setup - BioStar 2(x64)

Custom installation
If you choose database type, you must enter the Root privilege account information.

DB Type : MS-SQL mssql windows auth.

Server IP : 192.168.42.8 VE DB name : biostar2_ve

Server port : 50185 VE Username : timeware

AC DB name : biostar2_ac VE Password :

AC Username : timeware

AC Password :

TA DB name : biostar2_ta

TA Username : timeware

TA Password : Generate the database tables

< Back Next > Cancel

- When you get to the "Port Settings" page (see screen below), make sure nothing is using the assigned port for the "HTTPS Port for Web Server". If something is already using the default port, choose another one. Click on "next" and then "back" to return to the port screen to see if the newly chose port is available.

Setup - BioStar 2(x64)

Port Setting
Port Setting Enter a valid port number.

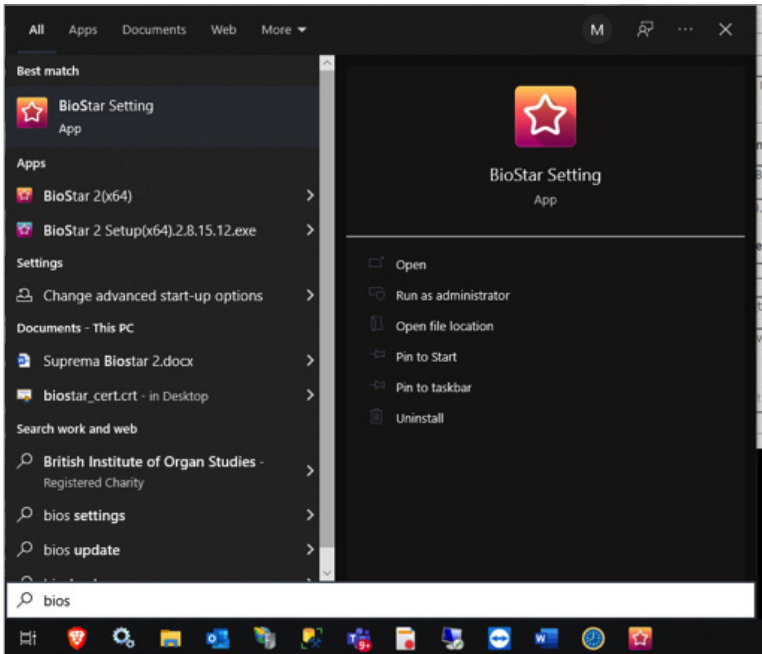
HTTPS Port for Web Server
Enter the desired port number between 10 and 65534.
The default port number is 443.
8443 Availability: OK

Device Port for Communication
Enter the desired port number between 10 and 65534.
The default port number is 51212.
51212 Availability: OK

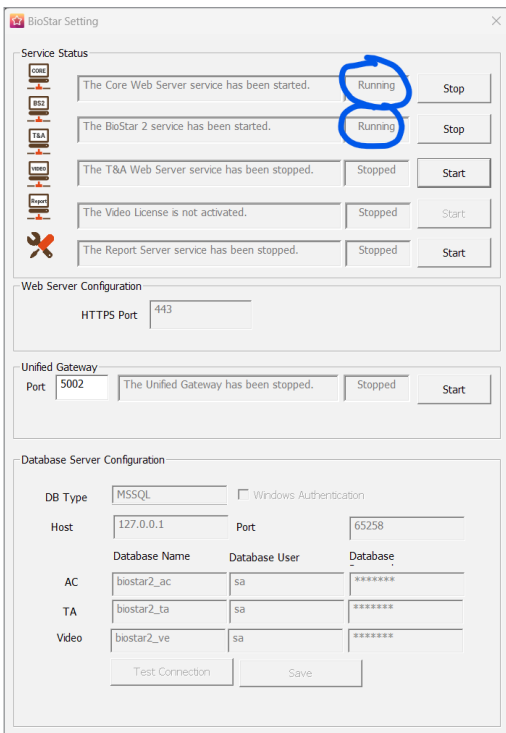
< Back Next > Cancel

NMD³ Hosting

- Run through the rest of the installer with the default settings, if you require a USB device connected to the server then install the USB driver when prompted
- Once installation has finished, search for "Biostar" in the windows start menu and open "Biostar settings".

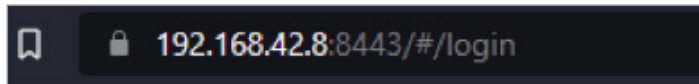


- Confirm that the top 3 services are running



If the Unified Gateway has been started, this will need to be stopped as this uses the same port as the HTTPS port and will swap them around, you may need to switch them back if this has been started.

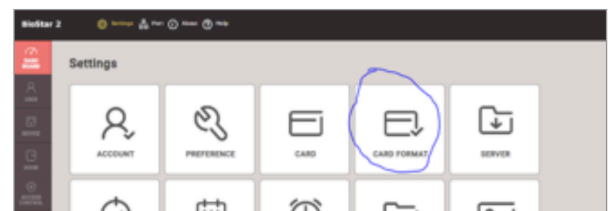
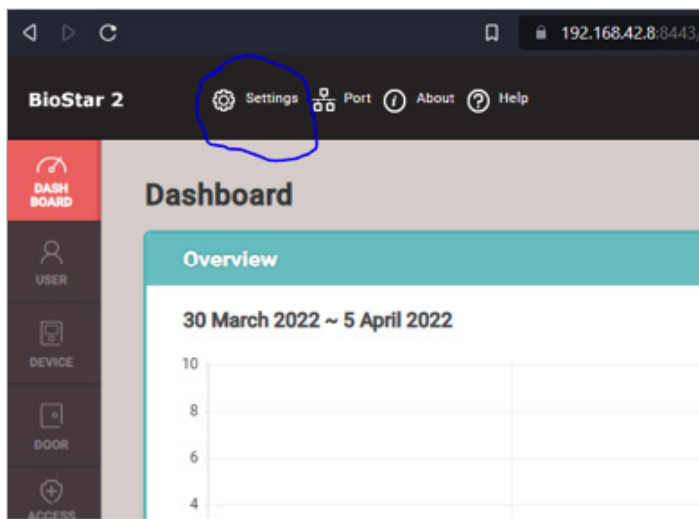
- We need to configure the HTTPS certificate, go to https://kb.supremainc.com/knowledge/doku.php?id=en:how_to_configure_https_settings_for_the_web_client and follow the instructions on there. We recommend using the IP of the server rather than "localhost"
- Once the above is completed, browse to [https://\[IP\]:\[PORT\]](https://[IP]:[PORT]) and you should be presented with the Biostar logon page. You should see the padlock icon next to the URL indicating the site is secure. You may need to close your browser down if it was already open.



- Login with the admin account and the password created previously, if successful you will be presented with the dashboard page.

Configuration:

- First up we need to configure our "standard" badge format. From the Biostar dashboard page, go to "Settings" at the top and then "Card Format".



- Click then pen icon on the next available slot, should be Weigand ID 6.
- Input the following settings and then click apply.

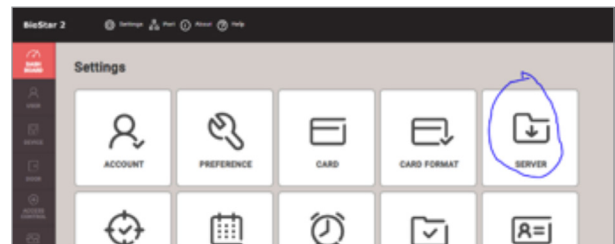
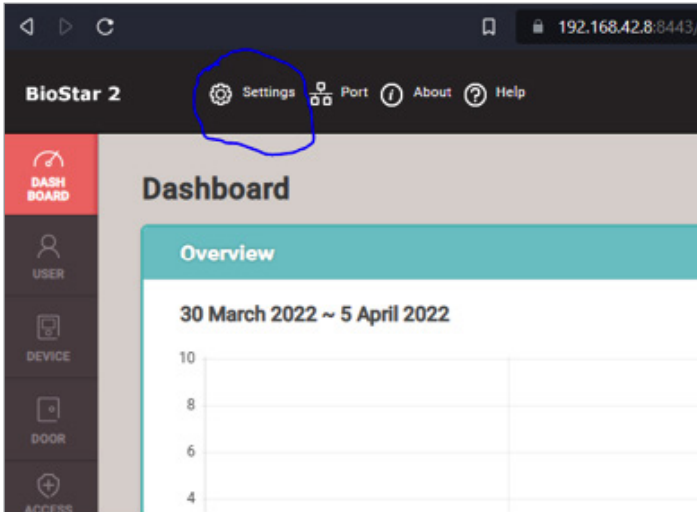
Information

- Name:
- Description:
- Total Bits:
- Facility Code Field:

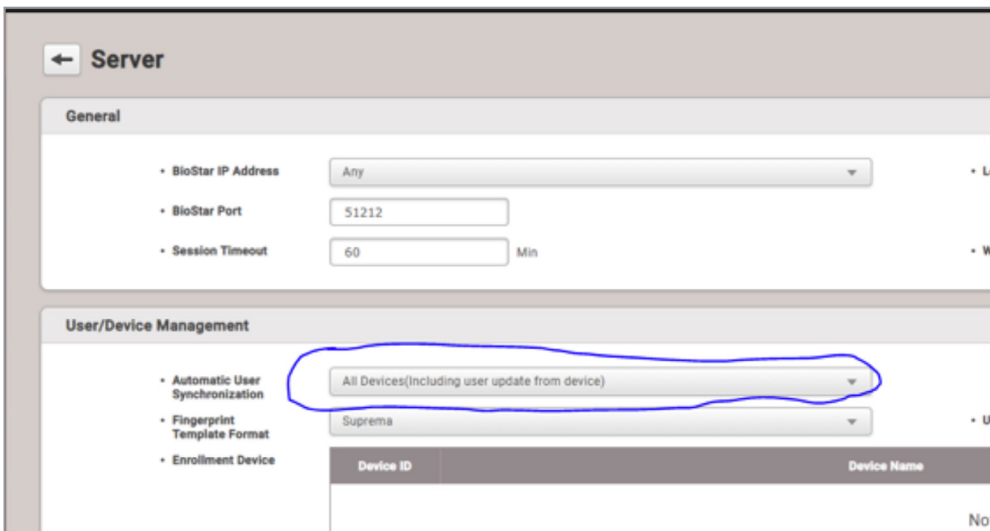
ID Field	Start Bit	End Bit	Size	
				+ Add
ID 0	1	32	32	🗑

Parity Bits	Position	Type	Start Bit	End Bit	Size	
						+ Add

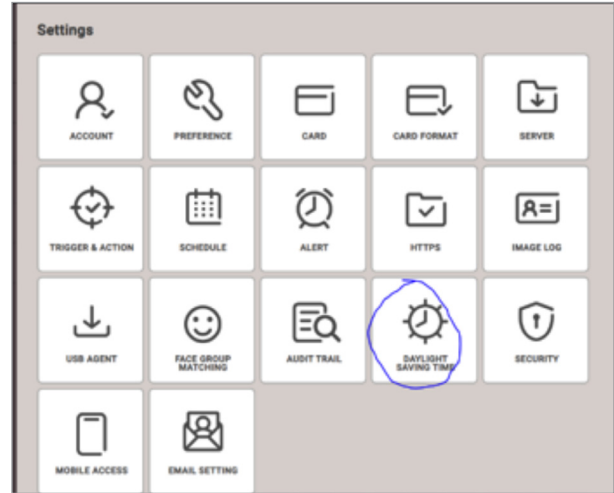
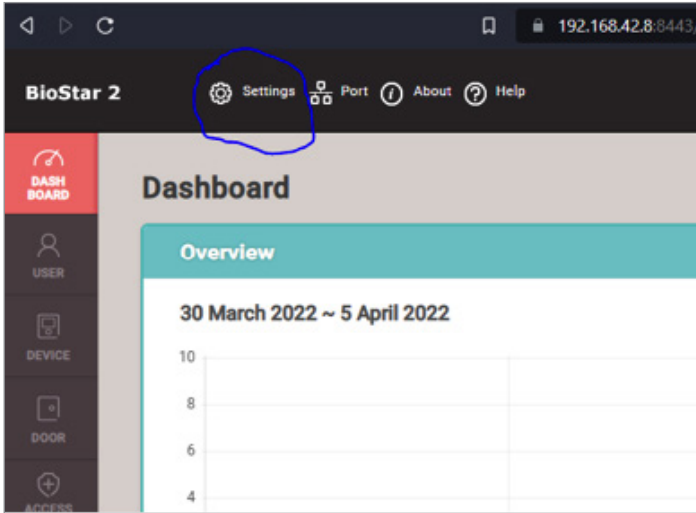
- Next up is enabling templates to be brought up into the software from the devices. If you go to "Settings" and then "Server".



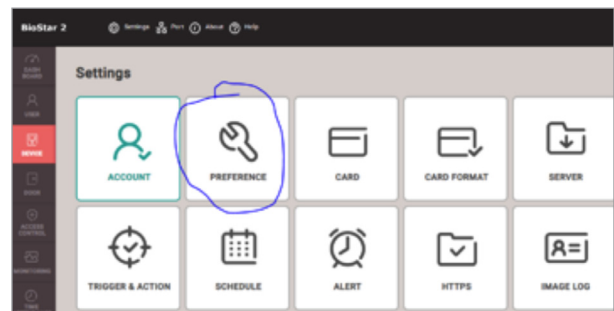
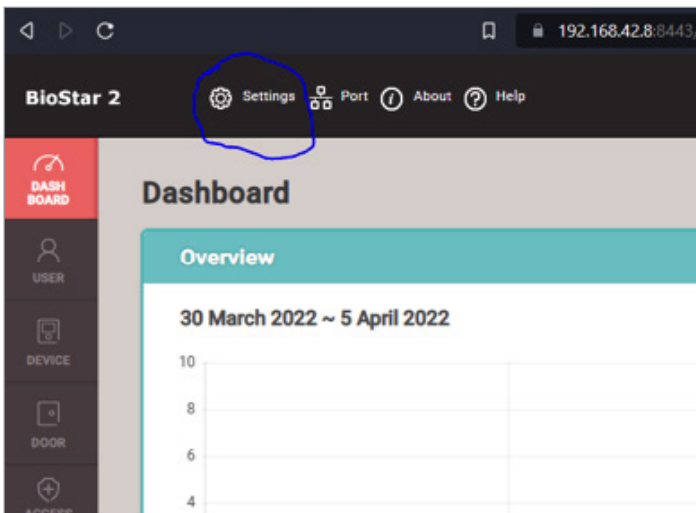
- Under the "User/Device Management" header, change "Automatic User Synchronization" from "All Devices" to "All Devices (Including user update from device)". This allows any changes to users that are made at the device to come up into Biostar.



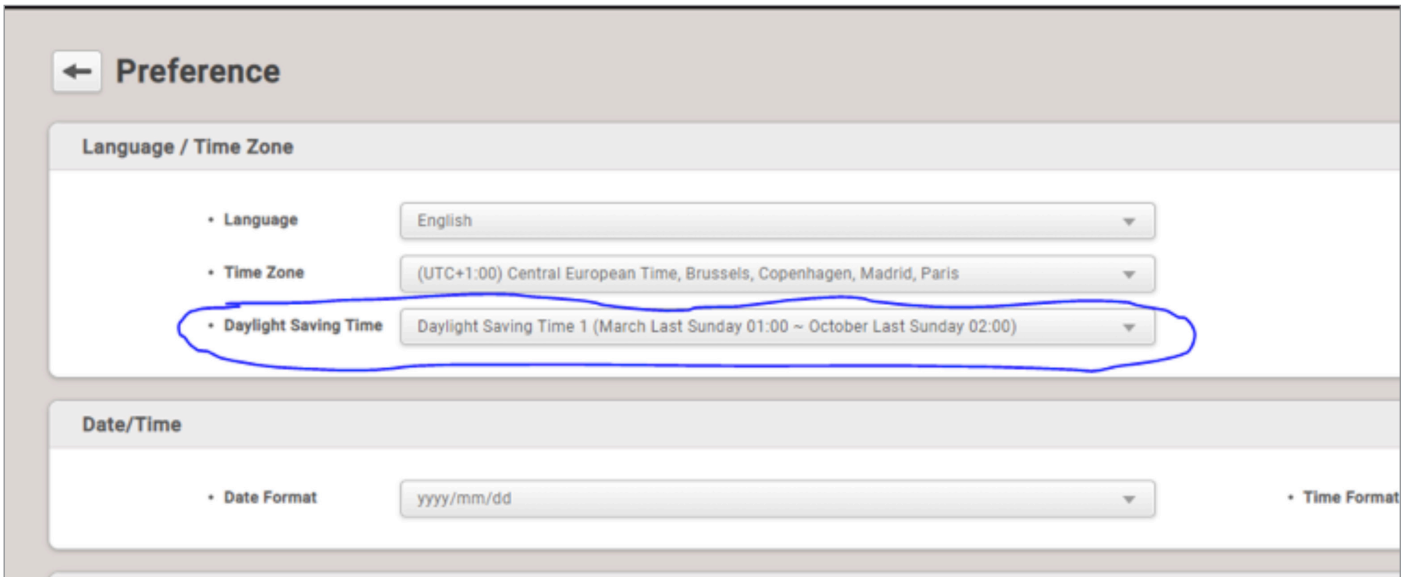
- We must also setup Daylight Saving Time, again go to "Settings" and then "Daylight Saving Time".



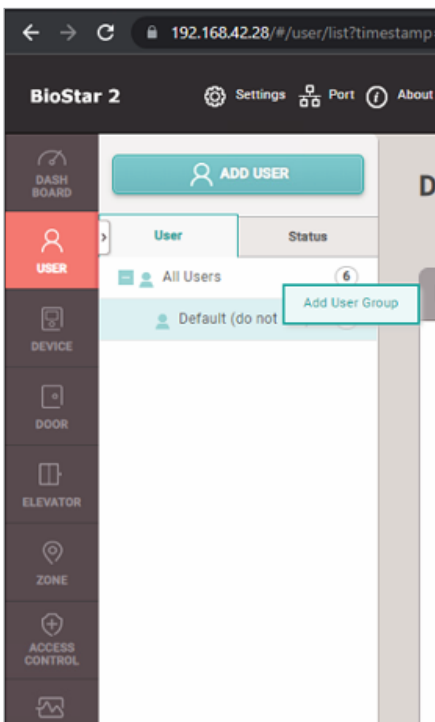
- Click the add button on the right-hand side and enter the following settings.
- Go back to "Settings" and then "Preferences"



- Apply the Daylight Saving time you just created in the following dropdown and then click apply.



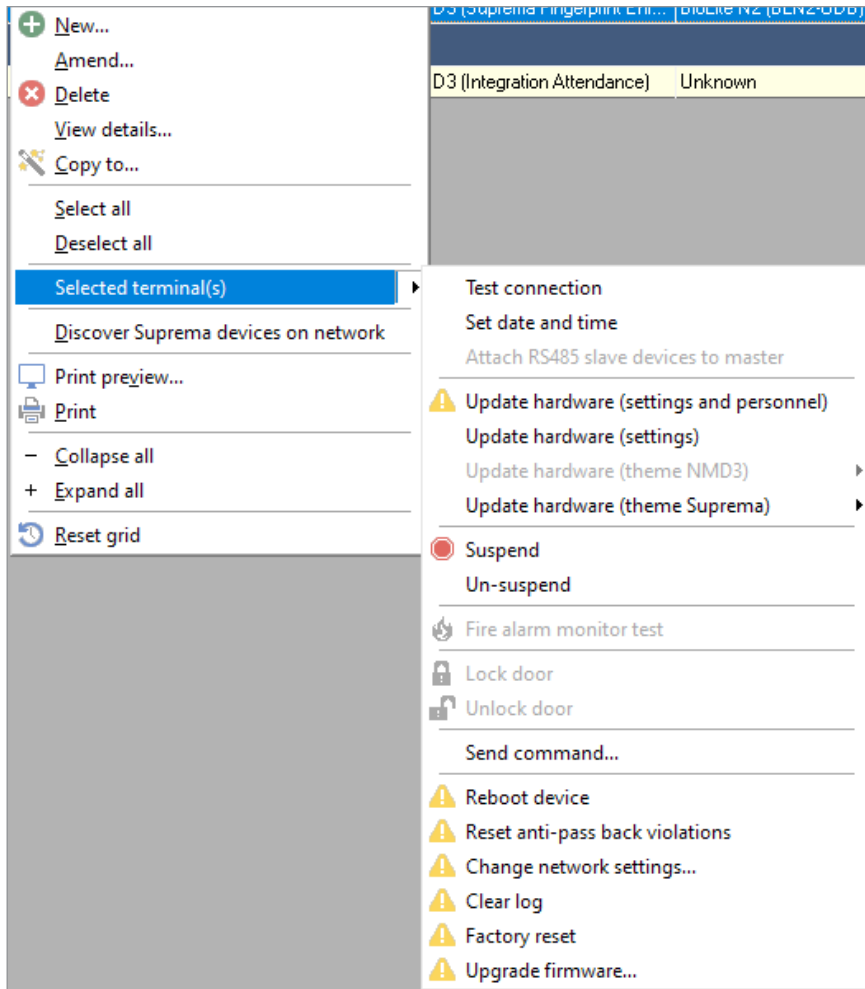
- We want to create a "default" user group which will contain no users. This is so we can assign users on an individual level to access groups from within timeware®. Go to Users, then right click on "All Users"-> "Add user group". Name this new user group "Default (do not use)".



(Only applicable if devices have already been used in timeware previously)

When devices have already been in use within timeware® for some time, it carries with it issues involving the log files and biostar2 not being able to catch up, resulting in nothing being posted to the event log (and in turn bring bookings in to timeware®!)

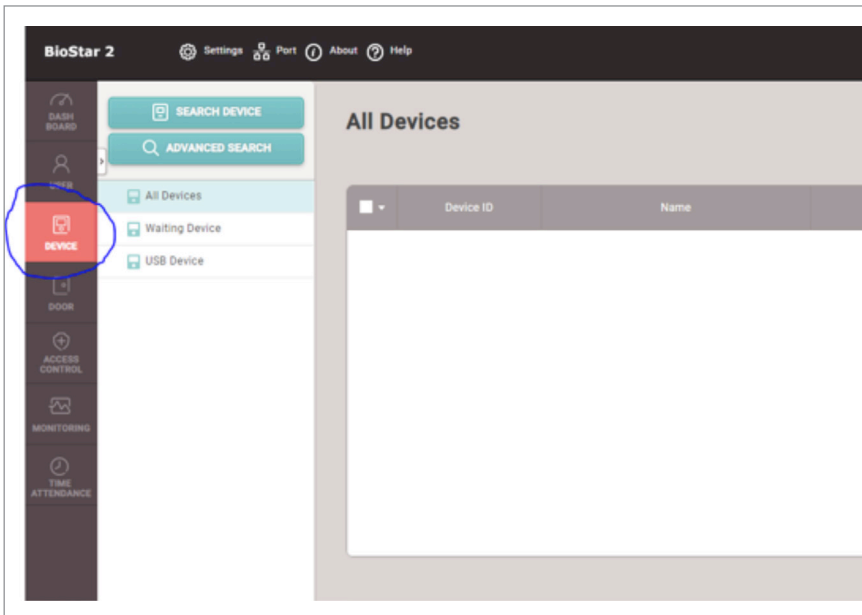
Within timeware® before you add any devices in to biostar2 you need to clear the logs from the devices. This is done via the terminal configuration screen by right clicking on the device, selected terminal(s) then Clear Log



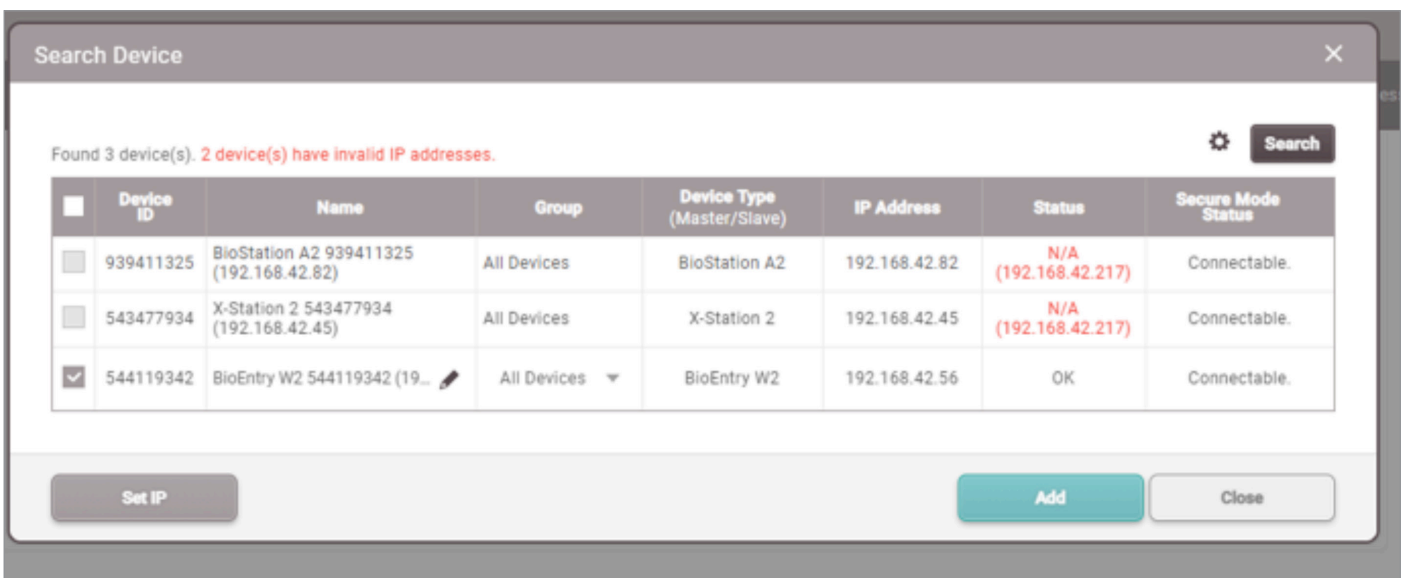
If you have issues with bookings not coming in to timeware® after you've completed the rest of this document, you may need to reset the latest log entry within tbiostar_event_log_management. If you right click on the tbiostar_event_log_management table with SSMS, and then edit. In here if you change the event_log_id for the current month to 0 based on the month_start and month_end fields, this will synchronise the log files between the devices and the timeware® database.

NMD³ Hosting

- Next is to add a device. Head to the device section.



- Click "Search for Devices". If your device is on the same LAN it should discover it. If not, you may need to use the "Advanced Search" option, where you enter the devices IP address manually. Select your device and then click "add".



- Click on the device you just added, make sure the correct time zone is selected and select the Daylight Saving Time preset we created earlier in the guide.
- Under "System" set the Date Format to "DD/MM/YYYY"

BioEntry W2 544119342 (192.168.42.56)

Information

- Name: BioEntry W2 544119342 (192.168.42.56)
- Device ID: 544119342
- Firmware Version: 1.6.3 (2021/04/19 12:47:39) [Firmware Upgrade](#)
- Kernel Version: 1.1.2 (2020/07/20 18:23:58)
- Restore to default: [All](#) [Without Network](#)
- Time Zone: (UTC) W. Europe Standard Time, London, Lisbon, Casablanca
- Daylight Saving Time: Daylight Saving Time 1 (March Last Sunday 01:00 - October Last Sunday 02:00)

System

- Display Date: 2021/04/25 09:57:14 [Get Time](#) [Set Time](#)

- Under the "Authentication" header, we want to change the 1:N Security level. If it is a face recognition device, we recommend "Secure", for a fingerprint device, we recommend "Most Secure".

Fingerprint

- 1:N Security Level: Most Secure

- If you are attaching any devices as slaves, please check on Suprema's website how to do this.
- We also need to enable the "26 bit – NMD3" Wiegand format we created earlier. Click into the device and in the "Authentication" section, enable the Wiegand format settings as below. If you are using a different card technology you can skip this step

Card Type

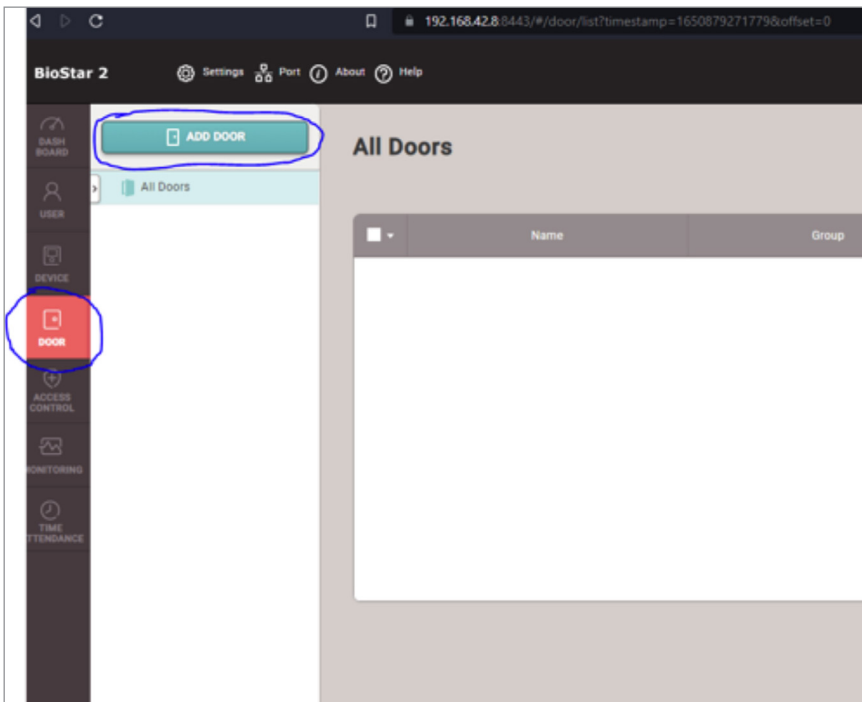
- CSN Card: Enabled
- EM4100: Mifare/Picco:
- Byte Order: MSB
- Format Type: Wiegand
- Wiegand Format: 26 bit - NMD3

- If it is being used as an attendance unit, we can simulate the "too soon after last booking" by adding a "dummy" slave device and enabling anti-passback. We can then change the resource file on the device to display "too soon" instead of the "APB Violation". You can skip these next steps if this doesn't apply.
 - Click into the device and scroll to the advanced section at the bottom. In the Wiegand section, change "Input/Output" to "Input", then save this away.

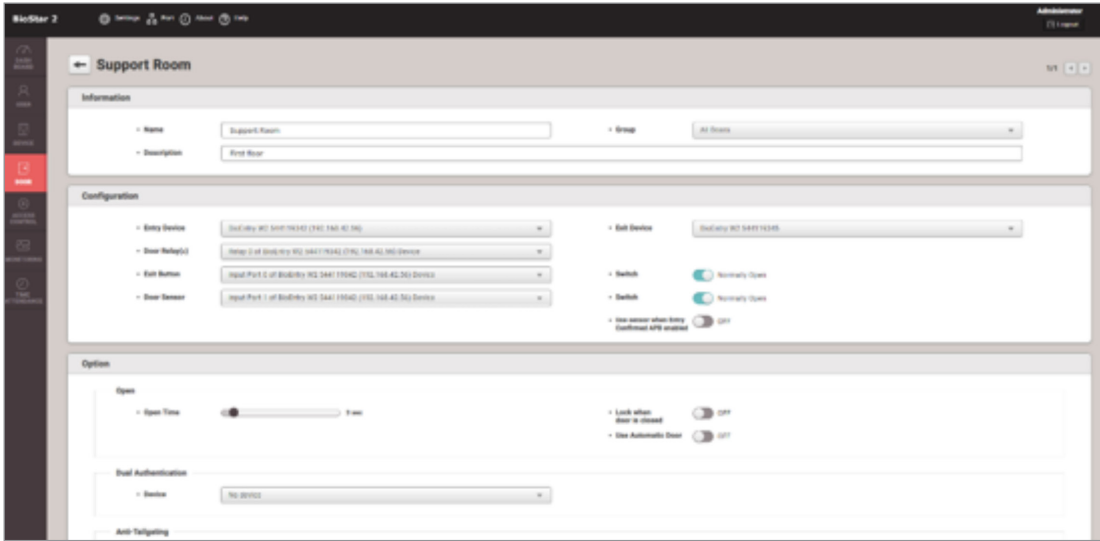
Wiegand

- Input/Output: Input

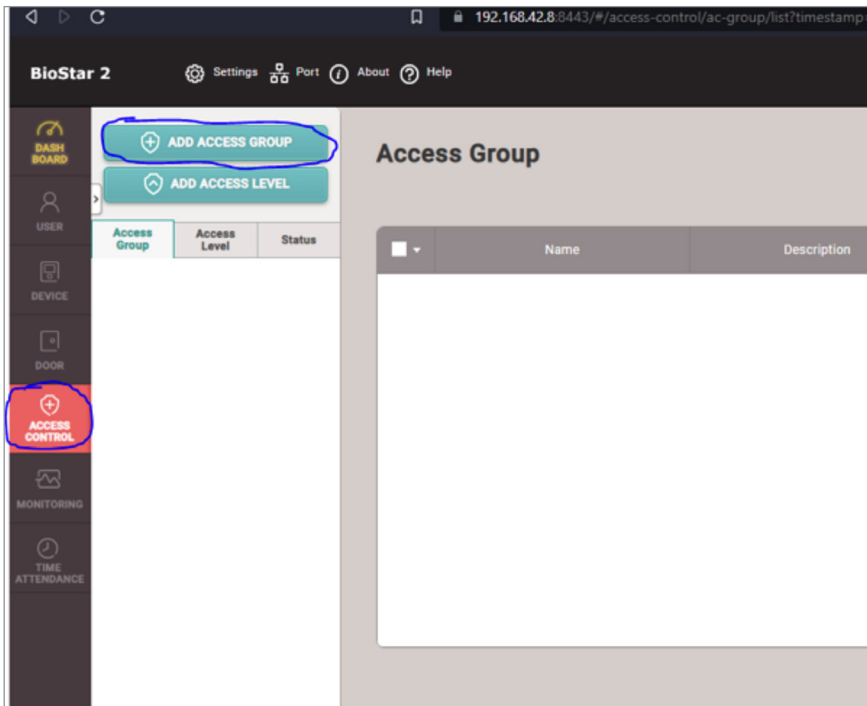
- Right click on the device in the left hand side pain and click on "Add Wiegand Device".
- Give this a name, we use the main device's name + Repeat Swipe as a standard.
- You can then carry on with the next steps in the guide, assigning this "Repeat Swipe" device we just created as the "Exit Device" for the door.
- Next, we need to add a door. Even if it is attendance only, we still need to set it up as a door. Navigate to door and then click "Add Door".



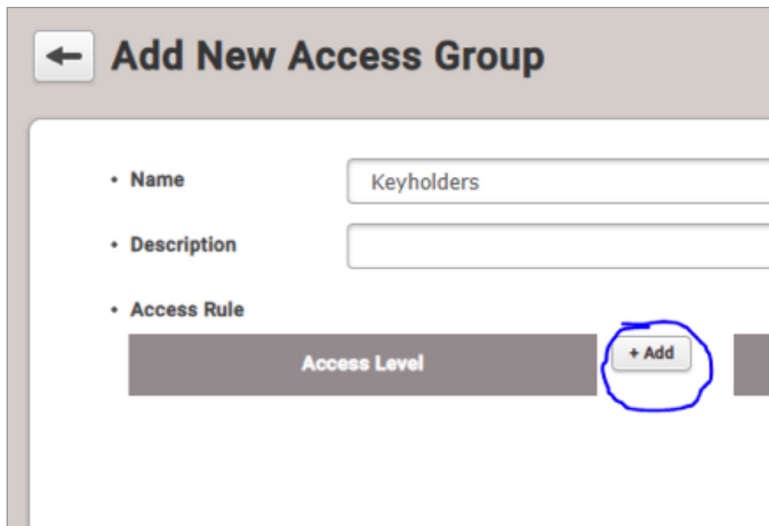
- Give the door a name and a description, the Group can be left as "All Doors". Under the configuration section, for "Entry Device" select the device you added previously. For "Door Relay" choose the relay of your entry device. For "Exit Button" and "Door Sensor" select the inputs each one is connected to. If you have a slave reader connected (or created the dummy repeat swipe device), assign this as the "Exit Device". If you have assigned an exit device, you will be able to configure the anti-pass back settings at the bottom of the page. If you are on the paid version of Biostar 2 that allows Global anti-pass back, a guide for this is available on Suprema's website. The rest of the settings can be left as default unless you want to configure additional features, these can be found on Suprema's website.



- We now need to set up access groups and access levels. Click on "Access Control" on the left-hand side and then click "Add Access Group"



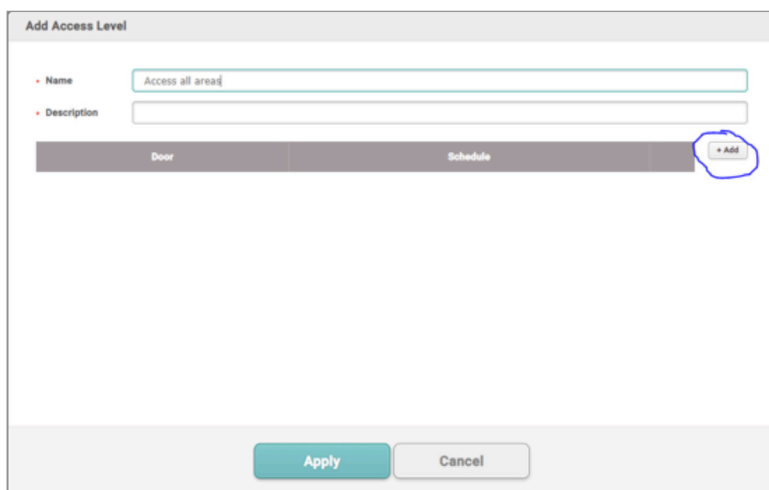
- Give the Access Group a name and description, and then click the "Add" next to "Access Level"



The screenshot shows a web form titled "Add New Access Group". It has a back arrow button in the top left. The form contains three main sections:

- Name:** A text input field containing the text "Keyholders".
- Description:** An empty text input field.
- Access Rule:** A section with a dark grey header bar containing the text "Access Level". To the right of this bar is a button labeled "+ Add", which is circled in blue.

- Once the menu has opened, select "Add Access Level". Give a name and description and then click the "Add" button on the right.



The screenshot shows a dialog box titled "Add Access Level". It contains:

- Name:** A text input field containing "Access all areas".
- Description:** An empty text input field.
- Configuration Row:** A dark grey bar with three sections: "Door", "Schedule", and a "+ Add" button circled in blue.
- Footer:** Two buttons, "Apply" (highlighted in teal) and "Cancel".

- Click on the dropdown for "Doors" and select any doors that you want to allow this Access Level to access from the list. On the schedule dropdown choose the correct schedule. "Always" allows access 24/7. If you want a custom schedule, click on the "Add schedule" and create your custom schedule. More information on this can be found on Suprema's website. Click apply.

Add Access Level

• Name:

• Description:

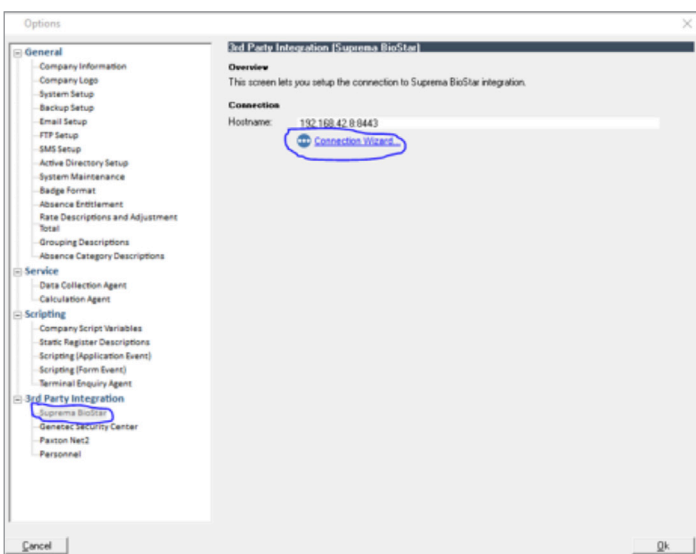
Door	Schedule	
Support Room	Always	

+ Add

User Group + Add

All Users	
-----------	--

- For the user group option, select the "Default (do not use) group we created earlier. This is so only the individuals synced from timeware® will get added to the Access Groups.
- That is pretty much it for the configuration in Biostar. We now need to point timeware® to the Biostar 2 web address. Open timeware® and go to Advanced->Options and then Suprema Biostar under the "3rd Party Integration" header. Click on the blue "Connection Wizard".



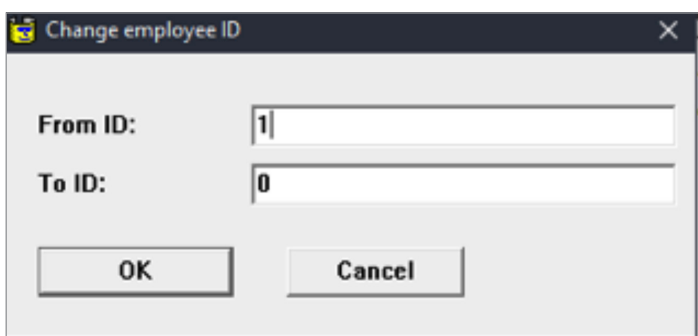
NMD³

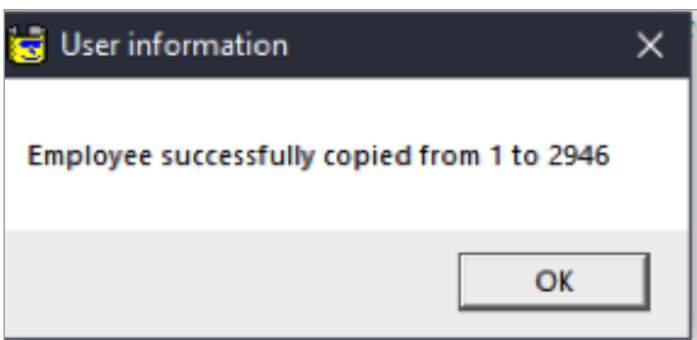
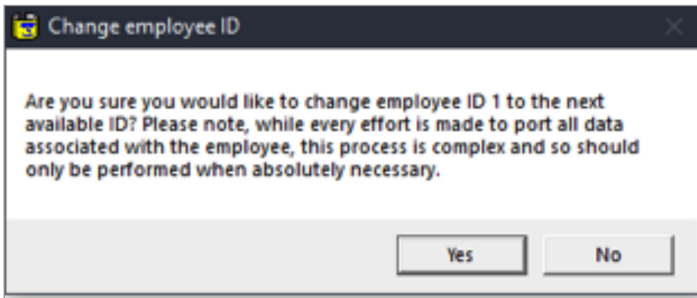
Hosting

- Run through the wizard and use the hostname and port that you registered the certificate to In the initial setup of Biostar. Enter the username and password you created when installing biostar. Click next and then finish the wizard. Click okay on the Advanced->Options screen to save away the settings.
- The next thing to do is start the service. Open command prompt and cd to "C:\Program Files (x86)\timeware Software\timeware\BioStarWindowsServiceBin". Run the following command "Toronto.BioStar.WindowsService.exe -d 0". This will start the service with a 0 second delay.
- If you have an employee set up in timeware® with employee_id=1, you will be presented with the following error.

```
Administrator: C:\WINDOWS\system32\cmd.exe
C:\Program Files (x86)\timeware Software\timeware\BioStarAgentBin>Toronto.BioStar.WindowsService.exe -d 0
info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
Service started.
info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
Awaiting service startup delay of 0 seconds.
info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
Verifying SQL connection.
info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
SQL connection is valid.
info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
Inspecting licence.
info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
Licence is valid.
info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
Verifying BioStar API connection.
info: Microsoft.Hosting.Lifetime[0]
Application started. Press Ctrl+C to shut down.
info: Microsoft.Hosting.Lifetime[0]
Hosting environment: Production
info: Microsoft.Hosting.Lifetime[0]
Content root path: C:\Program Files (x86)\timeware Software\timeware\BioStarAgentBin
info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
BioStar API connection is valid.
info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
Verifying integration suitability.
err: Toronto.BioStar.WindowsService.BackgroundWorker[0]
You cannot have an 'Employee Id' equal to 1 within your 'timeware® Professional' system. BioStar has reserved this Id for the 'Administrator'.
C:\Program Files (x86)\timeware Software\timeware\BioStarAgentBin>
```

- Go back into timeware® and go to Script Editor->Slider and run the "[Slider] Change employee ID". When prompted say "Change from 1 to 0", 0 being the next available ID. Confirm the prompts and let the script run. You should get a confirmation message.





- Rerun the command in the command prompt again and hopefully it should now run through with no errors. You should notice that some info lines display in regards to creating event logs etc. This shows that it is working as intended.

```
Administrator: C:\WINDOWS\system32\cmd.exe - Toronto.BioStar.WindowsService.exe -d 0
Inspecting licence.
Info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
Licence is valid.
Info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
Verifying BioStar API connection.
Info: Microsoft.Hosting.Lifetime[0]
Application started. Press Ctrl+C to shut down.
Info: Microsoft.Hosting.Lifetime[0]
Hosting environment: Production
Info: Microsoft.Hosting.Lifetime[0]
Content root path: C:\Program Files (x86)\timeware Software\timeware\BiostarAgentBin
Info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
BioStar API connection is valid.
Info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
Verifying integration suitability.
Info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
Inspecting BioStar for configuration changes.
Info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
Updated device changes.
Info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
Updated access group changes.
Info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
Retrieved event types.
Info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
Running poll and update at a frequency of 20 seconds.
Info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
Added new event log management month for 01 April 2022.
Info: Toronto.BioStar.WindowsService.BackgroundWorker[0]
Added new event log management month for 01 March 2022.
```

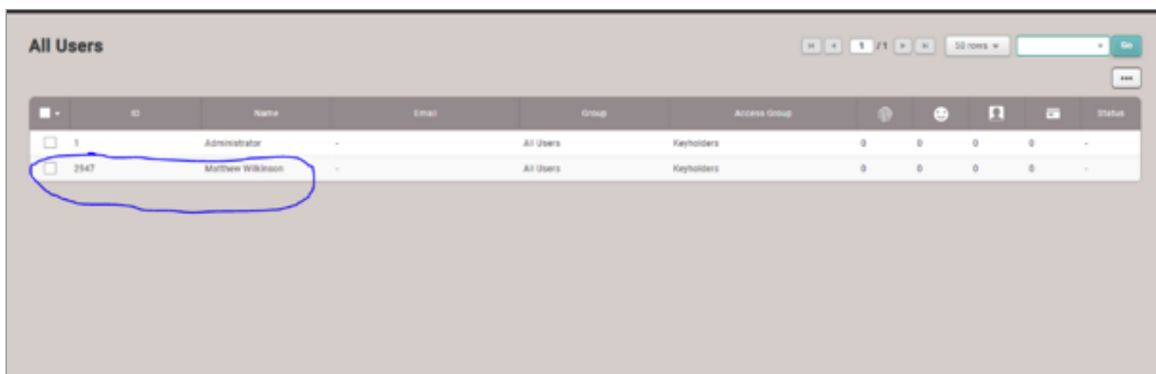

- If you now edit one of the personnel records in timeware® (assign access group etc), and save it away, the NMD3 Biostar service will then send this across to Biostar.
- If you are wanting to send people across on mass, I would set everyone on the relevant access groups via a SQL query, for example:

```
'use timeware_main_6;
update tempoyee set employee_biostar_access_group_id=1'
```

(You can add your own where clause on the end)

- Once they have been assigned, you can then add them to the tbiostar table, so the service sends them across, for example:

```
'use timeware_main_6;
insert into tbiostar(biostar_entity_ref_id,biostar_key,biostar_action_ref_id,guid)
select 1, employee.employee_id,2, employee.employee_guid
from tempoyee
where employee_biostar_access_group_id = 1'
```



ID	Name	Email	Group	Access Group	Status
1	Administrator	-	All Users	Keyholders	0 0 0 0 -
2947	Matthew Wilkinson	-	All Users	Keyholders	0 0 0 0 -



Personnel

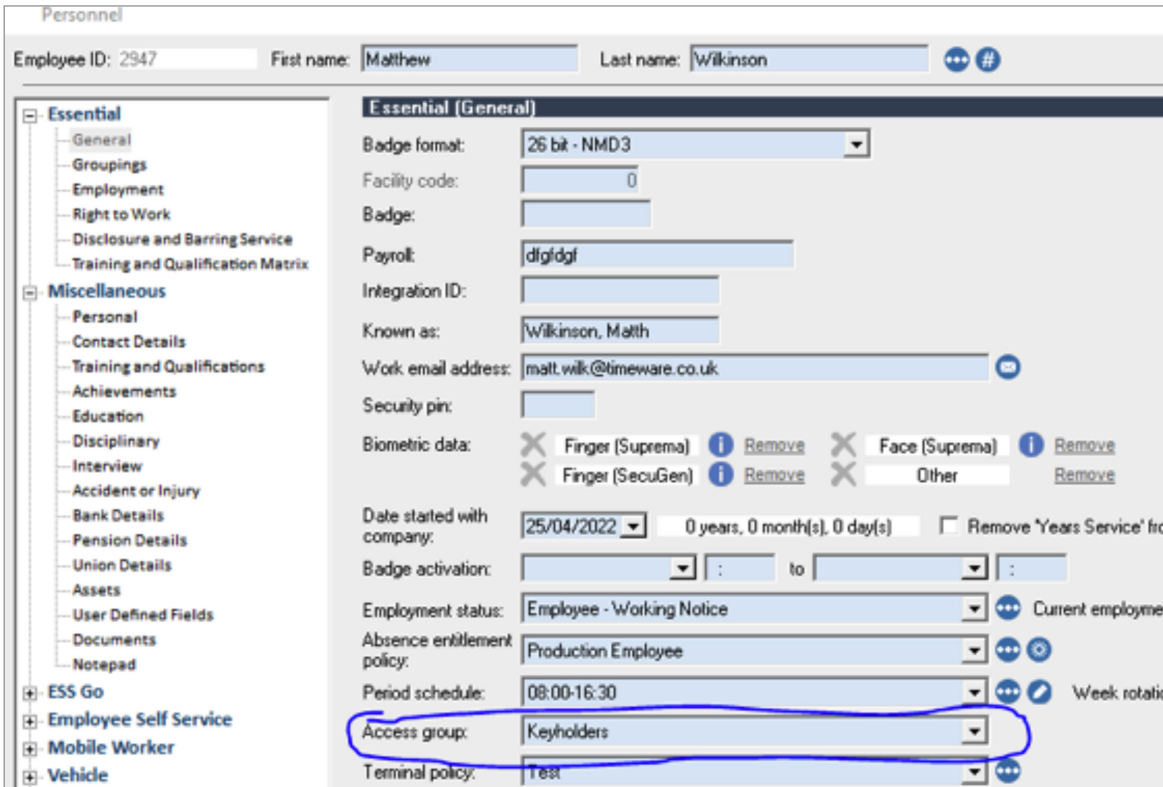
Employee ID: 2947 First name: Matthew Last name: Wilkinson ... #

Essential (General)

- If you go to terminal configuration, you will notice that any device that was set up in Biostar has now been brought in as an "Integration device". If you aren't wanting to bring data in from certain ones, leave them as suspended. By default, they are set as "NMD3 Integration Fire Alarm". If you are wanting to use the bookings towards access control data, then change the type to "NMD3 Integration Access Control". If it is an attendance unit, change it to "NMD3 Integration Attendance". Unsuspend all the integration devices you require and assign them to a relevant terminal group.

Attendance (3 rows)	Attendance	1003	101	Shop Floor (N2)	NMD3 (Suprema Attendance)	BiLife N2 (BLN2-008)	54542900	Standline	Push	152.188.42.77	No	Yes	1.2	Wed 15/09/21 09:00 (5:04 10 ago)
<input type="checkbox"/> Not tested in this session	Attendance	544119342	544119342	BiEntry v2 544119342 (152.1...	NMD3 (Integration Attendance)	Unknown	Unknown	Standline	Push	Unknown	No	No		Mon 25/04/22 15:10 (5:00 ago)
<input type="checkbox"/> Not tested in this session	Attendance	544119345	544119345	BiEntry v2 544119345	NMD3 (Integration Attendance)	Unknown	Unknown	Standline	Push	Unknown	No	No		Mon 25/04/22 15:10 (5:00 ago)

- If you go into "Personnel", you will notice we have brought in the access group(s) we created earlier on. Any new personnel record you create in timeware® you can now allocate an "Access Group" to.



Personnel

Employee ID: 2947 First name: Matthew Last name: Wilkinson

Essential (General)

Badge format: 26 bit - NMD3

Facility code: 0

Badge: []

Payroll: dfgldgf

Integration ID: []

Known as: Wilkinson, Matth

Work email address: malt.wilk@timeware.co.uk

Security pin: []

Biometric data:

- Finger (Suprema)
- Face (Suprema)
- Finger (SecuGen)
- Other

Date started with company: 25/04/2022 0 years, 0 month(s), 0 day(s) Remove 'Years Service' from badge

Badge activation: [] to []

Employment status: Employee - Working Notice

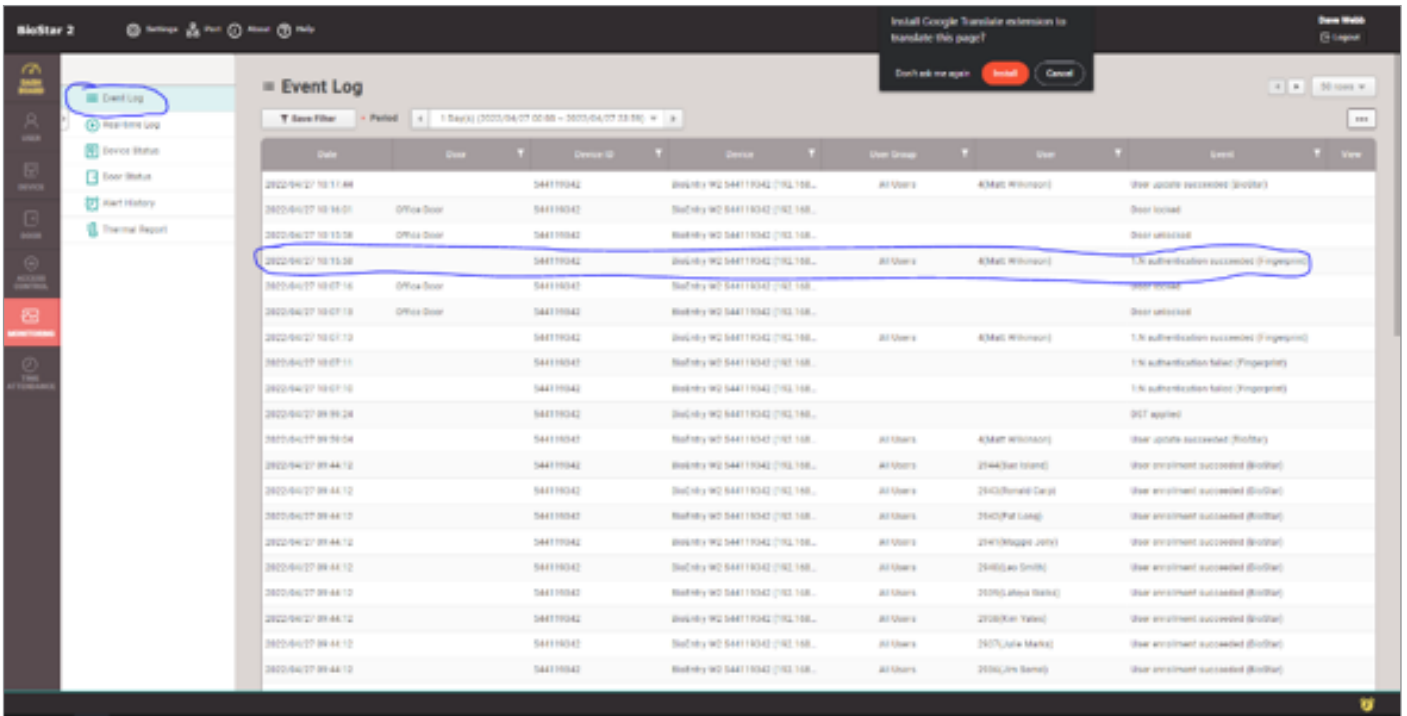
Absence entitlement policy: Production Employee

Period schedule: 08:00-16:30

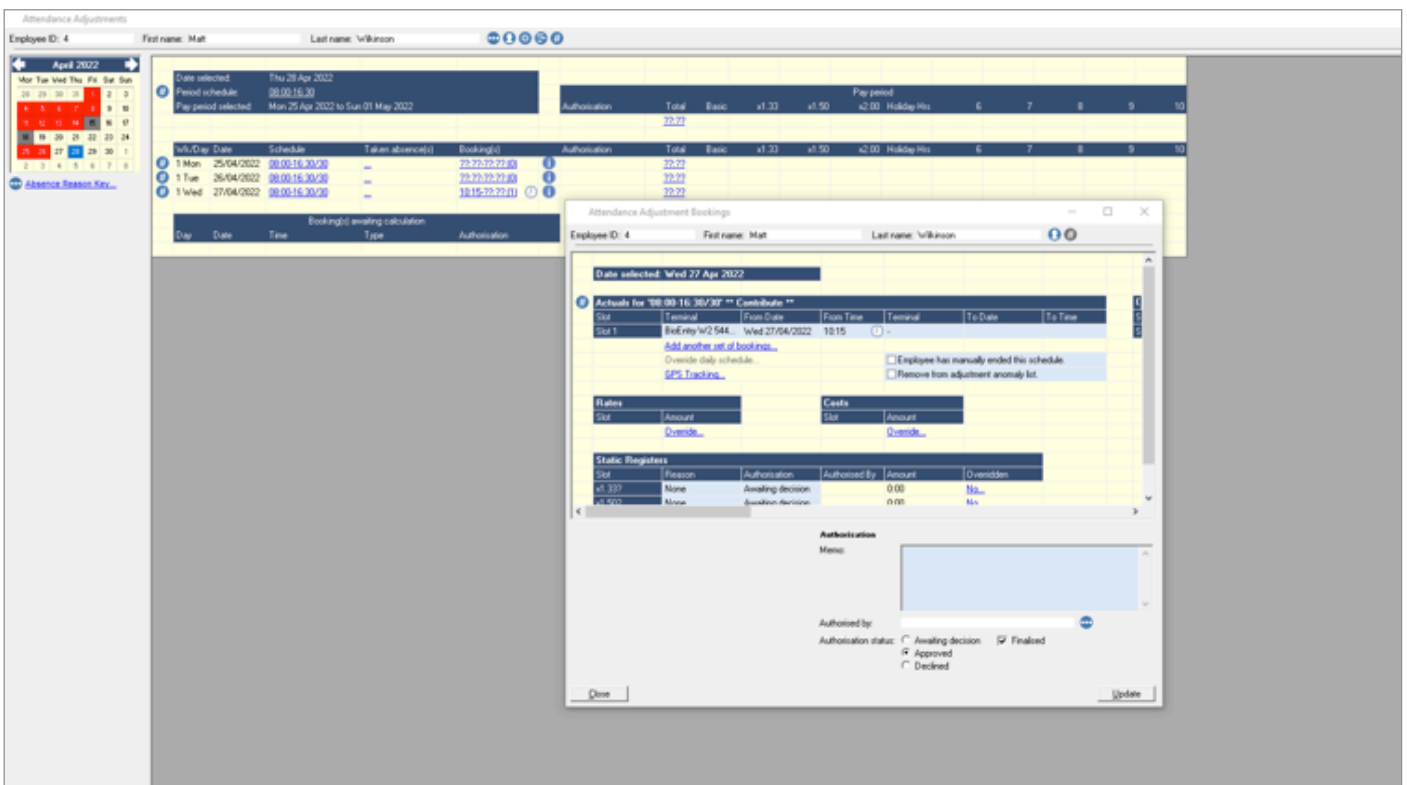
Access group: Keyholders

Terminal policy: Test

- We don't synchronize biometric templates between the two systems. I have created a separate guide for pulling out enrolments from a timeware® system and uploading them into Biostar. This can be found at <https://www.nmd3.com/repository/N2-0109-Suprema-Biostar-2-Migrating-devices.pdf>
- With Biostar, you can enrol either through the device or through Biostar itself. If the customer would like to still enter the badge numbers in timeware®, we have developed an Event Agent script to handle this. The guide for this can be found at https://www.nmd3.com/repository/n2-0108-Datasheet-Event_Agent_Script-Biostar2_Badge_Credential_NMD3.pdf. If they are using CSN format card, the guide is at https://www.nmd3.com/repository/n2-0106-Datasheet-Event_Agent_Script-Biostar2_Badge_Credential_CSN.pdf.
- In theory that it is for the configuration of the integration. Things such as changing authentication modes (Card+Finger) for example, there are guides for on Suprema's website. If you tested a clocking now for someone you enrolled, once you get the green light (booking accepted), if you head to the "Monitoring" tab, under "Event Log", you will see the "Authentication succeeded" entry.



- If you head back into timeware®, if you have it setup as an attendance device head to attendance adjustments for that employee and you should see the booking has been pulled through.



CSV Import
✕

mobile_expiry_date...	None	▼
csn_mobile	None	▼
qr	None	▼
26 bit SIA Standard...	None	▼
HID 37 bit-H10302	None	▼
HID 37 bit-H10304	None	▼
HID Corporate 1000	None	▼
HID Corporate 100...	None	▼
26 bit NMD3	26 bit NMD3	▼
face_image_file1	None	▼
face_image_file2	None	▼
pin	pin	▼

• When the same User ID exists in BioStar 2

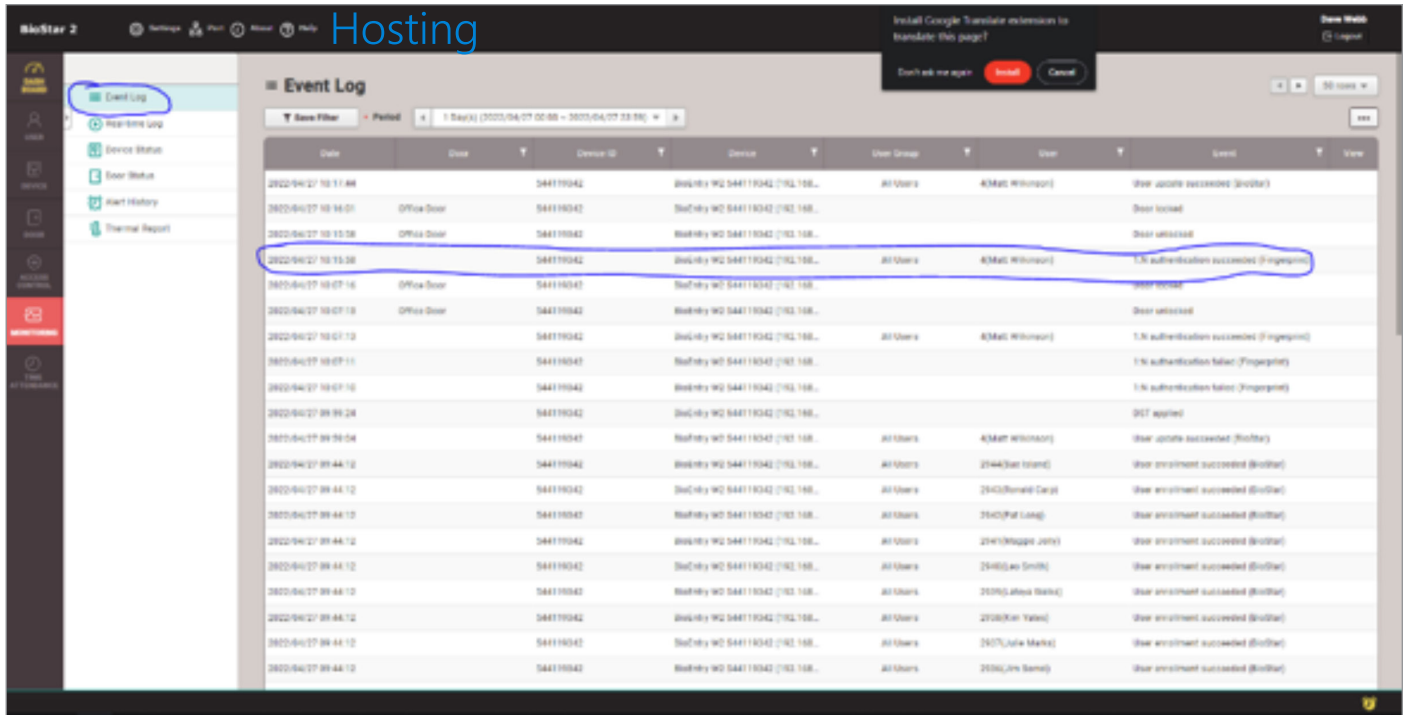
Preserve data Overwrite

Back
Next
Close

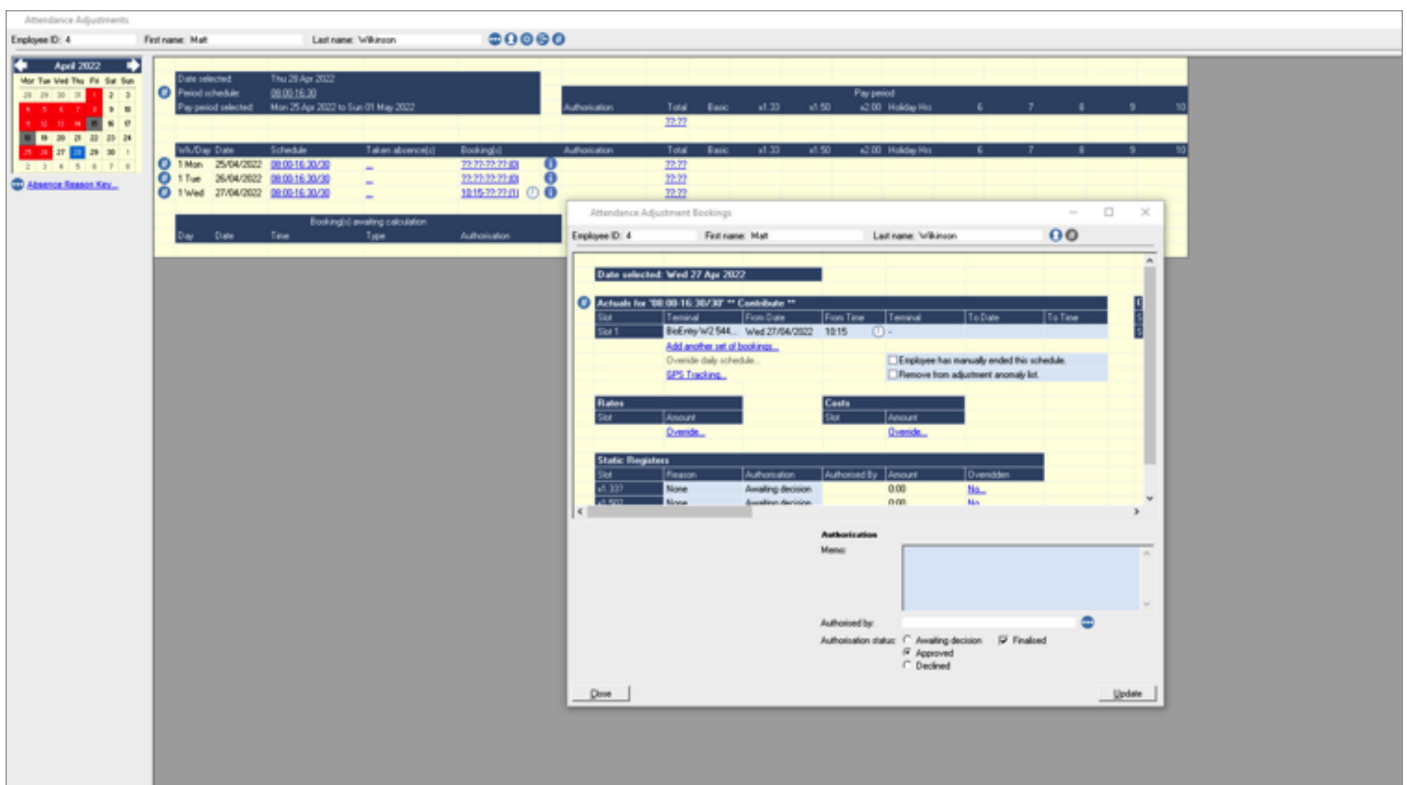
- The import should run through now, taking a few moments depending on the amount of people. If you want to check it has worked, if you check the column with the card icon for employees, and it should indicate they now have a card assigned.

☐	ID	Name	Email	Group	Access Group	🔒	😊	👤	📇	Status
☐	1	Administrator	-	All Users	Keyholders	0	0	0	0	-
☐	2	Michael Coope	-	All Users	Keyholders	0	0	0	1	-
☐	3	Simon Birchall	-	All Users	Keyholders	0	0	0	1	-
☐	4	Matt Wilkinson	-	All Users	Keyholders	0	0	0	1	-

- In theory that it is for the configuration of the integration. Things such as changing authentication modes (Card+Finger) for example, there are guides for on Suprema’s website. If you tested a clocking now for someone you enrolled, once you get the green light (booking accepted), if you head to the “Monitoring” tab, under “Event Log”, you will see the “Authentication succeeded” entry.



- If you head back into timeware®, if you have it setup as an attendance device head to attendance adjustments for that employee and you should see the booking has been pulled through.

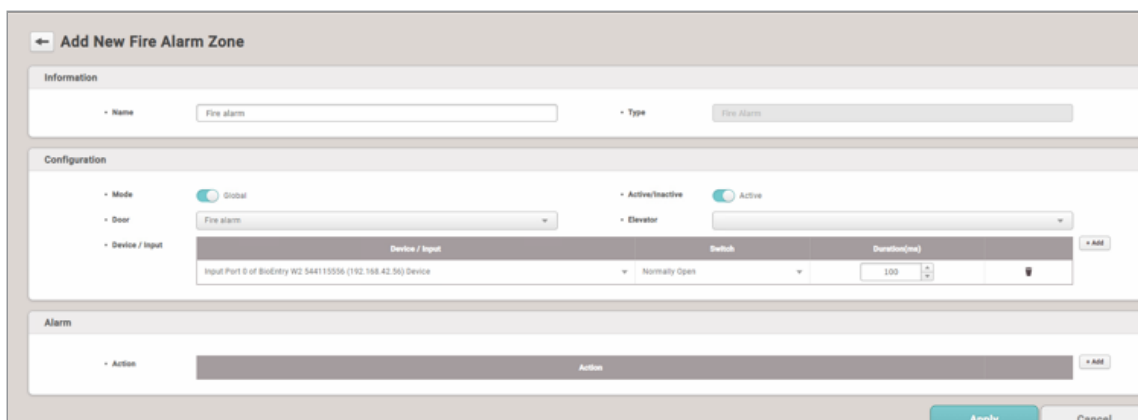


- If you have the device setup as an Access Control unit, it will then obviously show up in your access audit/real-time access activity.

Configuring a fire panel

We have the ability to print/email reports when a fire alarm is triggered, as well as multiple actions built into Biostar 2.

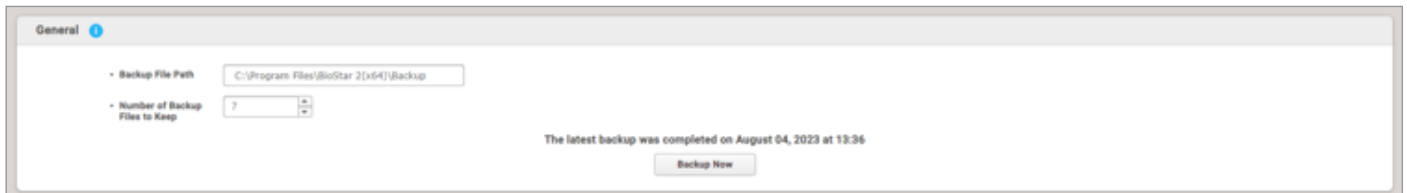
- Add the device the fire alarm is connected to into biostar, set it up as a door, but don't assign either the "door sensor" or "exit button" inputs.
- Go into the zone section, click "add zone", select "fire alarm" and then click "apply".
- Name the zone how you like, change the mode to "Global", and choose your "Fire Alarm" door you created earlier on. If you wanting to release other doors when the alarm goes off, select the additional doors here as well.
- On the "Device/Input" section, choose the "fire alarm" door we created earlier, and make sure it is set to "Normally Open" and "100ms".



- Click "apply" once finished.
- The next step is to setup the report emailing/printing. We will assume you have already configured a report to be used in the Dashboard and Report Viewer.
- Launch the Event Agent UI, and choose option 5 for "Build fire alarm command line..."
- Select the device being used as the trigger, if it is a multi site setup where a different report is setup for each site, you will need to repeat this step for each site.
- The rest of the steps you just select your report, printers and where to email it if required, just like the standard event agent reports. Once you have completed this it will generate you a command line, which is copied to your clipboard. I would save a copy of it as well just to be safe.
- Next, we need to create a service. Download the following batch file: <https://www.dropbox.com/s/lrg49nr1m8injzy/Event%20Agent%20Service%20Installer.bat?dl=0>
- Open the batch file in a text editor, replace the following text:
 - "REPLACENAME" – replace with a name of your fire alarm setup i.e "Rochdale site Roll Call"
 - "REPLACECMD" – replace with copied commandline i.e "-c xxxxxxx". Make sure there is a space after the ".exe"
 - "REPLACEDESC" – replace with brief description i.e "handles emailing of Roll call report"
- Once these have been edited save the file and then run it as an admin, this will install the service for you.
- Once installed all that left is to start it up, the service then monitors the DB for certain events, when these events are present it will trigger the report to be emailed/printed.

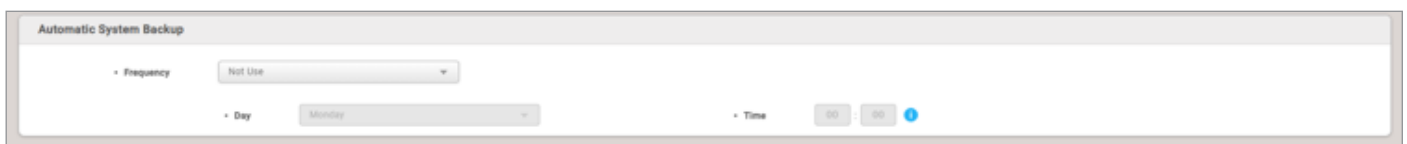
Creating Backups

- We now have the ability to set up automated backups through Biostar. (This is only available on versions 2.9.3 or greater)
- You will need to navigate to Settings -> System Backup and then decide on a path to save your backups to.



The screenshot shows the 'General' settings for system backups. It includes a text input for 'Backup File Path' with the value 'C:\Program Files\BioStar 2(x64)\Backup', a dropdown for 'Number of Backup Files to Keep' set to '7', and a status message: 'The latest backup was completed on August 04, 2023 at 13:36'. A 'Backup Now' button is located at the bottom center.

- We need to specify how many backups to store. We recommend backing up daily and keeping the 7 most recent backups.
- Under the "Automatic system backup" tab you will need to set the "Frequency" of the Backups.



The screenshot shows the 'Automatic System Backup' settings. It features a 'Frequency' dropdown menu currently set to 'Not Use', a 'Day' dropdown menu set to 'Monday', and a 'Time' section with two time selection buttons and a blue information icon.

- The options allow for "Daily", "Weekly" and "Monthly" Backups. We recommend a daily backup to be taken. Select a time for the backups to take place, we would recommend early morning or late at night when the system isn't being used as heavily.