# **Suprema Biostar 2 Integration**

## 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.
* Annual charge for Integration license. 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.

## Installation:

* Requirements
  + Biostar 2 software <https://www.supremainc.com/en/support/biostar-2-package.asp>
  + timeware 2022 (22.1.5 or greater)
  + .NET Runtime 6.0.X <https://dotnet.microsoft.com/en-us/download/dotnet/6.0>
* 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 recommended.
* 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.

Graphical user interface, text, application, email

Description automatically generated

* 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”.

Graphical user interface

Description automatically generated

* Confirm that the top 3 services are running

Graphical user interface

Description automatically generated

* 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>] 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”.

Graphical user interface, application, Teams

Description automatically generated

Graphical user interface

Description automatically generated

* Click then pen icon on the next available slot, should be Weigand ID 6.
* Graphical user interface, application

  Description automatically generatedInput the following settings and then click apply.
* Next up is enabling templates to be brought up into the software from the devices. If you go to “Settings” and then “Server”.

Graphical user interface, application, Teams

Description automatically generated

Graphical user interface

Description automatically generated

* 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.

Graphical user interface, application

Description automatically generated

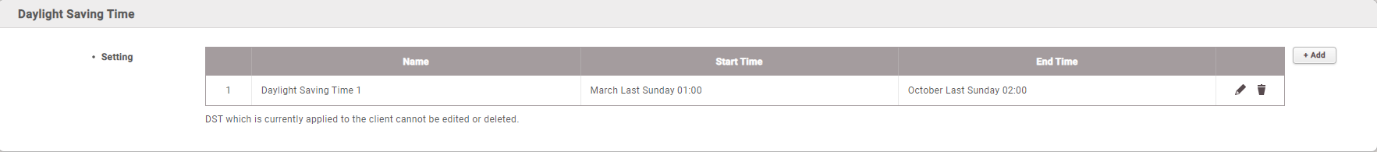
* We must also setup Daylight Saving Time, again go to “Settings” and then “Daylight Saving Time”.

A picture containing text, electronics

Description automatically generatedGraphical user interface, application, Teams

Description automatically generated

* Click the add button on the right-hand side and enter the following settings.



* Go back to “Settings” and then “Preferences”

A picture containing text, electronics, screenshot

Description automatically generatedGraphical user interface, application, Teams

Description automatically generated

* Graphical user interface, text, application, email

  Description automatically generatedApply the Daylight Saving time you just created in the following dropdown and then click apply.
* Next is to add a device. Head to the device section.

Graphical user interface, application

Description automatically generated

* 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”.

Table

Description automatically generated

* Graphical user interface, application

  Description automatically generatedClick 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.
* If you are attaching any devices as slaves, please check on Suprema’s website how to do this.
* Next, we need 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”.

Graphical user interface, application

Description automatically generated

* 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 you will get the option for “Exit Device”, select the slave reader for this. With the free version of Biostar 2, we can only configure anti pass back (repeat swipe) if there is a slave device connected. This means that if it is just a single attendance unit, there is the chance of being able to clock twice in the same minute. As long as your timeware system is set to not allow bookings in the same minute, this won’t cause an issue. If you have a slave connected, you can then 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.

Graphical user interface, text, application, email

Description automatically generated

* 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”

Graphical user interface, application

Description automatically generated

* Give the Access Group a name and description, and then click the “Add” next to “Access Level”

Graphical user interface, text, application

Description automatically generated

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

Graphical user interface, text, application

Description automatically generated

* 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.

Graphical user interface, text, application

Description automatically generated

* If you want to apply this to all users or a certain user group then click on the “Add” next to “User Group”. Select your specific User Group and then click apply.

Graphical user interface, application, table

Description automatically generated

* If you are wanting to apply it to certain individuals only, then click the “Add” next to “User” and select the relevant users. Click apply at the bottom.
* 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 Biostar 2 under the “3rd Party Integration” header. Click on the blue “Connection Wizard”.

Graphical user interface, text, application

Description automatically generated

* 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\BiostarAgentBin”. Run the following command “**Toronto.BioStar.WindowsService.exe -d 0**”. This will start the service with a 0 second delay.
* Text

  Description automatically generatedIf you have an employee set up in timeware with employee\_id=1, you will be presented with the following error. Biostar 2 reserves ID=1 for the Administrator account.
* 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.

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

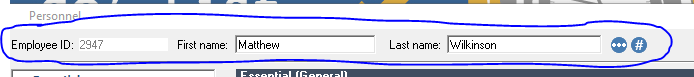
Description automatically generated

* Graphical user interface, text

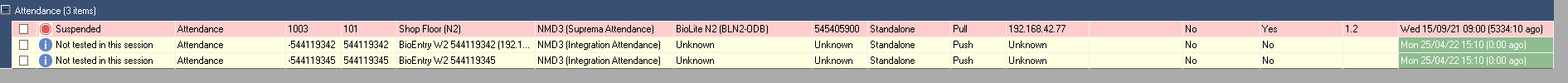
  Description automatically generatedRerun the command in the command prompt again and hopefully it should now run through with no errors. You should notice that some info lines display in regard to creating event logs etc. This shows that it is working as intended.
* If you head over to “User” now in Biostar, you should see that your “Personnel” records from timeware are now appearing as users in Biostar. This may take a few moments to complete depending on how many personnel records are being sent across.

Graphical user interface, text, application

Description automatically generated



* 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 Attendance”. If you are wanting to use the bookings towards access control data, then change the type to “NMD3 Integration Access Control”. Unsuspend all the integration devices you require and assign them to a relevant terminal group.



* 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. If you only created a single group in Biostar earlier, and set it to the “All user group”, it will default to this one in Biostar If you don’t assign an Access Group in timeware.

Graphical user interface

Description automatically generated

* Unfortunately, if you had biometric templates enrolled in timeware and are switching over to this integration, the templates will need to be re-enrolled. Please see Suprema’s website for complete guides on how to enrol either through Biostar or the devices itself if applicable. For badge numbers that are in timeware, we have created an export that can be imported into Biostar initially. Going forwards from that initial import though, all new badges will need to be enrolled via Biostar or the devices. Again, guides for this are available on Suprema’s website.
* To export the badges, open the new Dashboard and Report Viewer, and run the “Suprema Biostar Employee Export”. This is found in the Custom->Tools section in either the “Company” or “Standard” reports. Make a note of the location it saves the file.
* In Biostar 2 go to “Users, click the 3 dots at the top right, and choose “CSV import”

Graphical user interface, application, Teams

Description automatically generated

* Select the file that we just exported from timeware and click next on the first screen. On the second screen, it should automatically map all the fields for you. The important one for us is the “26 bit NMD3” field. Make sure it has correctly mapped the “26 bit NMD3” field from the CSV, and is not saying “None”. If it says “None”, click the dropdown and select the “26 bit NMD3” option. Make sure to change the “When the same User ID exists in Biostar 2” option to “Overwrite”, or you will end up creating duplicates.

Graphical user interface, application

Description automatically generated

* Graphical user interface

  Description automatically generatedThe 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.
* 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.

A screenshot of a computer

Description automatically generated

* 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.

Graphical user interface, timeline

Description automatically generated

* 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.