**SUPREMA ACCESS CONTROL AND TIME ATTENDANCE PLATFORM - BioStar 2**

**TECHNICAL SPECIFICATIONS**

2021-08-05

# ABBREBIATIONS

**AC** Access Control

**AES** Advanced Encryption Standard

**AoC** Access-on-Card

**APB** Anti-passback

**Auth** Authentication

**DB** Database

**DHCP** Dynamic Host Configuration Protocol

**HTTPS** Hypertext Transfer Protocol over Secure Socket

**PIN** Personal Identification Number

**SHA** Secure Hash Algorithm

**TA** Time Attendance

**VE** Video Event

# PART 1 - GENERAL

This document intent is to specify the minimum criteria for the design, supply, installation, and commissioning of the BioStar 2 which is a web-based security platform.

* 1. SUMMARY

1. Section includes a web-based security platform requirements
2. Product - A web-based security platform, capable of managing access control system, managing time attendance system, recording video log with Ethernet network connectivity, and managing visitor system.
   1. SUBMITTALS
   2. QUALIFICATIONS
3. All installation, configuration, and setup of the platform shall provide by qualified technicians.
4. Installers shall be trained by the Manufacturer to install, configure and commission the access control and time attendance system.

END OF SECTION

# PART 2 - PRODUCTS

1. MANUFACTURER
2. Suprema Inc.   
   17F Parkview Office Tower, Jeongja, Bundang, Seongnam, Gyeonggi, 463-863, Republic of Korea  
   Tel: 82-31-783-4502, Fax: 82-31-783-4503, [www.supremainc.com](http://www.supremainc.com)  
   <http://support.supremainc.com>
3. This specification is based on BioStar 2.8.12 manufactured by Suprema Inc.
4. MINIMUM SYSTEM REQUIREMENT
5. Access Control and Time Attendance
6. Small Business Server
7. Total devices: 50
8. Computer
9. 2 GHz Dual Core CPU
10. 8 GB RAM
11. 512 GB SSD
12. Operating system
13. Windows 7 (SP1 or later)
14. Windows 8
15. Windows 8.1
16. Windows 10
17. Windows Server 2008 R2 (SP2 or later)
18. Windows Server 2012
19. Windows Server 2012 R2
20. Windows Server 2016
21. Windows Server 2019

▪ Windows virtual environments on Mac Boot Camp are not supported.

1. Database
2. MariaDB 10.1.10
3. MS SQL Server 2012
4. MS SQL Server 2014 SP2
5. MS SQL Server 2016 SP1
6. MS SQL Server 2017
7. MS SQL Server 2019
8. Java 1.8.0\_201
9. Client Web Browser: Google Chrome 75 or later
10. Medium Business Server
11. Total devices: 100
12. Computer
13. 4 GHz Quad-core CPU
14. 16 GB RAM
15. 1 TB SSD
16. Operating system
17. Windows 7 (SP1 or later)
18. Windows 8
19. Windows 8.1
20. Windows 10
21. Windows Server 2008 R2 (SP2 or later)
22. Windows Server 2012
23. Windows Server 2012 R2
24. Windows Server 2016
25. Windows Server 2019

▪ Windows virtual environments on Mac Boot Camp are not supported.

1. Database
2. MariaDB 10.1.10
3. MS SQL Server 2012
4. MS SQL Server 2014 SP2
5. MS SQL Server 2016 SP1
6. MS SQL Server 2017
7. MS SQL Server 2019
8. Java 1.8.0\_201
9. Client Web Browser: Google Chrome 75 or later
10. Enterprise Business Server
11. Total devices: 1,000
12. Computer
13. 4 GHz 16 Core CPU
14. 32 GB RAM
15. 1 TB SSD
16. Operating system
17. Windows 7 (SP1 or later)
18. Windows 8
19. Windows 8.1
20. Windows 10
21. Windows Server 2008 R2 (SP2 or later)
22. Windows Server 2012
23. Windows Server 2012 R2
24. Windows Server 2016
25. Windows Server 2019

▪ Windows virtual environments on Mac Boot Camp are not supported.

1. Database
2. MariaDB 10.1.10
3. MS SQL Server 2012
4. MS SQL Server 2014 SP2
5. MS SQL Server 2016 SP1
6. MS SQL Server 2017
7. MS SQL Server 2019
8. Java 1.8.0\_201
9. Client Web Browser: Google Chrome 75 or later
10. Video Log
11. Computer (Minimum)
12. 4 GHz Quad-core CPU
13. 8 GB RAM
14. 2 TB HDD
15. Computer (Recommended)
16. 4 GHz Quad-core CPU
17. 16 GB RAM
18. 4TB HDD
19. BioStar 2 API Server
20. Computer (Minimum)
21. 4 GHz Quad-core CPU
22. 8 GB RAM
23. 1TB Free disk space
24. Computer (Recommended)
25. 4 GHz Quad-core CPU
26. 16 GB RAM
27. 2 TB Free disk space
28. PERFORMANCE CRITERIA
29. System Architecture
30. A web-based security platform, capable of managing access control system, managing time attendance system, recording video log with Ethernet network connectivity, and managing visitor system.
31. Access Control
32. User management
33. Device management
34. Door management
35. Elevator management
36. Zone management (Anti-passback, Fire Alarm, Schedule Lock, Schedule Unlock, Intrusion Alarm, Interlock, Muster, Occupancy Limit)
37. Access group management
38. Monitoring (Event log, Real-time log, Device status, Door status, Floor status, Zone status, Image log, Alert history and Graphic Map)
39. Alarm management
40. RFID card management
41. Audit trail
42. Time Attendance
43. Time code management
44. Shift management
45. Schedule template management
46. Overtime rule management
47. Schedule management
48. Leave management
49. Monitoring (Leave and Exception)
50. TA report generation
51. Video Log
52. Visitor Management
53. Standard Transmission Control Protocol (TCP/IP) networking communication protocol between servers, clients, and devices.
54. Support Dynamic Host Configuration Protocol (DHCP) or Static IP address.
55. Support network configuration.
56. Support Network Time Protocol (NTP).
57. Support HTTPS communication protected by Secure Socket Layer (SSL) between the client (Web browser) and platform.
58. Support AES-256 for User Name, Fingerprint Template, and Face Template.
59. Support AES-256 for Fingerprint Template and Face Template (Optional).
60. Support SHA-256 for PIN and Password.
61. Support export to CSV or PDF for list items.
62. Installation Wizard
63. Separate standalone installation package.
64. Shall support English and Korean.
65. Shall allow a user to perform the initial configuration.
66. Shall set the password for the admin account.
67. Shall select the database installation (MariaDB 10.1.10 or Custom).
68. Shall set the root password for MariaDB.
69. Shall set the custom database information including Server IP, Server Port, AC DB name, AC DB login information, TA DB login information, TA DB name, VE DB login information, and VE DB name.
70. Shall check the database connection.
71. Shall generate the database tables.
72. Shall change the port number for server.
73. Shall install the USB Device Agent for BioMini and DUALi DE-620.
74. License and System Capacity
75. License for Access Control

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Items** | | **Starter (Free)** | **Basic** | **Standard** | **Advanced** | **Professional** | **Enterprise** |
| **Access Control** | Max. User | Unlimited | Unlimited | Unlimited | Unlimited | Unlimited | Unlimited |
| Max. Device | 1,000 | 1,000 | 1,000 | 1,000 | 1,000 | 1,000 |
| Max. Door | 5 | 20 | 50 | 100 | 300 | 1,000 |
| Zone | - | - | Supported | Supported | Supported | Supported |
| Elevator | - | - | - | Supported | Supported | Supported |
| Graphic Map | - | - | - | Supported | Supported | Supported |
| Server Matching | - | - | - | Supported | Supported | Supported |
| Cloud | - | - | Supported | Supported | Supported | Supported |
| Active Directory | - | - | - | Supported | Supported | Supported |

2. License for Time Attendance

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Items** | **Starter (Free)** | **Standard** | **Advanced** | **Professional** |
| **Number of Users** | 100 | 500 | 1,000 | Unlimited |

3. License for Video

|  |  |  |
| --- | --- | --- |
| **Items** | **Starter (Free)** | **Video License** |
| **Video Log** | - | Supported |

4. License for Visitor

|  |  |  |
| --- | --- | --- |
| **Items** | **Starter (Free)** | **Visitor License** |
| **Visitor Management** | - | Supported |

1. Interface
2. Use a Web-based client user interface for configuration, administration, management, and monitoring.
3. Support for multi-lingual UI
4. English and Korean available.
5. Other languages available via language pack from website. (Supported languages may vary depending on the BioStar 2’s version)
6. German (Deutsch)
7. Latin Spanish
8. Spain Spanish
9. French
10. Italian
11. Japanese
12. Dutch (Nederlands)
13. Portuguese
14. Chinese
15. Russian
16. Arabic
17. Romanian
18. User
19. User ID
20. Support numeric user ID.
21. Support alphanumeric user ID (Optional).
22. Support expiration dates (Period) for the user.
23. Operator levels
24. Provide for a maximum of 6 pre-defined levels.
25. Provide for an unlimited number of custom operator levels.
26. Each level shall have a set of permissions and shall be able to be configured for different operator levels.
27. Custom Field
28. Provide 3 types of custom user fields.
29. Support the Text Input Box, Number Input Box, and Combo Box
30. Provide for a maximum of 20 custom fields.
31. Fingerprint
32. Support up to 10 fingers (20 templates) per user.
33. Support 3 types of fingerprint template format (SUPREMA / ISO 19794-2 / ANSI 378).
34. Face
35. Support up to 5 faces (150 templates) per user.
36. Visual Face
37. Support up to 2 faces per user and 20 templates (40 templates) per face.
38. Support Visual Face Mobile Enrollment.
39. Wiegand Card
40. Provide for a maximum of 15 customized formats including 5 pre-defined formats.
41. Support card formats with total bits, facility code, customizable ID fields, and parity bits.
42. Provide for a maximum of 5 pre-defined formats.
43. 26 bit SIA Standard-H10301
44. HID 37 bit-H10302
45. HID 37 bit-H10304
46. HID Corporate 1000
47. HID Corporate 1000 48bit
48. Smart Card
49. Support 3 types of smart card layout and mobile card.
50. MIFARE, iCLASS, DESFire, iCLASS Seos and Mobile
51. Store the fingerprint templates on the smart card up to 4. (Access-on Card)
52. Mobile Access
53. Support the connection with the Suprema Mobile Portal.
54. Issue and revoke mobile access cards remotely.
55. QR/Barcode
56. Support 2 types of QR/Barcode.
57. BioStar 2 QR: Directly issue a QR code that contains an encrypted PIN and card ID on BioStar 2.
58. QR/Barcode: Register users with QR/Barcodes issued from 3rd-party systems.
59. Import/Export User Information via CSV file
60. Support import and export data in Comma-separated Values (CSV) file format.
61. Support multiple languages.
62. Allow the user to import/export the user information and card information in CSV file.
63. Support the auto/manual mapping of CSV fields to the database fields.
64. Support long-term idle user management.
65. Device
66. Support auto search and manual search for a device.
67. Allow the user to change the device settings and perform the action that includes:
68. Firmware upgrade
69. Factory reset
70. Lock/Unlock
71. Time zone
72. Time synchronization
73. Network configuration
74. Serial (RS-485) configuration
75. Authentication settings
76. Card format settings
77. Trigger & action
78. Time attendance settings
79. Administrator level
80. Display and sound settings
81. Wiegand settings
82. Auto synchronization with server
83. Thermal camera and mask settings
84. Door
85. Supported door configuration includes:
86. Two devices (entry device and exit device) for one door
87. Entry device for one door with exit button
88. Entry device for one door without exit button
89. Support two types of relay setting for the exit button and door sensor.
90. Normally open and normally closed
91. Allow the user to configure the door settings that include:
92. Entry device selection
93. Relay selection for a door lock
94. TTL input port for an exit button
95. TTL input port for a door sensor
96. Relay release time for door lock
97. Dual authentication settings
98. Held open time and alarm
99. Forced open alarm
100. Anti-passback alarm
101. Elevator
102. Support the floor button control.
103. Support auto/manual mapping of floor names to the relay numbers.
104. Allow the user to configure the floor control that includes:
105. Controller selection
106. Reader selection
107. Module selection
108. Total number of floors
109. Relay release time for the floor button
110. Dual authentication settings
111. Tamper port setup
112. Alarm configuration
113. Trigger & Action
114. Zone
115. Anti-passback
116. User shall be able to define the areas and assign the entry devices and exit devices to configure an anti-passback zone.
117. Support the global APB zone which can be set with all devices enrolled in BioStar 2.
118. Support the local APB zone which can be set with the entry devices and exit device connected with RS-485.
119. Allow the user to configure an anti-passback zone that includes:
120. APB zone mode (Global or Local)
121. Temporary activation or deactivation of the APB zone
122. APB type (Hard APB or Soft APB)
123. Auto reset time
124. Entry device and exit devices selection for the APB zone
125. Network failure action
126. Customizable signal output for alarm
127. Bypass user group configuration
128. Fire Alarm
129. User shall be able to define the areas and assign the doors and/or elevators to configure a fire alarm zone.
130. Support the global fire alarm zone which can be set with all devices enrolled in BioStar 2.
131. Support the local fire alarm zone which can be set with the entry devices and exit device connected with RS-485.
132. Allow the user to configure a fire alarm zone that includes:
133. Fire alarm zone mode (Global or Local)
134. Temporary activation or deactivation of the Fire Alarm zone
135. Door and/or elevator selection for the fire alarm zone
136. Customizable signal output for alarm
137. Scheduled Lock
138. User shall be able to define the areas and assign the doors and schedule to configure a scheduled lock zone.
139. Allow the user to configure a scheduled lock zone that includes:
140. Temporary activation or deactivation of the Scheduled Lock zone
141. Door lock method selection
142. Door and schedule selection for the scheduled lock zone
143. Customizable signal output for alarm
144. Bypass user group configuration
145. Scheduled Unlock
146. User shall be able to define the areas and assign the doors and schedule to configure a scheduled unlock zone.
147. Allow the user to configure a scheduled unlock zone that includes:
148. Temporary activation or deactivation of the Scheduled Unlock zone
149. Started by user authentication option
150. Door and schedule selection for the scheduled unlock zone
151. Access group where the user belongs who can start a scheduled unlock
152. Intrusion Alarm
153. User shall be able to define the areas and assign the doors to configure an intrusion alarm zone.
154. Support the global intrusion alarm zone which can be set with all devices enrolled in BioStar 2.
155. Support the local intrusion alarm zone which can be set with the entry devices and exit device connected with RS-485.
156. Allow the user to configure an intrusion alarm zone that includes:
157. Intrusion alarm zone mode (Global or Local)
158. Temporary activation or deactivation of the Intrusion Alarm zone
159. Door selection for detecting intrusion
160. Arm and/or disarm settings
161. Customizable signal output for detecting intrusion alarm
162. Customizable signal output when a specified event occurs
163. Interlock
164. User shall be able to define the areas and assign the doors to configure an interlock zone.
165. Support the local interlock zone which can be set with the devices connected to CoreStation with RS-485.
166. Allow the user to configure an interlock zone that includes:
167. Temporary activation or deactivation of the Interlock zone
168. Door selection for the interlock zone
169. Option to detect the user's stay in the interlock zone
170. Customizable signal output for alarm
171. Muster
172. User shall be able to define the areas and assign the entry & exit devices and the access group to configure a muster zone.
173. Support the global muster zone which can be set with all devices enrolled in BioStar 2.
174. Allow the user to configure a muster zone that includes:
175. Temporary activation or deactivation of the Muster zone
176. Door and access group selection for the muster zone
177. Maximum amount of time that user can stay in the muster zone
178. Customizable signal output for alarm
179. Occupancy Limit
180. Users shall be able to define the areas and assign the entry & exit devices and limit the count to configure an occupancy limit zone.
181. Support the global occupancy limit zone, which can be with FaceStation F2 and FaceStation 2 added on BioStar 2.
182. Allow the user to configure an occupancy limit zone that includes:
183. Temporary activation or deactivation of the occupancy limit zone
184. Entry and exit devices selection for the occupancy limit zone
185. The maximum number of people who can enter the Occupancy limit zone
186. Access Control
187. Provide the access permission status by four pre-defined filters.
188. Door permission by Access Group
189. Elevator permission by Floor Level
190. Access Level
191. Support the user to create an access level which is combined with the doors and schedules.
192. Floor Level
193. Support the user to create a floor level which is combined with the elevators, floor names, and schedules.
194. Access Group
195. Support the user to create an access group for door access permission which is combined with the access levels and user groups/individual users.
196. Support the user to create an access group for floor access permission which is combined with the floor levels and user groups/individual users.
197. Monitoring
198. Provide export the access control event list to the CSV file.
199. Support the filter functionality for sort.
200. Provide all monitoring features of the access control system that includes:
201. Event log
202. Real-time log
203. Device Status
204. Door Status
205. Floor Status
206. Zone Status
207. Alert History
208. Graphic Map View
209. Provide the following operations for the selected door in Door Status.
210. Lock the door manually
211. Unlock the door manually
212. Release the manual lock/unlock
213. Open the door temporarily
214. Clear all door alarm
215. Clear the APB alarm
216. Provide the following operations for the selected floor in Floor Status.
217. Lock the floor manually
218. Unlock the floor manually
219. Release the manual lock/unlock
220. Open the floor temporarily
221. Clear all floor alarm
222. Provide the following operations for the selected zone in Zone Status.
223. Clear the APB alarm
224. Clear all alarm
225. Video
226. Record the video when occurs the specified access control event at door.
227. Support the user to change the video file path.
228. Support the user to change the weeks to keep the recorded files.
229. Support NVR setup and IP camera setup.
230. Support NVR manufacturers including:
231. ACTi
232. Dahua
233. Hikvision
234. Time Attendance
235. Support the user to configure a time attendance rule and tracking the TA records including:
236. Time code
237. Shift
238. Schedule Template
239. Rule
240. Schedule
241. TA Report
242. TA report shall include 8 pre-defined reports type that can be customized by the user:
243. Daily
244. Daily Summery
245. Individual
246. Individual Summery
247. Leave
248. Exception
249. Edit History
250. Working alarm time
251. Support the filter functionality for customized TA report.
252. Support the user to export the TA reports as CSV or PDF files.
253. Support the user to modify the TA records.
254. Visitor
255. Provide the visit application page for visitors:
256. Support the terms and conditions and the privacy policy information for visitors.
257. Support the fingerprint enrollment and card issuance for visitors.
258. Support to the USB fingerprint scanner connection.
259. BioMini
260. BioMini Plus
261. BioMini Plus 2
262. Support the shortcut of the visitor application page.
263. Provide the visitor management menu:
264. Support the list of registered, checked in, checked out, and total visitors.
265. Support the visitor search.
266. Support access control for visitors.
267. System Alert
268. Provide the user to 50 events for system alert include:

* Device Disconnection Detected
* Device restarted
* RS-485 disconnected
* Tamper on
* Supervised Input (Short)
* Supervised Input (Open)
* AC Power Failure
* Forced door opened
* Held door opened
* Forced door open alarmed
* Held door open alarmed
* Enable all floor relays
* Access denied (Exceeded threshold temp.)
* Access denied (Temp. not measured correctly)
* Access denied (Mask not detected)
* Access granted (Soft temp. violation on check only)
* Access granted (Soft mask violation on check only)
* Access granted (Soft temp. and mask violation on check only)
* Access denied (Exceeded threshold temp. on check only)
* Access denied (Temp. not measured correctly on check only)
* Access denied (Mask not detected on check only)
* Abnormal temp. detected (Exceeded Threshold temp.)
* Abnormal temp. detected (Temp. not measured correctly)
* Mask not detected
* Anti-passback zone alarm detected
* Fire alarm zone alarm detected
* Scheduled lock zone alarm detected
* Occupancy Full Detected
* Occupancy Availability Recovered
* Exit Occurred While Occupancy Count Zero
* Occupancy Count Alert 1 Detected
* Occupancy Count Alert 2 Detected
* Intrusion alarm detected
* Interlock door open denied alarm
* Interlock door open denied alarm (Occupied)
* Occupancy Limit Violation (Count Full)
* Muster zone alarm detected
* 1:1 authentication failed
* 1:1 duress authentication succeeded
* 1:N authentication failed
* 1:N duress authentication succeeded
* Access denied (Invalid access group)
* Access denied (Disabled user)
* Access denied (Invalid period)
* Access denied (Blacklist)
* Access denied (Hard anti-passback)
* Access denied (Forced lock schedule)
* Access denied (Soft anti-passback)
* Fake Fingerprint Detected
* Access Denied (Anti-tailgating)

1. Audit Trail
2. Provide the 2 pre-defined filters
3. Last 1 month
4. Last 3 months
5. Support the user to create a filter using each field item that includes:
6. Datetime
7. User
8. Operator Level
9. IP
10. Category
11. Target
12. Action
13. Modification
14. Security
15. Active Directory
16. Support the synchronizing user data stored in Microsoft Windows Active Directory to BioStar 2.
17. Mobile Access
18. Email Setting

END OF SECTION

# PART 3 - EXECUTION

1. INSTALLER
2. Contractor personnel shall comply with all applicable state and local licensing requirements.
3. Installer and technician requirements
4. Shall be experienced and qualified to accomplish all work promptly.
5. PREPARATION
6. IP addressing shall be coordinated with the Owner’s responsible IT personnel.
7. INSTALLATION
8. Control signal, communications, and data transmission line grounding shall be installed as necessary to preclude ground loops, noise, and surges from adversely affecting system operation.
9. Carefully follow the instructions in the manufacturers’ installation manual to ensure all steps have been taken to provide a reliable, easy-to-operate system.
10. EXAMINATION
11. All network connections shall be tested for proper levels of performance.

END OF SECTION