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

**TECHNICAL SPECIFICATIONS**

2020-04-02

# 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 2.7.14 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. 2GHz Dual Core CPU
10. 6GB RAM
11. 500GB Free disk space
12. Operating system
13. Windows 7 Home Basic 64bit SP1 or later (A 64bit machine is recommended)
14. Windows 7 Home Basic 32bit SP1 or later
15. Database
16. MariaDB 10.1.10
17. MS SQL Server 2012
18. MS SQL Server 2014 SP2
19. MS SQL Server 2016 SP1
20. MS SQL Server 2017
21. Java 1.8.0\_201
22. Client Web Browser: Google Chrome 75 or later
23. Medium Business Server
24. Total devices: 100
25. Computer
26. 4GHz Quad Core CPU
27. 10GB RAM
28. 1TB Free disk space
29. Operating system
30. Windows Server 2008 R2 Standard 64bit SP2 or later
31. Windows 7 Home Premium 64bit SP1 or later
32. Database
33. MariaDB 10.1.10
34. MS SQL Server 2012
35. MS SQL Server 2014 SP2
36. MS SQL Server 2016 SP1
37. MS SQL Server 2017
38. Java 1.8.0\_201
39. Client Web Browser: Google Chrome 75 or later
40. Enterprise Business Server
41. Total devices: 1,000
42. Computer
43. 4GHz Quad Core CPU
44. 16GB RAM
45. 4TB Free disk space
46. Operating system
47. Windows Server 2008 R2 Standard 64bit SP2 or later
48. Windows 7 Home Premium 64bit SP1 or later
49. Database
50. MariaDB 10.1.10
51. MS SQL Server 2012
52. MS SQL Server 2014 SP2
53. MS SQL Server 2016 SP1
54. MS SQL Server 2017
55. Java 1.8.0\_201
56. Client Web Browser: Google Chrome 75 or later
57. Video Log
58. Computer (Minimum)
59. 4GHz Quad Core CPU
60. 8GB RAM
61. 2TB Free disk space
62. Computer (Recommended)
63. 4GHz Quad Core CPU
64. 16GB RAM
65. 4TB Free disk space
66. BioStar 2 API Server
67. Computer (Minimum)
68. 4GHz Quad Core CPU
69. 8GB RAM
70. 1TB Free disk space
71. Computer (Recommended)
72. 4GHz Quad Core CPU
73. 16GB RAM
74. 2TB Free disk space
75. PERFORMANCE CRITERIA
76. System Architecture
77. 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.
78. Access Control
79. User management
80. Device management
81. Door management
82. Elevator management
83. Zone management (Anti-passback, Fire Alarm, Schedule Lock, Schedule Unlock, Intrusion Alarm, Interlock, and Muster)
84. Access group management
85. Monitoring (Event log, Real-time log, Device status, Door status, Floor status, Zone status, Image log, Alert history and Graphic Map)
86. Alarm management
87. RFID card management
88. Audit trail
89. Time Attendance
90. Time code management
91. Shift management
92. Schedule template management
93. Overtime rule management
94. Schedule management
95. Leave management
96. Monitoring (Leave and Exception)
97. TA report generation
98. Video Log
99. Visitor Management
100. Standard Transmission Control Protocol (TCP/IP) networking communication protocol between server, clients, and devices.
101. Support Dynamic Host Configuration Protocol (DHCP) or Static IP address.
102. Support network configuration.
103. Support Network Time Protocol (NTP).
104. Support HTTPS communication protected by Secure Socket Layer (SSL) between the client (Web browser) and platform.
105. Support AES-256 for User Name, Fingerprint Template, and Face Template.
106. Support AES-256 for Fingerprint Template and Face Template (Optional).
107. Support SHA-256 for PIN and Password.
108. Support export to CSV or PDF for list items.
109. Installation Wizard
110. Separate standalone installation package.
111. Shall support English and Korean.
112. Shall allow a user to perform the initial configuration.
113. Shall set the password for admin account.
114. Shall select the database installation (MariaDB 10.1.10 or Custom).
115. Shall set the root password for MariaDB.
116. 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.
117. Shall check the database connection.
118. Shall generate the database tables.
119. Shall change the port number for server.
120. Shall install the USB Device Agent for BioMini and DUALi DE-620.
121. License and System Capacity
122. 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 are 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 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 field.
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 (10 templates) per user.
36. Wiegand Card
37. Provide for a maximum of 15 customized formats including 5 pre-defined formats.
38. Support card formats with total bits, facility code, customizable ID fields, and parity bits.
39. Provide for a maximum of 5 pre-defined formats.
40. 26 bit SIA Standard-H10301
41. HID 37 bit-H10302
42. HID 37 bit-H10304
43. HID Corporate 1000
44. HID Corporate 1000 48bit
45. Smart Card
46. Support 3 types of smart card layout and mobile card.
47. MIFARE, iCLASS, DESFire, iCLASS Seos and Mobile
48. Store the fingerprint templates on the smart card up to 4. (Access-on Card)
49. Mobile Credential
50. Support the connection with the Suprema Mobile Portal.
51. Support for the issuance and retrieval of non-face to face of mobile credentials.
52. Import/Export User Information via CSV file
53. Support import and export data in Comma-separated Values (CSV) file format.
54. Support multiple languages.
55. Allow the user to import/export the user information and card information in CSV file.
56. Support the auto/manual mapping of CSV fields to the database fields.
57. Support the long-term idle user management.
58. Device
59. Support auto search and manual search for a device.
60. Allow the user to change the device settings and perform the action include:
61. Firmware upgrade
62. Factory reset
63. Lock/Unlock
64. Time zone
65. Time synchronization
66. Network configuration
67. Serial (RS-485) configuration
68. Authentication settings
69. Card format settings
70. Trigger & action
71. Time attendance settings
72. Administrator level
73. Display and sound settings
74. Wiegand settings
75. Auto synchronization with server
76. Door
77. Supported door configuration include:
78. Two devices (entry device and exit device) for one door
79. Entry device for one door with exit button
80. Entry device for one door without exit button
81. Support two types of relay setting for the exit button and door sensor.
82. Normally open and normally closed
83. Allow the user to configure the door settings include:
84. Entry device selection
85. Relay selection for a door lock
86. TTL input port for an exit button
87. TTL input port for a door sensor
88. Relay release time for door lock
89. Dual authentication settings
90. Held open time and alarm
91. Forced open alarm
92. Anti-passback alarm
93. Elevator
94. Support the floor button control.
95. Support auto/manual mapping of floor names to the relay numbers.
96. Allow the user to configure the floor control include:
97. Controller selection
98. Reader selection
99. Module selection
100. Total number of floors
101. Relay release time for the floor button
102. Dual authentication settings
103. Tamper port setup
104. Alarm configuration
105. Trigger & Action
106. Zone
107. Anti-passback
108. User shall be able to define the areas and assign the entry devices and exit devices to configure an anti-passback zone.
109. Support the global APB zone which can be set with all devices enrolled in BioStar 2.
110. Support the local APB zone which can be set with the entry devices and exit device connected with RS-485.
111. Allow the user to configure an anti-passback zone include:
112. APB zone mode (Global or Local)
113. Active or inactive temporarily
114. APB type (Hard APB or Soft APB)
115. Auto reset time
116. Entry device and exit devices selection for the APB zone
117. Network failure action
118. Customizable signal output for alarm
119. Bypass user group configuration
120. Fire Alarm
121. User shall be able to define the areas and assign the doors and/or elevators to configure a fire alarm zone.
122. Support the global fire alarm zone which can be set with all devices enrolled in BioStar 2.
123. Support the local fire alarm zone which can be set with the entry devices and exit device connected with RS-485.
124. Allow the user to configure a fire alarm zone include:
125. Fire alarm zone mode (Global or Local)
126. Active or inactive temporarily
127. Door and/or elevator selection for the fire alarm zone
128. Customizable signal output for alarm
129. Scheduled Lock
130. User shall be able to define the areas and assign the doors and schedule to configure a scheduled lock zone.
131. Allow the user to configure a scheduled lock zone include:
132. Active or inactive temporarily
133. Door lock method selection
134. Door and schedule selection for the scheduled lock zone
135. Customizable signal output for alarm
136. Bypass user group configuration
137. Scheduled Unlock
138. User shall be able to define the areas and assign the doors and schedule to configure a scheduled unlock zone.
139. Allow the user to configure a scheduled unlock zone include:
140. Active or inactive temporarily
141. Started by user authentication option
142. Door and schedule selection for the scheduled unlock zone
143. Access group where the user belongs who can start a scheduled unlock
144. Intrusion Alarm
145. User shall be able to define the areas and assign the doors to configure an intrusion alarm zone.
146. Support the global intrusion alarm zone which can be set with all devices enrolled in BioStar 2.
147. Support the local intrusion alarm zone which can be set with the entry devices and exit device connected with RS-485.
148. Allow the user to configure an intrusion alarm zone include:
149. Intrusion alarm zone mode (Global or Local)
150. Active or inactive temporarily
151. Door selection for detecting intrusion
152. Arm and/or disarm settings
153. Customizable signal output for detecting intrusion alarm
154. Customizable signal output when a specified event occurs
155. Interlock
156. User shall be able to define the areas and assign the doors to configure an interlock zone.
157. Support the local interlock zone which can be set with the devices connected to CoreStation with RS-485.
158. Allow the user to configure an interlock zone include:
159. Active or inactive temporarily
160. Door selection for the interlock zone
161. Option to detect the user's stay in the interlock zone
162. Customizable signal output for alarm
163. Muster
164. User shall be able to define the areas and assign the entry & exit devices and the access group to configure a muster zone.
165. Support the global muster zone which can be set with all devices enrolled in BioStar 2.
166. Allow the user to configure a muster zone include:
167. Active or inactive temporarily
168. Door and access group selection for the muster zone
169. Maximum amount of time that user can stay in the muster zone
170. Customizable signal output for alarm
171. Access Control
172. Provide the access permission status by four pre-defined filters.
173. Door permission by Access Group
174. Elevator permission by Floor Level
175. Access Level
176. Support the user to create an access level which is combined with the doors and schedules.
177. Floor Level
178. Support the user to create a floor level which is combined with the elevators, floor names, and schedules.
179. Access Group
180. Support the user to create an access group for door access permission which is combined with the access levels and user groups/individual users.
181. Support the user to create an access group for floor access permission which is combined with the floor levels and user groups/individual users.
182. Monitoring
183. Provide export the access control event list to CSV file.
184. Support the filter functionality for sort.
185. Provide all monitoring features of the access control system, including the following:
186. Event log
187. Real-time log
188. Device Status
189. Door Status
190. Floor Status
191. Zone Status
192. Alert History
193. Graphic Map View
194. Provide the following operations for the selected door in Door Status.
195. Lock the door manually
196. Unlock the door manually
197. Release the manual lock/unlock
198. Open the door temporarily
199. Clear all door alarm
200. Clear the APB alarm
201. Provide the following operations for the selected floor in Floor Status.
202. Lock the floor manually
203. Unlock the floor manually
204. Release the manual lock/unlock
205. Open the floor temporarily
206. Clear all floor alarm
207. Provide the following operations for the selected zone in Zone Status.
208. Clear the APB alarm
209. Clear all alarm
210. Video
211. Record the video when occurs the specified access control event at door.
212. Support the user to change the video file path.
213. Support the user to change the weeks to keep the recorded files.
214. Support NVR setup and IP camera setup.
215. Support NVR manufacturers include:
216. ACTi
217. Dahua
218. Hikvision
219. Time Attendance
220. Support the user to configure a time attendance rule and tracking the TA records, including the following:
221. Time code
222. Shift
223. Schedule Template
224. Rule
225. Schedule
226. TA Report
227. TA report shall include 8 pre-defined reports type that can be customized by the user:
228. Daily
229. Daily Summery
230. Individual
231. Individual Summery
232. Leave
233. Exception
234. Edit History
235. Working alarm time
236. Support the filter functionality for customized TA report.
237. Support the user to export the TA reports as CSV or PDF files.
238. Support the user to modify the TA records.
239. Visitor
240. Provide the visit application page for visitors:
241. Support the terms and conditions and the privacy policy information for visitors.
242. Support the fingerprint enrollment and card issuance for visitors.
243. Support to the USB fingerprint scanner connection.
244. BioMini
245. BioMini Plus
246. BioMini Plus 2
247. Support the shortcut of the visitor application page.
248. Provide the visitor management menu:
249. Support the list of registered, checked in, checked out, and total visitors.
250. Support the visitor search.
251. Support access control for visitors.
252. System Alert
253. Provide the user to 31 events for system alert include:
254. Device Disconnection Detected
255. Device restarted
256. RS-485 disconnected
257. Tamper on
258. Supervised Input (Short)
259. Supervised Input (Open)
260. AC Power Failure
261. Forced door opened
262. Held door opened
263. Forced door open alarmed
264. Held door open alarmed
265. Enable all floor relays
266. Anti-passback zone alarm detected
267. Fire alarm zone alarm detected
268. Scheduled lock zone alarm detected
269. Intrusion alarm detected
270. Interlock door open denied alarm
271. Interlock door open denied alarm (Occupied)
272. 1:1 authentication failed
273. 1:1 duress authentication succeeded
274. 1:N authentication failed
275. 1:N duress authentication succeeded
276. Access denied (Invalid access group)
277. Access denied (Disabled user)
278. Access denied (Invalid period)
279. Access denied (Blacklist)
280. Access denied (Hard anti-passback)
281. Access denied (Forced lock schedule)
282. Access denied (Soft anti-passback)
283. Fake Fingerprint Detected
284. Access Denied (Anti-tailgating)
285. Audit Trail
286. Provide the 2 pre-defined filters
287. Last 1 month
288. Last 3 months
289. Support the user to create a filter using each field item include:
290. Date and time
291. User name,
292. Operator Level
293. IP address
294. Category
295. Target
296. Action
297. Modification
298. Active Directory
299. Support the synchronizing user data stored in Microsoft Windows Active Directory to BioStar 2.

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