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

**TECHNICAL SPECIFICATIONS**

2024-12-06

# ABBREVIATIONS

**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's intent is to specify the minimum criteria for the design, supply, installation, and commissioning of 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 2.9.8 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 10
14. Windows 11
15. Windows Server 2016
16. Windows Server 2019
17. Windows Server 2022

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

1. Database
2. MariaDB 10.1.10
3. MS SQL Server 2012 SP3
4. MS SQL Server 2014 SP2
5. MS SQL Server 2016 SP1
6. MS SQL Server 2017
7. MS SQL Server 2019
8. Client Web Browser: Google Chrome version 100 or later
9. Medium Business Server
10. Total devices: 100
11. Computer
12. 4 GHz Quad-core CPU
13. 16 GB RAM
14. 1 TB SSD
15. Operating system
16. Windows 10
17. Windows 11
18. Windows Server 2016
19. Windows Server 2019
20. Windows Server 2022

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

1. Database
2. MariaDB 10.1.10
3. MS SQL Server 2012 SP3
4. MS SQL Server 2014 SP2
5. MS SQL Server 2016 SP1
6. MS SQL Server 2017
7. MS SQL Server 2019
8. Client Web Browser: Google Chrome version 100 or later
9. Enterprise Business Server
10. Total devices: 1,000
11. Computer
12. 4 GHz 16 Core CPU
13. 32 GB RAM
14. 1 TB SSD
15. Operating system
16. Windows 10
17. Windows 11
18. Windows Server 2016
19. Windows Server 2019
20. Windows Server 2022

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

1. Database
2. MariaDB 10.1.10
3. MS SQL Server 2012 SP3
4. MS SQL Server 2014 SP2
5. MS SQL Server 2016 SP1
6. MS SQL Server 2017
7. MS SQL Server 2019
8. Client Web Browser: Google Chrome version 100 or later
9. BioStar 2 API Server
10. Computer (Minimum)
11. 4 GHz Quad-core CPU
12. 8 GB RAM
13. 1TB Free disk space
14. Computer (Recommended)
15. 4 GHz Quad-core CPU
16. 16 GB RAM
17. 2 TB Free disk space
18. PERFORMANCE CRITERIA
19. System Architecture
20. A web-based security platform, capable of managing access control system, managing time attendance system, and managing visitor system.
21. Access
22. User management
23. Device management
24. Door management (Timed Anti PassBack)
25. Elevator management
26. Zone management (Anti-passback, Fire Alarm, Schedule Lock, Schedule Unlock, Intrusion Alarm, Interlock, Muster, Occupancy Limit)
27. Access group management
28. Monitoring (Event log, Real-time log, Device status, Door status, Floor status, Zone status, Image log, Alert history and Graphic Map)
29. Alarm management
30. RFID card management
31. Audit trail
32. Report
33. Time Attendance
34. Time code management
35. Shift management
36. Schedule template management
37. Overtime rule management
38. Schedule management
39. Leave management
40. Monitoring (Leave and Exception)
41. TA report generation
42. Visitor Management
43. Standard Transmission Control Protocol (TCP/IP) networking communication protocol between servers, clients, and devices.
44. Support Dynamic Host Configuration Protocol (DHCP) or Static IP address.
45. Support network configuration.
46. Support Network Time Protocol (NTP).
47. Support HTTPS communication protected by Secure Socket Layer (SSL) between the client (Web browser) and platform.
48. Support AES-256 for User Name, Fingerprint Template, and Face Template.
49. Support AES-256 for Fingerprint Template and Face Template (Optional).
50. Support SHA-256 for PIN and Password.
51. Support export to CSV or PDF for list items.
52. Installation Wizard
53. Separate standalone installation package.
54. Shall support English and Korean.
55. Shall allow a user to perform the initial configuration.
56. Shall set the password for the admin account.
57. Shall select the database installation (MariaDB 10.1.10 or Custom).
58. Shall set the root password for MariaDB.
59. 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.
60. Shall check the database connection.
61. Shall generate the database tables.
62. Shall change the port number for server.
63. Shall install the USB Device Agent for BioMini and DUALi DE-620.
64. License and System Capacity
65. 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 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. Arabic
7. Czech
8. German (Deutsch)
9. Greek
10. Latin Spanish
11. Spain Spanish
12. French
13. Italian
14. Japanese
15. Dutch (Nederlands)
16. Polish
17. Portuguese
18. Brazil Portuguese
19. Romanian
20. Russian
21. Chinese
22. User
23. User ID
24. Support numeric user ID.
25. Support alphanumeric user ID (Optional).
26. Supports expiration dates (Period) for the user.
27. Supports card printing for user.
28. Operator levels
29. Provide for a maximum of 6 pre-defined levels.
30. Provide for an unlimited number of custom operator levels.
31. Each level shall have a set of permissions and shall be able to be configured for different operator levels.
32. Custom Field
33. Provide 4 types of custom user fields.
34. Support the Text Input Box, Number Input Box, Combo Box and File Upload.
35. Provide for a maximum of 10 custom fields.
36. Fingerprint
37. Support up to 10 fingers (20 templates) per user.
38. Support 3 types of fingerprint template format (SUPREMA / ISO 19794-2 / ANSI 378).
39. Face
40. Support up to 5 faces (150 templates) per user.
41. Visual Face
42. Support up to 2 faces per user and 20 templates (40 templates) per face.
43. Support Visual Face Mobile Enrollment.
44. Support the feature to save both the actual image and the template in the visual face, or to save only the template without storing the actual image.
45. Wiegand Card
46. Provide for a maximum of 15 customized formats including 5 pre-defined formats.
47. Support card formats with total bits, facility code, customizable ID fields, and parity bits.
48. Provide for a maximum of 5 pre-defined formats.
49. 26 bit SIA Standard-H10301
50. HID 37 bit-H10302
51. HID 37 bit-H10304
52. HID Corporate 1000
53. HID Corporate 1000 48bit
54. MIFARE CSN 32bit
55. MIFARE CSN 34bit (Parity)
56. DESFire 56bit
57. DESFire 58bit (Parity)
58. Smart Card
59. Support 3 types of smart card layout and mobile card.
60. MIFARE, iCLASS, DESFire, iCLASS Seos and Mobile
61. Store the fingerprint templates on the smart card up to 4. (Access-on Card)
62. Support Custom Smart Card Layout.
63. MIFARE, DESFire, Felica
64. Mobile Access
65. Support the connection with the Suprema Mobile Portal.
66. Issue and revoke mobile access cards remotely.
67. QR/Barcode
68. Support 2 types of QR/Barcode.
69. BioStar 2 QR: Directly issue a QR code that contains an encrypted PIN and card ID on BioStar 2.
70. QR/Barcode: Register users with QR/Barcodes issued from 3rd-party systems.
71. Import/Export User Information via CSV file
72. Support import and export data in Comma-separated Values (CSV) file format.
73. Support multiple languages.
74. Allow the user to import/export the user information and card information in CSV file.
75. Support the auto/manual mapping of CSV fields to the database fields.
76. Support long-term idle user management.
77. Device
78. Support auto search and manual search for a device.
79. Allow the user to change the device settings and perform the action that includes:
80. Firmware upgrade
81. Factory reset
82. Lock/Unlock
83. Time zone
84. Time synchronization
85. Network configuration
86. Serial (RS-485) configuration
87. Authentication settings
88. Card format settings
89. Trigger & action
90. Time attendance settings
91. Administrator level
92. Display and sound settings
93. Wiegand settings
94. Auto synchronization with server
95. Thermal camera and mask settings
96. Door
97. Supported door configuration includes:
98. Two devices (entry device and exit device) for one door
99. Entry device for one door with exit button
100. Entry device for one door without exit button
101. Support two types of relay setting for the exit button and door sensor.
102. Normally open and normally closed
103. Allow the user to configure the door settings that include:
104. Entry device selection
105. Relay selection for a door lock
106. TTL input port for an exit button
107. TTL input port for a door sensor
108. Relay release time for door lock
109. Dual authentication settings
110. Held open time and alarm
111. Forced open alarm
112. Anti-passback alarm
113. Elevator
114. Support the floor button control.
115. Support auto/manual mapping of floor names to the relay numbers.
116. Allow the user to configure the floor control that includes:
117. Controller selection
118. Reader selection
119. Module selection
120. Total number of floors
121. Relay release time for the floor button
122. Dual authentication settings
123. Tamper port setup
124. Alarm configuration
125. Trigger & Action
126. Zone
127. Anti-passback
128. User shall be able to define the areas and assign the entry devices and exit devices to configure an anti-passback zone.
129. Support the global APB zone which can be set with all devices enrolled in BioStar 2.
130. Support the local APB zone which can be set with the entry devices and exit device connected with RS-485.
131. Allow the user to configure an anti-passback zone that includes:
132. APB zone mode (Global or Local)
133. Temporary activation or deactivation of the APB zone
134. APB type (Hard APB or Soft APB)
135. Auto reset time
136. Entry device and exit devices selection for the APB zone
137. Network failure action
138. Customizable signal output for alarm
139. Bypass user group configuration
140. Support the Timed Anti Passback
141. Fire Alarm
142. User shall be able to define the areas and assign the doors and/or elevators to configure a fire alarm zone.
143. Support the global fire alarm zone which can be set with all devices enrolled in BioStar 2.
144. Support the local fire alarm zone which can be set with the entry devices and exit device connected with RS-485.
145. Allow the user to configure a fire alarm zone that includes:
146. Fire alarm zone mode (Global or Local)
147. Temporary activation or deactivation of the Fire Alarm zone
148. Door and/or elevator selection for the fire alarm zone
149. Customizable signal output for alarm
150. Scheduled Lock
151. User shall be able to define the areas and assign the doors and schedule to configure a scheduled lock zone.
152. Allow the user to configure a scheduled lock zone that includes:
153. Temporary activation or deactivation of the Scheduled Lock zone
154. Door lock method selection
155. Door and schedule selection for the scheduled lock zone
156. Customizable signal output for alarm
157. Bypass user group configuration
158. Scheduled Unlock
159. User shall be able to define the areas and assign the doors and schedule to configure a scheduled unlock zone.
160. Allow the user to configure a scheduled unlock zone that includes:
161. Temporary activation or deactivation of the Scheduled Unlock zone
162. Started by user authentication option
163. Door and schedule selection for the scheduled unlock zone
164. Access group where the user belongs who can start a scheduled unlock
165. Intrusion Alarm
166. User shall be able to define the areas and assign the doors to configure an intrusion alarm zone.
167. Support the global intrusion alarm zone which can be set with all devices enrolled in BioStar 2.
168. Support the local intrusion alarm zone which can be set with the entry devices and exit device connected with RS-485.
169. Allow the user to configure an intrusion alarm zone that includes:
170. Intrusion alarm zone mode (Global or Local)
171. Temporary activation or deactivation of the Intrusion Alarm zone
172. Door selection for detecting intrusion
173. Arm and/or disarm settings
174. Customizable signal output for detecting intrusion alarm
175. Customizable signal output when a specified event occurs
176. Interlock
177. User shall be able to define the areas and assign the doors to configure an interlock zone.
178. Support the local interlock zone which can be set with the devices connected to CoreStation with RS-485.
179. Allow the user to configure an interlock zone that includes:
180. Temporary activation or deactivation of the Interlock zone
181. Door selection for the interlock zone
182. Option to detect the user's stay in the interlock zone
183. Customizable signal output for alarm
184. Muster
185. User shall be able to define the areas and assign the entry & exit devices and the access group to configure a muster zone.
186. Support the global muster zone which can be set with all devices enrolled in BioStar 2.
187. Allow the user to configure a muster zone that includes:
188. Temporary activation or deactivation of the Muster zone
189. Door and access group selection for the muster zone
190. Maximum amount of time that user can stay in the muster zone
191. Customizable signal output for alarm
192. Occupancy Limit
193. Users shall be able to define the areas and assign the entry & exit devices and limit the count to configure an occupancy limit zone.
194. Support the global occupancy limit zone, which can be with FaceStation F2 and FaceStation 2 added on BioStar 2.
195. Allow the user to configure an occupancy limit zone that includes:
196. Temporary activation or deactivation of the occupancy limit zone
197. Entry and exit devices selection for the occupancy limit zone
198. The maximum number of people who can enter the Occupancy limit zone
199. Access Control
200. Provide the access permission status by four pre-defined filters.
201. Door permission by Access Group
202. Elevator permission by Floor Level
203. Access Level
204. Support the user to create an access level which is combined with the doors and schedules.
205. Floor Level
206. Support the user to create a floor level which is combined with the elevators, floor names, and schedules.
207. Access Group
208. Support the user to create an access group for door access permission which is combined with the access levels and user groups/individual users.
209. Support the user to create an access group for floor access permission which is combined with the floor levels and user groups/individual users.
210. Monitoring
211. Provide export the access control event list to the CSV file.
212. Support the filter functionality for sort.
213. Provide all monitoring features of the access control system that includes:
214. Event log
215. Real-time log
216. Device Status
217. Door Status
218. Wireless Door Lock Status
219. Floor Status
220. Zone Status
221. Alert History
222. Graphic Map View
223. Provide the following operations for the selected door in Door Status.
224. Lock the door manually
225. Unlock the door manually
226. Release the manual lock/unlock
227. Open the door temporarily
228. Clear all door alarm
229. Clear the APB alarm
230. Provide the following operations for the selected floor in Floor Status.
231. Lock the floor manually
232. Unlock the floor manually
233. Release the manual lock/unlock
234. Open the floor temporarily
235. Clear all floor alarm
236. Provide the following operations for the selected zone in Zone Status.
237. Clear the APB alarm
238. Clear all alarm
239. Time Attendance
240. Support the user to configure a time attendance rule and tracking the TA records including:
241. Time code
242. Shift
243. Schedule Template
244. Rule
245. Schedule
246. TA Report
247. TA report shall include 8 pre-defined reports type that can be customized by the user:
248. Daily
249. Daily Summery
250. Individual
251. Individual Summery
252. Leave
253. Exception
254. Edit History
255. Working alarm time
256. Support the filter functionality for customized TA report.
257. Support the user to export the TA reports as CSV or PDF files.
258. Support the user to modify the TA records.
259. Visitor
260. Provide the visit application page for visitors:
261. Support the terms and conditions and the privacy policy information for visitors.
262. Support the fingerprint enrollment and card issuance for visitors.
263. Support to the USB fingerprint scanner connection.
264. BioMini
265. BioMini Plus
266. BioMini Plus 2
267. Support the shortcut of the visitor application page.
268. Provide the visitor management menu:
269. Support the list of registered, checked in, checked out, and total visitors.
270. Support the visitor search.
271. Support access control for visitors.
272. System Alert
273. 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
19. Backup & Restore

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