

GDPR Compliance Statement

The General Data Protection Regulation (GDPR) has come into force from May 2018 to set a new standard for protecting the personal data and privacy of EU citizens. Although companies in the EU still have a 2-year enforcement grace period, Suprema Inc has anticipated the regulation by providing technical features to our portfolio of solutions, in order to make it straightforward for our customers to be compliant with GDPR (Biometrics, Access Control, Video).

Each element of sensitive data handled by the Suprema system is protected by the following mechanisms:

- Fingerprint / Face templates:

During the process of enrollment, the raw image of the fingerprint / face is never stored in the device or server. Instead, a template is created, which is also encrypted by 128bit AES, 256bit AES, DES/3DES depending on the location where it is stored (Device, Server, SmartCard).

Example of ANSI 378 format template

Standard format template should start with 0x46

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f		
00000000h:	46	40	52	00	20	32	30	00	00	E6	00	00	00	00	00	00		
00000010h:	01	00	01	40	00	C5	00	C5	01	00	00	00	64	21	40	7C		
00000020h:	00	16	61	00	40	BE	00	2A	A7	00	40	31	00	34	6E	00		
00000030h:	40	3E	00	4E	0F	00	40	3A	00	53	6E	00	80	98	00	61		
00000040h:	55	00	80	65	00	62	6E	00	80	83	00	62	08	00	40	54		
00000050h:	00	70	73	00	40	E4	00	7A	41	00	40	88	00	78	6A	00		
00000060h:	40	EA	00	78	90	00	80	0F	00	83	22	00	80	EE	00	88		
00000070h:	92	00	40	00	00	33	7F	00	80	1A	00	8A	00	00	40	14		
00000080h:	00	CA	83	Minutiae information										69	00	F0	7F	00
00000090h:	40	5B	00	72	2A	00	80	S7	01	11	35	00	80	6F	01	13		
000000a0h:	94	00	80	A1	01	13	30	00	80	2C	01	17	88	00	80	5B		
000000b0h:	01	1C	95	00	40	66	01	1C	34	00	80	77	01	22	3D	00		
000000c0h:	80	3B	01	25	94	00	40	4F	01	26	33	00	80	66	01	26		
000000d0h:	9A	00	40	55	01	27	8E	00	40	97	01	28	2F	00	40	92		
000000e0h:	01	33	34	00	00	00	00	00	00	00	00	00	00	00	00	00		

◀ Example of a Fingerprint Template (raw number)

- Secure communication* :

TCP communication of data within the system is secured with the use of TLS 1.2 (including SSL / HTTPS). This ensures that no sensitive data is compromised during the communication between the devices and the central server.

* Feature needs to be activated from Server

- Secure Tamper* :

Devices are equipped with a secure tamper feature, which ensures the security of data stored in the devices. If the device is removed from the wall and tampered with, the secure data (biometric templates, User ID, Logs) within the device will automatically be deleted.



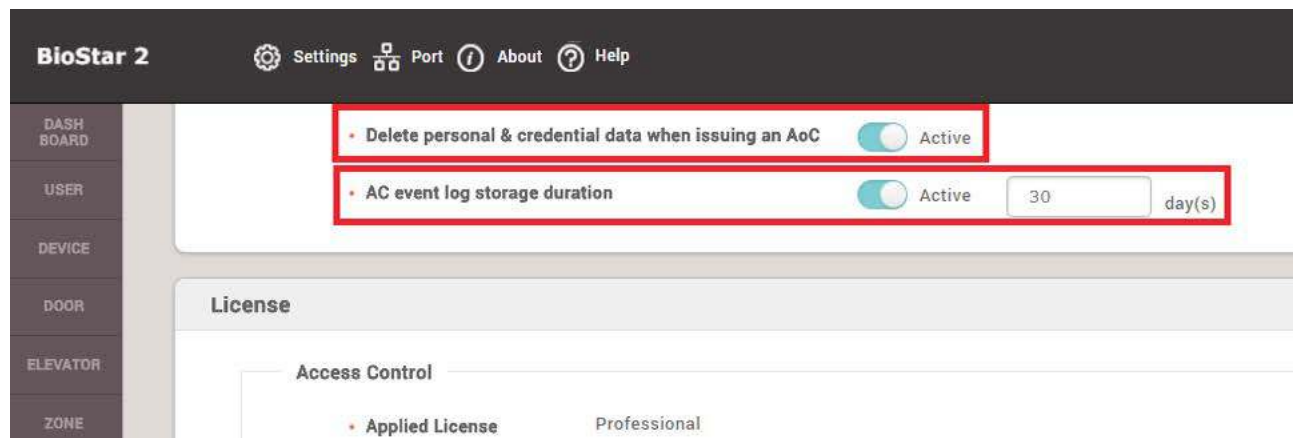
- Access on Card (AoC) :

All Suprema biometric readers are equipped with RFID technology. Smartcards allow for users credentials (fingerprint) to be stored and encrypted on the card chip. Suprema recommends the use of DesFire, EV1, EV2, HID Seos or Mifare Plus Smartcards or the use of Smartphone NFC/BLE emulated cards together with BioStar2 mobile App. The mode Authentication mode with template stored on SmartCard is called "Verification [1:1]" and explained in Suprema documentation as "Access on Card" (AoC).

Together with the AoC mode, BioStar 2 also proposes an option for Personal & Credential data not to remain in the central server after a successful AoC enrollment. So that the fingerprint templates that are encoded in the smartcard, encrypted and held by the Data-Subject himself are the only Biometric Data available (no other copy on Server/external devices remains).

- Event Log Management* :

In accordance with GDPR, Suprema makes it possible in BioStar 2 so that event logs and data stored in the server is automatically deleted after a certain period of time (set by the administrator). This is in line with the 'right to be forgotten' requirement in the GDPR.



△ Screenshot of the settings to automatically delete event logs

* Feature needs to be activated from Server

- BioStar 2 Application Account Settings (Accounts available by default and customizable):

In a company the System Installer, the Staff responsible for enrollment, the IT Managers, the Security Managers or the HR Managers do not all need to access the same level of data. In extension to GDPR, Suprema makes it possible in BioStar 2 to set up User Accounts that limits the scope of the right to access the Data Subject information.

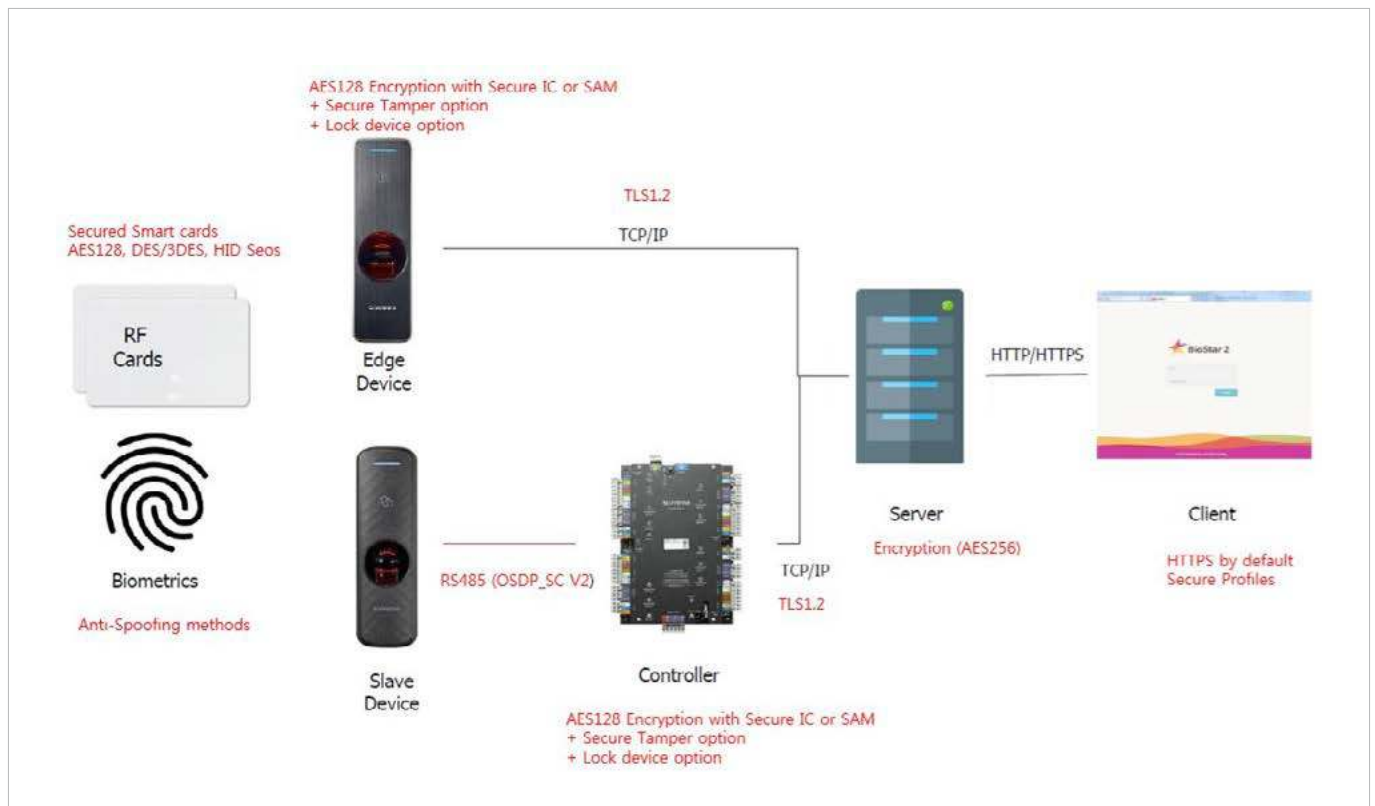
The screenshot displays the 'Security Operator' configuration page. On the left, a sidebar contains icons for 'DASH BOARD', 'USER', 'DEVICE', 'DOOR', and 'ELEVATION'. The 'USER' section is expanded, showing roles: Administrator, User Operator, Monitoring Operator, Security Operator, T&A Operator, and User. The main panel shows the 'Security Operator' settings. It includes a 'Name' field, a 'Description' field, and an 'Admin Menu Settings' section. Below this is a table with columns: Name, Custom Name, Add Button, Role, and Read. The table lists several operators, with two rows highlighted by red boxes. The first highlighted row is for a 'User' operator with 'All Users' and 'All Devices' selected in the dropdowns. The second highlighted row is for a 'Device' operator with 'All Devices' selected.

Furthermore, the Audit Trail allows one to know the different actions that have been taken by the Admin/Operators/Super Users in the BioStar 2 Software.

The screenshot displays the 'Audit Trail' page. The top bar shows 'BioStar 2' and navigation links: Settings, Port, About, Help. The left sidebar contains icons for 'DASH BOARD', 'USER', 'DEVICE', 'DOOR', 'ELEVATION', 'ACTION CONTROL', and 'REPORTS'. The main panel is titled 'Audit Trail' and includes a filter section with dropdowns for Date/Time, User, Operator Level, IP, Category, Target, and Action. Below the filter is a table with columns: Date/Time, User, Operator Level, IP, Category, Target, Action, and Modification. The table lists several actions, with one row highlighted by a red box. This row shows an 'Add' action for a 'Device' operator, with the target being 'BioStation 2 546832591 (19...)'. The 'Modification' column for this row is empty.

Security and Privacy by Design: From the Physical Door to the Client in premises Application

Below image summarizes all the measures taken by Suprema for the close respect of GDPR



△ Data protection mechanism in the BioStar 2 system

Please note that some of the security/privacy features are not switched on by default In BioStar 2. Please ensure that the administrator at the site is trained, that the DPO is aware and that the system installer has configured the Suprema system settings in order to ensure the GDPR compliance at its best.

Suprema would like to draw its customers' attention on the fact that configuring Suprema Inc Solutions the right way is not enough to get full compliance towards GDPR. GDPR hence requires the nomination by the company of a DPO, a Breach Notification process, Right to access rules, etc... Such requirement cannot be provided by Suprema and is under the sole responsibility of the Company.

If you have further questions/requirements about GDPR Compliancy with Suprema products, please check our Knowledge Base website – kb.supremainc.com ; or contact your local Suprema dealer.

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu,
Seongnam-si, Gyeonggi-do ZIP: 13554 Republic of Korea

T: +82-31-783-4502 E: sales_sys@supremainc.com

©2018 Suprema Inc. Suprema and identifying product names and numbers herein are registered trade marks of Suprema, Inc. All non-Suprema brands and product names are trademarks or registered trademarks of their respective companies. Product appearance, build status and/or specifications are subject to change without notice.

www.supremainc.com