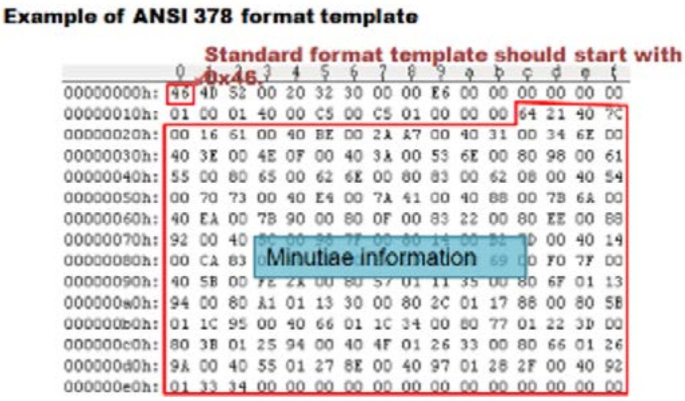
GDPR Compliance Statement

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

```
             0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
00000000h: 46 4D 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 7B 6A 00
00000060h: 40 EA 00 7B 90 00 80 0F 00 83 22 00 80 EE 00 88
00000070h: 92 00 40 [illegible] 00 40 14
00000080h: 00 CA 83 [illegible] 69 00 F0 7F 00
00000090h: 40 5B 00 7E 2A 00 80 57 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)

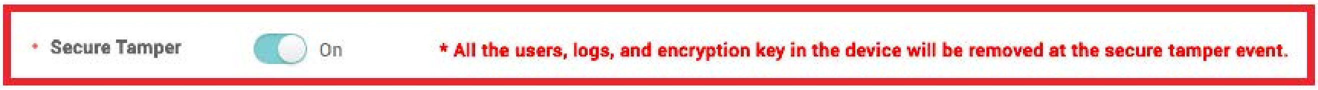
- Secure communication* :

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.



• Secure Tamper — On

* All the users, logs, and encryption key in the device will be removed at the secure tamper event.

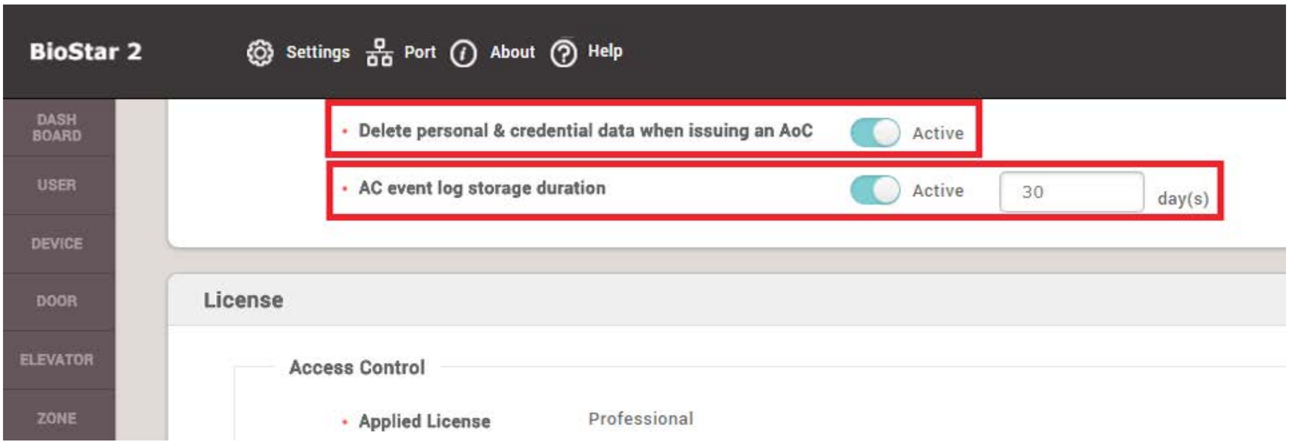
- Access on Card (AoC) :

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.



• Delete personal & credential data when issuing an AoC — Active

• AC event log storage duration — Active — 30 day(s)

License

Access Control

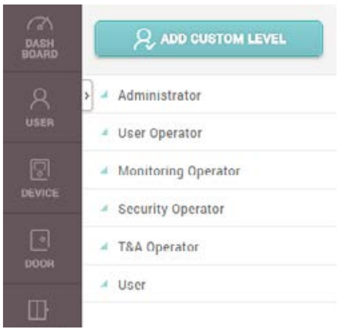
• Applied License — Professional

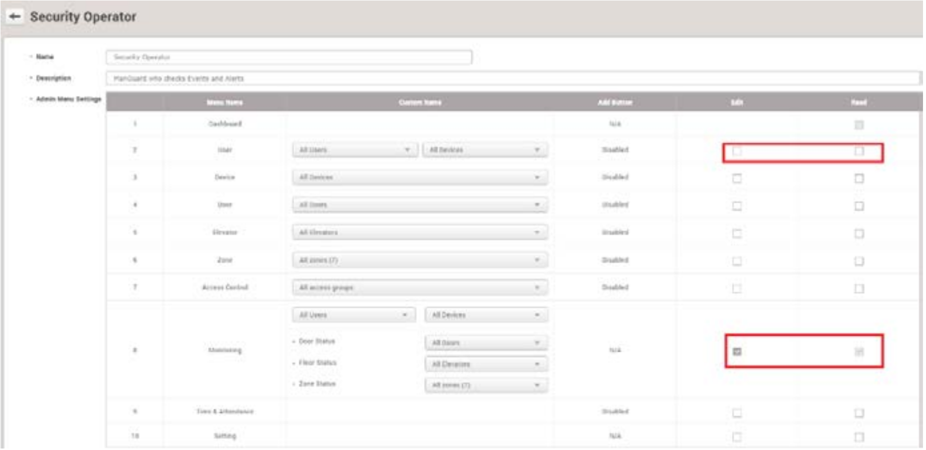
△ Screenshot of the settings to automatically delete event logs

* 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.

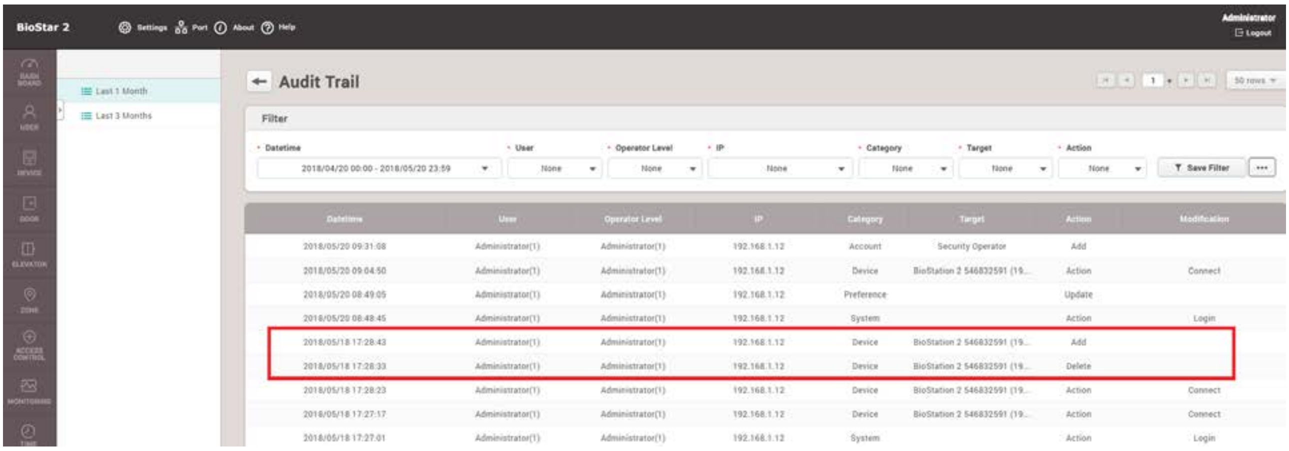



Security Operator

- Name: Security Operator
- Description: ManGuard who checks Events and Alerts
- Admin Menu Settings

	Menu Name	Custom Name	Add Button	Edit	Read
1	Dashboard		N/A		□
2	User	All Users All Devices	Disabled	□	□
3	Device	All Devices	Disabled	□	□
4	Door	All Doors	Disabled	□	□
5	Elevator	All Elevators	Disabled	□	□
6	Zone	All zones (7)	Disabled	□	□
7	Access Control	All access groups	Disabled	□	□
8	Monitoring	All Users All Devices Door Status: All Doors Floor Status: All Elevators Zone Status: All zones (7)	N/A	☑	☑
9	Time & Attendance		Disabled	□	□
10	Setting		N/A	□	□

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.



Audit Trail

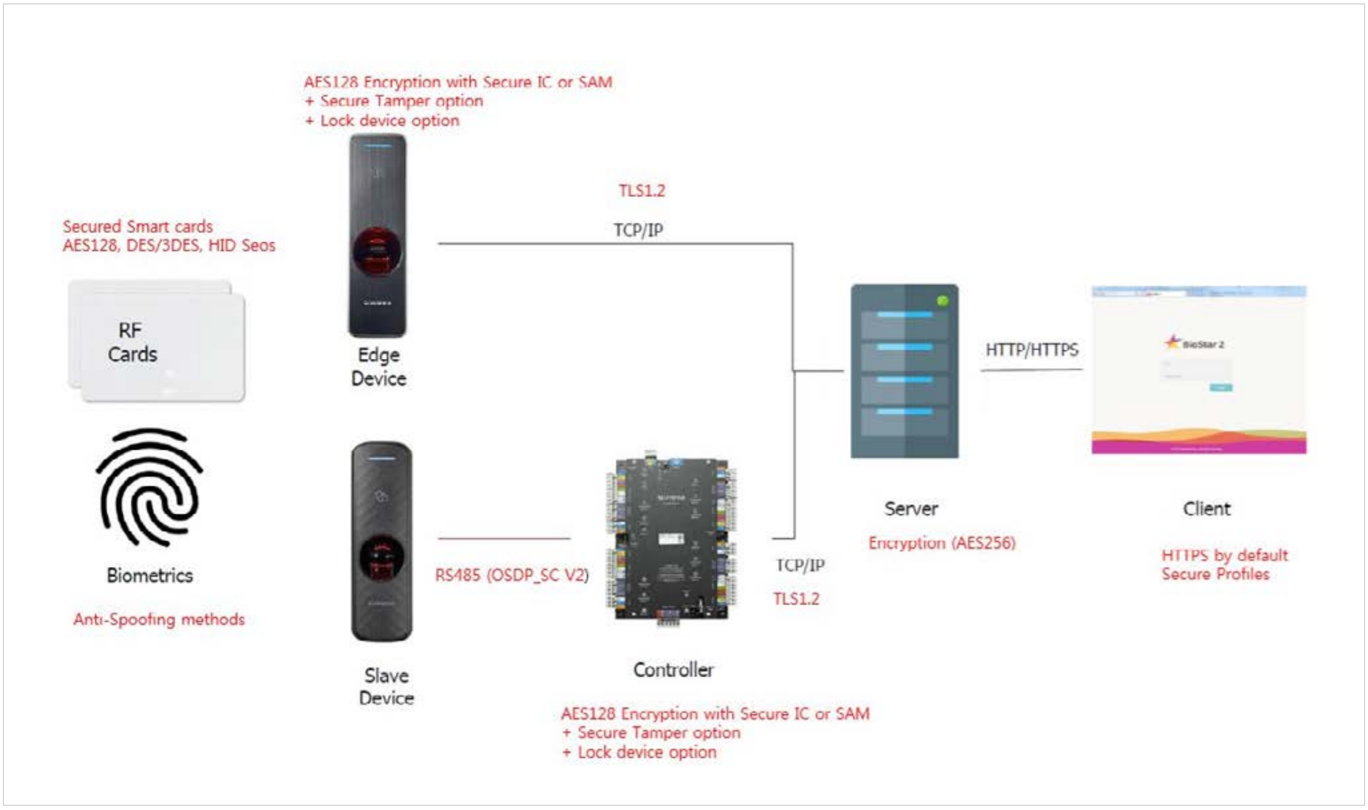
Filter

- Datetime: 2018/04/20 00:00 - 2018/05/20 23:59
- User: None
- Operator Level: None
- IP: None
- Category: None
- Target: None
- Action: None

Datetime	User	Operator Level	IP	Category	Target	Action	Modification
2018/05/20 09:31:08	Administrator(1)	Administrator(1)	192.168.1.12	Account	Security Operator	Add	
2018/05/20 09:04:50	Administrator(1)	Administrator(1)	192.168.1.12	Device	BioStation 2 546832591 (19...	Action	Connect
2018/05/20 08:49:05	Administrator(1)	Administrator(1)	192.168.1.12	Preference		Update	
2018/05/20 08:48:45	Administrator(1)	Administrator(1)	192.168.1.12	System		Action	Login
2018/05/18 17:28:43	Administrator(1)	Administrator(1)	192.168.1.12	Device	BioStation 2 546832591 (19...	Add	
2018/05/18 17:28:33	Administrator(1)	Administrator(1)	192.168.1.12	Device	BioStation 2 546832591 (19...	Delete	
2018/05/18 17:28:23	Administrator(1)	Administrator(1)	192.168.1.12	Device	BioStation 2 546832591 (19...	Action	Connect
2018/05/18 17:27:17	Administrator(1)	Administrator(1)	192.168.1.12	Device	BioStation 2 546832591 (19...	Action	Connect
2018/05/18 17:27:01	Administrator(1)	Administrator(1)	192.168.1.12	System		Action	Login

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.