Table of Contents

1.0.2 Version (V1.0.2)

Release

2021-01-05

New Features and Improvements

1. Improved the usability of Suprema Thermal Camera.

- Added minimum reference temperature setting function.
- Improved the user interface for the ROI.
- Improved temperature deviation in the room and low-temperature environments.
- Removed temperature bar from the temperature check screen.
- Changed the English function name for infrared emissivity.

2. Improved user interface for Suprema Thermal Camera and Mask Detection.

- Changed the notification, beeps, and voice guides.

3. Separated event logs of Mobile Access cards and RFID cards.

4. Added support for the option to toggle Screen Saver for slave devices.

5. Improved the Visual Face matching algorithm.

- Improved the issue where the detection UI was not displayed on the face recognition screen when the verification mode of Suprema thermal camera function was set to 'Check Only'.
- Improved the authentication performance when wearing masks.
- Improved the authentication performance for backlit, external light, and low-light use environments.
- Improved face detection performance.

Bug Fixes

1. The device stoped working when calling the BS2AuthConfig of a device using BioStar 2 Device SDK.

2. The slave device restarted abnormally when connected as master-slave.

3. The RS-485 disconnection log continuously occurred when Secure I/O 2 was connected.

4. Mask Detection and temperature measurement operations were not smooth when Dynamic ROI was set when the Check mode of the mask detection and Suprema Thermal Camera function was set to 'Check Only'.

5. An issue of Suprema Thermal Camera screen being maintained even when the thermal imaging

camera was toggled from 'Enabled' to 'Disabled'.

6. The device abnormally terminated when establishing a communication connection with 'Device→Server'.

7. The Wigand reader connected to the DM-20 operating from Lock to Unlock if the device was restarted when the device was connected as master-slave.

8. An issue that occurred when the device was restarted while the door was set to unlock manually, the door remained locked even after the restart was completed.

9. The Disarm button wss obscured by the device's fake face detection screen when the Intrusion Alarm Zone was set.

10. The Secure Tamper could not be manually turned off by the default hash key.

11. USB keyboard connection restriction to improve security vulnerabilities.

12. Fingerprint registered with AoC could be continuously authenticated with fingerprints without a card when sent to the device after changing them.

13. Image logs and count were not displayed properly in the event log.

14. The device abnormally restarted when attempting face recognition closer than the valid effective distance.