FaceLite

Firmware Revision Notes

Version 1.3.3

English

EN 301.00.FL V1.3.3

suprema

SECURITY & BIOMETRICS

Firmware Version 1.3.3 (Build No. 1.3.3_221118)

Release: 2022-11-24

Bug Fixes

1. Dot(.) is not entered when configuring **IP address** after configuring a specific menu (Affects version: v1.0.0).
2. When the LAN cable connected to the device is disconnected and reconnected, it takes a long time for IP to be assigned by DHCP (Affects version: v1.0.0).

Firmware Version 1.3.2 (Build No. 1.3.2_220207)

Release: 2022-02-09

New Features and Improvements

1. Supports a new BLE (Bluetooth Low Energy) chip.
   - The BLE chip part of the hardware have been changed, and the firmware has been upgraded to be compatible with both the existing and new BLE chips.

Firmware Version 1.3.1 (Build No. 1.3.1_211203)

Release: 2021-12-13

New Features and Improvements

1. Applied a code to compensate for the incorrect flag of the face template.
2. Improved security vulnerability,
   - Removed UDP port for debug.

Bug Fixes

1. Scanning a fingerprint to enroll on the slave device caused an error and failed enrollment (Affects version: v1.3.0).
2. Abnormal authentication failure occurred if a user authenticates with card+face or ID+face on the slave device when using server matching (Affects version: v1.2.0, v1.3.0).
3. Slave devices are disconnected when the master device is rebooted. (Affects version: v1.3.0 or earlier).
4. When enrolling a face, even though the device detected the user's face successfully, the color of the guideline on the screen was not displayed properly (Affects version: v1.3.0).
5. Abnormal authentication failure occurred when the slave device's auth mode was set to card+fingerprint (Affects version: v1.2.0 or later, v1.3.0 or earlier).

Firmware Version 1.3.0 (Build No. 1.3.0_210621)

Release: 2021-07-07

New Features and Improvements

1. Improved manually turning the secure tamper on or off even when the default hash key is set.
2. Upgraded to the 1.1.1i version of OpenSSL.
3. Separated event logs of Mobile Access cards and RFID cards.

Bug Fixes

1. The RS-485 communication did not work properly when connecting the device to a third-party controller after activating the Secure Communication mode. (Affects version: v1.2.0 or earlier)
2. The screen was abnormally displayed when the second user authentication was successful on a slave device with dual authentication. (Affects version: v1.2.0 or earlier)
3. After being disconnected from BioStar 2, an incorrect pop-up message was displayed until they were reconnected. (Affects version: v1.2.0 or earlier)
4. The device rebooted abnormally when the firmware version was upgraded to 1.2.0 after changing the slave device with firmware version 1.1.0 to a master device. (Affects version: v1.2.0 or earlier)
5. The relay operated as Off (Lock) after setting the scheduled unlock zone in the elevator and rebooting the master device. (Affects version: v1.2.0 or earlier)
6. All files in the database were deleted after exporting them to a USB. (Affects version: v1.2.0 or earlier)
7. The slave device rebooted abnormally. (Affects version: v1.2.0 or earlier)
8. The RS-485 disconnection log continuously occurred when Secure I/O 2 was connected. (Affects version: v1.2.0 or earlier)
9. The Wiegand reader operated as Unlock after setting the Wiegand reader connected to DM-20 to Lock and rebooting the device when using the device with DM-20. (Affects version: v1.2.0 or earlier)
10. The door remained locked and did not open after rebooting the device when it was set to Manual Unlock. (Affects version: v1.2.0 or earlier)
11. Ten administrators were still not deleted from the device when initializing the device that has 1,000 assigned administrators. (Affects version: v1.2.0 or earlier)
12. An improper error message was displayed when a user who only registered a card scanned the card after setting the authentication mode to Card + Face / PIN on the device. (Affects version: v1.2.0 or earlier)
13. When enrolling a new fingerprint to AoC, it was able to authenticate the user with both the new fingerprint data and the existing fingerprint data. (Affects version: v1.2.0 or earlier)

Firmware Version 1.2.0 (Build No. 1.2.0_201020)

Release: 2020-11-04

Main Fixes

1. Logs generated while the device is disconnected are not sent to BioStar 2, even after the device is reconnected.

New Features and Improvements

1. Added feature to change device ID.
2. Enhancement in the security of the device.
   - Restrict unencrypted connections.
   - Enhancement in security of encryption keys.
   - Encrypt and migrate user information.
3. Improved Anti-passback zone to operate based on the door status.
4. Improved the scheduled unlock zone function for each floor when controlling elevator.
5. Supports server matching.
6. Supports the Mobile Access V1.1.
7. Improved the face recognition algorithm for users with glasses.
8. Supports the new face template.
   * If the firmware of the face recognition device connected as a slave is the latest version (FaceStation 2: 1.4.0 or later, FaceLite: 1.2.0), authentication may fail because it is not compatible with the existing template.
9. Increased maximum number of users (1:N).
   - Before: 3,000
   - After: 4,000
10. Supports new device.
    - XPass D2 (Rev 2)

Bug Fixes

1. Connection status icon was not displayed when connecting RS-485.
2. Modified that the authentication mode of the slave device is set according to the setting of the master device.
3. Card data is output with wrong BitCount when the device is connected to a 3rd-party system via OSDP.
4. An OSDP security session error occurred when connecting OM-120 and XPass D2 as a slave device.
5. An error in the master-slave connection occurred due to the RS-485 communication key.
6. After a global anti-passback violation, an authentication success log occurred twice.
7. PIN authentication failed.
8. After the message ‘Invalid payload’ occurred on the slave device, it was disconnected abnormally and reconnection was impossible.
9. When Factory Default was performed using SDK, the device resource (logo image) did not initialize.
10. Device reboots or a timeout occurs when upgrading firmware or transferring user data during SSL secure communication.
11. It was unable to edit, delete or add an authentication mode.
12. When the delay for the output signal occurred repeatedly, the device did not work properly.
13. The output port of the BioStation 2 could not be set in the trigger & action.
14. Modified the sensor setting API related to face registration and authentication.
15. When a user authenticated on the slave device using a smart card or the face, the master device would reboot.
16. When a user authenticated the fingerprint after setting the byte order as LSB and the Wiegand output information as the user ID, the device would reboot.
17. Improved the device to recognize unknown cards by selecting the card type options.

Firmware Version 1.1.0 (Build No. 1.1.0_190809)

Release: 2019-08-16

Main Fixes

1. The master device abnormally shuts down if it is operated after reconnecting a disconnected slave device.
2. The master device reboots abnormally when a user authenticates the face to the slave device continuously.
3. The master device abnormally shuts down if the RS-485 mode of the master device is changed after disconnecting the 31 connected slave devices.

New Features and Improvements

1. OSDP Standardization
   - Improved to comply with OSDP V2.1.7 protocol when connecting with 3rd-party controllers.
2. Increase of the number of administrators that can be added.
3. Support to the Clear APB for each user.
4. Supports options by card type.
5. Increase of the maximum number of floor levels to up to 2,048.
6. Change the way new settings are applied when adding administrators using batch edit of devices.
   - Before: Overwrite a new setting to existing settings.
   - After: Add a new setting to existing settings.
7. Supports the duplicate face check when registering users on a device.
8. Supports setting options for Wiegand authentication result output.
   - User ID and Card ID
9. Supports Anti-Tailgating at doors.
10. If the data transmission fails when communicating with OSDP, it is transmitted again.
11. Improves the Enhanced fake face enrollment block.
12. Support for RS-485 connections to new devices
    - XPass 2(XP2-MDPB, XP2-GDPB, XP2-GKDPB)

Bug Fixes

1. If the value of menu timeout is shorter than the auth timeout, a pop-up for success or fail does not occur when an T&A pop-up message is output after authentication.
2. 64GB exFAT USB memory device is not recognized normally.
3. The device does not recognize AoC authentication.

Firmware Version 1.0.1 (Build No. 1.0.1_190724)

Release: 2019-07-25

Bug Fixes

1. Issue that camera image is output darkly in production mode.

Firmware Version 1.0.0 (Build No. 1.0.0_190611)

Release: 2019-06-11

Initial firmware developed.

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA
Tel: +82 31 783 4502 | Fax: +82 31 783 4503 | Inquiry: sales_sys@supremainc.com

For more information about Suprema's global branch offices,
visit the webpage below by scanning the QR code.
https://supremainc.com/en/about/global-office.asp