FaceStation 2

RELEASE NOTES

Version 1.5.5

English
EN 301.00.FS2

suprema
SECURITY & BIOMETRICS

CONTENTS

- Firmware Version 1.5.5
- Firmware Version 1.5.4
- Firmware Version 1.5.3
- Firmware Version 1.5.2
- Firmware Version 1.5.1
- Firmware Version 1.5.0
- Firmware Version 1.4.2
- Firmware Version 1.4.1
- Firmware Version 1.4.0
- Firmware Version 1.3.1
- Firmware Version 1.3.0
- Firmware Version 1.2.1
- Firmware Version 1.2.0
- Firmware Version 1.1.1
- Firmware Version 1.1.0
- Firmware Version 1.0.4
- Firmware Version 1.0.3
- Firmware Version 1.0.2
- Firmware Version 1.0.1
- Firmware Version 1.0.0

Firmware Version 1.5.5 (Build No. 1.5.5_240821)

Release | 2024-08-26

> **Caution**
> For devices with the new SE processor, after upgrading the firmware to v1.5.3 or higher, you cannot downgrade to a lower version and downgrade the firmware customized in the lower version.
>
> Devices with existing SE processor can be downgraded to a lower version.
>
> For more information, check the serial number of the device and contact the Suprema.

New Features and Improvements

1. Improved to get user update succeeded event log using the GetLogWithFilter function in the SDK.
2. Improved to ensure that values set with osdp_comset are correctly applied on the device connected as a slave.

Bug Fixes

1. Authentication result is displayed when accessing the admin menu via facial authentication. Affects version: 1.5.2
2. The user ID stored as a 32-character string is truncated to only 31 characters in a specific event log. Affects version: 1.0.0
3. When a user with a 32-character user ID authenticates to the device while the device is not connected to the server, the authentication event log is not updated in BioStar 2 even after the device is reconnected to the server. Affects version: 1.0.0
4. Deleted image logs from the device gets continuously uploaded to the server. Affects version: 1.5.2
5. When entering the **Wireless**, duplicate SSID are displayed. Affects version: 1.0.0

Firmware Version 1.5.4 (Build No. 1.5.4_230927)

Release | 2023-10-24

> **Caution**
> For devices with the new SE processor, after upgrading the firmware to v1.5.3 or higher, you cannot downgrade to a lower version and downgrade the firmware customized in the lower version.
>
> Devices with existing SE processor can be downgraded to a lower version.
>
> For more information, check the serial number of the device and contact the Suprema.

New Features and Improvements

1. Improved to select and update only the desired information when updating user information. (Compatible with BioStar v2.9.0 or higher)

Bug Fixes

1. When authenticating with a BLE mobile card running on iOS, authentication fails and the device restarts intermittently. Affects version: 1.4.0
2. Deleting all users included in an access group in BioStar 2 does not delete the access group from the device's user information. Affects version: 1.0.0
3. Device does not recognize certain HID iCLASS Seos cards. Affects version: 1.0.0
4. Door Locked event occurs when input signal gets detected while configured to Arm/Disarm by input signal. Affects version: 1.0.0
5. Intermittently, the door does not open even if authentication succeeds when the door uses the slave device's relay. Affects version: 1.0.0
6. When a user registered in BioStar 2 is sent to the device and authenticated with a face or card, the user is intermittently not authenticated and the device restarts. Affects version: 1.0.0
7. Restart log is not logged in the device's **Event Log** when the master device is restarted. Affects version: 1.5.3
8. Global APB behavior for the same input was different depending on firmware version. Affects version: 1.5.0
9. When the device with the working **Screen Saver** is not used for a long time, a black screen occurs and the device freezes. Affects version: 1.4.0

10. Device abnormally restarts when changing the device's **Network** settings in BioStar 2. Affects version: 1.0.0

Firmware Version 1.5.3 (Build No. 1.5.3_221005)

Release | 2022-11-01

> **Caution**
> For devices with the new SE processor, after upgrading the firmware to v1.5.3 or higher, you cannot downgrade to a lower version and downgrade the firmware customized in the lower version.
>
> Devices with existing SE processor can be downgraded to a lower version.
>
> For more information, check the serial number of the device and contact the Suprema.

New Features and Improvements

1. Supports the dual SE processor.

Bug Fixes

1. Migration malfunction occurs when the firmware is upgraded from v1.3.1 or earlier to v1.4.0 or later. Affects version: 1.4.0
   - Migration did not complete and the device boots to the main screen, some keys do not work or an abnormal screen is displayed.
2. Intermittently, the image log is logged abnormally. Affects version: 1.4.2
3. Mobile card authentication suddenly does not work. Affects version: 1.4.0
4. When using the card to authenticate to the device, the card that was normally authenticated fails intermittently. Affects version: 1.0.0
5. Device does not boot correctly. Affects version: 1.0.0
6. Device abnormally restarts when **Image Log** is **Enabled** and image log is logged on the device. Affects version: 1.5.1
7. User ID information was not included when using the BS2_GetLogSmallBlobEx function in the SDK to load the event log for the device's mask detection and temperature measurement operation. Affects version: 1.0.0
8. Device does not recognize certain HID iCLASS Seos cards. Affects version: 1.0.0

Firmware Version 1.5.2 (Build No. 1.5.2_220614)

Release | 2022-06-16

New Features and Improvements

1. Improved to check for the duplication of cards registered with users when transmitting user data from the server to devices.

Bug Fixes

1. The 'Delete the Root Certificate' was not displayed when a user with the administrator level accessed the menu on the device where the certificate was stored. Affects version: 1.1.1
2. Abnormal continuous authentication occurs when using the thermal camera. Affects version: 1.4.0
3. When initializing the master device with the 'Keep Network Settings' option, the RS-485 communication key was initialized and the slave device was disconnected. Affects version: 1.0.0
4. When loading the logs for the user who entered the admin menu using the SDK, the user ID was not displayed. Affects version: 1.0.0
5. 'Device → Server' connection did not work intermittently. Affects version: 1.4.0
6. If some ports of the OM-120 connected as a slave are set as a door relay and the device is rebooted, the relay was operated abnormally. Affects version: 1.0.0
7. The device rebooted abnormally when a user scanned a card on the device with several cards overlapped in a wallet or the like. Affects version: 1.0.0
8. The user did not touch the device's touchscreen, but an abnormal touch behavior occurred on the device. Affects version: 1.5.0
9. If the user authenticated on the device at the time of Auth Timeout, it was authenticated, but the door was not opened. Affects version: 1.4.0
10. Unable to edit Subnet Mask value on device. Affects version: 1.4.0
11. PIN authentication did not work properly when using Device Hashkey Management. Affects version: 1.4.0
12. The user ID was abnormally displayed in the event log if the user authenticated with AoC set as the blacklist card when the User ID Type was set to Alphanumeric. Affects version: 1.0.0
13. When authenticating on a device that has dual authentication set up, the authentication success sound is not output for

the dual authentication result, and the home screen is maintained. Affects version: 1.5.0

14. When authenticating on a device that has dual authentication set up, if the second user failed to authenticate, the failure message was displayed twice. Affects version: 1.5.1

15. When viewing the event log, the date selection pop-up window did not disappear even after the Menu Timeout. Affects version: 1.0.0

16. When setting the elevator to the scheduled unlock zone and using the 'Started by User Authentication' option, the floor is activated normally when a user belonging to the access group authenticates, but the 'Floor released' logs are output. Affects version: 1.0.0

17. When the LAN cable was removed and reconnected, it took a long time to receive the DHCP IP assignment. Affects version: 1.0.0

18. False Acceptance (FA) occurred continuously. Affects version: 1.5.0

Firmware Version 1.5.1 (Build No. 1.5.1_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: 1.5.0
2. The device failed to recognize the iCLASS Seos card suddenly (FS2-AWB). Affects version: 1.5.0 or earlier
3. Abnormal authentication failure occurred if a user authenticates with card+face or ID+face on the slave device when using server matching. Affects version: 1.5.0 or earlier
4. Slave devices are disconnected when the master device is rebooted. Affects version: 1.5.0 or earlier
5. Abnormal authentication failure occurred when the slave device's auth mode was set to card+fingerprint. Affects version: 1.4.0 or later, 1.5.0 or earlier

Firmware Version 1.5.0 (Build No. 1.5.0_210628)

Release | 2021-07-08

Main Fixes

1. Incorrect temperature was displayed when authenticating from a slave device with the thermal camera. Affects version: 1.4.0, 1.4.1, 1.4.2

New Features and Improvements

1. Occupancy limit zone support
2. Added support for the option to toggle Screen Saver for slave devices.
3. Improved manually turning the secure tamper on or off even when the default hash key is set.
4. Separated event logs of Mobile Access cards and RFID cards.
5. Improved that the thermal camera works first when both the thermal camera and Wiegand bypass are set.
6. Changed to a new touch pad
   - For devices with firmware version 1.4.2 or earlier, please follow the instructions below when replacing the front cover (touch pad).
     - Replace the front cover after upgrading the firmware to version 1.5.0 or later.
     - If you have already replaced the front cover before upgrading the firmware to version 1.5.0 or later, please upgrade to the latest version firmware again.

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: 1.4.2 or earlier
2. A large number of 'Door closed' logs occurred abnormally when the door sensor was set to the input port of Secure I/O 2 connected as a slave device.
3. Added defensive code to initialize if an error in the IR LED value occurs. Affects version: 1.3.0 or earlier
4. The screen was abnormally displayed when the second user authentication was successful on a slave device with dual authentication. Affects version: 1.4.2 or earlier
5. An abnormal event log occurred when the temperature measurement failed after setting the temperature mode to 'Temperature Check Before Authentication'. Affects version: 1.4.0, 1.4.1, 1.4.2

6. An abnormal event log occurred when measuring temperature after setting the temperature mode to 'Check Temperature Only'. Affects version: 1.4.0, 1.4.1, 1.4.2
7. The changed settings were reflected in the log but were not displayed properly on the screen when the time and attendance code settings were changed. Affects version: 1.4.2 or earlier
8. The relay operated as Off (Lock) after setting the scheduled unlock zone in the elevator and rebooting the master device. Affects version: 1.4.2 or earlier
9. The performed action, such as temperature output, was different from the intended action responding to the input signal set in the Trigger & Action feature when using the Suprema Thermal Camera. Affects version: 1.4.0, 1.4.1, 1.4.2
10. An issue of Suprema Thermal Camera screen being maintained even when the thermal imaging camera was toggled from 'Enabled' to 'Disabled'. Affects version: 1.4.0, 1.4.1, 1.4.2
11. The device abnormally terminated when establishing a communication connection with 'Device → Server'. Affects version: 1.4.2 or earlier
12. All files in the database were deleted after exporting them to a USB. Affects version: 1.4.2 or earlier
13. The slave device rebooted abnormally. Affects version: 1.4.2 or earlier
14. The RS-485 disconnection log continuously occurred when Secure I/O 2 was connected. Affects version: 1.4.2 or earlier
15. Ten administrators were still not deleted from the device when initializing the device that has 1,000 assigned administrators. Affects version: 1.4.2 or earlier
16. Device registration using Mobile Access app does not work on dynamic sites. Affects version: 1.4.2 or earlier
17. 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: 1.4.2 or earlier
18. 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: 1.4.2 or earlier
19. The door relay status was not displayed properly when rebooting the master device while Manual Lock or Manual Unlock was set. Affects version: 1.4.2 or earlier

Firmware Version 1.4.2 (Build No. 1.4.2_210409)

Release | 2021-04-12

New Features and Improvements

1. Replaced with a new LCD screen
    - After upgrading a firmware to v1.4.2, you cannot downgrade the firmware to the previous version that includes the kernel and U-Boot.
2. Added minimum and maximum threshold temperature functions.
    - Temperature input range: 1–45℃
    - Default value of minimum threshold temperature: 32℃

Bug Fixes

1. The thermal camera froze up when updating resources via BioStar 2.

Firmware Version 1.4.1 (Build No. 1.4.1_210203)

Release | 2021-02-16

New Features and Improvements

1. Suprema Thermal Camera (TCM10-FS2) SDK Revision
    - FPS 8.3 applied
    - The management service is separated to recover the system safely after the device stops working abnormally.
    - The infrared image motion stopped working or the device was restarted while using the thermal camera.
    - The specifications of captured image buffer were modified.
2. Renamed the thermal camera's feature (English only)
    - Before: Emission Rate
    - After: Emissivity

Bug Fixes

1. Disconnected logs frequently occurred when the device was used with Secure I/O 2. Affects version: 1.4.0 or earlier
2. Doors were not applied in the open state when the device was restarted with the door set to manual open mode. Affects version: 1.4.0
3. The Secure Tamper could not be manually turned off by the default hash key. Affects version: 1.4.0

Firmware Version 1.4.0 (Build No. 1.4.0_200918)

Release | 2020-09-28

Main Fixes

1. When all or user data were exported to a USB and then the user data were imported again after upgrading the device firmware, the event log was deleted.
2. 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. Supports the thermal camera.
8. Supports the Screen Saver.
9. Improved the face authentication algorithm for users with glasses.
10. Supports the new face template.
    - Face templates scanned or enrolled on devices with the firmware version 1.4.0 or later are not compatible with devices with firmware version 1.3.1 or earlier, and authentication may fail due to this incompatibility.
    - If the firmware of the face authentication 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.
11. Increased maximum number of users (1:N:).
    - Before: 3,000
    - After: 4,000
12. Supports new device.

- XPass D2 (Rev 2)

Bug Fixes

1. Modified that the authentication mode of the slave device is set according to the setting of the master device.
2. Authentication of fingerprints registered as duress fingerprints failed on the BioStation A2 connected as a slave device.
3. Card data is output with wrong BitCount when the device is connected to a 3rd-party system via OSDP.
4. The automatic Wi-Fi connection function did not work.
5. Some or all of the image log colors appear garbled.
6. It recognized registered users as unregistered when accessing job codes with assigned cards.
7. Device reboots if the face of an existing registered user is changed when the number of registered users is the maximum.
8. An OSDP security session error occurred when connecting OM-120 and XPass D2 as a slave device.
9. An excess error occurred when registering new user faces or editing registered users even though the number of registered faces did not reach the maximum capacity.
10. The registered user data disappeared and the device rebooted if a user attempted to register a card when the number of registered users was at maximum capacity.
11. An error occurs when matching with groups when there are 5,000 users and 5 user groups are used.
12. The slave device did not work with group matching even though the group matching was set in the master device.
13. When an administrator is resent from a device with a new firmware applied, it is recognized as an unregistered user and cannot enter the administrator menu.
14. An error in the master-slave connection occurred due to the RS-485 communication key.
15. After a global anti-passback violation, an authentication success log occurred twice.
16. After the message 'Invalid payload' occurred on the slave device, it was disconnected abnormally and reconnection was impossible.
17. When a locked device was rebooted for an RS-485 connection, the slave device became unlocked.
18. When Factory Default was performed using SDK, the device resource (logo image) did not initialize.
19. Device reboots or a timeout occurs when upgrading firmware or transferring user data during SSL secure communication.
20. It was unable to edit, delete or add an authentication mode.
21. When the delay for the output signal occurred repeatedly, the device did not work properly.
22. The output port of the BioStation 2 could not be set in the trigger & action.

23. Device tried to connect to an NTP server.
24. Device worked as DHCP even though the static IP and daylight-saving mode were set.
25. Infrared camera continues to activate abnormally when low light and authentication mode is set.
26. When a user authenticated on the slave device using a smart card or the face, the master device would reboot.
27. 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.
28. Device reboots when registering user faces.
29. Improved the device to recognize unknown cards by selecting the card type options.
30. Once a card had been registered on the Wiegand output device, the device would not work properly when trying to output data using a fingerprint registered to another user.

Firmware Version 1.3.1 (Build No. 1.3.1_200422)

Release | 2020-04-27

Bug Fixes

1. Changed the firmware downgrade policy.
    - The kernel of the firmware before the touch panel is replaced has been changed not to downgrade.
2. Adjusted the brightness of the IR LED.

Firmware Version 1.3.0 (Build No. 1.3.0_190805)

Release | 2019-09-25

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. Add the event items to IMAGE LOG menu.
7. 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.
8. Supports the duplicate face check when registering users on a device.
9. Supports setting options for Wiegand authentication result output.
    - User ID and Card ID
10. Supports Anti-Tailgating at doors.
11. If the data transmission fails when communicating with OSDP, it is transmitted again.
12. Improves the Enhanced fake face enrollment block.
13. Improves the usability.
    - expanded the area of the menu button.
14. Support for RS-485 connections to new devices

- XPass 2 (XP2-MDPB, XP2-GDPB, XP2-GKDPB)

Bug Fixes

1. When upgrading firmware using USB, upgrade fails due to a timeout.
    - Change the timeout from 90 seconds to 5 minutes.
2. Scanning a deleted card to the device causes the device to restart abnormally.
3. The device recognizes the iCLASS Seos card as a CSN card.
4. Importing user data exported from BioStation A2 causes the device to restart abnormally.
5. Start time is not applied in UTC when importing filtered logs using SDK.
6. Relay works after reconnecting for authentication that occurred when elevator connection is disconnected.
7. Access is denied and user ID is displayed abnormally when using a smart card or fingerprint authentication in One Device Mode.
8. The Wiegand output data are transmitted in duplicate.
9. A delay occurs in opening the door when authentication succeeds, and the device UI is generally slow to respond.

Firmware Version 1.2.1 (Build No. 1.2.1_190115)

Release | 2019-01-23

Main Fixes

1. When the server private message is activated on the device, the device does not operate normally if there is no registered authentication message.

Bug Fixes

1. A white line appears on the LCD screen.

Firmware Version 1.2.0 (Build No. 1.2.0_181119)

Release | 2018-11-29

Main Fixes

1. When attempting to connect to a wireless LAN, if a user deletes and saves the IP address and gateway, the device restarts repeatedly.
2. When Micom is reset, the output does not restore to its previous status.
3. Wiegand Out is not output when authenticating with blacklist card.
4. With Bypass enabled, authentication failure message is not displayed when unregistered ID is authenticated.
5. Authentication fails because the server matching enabled for RFID cards and IDs.
6. The user cannot issue a new File after the App and File are created when issuing the DESFire card.
7. The device reboots if a user authenticates the RFID card or face consecutively on the device.
8. If using Group Matching, the device displays the group name as None when authenticating a face.
9. A code is added to prevent the authentication fails because the cache memory is broken.

New Features and Improvements

1. Support to AES encryption type for DESFire card.
2. Support to DESFire/DESFire EV1 Advanced option.
3. Support to the creation of up to 2048 Access Levels and Access Groups.
4. If a user is registered, modified, or deleted, the event log shows whether the editing was done on the server or on the device.
5. If the data transmission fails when communicating with OSDP, it is transmitted again.
6. Improves the data protection.
    - Increase the items to encrypt the data.
    - Support to setting the period for storing the personal information.
    - Support for additional features in Secure Tamper: Delete Users, Logs, Data Encryption Key, SSL certificate, and Smart Card Layout when a secure tamper event occurs.
7. Change the maximum value of the width for the Wiegand Input.
8. Support to the number of users, fingerprints, faces, and cards in Manage Users in Device.
9. Support for Individual Authentication Successful Messages and Working alarm time reports.

10. When using The bypass, The card ID is output as Wiegand even though a user authenticates with the AoC.

Bug Fixes

1. The relay does not work even though a user successfully authenticated the face on the device.
2. The relays operate differently from the previous status if the slave device is reconnected.
3. Modified the firmware of that slave device so that it cannot be upgraded when a device not supported by the master device is connected as a slave.
4. With Bypass enabled, the device does not respond even if a user selects the Menu, T & A, or ID after authentication.
5. Change some special characters (\, /, :, *, ?, ", ', `, <, >, |, .) to be unavailable when setting a user name.
6. The setting value is not saved when Face Config is set to the slave device.
7. The device(FS2-D) intermittently reboots.
8. If a user authenticates the card to XPass D2 connected to as a slave device, the beep sounds twice.
9. 1: N authentication can also be added on the slave device even though the master device is only capable of 1: 1 authentication.
10. If the user uses the BS_GetLogBlob command to get the door ID, the door ID is not output normally.

Firmware Version 1.1.1 (Build No. 1.1.1_180801)

Release | 2018-08-10

New Features and Improvements

1. Improves RFID card read range in Factory mode.

Firmware Version 1.1.1 (Build No. 1.1.1_180705)

Release | 2018-07-23

New Features and Improvements

1. Support the bypass mode through Wiegand output on smart cards.
    - Bypass mode: It makes the device send out Card Data to 3rd party device without making an authentication. With this mode, the device works as a dummy device, and card data only can be transmitted through Wiegand.
2. Support the issuance of Secure Credential Card without the fingerprints when registering iCLASS 2K card.
3. Improves RFID card read range.
4. Support for connecting new devices.
    - FaceStation 2(FS2-DS), BioLite N2(BLN2-PAB), XPass D2(XPD2-GDB, XPD2-GKDB)

Bug Fixes

1. The bypass does not work when authentication with AoC in Wiegand output.
2. Event logs and real-time logs are not uploaded normally to BioStar 2.
3. The device's time is kept in daylight saving time even after the set daylight saving time is over.
4. The device does not work as set for relay alarms when connecting Secure I/O 2 as a slave to the device.
5. User Export is executed even though there is no saved user.
6. The arm/disarm key is displayed on a device not included in Intrusion Alarm Zone.
7. Wiegand Reader could not be unlocked.
8. The device restarts when authenticating on the slave device with an unregistered fingerprint.
9. An empty file is created when running USB Export, even though there is saved data.
10. The device cannot read CSN because the card recognized as an NFC tag.
11. All users are deleted in BioStar 2 if running USB Import when there are users.
12. "USB Connection Fail" message is displayed when the encryption key does not match during data import.
13. The device recognizes the smart card as a CSN card when changing the primary key of the smart card to the secondary key.

Firmware Version 1.1.0 (Build No. 1.1.0_180304)

Release | 2018-03-26

New Features and Improvements

1. Support the intrusion alarm zone, Interlock zone and Muster zone.
2. Support the Ethernet zone.
    - Ethernet zone: The zone master role is performed by a master device, not the BioStar 2 server, and establishes the zone using Ethernet communication between the devices.
    - Except Fire Alarm Zone.
3. Support Daylight Saving Time setting.
4. Improves Trigger & Action for duress finger.
5. Improves Private Authentication on AoC.
6. Add and change the function that import & export USB logs and users to be compatible with BioStar 2 V2.6.
    - Before: Provided a folder such as Device Type_Device ID_YYMMDD_HHMM.
    - After: Provides a compressed file such as BioStar2_YYYYMMDD_HHMMSS.tgz.
    - Beginning with V2.6.1 on BioStar 2 platform.
7. Improves to handle the encryption key of the important information stored in database differently from server to server.
8. Support One Device Mode(Legacy).
9. Improves the ability to set the user ID type in SIP server
    - Support number and alphanumeric options for entering up to 32 characters.
10. Support simultaneous use of Wiegand input and output.
11. Support the secure tamper.
12. Support fingerprint enrollment on slave device.
13. Improves user transfer speed.
14. Support SEOS smart cards (Elite Key).
15. Improves performance of SEOS smart card RF reading.
16. Performs the AoC matching when connected to a master device as a slave device.
17. Support Enhanced fake face enrollment block.
18. Support for connecting new devices.

- BioLite N2, XPass D2, BioEntry P2, BioEntry R2

Firmware Version 1.0.4 (Build No. 1.0.4_180116)

Release | 2018-01-17

New Features and Improvements

1. Changed the Touch IC firmware and the kernel changed by firmware difference
2. Adjusts the camera calibration offset due to Window PET film changes.

Firmware Version 1.0.3 (Build No. 1.0.3_171017)

Release | 2017-10-25

New Features and Improvements

1. **Backward Compatibility (Enrollment v1.0.1)** menu added for the compatibility of face template enrolled in firmware version 1.0.1 or older.

Firmware Version 1.0.3 (Build No. 1.0.3_170919)

Release | 2017-09-19

Bug Fixes

1. Issue where the device transfer to server the previous firmware version information after upgrading the firmware.

Firmware Version 1.0.2 (Build No. 1.0.2_170830)

Release | 2017-09-04

New Features and Improvements

1. Improved face authentication algorithm
2. Improved authentication UI
3. Support validation of the device settings.

Bug Fixes

1. Issue where the device when using VoIP video phone.
2. Issue where the device does not connect to the external network.
3. Issue where the device is malfunctioned when device log is full.

Firmware Version 1.0.1 (Build No. 1.0.1_170515)

Release | 2017-05-17

New Features and Improvements

1. Improved face extraction algorithm for user who wear glasses
2. Improved motion detection algorithm

Bug Fixes

1. Issue where the master device reboots when fingerprint authentication is performed continuously on the slave device

Firmware Version 1.0.0 (Build No. 1.0.0_170330)

Release | 2017-03-30

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

© 2026 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.