BioStation A2

Firmware Revision Notes

Version 1.9.3

English

EN 301.00.BSA2

suprema

SECURITY & BIOMETRICS

Firmware Version 1.9.3 (Build No. 1.9.3_240307)

Release: 2024-03-13

Firmware Repackaging

Firmware Version 1.9.2 (Build No. 1.9.2_240129)

Release: 2024-01-31

New Features and Improvements

1. Modified to limit downgrade based on the hardware version of the device.
   - Devices with hardware v1.1.0 or higher cannot downgrade firmware to versions lower than v1.9.2.
     The hardware version can be checked in the **Device Info** menu of the device or in the **DEVICE** menu of BioStar 2.

Firmware Version 1.9.1 (Build No. 1.9.1_220113)

Release: 2022-03-04

Bug Fixes

1. When initializing the master device with the 'Without Network' option, the RS-485 communication key was initialized and the slave device was disconnected (Affects version: v1.0.0).
2. Slave devices are disconnected when the master device is rebooted (Affects version: v1.0.0).
3. The device failed to recognize the iCLASS Seos card intermittently before rebooting the device (BSA2-OIPW) (Affects version: v1.0.0).
4. When loading the logs for the user who entered the admin menu using the SDK, the user ID was not displayed (Affects version: v1.0.0).
5. 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: v1.0.0).
6. 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: v1.0.0).
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: v1.0.0).
8. PIN authentication did not work properly when using Device Hashkey Management (Affects version: v1.8.0).
9. Abnormal authentication failure occurred when the slave device's auth mode was set to card+fingerprint (Affects version: v1.8.0).
10. 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: v1.0.0).
11. 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: v1.9.0).
12. 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: 1.5.0).
13. Improved to check for the duplication of cards registered with users when transmitting user data from the server to devices (Affects version: v1.7.0).

Firmware Version 1.9.0 (Build No. 1.9.0_210618)

Release: 2021-06-25

New Features and Improvements

1. Improved manually turning the secure tamper on or off even when the default hash key is set.
2. 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 via OSDP after activating the Secure Communication mode. (Affects version: v1.8.0 or earlier)
2. The screen was abnormally displayed when the second user authentication was successful on a slave device with dual authentication. (Affects version: v1.9.0 or earlier)
3. The firmware upgrade failed when the device was connected as a slave device. (Affects version: v1.8.0 or earlier)
4. It was not able to recognize Mobile Access Card after upgrading the firmware.
   (BSA2-OIPW, BSA2-OMPW / Affects version: v1.9.0 or earlier)
5. DNS queries were sent to an IP address that was not set. (Affects version: v1.8.0 or earlier)
6. 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: v1.8.0 or earlier)
7. The relay operated as Off (Lock) after setting the scheduled unlock zone in the elevator and rebooting the master device. (Affects version: v1.8.0 or earlier)
8. All files in the database were deleted after exporting them to a USB. (Affects version: v1.8.0 or earlier)
9. The slave device rebooted abnormally. (Affects version: v1.8.0 or earlier)
10. Disconnected logs frequently occurred when the device was used with Secure I/O 2. (Affects version: v1.8.0 or earlier)
11. 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: v1.8.0 or earlier)
12. The door remained locked and did not open after rebooting the device when it was set to Manual Unlock.
    (Affects version: v1.8.0 or earlier)
13. Ten administrators were still not deleted from the device when initializing the device that has 1,000 assigned administrators. (Affects version: v1.8.0 or earlier)
14. 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: v1.8.0 or earlier)
15. When the slave device in Fire Alarm Zone triggered an alarm, the alarm did not sound if the master device was rebooted. (Affects version: v1.8.0 or earlier)
16. The door relay status was not displayed properly when rebooting the master device while Manual Lock or Manual Unlock was set. (Affects version: v1.8.0 or earlier)

Firmware Version 1.8.0 (Build No. 1.8.0_201013)

Release: 2020-10-29

Main Fixes

1. Logs generated while the device is disconnected are not sent to BioStar 2, even after the device is reconnected.
2. Fingerprint authentication fails if the device is connected as a slave when using the ISO fingerprint template.

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 new device.
   - XPass D2 (Rev)
6. Support to the Mobile Access V1.1.

Bug Fixes

1. Writing and formatting of previously issued smart cards does not work properly.
2. If the maximum number of users and logs are stored on the device, the device reboot does not work properly.
3. Modified that the authentication mode of the slave device is set according to the setting of the master device.
4. Card data is output with wrong BitCount when the device is connected to a 3rd-party system via OSDP.
5. It recognized registered users as unregistered when accessing job codes with assigned cards.
6. An OSDP security session error occurred when connecting OM-120 and XPass D2 as a slave device.
7. 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.
8. An error in the master-slave connection occurred due to the RS-485 communication key.
9. After a global anti-passback violation, an authentication success log occurred twice.
10. PIN authentication failed.

11. After the message ‘Invalid payload’ occurred on the slave device, it was disconnected abnormally and reconnection was impossible.
12. When a locked device was rebooted for an RS-485 connection, the slave device became unlocked.
13. When Factory Default was performed using SDK, the device resource (logo image) did not initialize.
14. Authentication of fingerprints registered as duress fingerprints failed.
15. It was unable to edit, delete or add an authentication mode.
16. When the delay for the output signal occurred repeatedly, the device did not work properly.
17. When BioStation 2 was connected as a slave, the output port could not be set in the Trigger and Action.

Firmware Version 1.7.1 (Build No. 1.7.1_200115)

Release: 2020-02-05

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.

Firmware Version 1.7.0 (Build No. 1.7.0_190806)

Release: 2019-08-08

Main Fixes

1. The master device abnormally shuts down if it is operated after reconnecting a disconnected slave device.
2. 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 fingerprint 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. Support for connecting new devices.
   - XPass 2(XP2-MDPB, XP2-GDPB, XP2-GKDPB)

Bug Fixes

1. The master device does not be connected to the slave device intermittently if the master device is rebooted with schedule unlock and manual unlock set at the door.
2. Slave device (XPass D2) firmware upgrade via BLE fails.
3. When upgrading firmware using USB, upgrade fails due to a timeout.
   - Change the timeout from 90 seconds to 5 minutes.
4. Image logs are not generated for some events.
5. When dual authentication is set on the door, if the first user authenticates with the fingerprint and the second user authenticates with the ID, the wrong ID is displayed on the screen when authentication fails.
6. The device recognizes the iCLASS Seos card as a CSN card.
7. Firmware upgrade does not work normally due to SSL reconnection.
8. Applies the FA(False Acceptance) improvement algorithm.
9. Start time is not applied in UTC when importing filtered logs using SDK.
10. A user cannot access BioStar 1.93 when using the latest firmware.
11. The relay operates abnormally if the master device reboots after configuring multiple doors.
12. When a user with Administrator permission is configured as below, the device will not respond if the user tries to authenticate the card.
    - If the status is set to Disable.
    - If the period is set to be past or future.
13. Relay works after reconnecting for authentication that occurred when elevator connection is disconnected.
14. If a user enters the gateway and subnet mask values and then set to Enable DHCP, the wrong IP address is output to the user interface.
15. Access is denied and user ID is displayed abnormally when using a smart card or fingerprint authentication in One Device Mode.

Firmware Version 1.6.1 (Build No. 1.6.1_190405)

Release: 2019-04-10

Bug Fixes

1. The device's touch screen operates abnormally due to interference at a frequency of 125 kHz.

Firmware Version 1.6.0 (Build No. 1.6.0_190104)

Release: 2019-01-08

Main Fixes

1. When Micom is reset, the output does not restore to its previous status.
2. The device reboots when a user enrolls or edits a user on the device.
3. The device reboots when a user searches for a zone at the Event Log menu on the device.
4. Wiegand Out is not output when authenticating with blacklist card.
5. With Bypass enabled, authentication failure message is not displayed when unregistered ID is authenticated.
6. The user cannot issue a new File after the App and File are created when issuing the DESFire card.
7. A code is added to prevent the authentication fails because the cache memory is broken.
8. The device does not recognize EM card and HID Prox card.
9. When the server private message is activated on the device, the device does not operate normally if there is no registered authentication message.

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 relays operate differently from the previous status if the slave device is reconnected.
2. 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.
3. The master device reboots if a user authenticates the fingerprint consecutively to the master device or slave device.
4. The Authentication success or failure setting in Trigger & Action does not work normally.
5. Change some special characters (\, /, :, *, ?, “, ‘, `, <, >, |, .) to be unavailable when setting a user name.
6. When the elevator is configured as a Fire Alarm Zone, if a user clears the alarm, the event log that has not been set is displayed.
7. Modified a user interface in USB memory menu.
8. With Bypass enabled, the device does not respond even if a user selects the Menu, T & A, or ID after authentication.
9. If a user authenticates the card to XPass D2 connected to as a slave device, the beep sounds twice.
10. 1: N authentication can also be added on the slave device even though the master device is only capable of 1: 1 authentication.
11. If the user uses the BS_GetLogBlob command to get the door ID, the door ID is not output normally.
12. When the backlight is off, the device does not respond even if the user touches the screen.
13. The bit of the fingerprint image is broken.

Firmware Version 1.5.1 (Build No. 1.5.1_180726)

Release: 2018-07-31

New Features and Improvements

1. Support the issuance of Secure Credential Card without the fingerprints when registering iCLASS 2K card.
2. Support OP6 fingerprint sensor.
3. Support for connecting new devices.
   - 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 pop-up message is not displayed properly if the finger does not place exactly in the center of the sensor when enrolling the fingerprint while using Advanced Enrollment and View Image.
7. The arm/disarm key is displayed on a device not included in the intrusion alarm zone.
8. Wiegand Reader could not be unlocked.
9. The device restarts when authenticating with an unregistered fingerprint.
10. An empty file is created when running USB Export, even though there is saved data.
11. The device cannot read CSN because the card recognized as an NFC tag.
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.
14. The device restarts when authentication fails.
15. The device continuously restarts when configuring the device in BioStar 2 as follows:
    1) Set the device network as a WLAN.
    2) Deactivate a DHCP.
    3) Delete the IP address and Gateway.
    4) Save the settings.

Firmware Version 1.5.0 (Build No. 1.5.0_180304)

Release: 2018-03-05

New Features and Improvements

1. Support Interlock zone, Muster zone.
2. Support Daylight Saving Time setting.
3. Improves Trigger & Action for duress finger.
4. Support Private Authentication on AoC.
5. 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.
6. Improves to handle the encryption key of the important information stored in database differently from server to server.
7. Support One Device Mode(Legacy).
8. Improves the ability to set the user ID type in SIP server
   - Support number and alphanumeric options for entering up to 32 characters.
9. Support simultaneous use of Wiegand input and output.
10. Support the secure tamper.
11. Support connecting with BioLite N2, XPass D2.

Firmware Version 1.4.0 (Build No. 1.4.0_170919)

Release: 2017-09-22

New Features and Improvements

1. Support the intrusion alarm 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.
3. Support fingerprint enrollment on slave device.
4. Improves user transfer speed.
5. Support SEOS smart cards (Elite Key).
6. Improves performance of SEOS smart card RF reading.
7. Performs the Access on Card (AoC) matching when connected to a master device as a slave device.

Firmware Version 1.3.1 (Build No. 1.3.1_170728)

Release: 2017-07-31

New Features and Improvements

1. Support SEOS smart card settings

Bug Fixes

1. Issue where the device cannot recognize SEOS smart cards when multi-credential authentication mode (iCLASS SEOS smart card + Fingerprint) is used continuously.

Firmware Version 1.3.1 (Build No. 1.3.1_170710)

Release: 2017-07-31

New Features and Improvements

1. Support SEOS smart cards.
2. Support validation of the device settings.
3. User Operator cannot change another user's Operator Level as Administrator.

Bug Fixes

1. Issue where the device is malfunctioned when device log is full.
2. Issue where the device is malfunctioned when receiving or sending Wiegand signals.

Firmware Version 1.3.0 (Build No. 1.3.0_170221)

Release: 2017-02-21

New Features and Improvements

1. Apply eMMC alternatives (Samsung 8GB D Die to E Die)
2. Fixed issue where the device is restarted (Set Application GPU HW Accelerator as Off)

Firmware Version 1.3.0 (Build No. 1.3.0_170201)

Release: 2017-02-07

New Features and Improvements

1. Add reset code for changing LCD part.

Firmware Version 1.3.0 (Build No. 1.3.0_170201)

Release: 2017-02-07

New Features and Improvements

1. Support elevator control.
2. Support for alphanumeric ID.
3. Support for Secure Communication (SSL & TLS)
4. Private authentication mode can be added on access-on-card.
5. Up to 100,000 cards can be added to blacklist

Firmware Version 1.2.0 (Build No. 1.2.0_160627)

Release: 2016-06-27

New Features and Improvements

1. Added operation condition and action – device sound alarm support
2. NFC support.
3. Support for 256 bit card ID.
4. Support for automatic door configuration.
5. Support for multi-Wiegand input/output format.
6. Support for customizable UI.
7. Support for SIP-based videophone.

Firmware Version 1.1.0 (Build No. 1.1.0_160407)

Release: 2016-04-07

Bug Fixes

1. Logs not transmitting properly when logs in the device reaches the storage limit.

Firmware Version 1.0.0 (Build No. 1.0.0_160205)

Release: 2016-02-05

Bug Fixes

1. Issue with door relay operation.
2. Issue with alarm lasting time.

Firmware Version 1.0.0 (Build No.1.0.0_151223)

Release: 2015-12-23

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

© 2024 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.