BioStation L2

Firmware Revision Notes

Version 1.6.1

EN 301.00.BSL2 V1.6.1

suprema
SECURITY & BIOMETRICS

Firmware Version 1.6.1 (Build No. 1.6.1_210324)

Release: 2021-04-22

1. New Features and Improvements
   1.1. Upgraded to the 1.1.1i version of OpenSSL.
   1.2. Intelligent Slave Support
      - Intelligent Slave: A function that enables 1:1 or 1:N matching directly from the Suprema device and transmits the authentication result as OSDP card data to the third-party controller.
   1.3. Separated event logs of Mobile Access cards and RFID cards.
   1.4. Improved that LFD Driver IC damage does not affect fingerprint recognition performance.

2. Bug Fixes
   2.1. If 31 slave devices were connected and one of the devices got disconnected, the master device rebooted. (Affects version: v1.0.0)
   2.2. Incorrect BitCount was sent if a user authenticated with AoC when the device was connected to a 3rd-party system via OSDP. (Affects version: v1.0.0)
   2.3. The device responded that it supported transparent mode by OSDP_PDCAP when connecting as a slave while it did not support it. (Affects version: v1.0.0)
   2.4. It was not able to change secure tamper settings from the device menu. (Affects version: v1.6.0)
   2.5. The fingerprint recognition function worked even when a Secure-IC error occurred. (Affects version: v1.6.0)
   2.6. When calling the BS2_ResetConfigExceptNetInfo API from the BioStar 2 Device SDK, a 'Timeout' error occurred. (Affects version: v1.0.0)
   2.7. It was able to communicate using default keys after changing the key settings when the device was connected to a 3rd-party device via OSDP. (Affects version: v1.5.0)

Firmware Version 1.6.0 (Build No. 1.6.0_200729)

Release: 2020-08-04

1. New Features and Improvements
   1.1. Added feature to change device ID.
   1.2. Enhancement in the security of the device.
      - Restrict unencrypted connections.
      - Enhancement in the security of encryption keys.
      - Encrypt and migrate user information.
   1.3. Added screen to show data migration status.
   1.4. Improved Anti-passback zone to operate based on the door status.
   1.5. Improved the scheduled unlock zone function for each floor when controlling elevator.
   1.6. Supports new device.
      - XPass D2 (Rev 2)

2. Bug Fixes
   2.1. The problem that the job code can be registered in excess of the supported number when using SDK.
   2.2. OSDP Communication does not work normally if the value sent to the slave device is greater than the defined value.
   2.3. Device reboots or a timeout occurs when upgrading firmware or transferring user data during SSL secure communication.
   2.4. The event log of the device is not sent in the order in which it occurred.
   2.5. Issue that the option for card types is deactivated when the device is connected as a slave after the factory reset.
   2.6. Issue that the connection of the slave device is disconnected when the slave device is connected.
   2.7. Device reboots when there is no operation after connecting power.

Firmware Version 1.5.1 (Build No. 1.5.1_190911)

Release: 2019-09-20

1. Bug Fixes
   1.1. After a user scans and registers a card on a device set as Wiegand Out device, if an existing user authenticates with a credential other than the card, the Wiegand output will behave abnormally.
   1.2. The device restarts if a user authenticates a fingerprint on the device set as below.
      - Byte Order: LSB
      - Wiegand Out: User ID
   1.3. When using firmware V1.5.0 the connection to the I/O device that using the firmware version below is lost.
      - DM-20 FW V1.1.2
      - OM-120 FW V1.0.0
      - Secure I/O 2 FW V1.2.1
   1.4. The master device intermittently reboots when upgrading the firmware of the slave device.

Firmware Version 1.5.0 (Build No. 1.5.0_190708)

Release: 2019-07-12

1. Main Fixes

   1.1. When a door configured in a Scheduled Unlock Zone is opened by a Scheduled Unlock, the door is not locked if the zone is deleted.

   1.2. A code is added to prevent the authentication fails because the cache memory is broken.

2. New Features and Improvements

   2.1. OSDP Standardization

   - Improved to comply with OSDP V2.1.7 protocol when connecting with 3rd-party controllers.

   2.2. Supports Anti-Tailgating.

   2.3. Supports the duplicate fingerprint check when registering users on a device.

   2.4. Supports setting options for Wiegand authentication result output.

   2.5. Change the way new settings are applied when adding administrators using batch edit of devices.

   - Existing: Overwrite a new setting to existing settings.
   - Update: Add a new setting to existing settings.

   2.6. Increase of the number of administrators that can be added.

   2.7. Increase of the maximum number of floor levels.

   2.8. Supports options for selection by card type.

   2.9. Support to the Clear APB for each user.

   2.10. Supports checking module firmware version.

   2.11. Supports the latest version of I/O module Micom (V1.3.1).

   2.12. Support for connecting new devices.

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

3. Bug Fixes

   3.1. If the same fingerprint is authenticated successively after successful fingerprint authentication, the duplicated logs are left.

   3.2. Applies FA improvement algorithm.

   3.3. The code value set in T&A mode is not maintained.

   3.4. Start time is not applied in UTC when importing filtered logs using SDK.

   3.5. The waiting alarm does not stop even if the master device is disconnected when the waiting alarm occurs during the delay time in the intrusion alarm zone.

   3.6. Supports unsupported devices (FaceStation 2, FaceLite).

   3.7. EM cards are continously recognized.

   3.8. If the master device is disconnected when the intrusion alarm zone is set to 'Arm', it will be displayed as 'Arm' on the screen when the master device is reconnected even though the zone has been disarmed.

3.9. Relay works after reconnecting for authentication that occurred when elevator connection is disconnected.

3.10. The title of the credential input screen is displayed differently on the master device and the slave device when using multiple authentication mode.

- Existing: master device (user ID, user name), slave device (user ID)
- Update: master device and slave device (user ID, user name)

3.11. The device reboots when transferring the maximum number of users after deleting all users.

3.12. The device reboots during firmware upgrade with the maximum number of users registered.

3.13. The slave device operates according to the Auth Timeout set in the master device, not the Auth Timeout set in the slave device.

3.14. The output of Dual Authentication Timeout messages is delayed.

3.15. If more than 200,000 fingerprint templates are registered and the user tries to access the admin menu by fingerprint authentication while the user is registered, the error phrase is not output properly, and the user can access.

Firmware Version 1.4.0 (Build No. 1.4.0_181106)

Release: 2018-11-29

1. Main Fixes

   1.1. A code is added to prevent the authentication fails because the cache memory is broken.

   1.2. The device restarts when a user runs Date & Time menu on the device after setting the time zone on the server.

2. New Features and Improvements

   2.1. Support to the number of users, fingerprints, faces, and cards in Manage Users in Device.

   2.2. Change the maximum value of the interval and width for the Wiegand Input.

   2.3. Improves the data protection.

   - Increase the items to encrypt the data.
   - Support to setting the period for storing the personal information.

   2.4. Support for Individual Authentication Successful Messages and Working alarm time reports.

   2.5. If the data transmission fails when communicating with OSDP, it is transmitted again.

   2.6. The site key is initialized if a secure tamper event occurs.

   2.7. If an administrator has registered, modified, or deleted a user, the event log shows whether the editing was done on the server or on the device.

   2.8. Support to the creation of up to 2048 Access Levels and Access Groups.

   2.9. Support to DESFire/DESFire EV1 Advanced option.

   2.10. Support to AES encryption type for DESFire card.

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

3. Bug Fixes

   3.1. If the user uses the BS_GetLogBlob command to get the door ID, the door ID is not output normally.

   3.2. Change some special characters (\, /, :, *, ?, ", ', `, <, >, |, .) to be unavailable when setting a user name.

   3.3. When restarting the device, if a user authenticates before the device completely restarts, the device is locked.

   3.4. Improves I/O module Input and Output process.

   3.5. The device cannot read CSN because the card recognized as an NFC tag.

   3.6. 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.

   3.7. The sound of the arm before it starts works differently than the sound set.

   3.8. The relays operate differently from the previous status if the slave device is reconnected.

   3.9. The alarm can be released in the Floors status after a fire alarm occurs when the elevator is configured as a Fire Alarm Zone.

Firmware Version 1.3.2 (Build No. 1.3.2_180710)

Release: 2018-07-24

1. Bug Fixes
   1.1. The device restarts when authentication fails.
   1.2. Modified to limit kernel downgrade based on the hardware version of the device.

Firmware Version 1.3.1 (Build No. 1.3.1_180523)

Release: 2018-06-20

1. New Features and Improvements
   1.1. In a device with an LCD, the user name is displayed on the LCD when authentication is successful even when connected in slave mode.
   1.2. Support OP6 fingerprint sensor.
   1.3. Support for connecting new devices.
      - BioLite N2(BLN2-PAB), XPass D2(XPD2-GDB, XPD2-GKDB)

2. Bug Fixes
   2.1. Issue where the bypass does not work when authentication with AoC in Wiegand output.
   2.2. Issue where event logs and real-time logs are not uploaded normally to BioStar 2.
   2.3. Problem that relay state is not maintained when reconnecting a device connected by RS-485.
   2.4. Issue in which the door relay status operates as On when the device is reconnected after starting and ending the Schedule Unlock with the door relay device disconnected.
   2.5. Problem that does not proceed to the next step even though you enter the OK button after setting the daylight saving time.
   2.6. Problem that the device's time is kept in daylight saving time even after the set daylight saving time is over.
   2.7. Modified that the Job code can not be enter without using the time attendance menu.
   2.8. Problem that the same voice announcement is played when the intrusion arm and disarm.
   2.9. Issue where ID authentication works normally even though the device is set to lock when APB alarm occurs after dual authentication and APB setting.
   2.10. Problem that when a card is scanned in a fingerprint or PIN input situation, it is operated as a card authentication after the authentication timeout.
   2.11. Problem that the time zone is not initialized even if the factory reset is performed while secure communication and data encryption key are in use.
   2.12. Issue where if the authentication is successful when the device set as door relay is disconnected, the relay will operate according to previous value after reconnection of the device.
   2.13. Issue where the device restarts when authenticating with an unregistered fingerprint.

Firmware Version 1.3.0 (Build No. 1.3.0_180317)

Release: 2018-03-26

1. New Features and Improvements
   1.1. Output signal setting for Wiegand reader control.
   1.2. Improves that invalid values can not be entered in the authentication mode, AuthTimeout, MsgTimeout, ScanTimeout, and MatchingTimeout.
   1.3. Support fingerprint enrollment on the slave device.
   1.4. Support the intrusion alarm zone, Muster zone and 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.
   1.5. Performs the Access on Card (AoC) matching when connected to a master device as a slave device.
   1.6. Improves user transfer speed.
   1.7. Improves log search within device.
   1.8. User Operator cannot change another user's Operator Level as Administrator.
   1.9. Support Reset without Network Settings.
   1.10. Support Daylight Saving Time setting.
   1.11. Improves Trigger & Action for duress finger.
   1.12. Support Private Authentication on AoC.
   1.13. Improves to handle the encryption key of the important information stored in database differently from server to server.
   1.14. Support One Device Mode(Legacy).
   1.15. Added a message asking whether to delete the fingerprint in the database after completing AoC issuance.
   1.16. Support the secure tamper.
   1.17. Support ISO14443A 10 Byte CSN.
   1.18. Support connecting with BioEntry R2, BioEntry P2, BioLite N2, XPass D2.

2. Bug Fixes
   2.1. Problem trying to forward commands related to Config during connection after searching RS-485 slave device.
   2.2. Problem where changes were not reflected on the user interface after changing the device to DHCP disabled and IP and gateway settings.
   2.3. Issue where 'Auth Time Out' message is displayed when waiting after pressing random T & A key.
   2.4. Issue where RS-485 disconnect message is displayed when changing home screen of the slave device to user's logo.
   2.5. Problem not working in 256 bit Wiegand format.
   2.6. Issue that Wiegand output device prints wrong value when authenticating with fingerprint/ID authentication mode.

2.7. Issue where some alarm ports remain 'On' when rebooting the master device when an alarm occurs in Schedule Lock state.

2.8. Problems that do not work when set Open/Short with Supervised input of DM-20 in the elevator control.

2.9. Problem does not work when enroll fingerprint using Advance Enrollment in the slave device.

2.10. Problem disconnecting when adding a slave device after setting Log Upload to Manual.

2.11. Issue that Face authentication information is displayed on devices that do not support face authentication.

2.12. Problem that the mobile card recognizes as 'Unregistered User' when entering the admin menu.

2.13. Issue when user ID type is set to alphanumeric, even if a user with ID 32 is set as administrator, it is changed to the normal user.

2.14. Issue if the elevator is configured as a fire alarm zone, relay operation will be turned off when the alarm is released after the fire alarm.

2.15. 'Unknown' is displayed when trying to enter detail page of CST sub-slave device.

2.16. Total count error on filter value when searching.

2.17. Problem with reading mobile smart cards on Galaxy S4.

2.18. Galaxy S5 NFC is recognized as a CSN card when authenticating with NFC and the authentication fails.

2.19. Issue where the touch keypad does not work.

Firmware Version 1.2.4 (Build No. 1.2.4_170906)

Release: 2017-09-06

1. New Features and Improvements
   1.1. Improved Live Finger Detection(LFD) performance
   1.2. Authentication Mode is excluded from the validation of setting valaues.

2. Bug Fixes
   2.1. Issue where the device is reset when the fingerprint is authenticated.

Firmware Version 1.2.3 (Build No. 1.2.3_170628)

Release: 2017-06-29

1. New Features and Improvements
   1.1. Support 8GB eMMC
   1.2. Performs the validation when invalid values are sent to the device.

2. Bug Fixes
   2.1. Issue where the device sends an abnormal amount of logs to BioStar.
   2.2. Issue where User Operator can change another user's account level.

Firmware Version 1.2.2 (Build No. 1.2.2_170213)

Release: 2017-02-27

1. New Features and Improvements
   1.1. Add Lift I/O MFG Command
   1.2. Clean up the unused thread

2. Bug Fixes
   2.1. Issue where the slave device's time zone is changes when the device synchronization is perfomed.
   2.2. Wiegand Output malfunctions when fingerprint authentication is completed after authenticaing with the unregistered card.
   2.3. Slow-downs the performance.
   2.4. Issue that cannot check the individual log after the authenticating the card.

Firmware Version 1.2.1 (Build No. 1.2.1_161213)

Release: 2016-12-20

1. Bug Fixes
    1.1. Issue that cannot detect the device with UDP in BioStar 1.92.

Firmware Version 1.2.0 (Build No. 1.2.0_161129)

Release: 2016-12-13

1. New Features and Improvements
   1.1. Support for the secure communication (TLS) with BioStar 2
   1.2. Support for iCLASS SEOS card
   1.3. Support for the 1.x Template on Card
   1.4. Support for the daylight saving time
   1.5. OP6 sensor support
   1.6. Improved fingerprint algorithm
   1.7. Improved LFD calibration
   1.8. Support for alphanumeric ID

Firmware Version 1.1.1 (Build No. 1.1.1_160921)

Release: 2016-09-22

1. Bug Fixes
   1.1. Memory leak issue when a T&A device is registered as a slave device and users authenticate after pressing a T&A key.
   1.2. Issue where the master device reboots when a device with an old firmware version is connected as a slave device and a user authenticates with a card on the slave device.

Firmware Version 1.1.0 (Build No. 1.10_160701)

Release: 2016-07-01

1. New Features and Improvements
   1.1. Added operation condition and action – device sound alarm support
   1.2. NFC support.
   1.3. Support for 256 bit card ID.
   1.4. Support for automatic door configuration.
   1.5. Support for multi-Wiegand input/output format.
   1.6. Improved fingerprint input performance.

2. Bug Fixes
   2.1. Issue where a different time shows on the authentication screen and logs when time format is set to AM/PM.

Firmware Version 1.0.2 (Build No. 1.0.2_160602)

Release: 2016-06-02

1. Bug Fixes
   1.1. Issue where the device does not boot if the OP5 sensor isn't assembled.

Firmware Version 1.0.1 (Build No. 1.0.1_160601)

Release: 2016-06-01

1. Bug Fixes
   1.1. Issue where the fingerprint sensor intermittently did not scan fingers.

Firmware Version 1.0.0 (Build No.1.0.0_160330)

Release: 2016-03-30

1. Initial firmware developed.

Suprema Inc.
16F Parkview Tower
248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 463-863 Republic of Korea
Tel.+82-31-783-4502 Fax.+82-31-783-4503
sales@supremainc.com www.supremainc.com