BioLite N2

Firmware Revision Notes

Version 1.6.0

English

EN 301.00.BLN2 V1.6.0

suprema

SECURITY & BIOMETRICS

Firmware Version 1.6.0 (Build No. 1.6.0_230602)

Release: 2023-06-08

Devices with the new BLE chip and the SE processor cannot downgrade to a lower version after upgrading the firmware to v1.5.0 or higher. Devices with existing BLE chips and SE processor can be downgraded to a lower version.

For more information, check the serial number of the device and contact the Suprema (supremainc.com).

New Features and Improvements

1. Supports a new SE processor and new firmware.
2. Improved firmware to work with security-enhanced diag tool.
3. Improved the structure to prevent authentication fail caused by broken database or cache memory.
4. 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: v1.0.0)
2. Card authentication performance being slower than the previous versions. (Affects version: v1.5.0)
3. Improved the OSDP ID to also be deleted when a security tamper occurs on the device connected as a slave. (Affects version: v1.0.0)
4. When using the card to authenticate to the device, the card that was normally authenticated fails intermittently. (Affects version: v1.0.0)
5. Applying an invalid custom resource causes the device to restart. (Affects version: v1.0.0)
6. 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: v1.0.0)
7. Device does not recognize some HID iCLASS Seos cards. (Affects version: v1.0.0)
8. 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)
9. Door Locked event occurs when input signal gets detected while configured to Arm/Disarm by input signal. (Affects version: v1.0.0)
10. Intermittently, the door does not open even if authentication succeeds when the door uses the slave device's relay. (Affects version: v1.0.0)

Firmware Version 1.5.0 (Build No. 1.5.0_220621)

Release: 2022-06-21

Devices with the new BLE chip and the SE processor cannot downgrade to a lower version after upgrading the firmware to v1.5.0 or higher. Devices with existing BLE chips and SE processor can be downgraded to a lower version.

For more information, check the serial number of the device and contact the Suprema (supremainc.com).

New Features and Improvements

1. z that do not support BLE (Bluetooth Low Energy).
   - BLN2-OA, BLN2-OD
2. Supports setting the byte order for smart cards.
   - Supports setting the byte order of data to be output to Wiegand or OSDP.
3. Supports a new BLE (Bluetooth Low Energy) chip.
   - The BLE chip parts of the hardware have been changed, and the firmware has been upgraded to be compatible with both the existing and new BLE chips.
4. Supports the dual SE processor.
5. Separated the log related to the cause of the door unlock.
   - Door open request by exit button
   - Door open request by operator
6. Added relay deactivation option for exit button input.
   - Added the option to set the door open request log to occur but the relay not to operate when the exit button is pressed.
7. Supports Live Finger Detection.

Bug Fixes

1. Mobile card authentication suddenly does not work (Affects version: v1.3.2).
2. Global APB behavior for the same input was different depending on firmware version (Affects version: v1.4.0).
3. Device does not connect to a 3rd party controller (Software House iSTAR Edge G2) via OSDP (Affects version: v1.4.1).
4. When changing the intelligent slave settings on the detailed page of the device on BioStar 2, the settings were not applied (Affects version: v1.4.2).
5. Migration malfunction occurs when the firmware is upgraded from v1.2.0 or earlier to v1.3.0 or later (Affects version: v1.3.0).
   - Migration did not complete and the device boots to the main screen, some keys do not work or an abnormal screen is displayed.
6. When communicating with a 3rd party control panel via OSDP, the device incorrectly responds as 'Inactive' when receiving the Input Status Request command while the input port is grounded (Affects version: v1.4.1).
7. When communicating with a 3rd party control panel via OSDP, the device does not respond to the Output Status Report command while the relay reacts to it (Affects version: v1.4.1).
8. When communicating with a 3rd party control panel via OSDP, the device incorrectly responds as 'Inactive' when receiving the Output Status Request command while the relay status is 'On' (Affects version: v1.4.1).
9. Device does not recognize some HID iCLASS Seos cards (Affects version: v1.0.0).

Firmware Version 1.4.2 (Build No. 1.4.2_220125)

Release: 2022-02-11

New Features and Improvements

1. Supports a new BLE (Bluetooth Low Energy) chip.
   - The BLE chip parts of the hardware have been changed, and the firmware has been upgraded to be compatible with both the existing and new BLE chips.
2. Improved to transmit entire card data, including the parity bit, when a user authenticated the fingerprint while the Wiegand card was registered.

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 (BLN2-OAB, BLN2-PAB) (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. PIN authentication did not work properly when using Device Hashkey Management (Affects version: v1.3.0).
7. Abnormal authentication failure occurred when the slave device's auth mode was set to card+fingerprint (Affects version: v1.3.0).
8. 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: v1.4.0).
9. 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: v1.3.0).
10. Improved to check for the duplication of cards registered with users when transmitting user data from the server to devices (Affects version: v1.2.0).
11. 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).
12. When the device is connected as an intelligent slave and the first card registered to the user is a Wiegand card of a format other than 26-bit, the CSN value is output through OSDP when authenticated with the user's credentials other than the card (Affects version: v1.4.1).
13. 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: v1.3.0).
14. Failed upgrading firmware related to BLE (Affects version: v1.4.1).

Firmware Version 1.4.1 (Build No. 1.4.1_210917)

Release: 2021-09-28

New Features and Improvements

1. 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.

Bug Fixes

1. Smart card data were output with the wrong BitCount when the device was connected to a 3rd-party system via OSDP. (Affects version: v1.4.0 or earlier)

Firmware Version 1.4.0 (Build No. 1.4.0_210617)

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. Upgraded to the 1.1.1i version of OpenSSL.
3. Separated event logs of Mobile Access cards and RFID cards.

Bug Fixes

1. When the connection of the slave device in the Scheduled Unlock Zone was disconnected and then was reconnected, the relay did not maintain the previous status. (Affects version: v1.3.2 or earlier)
2. The screen was abnormally displayed when the second user authentication was successful on a slave device with dual authentication. (Affects version: v1.4.0)
3. After being disconnected from BioStar 2, an incorrect pop-up message was displayed until they were reconnected. (Affects version: v1.3.2 or earlier)
4. The device rebooted abnormally when the firmware version was upgraded to 1.3.2 after changing the slave device with firmware version 1.2.0 to a master device. (Affects version: v1.3.2 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: v1.3.2 or earlier)
6. The slave device rebooted abnormally. (Affects version: v1.3.2 or earlier)
7. Disconnected logs frequently occurred when the device was used with Secure I/O 2. (Affects version: v1.3.2 or earlier)
8. 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: v1.3.2 or earlier)
9. The door remained locked and did not open after rebooting the device when it was set to Manual Unlock. (Affects version: v1.3.2 or earlier)
10. Ten administrators were still not deleted from the device when initializing the device that has 1,000 assigned administrators. (Affects version: v1.3.2 or earlier)
11. It was not able to enter special symbols (., ?, /, *) in the server URL field. (Affects version: v1.3.2 or earlier)
12. Keystrokes were not working or a delay occurred in a user interface after upgrading the firmware. (Affects version: v1.3.2 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: v1.3.2 or earlier)
14. It was able to set not only Card Only but the other modes for Wiegand readers. (Affects version: v1.3.2 or earlier)

Firmware Version 1.3.2 (Build No. 1.3.2_200917)

Release: 2020-09-28

Bug Fixes

1. Device registration using Mobile Access app does not work on dynamic site.
2. When setting the device zone using SDK, an error occurs and does not work properly.

Firmware Version 1.3.1 (Build No. 1.3.1_200702)

Release: 2020-07-14

Main Fixes

1. Fingerprint authentication fails if the device is connected as a slave when using the ISO fingerprint template.

Firmware Version 1.3.0 (Build No. 1.3.0_200609)

Release: 2020-06-11

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

Bug Fixes

1. When the master device is rebooted with both the scheduled unlock and manual lock set, it operates using the scheduled unlock.
2. The device does not recognize the iCLASS cards issued by 1st generation devices.
3. Once a card has been registered on the Wiegand output device, the device will not work properly when trying to output data using a fingerprint registered to another user.
4. When a user authenticates the fingerprint after setting the byte order as LSB and the Wiegand output information as the user ID, the device will reboot.
5. When a user authenticates on the slave device using a smart card or the face, the master device will reboot.
6. When the user ID type is set to alphanumeric, a user ID with spaces can be registered on the device.
7. When BioStation 2 is connected as a slave device, the output port cannot be set in the Trigger and Action.
8. RS-485 communication with BioEntry R2 (BER2-OD) does not work properly.
9. A bug that caused delays in the output of motion signals.
10. The change in authentication mode is not applied.

11. The device reboots or a timeout occurs when upgrading firmware or transferring user data during SSL secure communication.
12. An error occurs when updating the fingerprint template.
13. Authentication of fingerprints registered as duress fingerprints fails.
14. Authentication mode setting does not work properly when XPass 2 is connected as a slave device.
15. Some resources are not initialized even when the BioStation 2 connected as a slave device is factory reset.
16. After the message 'Invalid payload' occurs on the slave device, it is disconnected abnormally and reconnection is impossible.
17. An error occurs when authenticating with an iCLASS SEOS card when a smart card layout is set but SEOS is not selected in the card type option.
18. An error occurs when authenticating with an AoC or SCC issued in DES/AES encryption mode.
19. In the case of anti-passback violations in the global anti-passback zone, an authentication success log is generated.
20. In the RS-485 communication, if a user attempts to perform fingerprint authentication continuously from the device, authentication fails.
21. The device does not recognize the iCLASS cards intermittently.

Firmware Version 1.2.0 (Build No. 1.2.0_190806)

Release: 2019-08-09

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.
3. Unable to enter the Job Code menu if a user authenticates with AoC.

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.

   

   You can add up to 1,000 device administrators. To add more than 10 device administrators, the device must be connected to BioStar 2 v2.7.3 or later.

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 fingerprint 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. Support for RS-485 connections to new devices
    - XPass 2(XP2-MDPB, XP2-GDPB, XP2-GKDPB)

Bug Fixes

1. Even if the CSN, Wiegand card option is disabled, the device recognizes EM and HID Prox cards (BLN2-OAB, BLN2-PAB).
2. 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.
3. The device response to fingerprint or key input is slow.
4. Start time is not applied in UTC when importing filtered logs using SDK.
5. The held open occurs abnormally if the door is configured with a slave device after the slave device reboots.
6. Applies FA(False Acceptance) improvement algorithm.
7. Users without Administrator permission can access all menus on the device.
8. Relay works after reconnecting for authentication that occurred when elevator connection is disconnected.
9. When using Auth Mode, only the user ID is displayed on the next critical request screen on the slave device.
10. Access is denied and user ID is displayed abnormally when using a smart card or fingerprint authentication in One Device Mode.

Firmware Version 1.1.0 (Build No. 1.1.0_181210)

Release: 2018-12-11

Main Fixes

1. When Micom is reset, the output does not restore to its previous status and the device cannot recognize the card.
2. The DESFire EV1 card issued with the AES encryption option is recognized as a CSN card.
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. The user cannot issue a new File after the App and File are created when issuing the DESFire card.
6. Some time zones are missing and the device reboots abnormally.
7. A code is added to prevent the authentication fails because the cache memory is broken.
8. The sensor does not work if a user reboots the device and then authenticates the fingerprint.

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. The alarm can be released in the Floors status after a fire alarm occurs when the elevator is configured as a Fire Alarm Zone.
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. Japanese language resource is not applied normally when the language is set to Japanese.
5. The new event log is missing and is not displayed.
6. Change some special characters (\, /, :, *, ?, “, ‘, `, <, >, |, .) to be unavailable when setting a user name.
7. An administrator cannot set the permissions of other administrators.
8. The tamper off event occurs when the bracket is removed and the device is rebooted.
9. The Authentication success or failure setting in Trigger & Action does not work normally.
10. If a user authenticates the card to XPass D2 connected to as a slave device, the beep sounds twice.
11. If the user uses the BS_GetLogBlob command to get the door ID, the door ID is not output normally.
12. When registering a fingerprint, the scanned fingerprint image is displayed on one side.

Firmware Version 1.0.2 (Build No. 1.0.2_180709)

Release: 2018-07-20

New features and improvements

1. Support for connecting new devices.
   - BioLite N2(BLN2-PAB), XPass D2(XPD2-GDB, XPD2-GKDB)

The following bugs were fixed:

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 does not work as set for relay alarms when connecting Secure I/O 2 as a slave to the device.
4. The arm/disarm key is displayed on a device not included in Intrusion Alarm Zone.
5. The device restarts when authenticating with an unregistered fingerprint.
6. The device cannot read CSN because the card recognized as an NFC tag.
7. The device restarts when authentication fails.
8. The device restarts if fingerprint authentication is tried continuously when BioLite N2(BLN2-PAB) is connected as a master device.

Firmware Version 1.0.1 (Build No. 1.0.1_180426)

Release: 2018-04-27

New features and improvements

1. Improves the product validation method for the fingerprint sensor.

Firmware Version 1.0.0 (Build No. 1.0.0_180403)

Release: 2018-04-04

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