BioStation 3

RELEASE NOTES

Version 1.5.1

English
EN 301.00.BS3

suprema
SECURITY & BIOMETRICS

CONTENTS

- Firmware Version 1.5.1
- Firmware Version 1.5.0
- Firmware Version 1.4.3
- 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 1.0.2
- Firmware Version 1.0.1
- Firmware Version 1.0.0

Firmware Version 1.5.1 (Build No. 1.5.1_260918)

Release | 2026-09-22

Caution

- If you are using a device with firmware version v1.4.0, you must upgrade to v1.4.1 before use.
  As important security and stability improvements are included, using the latest version after the upgrade is mandatory.
- After upgrading the firmware to v1.4.0, it is not able to downgrade to an earlier version of the firmware.
- For more information, check the serial number of the device and contact the Suprema.

Bug Fixes

1. **Lock Override** card authentication not working on a door created with a Wiegand reader when the reader is disabled. Affects version: 1.5.0
2. Card authentication not proceeding after unlocking **Auth Fail Lockout**, entering a menu, and returning to the main screen. Affects version: 1.5.0
3. Mismatch between the displayed popup and the actual behavior when authentication fails after entering **Job Code**. Affects version: 1.5.0
4. Device lock status not displayed in BioStar X even when the device is locked by **Auth Fail Lockout**. Affects version: 1.5.0
5. Unlocking **Auth Fail Lockout** with ID + PIN also releasing locks that were not intended to be released. Affects version: 1.5.0
6. Administrator authentication failure count decreasing when PIN entry fails while unlocking **Auth Fail Lockout**. Affects version: 1.5.0
7. Slave device locking immediately on a single authentication failure after being deleted and re-added while in **Auth Fail Lockout**. Affects version: 1.5.0
8. Administrator authentication failed event occurring when controlling a door while in **Auth Fail Lockout**. Affects version: 1.5.0
9. Second-stage lock remaining instead of switching to the first stage when **2nd Lockout Duration** is turned off during a second-stage **Auth Fail Lockout**. Affects version: 1.5.0
10. Authentication being processed as successful and releasing the lock when unlocking **Auth Fail Lockout**. Affects version: 1.5.0
11. Child Wiegand reader not being locked by **Trigger & Action** when a **Lock Override** card is assigned to a user. Affects version: 1.4.0

12. Newly set key not applied and the default key being used in OSDP secure communication. Affects version: 1.5.0
13. Slave **Auth Fail Lockout** releasing correctly only once after a master reboot and malfunctioning thereafter. Affects version: 1.5.0
14. PIN failure during Arm authentication resulting in access denial instead of being handled as **Auth Fail Lockout**. Affects version: 1.5.0
15. Slave **Auth Fail Lockout** not releasable through card authentication. Affects version: 1.5.0
16. Home screen logo image not reflected until reboot when changed via the SDK. Affects version: 1.0.0

Firmware Version 1.5.0 (Build No. 1.5.0_260819)

Release | 2026-08-19

Caution

- If you are using a device with firmware version v1.4.0, you must upgrade to v1.4.1 before use.
  As important security and stability improvements are included, using the latest version after the upgrade is mandatory.
- After upgrading the firmware to v1.4.0, it is not able to downgrade to an earlier version of the firmware.
- For more information, check the serial number of the device and contact the Suprema.

New Features and Improvements

1. Supports new device.
   - XPass Q2
2. Added **Auth Fail Lockout** feature, which locks the device after repeated PIN authentication failures.
3. Added and improved face authentication features
   - Improved face authentication performance
   - Added support for sequential multi-face authentication (device license required)
   - Added support for Anti-Tailgating
4. Supports feature to set the baud rate of slave devices.
5. Improved **Master Admin** to enforce re-enrollment when fewer than two credentials remain.
6. Improved USB export/import file name handling
   - Changed the file name generated during USB export to start with BioStarX
   - Fixed Files exported from BioStar X not appearing in the import list
7. Improved log display for unsupported events and errors on the device.
8. Changed the authentication success icon color to green.
9. Improved OSDP reader mode to display "Access Denied" when access is denied by a third-party control panel.
10. Improved zone status display and alarm clearing behavior after power restart following a fire alarm.
11. Improved BLE stability.
12. Expanded allowed characters for User ID and User Name
    - Added support for periods (.) in User ID
    - Added support for periods (.) and apostrophes (') in User Name

Bug Fixes

1. Suprema Mobile Access authentication failing on iPhones upgraded to iOS 26 or later. Affects version: 1.0.0
2. **Manual Lock** failing to release after the set time elapses. Affects version: 1.4.0
3. When multiple devices are connected to a third-party control panel, rebooting one device causes the RS-485 connections of the other devices to be disconnected. Affects version: 1.0.2
4. Attendance status not recorded correctly according to the configured schedule times. Affects version: 1.0.0
5. Card authentication not working on slave devices when the master device is downgraded to a version that does not support Secure Messaging. Affects version: 1.4.3
6. An incorrect authentication failure reason is displayed when authenticating with an EV1 card on a slave device with Secure Messaging enabled. Affects version: 1.4.3
7. CSN value being output for EV1 cards on a slave device connected to a third-party controller via OSDP when the Secure Messaging enforcement option is enabled. Affects version: 1.4.3
8. CSN value being transmitted to the Wiegand in device for EV1 cards when the Secure Messaging enforcement option is enabled on a bypass-configured Wiegand device. Affects version: 1.4.3
9. Suprema Mobile Access authentication failing on certain Android devices. Affects version: 1.0.0
10. Devices that do not support the buzzer failing to connect when integrated with an OSDP panel. Affects version: 1.0.0
11. Card authentication failure on connected Wiegand readers. Affects version: 1.0.0
12. Device freezing or rebooting when face authentication occurs while adding or deleting users. Affects version: 1.0.0
13. Device freezing or rebooting and delayed user enrollment during user synchronization. Affects version: 1.0.0

Firmware Version 1.4.3 (Build No. 1.4.3_260406)

Release | 2026-04-10

Caution

- If you are using a device with firmware version v1.4.0, you must upgrade to v1.4.1 before use.
  As important security and stability improvements are included, using the latest version after the upgrade is mandatory.
- After upgrading the firmware to v1.4.0, it is not able to downgrade to an earlier version of the firmware.
- For more information, check the serial number of the device and contact the Suprema.

New Features and Improvements

1. Supported EV2 Secure Messaging authentication and issuance for DESFire EV2 and EV3 cards.

Bug Fixes

1. Authentication success screen not closing after selecting a **T&A Code** upon successful card authentication when the device's **Auth Mode** is set to card only and the **T&A Required** option is enabled. Affects version: 1.0.0

Firmware Version 1.4.2 (Build No. 1.4.2_260309)

Release | 2026-03-12

Caution

- If you are using a device with firmware version v1.4.0, you must upgrade to v1.4.1 before use.
  As important security and stability improvements are included, using the latest version after the upgrade is mandatory.
- After upgrading the firmware to v1.4.0, it is not able to downgrade to an earlier version of the firmware.
- For more information, check the serial number of the device and contact the Suprema.

New Features and Improvements

1. Separated firmware builds for **CE** and **Global (Non-CE)** products.

> **CE** and **Global (Non-CE)** products can be identified via the label sticker on the back of the product. The **Master Admin** feature **is enabled only on products with a label bearing the CE mark**.

Bug Fixes

1. Card format and write failure after changing the **Primary Key** of an issued MIFARE SL1 card. Affects version: 1.4.1
2. After enrolling credentials for the **Master Admin** to the slave device in BioStar 2, the enrolled information is not displayed when re-entering the device details page. Affects version: 1.4.1

Firmware Version 1.4.1 (Build No. 1.4.1_250929)

Release | 2025-09-29

Caution

- If you are using a device with firmware version v1.4.0, you must upgrade to v1.4.1 before use.
  As important security and stability improvements are included, using the latest version after the upgrade is mandatory.
- After upgrading the firmware to v1.4.0, it is not able to downgrade to an earlier version of the firmware.
- For more information, check the serial number of the device and contact the Suprema.

Bug Fixes

1. Fixed issue where unnecessary logs were getting logged. Affects version: 1.4.0
2. Applying device settings in BioStar 2 causes a logout due to a WLAN encryption problem. Affects version: 1.4.0

Firmware Version 1.4.0 (Build No. 1.4.0_250909)

Release | 2025-09-09

Caution

- If you are using a device with firmware version v1.4.0, you must upgrade to v1.4.1 before use.
  As important security and stability improvements are included, using the latest version after the upgrade is mandatory.
- After upgrading the firmware to v1.4.0, it is not able to downgrade to an earlier version of the firmware.
- For more information, check the serial number of the device and contact the Suprema.

New Features and Improvements

1. Supports the **Lock Override** feature, which allows you to enroll a card that can open a door to be opened using a specific card.
2. Improved so that when authentication is attempted on a door set to **Manual Lock**, an authentication failure event occurs and a locked message appears.
3. Supports the **Master Admin** setting, which grants full administrator privileges.
4. Reflects global cybersecurity standards and the latest security requirements.
5. Supports real-time monitoring of the device's multiple statuses in BioStar X.
6. Supports the **Extended Door Open Time** feature, which allows certain users to have the door remain open longer than the default door open time.
7. Supports the **Door Mode Override** feature, which restores the door to its normal state after the administrator changes the door status and a certain period of time has elapsed.
8. Supports controlling the relay of a connected door from the device menu.
9. Improved facial authentication and face anti-spoofing performance in low-light and strong external light environments.
10. Improved RTSP playback compatibility with Genetec Security Center.
11. Improved to distinguish devices that support the **Server Private Message** feature.
12. Updated product power specifications in the **Regulatory & Licenses** menu.
    - 24V - 1.2A → 24V - 0.7A
    - 12V - 2.5A → 12V - 1A
13. Supports not logging events when the **Ignore Repeated Signals Duration** feature is activated.
14. Added identification code to support recognition of the latest cards.
    - DESFire EV3

15. Improved to distinguish devices that support the **Secure Tamper** feature.
16. Supports saving setting values other than **Check Before Authentication** when configuring the **Require No Mask** using the SDK.
17. Supports SL1, SL3, and SL1/SL3 Mix Mode for security level compatibility with MIFARE Plus EV1 cards.
    - SL1: Compatible mode with MIFARE Classic
    - SL3: Advanced security mode based on AES
18. Improved time synchronization behavior between server and devices.

Bug Fixes

1. Users created by adding the numeric string '00' to the user ID are set as administrators but fail to authenticate when entering the menu. Affects version: 1.0.0
2. When the AoC issued to a user whose user ID includes the string '00' is suspended, authentication is still successful. Affects version: 1.0.0
3. Authentication with a QR code fails when the **T&A Mode** is set to **By User** for large data QR codes, but re-authentication with the QR code succeeds without selecting **T&A**. Affects version: 1.3.0
4. Calling the BS2_GetDeviceCapabilities function on a slave device connected via RS-485 outputs incorrect values. Affects version: 1.0.0
5. When authenticating a custom smart card, there is an issue where the user ID value is incorrectly output. Affects version: 1.3.0
6. When network status is normal, unnecessary automatic connection occurring. Affects version: 1.0.0
7. Custom smart cards with the **DESFire Advanced** option enabled fail to be recognized. Affects version: 1.3.0
8. The **Scramble Keypad** setting changed on the server was not applied properly. Affects version: 1.3.1
9. Some smart cards fail to be recognized in environments using the new SE chip firmware. Affects version: 1.0.0
10. The master device restarts abnormally after 31 slave devices are connected. Affects version: 1.3.1
11. When a user with more than two cards enrolled attempts card authentication to the Wiegand output device, the ID of a card other than the authenticated card is output. Affects version: 1.0.2
12. The device fails to recognize inverted QR code images. Affects version: 1.1.0
13. Arm/Disarm actions did not operate correctly on specific Supervised Input port of the DM-20 connected as a slave. Affects version: 1.0.0
14. Wiegand format card data of 25 bits or less is not recognized. Affects version: 1.0.0

15. The device restarts abnormally when the **User** menu is continuously touched. Affects version: 1.3.1
16. Cannot connect to a hidden wireless network (Wi-Fi) without a password. Affects version: 1.3.1
17. When the issued Template on Mobile is tagged during **Write Smart Card** or **Format Card**, a failure sound occurs, but authentication is still successful. Affects version: 1.2.0
18. The database does not migrate when using the getOperator function in the SDK. Affects version: 1.0.0
19. When the card ID of an issued smart card is 32 digits, the card data is not correctly recognized during authentication with a Wiegand reader. Affects version: 1.0.0
20. The device abnormally restarts when exporting user information to USB memory. Affects version: 1.3.1
21. If a user is viewing the event log and the **Menu Timeout** elapses, causing the device screen to turn off, re-authentication of the device displays the duplicated event log. Affects version: 1.0.0

Firmware Version 1.3.1 (Build No. 1.3.1_240902)

Release | 2024-09-03

New Features and Improvements

1. Improved the issue that occurs when the **Display Name** of the saved extension number is long.
   - Improved to show an ellipsis in the extension number list for long display names.
   - On the call screen, only the middle part of the **Display Name** is displayed.
   - Improved wrapping of long display names on the call screen.
2. Improved UI in **Advanced Settings** screen in **AUTHENTICATION**.
3. Improved vulnerability in conditions required when setting **RTSP** login password.
4. Added **Store Visual Face Image** feature.
   - Supports the feature to save both the actual image and the template in the visual face, or to save only the template without storing the actual image.
5. Added an option to enable or disable the **Scramble Keypad**, which randomizes the position of numeric keys when entering a PIN.
   - **AUTHENTICATION** → **Scramble Keypad**
6. Added a feature that prevents facial authentication from occurring at close range to reduce false authentication during facial authentication at close range.
7. Improved face anti-spoofing performance.

   Info

   - Face anti-spoofing performance has been improved to pass the iBeta Level 1 ISO 30107-3 Presentation Attack Detection Test.
   - We recommend using the **Fake Detection** feature set to **Normal** in environments with strong sunlight.
8. Added **FAS_IR_SP** in **Device Info** to check the algorithm version of face anti-spoofing.
9. Added a **Require No Mask** option that allows rejecting authentication for users wearing a mask during face authentication.
10. Added **Hidden Network** that allows manually adding and connecting to a wireless network by directly entering network information on the device.
11. Improved to periodically check the Wi-Fi signal strength of the connected wireless network, ensuring the Wi-Fi signal strength icon on the home screen is updated.

Bug Fixes

1. When setting a user validity **Period**, an error message is not displayed when the **Start Date** is set to exceed the **End Date**. Affects version: 1.2.0
2. Fixed some strings in user validity **Period** settings. Affects version: 1.0.0
3. The keypad that appears when setting certain menus is hidden from view by obscuring the menu. Affects version: 1.0.0
4. When the name of a **Schedule** created in BioStar 2 is long, the schedule name overlaps with the UI in menus where schedule settings are required. Affects version: 1.0.0
5. When a long server address is entered in the **Edit Server** menu, the server URL text overlaps with the screen UI. Affects version: 1.0.0
6. When an initialized device is connected as a slave via RS-485, the LED status indicator on the slave device blinks blue and green. Affects version: 1.0.0
7. Intermittently, the settings in face authentication are not saved. Affects version: 1.0.0
8. When the device does not have a face authentication mode, after registering 50,000 face credential users and setting the face authentication mode, the menu freezes when entering the user menu. Affects version: 1.0.0
9. When deleting an **Extensions** from the extension list, the **Display Name** of other configured extension numbers disappears. Affects version: 1.0.0
10. The device language was changed, but some menus are not displayed in the selected language. Affects version: 1.0.0
11. When checking the event logs, if the user menu is accessed after scanning a face on the device via BioStar 2, the **EVENT LOG** screen remains open. Affects version: 1.0.0
12. In the extension number selection screen, the area at the bottom of the background screen should not be touchable, but it is responsive to touch. Affects version: 1.0.0
13. When entering an unsupported key in the **ID** field during user registration, the cursor moves one position forward. Affects version: 1.0.0
14. When activating **Voice Instruction** on a slave device connected to BioStar 2 and then accessing the user menu on the slave device, an authentication failure voice prompt is incorrectly played. Affects version: 1.0.0
15. The top-right corner of the background in the **Event Log Details** screen is touched, causing unintended interactions. Additionally, the event log search or the '**Delete all logs?**' pop-up messages may appear incorrectly. Affects version: 1.0.0
16. During an **Intercom** call, it is possible to scan a face or card on the device through BioStar 2. Affects version: 1.0.0
17. When exiting the **Arm** mode during an **Intercom** call, the home screen is displayed incorrectly. Affects version: 1.0.0
18. When the user ID is long, the **User ID** name overlaps with the UI on the event log detail view screen.

Affects version: 1.1.0

19. In BioStar 2, after setting **Image Log** to **Enabled**, the image log icon on the device does not display correctly when a **Template on Mobile** related log occurs. Affects version: 1.2.0

20. When authenticating an iClass AoC card and a fingerprint simultaneously, the device restarts abnormally. Affects version: 1.0.0

21. When the **Reset Time** for **Timed Anti PassBack** is set to 0, anti-passback does not work. Affects version: 1.0.0

22. During an **Intercom** call, the screen incorrectly displays 'Connected' instead of 'In Call'. Affects version: 1.0.0

23. When the maximum number of extensions that can be stored on the device is reached, a blank space appears at the bottom of the call screen. Affects version: 1.3.0

24. When automatically reconnecting to a previously connected wireless network, the WLAN icon on the home screen appears gray. Affects version: 1.0.0

25. When the bit interval is set for the **Facility Code** and **ID Field** of the Wiegand card format and the card is scanned during add user, the **Facility Code** is displayed as an incorrect value. Affects version: 1.0.0

26. When the device is restarted with the **Primary Key** set only in the **Suprema Smart Card Layout** and the **Secondary Key** set only in the **Custom Smart Card Layout**, the device recognizes the Custom Smart Card as a CSN card. Affects version: 1.3.0

27. When a short **DNS Server Address** is entered, the device fails to connect to the DNS server properly. Affects version: 1.0.0

28. When the face sensor sensitivity on the device is set to **High** using the SDK, the motion sensor intermittently does not work. Affects version: 1.0.0

29. The device freezes when the RS-485 mode on the device is set to **Not Use** using the SDK. Affects version: 1.0.0

30. Issue when attempting **Reconnect** on a device configured in **Trigger & Action** to deactivate upon disconnection from BioStar 2. Affects version: 1.1.0

    - Logs 'BioStar 2 Disconnected' and 'Device Locked' are repeatedly generated.
    - The device fails to reconnect to the server after the connection is lost.

Firmware Version 1.3.0 (Build No. 1.3.0_240514)

Release | 2024-06-28

New Features and Improvements

1. XPass D2 new BLE (Bluetooth Low Energy) chip firmware (Build No. 1.7.0_220921) support.
    - 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. Supports **Custom Smart Card Layout**.
3. Improved to not recognize SEOS configuration cards as CSN for 1 minute after device booting.
4. Added event code for QR authentication.
5. Support for adding FeliCa card to **Custom Smart Card Layout**.
6. Extended the user expiration period to a maximum of '**2037-12-31**'.
7. Supports the **Display Result from Controller** feature for displaying authentication success or failure results from a 3rd party controller on the device screen when using **Intelligent Slave**.
8. Supports the **Ignore Repeated Signals Duration** feature, which ignores repetitive authentication signals from the controller when the device is connected to a 3rd party controller via Wiegand.
9. Improved **Intercom** screen UI.
10. Supports the **SIP Server Transport** feature, which selects the SIP transmission method when setting up the SIP server of **Intercom** on the device.
11. Supports the feature of selecting the resolution of the video output from the device when using **Intercom** and **RTSP**.
    - Intercom Video Resolution
    - RTSP Video Resolution
12. Improved to get user update succeeded event log using the GetLogWithFilter function in the SDK.
13. Supports the **Auth Result Display Option** that allows you to select how the user ID and name are displayed on the authentication result screen of the device.
14. Improved pop-up message displayed when authentication fails for users who set the second credential as a fingerprint in **Extended Private Auth Mode**.

Bug Fixes

1. When the maximum number of extension numbers that can be stored on the device is exceeded, the **Add Extension** icon is still displayed. Affects version: 1.0.0

2. An issue occurs when authenticating with a face not wearing a mask on a device with the **Mask Detection** set to **Enabled (Soft)** and the mask check method set to **Check After Authentication**. Affects version: 1.0.0
   - An authentication mode error occurs intermittently.
   - The device freezes when facial authentication is continuous.
3. When the Wireless AP power is turned off and the device is restarted, the wireless network does not automatically reconnect when the AP power is turned back on. Affects version: 1.0.0
4. When the **Auth Mode** is set to Card / QR Code and the mask check method is set to **Check Before Authentication** on the device, QR authentication intermittently fails after wearing a mask and authenticating. Affects version: 1.1.0
5. If device settings are changed in BioStar 2 during an intercom call, card authentication fails after the call ends. Affects version: 1.1.0
6. Authentication fails when authenticating with a DESFire AoC while the device is connected as a slave. Affects version: 1.0.0
7. When **Relay** is set in the device menu, the door does not open with a mobile card. Affects version: 1.0.0
8. If a general user performs face authentication and checks the event log, the **Menu Timeout** elapses, and the device switches to a standby state, the **EVENT LOG** screen appears at the next face authentication. Affects version: 1.0.0
9. The authentication guide message was displayed incorrectly when pressing the **Arm/Disarm** button on the home screen while setting the **Intrusion Alarm Zone**. Affects version: 1.0.0
10. When network is repeatedly disconnected in an environment using a wireless network, RF card authentication will fail. Affects version: 1.0.0
11. 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
12. The device would not automatically reconnect to the previously connected wireless network when restarted while the network was connected as **Wireless**. Affects version: 1.0.0
13. If the network is connected to a wireless LAN and then enters **Wireless** again after changing to an ethernet connection, the wireless AP list is not displayed. Affects version: 1.0.0
14. Infinite loading occurred while attempting to connect via **Wireless**. Affects version: 1.0.0
15. When the network is connected to **Wireless**, switches to **Ethernet**, and then switches back to **Wireless**, it does not automatically reconnect to the previously connected wireless network. Affects version: 1.0.0
16. Image Logs were not deleted when performing **Factory Default** on the device. Affects version: 1.0.0
17. 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
18. If the number of fingerprints stored in the device exceeds the 1:N maximum, the **Finger** in **User Usage** count is displayed abnormally. Affects version: 1.0.0

19. The Wi-Fi signal strength of the connected wireless network was displayed differently in the wireless LAN list and the WLAN icon on the home screen. Affects version: 1.0.0

20. On the home screen of a device with **Auth Mode** set to ID + Face/PIN, after entering the ID, the **Input ID** icon allows to enter PIN instead of changing the authentication process to the entered ID. Affects version: 1.0.0

21. Deleted image logs from the device gets continuously uploaded to the server. Affects version: 1.0.0

22. When the device's **Device** → **Server** setting gets inactive while the device is on the **Waiting Device** list of BioStar 2, the device still appears in the **Waiting Device** list, and the BioStar 2 connect icon is displayed at the top of the device. Affects version: 1.0.0

23. The facial authentication process continues to operate even after mask detection is completed on a device where the Wiegand device's **Output Mode** is set to **Bypass** and the mask check mode is set to **Check Only**. Affects version: 1.1.0

24. When enrolling a Visual Face by uploading a photo using the API, a blank area appears on the photo, and authentication fails intermittently. Affects version: 1.0.0

25. When setting the face authentication operation mode on a device using the SDK's BS2_SetFaceConfig function, there is an issue where an infinite reboot occurs if an incorrect value is entered. Affects version: 1.0.0

26. When creating a schedule with an invalid ID using the SDK, the device fails to boot properly. Affects version: 1.0.0

27. When the number of faces stored on the device exceeds the 1:N maximum, administrator login is possible via facial authentication. Affects version: 1.1.0

28. When using **Device** → **Server** mode, the server IP address is reset if the connection to the DHCP server fails. Affects version: 1.0.0

Firmware Version 1.2.1 (Build No. 1.2.1_231113)

Release | 2023-11-27

Firmware Repackaging

Firmware Version 1.2.0 (Build No. 1.2.0_231005)

Release | 2023-10-05

New Features and Improvements

1. Supports **Template on Mobile**.
2. Improved face anti-spoofing performance when **Operation Mode** is set to **Fusion Matching** and **Fake Detection** is set to **Normal**.
3. Fixed strings in the **Use QR as Card** menu.
4. Separated event code for QR authentication.
5. Added Voice Instruction.
6. Updated Japanese regulatory certification electronic notation.

Bug Fixes

1. The **Server URL** for device's **Device ▸ Server Connection** in BioStar 2 does not appear on the device configuration. Affects version: 1.0.1
2. Authentication result does not appear when authenticating with entering ID followed by an action returning to home screen after entering the menu as an administrator. Affects version: 1.0.0
3. The screen overlaps when swiping to scroll the Event Log list screen. Affects version: 1.0.0
4. When authenticating with ID + PIN on a device connected as a slave, the user ID is displayed but the user name is not displayed. Affects version: 1.1.1
5. Firmware upgrade succeeds with an invalid resource file. Affects version: 1.0.0
6. When upgrading firmware, resource file included in the firmware does not get updated. Affects version: 1.0.0
7. When user information is sent from BioStar 2 to a master device that does not have 1:N authentication mode, 1:N authentication fails on the device connected as a slave. Affects version: 1.0.0
8. Restart log is not logged in the device's **Event Log** when the master device is restarted. Affects version: 1.0.1
9. The device turns off when the user **Format Card** in BioStar 2. Affects version: 1.0.0
10. Device freezes or restarts when continuously authenticating with an EM card. Affects version: 1.0.0
11. When devices are connected as a master-slave and the door is deleted and added again, the door does not open even if

authentication has succeeded with the device connected as a slave. Affects version: 1.0.0

12. Fixed string for scheduled lock zone violation. Affects version: 1.0.0

13. Fixed smartcard output byte order setting. Affects version: 1.1.0

    - When using Wiegand or OSDP output, it is fixed to be affected by the smartcard output byte order when the Wiegand output information is set to send user ID.

Firmware Version 1.1.1 (Build No. 1.1.1_230621)

Release | 2023-06-28

Bug Fixes

1. Device does not recognize certain HID iCLASS Seos cards. Affects version: 1.0.0
2. When authenticating with a BLE mobile card running on iOS, authentication fails and the device restarts intermittently. Affects version: 1.0.0
3. When a user registered from FaceStation F2 v1.x.x is sent to BioStation 3 through BioStar 2, the device restarts. Affects version: 1.1.0
4. Entering ID and PIN to access administrator menu reaches timeout quicker than expected. Affects version: 1.0.0
5. When authenticating with a card while face authentication mode is off and QR is disabled, the camera preview screen is displayed after the authentication result appears. Affects version: 1.0.0
6. LED indicator operation is maintained even when the device is locked due to an event set in **Trigger & Action**. Affects version: 1.0.0

Firmware Version 1.1.0 (Build No. 1.1.0_230414)

Release | 2023-04-19

New Features and Improvements

1. Supports QR code recognition and authentication using the camera.
2. Supports activating licenses for use of specific features on devices.
3. Improved LED operation according to illuminance.
4. Supports Thai font.
5. Added Japanese regulatory certification electronic notation.
6. Improved performance of the authentication result displayed when face authentication is performed from a slave device.
7. Improved smartcard output byte order setting.
    - When using Wiegand or OSDP output, it is improved to be affected by the smartcard output byte order when the Wiegand output information is set to send user ID.
8. Improved performance of the authentication result and LED action.
9. Improved scrolling performance in lists when querying users or logs.
10. Improved call failure pop-up messages and end call operation when **SIP Intercom** when there is no response from the other party.
11. Optimized camera performance to enhance face and QR authentication performance in various illuminance environments.
12. Improved mask detection algorithm.
13. Improved to display an error message when pressing **OK** when there are unentered items from **SIP Setting** in the **Intercom** of the device.
14. Improved face anti-spoofing performance.

Bug Fixes

1. Applying an invalid custom resource causes the device to restart. Affects version: 1.0.0
2. Face authentication fails on a slave device when the master device restarts without having any **Auth Mode**. Affects version: 1.0.0
3. Changing the **Auth Timeout** in BioStar 2 does not apply to the device. Affects version: 1.0.0

4. An issue where an administrator with the device setup operating level can initialize the device. 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 face authentication is performed while pressing the Call button on the main screen to use the **Intercom**, only the main screen is displayed instead of the intercom screen. Affects version: 1.0.0

Firmware Version 1.0.2 (Build No. 1.0.2_230111)

Release | 2023-01-20

New Features and Improvements

1. Supports a new SE processor and new firmware.
    - Support downgrade to lower version firmware.
2. Fixed incorrect **Partial Modify Fail (Server)** log occurred by changing user information from the server where the user does not exist on the device.

Bug Fixes

1. When using the relay of the master device for the door, the door does not open when authenticating from the device connected as a slave. Affects version: 1.0.0
2. Face authentication does not work when set to low **Baud Rate** in **Serial Setting**. Affects version: 1.0.0
3. Missing custom font files other than English and Korean. Affects version: 1.0.0
4. When authenticating with face, the Wiegand port outputs an incorrect value as other user information that was previously authenticated with card. Affects version: 1.0.0
5. Door Locked event occurs when input signal gets detected while configured to Arm/Disarm by input signal. Affects version: 1.0.0
6. Modifying the authentication mode causes other previously set authentication modes to disappear. Affects version: 1.0.0
7. The list number column and list column overlaps on the extension number screen. Affects version: 1.0.0
8. When issuing a smartcard including a visual face template using the SDK, the card scan screen suddenly disappears. Affects version: 1.0.0

Firmware Version 1.0.1 (Build No. 1.0.1_221020)

Release | 2022-10-21

New Features and Improvements

1. Improved motion detection performance for low-light environments.
2. Improved Visual Face matching algorithm.
3. Improved all pop-up messages displayed on the device to operate according to the time set in **Message Timeout**.
4. Fixed Korean and English strings in the **RTSP** menu.

Bug Fixes

1. When upgrading resources or firmware from BioStar 2, the device could not check the progress of the upgrade because no information was displayed. Affects version: 1.0.0
2. When synchronizing multiple users to a device in BioStar 2 and then restarting the device, the **User Usage** on the device displays a different number of visual faces than the number of synchronized. Affects version: 1.0.0
3. When entering the device detail page after adding a logo image to the device connected as a slave, an Invalid payload error occurs and the RS-485 get disconnected. Affects version: 1.0.0
4. When **Device Hashkey Management** is set to **Use** in BioStar 2 and migration proceeds, all users are deleted from the device, but a delete notification pop-up is not displayed. Affects version: 1.0.0
5. Device hangs intermittently and then restarts. Affects version: 1.0.0
6. When entering the **Wireless**, the new SSID does not appear, but only the previously searched SSID appears. Affects version: 1.0.0
7. When enrolling a visual face or card on a device using the BioStar 2, the scan screen is not visible and the screen saver state remains. Affects version: 1.0.0
8. When the call button on the main screen is pressed with only one extension number stored in the device, it does not connect directly. Affects version: 1.0.0
9. In **Edit User**, if you select **Extended Private Auth Mode** as **ID** + **Fingerprint/PIN** and press **OK**, the fingerprint icon is incorrectly displayed as a face icon in the **Extended Private Auth Mode** list. Affects version: 1.0.0
10. Authentication failure occurs when authenticating with AoC with private auth mode set to **Card** + **Face**. Affects version: 1.0.0

11. When the device is restarted via BioStar 2, only a notification sound plays and the restart pop-up message does not appear. Affects version: 1.0.0
12. Firmware upgrade via USB restarts the device without a success or failure popup message. Affects version: 1.0.0
13. In BioStar 2's **T&A** menu, the **Schedule** display part is blank when creating a **T&A Code** with a **Schedule** other than **Always** and selecting the **T&A Code** on the device. Affects version: 1.0.0
14. Memory usage incorrectly displayed in **DRAM Usage** in **Memory Info**. Affects version: 1.0.0
15. When entering the menu from a device connected as a slave, a normal menu touch sound plays instead of a warning sound. Affects version: 1.0.0
16. When enrolling a visual face in the **USER** menu in BioStar 2, when the scan waiting time exceeded while enrolling the 1st face and then scanning the 2nd face, the face enrolled in the 1st appears. Affects version: 1.0.0
17. If the network is connected to a wireless LAN and then enters **Wireless** again after changing to an ethernet connection, the wireless AP list is not displayed. Affects version: 1.0.0
18. Device hangs intermittently when Wiegand **Input/Output** setting is set to **Output**. Affects version: 1.0.0
19. Extension number gets stored in the phonebook while exceeding the maximum characters in the **Display Name** of the **Intercom** settings. Affects version: 1.0.0
20. When entering the edit screen by selecting the **Auth Mode** set in the device's **Auth Mode**, the touch sound does not play. Affects version: 1.0.0
21. Device connected as a slave intermittently operates while disconnected. Affects version: 1.0.0
22. An error occurs when calling the extension number when the **Intercom** of the device is set to **Not Use** via BioStar 2 while the list of extension numbers is displayed by pressing the call button on the main screen of the device. Affects version: 1.0.0
23. In the screen to set the **Schedule** in **Auth Mode**, the already created schedule is shown as a duplicate. Affects version: 1.0.0
24. When the device is in the middle of **Factory Default** process, the device hangs while loading. Affects version: 1.0.0
25. When the **Language** of the device is set to **Custom**, the **Voice Instruction** menu part of **Sound** displays as a blank. Affects version: 1.0.0
26. When the **Time Zone** of the master device connected via RS-485 is changed, the **Time Zone** of the slave device does not change. Affects version: 1.0.0
27. When authenticating with a mobile card set to NFC, authentication fails and the device restarts intermittently Affects version: 1.0.0
28. The correct message does not appear when an unenrolled card is scanned with **Filter** set to **Card** in the user search Affects version: 1.0.0
29. The pop-up to set the **Filter** on the **EVENT LOG** search screen does not disappear even after the time set in the device's **Menu Timeout** has elapsed. Affects version: 1.0.0

30. Event log is not logged when **Time Zone** is changed on the device. Affects version: 1.0.0
31. When scanning **Visual Face** via BioStar 2 while the device is in the **SETTINGS**, the scan screen does not close on the device even after scanning is complete. Affects version: 1.0.0
32. **Baud Rate** selection pop-up appears when touching an empty space at the bottom of the **Ethernet** screen. Affects version: 1.0.0
33. When sending a user whose card is duplicated with another user from BioStar 2 to the device, the user is deleted from the device. Affects version: 1.0.0
34. When the firmware is upgraded for each device connected as master-slave, the slave device completes normally, but the master device hangs. Affects version: 1.0.0
35. RTSP connection termination event log is not logged and RTSP icon is not deleted even after setting **RTSP** to **Not Use**. Affects version: 1.0.0
36. Does not restart on **Restore Default** due to setup error. Affects version: 1.0.0
37. **Date & Time** not displayed correctly. Affects version: 1.0.0
38. When adding a user, the backlight does not turn off when waiting without card input on the card scan screen. Affects version: 1.0.0
39. Search does not work when searching by **Start Time** and **End Time** in **EVENT LOG**. Affects version: 1.0.0
40. An incorrect schedule displays in the **Edit Auth Mode**. Affects version: 1.0.0
41. If you scan a Wiegand format card that is not set when enrolling a card to a user and then scan a normal card, it will not be scanned. Affects version: 1.0.0
42. The device retains the call screen even after the recipient terminates the call. Affects version: 1.0.0
43. **WiFi MAC** does not appear in **DASHBOARD** and **Device Info** for Wi-Fi supported models. Affects version: 1.0.0
44. On the scan card screen, the background allows touch and the face can get authenticated. Affects version: 1.0.0
45. When enrolling a card in BioStar 2, after selecting **Write Smart Card**, the device restarts while waiting for scan. Affects version: 1.0.0
46. An issue occurs when upgrading the firmware of a slave device from BioStar 2 while the device is connected as Master-Slave. Affects version: 1.0.0
    - Slave device disconnects and the firmware upgrade fails.
    - Master device restart fails.
47. The **OK** button does not work when repeatedly searching the **EVENT LOG**. Affects version: 1.0.0
48. Intermittently, the image log is logged abnormally. Affects version: 1.0.0
49. Speaker turns on and off repeatedly when multiple sound files are played continuously. Affects version: 1.0.0

50. The device restarts abnormally when the firmware is upgraded while the device is locked. Affects version: 1.0.0
51. Wireless connection intermittently disconnects when sending Visual face from BioStar 2 to device. Affects version: 1.0.0
52. The screen turns off at the time set in **Menu Timeout** during an Intercom call. Affects version: 1.0.0
53. When deleting all logs, image logs does not get deleted. Affects version: 1.0.0
54. **VFMCore** version information is not displayed when long-touching the **MAC** in **Device Info**. Affects version: 1.0.0
55. When issuing a **Smart Card**, if a fingerprint/face is included in **Private Auth Mode**, the issuance fails intermittently in a specific card. Affects version: 1.0.0

Firmware Version 1.0.0 (Build No. 1.0.0_220901)

Release | 2022-09-01

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.