Table of Contents

Version 1.4.0 (V1.4.0_250909)

Release

2025-09-09

- 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 (https://supremainc.com).

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: v1.0.0)

2. When the AoC issued to a user whose user ID includes the string '00' is suspended, authentication is still successful. (Affects version: v1.0.0)

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: v1.3.0)

4. Calling the BS2_GetDeviceCapabilities function on a slave device connected via RS-485 outputs incorrect values. (Affects version: v1.0.0)

5. When authenticating a custom smart card, there is an issue where the user ID value is incorrectly output. (Affects version: v1.3.0)

6. When network status is normal, unnecessary automatic connection occurring. (Affects version: v1.0.0)

7. Custom smart cards with the **DESFire Advanced** option enabled fail to be recognized. (Affects version: v1.3.0)

8. The **Scramble Keypad** setting changed on the server was not applied properly. (Affects version: v1.3.1)

9. Some smart cards fail to be recognized in environments using the new SE chip firmware. (Affects version: v1.0.0)

10. The master device restarts abnormally after 31 slave devices are connected. (Affects version: v1.3.1)

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: v1.0.2)

12. The device fails to recognize inverted QR code images. (Affects version: v1.1.0)

13. Arm/Disarm actions did not operate correctly on specific Supervised Input port of the DM-20 connected as a slave. (Affects version: v1.0.0)

14. Wiegand format card data of 25 bits or less is not recognized. (Affects version: v1.0.0)

15. The device restarts abnormally when the **User** menu is continuously touched. (Affects version: v1.3.1)

16. Cannot connect to a hidden wireless network (Wi-Fi) without a password. (Affects version: v1.3.1)

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: v1.2.0)

18. The database does not migrate when using the getOperator function in the SDK. (Affects version: v1.0.0)

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: v1.0.0)

20. The device abnormally restarts when exporting user information to USB memory. (Affects version: v1.3.1)

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: v1.0.0)

From:
https://kb.supremainc.com/knowledge/ -

Permanent link:
https://kb.supremainc.com/knowledge/doku.php?id=en:bs3_revision_note_140

Last update: **2025/12/26 07:57**