FaceStation F2

RELEASE NOTES

Version 2.3.1

English
EN 301.00.FSF2

suprema
SECURITY & BIOMETRICS

CONTENTS

- Firmware Version 2.3.1
- Firmware Version 2.3.0
- Firmware Version 2.2.2
- Firmware Version 2.2.1
- Firmware Version 2.2.0
- Firmware Version 2.1.4
- Firmware Version 2.1.3
- Firmware Version 2.1.2
- Firmware Version 2.1.1
- Firmware Version 2.1.0
- Firmware Version 2.0.3
- Firmware Version 2.0.2
- Firmware Version 1.1.4
- Firmware Version 1.1.2
- Firmware Version 1.1.1
- Firmware Version 1.0.5
- Firmware Version 1.0.4
- Firmware Version 1.0.3
- Firmware Version 1.0.2
- Firmware Version 1.0.1
- Firmware Version 1.0.0

Firmware Version 2.3.1 (Build No. 2.3.1_260922)

Release | 2026-09-22

Caution

- For devices with the new SE processor, after upgrading the firmware to v2.1.0 or higher, you cannot downgrade to a lower version and downgrade the firmware customized in the lower version.
  Devices with existing SE processor can be downgraded to a lower version.
- The devices using the new LCD display cannot be downgraded to a version earlier than v2.2.1 after upgrading the firmware to v2.2.1 or higher.
- 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: 2.3.0
2. **Anti-passback** status not updating after door control through authentication in a **Timed Anti-passback** environment. Affects version: 2.3.0
3. Child Wiegand reader not being locked by **Trigger & Action** when a door is created with a Wiegand reader. Affects version: 2.3.0
4. Logs recorded multiple times when a relay is configured in **Trigger & Action** or **Zone** alarm. Affects version: 2.3.0
5. Lock icon disappearing when a slave device is rebooted while the door is manually unlocked. Affects version: 2.3.0

Firmware Version 2.3.0 (Build No. 2.3.0_260818)

Release | 2026-08-19

Caution

- For devices with the new SE processor, after upgrading the firmware to v2.1.0 or higher, you cannot downgrade to a lower version and downgrade the firmware customized in the lower version.
  Devices with existing SE processor can be downgraded to a lower version.
- The devices using the new LCD display cannot be downgraded to a version earlier than v2.2.1 after upgrading the firmware to v2.2.1 or higher.
- 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. Supports real-time monitoring of the device's multiple statuses in BioStar X.
3. Supports the **Extended Door Open Time** feature, which allows certain users to have the door remain open longer than the default door open time.
4. 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.
5. Supports controlling the relay of a connected door from the device menu.
6. Added support for unlocking or normalizing a door through user authentication.
7. Improved so that when authentication is attempted on a door set to **Manual Lock**, an authentication failure event occurs and a locked message appears.
8. Improved OSDP reader mode to display "Access Denied" when access is denied by a third-party control panel.
9. Improved door control status to accurately display control results and change details in monitoring.
10. Improved BLE stability.
11. 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
12. Improved Fire alarm zone status display and alarm clearing behavior after power restart following a fire alarm.

Bug Fixes

1. Suprema Mobile Access authentication failing on certain Android devices. Affects version: 1.0.0
2. Devices that do not support the buzzer failing to connect when integrated with an OSDP panel. Affects version: 1.0.0
3. Card authentication failure on connected Wiegand readers. Affects version: 1.0.0
4. Device freezing or rebooting when face authentication occurs while adding or deleting users. Affects version: 1.0.0
5. Device freezing or rebooting and delayed user enrollment during user synchronization. Affects version: 1.0.0

Firmware Version 2.2.2 (Build No. 2.2.2_260518)

Release | 2026-05-19

Caution

- For devices with the new SE processor, after upgrading the firmware to v2.1.0 or higher, you cannot downgrade to a lower version and downgrade the firmware customized in the lower version.
  Devices with existing SE processor can be downgraded to a lower version.
- The devices using the new LCD display cannot be downgraded to a version earlier than v2.2.1 after upgrading the firmware to v2.2.1 or higher.
- For more information, check the serial number of the device and contact the Suprema.

New Features and Improvements

1. Supports feature to set the baud rate of slave devices.
2. 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
3. Improved to distinguish devices that support the **Secure Tamper** feature.

Bug Fixes

1. Calling the BS2_GetDeviceCapabilities function on a slave device connected via RS-485 outputs incorrect values. Affects version: 1.0.0
2. 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
3. Wiegand format card data of 25 bits or less is not recognized. Affects version: 2.2.0

Firmware Version 2.2.1 (Build No. 2.2.1_241204)

Release | 2024-12-09

> **Caution**
> For devices with the new SE processor, after upgrading the firmware to v2.1.0 or higher, you cannot downgrade to a lower version and downgrade the firmware customized in the lower version.
>
> Devices with existing SE processor can be downgraded to a lower version.
>
> For more information, check the serial number of the device and contact the Suprema.

New Features and Improvements

1. Changes to a new LCD screen.

> **Caution**
> For devices with firmware v2.2.0 or earlier, be sure to upgrade the firmware to the latest version before replacing it with a new LCD display.
>
> The devices using the new LCD display cannot be downgraded to a version earlier than v2.2.1 after upgrading the firmware to v2.2.1 or higher.

Bug Fixes

1. After a firmware upgrade, authentication failure occurs with the previously used cards. Affects version: 2.2.0
2. When using **Thermal Camera** mode with the TCM10 connected, the face authentication screen is displayed abnormally. Affects version: 2.0.1
3. Custom smart cards with the **DESFire Advanced** option enabled fail to be recognized. Affects version: 2.2.0
4. Some smart cards fail to be recognized in environments using the new SE chip firmware. Affects version: 2.1.4
5. The **Mask All but First Letter** option in the **Auth Result Display Option** is not applied correctly. Affects version: 2.2.0
6. After transferring more than 50,000 users with 1:N credentials to the device and then upgrading the firmware, the device freezes. Affects version: 2.1.1
7. 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: 2.1.1

Firmware Version 2.2.0 (Build No. 2.2.0_240704)

Release | 2024-07-10

> **Caution**
> For devices with the new SE processor, after upgrading the firmware to v2.1.0 or higher, you cannot downgrade to a lower version and downgrade the firmware customized in the lower version.
>
> Devices with existing SE processor can be downgraded to a lower version.
>
> For more information, check the serial number of the device and contact the Suprema.

New Features and Improvements

1. Supports **Custom Smart Card Layout**.
2. 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.
3. Supports **Template on Mobile**.
4. 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.
5. 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.
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 duplicate fingerprint detection.
10. Improved to get user update succeeded event log using the GetLogWithFilter function in the SDK.
11. 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.
    - **User ID Display**
    - **User Name Display**

12. Improved to ensure that values set with osdp_comset are correctly applied on the device connected as a slave.

Bug Fixes

1. When issuing an AoC (**Access On Card**) or **Secure Credential Card** using a **Face Template**, the device shuts down abnormally. Affects version: 1.1.0
2. 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: 1.1.0
3. When devices are connected as master-slave, if the slave device is disconnected or deleted, the master device restarts. Affects version: 1.1.0
4. Device abnormally restarts when changing the device's **Network** settings in BioStar 2. Affects version: 1.1.0
5. Face authentication fails on a slave device when the master device restarts without having any **Auth Mode**. Affects version: 1.1.0
6. Intermittently, the door does not open even if authentication succeeds when the door uses the slave device's relay. Affects version: 1.1.0
7. **Device -> Server** mode could be set without entering a **Server IP** address in the **Server** menu. Affects version: 1.1.0
8. When a fingerprint is entered into the slave device and fingerprint matching is in progress, the master device does not accept a fingerprint scan. Affects version: 1.0.0
9. Authentication fails when authenticating with a DESFire AoC while the device is connected as a slave. Affects version: 1.0.0
10. When **Relay** is set in the device menu, the door does not open with a mobile card. 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: 1.1.0
12. When the device and BioStar 2 are connected using two ethernet hubs, the device does not automatically reconnect to BioStar 2 after the LAN cable between the hubs is disconnected and reconnected. Affects version: 1.1.0
13. 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: 1.1.0
14. When the **Reset Time** for **Timed Anti PassBack** is set to 0, anti-passback does not work. Affects version: 1.1.0
15. The **Auth Mode** UI intermittently disappears on the device detail page of BioStar 2. Affects version: 1.1.0
16. 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
17. Fixed GPU issues causing broken graphics on the home screen or failures in facial detection. Affects version: 1.0.0

18. Deleted image logs from the device gets continuously uploaded to the server. Affects version: 2.1.1

Firmware Version 2.1.4 (Build No. 2.1.4_230810)

Release | 2023-08-11

> **Caution**
> For devices with the new SE processor, after upgrading the firmware to v2.1.0 or higher, you cannot downgrade to a lower version and downgrade the firmware customized in the lower version.
>
> Devices with existing SE processor can be downgraded to a lower version.
>
> For more information, check the serial number of the device and contact the Suprema.

New Features and Improvements

1. Improved face anti-spoofing performance when **Fusion Matching** and **Fake Detection** are set to **Normal**.
2. Added **Power Line Frequency** option to prevent flicker based on the illuminance environment in which the device is installed.

Bug Fixes

1. When authenticating with a BLE mobile card running on iOS, authentication fails and the device restarts intermittently. Affects version: 1.0.0
2. Device freezes when firmware upgrade to BioStar 2 with more than 50,000 registered users on the device. Affects version: 2.1.1
3. Restart log is not logged in the device's **Event Log** when the master device is restarted. Affects version: 2.1.1
4. Device does not recognize certain MIFARE Classic cards. Affects version: 1.0.0
5. Device does not recognize certain HID iCLASS Seos cards. Affects version: 1.0.0
6. When the device with the working **Screen Saver** is not used for a long time, a black screen occurs and the device freezes. Affects version: 1.0.0

Firmware Version 2.1.3 (Build No. 2.1.3_230525)

Release | 2023-05-30

Caution

For devices with the new SE processor, after upgrading the firmware to v2.1.0 or higher, you cannot downgrade to a lower version and downgrade the firmware customized in the lower version.

Devices with existing SE processor can be downgraded to a lower version.

For more information, check the serial number of the device and contact the Suprema.

New Features and Improvements

1. Improved face anti-spoofing performance.

Firmware Version 2.1.2 (Build No. 2.1.2_230130)

Release | 2023-02-01

Caution

For devices with the new SE processor, after upgrading the firmware to v2.1.0 or higher, you cannot downgrade to a lower version and downgrade the firmware customized in the lower version.

Devices with existing SE processor can be downgraded to a lower version.

For more information, check the serial number of the device and contact the Suprema.

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: 2.1.1
2. The door does not open on authentication when a door deleted from BioStar 2 gets re-added. Affects version: 1.0.0

Firmware Version 2.1.1 (Build No. 2.1.1_221130)

Release | 2022-11-30

> **Caution**
> For devices with the new SE processor, after upgrading the firmware to v2.1.0 or higher, you cannot downgrade to a lower version and downgrade the firmware customized in the lower version.
>
> Devices with existing SE processor can be downgraded to a lower version.
>
> For more information, check the serial number of the device and contact the Suprema.

New Features and Improvements

1. Improved to select and update only the desired information when updating user information. (Compatible with BioStar v2.9.0 or higher)
2. Improved face authentication speed.
3. Improved **Face Detection Setting**
   - **Detection Distance**, **Wide Search** option support.
4. Enhancement in the upgrade package encryption.

Bug Fixes

1. User ID information was not included when using the BS2_GetLogSmallBlobEx function in the SDK to load the event log for the device's mask detection and temperature measurement operation. Affects version: 1.1.2
2. When authenticating on the device where **Mask Detection** is set and the mask detection method set to **Check After Authentication**, the Access Success (Check Only) event occurs. Affects version: 2.0.1
3. In BioStar v2.9.x, a user transferred to the device having a blurry image as visual face credential gets enrolled normally. Affects version: 2.0.3
4. Face gets enrolled normally even if a duplicate face exists on the device. Affects version: 2.0.3
5. In the process of enrolling a face on the device, the scanned face image is tilted. Affects version: 2.0.3
6. Improved the structure to prevent authentication fail caused by broken database or cache memory. Affects version: 1.0.0
7. Door Locked event occurs when input signal gets detected while configured to Arm/Disarm by input signal.

Affects version: 1.0.0

8. When **Dynamic ROI** is activated on a device installed using the TCM-10 and the temperature is measured, the background behind the face is also detected and the temperature is measured higher than the actual temperature. Affects version: 2.0.1

9. Face authentication suddenly does not work on a device that has been using face authentication for a certain period of time (about 50 days or more). Affects version: 2.0.3

Firmware Version 2.1.0 (Build No. 2.1.0_221005)

Release | 2022-10-05

> **Caution**
> For devices with the new SE processor, after upgrading the firmware to v2.1.0 or higher, you cannot downgrade to a lower version and downgrade the firmware customized in the lower version.
>
> Devices with existing SE processor can be downgraded to a lower version.
>
> For more information, check the serial number of the device and contact the Suprema.

New Features and Improvements

1. Supports the dual SE processor.
2. Separated the log related to the cause of the door unlock.
   - Door open request by exit button
   - Door open request by operator
3. 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.
4. Supports setting the byte order for smart cards.
   - Supports setting the byte order of data to be output to Wiegand or OSDP.
5. Improved the OSDP ID to also be deleted when a security tamper occurs on the FaceStation F2 connected as a slave device.

Bug Fixes

1. Migration malfunction occurs when the firmware is upgraded from v1.1.0 or earlier to v1.1.1 or later. Affects version: 2.1.0
   - Migration did not complete and the device boots to the main screen, some keys do not work or an abnormal screen is displayed.
2. Mobile card authentication suddenly does not work. Affects version: 1.0.0
3. 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: 1.0.0

4. The device restarts when a user's face is enrolled consecutively or the main menu is repeatedly touched.
   Affects version: 1.0.0
5. When using the card to authenticate to the device, the card that was normally authenticated fails intermittently.
   Affects version: 1.0.0
6. The preview screen shown on the device during face authentication is different from the actual situation in front of the device. Affects version: 1.0.0
7. If a user enrolled a face while face auth mode is off, and face authentication fails when face auth mode is turned on.
   Affects version: 1.0.0
8. When the device sets the face auth mode to 1:N and sends many user faces on BioStar 2, it is stored even if the maximum number of faces that can be stored on the device is exceeded. Affects version: 1.0.0
9. Improved the structure to prevent authentication fail caused by broken database or cache memory.
   Affects version: 1.0.0

Firmware Version 2.0.3 (Build No. 2.0.3_220705)

Release | 2022-07-15

Bug Fixes

1. Stuck in migration progress after upgrading the firmware. Affects version: 2.0.2
2. Fingerprint sensor not responding after upgrading FSF2-ODB from v1.1.0 to v2.0.2. Affects version: 2.0.2

Firmware Version 2.0.2 (Build No. 2.0.2_220502)

Release | 2022-05-10

New Features and Improvements

1. Visual Face algorithm v2 support.
2. Improved to detect a mask when enrolling a face so that the face cannot be enrolled with a mask on or covering the mouth.
3. Improved Dynamic ROI (Region of Interest) performance.
4. Added a progress bar to screen during migration.
5. Improved to check for the duplication of cards registered with users when transmitting user data from the server to devices.
6. Improved the Arm/Disarm status is maintained if the device loses power.

Bug Fixes

1. When upgrading the firmware from v1.x.x to v2.x.x using a USB memory, the upgrade fails, and when the device is rebooted after removing the USB memory, the device stops in the loading state. Affects version: 1.0.0

   > **Info**
   > When upgrading the firmware using a USB memory inevitably, first set **Menu Timeout** to **Always On** in the **Display & Sound** menu before proceeding with the upgrade. Also, even if a failure message is displayed during the upgrade, DO NOT remove the USB memory and wait until a success message is displayed. The device will restart automatically when the upgrade is complete.

2. When upgrading the firmware from v1.x.x to v2.x.x while the device memory is full, the device does not boot. Affects version: 1.0.0
3. The device restarted abnormally after scanning some cards on the device. Affects version: 1.0.0
4. 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: 1.1.2
5. 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: 1.1.2
6. When communicating with a 3rd party control panel via OSDP, the device does not respond to the Device Capabilities command (FSF2-DB, FSF2-AB). Affects version: 1.0.0

7. The master device restarted abnormally if changing the floor settings after setting up the scheduled unlock zone. Affects version: 1.0.0
8. When different faces are enrolled in one user, authentication failed with the second enrolled face. Affects version: 1.0.0
9. When changing the intelligent slave settings on the detailed page of the device on BioStar 2, the settings were not applied. Affects version: 1.1.4
10. If the user authenticated on the device at the time of Auth Timeout, an incorrect error message was displayed. Affects version: 1.0.0
11. When authenticating with a duress fingerprint on a device with the auth mode set to ID+face+fingerprint/PIN, the duress fingerprint log does not leave. Affects version: 1.0.0
12. Device does not recognize certain HID iCLASS Seos cards. Affects version: 1.0.0
13. Device does not connect to a 3rd party controller (Software House iSTAR Edge G2) via OSDP. Affects version: 1.0.0
14. The device's face authentication and temperature measurement performance has deteriorated in outdoor environments with ceilings. Affects version: 1.0.0
15. The device's mask detection performance has deteriorated when the user wears a specific color mask. Affects version: 1.0.0
16. The device is slow to recognize the EM card. Affects version: 1.0.0
17. If the user authenticated on the device at the time of Auth Timeout, it was authenticated, but the door was not opened. Affects version: 1.0.0
18. When the dual authentication was set on the device, if the fake fingerprint was used in the second authentication, a screen unrelated to the situation was output after authentication failure (FSF2-ODB). Affects version: 1.0.0
19. 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: 1.0.0
20. 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: 1.0.0
21. When upgrading firmware using USB memory, the device reboots after an upgrade failure message is displayed, and the firmware is upgraded afterward. Affects version: 1.0.0
22. Global APB behavior for the same input was different depending on firmware version. Affects version: 1.1.1
23. 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: 1.1.2
24. 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: 1.0.0

25. 'Check Only' was displayed in the event log even though the Check Mode of the thermal camera was set to 'Check After Authentication'. Affects version: 1.1.1

26. When loading the logs for the user who entered the admin menu using the SDK, the user ID was not displayed. Affects version: 1.0.0

27. 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: 1.0.0

28. 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: 1.0.0

29. 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: 1.0.0

30. After issuing a secure credential card with face data to a user, when the user's face data was deleted and the secure credential card was authenticated, authentication failed even though the face template was stored in the card. Affects version: 1.0.0

31. When initializing the master device with the 'Keep Network Settings' option, the RS-485 communication key was initialized and the slave device was disconnected. Affects version: 1.0.0

Firmware Version 1.1.4 (Build No. 1.1.4_220315)

Release | 2022-03-22

> **Caution**
> Before upgrading this firmware, proceed with 'Delete Data & Sync Device' to prevent a very rare case of device lock-up.

New Features and Improvements

1. Changed firmware upgrade method according to dualization for the front cover (LCD & touchpad).
2. Improved to extract a new visual face template from the warped image only if necessary after checking the template version (Algorithm compatibility) when sending templates from BioStar 2 or BioStar Device SDK.

Bug Fixes

1. Structural issues were found in the flash memory. Affects version: 1.1.2 or earlier
   - Long usage of some scenarios could overflow the database, causing the device to lose the ability to boot.
2. After upgrading the firmware, the touchpad recognizes a different part from where the user actually touched. Affects version: 1.1.3
3. Slave devices were disconnected when the master device was rebooted. Affects version: 1.1.2 or earlier
4. The device failed to recognize the iCLASS Seos card intermittently before rebooting the device (FSF2-AB). Affects version: 1.1.2 or earlier
5. When synchronizing user data from the device to the BioStar2 server and retransmitting it to the device, only some users were transmitted or took a long time to transmit. Affects version: 1.1.2 or earlier
   - When a low-quality visual face warped image is synchronized to another device, the synchronization speed is slowed down by continuously retrying synchronization after the template extraction fails on that device due to the low quality.
6. If the 'Access Granted' event was set in Trigger & Action, the temperature was abnormally displayed as 'NaN' when a user authenticated on the device. Affects version: 1.1.0 or later, 1.1.2 or earlier

Firmware Version 1.1.2 (Build No. 1.1.2_210903)

Release | 2021-10-01

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. The device rebooted abnormally when adding an occupancy limit zone. Affects version: 1.1.1 or earlier
2. When the LAN connection of the device configured in the occupancy limit zone was removed, the device rebooted abnormally if a user belonging to the bypass group authenticated on the entry device. Affects version: 1.1.1 or earlier
3. An abnormal IP address was set when using DHCP. Affects version: 1.1.1 or earlier
4. 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: 1.1.1 or earlier
5. If the device is rebooted with Live Finger Detection turned on, then the device fails to detect a fake fingerprint. Affects version: 1.1.1 or earlier
6. Abnormal authentication failure occurred when the slave device's auth mode was set to card+fingerprint. Affects version: 1.1.1 or earlier
7. PIN authentication did not work properly. Affects version: 1.1.1 or earlier
8. Renamed and improved the light brightness feature Affects version: 1.1.1 or earlier
    - Changed the option name from 'LED Brightness' to 'Light Brightness'.
    - Fixed the device to automatically operate as 'Normal' option when the administrator sets the light brightness to an invalid option.
9. After setting the auth mode to include fingerprint and fingerprint/PIN, an abnormal error message is displayed if a user whose fingerprint or PIN is not enrolled authenticates on a slave device that does not support Extended Private Auth Mode. Affects version: 1.1.1 or earlier
10. If the face auth mode was not used for more than 10 hours. and then activated, the face authentication did not work. Affects version: 1.1.1 or earlier

11. When using server matching, the device rebooted abnormally during the loading if a user with an Operator Level of 'None' inquires about the event log. **Affects version: 1.1.1 or earlier**

    - This issue was caused by a conflict between uploading event logs to the server and outputting the user's event logs when the device has a large number of event logs that have not been uploaded to the server for a long period of time.

12. Capturing and authenticating face images in the background was activated during operations unrelated to face authentication. **Affects version: 1.1.1 or earlier**

Firmware Version 1.1.1 (Build No. 1.1.1_210623)

Release | 2021-06-25

New Features and Improvements

1. Improved Visual Face algorithms
    - The new visual face algorithm is not compatible with visual face templates registered in firmware Version 1.0.5 or earlier. When upgrading firmware from version 1.0.5 or earlier to version 1.1.0 or later, migration to extract the previously registered face templates is performed, which may take up to 10 hours depending on the number of registered users.
    - AoC with face data issued by version 1.0.5 or earlier is not compatible with devices with firmware version 1.1.0 or later.
    - When upgrading the firmware to version 1.1.0 or later, it is not able to downgrade to version 1.0.5 or earlier.
2. Occupancy limit zone support
3. Improved usability of the Suprema Thermal Camera.
    - Added voice guidance for temperature measurement distance and user movement
    - Improved the user interface for the ROI guide area.
    - Classified the display of the guide area according to its ROI setting.
    - Changed the default value for ROI Settings from Dynamic ROI to Default ROI
    - Added a guidance message when the temperature measurement failed.
4. Renamed the lighting brightness control feature and added the 'Not Use' option.
    - Changed the option name from 'Ambient Brightness' to 'LED Brightness'.
    - Improved turning off the light of the device by adding the 'Not Use' option.
    - Removed the 'Auto' option.
5. Improved manually turning the secure tamper on or off even when the default hash key is set.
6. Changed the face authentication time interval to 2.5 seconds.
7. Improved to prevent errors from occurring upon decompressing a file that is 2GB or larger after the file has been split and then compressed upon exporting to a USB.

Bug Fixes

1. The RS-485 communication did not work properly when connecting the device to a third-party controller after activating

the Secure Communication mode. Affects version: 1.0.5 or earlier

2. The brightness of the screen increased and this state persisted when the face authentication failed due to an environment that was too bright, too dark, or backlit. Affects version: 1.0.4 or earlier
3. The Suprema Thermal Camera did not work properly after upgrading the firmware to version 1.0.4 or later. Affects version: 1.0.4 or earlier
4. There was a difference in the time taken depending on whether the user was registered when exporting logs to a USB. Affects version: 1.1.0 or earlier
5. The administrator menu was not displayed intermittently when the authentication mode was set to ID+PIN. Affects version: 1.0.5 or earlier
6. The screen was abnormally displayed when the second user authentication was successful on a slave device with dual authentication. Affects version: 1.1.0 or earlier
7. After being disconnected from BioStar 2, an incorrect pop-up message was displayed until they were reconnected. Affects version: 1.0.5 or earlier
8. The duress authentication logs did not occur in order according to the set authentication mode. Affects version: 1.0.5 or earlier
9. The relay operated as Off (Lock) after setting the scheduled unlock zone in the elevator and rebooting the master device. Affects version: 1.1.0 or earlier
10. All files in the database were deleted after exporting them to a USB. Affects version: 1.0.5 or earlier
11. Improved the Visual Face matching algorithm. Affects version: 1.1.0 or earlier
    - Improved authentication performance when wearing masks.
    - Improved the facial authentication algorithm for glasses-wearers.

Firmware Version 1.0.5 (Build No. 1.0.5_210422)

Release | 2021-05-06

Bug Fixes

1. An infrared image was not displayed when connecting the device to the thermal camera.

Firmware Version 1.0.4 (Build No. 1.0.4_210303)

Release | 2021-03-10

New Features and Improvements

1. Changes to a new LCD screen
    - For devices with firmware version 1.0.3 or earlier, be sure to upgrade the firmware to the latest version before replacing it with a new LCD display. If you upgrade the firmware to version 1.0.4 or higher after replacing the LCD display first, a touch malfunction may occur.
2. Suprema Thermal Camera (TCM10-FSF2) SDK Revision
    - FPS 8.3 applied
    - The management service is separated to recover the system safely after the device stops working abnormally.
    - The infrared image motion stopped working or the device was restarted while using the thermal camera.
    - The specifications of captured image buffer were modified.

Bug Fixes

1. The firmware version of the thermal camera was not displayed.
2. The previous T&A code setting was maintained even after changing the setting.
3. A timeout occurred when a user set to Exclude Device Default Authentication Mode attempted to authenticate a card on a slave device with authentication mode set to Card+PIN.
4. The thermal camera froze up when updating resources via BioStar 2.
5. Improved the Visual Face matching algorithm.
    - Improved the face authentication algorithm for users with glasses.
    - Improved the authentication performance when wearing masks.

Firmware Version 1.0.3 (Build No. 1.0.3_210126)

Release | 2021-02-02

New Features and Improvements

1. Changes to a new LCD screen
    - After upgrading a firmware to v1.0.3, you cannot downgrade the firmware to the previous version that includes the kernel and U-Boot.

Bug Fixes

1. When a user authenticated using the iCLASS Seos AoC (Access on Card) after saving a face in it, the device timed out or recognized the AoC as a CSN.
2. Motion detection did not work properly after scanning a card.
3. When using T&A mode, the device did not recognize a card intermittently.

Firmware Version 1.0.2 (Build No. 1.0.2_210104)

Release | 2021-01-05

New Features and Improvements

1. Improved the usability of Suprema Thermal Camera.
    - Added minimum reference temperature setting function.
    - Improved the user interface for the ROI.
    - Improved temperature deviation in room and low temperature environments.
    - Removed temperature bar from the temperature check screen.
    - Changed the English function name for infrared emissivity.
2. Improved user interface for Suprema Thermal Camera and Mask Detection.
    - Changed the notification, beeps, and voice guides.
3. Separated event logs of Mobile Access cards and RFID cards.
4. Added support for the option to toggle Screen Saver for slave devices.
5. Improved the Visual Face matching algorithm.
    - Improved the issue where the detection UI was not displayed on the face authentication screen when the verification mode of Suprema thermal camera function was set to 'Check Only'.
    - Improved the authentication performance when wearing masks.
    - Improved the authentication performance for backlit, external light, and low-light use environments.
    - Improved face detection performance.

Bug Fixes

1. The device stoped working when calling the BS2AuthConfig of a device using BioStar Device SDK.
2. The slave device restarted abnormally when connected as master-slave.
3. The RS-485 disconnection log continuously occurred when Secure I/O 2 was connected.
4. Mask Detection and temperature measurement operations were not smooth when Dynamic ROI was set when Check mode of the mask detection and Suprema Thermal Camera function was set to 'Check Only'.
5. An issue of Suprema Thermal Camera screen being maintained even when the thermal imaging camera was toggled from 'Enabled' to 'Disabled'.

6. The device abnormally terminated when establishing a communication connection with 'Device → Server'.
7. The Wigand reader connected to the DM-20 operating from Lock to Unlock if the device was restarted when the device was connected as master-slave.
8. An issue that occurred when the device was restarted while the door was set to unlock manually, the door remained locked even after the restart was completed.
9. The Disarm button wss obscured by the device's fake face detection screen when the Intrusion Alarm Zone was set.
10. The Secure Tamper could not be manually turned off by the default hash key.
11. USB keyboard connection restriction to improve security vulnerabilities.
12. Fingerprint registered with AoC could be continuously authenticated with fingerprints without a card when sent to the device after changing them.
13. Image logs and count were not displayed properly in the event log.
14. The device abnormally restarted when attempting face authentication closer than the valid effective distance.

Firmware Version 1.0.1 (Build No. 1.0.1_201110)

Release | 2020-11-13

New Features and Improvements

1. Improved the algorithm for the Visual Face matching.
    - Improved to update templates not only the first one but the others when authenticating faces after registering face templates with photos and setting up the Face Matching mode.
    - Improved authentication failures due to quality issues in infrared templates when authenticating faces with the Fusion Matching mode on after registering face templates with photos.
    - Improved authentication failures when authenticating faces getting backlight in the dark environment after registering face templates with photos.
    - Improved both the algorithm for Mask Detection and usability.
2. Added the feature to configure the Screen Saver setting.
3. Changed the default ROI values of the Suprema Thermal Camera.
    - ROI X(%): 30
    - ROI Y(%): 25
    - ROI Width(%): 50
    - ROI Height(%): 55
    - If the firmware has been upgraded from version 1.0.0, modified ROI values are not applied automatically. To set the default settings for ROI, enter the values manually as shown above.

Bug Fixes

1. The performed action, such as temperature output, was different from the intended action responding to the input signal set in the Trigger & Action feature when using the Suprema Thermal Camera.
2. Time shown on the device was displayed incorrectly when setting up time with the BioStar Device SDK.
3. An abnormal device shutdown occurred when sending face templates of FaceStation 2 or FaceLite to the device by using the BioStar Device SDK.
4. The text on the Advanced tab was displayed abnormally when entering the detailed page of the device on BioStar 2 after the device database initialized for Security Tamper.
5. It was not able to register a device on the Dynamic site when registering devices directly from Airfob Pass.

6. The image log function was not working properly.
7. Modified the Check Mode to operate depending on the Check Mode of the Suprema Thermal Camera when the Suprema Thermal Camera was in use and the Wiegand Output mode was set to Bypass.
8. The firmware upgrade of XPass D2 (Rev 2) connected as a slave did not work properly.

Firmware Version 1.0.0 (Build No. 1.0.0_200915)

Release | 2020-09-15

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.