CoreStation

RELEASE NOTES

Version 1.7.4

English
EN 301.00.CS40

suprema
SECURITY & BIOMETRICS

CONTENTS

- Firmware Version 1.7.4
- Firmware Version 1.7.3
- Firmware Version 1.7.2
- Firmware Version 1.7.1
- Firmware Version 1.6.1
- Firmware Version 1.5.3
- Firmware Version 1.5.2
- Firmware Version 1.5.1
- Firmware Version 1.4.1
- Firmware Version 1.4.0
- Firmware Version 1.3.1
- Firmware Version 1.3.0
- Firmware Version 1.2.0
- Firmware Version 1.1.2
- Firmware Version 1.1.1
- Firmware Version 1.1.0
- Firmware Version 1.0.0

Firmware Version 1.7.4 (Build No. 1.7.4_261020)

Release | 2026-10-22

New Features and Improvements

1. Improved CoreStation Setup Manager security vulnerabilities

Bug Fixes

1. Disconnected slave devices shown as online after restoring CoreStation settings. Affects version: 1.7.3
2. Child Wiegand reader not being locked by **Trigger & Action** when a **Lock Override** card is assigned to a user. Affects version: 1.7.2
3. **Lock Override** card authentication not working on a door created with a Wiegand reader when the reader is disabled. Affects version: 1.7.2
4. Registered card operating as a lock override instead of arm/disarm during arm/disarm authentication. Affects version: 1.7.2
5. Lock Override Card authentication not working when a device is disabled. Affects version: 1.7.2
6. Device not connecting when deleted and re-registered after an SCB Key is applied in an OSDP standard environment. Affects version: 1.0.0

Firmware Version 1.7.3 (Build No. 1.7.3_260610)

Release | 2026-06-12

New Features and Improvements

1. Improved CoreStation Setup Manager features
    - Supported manual configuration of SCB Keys.
    - Supported backup and restoration of network information (Device ID, SCB Keys, etc.).
    - Improved the ability to transfer existing settings when replacing the CoreStation.
    - Improved the overall font sizes and UI.
2. Supports feature to set the baud rate of slave devices.
3. Improved to distinguish devices that support the **Secure Tamper** feature.
4. Improved to allow the use of **Secure Tamper** regardless of the **Device Hashkey Management** option.

Bug Fixes

1. The master device disconnecting or alarms failing to clear when performing **Clear Alarm** on alarms triggered by **Trigger & Action** settings on master or slave devices. Affects version: 1.7.2
2. When a specific device is connected as a slave, configuration changes are not properly applied. Affects version: 1.0.0
3. The firmware upgrade failing for BioStation 2a devices connected as slaves. Affects version: 1.7.1
4. Card authentication failure on connected Wiegand readers. Affects version: 1.0.0
5. Some devices are displayed as "Unknown" in the CoreStation Setup Manager. Affects version: 1.7.2
6. **Custom Smart Card Layout** set through **Batch Edit** is not applied on the device detail page. Affects version: 1.0.0

Firmware Version 1.7.2 (Build No. 1.7.2_260429)

Release | 2026-04-30

New Features and Improvements

1. Supported EV2 Secure Messaging authentication and issuance for DESFire EV2 and EV3 cards.
2. Supports the **Lock Override** feature, which allows you to enroll a card that can open a door to be opened using a specific card.
3. 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
4. Supports **Custom Smart Card** of devices connected as slaves.
5. Supports new device.
    - XPass Q2
6. 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.

Bug Fixes

1. Access group authentication behaves abnormally according to the schedule (Daily) when DST is applied.
   Affects version: 1.0.0
2. Inability to access the CoreStation Setup Manager after performing a factory reset. Affects version: 1.0.0
3. The device freezes when the RS-485 network mode on the device is set to **Not Use** using the SDK.
   Affects version: 1.0.0

Firmware Version 1.7.1 (Build No. 1.7.1_240130)

Release | 2024-02-06

New Features and Improvements

1. Supports **Wireless Door Lock**.
2. Improved synchronization to complete if user enrollment fails when synchronizing multiple users to the device in BioStar 2.
3. Improved to select and update only the desired information when updating user information. (Compatible with BioStar v2.9.0 or higher)
4. Supports new devices.
    - BioStation 2a

Bug Fix

1. When using **Server Matching**, **Card + Face** or **ID + Face** authentication fails on FaceStation 2 connected as a slave. Affects version: 1.4.0
2. Resource file update fails on the device connected as a slave. Affects version: 1.5.2
3. After authenticating with **ID + Face** on a device connected as a slave, the **ID Input** screen does not appear when the **ID** icon is touched. Affects version: 1.0.0
4. Slave device that is set to be locked will not be locked if **Secure Tamper** occurs on the master device. Affects version: 1.4.0
5. The settings of the connected IM-120 are not being applied. Affects version: 1.6.1
6. Authentication fails when authenticating with a DESFire AoC while the device is connected as a slave. Affects version: 1.0.0
7. Device abnormally restarts when changing the device's **Network** settings in BioStar 2. Affects version: 1.0.0
8. When settings that are not supported are configured through the SDK, the device fails to boot properly. Affects version: 1.0.0

Firmware Version 1.6.1 (Build No. 1.6.1_230217)

Release | 2023-02-21

New Features and Improvements

1. Supports 3rd party OSDP reader connection.

Bug Fix

1. Event log is not logged when the database or cache memory is broken Affects version: 1.0.0.
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: 1.0.0.
3. Improved the structure to prevent authentication fail caused by broken database or cache memory Affects version: 1.0.0.

Firmware Version 1.5.3 (Build No. 1.5.3_221026)

Release | 2022-11-02

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. 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.
3. Separated the log related to the cause of the door unlock.
    - Door open request by exit button
    - Door open request by operator
4. Improved the Arm/Disarm status is maintained if the device loses power.

Bug Fix

1. Slave devices connected to specific RS-485 ports not being searched. Affects version: 1.0.0

Firmware Version 1.5.2 (Build No. 1.5.2_211105)

Release | 2021-11-09

New Features and Improvements

1. Supports new devices
    - X-Station 2
    - Input Module (IM-120)

Firmware Version 1.5.1 (Build No. 1.5.1_210511)

Release | 2021-05-24

New Features and Improvements

1. Upgraded to the 1.1.1i version of OpenSSL.
2. Increased maximum number of face users (1:N).
    - Before: 3,000
    - After: 4,000

Bug Fix

1. The device rebooted when the Supervised Input short circuit occurred without the CoreStation SETUP Manager IP being completely saved. Affects version: 1.3.1
2. When calling the BS2_ResetConfigExceptNetInfo API from the BioStar Device SDK, a 'Timeout' error occurred. Affects version: 1.0.0
3. It failed to transfer user data during user synchronization as the face data size exceeded the maximum size allowed for the system. Affects version: 1.4.0

Firmware Version 1.4.1 (Build No. 1.4.1_200902)

Release | 2020-09-25

New Features and Improvements

1. Separated event logs of Mobile Access cards and RFID cards.
2. Delete Change Device ID in CoreStation SETUP Manager user interface.
    - Change Device ID not supported through CoreStation SETUP Manager.

Bug Fix

1. Issue that the connection of the slave device is disconnected when the slave device is connected.
2. Hash key stored unencrypted.
3. An error occurs when a secure tamper occurs while upgrading the firmware version from 1.3.1 to 1.4.0.
4. When using a static IP while DNS server address is configured, a reboot on the device causes communication problems between the server.

Firmware Version 1.4.0 (Build No. 1.4.0_200525)

Release | 2020-05-29

New Features and Improvements

1. Supports face authentication devices.
    - FaceStation 2
    - FaceLite
2. Supports new device.
    - XPass D2 (Rev)
3. Added feature to change device ID.
4. Enhancement in the security of the device.
    - Restrict unencrypted connections.
    - Enhancement in security of encryption keys.
    - Encrypt and migrate user information.
    - Restrict access through communications such as TCP/IP, RS-232, and USB.
5. Improved Anti-passback zone to operate based on the door status.
6. Improved the scheduled unlock function for each floor when controlling elevator.
7. Improved the CoreStation SETUP Manager
    - Added feature to change device ID.
    - Added feature to set IP.
    - Duplicate check for device IP and CoreStation SETUP Manager IP settings.
    - Supports FW upgrade for slave devices.
    - Improved to show a warning message when a relay port in output status is 'On' in the Monitoring menu.
    - Improved Setting menu by allowing scroll.
    - Improved to show a warning message when a user sets the IP address of the CoreStation SETUP Manager.

Bug Fix

1. When rebooting the master device with multiple slave devices connected, Trigger & Action does not work as set.

2. A bug where the master device is rebooted if the value sent to the slave device is greater than the defined value.
3. Issue that it is possible to connect to the CoreStation SETUP Manager with the IP address of a device when using DHCP.
4. A bug where OSDP Communication does not work normally if the value sent to the slave device is greater than the defined value.
5. An issue where device gets disconnected or a timeout occurs when upgrading firmware or transferring users under SSL secure communication.
6. A bug where the event log of the device is not sent in the order in which it occurred.

Firmware Version 1.3.1 (Build No. 1.3.1_191203)

Release | 2019-12-03

New Features and Improvements

1. Supports CoreStation Setup Manager.

Bug Fix

1. The list of connected slave devices is initialized if rebooting the master device after changing the RS-485 baudrate.
2. When using firmware V1.3.0 the connection to the I/O device that using the firmware version below is lost.
    - DM-20 FW V1.1.2 and below
    - OM-120 FW V1.0.0 and below
    - Secure I/O 2 FW V1.2.1 and below

Firmware Version 1.3.0 (Build No. 1.3.0_190626)

Release | 2019-07-12

Important Bug Fix

1. When a door configured in a Scheduled Unlock Zone is opened by a Scheduled Unlock, the door is not locked if the zone is deleted.
2. A code is added to prevent the authentication fails because the cache memory is broken.

New Features and Improvements

1. Supports Anti-Tailgating.
2. Change the way new settings are applied when adding administrators using batch edit of devices.
    - Existing: Overwrite a new setting to existing settings.
    - Update: Add a new setting to existing settings.
3. Increase of the number of administrators that can be added.
4. Increase of the maximum number of floor levels.
5. Support to the Clear APB for each user.
6. Supports checking module firmware version.
7. Support for connecting new devices.
    - XPass 2(XP2-MDPB, XP2-GDPB, XP2-GKDPB)

Bug Fix

1. The device does not send the Seos config to the slave device even though the slave device supports iCLASS Seos card.
2. Applies FA improvement algorithm.
3. Start time is not applied in UTC when importing filtered logs using SDK.
4. Fixed mask error of DesFireCardConfig.
5. Supports unsupported devices (FaceStation 2, FaceLite).
6. The door operates as the Scheduled Unlock when restarting the master device while the door is configured to the Scheduled Unlock and Manual Lock.

7. The master device is rebooted if deleting the zone while disconnected with the slave device.
8. The title of the credential input screen is displayed differently on the master device and the slave device when using multiple authentication mode.
    - Existing: master device (user ID, user name), slave device (user ID)
    - Update: master device and slave device (user ID, user name)
9. Relay works after reconnecting for authentication that occurred when elevator connection is disconnected.
10. When an alarm occurs in the interlock zone, the alarm does not clear even though restarting the master device.
11. Even though the fingerprint templates are set differently on the server and the device, the fingerprint enrollment succeeds in the slave device.

Firmware Version 1.2.0 (Build No. 1.2.0_181112)

Release | 2018-11-29

Important Bug Fix

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

New Features and Improvements

1. Improves the data protection.
    - Increase the items to encrypt the data.
    - Support to setting the period for storing the personal information.
2. Change the maximum value of the interval and width for the Wiegand Input.
3. Support to the number of users, fingerprints, faces, and cards in Manage Users in Device.
4. If the data transmission fails when communicating with OSDP, it is transmitted again.
5. The site key is initialized if a secure tamper event occurs.
6. If an administrator has registered, modified, or deleted a user, the event log shows whether the editing was done on the server or on the device.
7. Support to the creation of up to 2048 Access Levels and Access Groups.
8. Support to DESFire/DESFire EV1 Advanced option.

Bug Fix

1. A slave device that supports an iCLASS Seos card does not properly read the iCLASS Seos card.
2. The device restarts if more than 8 outputs are set.
3. Modified that if the same key is not sent to the slave device when the RS-485 primary key is set up on the master device, the master device sends it again.
4. If the user uses the BS_GetLogBlob command to get the door ID, the door ID is not output normally.
5. When physically disconnecting the RS-485 connection of the slave device and connecting another slave device to the same port, the connection status is displayed by the information of the slave device that was connected before.
6. Improves I/O module Input and Output process.

7. Modified the firmware of that slave device so that it cannot be upgraded when a device not supported by the master device is connected as a slave.
8. The relays operate differently from the previous status if the slave device is reconnected.
9. The authentication result value is sent from the Wiegand port even though any Wiegand reader is not connected.
10. The alarm can be released in the Floors status after a fire alarm occurs when the elevator is configured as a Fire Alarm Zone.

Firmware Version 1.1.2 (Build No. 1.1.2_180706)

Release | 2018-07-24

Bug Fix

1. The device restarts when authentication fails.

Firmware Version 1.1.1 (Build No. 1.1.1_180523)

Release | 2018-06-20

New Features and Improvements

1. In a device with an LCD, the user name is displayed on the LCD when authentication is successful even when connected in slave mode.
2. Changed the default for the input from Supervised Input to Normal.
3. Support for connecting new devices.
    - BioLite N2(BLN2-PAB), XPass D2(XPD2-GDB, XPD2-GKDB)

Bug Fix

1. Problem where logs are duplicated by repeatedly attempting to input Manual Lock, Manual Unlock, Release, etc. to the door disconnected from the device.
2. Issue where event logs and real-time logs are not uploaded normally to BioStar 2.
3. Problem that relay state is not maintained when reconnecting a device connected by RS-485.
4. Issue in which the door relay status operates as On when the device is reconnected after starting and ending the Schedule Unlock with the door relay device disconnected.
5. Problem that the time zone is not initialized even if the factory reset is performed while secure communication and data encryption key are in use.
6. Issue where if the authentication is successful when the device set as door relay is disconnected, the relay will operate according to previous value after reconnection of the device.
7. Issue where the device restarts when authenticating with an unregistered fingerprint.
8. Issue that are not initialized for the tamper, AC Fail, and Supervised input when the factory reset is performed.

Firmware Version 1.1.0 (Build No. 1.1.0_180317)

Release | 2018-03-26

New Features and Improvements

1. Support Interlock zone.
2. Support Reset without Network Settings.
3. Support Daylight Saving Time setting.
4. Improves Trigger & Action for duress finger.
5. Improves to handle the encryption key of the important information stored in database differently from server to server.
6. Support the secure tamper.
7. Support ISO14443A 10 Byte CSN.
8. Support connecting with BioLite N2, XPass D2.

Bug Fix

1. Issue where RS-485 disconnect when changing home screen of the slave device to user's logo.
2. Problem that the slave device is disconnected when the slave device finishes booting more slowly than the master device with the RS-485 encryption key set.
3. Issue if the elevator is configured as a fire alarm zone, relay operation will be turned off when the alarm is released after the fire alarm.
4. Fixed to retain previous rate when setting to the unsupported RS-485 rate.
5. Problem that the duration of the supervised input behaves differently from the setting in Trigger & Action.
6. Fixed to output the logs that the input information and the door open information of the intrusion sensor in the intrusion alarm zone.
7. Problem that delay time of Action Signal Output is not applied in the slave device.

Firmware Version 1.0.0 (Build No.1.0.0_170919)

Release | 2017-09-19

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.