Table of Contents

Version 1.7.0 (V1.7.0_190806)

Release

2019-08-08

New Features and Improvements

1. OSDP Standardization

- Improved to comply with OSDP V2.1.7 protocol when connecting with 3rd-party controllers.

2. Increase of the number of administrators that can be added.

3. Support to the Clear APB for each user.

4. Supports options by card type.

5. Increase of the maximum number of floor levels to up to 2,048.

6. Add the event items to IMAGE LOG menu.

7. Change the way new settings are applied when adding administrators using batch edit of devices.

- Before: Overwrite a new setting to existing settings.
- After: Add a new setting to existing settings.

8. Supports the duplicate fingerprint check when registering users on a device.

9. Supports setting options for Wiegand authentication result output.

- User ID and Card ID

10. Supports Anti-Tailgating at doors.

11. If the data transmission fails when communicating with OSDP, it is transmitted again.

12. Support for connecting new devices.

- XPass 2(XP2-MDPB, XP2-GDPB, XP2-GKDPB)

Main fixes

1. The master device abnormally shuts down if it is operated after reconnecting a disconnected slave device.

2. The master device abnormally shuts down if the RS-485 mode of the master device is changed after disconnecting the 31 connected slave devices.

Bug fixes

1. The master device does not be connected to the slave device intermittently if the master device is rebooted with schedule unlock and manual unlock set at the door.

2. Slave device (XPass D2) firmware upgrade via BLE fails.

3. When upgrading firmware using USB, upgrade fails due to a timeout.

- Change the timeout from 90 seconds to 5 minutes.

4. Image logs are not generated for some events.

5. When dual authentication is set on the door, if the first user authenticates with the fingerprint and the second user authenticates with the ID, the wrong ID is displayed on the screen when authentication fails.

6. The device recognizes the iCLASS Seos card as a CSN card.

7. Firmware upgrade does not work normally due to SSL reconnection.

8. Applies the FA(False Acceptance) improvement algorithm.

9. Start time is not applied in UTC when importing filtered logs using SDK.

10. A user cannot access BioStar 1.93 when using the latest firmware.

11. The relay operates abnormally if the master device reboots after configuring multiple doors.

12. When a user with Administrator permission is configured as below, the device will not respond if the user tries to authenticate the card.

- If the status is set to Disable.
- If the period is set to be past or future.

13. Relay works after reconnecting for authentication that occurred when elevator connection is disconnected.

14. If a user enters the gateway and subnet mask values and then set to Enable DHCP, the wrong IP address is output to the user interface.

15. Access is denied and user ID is displayed abnormally when using a smart card or fingerprint authentication in One Device Mode.