Table of Contents

Version 1.4.0 (V1.4.0_200918)

Release

2020-09-28

New Features and Improvements

1. Added feature to change device ID.

2. Enhancement in the security of the device.

- Restrict unencrypted connections.
- Enhancement in the security of encryption keys.
- Encrypt and migrate user information.

3. Improved Anti-passback zone to operate based on the door status.
4. Improved the scheduled unlock zone function for each floor when controlling elevator.
5. Supports server matching.
6. Supports the Mobile Access V1.1.
7. Supports the thermal camera.
8. Supports the Screen Saver.
9. Improved the face authentication algorithm for users with glasses.
10. Supports the new face template.

> - Face templates scanned or enrolled on devices with the firmware version 1.4.0 or later are not compatible with devices with firmware version 1.3.1 or earlier, and authentication may fail due to this incompatibility.
> - If the firmware of the face authentication device connected as a slave is the latest version (FaceStation 2: 1.4.0 or later, FaceLite: 1.2.0), authentication may fail because it is not compatible with the existing template.

11. Increased maximum number of users (1:N).

- Before: 3,000
- After: 4,000

12. Supports new device.

- XPass D2 (Rev 2)

Main Fixes

1. When all or user data were exported to a USB and then the user data were imported again after upgrading the device firmware, the event log was deleted.
2. Logs generated while the device was disconnected were not sent to BioStar 2, even after the device was reconnected.

Bug Fixes

1. Modified that the authentication mode of the slave device was set according to the setting of the master device.
2. Authentication of fingerprints registered as duress fingerprints failed on the BioStation A2 connected as a slave device.
3. Card data were output with wrong BitCount when the device was connected to a 3rd-party system via OSDP.
4. The automatic Wi-Fi connection function did not work.
5. Some or all of the image log colors appeared garbled.
6. It recognized registered users as unregistered when accessing job codes with assigned cards.
7. Device rebooted if the face of an existing registered user was changed when the number of registered users was the maximum.
8. An OSDP security session error occurred when connecting OM-120 and XPass D2 as a slave device.
9. An excess error occurred when registering new user faces or editing registered users even though the number of registered faces did not reach the maximum capacity.
10. The registered user data disappeared and the device rebooted if a user attempted to register a card when the number of registered users was at maximum capacity.
11. An error occurred when matching with groups when there were 5,000 users and 5 user groups were used.
12. The slave device did not work with group matching even though the group matching was set in the master device.
13. When an administrator was resent from a device with a new firmware applied, it was recognized as an unregistered user and could not enter the administrator menu.
14. An error in the master-slave connection occurred due to the RS-485 communication key.
15. After a global anti-passback violation, an authentication success log occurred twice.
16. After the message 'Invalid payload' occurred on the slave device, it was disconnected abnormally and reconnection was impossible.
17. When a locked device was rebooted for an RS-485 connection, the slave device became unlocked.
18. When Factory Default was performed using SDK, the device resource (logo image) did not initialize.
19. Device reboots or a timeout occurred when upgrading firmware or transferring user data during SSL secure communication.
20. It was unable to edit, delete or add an authentication mode.
21. When the delay for the output signal occurred repeatedly, the device did not work properly.
22. The output port of the BioStation 2 could not be set in the trigger & action.

23. Device tried to connect to an NTP server.
24. Device worked as DHCP even though the static IP and daylight-saving mode were set.
25. Infrared camera continues to activate abnormally when low light and authentication mode is set.
26. When a user authenticated on the slave device using a smart card or the face, the master device would reboot.
27. When a user authenticated the fingerprint after setting the byte order as LSB and the Wiegand output information as the user ID, the device would reboot.
28. Device rebooted when registering user faces.
29. Improved the device to recognize unknown cards by selecting the card type options.
30. Once a card had been registered on the Wiegand output device, the device would not work properly when trying to output data using a fingerprint registered to another user.