Table of Contents

Version 1.2.0 (V1.2.0_181119)

Release

2018-11-29

New Features and Improvements

1. Support to AES encryption type for DESFire card.

2. Support to DESFire/DESFire EV1 Advanced option.

3. Support to the creation of up to 2048 Access Levels and Access Groups.

4. If a user is registered, modified, or deleted, the event log shows whether the editing was done on the server or on the device.
5. If the data transmission fails when communicating with OSDP, it is transmitted again.
6. Improves the data protection.

- Increase the items to encrypt the data.
- Support to setting the period for storing the personal information.
- Support for additional features in Secure Tamper: Delete Users, Logs, Data Encryption Key, SSL certificate, and Smart Card Layout when a secure tamper event occurs.

7. Change the maximum value of the width for the Wiegand Input.

8. Support to the number of users, fingerprints, faces, and cards in Manage Users in Device.

9. Support for Individual Authentication Successful Messages and Working alarm time reports.

10. When using The bypass, The card ID is output as Wiegand even though a user authenticates with the AoC.

Main Fixes

1. When attempting to connect to a wireless LAN, if a user deletes and saves the IP address and gateway, the device restarts repeatedly.
2. When Micom is reset, the output does not restore to its previous status.
3. Wiegand Out is not output when authenticating with blacklist card.
4. With Bypass enabled, authentication failure message is not displayed when unregistered ID is authenticated.
5. Authentication fails because the server matching enabled for RFID cards and IDs.
6. The user cannot issue a new File after the App and File are created when issuing the DESFire card.

7. The device reboots if a user authenticates the RFID card or face consecutively on the device.
8. If using Group Matching, the device displays the group name as None when authenticating a face.
9. A code is added to prevent the authentication fails because the cache memory is broken.

Bug Fixes

1.The relay does not work even though a user successfully authenticated the face on the device.

2. The relays operate differently from the previous status if the slave device is reconnected.

3. 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.

4. With Bypass enabled, the device does not respond even if a user selects the Menu, T & A, or ID after authentication.

5. Change some special characters (\, /, :, *, ?, “, ', `, <, >, |, .) to be unavailable when setting a user name.

6. The setting value is not saved when Face Config is set to the slave device.
7. The device(FS2-D) intermittently reboots.
8. If a user authenticates the card to XPass D2 connected to as a slave device, the beep sounds twice.
9. 1: N authentication can also be added on the slave device even though the master device is only capable of 1: 1 authentication.

10. If the user uses the BS_GetLogBlob command to get the door ID, the door ID is not output normally.