Table of Contents

Version 1.1.0 (V1.1.0_181210)

Release

2018-12-11

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 Micom is reset, the output does not restore to its previous status and the device cannot recognize the card.
2. The DESFire EV1 card issued with the AES encryption option is recognized as a CSN card.
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. The user cannot issue a new File after the App and File are created when issuing the DESFire card.
6. Some time zones are missing and the device reboots abnormally.
7. A code is added to prevent the authentication fails because the cache memory is broken.

8. The sensor does not work if a user reboots the device and then authenticates the fingerprint.

Bug Fixes

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

2. The alarm can be released in the Floors status after a fire alarm occurs when the elevator is configured as a Fire Alarm Zone.

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. Japanese language resource is not applied normally when the language is set to Japanese.

5. The new event log is missing and is not displayed.

6. Change some special characters (\, /, :, *, ?, “, ', `, <, >, |, .) to be unavailable when setting a user name.
7. An administrator cannot set the permissions of other administrators.
8. The tamper off event occurs when the bracket is removed and the device is rebooted.
9. The Authentication success or failure setting in Trigger & Action does not work normally.
10. If a user authenticates the card to XPass D2 connected to as a slave device, the beep sounds twice.
11. If the user uses the BS_GetLogBlob command to get the door ID, the door ID is not output normally.
12. When registering a fingerprint, the scanned fingerprint image is displayed on one side.