Table of Contents

Version 1.5.0 (V1.5.0_190708)

Release

2019-07-12

New Features and Improvements

1. OSDP Standardization

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

2. Supports Anti-Tailgating.

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

4. Supports setting options for Wiegand authentication result output.

- User ID and Card ID

5. 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.

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

7. Increase of the maximum number of floor levels.

8. Supports options for selection by card type.

9. Support to the Clear APB for each user.

10. Supports checking module firmware version.

11. Supports the latest version of I/O module Micom (V1.3.1).

12. Support for connecting new devices.

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

Main fixes

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.

Bug fixes

1. If the same fingerprint is authenticated successively after successful fingerprint authentication, the duplicated logs are left.

2. Applies FA improvement algorithm.

3. The code value set in T&A mode is not maintained.

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

5. The waiting alarm does not stop even if the master device is disconnected when the waiting alarm occurs during the delay time in the intrusion alarm zone.

6. Supports unsupported devices (FaceStation 2, FaceLite).

7. EM cards are continously recognized.

8. If the master device is disconnected when the intrusion alarm zone is set to 'Arm', it will be displayed as 'Arm' on the screen when the master device is reconnected even though the zone has been disarmed.

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

10. 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)

11. The device reboots when transferring the maximum number of users after deleting all users.

12. The device reboots during firmware upgrade with the maximum number of users registered.

13. The slave device operates according to the Auth Timeout set in the master device, not the Auth Timeout set in the slave device.

14. The output of Dual Authentication Timeout messages is delayed.

15. If more than 200,000 fingerprint templates are registered and the user tries to access the admin menu by fingerprint authentication while the user is registered, the error phrase is not output

properly, and the user can access.

From:
http://kb.supremainc.com/knowledge/ -

Permanent link:
http://kb.supremainc.com/knowledge/doku.php?id=en:bsl2_revision_note_150

Last update: **2021/05/17 13:22**