Table of Contents

Version 2.8.3 (V2.8.3.10)

Release

2020-07-21

New Features and Improvements

1. Supports Zone in the Admin Item Settings of the custom level.

2. Supports FaceStation 2 and FaceLite as a slave of CoreStation.

3. Renamed 'Mobile Access' service name.

- Before: Mobile Credential
- After: Mobile Access

4. Supports Mobile Access on BioLite N2.

5. Improved user group tree output performance while massive user groups (20,000 or more groups) are used.

6. Supports operation options on Anti-Passback zone to operate based on the door status.

7. Improved the scheduled unlock zone function to support elevator.

8. Improved Trigger & Actions to be able to use the output port of the BioStation 2.

9. Improved db-converter to check the error during query execution when installing BioStar 2.

10. Updated language resource files.

Main fixes

1. The device rebooted abnormally when adding the device while Secure Communication with Device is on.

2. An error occurred when exporting user data to FaceStation 2.

3. The event log and the real-time log did not display Muster zone time limit event when logged in as a custom level operator.

4. When accessing as a custom level administrator with the permission for some the intrusion alarm zones, the event logs without zone IDs were not displayed when logged in as a custom level operator with permission on Intrusion alarm zones.

5. When using a large number of user groups, some user groups did not appear on the monitoring menu.

6. When the language is set to Spanish, the month, and day of the week were not displayed in the schedule of the TIME ATTENDANCE menu.

7. When device connect and disconnect were abnormally repeated, the server responds slowly.

8. An error occurred if the following actions are executed when logged in as a custom level operator who has permission to modify a specific user group and users.

- Selecting a user and executing CSV export.
- Selecting a user and then printing.
- Entering the Status tab of the user menu.
- Disabling of Anti-Passback for specific users.

9. Image log files were not encrypted.

10. When using Personal Information DB Encryption, if a user having a mobile access card gets deleted, the card was deleted in BioStar 2, but not in the Suprema Airfob portal.

11. Intrusion detection log was not displayed in the real-time log.