XPass 2

Firmware Revision Notes

Version 1.2.1

suprema
SECURITY & BIOMETRICS

Firmware Version 1.2.1 (Build No. 1.2.1_200612)

Release: 2020-06-26

1. New Features and Improvements

    1.1. Support encryption for the blacklist and user ID set as an administrator when migrating user information.

    1.2. Improved not to initialize the network and SSL settings when the device ID is changed.

2. Bug Fixes

    2.1. Issue that the value is not sent to the server since corrupted logs occur.

    2.2. Issue that the connection of the slave device is disconnected when the slave device is connected.

    2.3. Issue that the option for card types is deactivated when the device is connected as a slave after the factory reset.

    2.4. Issue that logs of devices are not sent to the server after the factory reset.

Firmware Version 1.2.0 (Build No. 1.2.0_200409)

1. New Features and Improvements

    1.1. Support to the Change Deivce ID.

    1.2. Enhancement in the security of the device.

    - Restrict unencrypted connections.

    - Support for Secure Tamper on slave devices.

    - Enhancement in the security of encryption keys.

    - Encrypt user information.

    - Restrict access through communications such as TCP/IP, RS-232, and USB.

    1.3. Support for connecting new devices.

    - XPass D2 (Rev 2)

    1.4. Improved Anti-passback zone to operate based on the door status.

    1.5. Support to the BioStar 2 Mobile Access.

    1.6. Support to the Mobile Access V1.1.

    1.7. Support to the scheduled unlock function for each floor when controlling elevator.

2. Bug Fixes

    2.1. Problem that the password set in the Device Manager app is not initialized even if the factory default is performed.

    2.2. The device does not recognize LF (Low Frequency) cards well.

    2.3. OSDP Communication does not work normally if the value sent to the slave device is greater than the defined value.

    2.4. The Secure Tamper occurs again if a user reboots the device after setting the smart card layout while the Secure Tamper has already occurred.

    2.5. The event log of the device is not sent in the order in which it occurred.

Firmware Version 1.1.0 (Build No. 1.1.0_190911)

1. New Features and Improvements

    1.1. Support to the Mobile Credential (NFC, BLE).

    1.2. Added CSN mask for the unknown card type.

    - Before: Cards other than MIFARE, iCLASS, DESFire, iCLASS Seos, FeliCa, ISO-15693 was recognized as CSN.

    - After: User can select whether to recognize cards other than MIFARE, iCLASS, DESFire, iCLASS Seos, FeliCa, and ISO-15693.

2. Bug Fixes

    2.1. The device recognizes the DESFire(Adv) card as a CSN if the device is restarted when the smart card layout set as DESFire (Adv).

    2.2. The LED indicator operates abnormally when the Device Manager app is disconnected.

    2.3. Changed the color of some of the status lights that previously worked in yellow to green.

    2.4. When using firmware V1.0.1 the connection to the I/O device that using the firmware version below is lost.

    - DM-20 FW V1.1.2

    - OM-120 FW V1.0.0

    - Secure I/O 2 FW V1.2.1

    2.5. The master device intermittently reboots when upgrading the firmware of the slave device.

Firmware Version 1.0.0 (Build No. 1.0.0_190530)

1. Initial firmware developed.