Table of Contents

Version 1.3.0 (V1.3.0_240514) 1
Release 1
New Features and Improvements 1
Bug Fixes 2

Version 1.3.0 (V1.3.0_240514)

Release

2024-05-30

New Features and Improvements

1. XPass D2 new BLE (Bluetooth Low Energy) chip firmware (Build No. 1.7.0_220921) support.

- The BLE chip parts of the hardware have been changed, and the firmware has been upgraded to be compatible with both the existing and new BLE chips.

2. Supports **Custom Smart Card Layout**.
3. Improved to not recognize SEOS configuration cards as CSN for 1 minute after device booting.
4. Added event code for QR authentication.
5. Support for adding FeliCa card to **Custom Smart Card Layout**.
6. Extended the user expiration period to a maximum of '**2037-12-31**'.
7. Supports the **Display Result from Controller** feature for displaying authentication success or failure results from a 3rd party controller on the device screen when using **Intelligent Slave**.
8. Supports the **Ignore Repeated Signals Duration** feature, which ignores repetitive authentication signals from the controller when the device is connected to a 3rd party controller via Wiegand.
9. Improved **Intercom** screen UI.
10. Supports the **SIP Server Transport** feature, which selects the SIP transmission method when setting up the SIP server of **Intercom** on the device.
11. Supports the feature of selecting the resolution of the video output from the device when using **Intercom** and **RTSP**.

- Intercom Video Resolution
- RTSP Video Resolution

12. Improved to get user update succeeded event log using the GetLogWithFilter function in the SDK.
13. Supports the **Auth Result Display Option** that allows you to select how the user ID and name are displayed on the authentication result screen of the device.
14. Improved pop-up message displayed when authentication fails for users who set the second credential as a fingerprint in **Extended Private Auth Mode**.

Bug Fixes

1. When the maximum number of extension numbers that can be stored on the device is exceeded, the **Add Extension** icon is still displayed. (Affects version: v1.0.0)
2. An issue occurs when authenticating with a face not wearing a mask on a device with the **Mask Detection** set to **Enabled (Soft)** and the mask check method set to **Check After Authentication**. (Affects version: v1.0.0)

- An authentication mode error occurs intermittently.
- The device freezes when facial authentication is continuous.

3. When the Wireless AP power is turned off and the device is restarted, the wireless network does not automatically reconnect when the AP power is turned back on. (Affects version: v1.0.0)
4. When the **Auth Mode** is set to Card / QR Code and the mask check method is set to **Check Before Authentication** on the device, QR authentication intermittently fails after wearing a mask and authenticating. (Affects version: v1.1.0)
5. If device settings are changed in BioStar 2 during an intercom call, card authentication fails after the call ends. (Affects version: v1.1.0)
6. Authentication fails when authenticating with a DESFire AoC while the device is connected as a slave. (Affects version: v1.0.0)
7. When **Relay** is set in the device menu, the door does not open with a mobile card. (Affects version: v1.0.0)
8. If a general user performs face authentication and checks the event log, the **Menu Timeout** elapses, and the device switches to a standby state, the **EVENT LOG** screen appears at the next face authentication. (Affects version: v1.0.0)
9. The authentication guide message was displayed incorrectly when pressing the **Arm/Disarm** button on the home screen while setting the **Intrusion Alarm Zone**. (Affects version: v1.0.0)
10. When network is repeatedly disconnected in an environment using a wireless network, RF card authentication will fail. (Affects version: v1.0.0)
11. The user ID stored as a 32-character string is truncated to only 31 characters in a specific event log. (Affects version: v1.0.0)
12. The device would not automatically reconnect to the previously connected wireless network when restarted while the network was connected as **Wireless**. (Affects version: v1.0.0)
13. If the network is connected to a wireless LAN and then enters **Wireless** again after changing to an ethernet connection, the wireless AP list is not displayed. (Affects version: v1.0.0)
14. Infinite loading occurred while attempting to connect via **Wireless**. (Affects version: v1.0.0)
15. When the network is connected to **Wireless**, switches to **Ethernet**, and then switches back to **Wireless**, it does not automatically reconnect to the previously connected wireless network. (Affects version: v1.0.0)
16. Image Logs were not deleted when performing **Factory Default** on the device. (Affects version: v1.0.0)
17. When a user with a 32-character user ID authenticates to the device while the device is not connected to the server, the authentication event log is not updated in BioStar 2 even after the device is reconnected to the server. (Affects version: v1.0.0)
18. If the number of fingerprints stored in the device exceeds the 1:N maximum, the **Finger** in **User Usage** count is displayed abnormally. (Affects version: v1.0.0)
19. The Wi-Fi signal strength of the connected wireless network was displayed differently in the

wireless LAN list and the WLAN icon on the home screen. (Affects version: v1.0.0)

20. On the home screen of a device with **Auth Mode** set to ID + Face/PIN, after entering the ID, the **Input ID** icon allows to enter PIN instead of changing the authentication process to the entered ID. (Affects version: v1.0.0)

21. Deleted image logs from the device gets continuously uploaded to the server. (Affects version: v1.0.0)

22. When the device's **Device → Server** setting gets inactive while the device is on the **Waiting Device** list of BioStar 2, the device still appears in the **Waiting Device** list, and the BioStar 2 connect icon is displayed at the top of the device. (Affects version: v1.0.0)

23. The facial authentication process continues to operate even after mask detection is completed on a device where the Wiegand device's **Output Mode** is set to **Bypass** and the mask check mode is set to **Check Only**. (Affects version: v1.1.0)

24. When enrolling a Visual Face by uploading a photo using the API, a blank area appears on the photo, and authentication fails intermittently. (Affects version: v1.0.0)

25. When setting the face authentication operation mode on a device using the SDK's BS2_SetFaceConfig function, there is an issue where an infinite reboot occurs if an incorrect value is entered. (Affects version: v1.0.0)

26. When creating a schedule with an invalid ID using the SDK, the device fails to boot properly. (Affects version: v1.0.0)

27. When the number of faces stored on the device exceeds the 1:N maximum, administrator login is possible via facial authentication. (Affects version: v1.1.0)

28. When using **Device → Server** mode, the server IP address is reset if the connection to the DHCP server fails. (Affects version: v1.0.0)