

# BioStar 2

## Revision Notes

Version 2.8.10

## Precautions when upgrading BioStar 2

- Do not install BioStar 2 on a PC where BioStar 1 is installed. This may cause performance problems.
- If BioStar 2.3.0 is installed on top of a BioStar 2.2.1 or 2.2.2 installation, all information stored in the SQLite database is migrated to a new MariaDB database.
- Upgrading directly from the existing version to the latest version is possible from BioStar 2.6.0 or higher. If the installed version is lower than 2.6.0, installing all versions in a correct sequence until reaching version v2.6.0 is essential.

Current Version	Upgrade Path
<b>2</b>	2.2.1 > 2.3 > 2.4 > 2.4.1 > 2.5.0 > 2.6.x or 2.7.x > 2.8.x
<b>2.2</b>	2.3 > 2.4 > 2.4.1 > 2.5.0 > 2.6.x or 2.7.x > 2.8.x
<b>2.2.1</b>	2.3 > 2.4 > 2.4.1 > 2.5.0 > 2.6.x or 2.7.x > 2.8.x
<b>2.2.2</b>	2.3 > 2.4 > 2.4.1 > 2.5.0 > 2.6.x or 2.7.x > 2.8.x
<b>2.3</b>	2.4 > 2.4.1 > 2.5.0 > 2.6.x or 2.7.x > 2.8.x
<b>2.4</b>	2.4.1 > 2.5.0 > 2.6.x or 2.7.x > 2.8.x
<b>2.5</b>	2.6.x or 2.7.x > 2.8.x
<b>2.6</b>	2.8.x
<b>2.7</b>	2.8.x

- If you are using Windows 8.1 or Windows Server 2012 R2, install the KB2919355 update by referring to the following web page.  
<https://support.microsoft.com/en-us/help/2919355/windows-rt-8-1--windows-8-1--and-windows-server-2012-r2-update-april-2>
- If MS SQL Server and BioStar 2 are installed on different PCs, you should install the Native Client on a PC with BioStar 2 installed.  
<https://www.microsoft.com/en-us/download/details.aspx?id=50402>
- When backing up a database from an older version of BioStar 2, disable all services and procedures. Furthermore, if you do not back up and restore the AC database and the TA database together, you will not be able to use the TA database.
- If you want to back up the database of BioStar 2, be sure to also back up the enckey in the \Program Files\BioStar 2 (x64)\util folder and the system.conf and setting.conf file in the \Program Files\BioStar 2(x64) folder. Otherwise, the database will be unavailable.
- The default values for the ports used by BioStar 2 are as follows. If another program occupies the same port, BioStar 2 may not work properly.

• HTTP Port	80		Available	• HTTPS Port	443		Available
• Web-socket Port	9002		Available	• API Port	9010		Available
• Database Port	3312		Available	• T&A HTTP Port	3000		Available
• T&A HTTPS Port	3002		Available	• T&A Cloud Port	52001		Available
• AC Cloud Port	52000		Available	• FastCGI Port	9000		Available

# Version 2.8.10 (Build No. 2.8.10.37)

Release: 2021-04-08

## 1. Main Fixes

- 1.1. User and user groups were not getting updated after upgrading to 2.7.11 or later from BioStar 2 version 2.6.0 or earlier in an HTTP-enabled environment. (Affects version: v2.7.11)
- 1.2. A warning message indicating to upgrade the firmware to the latest release was not displayed when connecting to FaceStation F2 running an older version of the firmware. (Affects version: v2.8.6)
- 1.3. Device default authentication mode was able to be used for users while Private Mode was set to "Exclude Device Default Authentication Mode". (Affects version: v2.8.6)
- 1.4. The Celsius/Fahrenheit mark was incorrectly displayed in the Trigger & Action alert email. (Affects version: v2.8.8)
- 1.5. The server did not work properly if the event code contained invalid values when generating Trigger & Action-related event logs. (Affects version: v2.7.12)
- 1.6. Registering a Visual Face was not correctly done due to image rotation when using Chrome version 86. (Affects version v2.8.6)
- 1.7. A simultaneous connection error occurred when connecting with the same account at the same time, even though Simultaneous Connection Allow was disabled. (Affects version: v2.7.11)
- 1.8. Visual Face CSV import failed when using the Wiegand format or a Custom User Field. (Affects version: v2.8.8)
- 1.9. Email transmission did not function properly when SMTP Security Type was 'None' or 'TLS' in email settings. (Affects version: v2.8.6)
- 1.10. From BioStar 2 version 2.8.5 or earlier using MS SQL Server database, if the BioStar 2 was upgraded to a higher version after turning off the "Encrypt Personal Data on Database" the event logs did not appear from the Event Log menu. (Affects version: v2.8.0)
- 1.11. If there were duplicate rows in the TA database's Punch Log, the TIME ATTENDANCE menu could not be accessed after upgrading the version to 2.8.9. (Affects version: v2.8.9)
- 1.12. Face Detect Settings was initialized after changing face settings from the FaceStation F2's configuration page. (Affects version: v2.8.9)
- 1.13. User synchronization in the T&A menu did not work properly when adding users or editing user information after deleting a user with a history of modifying the punch logs. (Affects version: v2.8.9)
- 1.14. The event list was not displayed in event log data exported to PDF. (Affects version: v2.8.9)
- 1.15. The options for Wiegand Input, Output, and Input/Output were displayed as if they were able to be set simultaneously from the FaceStation F2's configuration page. (Affects version: v2.8.6)
- 1.16. If clicking Apply in the SERVER menu after setting the mobile access card option to 'Use', the setting was changed to 'Not Use'.
- 1.17. When registering a new user by using the same user ID of the deleted user who had Punch logs, the previous user's Punch logs were displayed. (Affects version: v2.8.9)

## 2. New Features and Improvements

### 2.1. Enhanced Visual Face functionality.

- Supports drag & drop when registering Visual Face with 'Upload Image.'
- Provides guidance on success or failure of Visual Face Mobile Enrollment so that users can retry registration in the case of failure.
- Changed the maximum size and capacity for Visual Face image files.

### 2.2. Improved Thermal Camera functionality.

- Added minimum threshold temperature setting.
- \* Device firmware versions that support minimum threshold temperature setting:
- FaceStation 2 firmware 1.4.2 or later
  - FaceStation F2 firmware 1.0.2 or later

### 2.3. Improved Email Settings.

- Limited the file size of a company logo image to 5 MB.
- Added a warning message for attempting to send a Send Visual Face Mobile Enrollment Link without setting the SMTP.
- Added a warning message for attempting to send a Visual Face Mobile Enrollment Link to users without email information.
- Supports SMTP servers that do not require a username and password.

### 2.4. Intelligent Slave Support

- Intelligent Slave: A function that enables 1:1 or 1:N matching directly from the Suprema device and transmits the authentication result as OSDP card data to the third-party controller.
- Supported devices: BioEntry W2 firmware 1.6.3 or later

### 2.5. Supports new Export/Import User Information.

\* The existing data file Export/Import User Information method from older BioStar 2 versions will not be supported after upgrading to this version.

\* Device firmware versions that support new Export/Import User Information:

- BioStation 2 firmware 1.9.0 or later
- BioStation A2 firmware 1.8.0 or later
- FaceStation 2 firmware 1.4.0 or later
- FaceStation F2 firmware 1.0.0 or later

\* For Visual Face registered through Upload Image or mobile links, data cannot be transferred to the FaceStation F2 using the Export/Import User Information.

### 2.6. Screensaver support for FaceStation 2 and FaceStation F2.

### 2.7. New API 2.8.10 standard supplement

- The largest user group ID was sent as a response value regardless of the user group ID when creating a user group using POST/api/user\_groups.
- Stabilized Swagger API functions related to server matching, CSV export and import.

### 2.8. Improved to recover only the file having an error when a conf file error occurs.

### 2.9. Updated the German resource file.

## 3. Bug fixes

### 3.1. Time between device and server was displayed differently when receiving email from BioStar 2. (Affects version: v2.6.0)

### 3.2. The new notification indication (N) remained at the bottom of the screen when an event occurred,

- even after clicking "Acknowledge" in the alert notification message. (Affects version: v2.7.11)
- 3.3. Logs were not displayed in real-time intermittently. (Affects version: v2.0.0)
  - 3.4. The real-time log was updated with delay or was missing when disconnected web socket session information remained. (Affects version: v2.0.0).
  - 3.5. Encryption was performed before the file was created in the image log creation process, creating a 0 KB file in the image log while using "Encrypt Personal Data on Database". (Affects version: v2.8.7)
  - 3.6. The filter condition setting screen was not displayed when selecting an event log filter in an environment using a specific Chrome version. (Affects version: v2.6.0)
  - 3.7. The BioStar server occupied too much memory in certain cases. (Affects version: v2.7.14)
  - 3.8. Punch log table data synchronization did not work properly when using MS SQL Server database. (Affects version: v2.8.9)

# Version 2.8.9 (Build No. 2.8.9.53)

Release: 2020-12-29

## 1. Main Fixes

- 1.1. Extended auth mode gets disabled intermittently when multiple FaceStation F2 devices try to connect to the server simultaneously. (Affects version: v2.8.8)
- 1.2. Punch logs were not displayed if the punch type was null in the updated individual reports by selecting the 'All Punches' option. (Affects version: v2.7.10)
- 1.3. Punch logs were not recorded properly in the individual reports updated by selecting the 'All Punches' option. (Affects version: v2.7.10)
  - The 'Check In' log was only recorded in the report even though the user selected 'Check Out' on the T&A device.
- 1.4. BioStar 2 could not connect with the TA database if using a port other than the default port when installed using MS SQL Windows authentication. (Affects version: v2.7.14)
- 1.5. PIN authentication failed due to the device default hash key transmission error. (Affects version: v2.4.0)
- 1.6. If both user data registered with a face template and user data registered with a visual face template were sent to FaceStation 2 and FaceStation F2 at the same time, the authentication failed on FaceStation F2. (Affects version: v2.8.6)
- 1.7. T&A device synchronization problems
  - Devices added in DEVICE menu were not synchronized with the TIME ATTENDANCE menu.
  - FaceLite added in DEVICE menu were not displayed in the T&A device list. (Affects version: v2.7.10)
  - Devices added in DEVICE menu were not displayed in the T&A device list because the value of device group ID became null due to a synchronization problem. (Affects version: v2.7.5)
- 1.8. When starting the T&A service, a user was automatically signed out of BioStar 2 and was not able to sign in again. (Affects version: v2.8.4)
  - When accessing the T&A service while a user was signed in to BioStar 2, 'Unknown error. Check the log file for detailed information' error message was displayed.
- 1.9. If clicking Apply in the SERVER menu after setting the mobile access card option to 'Use', the setting was changed to 'Not Use'.
- 1.10. An email notification about users who have reached their specified working hours was not sent even after configuring the SMTP setting of Automated Email. (Affects version: v2.8.6, v2.8.8)

## 2. New Features and Improvements

- 2.1. Stabilization of features for Mobile Access.
  - Supports Dynamic site.
  - Displays user information, such as photo, department, title, and period on the Mobile Access Cards.
  - Improves a user interface for resending Mobile Access Cards.
- 2.2. Provides a guide on the screen when registering Visual Face on the mobile device.
- 2.3. Renamed 'Email Setting' menu.

- Before: Email Contents
  - After: Email Setting
- 2.4. Renamed some events related to scheduled unlock zones.
  - 2.5. Updated some language resource files.
  - 2.6. Changed the names of db-converter log files.
  - 2.7. Changed to possible to edit the device's T&A settings only while the device is connected.
3. Bug fixes
- 3.1. An error occurred when creating work history after running user sync with personal information DB turned on or off. (Affects version: v2.8.0)
  - 3.2. A migration error occurred when encrypting and decrypting personal information DB since the table name was checked incorrectly during the Swap process. (Affects version: v2.8.0)
  - 3.3. The calculation was not possible if the calculation scope of the parity bit was overlapped with the scope of the other parity bits when setting the Wiegand format.
  - 3.4. BioStar 1.x logs did not appear in the event log list after the log migration since the Temper column was not supported on BioStar 1.x. (Affects version: v2.8.6)
  - 3.5. BioStar 2 occupied excessive memory when logging in as a custom level administrator with permissions for a lot of user groups in an environment using the MS SQL Server database. (Affects version: v2.8.7)
  - 3.6. When issuing mobile cards, model names of some devices were not correctly displayed in the pop-up message. (Affects version: v2.6.0)
  - 3.7. Delay occurred when uploading event logs related with temperature from FaceStation F2 to the server and unnecessary logs, such as temperature data with zero value, were uploaded. (Affects version: v2.8.6)

# Version 2.8.8 (Build No. 2.8.8.10)

Release: 2020-10-29

## 1. Main Fixes

- 1.1. Event logs from slave devices could not be viewed after applying an event filter.
- 1.2. When Mobile Access Cards were issued using CSV Import while Personal Information DB Encryption was in use, if there was a duplicate card ID within the unassigned CSN card list, an error occurred.
- 1.3. Even though Mobile Access had not been set to be used, Mobile Access was able to be registered using CSV Import.
- 1.4. When the server restarted, Automatic User Synchronization settings were changed to the default values.
- 1.5. If an image log file path was changed while using Personal Information DB Encryption, the image log files in the changed path was not encrypted.
- 1.6. When migration was conducted using the BioStar 1.x to BioStar 2.x Migration Tool, the cards of some users were missing.
- 1.7. When using the Automatic User Synchronization option in 'Specific Devices', the user data was deleted due to synchronization errors.
- 1.8. When using the Automatic User Synchronization option in 'Specific Devices', data of users who registered visual faces were not synchronized.
- 1.9. Language resource was not applied successfully to the device. (FSF2-ODB)

## 2. New Features and Improvements

- 2.1. Supports batch registration of Visual Face using CSV import.
- 2.2. Stabilization of the thermal camera function
  - The temperature indicator was added to notification emails.
  - A thermal inspection report has been added for monitoring.
- 2.3. When using the Automatic User Synchronization option in 'Specific Devices,' the server will limit the retry attempt to three times for failed transfers.
- 2.4. BioStar 2 performance improvements
  - Improved CSV import speed.
  - Reduced slowdown due to database load.
  - Improved screen loading and inquiry speed for users, devices, doors, and monitoring menus.
  - Improved card inquiry speed.
  - Improved login speed through changes in the frequency by changing the period of the log inquiry when entering the dashboard to weekly.
- 2.5. Improvements on New API 2.8.7
  - The problem of missing parameter size check logic when the period option is set as between while calling a User API query has been improved.
  - Stabilization of the Swagger API.

- The problem that the status value was displayed abnormally when viewing a user card using GET/api/cards has been improved.
- 2.6. Changed db-converter to run in the background when installing BioStar 2.
  - 2.7. Improved to check whether the encryption key matches when logging and show an error message if there is a mismatch.
  - 2.8. Improved the logic confirming database connection upon installing BioStar 2.
  - 2.9. Support of user synchronization exceptions in the Active Directory.
  - 2.10. Changed to not display login permission in the logs.
  - 2.11. Changed temperature column not to be a default column for event logs and real-time logs.
  - 2.12. Visual Face Mobile Enrollment email content had been improved.
3. Bug fixes
- 3.1. Card settings were set to 'Disabled' after changing the card settings in the CoreStation device detail page.
  - 3.2. Modified DB queries to ensure correct use of case-sensitive table names when using MariaDB in a Linux environment.
  - 3.3. It took a long time by referring a wrong address when entering MONITORING menu through the BioStar 2 cloud.
  - 3.4. When the System.conf file was corrupted, the enckey file was also corrupted.
  - 3.5. When User ID Type was set to Alphanumeric and Smart Card Type was set to Access on Card, the card ID did not automatically appear in the card ID section from the smart card issue screen.
  - 3.6. When a user was registered in numbers of access groups, the order of the access groups appearing in the user list was different every time.
  - 3.7. Errors related to running the video service
    - Modified redis service to run depending on whether the video service was running or not.
    - Modified to run http or https service depending on the use of the SSL.
  - 3.8. Problem where the Extended Auth Mode was deleted from BioStar 2, including the database.
  - 3.9. When running Send Visual Face Mobile Enrollment Link with the cloud disabled, the error message text was not appearing correctly.
  - 3.10. Visual Face image aspect ratio had been corrected.
  - 3.11. An abnormal delay when scanning fingerprints for visitors.
  - 3.12. Errors in the TIME ATTENDANCE menu
    - Punch Log History was not able to be modified.
    - The infinite loading occurred when updating Individual Report.
  - 3.13. When more than 20 devices were registered to use Mobile Access, up to 20 devices were only displayed in the device list.

# Version 2.8.6 (Build No. 2.8.6.38)

Release: 2020-09-21

## 1. New Features and Improvements

- 1.1. Supports server matching for face recognition devices.
  - FaceStation 2
- 1.2. Supports thermal camera on face recognition devices.
  - FaceStation 2
  - FaceStation F2
- 1.3. Adds the new credential.
  - Supports Visual Face and visual face mobile enrollment.
- 1.4. Supports the new devices.
  - FaceStation F2
  - BioEntry W2 (Rev 2)
- 1.5. Logs related to Thermal Camera were added to Trigger & Action in the device settings menu.

## 2. Bug fixes

- 2.1. Stabilization of Thermal Camera functions
  - A pop-up message not related to the function was displayed.
  - Event log was displayed in the temperature column of the CSV file.
  - Event logs were output in ascending order.
- 2.2. XPass D2 connected as a slave device of CoreStation was not displayed in the TIME ATTENDANCE device list.

# Version 2.8.5 (Build No. 2.8.5.46)

Release: 2020-08-25

## 1. Main Fixes

- 1.1. When the individual report was updated by selecting the 'All Punches' option, screen entered into an infinite loop state.
- 1.2. Upon setting a temporary schedule or leave, if 'Apply to Other user(s)' was selected, an error occurred.
- 1.3. List sorting by name and date did not work properly in individual reports.
- 1.4. Daily reports did not display the time of In and Out correctly after generating individual reports with 'All Punches' option
- 1.5. When there are many accumulated time cards, the speed of updating reports will slow down.

## 2. New Features and Improvements

- 2.1. Supports Wiegand devices as a time and attendance management device.
- 2.2. Improvement on usability of individual reports.
  - Added a row to display working hours to at the top of the report list for the period selected.
  - Changed column order and initial settings of the updated individual reports when selecting 'All Punches' option.
  - Improvement to the speed of viewing updated individual reports by selecting the 'In/Out Only' option.
- 2.3. Improvement to allow users with general user permissions to update own TA reports.

## 3. Bug fixes

- 3.1. Items not supported in the column settings of daily reports were displayed.
- 3.2. Upon running a CSV export in the updated individual reports by selecting the 'All Punches' option, the blank was displayed as null.
- 3.3. When setting a column other than the default settings in an individual report with the 'All Punches' option, the value was repeatedly displayed in the punch log column.
- 3.4. The name of a user group that had been changed in the updated individual reports by selecting the 'All Punches' option was not reflected.
- 3.5. If the exception column of the updated individual reports with the 'All Punches' option was an empty value, the value was displayed as '- '.
- 3.6. The data in the In and Out columns of the updated individual reports with the 'All Punches' option was not displayed and the Leave column was not displayed in a clickable form.
- 3.7. The individual report was not displayed according to the set list display count.
- 3.8. If the login ID was the same, the time card was displayed even if the session ID was different.
- 3.9. The time cards created in the past with the same session ID were accumulated.

# Version 2.8.4 (Build No. 2.8.4.34)

Release: 2020-08-05

## 1. Main Fixes

- 1.1. Allowed the unassigned card on the server to be registered by card reader or enter manually.
- 1.2. Data files using unsupported time formats failed to be imported.
- 1.3. Active Directory failed to synchronize when using Personal Information DB Encryption.
- 1.4. When searching for a user in the MS SQL Server database environment, the user failed to be found even though the user ID is within the supported range.
- 1.5. Partially missing event logs in the database when the server was overloaded.

## 2. New Features and Improvements

- 2.1. Stabilization of features for Mobile Access.
  - Improved the logic for issuing Mobile Access Cards.
  - Improved the logic for issuing Mobile Access Cards using CSV.
  - Added pop-up error code messages.
  - Added and improved messages related to Mobile Access Cards.
  - Limited the number of Mobile Access Cards that can be issued on the User details page.
  - Added pop-up messages to display dynamic sites are not supported yet.
  - Added check logic for devices that do not support Mobile Access Cards.
- 2.2. Improvement of backup and recovery logic for Web-App, CGI server system.conf.
- 2.3. Exclusion of TLS V1.1 for improved security
- 2.4. Improvement of redirection to the Suprema technical support page link ([support.supremainc.com](http://support.supremainc.com)) when REST API request fails.
- 2.5. Improved Thrift communication logic log.
- 2.6. Improved security vulnerabilities on Redis.
- 2.7. Improvements on New API 2.8.0
  - Updated API descriptions and phrases.
  - Disabled filters for users who have not accessed the system for a long time when outputting a new API list.
  - Disabled blacklist filter when outputting a new API list.
  - Added descriptions for required parameters in relation to the elevator.
  - Added API for unlocking devices.
  - Improved the problem of an error occurring when specifying an ID upon creating a user group by using POST/api/user\_groups.
- 2.8. Improvements on usability
  - Allowed users to enter a domain of at least 6 characters in '86 character@60-.20-.6-' format, depending on the user's email address type.
  - Changed the 'Edit' column of Custom Account Levels Set to 'Edit/Read'.

- Added Central European Time (CET) to the time zone option.
  - Displayed required items on the User details page.
  - Changed the default value to Access on Card from the smart card issue menu.
  - Improved sequence to move back to the device list page when the device is rebooted for language change, firmware upgrade, factory reset, etc.
  - Allowed device filtering in the MONITORING menu upon accessing it as a custom level administrator.
  - Changed the fields of Login ID and Password to be automatically hidden when the user's operation level is set to 'None'.
  - Prevented creation on user ID with only 0s.
  - Excluded unnecessary error logs.
- 2.9. Changed queries to retry for lock error occurring when multiple queries are executed at the same time.
- 2.10. Added step of checking the root password upon upgrading BioStar 2.
3. Bug fixes
- 3.1. A description of Base64 data has been added to the POST:/api/users fingerprint template in the BioStar 2 API document.
  - 3.2. Triggers and actions were not applied as set.
  - 3.3. When the log upload is set as automatic it was not outputted as a log.
  - 3.4. When the port was changed upon installing BioStar 2, the change did not automatically reflect in the server\_url.conf file.
  - 3.5. When a fingerprint registered by the visitor at check-in was stored in a decrypted state, upon the use of Personal Information DB Encryption, the fingerprint image was not displayed after the registered fingerprint was identified.
  - 3.6. If system.conf and setting.conf files were deleted, the TA server could not be started.
  - 3.7. Incorrect error codes were displayed in the graphic map.
  - 3.8. When performing migration using the BioStar 1.x to BioStar 2.x Migration Tool, the user group was not deleted so the migration fails.
  - 3.9. The Windows authentication connection failed when the database name, database user, and database password of the video were not entered in BioStar Settings.
  - 3.10. When adding a big image as a user profile image to PUT/api/users/, some of the image was cut off on the side of the screen.
  - 3.11. The INVALID\_JSON\_FORMAT error message appeared when clicking <Set Time> if the time setting on the Device details page wasn't changed.
  - 3.12. Mysqld.exe took up too much space on the CPU of the PC when querying an alarm from the MONITORING menu in an environment using MariaDB.
  - 3.13. When searching for a user name containing a specific character after encrypting personal information in the DB under an environment using an MS SQL Server database, if the resulting value did not exceed 1,000, the search was not performed.
  - 3.14. When failing to add a user after using the Automatic Synchronization Option of a user with a 'Specific Devices,' attempts for synchronization to all devices was conducted repeatedly.

3.15. Upon user synchronization in Active Directory, the number of users was not updated.

# Version 2.8.3 (Build No. 2.8.3.10)

Release: 2020-07-21

## 1. Main Fixes

- 1.1. The device rebooted abnormally when adding the device while Secure Communication with Device is on.
- 1.2. An error occurred when exporting user data to FaceStation 2.
- 1.3. The event log and the real-time log did not display Muster zone time limit event when logged in as a custom level operator.
- 1.4. 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.
- 1.5. When using a large number of user groups, some user groups did not appear on the monitoring menu.
- 1.6. 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.
- 1.7. When device connect and disconnect were abnormally repeated, the server responds slowly.
- 1.8. 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.
- 1.9. Image log files were not encrypted.
- 1.10. 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.
- 1.11. Intrusion detection log was not displayed in the real-time log.

## 2. New Features and Improvements

- 2.1. Supports Zone in the Admin Item Settings of the custom level.
- 2.2. Supports FaceStation 2 and FaceLite as a slave of CoreStation.
- 2.3. Renamed 'Mobile Access' service name.
  - Before: Mobile Credential
  - After: Mobile Access
- 2.4. Supports Mobile Access on BioLite N2.
- 2.5. Improved user group tree output performance while massive user groups (20,000 or more groups) are used.
- 2.6. Supports operation options on Anti-Passback zone to operate based on the door status.
- 2.7. Improved the scheduled unlock zone function to support elevator.
- 2.8. Improved Trigger & Actions to be able to use the output port of the BioStation 2.

- 2.9. Improved db-converter to check the error during query execution when installing BioStar 2.
- 2.10. Updated language resource files.

# Version 2.8.2 (Build No. 2.8.2.3)

Release: 2020-07-10

## 1. New Features and Improvements

### 1.1. Fixed local file inclusion (LFI) vulnerability.

- The vulnerability that could allow an attacker to gain local access via a web browser.

# Version 2.8.1 (Build No. 2.8.1.35)

Release: 2020-06-10

## 1. Main Fixes

- 1.1. When connecting as an administrator with device and user viewing privileges, only the event log containing both the device ID and user ID is displayed.
- 1.2. When setting up some languages, some functions of the TIME ATTENDANCE menu does not work properly.
  - Even if a user logs in as an administrator who has a reading permission for the TIME ATTENDANCE menu, only certain screens of the menu are displayed.
  - PDF export for daily reports does not work properly.
  - PDF export of the individual reports updated by selecting the 'All Punches' option does not work properly.
  - Unable to output some selection items on the Rule setting page.
- 1.3. Some TA reports are only displayed in portrait format from print preview screen when exporting to PDF.
- 1.4. In the environment using MS SQL Server database, after importing users when the user ID type is set to Number, the user list cannot be displayed correctly.
- 1.5. When importing a CSV file without the mobile credential column, the result pop-up message does not show.
- 1.6. When migrating from BioStar 1.x to BioStar 2.x, the existing users and user groups of BioStar 2 are not deleted.
- 1.7. In the environment using MS SQL Server database, the automated emails of Working Alarm Time Report are sent only once a week even if setting to send more than twice a week.
- 1.8. The individual report does not work as the column setting of the saved filter.
- 1.9. Even if connecting as an administrator with only devices, users, doors, and elevators reading permissions, the real-time logs and alarms of objects for which the administrator has no permission are shown.
- 1.10. Fixed to not access cache memory simultaneously.
- 1.11. When using personal information DB encryption, card authentication fails if an administrator sets to use server matching.
- 1.12. Users are not synchronized to the TIME ATTENDANCE menu intermittently.
- 1.13. BioStar 2 cannot be upgraded when installed using MS SQL Windows authentication.

## 2. New Features and Improvements

- 2.1. Supports MS SQL Server 2019.
- 2.2. Updated BioStar 2 copyright year.
- 2.3. Moved the 'In/Out Punches' and 'All Punches' options in the Individual Report.

### 3. Bug Fixes

- 3.1. Even if the user ID type is set to Number, an alphanumeric ID will be registered when registering the user through the API or device.
- 3.2. The CSV export on TA report does not work properly if an administrator moves the user group which is placed before the 1,000th unit to the subordinate folder of the user group which is placed after the 1,000th unit when the created user groups are more than 1,000 units.
- 3.3. The failed pop-up message is not displayed for users who failed to import due to mismatch of user ID type when importing user list by importing data files.
- 3.4. If the path related to ngrok in setting.conf is different from the actual ngrok installation path, the cloud will not work properly.
- 3.5. When migrating from BioStar 1.x to BioStar 2.x, the cards duplicated in BioStar v1.x cannot be assigned to users in BioStar 2.
- 3.6. When migrating from BioStar 1.x to BioStar 2.x, if the administrator sets the CSN type to LSB, the custom ID migration fails.
- 3.7. When connecting as a visitor operator, the custom visitor field does not appear on the visitor settings page.
- 3.8. The set number of days is counted incorrectly when setting the leave on the Schedule of the TIME ATTENDANCE menu.
- 3.9. When the language is set to Korean, if an administrator exports the updated individual report to CSV or PDF by selecting the 'All Punches' option, some column names are displayed differently from the client.
- 3.10. Fixed the individual report column settings to be displayed differently depending on the 'In/Out Punches' or 'All Punches' options.
- 3.11. PDF export of the individual reports does not work properly.
  - The date is not displayed on the first page.
  - Unnecessary pages are shown.
- 3.12. 'All Users' is displayed in English even if it is set as a language other than English when accessing the user menu in GNB.
- 3.13. Day start time and end time of time segment were able to be set to the same when Shift is set to Fixed or Floating.
- 3.14. The leave column in daily or individual reports does not appear in a clickable form.
- 3.15. Administrators other than the first administrator cannot activate the cloud.
- 3.16. Delete unnecessary device security communication codes in server settings.
- 3.17. CSN is not added when adding a user by importing CSV in version 2.7.14.
- 3.18. Two or more schedules were able to be set in the same period for the same user.
- 3.19. When exporting the individual report to PDF with "All Punches" option selected, the title information of each date is not displayed.

# Version 2.8.0 (Build No. 2.8.0.106)

Release: 2020-05-15

## 1. Main Fixes

- 1.1. Firmware upgrade does not succeed properly when using 'Secure Communication with Device' option.

## 2. New Features and Improvements

### 2.1. DB encryption to enhance security on personal information

- Encrypts profile image, user ID, name, phone number, user IP, Email information for sender and recipients, login ID, login password, face template, fingerprint template, card ID, smart card layout key, custom information for user and visitor, and image logs.
- Supports manual key storage path setting for encryption key.

### 2.2. Changed to allow upgrading from BioStar 2.6.0 or higher to the latest version.

## 3. Bug Fixes

- 3.1. An issue when using 'Secure Communication with Device' generates a false error indicating Wiegand readers cannot be used since the firmware or device does not support the option.

# Version 2.7.14 (Build No. 2.7.14.52)

Release: 2020-04-03

## 1. Main Fixes

- 1.1. Slow loading of BioStar 2 when there are a large number of created user groups.
- 1.2. A problem where the offline activation for AC, TA, Video and Visitor licenses doesn't work properly in version 2.7.11 and 2.7.12.
- 1.3. When the license for TA is activated offline, offline activation for other licenses cannot be performed without refreshing or reentering the server menu.
- 1.4. In the environment using MS SQL Server database and when two or more <Trigger & Action> of the device were created, setting different actions for the same trigger causes an error.
- 1.5. Error occurs when installing BioStar 2 on any path other than the default installation path.
  - The service does not start normally.
  - The page does not load when connecting via HTTPS from a web browser.
- 1.6. User menu cannot be accessed properly by other clients at the same time when a user's face is being registered.
- 1.7. If User ID Type is set as alphanumeric, authentication succeeds even with AoC (Access on Card) registered on a blacklist.
- 1.8. When the User ID Type is set to alphanumeric, an error occurs if the user ID registered directly on the device contained a space or some symbol (,).
  - When entering the setting page of the device from the BioStar 2, BioStar 2 is abnormally terminated.
- 1.9. Problems with user group information not being display normally on the Schedule setting screen of the TA menu when there are more than 1,000 user groups created.
- 1.10. Printing of a user list doesn't work properly when there are a large number of registered users.
- 1.11. Event logs not transferred to the server when the device gets disconnected from the server and then reconnected following by a certain condition.
- 1.12. Problem where the device is not displayed in the list if the user doesn't click the refresh button after changing the port of the USB Device Agent.
- 1.13. When upgrading the version of BioStar 2, db-converter error log occurs.
- 1.14. Punch log manually entered by the administrator does not appear in the individual report correctly when updated with the 'All Punches' option selected.
- 1.15. When there are a large number of registered users, the print preview screen of the user list shows only some users.

## 2. New Features and Improvements

- 2.1. Support for connecting new devices.
  - XPass D2 (Rev 2)
- 2.2. Enhancement in Mobile Credential usage.
  - Added feature to send mobile credential certificates directly to connected devices on the BioStar 2.

- 2.3. Supports MS SQL Server 2017.
  - 2.4. Supports Windows Authentication for MS SQL database server connections.
  - 2.5. Added option to receive results sorted as desired when retrieving event logs using api/events/search from the BioStar 2 local API.
  - 2.6. Stabilization of 'Specific Devices' Automatic User Synchronization option
    - Improved synchronization speed.
    - Improved to synchronize only devices that belong to the corresponding access level or floor level.
    - Improved the problem of changes not being applied properly if the user group is changed by drag-and-drop when access groups are set as user groups.
  - 2.7. Added Floor Control API to BioStar 2 API Documents.
  - 2.8. Allowed additional symbols (-, \_) in the user's email account field.
3. Bug Fixes
- 3.1. An issue where the number of user faces registered on the BioStar 2 server is 3,000 or more, a face cannot be set in the authentication mode even though the number stored on the FaceStation 2 is less than 3,000.
  - 3.2. A bug where signal setting changes in <Trigger & Action> of a device does not get applied properly.
  - 3.3. A bug when using the USB fingerprint scanner, the fingerprints cannot be registered in ISO, ANSI378 template formats.
  - 3.4. Removed unnecessary UI from the setting pages of BioEntry R2 and XPass D2.
  - 3.5. A bug where the text of each item displays in overlap on the image log screen when the language is set as Russian.
  - 3.6. A problem where the CSV user import list not being displayed properly.
    - Some characters in user IDs are missing.
    - Some users are missing.
  - 3.7. Incorrect messages when clicking a cell that does not have the time value in the IN or Out column from the individual report updated with the 'All Punches' option selected.
  - 3.8. Incorrect labeling in the individual report updated with the 'All Punches' option selected.
    - 'Meal Start', 'Break Start' incorrectly output to 'In'.
    - 'Meal End' and 'Break End' incorrectly output to 'Out'.
  - 3.9. A bug when the 'First check-in Last check-out' option is not enabled, events without punch type does not appear in the individual report when updated with the 'All Punches' option selected.

# Version 2.7.12 (Build No. 2.7.12.39)

Release: 2020-01-15

## 1. Main Fixes

- 1.1. A problem where BioStar 2 server does not start correctly when a certain Windows OS event does not exist.
- 1.2. Improved Muster Zone to not fall into a deadlock while processing event logs.
- 1.3. A bug in TA module where it did not allow the next leave's start time to overlap the previous leave's end time.
- 1.4. Improved performance when having a great deal of user groups.
- 1.5. An issue where access through BioStar 2 Cloud doesn't work due to an abnormal behavior of ngrok.
- 1.6. An issue where access through BioStar 2 Cloud doesn't work due to an automatic update on ngrok.
- 1.7. Fixed TA module to update reports related to break time properly.
- 1.8. Fixed the 'Specific Devices' Automatic User Synchronization option to work accurately when users are created using CSV import.

## 2. New Features and Improvements

- 2.1. Added the new Suprema Mobile Credential.
- 2.2. Stabilized 'Specific Devices' Automatic User Synchronization option.
- 2.3. Improved TA module to allow generating reports simultaneously on multiple clients.
- 2.4. Applied code signing on BioStar2 installer including executables and library files.
- 2.5. Changed version of Java due to subscription policy on versions higher than 1.8.0\_201.
  - Before: 1.8.0\_231
  - After: 1.8.0\_201

## 3. Bug Fixes

- 3.1. An issue where Chinese characters were not displayed correctly on the exported PDF TA report.
- 3.2. A bug in an environment using MS SQL Server database where the results are not correct when searched in languages using Unicode.
- 3.3. An issue where the user does not get displayed on the user list properly due to a bug when CSV file contains user group information.
- 3.4. A bug where 'Image Log' did not work correctly with 'Access Denied(Anti-tailgating)' event.
- 3.5. An issue where a custom level administrator with permission only on a specific user group could view all user's real-time logs.
- 3.6. A bug where 'Time Code' does not appear from the <Rule> menu on TA module when the language is set as Japanese.
- 3.7. A bug where the action of 'Trigger & Action' configuration from device disappears after saving the settings.

- 3.8. An issue where an error occurs when updating the TA report that has data exceeding the maximum length of the 'Exception' column.
- 3.9. Fixed an error message that shows inaccurate status.
  - Incorrect password popup displays when the BioStar 2 server cannot connect to the database.

# Version 2.7.11 (Build No. 2.7.11.65)

Release: 2019-12-04

## 1. Main Fixes

- 1.1. Even though the card type is changed on the Device setting page, the setting is not applied.
- 1.2. The CPU usage increases because the event log import module operates continuously without idle time.

## 2. New Features and Improvements

### 2.1. Enhanced Security Settings

- Added logic to check file extensions to limit malicious file uploads.
- Improved to select whether to allow simultaneous access using the same account.
- Limited to connect only when the IP information of the account and the IP information of the accessing PC match when logging in by adding an IP address item to the user information.

### 2.2. Added 'Specific Devices(Only devices belonging to the access group)' option to <Automatic User Synchronization>.

### 2.3. Improved 'Alert List' and 'Alarm Monitor' features to reduce the load time of the dashboard page.

- Changed icons and phrases.
- Changed to output only alert list of the last 6 months.
- Changed to output only the last 15 alarms out of those that have not been checked in the last 6 months.

### 2.4. Applied the latest BioMini Plus SDK library to the USB Device Agent.

### 2.5. Supports the alert sound for 'Input(Event Name Change)' in the <Trigger & Action> of the device.

### 2.6. Supports the sorting of lists for the User Group column of the <Muster Status> page on the MONITORING menu.

### 2.7. Supports the sorting of lists according to the <User ID Type> settings.

- The 'ID' column of the user list on the USER menu
- The 'User ID' column of the <Muster Status> page on the MONITORING menu
- The list of 'User' on the Add New Access Group page

### 2.8. Changes the Java version.

- Before: 1.8.0\_221
- After: 1.8.0\_231

## 3. Bug Fixes

### 3.1. When using the CoreStation as multiple elevator controllers, the logic for checking the maximum number of connections (32) does not work.

### 3.2. When stopping the BioStar 2 server, related processes such as Java.exe and node.exe do not terminate.

### 3.3. The Cloud Use setting is changed to 'Not Use' when upgrading the version of BioStar 2.

- 3.4. Emails aren't sent even though automatic emails for overtime have been set up.
- 3.5. The 'ACB\_ERROR\_CODE.150' error occurs because the current time value was not entered normally when setting the elevator.
- 3.6. The image file storage path changes to a wrong path when the image log delete option is enabled.
- 3.7. The timeout event in the muster zone does not function properly.
- 3.8. The button to go to the last page on the Audit Trail page does not function properly.
- 3.9. The added device list does not display properly on the screen.
- 3.10. Modified to install the BioStar 2 properly even if some setting is missing in Setting.conf file when upgrading the version.
- 3.11. The values entered in custom user fields are not reflected in the T&A report.
- 3.12. Stabilization of Time Attendance
  - Users are not synchronized to the TIME ATTENDANCE menu.
  - The TIME ATTENDANCE menu is not loaded properly.
- 3.13. Stabilization of the Swagger API
  - Even if the parameter of /api/devices is not mandatory in the Swagger API, the query is impossible if the value is not selected.
  - Duplicate description of two different APIs

# Version 2.7.10 (Build No. 2.7.10.21)

Release: 2019-09-19

## 1. Main Fixes

- 1.1. When the User ID Type is set to Alphanumeric, the card ID is not displayed and authentication fails when authenticating with AoC (Access on Card).
- 1.2. If the start or end date of the Temporary Schedule is set as a holiday or the end date is set as the day before a holiday, the schedule cannot be created.
- 1.3. Temporary Schedules is created on a date that does not have a shift applied.
- 1.4. Users without the permission for Monitoring can view real-time logs of devices through a web socket.
- 1.5. When adding a door, the setting of door sensor is applied differently than the settings.
- 1.6. If the T&A device is disconnected and the device is not reconnected after restarting the server, the following problems occur.
  - The device is not displayed in the T&A device list.
  - T&A report is not available with USB import and export on that device.
- 1.7. If changing a user group or access group on the user settings page, the user's access group is deleted when the user is transferred to the device by Automatic User Synchronization.
- 1.8. Authentication fails if a user authenticates with AoC (Access on Card) issued as the mobile card.
- 1.9. When you assign a schedule to a user on the Schedule page of the TIME ATTENDANCE menu and apply it, loading is not completed due to the overload of the TA server.
- 1.10. When a user without administrator permissions logs in through the cloud, the user cannot log in normally because of the permission check.
- 1.11. An error occurs when a user requests the offline key for Time Attendance license.

## 2. New Features and Improvements

- 2.1. Support for connecting new devices.
  - FaceLite
  - XPass 2 (XP2-MDPB, XP2-GDPB, XP2-GKDPB)
- 2.2. Support to the USB fingerprint scanner in VISITOR menu.
  - Supported devices: BioMini, BioMini Plus, BioMini Plus 2
- 2.3. Added the BioStar 2 Swagger.
- 2.4. Improved to control access when a user without administrator permissions attempts to access menus that the user does not have access to.
- 2.5. Improved the Custom Level for T&A management.
  - User can use Time Code, Shift, Schedule Template, Rule and Schedule regardless of permission, and can edit or read according to the permission of Admin Menu Settings.
- 2.6. Add Automatic backup function for Setting.conf file.
  - Automatic backup of Setting.conf file
  - Support to the logs to determine cause if Setting.conf file is corrupted

- 2.7. Improved the resource files not to be deleted when upgrading BioStar 2 version if a user creates and uses language resource files other than that supported by the regular version.
  - 2.8. Modified to allow the user to edit 'User ID' in <User Field Mapping> of Active Directory.
  - 2.9. Update the resource files of Japanese, Arabic, and Spanish.
  - 2.10. Support to allow the custom user field that added in the <SERVER> of Settings to be used in the T&A report.
  - 2.11. Supports the sorting for entire data in the T&A report.
  - 2.12. Added option to select 'First in & Last Out' or 'All Punches' to search conditions of the individual report.
  - 2.13. Changes the Java version.
    - Before: 1.8.0\_212
    - After: 1.8.0\_221
3. Bug Fixes
- 3.1. The titles of the list for USER, DEVICE, DOOR and ELEVATOR menus are displayed in English even if it is set as a language other than English.
  - 3.2. When setting up a language other than Korean or English, the 'All Users' and 'Different Users' options do not appear due to misalignment of options on the <Manage Users in Device> page if the string is long.
  - 3.3. The fingerprint search function does not work properly for application to visit the Terms and Conditions.
  - 3.4. In the TIME ATTENDANCE menu, only 1,000 schedules are visible.
    - Modified to display up to 20,000 items.
  - 3.5. BioStar 2 and Suprema 2nd generation devices support Wiegand card format up to 256 bits, but only up to 32 digits when inputting card data values manually.
    - Modified to support up to 78 digits when inputting card data.
  - 3.6. User cannot access TIME ATTENDANCE menu when connecting to BioStar 2 with a domain name.
  - 3.7. When upgrading the version, the upgraded version is not applied in the system config item of AC, TA and Video database.
  - 3.8. Restricted special characters can be input in usernames.
  - 3.9. Visitors who have already agreed to the visit terms and conditions on the Visit Application Page are asked to agree again at check-in in the VISITOR menu.
  - 3.10. The event name is output in English when exporting the event logs to CSV file if the language is set to a newly supported language (Spanish, Arabic).
  - 3.11. Modified to allow addition of up to 32 events when setting up the image log.
  - 3.12. If BioStar 2 service file is not replaced during the version upgrade, BioStar 2 will not be installed normally.
    - Modified that the service file to replace automatically when restarting the operating system after the BioStar 2 installation is complete.
    - Outputs a pop-up message that prompts users to restart the operating system after the BioStar 2 installation completes.
  - 3.13. In version 2.7.7 of BioStar, local APIs could be registered and used even though access control license was not activated.

- 3.14. The ID of Wiegand Reader is displayed differently from the actual ID when checking the door information with [GET] doors in BioStar 2 API.
- 3.15. If a user sets the Date Format to dd/mm/yyyy, the error popup for the Period item is displayed even though the user set the period normally on the Visitor page.
- 3.16. Some user groups are missing during the migration in BioStar 1.x to BioStar 2.x Migration Tool.
- 3.17. If you upgrade XPass 2 (XP2-GKDPB) from the pop-up message that prompts users to upgrade the firmware at BioStar 2 login, the upgrade fails.

# Version 2.7.8 (Build No. 2.7.8.42)

Release: 2019-07-17

## 1. Main Fixes

- 1.1. A user cannot access to BioStar 2 if the language is set to Turkish on Windows.
- 1.2. A user cannot access to BioStar 1.x to BioStar 2.x Migration Tool in an environment using Oracle database.
- 1.3. Some logs are missing during log migration in BioStar 1.x to BioStar 2.x Migration Tool.

## 2. New Features and Improvements

- 2.1. Enables users to search for visitors using fingerprints in the visit application page and VISITOR menu.
- 2.2. Supports user group synchronization in Active Directory.
- 2.3. Supports multiple use function of controllers.
  - Supported Devices: CoreStation
  - Detail: Supports configuring the CoreStation as a controller for up to 32 elevators
- 2.4. Supports Anti-Tailgating.
- 2.5. Supports setting options for Wiegand authentication result output.
  - User ID and Card ID
- 2.6. Supports options for selection by card type
  - Displays card options supported by each device in the BioStar 2 device settings to allow users to select those options.
- 2.7. Supports the fingerprint/face duplicate check when registering users on a device.

## 3. Bug Fixes

- 3.1. Improved user interface in VISITOR menu.
  - Duress fingerprint option is displayed.
  - The duplicate check button is displayed when registering visitor fingerprints.
  - A prompt for visitor PC assignment appearing as a pop-up message, but then connects to the login screen, when accessing the visit application page without setting up a visitor PC.
  - <Delete Visitor> button remains in the output state even when the user changes the status filter to "Visit application (expired)" after checking the visitor in the visit application list.
  - Improved pop-up prompts to confirm deletion when deleting fields created in visitor settings.
  - Check-in approval is possible even if the user does not agree to the privacy policy when checking in visitors.
  - The day is not selectable if <Expiry Date> of <Period> is selected on the calendar when applying for a visit on the visit application page.
  - A statement about the duration of personal information retention is displayed on the visit application page.
  - The changed language does not apply to phrases in the input field in real time when changing

- language settings on the visit application page.
- Running <Column Setting> in the visitor's main screen automatically deselects all selections.
  - When accessing the visit application page without setting up a Visit PC, entering the BioStar 2 server address in the address bar while switching to the Visit PC settings screen causes an error.
  - Improved wording of expressions in Visitor settings, VISITOR menu, and visit application page.
- 3.2. Deleted unused events in image log settings.
  - 3.3. The user information is not output in <Manage Users in Device>.
  - 3.4. The connection between BioStar 2 and Active Directory servers fails when the Active Directory encryption option is enabled after connecting to an Active Directory server.
  - 3.5. Modified to check session expiration on some API calls.
  - 3.6. The last sync time, as well as the connection test success or failure times, are output on <Synchronization> in Active Directory settings.
  - 3.7. The sync time in the Active Directory settings is not updated in real time.
  - 3.8. Errors occur when setting the period entry for user or visitor registration if the date format is set to 'dd/mm/yyyy'.

# Version 2.7.7 (Build No. 2.7.7.38)

Release: 2019-06-19

## 1. Main Fixes

- 1.1. Even if changing the Smart Card Layout option to 'None', that setting is not applied.
- 1.2. When restarting MS SQL Server, the database is not connected normally.
- 1.3. 'Soft anti-passback violation detected' and 'Hard anti-passback violation detected' options are missed from the event item of IMAGE LOG.
- 1.4. Some devices(BS2-OIPW, BSA2-OIPW) support the RFID cards that are different from the correct options.
- 1.5. If Custom User Field is configured, the custom field name is displayed but data is not output when printing the user list.
- 1.6. When the Administrator option is set in the device setting, that setting is not reset even if the device is reset.
- 1.7. The BioStar 2 server will not be able to connect to the Active Directory server without restarting the server after copying the root certificate when setting the encryption of the Active Directory.
- 1.8. The custom level administrator created in BioStar 2.3.0 or earlier will not be output in versions 2.6.3 or later.
- 1.9. When changing the settings of the smart card layout, only the layout of the card type with the changes is synchronized.
- 1.10. In an environment that uses an MS SQL Server database, an error occurs if there is a log with 32 characters of user ID when importing the event logs manually or automatically.
- 1.11. Some logs are not imported when importing the event logs manually or automatically.

## 2. New Features and Improvements

- 2.1. Add the visitor management.
- 2.2. The license policy of Time & Attendance is changed.
- 2.3. Improved that a user can access the Time Attendance menu using a private domain address.
- 2.4. Improved to allow users with login IDs to proceed first when users are synchronized to the Time Attendance menu.
- 2.5. Provided the 'Error dbscript db-converter' message on the Completing the BioStar 2 Setup Wizard screen if a db script error occurs during the BioStar 2 installation.
- 2.6. Changes the Java version.
  - Before: 1.8.0\_201
  - After: 1.8.0\_212

## 3. Bug Fixes

- 3.1. Problems that the user interface does not output properly.
  - Icons and strings are displayed abnormally when a user select the user group in FACE GROUP MATCHING.

- The Admin Item Settings of ACCOUNT is not displayed properly.
  - Strings are not displayed properly when a user selects an item from the Admin Item Settings in ACCOUNT.
- 3.2. Even if the Use Automatic Door is set to 'ON' in the door setting, it will still be displayed as 'OFF' on the screen.
- 3.3. When the language is set to Spanish(Spain), the schedule calendar of the Time Attendance menu is displayed Chinese characters.

# Version 2.7.6 (Build No. 2.7.6.16)

Release: 2019-05-20

## 1. Main Fixes

- 1.1. If an administrator set the language to Spanish(Spain), exporting the T&A report in PDF does not work properly.
- 1.2. If you set an event by selecting the Input (Event Name Change) option in Trigger & Action of the device settings, the event does not work properly as follows:
  - DM-20
    - a) The alert does not occur.
    - b) '-1' is displayed instead of the event name set in Real-time Log.
    - c) 'Input detect' is displayed instead of the event name set in Event Log.
  - All devices
    - a) The code name is displayed instead of the event name set in DASH BOARD and MONITORING menu.
- 1.3. Change the recording method for users who do not have access logs.
  - Displayed in Long-term Idle Users menu.
  - Log 'No history' on the Last Entrance Date column.
- 1.4. When an administrator logs in as the custom level with permissions to a user group, the administrator cannot select the devices and subgroups belonging to the device group in <Delete From Device>.
- 1.5. Deactivate 'Check the database connection' and 'Generate the database tables' options in the Custom installation window when upgrading the BioStar 2 version.

## 2. New Features and Improvements

- 2.1. Support to the Clear APB for each user.
- 2.2. Add BioStar 1.x to BioStar 2.x Migration Tool.
  - Supports the use of user and event logs from BioStar 1.x in BioStar 2.
- 2.3. Add the event items to IMAGE LOG menu.
- 2.4. Add the encryption option to Active Directory.
- 2.5. Improve that the administrator can change the port 9000 in FastCGI of Port menu.
- 2.6. Improve that the time of events is displayed as the time zone, device time, and server time on the alarm email.

## 3. Bug Fixes

- 3.1. Fixed a security vulnerability by deactivating the 3DES encryption option.
- 3.2. If an administrator sets the language other than Korean or English, an error occurs when a user logs in and select Help menu.
- 3.3. The 'Input detect' event that occurred in the interlock zone is displayed as '-1' in Real-time log.

- 3.4. If an administrator selects a user group when adding an access group, the information and the number of the access group are not output properly.

# Version 2.7.5 (Build No. 2.7.5.7)

Release: 2019-04-11

1. New Features and Improvements
  - 1.1. Add the Active Directory menu.
    - Supports the use of Windows Active Directory user data in BioStar 2.
  - 1.2. Supports the sorting of lists in the USER, DEVICE, and DOOR menus.
    - USER: Group, Status column
    - DEVICE: RS-485 column
    - DOOR: Group column
  - 1.3. Removes the unsupported AoC events from the DEVICE, VIDEO and the Trigger & Action of Settings.
  - 1.4. Supports that the administrator can change the port 9000 in setting.conf.
  - 1.5. Added an Ambient Brightness option to the FaceStation 2 slave device.
2. Bug Fixes
  - 2.1. The iCLASS Seos and DESFire Advanced card formats are not applied when the administrator sets up the smart card layout.
  - 2.2. If an administrator set a device as an Arm / Disarm device in the Intrusion Alarm Zone, and then exclude the door that is configured by that device, a 'Failed to parse JSON (700)' error occurs.
  - 2.3. If user group information is not created normally when an administrator adds or edits a user group, the user list is not displayed when that group is selected.
  - 2.4. Even if an administrator adds more than 249 custom levels, only 249 are displayed on the screen.

# Version 2.7.4 (Build No. 2.7.4.25)

Release: 2019-03-20

## 1. Main Fixes

- 1.1. If you set a language that has more than two characters for the language delimiter in the resource file, that language will not properly be applied to the T & A menu.
- 1.2. One of the BioStar 2 configuration files, the nssm.exe, is not installed or has been deleted from the T&A and Video web server services list because some antivirus programs have determined that the file is a malicious program.
- 1.3. The door information of access level setting is displayed differently from the setting.
- 1.4. When operating the Delete From Device in the USER menu, devices belonging to the group cannot be selected.

## 2. New Features and Improvements

- 2.1. Enhanced security of login passwords.
  - Limits the use of passwords that contain the same string, consecutive string, and login ID
  - Limits reuse of the same password
- 2.2. Support for Quick Enrollment for FaceStation 2.
  - FaceStation 2 FW V1.2.2 or later
- 2.3. Support to Spanish and Arabic.
- 2.4. Support to the unlimited number of Custom Levels.
- 2.5. Changes the Java version.
  - Before: 1.8.0\_191
  - After: 1.8.0\_201

## 3. Bug Fixes

- 3.1. The Dual Authentication setting does not display properly in the user interface even if you enable that option in elevator settings.

# Version 2.7.3 (Build No. 2.7.3.23)

Release: 2019-02-25

## 1. Main Fixes

- 1.1. Arabic does not display properly if an administrator exports the T&A report in PDF.
- 1.2. When an administrator logs in as the custom level, even though the administrator has permissions to a specific device and the user, cannot transfer users to that device.
- 1.3. If upgrading to version 2.7.0 or later, the administrator cannot add a leave in a previously set schedule.
- 1.4. When there are more than 50 user groups, you cannot export the T & A report to a CSV file if any groups contain subgroups.

## 2. New Features and Improvements

- 2.1. Increase the number of administrators that can be added per device.
  - Before: 10
  - After: up to 1,000 (depends on the firmware version of the device.)
- 2.2. Change the way new settings are applied when adding administrators using batch edit of devices.
  - Before: Overwrite a new setting to existing settings.
  - After: Add a new setting to existing settings.
- 2.3. Improved that the device will be normally connected when you reconnect the device even when it is configured as a port forwarding.

## 3. Bug Fixes

- 3.1. When creating an Access Group, the setting is not applied properly if you add the same user to the User Group and User at the same time.
- 3.2. If an administrator edits the settings of the device on the server, Server Private Msg option on that device will always change to disabled.
- 3.3. The T&A function does not work properly if you upgrade from version 2.7.0 or earlier to 2.7.2.

# Version 2.7.2 (Build No. 2.7.2.19)

Release: 2019-01-15

## 1. Main Fixes

- 1.1. If more than 16 cameras are added to the server, the camera screen is not output.
- 1.2. In an environment that uses an MS SQL Server database, the server restarts when an administrator adds more than one signal input event to the trigger & action of the device.

## 2. New Features and Improvements

- 2.1. Add the Security menu.
  - Change Password Level options.
  - Support to the setting for Maximum Password Age.
  - Support to the setting for Maximum Password Change Limit.
  - Support to the setting options for password failures at login.
- 2.2. Support to Live Video View on Graphic Map.
- 2.3. Support to viewing Anti-passback Zone and Fire Alarm Zone on Graphic Map.
- 2.4. Support to the Storage Path Settings for image logs.
- 2.5. Supports Allowed a day before/after time setting for working 24 hours or longer.

## 3. Bug Fixes

- 3.1. The HTML tag is displayed in the daylight saving time settings page.
- 3.2. Once an image file set with a graphics map is deleted, the graphics map image cannot be modified.

# Version 2.7.1 (Build No. 2.7.1.13)

Release: 2018-12-20

## 1. Main Fixes

- 1.1. Fixed a security vulnerability: Cross Site Scripting.
- 1.2. The row setting changes when the page is refreshed after setting the number of rows in the monitoring menu.
- 1.3. The log does not display normally when a user moves the page back and forth after setting the event log filter in the Monitoring menu.

## 2. New Features and Improvements

- 2.1. Supports synchronization of all devices connected to the server when users update the device.
- 2.2. Improves the ability to delete users on a device from the server's user menu.
- 2.3. Support to Input(Event Name Change) of Trigger & Action in the device advanced setting.
- 2.4. Changes the Java version.
  - Before: 1.8.0\_161
  - After: 1.8.0\_191
- 2.5. Provides the log about whether a user has been updated on the device or the server.
- 2.6. Adds root password verification procedures during installation and upgrade.

## 3. Bug Fixes

- 3.1. Support to the OM-120 Relay time setting value from 1 second.

# Version 2.7.0 (Build No. 2.7.0.50)

Release: 2018-11-21

## 1. New Features and Improvements

- 1.1. Support to Graphic Map
  - 1.2. Support to the working alarm time report and an automated alarm email
  - 1.3. Improves the option to Add Custom Level.
- Adds a graphic map group to Admin Item Settings.
  - Improves the ability to set up user groups and device groups according to Custom Account Level in Time & Attendance.
    - 1.4. Support to the floating shift.
    - 1.5. Support to Punch out Time Limit in the flexible shift.
    - 1.6. Improves that an administrator can select weekend days when setting up the Schedule Template.
    - 1.7. Support to the minimum duration setting when configuring the overtime management.
    - 1.8. Separate the rounding setting of shift and overtime management.
    - 1.9. Support Fixed option for Meal deduction and Break Time setting.
    - 1.10. The Attendance management time added from Time Code is displayed in the Daily Summary Report and Individual Summary Report.
    - 1.11. Support for AES encryption option on DESFire card.
    - 1.12. Support to DESFire advanced option.
    - 1.13. Support to the number of users, fingerprints, faces, and cards in Manage Users in Device.
    - 1.14. Support to unlimited number of access levels and access groups.
    - 1.15. Punch Log History report has been improved to display the modified time.
    - 1.16. Improve the process for generating the time card.
    - 1.17. Improves the T&A report to display only the time excluding the dates in Check In and Check Out.
    - 1.18. Change the default value of the period in the T&A report.
    - 1.19. Improves to upgrading the version to the latest version directly in BioStar 2.5.0 or higher.
    - 1.20. Improves usability
  - Support to the separator option in CSV export.
  - Add <Apply & Add New> button to Time Code, Shift, Schedule Template, Rule, Schedule setting screen.
  - Change some special characters (\, /, ;, \*, ?, ", ', ` , <, >, |, .) to be unavailable when setting a user name.
  - Improves that the Edit popup or T&A report page is displayed if clicking the result value of the T&A report.
  - Improves to set the time of overtime work in minutes.

- Change the start date of the week to Monday.
- Remove the Temporary Schedule from the Time Card.
- Support for Arabic.
- Change the loading icon of the Time Attendance menu like any other menu.

## 2. Bug Fixes

- 2.1. If a user connects to BioStar 2 after specifying the hostname in the Windows, the user cannot access the T&A menu.
- 2.2. Unable to add a Wigand device to BioEntry W2.
- 2.3. Users can access a higher level of Web Server Home in the web server.
- 2.4. If you set Leave to start or end date of Daylight Saving Time, the incorrect time is displayed.
- 2.5. Change the <Punch in Time Limit> setting of Flexible Shift to operate based on the setting of <Day start time>.
- 2.6. Users who have special characters (-, \_) in the ID cannot be selected in the T & A report.
- 2.7. If you change the server port value for the cloud and then restore the value before the change, a user cannot enter the Time Attendance menu.
- 2.8. Department information does not display from root when exporting the T&A report to CSV format.
- 2.9. The APB database management table is reset periodically, regardless of the Reset Time setting in the global APB zone.
- 2.10. In an environment that uses an MS SQL Server database, the modified date format setting is not normally applied to Audit Trail menu.
- 2.11. When a user upgrades the version of BioStar 2, the number of user access groups is displayed differently than the existing settings.

# Version 2.6.4 (Build No. 2.6.4.7)

Release: 2018-10-26

## 1. Bug Fixes

- 1.1. The duplicate logs are output when a user runs CSV export.
- 1.2. The server receives requests with a version lower than TLS 1.1 (Supports TLS 1.1 and above).
- 1.3. The user cannot set the same action for different triggers when setting Trigger & Action, Intrusion Alarm Zone, or Interlock Zone.
- 1.4. The assignment complete message is displayed even if a user assigns an already assigned card to another user using the API.
- 1.5. When a user who does not have permission on the door menu logs, the door list of the zone menu is disabled.
- 1.6. The Add Zone option is not displayed when a user right-clicks each item in the zone menu.

# Version 2.6.3 (Build No. 2.6.3.73)

Release: 2018-09-18

## 1. New Features and Improvements

- 1.1. Improves the performance of showing lists.
- 1.2. Improves the option to Add Custom Level.
  - Adds Admin Item Settings option.
- 1.3. Improves to allow the custom level administrator with edit or read permission to the monitoring menu to receive alerts.

## 2. Bug Fixes

- 2.1. The Video menu in Settings is not displayed on the screen if the PC with BioStar 2 is not connected to the network.
- 2.2. If an elevator group that contains subgroups moves to a child of another elevator group, it causes an error and BioStar 2 does not work normally.
- 2.3. RTC and DHCP are displayed on Display/Sound of XPass D2(XPD2-GKDB) device page.
- 2.4. The firmware upgrade notification does not appear even though connecting XPass D2(XPD2-GKDB) that has a previous version firmware to BioStar 2.
- 2.5. XPass D2(XPD2-GKDB) succeeds in authentication if AoC ID is entered as keypad even though server matching is enabled.
- 2.6. If an upper and lower group without elevator is moved at the same time, the group is not displayed normally.
- 2.7. If the date format is set on the device and then it is connected to BioStar 2, the date format changes to the different option.
- 2.8. Scanning the fingerprint on the BioMini causes an error and BioStar 2 does not work normally.
- 2.9. If the user name is set to Arabic, the name does not display normally.
- 2.10. Fixed a security vulnerability that allows a user account to acquire an administrator permissions.
- 2.11. BioStar 2 version upgrade fails when using Java 1.8.0 or later on PC with BioStar 2 installed.
- 2.12. Some records are missing in T&A reports.

# Version 2.6.2 (Build No. 2.6.2.64)

Release: 2018-06-25

## 1. New Features and Improvements

- 1.1. Support for user and log import and export via USB.
- 1.2. Support an option for processing PIN input for XPass D2 (XPD2-GKDB) the same as card ID.
- 1.3. Support for real-time video viewing.
- 1.4. Improves usability and phraseology.
- 1.5. Improves event log retrieval speed.
- 1.6. Support for connecting new devices.
  - FaceStation 2 (FS2-DS), BioLite N2 (BLN2-PAB), XPass D2 (XPD2-GDB, XPD2-GKDB)

## 2. Bug Fixes

- 2.1. Issue where BioStar 2 log continues to be displayed as daylight saving time even after the set period of daylight saving time has ended.
- 2.2. Issue where the video server does not work if the video license is activated offline.
- 2.3. Issue where it is not possible to change configurable options when a user with administrator logs in from a mobile device.
- 2.4. Issue in version 2.4.1 or earlier where database does not migrate and login page does not appear when a version upgrade has been carried out while HTTPS default port is used.
- 2.5. Issue where server does not retry after failing to connect to database.
- 2.6. Issue where device is not auto-synced when face template has been deleted.
- 2.7. Issue where device secure communication status can be changed to 'Disabled' even when user login ID, password, and PIN have been set.
- 2.8. Issue where page display error occurs when device details page is accessed with OM-120 and DM-20 disconnected.
- 2.9. Issue where after a daylight saving time schedule has been set up on BioStar 2 server, a daylight saving schedule cannot be assigned to FaceStation 2 device.
- 2.10. Issue where model names of XPass D2 and BioLite N2 are not correctly displayed in the firmware upgrade list.
- 2.11. Issue where daylight saving time cannot be set up for FaceStation 2 device when version 2.6.0 has been installed newly.
- 2.12. Issue regarding selecting start date for daily schedule or selecting holiday dates where an extra month is added to the resulting screen in the case of months without a 31st day.
- 2.13. Issue where it is not possible to set system log storage period to 120 days.
- 2.14. Issue in a version upgraded from version 2.5.0 where USB Agent does not start automatically when user account control is set to default value.
- 2.15. Issue where incorrect IP address notification pop-up appears when a string is entered in the server address field.
- 2.16. Issue where video server does not shut down when changing database port.
- 2.17. Issue where NVR details screen is displayed when scrolling the page with arrow keys at the upper right corner of Device Details.

- 2.18. Issue where "17677" is displayed in BioStar 2 event log when reset without network.
- 2.19. Changed data encryption related pop-up text that appears when adding a device.
- 2.20. Issue where it is possible to configure devices other than those connected to the same RS-485 network when editing pre-configured schedule unlocked zone.
- 2.21. Issue where error pop-up does not appear when you change user ID type to alphanumeric characters after adding BioLite Net and Xpass S2.
- 2.22. Issue where despite daylight saving time having been set up, a time not applicable to Monitoring's floor and zone statuses is displayed.
- 2.23. Issue regarding changing the status of one or more global zones where changing the status of one zone does not automatically change the status of the other zones.
- 2.24. Issue where video license input window is activated after an upgrade to version 2.6.2.
- 2.25. Issue where master device switches to synchronization error status when deleting a door belonging to Access Level.
- 2.26. Issue where fingerprint image does not appear normally when a smart card has been added after the addition of two or more fingerprints of user.
- 2.27. Issue where device name does not show in tamper-on alarm pop-up if a tamper has occurred on the device after reset without network.
- 2.28. Issue where UI does not show normally when displaying an image log with a user name on a larger screen.
- 2.29. Issue regarding batch-editing doors where incorrect notification pop-up appears when the OK button is clicked without changing the settings.
- 2.30. Issue where column switches to its default value when entering the card menu again after changing the column settings in the card menu in Settings.
- 2.31. Issue where NVR appears when filtering by device name in Device Status or Alert History in Monitoring.
- 2.32. Issue where the "unknown" message does not appear in Schedule Lock/Unlock zone status when the device has been disconnected from the network.
- 2.33. Issue where Add, Delete, Modify NVR/camera features do not function when user has logged in as a video operator.
- 2.34. Issue where schedules are not updated in the video menu.
- 2.35. Issue where session timeout notification occurs when accessing video menu while using Time Attendance menu.
- 2.36. Issue where camera recording events for daily/holiday schedules do not function properly.
- 2.37. Problem that the change point is not updated even if the setting of the door configured in the camera menu is changed.
- 2.38. Issue where device search fails when adding a camera after failure to updating NVR configuration information.
- 2.39. Issue where you cannot proceed to the next step when selecting NVR in video menu after deleting schedules set up for camera.

# Version 2.6.1 (Build No. 2.6.1.10)

Release: 2018-05-15

## 1. Bug Fixes

- 1.1. Issue where it is not possible to sync new logs to Time Attendance and Video when using MSSQL.
- 1.2. Execution time error when upgrading version 2.4.1 > 2.5 > 2.6.
- 1.3. A change has been made so that moving is possible only when upgrading to a new version and the version of existing BioStar 2 is 2.5.

# Version 2.6.0 (Build No 2.6.0\_155)

Release: 2018-03-23

1. New Features and Improvements
  - 1.1. Support for Daylight Saving Time setting.
  - 1.2. Strengthened security settings.
    - Manual management of server and device encryption keys.
  - 1.3. Support for event log retention period setup.
  - 1.4. Support for muster zone and interlock zone.
  - 1.5. Changed AC license.
  - 1.6. Support for device connectivity
    - BioMini Plus 2, BioLite N2, ad XPass D2
  - 1.7. Support Reset without Network Settings.
  - 1.8. Support for Seos card.
  - 1.9. Support for user ID auto addition.
  - 1.10. Improved system log setup UI.
  - 1.11. Added an option to delete personal information and credentials when issuing AoC.
  - 1.12. Support for personal authentication for AoC.
  - 1.13. Support for customized advanced permissions for monitoring.
  - 1.14. Added port settings for port management.
  - 1.15. Support for one device mode (legacy).
  - 1.16. Support for simultaneous use of Wiegand I/O.
  - 1.17. Support for security tamper.
  - 1.18. Support for unassigned blacklist card reassignment.
  - 1.19. Added video storage status and management options.
  - 1.20. Added video recording status indication to event log.
  - 1.21. Improved Wiegand card search function.
  - 1.22. Improved working conditions and behavior.
  - 1.23. Changed site key hexadecimal value entry for smart cards.
  - 1.24. Improved firmware upgrade message and alert behavior.
  - 1.25. Stabilized MSSQL performance.
  - 1.26. A change has been made so that if there exists a user, device, door, or elevator belonging to a group, the group cannot be deleted.
  - 1.27. Support for BioEntry W2 (BEW2-OHP) smart settings.

**Suprema**  
SECURITY & BIOMETRICS

Suprema Inc.  
16F Parkview Tower  
248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 463-863 Republic of Korea  
Tel.+82-31-783-4502 Fax.+82-31-783-4503  
sales@supremainc.com www.supremainc.com