

# BioStar 2

## Revision Notes

Version 2.9.6

English  
EN 301.00.BS2

# 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
2	2.2.1 > 2.3 > 2.4 > 2.4.1 > 2.5.0 > 2.6.4 > Latest Version
2.2 2.2.1 2.2.2	2.3 > 2.4 > 2.4.1 > 2.5.0 > 2.6.4 > Latest Version
2.3	2.4 > 2.4.1 > 2.5.0 > 2.6.4 > Latest Version
2.4	2.4.1 > 2.5.0 > 2.6.4 > Latest Version
2.5 2.6	2.6.4 > Latest Version
2.6.4 or higher	Latest Version

- 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.

Port			
• HTTP Port	80		Available
• Web-socket Port	9002		Available
• Database Port	3312		Available
• T&A HTTPS Port	3002		Available
• FastCGI Port	9000		Available
• Unified Gateway HTTPS Port	5002		Available
• Report HTTPS port	4214		Available
• HTTPS Port	443		Available
• API Port	9010		Available
• T&A HTTP Port	3000		Available
• T&A Cloud Port	52001		Available
• Unified Gateway HTTP Port	5000		Available
• Report HTTP port	4213		Available



## Notice on improved Administrator Guide

Starting with BioStar v2.9.5, **Feature Guide** is provided separately by topic on how to use new or improved features.

## New Features and Improvements

1. Supports a new device.
  - XPass 2 (XP2-MAPB)
2. 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**.
3. 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.
4. Supports the feature to select the resolution of the video transmitted from the device when using **Intercom** or **RTSP**.
  - **Intercom Video Resolution**
  - **RTSP Video Resolution**
5. The authentication result display option supports selecting how the user ID and name are displayed on the device's authentication result screen.
  - **User ID Display**
  - **User Name Display**
6. Supports **SIP Server Transport**, which selects the SIP transmission method when setting up the SIP server of the **Intercom** on the device.
7. Supports **Auth Mode** editing in **Batch Edit** of devices.
8. FaceStation F2 (firmware v2.1.4 or higher) - Added **Power Line Frequency** option to prevent flicker based on the illuminance environment in which the device is installed.
9. Supports FeliCa card from **Custom Smart Card Layout**.
10. The **Face Detection** feature on X-Station 2 is discontinued.
11. Improved security vulnerabilities.
  - Improved XSS security vulnerability.
  - Improved web socket security vulnerabilities.
  - Improved CSRF security vulnerability.
  - Upgraded 7zip version.
  - Improved security vulnerabilities of SSL/TLS Diffie-Hellman Modulus.
  - Upgraded Spring Framework version.
  - Improved security vulnerabilities of HTTP Content-Security-Policy.
  - Removed the auto-completion feature from all input fields.
  - Improved SQL Injection security vulnerabilities.
  - Improved BioStar 2 certificate security vulnerabilities.
  - Improved **Active Directory** security vulnerabilities.

12. Improved Time and Attendance security vulnerabilities.
  - Improved security vulnerabilities of Access-Control-Allow-Origin.
  - Added X-Frame-Options to T&A API document.
13. Improved user inquiry screen performance in the **TIME ATTENDANCE** → **Schedule** menu.
14. Added a refresh button to the T&A record details view screen (calendar, list) in the **TIME ATTENDANCE** → **Report** menu.
15. Changed the TLS default version of the T&A server to 1.2 when using MS SQL Server database.
16. Improved time display method in the T&A Report in countries that do not use Daylight Saving Time (DST).
17. Improved synchronization performance of the latest data when there is a large volume of old T&A report data.
18. Improved to display both the user name and user ID in the **User** column of the **Alert List**.
19. Improved the time to be displayed in seconds in the **Date** column of the **Alert List**.
20. Improved performance when Automatic User Synchronization is set to Specific Devices(Only devices belonging to the access group) option.
  - Improved performance when adding, modifying, or deleting **ZONE**.
  - Improved **Access Level** edit performance.
21. Improved **User Group** and **Device Group** synchronization of **TIME ATTENDANCE**.
22. Fixed error pop-up message is displayed when uploading visual face files with filenames starting with '0' while the **User ID Type** is set to **Number**.
23. Improved check logic for duplicate user IDs when using **User ID Type** as **Alphanumeric**.
24. Improved to use a static IP address when calling internal APIs from C to Java.
25. Increased the maximum number of authentication modes for a specific device.
26. Added new index for environments using MS SQL Server databases.
27. Adjusted the maximum number of characters that can be entered in the card ID when issuing a CSN mobile card.
28. Improved to display a pop-up message when the user sets the encryption key storage path directly with special characters in the path.
29. Improved Wiegand reader to be supported in **TRIGGER & ACTION**.
30. Improved to check the server's readiness before starting the BioStar 2 server and display a popup message in case of any issues.
31. Improved the display of user-related event logs in **CSV Export** or **Print** to differentiate whether the event occurred from the device or server.
32. Improved to leave an event log and alert in real-time when **Maximum Invalid Attempts** is exceeded.
33. Added API to edit information in batch up to 100 users.
34. Improved password **Maximum Invalid Attempts** limit option to be applied by default value.
35. Added notification pop-up messages for unset items and reduced the conditions required when creating an **Access Group**.
36. Improved login API.
37. Improved mobile card ID check logic.
38. Improved BioStar 2 Setting UI
39. Improved display in the status window of BioStar 2 Setting when the service ports are in use.
40. Updated Spanish resource file.

## Bug Fixes

1. Email sending fails in certain SMTP environments. (Affects version: v2.6.0)
2. When using Global APB and dual authentication mode on a specific device, authentication failure occurs for the first user. (Affects version: v2.9.0)
3. In the **Fire Alarm** zone list, the **Active/Inactive** column is not sorted properly in ascending or descending order. (Affects version: v2.4.0)
4. **Visitor Operator** is displayed in the **Operator Level** of a user without a visitor license. (Affects version: v2.7.7)
5. Fixed display errors in Arabic for certain items. (Affects version: v2.8.9)
6. The card gets falsely issued in BioStar 2 when a smart card is issued with Visual Face template using a disconnected device. (Affects version: v2.8.2)
7. The launcher service (biostar-server.exe) terminates in specific environments. (Affects version: v2.0.0)
8. When exporting **Elevator permission by Floor** as CSV and **Elevator Permission by User** list in **Status** of the **ACCESS CONTROL** menu, the user ID and name are encrypted and output. (Affects version: v2.8.0)
9. When restarting the BioStar 2 service, the **Security Level** of Face in **Server Matching** and the **Display user profile image when there is no image log for the events** settings in **Image Log** are initialized. (Affects version: v2.2.1)
10. After locking a specific device, no sound is being played. (Affects version: v2.9.1)
11. The **Full Access** is activated even though the device is included in specific access levels or access groups. (Affects version: v2.8.16)
12. When selecting all devices in a device group and performing **Delete Data & Sync Device**, all devices are synchronized, leading to unintended synchronization. (Affects version: v2.0.0)
13. When editing device settings using device **Batch Edit**, the **Use QR as Card** is activated. (Affects version: v2.8.16)
14. After logging in and out with an account that has a **Custom Level** without user menu permissions, and then logging in with an Administrator account, the **Add New User** screen is displayed when entering the **USER** menu. (Affects version: v2.7.2)
15. When using **Specific Devices(Only devices belonging to the access group)** mode, modifying the visitor's credentials does not synchronize with the device. (Affects version: v2.8.14)
16. The device registered to the mobile access card does not get deleted. (Affects version: v2.8.7)
17. When printing the door list, status of all doors are printed as **Normal**. (Affects version: v2.4.0)
18. The device selected to enroll a credential is displayed in the device list in the **User** → **Credential** even after being deleted. (Affects version: v2.0.0)
19. Images that cannot be used for authentication gets enrolled. (Affects version: v2.9.0)
20. An error occurs when deleting BioStar 2 event logs from an operating system that does not use the Gregorian calendar. (Affects version: v2.6.0)
21. **Column List** is displayed abnormally when configuring **Column Setting** in a specific zone. (Affects version: v2.5.0)
22. Device groups are displayed abnormally when the device ID exceeds a certain number of digits. (Affects version: v2.6.3)
23. When a device that supports **Occupancy Limit** is in Arm mode state, **Delete Data & Sync Device** proceeds while the attempt should fail. (Affects version: v2.8.11)
24. When changing the user name while logging in, the user name in the upper right corner is not updated. (Affects version: v2.0.0)
25. When executing the **Send Visual Face Mobile Enrollment Link** in a user group without users, an error popup message does not appear. (Affects version: v2.8.6)

26. When importing a CSV file containing **User Group** structured in 8 depths, the User Groups are not added correctly. (Affects version: v2.4.0)
27. Fixed error message that appears when user expiration period is out of range when importing a CSV file. (Affects version: v2.8.16)
28. When setting **Scheduled Lock** and **Scheduled Unlock** Zone, doors from a different RS-485 network appears. (Affects version: v2.4.0)
29. After logging in, when entering **Settings** → **TRIGGER & ACTION**, the **Action - Output** list does not appear. (Affects version: v2.0.0)
30. **User ID Type** changes when all devices are not connected to the server. (Affects version: v2.4.0)
31. PDF is not printed properly when sorting columns by **User Group** in the **USER** menu. (Affects version: v2.7.8)
32. When **Encrypt Personal Data on Database** is enabled, if more than 16 characters are entered for the user ID and then decrypted, an error occurs in user ID sorting. (Affects version: v2.8.9)
33. Unsupported menu appears on the device detail page of the BioStation 2a (BS2A-ODPB) model. (Affects version: v2.9.4)
34. Any changes on **Access Group** does not synchronize with the user information in the **Muster Zone**. (Affects version: v2.6.0)
35. When selecting all users in a specific user group and then **Send Visual Face Mobile Enrollment Link**, an email is also sent to all users not included in the group. (Affects version: v2.9.0)
36. Device type could be changed using the API on registered devices. (Affects version: v2.5.0)
37. When creating or editing a user using the User API, logout occurs when the API is called with empty credentials values. (Affects version: v2.0.0)
38. **Data File Import** from **Event Log** causes an unintended logout intermittently. (Affects version: v2.9.1)
39. An error pop-up does not occur under certain conditions when running **Data File Import** from the **USER** menu. (Affects version: v2.9.3)
40. **Custom Smart Card Layout** with status 'Unknown' is synced to the device. (Affects version: v2.9.4)
41. Changing the **Custom Smart Card Layout** to **None** on a device with the **Custom Smart Card** set results in the device being synchronized with the default layout. (Affects version: v2.9.4)
42. When a user with permission to only some device groups enrolls a card, devices without permission also appear in the list. (Affects version: v2.8.14)
43. Entering the **Access Control** menu causes an unintended logout intermittently. (Affects version: v2.2.0)
44. When users click the + or - buttons for schedules where users are not registered in the **Schedule** menu, an error popup message appears. (Affects version: v2.8.1)
45. In an environment using MS SQL Server database, the **TIME ATTENDANCE** menu cannot be accessed when BioStar 2 is upgraded from a specific version (2.8.10 ~ 2.8.12). (Affects version: v2.8.10)
46. When using the **First check-in & Last check-out** option and setting **Break Time** to **Fixed** in **Shift**, the T&A report time is not displayed correctly. (Affects version: v2.7.0)
47. When exporting to PDF, certain languages are displayed abnormally. (Affects version: v2.7.0)
48. Improved the Time and Attendance API document page.
  - Connections are successfully made when using other protocols. (Affects version: v2.2.0)
49. When there are many temporary schedules, accessing the Schedule becomes slow. (Affects version: v2.7.0)
50. When logging in as a user with **Edit/Read** permission to the **TIME ATTENDANCE** menu, some T&A menus do not appear. (Affects version: v2.8.9)
51. When calling the Report API, the data is not returned as specified by the designated fields. (Affects version: v2.8.11)

- 52. After editing the **Punchlogs storage duration** in the **Setting** of the **TIME ATTENDANCE** menu, editing certain other options without clicking the **Apply** button results in the **Punchlogs storage duration** being applied. (Affects version: v2.8.17)
- 53. Infinite loading occurs when calling Schedule Create API in the T&A API document. (Affects version: v2.8.9)
- 54. An error occurs when a user with **T&A Operator** permissions generates a T&A **Report** for the **Custom User Field**. (Affects version: v2.8.14)
- 55. T&A report events for a specific device are not synchronized. (Affects version: v2.8.9)
- 56. **REPORT** and **New Dashboard** menu screens are displayed abnormally after changing to some languages. (Affects version: v2.9.5)
- 57. An error occurs when generating a **Custom Report** after logging in as a custom level account. (Affects version: v2.9.3)
- 58. When backing up repeatedly using the **System Backup** feature, folders and files already saved in the backup file storage path are deleted. (Affects version: v2.9.3)
- 59. The event log is not saved properly when the month changes while using the **Automatic System Backup** option. (Affects version: v2.9.3)
- 60. When generating a **Custom Report** with filter conditions set, the correct data is not generated. (Affects version: v2.9.3)
- 61. The events in **MONITORING** and **REPORT** are logged with different timestamps. (Affects version: v2.9.3)
- 62. When using the **BioStar 2 Restore** tool to restore data backed up from the same version as the current BioStar 2, errors occur during the restoration process. (Affects version: v2.9.4)



## Notice on improved Administrator Guide

Starting with BioStar v2.9.5, **Feature Guide** is provided separately by topic on how to use new or improved features.

## New Features and Improvements

1. Added **New Dashboard** feature.
2. Added **Quick Action** feature.
3. Added **Timed Anti PassBack** feature in the **DOOR** menu.
4. Supports user profile photo and visual face enrollment using webcam.
5. Improved **USER** menu.
  - Added column types that can be displayed on the **USER** menu screen.  
**Period (Start datetime, End datetime), Operator Level, Login ID, User IP, PIN, QR/Barcode, Mobile Access Card**
  - Added **Advanced Search** feature.  
**ID, Name, Email, Department, Title, Telephone, Group, Access Group, Status, Operator Level, Card, Custom User Field**
6. Improved **TRIGGER & ACTION** menu.
  - Added events displayed in **MONITORING**.
  - Supports door relay operation settings.
  - Added notification email sending function based on action.
  - Added **Action List** where multiple actions can be set as one.
7. Improvements have been made to allow setting **Suprema Smart Card** from **Batch Edit**.
8. Added **CSV Field** to prevent already issued **Template on Mobile** from being deleted when overwritten by **CSV Import**.
  - ToM AoC, ToM SCC
9. Changed CoreStation's wireless antenna module and wireless door lock connection specification
  - Wireless antenna modules that can be connected to one CoreStation: 1 → 2
  - Wireless door locks that can be connected to one wireless antenna module: 8 → 6
  - Maximum connectable wireless door lock: 8 → 12
10. Improved certificate errors due to Google Chrome and Microsoft Edge browser updates.



## Bug Fixes

1. **REPORT** menu is not available when using a separate domain and private certificate. (Affects version: v2.9.3)
2. **REPORT** menu is not available when installed on an Azure database. (Affects version: v2.9.3)
3. When printing Unicode characters on cards using **Card Printer**, the characters are printed garbled. (Affects version: v2.9.3)
4. The operation fails if it takes more than 1 minute when using **Unified Gateway**. (Affects version: v2.9.3)
5. In an environment where multiple OM-120s are connected to the master device and the device is synchronized using the **Automatic User Synchronization - Specific Devices** mode and then authenticated, the relay malfunctions. (Affects version: v2.7.14)

## New Features and Improvements

1. Supports a new device.
  - BioStation 2a
2. Added **Template on Mobile** feature.
  - BioStation 3 FW 1.2.0 or higher
3. Supports Wireless Door Lock connection to CoreStation.
  - Supported OSDP antenna and wireless door lock are as below.
    - U&Z OSDP Antenna: CX8936
    - U&Z Wireless Door Lock: CX217x(Handle), CX212x(Knob)
4. Supports **Custom Smart Card Layout**.
  - Xpass D2 FW 1.7.1 or higher
5. Improved **Smart Card Layout** settings.
6. Improved **Administrator** menu UI on the **DEVICE** detail page.
7. Improved UX of **Use for BioStar 2 Login** menu in **ACTIVE DIRECTORY**.
8. Updated OpenSSL.
9. Updated OpenJDK.
10. Improved SQL Injection vulnerability.
11. Improved security vulnerabilities in **Active Directory** account settings.
12. Separated ID storage for **Active Directory** login and BioStar 2 login.
13. Improved security vulnerabilities in video packages.
14. Improved **Audit Trail** to be logged when a user attempts to log in with an incorrect password and exceeds the set Maximum Invalid Attempts.
15. Blocked modifying **Login ID** to '1', the default ID of the initial administrator.
  - After upgrading to BioStar 2 v2.9.4, cannot log in using the administrator account with **Login ID** set to '1'.
16. Improved **User Group** sync performance.
17. Improved performance when **Automatic User Synchronization** is set to **Specific Devices(Only devices belonging to the access group)** option.
  - Improved **Access Group** edit performance.
  - Improved device **Batch Edit** performance.
  - Improved **Access Level** and **Floor Level** creation performance.
  - Improved **DOOR** edit and deletion performance.
18. Improved sync performance when device gets reconnected to server.
19. Improved user search performance in **VISITOR**.
20. Blocked issuing **Secure Credential** when **Card ID** starts with 0.
21. Improved device initialization guidance message not to be displayed if the Smart Card Layout set on the device does not exist in BioStar 2.
22. Improved to stop requesting logs to a device if it sends abnormal event logs to the server more than 5 times.

23. Added to check for duplicate user IDs or login IDs while decrypting data by setting **Encrypt Personal Data on Database to Not Use**.
24. Deleted unsupported ports from the **Port** menu.
  - **Report Cloud Port**
25. Improved to display of supported special characters in a pop-up message when a user name contains unsupported characters.
26. Improved the error message displayed when connecting a dormant account in the Airfob Portal or an account using private authentication mode to Mobile Access in BioStar 2.
27. Improved error message appears when attempting to delete a disconnected device from the **MOBILE ACCESS**.
28. Changed device names
  - Xpass 2 → XPass 2
  - Xpass D2 → XPass D2
29. Improved Japanese in **Send Visual Face Mobile Enrollment Link** mail.

## Bug Fixes

1. Server freezes when printing PDF from specific lists in the **MONITORING** menu. (Affects version: v2.9.3)
2. Email is not received after issuing and saving a **BioStar 2 QR** in the **USER** menu. (Affects version: v2.8.11)
3. When connecting a specific device, the set **T&A Key** is not logged intermittently in **Event Log**. (Affects version: v2.8.14)
4. When searching for an **Access Group** in the **ACCESS CONTROL** menu, the page move button from the detail page of **Access Group** does not navigate within the searched list but navigates from the all **Access Group** list. (Affects version: v2.3.0)
5. Not receiving updated door relay status from **Graphic Map**. (Affects version: v2.8.16)
6. When creating a user using the API, assigning a card that is being used by another user causes a duplicate card error and the user creation fails. (Affects version: v2.8.14)
7. Repeatedly changing the **Mode** when adding a **Fire Alarm Zone** does not display the changes correctly. (Affects version: v2.6.3)
8. When logging in with a Custom Level account, filtering in **Real-time Log** does not work as set. (Affects version: v2.6.3)
9. Displaying 'Login Required' pop-up when logging out of BioStar 2. (Affects version: v2.8.10)
10. Enabling **Maximum Password Age** in the **SECURITY** menu, will not be able to log in with an **Active Directory** account. (Affects version: v2.8.16)
11. Intermittent failure when creating more than 1000 users using **CSV Import**. (Affects version: v2.9.3)
12. Incorrect user ID can be created using **CSV Import**. (Affects version: v2.8.16)
13. When changing user information by overwriting it with **CSV Import** for a user with Access on Card issued, the AoC information is deleted but does not get added to a blacklist. (Affects version: v2.3.0)
14. From devices connected as master-slave-Wiegand, the Wiegand reader's operation log is not displayed when a user with an access level for a specific device group views the event log. (Affects version: v2.6.3)
15. Adding a resource file for some languages and changing the language setting to that language does not display in that language. (Affects version: v2.8.14)
16. Intermittent logout issue when adding BioEntry W2. (Affects version: v2.9.0)
17. Devices does not get deleted when deleting more than 1000 devices in an environment using MSSQL. (Affects version: v2.9.3)
18. User search does not work in an environment using MSSQL. (Affects version: v2.8.0)
19. Logout issue when calling the event search API without filling in required parameters. (Affects version: v2.0.0)
20. Authentication fails with **CSN Mobile** card when using **Server Matching**. (Affects version: v2.9.0)
21. Adding the AoC (Access on Card) to the blacklist when card writing fails. (Affects version: v2.4.1)

22. The server does not shut down normally when executing encryption and decryption. (Affects version: v2.8.0)
23. When **Use for BioStar 2 Login** is enabled in **ACTIVE DIRECTORY** menu, and the user's Operator Level is set to None, the login ID information gets deleted. (Affects version: v2.8.16)
24. If **Use for BioStar 2 login** is enabled in **ACTIVE DIRECTORY** menu, login will fail with user IDs starting with numbers. (Affects version: v2.8.16)
25. After exporting users to USB from FaceStation F2 v2.x.x, visual faces are not uploaded when running **Data File Import** from BioStar 2. (Affects version: v2.8.10)
  - \* FaceStation F2 firmware v1.x.x no longer supports **Data File Export** in BioStar 2. Please upgrade your device firmware to use **Data File Export**.
26. When deleting a user with an enrolled mobile card after setting **Mobile Access Setting** to **Not Use**, an unnecessary error pop-up is displayed. (Affects version: v2.9.0)
27. When calling an API using /api/users/data\_export?id=\*, the server terminates if the user entered in the id parameter does not exist on the server. (Affects version: v2.8.10)
28. When issuing CSN cards using API, it is possible to issue with an invalid CARD\_ID. (Affects version: v2.0.0)
  - CARD\_ID contains non-numeric values
  - CARD\_ID exceeds 32 characters
  - CARD\_ID starts with 0
29. A smart card issued using DE-620 with a default key gets incorrect key written to the card. (Affects version: v2.8.14)
30. After upgrading BioStar 2 in an environment that uses **VIDEO**, the **Video Log** is not displayed in the **Event Log**. (Affects version: v2.8.4)
31. **BioStar Setting** application closes when clicking the **Test Connection** button in **BioStar Setting** application. (Affects version: v2.9.3)
32. When creating a **User Detail** report in the **REPORT** menu, an error occurs if there is a user with **User Group** selected. (Affects version: v2.9.3)
33. When BioStar 2 is installed on the D drive, the report service does not start. (Affects version: v2.9.3)
34. Authentication events for **Muster Zone** not updating in the **Event Log** when authenticating with a mobile card. (Affects version: v2.8.6)
35. When entering the device details page by selecting a device, the server terminates intermittently. (Affects version: v2.0.0)

## New Features and Improvements

1. Added **REPORT** feature.
2. Added **CARD PRINTER** feature.
  - Supports card printing directly from BioStar 2 using the cardPresso.
3. Added **SYSTEM BACKUP** and **RESTORE** feature.
  - Provides **BioStar Restore** program that can restore the system using backup files (included in BioStar 2 installer).
4. Supports QR code authentication in BioStation 3.
  - Firmware v1.1.0 or higher.
5. Supports Xpass D2 **Keypad Backlight**.
  - XPass D2 (XPD2-GKDB) hardware V02M, firmware v1.7.1 or higher.
6. Improved security vulnerabilities.
  - Update Moment.js library version.
  - Updated Lodash library version.
  - Improved enckey file creation logic.
7. Improved update speed on **CSV Import** when using **Encrypt Personal Data on Database**.
8. Improved to properly recognize characters using UTF-16 in CSV files when **CSV Import**.
9. Improved Time & Attendance security vulnerabilities.
  - Swagger UI Version upgrade.
  - Added X-Frame-Options.
  - Improvement of iframe vulnerability by providing Unified Gateway feature.
10. Improved pop-up messages that appear when adding users to the **TIME ATTENDANCE** menu when exceeding the maximum number of users set by license type.
11. Improved performance when **Automatic User Synchronization** is set to **Specific Devices(Only devices belonging to the access group)** option.
  - Improved device setup performance.
  - Improved processing performance on zone activation/inactivation.
  - Improved synchronization performance when moving user groups.
12. Improved inefficient DB check logics when executing queries on the server.
13. Improved performance by adding missing indexes to temporary tables.
14. Optimized subquery when updating or deleting temporary tables using the User API.
15. Improved **Door Status** inquiry performance of **MONITORING**.
16. Improved to check whether unsupported characters are used in user names when enrolling mobile access card.
17. Supports entering symbols (+, -, @, .) in configuration of the **Intercom** menu.
  - **SIP Username, Authorization ID, Extension Number**
18. Added event code related to QR code authentication.

19. Added a guide message to the existing license menu location (**Settings > SERVER**) to prevent location confusion due to the new **LICENSE** menu.
20. Improvement of error message that appears when enrolling mobile access card when an **Email** is not entered in the user information.
21. Improved visibility of icons for each device in the device list.
22. Updated login page.

## Bug Fixes

1. The **Enroll** button is intermittently disabled on the **Enroll Mobile Access Card** screen. (Affects version: v2.8.9)
2. The server crashes when the server fails to retrieve tracking data using `getTrackingInfo`. (Affects version: v2.6.0)
3. When **Select All** and **Delete From Device** are performed on users searched with specific conditions, unselected users get deleted. (Affects version: v2.7.1)
4. Device added as **Enrollment Device** in the **SERVER** menu does not get deleted properly. (Affects version: v2.2.1)
5. When adding a device to **Enrollment Device** in the **SERVER** menu, the device is not searched. (Affects version: v2.2.1)
6. When the server is restarted while the **Session Timeout** in the **SERVER** menu is set, the **Session Timeout** operates as the default value (60 minutes). (Affects version: v2.8.14)
7. Incorrectly displaying the values of items that exceed the maximum in **Usage** on the **Dashboard**. (Affects version: v2.0.0)
8. Authentication succeeded with a blacklisted **Access On Card** containing a specific alphabet or symbol in the card ID. (Affects version: v2.7.14)
9. User data not syncing to the device after completing **Data File Import** in the **USER** menu. (Affects version: v2.1.0)
10. When **Leave** is set in **Schedule** in the **TIME ATTENDANCE** menu and the user who is the approver is deleted, the T&A reports are not searched. (Affects version: v2.7.0)
11. Some 1:N authentication succeeded events missing from Time & Attendance. (Affects version: v2.8.6)
12. An error occurs when adding a device in the TA setting after upgrading version from 2.8.8 or earlier to 2.8.9 or later. (Affects version: v2.8.9)

# Version 2.9.2 (Build No. 2.9.2.4)

---

Release: 2023-02-24

## New Features and Improvements

1. Improved security of login password vulnerabilities for brute-force attack.

## New Features and Improvements

1. Supports 3rd party OSDP reader connection.
2. Supports activating licenses for use of specific features on devices.
3. Improved **Face Detection Setting**
  - **Detection Distance, Wide Search** option support.
4. Improved security vulnerabilities
  - Updated jQuery to the latest version of help menu
  - Improved security vulnerabilities for administrator permissions
  - Improved HTTP vulnerability
  - Improved Injection vulnerability
  - Improved Authentication vulnerability
  - Improved minor vulnerabilities
5. Improved saved file name of CSV Export.
6. Improvement to use only the directory that has already been created when setting the storage path for the image log.
7. Improved SMTP setting security vulnerabilities.
8. Added case insensitivity guide for databases and tables in custom installation.
9. Improved Time & Attendance security vulnerabilities
  - Improved HTTP Content-Security-Policy, X-XSS-Protection, X-Content-type-options vulnerability
  - Improved TA Path Traversal vulnerability
10. Improved real-time event log performance.
11. Improved performance on adding users and user groups.
12. Improved performance on loading unacknowledged alarms.
13. Improved performance for high-volume environments with many users.
14. Improved encryption/decryption data processing performance.
15. Improved BioStar 2 logout speed.
16. Optimized memory settings for Maria DB when installing BioStar 2.
17. Improved pop-up message when checking image logs of the disconnected device.
18. Improved pop-up message when setting an elevator unlock schedule with a 1st generation device.
19. Improved photo deterioration due to noise when uploading photos for enrolling Visual Face.
20. Improved to check image data to be encoded when enrolling Visual Face using API.
21. Improved the SMTP information of **Trigger & Action** and **Email Setting** to be synchronized with each other.
22. Improved visitor search performance in an environment using MS SQL Server database.
23. Added new login page.
24. Minor string fixes.
25. Minor performance improvements.
26. Minor stabilization of server.



## Bug Fixes

1. When **Delete User** after checking the checkbox of all users in the specific user group, the mobile cards of users included in other user groups are also deleted. (Affects version: v2.7.12)
2. Certain library not installing on Windows Server 2012. (Affects version: v2.9.0)
3. If more than 1000 users are deleted using the API, the users do not get deleted properly. (Affects version: v2.8.0)
4. When using API to add a user and setting time in start\_datetime and expiry\_datetime, the exact time is not applied. (Affects version: v2.0.0)
5. Device's sound file cannot be deleted even with the proper permission. (Affects version: v2.8.14)
6. Icons for certain devices do not display properly. (Affects version: v2.3.0)
7. Device disconnects intermittently. (Affects version: v2.0.0)
8. If user group information is changed when there are many users, the change is not applied. (Affects version: v2.7.14)
9. When deleting an access group with a user group set among access groups using the same access level, the user included in the user group is also deleted from other access groups that are added alone. (Affects version: v2.8.14)
10. Some **Device Disconnection Detected** events not getting uploaded after server restart. (Affects version: v2.8.11)
11. FaceStation F2 device logs not getting uploaded to server intermittently. (Affects version: v2.8.6)
12. Intermittently going to the login page when connecting a device. (Affects version: v2.9.0)
13. In an environment using MS SQL Server database, even if the email address of user information is changed to an email address that is already in use, duplicates are not checked. (Affects version: v2.8.16)
14. Spanish footer not displayed when sending Visual Face Mobile Enrollment Link email. (Affects version: v2.8.16)
15. When issuing a CSN mobile card using **CSV Import**, if a slash (/) is used in the expiration date, the expiration date is not displayed correctly. (Affects version: v2.8.9)
16. Firmware upgrade notification for some older versions of devices does not appear when logging in to BioStar 2. (Affects version: v2.8.6)
17. When **Automatic User Synchronization** is set to **Specific Devices(Only devices belonging to the access group)**, user information updated by **CSV Import** is not synchronized to the device. (Affects version: v2.7.11)
18. When issuing a card using API, it is issued even if the maximum number of issues is exceeded. (Affects version: v2.0.0)
19. When **Use for BioStar 2 Login** is disabled in **Active Directory**, synchronizing active directory causes current logged-in IDs to be synchronized. (Affects version: v2.8.16)
20. The server freezes when exporting data for users enrolled with many visual faces. (Affects version: v2.8.10)
21. **CSV Import** fails even if the maximum number of input characters is not exceeded in the user information of the CSV file. (Affects version: v2.8.16)
22. In an environment using MS SQL Server database, if a Leave is registered using a specific language, the language texts are not displayed correctly when searching for T&A Report. (Affects version: v2.2.1)
23. Synchronization does not work correctly when moving repeat between many user groups in the **User** menu. (Affects version: v2.8.9)
24. If many **Time Codes** are created, unable to access the **TIME ATTENDANCE** menu. (Affects version: v2.2.1)
25. In an environment using MS SQL Server database, unable to access the **TIME ATTENDANCE** menu when applying a certificate with long contents. (Affects version: v2.2.1)
26. Users registered in the schedule were initialized while adding new users to the **Schedule**. (Affects version: v2.4.0)
27. Session ends when entering the **MONITORING** menu in specific languages. (Affects version: v2.9.1.25)

## New Features and Improvements

1. Supports BioStation 3
2. Supports user information partial update
  - Supporting device: BioStation 3 v1.0.0
3. Improved extraction of images used for visual face credentials
4. Simplified visual mobile face enrollment process
5. Supports visual face import
  - Enrolls visual face when file name of the image matches user ID
6. Supports visual face migration
7. Device added supporting Fingerprint LFD
  - Supporting device: BioLite N2 v1.5.0
8. Improved door open logs
9. Added logs to indicate full capacity on devices
10. Improved security vulnerabilities
  - Improved Unquoted Service Path vulnerability
  - Improved Clickjacking vulnerability
  - Improved minor vulnerabilities
11. CSV Improved error messages on CSV import fail

## Bug Fixes

1. QR/Barcode having the same card ID as a CSN or Wiegand card being authenticated while using 'Server matching' with X-Station 2 (Affects version: v2.8.11)
2. Operator having privilege to edit users couldn't edit user information due to not having email setting view privilege (Affects version: v2.8.14)
3. Event logs not getting stored in the database while 'Real-time Monitoring' displaying the logs (Affects version: v2.8.6)
4. Visitor's fingerprint enrollment failing from 'Visitor' menu (Affects version: v2.8.14)
5. BioStar 2 not running properly due to incorrect MSSQL table constraints (Affects version: v2.8.5)
6. Requiring phone number, a non-required field, when issuing mobile access card via CSV import (Affects version: v2.7.12)
7. Visual face not being synchronized to devices intermittently (Affects version: v2.8.12)
8. Sending users to devices that doesn't need synchronization when another device fails on synchronization when using 'All Devices' as the option of 'Automatic User Synchronization' menu (Affects version: v2.8.6)

9. Users not related to the action of 'Batch Edit' being synchronized to devices that belongs to the target of editing (Affects version: v2.8.14)
10. BioStar 2 abnormally occupying memory when manually locking and releasing a door (Affects version: v2.0.0)
11. Visual face enrollment page not showing any strings when the browser language is set to a language that the enrollment page does not support (Affects version: v2.8.5)
12. BioStar 2 showing success as result when uploading a user having a card ID that already exists within BioStar 2 (Affects version: v2.8.9)
13. Devices supporting 'Extended Auth Mode' intermittently not displaying auth modes correctly (Affects version: v2.8.6)
14. BioStar 2 not finding the correct port when checking licenses (Affects version: v2.7.11)
15. Unassigned 'Mobile Access Cards' being sorted in a descending order in BioStar 2 running with MariaDB (Affects version: v2.8.7)
16. Video logs being recorded shorter than the configured settings (Affects version: v2.5.0)
17. 'Mobile Access Card' issue page not following the 'Date Format' settings when its set as mm/dd/yyyy or dd/mm/yyyy (Affects version: v2.8.9)
18. Export displaying expiry date on 'Mobile Access Cards' that does not have any expiry date (Affects version: v2.8.9)
19. 'Enroll' and 'Search' buttons intermittently disappearing from 'Visitor' menu when enrolling a visitor (Affects version: v2.8.7)
20. Error message indicating the maximum number of face credentials displaying incorrect numbers (Affects version: v2.8.6)
21. BioStar 2 API Swagger not displaying Unicode characters for response (Affects version: v2.8.14)
22. 'Mobile Access Cards' only being issued for 100 cards when the CSV contains more than 100 (Affects version: v2.7.12)
23. Result of the 'Muster Status' on print and CSV having different time zones (Affects version: v2.8.6)
24. Wiegand card ID accepting only 32 characters when is should accept to 78 characters (Affects version: v2.7.12)
25. Authentication succeeding when the authentication failed to pass the global 'Anti-passback' check (Affects version: v2.8.11)
26. X-Station 2 firmware files not displaying correctly on the firmware upgrade page (Affects version: v2.8.12)
27. Image and video logs not being displayed when accessing 'Monitoring' menu without accessing 'Video' menu (Affects version: v2.7.0)
28. Event logs not displaying when a custom operator sets a filter from 'Event Log' menu having more than 1,000 user groups (Affects version: v2.8.3)
29. Video logs not being displayed when accessing BioStar 2 using a domain URL (Affects version: v2.6.0)
30. Card not being able to re-used as an arm/disarm card or assigning to a user when the card was registered as an arm/disarm card for an 'Intrusion Alarm Zone' and the zone itself gets deleted (Affects version: v2.5.0)

## New Features and Improvements

1. Improved Time & Attendance security vulnerabilities
  - Restricted unsupported cipher suites from server settings
  - Updated DB driver to the latest version
  - Updated jQuery to the latest version
  - Added security check while using Time & Attendance API through websocket
2. Supports deleting Time & Attendance punch logs after a certain period
3. Improved the API creating modified punch logs to have custom device names

## Bug Fixes

1. 'Floating shift' not being able to set 'Punch in granted time range' to start from 00:00 (Affects version: v2.7.2)
2. 'Floating shift' not being able to set the time segment from 00:00 to before the 'Day start time' (Affects version: v2.7.0)
3. Not able to access the Time & Attendance menu when changing the server protocol to HTTP from HTTPS (Affects version: v2.8.10)
4. Searching users in a specific language doesn't work in an environment using MS SQL Server database (Affects version: v2.2.1)
5. Work time not calculated correctly when using 'First check-in & Last check-out' and 'Meal deduction' configured as 'Fixed' at the same time (Affects version: v2.7.0)
6. 'T&A Required' option could not be changed to No from Yes when device's 'T&A Mode' is set as 'By User' from the Time & Attendance Setting menu (Affects version: v2.8.9)
7. Users get deleted intermittently from Time & Attendance menu when moving users to another user group and deleting the previous group itself (Affects version: v2.8.9)
8. Reports not being generated when operators logged in concurrently (Affects version: v2.2.1)
9. Custom fields get applied only after 2 attempts from the column settings of the reports' 'Filter Conditions' (Affects version: v2.7.9)
10. Filter conditions not showing the full result of user group search once the search result gets deleted and followed by another user group (Affects version: v2.2.1)
11. Deleted users from BioStar 2 still appears in the Time & Attendance menu (Affects version: v2.8.16)
12. When the Device Setting is changed after the T&A service is started, the "Login Required" Alert pop-up continuously occurs (Affects version: v2.8.9)

## New Features and Improvements

1. Added visual face to the dashboard.
2. Improved the user interface of Visual Face Mobile Enrollment page.
3. Added footer to email sending the visual face mobile enrollment link.
4. Deleted the option to use user ID as card ID from Enroll QR/Barcode page.
5. Improved sharpness by changing image size of the QR/barcode when issuing BioStar 2 QR.
6. Fixed constraint that Wiegand card ID cannot start with 0.
  - Allowed 0 to be entered in the first field.
  - Imposed restriction that all four data fields cannot consist only of zeros.
7. Added Error\_Description column to user list file (User\_Import\_Error) that failed CSV import.
8. Added logic to check that AC, TA, VE services do not use the same DB name during custom installation.
9. Changed the version of Chrome included when installing BioStar 2 to 75.
10. Improved USB Device Agent security vulnerabilities.
11. Improved video security vulnerabilities.
12. Updated to inquire the correct result value by checking the schema name, when the same table name exists in the TA and VE databases during database encryption/decryption
13. Added option to delete unassigned card
14. Added relay deactivation option for exit button input
  - Added the option to set the door open request log to occur but the relay not to operate when the exit button is pressed.
15. Separated the log related to the cause of the door unlock.
  - Door open request by exit button
  - Door open request by operator
16. Supports setting the byte order for smart cards.
  - Supports setting the byte order of data to be output to Wiegand or OSDP.
17. Added setting.config file initialization logic.
18. Improved so as not send to the portal when the user's phone number is out of the allowable range of the Airfob Portal when issuing a mobile access.
19. Added procedure to accept to collection and use of the privacy when using cloud.
20. Added 'All Devices' option to dual authentication setting to door.
21. Improved the occupancy limit zone monitoring page to adjust to the screen resolution of the monitoring device.
22. Allows connecting X-Station 2 as a slave device of CoreStation.
23. Added Hide Face Credential Preview Image option.
  - Supports hiding the face preview screen of users registered on the server for privacy protection.

24. Added the Use QR as card option.
  - Supports selecting whether to allow authentication when the QR data scanned by the device is the same as the card data issued to the user.
25. Support to log in to BioStar 2 with Active Directory account.
26. Amended to include user name in data when sending user data to devices without LCD screens.
  - Applied devices: CoreStation, BioEntry W2, BioEntry P2, XPass 2
27. Updated German and French resource files.

## Bug fixes

1. The screen displayed abnormally when entering the details page of the disconnected slave device (Affects version: v2.8.6).
2. Description of the photo value of POST/api/users was incorrectly written as binaryDatas (Affects version: v2.7.12).
3. Last authentication record of a user was not displayed when searching for long-term idle users for more than 6 months (Affects version: v2.5.0).
4. Although FaceStation 2 supports the option to select whether to use the screensaver from firmware version 1.5.0 or later, the option is displayed on the details page of devices with an earlier version (Affects version: v2.8.10).
5. Name of the operation level set in Georgian displayed as a question mark in the audit trail menu (Affects version: v2.7.6).
6. CSN card, smart card, and mobile card activation settings of BioEntry W2 (BEW2-OHP) device were not saved (Affects version: v2.7.6).
7. In an environment using MS SQL Server database, If the Output Module (OM-120), a slave device of CoreStation, was deleted, the device list was not queried (Affects version: v2.8.12).
8. Encryption migration failed in the decryption environment (Affects version: v2.8.0).
9. Visual Face data intermittently not syncing to other devices (Affects version: v2.8.6).
10. When a user is deleted from Manage Users in Device, other information in the synchronization table was also deleted and synchronization failed (Affects version: v2.4.0).
11. Users using custom user field were not updated during 'All Devices (including user update from device)' automatic user synchronization (Affects version: v2.8.0).
12. Target of the audit trail was output in the format of 'eventType.number' when alert setting changed (Affects version: v2.8.9).
13. Airfob Portal connection failed with unknown error message (Affects version: v2.7.12).
14. Access level could be assigned on a device with full access enabled (Affects version: v2.4.0).
15. If the relay was not set, user could not create a door, but the previously added door was saved without setting the relay (Affects version: v2.5.0).
16. The log recorded in the real-time log could not be queried in the event log (Affects version: v2.8.4).
17. Temperature measurement error pop-up messages showed only the user ID but not the name (Affects version: v2.8.11).
18. Daylight Saving Time (DST) setting not reflected in image log time (Affects version: v2.0.0).
19. VIDEO menu not accessible when using subdomain (Affects version: v2.6.0).
20. When synchronizing added users on the device, the user group was not counted (Affects version: v2.0).

21. Anti-passback violation alarm occurred even for normal authentication when a device configured as an anti-passback zone under the following conditions was duplicated as a muster zone.
  - Configure the entry device of the anti-passback zone as the exit device of the muster zone, and set the exit device of the anti-passback zone as the entry device of the muster zone.
22. When setting the home screen logo and slideshow of the device, image was not resized to match the resolution of the device screen, causing the screen to look distorted (Affects version: v2.6.0).
23. When using Personal Information DB Encryption, if user information was edited in Active Directory and then synchronized, the changes were not synchronized (Affects version: v2.8.0).
24. When setting alarms in muster zones and interlock zones, if the number of devices was large, the entire device list was displayed on the add alarm screen (Affects version: v2.6.0).
  - List changed to scroll format.
25. When the language is set to Japanese, if the event log was exported as a CSV file, the text in the file was output in English (Affects version: v2.8.9).
26. If the administrator clicked 'OK' when the device was disconnected while entering the device detail page, an irrelevant error message was displayed (Affects version: v2.7.10).
  - Amended to display message stating that the device is not connected.
27. Error message not displayed when adding doors that exceeds the number supported by the license (Affects version: v2.8.3).
28. When updating user information using the API, an 'E-mail already exists' message was returned if the same email was maintained (Affects version: v2.0.1).
29. 'Visual Face Extraction Failed' event not searchable through the event log filter (Affects version: v2.8.10).
30. Symbols could be entered through API even though it does not support the use of symbols when entering department and title in user information (Affects version: v2.8.9).
31. Synchronization proceeded even when OK clicked without changing settings on the user's detail page after importing CSV when custom user fields existed (Affects version: v2.8.12).
32. Certain symbols (-) could not be entered in the name of a user who issued the QR/Barcode (Affects version: v2.8.11).
33. Unnecessary date was displayed on Visual Face Mobile Enrollment page (Affects version: v2.8.11).
34. Last sync time and last update time not displayed even when syncing from Active Directory (Affects version: v2.7.11).
35. Error message displayed when the 'Connect' button on the mobile access setting screen was clicked while the mobile access is set (Affects version: v2.8.14).
36. Fingerprint scan request runs twice when enrolling a fingerprint with the USB enrollment device (BioMini) in an environment using the latest version of Chrome (Chrome 98) (Affects version: v2.0.0).
37. T&A related settings were displayed on the details page of devices that do not support T&A (Affects version: v2.8.14).
38. Failure to function properly when exporting some T&A reports more than two pages PDF (Affects version: v2.8.14).

## New Features and Improvements

1. Applied Log4j 2 v2.17.1.
2. Improved Automatic User Synchronization performance.
  - Improved the synchronization speed when adding or modifying doors while using 'Specific Devices' Automatic User Synchronization.
  - Improved 'Delete Data & Sync Device' performance when using 'Specific Devices' Automatic User Synchronization.  
: Fixed the problem that the synchronization performance deteriorated by retrieving all user data from all connected devices when 'Delete Data & Sync Device' was performed.
3. Adjusted the number of threads for Thrift communication between C server and Java server.
  - Improved API request processing performance by reducing the number of threads used in 'Specific Devices' Automatic User Synchronization.
  - Improved to change to 10 if it was less than the minimum value (10) by checking the number of BioStar 2 Thrift threads when running the server.

## Bug fixes

1. DB Lock occurred when user data changes frequently, such as adding, deleting, or editing, were made in a short period of time during Automatic User Synchronization (Affects version: v2.7.14).
2. In the MS SQL Server database environment, BioStar 2 did not operate normally if more than 526 user groups or users were set in the access group when using 'Specific Devices' Automatic User Synchronization (Affects version: v2.8.14).
3. The data of the already deleted devices were logged in the user synchronization fail table when using 'Specific Devices' Automatic User Synchronization (Affects version: v2.7.11).



## New Features and Improvements

1. Supports a new device.
  - Input Module (IM-120)
2. Face 1:N security level setting support for CoreStation.
3. Applied OpenJDK.
  - \* As of BioStar 2 version 2.8.14, OpenJDK is applied to allow users to use BioStar 2 regardless of the Java version installed on the PC.
4. Added Department, Title, and Telephone to User Column Settings.
5. Improved to be able to enter and modify PIN when using user CSV import.
6. Improved performance by no longer inquiring unnecessary user information when calling API.
7. Improved device search speed using API.
8. Improved Automatic User Synchronization performance.
  - Added missing indexes to database columns used for synchronization.
  - Improved 'All Devices' Automatic User Synchronization speed and fixed synchronization errors.
  - Improved 'Specific Devices' Automatic User Synchronization speed.
  - Improved to send changes in bulk when using 'Specific Devices' Automatic User Synchronization.
  - Added exception handling for null value when retrying after 'Specific Devices' Automatic User Synchronization failed.
9. Improved security vulnerabilities.
  - Applied Log4j 2 v2.16.0.
  - Applied OpenSSL 1.1.1k.
  - Applied jQuery 3.4.1.
  - Improved to check Operator Level and Custom Account Level when using API.
  - Fixed an issue where if the CSV export file contains a formula symbol (=), the formula is applied when the file is executed.
  - Improved to perform CORS check and security check for session ID when connecting to web socket.
  - Prevention for SQL Injection attack.
  - Improved to display error messages (error name, http error code, description) when a server status response error occurs.
10. Updated APIs in Swagger.
  - Updated the description of device Trigger and Action API
  - Added Visual Face Image Upload API.
  - Fixed an issue where users were not added to the actual device differently from the result returned when adding users to devices using [POST] /devices/{id} /users or [POST] /api/users/export.

11. Improved event log processing performance.
  - Improved event log inquiry speed in MS SQL Server database environment.
  - Improved database processing speed when generating device event logs.
  - Fixed to update only devices with changes in the database when synchronizing device log data.
12. Improved the loading speed of the device menu when restarting the BioStar 2 server with multiple devices connected.
13. Improved device connection speed.
14. Improved performance dealing devices by increasing the default number of device threads.
15. Improved loading speed of the monitoring menu by deleting unnecessary check logic.
16. Improved access group link speed by deleting unnecessary codes.
17. Improved blacklist card synchronization speed.
18. Improved database data processing speed.
19. Improved server performance.
  - Improved to maintain the existing connection without reallocating the client port every time when communicating between the C server and the Java server.
  - Improved to prevent unnecessary function calls according to log level in C server.
  - Improved to reuse objects for encrypt personal data in Java server instead of reallocating them every time.
20. Improved the speed of querying registerable devices using API.
21. 26 bit Wiegand card support for BioStar 1.x to BioStar 2.x Migration Tool.
22. Improved to check the database connection status before proceeding with the BioStar 2 installation.
  - Removed 'Check the database connection' option from the custom installation process.
23. Improved to be able to run Swagger documents locally without a server address.
24. Changed the default value of Held Open.
  - Before: 3 seconds
  - After: 10 seconds
25. Changed the device icon of OM-120.

## Bug fixes

1. Even though the screen saver function is supported, the function was not displayed on the Settings of the X-Station 2 fingerprint model (XS2-ODPB, XS2-OAPB) (Affects version: v2.8.12)
2. When using the 'Specific Devices' Automatic User Synchronization option, it did not sync if the user ID contains some symbols (\_) (Affects version: v2.7.11).
3. When using the 'Specific Devices' Automatic User Synchronization option, the synchronization logic operated as 'All Devices' when executing Write Smart Card (Affects version: v2.7.11).
4. Chrome autocomplete function was mapped incorrectly in the information input field on the Add User screen (Affects version: v2.7.8).
5. some languages were displayed as question marks in Audit Trail when using MS SQL Server database (Affects version: v2.7.0).
6. When using the Visual Face as a user profile image, it exceeded the allowed size of the profile image and did not sync to devices (Affects version: v2.8.6).

7. Fake Detection was set to 'Normal' instead of the default value (Secure) when resetting after disabling Fusion Matching Mode on FaceStation F2 (Affects version: v2.6.0).
8. When setting the logo image as the home screen for FaceStation F2, the image was not applied in the correct resolution for the device (Affects version: v2.8.6).
9. It was not possible to enter uppercase letters in the server address when using 'Device → Server Connection' (Affects version: v2.7.0).
10. Custom user field data was not reflected in the T&A report (Affects version: v2.8.3).
11. Fixed an issue where key values were exposed when fetching smart card layouts using API. (Affects version: v2.0)
12. The server crashed intermittently.
  - C server crash occurred when database inquiry failed while creating user group cache (Affects version: v2.0).
  - Lock handling was missing in serviceTask JsonResult (Affects version: v2.0).
13. Even after deletion, devices previously used for credential enrollment continued to display in the credential enroll device list (Affects version: v2.0).
14. When BioStar 2 was newly installed and then launched, the migration screen was executed instead of the login screen (Affects version: v2.4.0).
15. When running 'Manage Users in Device' by selecting a device that supports only cards, the status of the user with the enrolled fingerprint was displayed as 'Different' (Affects version: v2.0).
16. When entering an email subject in a language with Unicode applied in the email settings, the text of the email subject was sent in a garbled state depending on the set SMTP server. (Affects version: v2.0)
17. When restoring a backed-up log table, if the log table index and the current log table were different and could not be matched, the table creation failed (Affects version: v2.7.11).
18. When generating more than 10 events by selecting 'Input (Event Name Change)' in the Trigger & Action settings of CoreStation, it did not work properly. (Affects version: v2.8.8)
19. If there is a language not supported by BioStar 2 in the local storage language of the browser, it was not possible to enter the BioStar 2 login page (Affects version: v2.0).
20. When creating a user group, an error code occurred on the browser and the user group was not created (Affects version: v2.7.14).
21. When using server matching with FaceStation 2's authentication mode set to Card+Face, the face authentication mode did not work after card authentication (Affects version: v2.8.6).
  - \* This modification will be applied to devices with firmware version 1.5.1 or later installed.
22. During 'All Devices' Automatic User Synchronization, the access group and door synchronization results were not updated intermittently (Affects version: v2.0).
23. Devices were disconnected when the amount of data was large during Automatic User Synchronization (Affects version: v2.0).
24. When adding a user using API, it was possible to create a user ID with a value not supported by BioStar 2 (Affects version: v2.8.1).
25. When adding events by selecting 'Input (Event Name Change)' in the device's Trigger & Action settings, the 'Add Event Name' button was cut off if there were many registered events (Affects version: v2.0).
26. When importing users with CSV import, 'Upload successful' message was displayed even if there was information that was not updated (Affects version: v2.3.0).
27. When a device that does not support the intelligent slave sent OSDP ID as an invalid value, BioStar 2 initialized the value to 0, updating RS-485 settings and disconnecting the existing RS-485 connection (Affects version: v2.8.10).
28. Even though the server matching is supported, the function was not displayed on the settings of BioStation 2 (Affects version: v2.2.2).
29. When a user has abnormal profile image, the user sync process was not finished properly (Affects version: v2.8.0).

## New Features and Improvements

1. Created the T&A report inquiry API.
2. Supports private SSL certificates with a specific passphrase on the T&A server.
3. Changed the TLS default version of the T&A server to 1.2.
4. Updated T&A APIs in Swagger.
5. Improved T&A report inquiry performance.
  - Improved T&A report management structure: Improved to archive the punch log table data by month to prevent the system from slowing down caused by accumulated logs.

## Bug fixes

1. When returning to the individual summary report and edit history report list after checking details of a selected report, the item selection did not work properly in the list. (Affects version: v2.7.10)
2. Punch out rounding setting was not applied to the individual summary report. (Affects version: v2.8.5)
3. T&A synchronization was abnormally interrupted when BioStar 2 was upgraded to v2.8.9 or later under the following conditions. (Affects version: v2.8.9)
  - BioStar 2 v2.8.5 or later
  - Use MS SQL Server database
  - Connect the Wiegand Reader 1 to DM-20
4. When using MS SQL Server database, T&A synchronization was abnormally interrupted if a large number of user data was deleted. (Affects version: v2.8.9)
5. When deleting a user or user group, T&A synchronization was abnormally interrupted because the related data was not completely deleted. (Affects version: v2.8.9)
6. Wiegand devices connected to the DM-20 were not displayed on the Time & Attendance device list. (Affects version: v2.8.9)

## New Features and Improvements

1. Supports a new device.
  - X-Station 2 Fingerprint model (XS2-ODPB, XS2-OAPB)

## Bug fixes

1. The logo image was not displayed in the email when issuing the visual face enrollment link after setting a company logo in the Visual Face Mobile Enrollment under EMAIL SETTING. (Affects version: v2.8.11)
2. An error message was not displayed when a user tried to upload a company logo image which exceeded a maximum capacity of 5 MB. (Affects version: v2.8.11)
3. The QR Use value was not updated in the database when connecting X-Station 2 to BioStar 2 for the first time. (Affects version: v2.8.11)

## New Features and Improvements

1. Supports Occupancy Limit Zone.
  - Occupancy Limit Zone: This feature enables an administrator to manage and control the population density of a place to prevent overcrowding and monitor the zone status.
2. Supports a new device.
  - X-Station 2
3. Renamed the lighting brightness control feature and added the 'Not Use' option to FaceStation F2.
  - Changed the option name from 'Ambient Brightness' to 'Light Brightness'.
  - Improved turning off the light of the device by adding the 'Not Use' option.
  - Removed the 'Auto' option.
4. Separated email settings of both Visual Face Mobile Enrollment and QR.
5. Updated APIs in Swagger.
  - Created a new API related to Occupancy Limit Zone.
  - Updated the existing APIs related to Visual Face, CSV export and import, thermal camera settings, and temperature log.
  - Created a new API related to QR/barcode for X-Station 2.
6. Updated the Japanese resource file.

## Bug fixes

1. A 'TypeError: Cannot read property 'replace' of undefined' error occurred in the browser console when issuing a CSN card to users. (Affects version: v2.8.9)
2. Fingerprint authentication failed on the device where the data was transferred from BioStar 2 via Data File Export. (Affects version: v2.8.10)
3. When performing Import Event Logs from the device with a compatible version of firmware installed, a compatibility error occurred and it was not able to import data. (Affects version: v2.8.10)
4. It was not able to log in with users registered in the BioStar 2 version 2.6.4 when upgrading the version to 2.8.9 or later. (Affects version: v2.8.9)

## Main Fixes

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)
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)
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)
4. The Celsius/Fahrenheit mark was incorrectly displayed in the Trigger & Action alert email. (Affects version: v2.8.8)
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)
6. Registering a Visual Face was not correctly done due to image rotation when using Chrome version 86. (Affects version v2.8.6)
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)
8. Visual Face CSV import failed when using the Wiegand format or a Custom User Field. (Affects version: v2.8.8)
9. Email transmission did not function properly when SMTP Security Type was 'None' or 'TLS' in email settings. (Affects version: v2.8.6)
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)
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)
12. Face Detect Settings was initialized after changing face settings from the FaceStation F2's configuration page. (Affects version: v2.8.9)
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)
14. The event list was not displayed in event log data exported to PDF. (Affects version: v2.8.9)
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)
16. If clicking Apply in the SERVER menu after setting the mobile access card option to 'Use', the setting was changed to 'Not Use'.
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)

## New Features and Improvements

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. 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
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.
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
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.
6. Screensaver support for FaceStation 2 and FaceStation F2.
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.
8. Improved to recover only the file having an error when a conf file error occurs.
9. Updated the German resource file.



## Bug fixes

1. Time between device and server was displayed differently when receiving email from BioStar 2. (Affects version: v2.6.0)
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. Logs were not displayed in real-time intermittently. (Affects version: v2.0.0)
4. The real-time log was updated with delay or was missing when disconnected web socket session information remained. (Affects version: v2.0.0).
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)
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)
7. The BioStar server occupied too much memory in certain cases. (Affects version: v2.7.14)
8. Punch log table data synchronization did not work properly when using MS SQL Server database. (Affects version: v2.8.9)

## Main Fixes

1. Extended auth mode gets disabled intermittently when multiple FaceStation F2 devices try to connect to the server simultaneously. (Affects version: v2.8.8)
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)
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.
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)
5. PIN authentication failed due to the device default hash key transmission error. (Affects version: v2.4.0)
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)
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)
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.
9. If clicking Apply in the SERVER menu after setting the mobile access card option to 'Use', the setting was changed to 'Not Use'.
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)

## New Features and Improvements

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. Provides a guide on the screen when registering Visual Face on the mobile device.
3. Renamed 'Email Setting' menu.
  - Before: Email Contents
  - After: Email Setting
4. Renamed some events related to scheduled unlock zones.
5. Updated some language resource files.
6. Changed the names of db-converter log files.
7. Changed to possible to edit the device's T&A settings only while the device is connected.

## Bug fixes

1. An error occurred when creating work history after running user sync with personal information DB turned on or off. (Affects version: v.2.8.0)
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: v.2.8.0)
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.
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)
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)
6. When issuing mobile cards, model names of some devices were not correctly displayed in the pop-up message. (Affects version: v2.6.0)
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)

## Main Fixes

1. Event logs from slave devices could not be viewed after applying an event filter.
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.
3. Even though Mobile Access had not been set to be used, Mobile Access was able to be registered using CSV Import.
4. When the server restarted, Automatic User Synchronization settings were changed to the default values.
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.
6. When migration was conducted using the BioStar 1.x to BioStar 2.x Migration Tool, the cards of some users were missing.
7. When using the Automatic User Synchronization option in 'Specific Devices', the user data was deleted due to synchronization errors.
8. When using the Automatic User Synchronization option in 'Specific Devices', data of users who registered visual faces were not synchronized.
9. Language resource was not applied successfully to the device. (FSF2-ODB)

## New Features and Improvements

1. Supports batch registration of Visual Face using CSV import.
2. Stabilization of the thermal camera function
  - The temperature indicator was added to notification emails.
  - A thermal inspection report has been added for monitoring.
3. When using the Automatic User Synchronization option in 'Specific Devices,' the server will limit the retry attempt to three times for failed transfers.
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.

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.
6. Changed db-converter to run in the background when installing BioStar 2.
7. Improved to check whether the encryption key matches when logging and show an error message if there is a mismatch.
8. Improved the logic confirming database connection upon installing BioStar 2.
9. Support of user synchronization exceptions in the Active Directory.
10. Changed to not display login permission in the logs.
11. Changed temperature column not to be a default column for event logs and real-time logs.
12. Visual Face Mobile Enrollment email content had been improved.

## Bug fixes

1. Card settings were set to 'Disabled' after changing the card settings in the CoreStation device detail page.
2. Modified DB queries to ensure correct use of case-sensitive table names when using MariaDB in a Linux environment.
3. It took a long time by referring a wrong address when entering MONITORING menu through the BioStar 2 cloud.
4. When the System.conf file was corrupted, the enckey file was also corrupted.
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.
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.
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.
8. Problem where the Extended Auth Mode was deleted from BioStar 2, including the database.
9. When running Send Visual Face Mobile Enrollment Link with the cloud disabled, the error message text was not appearing correctly.
10. Visual Face image aspect ratio had been corrected.
11. An abnormal delay when scanning fingerprints for visitors.
12. Errors in the TIME ATTENDANCE menu
  - Punch Log History was not able to be modified.
  - The infinite loading occurred when updating Individual Report.
13. When more than 20 devices were registered to use Mobile Access, up to 20 devices were only displayed in the device list.

## New Features and Improvements

1. Supports server matching for face authentication devices.
  - FaceStation 2
2. Supports thermal camera on face authentication devices.
  - FaceStation 2
  - FaceStation F2
3. Adds the new credential.
  - Supports Visual Face and visual face mobile enrollment.
4. Supports the new devices.
  - FaceStation F2
  - BioEntry W2 (Rev 2)
5. Logs related to Thermal Camera were added to Trigger & Action in the device settings menu.

## Bug fixes

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. XPass D2 connected as a slave device of CoreStation was not displayed in the TIME ATTENDANCE device list.

## Main Fixes

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

## New Features and Improvements

1. Supports Wiegand devices as a time and attendance management device.
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.
3. Improvement to allow users with general user permissions to update own TA reports.

## Bug fixes

1. Items not supported in the column settings of daily reports were displayed.
2. Upon running a CSV export in the updated individual reports by selecting the 'All Punches' option, the blank was displayed as null.
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.
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.
5. If the exception column of the updated individual reports with the 'All Punches' option was an empty value, the value was displayed as '-'.
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.
7. The individual report was not displayed according to the set list display count.
8. If the login ID was the same, the time card was displayed even if the session ID was different.
9. The time cards created in the past with the same session ID were accumulated.

## Main Fixes

1. Allowed the unassigned card on the server to be registered by card reader or enter manually.
2. Data files using unsupported time formats failed to be imported.
3. Active Directory failed to synchronize when using Personal Information DB Encryption.
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.
5. Partially missing event logs in the database when the server was overloaded.

## New Features and Improvements

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. Improvement of backup and recovery logic for Web-App, CGI server system.conf.
3. Exclusion of TLS V1.1 for improved security
4. Improvement of redirection to the Suprema technical support page link ([support.supremainc.com](https://support.supremainc.com)) when REST API request fails.
5. Improved Thrift communication logic log.
6. Improved security vulnerabilities on Redis.
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`.



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.
9. Changed queries to retry for lock error occurring when multiple queries are executed at the same time.
10. Added step of checking the root password upon upgrading BioStar 2.

## Bug fixes

1. A description of Base64 data has been added to the POST:/api/users fingerprint template in the BioStar 2 API document.
2. Triggers and actions were not applied as set.
3. When the log upload is set as automatic it was not outputted as a log.
4. When the port was changed upon installing BioStar 2, the change did not automatically reflect in the server\_url.conf file.
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.
6. If system.conf and setting.conf files were deleted, the TA server could not be started.
7. Incorrect error codes were displayed in the graphic map.
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.
9. The Windows authentication connection failed when the database name, database user, and database password of the video were not entered in BioStar Settings.
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.
11. The INVALID\_JSON\_FORMAT error message appeared when clicking <Set Time> if the time setting on the Device details page wasn't changed.
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.
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.
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.
15. Upon user synchronization in Active Directory, the number of users was not updated.

## 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.

## 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.

# Version 2.8.2 (Build No. 2.8.2.3)

---

Release: 2020-07-10

## New Features and Improvements

1. Fixed local file inclusion (LFI) vulnerability.
  - The vulnerability that could allow an attacker to gain local access via a web browser.

## Main Fixes

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.
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.
3. Some TA reports are only displayed in portrait format from print preview screen when exporting to PDF.
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.
5. When importing a CSV file without the mobile credential column, the result pop-up message does not show.
6. When migrating from BioStar 1.x to BioStar 2.x, the existing users and user groups of BioStar 2 are not deleted.
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.
8. The individual report does not work as the column setting of the saved filter.
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.
10. Fixed to not access cache memory simultaneously.
11. When using personal information DB encryption, card authentication fails if an administrator sets to use server matching.
12. Users are not synchronized to the TIME ATTENDANCE menu intermittently.
13. BioStar 2 cannot be upgraded when installed using MS SQL Windows authentication.

## New Features and Improvements

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

## Bug Fixes

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.
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. 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.
4. If the path related to ngrok in setting.conf is different from the actual ngrok installation path, the cloud will not work properly.
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.
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.
7. When connecting as a visitor operator, the custom visitor field does not appear on the visitor settings page.
8. The set number of days is counted incorrectly when setting the leave on the Schedule of the TIME ATTENDANCE menu.
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.
10. Fixed the individual report column settings to be displayed differently depending on the 'In/Out Punches' or 'All Punches' options.
11. PDF export of the individual reports does not work properly.
  - The date is not displayed on the first page.
  - Unnecessary pages are shown.
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.
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.
14. The leave column in daily or individual reports does not appear in a clickable form.
15. Administrators other than the first administrator cannot activate the cloud.
16. Delete unnecessary device security communication codes in server settings.
17. CSN is not added when adding a user by importing CSV in version 2.7.14.
18. Two or more schedules were able to be set in the same period for the same user.
19. When exporting the individual report to PDF with "All Punches" option selected, the title information of each date is not displayed.

## Main Fixes

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

## New Features and Improvements

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

## Bug Fixes

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.

## Main Fixes

1. Slow loading of BioStar 2 when there are a large number of created user groups.
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.
3. When the license for TA is activated offline, offline activation for other licenses cannot be performed without refreshing or reentering the server menu.
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.
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.
6. User menu cannot be accessed properly by other clients at the same time when a user's face is being registered.
7. If User ID Type is set as alphanumeric, authentication succeeds even with AoC (Access on Card) registered on a blacklist.
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.
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.
10. Printing of a user list doesn't work properly when there are a large number of registered users.
11. Event logs not transferred to the server when the device gets disconnected from the server and then reconnected following by a certain condition.
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.
13. When upgrading the version of BioStar 2, db-converter error log occurs.
14. Punch log manually entered by the administrator does not appear in the individual report correctly when updated with the 'All Punches' option selected.
15. When there are a large number of registered users, the print preview screen of the user list shows only some users.

## New Features and Improvements

1. Support for connecting new devices.
  - XPass D2 (Rev 2)
2. Enhancement in Mobile Credential usage.
  - Added feature to send mobile credential certificates directly to connected devices on the BioStar 2.
3. Supports MS SQL Server 2017.
4. Supports Windows Authentication for MS SQL database server connections.
5. Added option to receive results sorted as desired when retrieving event logs using api/events/search from the BioStar 2 local API.
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.
7. Added Floor Control API to BioStar 2 API Documents.
8. Allowed additional symbols (-, \_) in the user's email account field.

## Bug Fixes

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.
2. A bug where signal setting changes in <Trigger & Action> of a device does not get applied properly.
3. A bug when using the USB fingerprint scanner, the fingerprints cannot be registered in ISO, ANSI378 template formats.
4. Removed unnecessary UI from the setting pages of BioEntry R2 and XPass D2.
5. A bug where the text of each item displays in overlap on the image log screen when the language is set as Russian.
6. A problem where the CSV user import list not being displayed properly.
  - Some characters in user IDs are missing.
  - Some users are missing.
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.
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'.
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.



## Main Fixes

1. A problem where BioStar 2 server does not start correctly when a certain Windows OS event does not exist.
2. Improved Muster Zone to not fall into a deadlock while processing event logs.
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.
4. Improved performance when having a great deal of user groups.
5. An issue where access through BioStar 2 Cloud doesn't work due to an abnormal behavior of ngrok.
6. An issue where access through BioStar 2 Cloud doesn't work due to an automatic update on ngrok.
7. Fixed TA module to update reports related to break time properly.
8. Fixed the 'Specific Devices' Automatic User Synchronization option to work accurately when users are created using CSV import.

## New Features and Improvements

1. Added the new Suprema Mobile Credential.
2. Stabilized 'Specific Devices' Automatic User Synchronization option.
3. Improved TA module to allow generating reports simultaneously on multiple clients.
4. Applied code signing on BioStar2 installer including executables and library files.
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

## Bug Fixes

1. An issue where Chinese characters were not displayed correctly on the exported PDF TA report.
2. A bug in an environment using MS SQL Server database where the results are not correct when searched in languages using Unicode.
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.
4. A bug where 'Image Log' did not work correctly with 'Access Denied(Anti-tailgating)' event.
5. An issue where a custom level administrator with permission only on a specific user group could view all user's real-time logs.
6. A bug where 'Time Code' does not appear from the <Rule> menu on TA module when the language is set as Japanese.
7. A bug where the action of 'Trigger & Action' configuration from device disappears after saving the settings.
8. An issue where an error occurs when updating the TA report that has data exceeding the maximum length of the 'Exception' column.
9. Fixed an error message that shows inaccurate status.
  - Incorrect password popup displays when the BioStar 2 server cannot connect to the database.

## Main Fixes

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

## New Features and Improvements

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. Added 'Specific Devices(Only devices belonging to the access group)' option to <Automatic User Synchronization>.
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.
4. Applied the latest BioMini Plus SDK library to the USB Device Agent.
5. Supports the alert sound for 'Input(Event Name Change)' in the <Trigger & Action> of the device.
6. Supports the sorting of lists for the User Group column of the <Muster Status> page on the MONITORING menu.
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
8. Changes the Java version.
  - Before: 1.8.0\_221
  - After: 1.8.0\_231

## Bug Fixes

1. When using the CoreStation as multiple elevator controllers, the logic for checking the maximum number of connections (32) does not work.
2. When stopping the BioStar 2 server, related processes such as Java.exe and node.exe do not terminate.
3. The Cloud Use setting is changed to 'Not Use' when upgrading the version of BioStar 2.
4. Emails aren't sent even though automatic emails for overtime have been set up.
5. The 'ACB\_ERROR\_CODE.150' error occurs because the current time value was not entered normally when setting the elevator.
6. The image file storage path changes to a wrong path when the image log delete option is enabled.
7. The timeout event in the muster zone does not function properly.
8. The button to go to the last page on the Audit Trail page does not function properly.
9. The added device list does not display properly on the screen.
10. Modified to install the BioStar 2 properly even if some setting is missing in Setting.conf file when upgrading the version.
11. The values entered in custom user fields are not reflected in the T&A report.
12. Stabilization of Time Attendance
  - Users are not synchronized to the TIME ATTENDANCE menu.
  - The TIME ATTENDANCE menu is not loaded properly.
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

## Main Fixes

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).
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.
3. Temporary Schedules is created on a date that does not have a shift applied.
4. Users without the permission for Monitoring can view real-time logs of devices through a web socket.
5. When adding a door, the setting of door sensor is applied differently than the settings.
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.
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.
8. Authentication fails if a user authenticates with AoC (Access on Card) issued as the mobile card.
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.
10. When a user without administrator permissions logs in through the cloud, the user cannot log in normally because of the permission check.
11. An error occurs when a user requests the offline key for Time Attendance license.

## New Features and Improvements

1. Support for connecting new devices.
  - FaceLite
  - XPass 2 (XP2-MDPB, XP2-GDPB, XP2-GKDPB)
2. Support to the USB fingerprint scanner in VISITOR menu.
  - Supported devices: BioMini, BioMini Plus, BioMini Plus 2
3. Added the BioStar 2 Swagger.
4. Improved to control access when a user without administrator permissions attempts to access menus that the user does not have access to.
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.

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
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.
8. Modified to allow the user to edit 'User ID' in <User Field Mapping> of Active Directory.
9. Update the resource files of Japanese, Arabic, and Spanish.
10. Support to allow the custom user field that added in the <SERVER> of Settings to be used in the T&A report.
11. Supports the sorting for entire data in the T&A report.
12. Added option to select 'First in & Last Out' or 'All Punches' to search conditions of the individual report.
13. Changes the Java version.
  - Before: 1.8.0\_212
  - After: 1.8.0\_221

## Bug Fixes

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.
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. The fingerprint search function does not work properly for application to visit the Terms and Conditions.
4. In the TIME ATTENDANCE menu, only 1,000 schedules are visible.
  - Modified to display up to 20,000 items.
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.
6. User cannot access TIME ATTENDANCE menu when connecting to BioStar 2 with a domain name.
7. When upgrading the version, the upgraded version is not applied in the system config item of AC, TA and Video database.
8. Restricted special characters can be input in usernames.
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.
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).
11. Modified to allow addition of up to 32 events when setting up the image log.
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.

13. In version 2.7.7 of BioStar, local APIs could be registered and used even though access control license was not activated.
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.
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.
16. Some user groups are missing during the migration in BioStar 1.x to BioStar 2.x Migration Tool.
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.

## Main Fixes

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

## New Features and Improvements

1. Enables users to search for visitors using fingerprints in the visit application page and VISITOR menu.
2. Supports user group synchronization in Active Directory.
3. Supports multiple use function of controllers.
  - Supported Devices: CoreStation
  - Detail: Supports configuring the CoreStation as a controller for up to 32 elevators
4. Supports Anti-Tailgating.
5. Supports setting options for Wiegand authentication result output.
  - User ID and Card ID
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.
7. Supports the fingerprint/face duplicate check when registering users on a device.

## Bug Fixes

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.
2. Deleted unused events in image log settings.
3. The user information is not output in <Manage Users in Device>.
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.
5. Modified to check session expiration on some API calls.
6. The last sync time, as well as the connection test success or failure times, are output on <Synchronization> in Active Directory settings.
7. The sync time in the Active Directory settings is not updated in real time.
8. Errors occur when setting the period entry for user or visitor registration if the date format is set to 'dd/mm/yyyy'.



## Main Fixes

1. Even if changing the Smart Card Layout option to 'None', that setting is not applied.
2. When restarting MS SQL Server, the database is not connected normally.
3. 'Soft anti-passback violation detected' and 'Hard anti-passback violation detected' options are missed from the event item of IMAGE LOG.
4. Some devices(BS2-OIPW, BSA2-OIPW) support the RFID cards that are different from the correct options.
5. If Custom User Field is configured, the custom field name is displayed but data is not output when printing the user list.
6. When the Administrator option is set in the device setting, that setting is not reset even if the device is reset.
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.
8. The custom level administrator created in BioStar 2.3.0 or earlier will not be output in versions 2.6.3 or later.
9. When changing the settings of the smart card layout, only the layout of the card type with the changes is synchronized.
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.
11. Some logs are not imported when importing the event logs manually or automatically.

## New Features and Improvements

1. Add the visitor management.
2. The license policy of Time & Attendance is changed.
3. Improved that a user can access the Time Attendance menu using a private domain address.
4. Improved to allow users with login IDs to proceed first when users are synchronized to the Time Attendance menu.
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.
6. Changes the Java version.
  - Before: 1.8.0\_201
  - After: 1.8.0\_212

## Bug Fixes

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.
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. When the language is set to Spanish(Spain), the schedule calendar of the Time Attendance menu is displayed Chinese characters.

## Main Fixes

1. If an administrator set the language to Spanish(Spain), exporting the T&A report in PDF does not work properly.
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.
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.
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>.
5. Deactivate 'Check the database connection' and 'Generate the database tables' options in the Custom installation window when upgrading the BioStar 2 version.

## New Features and Improvements

1. Support to the Clear APB for each user.
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.
3. Add the event items to IMAGE LOG menu.
4. Add the encryption option to Active Directory.
5. Improve that the administrator can change the port 9000 in FastCGI of Port menu.
6. Improve that the time of events is displayed as the time zone, device time, and server time on the alarm email.

## Bug Fixes

1. Fixed a security vulnerability by deactivating the 3DES encryption option.
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. The 'Input detect' event that occurred in the interlock zone is displayed as '-1' in Real-time log.
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.

## New Features and Improvements

1. Add the Active Directory menu.
  - Supports the use of Windows Active Directory user data in BioStar 2.
2. Supports the sorting of lists in the USER, DEVICE, and DOOR menus.
  - USER: Group, Status column
  - DEVICE: RS-485 column
  - DOOR: Group column
3. Removes the unsupported AoC events from the DEVICE, VIDEO and the Trigger & Action of Settings.
4. Supports that the administrator can change the port 9000 in setting.conf.
5. Added an Ambient Brightness option to the FaceStation 2 slave device.

## Bug Fixes

1. The iCLASS Seos and DESFire Advanced card formats are not applied when the administrator sets up the smart card layout.
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.
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.
4. Even if an administrator adds more than 249 custom levels, only 249 are displayed on the screen.

## Main Fixes

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.
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.
3. The door information of access level setting is displayed differently from the setting.
4. When operating the Delete From Device in the USER menu, devices belonging to the group cannot be selected.

## New Features and Improvements

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. Support for Quick Enrollment for FaceStation 2.
  - FaceStation 2 FW V1.2.2 or later
3. Support to Spanish and Arabic.
4. Support to the unlimited number of Custom Levels.
5. Changes the Java version.
  - Before: 1.8.0\_191
  - After: 1.8.0\_201

## Bug Fixes

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

## Main Fixes

1. Arabic does not display properly if an administrator exports the T&A report in PDF.
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.
3. If upgrading to version 2.7.0 or later, the administrator cannot add a leave in a previously set schedule.
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.

## New Features and Improvements

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. 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.
3. Improved that the device will be normally connected when you reconnect the device even when it is configured as a port forwarding.

## Bug Fixes

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.
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. The T&A function does not work properly if you upgrade from version 2.7.0 or earlier to 2.7.2.

## Main Fixes

1. If more than 16 cameras are added to the server, the camera screen is not output.
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.

## New Features and Improvements

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. Support to Live Video View on Graphic Map.
3. Support to viewing Anti-passback Zone and Fire Alarm Zone on Graphic Map.
4. Support to the Storage Path Settings for image logs.
5. Supports Allowed a day before/after time setting for working 24 hours or longer.

## Bug Fixes

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

## Main Fixes

1. Fixed a security vulnerability: Cross Site Scripting.
2. The row setting changes when the page is refreshed after setting the number of rows in the monitoring menu.
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.

## New Features and Improvements

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

## Bug Fixes

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

## New Features and Improvements

1. Support to Graphic Map
2. Support to the working alarm time report and an automated alarm email
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.
4. Support to the floating shift.
5. Support to Punch out Time Limit in the flexible shift.
6. Improves that an administrator can select weekend days when setting up the Schedule Template.
7. Support to the minimum duration setting when configuring the overtime management.
8. Separate the rounding setting of shift and overtime management.
9. Support Fixed option for Meal deduction and Break Time setting.
10. The Attendance management time added from Time Code is displayed in the Daily Summary Report and Individual Summary Report.
11. Support for AES encryption option on DESFire card.
12. Support to DESFire advanced option.
13. Support to the number of users, fingerprints, faces, and cards in Manage Users in Device.
14. Support to unlimited number of access levels and access groups.
15. Punch Log History report has been improved to display the modified time.
16. Improve the process for generating the time card.
17. Improves the T&A report to display only the time excluding the dates in Check In and Check Out.
18. Change the default value of the period in the T&A report.
19. Improves to upgrading the version to the latest version directly in BioStar 2.5.0 or higher.
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.



## Bug Fixes

1. If a user connects to BioStar 2 after specifying the hostname in the Windows, the user cannot access the T&A menu.
2. Unable to add a Wigand device to BioEntry W2.
3. Users can access a higher level of Web Server Home in the web server.
4. If you set Leave to start or end date of Daylight Saving Time, the incorrect time is displayed.
5. Change the <Punch in Time Limit> setting of Flexible Shift to operate based on the setting of <Day start time>.
6. Users who have special characters (-, \_) in the ID cannot be selected in the T & A report.
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.
8. Department information does not display from root when exporting the T&A report to CSV format.
9. The APB database management table is reset periodically, regardless of the Reset Time setting in the global APB zone.
10. In an environment that uses an MS SQL Server database, the modified date format setting is not normally applied to Audit Trail menu.
11. When a user upgrades the version of BioStar 2, the number of user access groups is displayed differently than the existing settings.

## Bug Fixes

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

## New Features and Improvements

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

## Bug Fixes

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. 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.
3. RTC and DHCP are displayed on Display/Sound of XPass D2(XPD2-GKDB) device page.
4. The firmware upgrade notification does not appear even though connecting XPass D2(XPD2-GKDB) that has a previous version firmware to BioStar 2.
5. XPass D2(XPD2-GKDB) succeeds in authentication if AoC ID is entered as keypad even though server matching is enabled.
6. If an upper and lower group without elevator is moved at the same time, the group is not displayed normally.
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.
8. Scanning the fingerprint on the BioMini causes an error and BioStar 2 does not work normally.
9. If the user name is set to Arabic, the name does not display normally.
10. Fixed a security vulnerability that allows a user account to acquire an administrator permissions.
11. BioStar 2 version upgrade fails when using Java 1.8.0 or later on PC with BioStar 2 installed.
12. Some records are missing in T&A reports.

## New Features and Improvements

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

## Bug Fixes

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. Issue where the video server does not work if the video license is activated offline.
3. Issue where it is not possible to change configurable options when a user with administrator logs in from a mobile device.
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.
5. Issue where server does not retry after failing to connect to database.
6. Issue where device is not auto-synced when face template has been deleted.
7. Issue where device secure communication status can be changed to 'Disabled' even when user login ID, password, and PIN have been set.
8. Issue where page display error occurs when device details page is accessed with OM-120 and DM-20 disconnected.
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.
10. Issue where model names of XPass D2 and BioLite N2 are not correctly displayed in the firmware upgrade list.
11. Issue where daylight saving time cannot be set up for FaceStation 2 device when version 2.6.0 has been installed newly.
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.
13. Issue where it is not possible to set system log storage period to 120 days.
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.
15. Issue where incorrect IP address notification pop-up appears when a string is entered in the server address field.
16. Issue where video server does not shut down when changing database port.

17. Issue where NVR details screen is displayed when scrolling the page with arrow keys at the upper right corner of Device Details.
18. Issue where "17677" is displayed in BioStar 2 event log when reset without network.
19. Changed data encryption related pop-up text that appears when adding a device.
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.
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.
22. Issue where despite daylight saving time having been set up, a time not applicable to Monitoring's floor and zone statuses is displayed.
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.
24. Issue where video license input window is activated after an upgrade to version 2.6.2.
25. Issue where master device switches to synchronization error status when deleting a door belonging to Access Level.
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.
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.
28. Issue where UI does not show normally when displaying an image log with a user name on a larger screen.
29. Issue regarding batch-editing doors where incorrect notification pop-up appears when the OK button is clicked without changing the settings.
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.
31. Issue where NVR appears when filtering by device name in Device Status or Alert History in Monitoring.
32. Issue where the "unknown" message does not appear in Schedule Lock/Unlock zone status when the device has been disconnected from the network.
33. Issue where Add, Delete, Modify NVR/camera features do not function when user has logged in as a video operator.
34. Issue where schedules are not updated in the video menu.
35. Issue where session timeout notification occurs when accessing video menu while using Time Attendance menu.
36. Issue where camera recording events for daily/holiday schedules do not function properly.
37. Problem that the change point is not updated even if the setting of the door configured in the camera menu is changed.
38. Issue where device search fails when adding a camera after failure to updating NVR configuration information.
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

## Bug Fixes

1. Issue where it is not possible to sync new logs to Time Attendance and Video when using MSSQL.
2. Execution time error when upgrading version 2.4.1 > 2.5 > 2.6.
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.

## New Features and Improvements

1. Support for Daylight Saving Time setting.
2. Strengthened security settings.
  - Manual management of server and device encryption keys.
3. Support for event log retention period setup.
4. Support for muster zone and interlock zone.
5. Changed AC license.
6. Support for device connectivity
  - BioMini Plus 2, BioLite N2, ad XPass D2
7. Support Reset without Network Settings.
8. Support for Seos card.
9. Support for user ID auto addition.
10. Improved system log setup UI.
11. Added an option to delete personal information and credentials when issuing AoC.
12. Support for personal authentication for AoC.
13. Support for customized advanced permissions for monitoring.
14. Added port settings for port management.
15. Support for one device mode (legacy).
16. Support for simultaneous use of Wiegand I/O.
17. Support for security tamper.
18. Support for unassigned blacklist card reassignment.
19. Added video storage status and management options.
20. Added video recording status indication to event log.
21. Improved Wiegand card search function.
22. Improved working conditions and behavior.
23. Changed site key hexadecimal value entry for smart cards.
24. Improved firmware upgrade message and alert behavior.
25. Stabilized MSSQL performance.
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.
27. Support for BioEntry W2 (BEW2-OHP) smart settings.



#### **Suprema Inc.**

17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA  
Tel: +82 31 783 4502 | Fax: +82 31 783 4503 | Inquiry: sales\_sys@supremainc.com



For more information about Suprema's global branch offices,  
visit the webpage below by scanning the QR code.  
<https://supremainc.com/en/about/global-office.asp>

© 2024 Suprema Inc. Suprema and identifying product names and numbers herein are registered trade marks of Suprema, Inc.  
All non-Suprema brands and product names are trademarks or registered trademarks of their respective companies.  
Product appearance, build status and/or specifications are subject to change without notice.