

Table of Contents

Version 2.9.6 (V2.9.6.36)	1
Release	1
New Features and Improvements	1
Bug Fixes	3

Version 2.9.6 (V2.9.6.36)

Release

2024-05-22

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)
63. When restarting the Core Web Server service in **BioStar 2 Setting** while using the **Automatic System Backup**, the setting of **Automatic System Backup** is reset to **Not Use**. (Affects version: v2.9.5)

From:

<http://kb.supremainc.com/knowledge/> -

Permanent link:

http://kb.supremainc.com/knowledge/doku.php?id=en:release_note_296&rev=1717032230

Last update: **2024/05/30 10:23**