BioStar 2

Revision Notes

Version 2.7.4

suprema
BIOMETRICS & SECURITY

Version 2.7.4 (Build No. 2.7.4.25)

Release: 2019-03-20

1. Important Bug Fix

1.1. If you set a language that has more than two characters for the language delimiter in the resource file, that language will not properly be applied to the T & A menu.

1.2. One of the BioStar 2 configuration files, the nssm.exe, is not installed or has been deleted from the T&A and Video web server services list because some antivirus programs have determined that the file is a malicious program.

1.3. The door information of access level setting is displayed differently from the setting.

1.4. When operating the Delete From Device in the USER menu, devices belonging to the group cannot be selected.

2. New Features and Improvements

2.1. Enhanced security of login passwords.
   - Limits the use of passwords that contain the same string, consecutive string, and login ID
   - Limits reuse of the same password

2.2. Support for Quick Enrollment for FaceStation 2.
   - FaceStation 2 FW V1.2.2 or later

2.3. Support to Spanish and Arabic.

2.4. Supports up to 249 Custom Levels.

2.5. Changes the Java version.
   - Before: 1.8.0_191
   - After: 1.8.0_201

3. Bug Fix

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

Version 2.7.3 (Build No. 2.7.3.23)

1. Important Bug Fix

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

2. New Features and Improvements
   2.1. Increase the number of administrators that can be added per device.
   - Before: 10
   - After: up to 1,000 (depends on the firmware version of the device.)

   2.2. Change the way new settings are applied when adding administrators using batch edit of devices.
   - Before: Overwrite a new setting to existing settings.
   - After: Add a new setting to existing settings.

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

3. Bug Fix
   3.1. When creating an Access Group, the setting is not applied properly if you add the same user to the User Group and User at the same time.

   3.2. If an administrator edits the settings of the device on the server, Server Private Msg option on that device will always change to disabled.

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

Version 2.7.2 (Build No. 2.7.2.19)

1. Important Bug Fix

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

   1.2. In an environment that uses an MS SQL Server database, the server restarts when an administrator adds more than one signal input event to the trigger & action of the device.

2. New Features and Improvements

   2.1. Add the Security menu.
      - Change Password Level options.
      - Support to the setting for Maximum Password Age.
      - Support to the setting for Maximum Password Change Limit.
      - Support to the setting options for password failures at login.

   2.2. Support to Live Video View on Graphic Map.

   2.3. Support to viewing Anti-passback Zone and Fire Alarm Zone on Graphic Map.

   2.4. Support to the Storage Path Settings for image logs.

   2.5. Supports Allowed a day before/after time setting for working 24 hours or longer.

3. Bug Fix

   3.1. The HTML tag is displayed in the daylight saving time settings page.

   3.2. Once an image file set with a graphics map is deleted, the graphics map image cannot be modified.

Version 2.7.1 (Build No. 2.7.1.13)

1. Important Bug Fix

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

2. New Features and Improvements

   2.1. Supports synchronization of all devices connected to the server when users update the device.

   2.2. Improves the ability to delete users on a device from the server's user menu.

   2.3. Support to Input(Event Name Change) of Trigger & Action in the device advanced setting.

   2.4. Changes the Java version.

   - Before: 1.8.0_161
   - After: 1.8.0_191

   2.5. Provides the log about whether a user has been updated on the device or the server.

   2.6. Adds root password verification procedures during installation and upgrade.

3. Bug Fix

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

Version 2.7.0 (Build No. 2.7.0.50)

1. New Features and Improvements

    1.1. Support to Graphic Map

    1.2. Support to the working alarm time report and an automated alarm email

    1.3. Improves the option to Add Custom Level.

    - Adds a graphic map group to Admin Item Settings.

    - Improves the ability to set up user groups and device groups according to Custom Account Level in Time & Attendance.

    1.4. Support to the floating shift.

    1.5. Support to Punch out Time Limit in the flexible shift.

    1.6. Improves that an administrator can select weekend days when setting up the Schedule Template.

    1.7. Support to the minimum duration setting when configuring the overtime management.

    1.8. Separate the rounding setting of shift and overtime management.

    1.9. Support Fixed option for Meal deduction and Break Time setting.

    1.10. The Attendance management time added from Time Code is displayed in the Daily Summary Report and Individual Summary Report.

    1.11. Support for AES encryption option on DESFire card.

    1.12. Support to DESFire advanced option.

    1.13. Support to the number of users, fingerprints, faces, and cards in Manage Users in Device.

    1.14. Support to unlimited number of access levels and access groups.

    1.15. Punch Log History report has been improved to display the modified time.

    1.16. Improve the process for generating the time card.

    1.17. Improves the T&A report to display only the time excluding the dates in Check In and Check Out.

    1.18. Change the default value of the period in the T&A report.

    1.19. Improves to upgrading the version to the latest version directly in BioStar 2.5.0 or higher.

    1.20. Improves usability

    - Support to the separator option in CSV export.

    - Add <Apply & Add New> button to Time Code, Shift, Schedule Template, Rule, Schedule setting screen.

    - Change some special characters (\, /, :, *, ?, ", ', `, <, >, |, .) to be unavailable when setting a user name.

    - Improves that the Edit popup or T&A report page is displayed if clicking the result value of the T&A report.

    - Improves to set the time of overtime work in minutes.

    - Change the start date of the week to Monday.

    - Remove the Temporary Schedule from the Time Card.

    - Support for Arabic.

    - Change the loading icon of the Time Attendance menu like any other menu.

2. Bug Fix

    2.1. If a user connects to BioStar 2 after specifying the hostname in the Windows, the user cannot access the T&A menu.

    2.2. Unable to add a Wigand device to BioEntry W2.

    2.3. Users can access a higher level of Web Server Home in the web server.

    2.4. If you set Leave to start or end date of Daylight Saving Time, the incorrect time is displayed.

    2.5. Change the <Punch in Time Limit> setting of Flexible Shift to operate based on the setting of <Day start time>.

    2.6. Users who have special characters (-, _) in the ID cannot be selected in the T & A report.

    2.7. If you change the server port value for the cloud and then restore the value before the change, a user cannot enter the Time Attendance menu.

    2.8. Department information does not display from root when exporting the T&A report to CSV format.

    2.9. The APB database management table is reset periodically, regardless of the Reset Time setting in the global APB zone.

    2.10. In an environment that uses an MS SQL Server database, the modified date format setting is not normally applied to Audit Trail menu.

    2.11. When a user upgrades the version of BioStar 2, the number of user access groups is displayed differently than the existing settings.

Version 2.6.4 (Build No. 2.6.4.7)

1. Bug Fix

    1.1. The duplicate logs are output when a user runs CSV export.

    1.2. The server receives requests with a version lower than TLS 1.1 (Supports TLS 1.1 and above).

    1.3. The user cannot set the same action for different triggers when setting Trigger & Action, Intrusion Alarm Zone, or Interlock Zone.

    1.4. The assignment complete message is displayed even if a user assigns an already assigned card to another user using the API.

    1.5. When a user who does not have permission on the door menu logs, the door list of the zone menu is disabled.

    1.6. The Add Zone option is not displayed when a user right-clicks each item in the zone menu.

Version 2.6.3 (Build No. 2.6.3.73)

1. New Features and Improvements

    1.1. Improves the performance of showing lists.

    1.2. Improves the option to Add Custom Level.

        - Adds Admin Item Settings option.

    1.3. Improves to allow the custom level administrator with edit or read permission to the monitoring menu to receive alerts.

2. Bug Fix

    2.1. The Video menu in Settings is not displayed on the screen if the PC with BioStar 2 is not connected to the network.

    2.2. If an elevator group that contains subgroups moves to a child of another elevator group, it causes an error and BioStar 2 does not work normally.

    2.3. RTC and DHCP are displayed on Display/Sound of XPass D2(XPD2-GKDB) device page.

    2.4. The firmware upgrade notification does not appear even though connecting XPass D2(XPD2-GKDB) that has a previous version firmware to BioStar 2.

    2.5. XPass D2(XPD2-GKDB) succeeds in authentication if AoC ID is entered as keypad even though server matching is enabled.

    2.6. If an upper and lower group without elevator is moved at the same time, the group is not displayed normally.

    2.7. If the date format is set on the device and then it is connected to BioStar 2, the date format changes to the different option.

    2.8. Scanning the fingerprint on the BioMini causes an error and BioStar 2 does not work normally.

    2.9. If the user name is set to Arabic, the name does not display normally.

    2.10. Fixed a security vulnerability that allows a user account to acquire an administrator permissions.

    2.11. BioStar 2 version upgrade fails when using Java 1.8.0 or later on PC with BioStar 2 installed.

    2.12. Some records are missing in T&A reports.

Version 2.6.2 (Build No. 2.6.2.64)

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

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

right corner of Device Details.

2.18. Issue where "17677" is displayed in BioStar 2 event log when reset without network.

2.19. Changed data encryption related pop-up text that appears when adding a device.

2.20. Issue where it is possible to configure devices other than those connected to the same RS-485 network when editing pre-configured schedule unlocked zone.

2.21. Issue where error pop-up does not appear when you change user ID type to alphanumeric characters after adding BioLite Net and Xpass S2.

2.22. Issue where despite daylight saving time having been set up, a time not applicable to Monitoring's floor and zone statuses is displayed.

2.23. Issue regarding changing the status of one or more global zones where changing the status of one zone does not automatically change the status of the other zones.

2.24. Issue where video license input window is activated after an upgrade to version 2.6.2.

2.25. Issue where master device switches to synchronization error status when deleting a door belonging to Access Level.

2.26. Issue where fingerprint image does not appear normally when a smart card has been added after the addition of two or more fingerprints of user.

2.27. Issue where device name does not show in tamper-on alarm pop-up if a tamper has occurred on the device after reset without network.

2.28. Issue where UI does not show normally when displaying an image log with a user name on a larger screen.

2.29. Issue regarding batch-editing doors where incorrect notification pop-up appears when the OK button is clicked without changing the settings.

2.30. Issue where column switches to its default value when entering the card menu again after changing the column settings in the card menu in Settings.

2.31. Issue where NVR appears when filtering by device name in Device Status or Alert History in Monitoring.

2.32. Issue where the "unknown" message does not appear in Schedule Lock/Unlock zone status when the device has been disconnected from the network.

2.33. Issue where Add, Delete, Modify NVR/camera features do not function when user has logged in as a video operator.

2.34. Issue where schedules are not updated in the video menu.

2.35. Issue where session timeout notification occurs when accessing video menu while using Time Attendance menu.

2.36. Issue where camera recording events for daily/holiday schedules do not function properly.

2.37. Problem that the change point is not updated even if the setting of the door configured in the camera menu is changed.

2.38. Issue where device search fails when adding a camera after failure to updating NVR configuration information.

2.39. Issue where you cannot proceed to the next step when selecting NVR in video menu after deleting schedules set up for camera.

Version 2.6.1 (Build No. 2.6.1.10)

1. Bug Fix

    1.1. Issue where it is not possible to sync new logs to Time Attendance and Video when using MSSQL.

    1.2. Execution time error when upgrading version 2.4.1 > 2.5 > 2.6.

    1.3. A change has been made so that moving is possible only when upgrading to a new version and the version of existing BioStar 2 is 2.5.

Version 2.6.0 (Build No 2.6.0_155)

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