Table of Contents

Version 2.8.4 (V2.8.4.34)

Release

2020-08-05

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) 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.

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.

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.