Table of Contents

System Configuration, BioStar 2, Custom Level, custom admin, custom operator

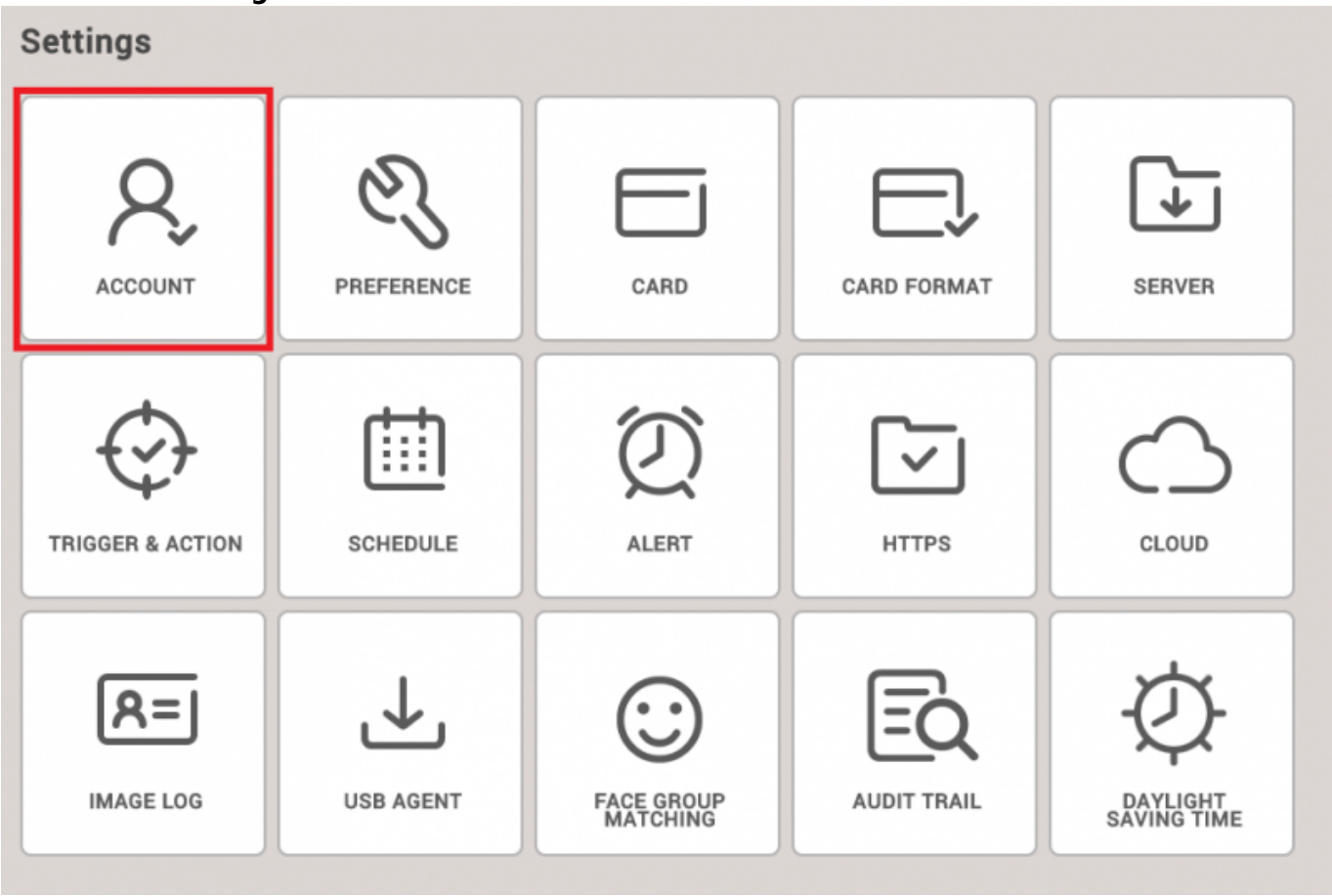
How to Configure a Custom Level

The custom level feature allows you to give specified privileges to administrators in specific menus.

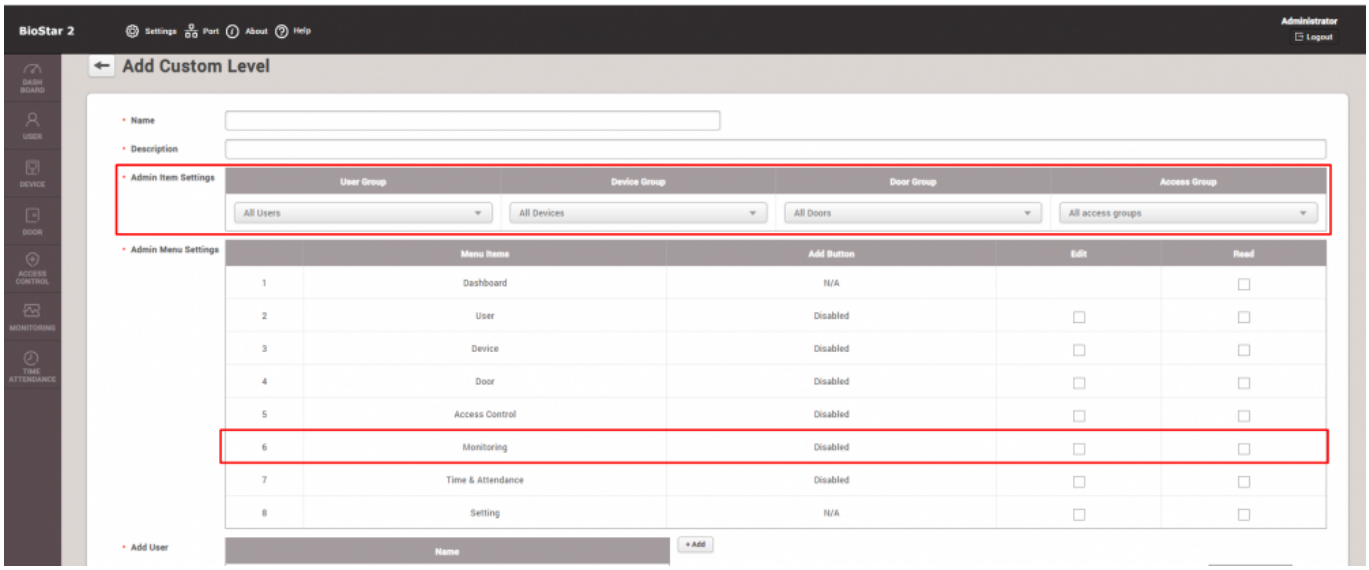
BioStar version 2.6 and above

From BioStar 2.6.3, the Admin Item Setting is changed so that a custom level can be assigned for a specific User Group, Device Group, Door Group, and Access Group. Also Monitoring menu is now allowing the administrator to assign “Read” rights.

1. Go to the **Settings** > **ACCOUNT**.



2. Create new Custom Level. At this point, you can configure the item settings and menu settings.



You can also see now that the Monitoring Admin Menu Setting allows “Read” assignment.

Admin Item Settings includes User Group, Device Group, Door Group, and Access Group(including Elevator Group).
Each item can be configured for each group or for all groups.
Admin Menu Settings consists of Dashboard, User, Device, Door, Elevator, Zone, Access Control, Monitoring, Time and Attendance, Setting, and Video categories.
For each menu you can set “Edit” and “Read” privileges.
When checking “Edit” it will automatically check “Read.”
Depending on such privilege settings, “Add Button” column value will be changed (N/A, Disabled, or Enabled)

Dashboard only allows “Read” privilege and its “Add Button” will show “N/A” status.
When the “Read” is checked the dashboard will be shown when you log in to BioStar 2.
Depending on Admin Item Settings, dashboard use status is not supported but is shown by the number of use status according to Admin Menu Settings.

User menu sets who can see the user menu depending on the privilege that is set here. The privilege to this menu is affected by User Group, Access Group, and Device Group.

- User Group: Add/Edit privilege limit on a menu
- Access Group: Display/Select privilege limit on a user specific page
- Device Group: Device display privilege limit when enrolling fingerprint/face/card for a user

Device menu dictates display privilege of Device menu depending on its “Edit/Read” setting.
Device menu privilege is affected by User Group, Device Group of Admin Item Settings. User Group influences administrator Display/Add/Edit privilege limit of a device specific page. For an administrator who does not have privilege to a device is set, an administrator who does not have privilege is displayed when entering a device specific page, and this can be deleted.

- Device Group: limits display of a device on a menu, and limits device Add/Edit privilege.

Door menu dictates display limit of a Door menu depending on its Door menu Edit/View privilege settings.
Door menu privilege is affected by Admin Item Settings(whether set to Device Group, Door Group, and Access Group).

- Device Group: limits Display/Add/Edit privilege of a Door specific page
- Door Group: limits Display/Add/Edit privilege of Door on a menu
- Access Group: limits

Access Control menu dictates display limit of elevator menu depending on Edit/Display privilege settings.
Access Control menu is affected by Admin Item Settings(User Group, Door Group, Access Group).

- User Group: User Display/Add/Edit limit on an access group specific page
  - Can only Add users with privilege
  - Can only Delete users when an user is added to an Access Group without privilege within a created Access Group
- Door Group: Door Group Display/Add/Edit limit on a menu
- Access Group: Dual Authentication Add/Edit limit on a Door specific page
  - All Groups: Can Create/Edit/Delete Access Group and Elevator Group
  - Specific User Group: Can Add/Delete an User Group or an User with privilege, within an Access Group(does not include Access/Elevator Level)

Monitoring dictates display of Monitoring menu depending on Edit/Read settings.
Monitoring menu privilege is affected by all items in the Admin Item Settings.

- Event/Real-Time Log
  - Only devices with privilege in the device ID by default can be filtered, and the filter cannot be deleted
  - Filter cannot be set for Device and Device Group(because device filter is applied to a device with privilege for logs)
  - Upper right-hand corner option is displayed only when with Edit privilege settings
- Device Status
  - Device is displayed according to Device Group privilege settings
  - Device Alarm Enable/Disable is displayed only with Edit privilege settings
- Door Status
  - Door is displayed according to Door Group privilege settings
  - Door control is possible and option buttons can be displayed depending on Edit privilege settings
- Elevator Status
  - Elevator is displayed according to Elevator Group privilege settings
  - Elevator control is possible and option buttons can be displayed depending on Edit privilege settings
- Zone Status
  - All of the zones can be displayed
  - Zone control(alarm clear) is possible and option buttons can be displayed depending on Edit privilege settings
    - Access Denied popup is displayed when a zone tracking window cannot be displayed due to no privilege to access added devices to the zone.
- Alert Status
  - Alert popup is displayed when Monitoring Edit/Read privilege is set(Alert popup is only displayed for device IDs with the privilege settings).
  - With Monitoring Read privilege only, a confirm button for an alert is not displayed and can only be ignored, alert history can be checked, and alert list can be displayed and the checkbox is enabled to allow creating and checking memos.
- Real-time Videos
  - Videos can be displayed depending on Video privilege(Edit/Read) settings

- Videos are not displayed if no Video privilege is set
- The Door Control is affected by Door Group of Admin Item Settings set to Video camera of Real-Time video when Monitoring Edit privilege is set

Time and Attendance

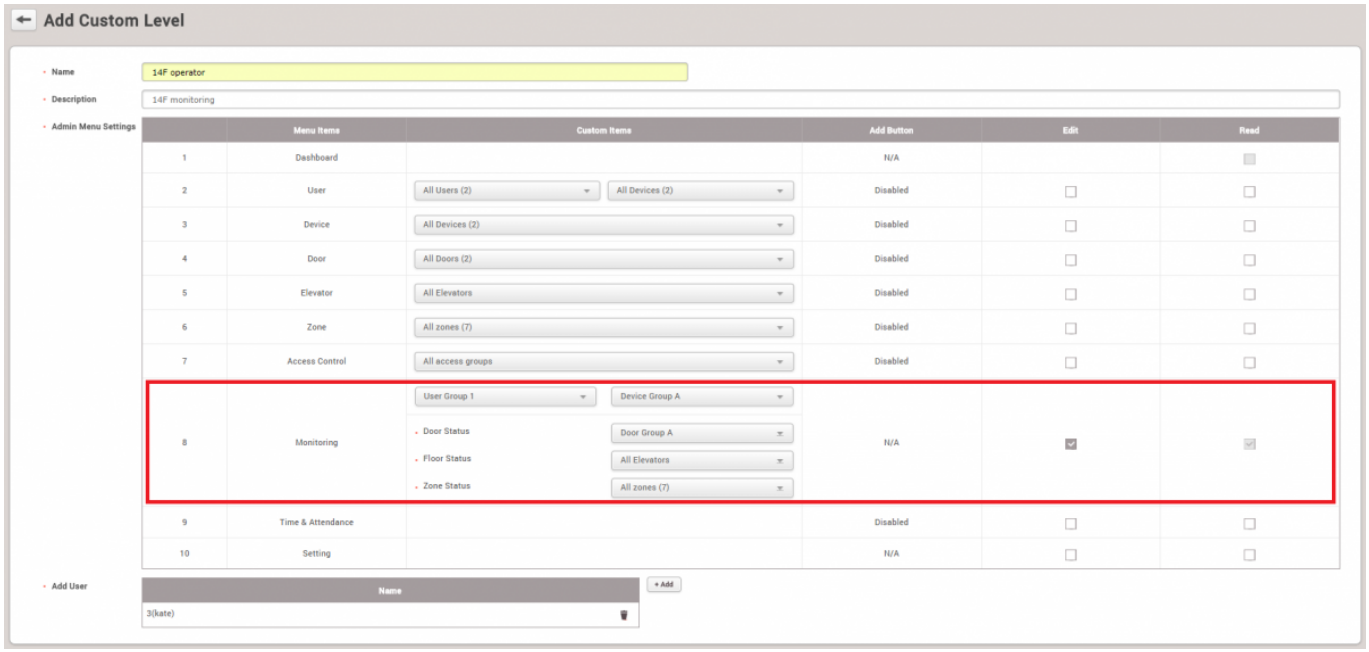
- The same way as 2.6.2 works (is not affected by Admin Item Settings)

Settings

- Only Preferences and Https are displayed if Settings menu Edit/Read privilege is not set
- Settings menu Read privilege
  - Everything is displayed except Account menu
  - No Video menu should be displayed in the Settings for Accounts with only Settings privilege
  - Device display limit of server, working conditions, and face group-matching depending on Admin Item Settings (User Group, Device Group, and Door Group)
- Settings menu Edit privilege
  - Everything except Accounts menu is displayed, and Add/Edit is possible for each menu of the Settings
  - Video menu of the Settings should not be displayed for accounts with only Settings privilege
  - Device display limit of server, working conditions, and face group-matching depending on Admin Item Settings (User Group, Device Group, and Door Group)
- Video
  - Video menu is displayed depending on Settings menu Read/Edit privilege & Video Read/Edit privilege(Video display of the Settings with Video Read/Edit privilege, Video on Settings operate depending on Read/Edit privilege settings)

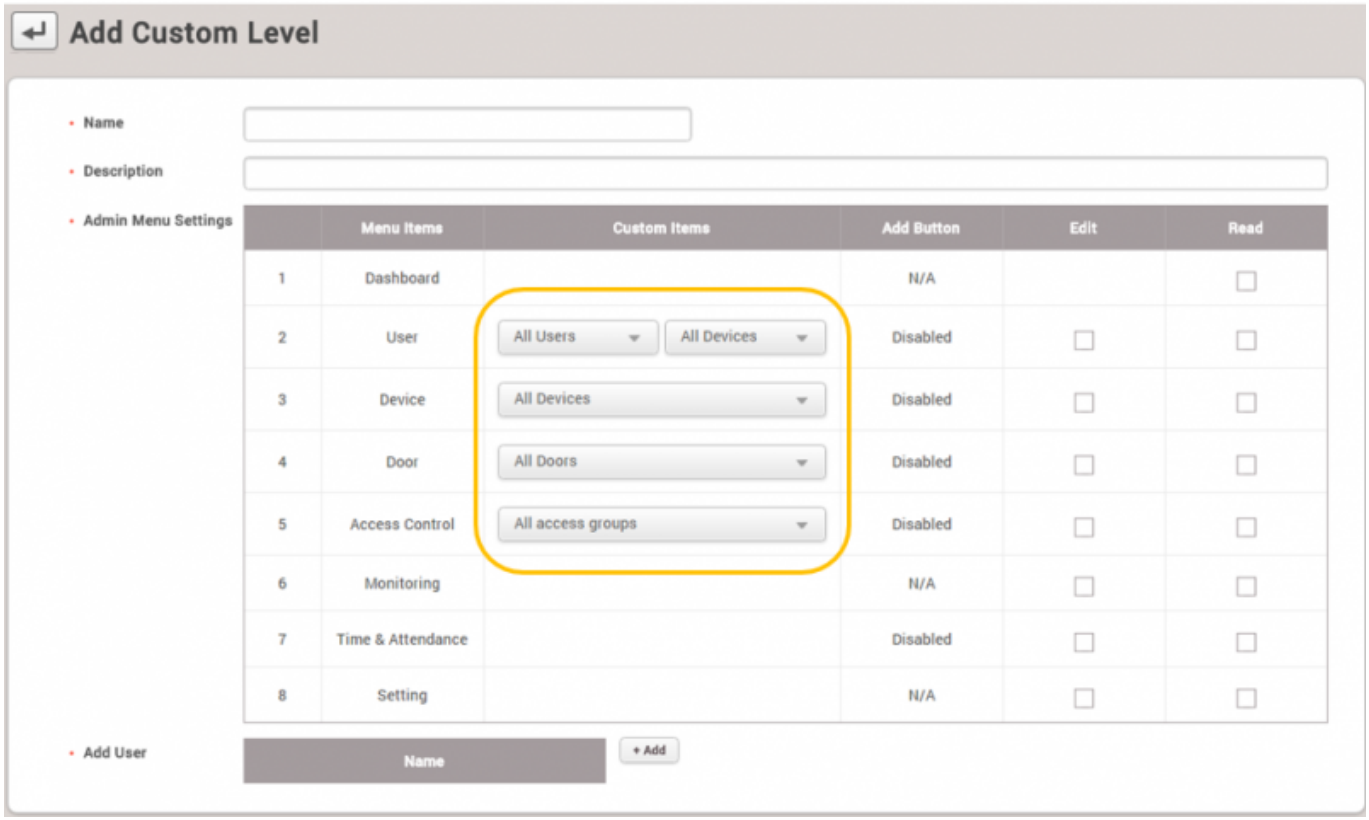
> - The expansion of Admin Item Settings to universal setting of the Custom Level will influence the Admin Menu Settings.
> - The Account button can only be visible to the Administrator.
> - If you are upgrading from previous versions to BioStar 2.6.3, you need to perform migration on the Custom Level
> - The Administrator will receive alert regarding Custom Level activities

Up to BioStar 2.6.2, Admin Item Settings were only limited to Monitoring section as in the screenshot below.



BioStar version 2.4 and above

In BioStar version 2.4, the custom level was further expanded to allow custom levels that controls specific users, devices, doors, and access groups.



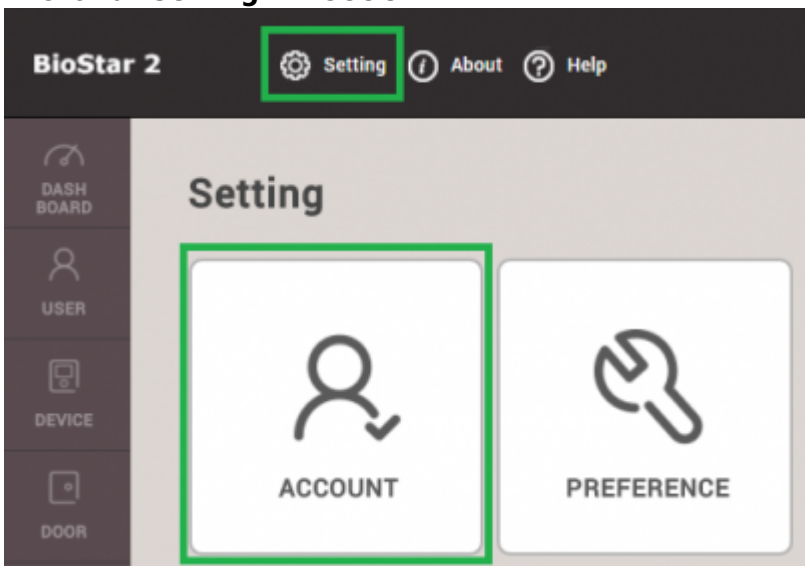
However, be aware that the custom items only apply to its specific menu.
This means that even if you apply a specific user in the **User** menu item and specific devices in the **Device** menu item, the custom operator will see *all* logs of devices and users in the **Monitoring** menu because the settings do not apply other menus.

Known Issue
You can only add new custom levels with the default administrator (ID 1) account in BioStar 2.4.
Refer to the following link: Freshdesk Known Issue Forum

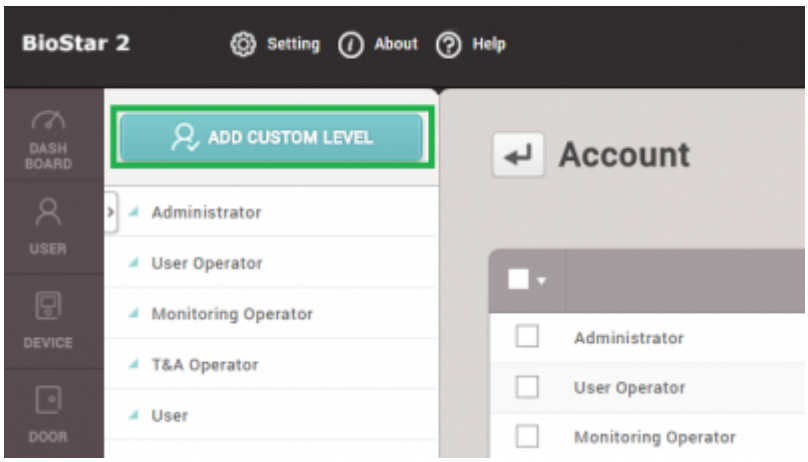
BioStar version 2.3

In BioStar 2.3, the feature to create custom administrators was introduced. You can add a custom administrator at **Settings** > **ACCOUNT**.
Below is a sample scenario where we will create a custom administrator that can only edit users and the T&A menu.

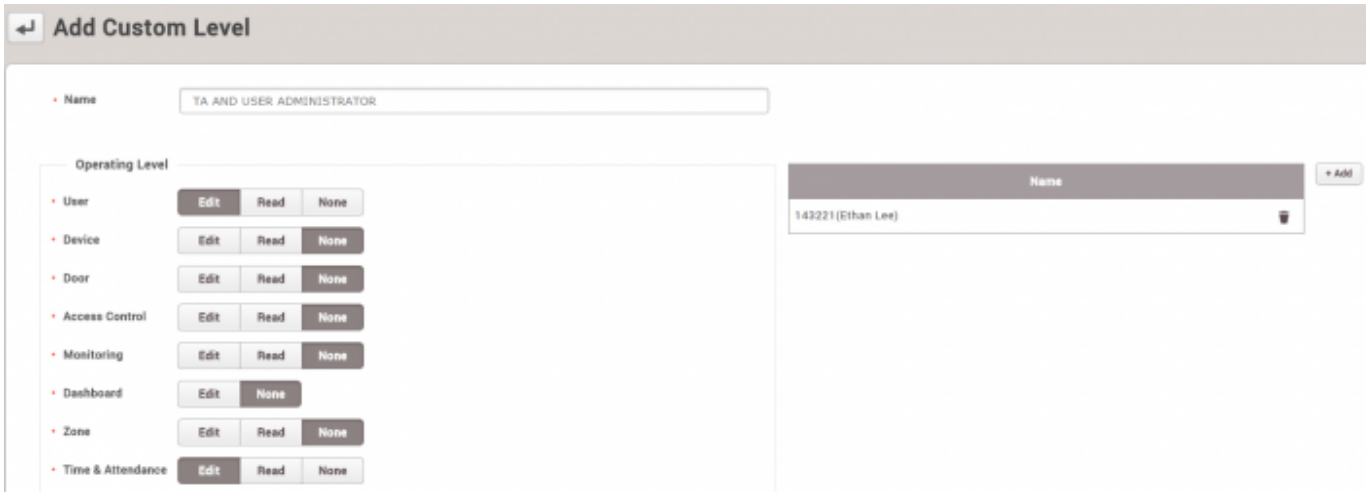
1. Click on **Setting** > **ACCOUNT**.



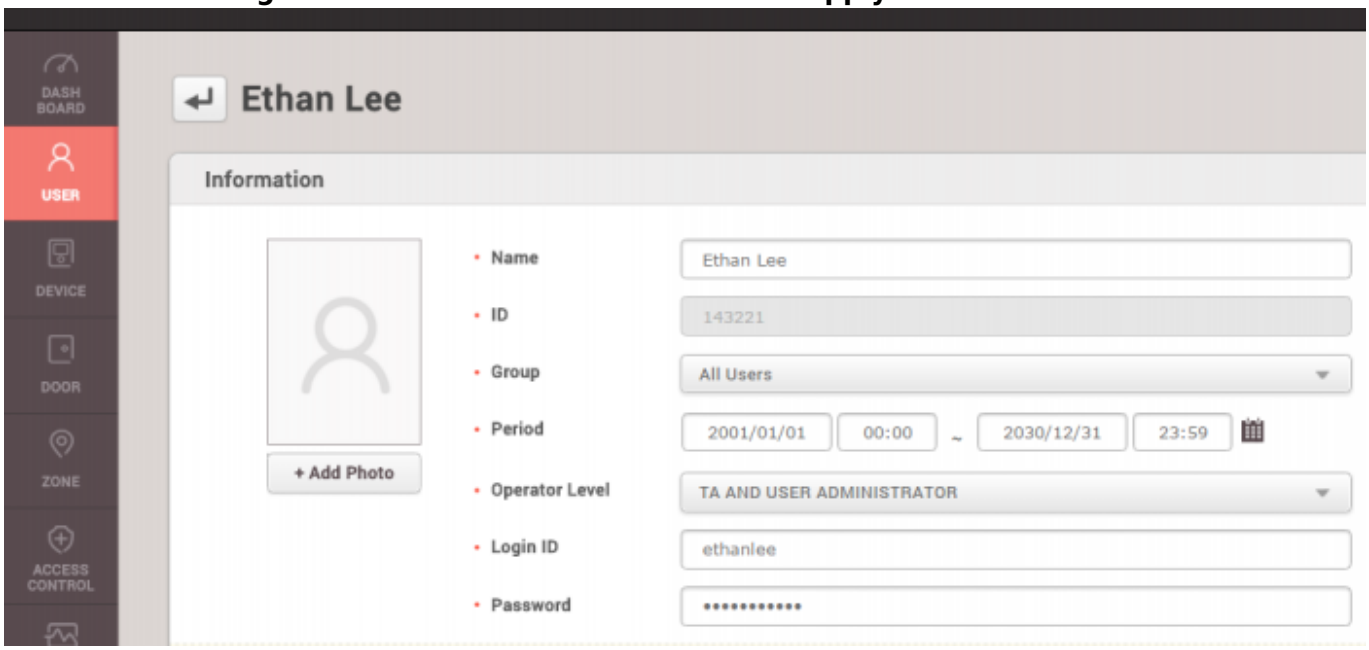
2. Click **ADD CUSTOM LEVEL**.



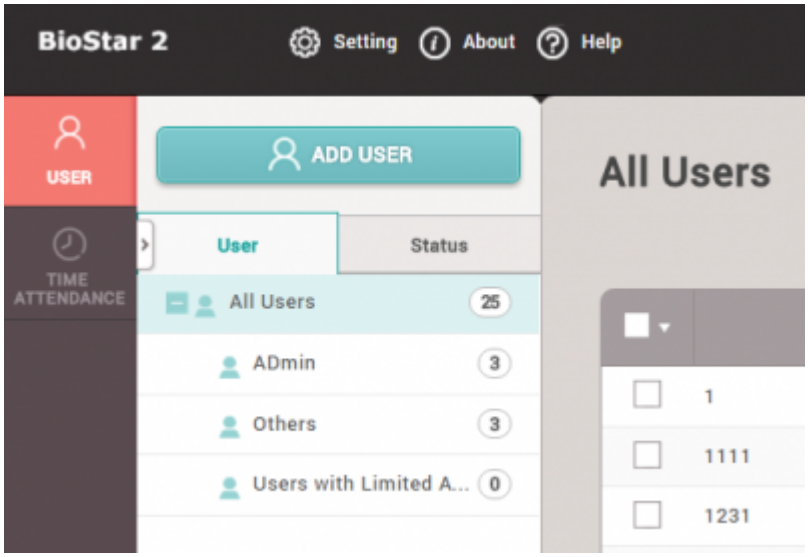
3. Type in a name for the custom level.
4. Click on **Edit** for **User** and **Time & Attendance** for the operating level.
5. Select a user to use this custom level by clicking on **+ Add**.



6. Now if you check the user in the **USER** tab, you will see that this user has the custom **Operator Level**. Create a **Login ID** and **Password** for the user. Click **Apply**.



7. Log out and log in as your new custom admin user.
8. You will see that this user only has full access and privilege for the **USER** and **TIME & ATTENDANCE** menu.



Before versions before 2.3

Before the release of BioStar 2.3, there were only 4 operator levels for users. There functions were limited to their roles as shown below:

1. Administrator : full privileges over all operations
2. User Operator : only full privileges to edit users
3. Monitoring Operator : only full privileges over the monitoring page
4. Mobile User : only privilege to read all menus.