BioStar X Mobile

ADMINISTRATOR GUIDE

Version 1.0.5

English

EN 102.00.BSX

suprema

SECURITY & BIOMETRICS

CONTENTS

Before You Start 5

Supported environment 5

License and network requirements 5

Getting Started 7

Download the BioStar X Mobile app 7

App permissions 7

Starting the app and initial setup 8

Connection troubleshooting 8

Using the app 9

Set Up the App 10

Check app version information 10

Login settings 11

Standard time zone settings 13

Date and time display format settings 14

Confirm changes with biometrics 14

Viewing license information and the privacy policy 15

Manage Users 16

Register Users 16

Edit and Delete Users 31

View User Log Events 32

Search and Filter Users 34

Manage Doors 36

Remote Control of Doors 36

View Door Details 38

Manage Devices 42

Check device information 42

Check device status 42

Release authentication failure lockout 43

Device search 44

Filter the device list 45

Real-time Log Monitoring 46

View real-time logs 46

View only certain logs 47

View log details 48

View Past Event Logs 49

View past event logs 49

View only specific logs 50

View log details 48

Check and Resolve Alerts 52

Alert list 52

Alert history 53

Getting Started with Roll Call 54

Use roll call in the mobile app 54

Use Quick Actions 61

Run a Quick Action 61

Quick Action details 61

Change Account Password 63

Appendices **64**

Disclaimers 64

Copyright Notice 65

Open Source License 65

Before You Start

Before using the BioStar X mobile app, check the following requirements and install the app.

Supported environment

The BioStar X mobile app can be used under the following conditions.

- **Supported system**: BioStar X
- **Server requirements**: A BioStar X server with API access is required.
- **Users**: Supported privileges include all pre-defined account levels, and support for custom account levels will be added later.
- **Mobile device**: iOS 13.0 or later, or Android 7.0 or later.

> **Info**
>
> The BioStar X mobile app cannot operate independently. Connect it to a BioStar X server running on the customer network.
>
> - For more information on the minimum requirements for installing BioStar X, see System Minimum Requirements.
> - For more information on installing BioStar X, see Express Installation.

License and network requirements

A BioStar X license is required to use the BioStar X mobile app. Purchase an add-on license option to use it. For more information on licensing policies, see License Policy.

Access environment	Required license
Same network	Mobile app license
External network (public IP)	Mobile app license
External network (no public IP)	Mobile app license + Remote Access license

- A **mobile app** license is required to integrate the BioStar X server with the mobile app.
- By default, use the mobile app by connecting to the BioStar X server on the same network.
- Access from an external network requires a public IP address. Otherwise, purchase an additional **Remote Access** license.

Info

- For more information on applying licenses in BioStar X, see BioStar X License.
- For more information on BioStar X server settings, see Server Detailed Settings.
- For more information on the Remote Access feature in BioStar X, see Remote Access Settings.

Next step

After completing the prerequisites, see how to install the BioStar X mobile app.

Getting Started

The BioStar X mobile app is available on iOS and Android. Install the app by following the instructions, then connect to the BioStar X server.

Download the BioStar X Mobile app

Download the app using the links or QR codes below.

Platforms	Download link	QR code
iOS	App Store	
Android	Google Play	

App permissions

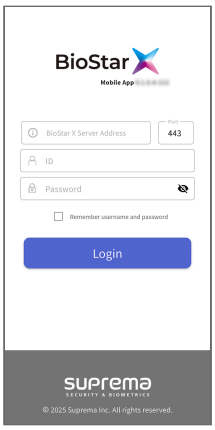
The BioStar X mobile app requests the following permissions when certain features are used. It does not request permissions during initial installation.

Permission	Required	Purpose
Storage	Optional	Required to manage and upload user images, such as gallery or device storage images.
Camera	Optional	Used to capture images for facial credential enrollment and video recording.
Biometric	Optional	Required for secure login using fingerprint or facial authentication on a mobile device.

> **Info**
> All permissions are optional, and users can deny them without affecting the app's basic features.

Starting the app and initial setup

When the app starts, a screen appears where you enter information to connect to the BioStar X server.



- **BioStar X Server Address**: Enter the IP address or domain address of the BioStar X server.
- **Port**: Enter the port number of the BioStar X server. The default is `443`.
- **ID** / **Password**: Enter your ID and password to log in to the BioStar X server.

After entering all required information, tap **Login** to sign in.

> **Info**
>
> - To save the account ID and password in the input fields, select the **Remember username and password** checkbox. The entered ID and password are automatically filled in on the next login.
> - For information on the BioStar X server IP address and port number, see Server Detailed Settings.

Connection troubleshooting

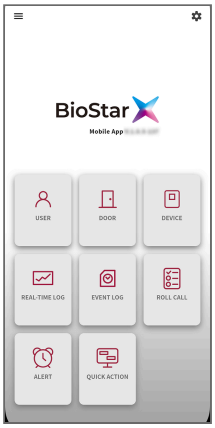
If login fails, check the following:

- Check that the BioStar X server address and port number are correct.
- Check that the account ID and password are correct.
- Check whether the mobile device and BioStar X are connected to the network.

> **Info**
>
> Access from an external network requires a public IP address. Otherwise, purchase an additional **Remote Access** license. For more information, see Before You Start.

Using the app

After login succeeds, the BioStar X mobile app home screen appears. On the home screen, view registered users, doors, real-time logs, event logs, and alerts. You can also access the side menu and settings menu.

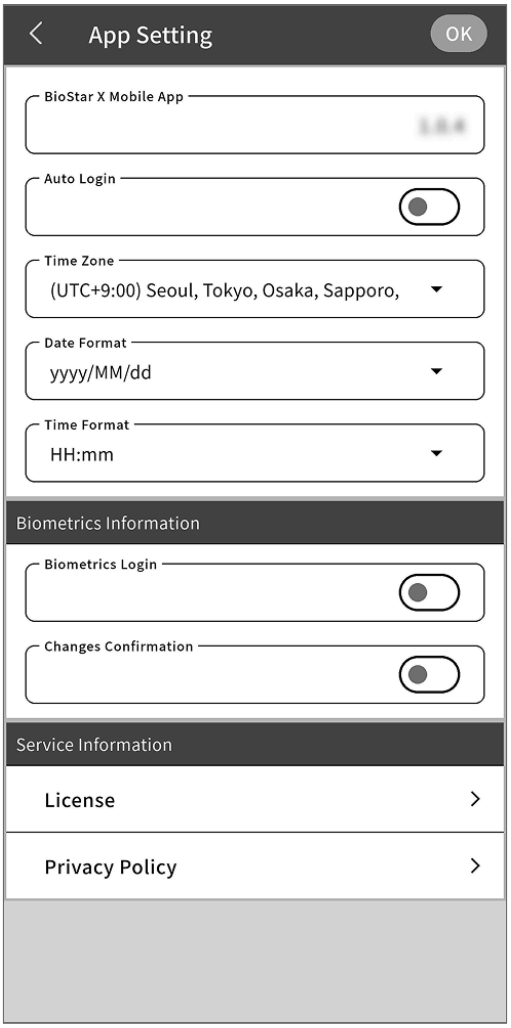


- ☰: Opens the side menu. In the side menu, change the password or log out, and access the main menus.
- ⚙: Opens the settings menu. For more information on app settings, see Set Up the App.
- **USER**: View the list of registered users and manage users. For more information on user management, see Manage Users.
- **DOOR**: View the list of registered doors and control them remotely. For more information on door management, see Manage Doors.
- **DEVICE**: Check the device status in the registered device list and remotely unlock locked devices. For more information on device management, see Manage Devices.
- **REAL-TIME LOG**: View real-time access event logs. For more information on real-time log monitoring, see Real-time Log Monitoring.
- **EVENT LOG**: View all event logs stored on the BioStar X server. For more information on log lookup, see View Past Event Logs.
- **ROLL CALL**: In the event of an emergency, the user can determine whether they have arrived at the roll call location by authenticating through entry or exit devices at a pre-designated location. The Roll Call feature is available through an add-on option with an **Essential** license or higher. For more information on the Roll Call feature, see Getting Started with Roll Call.
- **ALERT**: View alerts for doors, devices, and advanced access control. For more information on alerts, see Alert Settings.
- **QUICK ACTION**: Automates complex control procedures in emergencies. Execute the actions of multiple predefined devices instantly with a single button to respond quickly. You must create Quick Actions in the BioStar X web interface before using them in the mobile app. For more information about the **Quick Action** feature, see Use Quick Actions.

> **Info**
>
> All features are also accessible through the side menu (☰).

Set Up the App

In the BioStar X Mobile App settings menu, manage the app's main features, including login, time zone, and security. To access the app settings menu, tap ⚙ in the upper right corner of the Home screen.



Check app version information

In **BioStar X Mobile App**, check the version information for the currently installed BioStar X Mobile App. Tap **BioStar X Mobile App** to check whether the installed app is the latest version.

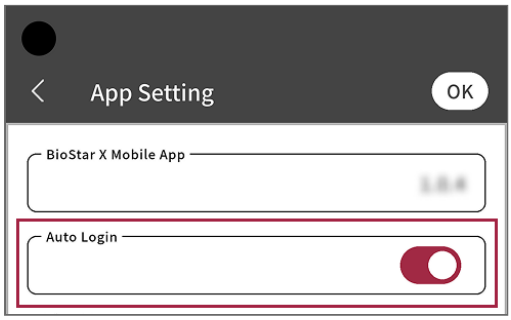
> **Info**
> Use the app version information when contacting support for troubleshooting.

Login settings

Automatic login settings

Users can enable the automatic login feature instead of entering login information each time they open the app or log in again after the session expires.

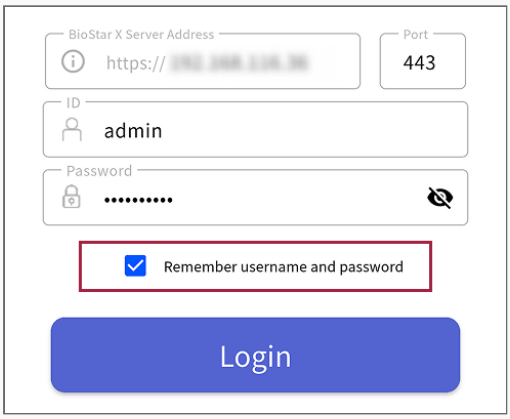
1. To enable the automatic login feature, turn on the **Auto Login** option.



2. To save changes, tap **OK** in the upper right corner of the screen.
3. When the confirmation message appears, tap **Yes**.

Info

- Use the automatic login feature only when **Remember username and password** is enabled on the login screen. If this option is not enabled, the automatic login feature is unavailable.

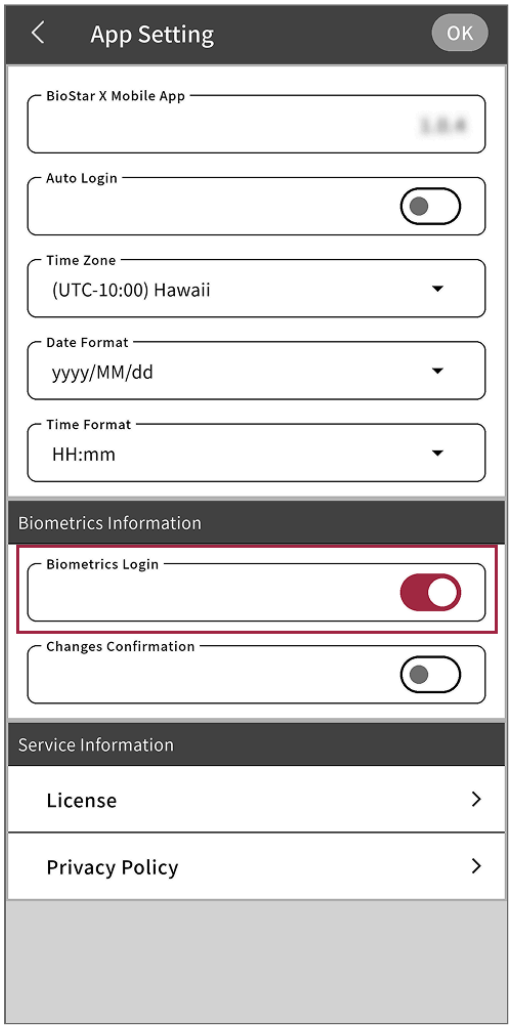


- If the automatic login feature is enabled, logout is unavailable. To log out, disable the automatic login feature first, and then log out.

Biometric login settings

On mobile devices with biometric authentication, enable the biometric login feature. When this feature is enabled, users can log in with the fingerprint enrolled on their mobile device instead of an ID and password.

1. To enable the biometric login feature, tap **Biometrics Information** → **Biometrics Login**.



2. To save changes, tap **OK** in the upper right corner of the screen.
3. When the confirmation message appears, tap **Yes**.

Use biometric authentication on the login screen.

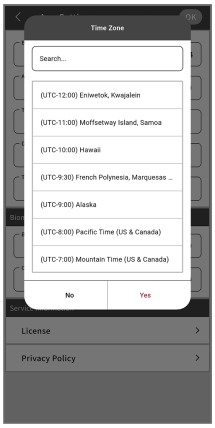


Info

This feature requires biometric authentication on the mobile device and the **Remember username and password** option enabled on the login screen.

Standard time zone settings

Set the time zone for the location where the BioStar X server is installed. A correct time zone setting is important for accurate timestamps in event logs and notifications.

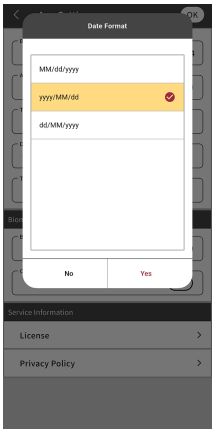


1. Tap **Time Zone**.
2. Select the time zone for the location where the BioStar X server is installed from the time zone list.
3. Tap **Yes**.
4. To save changes, tap **OK** in the upper right corner of the screen.
5. When the confirmation message appears, tap **Yes**.

> **Info**
>
> The changed setting also applies to the BioStar X server, and the timestamps in event logs and notifications shown in the app reflect the updated time zone.

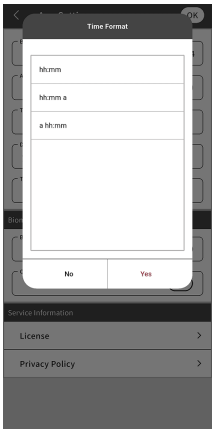
Date and time display format settings

You can set the date and time display format to be used across the system.



Date display format

1. Tap **Date Format**.
2. Select the desired date display format from the **Date Format** list.
   - **MM/dd/yyyy**: 01/31/2025
   - **yyyy/MM/dd**: 2025/01/31
   - **dd/MM/yyyy**: 31/01/2025
3. Tap **Yes**.
4. To save changes, tap **OK** in the upper right corner of the screen.
5. When the confirmation message appears, tap **Yes**.

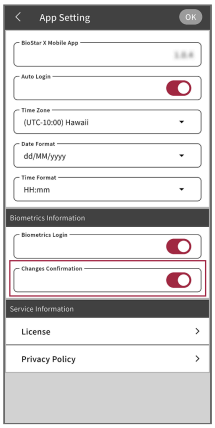


Time display format

1. Tap **Time Format**.
2. Select the desired time display format from the **Time Format** list.
   - **hh:mm**: 23:59, 24-hour format
   - **hh:mm a**: 11:59 PM, 12-hour format
   - **a hh:mm**: PM 11:59, 12-hour format
3. Tap **Yes**.
4. To save changes, tap **OK** in the upper right corner of the screen.
5. When the confirmation message appears, tap **Yes**.

Confirm changes with biometrics

When making important system changes, you can require additional authentication with biometrics. This helps prevent unauthorized changes by other users.

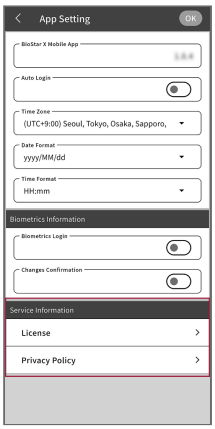


1. Tap **Biometrics Information** → **Changes Confirmation**.
2. To save changes, tap **OK** in the upper right corner of the screen.
3. When the confirmation message appears, tap **Yes**.

The following changes require biometric authentication.

- Change account password
- Change app settings
- Register a new user
- Edit user information
- Delete users

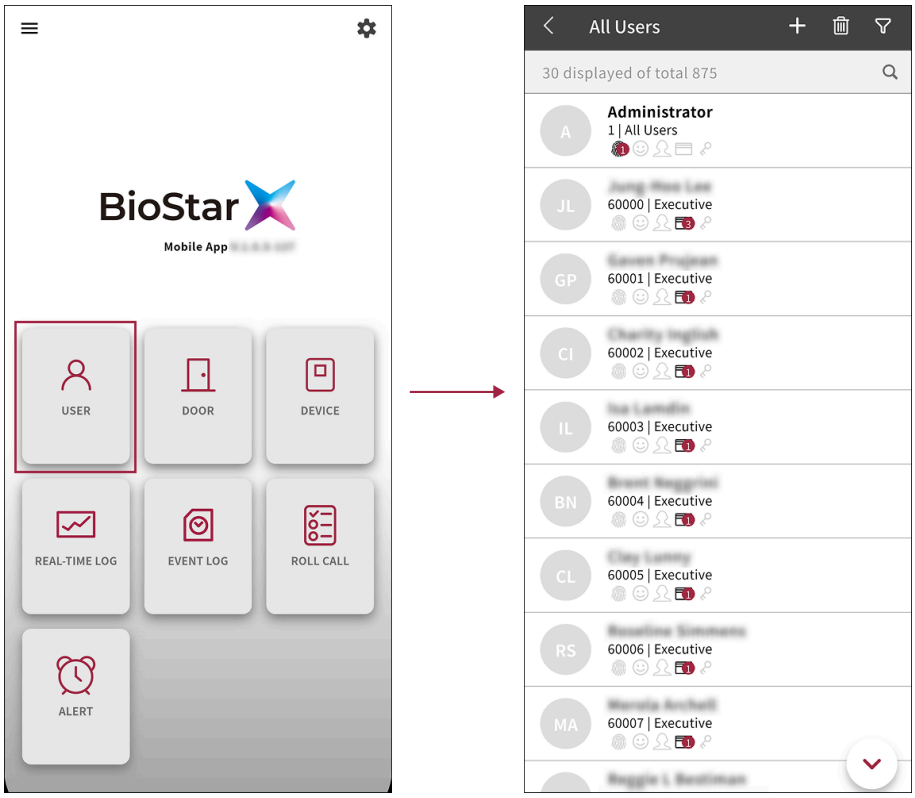
Viewing license information and the privacy policy



- To view the license information applied to the BioStar X Mobile App, tap **Service Information** → **License**.
- To view Suprema's privacy policy, tap **Service Information** → **Privacy Policy**. Use the link provided in the app to view Suprema's privacy policy posted on the official website.

Manage Users

Manage new user registration, remove departing users, and update user information from the user list. User search and log lookup are also supported.

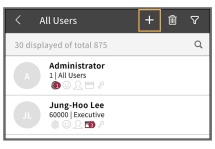


Info

For more information on user management in BioStar X, see User.

Register Users

When you need to register a new user or a temporary visitor to the system, enroll basic information, permissions, and authentication methods together.

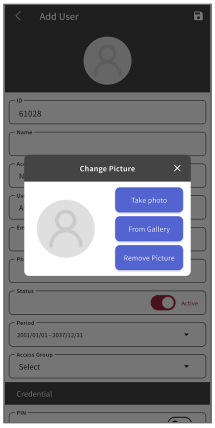


1. On the app home screen, tap **USER**.

   You can also access it through the side menu. Tap ☰ → **User**.

2. Tap + at the top right of the screen.
3. Enter the user's basic information and set up credentials.

Enroll profile image

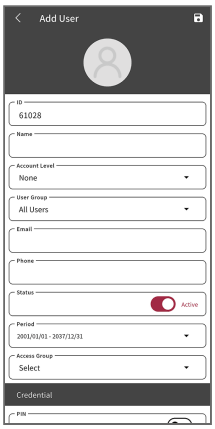


To enroll a user's profile image, tap the profile icon at the top of the screen.

- **Take photo**: Take a photo with your mobile device's camera and use it as the profile image.
- **From Gallery**: Select a saved photo on your mobile device and use it as the profile image.

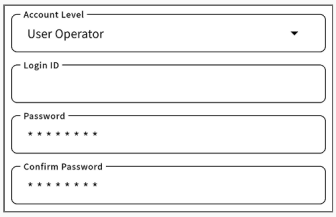
> **Info**
> To delete an enrolled profile image, tap **Remove Picture**.

Enter user information and set permissions



- **ID**: The unique ID assigned to the user. The value generated automatically by the system is prefilled. You can also enter it manually.
- **Name**: Enter the user's name.
- **Account Level**: Select the user's account level.

Account level	Permissions by menu	
None	-	None
Administrator	All menus	All permissions
User Operator	**User**	Read, Write
Monitoring Operator	**Monitoring**, **Data**, **Dashboard**	Read, Write
T&A Operator	**TIME ATTENDANCE**	Read, Write
Visitor Operator	**VISITOR**	Read, Write

> When you set an administrator level, you can set a login ID and password so the user can log in to the BioStar X server.
>
> 
>

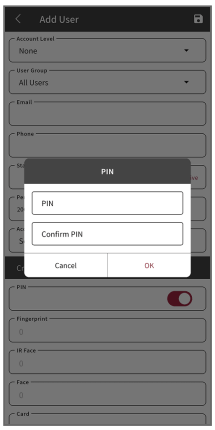
- **User Group**: Select the group the user belongs to.

- **Email**: Enter the user's email address.
- **Phone**: Enter the user's phone number.
- **Status**: Activate or deactivate the user account.
- **Period**: Set the period for using the user account. Set the start and end dates to use the user account only during that period.
- **Access Group**: Select the user's access group.

> **Info**
>
> - The available user ID values may vary depending on the **Settings** → **Server** menu's **User ID Type** option. For more information, refer to Server Detailed Settings.
> - The **T&A Operator** and **Visitor Operator** levels require a separate license. For more information on licensing policies, see License Policy.
> - For more information about adding and setting up access groups, refer to Manage Access Groups.

Enroll credential

When you register a user, you can also enroll a credential so the user can access the access control system. Users can enroll their fingerprints, faces, card information, and PINs as credentials. Credentials can be added or modified when registering or updating a user.

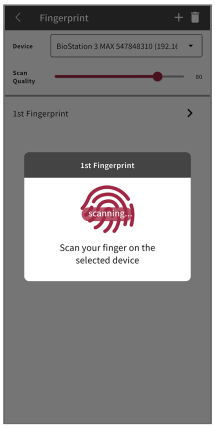


Enroll a PIN

You can enroll a PIN credential so the user can gain access by entering a PIN on the device.

1. Tap **Credential** → **PIN**.
2. When the PIN entry window appears, enter the desired PIN one by one.
3. When you finish entering it, tap **OK**.

> **Info**
>
> - The PIN must be 4~16 digits long and contain only numbers.
> - You can enroll a maximum of one PIN credential per user.



Enroll fingerprints

You can enroll the user's fingerprint as a means of authentication for access control. Enroll the user's fingerprint information through a device that supports fingerprint authentication.

Before enrolling fingerprints...

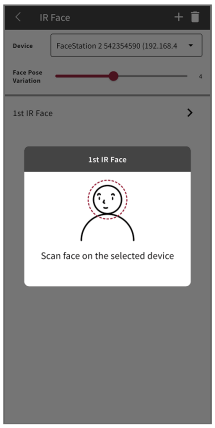
- Ensure that the user's fingerprint is clean and dry.
- Do not enroll fingerprints that are injured or blurry.

1. Tap **Credential** → **Fingerprint**.
2. Tap **Device** to select a device to enroll the fingerprint.
3. In the **Add Device** pop-up, select a device for fingerprint enrollment and tap **Yes**.
4. Use **Scan Quality** to adjust fingerprint quality. The default is **80**. Cannot enroll fingerprint information if it does not meet the configured quality level.
5. Tap + at the top right of the screen.
6. When **1st Fingerprint** appears in the list, tap it.
7. **scanning...** When the pop-up appears, scan the fingerprint on the selected device.
8. To verify the fingerprint, scan the same fingerprint again.
9. When fingerprint scanning is complete, tap **OK**.



Info

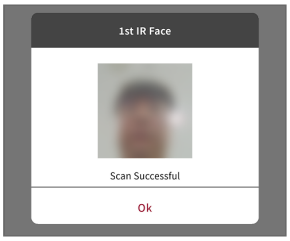
- The device list shows only fingerprint devices registered on the BioStar X server that support fingerprint enrollment.
- Repeat steps 5–9 to enroll additional fingerprints. You can enroll up to 10 fingerprints per user.
- To edit an enrolled fingerprint, tap the fingerprint credential and repeat the previous steps.



Enroll IR face

You can enroll the user's face as a means of authentication for access control. IR face enrollment is an authentication method that captures the user's face using an infrared camera.

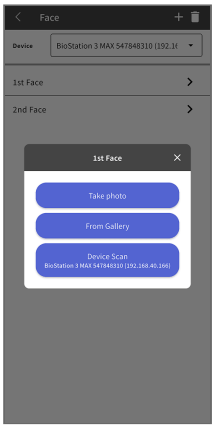
1. Tap **Credential** → **IR Face**.
2. Tap **Device**, select a device that supports IR face enrollment, and then tap **Yes**.
3. Adjust **Face Pose Variation** to set sensitivity for face position, angle, and distance. The default is **4**. Set it high to obtain a precise IR face template.
4. Tap + at the top right of the screen.
5. When **1st IR Face** appears in the list, tap it.
6. When the face enrollment pop-up appears, scan the face on the selected device. When the face is recognized, the face image appears in the pop-up.



7. To complete IR face enrollment, tap **OK**.

Info

- Devices that can enroll IR face are as follows:
  - FaceStation 2
  - FaceLite
- You can enroll up to 5 IR faces.
- If the face authentication rate is low, delete face information and enroll a new face.
- To edit an enrolled IR face, tap the IR face credential and repeat the previous steps.



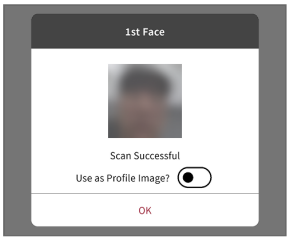
Face enrollment

You can enroll the user's face as a means of authentication for access control. Facial enrollment is an authentication method that captures the user's face with a camera. In the BioStar X mobile app, you can also import a face image saved on your mobile device or take a photo with the camera to enroll a face. You can also scan a face on a device that supports face recognition and enroll it.

1. Tap **Credential** → **Face**.
2. Tap **Device**, select a device that supports face enrollment, and then tap **Yes**.

   - If you do not select a device, you can import a photo from your mobile device or take a photo with the camera to enroll a face.
   - If you select a device, you can scan a face on that device and enroll it.

3. Tap + at the top right of the screen.
4. When **1st Face** appears in the list, tap it.
5. In the pop-up, select the face enrollment method you want.
   - **Take photo**: Take a photo with your mobile device's camera and enroll the face.
   - **From Gallery**: Select a photo saved on your mobile device and enroll the face.
   - **Device Scan**: Scan the face with the device selected in **Device**.
6. When the face is recognized, the face image appears in the pop-up.



7. To complete face enrollment, tap **OK**.

Info

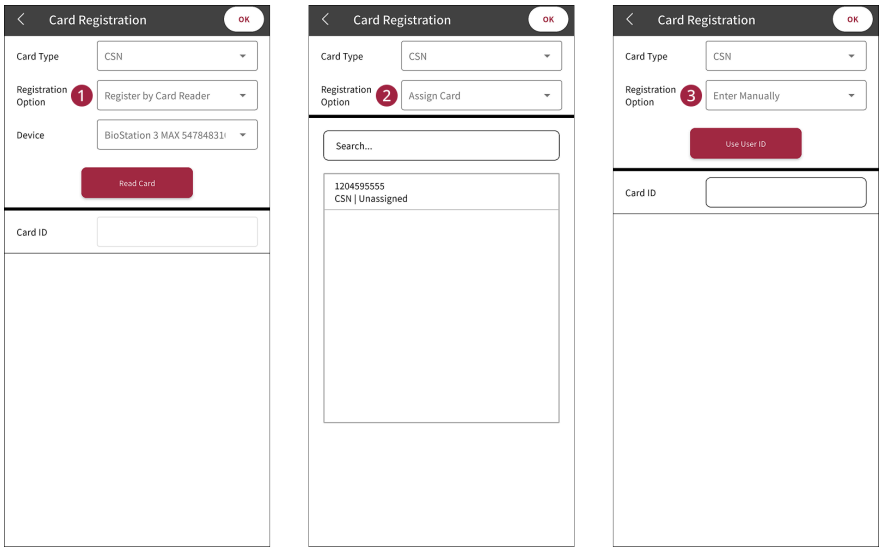
- To use the enrolled face image as the profile image, enable **Use as Profile Image?** option.
- When you take a face photo with your mobile device's camera or import a saved photo, access permission is required. Select Allow in the permission request pop-up to enroll the face photo.
- To edit an enrolled face, tap the face credential and repeat the previous steps.

Register access card

You can register a new access card or assign an registered access card as an authentication method for access. There are ways to register an access card: scan the card on a card reader, assign an already enrolled card, or enter the card number manually.

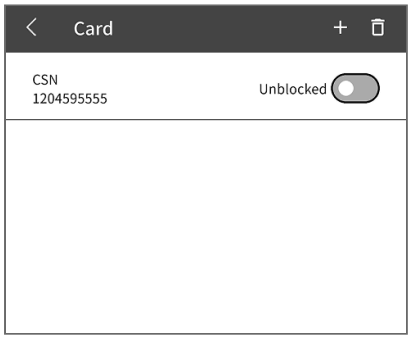
CSN card

1. Tap **Credential** → **Card**.
2. Tap + at the top right of the screen.
3. In **Card Type**, select **CSN** and tap **Yes**.
4. In **Registration Option**, select the registration method you want.



- 1 **Register by Card Reader**: Scan the card on a card reader to register it. In **Device**, select the device to read the card, and then tap **Read Card**. Hold the card up to the card reader to scan it. When the card is scanned successfully, the card number appears in **Card ID**.
- 2 **Assign Card**: Assign an registered access card to a user. Select one of the registered card numbers from the list.
- 3 **Enter Manually**: Enter the card number manually. Enter the card number in the **Card ID** input field. To use the user's ID as the card number, tap **Use User ID**.

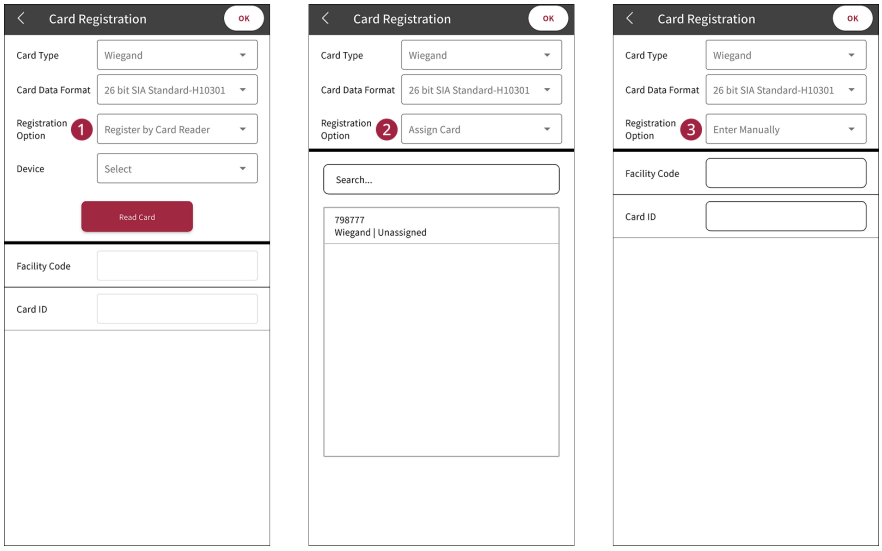
5. To complete card registration, tap **OK** at the top right of the screen.
6. When you return to the card list, the registered card number appears.



> **Info**
> To stop using an registered card, tap the card's toggle switch to set it to **Blocked**.

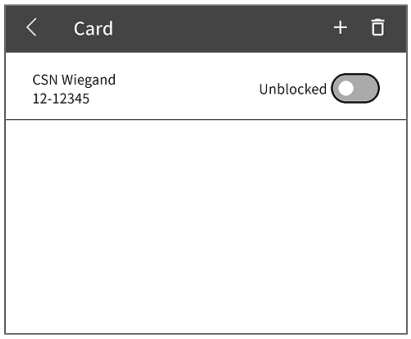
Wiegand card

1. Tap **Credential** → **Card**.
2. Tap + at the top right of the screen.
3. In **Card Type**, select **Wiegand** and tap **Yes**.
4. In **Card Data Format**, select the card format you want.
5. In **Registration Option**, select the registration method you want.



- 1 **Register by Card Reader**: Scan the card on a card reader to register it. In **Device**, select the device to read the card, and then tap **Read Card**. Hold the card up to the card reader to scan it. When the card is scanned successfully, the card number appears in **Facility Code** and **Card ID**.
- 2 **Assign Card**: Assign an registered access card to a user. Select one of the registered card numbers from the list.
- 3 **Enter Manually**: Enter the card number manually. Enter the card number in the **Facility Code** and **Card ID** input fields.

6. To complete card registration, tap **OK** at the top right of the screen.
7. When you return to the card list, the registered card number appears.



Info

To stop using an registered card, tap the card's toggle switch to set it to **Blocked**.

Smart Card

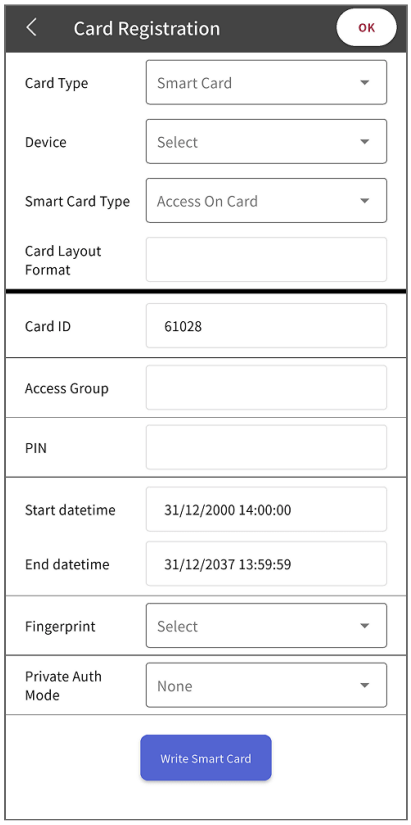
Info

- To issue a smart card, the correct card type must be set. For more information on card formats, refer to Set Smart Card Format.
- The user information stored on the smart card uses information stored in **BioStar X**. Failure to store updated user information may result in incorrect information being stored on the smart card. Additionally, if the updated user information is not synchronized with the device, the device may fail to perform authentication.
- To add PIN authentication information, enroll a PIN first. For more information on enrolling a PIN, refer to Enroll a PIN.
- To add fingerprint credential information, enroll a fingerprint first. For more information on fingerprint enrollment, refer to Enroll fingerprints.

Access on Card

User information (card ID, PIN, access group, period, fingerprint template, face template, and private authentication mode) can be stored on the card.

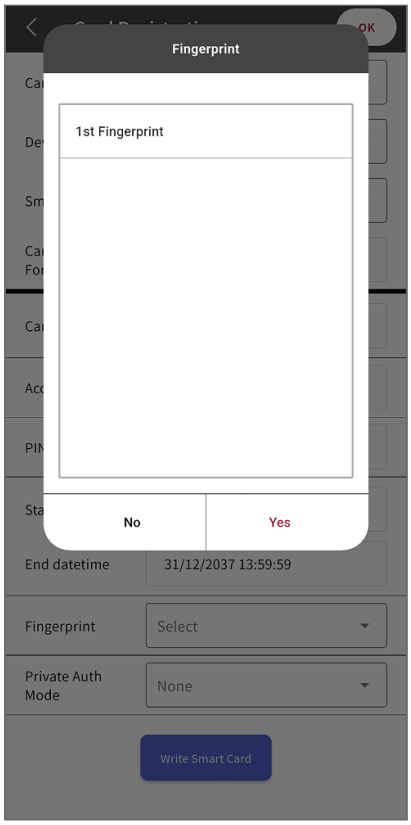
1. Tap **Credential** → **Card**.
2. Tap + at the top right of the screen.
3. In **Card Type**, select **Smart Card** and tap **Yes**.



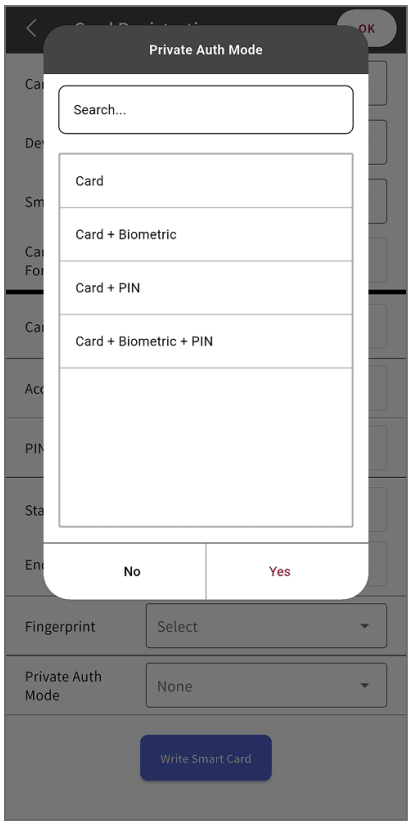
4. In **Device**, select the device to register the card, and then tap **Yes**.

> The card layout set on the selected device appears in **Card Layout Format**.

5. (Optional) To add fingerprint authentication, tap **Figerprint** and select an enrolled fingerprint.



6. (Optional) To add private authentication mode, tap **Private Auth Mode** and select the authentication method you want.

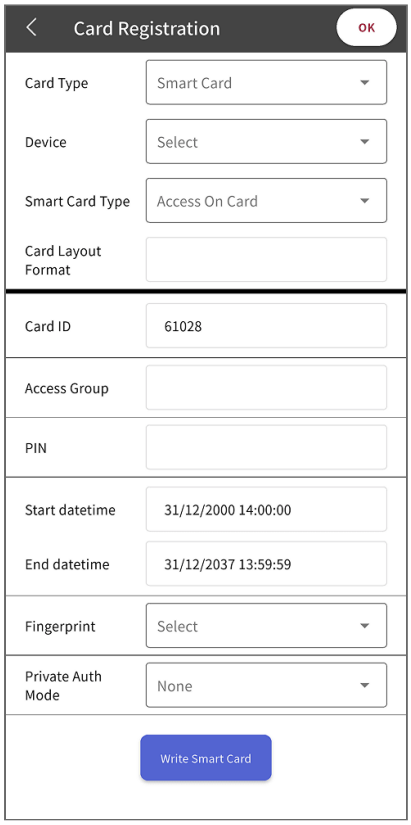


7. To register the card, tap **Writes Smart Card**.
8. Hold the card up to the selected device to register the user information on it.
9. When card registration is complete, tap **OK** at the top right of the screen.

Secure Credential Card

User information (card ID, PIN, fingerprint template, and face template) can be stored on the card.

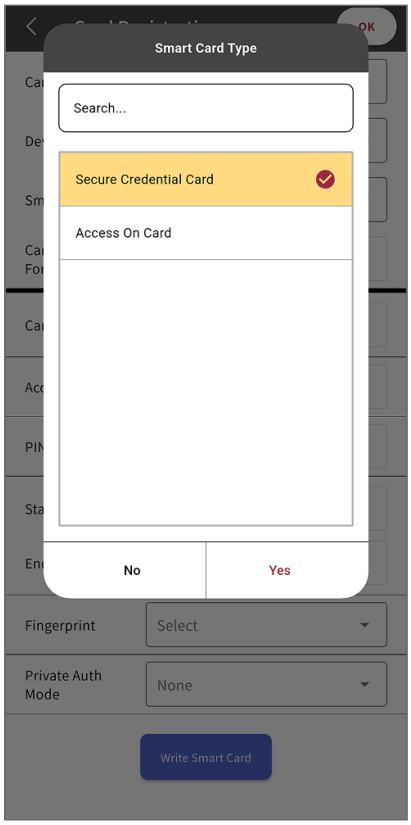
1. Tap **Credential** → **Card**.
2. Tap + at the top right of the screen.
3. In **Card Type**, select **Smart Card** and tap **Yes**.



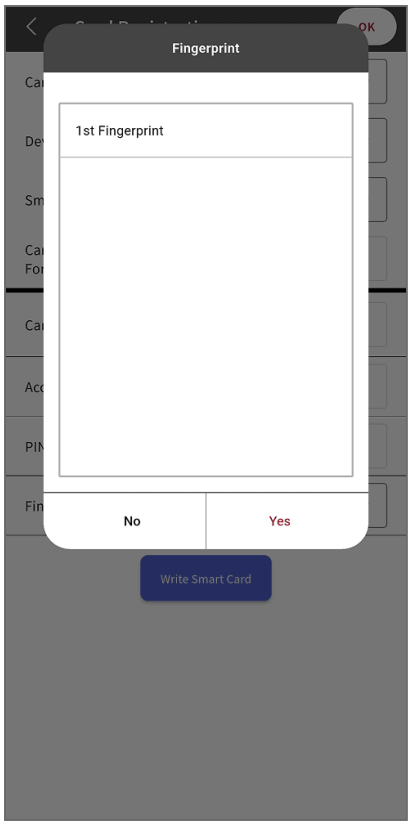
4. In **Device**, select the device to register the card, and then tap **Yes**.

> The card layout set on the selected device appears in **Card Layout Format**.

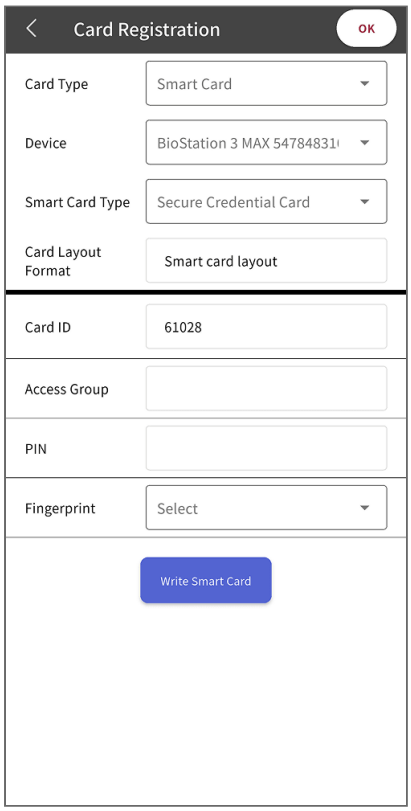
5. Tap **Smart Card Type**, select **Secure Credential Card**, and then tap **Yes**.



6. (Optional) To add fingerprint authentication, tap **Figerprint** and select an enrolled fingerprint.



7. To register the card, tap **Writes Smart Card**.



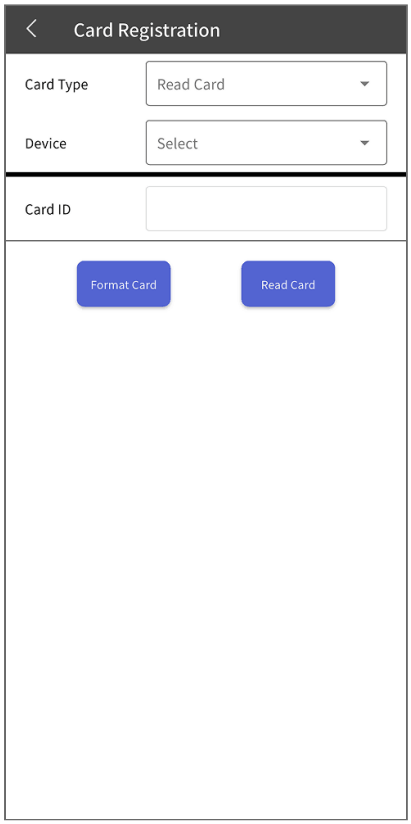
8. Hold the card up to the selected device to register the user information on it.

9. When card registration is complete, tap **OK** at the top right of the screen.

Read Card / Format

You can format smart cards and rewrite information.

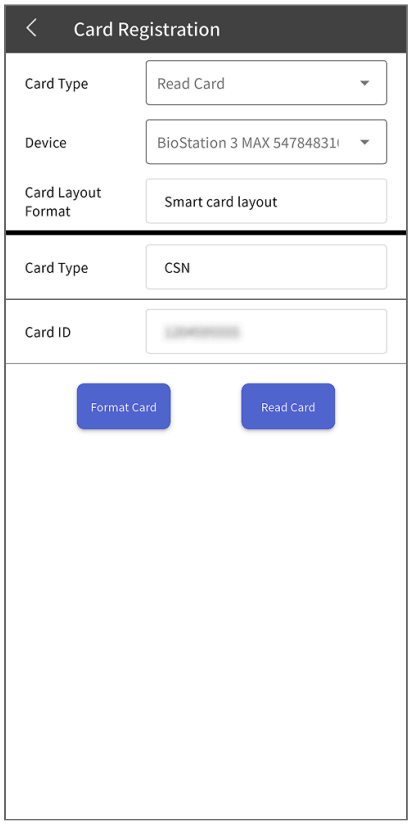
1. Tap **Credential** → **Card**.
2. Tap ＋ at the top right of the screen.
3. In **Card Type**, select **Read Card** and tap **Yes**.



4. In **Device**, select the device to read the card, and then tap **Yes**.

> The card layout set on the selected device appears in **Card Layout Format**.

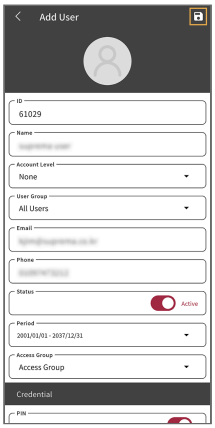
5. Tap **Read Card** and hold the card up to the device to scan it.



6. After you check the card information, tap **Format Card** to format the card.

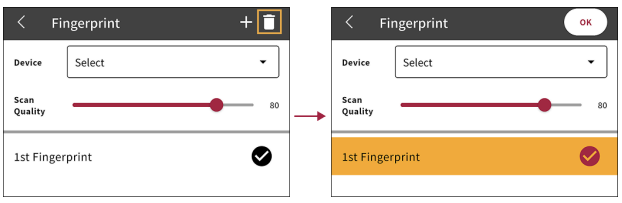
> **Info**
> Custom smart cards cannot be formatted.

Complete user registratioin



After you set the user's basic information, permissions, and credentials, tap at the top right of the screen to complete user registration.

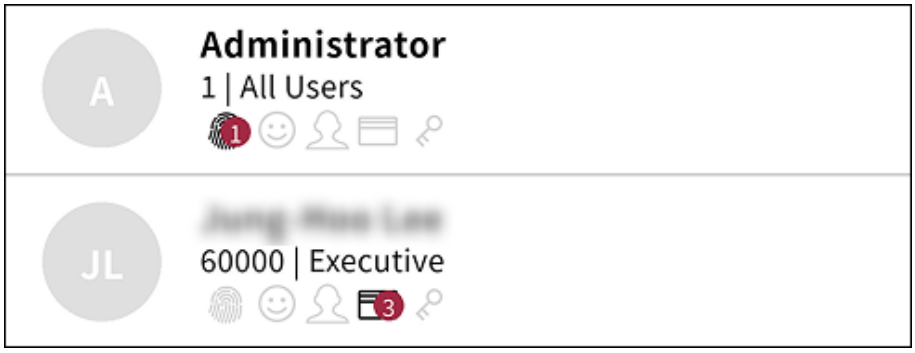
- In the **Credential** section, you can check the number of enrolled credentials for each credential.
- To delete a enrolled credential, tap the credential to delete, then tap at the top right of the screen. Select the credential to delete, then tap **OK**.



> **Info**
> For more information about registering and managing users in BioStar X, refer to User.

Check user information

You can check registered users in the user list. Each user includes the following information.

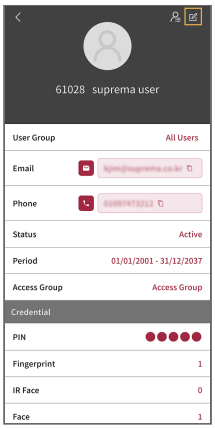


- User name
- User ID | User group
- Enrolled credential information: Fingerprint / IR face / Face / Card / PIN

Edit and Delete Users

Edit user information when a user's affiliation changes or permissions need to be adjusted. Learn how to delete users when they leave the company or their contracts end to enhance security.

Edit user



You can edit user information, permissions, and credentials from the User Details screen.

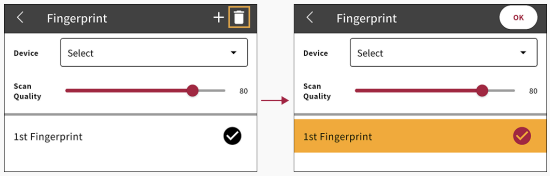
1. On the app home screen, tap **USER**.

   > You can also access it through the side menu. Tap ☰ → **User**.

2. Tap the user to edit in the user list.
3. In User Details, tap ✎ at the top right of the screen.
4. In **Edit User**, you can edit basic user information, change permissions, and manage credentials.
5. To save changes, tap 💾 at the top right of the screen.

Info

- For more information on user information, permissions, and credentials, refer to Register Users.
- To temporarily deactivate a user, tap the toggle switch in **Status** and set it to **Inactive**. Inactive users are blocked from access.
- To delete a enrolled credential, tap the credential to delete, then tap at the top right of the screen. Select the credential to delete, then tap **OK**.



Delete users



If you need to delete a user, follow these instructions.

1. On the app home screen, tap **USER**.

   You can also access it through the side menu. Tap ☰ → **User**.

2. Tap at the top right of the user list.
3. Select the user to delete. You can select more than one user.
4. Tap **OK** at the top right of the screen.
5. When the confirmation message appears, tap **Yes**.

The selected user is deleted. Deleted users cannot be recovered.

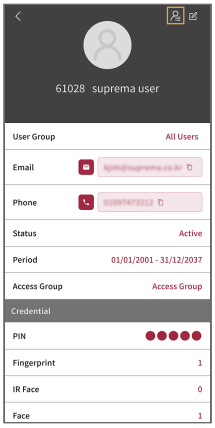
Info

The administrator account with ID `1` cannot be deleted.

View User Log Events

View a user's access history to check for abnormal access or access outside authorized hours. Filter log events to easily find history for a desired period and location.

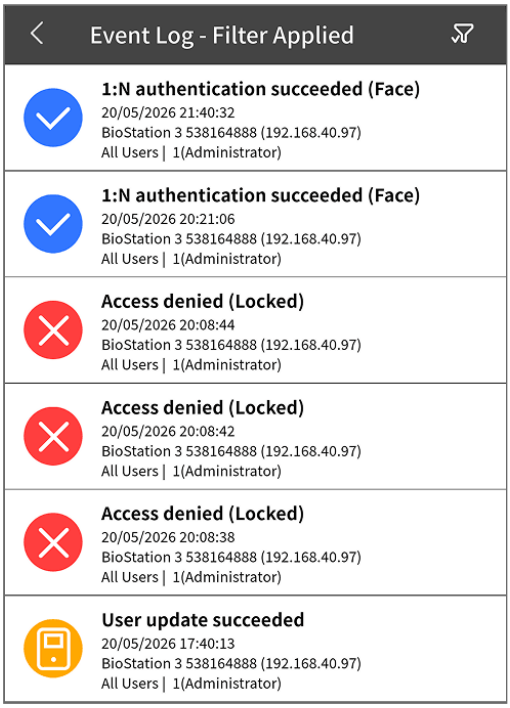
View user access history



1. On the app home screen, tap **USER**.

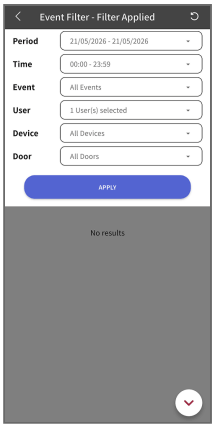
   > You can also access it through the side menu. Tap ☰ → **User**.

2. Tap the user whose log events you want to view in the user list.
3. Tap  in the upper right in user details.
4. In **Event Log**, you can view the user's access history.



The latest log events are displayed first, and you can review the access location and event details.

Filter log events



You can filter a user's log events by various conditions, such as date and time, event type, and access location.

1. Tap  in the upper right of Event Log.
2. When the filter criteria appear, set the desired criteria.
   - **Period**: Set the period when the log event occurred.
   - **Time**: Set the time when the log event occurred.
   - **Event**: Select the log event type. For example, select access authentication success or access authentication failure.
   - **User**: View log events for users other than the current user.

- **Device**: Select the device where the log event occurred.
- **Door**: Select the door where the log event occurred.

3. To filter log events with the selected criteria, tap **Apply**.

> **Info**
>
> To reset the filter conditions, tap → in the upper right corner of the screen.

Search and Filter Users

When the user list is long and hard to search, use search and filtering to find users quickly.

User search



You can search by user ID, name, or email address.

1. On the app home screen, tap **USER**.

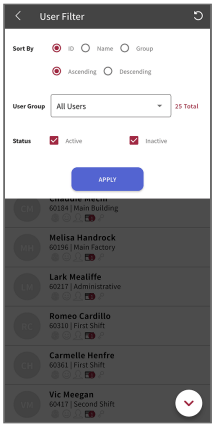
> You can also access it through the side menu. Tap ☰ → **User**.

2. Tap 🔍 at the top of the user list.
3. Enter a search term in the search field. You can search by combining the user ID, name, and email address.
4. After you finish entering the search term, tap 🔍.

Users that match the search term appear in the search results. In the search results, tap the user you want to open the user details.

> **Info**
>
> - Recent search history appears below the search input field. Tap a recent search entry to search again with that term.
> - To close the search input field, tap ✕.

Filter the user list



Filter the user list by various conditions to find users quickly.

1. On the app home screen, tap **USER**.

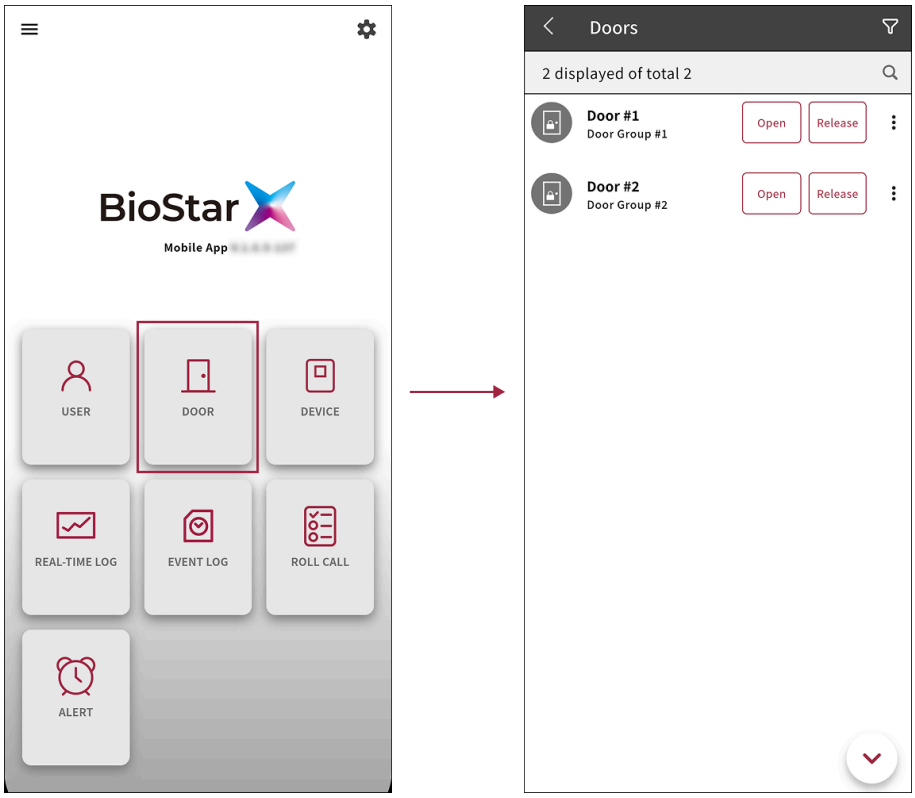
   > You can also access it through the side menu. Tap ☰ → **User**.

2. Tap the filter icon at the top of the user list.
3. Set the desired conditions in **User Filter**.
   - **Sort By**: Select ascending or descending order by user ID, name, or group.
   - **User Group**: Select a specific user group to show only users in that group.
   - **Status**: To show only active users, select **Active**. To show only inactive users, select **Inactive**.
4. To filter the user list with the selected conditions, tap **Apply**.

> **Info**
>
> To reset the filter conditions, tap the filter icon → the reset icon in the upper right corner of the screen.

Manage Doors

Remotely control doors to manage access conveniently. Check door status in real time, and change door settings as needed. You can also view log events related to the door.



Info

For more information on monitoring and managing doors in BioStar X, refer to the following document.

- Monitor Doors
- Manage Doors

Remote Control of Doors

In the door list, check each door's status in real time and control it as needed. During normal operation, manage doors with basic control features. Use additional control options for stronger security or emergencies.

Tap **DOOR** on the app home screen. The list of doors registered in BioStar X appears.

Info

You can also access it through the side menu. Tap ☰ → **Door**.

Check door status

In the door list, the status icon lets you see abnormal conditions for the device assigned to each door at a glance. The door status icon indicates whether the door is open, closed, or has an alarm.



Status Icon	Description
	The door has a problem. Abnormal status: The system lost connection to the door's assigned device, or a Multi Communications Server or synchronization error occurred.
	The door is open.
	The door is closed.
	An alarm has occurred at the door.
	An APB alarm has occurred at the door.

Open/Lock door

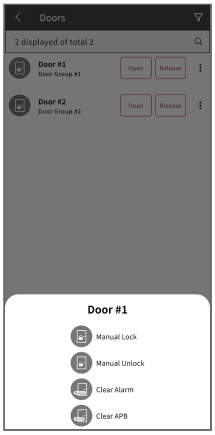


The remote door control feature lets you open or lock door to allow or block access.

- **Open**: Temporarily opens the door to allow access. The door closes automatically after the set time.
- **Release**: Sets the door to allow access only for authenticated users. The door status changes according to the schedule set for the door.

> **Info**
>
> For more information on how to temporarily open a door and set the auto-close time, see **Open** → **Open Time** in Register Door.

Additional control



When stronger security is needed or access must be controlled for a long period, manually lock or unlock the door without a time limit. You can also clear the triggered alarm.

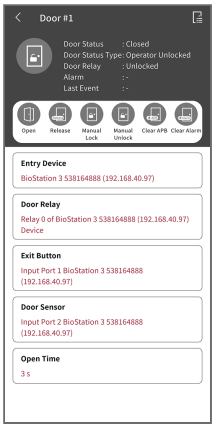
Tap ⋮ at the far right of the door to use additional control options.

- **Manual Lock**: Manually locks the door to block access. This feature locks the door without a time limit. In this state, access is blocked for all users.
- **Manual Unlock**: Manually unlocks the door to allow access. This feature unlocks the door without a time limit. In this state, access is allowed for all users.
- **Clear Alarm**: Clear the alarm that occurred at the door.
- **Clear APB**: Clear APB status for all users at the selected door.

> **Info**
>
> After you manually lock or unlock a door, the door status does not change automatically. For security, use **Release** to make the door operate according to the set schedule.

View Door Details

Select a door to view the current status and configured devices. If a problem occurs, control it immediately or view recent activity logs.



View the door's status information, remote control feature, device information assigned to the door, and open time.

1. Tap **DOOR** on the app home screen.

   > You can also access it through the side menu. Tap ☰ → **Door**.

2. Tap the door whose details you want to view in the door list.

Door status information

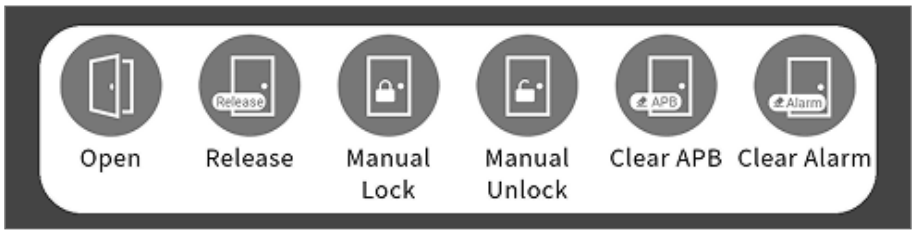
View the door's current status in real time.



- **Door Status**: Shows whether the door is open or closed.
- **Door Status Type**: Shows the door status type. For example, Normal, Operator Unlocked, and Operator Locked.
- **Door Relay**: Shows the status of the relay connected to the door.
- **Alarm**: Shows alarm events that occurred at the door.
- **Last Event**: Shows the date, time, and event type of the last event that occurred at the door.

Remote control feature

Control the door remotely to manage access.



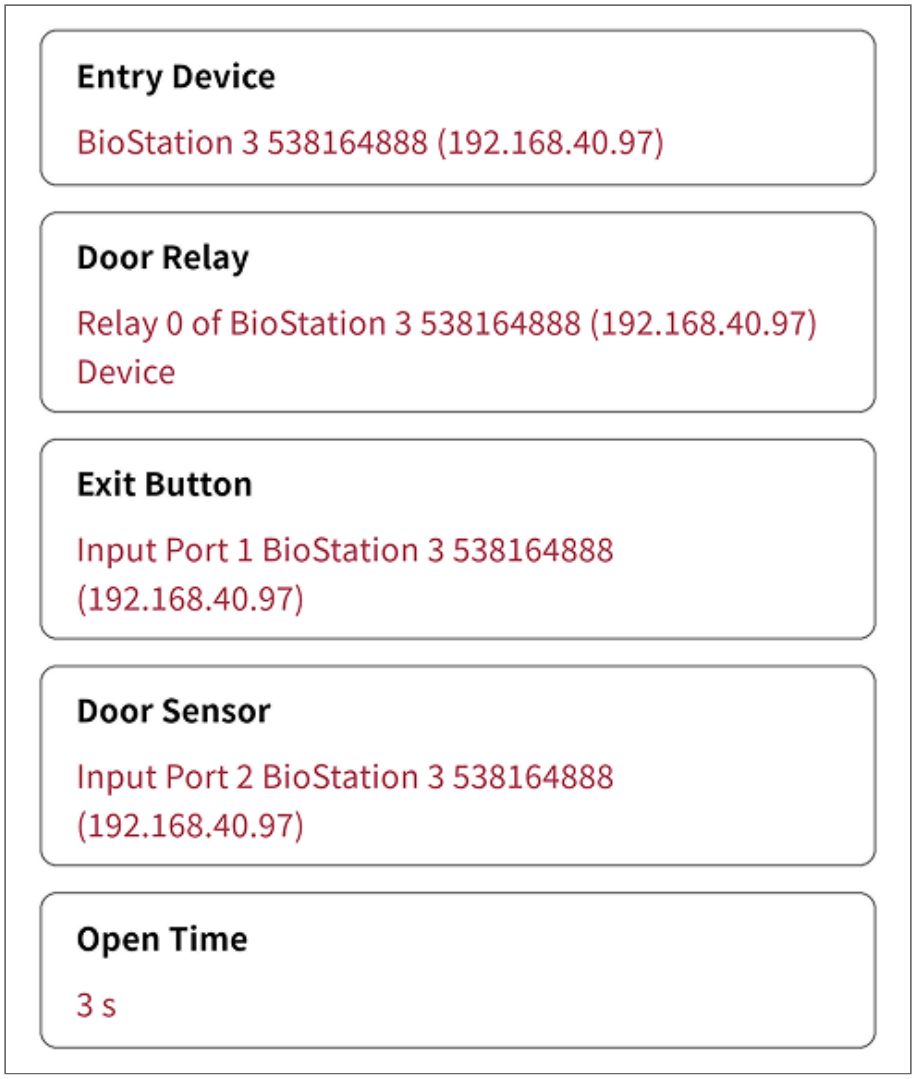
- **Open**: Temporarily opens the door to allow access. The door closes automatically after the set time.
- **Release**: Sets the door to allow access only for authenticated users. The door status changes according to the schedule set for the door.
- **Manual Lock**: Manually locks the door to block access. This feature locks the door without a time limit. In this state, access is blocked for all users.
- **Manual Unlock**: Manually unlocks the door to allow access. This feature unlocks the door without a time limit. In this state, access is allowed for all users.
- **Clear APB**: Clear APB status for all users at the selected door.
- **Clear Alarm**: Clear the alarm that occurred at the door.

Info

- The time the door stays open temporarily before it closes automatically is shown in **Open Time** below.
- After you manually lock or unlock a door, the door status does not change automatically. For security, use **Release** to make the door operate according to the set schedule.

Door device information

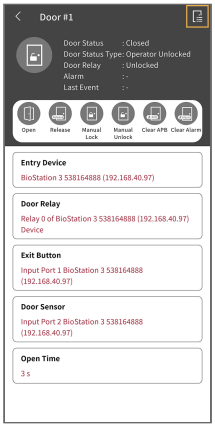
View the device information assigned to the door.



- **Entry Device**: The device information assigned as the entry device.
- **Door Relay**: The relay information that operates as the door lock.
- **Exit Button**: The port information of the device used as the exit button.
- **Door Sensor**: The port information of the device assigned as the sensor that detects the door opening and closing.
- **Open Time**: The time the door stays open after it is opened temporarily before it closes automatically.

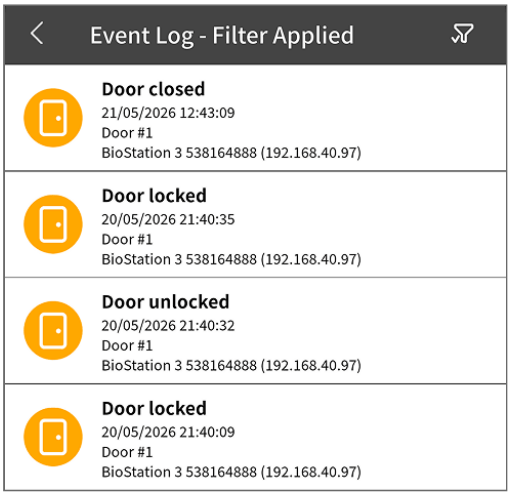
> **Info**
> For more information on the **Open Time** setting, see **Open** → **Open Time** in Register Door.

View door log events

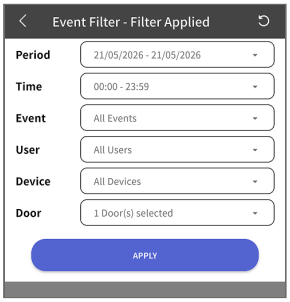


View log events that occurred at the door and check events such as access attempts and alarms.

1. On the Door Details screen, tap in the upper right corner.



2. To filter door log events, tap in the upper right corner of the screen.



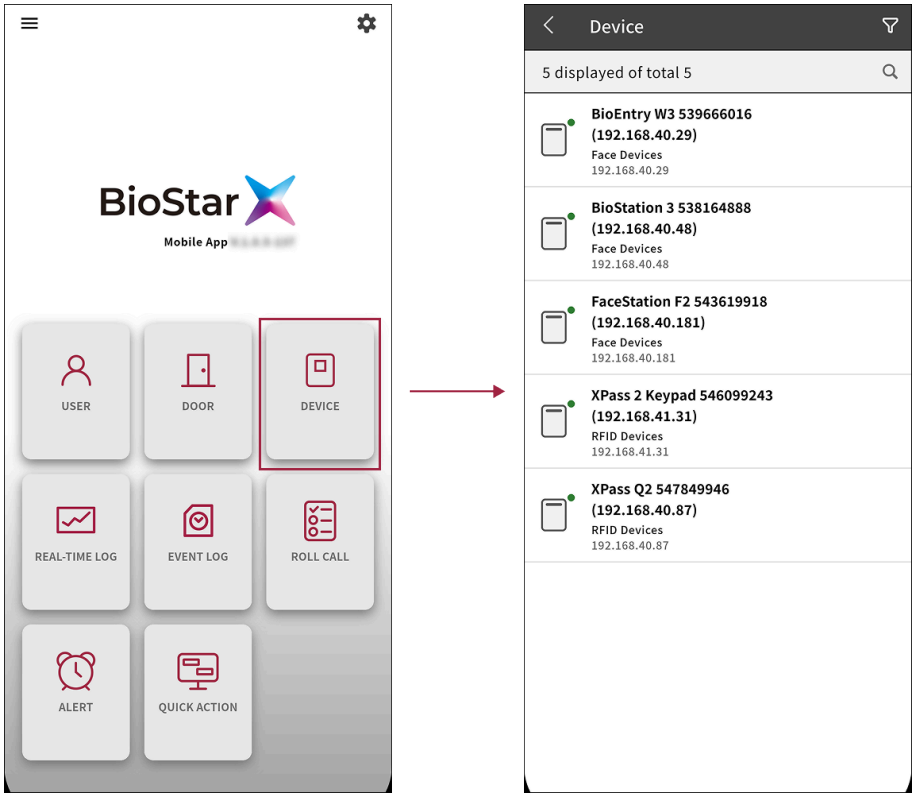
   - **Period**: Set the period when the log event occurred.
   - **Time**: Set the time when the log event occurred.
   - **Event**: Select the log event type. For example, select access authentication success or access authentication failure.
   - **User**: Select the user who triggered the log event.
   - **Device**: Select the device where the log event occurred.
   - **Door**: View log events for doors other than the current door.

3. When the filter criteria appear, set the desired criteria.
4. To filter log events with the selected criteria, tap **Apply**.

> **Info**
>
> To reset the filter conditions, tap → in the upper right corner of the screen.

Manage Devices

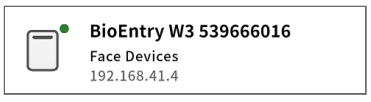
In the device list, check each device's status and remotely release locked devices. From the app home screen, tap **DEVICE**.



Info

- The mobile app does not allow adding or editing devices.
- You can also access it through the side menu. Tap ☰ → **Device**.

Check device information



Each device in the device list includes the following information.

- Device name
- Device group name (shows as **All Devices** if not in a group)
- Device IP address

Check device status

Check device status from the status icons in the device list.

Status Icon	Description
	The device is connected properly.
	The device is off or disconnected.

Info
Pull down the device list to refresh device status.

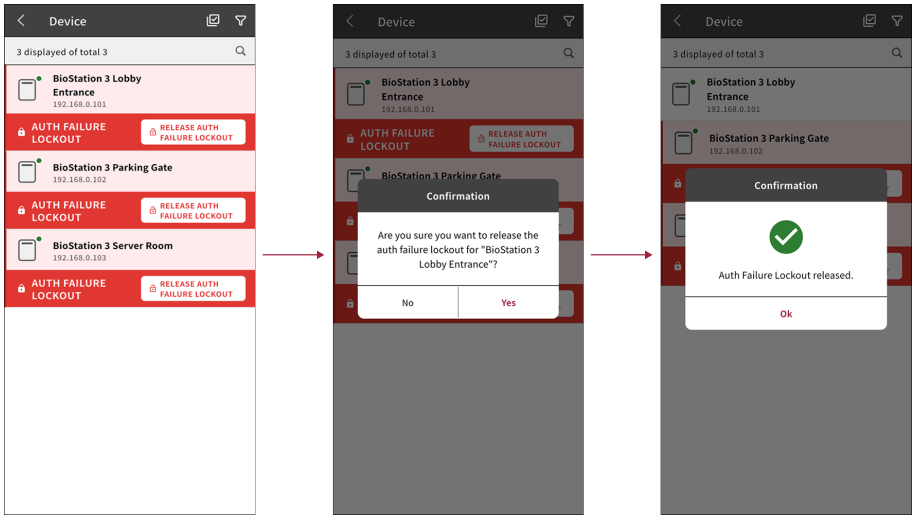
Release authentication failure lockout

If consecutive authentication failures lock a device, use the mobile app to release the lockout.

Info
For more information on the authentication failure lockout setting in **BioStar X**, see Authentication Settings.

Release lockout for an individual device

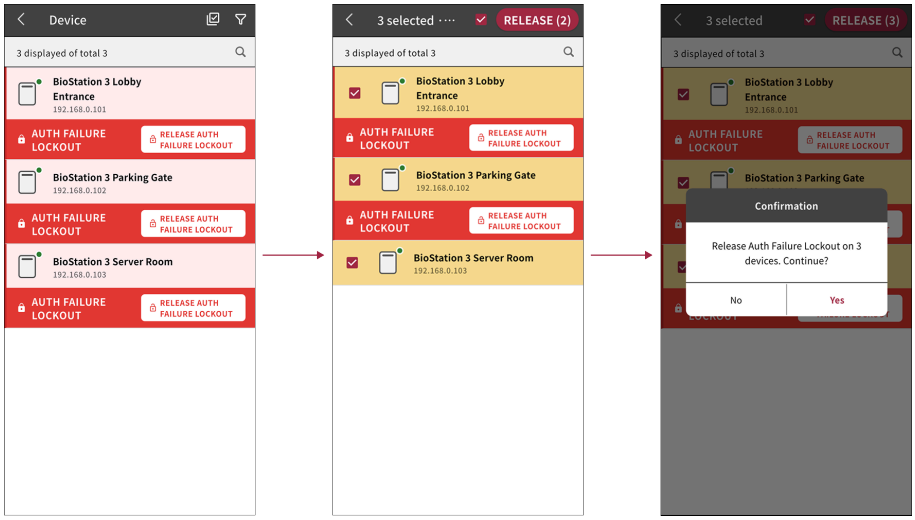
Release authentication failure lockouts for devices in the device list.



1. In the device list, find devices labeled **AUTH FAILURE LOCKOUT**.
2. Tap **RELEASE AUTH FAILURE LOCKOUT** to release the lockout.
3. When the confirmation message appears, tap **Yes**.
4. When the lockout release success message appears, tap **OK**.

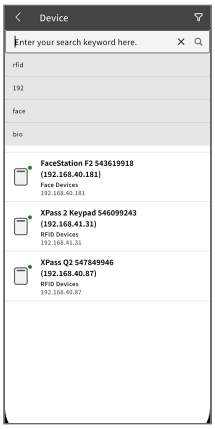
Release lockout for multiple devices

Release lockouts for multiple devices labeled **AUTH FAILURE LOCKOUT** at the same time.



1. Tap ☑ at the top right of the device list.
2. Select at least one device labeled **AUTH FAILURE LOCKOUT**.
3. Tap **RELEASE** in the top right.
4. When the confirmation message appears, tap **Yes**.
5. When the lockout release success message appears, tap **OK**.

Device search



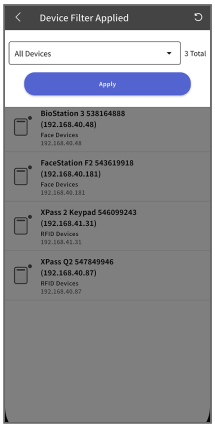
Search by device name, group, or IP address.

1. Tap 🔍 at the top of the device list.
2. Enter a search term in the search field. Search by device name, group name, or IP address.
3. After you finish entering the search term, tap 🔍.

Devices that match the search term appear in the results.

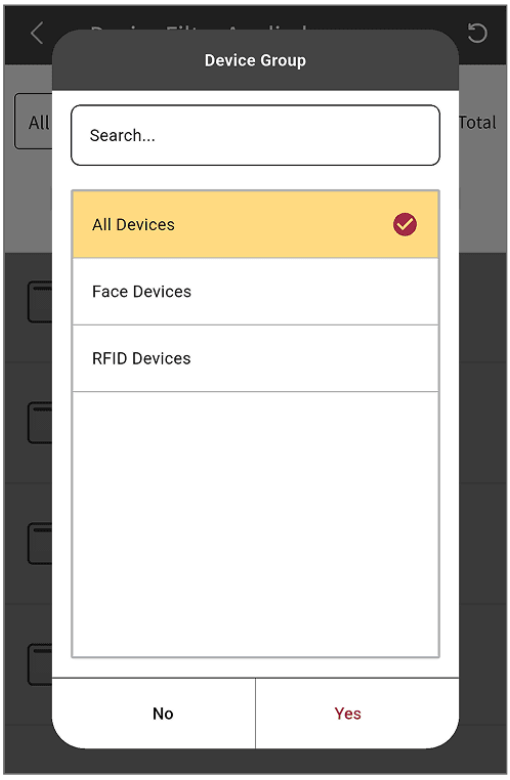
> **Info**
>
> - Recent search history appears below the search input field. Tap a recent search entry to search again with that term.
> - To close the search input field, tap ✕.

Filter the device list



Filter the device list by device group.

1. Tap at the top of the device list.
2. Tap **All Devices**.
3. Select the desired group from the device group list.



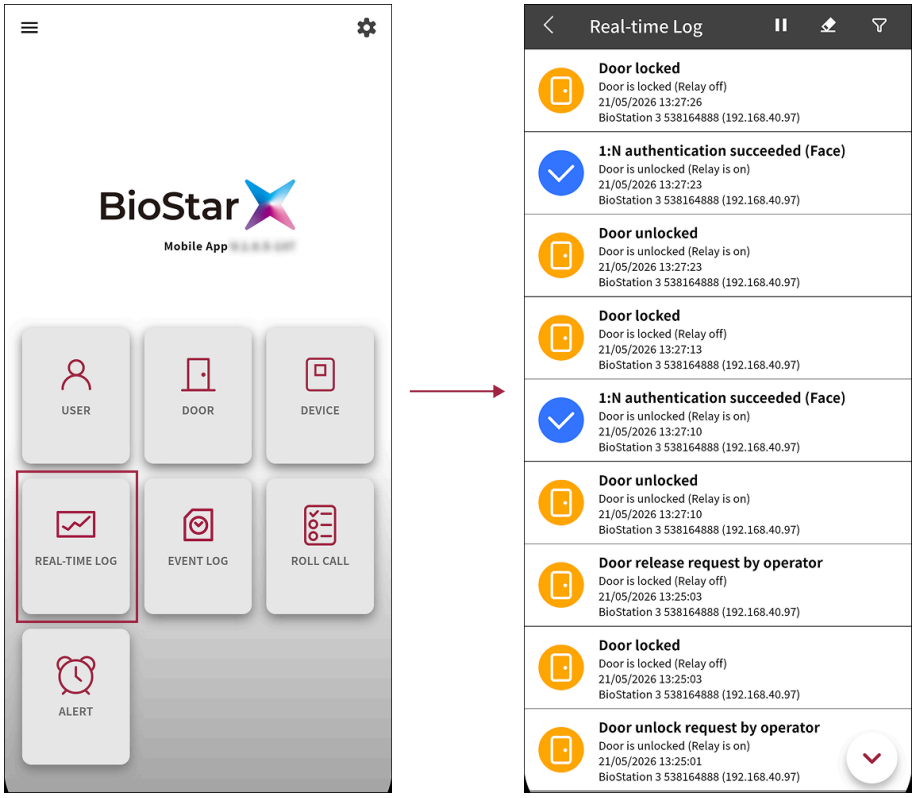
4. After selecting a device group, tap **Yes**.
5. Tap **Apply** to filter the device list based on the selected criteria.

The list shows devices in the selected device group.

> **Info**
>
> To reset the filter conditions, tap → in the upper right corner of the screen.

Real-time Log Monitoring

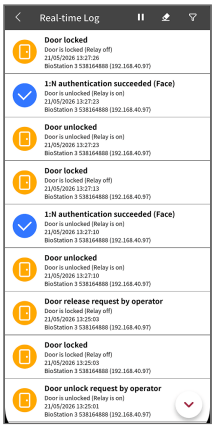
View events that occur on the BioStar X server in real time. On the app home screen, tap **REAL-TIME LOG**.



Use the **REAL-TIME LOG** feature in the following situations.

- Monitor access attempts during commute hours
- Check currently received events in real time

View real-time logs



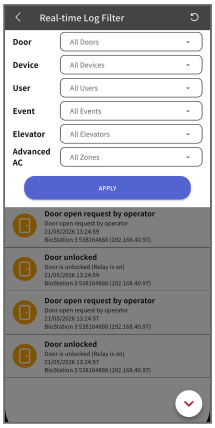
On the app home screen, tap **REAL-TIME LOG**. When you first open the Real-time Log (**Real-time Log**) screen, the list is empty.

- When a new event occurs, it is automatically added to the list in real time. There is no limit to the number of rows in the list, and new events are added at the top.
- To pause real-time event reception, tap ⏸ in the upper right corner of the screen. When paused, new events are not added to the list, but they are queued in the background. To resume real-time event reception, tap ▶. Events added to the queue appear before newer events.
- To clear the real-time log list, tap ⌫ in the upper right corner of the screen. The log list is cleared, and new events are added in real time as they occur.
- Filter the real-time log list to show only related logs such as certain events, users, doors, or devices. For more information, refer to View only certain logs.

Info

- If you move to another menu and return to **Real-time Log**, the log list is cleared, and new logs are added in real time as they occur.
- The date and time shown in the logs follow the BioStar X server locale settings. For more information on date and time display format settings in BioStar X, refer to Configure Preferences.
- You can also open the Real-time Log screen by tapping Side menu (☰) → **Monitoring** → **Real-time Log**.

View only certain logs



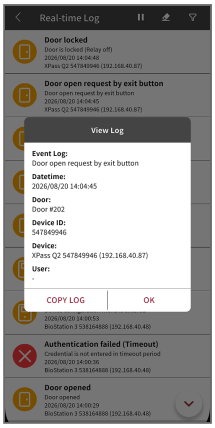
Filter the Real-time Log list to show only related logs such as certain events, users, doors, or devices.

1. Tap in the upper right corner of the screen.
2. Set the following filter conditions to show only the logs you want.
   - **Door**: A certain door (for example, the first-floor main entrance)
   - **Device**: A certain device (for example, an event generated by a certain access control device)
   - **User**: A certain user (for example, access records for a VIP user)
   - **Event**: A certain event type (for example, facial authentication failure, intrusion alarm, and more)
   - **Elevator**: A certain elevator (for example, an elevator on a certain floor)
   - **Advanced AC**: Certain advanced access control events (for example, anti-passback, fire alarm, scheduled open/lock, and more)
3. To filter the log list with the set conditions, tap **Apply**.

Info

- To reset the filter conditions, tap → in the upper right corner of the screen.
- Elevator and advanced access control require an **Essential** or higher license. For more information on the licensing policy, see License Policy.

View log details



Tap a log entry to view detailed information about that log.

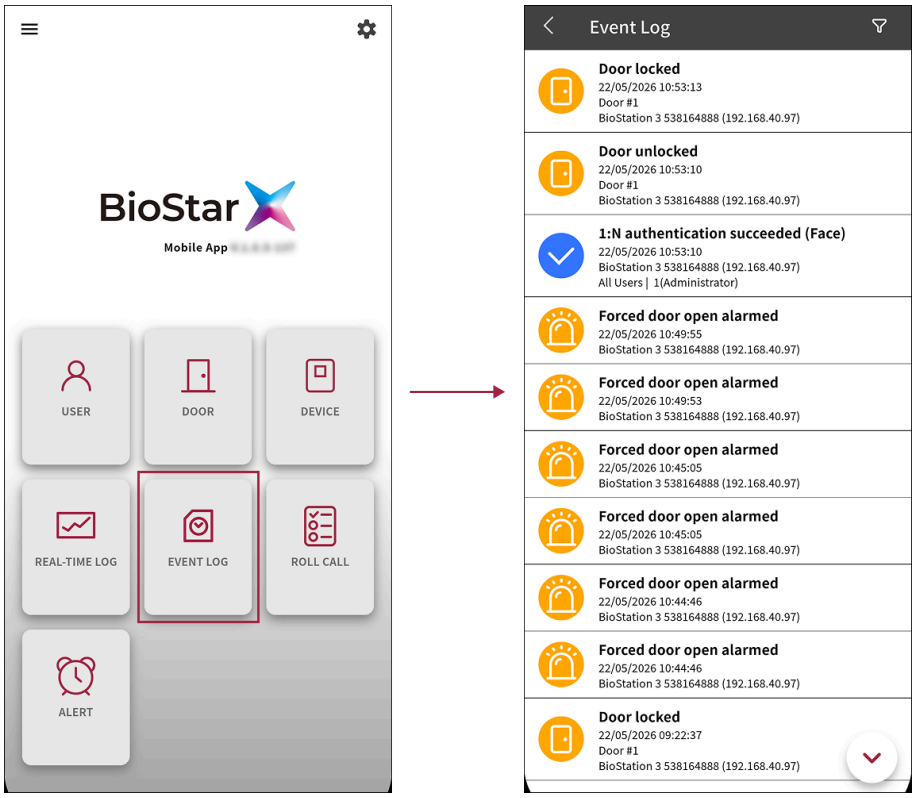
- **Event Log**: The event type. Shows which type of event occurred.
- **Datetime**: The date and time the event occurred.
- **Door**: The door where the event occurred.
- **Device ID**/**Device**: The ID and name of the device where the event occurred.
- **User**: The user who triggered the event. For example, for an access authentication event, the user who attempted access appears.

Tap the buttons at the bottom of the details popup to perform the following actions.

- Tap **COPY LOG** to copy event details to the clipboard.
- To close the details popup, tap **OK**.

View Past Event Logs

View past logs to check access history that occurred during a specific period and at a specific location. Filter logs to easily find events that match your desired conditions.



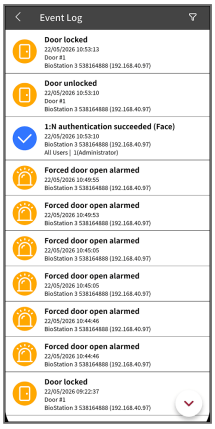
Use the **EVENT LOG** feature in the following situations.

- Check a specific user's past access history
- Track security event history within a specific period
- Audit and report access control

Differences from real-time logs

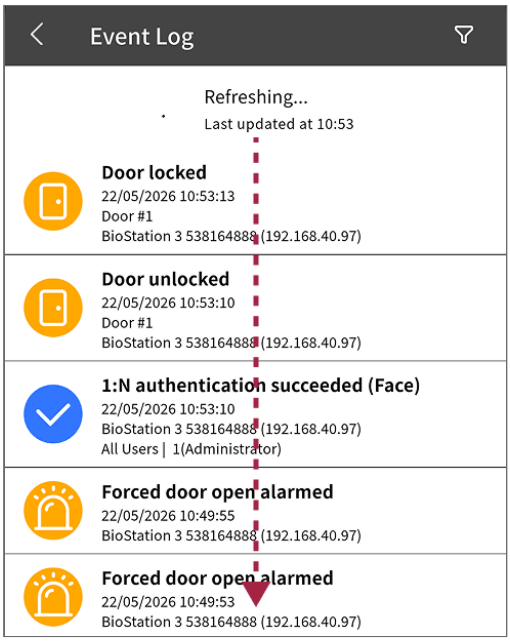
- **Real-time logs**: Monitor current events immediately. Real-time logs are useful when you need to understand the current situation and respond immediately.
- **Past logs**: Search and view event history for a specific period.

View past event logs



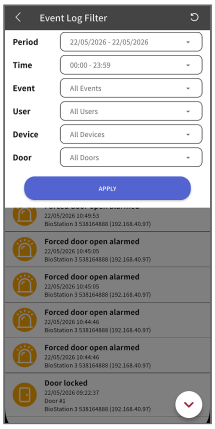
From the app home screen, tap **EVENT LOG**.

- Each log shows the event type, time, door/device, and user information.
- Pull down the log list to refresh it and show the latest logs.



> **Info**
>
> - The date and time shown in the logs follow the BioStar X server locale settings. For more information on date and time display format settings in BioStar X, refer to Configure Preferences.
> - You can also open the Event Log screen by tapping the side menu (☰) → **Monitoring** → **Event Log**.

View only specific logs



Filter the log list to show only logs related to a specific event, user, door, or device.

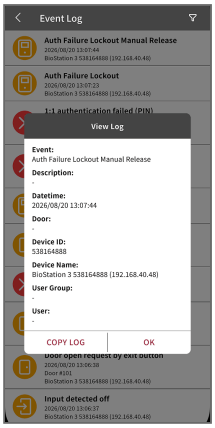
1. Tap the filter icon in the upper right corner of the screen.
2. Set the following filter conditions to show only the logs you want.
   - **Period**: Set the event period
   - **Time**: Set the event time
   - **Event**: Select a specific event type (for example, facial authentication failure, intrusion alarm, and more)

- **User**: Select a specific user (for example, a VIP user's access history)
- **Device**: Select a specific device (for example, an event from a specific access control device)
- **Door**: Select a specific door (for example, the first-floor main entrance)

3. To filter the log list with the set conditions, tap **Apply**.

> **Info**
>
> To reset the filter conditions, tap → in the upper right corner of the screen.

View log details



Tap the log you want in the log list to view its details.

- **Event**: The type of event that occurred. (e.g., access authentication success, access authentication failure, alarm triggered, etc.)
- **Description**: A description of the event.
- **Datetime**: The date and time the event occurred.
- **Door**: The door where the event occurred.
- **Device ID**/**Device Name**: The ID and name of the device where the event occurred.
- **User Group**: The name of the user group that triggered the event.
- **User**: The user who triggered the event.

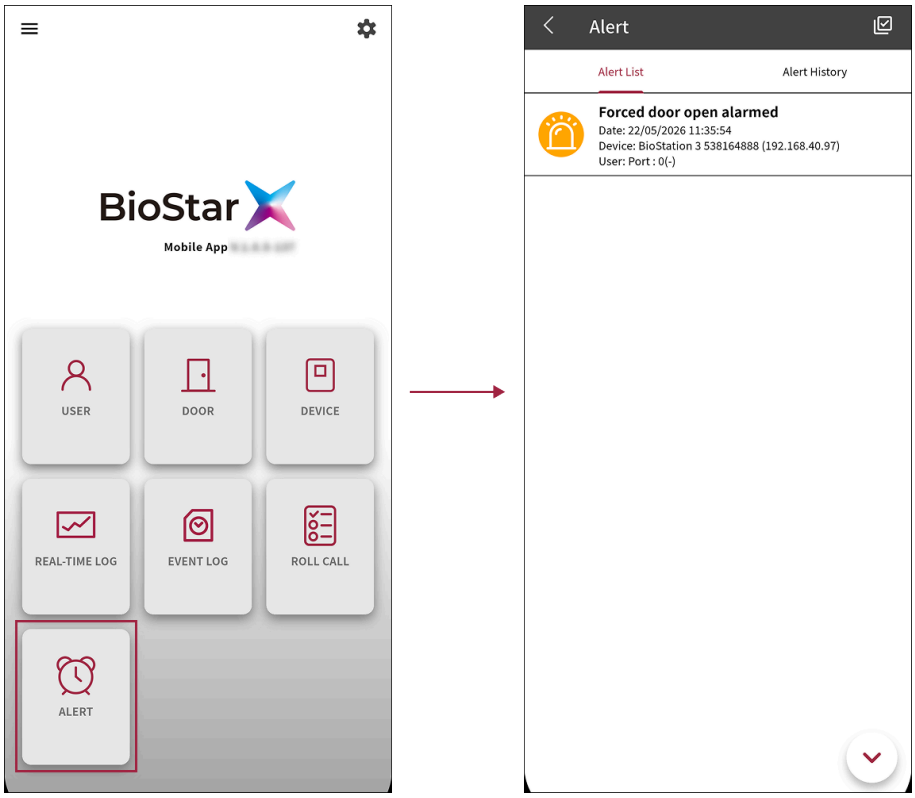
Tap the buttons at the bottom of the details popup to perform the following actions.

- Tap **COPY LOG** to copy event details to the clipboard.
- To close the details popup, tap **OK**.

> **Info**
>
> If the event log is related to a door, additional information regarding door control is displayed in the log details.

Check and Resolve Alerts

In the mobile app, check alerts from BioStar X and resolve them as needed. When an alert event such as a forced door open occurs, check the alert in the app and record the action taken.



Info

- For more information on checking and resolving alerts in BioStar X, see Monitor Event.
- The date and time shown in the alert list follow the BioStar X server's time settings. For more information on date and time display format settings in BioStar X, refer to Configure Preferences.

Alert list

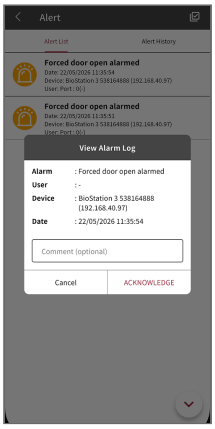


Tap **ALERT** on the app home screen. View the **Alert List**.

In the alert list, view alert events such as forced door opens in reverse chronological order. When a new alert event occurs, it is added to the list in real time.

Info

You can also open the alert screen by tapping the side menu (☰) → **Alert**.

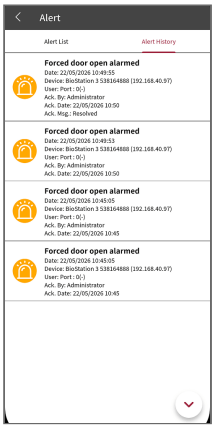


View alert details

In the alert list, tap a specific alert to view its details. Alert details show the event type, user, occurrence time, and the door/device.

- To record the action taken after checking an alert, enter the details in the **Comment (optional)** field. The entered details are saved on the BioStar X server and appear in the alert event details.
- To enter the action taken and resolve the alert, tap **ACKNOWLEDGE**. The alert is resolved, and the event disappears from **Alert List**.

Alert history



In alert history, you can view acknowledged alert events. View information such as each event's type, occurrence time, door/device, and user. Acknowledged alert events also show who acknowledged them and when.

Getting Started with Roll Call

Roll Call quickly generates a personnel list based on entry records within a specific time and place. When an emergency occurs, the system can determine whether a user has arrived at the roll call location by authenticating through the entry or exit device at a predesignated location.

Can be used for emergency response, safety checks, and providing rescue team information. This allows for efficient management of personnel status utilizing entry and exit records.

> **Info**
>
> - Before starting Roll Call, complete the Roll Call settings in BioStar X. For more information on how to set up Roll Call, refer to Roll Call.
> - Roll call settings can be used through an add-on option with an **Essential**(Essential) license or higher. For more information on licensing policies, see License Policy.

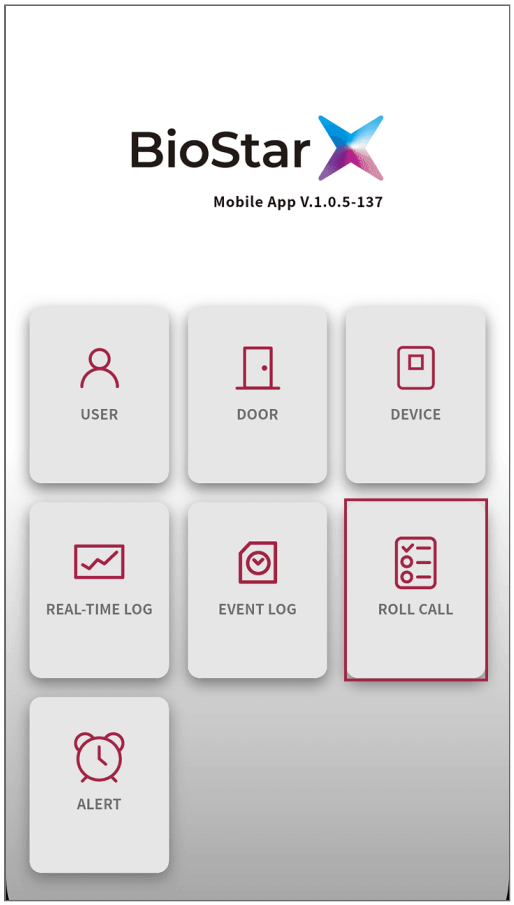
Use roll call in the mobile app

The roll call feature is available in the BioStar X mobile app.

Start roll call

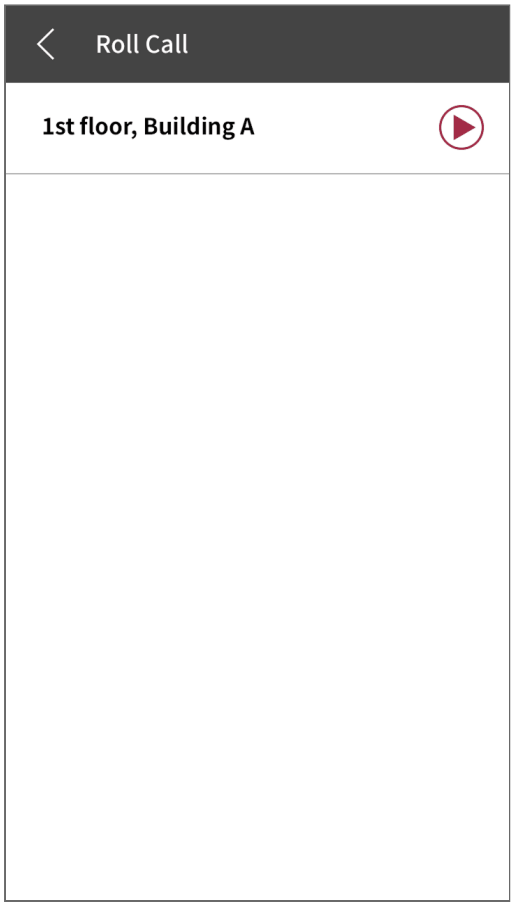
To start the roll call feature in the mobile app, follow these steps.

1. Launch the BioStar X mobile app on your mobile device.
2. From the app home screen, tap **ROLL CALL**.



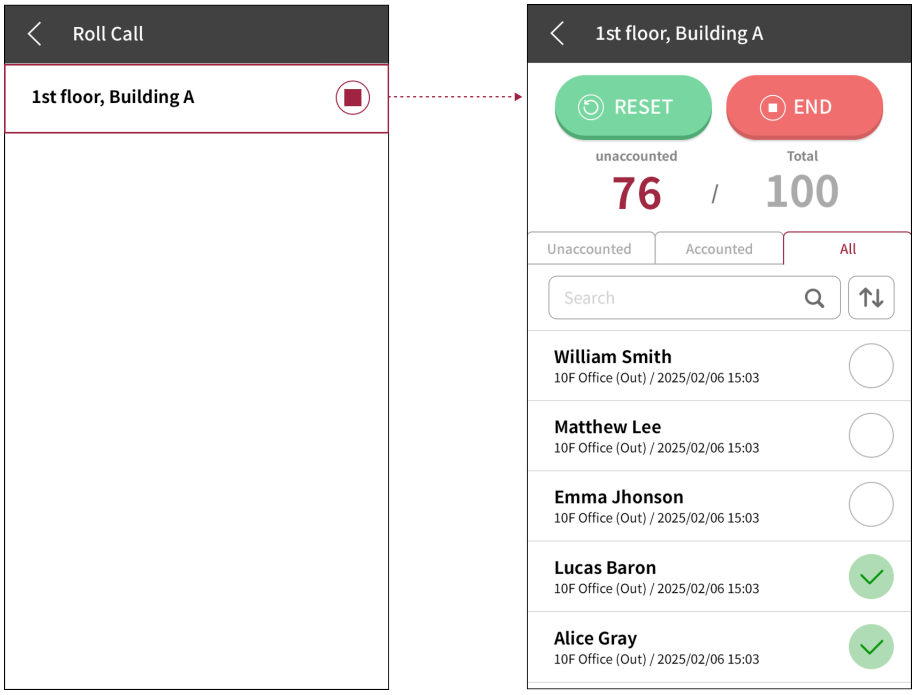
> You can also access it through the side menu. Tap ☰ → **Monitoring** → **Roll Call**.

3. In the Roll Call list, tap ▶ for the item you want to execute roll call.



4. When the confirmation message appears, tap **Yes**.

Roll call will start, and by tapping on the ongoing roll call item, you can check the status of the roll call.



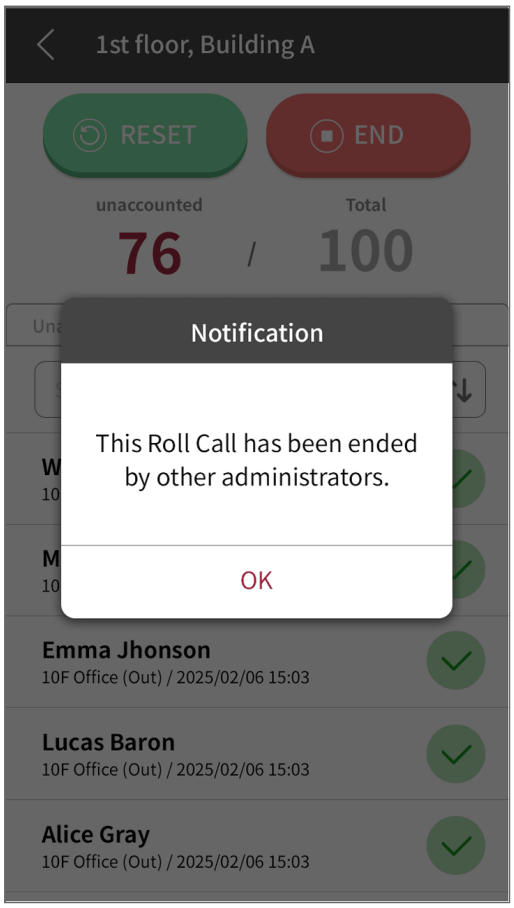
Control an in-progress roll call

- Users entering will be marked with the icon. When all users have entered, a message indicating that roll call has ended will appear. To end the roll call, tap **Yes**.

- The administrator can manually change the user's entry or status. Long press the round button on the far right of the user whose status you wish to change from the user list.



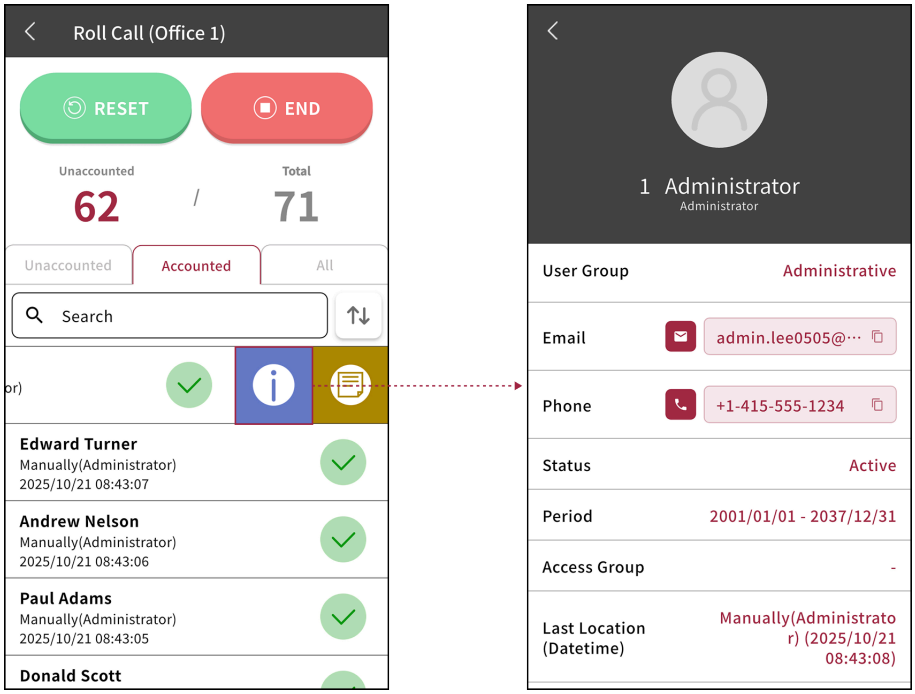
- To reset the roll call, tap **Reset**. All progress is discarded and the roll call restarts from the beginning.
- If roll call is ended by another administrator, a notification message will appear.



User information during roll call

During roll call in the mobile app, you can check each user's information. View details such as contact information for emergency contact and the user's last known location.

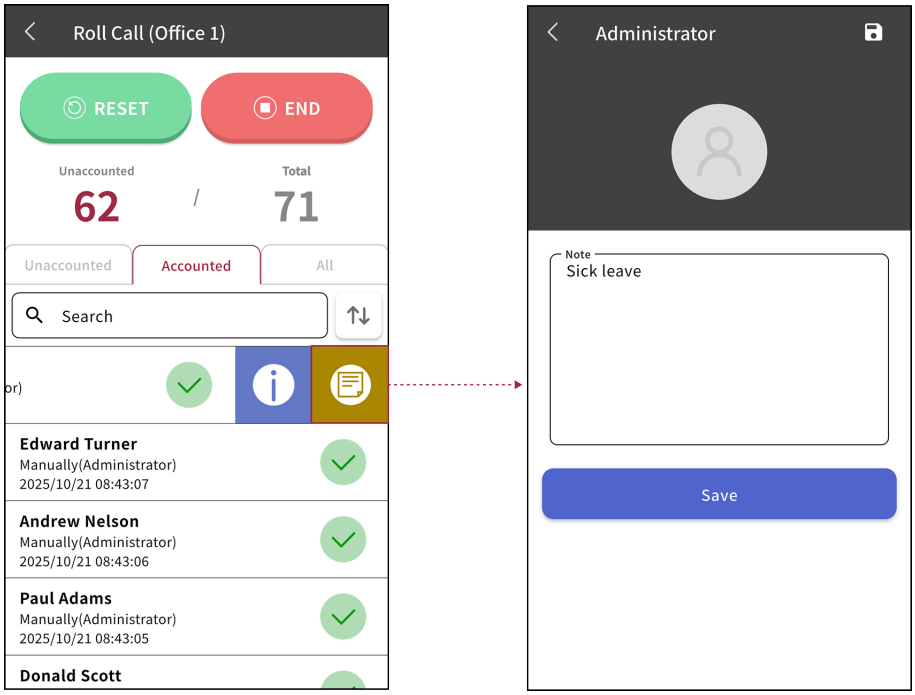
Swipe left on the user item for which you want to check details during roll call. Then tap ⓘ.



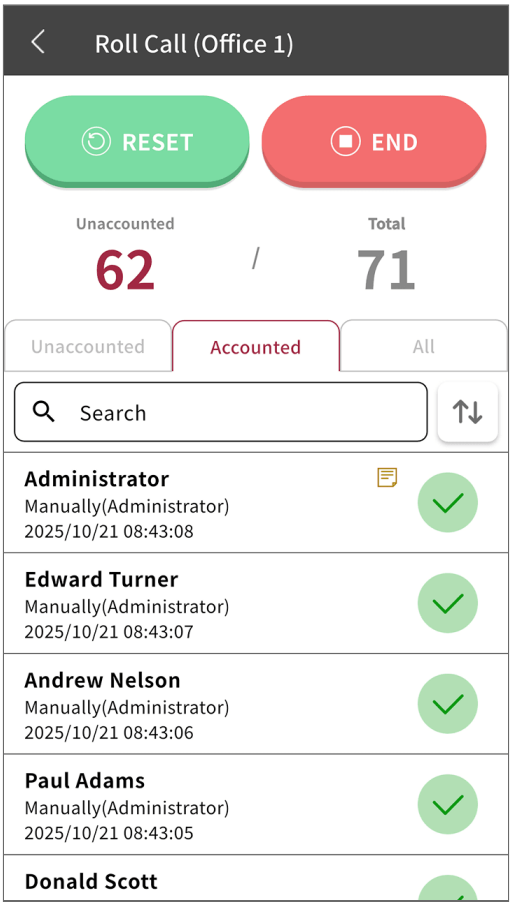
Leave a note for users during roll call

If a specific user has not entered during roll call in the mobile app, you can leave a note for that user.

Swipe left on the user item where you want to input a note during roll call. Then tap . On the note input screen, enter the content and tap **Save**.



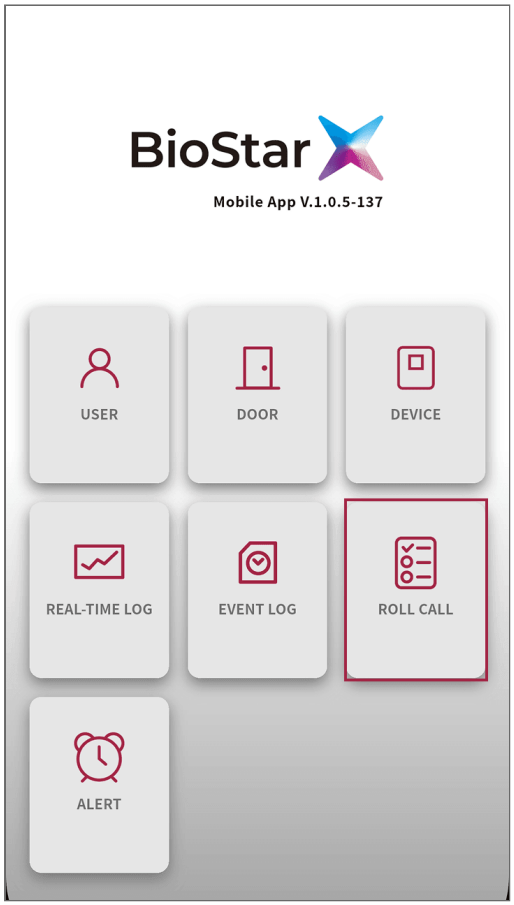
Users who have entered notes will be marked with the icon in the roll call list.



Check roll call details

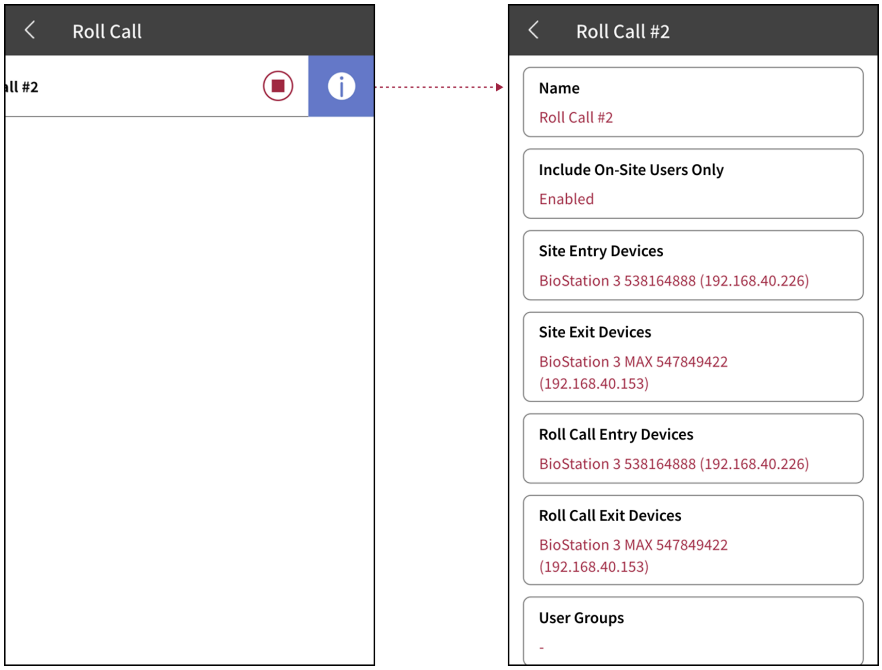
You can check the details of the roll call settings in the mobile app.

1. Launch the BioStar X mobile app on your mobile device.
2. From the app home screen, tap **ROLL CALL**.



> You can also access it through the side menu. Tap ☰ → **Monitoring** → **Roll Call**.

3. Swipe left on the item to check details from the list, then tap ⓘ.

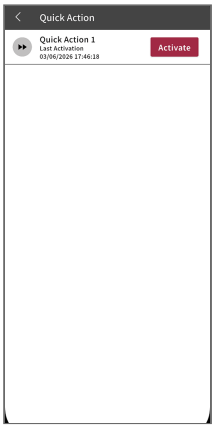


Use Quick Actions

Quick Action is a feature that automates complex control procedures during emergencies. Execute the actions of multiple predefined devices instantly with a single button to respond quickly.

> **Info**
>
> - For more information on the **Quick Action** feature, see How to Use the Quick Action.
> - In the mobile app, you can run the Quick Action feature or view detailed information about Quick Action entries. To create or edit a Quick Action item, log in to the BioStar X web interface and configure it.

Run a Quick Action



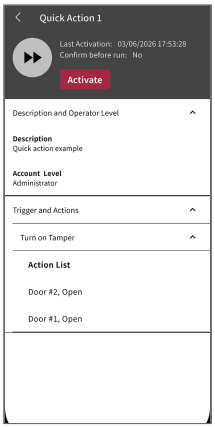
You must create Quick Actions in the BioStar X web interface before using them in the mobile app.

1. Tap **QUICK ACTION** on the app home screen.
2. In the Quick Action list, tap the **Activate** button for the Quick Action entry you want to run.

When Quick Action runs successfully, a success message appears.

> **Info**
>
> - Depending on the Quick Action setting, a pop-up may appear asking whether to run it.
> - Each Quick Action entry shows the most recent activation date and time.

Quick Action details



To view detailed information configured for a Quick Action entry, tap the entry in the Quick Action list.

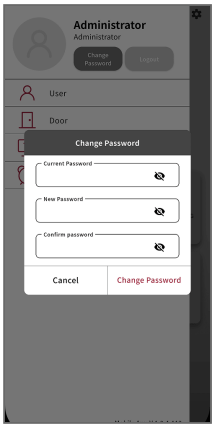
- **Last Activation**: The date and time when the Quick Action was last run.
- **Confirm before run**: Indicates whether a pop-up appears asking whether to run the Quick Action.
- **Activate**: The button that runs the Quick Action.
- **Description and Operator Level**: The Quick Action description and the administrator level required to run it.
- **Trigger and Actions**: The doors controlled when the Quick Action runs and the actions applied to those doors.

Info

For more information on trigger conditions and actions, see Trigger and Action Settings.

Change Account Password

You can change your account password in the BioStar X mobile app. Change your account password regularly to enhance account security.



1. On the app home screen, tap ☰ in the upper-left corner.
2. Tap **Change Password** in the side menu.
3. Enter the current password in the **Current Password** field.
4. Enter the new password in the **New Password** and **Confirm password** fields, in that order.
5. Tap **Change Password** to complete the password change.

Appendices

Includes legal notices contained in the product.

Disclaimers

- Information in this web site is provided in connection with Suprema products.
- The right to use is acknowledged only for Suprema products included in the terms and conditions of use or sale for such products guaranteed by Suprema. No license, express or implied, by estoppel or otherwise, to any intellectual property is granted by this web site.
- Except as expressly stated in an agreement between you and Suprema, Suprema assumes no liability whatsoever, and Suprema disclaims all warranties, express or implied including, without limitation, relating to fitness for a particular purpose, merchantability, or noninfringement.
- All warranties are VOID if Suprema products have been: 1) improperly installed or where the serial numbers, warranty date or quality assurance decals on the hardware are altered or removed; 2) used in a manner other than as authorized by Suprema; 3) modified, altered or repaired by a party other than Suprema or a party authorized by Suprema; or 4) operated or maintained in unsuitable environmental conditions.
- Suprema products are not intended for use in medical, lifesaving, life-sustaining applications, or other applications in which the failure of the Suprema product could create a situation where personal injury or death may occur. Should you purchase or use Suprema products for any such unintended or unauthorized application, you shall indemnify and hold Suprema and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Suprema was negligent regarding the design or manufacture of the part.
- Suprema reserves the right to make changes to specifications and product descriptions at any time without notice to improve reliability, function, or design.
- Personal information, in the form of authentication messages and other relative information, may be stored within Suprema products during usage. Suprema does not take responsibility for any information, including personal information, stored within Suprema’s products that are not within Suprema’s direct control or as stated by the relevant terms and conditions. When any stored information, including personal information, is used, it is the responsibility of the product users to comply with national legislation (such as GDPR) and to ensure proper handling and processing.
- You must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Suprema reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.
- Except as expressly set forth herein, to the maximum extent permitted by law, the Suprema products are sold "as is".
- Contact your local Suprema sales office or your distributor to obtain the latest specifications and before placing your product order.

Copyright Notice

The copyright for this website is owned by Suprema. Rights to other product names, trademarks, and registered trademarks belong to the respective individuals or organizations that own them.

Open Source License

This product contains open-source software. To request the source code covered under GPL, LGPL, MPL, and other open-source licenses which require distribution of the source code, please visit Suprema Global Technical Support Team.

You may obtain the source code for three years after our last shipment of this product on Suprema Global Technical Support Team.

If you want to obtain the source code in the physical medium, the cost of performing such distribution may be charged. This offer is valid to anyone in receipt of this information.

Open-source licenses and the corresponding license terms for open-source software contained in this product are as follows: ⚙ → **License**.

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

© 2026 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.