BioStar Air

ADMINISTRATOR GUIDE

Version 2.13.0

English

EN 102.00.BSA

suprema

SECURITY & BIOMETRICS

CONTENTS

What is BioStar Air? 4

100% cloud access control platform 4

Unparalleled credential flexibility 4

No on-prem infrastructure required 4

Easy multi-site management 4

Future-proof scalability with edge architecture 5

Optimized for cloud-centric businesses 5

BioStar Air features 5

Supported Devices 6

Security Framework 7

Site Administrator 10

Getting Started 10

Site Selector 21

Getting Started with the BioStar Air App 23

Manage Sites 25

Configure Site Settings 209

Set Up SSO & SCIM 230

Additional Site Configuration 260

Partners & Installers 289

Use the Partner Portal 289

Manage Federated Sites 291

Invite Partner Administrators 293

Invite Site Administrator 298

Manage Partner Technicians 303

Installing the Hardware 316

Credential User 337

Using Mobile Credentials 337

Set Up Advanced Features 339

Set Bluetooth Sensitivity 343

Developer 345

Quick Start 345

API Authentication 347

Using the User Management API 350

Troubleshooting 63

Fix Bulk User Addition Issues 355

Fix Mobile Card Issues 358

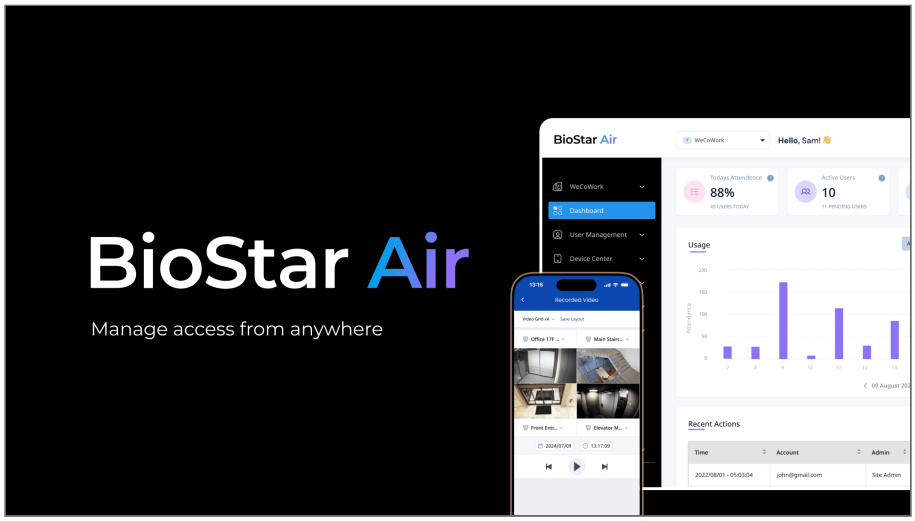
Why Am I Being Asked to Enable Location Services? 360

Troubleshoot Video Playback Issues 361

What is BioStar Air?

100% cloud access control platform

BioStar Air is a cloud-native access control solution developed by Suprema, a global leader in biometric security. Designed to eliminate the need for on-premises infrastructure, BioStar Air provides secure, flexible, and scalable access control that can be managed from anywhere. With smart readers that connect directly to the cloud, organizations can easily control access at multiple sites using only a phone or a browser.



Unparalleled credential flexibility

BioStar Air provides the most comprehensive range of authentication options, enabling organizations to manage facility access in multiple secure and convenient ways.

- **Facial authentication**
- **Custom mobile credentials for iOS and Android** (free)
- **Multiple RFID formats**
- **App-free Dynamic QR and LinkPass**

No on-prem infrastructure required

BioStar Air eliminates the need for on-site servers, virtual machines, VPNs, or door controllers. No IT maintenance is required. Install a **smart reader** and connect it to the cloud to start managing access immediately. Readers operate across multiple sites regardless of network or physical location.

Easy multi-site management

Whether managing access for **offices**, **warehouses**, **retail stores**, or **remote sites**, BioStar Air provides a complete solution to control access to all locations from a single system.

Future-proof scalability with edge architecture

BioStar Air's **edge architecture** embeds access control directly in the smart reader, removing the need for separate door controllers. This lets organizations **scale effortlessly**. Purchase only what is needed today and expand easily without complex upgrades.

Optimized for cloud-centric businesses

BioStar Air is designed for **system integrators** and **customers** seeking a fully cloud-native access control solution with industry-leading biometrics. It offers a modern, flexible, and highly secure approach to access management for cloud-centric enterprises.

BioStar Air features

Feature	Description
Complete access control solution	Supported
High security	ISO 27001 / 27701, TLS 1.2, AES-256
Biometrics: face and fingerprint	Provides native support for Suprema readers and includes a built-in biometric database.
RFID cards	MIFARE Classic, DESFire, FeliCa, EM4100, custom Wiegand formats, iCLASS, Seos. Supports up to eight cards per user.
Mobile credentials	Free and unlimited. Includes secure BLE/NFC credentials (iOS, Android), app-free LinkPass, and QR authentication.
Deployment	Cloud native
Interface	Browser, iOS app, Android app
Pricing model	Subscription-based
Integration	Extensive APIs, webhooks, and SDKs
Edge architecture	Readers include a built-in controller and connect directly to the cloud over Ethernet. No additional cloud nodes or access control panels are required.
login	Accessible from anywhere.
Server location	Korea (global) and Germany (Europe)

Feature	Description
Time and attendance	Time-and-attendance keys on the reader are logged as events and can be integrated into work-hour reports.
Video	Built-in VMS with support for ONVIF and Uniview. No NVR required; the reader acts as the gateway.
Alarms	Supports administrator notifications for intrusion alarm zones.
Data partitioning	Standard
Target	Franchises, multi-site, multi-tenant, remote locations, and more

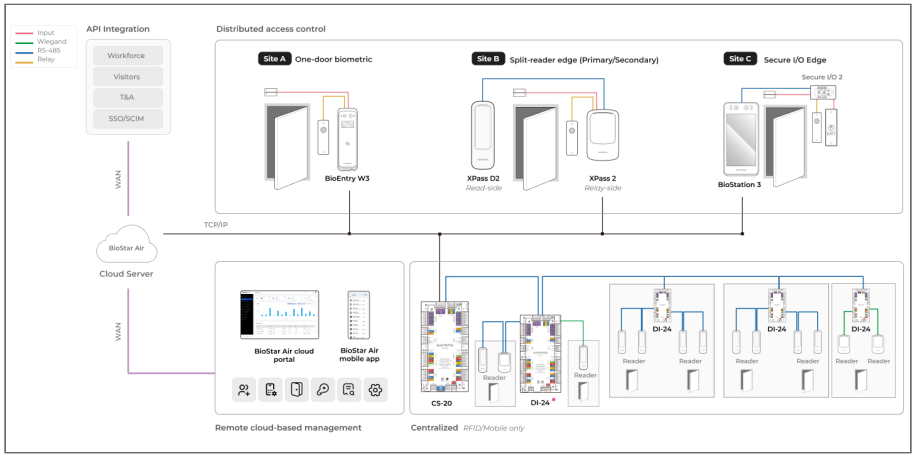
Supported Devices

BioStar Air supports flexible device management for both distributed and centralized access control architectures. Devices can be registered, configured, monitored, updated, and operated from the cloud, allowing each site to use the best setup for its doors, wiring, and security requirements.

Sites can use edge devices that connect directly to the cloud, or control panels that manage downstream readers through RS-485 or Wiegand. Both architectures can be used within the same site, supporting new installations, biometric deployments, retrofits, and centralized panel-based configurations.

Supported devices

BioStar Air is compatible with various access control devices and seamlessly integrates with devices in Suprema to enable cloud-based access control.



Readers

- **XPass 2** (MDPB, GDPB, GKDPB)
- **X-Station 2** (DPB)
- **BioEntry W3**
- **BioStation 3**

- **XPass D2**

Panels

- **CoreStation 20** (CS-20)

Patch devices

- **Airfob Patch** (AP-H)
- **Airfob Tag** (AP-B)

Other compatible devices

- **Output Module** (OM-120)
- **Secure I/O 2** (SIO2)
- **Door Interface** (DI-24, coming soon)

Security Framework

BioStar Air is Suprema's secure, cloud-based mobile access control solution. Suprema's hardware, software, and firmware engineering teams work according to a "security by design" principle. Every layer of the system architecture and every communication touchpoint is designed to maintain privacy and data integrity.

Key measures:

- Data protection and encryption of the BioStar Air management portal and database
- Encryption and protection of data in transit between the BioStar Air API and clients
- Encryption of mobile card data stored on the smartphone
- Protection of communication between the smartphone and reader (Suprema Pass)
- Prevention of mobile credential forgery (Suprema Pass)

ISO 27001 certification

Suprema has obtained ISO 27001 certification, meeting global standards for data protection management, security controls, and privacy management. Established in August 2019, ISO 27001 compliance also aligns with similar regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Proven technology for end-to-end security

Secure portal access and data protection

The BioStar Air management portal runs on an AWS Amazon RDS encrypted DB instance that uses AES-256 or stronger encryption. All personal data is additionally encrypted.

Encrypted communication with the BioStar Air API

All communication with the BioStar Air REST API is encrypted with TLS 1.2 over HTTPS and requires an access token (1-hour expiration by default). AWS API Gateway throttles API requests to prevent brute-force attacks.

Encrypted and hashed mobile card IDs

Mobile card ID numbers are encrypted with AES-256 to prevent exposure on third-party servers. Card data is digitally signed for authenticity verification.

Secure storage of mobile cards on the device

Suprema Pass mobile credentials and related data are encrypted with AES-256. Encryption keys are stored in the device's trusted execution environment (TEE), such as Secure Enclave (Apple) or TrustZone (ARM).

Secure communication between the mobile device and reader

To block replay attacks over Bluetooth Low Energy (BLE), BioStar Air uses a one-time encryption key for each connection and terminates the connection immediately after transmission, preventing man-in-the-middle (MITM) attacks.

Mobile card forgery prevention

Each Suprema Pass mobile credential is protected by a PKI-based digital signature unique to each BioStar Air site. A proprietary verification process detects any attempt at modification or forgery.

Vulnerability management

Suprema's information security team leads vulnerability management, supported by external security experts.

- Continuous automated threat scans
- Annual ISO 27001 renewal audit with full system review
- Penetration testing and risk assessment before major releases
- Checks for password hygiene, social-engineering resistance, and procedural compliance
- Comprehensive documentation and reporting of all vulnerabilities and remediation actions

Risk assessment approach

Assets are classified according to confidentiality, integrity, and availability ratings. Threats are identified, vulnerabilities are assessed, and risks are evaluated based on likelihood and impact. Mitigation actions are prioritized according to risk severity.

Multi-factor authentication (MFA)

Multi-factor authentication (MFA) is being rolled out in phases.

- Email-based 2FA for administrator accounts
- Passcode-based 2FA for the BioStar Air app
- Automatic lock of inactive administrator accounts after 90 days

- Configurable password expiration (30, 60, or 90 days)

Key security policies

- Data encryption in transit: TLS 1.2
- Data encryption at rest: AES-256
- DoS protection: AWS API Gateway request throttling
- Service availability: 99.9% uptime (per SLA)
- API security: token-based authentication, HTTPS only, strict endpoint validation
- Portal access: cloud-based for global management; a private cloud option is under development

Site Administrator

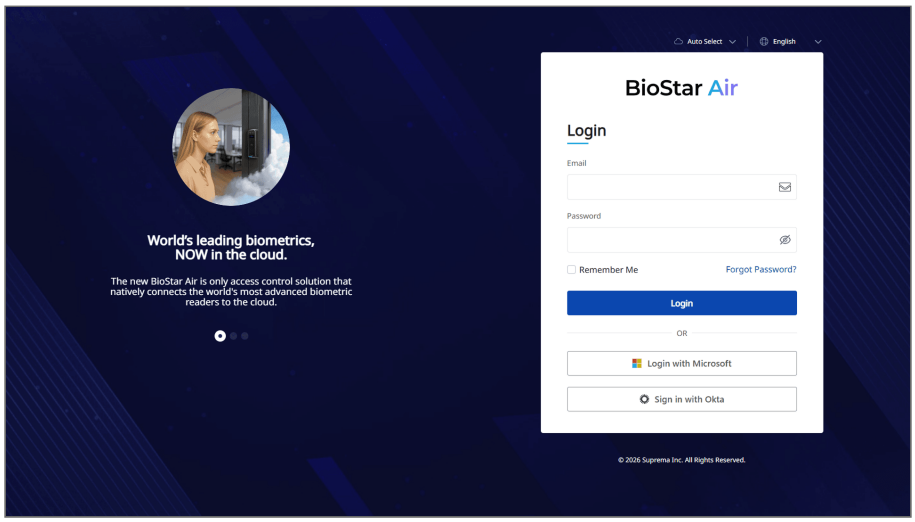
The site administrator is responsible for the overall operation of a BioStar Air site. Guides administrators through all necessary management tasks, including user enrollment and credential management; configuring devices, doors, and elevators; setting access permissions and schedules; monitoring events; and configuring system settings and services.

Getting Started

The BioStar Air portal provides a unified interface across the web and mobile apps, delivering a consistent user experience. Through the BioStar Air portal, administrators can manage access control settings, monitor site usage, and seamlessly configure users and devices.

Access the portal

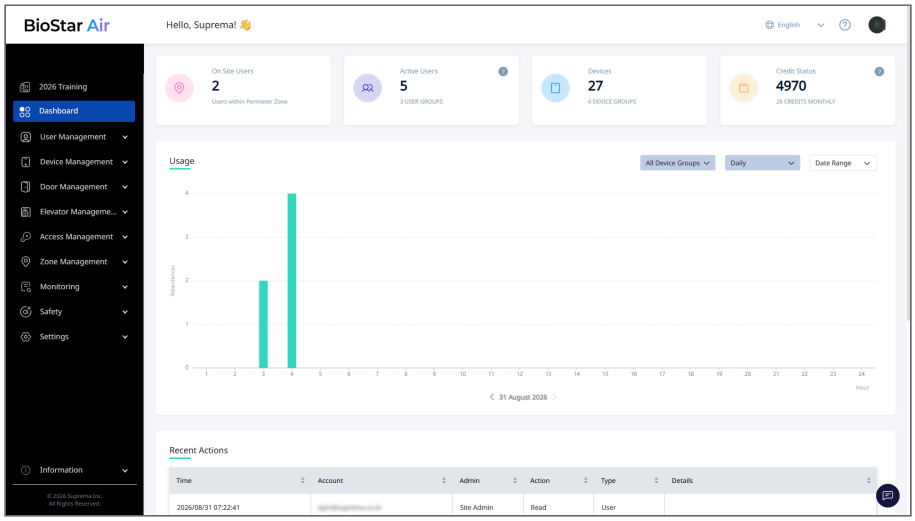
Open a web browser and go to https://admin.biostarair.com to access the BioStar Air portal. When the login page appears, select **Global Server** or **EU Server** based on your location.



> **Info**
>
> You cannot create an account by signing up. The system installer or an existing administrator must invite you to the site. For more information on managing administrator accounts and invitations, see Manage Administrator Accounts and Roles.

Explore the dashboard

After logging in, the **Dashboard** appears and shows key site information.



- **On Site Users**: View on-site users in real time. Presence status is calculated based on authentication logs from the entry and exit devices configured in **Perimeter**. For more information, refer to the followings.
  - Manage Zones
  - Check Presence
- **Active Users**: View the total number of registered and active users. Click the card to open **User Management**.
- **Devices**: View the number of registered devices. Click the card to open **Device Management**.
- **Credit Status**: View the remaining account credits. Click the card to open **Settings** → **Credit Center**.
- **Usage**: Sort usage by device group, frequency (daily, weekly, monthly), or custom date range.
- **Recent Actions**: Shows an activity log of administrator actions such as sign-ins, device updates, and user creation.

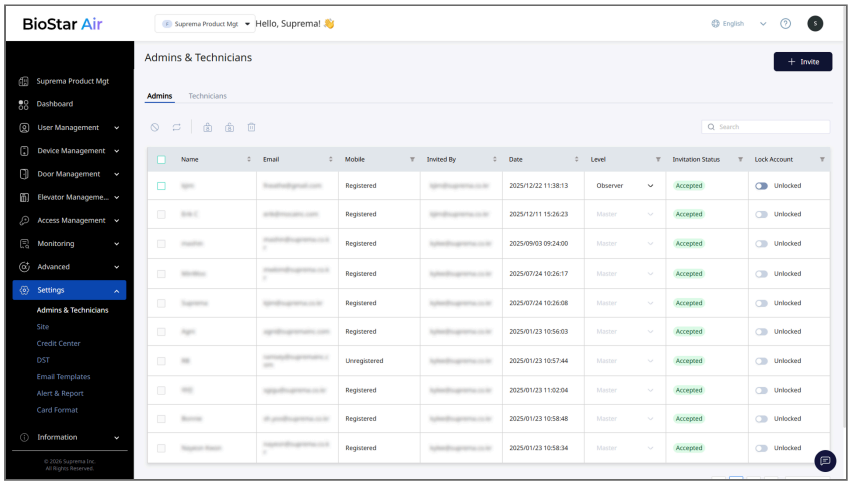
Site setup guide

Follow these instructions to set up a new site.

1 Add administrators

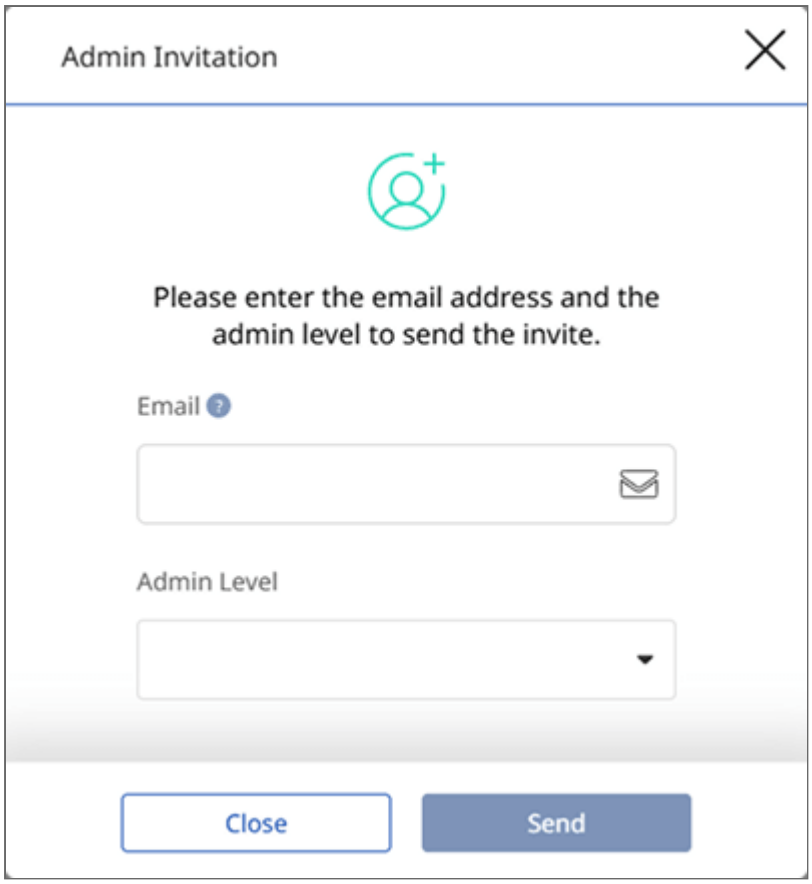
Invite administrators.

1. Click **Settings** → **Admins & Technicians** in the left sidebar.



2. Click **Invite** at the top right of the screen.

3. When the **Admin Invitation** window appears, enter the administrator's email address and assign a role.

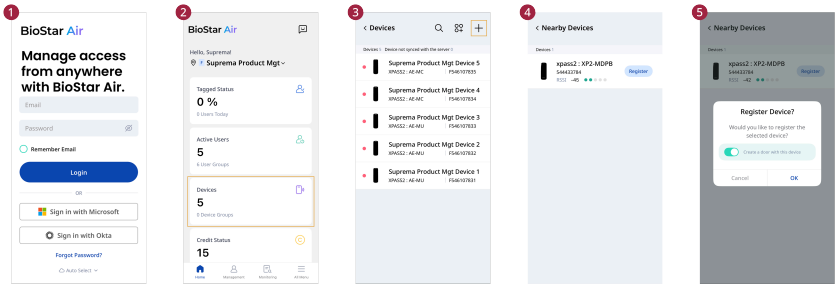


4. Click **Send**.

> **Info**
>
> Site administrators can manage the site, and authenticated users can only access the site through the **Suprema Pass** app.

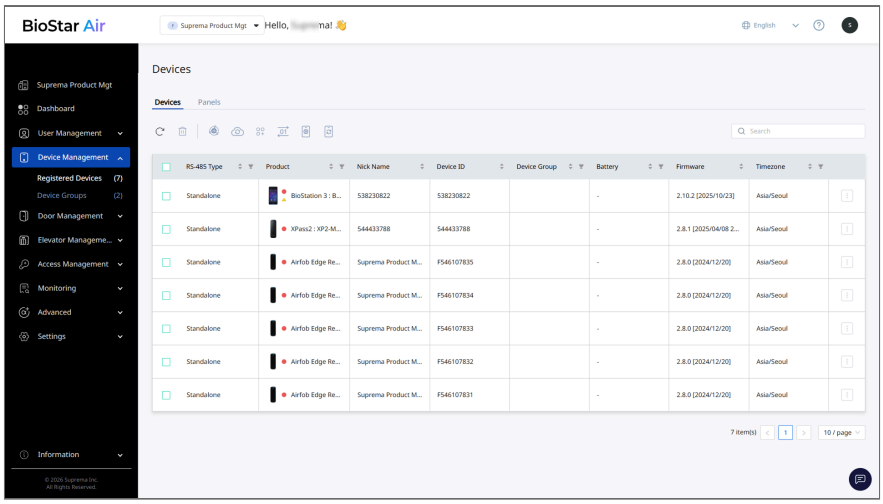
2 Register devices

Use the BioStar Air mobile app to register devices. Register devices using Bluetooth Low Energy (BLE), and manage them through the BioStar Air portal.



1. Open the BioStar Air app on your mobile device and log in.
2. Tap the **Devices** card.
3. Tap + at the top right of the screen.
4. In the device search screen, tap **Register** for the device to register.
5. When the device registration window appears, tap **OK**.

Return to the device list and confirm the added device. Click **Device Management** → **Registered Devices** in the left sidebar.

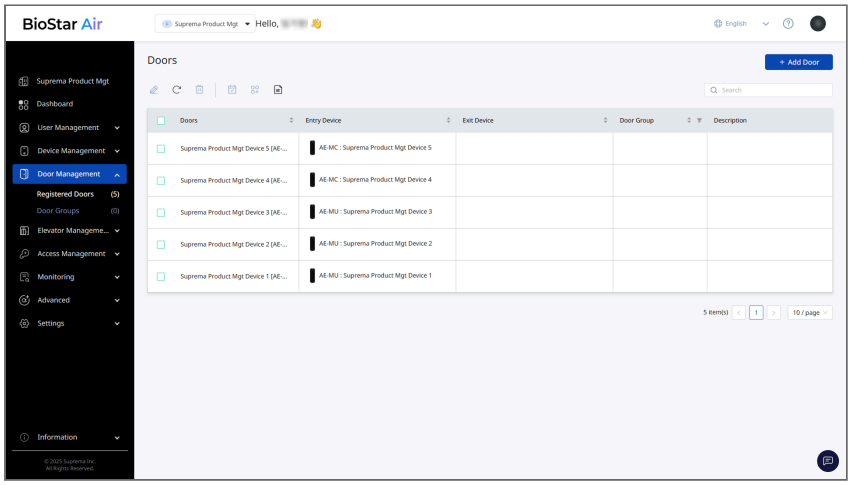


- If the device is not registered, ask another administrator to register it on-site with the BioStar Air mobile app.
- In **Registered Devices**, delete devices, update firmware, and manage device groups.

3 Create and manage doors

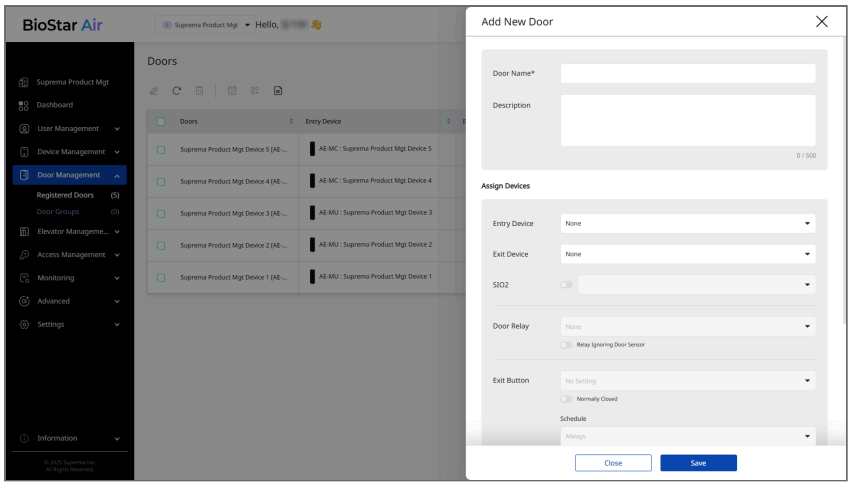
Add doors and assign devices.

1. Click **Door Management** → **Registered Doors** in the left sidebar.



2. If no doors are listed, click **Add Door** in the upper-right corner.

3. When the **Add New Door** panel appears, enter a name and description.



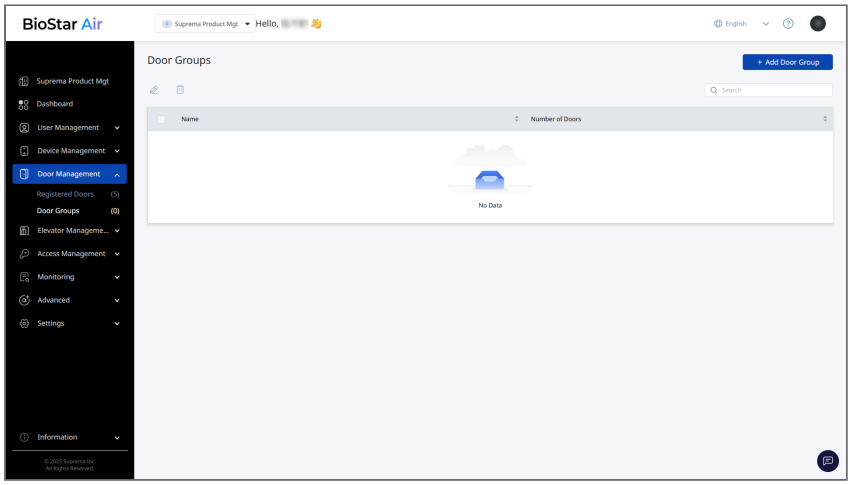
4. Assign registered devices to **Entry Device** and **Exit Device**.

In **Door Management**, edit or delete doors, configure door schedules, and manage them by group.

4 Categorize doors into groups

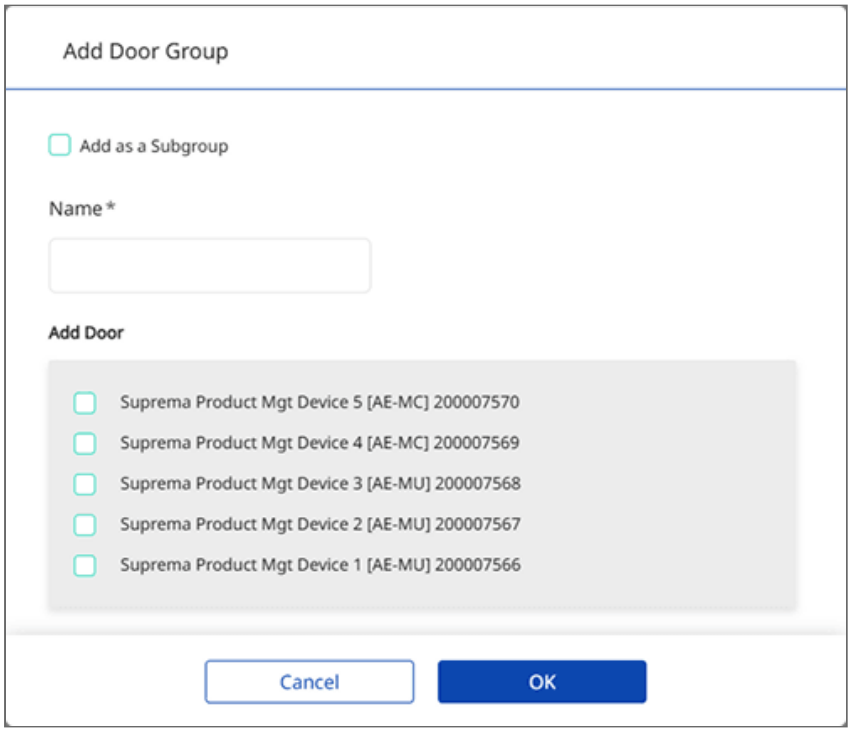
Categorize doors into groups.

1. Click **Door Management** → **Door Groups** in the left sidebar.



2. Click **Add Door Group** at the top right of the screen.

3. When the **Add Door Group** window appears, enter a group name such as **Indoor**, **Outdoor**, or **Trap Doors**, and select the desired doors.



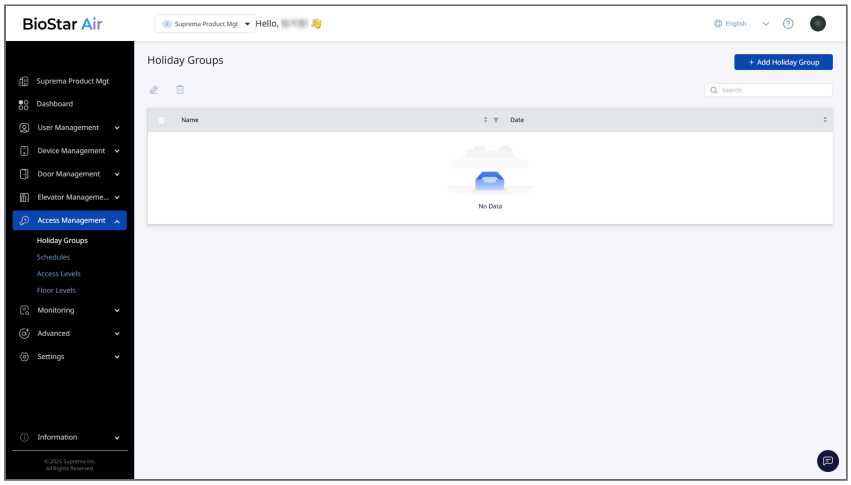
4. After selecting all doors, click **OK**.

5 Configure access rights

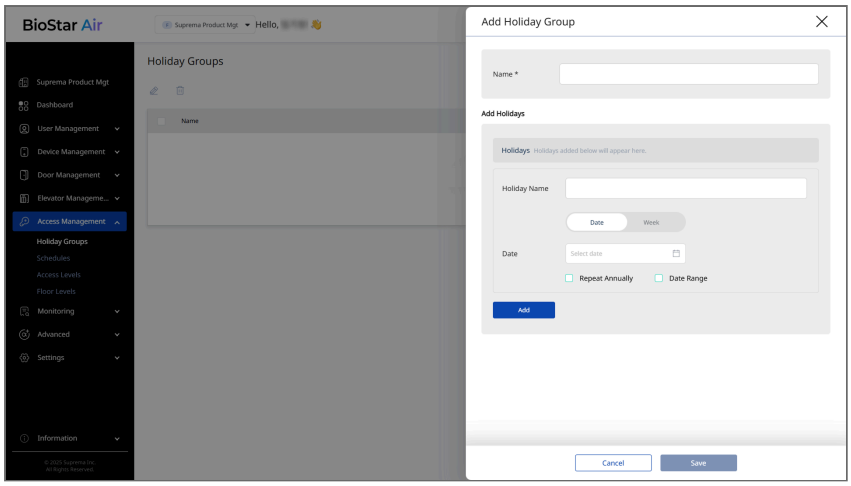
Follow these steps to manage access rights.

6 Set up holiday groups

1. In the left sidebar, click **Access Management** → **Holiday Groups**.



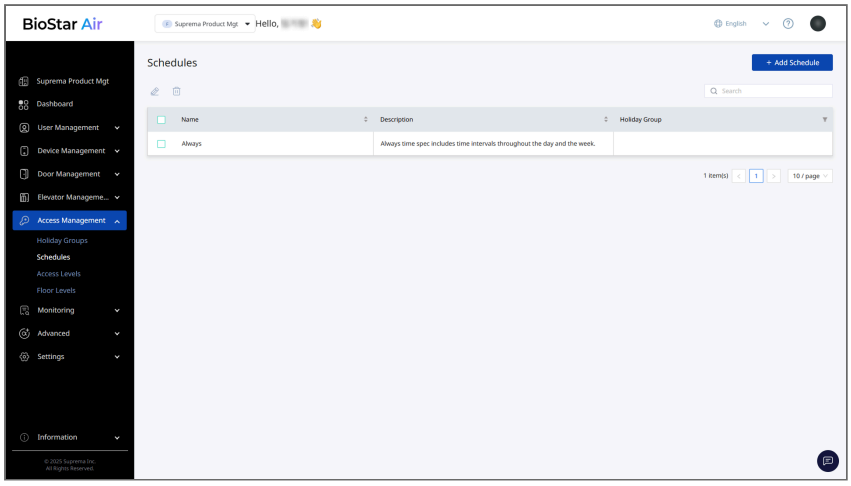
2. Click **Add Holiday Group** at the top right of the screen.
3. When the **Add Holiday Group** panel appears, enter a name (for example, "Korea Holidays").



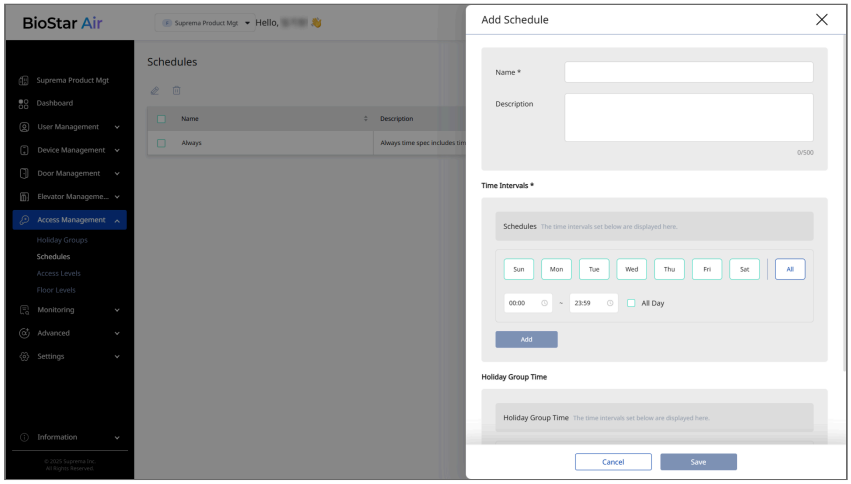
4. In the **Add Holidays** section, set the holidays on which to restrict access, and click **Add**.
5. After adding all holidays, click **Save**.

7 Create schedules

1. Click **Access Management** → **Schedules** in the left sidebar.



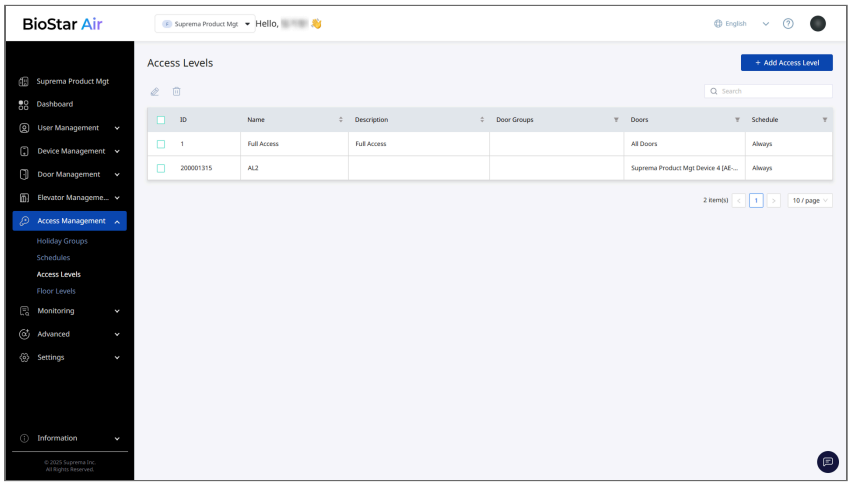
2. Click **Add Schedule** at the top right of the screen.
3. When the **Add Schedule** panel appears, enter a name.



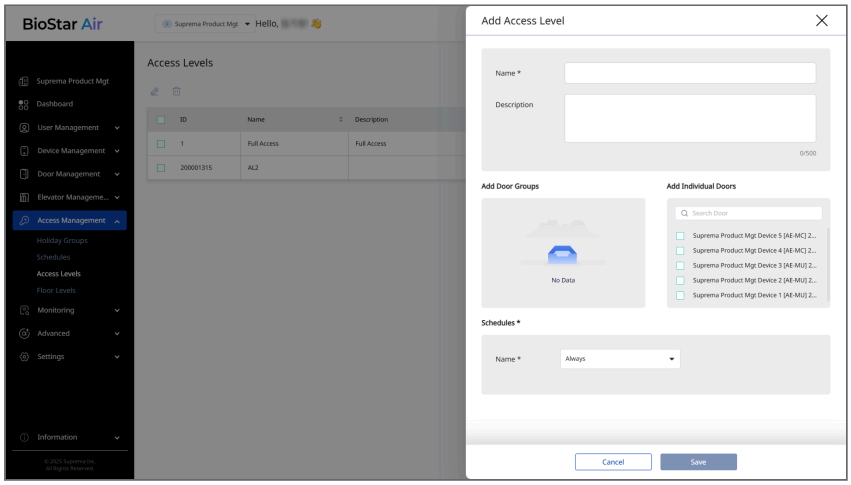
4. Select the days to activate and link a holiday group.
5. When the schedule is complete, click **Save**.

8 Define access levels

1. Click **Access Management** → **Access Levels** in the left sidebar.



2. Click **Add Access Level** at the top right of the screen.
3. When the **Access Level** panel appears, enter a name, and assign door groups, individual doors, and schedules.

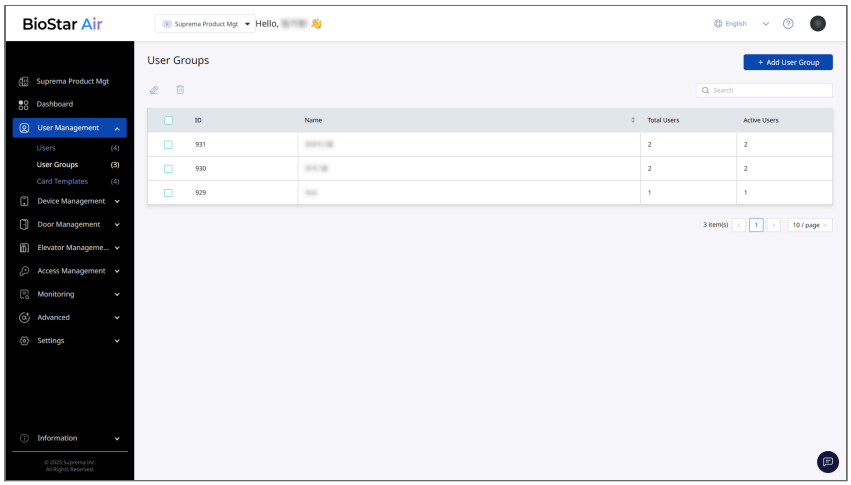


4. When the access level is configured, click **Save**.

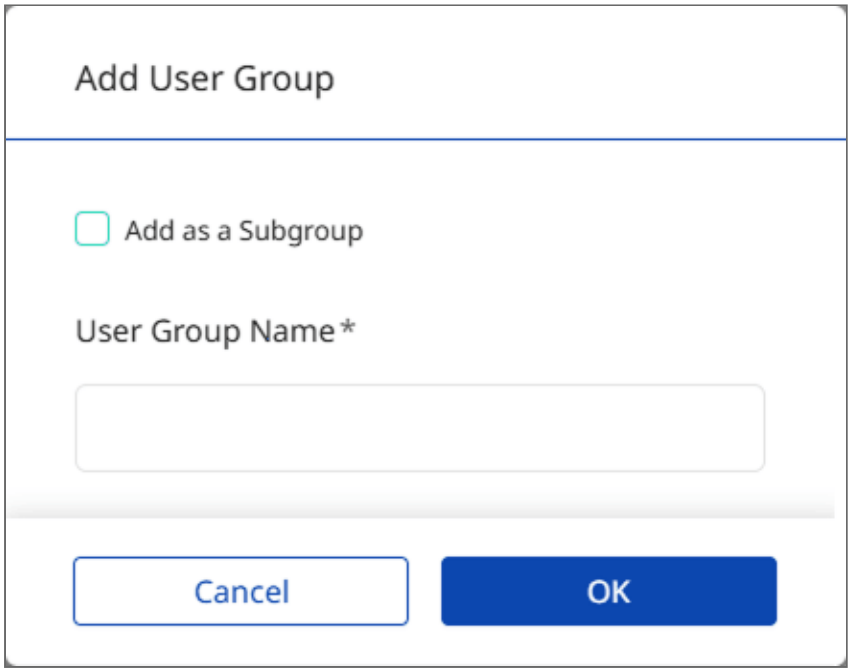
9 Create user groups and add users

Create a user group and add users to the new group.

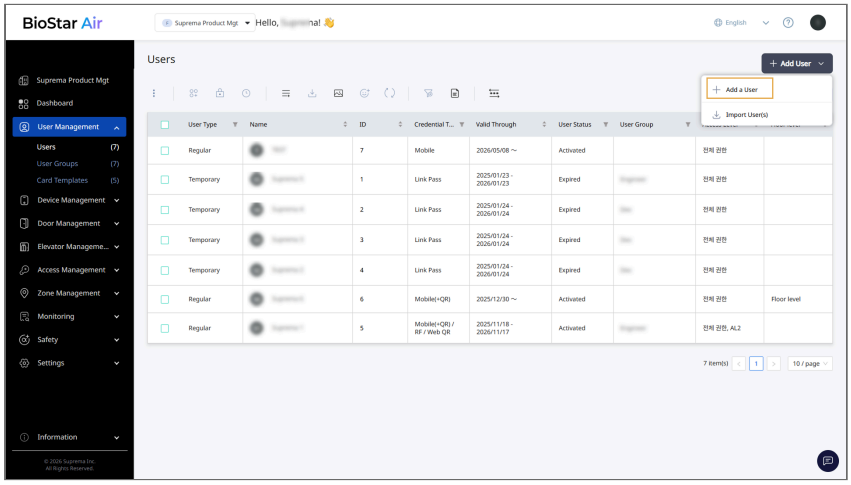
1. Click **User Management** → **User Groups** in the left sidebar.



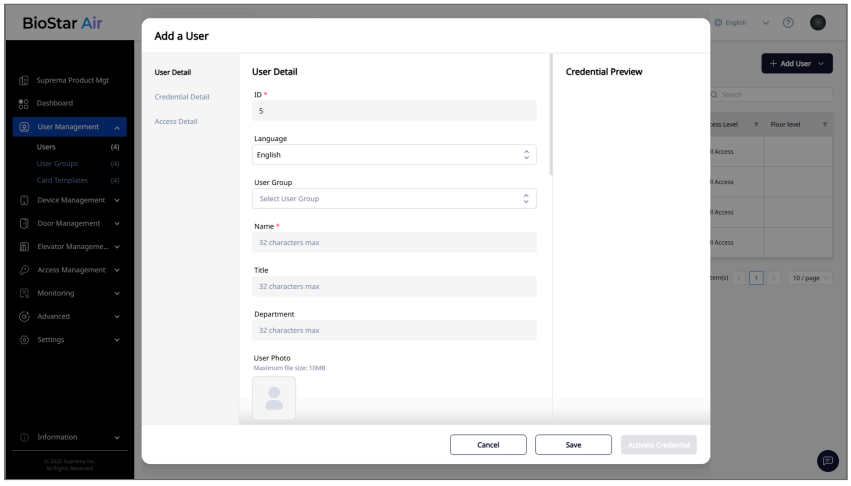
2. Click **Add User Group** at the top right of the screen.
3. When the **Add User Group** window appears, enter the user group name.



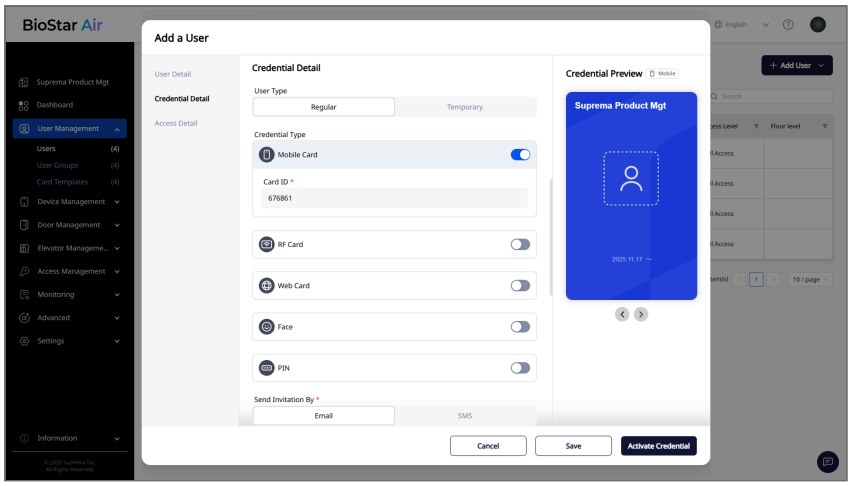
4. Click **OK** to save the user group.
5. Click **User Management** → **Users** in the left sidebar.
6. Click **Add User** → **Add a User** at the top right of the screen.



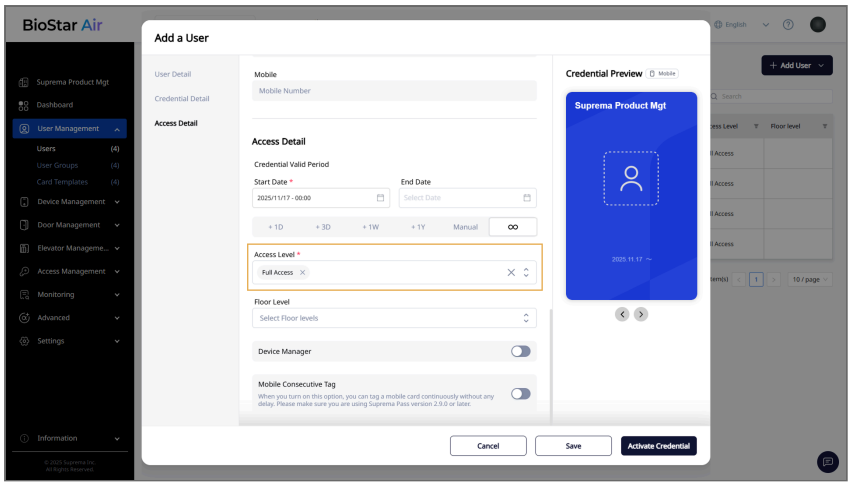
7. When the **Add a User** window appears, enter the user ID, name, and so on in the **User Detail** section.



8. In the **Credential Detail** section, enable one or more credential types.



9. In the **Access Detail** section, select an access level.



10. To finish configuring the user's access, click **Activate Credential** in the lower-right corner.

> **Info**
>
> In the **User Management** → **User Groups** menu, bulk-manage users, reissue, suspend, or delete them, export data, and upload profile images in bulk.

Tip

Checklist

To summarize, follow these steps.

1. Add administrators.
2. Register devices.
3. Create doors and assign devices.
4. Categorize doors into groups.
5. Configure access rights (holidays, schedules, access levels).
6. Create user groups and add users.

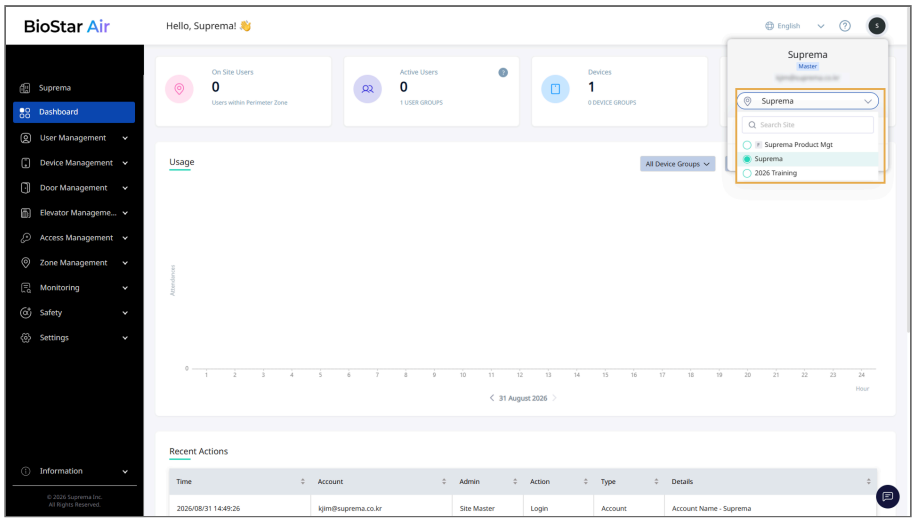
Following these steps sets up the BioStar Air site smoothly. Refer to the individual video tutorials in the user guide for more details.

Site Selector

The **Site Selector** feature simplifies processes and reduces the need to log in multiple times by allowing management of multiple sites with a single email address.

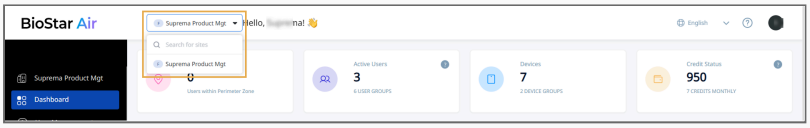
What is Site Selector?

The **Site Selector** feature enables signing in to the BioStar Air portal with a single, unified email address even when managing multiple sites. There is no need to sign in with different email addresses for each site. Sign in once with a single email address, and then use the **Site Selector** menu to switch easily between the sites being managed.



Info

- Even with a unified email, each site's permissions and settings remain independent. Administrator roles and access rights are managed separately for each site.
- If the **Site Selector** feature does not appear or an incorrect site is shown, verify that the migration request is complete or contact the support team for further assistance.
- By streamlining the sign-in process and consolidating multiple sites under one account, the Site Selector feature saves time and effort when managing several sites in BioStar Air.
- Sites marked with an F icon are Federation Site in the site selection list. Federation Sites are displayed in the upper-left corner of the screen. For more information on Federation Site, see Manage Federated Sites.



Create a new site

When creating a new site through the Partner Portal, use an email address that is already registered as an administrator account for another site. The system automatically links the new site to the existing email, allowing management of multiple sites with a single account.

- Create a new site via the Partner Portal.
- When prompted for the administrator email, enter the email address that is already linked to another site.
- The new site is automatically linked to the existing account.

Info

For detailed information on signing up for and using the Partner Portal, see Use the Partner Portal.

Using one email across multiple sites

If multiple sites are already managed but each uses separate sign-in credentials, request a manual migration from **Suprema**. This process consolidates the email addresses, enabling management of all sites with a single sign-in.

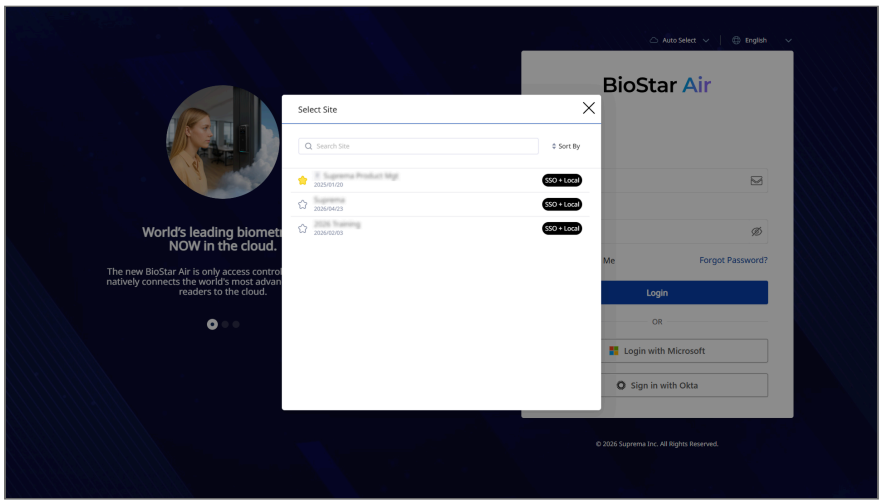
- Contact the support team and request a manual migration for the sites.
- If alias addresses such as bob+site1@example.com and bob+site2@example.com are used, provide the root email address (bob@example.com).
- If completely unique email addresses are used for each site, provide the full list of email addresses.
- Once migration is complete, access all sites with a single email address through the **Site Selector** feature.

Using the Site Selector

If your email address is associated with multiple sites, signing in and switching between them is easy.

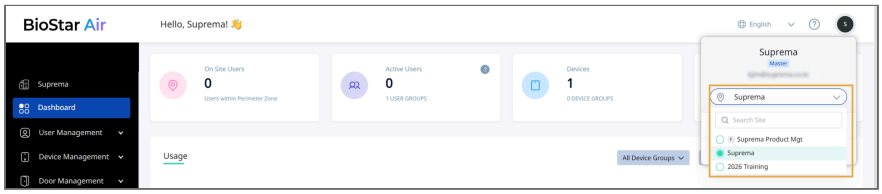
1. Enter your email address and password.

2. If you manage multiple sites, use the **Select Site** window to quickly find the site you want. Selecting a site takes you to the dashboard.



3. After signing in, click the profile icon in the top right corner of the screen.

4. When the pop-up menu appears, click the **Site selector** option below your email address.



You can view a list of all sites associated with the email address.

Getting Started with the BioStar Air App

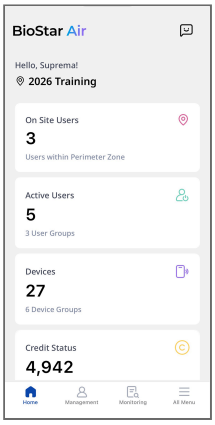
The BioStar Air app offers all the same features as the BioStar Air web portal. Users can manage access control, monitor event logs, control devices, and perform administrative tasks directly from a mobile device.

Download the mobile app

Download the BioStar Air app on your mobile device and log in.

- Download and install the BioStar Air app on your mobile device.
  - iOS
  - Android
- Log in using the same ID and password you use for the BioStar Air web portal.

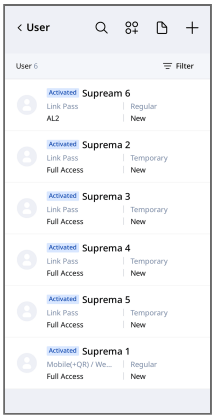
> **Info**
>
> - Verify that you logged in with the same credentials as the web version.
> - Stay close to the device to update it in BLE mode.
> - Certain features, such as real-time video monitoring, require a connected camera.



Dashboard

After logging in to the mobile app, **Dashboard** on the home screen provides the following information.

- Daily user accesses
- Total active registered users
- Connected devices
- Credit status

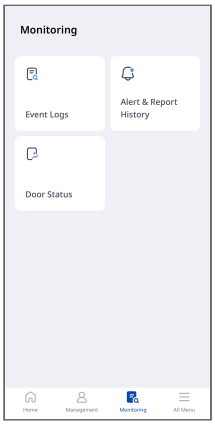


User management

Tap the **Active Users** card on the home screen, or tap **Management** → **Users** in sequence.

- Select a user and review the details.
- Modify user status (reissue, suspend, delete, or activate).
- Tap the + button and enter the required details to add a new user.

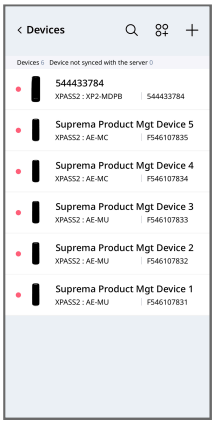
> **Info**
>
> - To learn how to add users using the mobile app, see Add Users.
> - To learn how to add users through the BioStar Air portal, see Add Users.
> - For more information about user management, see Manage Users.



Monitoring

Monitoring provides the following information.

- **Event Logs**: Monitor and analyze event logs and audit logs. For more information, see Use Event Logs and Use Audit Logs.
- **Alert & Report History**: View past alerts and generated report history through the web portal and mobile app. For more information, see Check Alert & Report History.
- **Door Status**: Monitor the real-time status of doors connected to the site. For more information, see Monitor Door Status.
  - Check door status and control it remotely.
  - Tap a door once to edit it, or touch and hold to select multiple doors and perform batch actions.
  - Setting a door to **Unlock Mode** or **Lock Mode** overrides relay settings or schedules.
  - Delete unused doors as needed.
- Real-time video (if a camera is connected)



Devices

Tap the **Devices** card on the home screen, or tap **Management** → **Devices** in sequence.

- View all registered devices.
- Select a device to edit, update firmware, or reboot it.
- If the device is not connected to the network, use **BLE mode** close to the device to update its firmware.
- Tap the + button to add a new device.

> **Info**
> For more information about device management, see the following.
> - BioStar Air App: Register and Delete Edge Devices
> - BioStar Air portal: Devices

Manage Sites

In BioStar Air, a **site** is the core unit of the access control system and represents a physical location users can access. Each site can have unique settings, users, devices, and access rights. Administrators can create and manage multiple sites to operate access control efficiently across various locations.

Refer to the following documents to learn how to manage sites effectively in the BioStar Air portal.

Users

This section explains how to create user accounts in BioStar Air, configure various credentials (mobile card, RF card, web card, facial authentication, PIN), and set access permissions and validity periods. It covers all aspects of user management, from managing individual users to performing bulk operations, managing user groups, and filtering.

> **Tip**
> Watch the following video to understand the user management features more easily.

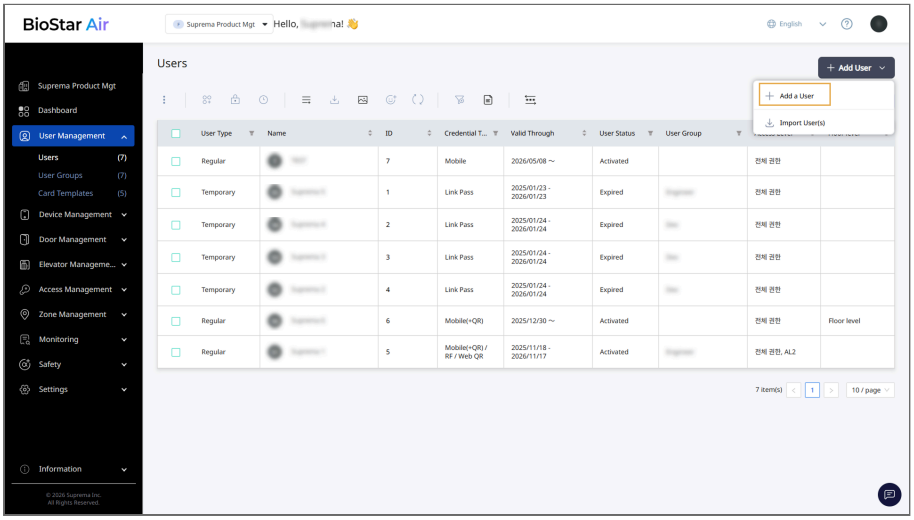
Add Users
This document provides step-by-step instructions on adding and managing individual users in BioStar Air. It covers the entire process of selecting the user type (regular or temporary), issuing the appropriate credentials, and setting access levels and validity periods. It also includes how to edit or delete the added user's information.

> **Tip**
> Refer to the following video for step-by-step guidance on the entire process of adding a new user.

Add users

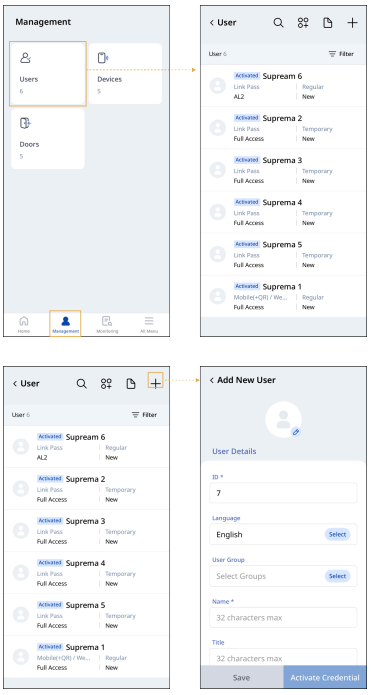
Web

1. Click **User Management** → **Users** in the left sidebar.
2. A list of users appears.
3. Click **Add User** → **Add a User** at the top right of the screen.



When the **Add a User** window appears, enter and configure the required information in each section. Set the required fields in all sections and click **Activate Credential** at the bottom right.

Mobile



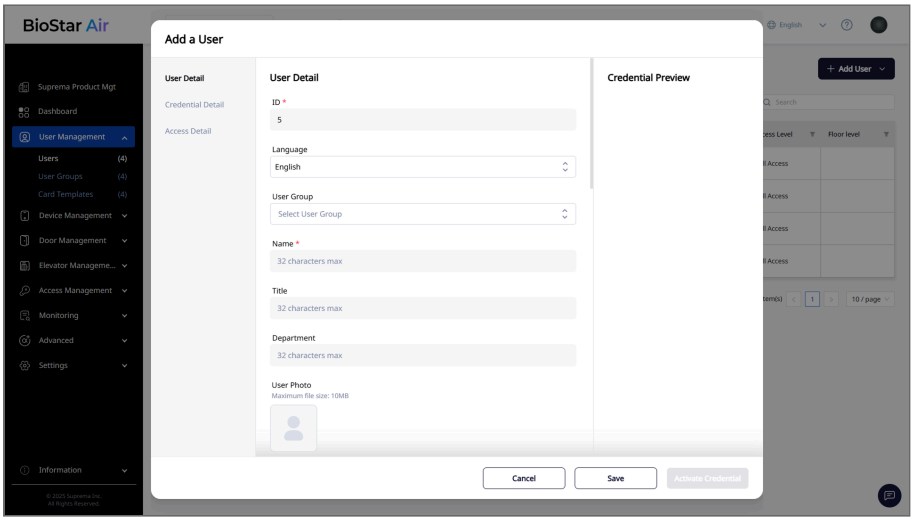
1. Log in with the mobile app.
2. Tap **Management** at the bottom of the screen.
3. Tap the **Users** card.
4. Tap + at the top of the user list.

When the **Add a User** screen appears, enter and configure the required information in each section. Set the required fields in all sections and click **Activate Credential** at the bottom right.

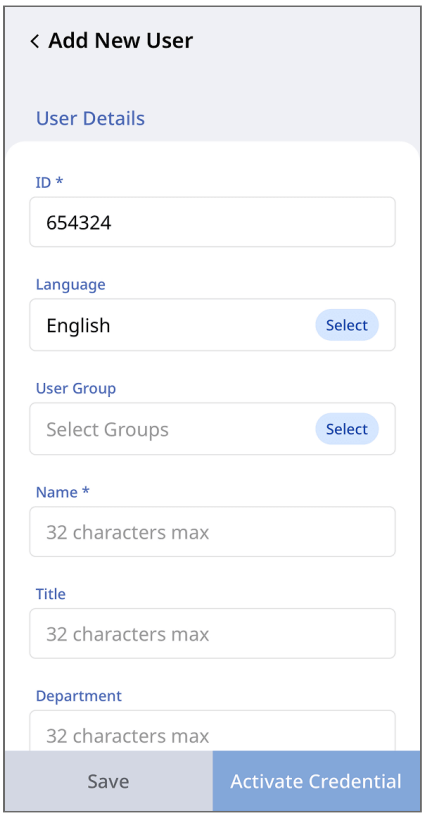
Enter user information

Enter the new user's basic information in the **User Detail** section.

Web



Mobile



- **ID**: Enter a specific ID manually or allow the system to generate it sequentially.
- **Language**: Select the user's default language.
- **User Group**: Select the group to which the user belongs.
- **Name**: Enter the user's full name.
- **Title**: Enter the user's title.
- **Department**: Enter the name of the user's department.
- **User Photo**: Upload the user's profile image. For more information, see Upload profile image.

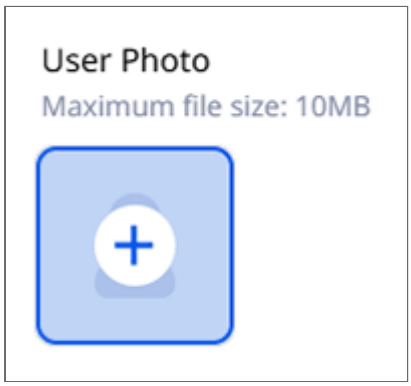
Info

- * indicates a required field.
- Enter the user's email and phone number in **Send Invitation By** in the **Credential Detail** section.

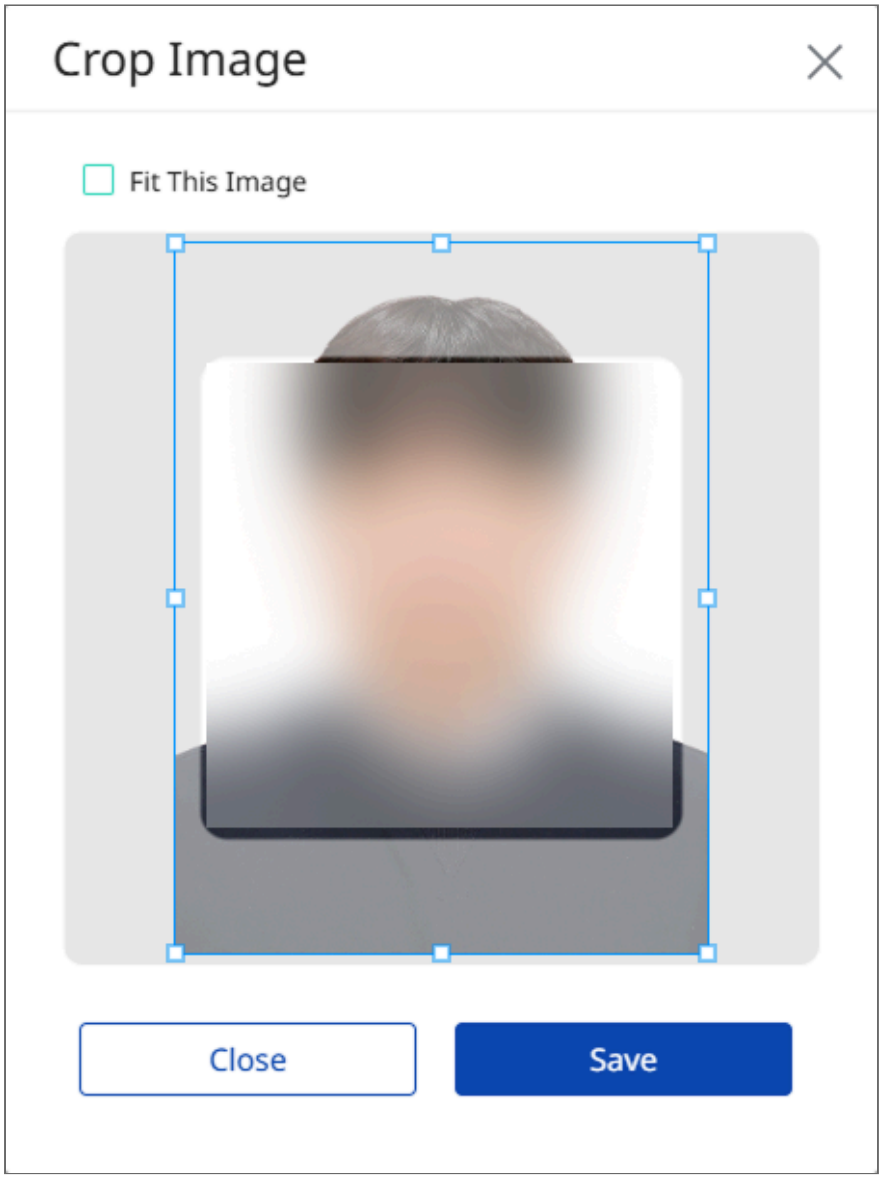
Upload profile image

Web

1. Hover over the profile image area and click the plus icon.

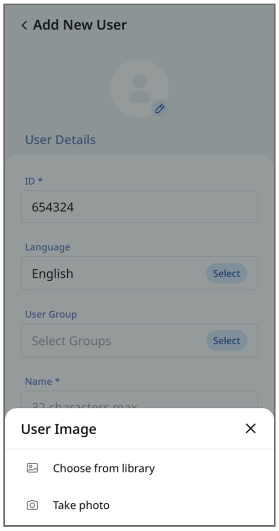


2. Select the image file saved locally.
3. When the **Crop Image** window appears, adjust the photo to the desired size. Click **Fit This Image** to resize the image automatically.



4. Click **Save** to save the uploaded image as the profile image.

Mobile



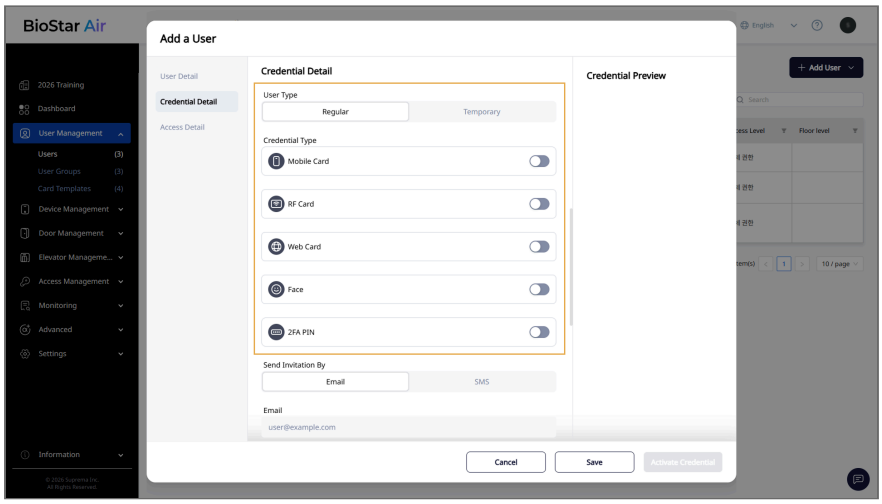
1. Tap the user profile image.
2. Choose how to add an image from the menu that appears at the bottom.
   - **Choose from library**: Select an image file saved on your mobile device to upload.
   - **Take photo**: Use your mobile device's camera to take a photo and upload it.
3. Resize the uploaded image to an appropriate size and save it.

Select user type

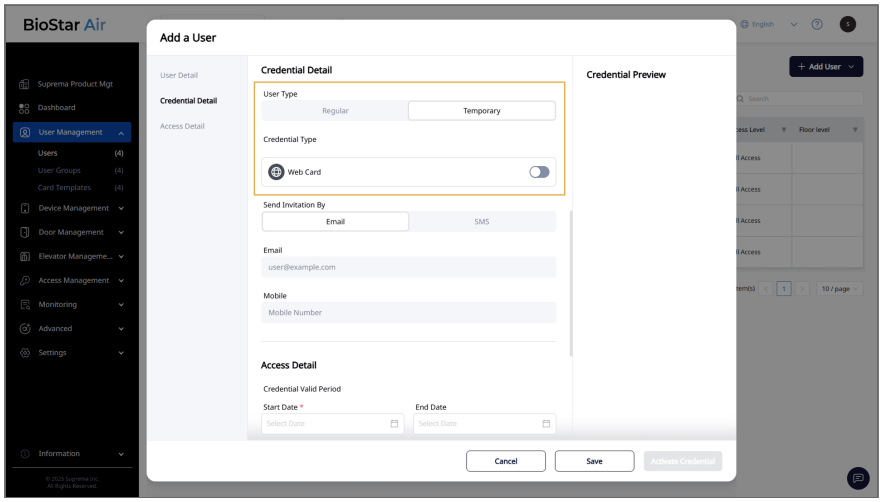
Web

Select whether the user you are adding in the **Credential Detail** section is a regular user or a visitor. The credential types that can be issued vary by user type.

- **Regular**: A user who is a regular member of an organization or facility and requires long-term, ongoing access. All credential types can be issued.

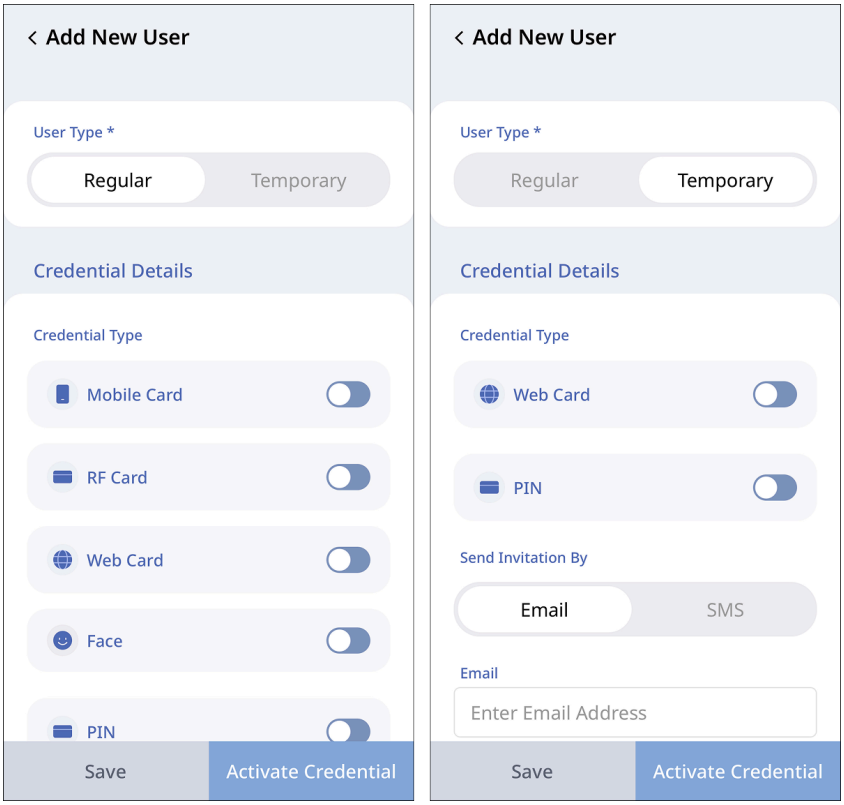


- **Temporary**: A visitor or non-regular member who needs short-term, limited access. This can include guests, external visitors, short-term contractors, delivery couriers, and so on. Only **Web Card** credentials, including QR code and LinkPass, can be issued.



Mobile

Select whether the user you are adding in **Credential Detail** is a regular user or a visitor. The credential types that can be issued vary by user type.



- **Regular**: A user who is a regular member of an organization or facility and requires long-term, ongoing access. All credential types can be issued.
- **Temporary**: A visitor or non-regular member who needs short-term, limited access. This can include guests, external visitors, short-term contractors, delivery couriers, and so on. Only **Web Card** credentials, including QR code and LinkPass, can be issued.

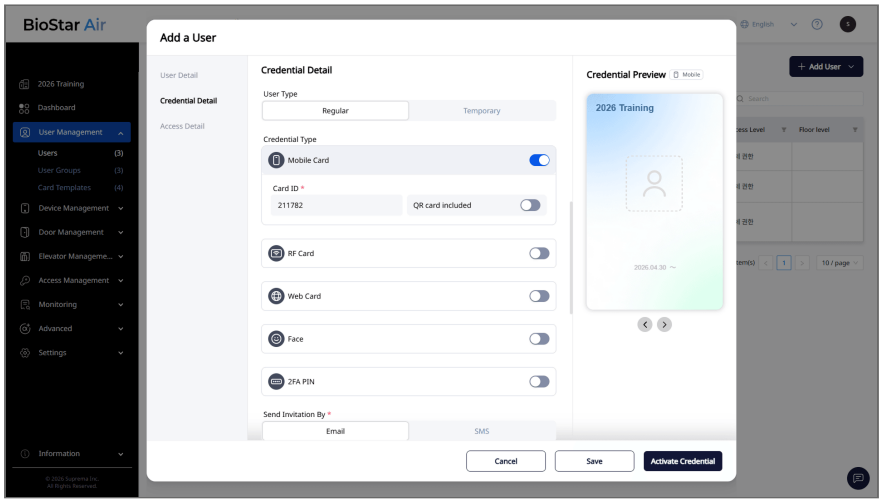
> **Info**
>
> - **Regular** users are automatically assigned the full access level, whereas **Temporary** users must manually select an access level.
> - **User Type** is supported in BioStar Air version 2.6 or higher.

Issue credentials

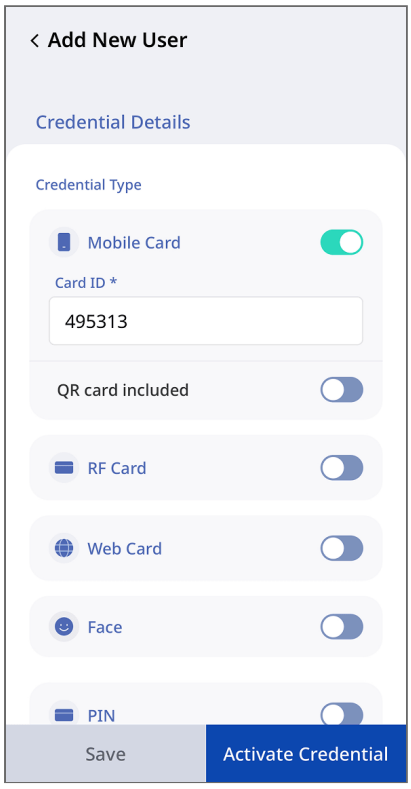
Enter user information, and then set the credentials to use for access authentication in the **Credential Detail** section. Each credential has a toggle switch to enable or disable it.

- **Mobile Card**: Use the Suprema Pass mobile app as an access authentication method. The administrator can edit the card ID number.

Web

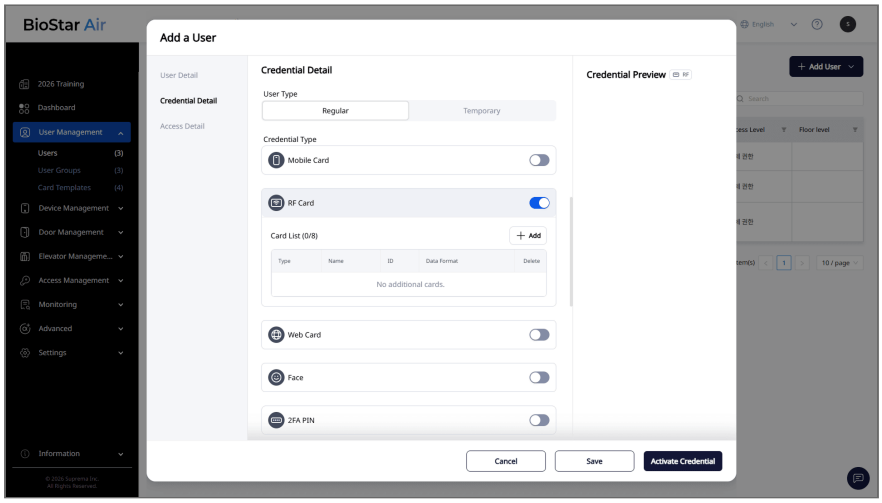


Mobile

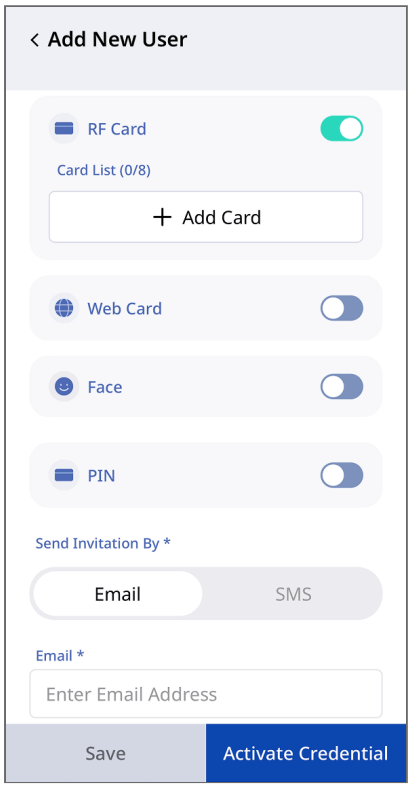


- **RF Card**: Add up to eight RFID cards per user for access authentication. Click **Add**.

Web

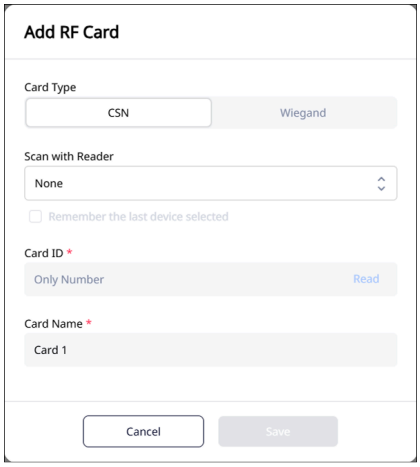


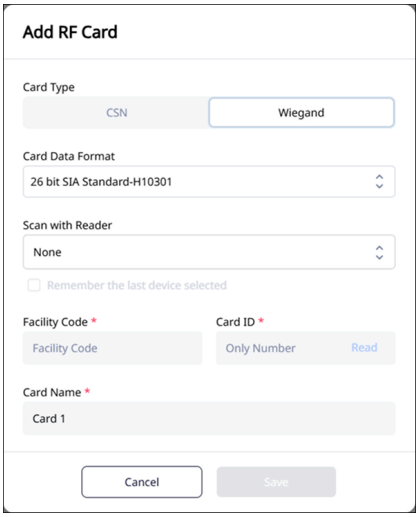
Mobile



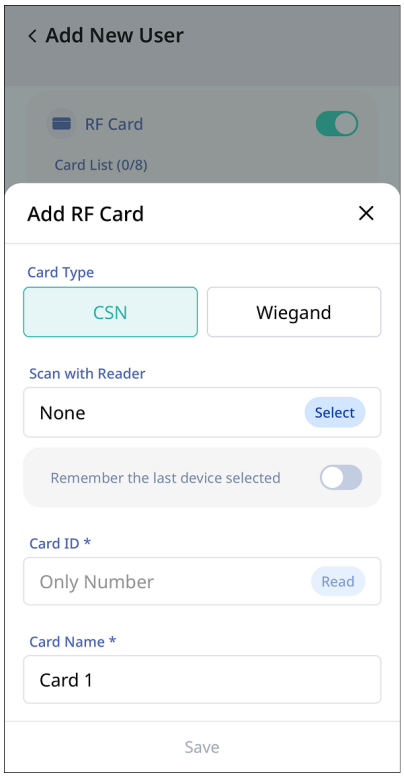
Configure the card type (CSN or Wiegand), card ID, and card name. Select a reader in **Scan with Reader**. Alternatively, scan a physical RFID card with the connected reader.

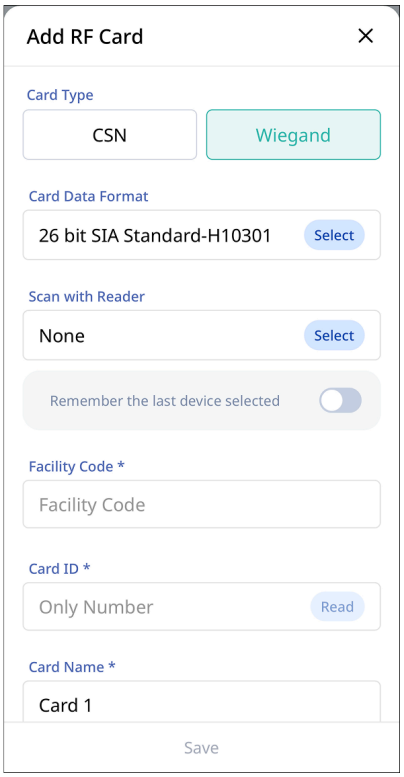
Web





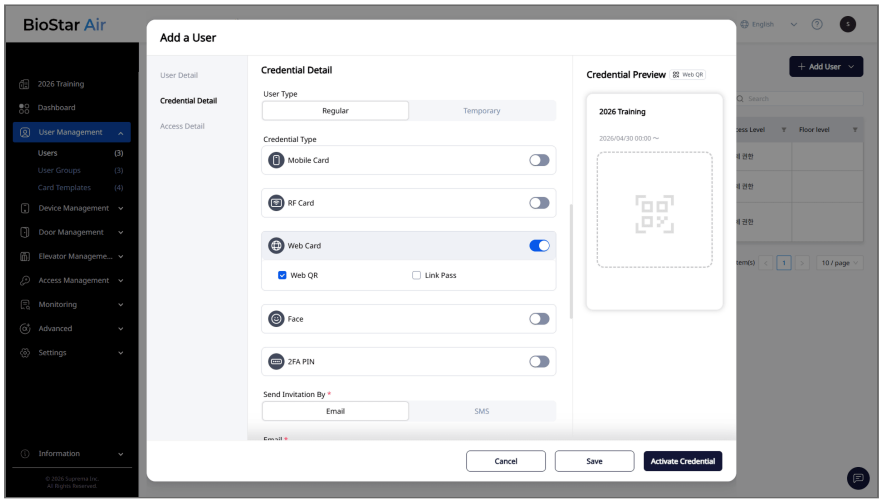
Mobile



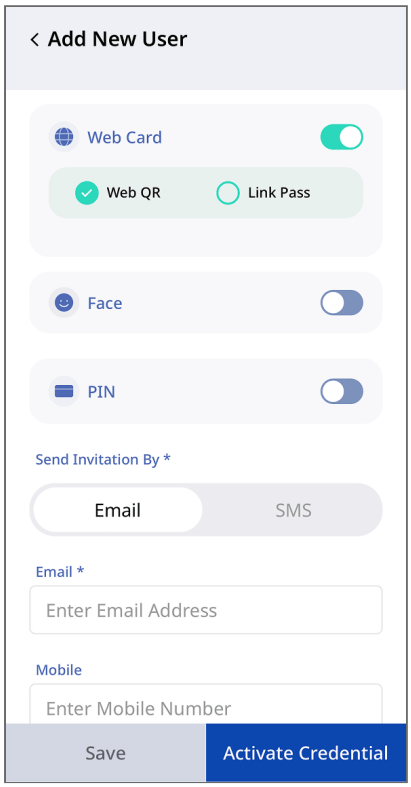


- **Web Card**: Use **Web QR** or **Link Pass** as access authentication methods.

Web



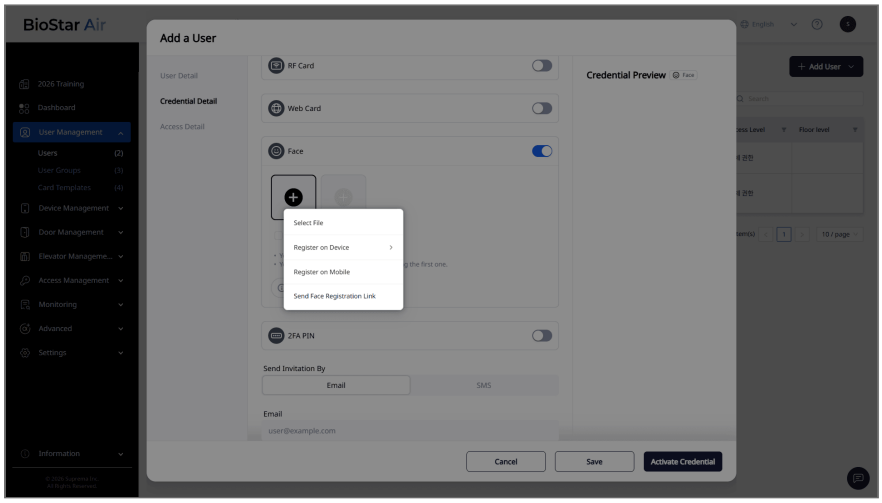
Mobile



> **Web QR** appears only after enabling **QR Reader** at **Settings** → **Site** → **Additional Features**.

- **Face**: Add up to two face profile images for access authentication. You can upload an existing image or enroll it using a connected reader. Alternatively, send the user a link by email or SMS so they can enroll directly using their mobile device's camera.

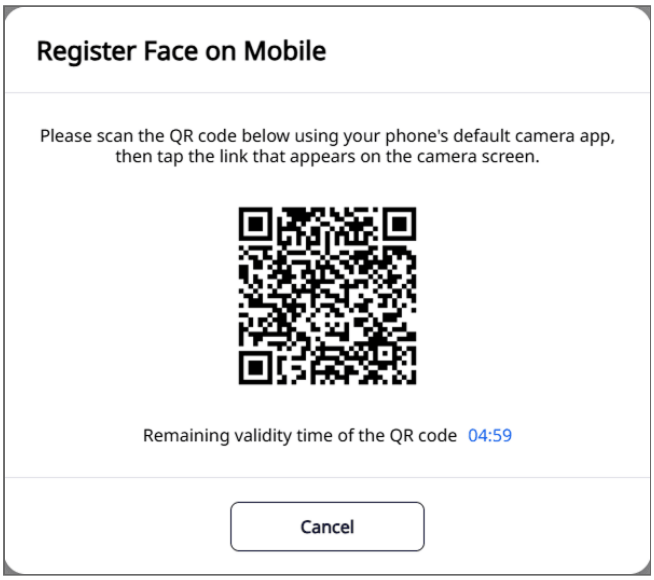
Web



– **Select File**: Select an image file saved locally to upload.

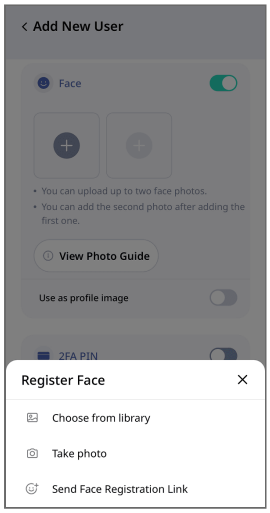
– **Register on Device**: Use the connected reader to enroll a face image.

– **Register on Mobile**: Scan a QR code with a mobile device's camera to open a link for face image enrollment.



– **Send Face Registration Link**: Send the user a face enrollment link by email or SMS so they can enroll their face directly using their mobile device's camera.

Mobile



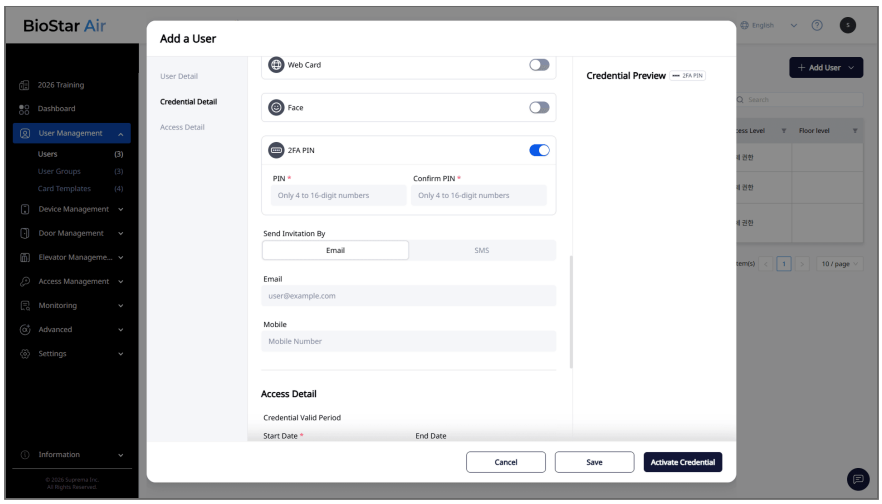
Tap + to add a face photo. Choose how to add a face photo from the menu that appears at the bottom.

- **Choose from library**: Select an image file saved on your mobile device to upload.
- **Take photo**: Use your mobile device's camera to take a photo and upload it.
- **Send Face Registration Link**: Send the user a face enrollment link by email so they can enroll their face directly using their mobile device's camera.
- **Use as profile image**: You can use the image currently set as your profile picture as your face credential.

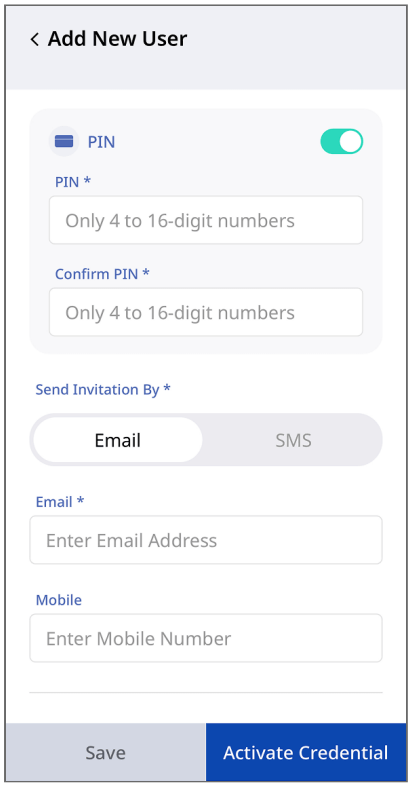
> For more information on enrolling a face photo, see **View Photo Guide**.

- **2FA PIN**: Set a 4–16-digit PIN to use as part of two-factor authentication (2FA).

Web



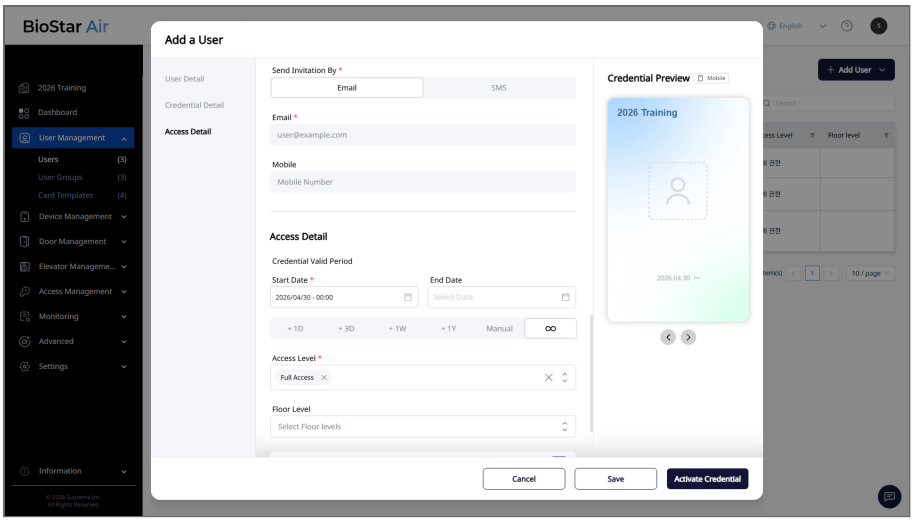
Mobile



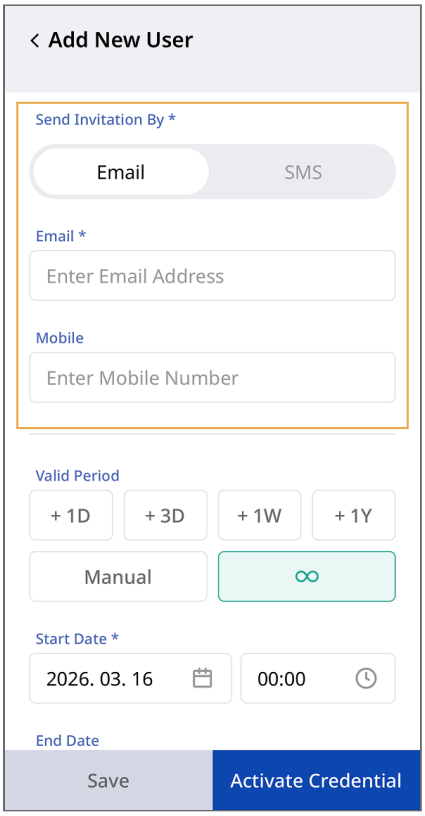
Send invitation link

Email the Suprema Pass app download link to users who use **Mobile Card** or **Web Card**. Enter the email address (required) and phone number (optional).

Web



Mobile



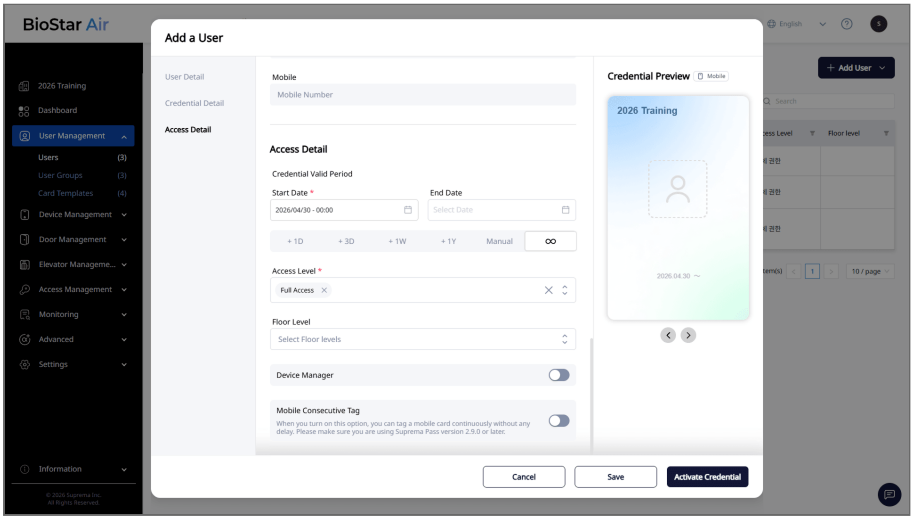
Info

Request SMS credit recharge in **Settings** → **Credit Center** to use the **SMS** option.

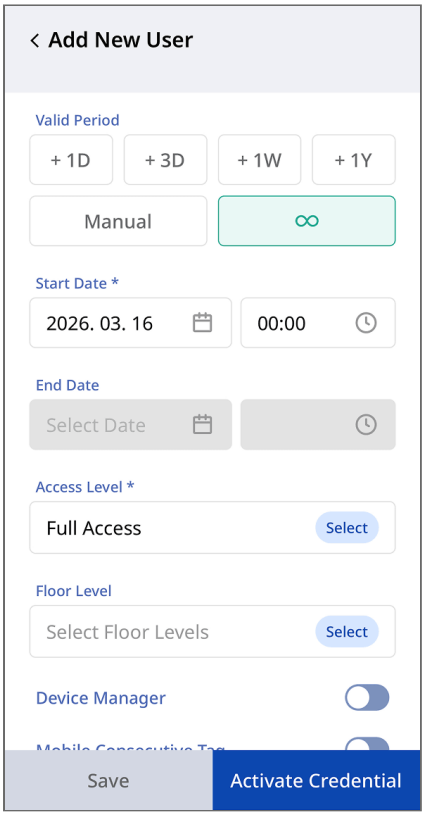
Set access levels and validity

After selecting credentials, configure the credential validity period, access levels, and floor levels in the **Access Detail** section.

Web



Mobile



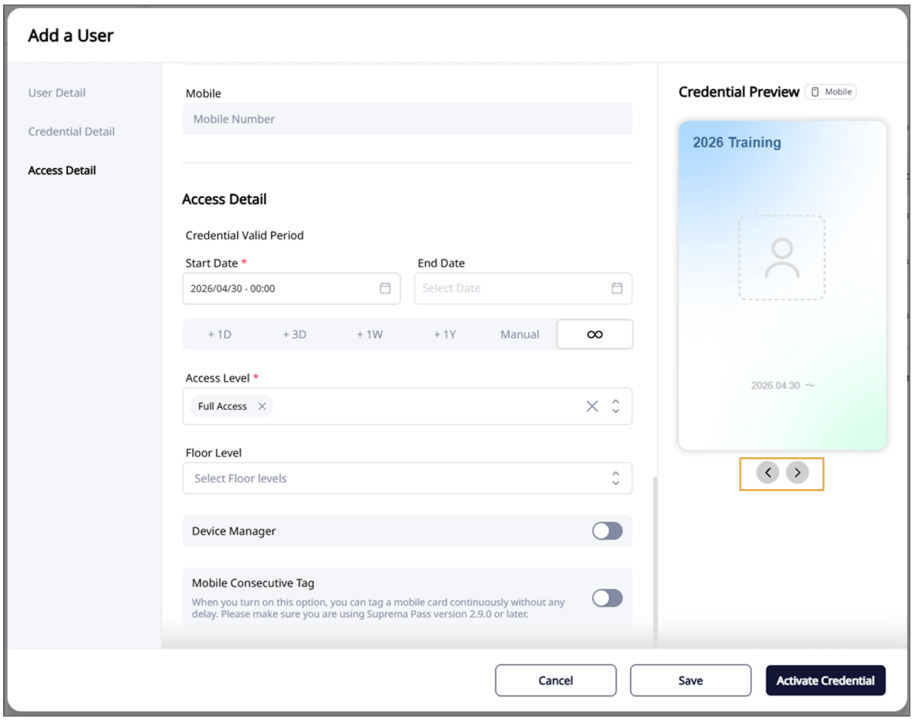
- **Credential Valid Period**: Set the validity period of the credentials issued to the user. Click ∞ to leave the expiration date open-ended.
- **Access Level**: Select the access levels for the user. Grant full access or choose a predefined access level.
- **Floor Level**: Select the floor levels the user can access.
- **Device Manager**: Allow a user to manage access permissions on a specific reader.
- **Mobile Consecutive Tag**: Allows consecutive mobile card tags without wait time. This feature is supported in Suprema Pass app version 2.9.0 or higher.

> **Info**
>
> - For more information on floor-level settings, see Manage Floor Levels.
> - The **Device Manager** option is available only to BioStation 3 and X-Station 2 users. Users set as device managers can access the administrator menu on BioStation 3 and X-Station 2 devices.

Select card template

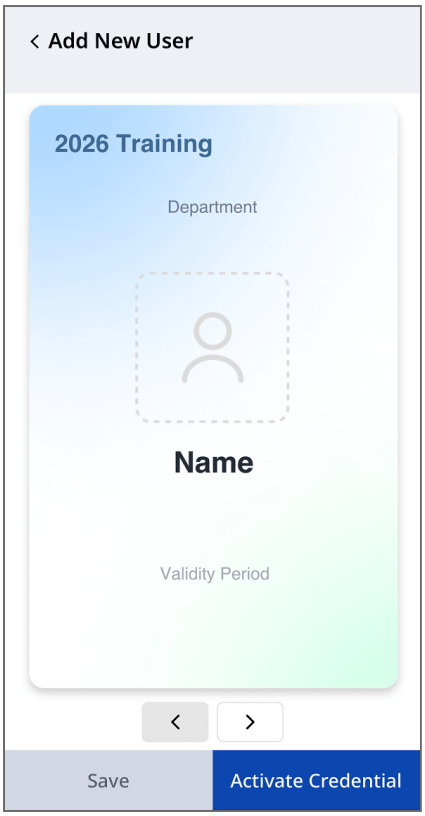
Web

Click ‹ or › under Card Template in the right panel to change the card template design.



Mobile

Tab ‹ or › on **Credential Preview** to change the card template design.



Info

For more information about creating new card templates, see Manage Card Templates.

Save or activate the user

After configuring all user settings, choose one of the following options.

- Click **Save** to save the user for later activation.
- Click **Activate Credential** to issue and activate the credentials immediately.

Next step

After you've learned how to add individual users, learn how to register multiple users at once.

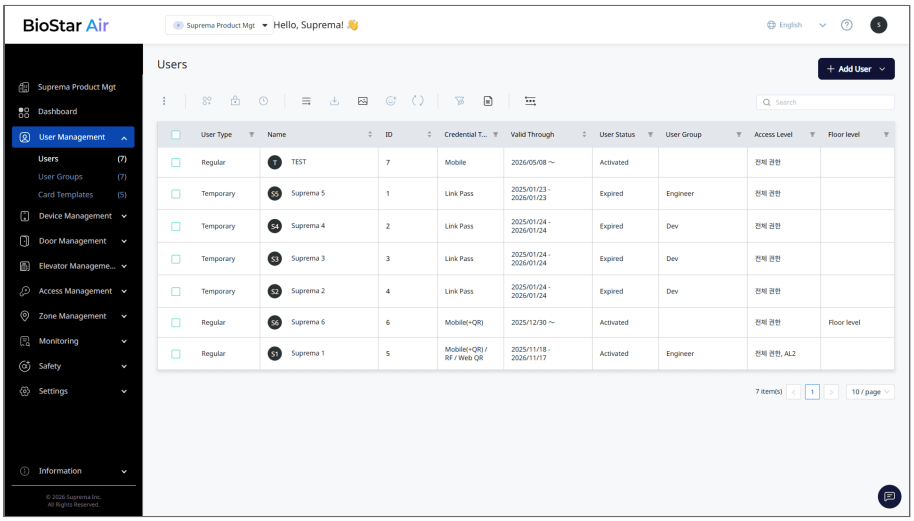
Manage Users
The user list is an essential management tool for administrators responsible for access control in an organization. You can perform all user management tasks, including organizational management through user grouping, immediate response to new or departing employees with real-time activation/suspension, integrated management of various credentials, enhanced security through validity period monitoring, and preparation for reporting and auditing through filtering and report generation.

View the user list

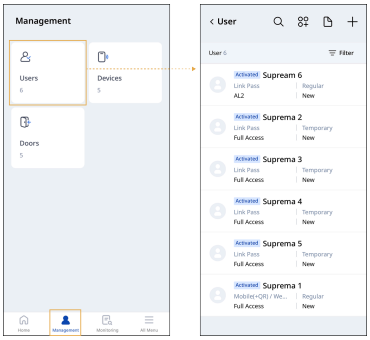
The user list shows all users registered in BioStar Air at a glance. View each user's details and use the filter and sort features to quickly find specific users. Edit, delete, and assign groups to users directly from the user list.

Web

Click **User Management** → **Users** in the left sidebar.



Mobile



Use the user management feature in the BioStar Air app.

1. Run **BioStar Air** on your mobile device.
2. Tap **Management** in the bottom navigation bar.
3. Tap **Users**.

A list of users appears. Add new users or edit existing user details.

User information

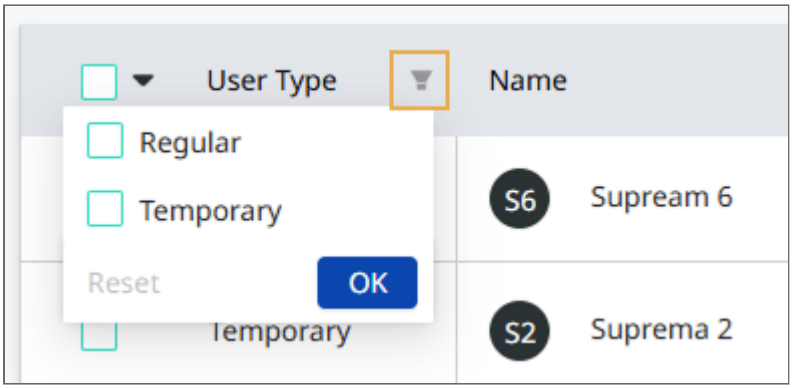
The table in the user list provides the following information.

- **User Type**: Indicates whether the user is a regular or temporary user. For more information on regular and temporary users, refer to User Card and Credential Types.
- **Name**: The user's name.
- **ID**: The user's unique ID.
- **Credential Type**: Shows the credentials issued to the user. For more information on the types of credentials, refer to User Card and Credential Types.
- **Valid Through**: The validity period of the credentials issued to the user.
- **User Status**: Indicates whether the user is active or inactive.
- **User Group**: The group to which the user belongs. For more information on user groups, refer to Manage User Groups.
- **Access Level**: The access level assigned to the user. For more information on access levels, refer to Manage Access Levels.
- **Floor level**: The user's permissions for floors they can access. For more information on floor levels, refer to Manage Floor Levels.

Filter

Web

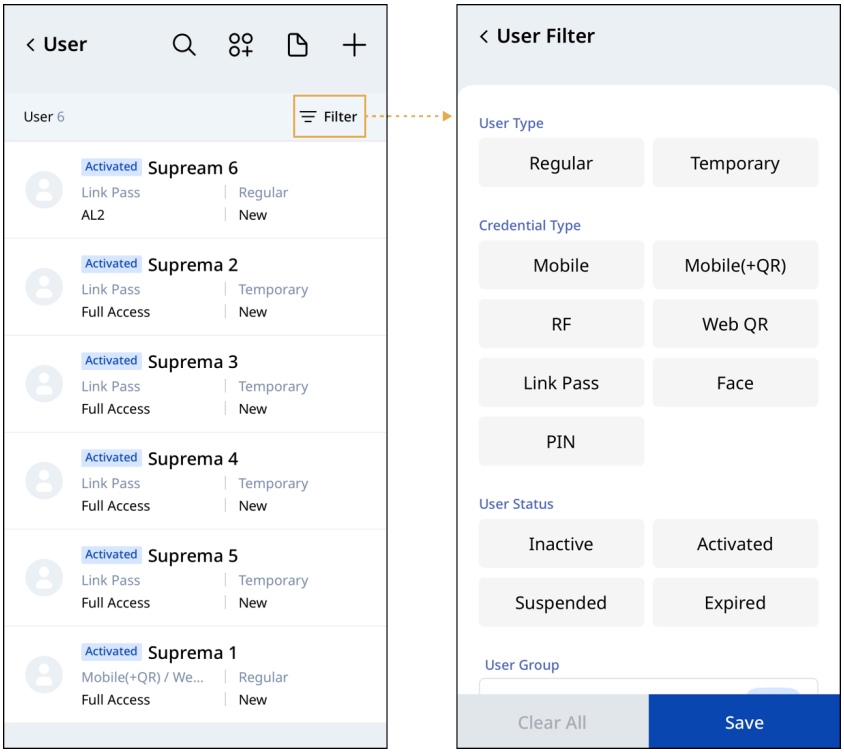
Use the filter feature in the top header of the user list. Click in the header to set the desired conditions.



> **Info**
>
> Click at the top of the user list to reset the applied filter conditions.

Mobile

In the mobile app, you can filter and view users in the user list by the desired criteria. Tap **Filters** at the top right of the user list. Users can be filtered by the following criteria.

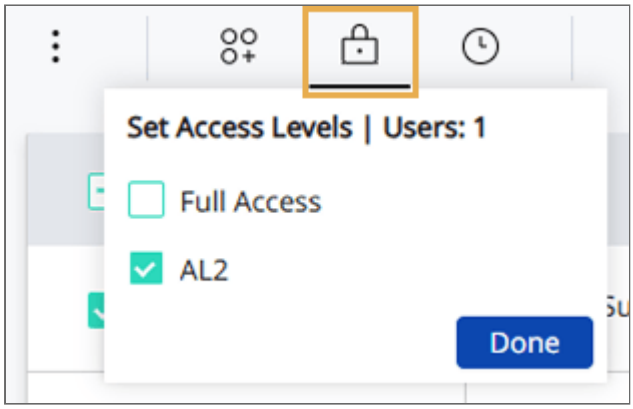


- **User Type**: Filters by user type (regular or temporary).
- **Credential Type**: Filters by credential type.
- **User Status**: Filters by activation status.
- **User Group**: Filters by user group.

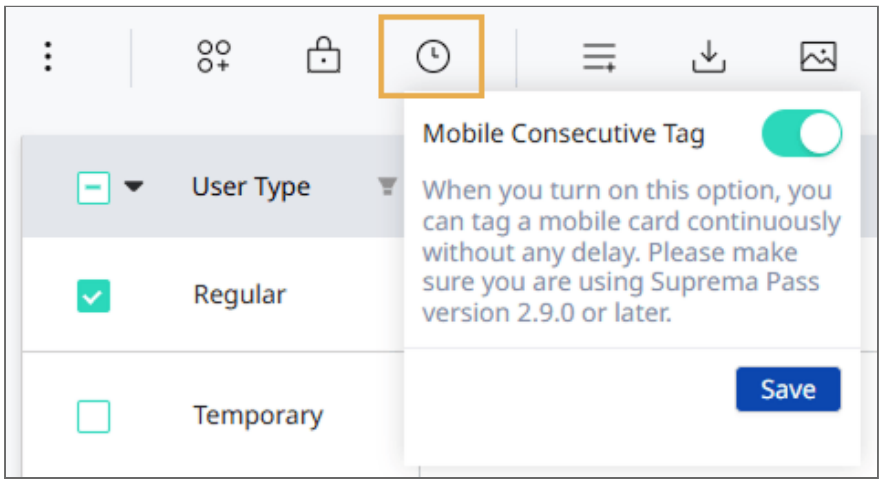
Additional features

The features available at the top of the user list are as follows.

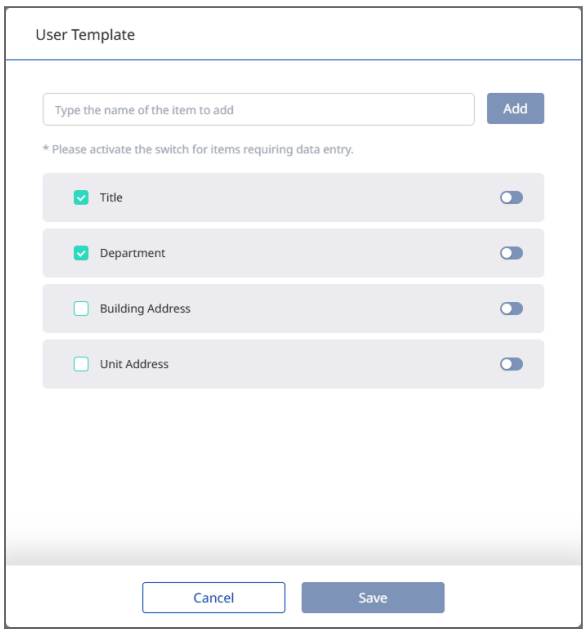
- : Assign, remove, or move the selected users to a group. For more information, refer to Manage user groups.
- : Change the access level of the selected users. For more information about access levels, see Manage Access Levels.



- : Allow the selected users to tag mobile cards consecutively without waiting time. The Suprema Pass app supports this starting from version 2.9.0.



- : Apply a user template to the selected users. Add any other information needed in addition to the default user information.



- : Export the selected user information to a PDF or CSV file.
- : Upload user images in bulk. The name of each image file to upload must match the user's ID.

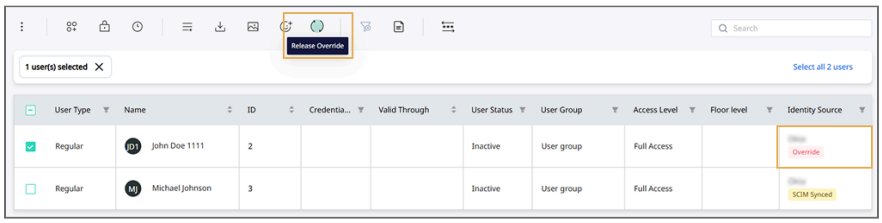
  For example, the file 601.jpg corresponds to user ID 601.

> **File format requirements**
> – Supported formats: *.jpg*, *.jpeg*, *.png*
> – File size limit: **1 MB** per image

- : Send a face enrollment link to the selected users by email or text message. When a user clicks the link and enrolls their face on the webpage, they are granted access via facial authentication.

> The link cannot be sent to users without a registered email address or phone number.

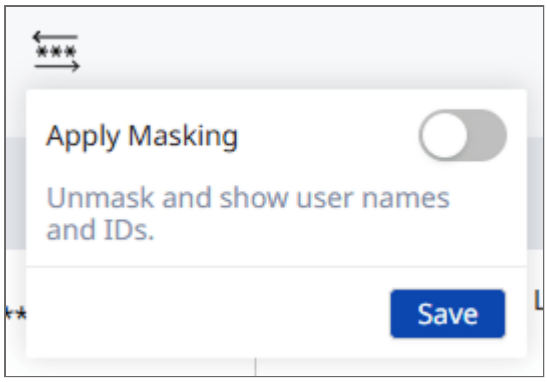
- : If you manually change local user information for SCIM-synced users, the status changes to **Override**. Cancel local changes to return to SCIM-managed status. For more information, see Set Up SSO & SCIM.



- : Reset all filters applied to the user list. This feature is available only when filters are applied. For more information on applying filtering, refer to Filter.

- : Configure user reports. After a report is generated, it is sent to the administrator's email. For more information on report configuring, refer to Create a user report.

- : Mask(***) the information such as name and ID in the user list to protect privacy. This feature is useful in environments requiring privacy. Select the toggle button to enable this feature, and click **Save**.

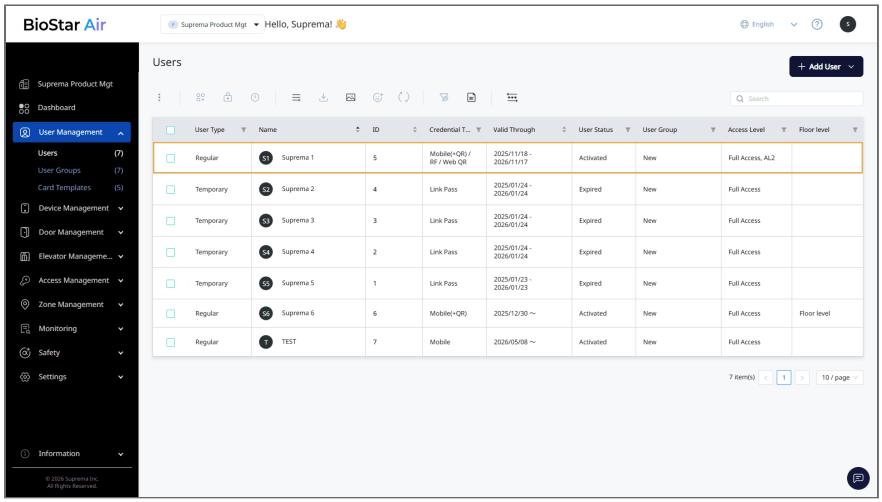


Edit user information

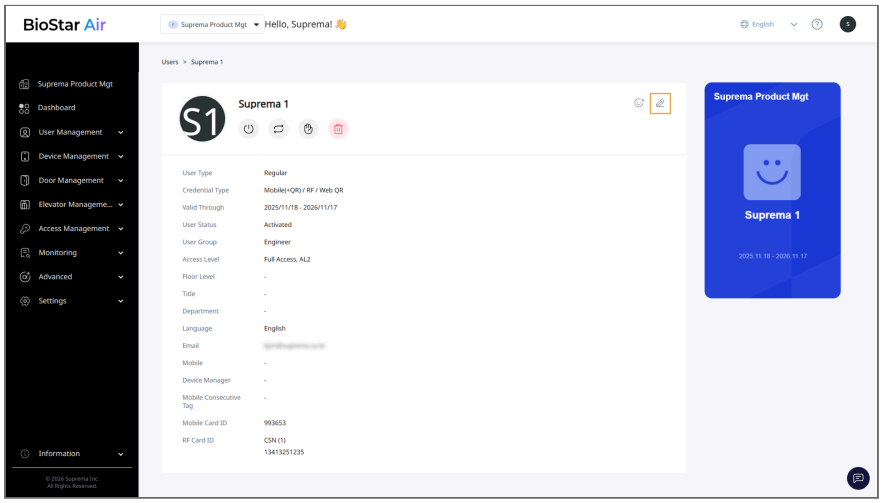
Web

Follow these steps to edit a user's details or change their credentials.

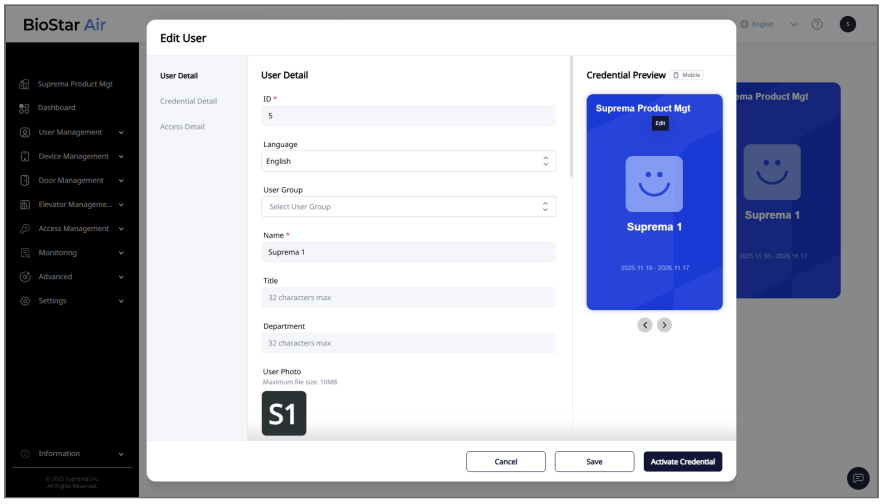
1. Click **User Management** → **Users** in the left sidebar.
2. Click the user you want to edit in the list.



3. Click ✎ in the top right of the user details.

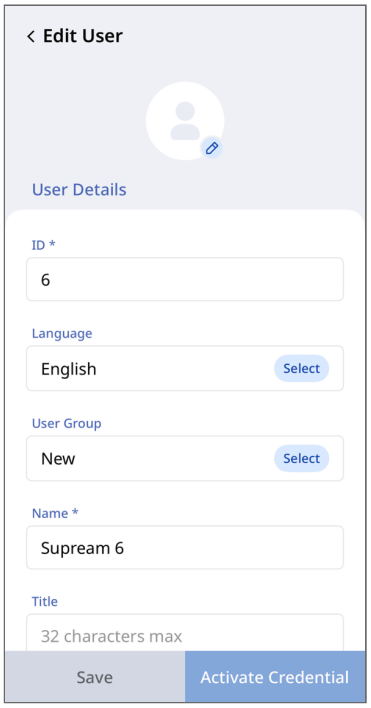


4. Edit the required details when the **Edit User** window appears.



5. After editing, click **Save** at the bottom right.

Mobile



To edit the detail information of user in the mobile app, follow these steps.

1. Tap the user to edit in the user list.
2. Tap in the top right.
3. Edit the necessary information on the **Edit User** screen.
4. To save the changes, tap **Save**.

   Use **Activate Credential** to issue credentials.

> **Info**
> For more information on user information, refer to Add Users.

Manage user groups

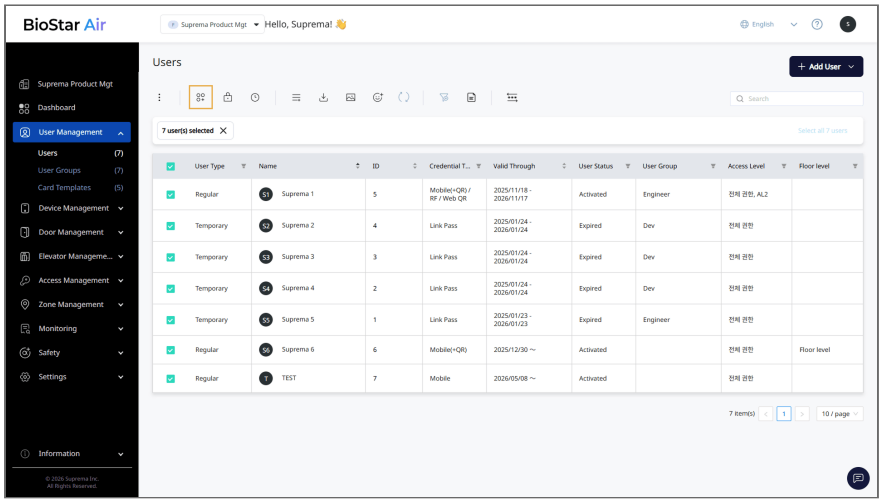
This guide describes how to assign or move, exclude user from user group. For more information on creating and managing user group, refer to Manage User Groups.

Web

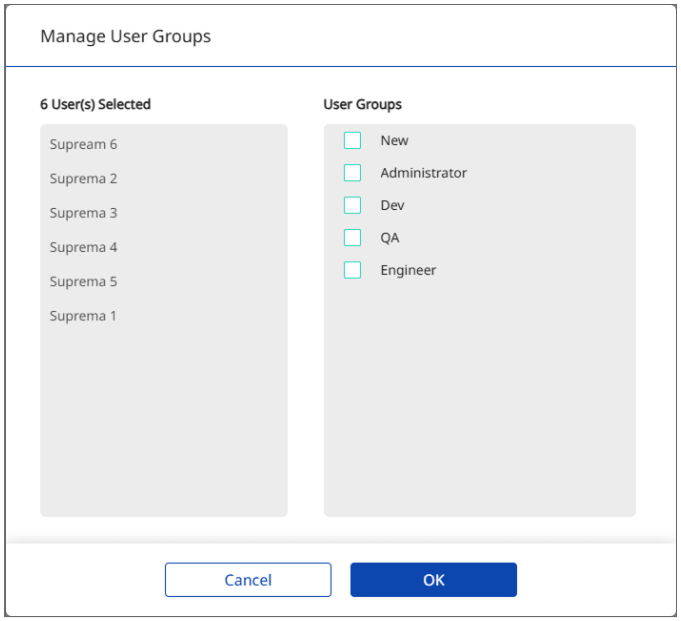
Assign users to a group

After creating a user group, you can add users to the group from the user list.

1. Click **User Management** → **Users** in the left sidebar.
2. Click the checkbox next to the users to assign to the group in the user list.
3. Click at the top left of the user list.

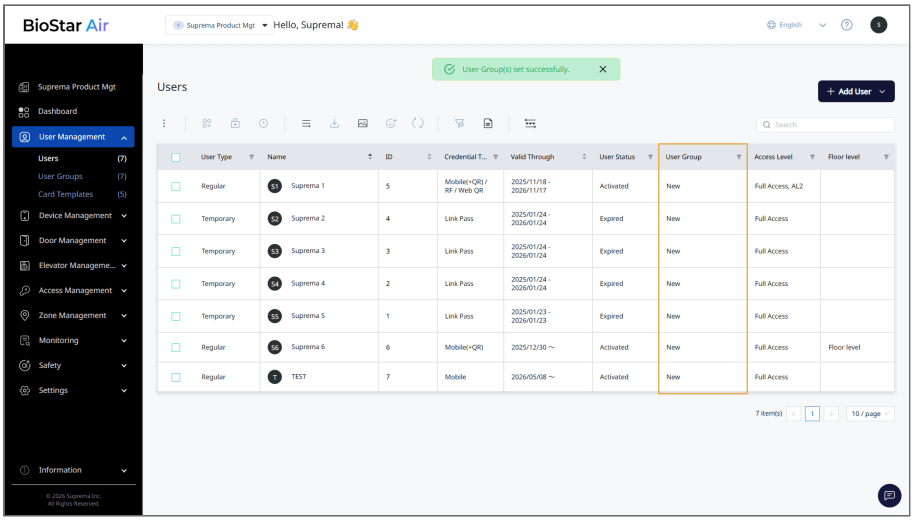


4. When the **Manage User Groups** window appears, select the parent group or subgroup to assign the users.



5. Complete the selecting, and save group settings, click **OK**.

Confirm that the users are assigned to the new group in the **User Group** column of the user list.



Return to **User Groups** to confirm that the group's **Total Users** is updated.

Remove or move group

You can exclude users from a user group or move them to another group.

1. Click **User Management** → **Users** in the left sidebar.
2. Click the checkbox next to the users to remove from or move between groups in the user list.

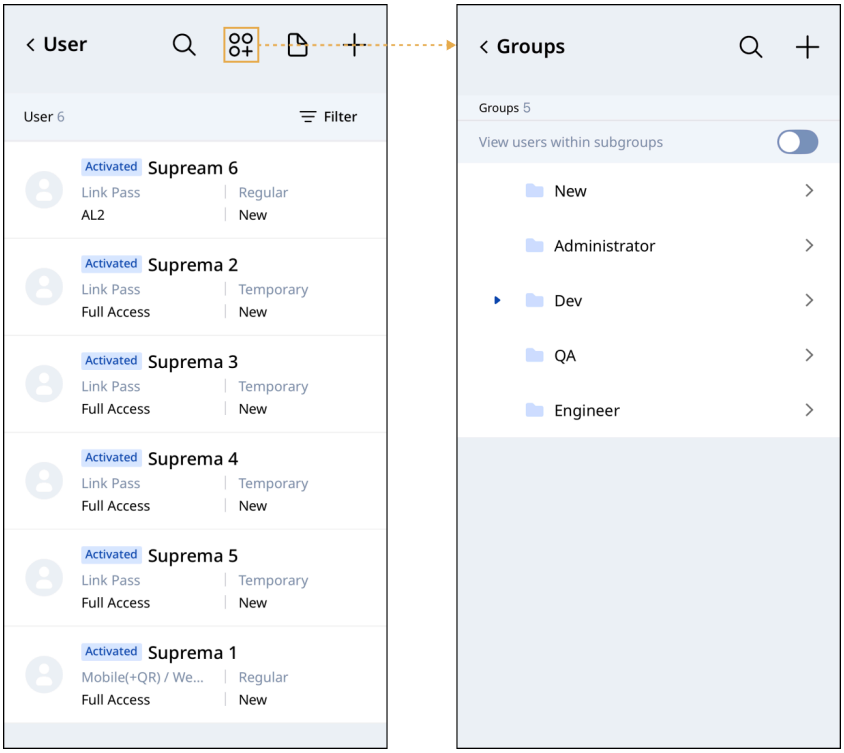
> When moving users, first select users from the same group, then proceed.

3. Click at the top left of the user list.
4. When the **Manage User Groups** window appears, perform one of the following:
   - To unassign the group, clear the selected group's checkbox.
   - To move the group, select the checkbox for the current group and then choose the target group.
5. Click **OK** to save the group settings.

Confirm the group changes in the **User Group** column of the user list.

Mobile

You can manage user groups in the mobile app. Tap at the top of the user list. The user group list appears.



- To view users in a group, tap › to the right of the desired group.
- To add a new group, tap + in the top right.
- To edit a group name, long-press the desired group and tap at the bottom.
- To delete a group, long-press the desired group and tap at the bottom. Select one or more groups to delete them.

> **Info**
>
> For more information on managing user group, refer to Manage User Groups.

Manage user status

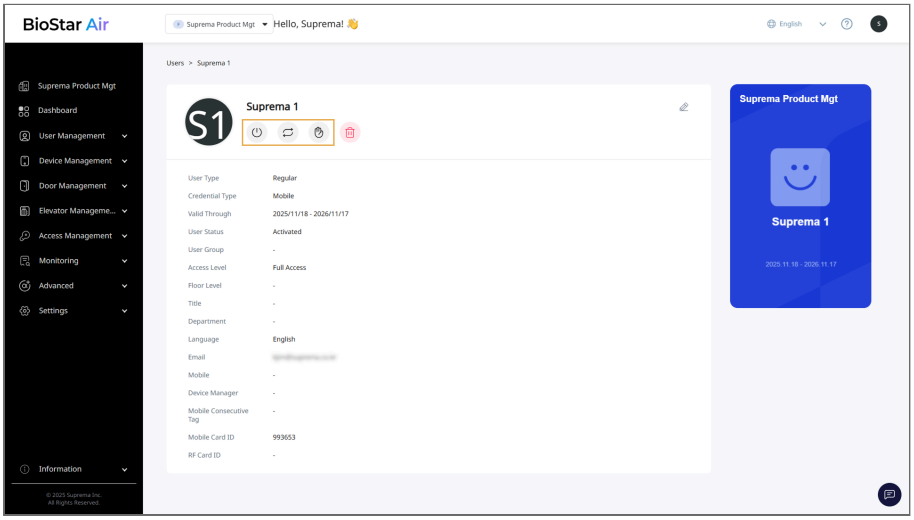
Activate or suspend a user's access permissions. Reissue credentials as well.

> **Info**
>
> When an administrator reissues a user's credentials in BioStar Air, previously issued mobile credentials, QR codes, and LinkPasses are revoked and replaced. The user will receive an email or SMS, depending on site settings, containing a link to the updated credentials. The user must follow the link to download the new mobile credential into the Suprema Pass app or access the new QR code or LinkPass. Access attempts using revoked mobile credentials, QR codes, or LinkPasses will fail.

Individual user

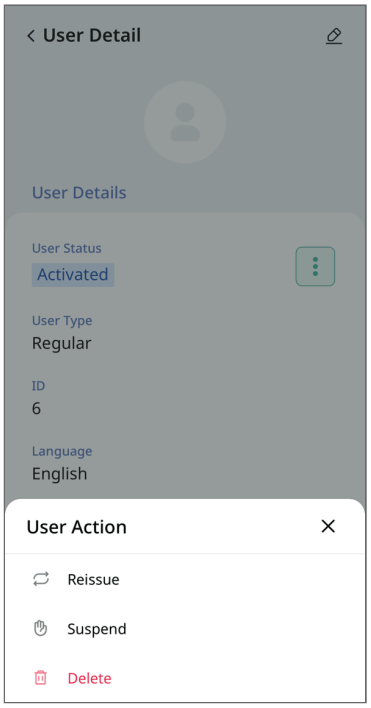
Web

1. Click **User Management** → **Users** in the left sidebar.
2. Click the user in the list to change their status.
3. Select the desired action at the top of the user details.



- : Activate the user's access permissions. Use this feature for initial activation of new users or reactivation of suspended users.
- : Reissue credentials. Use this feature when the user's credentials have expired or are unavailable.
- : Block the user's access. Use this feature when the user is active.

Mobile



In the mobile app, tap a user in the list. In the **User Detail** screen, tap ⋮. The **User actions** menu appears.

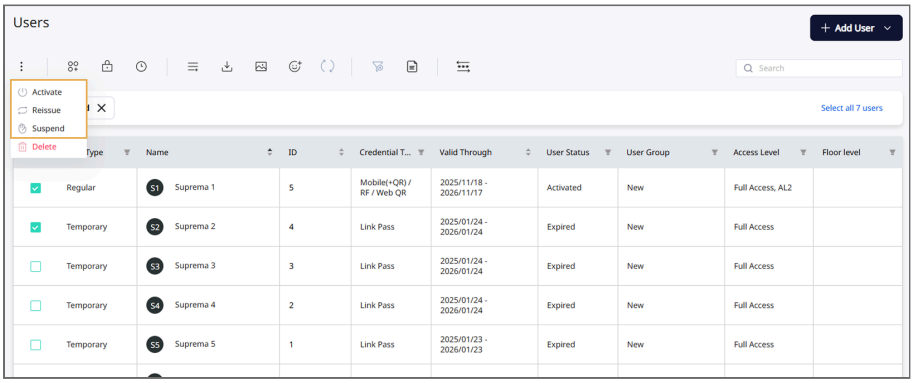
- **Activate** / **Reactivate**: Activate the user's access permissions. Use this feature for initial activation of new users or reactivation of suspended users.
- **Reissue**: Reissues the user's credentials.
- **Suspend**: Temporarily deactivates the user. Suspended users cannot access.
- **Delete**: Deletes the user from the system.

> **Info**
> The **Reactivate** option appears only for suspended users.

Batch actions

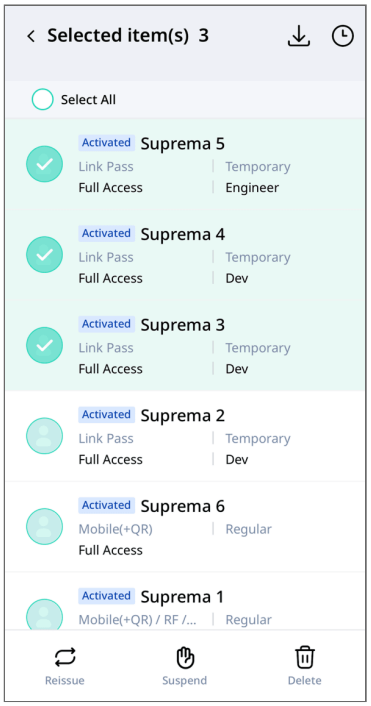
Web

1. Click **User Management** → **Users** in the left sidebar.
2. Click the checkbox of each user in the list to change their status. You can select more than one user.
3. Click ⋮ at the top left of the screen and select the desired action from the pop-up menu.



- **Activate** / **Reactivate**: Activate the user's access permissions. Use this feature for initial activation of new users or reactivation of suspended users.
- **Reissue**: Reissue credentials. Use this feature when the user's credentials have expired or are unavailable.
- **Suspend**: Block the user's access. Use this feature when the user is active.

Mobile



In the mobile app, long-press a user in the list to change their status. Select any additional users whose status you want to change. Tap the desired action in the **User actions** menu at the bottom of the screen.

- **Activate** / **Reactivate**: Activate the user's access permissions. Use this feature for initial activation of new users or reactivation of suspended users.
- **Reissue**: Reissues the user's credentials.
- **Suspend**: Temporarily deactivates the user. Suspended users cannot access.
- **Delete**: Deletes the user from the system.

> **Info**
> The **Reactivate** option appears only for suspended users.

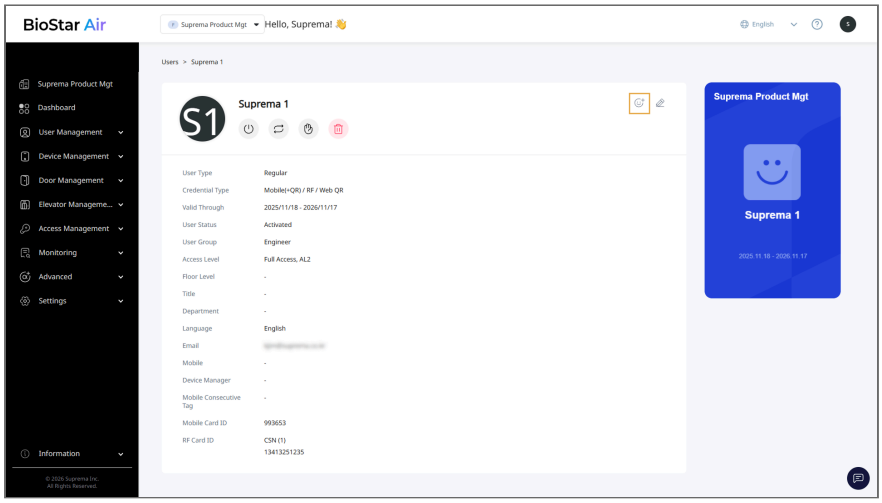
Send face enrollment link

Send a face enrollment link to existing users by email or text message to guide them to enroll faces. When a user clicks the link and enrolls their face on the web page, they are granted access via Facial Authentication.

> **Info**
> The link cannot be sent to users without a registered email address or phone number.

Individual user

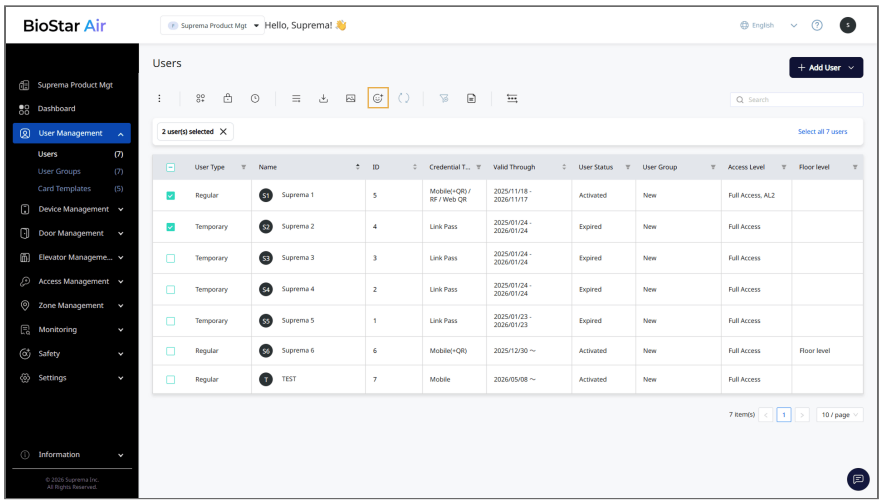
1. Click **User Management** → **Users** in the left sidebar.
2. Click the user in the list to send the face enrollment link.
3. Click the button in the top right of the user details.



4. When a pop-up message appears, click the **Yes** button.

Batch actions

1. Click **User Management** → **Users** in the left sidebar.
2. Select the checkboxes of the users in the list to send the face enrollment link. You can select more than one user.
3. Click the button in the upper left of the screen.



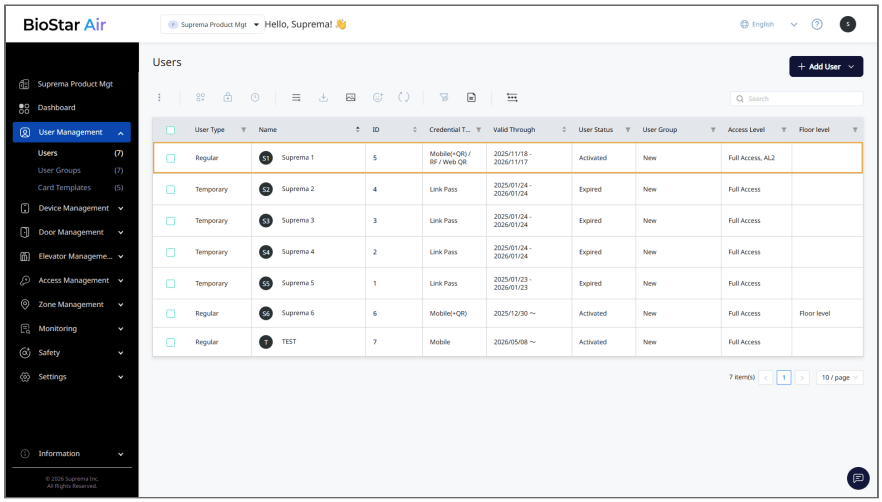
4. When a pop-up message appears, click the **Yes** button.

Delete users

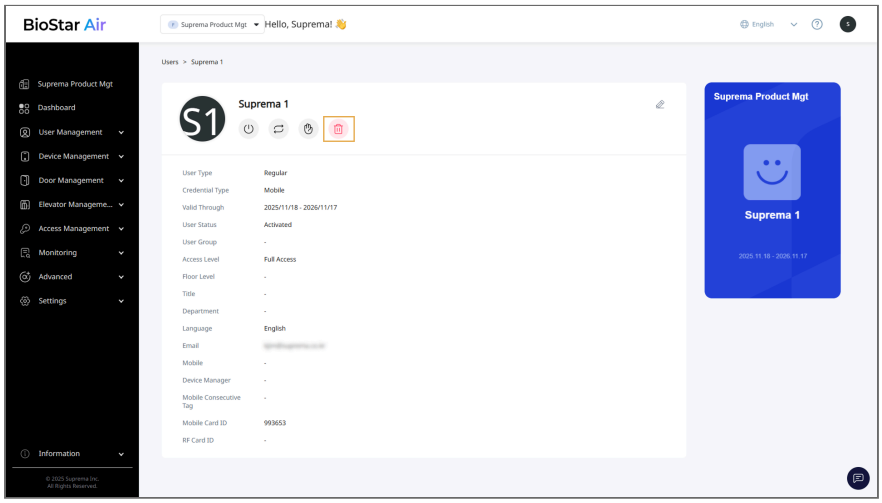
> **Caution**
> Deleted users cannot be recovered. Be sure to verify before deleting.

Individual user

1. Click **User Management** → **Users** in the left sidebar.
2. Click the user you want to delete in the list.



3. Click in the user details.

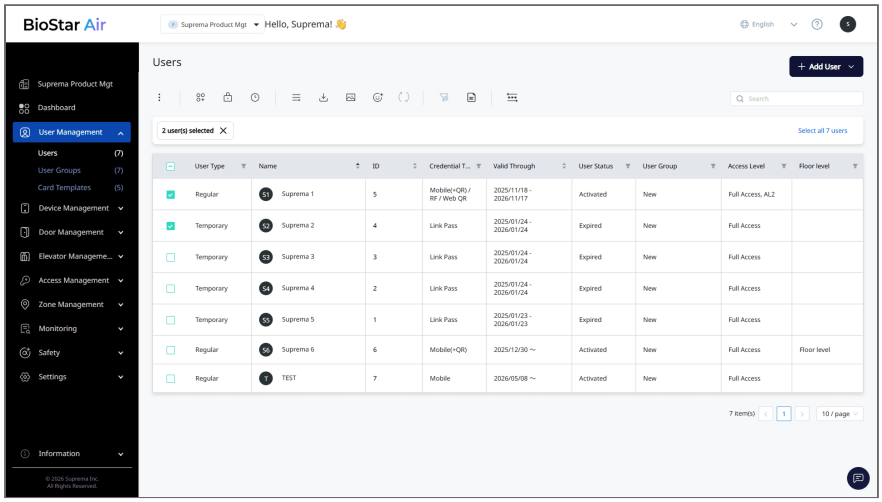


4. When a warning message appears, click **Yes**.

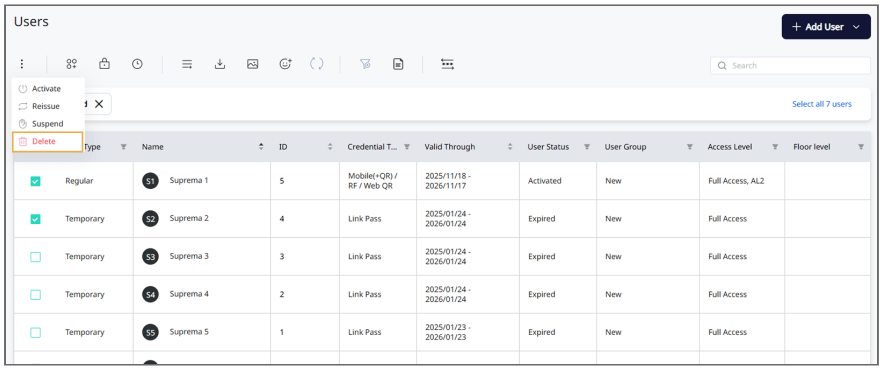
Batch delete users

1. Click **User Management** → **Users** in the left sidebar.

2. Click the checkbox of each user you want to delete in the list. You can select more than one user.



3. Click ⋮ → **Delete** at the top left of the screen.

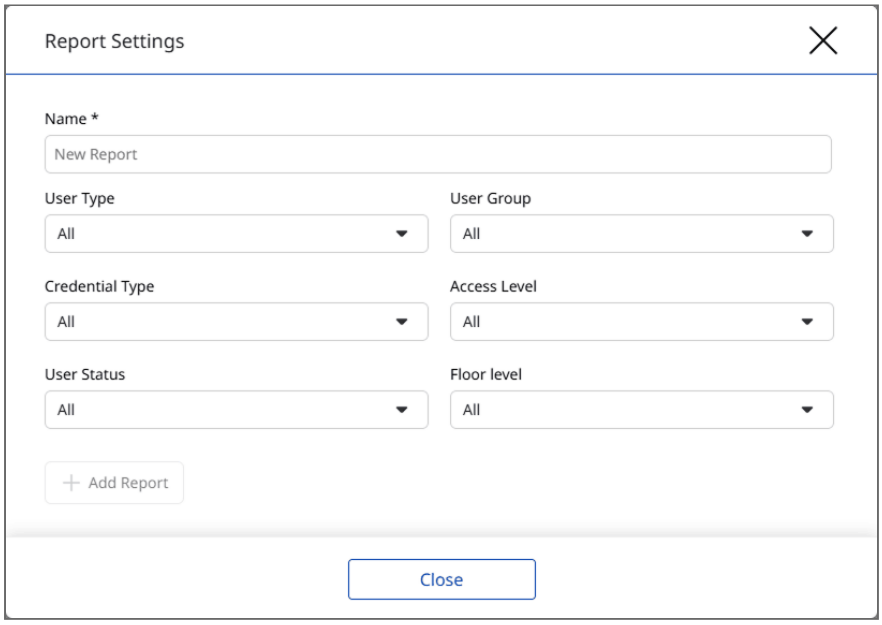


4. When a warning message appears, click **Yes**.

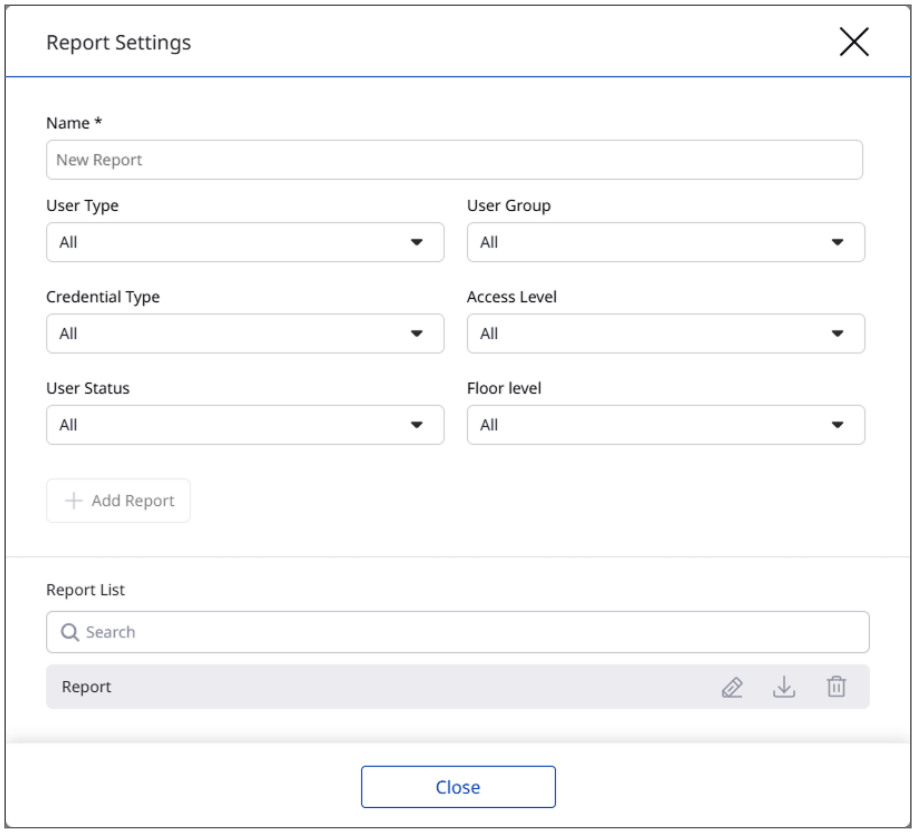
Create a user report

Create a user report and send it to the administrator's email.

1. Click at the top of the user list.
2. When the **Report Settings** window appears, enter a report name.



3. Select the items to include in the report from each filter option.
4. Click **Add Report** to save the report.
5. A **Report List** is created and a download link is sent to the administrator's email.

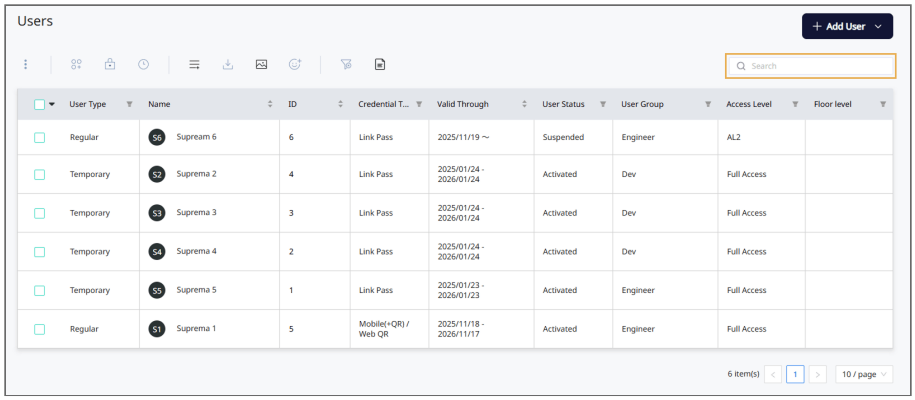


Info

In **Report List**, search for, edit, download, or delete generated reports.

Search users

Use the search field in the top right of the user list to quickly find specific users. Search by user name, ID, or phone number.



Add Users in Bulk

If you need to add multiple users at once, use BioStar Air's bulk user import feature. Upload a CSV file to register tens or hundreds of employees in just minutes. You can also bulk-upload profile images while entering user information. This document provides step-by-step instructions for downloading the CSV template, preparing the file, uploading it, managing profile images, and verifying user information after upload.

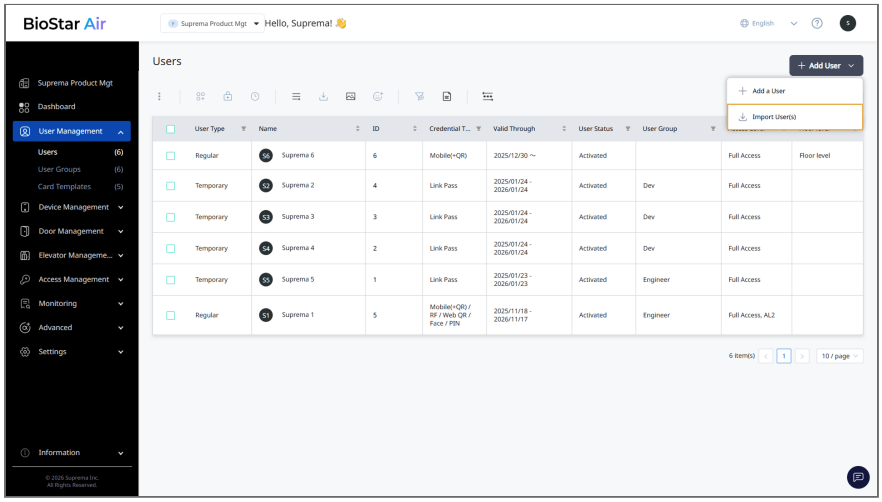
Tip

Refer to the following video for a step-by-step guide to adding multiple users in bulk.

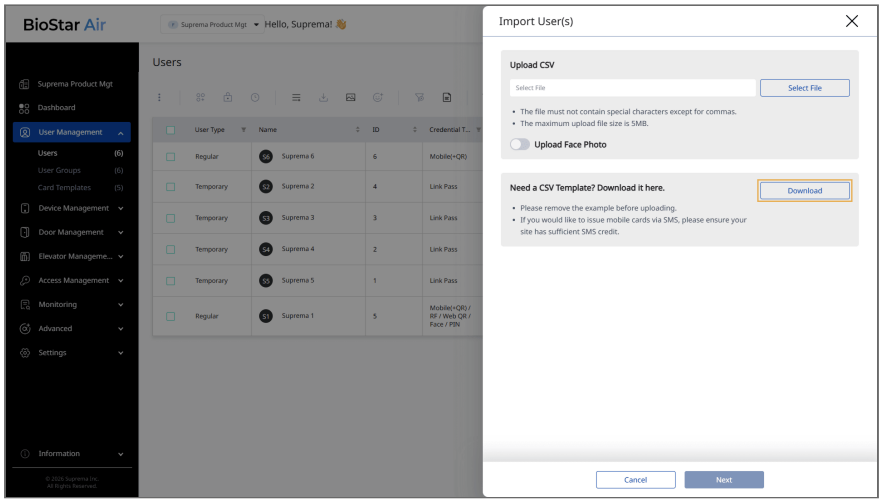
Download the CSV template

Follow these steps to download the CSV template file.

1. Click **User Management** → **Users** in the left sidebar.
2. Click **Add User** → **Import User(s)** at the top right of the screen.



3. When the **Import User(s)** panel appears, click **Download**.



4. Save the CSV template file (*biostar-import-user-csv-example.csv*) locally.

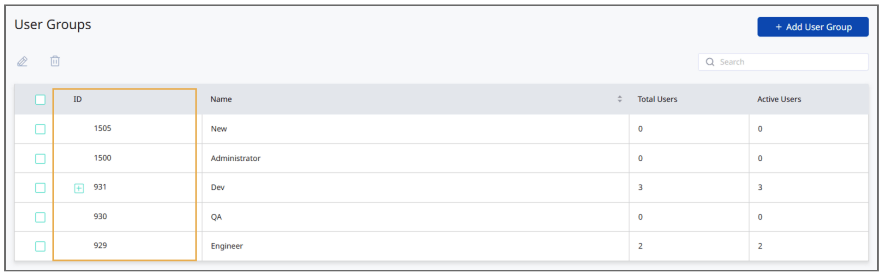
Prepare the CSV file

Download the CSV template and enter the required details for each user.

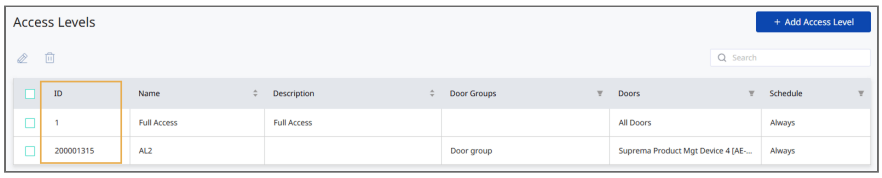
Key input fields

The key fields to enter are as follows.

- **Group IDs**: Check the group ID in **User Management** → **User Groups**.



- **Access level IDs**: Check the access level ID in **Access Management** → **Access Levels**. **Full Access** is always set to **1**. Use commas (`,`) as separators to specify multiple access levels.



- **Email**: Enter this if you plan to send invitations by email.
- **Mobile**: Enter this if you plan to send invitations by mobile SMS.

> **Caution**
> **Email** and **Mobile** must not be duplicated. Uploading a CSV file with duplicate values may cause errors.

Support for custom Wiegand formats

You can freely configure any Wiegand format, including facility codes, segments, parity bits, and more.

- HID Corporate 1000 and iCLASS SE and Seos formats are supported.
- **CSV template**
  - Each defined format (custom or default) appears as a separate column in the CSV file.

    > ***26 bit SIA Standard-H10301***, ***HID 37 bit-H10302***, ***HID 37 bit-H10304***, ***HID Corporate 1000***, ***HID Corporate 1000 48bit***

  - Separate multiple entries in a single field with a slash (`/`).
  - Use single quotes (`'`) around the card name. Avoid using double quotes (`"`); they may cause errors.

    > ✓ *'CardName'* | ✗ *"CardName"*

> **Example**
> - With a facility code: *1234567-100-'Main Office Card'* (`CardID` - `FacilityCode` - `'CardName'`)
> - With multiple segments: *12-3456-78-'Lab Entry Card'*

Support for multiple cards

- Assign up to eight CSN or Wiegand card formats per user.
- **CSV template**

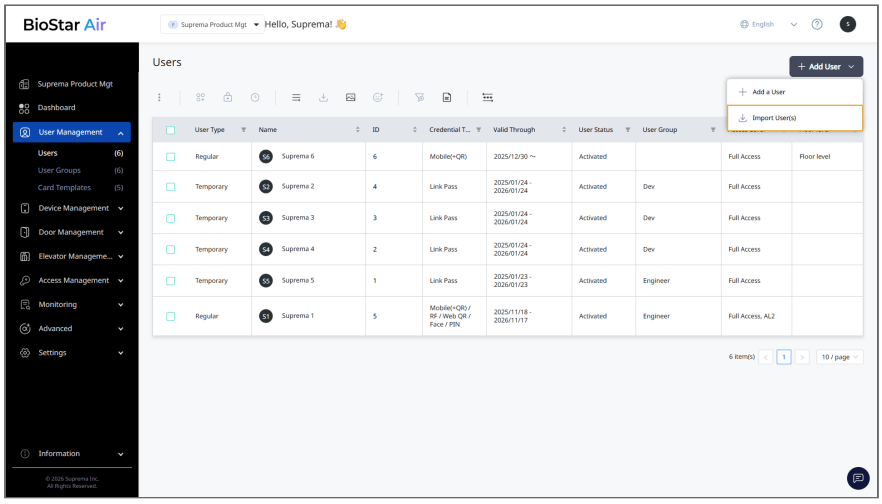
- For a single card, enter the CSN card number.
- Separate CSN card numbers with a slash (/) when enrolling multiple cards.

> **Card naming format:** CSN - 'Card Name'
>
> Example: *1234567-'Main Entry' / 7654321-'Back Door'*

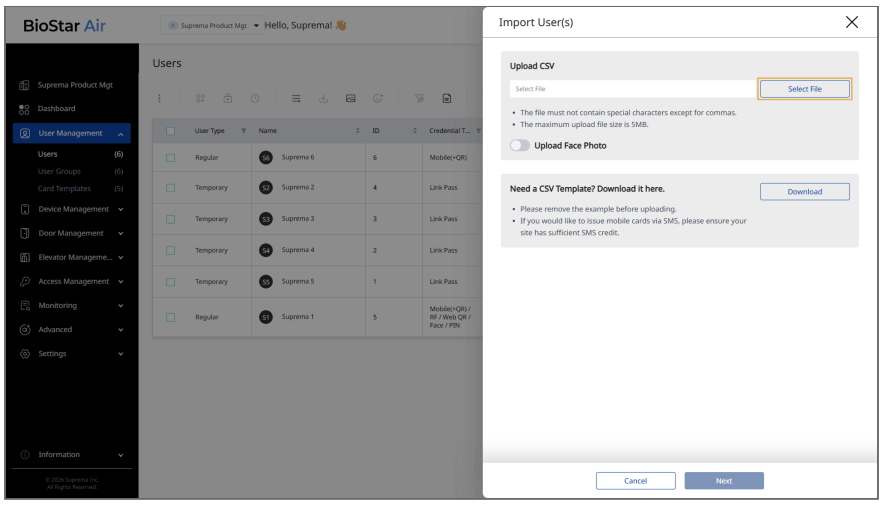
Upload the CSV file

After preparing the CSV file, upload it.

1. Click **User Management** → **Users** in the left sidebar.
2. Click **Add User** → **Import User(s)** at the top right of the screen.



3. When the **Import User(s)** panel appears, click **Select File**.

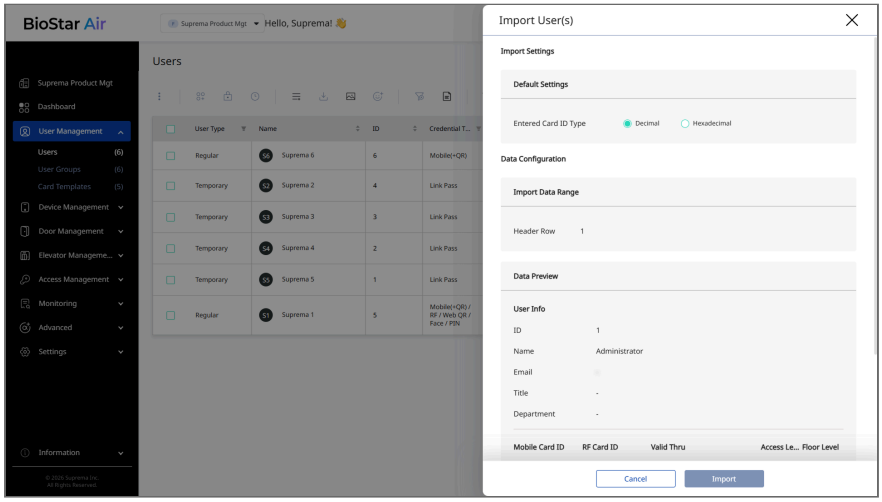


4. Select the CSV file you prepared.

> If the users' profile images are ready, enable the **Upload Face Photo** option. For more information, see Upload user profile images.

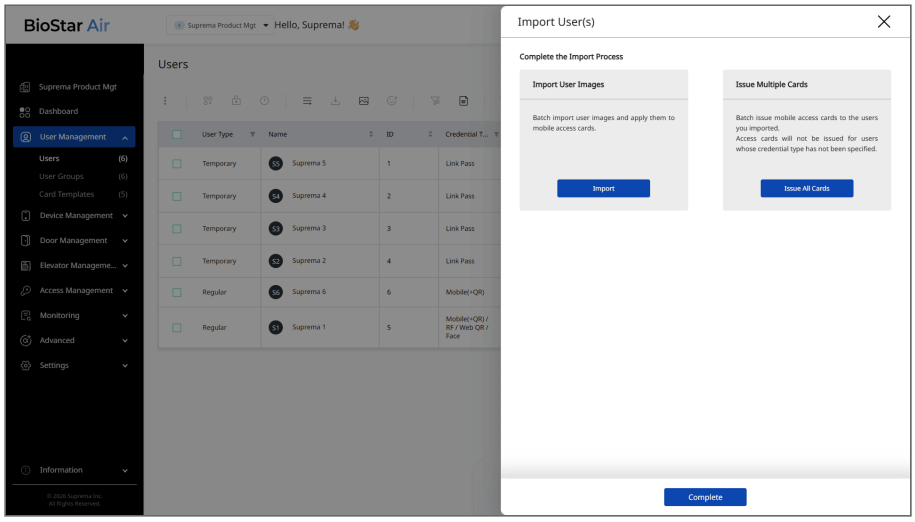
5. Click **Next** at the bottom right of the screen.

6. In the **Data Preview** section, review the accuracy of the data in the first column.



7. If there are no issues, click **Import** in the bottom right corner.

After the upload completes, you can import user images or issue mobile cards in bulk on the next screen. Select the desired action.

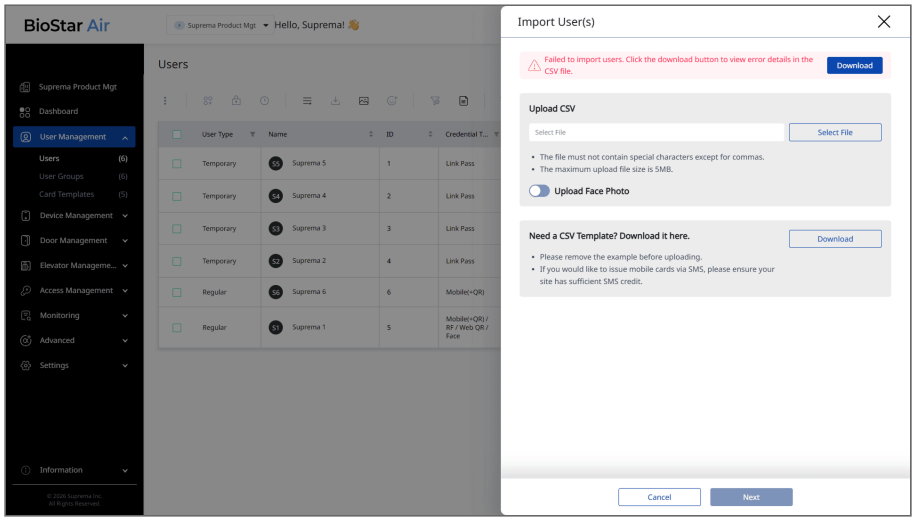


Info

- Do not use special characters other than commas (,) in the CSV file name.
- The maximum CSV file size is **5MB**.
- Alternatively, drag and drop the CSV file into the **Upload CSV** field of the **Import User(s)** panel.

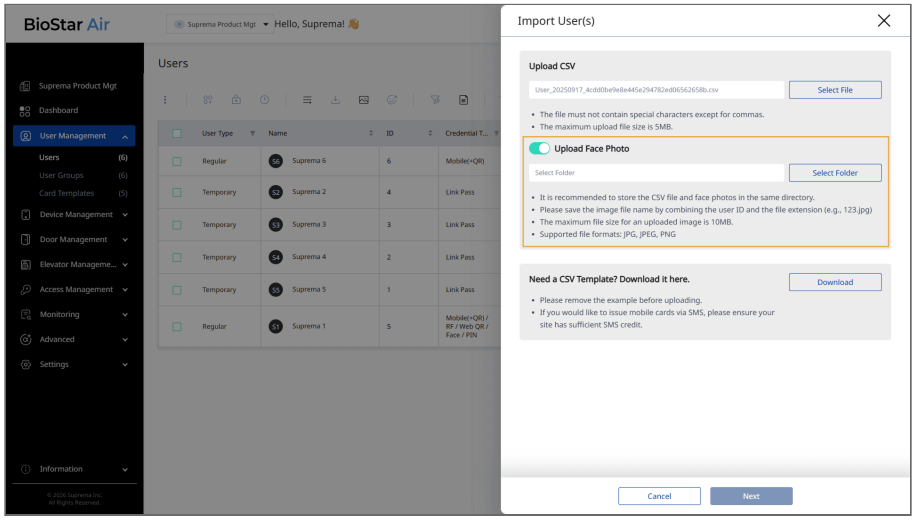
CSV File Validation

The CSV upload process now provides **row-level error feedback**, making troubleshooting easier. If errors occur during upload, a detailed report is provided for review. Click **Download** to download the report.



Upload user profile images

Profile images can be uploaded automatically with the CSV file or manually in bulk later.



1. Prepare profile image files that match the **User Key** column in the CSV file.

   For example, the *601.jpg* file corresponds to user ID **601**.

2. After uploading the CSV file in the **Import User(s)** panel, enable the **Upload Face Photo** option.

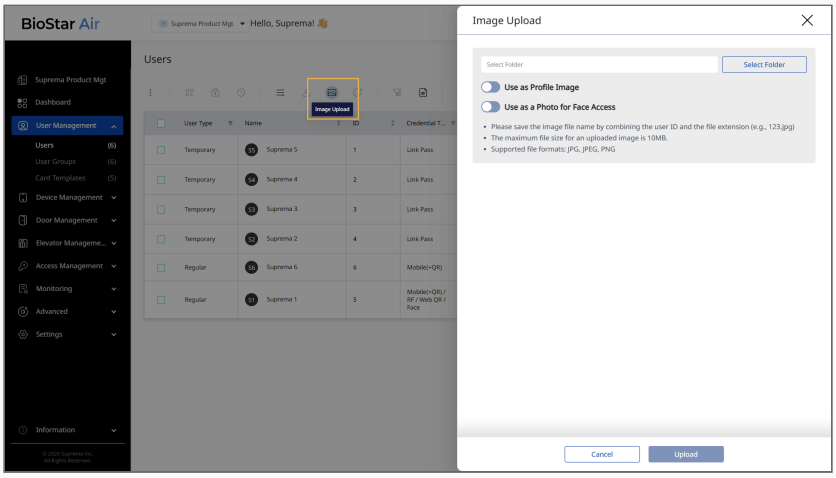
3. Click **Select Folder**, then select the folder that contains the profile images.

File format requirements

- Supported formats: *.jpg*, *.jpeg*, *.png*
- File size limit: **1 MB** per image

Tip

If profile images were not ready when the CSV file was uploaded, use **Image Upload**(🖼) in the user list to add them later.



Finalize the bulk upload

After all user data and images are uploaded, the system processes the entries, and the new users appear in the list with their assigned credentials.

Troubleshooting

If you encounter issues with CSV upload, see Fix Bulk User Addition Issues for help troubleshooting common problems. The document also includes Excel formulas that help validate data and remove duplicates.

Manage User Groups

Use user groups to classify and manage users by department, role, location, and more. BioStar Air user groups are non-hierarchical, so a user can belong to multiple groups simultaneously, allowing you to freely combine department, role, and location groups. Groups let you manage access levels centrally and efficiently handle event log filtering, report generation, and assigning devices to muster areas.

Tip

Refer to the following video to watch the guide on managing user groups.

Before you start

User group composition

User groups are not organized hierarchically.

- Users in a subgroup do **not** automatically appear in the parent group.
- The parent group's total user count does not include subgroup members unless they are added manually.
- Selecting a subgroup shows only the users assigned to that subgroup.

Configure multiple user groups

Users in BioStar Air can belong to **multiple user groups**.

In BioStar 2, user groups were typically linked to a single department. BioStar Air separates these, allowing more dynamic use.

- Filter the user list by group to quickly manage access levels.

  > *e.g., HR department*

- Create context-specific groups that span multiple departments.

  > *e.g., men's locker room*

- User groups are used for **event log filtering** and **report generation**.
- Assign user groups to **muster zone** devices or device groups to enforce specific safety protocols.

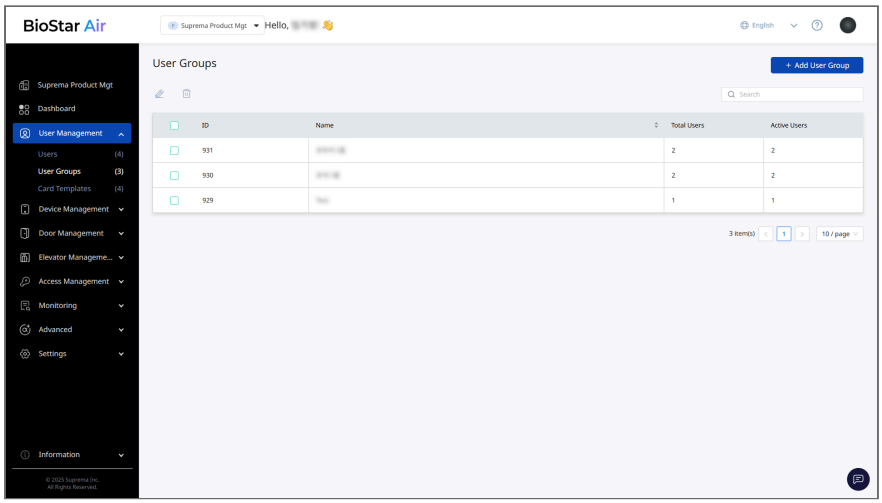
This flexibility makes it easier to manage overlapping user roles and access scenarios.

Create group

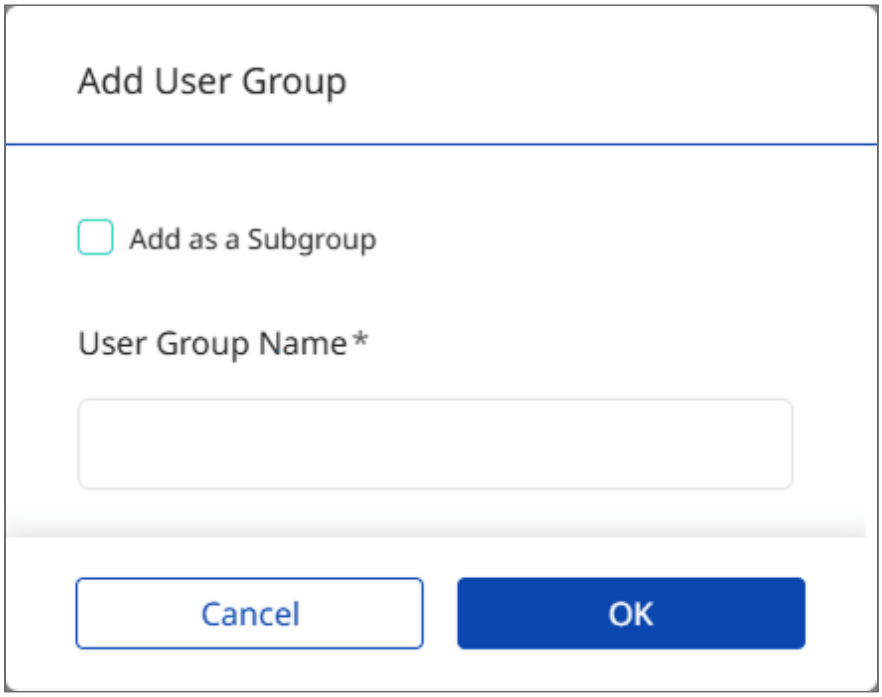
Create user group

Create a new user group.

1. Click **User Management** → **User Groups** in the left sidebar.



2. Click **Add User Group** at the top right of the screen.
3. When the **Add User Group** window appears, enter the user group name.



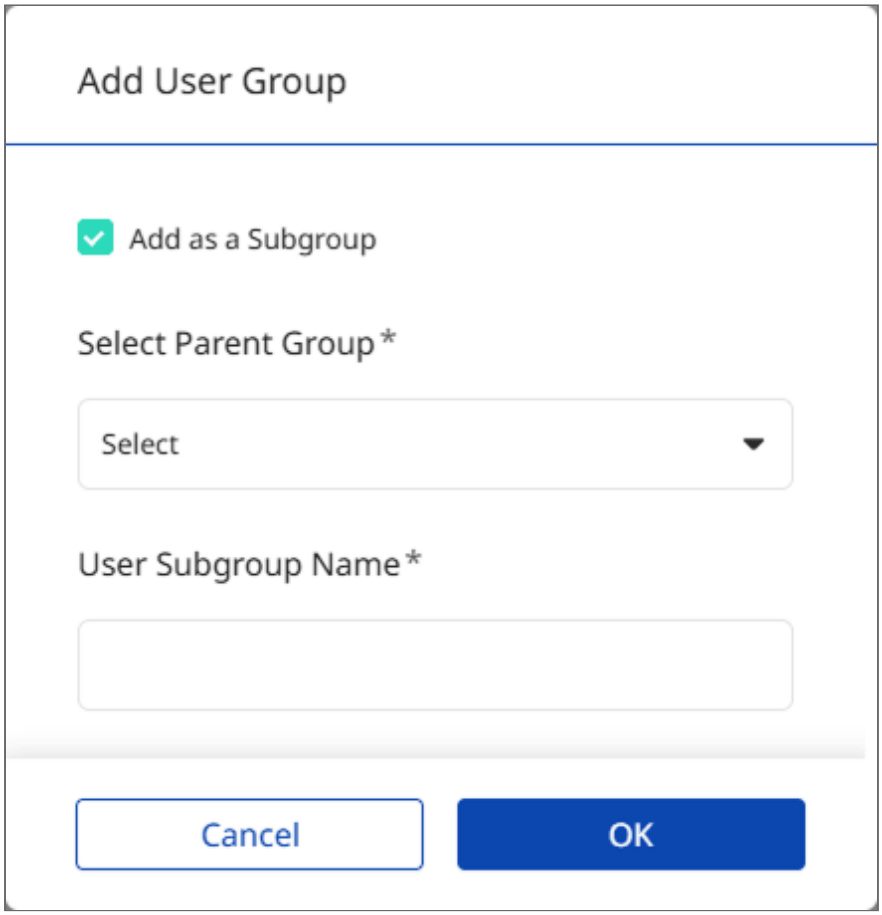
4. Click **OK** to create the group.

> **Info**
>
> - Deleting a group does not delete the users in that group. The users are only removed from the group.
> - For more information about assigning users to groups, see Manage Users.

Create subgroup

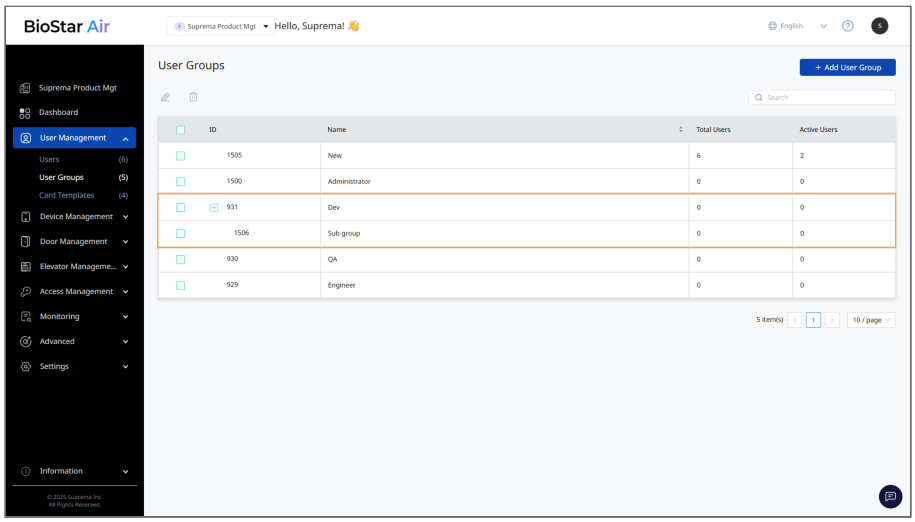
You can use subgroups to further classify user groups. However, subgroups are **not hierarchical**. This means users in a subgroup are not automatically included in the parent group.

1. Click **User Management** → **User Groups** in the left sidebar.
2. Click **Add User Group** at the top right of the screen.
3. When the **Add User Group** window appears, click the **Add as a Subgroup** option.



4. From **Select Parent Group**, select the parent group.
5. Enter the group name in **User Subgroup Name**.
6. Click **OK** to create a subgroup.

The newly created subgroup appears indented under the parent group in the user group list.

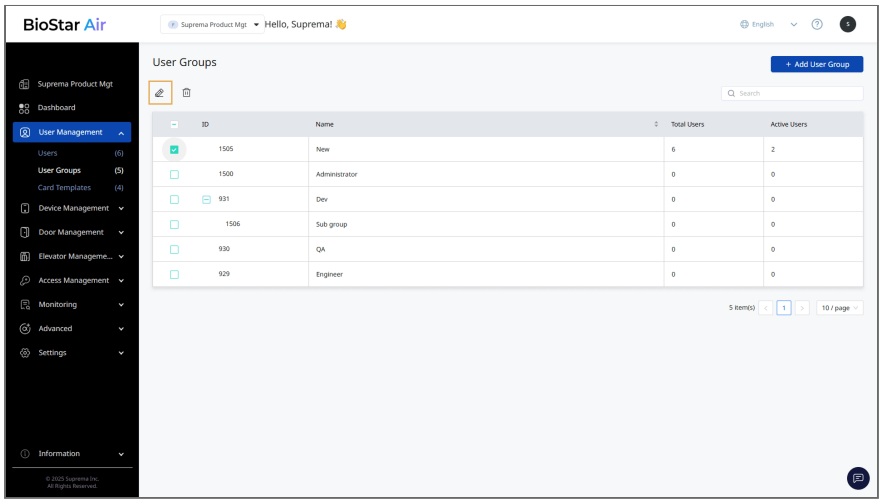


Edit group name

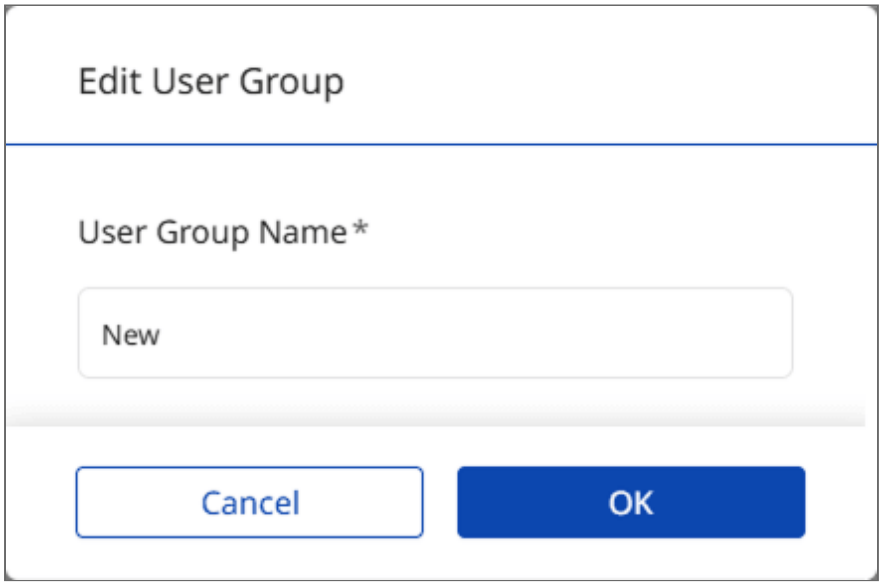
Modify the name of an existing user group.

1. Click **User Management** → **User Groups** in the left sidebar.
2. Click the checkbox for the user group to edit in the list.

3. Click at the top left of the user group list.



4. When the **Edit User Group** window appears, edit the group name.



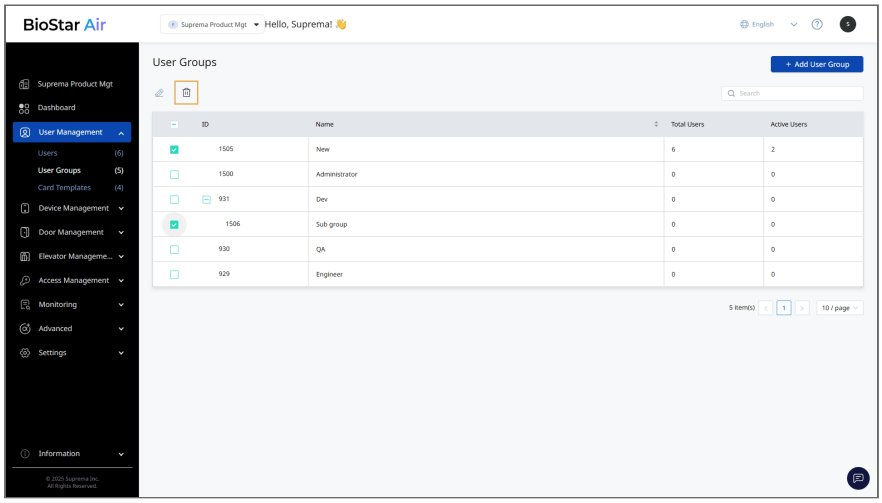
5. Click **OK** to save the changes.

> **Info**
> The group name can be edited only when a single group is selected.

Delete group

Delete any user groups that are no longer needed.

1. Click **User Management** → **User Groups** in the left sidebar.
2. Click the checkbox for the user group to delete in the list.
3. Click at the top left of the user group list.



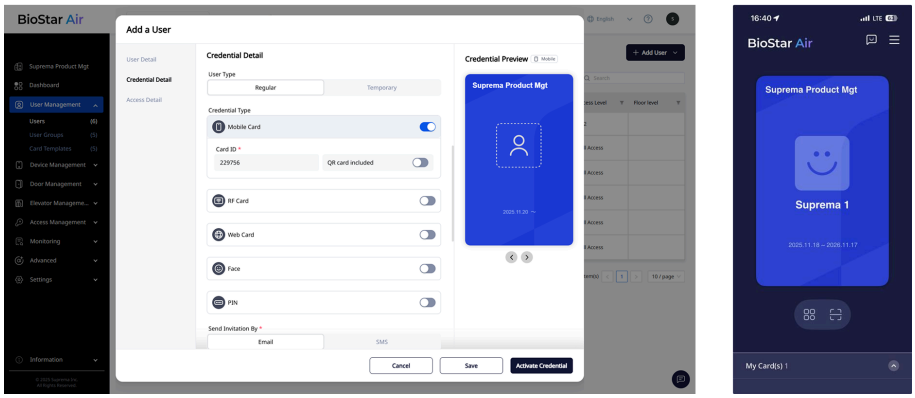
4. When a warning message appears, click **Yes**.

Manage Card Templates

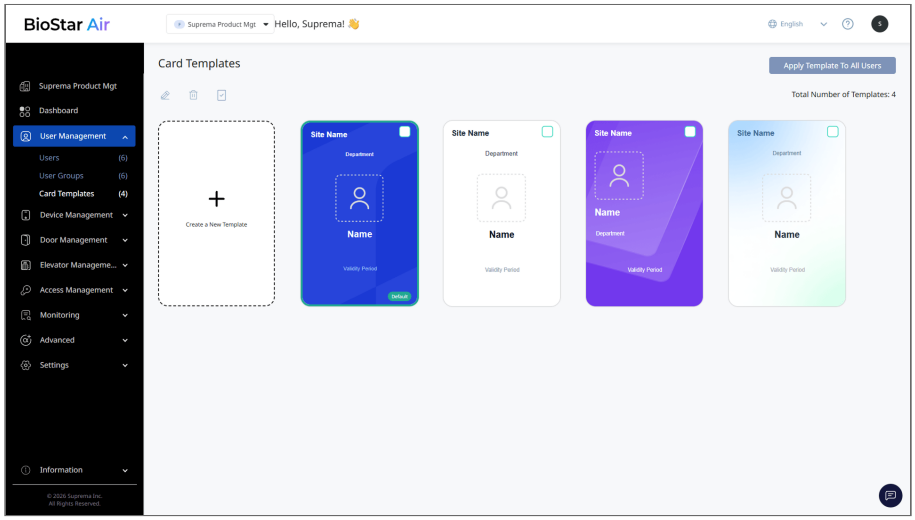
With card templates in BioStar Air, administrators design and customize mobile cards for users. The templates enhance branding by including corporate colors, logos, and personalized details. Card templates apply to mobile cards used in the Suprema Pass app.

BioStar Air

Mobile device



Every site in BioStar Air includes default templates. Click **User Management** → **Card Templates** in the left sidebar.



View the default templates. Administrators apply mobile card templates in one of the following three ways.

- Apply the default card template to a user's mobile card
- Modify parameters of an existing template to apply a customized mobile card

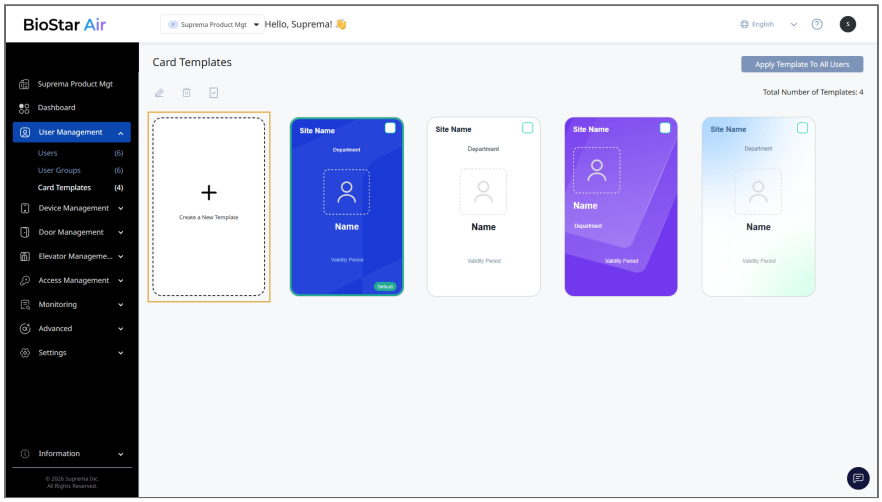
- Create a new custom template and apply it instead of the existing template

> **Tip**
> Refer to the following video to learn how to manage card templates.

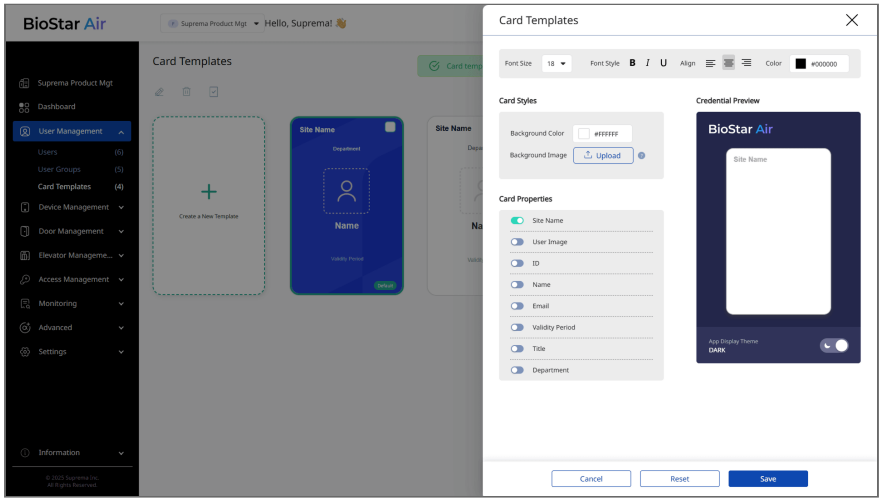
Create a new card template

Create a new card template.

1. Click **User Management** → **Card Templates** in the left sidebar.
2. Click **Create a New Template**.



3. When the **Card Templates** panel appears, set the card design and layout.



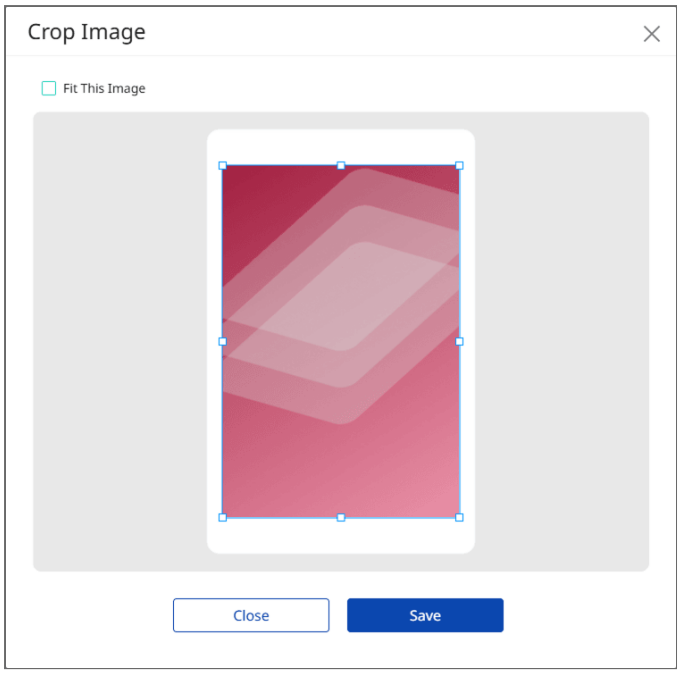
4. After applying the desired settings, click **Save** to save the mobile card template.

Card Styles

In the **Card Styles** section, you can set the card's background color or background image.

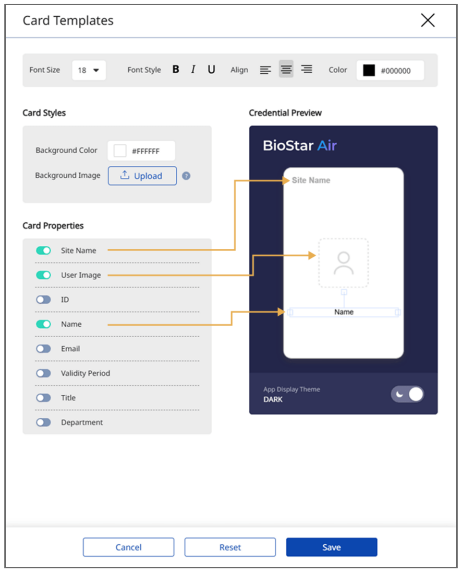
- **Background Color**: Set the background color of the mobile card.
- **Background Image**: Upload a background image for the mobile card. Click **Upload**, and then select a background image file stored locally. When the **Crop Image** window appears, click the **Fit This Image** option or manually adjust the

size. After completing the image adjustments, click **Save**.

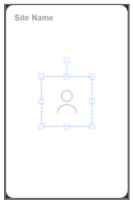


Card Properties

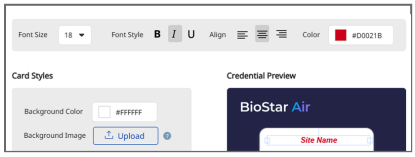
In the **Card Properties** section, you can select which attributes to include in the mobile card. Click the toggle switch to show the selected attributes in the **Credential Preview** on the right.



- After placing an attribute, click it in the **Credential Preview** to reveal handles for resizing, repositioning, and rotating.



- Customize the font of each attribute. Click a placed attribute, and then use the font options at the top. Adjust the font size, style, alignment, and color.

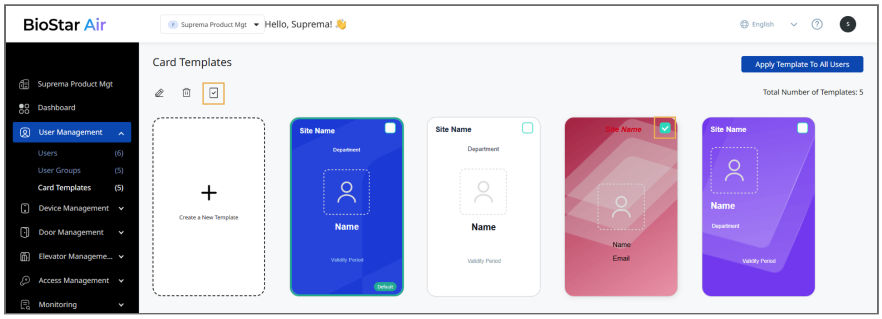


- Select dark mode or light mode in **App Display Theme**.
- Click **Reset** to initialize the configured design.
- After completing all settings, click **Save** to save the mobile card template.

Set the default card template

Set a newly added mobile card template as the default.

1. Click **User Management** → **Card Templates** in the left sidebar.
2. Click the checkbox in the upper right corner of the desired template.
3. Click ☑ at the top left of the template list.



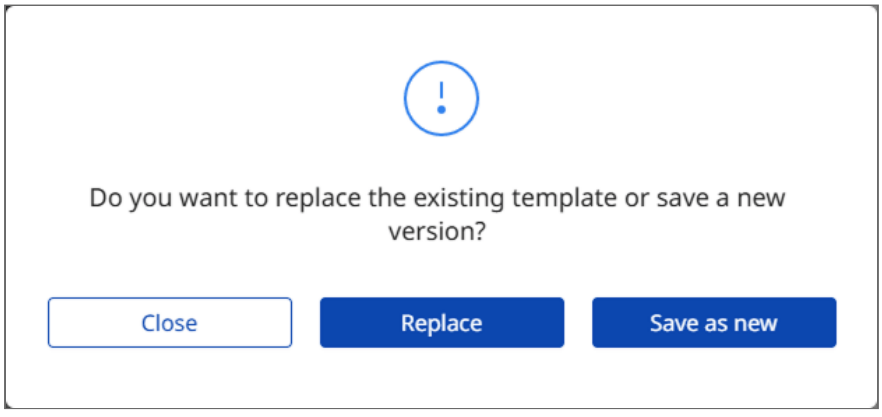
4. When the message window appears, click **Yes**.

The default mobile card template is automatically applied when a new user is added.

> **Info**
> Only one template can be set as default.

Edit card templates

1. Click **User Management** → **Card Templates** in the left sidebar.
2. Click the template you want to edit in the template list. Alternatively, select the checkbox at the top right of the template, then click the ✎ button.
3. When the **Card Templates** panel appears, modify the card design and layout.
4. Click **Save** to save the changes.
5. When the message window appears, click **Replace** or **Save as new**.



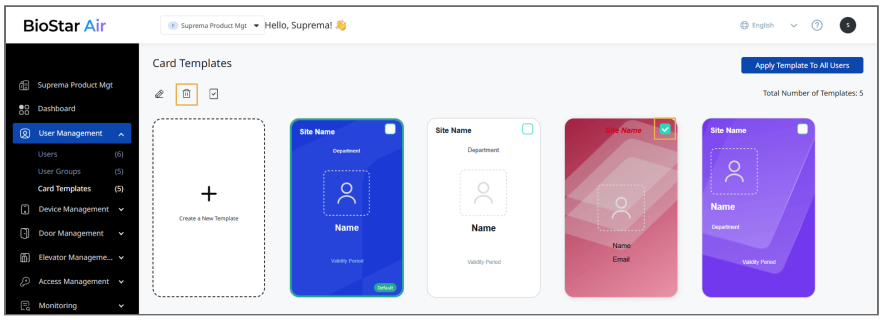
- **Replace**: Save the changes to the existing template.
- **Save as new**: Save the changes as a new template.

Delete card templates

1. Click **User Management** → **Card Templates** in the left sidebar.

2. In the template list, click the checkbox in the upper right of the template you want to delete. Select one or more templates.

3. Click at the top left of the template list.



4. When the message window appears, click **Yes**.

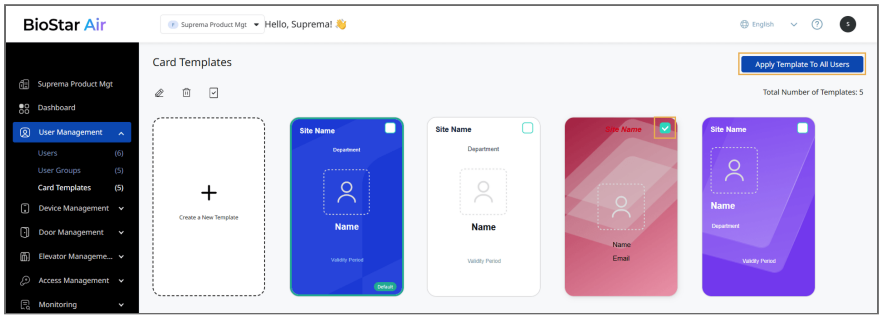
> **Info**
>
> Default templates cannot be deleted.

Apply templates to all users

1. Click **User Management** → **Card Templates** in the left sidebar.

2. In the template list, click the checkbox in the upper right of the template you want to apply.

3. Click **Apply Template To All Users** at the top right of the screen.



4. When the message window appears, click **Yes**.

> **Info**
>
> - Applying the selected card template to all users replaces any template previously set.
> - Only one card template can be applied to all users.

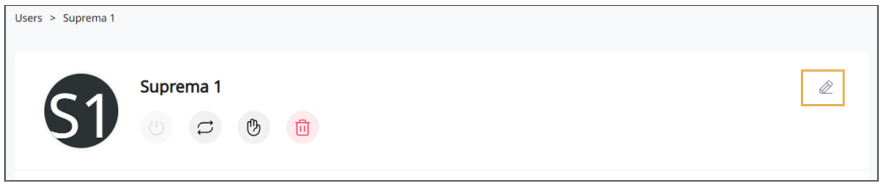
Change a user's card template

Follow these steps to change an individual user's card template.

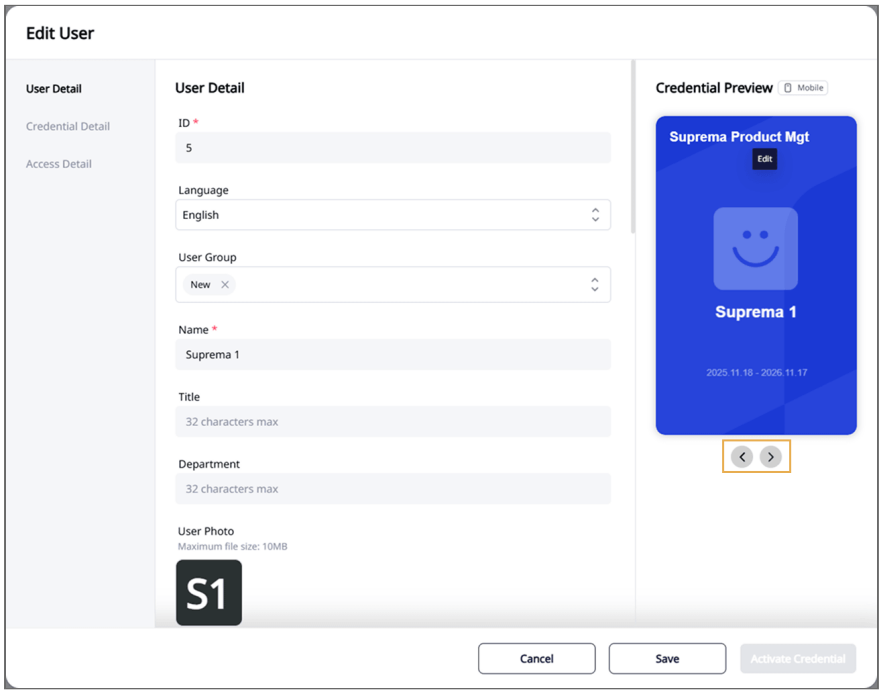
1. Click **User Management** → **Users** in the left sidebar.

2. Click the user in the user list to apply a card template.

3. Click in the top right of the user details.



4. When the **Edit User** window appears, click or under Card Template in the right panel to select the desired card template.



5. Click **Save** to apply the changes.

User Card and Credential Types

From BioStar Air version 2.6, two user types were introduced to enhance user management.

- **Regular**: A user who is a regular member of an organization or facility and requires long-term, ongoing access. All credential types can be issued.
- **Temporary**: A visitor or non-regular member who needs short-term, limited access. This can include guests, external visitors, short-term contractors, delivery couriers, and so on. Only **Web Card** credentials, including QR code and LinkPass, can be issued.

> **Info**
> For more information on issuing credentials when adding or editing users, refer to Add Users.

> **Tip**
> Watch the video below for a tutorial on user and card types.

Regular user card types

The credentials you can issue to regular users are as follows.

> **Info**
> For more information on how to use mobile credentials with the Suprema Pass app, refer to Using Mobile Credentials.

Mobile Card

- A unique **Card ID** is automatically assigned but can also be set manually.
- When using an **Airfob Tag** or **Airfob Patch**, integrate with an existing access control system by using the mobile card number as the card serial number.
- For compatibility with a previous system, the mobile card ID can match the RF card number of the former site.

RF Card

- Add up to eight RFID cards per user.
- Configure **Card Type**(CSN or Wiegand), **Card ID**, and **Card Name** to simplify management when multiple cards are assigned.
- Select a reader in **Scan with Reader** to scan an existing RFID card with a connected Suprema device.
- If an existing RF card has a **CSN** (card serial number), enter the CSN manually.

Web QR

- Regular users can use the **QR code** of a mobile card.
- Access the QR code by tapping the button on the mobile card interface.

Link Pass

- Send a web link to the user's email address or phone number.
- The user opens the received link in a web browser and clicks **Open** to gain access.

> **Info**
> For more information on LinkPass credentials, refer to LinkPass Credentials.

Facial credential

- Add up to two face profile images per user.
- Register through a connected reader or by uploading an image.
- Send an email link to the user, then capture a photo with a mobile device camera to enroll.

2FA PIN

Set a 4–16-digit PIN to use as part of two-factor authentication (2FA).

Temporary user card types

Temporary users do not receive mobile or RFID cards. Instead, issue **web-based credentials** that do not require an app download. Available options are as follows:

Web QR

- Send via email or text message.
- Accessible through a web browser.
- Use a **dynamic QR code**, which updates every five minutes, to enhance security.

Link Pass

Send a web link to the user via email or text message. The user gains access by clicking **Open** in a web browser.

> **Info**
> For more information on LinkPass credentials, refer to LinkPass Credentials.

Managing access levels

Set **access levels** to control where credentials are allowed, regardless of whether the user is regular or temporary.

> **Caution**
> If the user is temporary, assign restrictive access levels carefully and avoid issuing credentials with unlimited access.

LinkPass Credentials

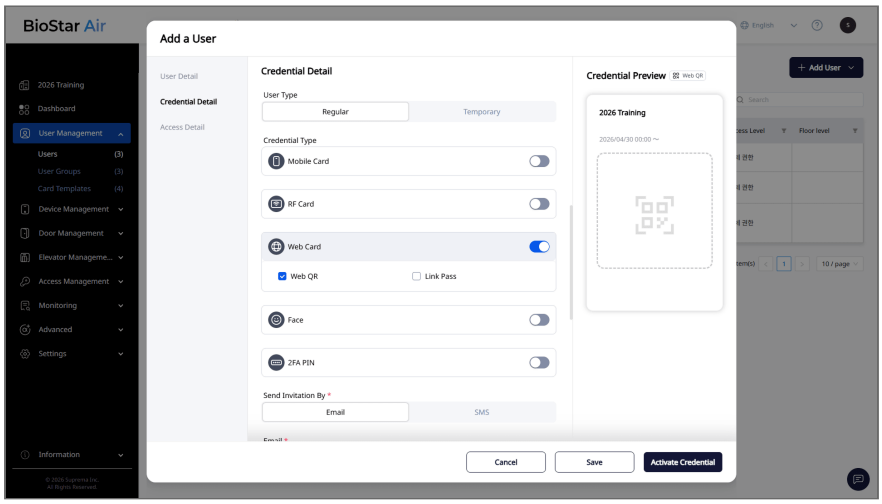
LinkPass is a mobile credential that can be used in BioStar Air without an app. Administrators can grant users access without installing an app or using BLE or NFC. Because LinkPass operates through the BioStar Air cloud and is activated via a secure web link, it is ideal for customer entry, deliveries, or low-security entrances such as parking gates and lobbies.

- **Credential scope**: A LinkPass credential grants access to the same doors as the user's other assigned credentials. Issuing a LinkPass credential to users who do not have access to high-security areas is not recommended.
- **No app required**: LinkPass works through a web browser, so it does not need a mobile app, Bluetooth, or NFC communication.
- **Cloud-based access**: LinkPass commands are sent through the BioStar Air cloud and can be activated from anywhere with an internet connection. It does not share or track location.
- **Reader connectivity**: The door reader must be online and connected to BioStar Air for LinkPass to work properly.
- **Recommended use cases**: LinkPass is suitable for temporary visitors, deliveries, and low-security areas such as lobbies or parking gates.

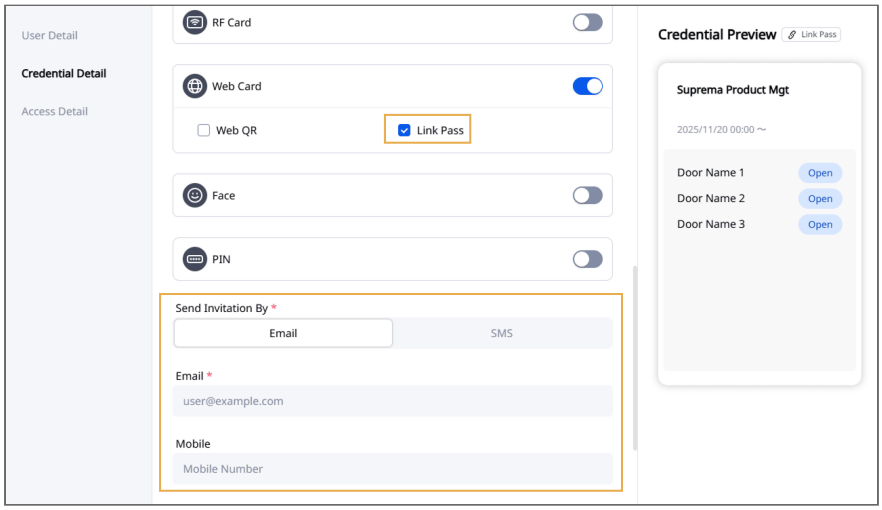
Activate LinkPass credentials

1. Log in to the BioStar Air website.
2. Click **User Management** → **Users** in the left sidebar.

3. Navigate to the **Edit User** or **Add New User** screen using one of the following methods.
   - Select an existing user in the list, and then click ✎ at the top right.
   - Click **Add User** → **Add User** at the top right of the screen.
4. Go to the **Credential Detail** section.
5. Enable the **Web Card** option.



6. Click the **Link Pass** checkbox.
7. Enter a unique **email address** or **phone number** in **Send Invitation By** where the user can receive the credential link.



8. Select the appropriate **Access Level**, and set the user's **Valid Through**.
9. Click **Activate Credential** to issue the credential.
10. Send the user an invitation containing the unique LinkPass URL by email or SMS.

Use LinkPass

1. On a mobile device, open the LinkPass URL in the email or SMS.
2. The web page displays all doors assigned to the user, and each door has **Open**.
3. Click **Open** to open the door by sending a cloud-based unlock command to the reader.

> **Info**
> LinkPass does not require Bluetooth or NFC communication.

Devices

BioStar Air's flexible device management settings ensure that sites can be configured exactly as required for any site. In this document, device management refers to the full lifecycle of a device, including registration, configuration, firmware management, monitoring, and ongoing operation.

BioStar Air supports two different device architectures. Both architectures can be used on the same site, allowing organizations to choose the best approach for each door or area.

Distributed architecture

In a distributed architecture, each edge device contains its own controller and connects directly to the cloud using Ethernet. Devices continue operating independently during network interruptions and synchronize automatically when connectivity is restored.

Edge devices can also act as controllers for secondary readers connected via RS-485.

This architecture is commonly used for:

- New installations
- Biometric devices
- Deployments where minimizing infrastructure is important

Centralized architecture

In a centralized architecture, readers connect to a control panel using RS-485 or Wiegand. The control panel connects to the cloud via Ethernet and acts as the controller for downstream devices.

The control panel manages redundancy and access decisions for connected readers during network interruptions.

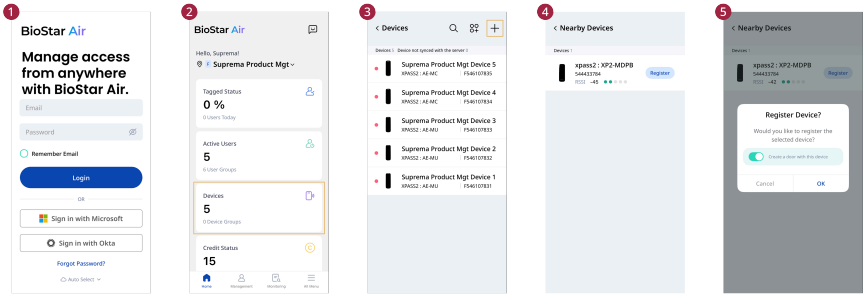
This architecture is commonly used for:

- Retrofit projects with existing low-voltage wiring
- Sites replacing legacy access control systems
- Deployments with centralized security rooms or panels

Register and Delete Edge Devices
To add devices to BioStar Air, use the BioStar Air mobile app. Use the mobile app to register new devices, delete existing ones, and upgrade firmware over a wireless connection.

Register Device

Use the BioStar Air mobile app to register devices. Register devices using Bluetooth Low Energy (BLE), and manage them through the BioStar Air portal.



1. Open the BioStar Air app on your mobile device and log in.
2. Tap the **Devices** card.
3. Tap + at the top right of the screen.
4. In the device search screen, tap **Register** for the device to register.
5. When the device registration window appears, tap **OK**.

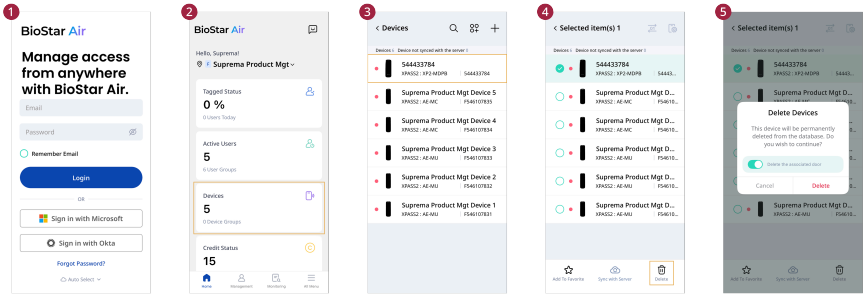
Return to the device list and confirm the added device.

> **Tip**
>
> For best performance, reliability and access to the latest features, make sure to check for firmware updates as soon as devices are registered. New firmware may have become available between the time the device was packaged and installed. For more information on firmware upgrades, see Upgrade Firmware.

> **Info**
>
> - Devices cannot be registered on the web portal. Register the device via the BioStar Air mobile app.
> - When registering a device, keep the device close to the mobile device and ensure that Bluetooth is enabled on the mobile device.
> - Disable the **Create a door with this device** option in the device registration window to avoid setting the registered device as a door.

Delete Devices

If a device appears offline in the device list on the BioStar Air portal, delete it using the mobile app.



1. Open the BioStar Air app on your mobile device.
2. Tap the **Devices** card.

3. Touch and hold the device you want to delete. Select any additional devices to delete.
4. Tap the button at the bottom right.
5. In the pop-up, choose whether to delete the linked door.
6. Tap **Delete**.

> **Info**
>
> Devices other than X-Station 2 can be deleted from the BioStar Air portal. However, the device must be online. It is recommended deleting the device using the BioStar Air mobile app.

Manage Registered Edge Devices

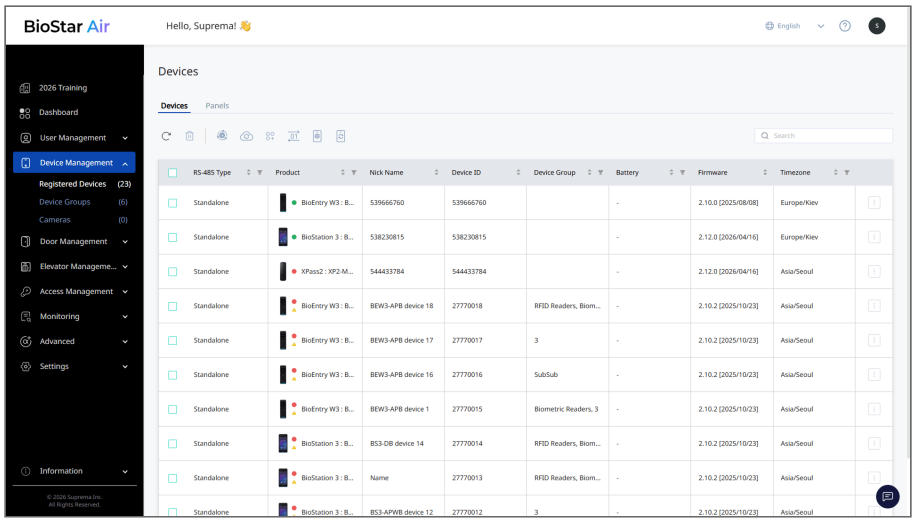
View the connection status of registered devices at a glance, change biometric and card settings, or update firmware. Manage a few devices individually and many devices in bulk to operate your security system efficiently.

> **Info**
>
> - Devices can be registered only in the **BioStar Air mobile app** for iOS or Android. You cannot register devices from the web portal. For detailed instructions on registering devices using the mobile app, refer to Register and Delete Edge Devices.
> - Internet access is required to use certain features, such as **remote access**, **biometric authentication**, **QR code access**, and **firmware updates**.

> **Tip**
>
> Refer to the following video to watch the device registration and management guide.

View the device list

The device list lets you see all devices registered in BioStar Air at a glance. View key information for each device at a glance, such as connection status, model name, and firmware version. Click a device to view details and modify settings.



Click **Device Management** → **Registered Devices** in the left sidebar.

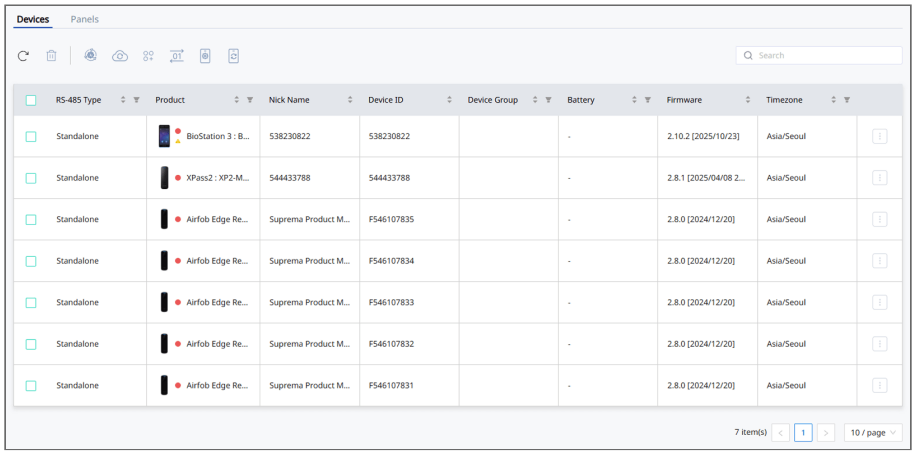
Device connection status

Check each device's connection status from the status icons in the device list.

- 🟢 **Green**: The device is online, can be controlled remotely, and can accept and update QR authentication.
- 🔴 **Red**: The device is offline.
- 🟠 **Orange**: Firmware is updating.
- ○ **Not connected**: The device has no network connection. (e.g., Airfob Patch)
- ⚠️ **Warning**: Synchronization is required between the server and the device. See Resync offline devices for resync instructions.

Device information

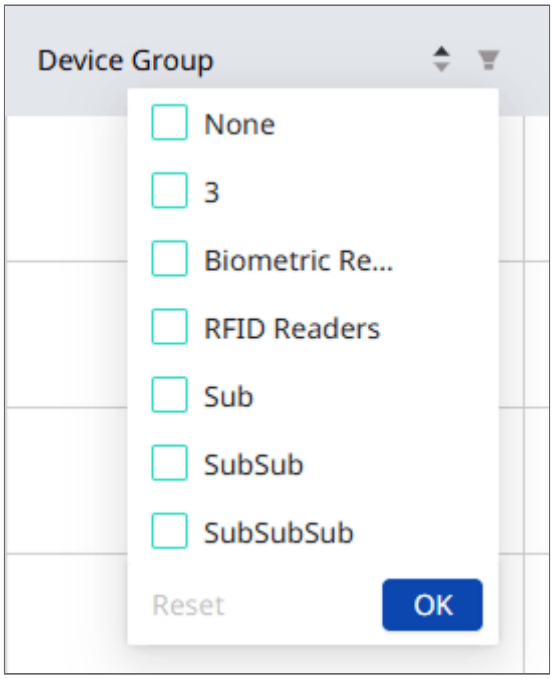
Each column in the device list includes the following information.



- **RS-485 Type**: Available on devices that support RS-485 communication. You can check whether the device is a primary or a secondary. Devices not set as primary or secondary appear as **Standalone**.
- **Product**: The device name and model retrieved from the Suprema database.
- **Nick Name**: A user-editable field for easier identification. Edit it in the **Edit Device** window that appears after clicking the device in the list.
- **Device ID**: The unique identifier assigned to the device.
- **Device Group**: The group to which the device belongs.
- **Battery**: Available only on battery-powered devices. Supported only by Airfob Tag devices.
- **Firmware**: The currently installed firmware version.
- **Timezone**: The time zone set on the device.

Filter

You can use the filter feature in the top header of the device list. Click ▼ in the header to set the desired conditions.

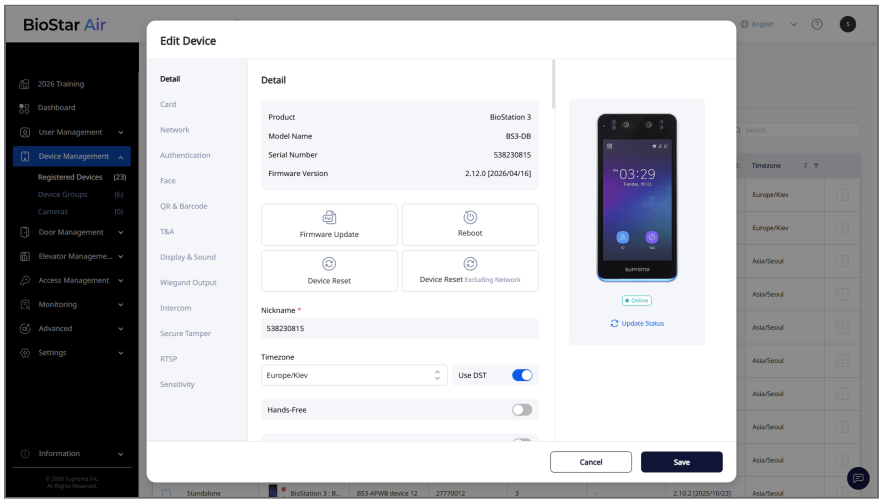


Info

To reset the applied filters, click and select **Reset**.

Edit individual device information and settings

1. Click **Device Management** → **Registered Devices** in the left sidebar.
2. Click the device you want to edit in the list.
3. The **Edit Device** window appears.



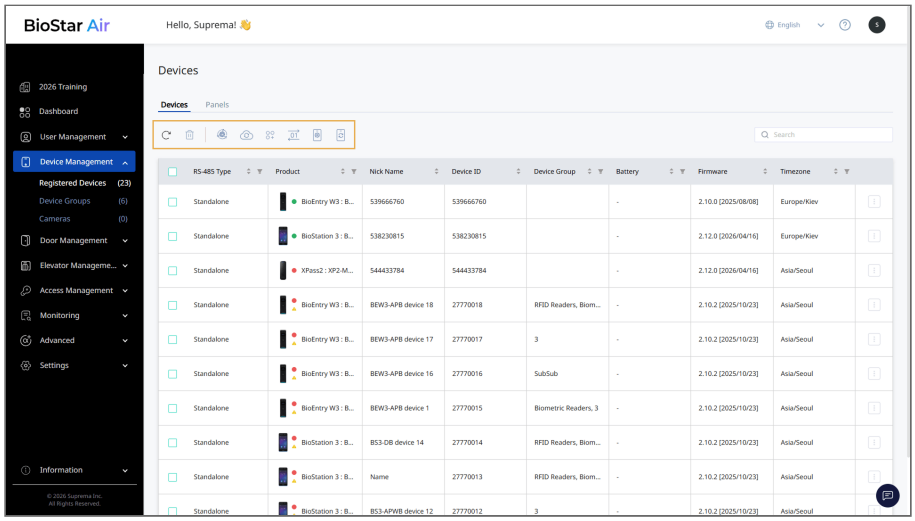
The image above is an example screen and may differ from the actual screen.

4. Edit the device's details or settings.
5. Click **Save** at the bottom to save the changes.

For more information on editing fields and setting options for each section, see Device and Panel Configuration Options.

Bulk device actions

Use the controls at the top of the device list to manage multiple devices at once.



- : Refresh the device list.
- : Delete devices registered to the site.

> **Warning**
> Only online devices can be deleted permanently. If the device is offline, delete it first in the BioStar Air mobile app before adding it to another site. For more information on deleting devices using the mobile app, see Register and Delete Edge Devices.

- : Update the firmware of selected devices. For more information about firmware upgrades, see Upgrade Firmware.
- : Synchronize biometric templates from selected devices to the server.
- : Assign selected devices to a group. For more information about device group management, see Device group management.
- : Switch the RF card byte order of the selected device in the list to **MSB** or **LSB**.
  - **MSB**: Processes card data in order from large byte units to small byte units, sequentially storing the card serial number (CSN) from left to right.
  - **LSB**: Processes card data in order from small byte units to large byte units, storing the card serial number (CSN).
- : Import the device settings originally configured in standalone mode.
- : Update the status of the selected devices in the device list.

Resync offline devices

If a device has been offline for a long time, its information may no longer match the server, and you may need to resync it manually.

1. Click **Device Management** → **Registered Devices** in the left sidebar.
2. Check for devices with the ⚠ icon in the **Product** column in the device list.

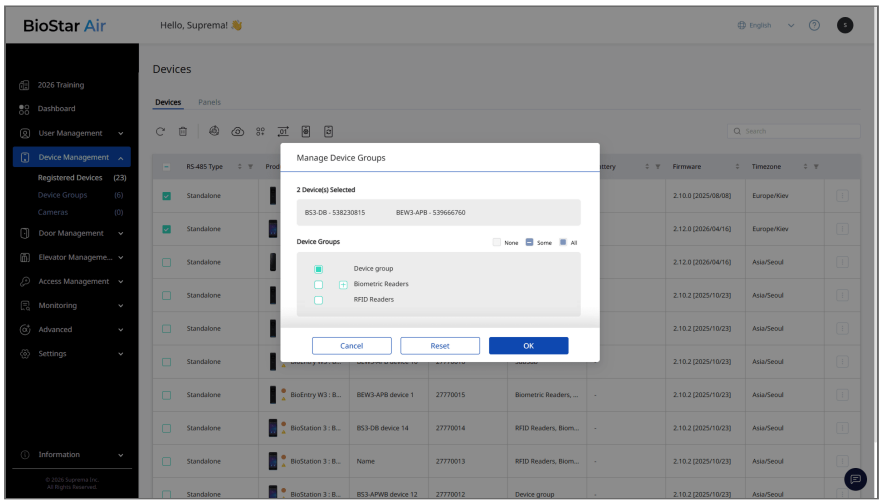
3. Select the checkbox for the device.
4. In the toolbar at the top of the list, click the button.

> **Info**
>
> Devices that have been offline for less than 7 days sync automatically when they reconnect, so no additional action is required.

Device group management

From the device list, select individual devices to add them to a device group or remove them from an existing group.

1. Click **Device Management** → **Registered Devices** in the left sidebar.
2. In the device list, click the checkbox for the device you want to add to or remove from a group.
3. Click at the top of the device list.
4. When the **Manage Device Groups** window appears, add or remove the selected devices from the group.



Device Groups checkboxes have the following meanings:

- **None**: Removes the selected devices from the group.
- **Some**: Certain selected devices are currently in the group.
- **All**: Adds the selected devices to the group.

5. Click **OK** to save the changes.

> **Info**
>
> - Selecting another group in the **Manage Device Groups** window moves the selected devices to that group.
> - A device can belong to multiple groups. A single device can be assigned to multiple groups.
> - Click **Reset** to initialize the changes.

Register and Delete Panels

BioStar Air version 2.12 supports expanding the access control system using the CoreStation 20 (CS-20) panel. Using

existing RS-485 wiring to connect additional devices locally reduces infrastructure costs while supporting complex door configurations.

This document provides step-by-step instructions to register the CS-20 panel and configure RS-485, OSDP, and Wiegand devices as secondary devices.

> In BioStar Air, devices are classified as primary devices that act as controllers and secondary devices that connect to controllers. Some systems use the terms Master/Slave for this concept, but BioStar Air documentation does not use those terms.

Register panel

The CoreStation 20 (CS-20) enables expansion of the access control system by connecting to devices that use RS-485 communication. Follow these steps to register the CS-20.

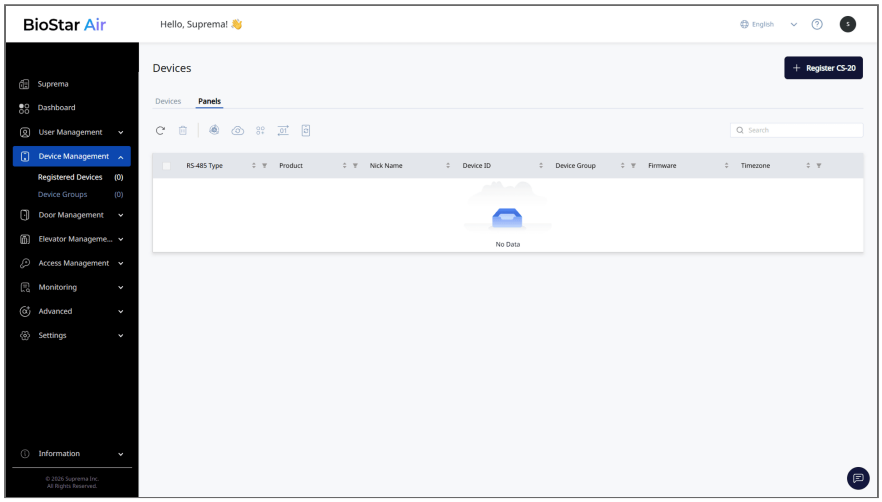
Before you start

- Ensure the CS-20 is powered on and physically accessible to press the **INIT** button.
- The CS-20 must be connected to the internet. If the network connection is unstable, issues may occur during registration.
- A 9-digit serial number is required. The serial number can be found on the label on the back of the unit.

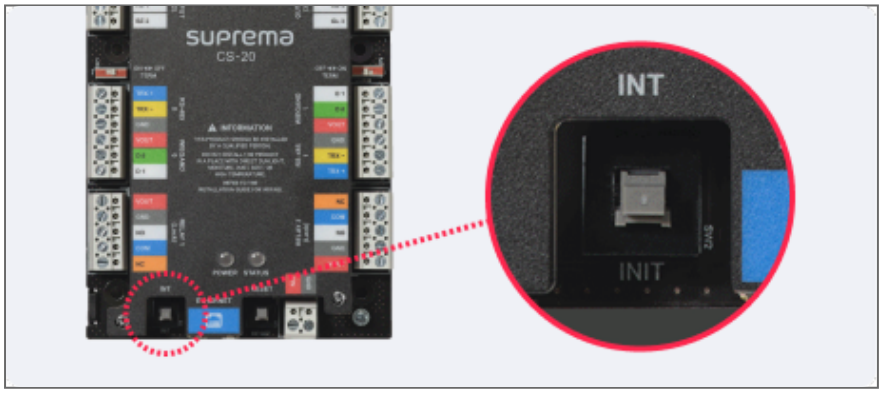
> **Info**
> For more information on the CoreStation 20, refer to the CoreStation 20 Installation Guide.

Register CS-20

1. Click **Device Management** → **Registered Devices** in the left sidebar.
2. Click the **Panels** tab.

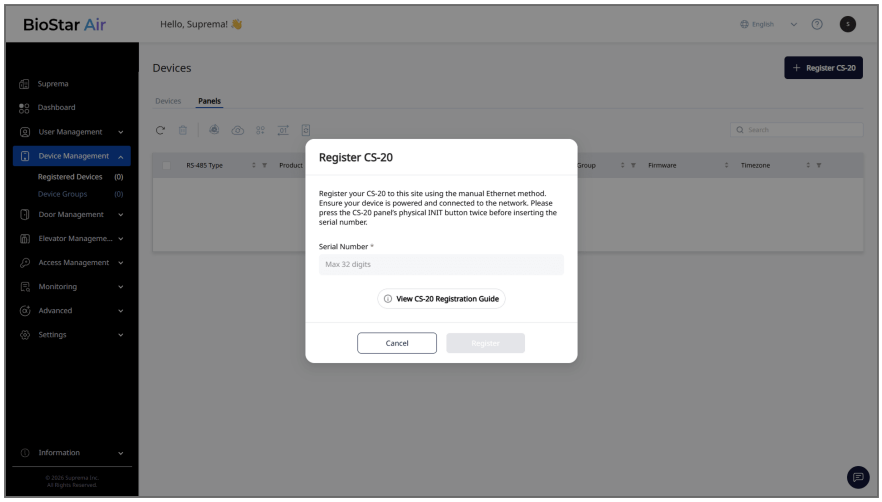


3. Click **Register CS-20** at the top right of the screen.
4. When the **Register CS-20** window appears, press the INIT button on the CS-20 panel twice.



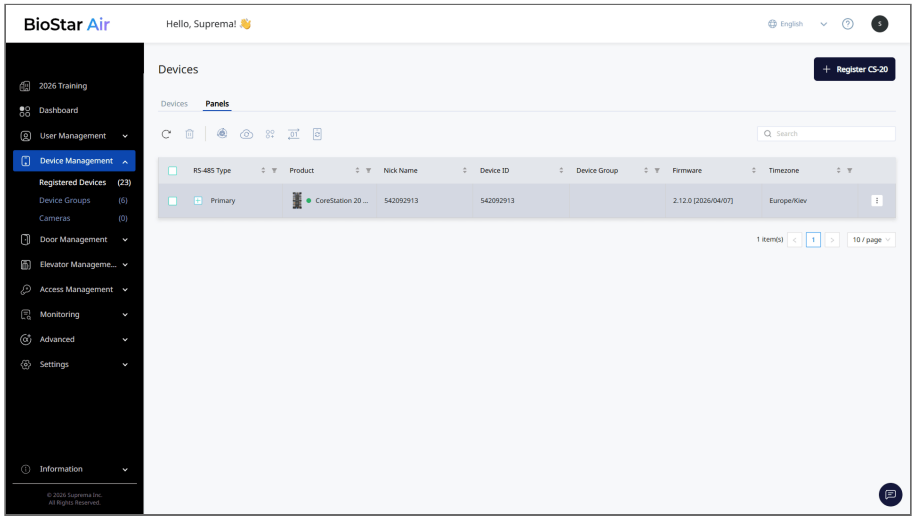
> **Caution**
>
> After pressing the **INIT** button, there is a 5-minute window to complete CS-20 registration.

5. Enter the serial number.



6. After entering the full serial number, click **Register**.

After registration is complete, the system automatically sets up a secure connection and displays the new CS-20 in the panel list. If registration is successful, a green dot appears next to the device name.



Tip

For best performance, reliability and access to the latest features, make sure to check for firmware updates as soon as devices are registered. New firmware may have become available between the time the device was packaged and installed. For more information on firmware upgrades, see Upgrade Firmware.

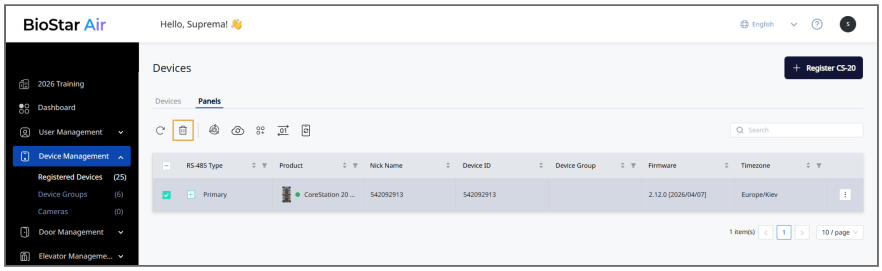
Info

For more information on the CS-20 registration process, see **View CS-20 Registration Guide**.

Delete panel

Follow these steps to delete a panel registered in BioStar Air. Deleted panels cannot be recovered. Before deleting a panel, confirm that any peripheral devices connected to it are no longer needed.

1. Click **Device Management** → **Registered Devices** in the left sidebar.
2. Click the **Panels** tab.
3. In the list, click the checkbox for the panel you want to delete.
4. Click in the upper left of the screen.



5. When the pop-up appears, click **Confirm**.

Caution

If you need to reuse connected peripheral devices, delete those devices before deleting the panel, since the SCB key may be bound.

Manage Registered Panels

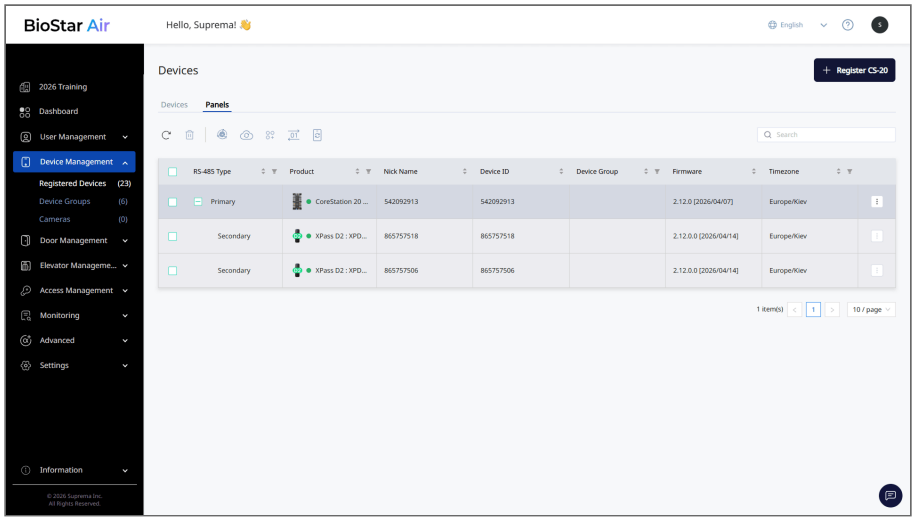
Manage all panels registered in BioStar Air from a single location. Monitor each panel's status, edit information as needed, organize panels into groups, and update firmware. This document covers all necessary features, from viewing the panel list to managing groups.

Info

In BioStar Air, devices are classified as primary devices that act as controllers and secondary devices that connect to controllers. Some systems use the terms Master/Slave for this concept, but BioStar Air documentation does not use those terms.

View the panel list

Manage registered panels from the **Panels** tab. The panel list provides key information at a glance, including the type and status of each panel or secondary device, name, ID, group, firmware, and time zone.



Panel and device status

Check each panel or secondary device's connection status from the status icons in the panel list.

- **Green**: The panel or secondary device is online, can be controlled remotely, and can be updated.
- **Red**: The panel or secondary device is offline.
- **Orange**: Firmware is updating.
- **Warning**: Synchronization is required between the server and the panel or secondary device. See Resync offline panels and secondary devices for resync instructions.

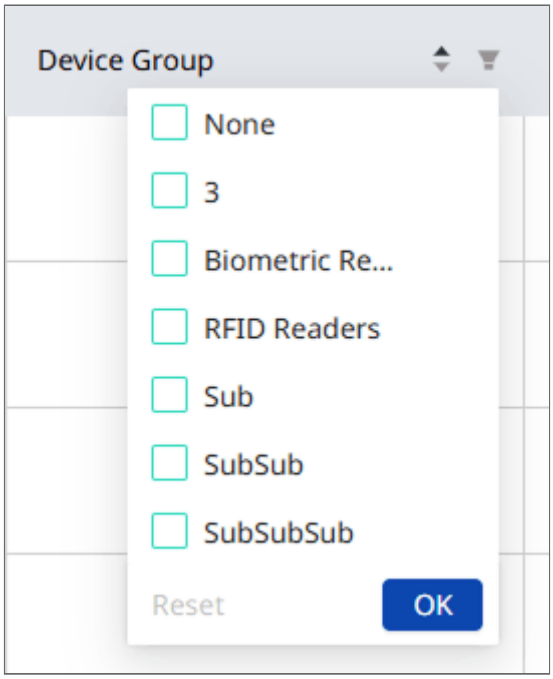
Panel and device information

Each column in the panel list includes the following information.

- **RS-485 Type**: Indicates panels or secondary devices that support RS-485 communication. Indicates whether the device is a primary or a secondary.
- **Product**: The panel or secondary device name, model, and status retrieved from the Suprema database.
- **Nick Name**: A user-editable field for easier identification. You can edit the information in the window that appears when you click a panel or subdevice in the list.
- **Device ID**: The unique identifier assigned to the panel or subdevice.
- **Device Group**: The group to which the panel belongs.
- **Firmware**: The currently installed firmware version.
- **Timezone**: The time zone set on the panel or subdevice.

Filter

Use the filter in the header of the panel list. Click in the header to set the desired conditions.

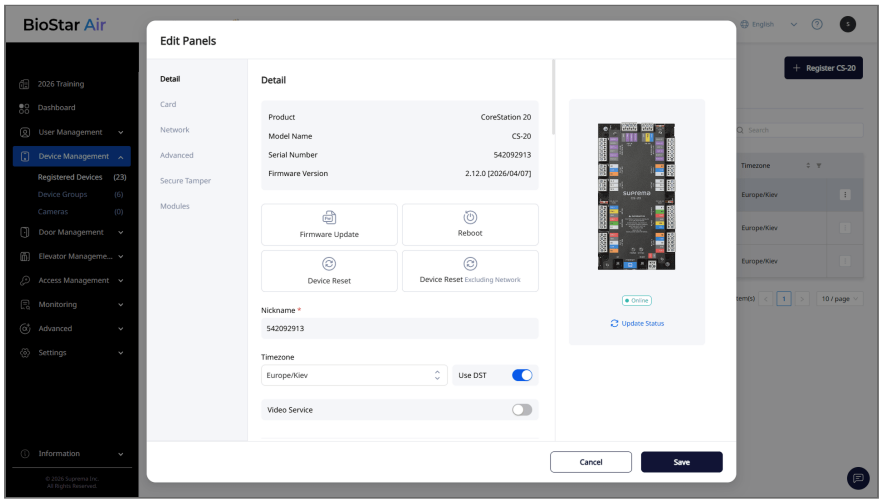


Info

To reset the applied filters, click and select **Reset**.

Edit panel information

1. Click **Device Management** → **Registered Devices** in the left sidebar.
2. Click the **Panels** tab.
3. Click the panel whose information you want to edit in the list to open the **Edit Panels** window.

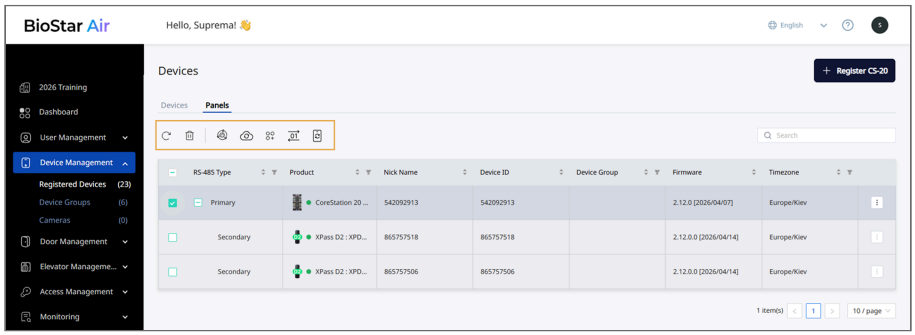


4. Edit the panel's details or settings.
5. Click **Save** at the bottom to save the changes.

> **Info**
>
> For more information on editing fields and setting options for each section, see Device and Panel Configuration Options.

Panel management features

Select a panel in the list to use the management features at the top.



- : Refresh the list.
- : Delete registered panels or subdevices.
- : Update the firmware of selected panels or subdevices in the list. For more information about firmware upgrades, see Upgrade Firmware.

  > – Subdevices connected to a CS-20 can be upgraded one at a time.
  > – For more information on upgrading XPass D2 devices, see Upgrade Firmware.

- : Synchronize biometric templates from selected panels to the server.
- : Assign selected panels to a group. For more information on managing groups, see Manage panel groups.
- : Switch the RF card byte order of the selected panel in the list to **MSB** or **LSB**.
  - **MSB**: Processes card data in order from large byte units to small byte units, sequentially storing the card serial number (CSN) from left to right.
  - **LSB**: Processes card data in order from small byte units to large byte units, storing the card serial number (CSN).
- : Import settings originally configured in standalone mode.
- : Update the status of selected panels.

> **Info**
>
> Subdevices connected to a CS-20 only support the refresh ( ), delete ( ), and firmware update ( ) functions.

Resync offline panels and secondary devices

If a panel or auxiliary device has been offline for a long time, its information may fall out of sync with the server and require

manual resync.

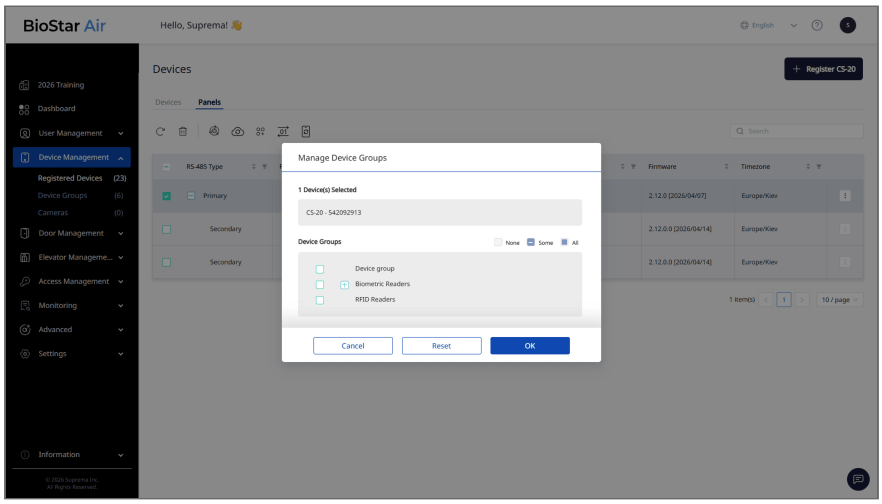
1. Click **Device Management** → **Registered Devices** in the left sidebar.
2. Click the **Panels** tab.
3. In the list, check the panel or auxiliary device with the ⚠ icon in the **Product** column.
4. Select the checkbox for the panel or auxiliary device.
5. In the toolbar at the top of the list, click the ☁ button.

> **Info**
> Panels or auxiliary devices that have been offline for less than 7 days sync automatically when they reconnect, so no action is required.

Manage panel groups

Select individual panels in the panel list to add them to or remove them from a group.

1. Click **Device Management** → **Registered Devices** in the left sidebar.
2. Click the **Panels** tab.
3. In the panel list, select the checkbox for the panel you want to add to or remove from a group.
4. Click ⁘ at the top of the panel list.
5. When the **Manage Device Groups** window appears, add the selected panels to a group or remove them from it.



Device Groups checkboxes have the following meanings:

- **None**: Removes the selected panels from the group.
- **Some**: Some of the selected panels are in the group.
- **All**: Adds the selected panels to the group.

6. Click **OK** to save the changes.

Info

- Selecting another group in the **Manage Device Groups** window moves the selected panels to that group.
- A panel can belong to multiple groups. A single panel can be assigned to multiple groups.
- Secondary devices in the panel list only support firmware upgrades.
- Click **Reset** to initialize the changes.

Add and Manage Devices on the Panel

BioStar Air connects multiple types of secondary devices to the CS-20 primary panel. Support for RS-485, OSDP, and Wiegand enables easy integration with existing security systems. This article explains how to configure, manage, and remove secondary devices.

Configure secondary devices

After registering the CS-20, configure secondary devices using one of the following methods:

Secondary devices	Description
Suprema RS-485 devices	Connect XPass D2 and OM-120 via existing RS-485 wiring and standard communication protocols.
OSDP device	Uses a security-enhanced communication protocol
Wiegand device	Existing Wiegand-compatible devices, such as card readers

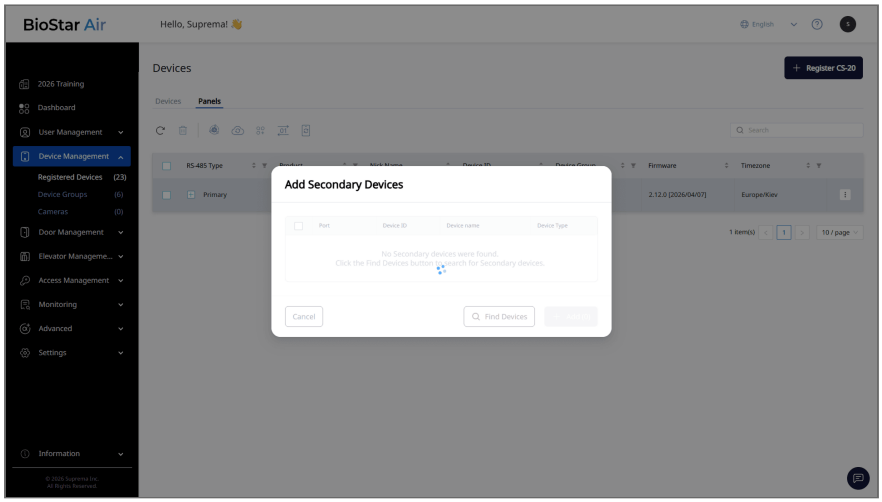
Configure secondary devices

Connect devices that support RS-485 communication to the CS-20 to configure them as secondary devices. Secondary devices appear nested under the CS-20 in the panel list.

1. In the panel list, click ⋮ at the far right of the registered CS-20 panel.



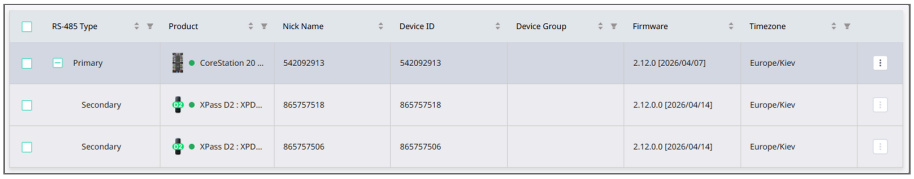
2. Click **Add Secondary Devices** to open the **Add Secondary Devices** window.



> If no secondary devices are found, click **Find Devices** to re-scan devices connected to the CS-20.

3. When connected secondary devices appear in the list, click the checkbox next to each device to select the ones to add.
4. Once your selections are complete, click **Add**.

Connected secondary devices appear nested under the CS-20. View all devices connected to the CS-20 at a glance in the panel list.



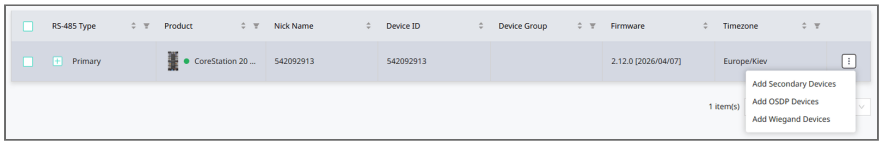
> **Tip**
>
> For best performance, reliability and access to the latest features, make sure to check for firmware updates as soon as devices are registered. New firmware may have become available between the time the device was packaged and installed. For more information on firmware upgrades, see Upgrade Firmware.

> **Info**
>
> - For more information on editing and managing secondary devices, see Manage Registered Edge Devices.
> - For more information on secondary device fields and settings, see Device and Panel Configuration Options.
> - For more information on upgrading XPass D2 devices, see Upgrade Firmware.

Configure OSDP devices

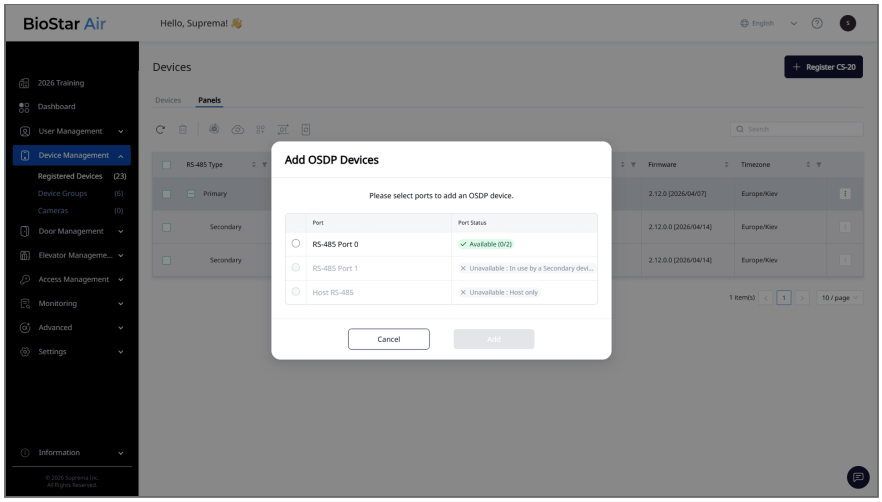
OSDP (Open Supervised Device Protocol) is a security-enhanced communication protocol. In environments requiring high security, connect OSDP-compatible devices to the CS-20.

1. In the panel list, click ⋮ at the far right of the registered CS-20 panel.



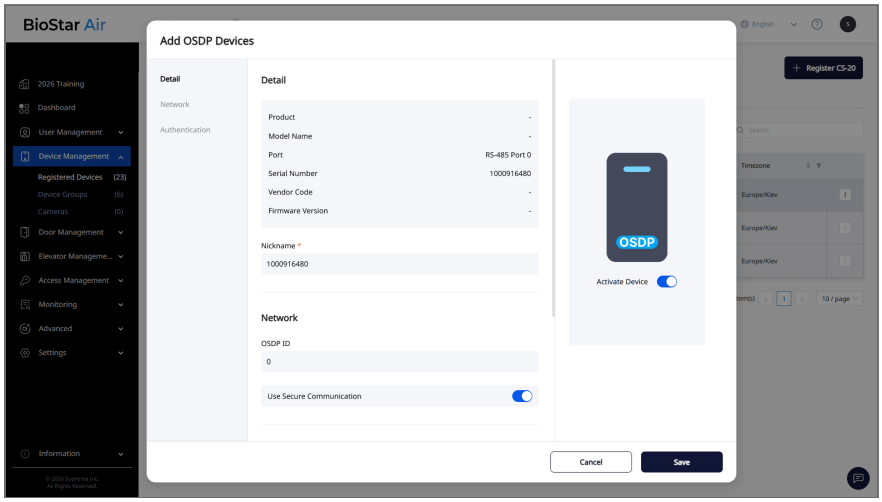
2. Click **Add OSDP Devices** from the popup menu.

3. When the **Add OSDP Devices** window appears, select the port to add the device to.



4. After selecting a port, click **Add**.

5. After completing the required settings in the **Add OSDP Devices** window, click **Save**.



Configure Wiegand devices

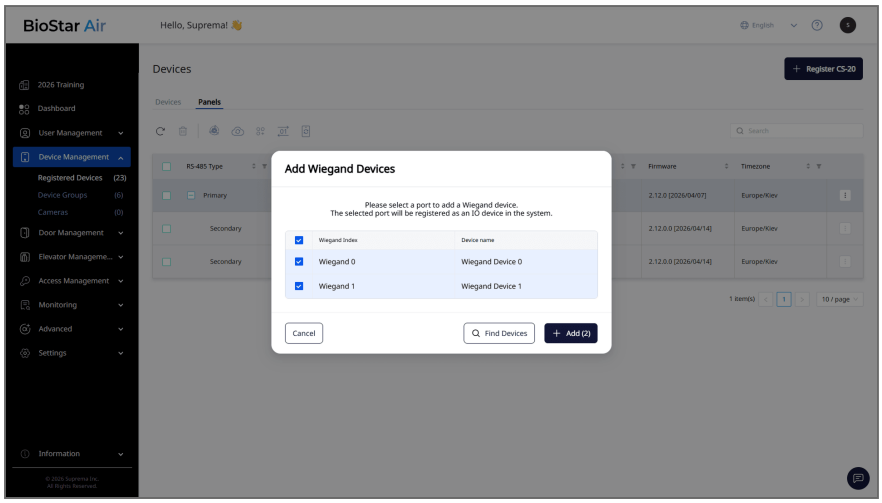
Wiegand is a communication protocol widely used in access control systems. Connect a Wiegand device to the CS-20 to configure it as a Wiegand secondary device.

1. In the panel list, click ⋮ at the far right of the registered CS-20 panel.



2. In the popup menu, click **Add Wiegand Devices**.

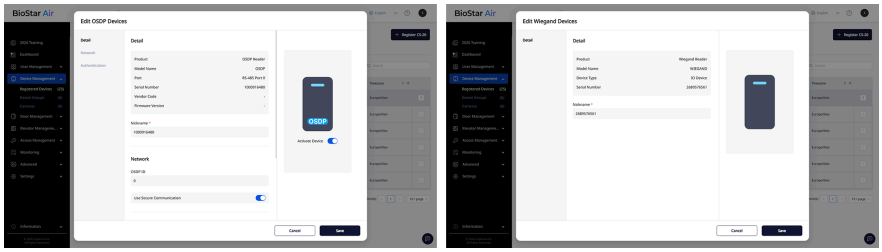
3. When the **Add Wiegand Devices** window appears, select a port to add a device.



4. After selecting a port, click **Add**.

Edit OSDP/Wiegand device information

1. Click **Device Management** → **Registered Devices** in the left sidebar.
2. Click the **Panels** tab.
3. Click the primary device's + icon in the list to expand the list of connected secondary devices.
4. Click the OSDP or Wiegand secondary device to edit its information.
5. When the Edit device information window appears, edit the details or settings.

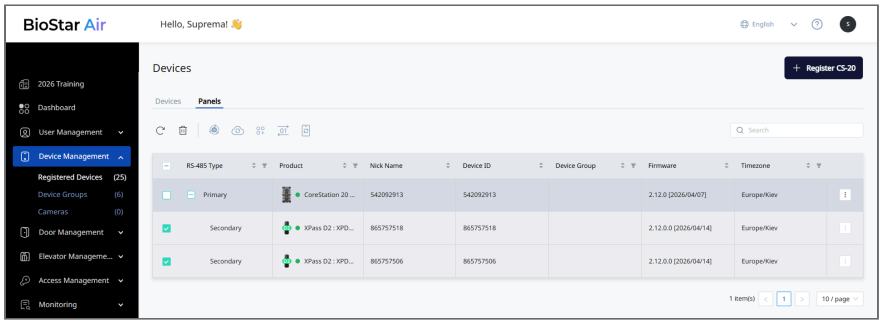


   - OSDP device: Set device name, network settings, authentication settings (RF Card, RF Card + PIN), and authentication timeout.
   - Wiegand device: Edit the device name.

6. Click **Save** at the bottom to save the changes.

Delete secondary devices

1. Click **Device Management** → **Registered Devices** in the left sidebar.
2. Click the **Panels** tab.
3. Click the primary device's + icon in the list to expand the list of connected secondary devices.
4. Click the checkbox for the secondary device to remove.
5. Click the 🗑 button at the top of the list.



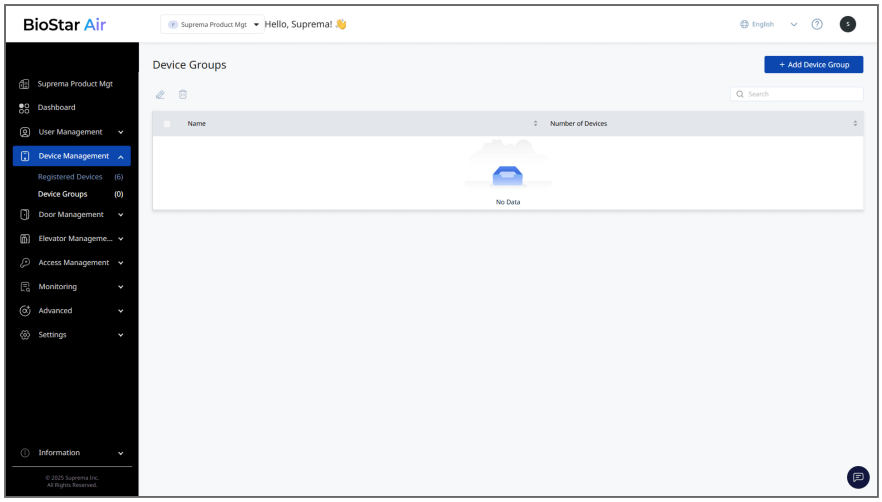
6. When the pop-up appears, click **Confirm**.

Manage Device and Panel Groups

BioStar Air enables efficient management of multiple devices and panels by grouping them. Device groups allow you to apply the same setting to multiple devices at once or easily monitor the status of devices in a certain group.

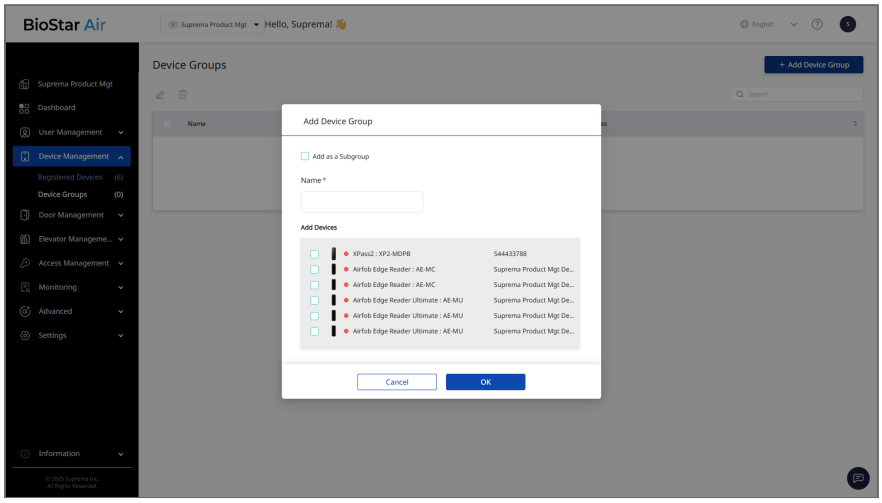
Add a device group

1. Click **Device Management** → **Device Groups** in the left sidebar.



2. Click **Add Device Group** at the top right of the screen.

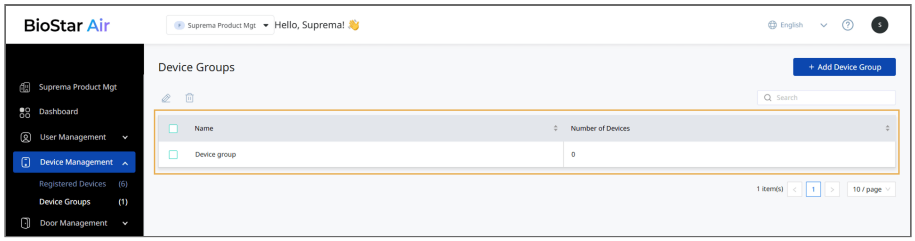
3. When the **Add Device Group** window appears, enter the group name.



> Click **Add as a Subgroup**, and then select the parent group to add the device group as a subgroup.

4. In **Add Devices**, select the devices to include in the group.
5. After selecting all devices, click **OK**.

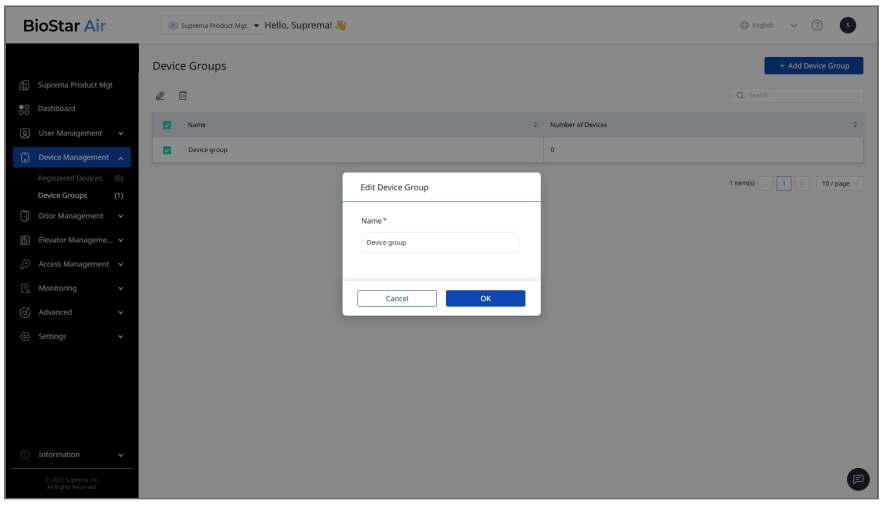
The device group list shows the newly added group and the number of devices in that group. Click a device group to view the devices in that group.



> **Info**
>
> For more information on how to add devices to a group or remove them from an existing group, see Manage Registered Edge Devices.

Rename a device group

1. Click **Device Management** → **Device Groups** in the left sidebar.
2. Select the checkbox for the device group to rename.
3. Click at the top of the device group list.
4. When the **Edit Device Group** window appears, enter the new group name.



5. Click **OK** to save the new group name.

Delete a device group

1. Click **Device Management** → **Device Groups** in the left sidebar.
2. Select the checkbox for the device group to delete.

3. Click 🗑 at the top of the device group list.

4. When a warning message appears, click **Yes**.

The selected device group is deleted from the list. Its subgroups are also deleted. Deleting a group does not delete the devices.

Use Edge Readers as Primary Devices

Set XPass 2 as the primary device to connect XPass D2 as a secondary device. Manage all access control logic on XPass 2. Configure a door with entry and exit devices without requiring two network connections.

This document provides step-by-step instructions to set XPass 2 as the primary device and connect XPass D2 as a secondary device. It also explains the features supported and the limitations of the primary-secondary configuration.

Before you start

Update the firmware to version 2.12 or later before setting XPass 2 as the primary device. For more information about firmware upgrades, see Upgrade Firmware.

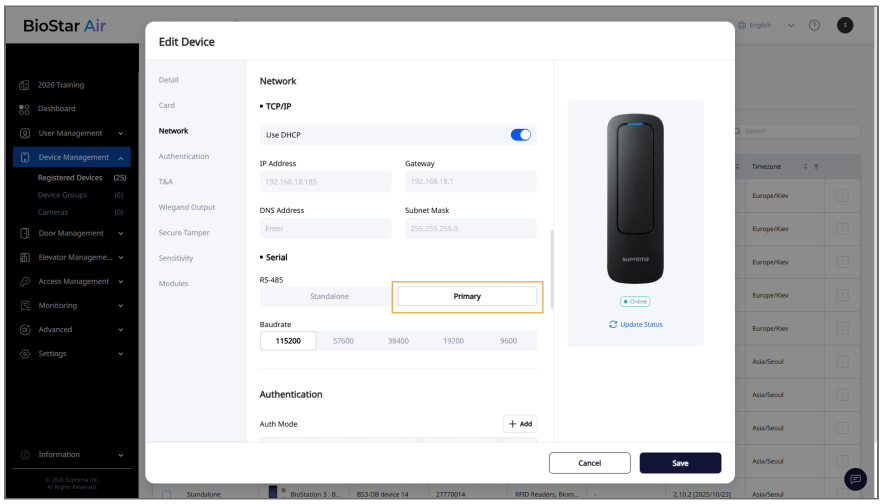
Set XPass 2 as the primary device

1. Click **Device Management** → **Registered Devices** in the left sidebar.

2. In the device list, click XPass 2.

3. When the **Edit Device** window appears, go to the **Network** section.

4. Change the **RS-485** setting to **Primary**.

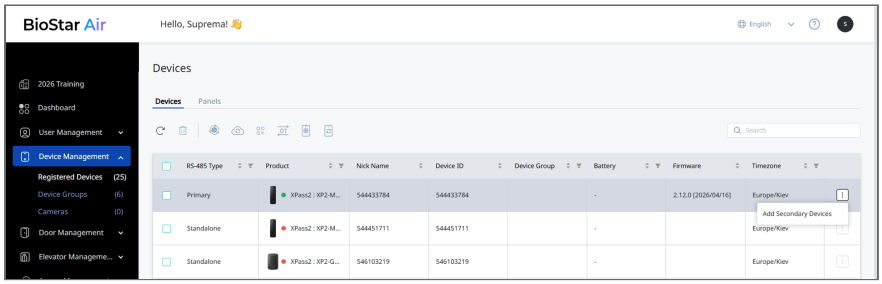


5. Click **Save** at the bottom to save the changes.

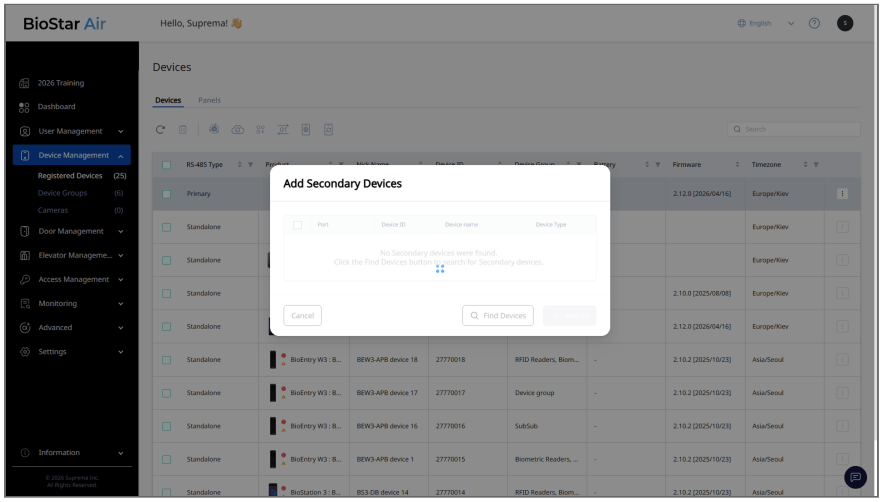
Add a secondary device

Add a slave device such as XPass D2 or Secure I/O 2 (SIO2).

1. In the device list, click ⋮ at the far right of the XPass 2 set as the primary device.



2. Click **Add Secondary Devices** to open the **Add Secondary Devices** window.



> If no secondary devices are found, click **Find Devices** to search again for devices connected to XPass 2.

3. When connected secondary devices appear in the list, click the checkbox next to each device you want to add.
4. Once your selections are complete, click **Add**.

Connected secondary devices appear hierarchically under XPass 2. See all devices connected to XPass 2 at a glance in the panel list.

> **Info**
>
> - For more information on XPass D2, see the XPass D2 installation guide.
> - An XPass 2 set as the primary device can have up to 31 secondary devices assigned.
> - For more information about the Secure I/O 2 (SIO2), see the Secure I/O 2 installation guide.

Device and Panel Configuration Options

This document is a reference for device and panel settings in BioStar Air. Administrators can check basic hardware information, perform actions such as firmware update, reboot, or reset. They can configure operation settings such as network, authentication, card format, time and attendance, Wiegand, sensitivity, and connected modules. Available settings vary depending on the device model and panel type.

▼ AirFob Edge

Detail

The **Detail** section provides basic information — such as the device name, model, serial number, and firmware version —

and includes an action menu for controlling features and default settings.

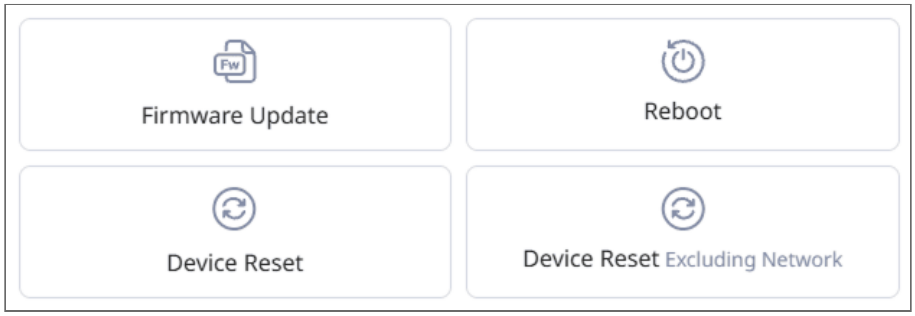
Basic Information

View the device's basic information. This information cannot be edited.

- **Product**: The product name.
- **Model Name**: The device's model name.
- **Serial Number**: The device's serial number.
- **Firmware Version**: The firmware version installed on the device.

Actions

The **Action** feature lets you control the device's functions.



- **Update Firmware**: Update the device firmware to the latest version.
- **Reboot**: Reboot the device remotely when an issue or anomaly occurs.
- **Device Reset**: Initialize all settings stored on the device. This action deletes all settings and data on the device.
- **Device Reset Excluding Network**: Initialize all settings except the network settings. This action deletes all settings and data but keeps the network settings.

Initial Settings

Modify the device's default settings.

- **Nickname**: The alias shown in the device list and logs. You can edit this field directly.
- **Timezone**: Set the device time zone to keep logs consistent when the site and device clocks differ. Activate the **Use DST** option to apply daylight saving time (DST).
- **Hands-Free**: Extend the BLE range.
- **QR Reader**: Confirm that an RS-485 QR reader is connected to the device.

> – When a QR reader is connected to the device, you cannot use another RS-485 device.
> – When using an SIO2, you cannot use a QR reader on the device connected to that door.

- **NFC/RF Card**: Activate or deactivate card authentication. DESFire and Felica card formats are supported.
- **Beep Setting**: Configure the success beep for access authentication.

Proprietary Cards

For Wiegand cards, you can select **iClass (SE / SEOS)** and **HID Prox**. Click the toggle to enable the feature, then select the

desired card format in **Proprietary Cards**.

> **Info**
>
> - Support may vary by device.
> - Wiegand supports 5 default formats. Add more formats in **Settings** → **Card Format**. For more information about custom card format settings, see Custom Wiegand card format.

Network

Modify the device's network settings.

- **Use DHCP**: Configure the device to obtain an IP address automatically.

  To set the network manually, disable **Use DHCP** and fill in the following fields.
  - **IP Address**
  - **Gateway**
  - **DNS Address**
  - **Subnet Mask**

T&A(Time & Attendance, T&A)

When this feature is enabled, **T&A Event** is logged in **Event Log** and used in **T&A Report**.

- **Use T&A**: Click the toggle switch to turn attendance management on or off.
- **T&A Mode**: Select the desired attendance mode.
  - **By Schedule**: Attendance events change automatically according to the set schedule. You can select a schedule to apply to attendance events.
  - **Fixed**: Only the selected attendance event is available.
  - **Mobile**: When presenting a mobile credential, the Suprema Pass app lets the user select the attendance event.

> **Info**
>
> For more information on configuring time and attendance, see Time & Attendance (T&A).

Wiegand Output

This feature integrates with external systems (e.g., alarm panels). Activate the **Use Wiegand Output** option to use this feature.

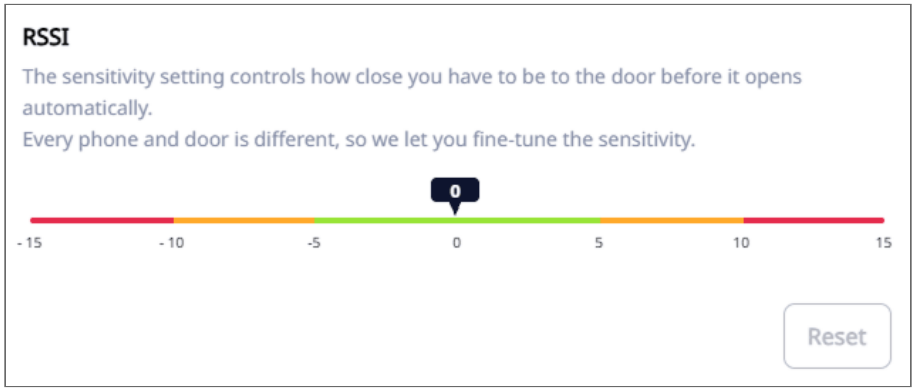
- **Output Mode**: Configure the Wiegand signal output mode.
  - **Regular**: Scan cards using the configured Wiegand format.
    - **Use Fail Code**: You can set error codes and choose the value to send when Wiegand card authentication fails.

  - **Bypass**: Send the CSN regardless of Wiegand authentication. Set this if you are using it as a device without door control functionality.
- **Output Info**: Select the information output during authentication.
- **Pulse Width**: Set the pulse width for the Wiegand signal.
- **Pulse Interval**: Set the pulse interval for the Wiegand signal.
- **Mobile Consecutive Tag**: Tag mobile cards consecutively without wait time.
- **Consecutive Tag Limit**: Set the maximum number of consecutive mobile card tags.

> **Info**
> The **Mobile Consecutive Tag** feature is supported in Suprema Pass app 2.9.0 or later.

Sensitivity

Adjust the RSSI value to set how close the mobile device must be to unlock the door.



- Lower values help block unintended activation.
- Higher values improve detection in high-interference environments.

> **Info**
> To reset the settings, click **Reset**.

Modules

Option to detect an OM-120 module connected to the device. Click **Add** to detect the module.

▼ XPass 2

Detail

The **Detail** section provides basic information — such as the device name, model, serial number, and firmware version — and includes an action menu for controlling features and default settings.

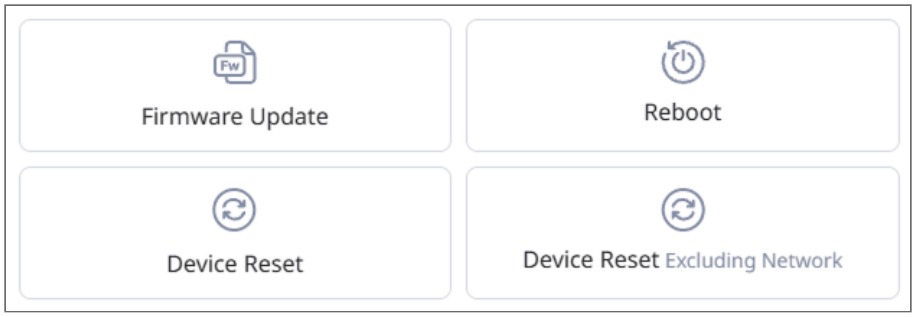
Basic Information

View the device's basic information. This information cannot be edited.

- **Product**: The product name.
- **Model Name**: The device's model name.
- **Serial Number**: The device's serial number.
- **Firmware Version**: The firmware version installed on the device.

Actions

The **Action** feature lets you control the device's functions.



- **Update Firmware**: Update the device firmware to the latest version.
- **Reboot**: Reboot the device remotely when an issue or anomaly occurs.
- **Device Reset**: Initialize all settings stored on the device. This action deletes all settings and data on the device.
- **Device Reset Excluding Network**: Initialize all settings except the network settings. This action deletes all settings and data but keeps the network settings.

Initial Settings

Modify the device's default settings.

- **Nickname**: The alias shown in the device list and logs. You can edit this field directly.
- **Timezone**: Set the device time zone to keep logs consistent when the site and device clocks differ. Activate the **Use DST** option to apply daylight saving time (DST).
- **Use RFID card number as PIN**: Enter the RF card number using the keypad to use it.

> This feature is supported only on the **XP2-GKDPB** model, which has a keypad.

- **Hands-Free**: Extend the BLE range.
- **QR Reader**: Confirm that an RS-485 QR reader is connected to the device.

> – When a QR reader is connected to the device, you cannot use another RS-485 device.
> – When using an SIO2, you cannot use a QR reader on the device connected to that door.

- **Beep Setting**: Configure the success beep for access authentication.
- **Video Service**: Connect IP cameras to the device to view live and recorded video. For more information on IP camera

connection settings, see IP Camera Support and Setup.

Card

In the **Card** section, you can modify card authentication settings.

NFC/RF Card

- **NFC/RF Card**: Click the toggle switch to enable or disable card access authentication. Select the card types supported for card authentication.
  - **EM4100 (125 KHz)**
  - **Mifare Classic/Mifare DESFire/FeliCa**
- **Byte Order**
  - **MSB**: Processes card data in order from large byte units to small byte units, sequentially storing the card serial number (CSN) from left to right.
  - **LSB**: Processes card data in order from small byte units to large byte units, storing the card serial number (CSN).
- **Data Reading Method**: Select CSN (default) or Wiegand format.

> Wiegand supports 5 default formats. Add more formats in **Settings** → **Card Format**. For more information about custom card format settings, see Custom Wiegand card format.

Proprietary Cards

For Wiegand cards, you can select **iClass (SE / SEOS)** and **HID Prox**. Click the toggle to enable the feature, then select the desired card format in **Proprietary Cards**.

> **Info**
>
> - Support may vary by device.
> - Wiegand supports 5 default formats. Add more formats in **Settings** → **Card Format**. For more information about custom card format settings, see Custom Wiegand card format.

Network

Modify the device's network settings.

- **Use DHCP**: Configure the device to obtain an IP address automatically.

  To set the network manually, disable **Use DHCP** and fill in the following fields.
  - **IP Address**
  - **Gateway**
  - **DNS Address**
  - **Subnet Mask**

- **RS-485**: Set the device to master mode to add XPass D2 devices as auxiliary devices.
- **Baudrate**: Set the serial communication baud rate between the device and auxiliary devices.

Authentication

- **Auth Mode**: Add authentication methods. Click **Add** to add an authentication method.
  - **XP2-MDPB / XP2-GDPB**: Only RF cards can be selected as the authentication method.
  - **XP2-GKDPB**: You can use a combination of an RF card and a PIN as the authentication method.
- **Auth Timeout**: Authentication fails if the credential is not authenticated within the set time.

> This feature is supported only on the **XP2-GKDPB** model.

> **Info**
> You can configure different authentication methods for the selected schedule. For example, you can allow card-only authentication during work hours and allow card-and-PIN authentication outside work hours.

T&A(Time & Attendance, T&A)

When this feature is enabled, **T&A Event** is logged in **Event Log** and used in **T&A Report**.

- **Use T&A**: Click the toggle switch to turn attendance management on or off.
- **T&A Mode**: Select the desired attendance mode.
  - **By Schedule**: Attendance events change automatically according to the set schedule. You can select a schedule to apply to attendance events.
  - **Fixed**: Only the selected attendance event is available.
  - **Mobile**: When presenting a mobile credential, the Suprema Pass app lets the user select the attendance event.

> **Info**
> For more information on configuring time and attendance, see Time & Attendance (T&A).

Wiegand Output

This feature integrates with external systems (e.g., alarm panels). Activate the **Use Wiegand Output** option to use this feature.

- **Output Mode**: Configure the Wiegand signal output mode.
  - **Regular**: Scan cards using the configured Wiegand format.
    - **Use Fail Code**: You can set error codes and choose the value to send when Wiegand card authentication fails.

  - **Bypass**: Send the CSN regardless of Wiegand authentication. Set this if you are using it as a device without door control functionality.
- **Output Info**: Select the information output during authentication.
- **Pulse Width**: Set the pulse width for the Wiegand signal.
- **Pulse Interval**: Set the pulse interval for the Wiegand signal.
- **Mobile Consecutive Tag**: Tag mobile cards consecutively without wait time.
- **Consecutive Tag Limit**: Set the maximum number of consecutive mobile card tags.

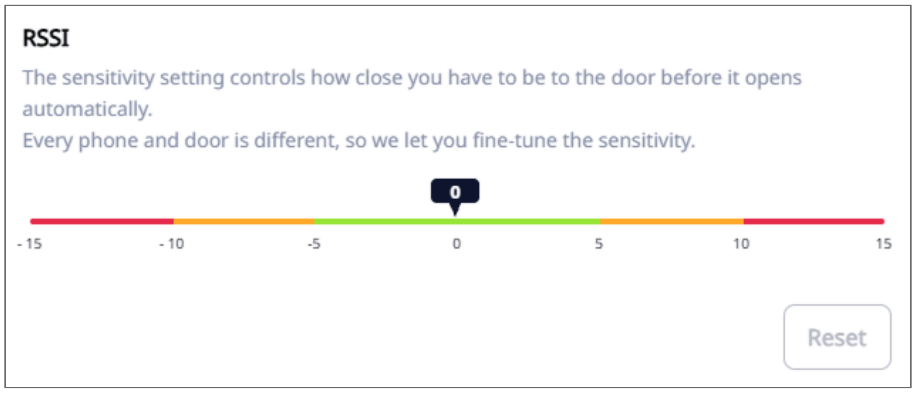
> **Info**
> The **Mobile Consecutive Tag** feature is supported in Suprema Pass app 2.9.0 or later.

Secure Tamper

If a tamper event occurs, configure the device to delete **all user information**, **all logs**, and **security keys** stored on the device.

Sensitivity

Adjust the RSSI value to set how close the mobile device must be to unlock the door.



- Lower values help block unintended activation.
- Higher values improve detection in high-interference environments.

> **Info**
> To reset the settings, click **Reset**.

Modules

Option to detect an OM-120 module connected to the device. Click **Add** to detect the module.

▼ XPass D2

Detail

The **Detail** section provides basic information — such as the device name, model, serial number, and firmware version — and includes an action menu for controlling features and default settings.

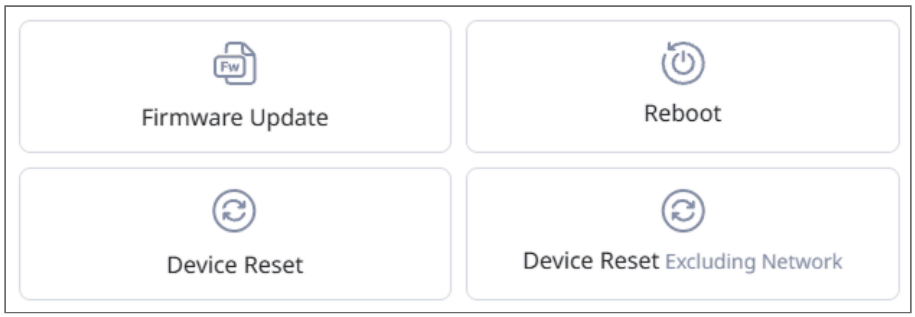
Basic Information

View the device's basic information. This information cannot be edited.

- **Product**: The product name.
- **Model Name**: The device's model name.
- **Serial Number**: The device's serial number.
- **Firmware Version**: The firmware version installed on the device.

Actions

The **Action** feature lets you control the device's functions.



- **Update Firmware**: Update the device firmware to the latest version.
- **Reboot**: Reboot the device remotely when an issue or anomaly occurs.
- **Device Reset**: Initialize all settings stored on the device. This action deletes all settings and data on the device.
- **Device Reset Excluding Network**: Initialize all settings except the network settings. This action deletes all settings and data but keeps the network settings.

Initial Settings

Modify the device's default settings.

- **Nickname**: The alias shown in the device list and logs. You can edit this field directly.
- **Hands-Free**: Extend the BLE range.
- **Beep Setting**: Configure the success beep for access authentication.

Card

In the **Card** section, you can modify card authentication settings.

NFC/RF Card

- **NFC/RF Card**: Click the toggle switch to enable or disable card access authentication. Select the card types supported for card authentication.
  - **EM4100 (125 KHz)**
  - **Mifare Classic/Mifare DESFire/FeliCa**
- **Byte Order**
  - **MSB**: Processes card data in order from large byte units to small byte units, sequentially storing the card serial number (CSN) from left to right.
  - **LSB**: Processes card data in order from small byte units to large byte units, storing the card serial number (CSN).
- **Data Reading Method**: Select CSN (default) or Wiegand format.

> Wiegand supports 5 default formats. Add more formats in **Settings** → **Card Format**. For more information about custom card format settings, see Custom Wiegand card format.

Proprietary Cards

For Wiegand cards, you can select **iClass (SE / SEOS)** and **HID Prox**. Click the toggle to enable the feature, then select the desired card format in **Proprietary Cards**.

> **Info**
>
> - Support may vary by device.
> - Wiegand supports 5 default formats. Add more formats in **Settings** → **Card Format**. For more information about custom card format settings, see Custom Wiegand card format.

Authentication

- **Auth Mode**: Add authentication methods. Click **Add** to add an authentication method. Only RF cards can be selected as the authentication method.

> **Info**
>
> You can configure different authentication methods for the selected schedule. For example, you can allow card-only authentication during work hours and allow card-and-PIN authentication outside work hours.

T&A(Time & Attendance, T&A)

When this feature is enabled, **T&A Event** is logged in **Event Log** and used in **T&A Report**.

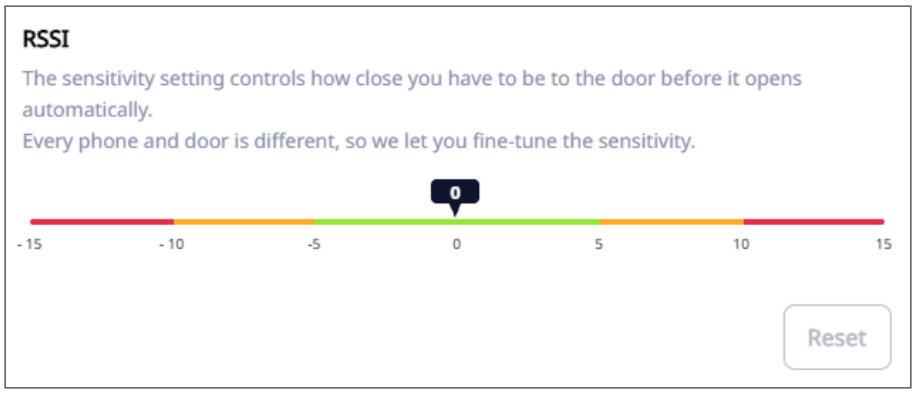
- **Use T&A**: Click the toggle switch to turn attendance management on or off.
- **T&A Mode**: Select the desired attendance mode.

- **By Schedule**: Attendance events change automatically according to the set schedule. You can select a schedule to apply to attendance events.
- **Fixed**: Only the selected attendance event is available.

> **Info**
> For more information on configuring time and attendance, see Time & Attendance (T&A).

Sensitivity

Adjust the RSSI value to set how close the mobile device must be to unlock the door.



- Lower values help block unintended activation.
- Higher values improve detection in high-interference environments.

> **Info**
> To reset the settings, click **Reset**.

▼ X-Station 2

Detail

The **Detail** section provides basic information — such as the device name, model, serial number, and firmware version — and includes an action menu for controlling features and default settings.

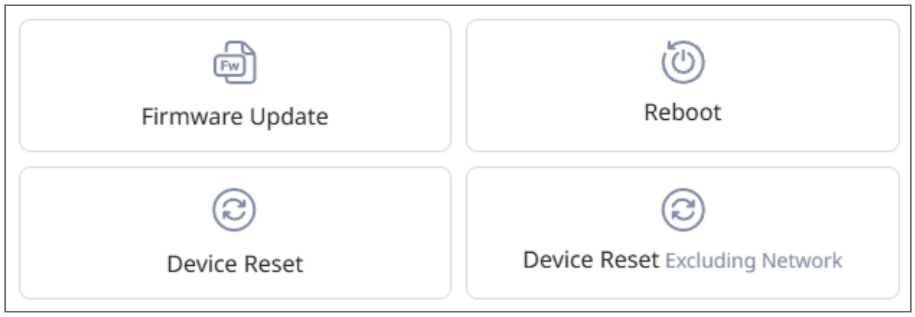
Basic Information

View the device's basic information. This information cannot be edited.

- **Product**: The product name.
- **Model Name**: The device's model name.
- **Serial Number**: The device's serial number.
- **Firmware Version**: The firmware version installed on the device.

Actions

The **Action** feature lets you control the device's functions.



- **Update Firmware**: Update the device firmware to the latest version.
- **Reboot**: Reboot the device remotely when an issue or anomaly occurs.
- **Device Reset**: Initialize all settings stored on the device. This action deletes all settings and data on the device.
- **Device Reset Excluding Network**: Initialize all settings except the network settings. This action deletes all settings and data but keeps the network settings.

Initial Settings

Modify the device's default settings.

- **Nickname**: The alias shown in the device list and logs. You can edit this field directly.
- **Timezone**: Set the device time zone to keep logs consistent when the site and device clocks differ. Activate the **Use DST** option to apply daylight saving time (DST).
- **Hands-Free**: Extend the BLE range.
- **QR Reader**: Confirm that an RS-485 QR reader is connected to the device.

> – When a QR reader is connected to the device, you cannot use another RS-485 device.
> – When using an SIO2, you cannot use a QR reader on the device connected to that door.

- **NFC/RF Card**: Activate or deactivate card authentication. DESFire and Felica card formats are supported.

Proprietary Cards

For Wiegand cards, you can select **iClass (SE / SEOS)** and **HID Prox**. Click the toggle to enable the feature, then select the desired card format in **Proprietary Cards**.

> **Info**
>
> - Support may vary by device.
> - Wiegand supports 5 default formats. Add more formats in **Settings** → **Card Format**. For more information about custom card format settings, see Custom Wiegand card format.

Network

Modify the device's network settings.

- **Use DHCP**: Configure the device to obtain an IP address automatically.

To set the network manually, disable **Use DHCP** and fill in the following fields.
- **IP Address**
- **Gateway**
- **DNS Address**
- **Subnet Mask**

T&A(Time & Attendance, T&A)

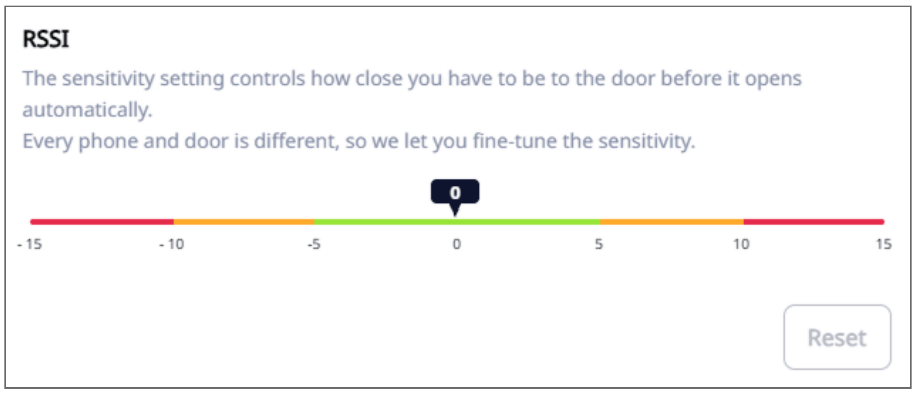
When this feature is enabled, **T&A Event** is logged in **Event Log** and used in **T&A Report**.

- **Use T&A**: Click the toggle switch to turn attendance management on or off.
- **T&A Mode**: Select the desired attendance mode.
  - **By Schedule**: Attendance events change automatically according to the set schedule. You can select a schedule to apply to attendance events.
  - **Fixed**: Only the selected attendance event is available.
  - **Mobile**: When presenting a mobile credential, the Suprema Pass app lets the user select the attendance event.

> **Info**
> For more information on configuring time and attendance, see Time & Attendance (T&A).

Sensitivity

Adjust the RSSI value to set how close the mobile device must be to unlock the door.



- Lower values help block unintended activation.
- Higher values improve detection in high-interference environments.

> **Info**
> To reset the settings, click **Reset**.

Modules

Option to detect an OM-120 module connected to the device. Click **Add** to detect the module.

▼ BioEntry W3

Detail

The **Detail** section provides basic information — such as the device name, model, serial number, and firmware version — and includes an action menu for controlling features and default settings.

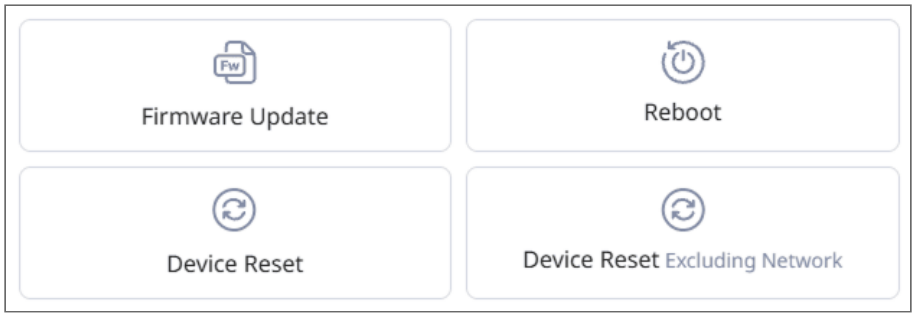
Basic Information

View the device's basic information. This information cannot be edited.

- **Product**: The product name.
- **Model Name**: The device's model name.
- **Serial Number**: The device's serial number.
- **Firmware Version**: The firmware version installed on the device.

Actions

The **Action** feature lets you control the device's functions.



- **Update Firmware**: Update the device firmware to the latest version.
- **Reboot**: Reboot the device remotely when an issue or anomaly occurs.
- **Device Reset**: Initialize all settings stored on the device. This action deletes all settings and data on the device.
- **Device Reset Excluding Network**: Initialize all settings except the network settings. This action deletes all settings and data but keeps the network settings.

Initial Settings

Modify the device's default settings.

- **Nickname**: The alias shown in the device list and logs. You can edit this field directly.
- **Timezone**: Set the device time zone to keep logs consistent when the site and device clocks differ. Activate the **Use DST** option to apply daylight saving time (DST).
- **Hands-Free**: Extend the BLE range.

Card

In the **Card** section, you can modify card authentication settings.

NFC/RF Card

- **NFC/RF Card**: Click the toggle switch to enable or disable card access authentication. Select the card types supported for card authentication.
  - **EM4100 (125 KHz)**
  - **Mifare Classic/Mifare DESFire/FeliCa**
- **Byte Order**
  - **MSB**: Processes card data in order from large byte units to small byte units, sequentially storing the card serial number (CSN) from left to right.
  - **LSB**: Processes card data in order from small byte units to large byte units, storing the card serial number (CSN).
- **Data Reading Method**: Select CSN (default) or Wiegand format.

> Wiegand supports 5 default formats. Add more formats in **Settings** → **Card Format**. For more information about custom card format settings, see Custom Wiegand card format.

Proprietary Cards

For Wiegand cards, you can select **iClass (SE / SEOS)** and **HID Prox**. Click the toggle to enable the feature, then select the desired card format in **Proprietary Cards**.

> **Info**
>
> - Support may vary by device.
> - Wiegand supports 5 default formats. Add more formats in **Settings** → **Card Format**. For more information about custom card format settings, see Custom Wiegand card format.

Network

Modify the device's network settings.

- **Use DHCP**: Configure the device to obtain an IP address automatically.

  To set the network manually, disable **Use DHCP** and fill in the following fields.
  - **IP Address**
  - **Gateway**
  - **DNS Address**
  - **Subnet Mask**

Authentication

- **Auth Mode**: Add authentication methods. Click **Add** to add an authentication method. You can use a combination of an RF card and facial recognition as the authentication method.

> **Info**
> You can configure different authentication methods for the selected schedule. For example, you can allow card-only authentication during work hours and allow card-and-PIN authentication outside work hours.

Face

Security

- **Fake Detection**: Prevent user authentication with spoofed faces such as photos.
- **Duplicate Check**: Check for duplicate registrations when enrolling facea.

Detection

- **Motion Sensor Sensitivity**: Set the sensitivity for detecting movement around the device.
- **Maximum Head Pose Angle**: Set the maximum rotation angle allowed for a face.
- **Wide Search**: Expand the area in the camera view where faces are recognized.
- **Detection Distance (cm)**: Set the minimum and maximum recognition distance.
- **Enrollment Time (sec)**: If a face is not enrolled within the set time during enrollment, the process is canceled.

Mask Detection

Activate the **Mask Detection** option to configure mask detection.

- **Mask Detect Level**: Select mask detection sensitivity.
- **If Mask Detection Fails**
  - **Deny Access**: Users not wearing a mask are denied authentication, and a mask-non-compliance event log is recorded.
  - **Allow Access After Logging**: Users not wearing a mask can still authenticate, but a mask-non-compliance event log is recorded.
- **Mask Check**
  - **After Access**: After authentication, check mask usage or measure temperature.
  - **Before Access**: Check mask usage or measure temperature before authentication. In this case, users not wearing a mask or exceeding the threshold temperature cannot authenticate.
  - **Without Access**: Use the device only to check mask usage or measure temperature. Users wearing a mask or having a temperature below the threshold can enter regardless of authentication.
- **Authenticate QR or Barcode with Device Camera**: Set whether to allow QR/barcode authentication via the device's camera.
- **Authenticate Card Number with QR**: Set authentication to accept a QR code containing the same data as the CSN card or Wiegand card issued to the user. This feature is available when the **Authenticate QR or Barcode with Device Camera** option is enabled.

> **Info**
> When using non-face credentials, the timing of "before" and "after" is usually important.

T&A(Time & Attendance, T&A)

When this feature is enabled, **T&A Event** is logged in **Event Log** and used in **T&A Report**.

- **Use T&A**: Click the toggle switch to turn attendance management on or off.
- **T&A Mode**: Select the desired attendance mode.
  - **By Schedule**: Attendance events change automatically according to the set schedule. You can select a schedule to apply to attendance events.
  - **Fixed**: Only the selected attendance event is available.

> **Info**
> For more information on configuring time and attendance, see Time & Attendance (T&A).

Wiegand Output

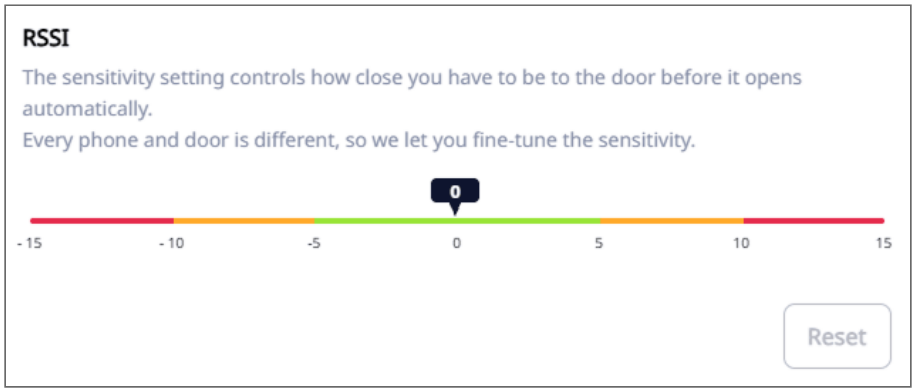
This feature integrates with external systems (e.g., alarm panels). Activate the **Use Wiegand Output** option to use this feature.

- **Output Mode**: Configure the Wiegand signal output mode.
  - **Regular**: Scan cards using the configured Wiegand format.
    - **Use Fail Code**: You can set error codes and choose the value to send when Wiegand card authentication fails.
  - **Bypass**: Send the CSN regardless of Wiegand authentication. Set this if you are using it as a device without door control functionality.
- **Output Info**: Select the information output during authentication.
- **Pulse Width**: Set the pulse width for the Wiegand signal.
- **Pulse Interval**: Set the pulse interval for the Wiegand signal.
- **Mobile Consecutive Tag**: Tag mobile cards consecutively without wait time.
- **Consecutive Tag Limit**: Set the maximum number of consecutive mobile card tags.

> **Info**
> The **Mobile Consecutive Tag** feature is supported in Suprema Pass app 2.9.0 or later.

Sensitivity

Adjust the RSSI value to set how close the mobile device must be to unlock the door.



- Lower values help block unintended activation.
- Higher values improve detection in high-interference environments.

> **Info**
> To reset the settings, click **Reset**.

▼ BioStation 3

Detail

The **Detail** section provides basic information — such as the device name, model, serial number, and firmware version — and includes an action menu for controlling features and default settings.

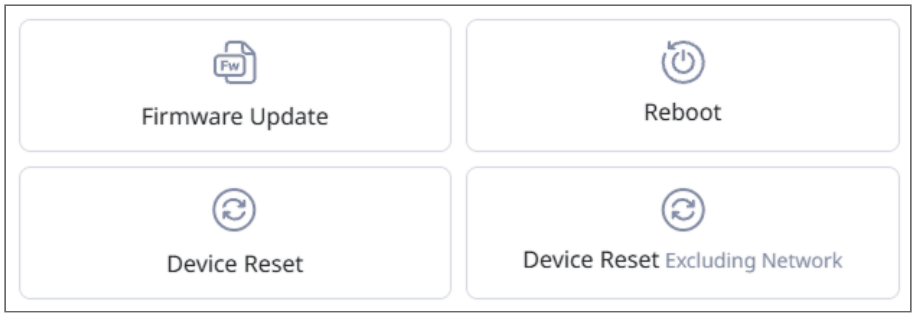
Basic Information

View the device's basic information. This information cannot be edited.

- **Product**: The product name.
- **Model Name**: The device's model name.
- **Serial Number**: The device's serial number.
- **Firmware Version**: The firmware version installed on the device.

Actions

The **Action** feature lets you control the device's functions.



- **Update Firmware**: Update the device firmware to the latest version.
- **Reboot**: Reboot the device remotely when an issue or anomaly occurs.
- **Device Reset**: Initialize all settings stored on the device. This action deletes all settings and data on the device.
- **Device Reset Excluding Network**: Initialize all settings except the network settings. This action deletes all settings and

data but keeps the network settings.

Initial Settings

Modify the device's default settings.

- **Nickname**: The alias shown in the device list and logs. You can edit this field directly.
- **Timezone**: Set the device time zone to keep logs consistent when the site and device clocks differ. Activate the **Use DST** option to apply daylight saving time (DST).
- **Hands-Free**: Extend the BLE range.
- **Video Service**: Connect IP cameras to the device to view live and recorded video. For more information on IP camera connection settings, see IP Camera Support and Setup.

Card

In the **Card** section, you can modify card authentication settings.

NFC/RF Card

- **NFC/RF Card**: Click the toggle switch to enable or disable card access authentication. Select the card types supported for card authentication.
  - **EM4100 (125 KHz)**
  - **Mifare Classic/Mifare DESFire/FeliCa**
- **Byte Order**
  - **MSB**: Processes card data in order from large byte units to small byte units, sequentially storing the card serial number (CSN) from left to right.
  - **LSB**: Processes card data in order from small byte units to large byte units, storing the card serial number (CSN).
- **Data Reading Method**: Select CSN (default) or Wiegand format.

> Wiegand supports 5 default formats. Add more formats in **Settings** → **Card Format**. For more information about custom card format settings, see Custom Wiegand card format.

Proprietary Cards

For Wiegand cards, you can select **iClass (SE / SEOS)** and **HID Prox**. Click the toggle to enable the feature, then select the desired card format in **Proprietary Cards**.

> **Info**
>
> - Support may vary by device.
> - Wiegand supports 5 default formats. Add more formats in **Settings** → **Card Format**. For more information about custom card format settings, see Custom Wiegand card format.

Network

Modify the device's network settings.

- **Use DHCP**: Configure the device to obtain an IP address automatically.

  To set the network manually, disable **Use DHCP** and fill in the following fields.
  - **IP Address**
  - **Gateway**
  - **DNS Address**
  - **Subnet Mask**

Authentication

- **Auth Mode**: Add authentication methods. Click **Add** to add an authentication method. You can choose a combination of RF card, face, ID, and PIN for authentication.
- **Display User Name** / **Display User ID**: Choose whether to show the user name or ID on the authentication screen. Select **Hidden** to hide them.
- **Auth Timeout**: Authentication fails if the credential is not authenticated within the set time.

> **Info**
> You can configure different authentication methods for the selected schedule. For example, you can allow card-only authentication during work hours and allow card-and-PIN authentication outside work hours.

Face

Security

- **Fake Detection**: Prevent user authentication with spoofed faces such as photos.
- **Duplicate Check**: Check for duplicate registrations when enrolling facea.

Detection

- **Motion Sensor Sensitivity**: Set the sensitivity for detecting movement around the device.
- **Maximum Head Pose Angle**: Set the maximum rotation angle allowed for a face.
- **Wide Search**: Expand the area in the camera view where faces are recognized.
- **Detection Distance (cm)**: Set the minimum and maximum recognition distance.
- **Enrollment Time (sec)**: If a face is not enrolled within the set time during enrollment, the process is canceled.

Mask Detection

Activate the **Mask Detection** option to configure mask detection.

- **Mask Detect Level**: Select mask detection sensitivity.

- **If Mask Detection Fails**
  - **Deny Access**: Users not wearing a mask are denied authentication, and a mask-non-compliance event log is recorded.
  - **Allow Access After Logging**: Users not wearing a mask can still authenticate, but a mask-non-compliance event log is recorded.
- **Mask Check**
  - **After Access**: After authentication, check mask usage or measure temperature.
  - **Before Access**: Check mask usage or measure temperature before authentication. In this case, users not wearing a mask or exceeding the threshold temperature cannot authenticate.
  - **Without Access**: Use the device only to check mask usage or measure temperature. Users wearing a mask or having a temperature below the threshold can enter regardless of authentication.
- **Authenticate QR or Barcode with Device Camera**: Set whether to allow QR/barcode authentication via the device's camera.
- **Authenticate Card Number with QR**: Set authentication to accept a QR code containing the same data as the CSN card or Wiegand card issued to the user. This feature is available when the **Authenticate QR or Barcode with Device Camera** option is enabled.

> **Info**
> When using non-face credentials, the timing of "before" and "after" is usually important.

T&A(Time & Attendance, T&A)

When this feature is enabled, **T&A Event** is logged in **Event Log** and used in **T&A Report**.

- **Use T&A**: Click the toggle switch to turn attendance management on or off.
- **T&A Mode**: Select the desired attendance mode.
  - **User Selects**: When the attendance key appears on the screen, the user selects the attendance event during authentication.

    > **T&A is Required**: Enable this option to require users to register an attendance event when authenticating.

  - **By Schedule**: Attendance events change automatically according to the set schedule. You can select a schedule to apply to attendance events.
  - **Last Choice**: The user continues to use the last selected attendance event.
  - **Fixed**: Only the selected attendance event is available.

> **Info**
> For more information on configuring time and attendance, see Time & Attendance (T&A).

Display & Sound

Display

- **Use Screensaver**: Reduce LCD brightness when the device is not in use to lower unnecessary power consumption.
- **Always On Backlight**: Keep the backlight always on or dim it after inactivity.
- **Backlight Timeout**: Set the time before the backlight turns off automatically.
- **Language**: Set the language shown on the device screen.
- **Home Screen**: Configure the items displayed on the device's home screen background.
  - **Normal**: Display the default image on the home screen.
  - **Logo**: Display a user-registered image on the home screen.
  - **Notice**: Display administrator input on the home screen.

> After clicking **Update** and saving, the image or notice no longer appears in the edit screen but remains on the device.

Sound

- **Use Voice Instruction**: Use voice guidance instead of notification tones.
- **Device Volume**: Adjust the volume of sounds generated by the device.
- **Intercom Speaker Volume** / **Intercom Microphone Volume**: Adjust the output or input volume when using the IP intercom feature.

Wiegand Output

This feature integrates with external systems (e.g., alarm panels). Activate the **Use Wiegand Output** option to use this feature.

- **Output Mode**: Configure the Wiegand signal output mode.
  - **Regular**: Scan cards using the configured Wiegand format.
    - **Use Fail Code**: You can set error codes and choose the value to send when Wiegand card authentication fails.
  - **Bypass**: Send the CSN regardless of Wiegand authentication. Set this if you are using it as a device without door control functionality.
- **Output Info**: Select the information output during authentication.
- **Pulse Width**: Set the pulse width for the Wiegand signal.
- **Pulse Interval**: Set the pulse interval for the Wiegand signal.
- **Mobile Consecutive Tag**: Tag mobile cards consecutively without wait time.
- **Consecutive Tag Limit**: Set the maximum number of consecutive mobile card tags.

> **Info**
>
> The **Mobile Consecutive Tag** feature is supported in Suprema Pass app 2.9.0 or later.

Intercom

- **Use Intercom**: Activate or deactivate the IP intercom feature.
- **SIP Server Transport**: Choose the SIP transport method when configuring the intercom's SIP server.
- **SIP Server Address**: Enter the SIP server address.
- **SIP Server Port**: Enter the SIP server port.
- **Registration Duration**: Enter the registration duration. The device attempts to register with the SIP server every time the registration duration expires.
- **SIP Username**: Enter the SIP account username.
- **Password**: Enter the SIP account password.
- **Authorization ID**: Enter the SIP account authorization ID.
- **Outbound Proxy Server**: Use a separate outbound proxy server for SIP services if required.
- **Extension Number**: Add or edit extension numbers.
- **Video Resolution**: Select the video resolution when using the intercom.
- **Open Door Button**: Specify a button to unlock the door during a call.

Secure Tamper

If a tamper event occurs, configure the device to delete **all user information**, **all logs**, and **security keys** stored on the device.

RTSP

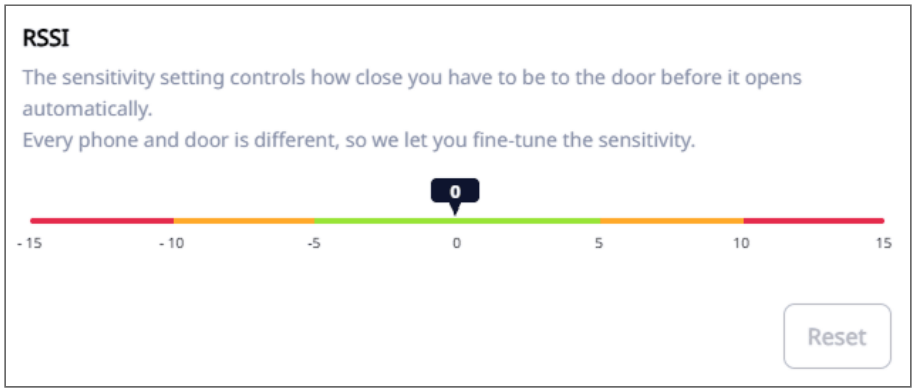
Configure details for **Real Time Streaming Protocol** (RTSP) streaming. The device's camera can stream live video.

- **Use RTSP**: Turn RTSP streaming on or off.
- **Address**: RTSP server address.
- **Port**: Enter the RTSP server port.
- **ID** / **Password**: Enter the RTSP server ID and password.
- **RTSP Video Resolution**: Select the video resolution when using RTSP.

> **Info**
> The RTSP streaming feature is supported only on BioStation 3.

Sensitivity

Adjust the RSSI value to set how close the mobile device must be to unlock the door.



- Lower values help block unintended activation.
- Higher values improve detection in high-interference environments.

> **Info**
> To reset the settings, click **Reset**.

▼ CoreStation 20

Detail

The **Detail** section provides basic information — such as the device name, model, serial number, and firmware version — and includes an action menu for controlling features and default settings.

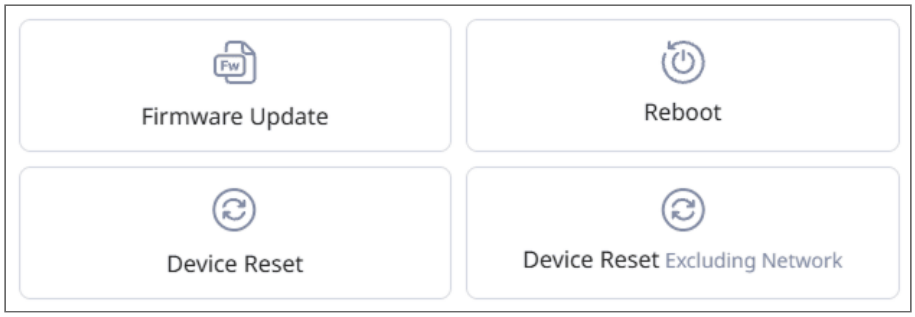
Basic Information

View the device's basic information. This information cannot be edited.

- **Product**: The product name.
- **Model Name**: The device's model name.
- **Serial Number**: The device's serial number.
- **Firmware Version**: The firmware version installed on the device.

Actions

The **Action** feature lets you control the device's functions.



- **Update Firmware**: Update the device firmware to the latest version.
- **Reboot**: Reboot the device remotely when an issue or anomaly occurs.
- **Device Reset**: Initialize all settings stored on the device. This action deletes all settings and data on the device.
- **Device Reset Excluding Network**: Initialize all settings except the network settings. This action deletes all settings and

data but keeps the network settings.

Initial Settings

Modify the device's default settings.

- **Nickname**: The alias shown in the device list and logs. You can edit this field directly.
- **Timezone**: Set the device time zone to keep logs consistent when the site and device clocks differ. Activate the **Use DST** option to apply daylight saving time (DST).
- **Video Service**: Connect IP cameras to the panel to view live and recorded video. For more information on IP camera connection settings, see IP Camera Support and Setup.

Card

In the **Card** section, you can modify card authentication settings.

NFC/RF Card

- **NFC/RF Card**: Click the toggle switch to enable or disable card access authentication. Select the card types supported for card authentication.
  - **EM4100 (125 KHz)**
  - **Mifare Classic/Mifare DESFire/FeliCa**
- **Byte Order**
  - **MSB**: Processes card data in order from large byte units to small byte units, sequentially storing the card serial number (CSN) from left to right.
  - **LSB**: Processes card data in order from small byte units to large byte units, storing the card serial number (CSN).
- **Data Reading Method**: Select CSN (default) or Wiegand format.

> Wiegand supports 5 default formats. Add more formats in **Settings** → **Card Format**. For more information about custom card format settings, see Custom Wiegand card format.

Network

Modify the device's network settings.

- **Use DHCP**: Configure the device to obtain an IP address automatically.

  To set the network manually, disable **Use DHCP** and fill in the following fields.
  - **IP Address**
  - **Gateway**
  - **DNS Address**
  - **Subnet Mask**
- **SCB Key**: Enter the Serial Communication Block (SCB) security key. Enter up to 32 characters. This is used to secure serial communication.
- **SCB Key Confirm**: Re-enter the same value to prevent security key errors.

- **Baud Rate**: Set the serial communication baud rate between the panel and secondary devices.
  - **Host**: Panel communication baud rate
  - **0** / **1**: Baud rate for each port connected to an auxiliary device

> **Info**
>
> - Set the SCB key before adding OSDP devices. If OSDP devices have already been added, the SCB key cannot be changed.
> - If a third-party OSDP device manufacturer uses a specific SCB key, configure the CS-20 to use the same key as the OSDP device.
> - If the SCB keys on the CS-20 and the OSDP device do not match, connecting to the device via **Secure Session** is not possible.
> - **Baud Rate**: Set a different baud rate independently; the default is `115200`.

Advanced

Device Input Status

If a tamper sensor, power-failure sensor, or fire detector is connected to the AUX IN terminal, you can enable or disable it.

- **Tamper**
- **AC Fail**
- **Fire**

> **Info**
>
> To use a Fail Safe Lock, connect an **N/C** relay; to use a Fail Secure Lock, connect an **N/O** relay. For more information on relay connections, see the CoreStation 20 installation guide.

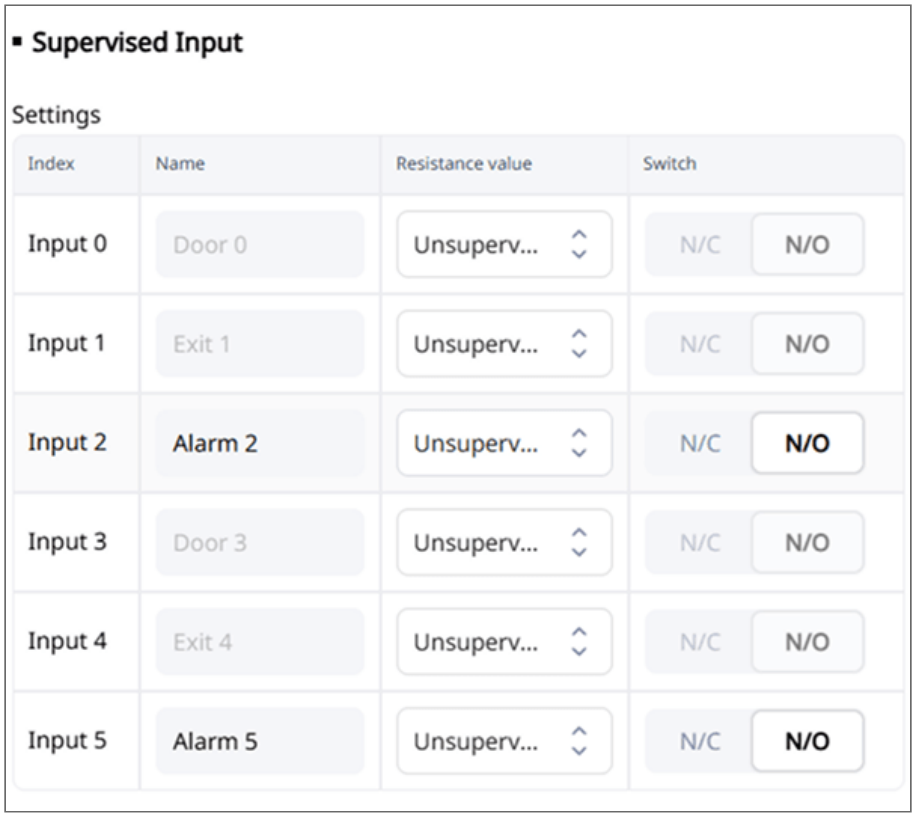
Wiegand Input

Configure detailed Wiegand input settings.

- **Use Wiegand Input**: Enable or disable the Wiegand input feature.
- **Input Format**: Select the Wiegand input format.
- **Pulse Width**: Set the pulse width for the Wiegand signal.
- **Pulse Interval**: Set the pulse interval for the Wiegand signal.

Supervised Input

You can set the Supervised Input port to function as an Input port and configure the resistor value used for Supervised Input. Resistor values can be set to 1 kΩ, 2.2 kΩ, 4.7 kΩ, or 10 kΩ.



Secure Tamper

If a tamper event occurs, configure the panel to delete **all user information**, **all logs**, and **security keys** stored on the panel.

Modules

Option to detect an OM-120 module connected to the panel. Click **Add** to detect the module.

Configure Airfob Patch and Tag

Register the Airfob Patch in the BioStar Air app

Before you start

- Install the BioStar Air app on your mobile device. Install the mobile app through the following link.
  - iOS
  - Android
- Log in using the same ID and password you use for the BioStar Air admin portal.
- Make sure BLE is enabled on your mobile device.
- Attach the Airfob Patch to the reader permanently or temporarily. For more information, see Install Airfob Patch.

> **Info**
> For more information on using the BioStar Air mobile app, see Getting Started with the BioStar Air App.

Register Airfob Patch

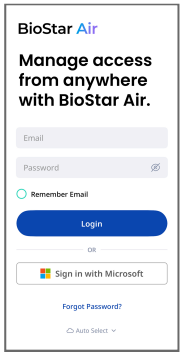
1. Open the BioStar Air app on your mobile device and log in.
2. On the BioStar Air home screen, tap **Management** at the bottom.
3. Bring your mobile device within 10 cm of the Airfob Patch, then tap the + button in the upper-right corner of the screen.
4. In the device search screen, tap **Register** for Airfob Patch to register.
5. When the device registration window appears, tap **OK**.

Return to the device list and confirm the added Airfob Patch.

Configuration steps

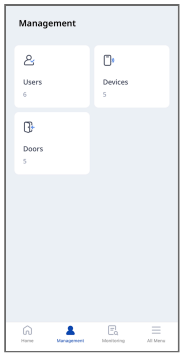
Install the Airfob Patch or Tag and register it to the BioStar Air app. Follow these steps to configure the device.

1 Run the app



1. Run **BioStar Air** on your mobile device.
2. Sign in to the site where the Airfob Patch or Tag is registered.

2 Go to device settings



1. On the **BioStar Air** home screen, tap **Management** at the bottom.
2. To view the registered devices, tap **Devices**.
3. Select the Airfob Patch or Tag from the device list.

3 Enable BLE mode

- Hold the mobile device close to the unit.
- Activate the **BLE Mode** in the app.

4 Set the card ID output method

- Scroll to **Card ID Output Method** and tap **Edit**.
- Tap **Select** next to **User Card ID**.

5 Choose the output method

- **None**: Select this option when you do not want to send a card ID. Useful for time and attendance to extend battery life.
- **Fixed Device**: Sends the pre-programmed fixed card ID. Useful for door locks or intercoms that require each RFID card to be programmed individually. Only this fixed card ID appears in the device logs.
- **User Card ID**: Sends a unique card ID for each user that matches the existing RFID card number in the access control system. This enables seamless integration without issuing new physical cards.
- **Direct Input**: Manually specify the card ID to be sent. Useful for custom configurations where one ID must be used on multiple units.

6 Save your settings

- Keep the mobile device near the unit, tap **Save**, and confirm the selections.
- The update complete message appears.

Biometric Readers and Credentials
BioStar Air now supports biometric readers and biometric credentials to enhance secure access control. Register and configure compatible biometric devices, such as BioStation 3 (BS3) and BioEntry W3 (W3), to authenticate users via facial authentication. The feature supports both single and two factor authentication, enhancing flexibility and security.

- **Register readers**: Use the BioStar Air mobile app to register biometric readers.
- **Device setting**: Go to the BioStar Air Portal → **Device Management** → **Registered Devices** to configure the device facial authentication setting.
- **Face credential setting**: Go to the BioStar Air Portal → **User Management** → **Users** to add or edit users. Activate the facial credential in the **Credential Detail** section.

Before you start

- BioStar Air-compatible firmware must be installed for the biometric reader to operate normally.
- Up to two face templates can be used per user.
- For advanced configuration, refer to the BioEntry W3 or BioStation 3 user guide.
- Enroll at least two credentials to use two-factor authentication. For example, enroll both RF card and face credentials.

Step-by-step

1 Register biometric device

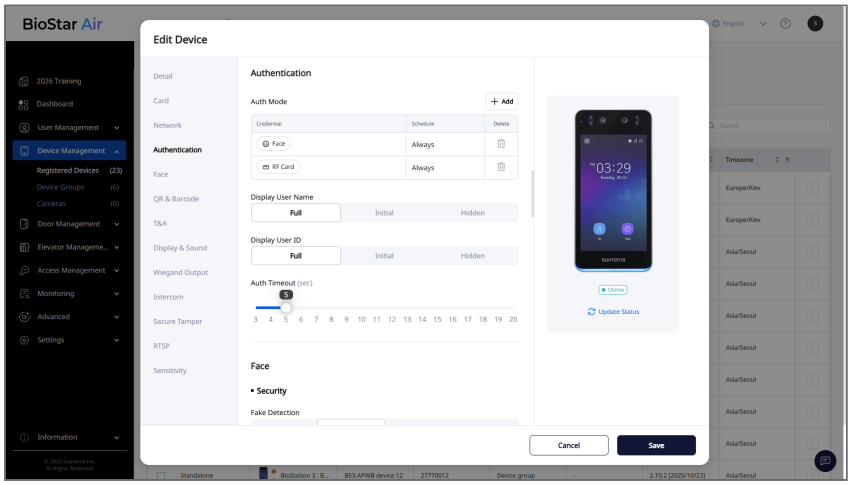
Verify that BioStar Air-compatible firmware is installed on the BioEntry W3 or BioStation 3. Models whose names end with `-AIR` already include the default firmware supplied by Suprema.

Launch the BioStar Air app on the mobile device and sign in with the administrator ID and password. Register the device in the same way as any other reader.

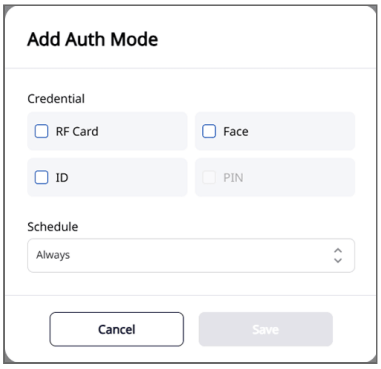
> **Info**
> For more information about registering devices, see Register and Delete Edge Devices.

2 Configure device

1. Log in to the BioStar Air Portal with an administrator account.
2. Click **Device Management** → **Registered Devices** in the left sidebar.
3. Click the biometric reader in the device list.
4. When the **Edit Device** window appears, go to the **Authentication** section.



5. Set **Auth Mode**.
   - **Single-factor**: Authenticate with either an RF card or facial authentication.
   - **Two-factor**: Delete either the RF card or facial authentication factor, then re-enroll both to enable two-factor authentication. Click **Add** and combine desired authentication methods.

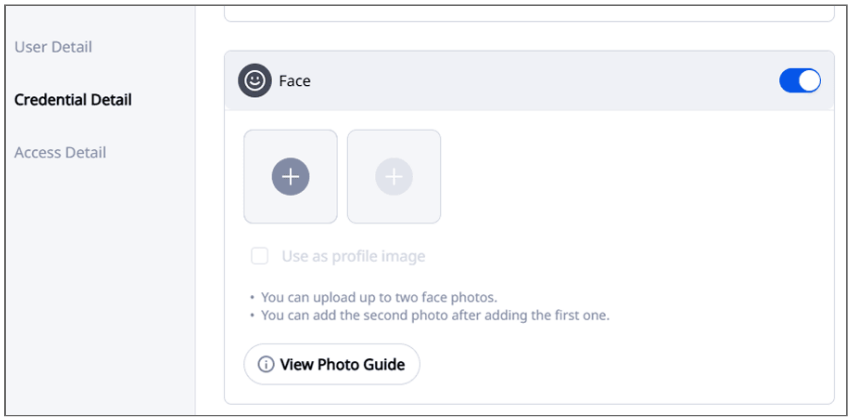


6. Set **Auth Timeout**. If the credential is not authenticated within the specified time, authentication will fail.
7. Configure the following options in the **Face** section.
   - **Fake Detection**
   - **Motion Sensor Sensitivity**
   - **Maximum Head Pose Angle**
   - **Detection Distance**
8. Configure additional options.
   - **Duplicate Check**
   - **Enrollment Time**
   - **Mask Detection**

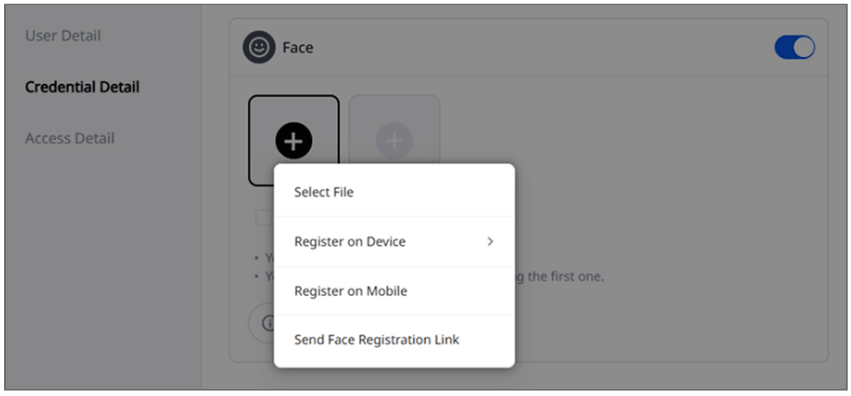
> **Info**
> For more information about the settings in the **Authentication** section, see Device and Panel Configuration Options.

3 Enroll user faces

1. Click **User Management** → **Users** in the left sidebar.
2. Open the window to add a new user or edit an existing user.
   - **Add a new user**: Click **Add User** in the upper right of the user list.
   - **Edit an existing user**: Select the user in the list, then click ✎.
3. From the user information window, go to the **Credential Detail** section and enable the **Face** credential.



4. Click + and add the facial template.



- **Select File**: Select a photo file stored locally
- **Register on Device**: Use the connected biometric reader (BioEntry W3 or BioStation 3)
- **Register on Mobile**: Scan the QR code sent to the user's mobile device and enroll the face from the mobile device
- **Send Face Registration Link**: Send a face enrollment link to the user's email or phone via SMS so they can enroll their face directly using their mobile device's camera.

> Only two face photos can be uploaded per user. Generally, one photo is sufficient.

5. Click **Save** to complete face enrollment.

> **Info**
> For more information about uploading user profile photos in bulk, see Add Users in Bulk.

Upgrade Firmware

Upgrade BioStar Air firmware to enhance device performance, strengthen security, and take advantage of new features. This simple process can be performed through the BioStar Air web portal or mobile app.

Before you start

- Devices must be **online** to update firmware. Check the device status in the **Product** column of the device list. A green dot (🟢) next to the device image indicates the device is online.

- During a firmware update, the device becomes **temporarily offline**, but it should reconnect within **3–5 minutes**.
- We recommend running firmware updates outside business hours, as devices become temporarily offline.
- Configure notifications to receive alerts when new firmware is updated. For more information on alert settings, see Set Up Alerts and Reports.

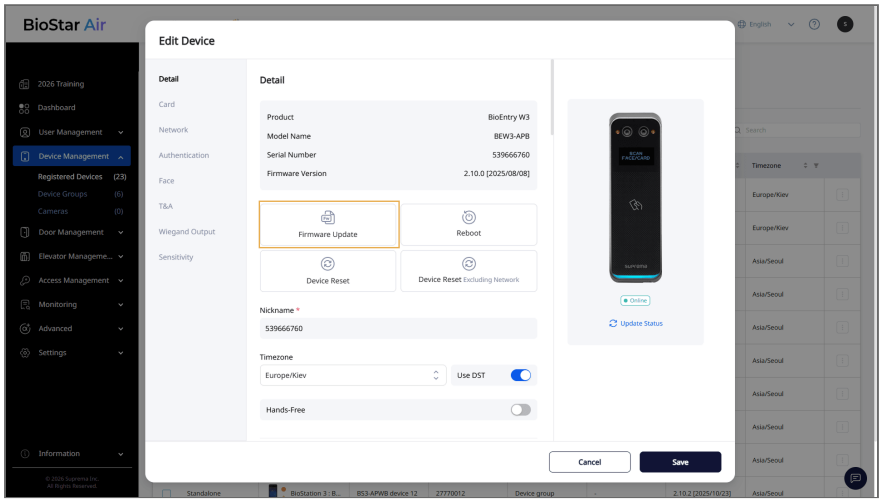
> **Info**
> For more information on device management, see Manage Registered Edge Devices.

Upgrade the firmware for an individual device

Web

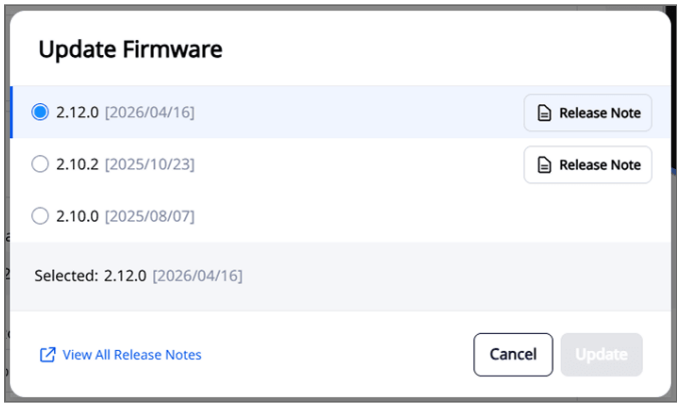
Log in to the BioStar Air portal and follow these steps to upgrade firmware.

1. Click **Device Management** → **Registered Devices** in the left sidebar.
2. Click the device in the device list that you want to upgrade.
3. When the **Edit Device** window appears, go to the **Detail** section.
4. Click **Update Firmware**.



The image above is an example screen and may differ from the actual screen.

5. When the **Update Firmware** window appears, select the latest firmware version and click **Update**.



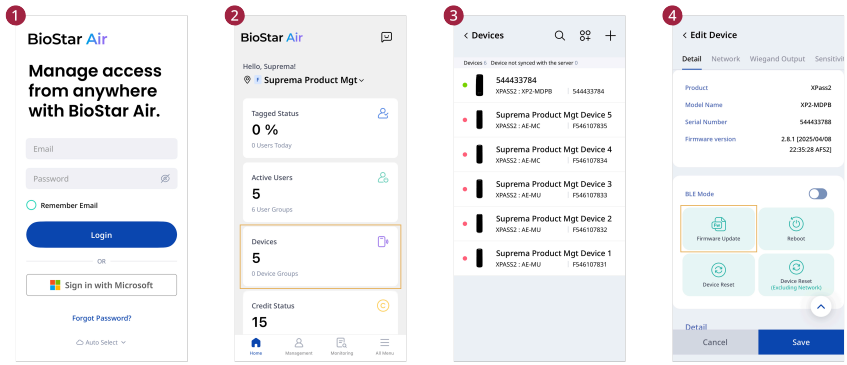
Wait for the device to restart automatically and come back online. A green dot (●) next to the device image indicates the

device is online.

> **Info**
>
> - Click **Release Note** to view the release notes for that firmware version.
> - Click **View All Release Notes** to view the firmware release notes for all devices.

Mobile

This guide explains how to upgrade the firmware using the mobile app.

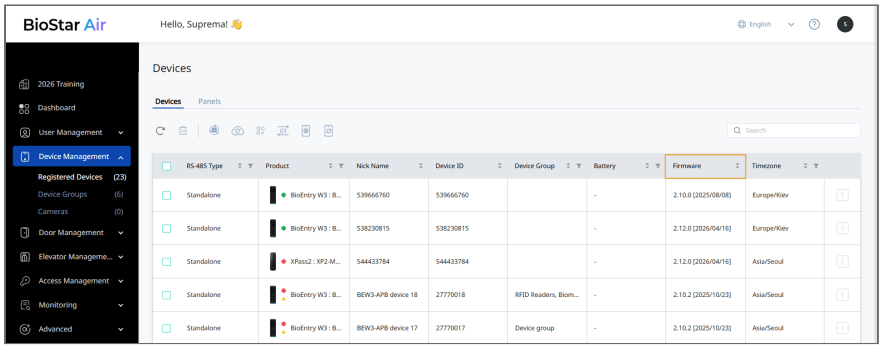


1. Open the BioStar Air app on your mobile device and log in.
2. Tap the **Devices** card.
3. Tap the device in the list whose firmware you want to upgrade.
4. Tap **Update Firmware**.
5. Select the latest firmware version and tap **OK**.
6. When the message window appears, review the information and tap **Confirm**.

> **Info**
>
> - Firmware upgrade may take 5–10 minutes, during which the device is unavailable.
> - Do not power off the device.
> - The device restarts automatically after the firmware upgrade is complete.

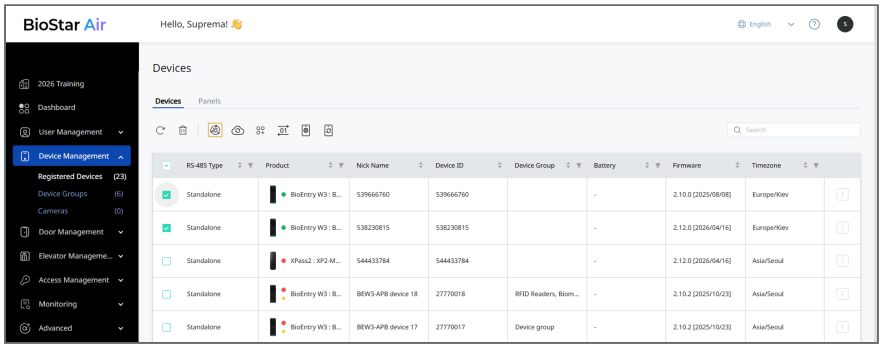
Upgrade firmware on multiple devices at once

1. Click **Device Management** → **Registered Devices** in the left sidebar.
2. Check the current version for each device in the **Firmware** column in the device list.
3. Click the arrow on the right side of the **Firmware** column to sort devices by firmware version.

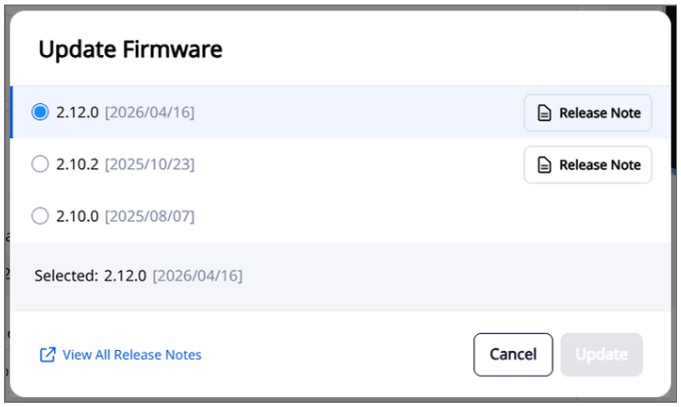


4. Select the checkbox to the left of each device you want to upgrade. You must select devices of the same type.

5. Click the button at the top of the device list.



6. When the **Update Firmware** window appears, select the latest firmware version and click **Update**.



Wait for the selected devices to restart automatically and come back online. A green dot (🟢) next to the device image indicates the device is online.

> **Info**
>
> - Firmware upgrade may take 5–10 minutes, during which the device is unavailable.
> - Do not power off the device.
> - The device restarts automatically after the firmware upgrade is complete.
> - Click **Release Note** to view the release notes for that firmware version.
> - Click **View All Release Notes** to view the firmware release notes for all devices.

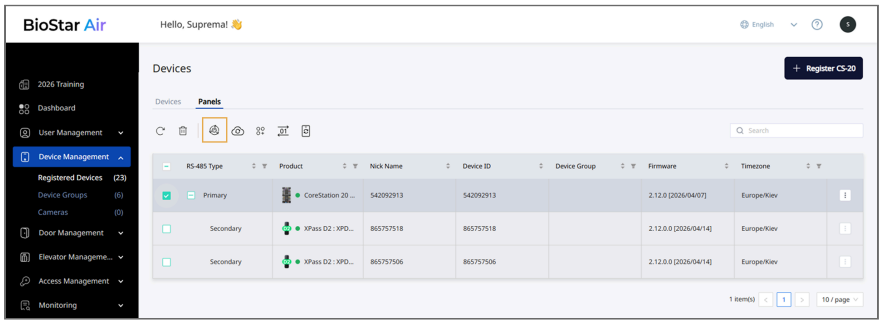
XPass D2 Firmware Upgrade

XPass D2 uses two firmware components.

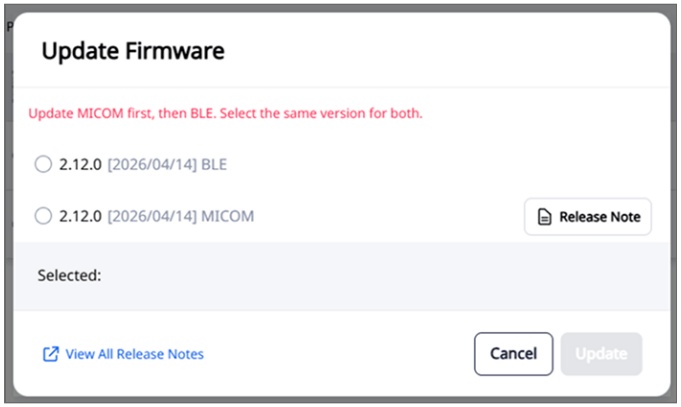
- **MICOM**: Includes updates for device operation, RS-485 communication, authentication processing, stability, and general bug fixes.
- **BLE**: Includes updates related to Bluetooth communication.

XPass D2 firmware must be updated in the order **MICOM** → **BLE**.

1. Click **Device Management** → **Registered Devices** in the left sidebar.
2. Click the **Panels** tab.
3. Click the XPass D2 checkbox. You can select only 1 device.



4. Click  at the top of the list.
5. When the **Update Firmware** window appears, select the **MICOM** firmware version.



6. Click **Update**.
7. Wait for the device to restart automatically and come back online. A green dot (🟢) next to the device image indicates the device is online.
8. Repeat the firmware upgrade process to select and update the **BLE** firmware version.

> **Caution**
>
> - The firmware version shown on screen does not allow you to individually verify the installation status of the **MICOM** and **BLE** components. Continue the firmware upgrade until the BLE upgrade completes.
> - The device comes back online after the **MICOM** update and again after the **BLE** update. Do not rely on the green online indicator (🟢) alone to confirm that the full upgrade is complete. Confirm both steps are complete.
> - Only one secondary device connected via CS-20 can have its firmware upgraded at a time.

Doors

Door management in BioStar Air is key to operating security and access control efficiently. Register doors, configure entry and exit devices, and manage large-scale access control with groups and schedules. Automated lock and unlock policies and authentication-based access control further enhance security.

Manage Registered Doors

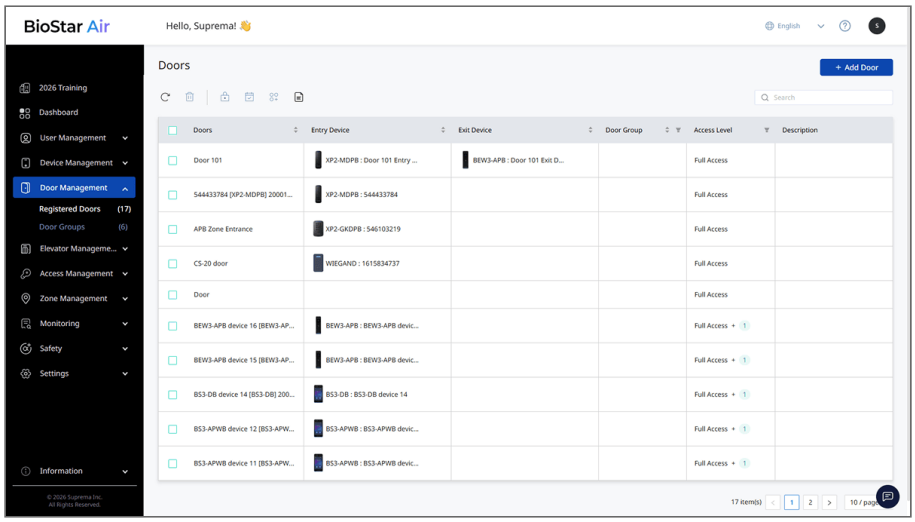
Assign access devices to registered doors, configure relays and access levels, and set access schedules. Systematically control access for security, fire evacuation, and time and attendance (T&A).

> **Tip**
> Watch the following video for a tutorial on registering and managing doors.

Explore the door list

The door list displays all doors registered in BioStar Air at a glance. View key information for each door, such as its name, assigned devices, group, and access levels. Click a door in the list to view details and modify settings.

Click **Door Management** → **Registered Doors** in the left sidebar to view registered doors.



Door information

The door list provides the following information.

- **Doors**: The name of the door. This is usually assigned automatically during device registration, but administrators can change the door name.
- **Entry Device**: Device that authenticates users entering the door.
- **Exit Device**: Device that authenticates users exiting the door.
- **Door Group**: Name of the group assigned to the door.
- **Access Level**: Access level the system assigns to the door. For more information on assigning access levels, see Batch assign access levels.
- **Description**: Description of the door.

- **Camera**: Displays camera information linked to the door. **Camera** column appears only after you enable the **Video Management** feature at **Settings** → **Site** → **Additional Features**.

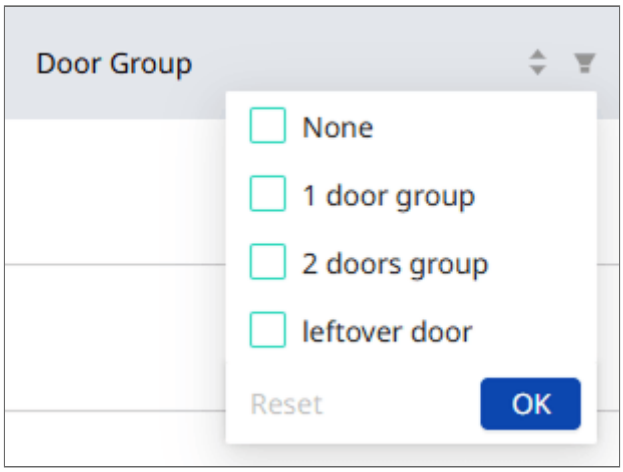
Additional features

When one or more doors are selected in the list, administrators can manage them using the following tools.

- : Refresh the door list.
- : Remove the selected doors from the list.
- : Set access levels for the selected doors. For more information, see Batch assign access levels.
- : Set a schedule for door open and locked states. For more information on managing door schedules, see Manage Door Schedules.
- : Group the selected doors. For more information on managing door groups, see Manage Door Group.
- : Generate door reports. For more information on generating door reports, see Generate door reports.

Filter

Filter the door list by door group. Click the **Door Group** column's button and select the desired group. Click **OK** to show only the doors in the selected group.



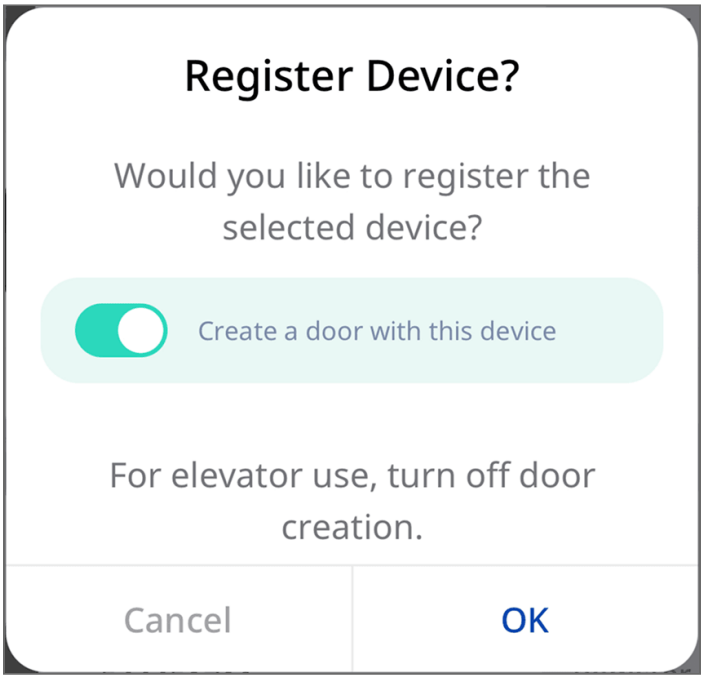
Info

To reset the applied filters, click and select **Reset**.

Add doors

Add with a device

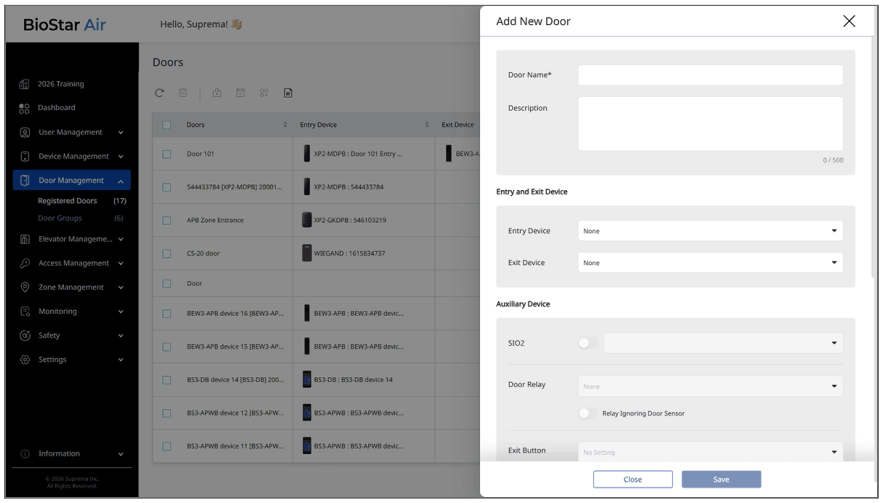
In the final step of device registration in the mobile app, select the **Create a door with this device** option to create a door. For more information on how to register a device with the mobile app, see Register and Delete Edge Devices.



Add from the web portal

Follow the steps below to add a new door in the BioStar Air portal.

1. Click **Door Management** → **Registered Doors** in the left sidebar.
2. Click **Add New Door** at the top right of the screen.
3. When the **Add New Door** panel appears, enter **Door Name**.



4. Select **Entry Device** and **Exit Device**.
5. Click **Save** to save and add the door settings.

Rules for assigning devices to doors

- Each device can be assigned to **one door** only.
- If a device is already registered but does not appear in the available device list, check whether it is assigned to another door. If it is assigned to another door, remove it from that door and try again.
- **A device cannot be assigned to both a door and an elevator at the same time.**

Doors that use primary/secondary devices

- The door is controlled by a primary device (XPass 2 or CoreStation 20).
- An XPass 2 configured as a primary can be assigned to only one door, regardless of how many secondary devices or modules are assigned.
- An XPass 2 configured as a primary can have up to 31 slave devices assigned, and it can add a new door whose relay is controlled by a slave Secure I/O 2 (SIO2).
- Doors that use a CoreStation 20 (CS-20) together with a Secure I/O 2 (SIO2) cannot be created.

Door configuration limitations

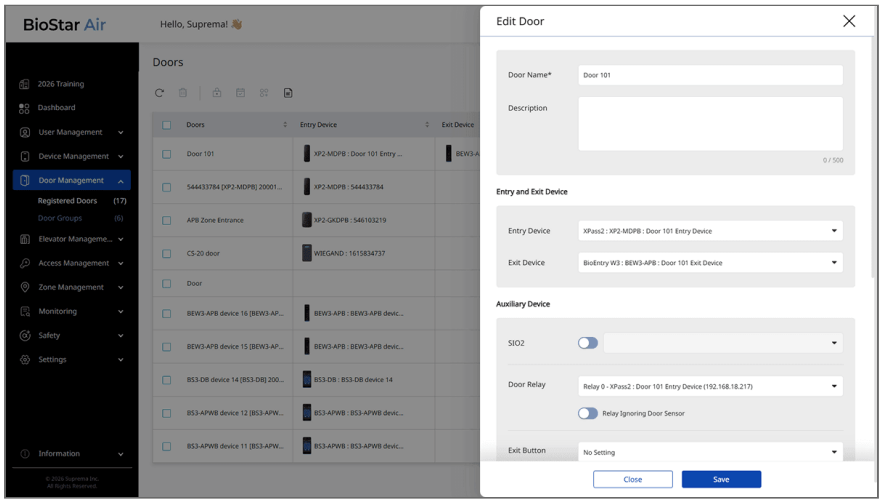
The following limitations apply to door configuration.

- 1 XPass D2 + SIO2 (relay owned by SIO2)
- 1 XPass 2 + XPass D2 (relay owned by XPass 2)
- 2 XPass D2 (relay owned by XPass 2)
- 1 or 2 OSDP/Wiegand devices (relay owned by CS-20)
- Only one SIO2 is allowed per door (relay for I/O): it must be wired to the same XPass 2 as the XPass D2

Edit doors

Follow these steps to edit door details and settings.

1. Click **Door Management** → **Registered Doors** in the left sidebar.
2. Click the door you want to edit in the list. Or select the checkbox to the left of the door and click in the top left sidebar.
3. When the **Edit Door** panel appears, edit **Door Name** and **Description**.

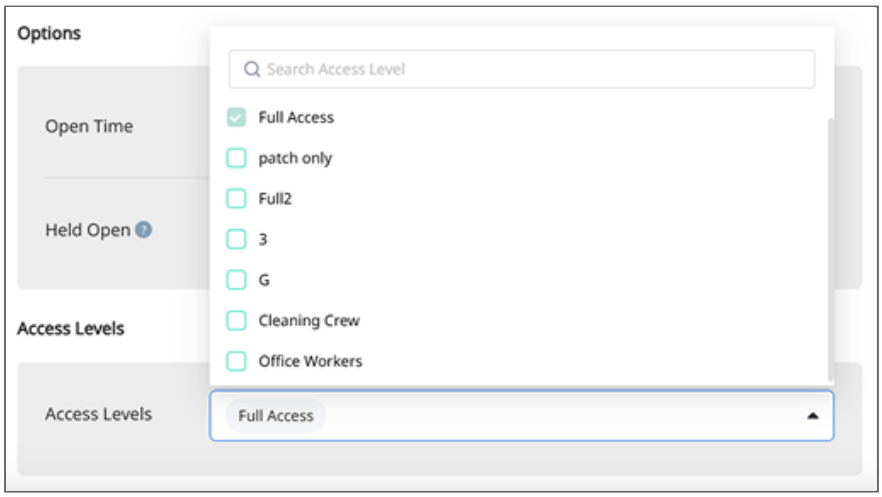


4. Select the device for door entry authentication from the **Entry and Exit Device** section.
   - **Entry Device**: Select the device that authenticates users entering the door.
   - **Exit Device**: Select the device that authenticates users exiting the door.
5. Configure the relay device in the **Auxiliary Device** section.

- **Camera**: Connect CCTV cameras for event logs.
- **Door Relay**: Select the relay device that controls the door lock.
- **Relay Ignoring Door Sensor**: Set the relay to ignore the door sensor.

> To use the camera, enable the **Video Management** feature under **Settings** → **Site** → **Additional Features**.

6. Configure additional settings.
   - If installed, select the port to set to **Exit Button**.
   - Select the port to set to **Door Sensor**.
   - Set how long the door remains open in **Open Time**. (Default: 3 seconds)
7. In the **Access Level** section, click the check boxes for the access levels to assign to or remove from the door.



8. Click **Save** to apply the changes.

> **Info**
>
> - For security, the relay must always connect to the device on the secure side of the door. Use the exit device's relay or an SIO2 module.
> - When configured for a direct cloud connection, both the entry and exit devices require separate network cables.
> - When using a primary-secondary configuration, the primary device (usually the exit device) needs a network connection and the secondary device connects to the primary via RS-485.
> - For more information on configuring the SIO2 secure module, see Configure SIO2 Secure Module.

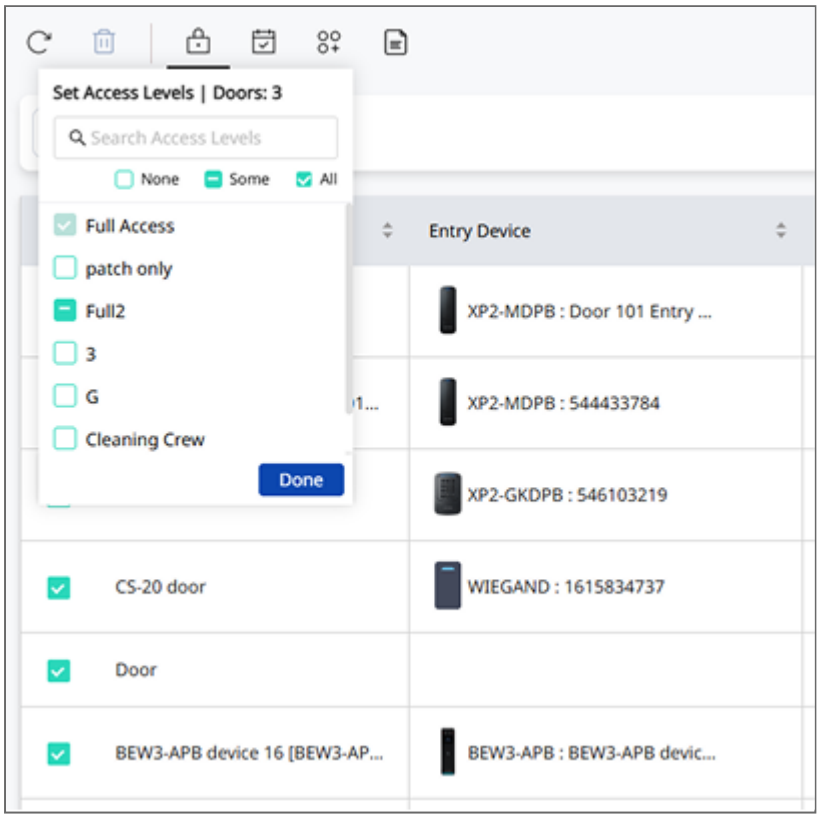
Batch assign access levels

Assign or unassign an access level for multiple doors at once, instead of editing doors one by one.

1. Click **Door Management** → **Registered Doors** in the left sidebar.
2. Select the check box for at least one door to set access levels.

3. Click at the top of the door list.

4. When the **Set Access Levels** pop-up menu appears, click the check boxes for the access levels to apply to the selected doors.



Search for the access level in the search field, if needed.

- **None**: The system removes the access level from the selected doors.
- **Some**: Only certain selected doors have the access level assigned.
- **All**: All selected doors have the access level assigned.

5. To finish, click **Done**.

> **Info**
>
> - If one or more doors are offline, the system applies the changes when the device reconnects.
> - The **Full Access** access level is managed automatically by the system, so it cannot be changed.
> - Errors on certain doors may prevent the system from applying access levels. A dialog shows doors where the access level change failed. To try again, click **Retry failed**.

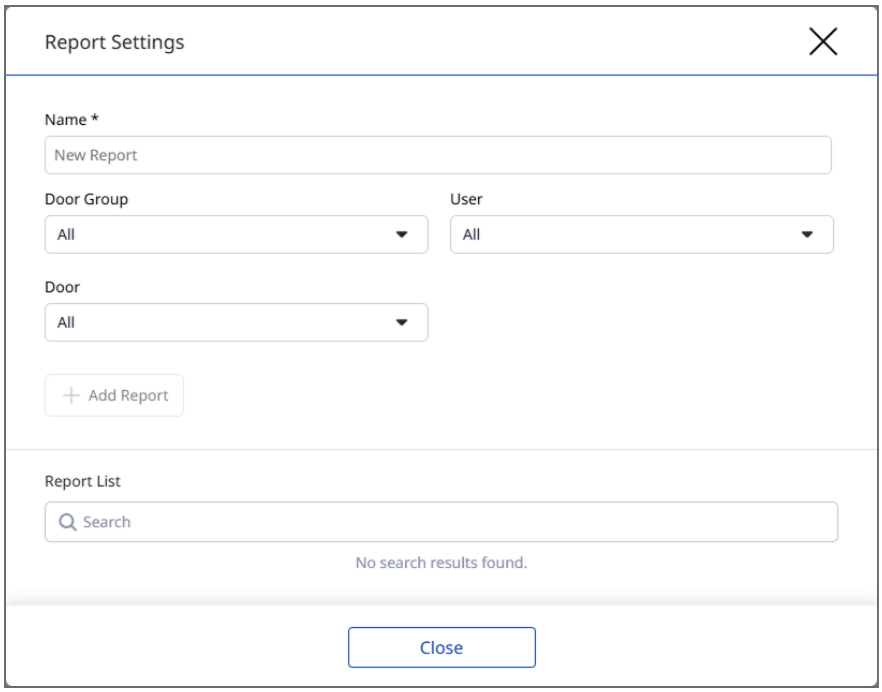
Generate door reports

Generate door reports and send them to the administrator's email. A door report provides information about users who accessed through the door.

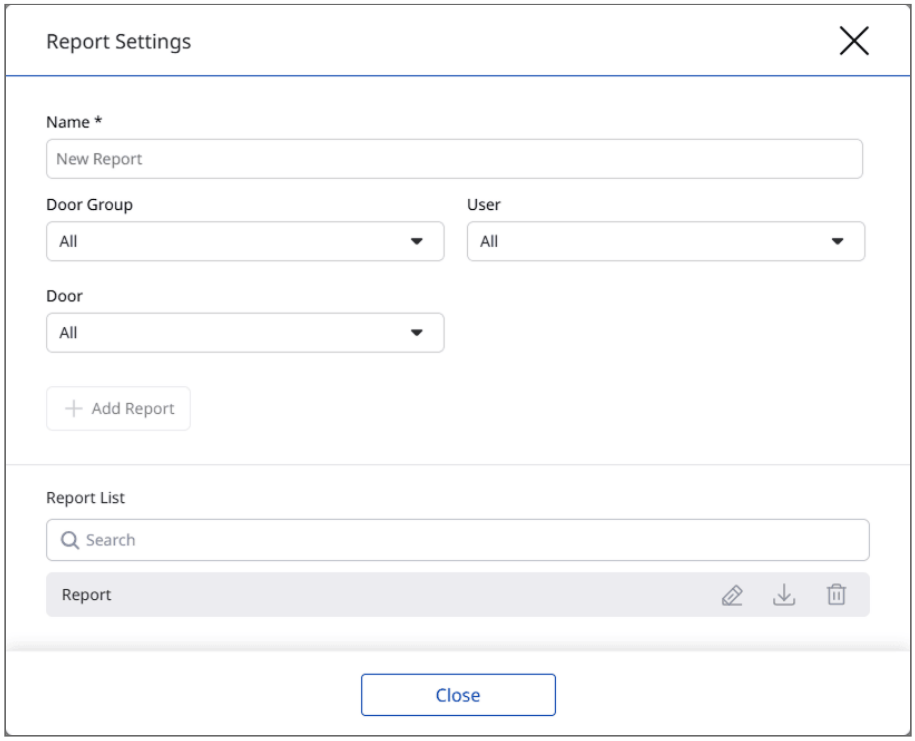
1. Click **Door Management** → **Registered Doors** in the left sidebar.

2. Click at the top of the door list.

3. When the **Report Settings** window appears, enter a report name.



4. Select the items to include in the report.
5. Click **Add Report** to save the report.
6. A **Report List** is created and a download link is sent to the administrator's email.



Info

In **Report List**, search for, edit, download, or delete generated reports.

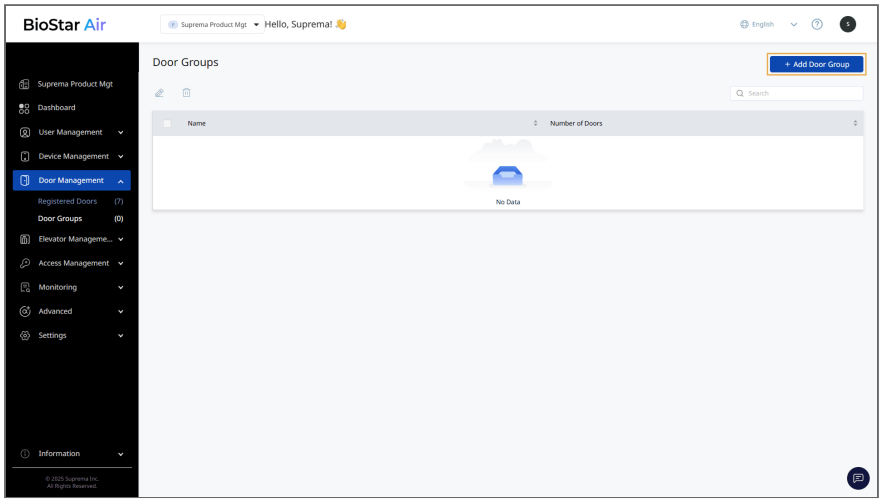
Manage Door Group

By grouping doors, you can manage access control policies more efficiently. Apply consistent security policies across multiple doors by setting access levels and permissions for groups at once.

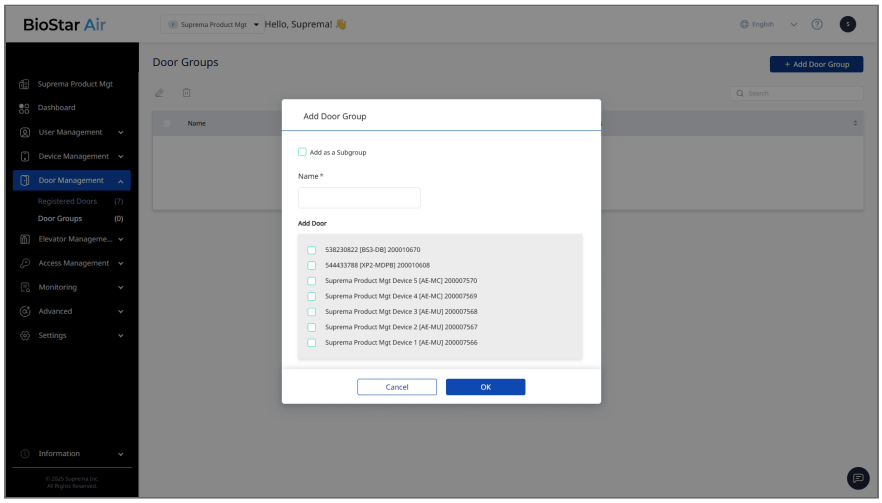
> **Info**
>
> - For more information on managing registered doors, see Manage Registered Doors.
> - For more information about access levels, see Manage Access Levels.

Add door group

1. Click **Door Management** → **Door Groups** in the left sidebar.
2. Click **Add Door Group** at the top right of the screen.



3. When the **Add Door Group** window appears, enter the door group name.

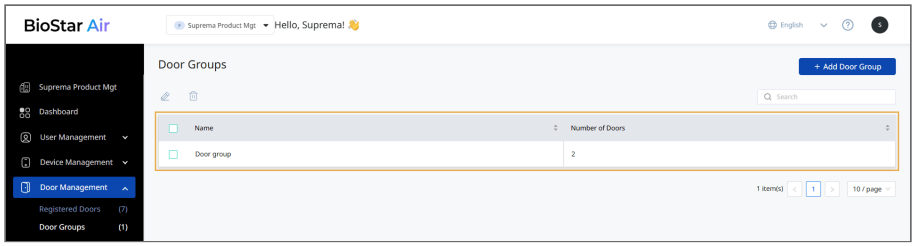


> Click **Add as a Subgroup** and select the parent group to add the device group as a subgroup of a specific group.

4. In **Add Door**, select the doors to include in the group.

5. Click **OK** to save the door group.

The door group list shows the newly added group and the number of doors it contains. Click a door group to view the doors it contains.

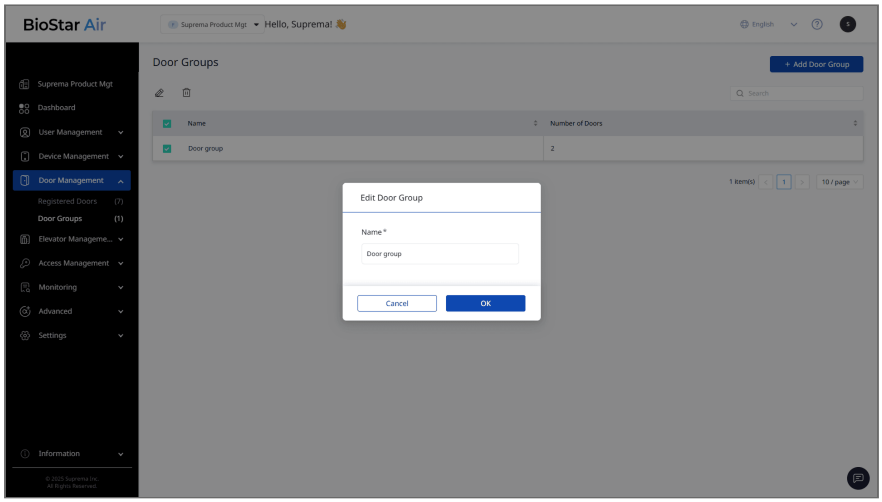


Info

- Doors added to a subgroup are not automatically included in the parent group.
- Add an empty parent group without devices or doors.

Rename door group

1. Click **Door Management** → **Door Groups** in the left sidebar.
2. Check the checkbox for the door group you wish to rename in the list.
3. Click ✎ at the top of the door group list.
4. When the **Edit Door Group** window appears, enter the new group name.



5. Click **OK** to save the changed group name.

Delete door group

1. Click **Door Management** → **Door Groups** in the left sidebar.
2. Check the checkbox for the door group you wish to delete in the list.
3. Click 🗑 at the top of the door group list.
4. When a warning message appears, click **Yes**.

The selected door group is removed from the list. Its subgroups are also deleted. The access doors will not be deleted even if the group is deleted.

Manage Door Schedules

You can set door schedules to automatically lock and unlock doors based on time periods. Configure lock and unlock times, and utilize advanced options such as **open after first authentication** to set up secure and controlled access.

> **Info**
>
> - Schedules apply only to doors and devices that are connected to the internet.
> - Holiday groups ignore unlock schedules unless they are configured separately.
> - Keep at least one administrator with unrestricted access for emergencies.

When Do You Need Schedules

Door schedules are optional. Most sites operate effectively with basic access control alone. When an authorized user presents a valid credential, the door unlocks automatically—no additional schedule configuration required.

Configure schedules only in the following situations:

- When you need to allow unrestricted access during specific time periods
- When you need to block all users from entering during specific time periods
- When you need to apply different access policies for different times

To avoid confusion between **Unlock Schedule** and **Lock Schedule** in BioStar Air, understand how each schedule works and when to use it.

Unlock Schedule vs Lock Schedule

Category	Unlock schedule	Lock schedule
Door state during schedule	Always unlocked	Always locked
Authentication required	Not required, anyone can freely access	Credentials cannot unlock the door
Manual unlock	Possible	Only site administrator can unlock
Relay operation	Continuously triggered	Does not trigger

> **Info**
>
> Site administrator refers to designated administrators in the BioStar Air Admin portal or mobile app.

Unlock schedule

During the scheduled period, the door remains unlocked and the relay stays continuously triggered. No authentication is required for anyone to enter freely during this time.

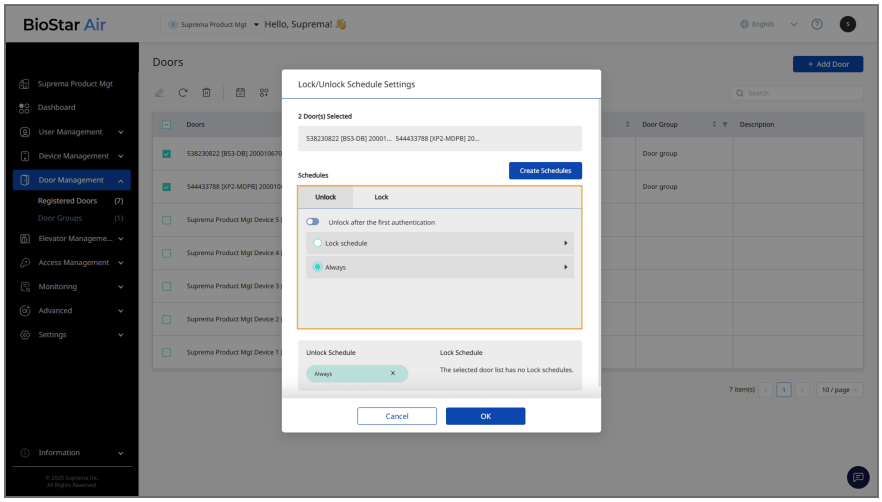
Typical use cases

- Main entrance doors in public areas
- Shared amenities in residential communities
- Office lobby doors during business hours

Configure unlock schedules

Configure an unlock schedule as instructed below.

1. Click **Door Management** → **Registered Doors** in the left sidebar.
2. In the list, click the checkbox for the door to configure its unlock schedule.
3. Click ☑ at the top of the door list.
4. When the **Lock/Unlock Schedule Settings** window appears, select a predefined schedule or create a new one in the **Unlock** tab.



5. Click **OK** to apply the unlock schedule.

> **Info**
>
> - When **Unlock after the first authentication** is enabled, the door stays unlocked according to the selected schedule after the first user authenticates. This option can be useful in the following situations.
>   - Retail stores that open only after staff arrive
>   - Offices where the first employee arriving unlocks the building for others
>   - Membership facilities that require staff to initiate access before members can enter
> - For more information on registering schedules, refer to Register a new schedule.

Lock schedule

During the scheduled period, the door remains locked and the relay does not trigger. Even if a valid credential is presented, the door cannot be unlocked through authentication. Only a site administrator can manually unlock the door through the BioStar Air Admin portal or mobile app.

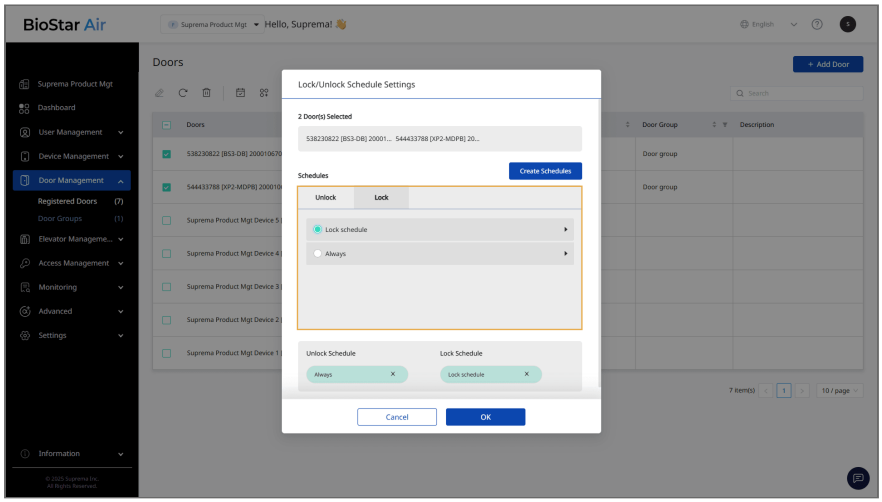
Typical use cases

- Areas that must be strictly closed after certain hours
- Facilities such as pools, gyms, or other restricted areas

Configure lock schedules

Configure a lock schedule as instructed below.

1. Click **Door Management** → **Registered Doors** in the left sidebar.
2. In the list, click the checkbox for the door to configure its lock schedule.
3. Click ☑ at the top of the door list.
4. When the **Lock/Unlock Schedule Settings** window appears, select a predefined schedule or create a new one in the **Lock** tab.



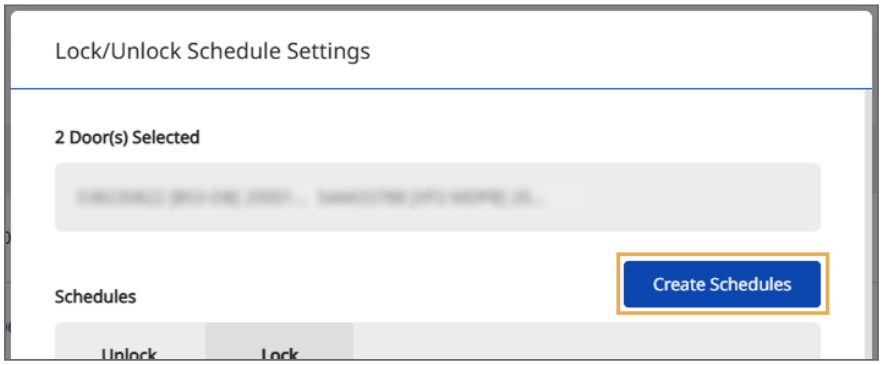
5. Click **OK** to apply the lock schedule.

> **Info**
>
> - Because a lock schedule overrides standard access rights, users cannot set the door to unlocked during the lock period.
> - For more information on registering new schedules, refer to Register a new schedule.

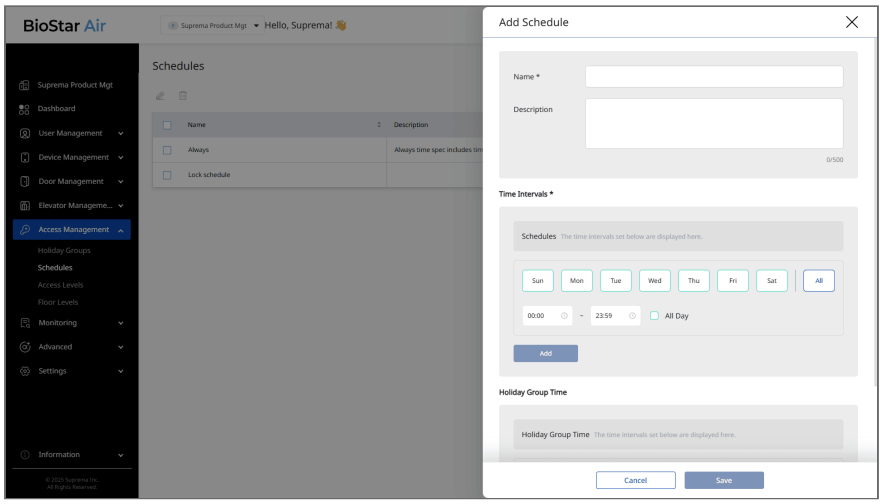
Register a new schedule

Follow the steps below to register a new schedule.

1. In the **Lock/Unlock Schedule Settings** window, click **Create Schedules**.



2. On the Add Schedule screen, enter **Name** and **Description** (optional).



3. In the **Time Intervals *** section, select the days and times when the door should be open without authentication, then click **Add**.

4. Click **Save** to save the schedule.

After registering a new schedule, return to **Door Management** → **Registered Doors** and configure the door schedule.

Elevators

BioStar Air supports elevator access control using Suprema's OM-120 module. Using the OM-120 module, administrators can integrate with readers compatible with BioStar Air to control floor access. A daisy chain of OM-120 devices supports up to 144 floors.

> **Tip**
> Watch the following video guide on managing elevators.

Manage Elevators

To configure elevator access control, first connect the OM-120 module to the access control device. Then set each floor's name and relay number, and restrict access times per floor using schedules to enhance security.

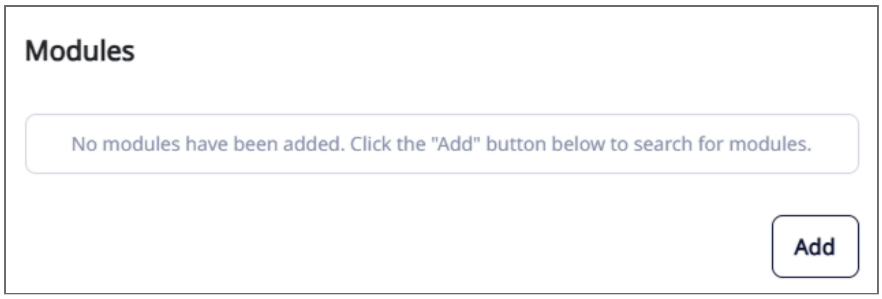
Requirements

Meet the following requirements to enable the elevator access control feature.

- Suprema OM-120 module: Each module supports up to 12 floors. Connecting up to 12 OM-120 modules to a single access control device supports up to 144 floors.
- A device compatible with BioStar Air that can connect to the OM-120 is required.
- Proper wiring to the elevator control panel is required. For wiring details, contact the elevator manufacturer.
- Floor access schedules take precedence, and holiday settings can override the normal access rules.

Connect devices and modules

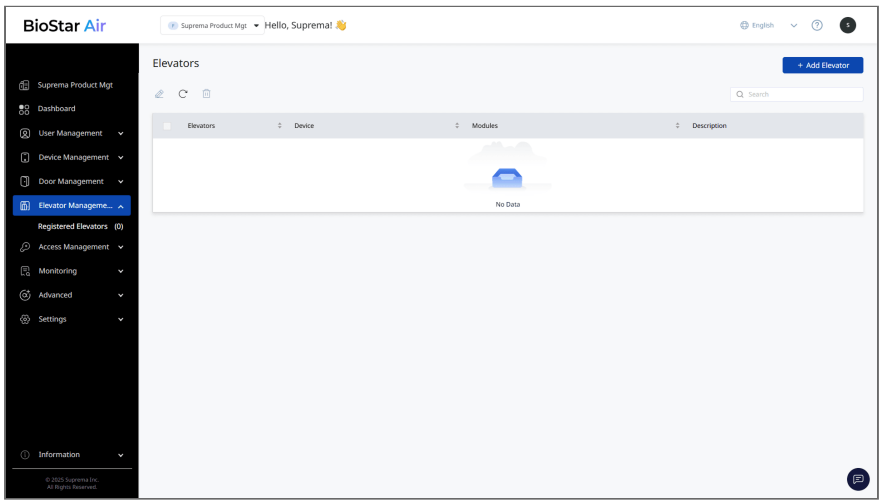
1. Click **Device Management** → **Registered Devices** in the left sidebar.
2. Click the access control device with an OM-120 module from the device list.
3. In the **Modules** section, click **Add**.



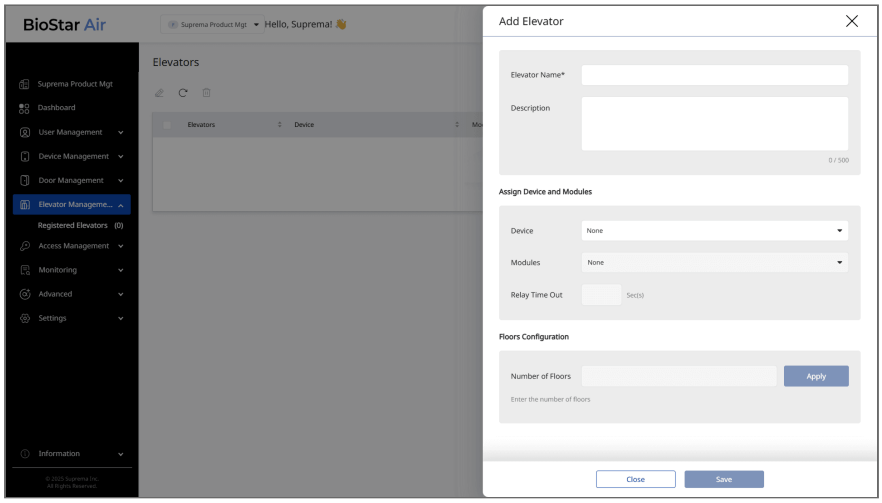
4. Select the OM-120 module connected to the device, then click **Save**.

Register elevators

1. Click **Elevator Management** → **Registered Elevators** in the left sidebar.
2. Click **Add Elevator** at the top right of the screen.



3. When the **Add Elevator** panel appears, enter **Elevator Name** and **Description** (optional).



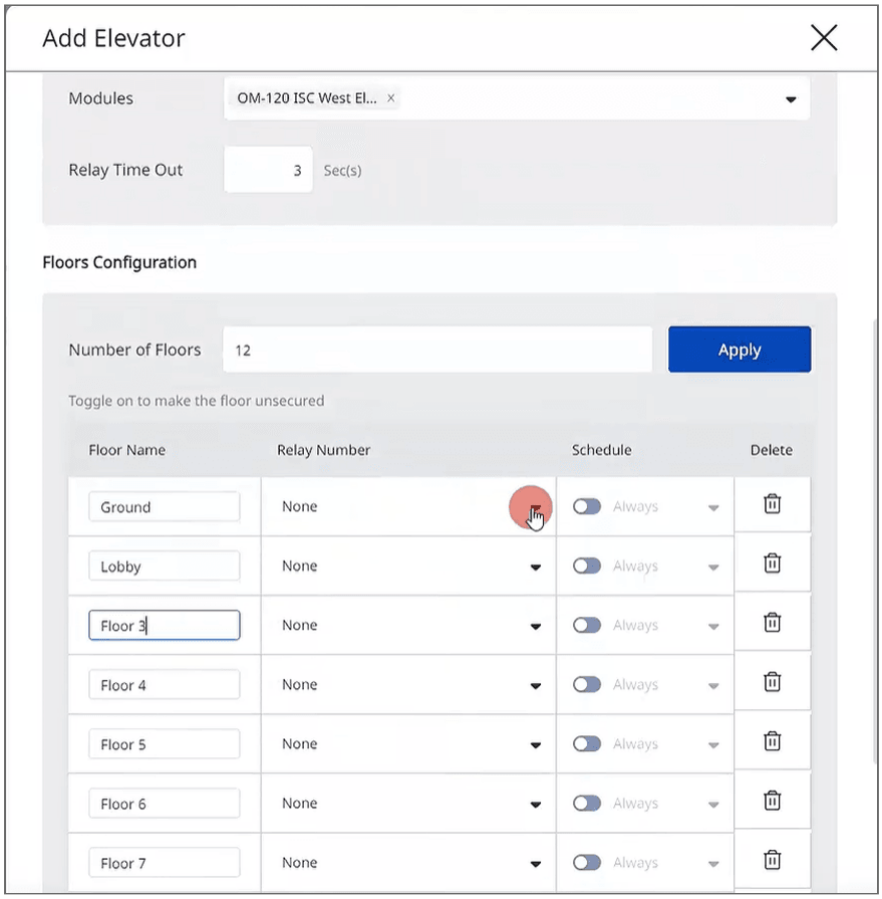
4. In the **Assign Device and Modules** section, select the device and module for access authentication.

   - **Device**: Select the device for access authentication.

     > **Caution**
     >
     > If the device doesn't appear in the list, make sure it has been assigned to a door. A device cannot be assigned to both a door and an elevator at the same time.

   - **Modules**: Select the OM-120 module that will control the elevator button relay.
   - **Relay Time Out**: Set the time for which the floor button remains active after authentication is complete. After this time, the relay will not signal the floor button.

5. In the **Floors Configuration** section, enter the number of floors to control and click **Apply**.
6. Set each floor's name, relay number, and schedule.



The image above is an example screen and may differ from the actual screen.

- **Floor Name**: Enter the floor name. Use easily identifiable names such as 1F, Lobby, or Conference Floor.
- **Relay Number**: Select the relay output that corresponds to each floor button on the elevator control panel.
- **Schedule**: Set the schedule for accessing each floor. For example, restrict access to the maintenance floor outside working hours.

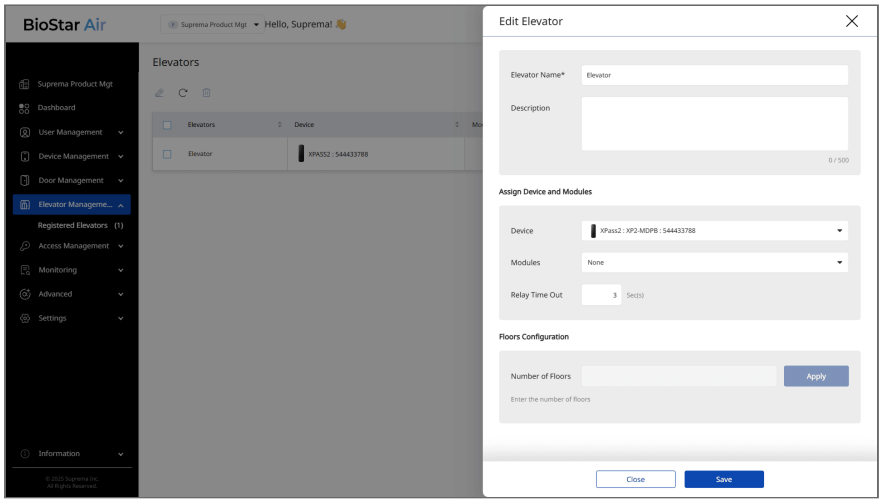
7. Click **Save** to save and register the elevator settings.

> **Info**
>
> - Each OM-120 module supports up to 12 floors. Connect multiple OM-120 modules in a daisy chain to expand up to 144 floors.
> - In the **Floors Configuration** section, click to delete a floor.
> - For more information on registering schedules, see Manage Schedules.

Edit elevators

Follow these steps to change the details or settings of a registered elevator.

1. Click **Elevator Management** → **Registered Elevators** in the left sidebar.
2. In the list, click the elevator to edit. Alternatively, select the elevator's checkbox and click at the top of the list.
3. When the **Edit Elevator** panel appears, change the necessary information or modify the settings.



4. Click **Save** to save the changes.

Delete elevators

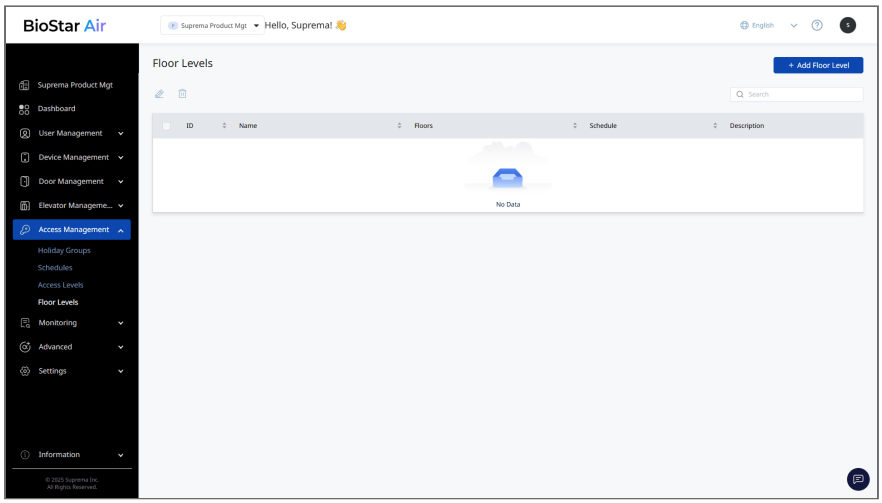
Follow these steps to delete a registered elevator.

1. Click **Elevator Management** → **Registered Elevators** in the left sidebar.
2. Select the checkbox of the elevator to delete in the list. Select one or more elevators.
3. Click 🗑 at the top of the list.
4. When a warning message appears, click **Yes**.

Set floor access permissions

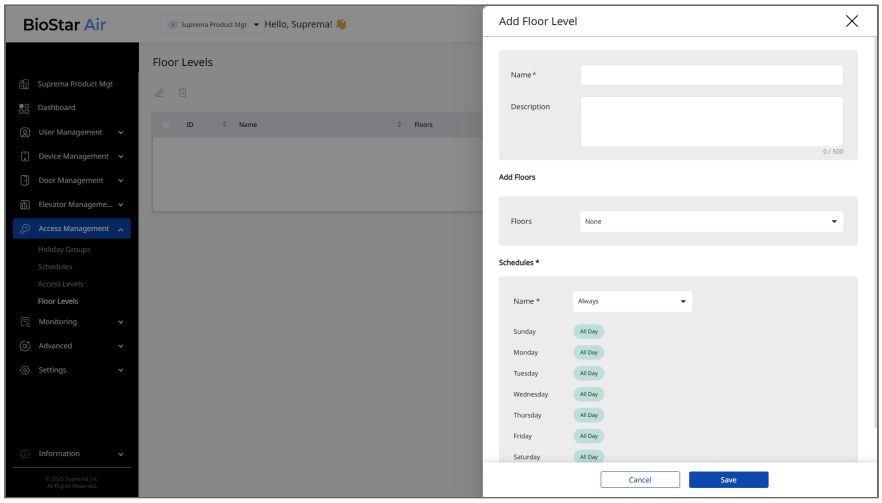
Register an elevator and define floor levels to restrict the floors that users and groups can access. For each floor level, set access schedules (e.g., during business hours) and holiday policies to manage security and accessibility.

1. Click **Access Management** → **Floor Levels** in the left sidebar.
2. Click **Add Floor Level** at the top right of the screen.



3. When the **Add Floor Level** panel appears, enter **Name** and (optional) **Description**.

> *For example, Security team, Cleaning staff*



4. In the **Add Floors** section, select the floors to apply the floor level to.
5. In the **Schedules** section, set the access schedule.

   > *For example, allow cleaning staff to access only outside working hours.*

6. If necessary, add **Holiday Groups** to restrict access on specific dates.
7. Click **Save** to add the floor level.

> **Info**
> For more information on adding, editing, or deleting floor levels, see Manage Floor Levels.

Access Permissions

Managing access authority is central to a security system. Combine holiday groups, schedules, access levels, and floor levels to finely control when and where users access.

> **Tip**
> Watch the following video guide on managing access authority.

Manage Holiday Groups

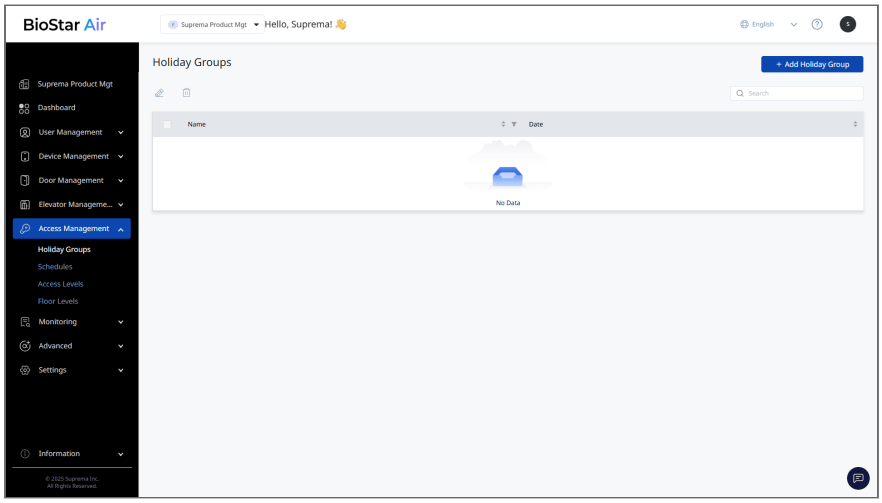
In BioStar Air, a holiday group is used to adjust access rules for specific dates or periods. By configuring a holiday group, administrators can restrict or change access permissions on public holidays or special days. This approach maintains security while providing flexible access control.

> **Tip**
> Watch the following video for a guide on access control management.

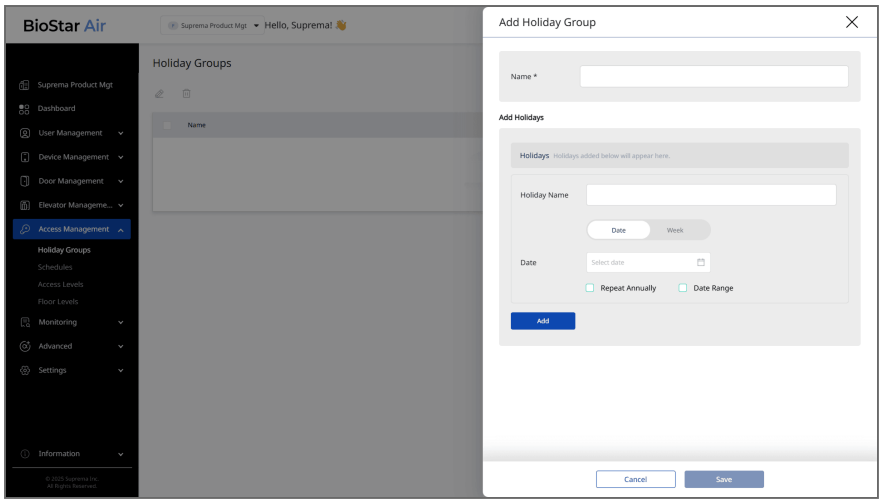
Add a holiday group

A holiday group defines holidays that recur annually and holidays within specific periods, and is used to restrict or change access permissions during those periods.

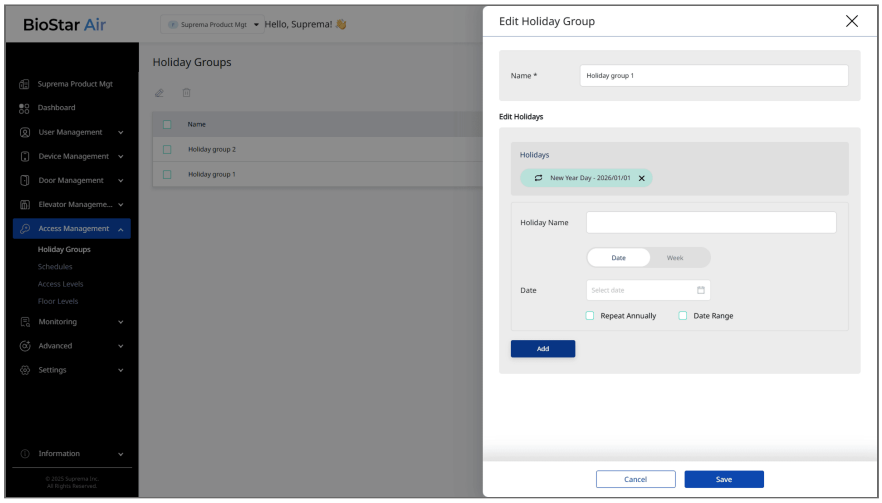
1. Click **Access Management** → **Holiday Groups** in the left sidebar.
2. Click **Add Holiday Group** at the top right of the screen.



3. Enter the group name when the **Add Holiday Group** panel appears.



4. In the **Add Holidays** section, specify the holiday name and date, and click **Add**.
   - Set the name and date, and select the **Repeat Annually** option to add a fixed-date public holiday.
   - Set the name and date, and select the **Date Range** option for holidays that recur annually but span a specific period.
5. Add other holidays in the same way.

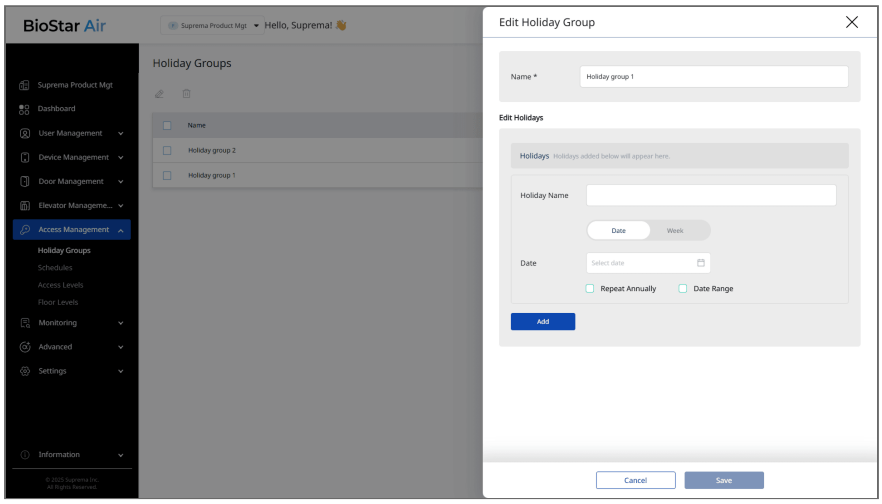


6. Click **Save** to save the holiday group settings.

> **Info**
>
> - Holiday groups take precedence over schedules. Grant unrestricted access to users who always need entry.
> - Only one holiday group can be applied to a single door.

Edit a holiday group

1. Click **Access Management** → **Holiday Groups** in the left sidebar.
2. Click the holiday group you want to edit from the list. Alternatively, select the holiday group's checkbox, and then click at the top of the list.
3. When the **Edit Holiday Group** panel appears, edit the necessary items.



4. Click **Save** to save the changes.

Delete a holiday group

1. Click **Access Management** → **Holiday Groups** in the left sidebar.
2. Select the holiday group's checkbox in the list. Multiple holiday groups can be selected.

3. Click at the top of the list.

4. When a warning message appears, click **Yes**.

Manage Schedules

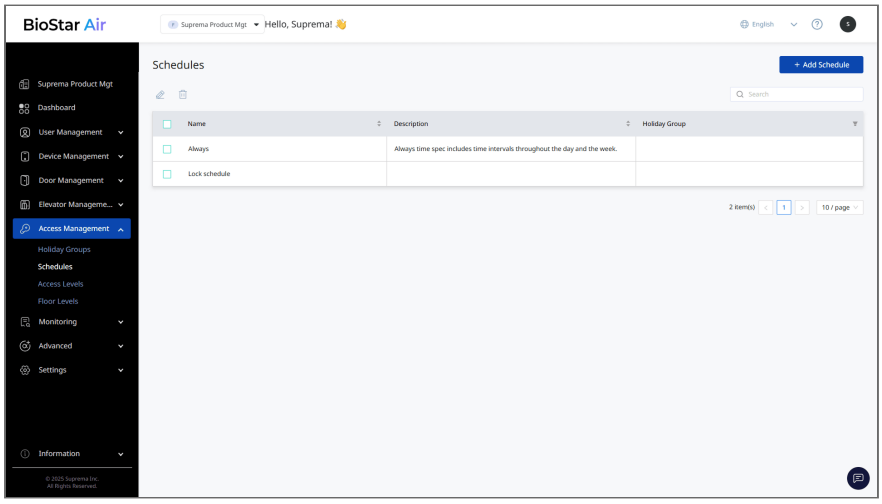
Create schedules to allow or restrict access to doors or elevators on specific days and time periods. Use with holiday groups to fine-tune access rules.

> **Info**
>
> - Holiday groups take precedence over schedules. Grant unrestricted access to users who always need entry.
> - For more information about holiday group settings, see Manage Holiday Groups.
> - For more information about applying schedules to doors, see Manage Door Schedules.
> - For more information about configuring schedules to control access to each elevator floor, see Elevators.

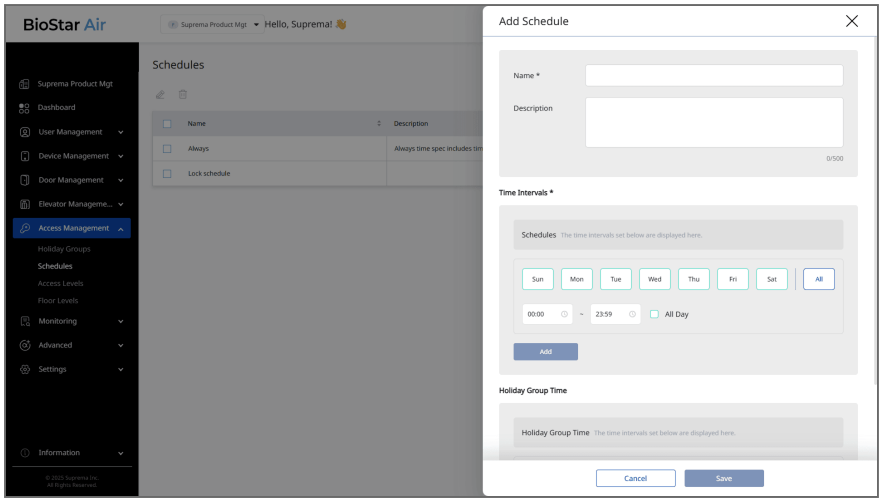
Add schedule

1. Click **Access Management** → **Schedules** in the left sidebar.

2. Click **Add Schedule** at the top right of the screen.



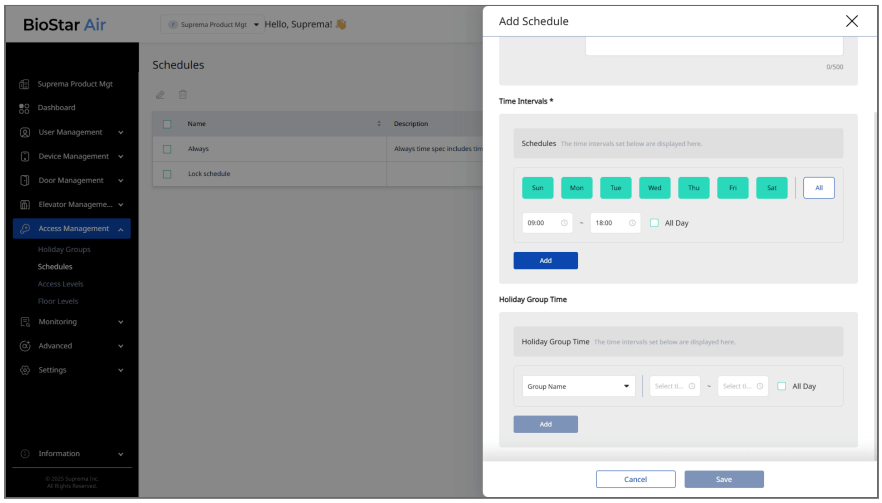
3. When the **Add Schedule** panel appears, enter **Name** and **Description** (optional).



4. In the **Time Intervals *** section, select the days and times.

> *Select Monday to Friday and 9:00 AM to 6:00 PM to set working hours. Select Saturday and Sunday, or 6:00 PM to 9:00 AM daily, to set a schedule for non-working hours.*

5. Click **Add** to apply the selected schedule.
6. In the **Holiday Group Time** section, select the holiday group to apply to the schedule and set the times.



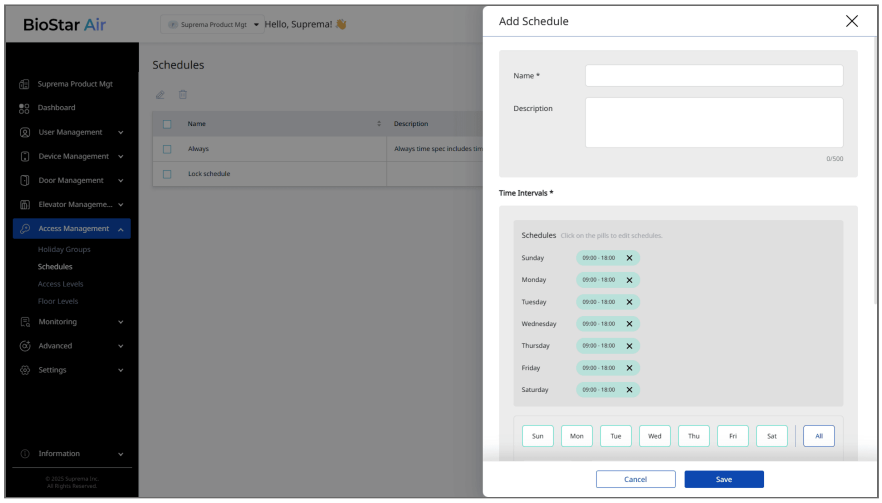
7. Click **Add** to apply the holiday group.
8. Click **Save** to add the schedule.

Info

- Add open schedules to allow access and locked schedules to restrict access, and apply them to doors. For more information about applying schedules to doors, see Manage Door Schedules.
- Only one holiday group can be assigned to a schedule.
- For more information about configuring schedules to control access to each elevator floor, see Elevators.

Edit schedule

1. Click **Access Management** → **Schedules** in the left sidebar.
2. Click the schedule to edit in the list. Alternatively, select the schedule's checkbox and click ✎ at the top of the list.
3. When the **Edit Schedule** panel appears, update the required information or modify the schedule.



4. Click **Save** to save the changes.

Delete schedule

1. Click **Access Management** → **Schedules** in the left sidebar.
2. Select the checkbox of the schedule to delete in the list. Select one or more schedules.
3. Click at the top of the list.
4. When a warning message appears, click **Yes**.

> **Info**
> Deleting a schedule removes it from all related sections. For example, if a schedule applied to a door or elevator is deleted, the schedule is no longer applied to that door or elevator.

Manage Access Levels

Use access levels to precisely control user access. Access levels define who can access where and when. An access level consists of the following elements.

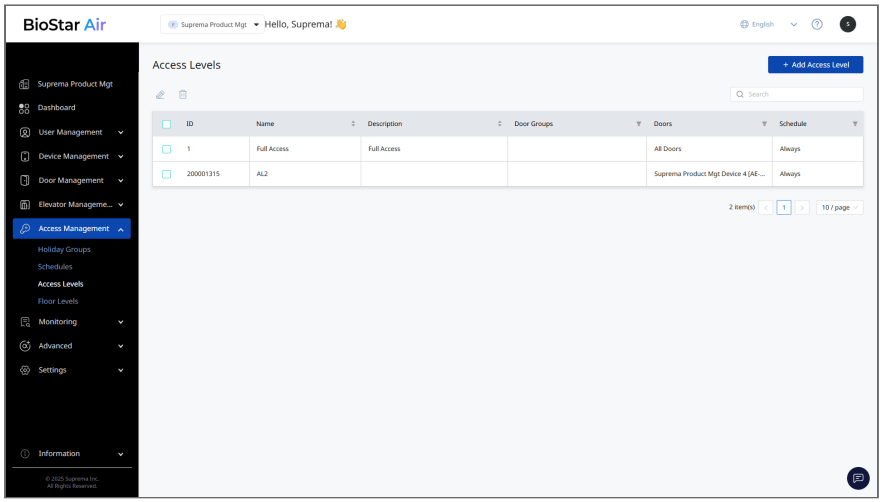
- **Door / door group**: Location where access is allowed
- **Schedule**: Time when access is allowed
- **Holiday group**: Dates or periods that restrict or adjust access

Set up access levels before adding users to streamline the user management process.

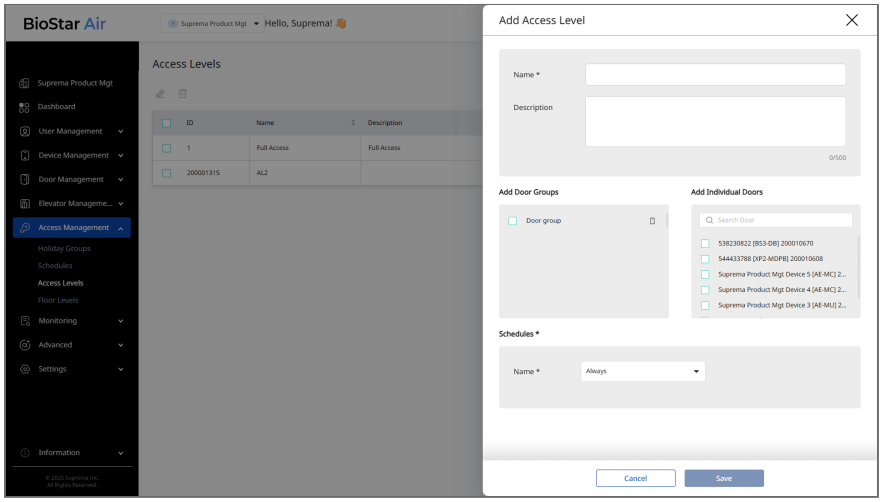
Add access level

Use access levels to set user permissions by door, schedule, and holiday.

1. Click **Access Management** → **Access Levels** in the left sidebar.
2. Click **Add Access Level** at the top right of the screen.



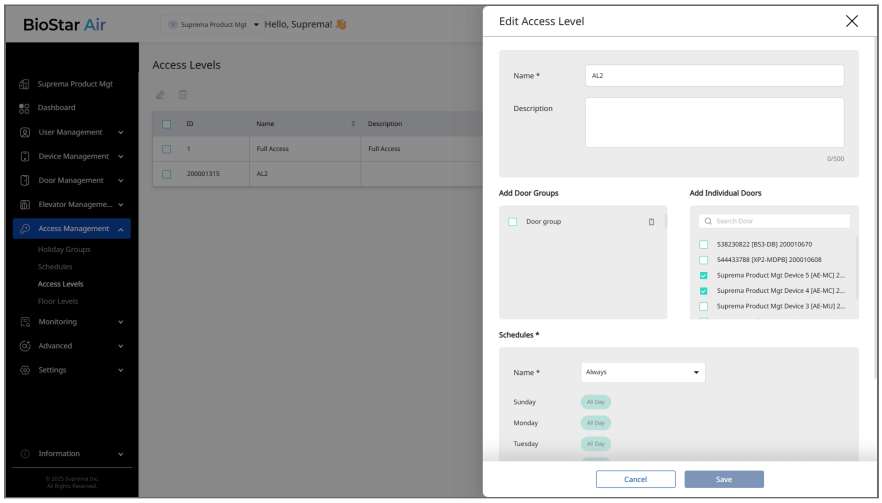
3. When the **Add Access Level** panel appears, enter **Name** and **Description** (optional).



4. In the **Add Door Groups** or **Add Individual Doors** section, select door groups or individual doors.
5. In the **Schedules** section, select the schedule to apply to the access level. Select **Always** to allow unrestricted access.
6. Click **Save** to add the access level.

Edit access level

1. Click **Access Management** → **Access Levels** in the left sidebar.
2. Click the access level you wish to modify from the access level list. Alternatively, select the checkbox of the access level you wish to modify and click ✎ at the top of the list.



3. When the **Edit Access Level** panel appears, edit the required information or change the settings.
4. Click **Save** to save the changes.

Delete access level

1. Click **Access Management** → **Access Levels** in the left sidebar.
2. Check the checkbox of the access level you wish to delete from the access level list. You can select more than one access level.
3. Click 🗑 at the top of the list.
4. When a warning message appears, click **Yes**.

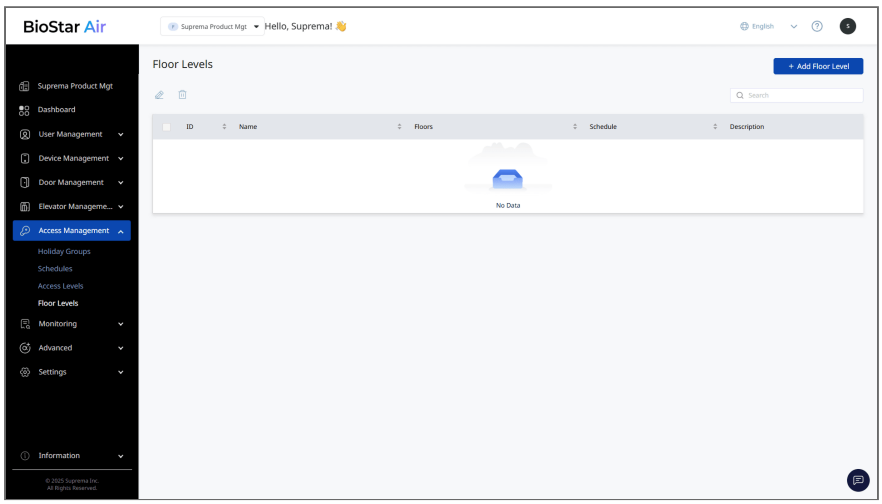
Manage Floor Levels

Floor levels are used in elevator access control settings. Floor levels enable fine-grained control over access permissions for each floor. For example, configure certain user groups so they can access only specific floors.

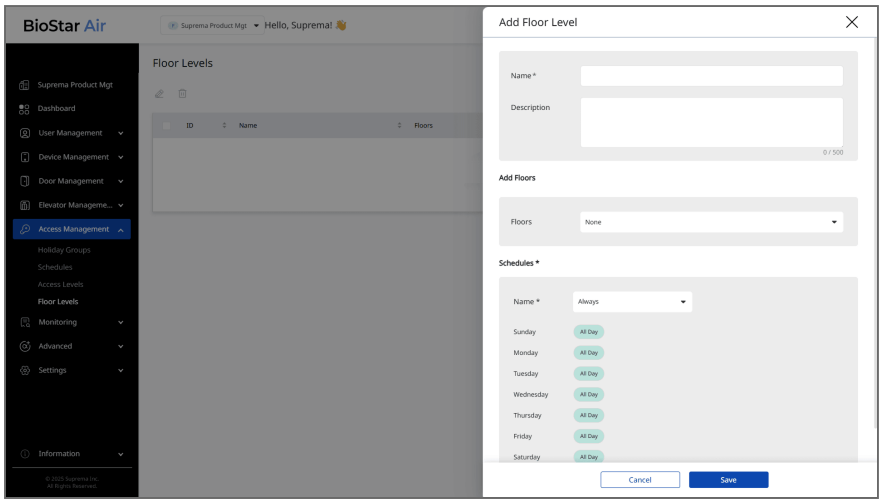
Add floor levels

Assign users or groups that can access specific floors.

1. Click **Access Management** → **Floor Levels** in the left sidebar.
2. Click **Add Floor Level** at the top right of the screen.



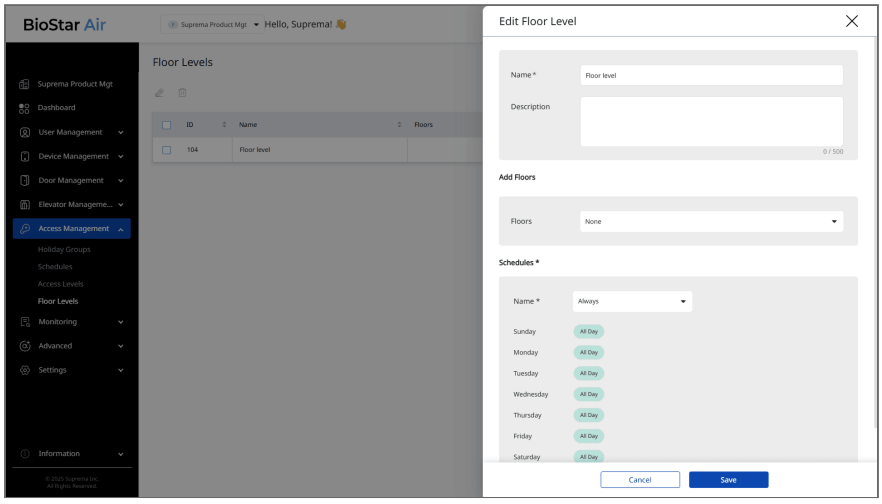
3. When the **Add Floor Level** panel appears, enter **Name** and **Description** (optional).



4. Select the floors to apply floor permissions in the **Add Floors** section.
5. Select the schedule to apply to the floor level in the **Schedule** section. Select **Always** to allow unrestricted access.
6. Click **Save** to add the floor level.

Edit floor levels

1. Click **Access Management** → **Floor Levels** in the left sidebar.
2. Click the floor level you want to edit from the list. Alternatively, select the checkbox of the floor level you want to edit, then click at the top of the list.



3. When the **Edit Floor Level** panel appears, modify the necessary information or change the settings.
4. Click **Save** to save the changes.

Delete floor levels

1. Click **Access Management** → **Floor Levels** in the left sidebar.
2. Select the checkbox of the floor level you want to delete from the list. More than one floor level can be selected.
3. Click at the top of the list.

4. When a warning message appears, click **Yes**.

Zone Management

Zones are logical groupings of doors and devices, which can be used for Anti-passback, on-site status, people counting, and other future applications.

Understanding zones and Anti-Passback (APB)

When using Zones for Anti-Passback, the administrator should define entry points and exit points for the zone. These determine when a credential user is inside of the zone or outside of the zone. A credential user cannot reenter the zone – even using a different credential – without first exiting the zone. Anti-passback can also be used to define clear entry points and exit points, preventing users from doubling back and exiting through an entrance.

Perimeter zone

Similar to Anti-Passback, BioStar Air defines a **perimeter zone** that determines a credential user's on-site status. This is important for the **On-Site Now** and **Roll Call** features. The Perimeter Zone may optionally be configured for Anti-Passback.

Refer to the following documents to learn how to manage zones and APB violations in the BioStar Air portal.

Manage Zones
With BioStar Air's **Zone** feature, organize doors into logical zones and apply **Anti-Passback (APB)** rules as needed to enforce users entering and exiting in the correct order. Optionally apply Anti-Passback rules per zone. Zones without APB can still use other Zone features, such as Presence to see who is inside. **Zones** can range from perimeter zones that cover an entire site to specific areas inside a building.

Before you start

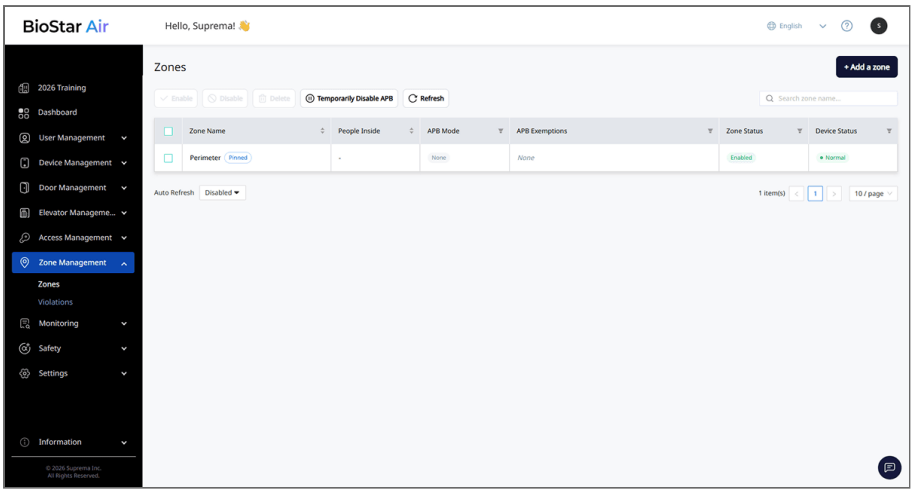
Check the following before creating a zone.

- Add the doors to the system before assigning them to a zone. For more information on registering doors, see Manage Registered Doors.
- A device can be used in only one zone at a time.
- Changing the zone’s entry and exit devices does not change the door settings.
- If the zone’s entry and exit devices are not set correctly, APB behavior and the presence count may differ from actual movement.
- Offline devices may apply changes later than online devices. Changes apply to online devices first. Offline devices apply changes after they reconnect.
- Only devices with firmware **v2.13** or later can be assigned to a zone. Make sure that verify the device assigned to the zone uses the latest firmware.
- Doors used in an APB zone are protected to prevent setting conflicts. To change door settings that affect APB behavior, remove the door from the zone first.

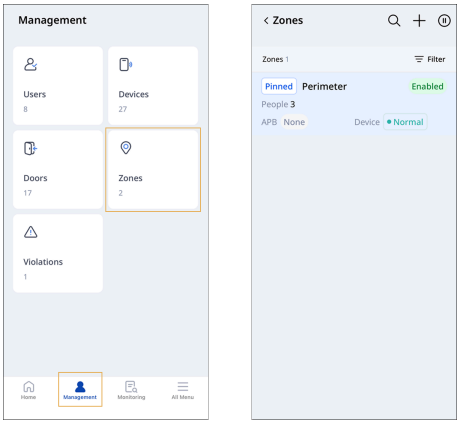
Explore zone list

Web

Click **Zone Management** → **Zones** on the left sidebar.



Mobile



1. Open the BioStar Air app on your mobile device and log in.
2. Tap **Management** at the bottom of the screen.
3. Tap the **Zones** card.

The zone list shows all zones set up for the site at a glance.

- **Zone Name**: Zone name. **Perimeter** shows the **Pinned** badge next to the name.
- **People Inside**: Number of users recorded as present in the zone. For more information, see Checking people inside.
- **APB Mode**: The APB mode applied to the zone (**Hard** / **Soft** / **None**).
- **APB Exemptions**: The APB exemption group assigned to the zone.
- **Zone Status**: This indicates whether the zone is activated.
- **Device Status**: This indicates whether devices assigned to the zone are online.

Perimeter zones and internal zones

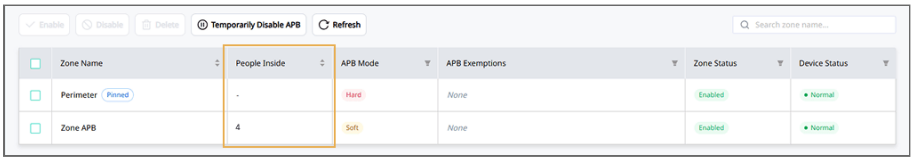
On first site setup, the system provides **Perimeter** by default. **Perimeter** is like the site's main gate. Rename and delete are unavailable, and the list shows the **Pinned** badge.

- Entry and exit devices in **Perimeter** help calculate Presence in **Dashboard** > **On Site Users** and **Safety** > **Presence**.
- Create separate zones for areas that need internal control (e.g., server rooms, specific floors) in addition to perimeter zones, enabling fine-grained movement control within the site.

Checking people inside

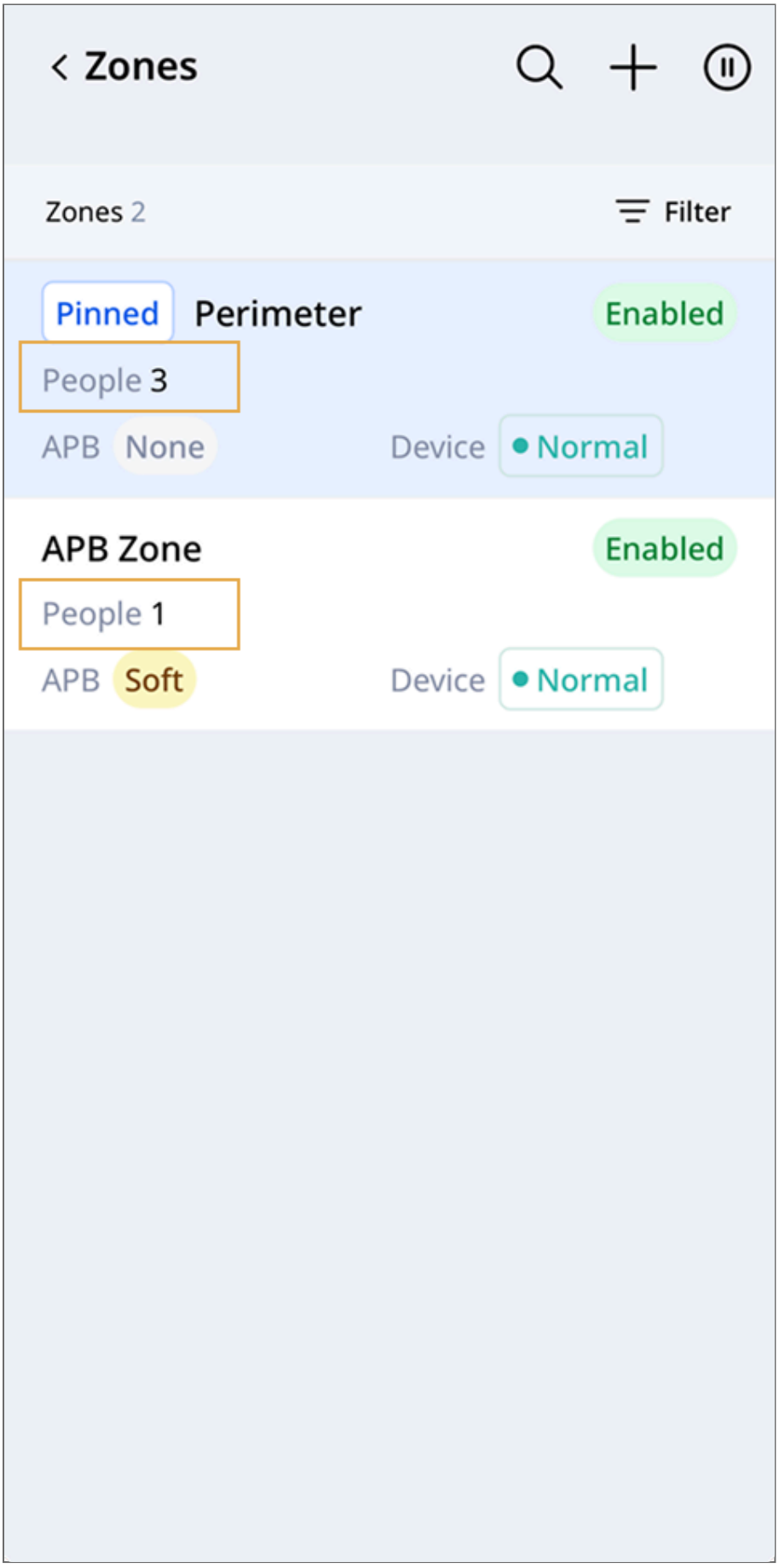
Web

Check how many people are currently in each zone in the **People Inside** column of the zone list.



Mobile

Check how many people are currently in each zone in the **People** item of the zone list.

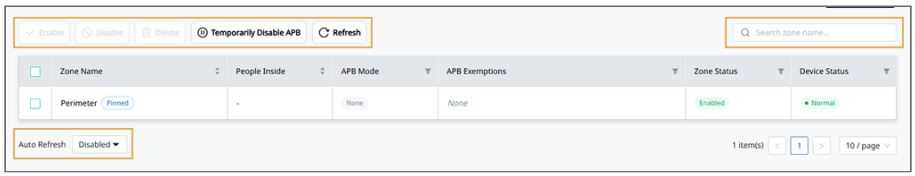


- The system calculates this number based on authentication logs from the entry and exit devices set for the zone. Authenticate at an entry device to increase the count, and authenticate at an exit device to decrease it.

- Users in an APB exemption group are not subject to APB rules, but remain included in the people-inside count.
- Deactivating a zone initializes the zone's people-inside count to 0.
- To keep the latest value, click **Refresh** at the top of the list or set an auto-refresh interval.

Zone management feature

Use the management features at the top and bottom of the zone list to complete the following tasks.



- **Enable** / **Disable**: Enable or disable selected zones.
- **Delete**: Delete selected zones. **Perimeter** cannot be deleted.
- **Temporarily Disable APB**: Pause APB for all zones on the site, including the perimeter zone.
- **Refresh**: Refresh the list immediately to show the latest status. In **Auto Refresh** at the bottom of the list, select an auto refresh interval (**Disabled** / **5 Seconds** / **1 Minute**). The list refreshes automatically at the set interval.
- **Search zone name...**: Search the list by zone name.

Filter zone list

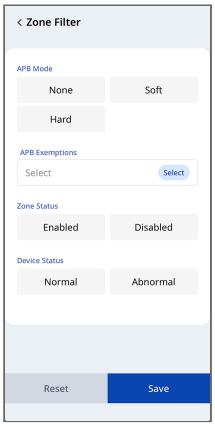
Web

In the list header, click the ▼ button in the **APB Mode**, **APB Exemptions**, **Zone Status**, or **Device Status** column to filter the list by that condition.



> **Info**
> Click **Reset** to clear the filter.

Mobile



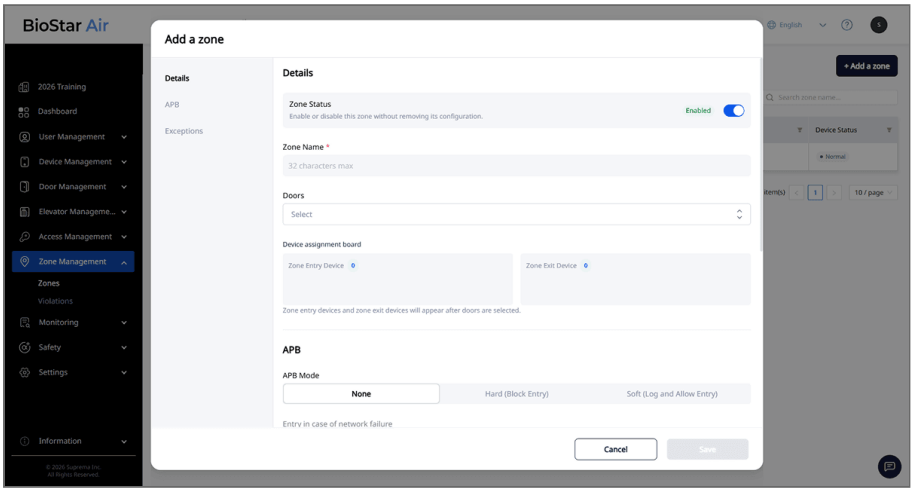
1. Tap **Filters** at the top right of the zone list.
2. Select criteria in **APB Mode**, **APB Exemptions**, **Zone Status**, or **Device Status**.
3. Tap **Save** to filter the list by the selected criteria.

> **Info**
> Tap **Reset** to clear the filter.

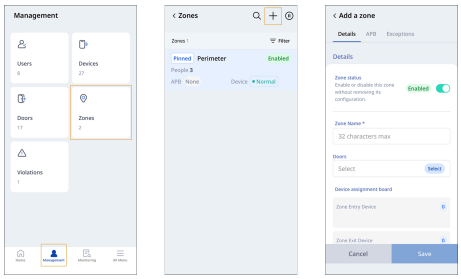
Add zones

Web

Click **Zone Management** → **Zones** on the left sidebar. Click **+ Add a zone** at the top right of the screen.



Mobile

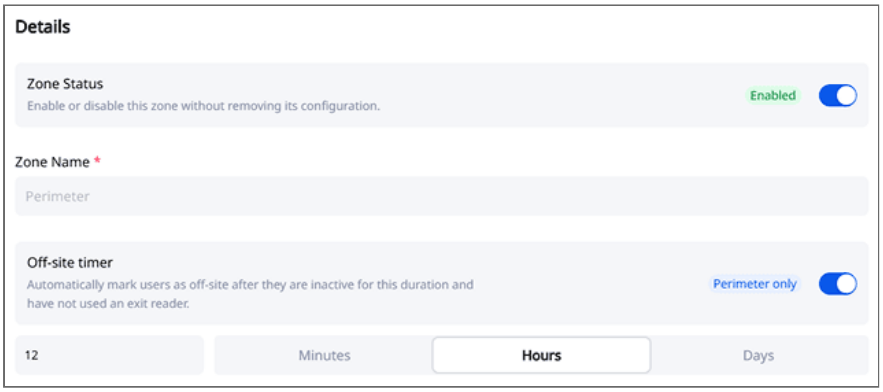


1. In the BioStar Air app, tap **Management** at the bottom of the screen.
2. Tap the **Zones** card.
3. Tap + at the top right of the screen.

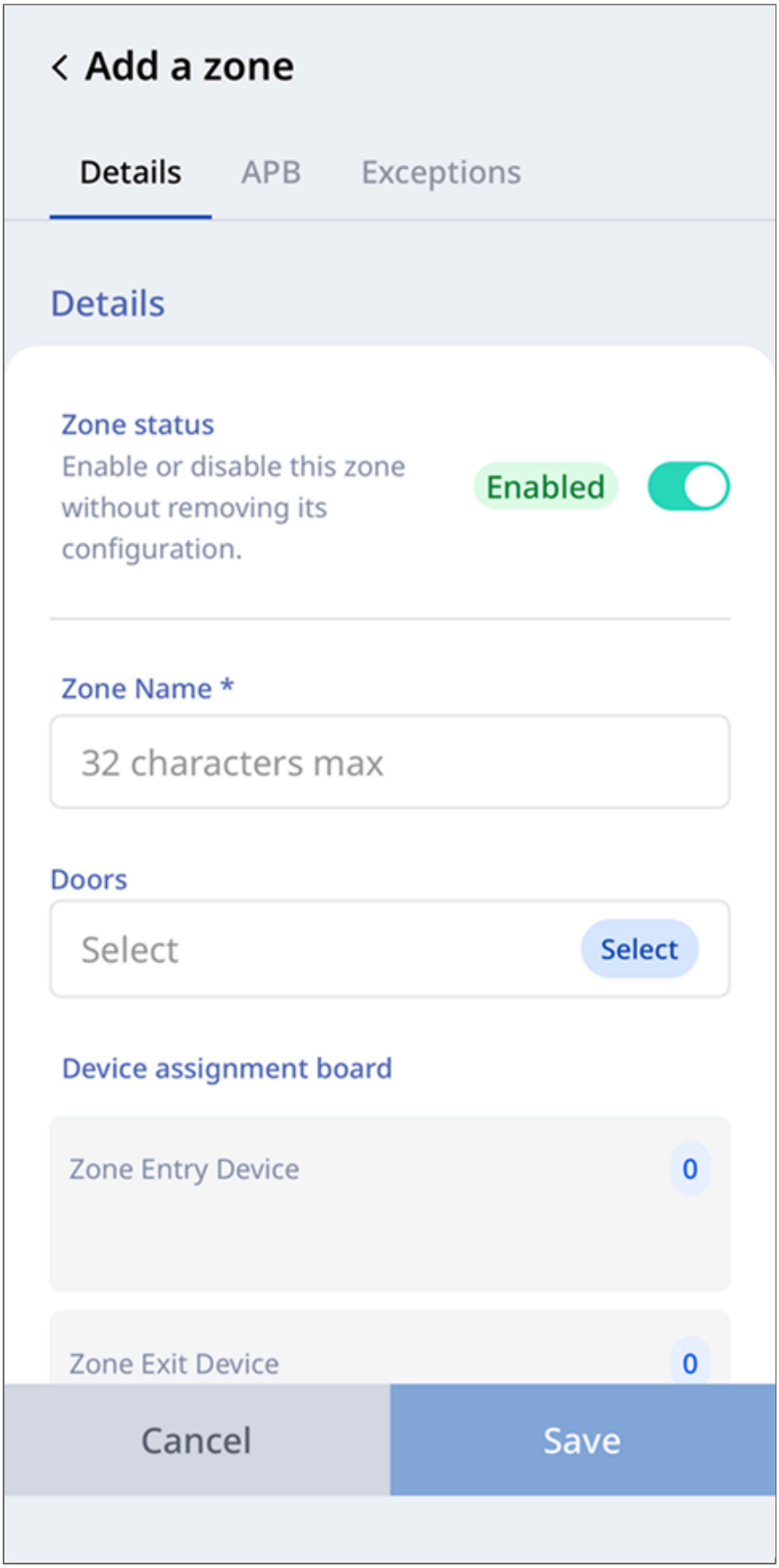
1 Enter basic information

Enter the zone's basic information in the **Details** section.

Web


Details
Zone Status
Enable or disable this zone without removing its configuration.
Enabled
Zone Name *
Perimeter
Off-site timer
Automatically mark users as off-site after they are inactive for this duration and have not used an exit reader.
Perimeter only
12
Minutes
Hours
Days

Mobile



- **Zone Status**: Select whether to activate the zone immediately. Activate or deactivate the zone later without changing the settings.
- **Zone Name**: Enter up to 32 characters. For sites with multiple buildings, use a name that clearly indicates the

location.

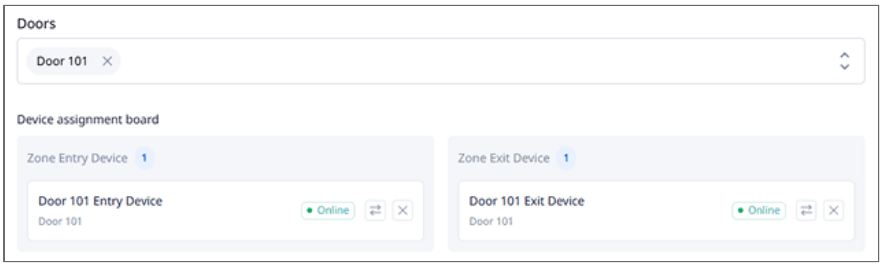
- **Off-site timer**: Users with no activity for the set time and who did not use an exit device automatically switch to **Off Site** status. If no exit device is assigned to the perimeter zone, set this option.

> **Info**
> The **Off-site timer** option appears only when setting a perimeter zone.

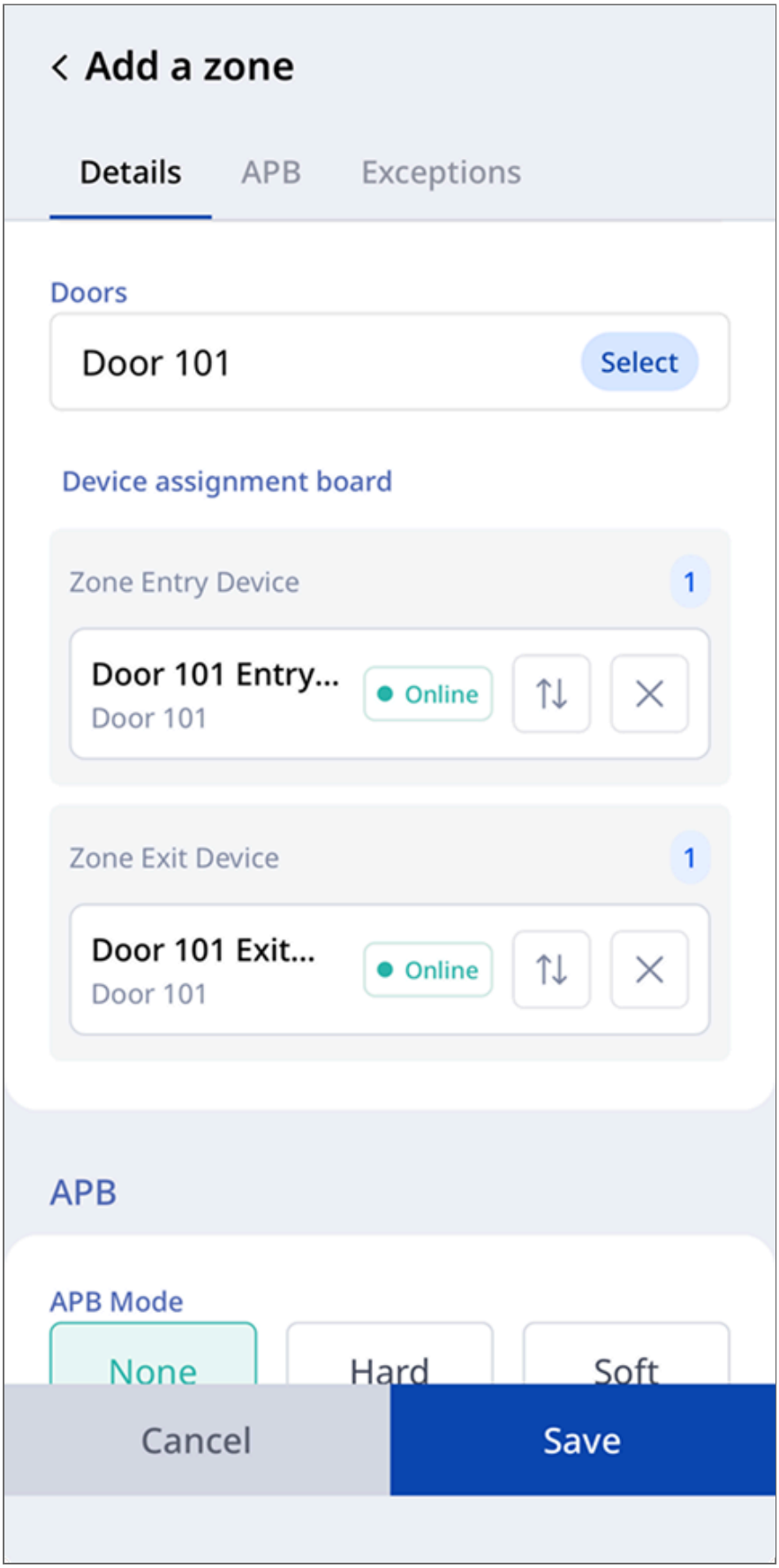
2 Assign doors and devices

Select the doors and devices to assign to the zone.

Web



Mobile



- **Door**: Select the doors to include in the zone. More than one door can be selected. Select a door, and its devices appear in **Device assignment board**.
- **Device assignment board**: Assign each device as **Zone Entry Device** or **Zone Exit Device**. Devices appear with

Device ID to distinguish them. Click the Move (⇄) button to set the device as an entry or exit device.

> **Info**
>
> - Only devices with firmware v2.13 or later appear in **Device assignment board**. Make sure that verify the device assigned to the zone uses the latest firmware.
> - For more information on device management, see Manage Device and Panel Groups.
> - For more information on managing registered doors, see Manage Registered Doors.

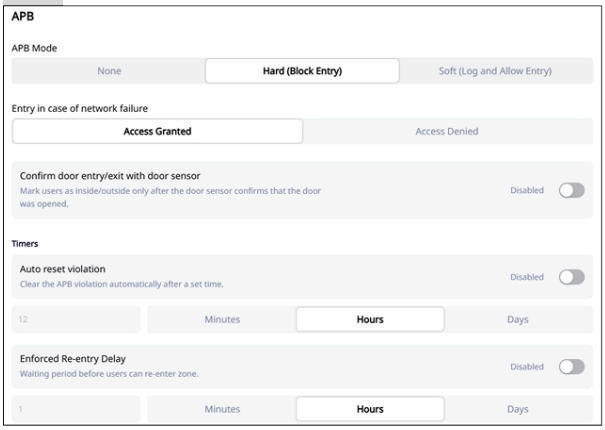
3 Set APB mode

In the **APB** section, set anti-passback rules. Anti-Passback rules are optional. If strict control is unnecessary, select **None** mode to use zones only for Presence checks.

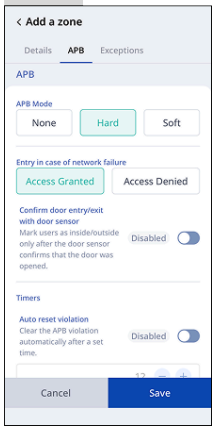
Hard

Hard (Block Entry)

Web



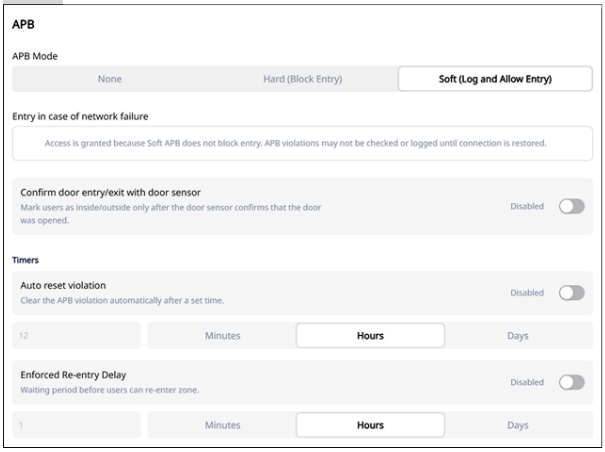
Mobile



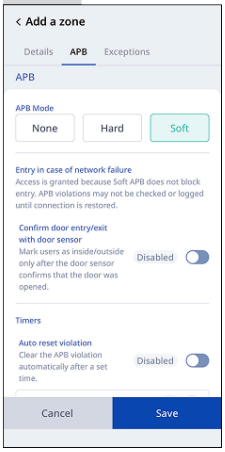
Soft

Soft (Log and Allow Entry)

Web



Mobile



- **APB Mode**: Select the APB mode.
  - **Hard (Block Entry)**: Blocks access when a user violates an APB rule and logs a violation event.

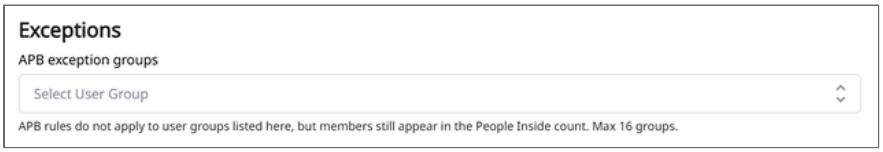
  - **Soft (Log and Allow Entry)**: Allows access but logs an APB violation in the event log.
  - **None**: Does not apply APB to the zone. Zones without an APB mode continue to count presence.

- **Entry in case of network failure**: Select whether to allow or deny access if the BioStar Air server is unreachable due to a network failure. **Soft** mode does not block access, so access is always allowed, and the system may not verify or log violations until the network connection recovers.
- **Confirm door entry/exit with door sensor**: When enabled, the door sensor must confirm the door opens before marking users as **On Site** or **Off Site**.
- **Timers**
  - **Auto reset violation**: Automatically clears an APB violation after the set time.
  - **Enforced Re-entry Delay**: The wait time before a user can enter the same zone again.

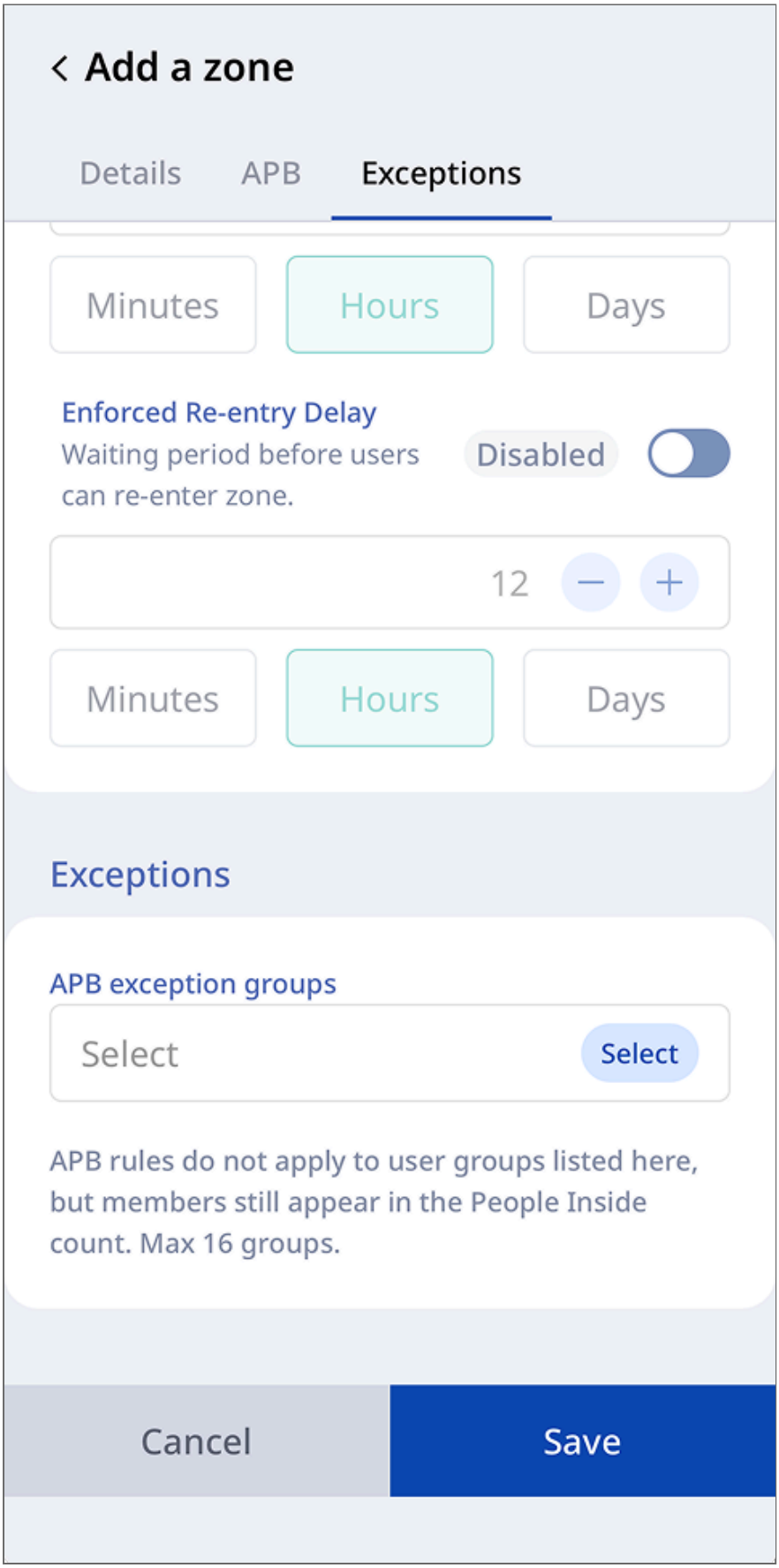
4 Set exceptions

In the **Exceptions** section, select user groups exempt from APB rules.

Web



Mobile



- Specify up to 16 user groups as exceptions per zone.
- Users in an exception group are exempt from APB rules but remain in the presence count.

- If **APB Mode** is **None**, the **Exceptions** section is disabled.

> **Info**
> For more information on managing user group, refer to Manage User Groups.

5 Save zone

Click **Save** to save the zone settings.

> **Notes for adding a zone**
> - Doors already assigned to another APB zone, doors with no device, or doors dedicated to Airfob Patch do not appear in the door selection list.
> - Enable **Auto reset violation** (if the zone is not a perimeter) or **Off-site timer** (if the zone is a perimeter) to save a zone without an exit device.
> - Zones must have unique names.
> - Changing **APB Mode** to **None** initializes all saved detailed settings (**APB Mode**, **Timers**, **APB exception groups**) for the zone. Use the Disable zone or Temporarily Disable APB feature to pause APB enforcement without changing settings.

Enable or disable zones

This feature lets administrators enable or disable zones. The settings remain unchanged. Disabling a zone initializes the zone presence count to 0. However, existing APB violations remain. Clear them from the Check APB Violations menu.

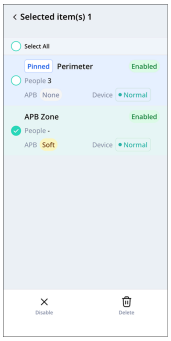
Web

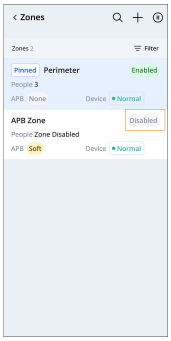
1. Click the checkbox for the zone to enable or disable in the list. Select one or more zones.
2. Click **Enable** or **Disable** at the top of the list.
3. When the confirmation message appears, click **Enable** or **Disable**.

Check each zone status in the **Zone Status** column in the list.



Mobile





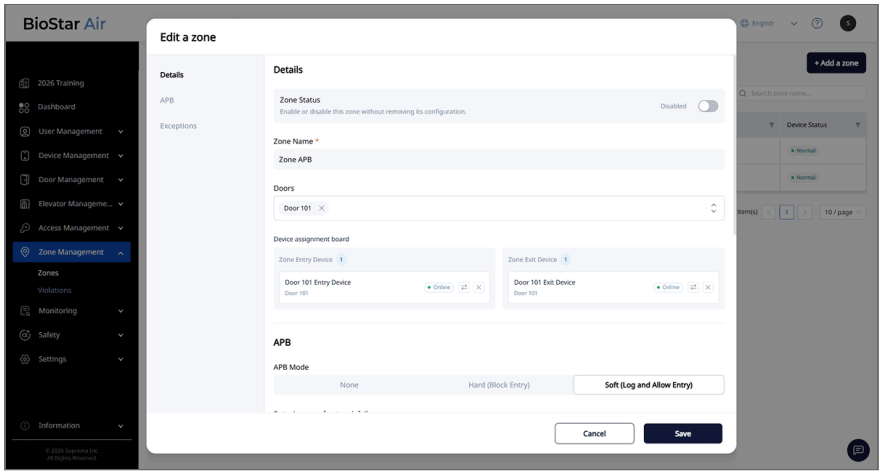
1. Touch and hold the zone to enable or disable in the list.
2. Select the zone to enable or disable. Select one or more zones.
3. Tap **Enable** or **Disable** at the bottom of the screen.
4. When the confirmation message appears, click **Enable** or **Disable**.

Edit zone

Edit the details, APB settings, and exception settings for an existing zone.

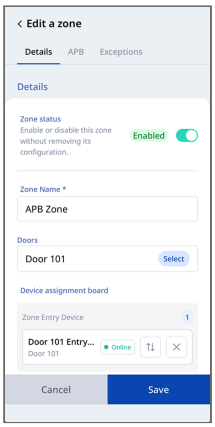
Web

1. Click the zone to edit in the list.
2. The **Edit a zone** window appears.



3. Edit the required fields in the **Details**/**APB**/**Exceptions** section.
4. Click **Save** to save the changes.

Mobile



1. Tap the zone to edit in the list.
2. The **Edit a zone** screen appears.
3. Edit the required fields in the **Details**/**APB**/**Exceptions** section.
4. To save the changes, tap **Save**.

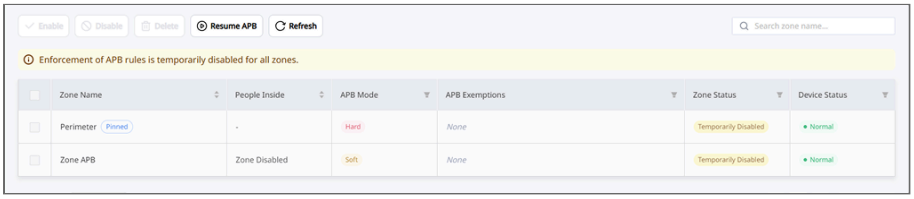
> **Info**
> For more information about the detailed settings in the **Details**/**APB**/**Exceptions** section, see Add zones.

Temporarily Disable APB

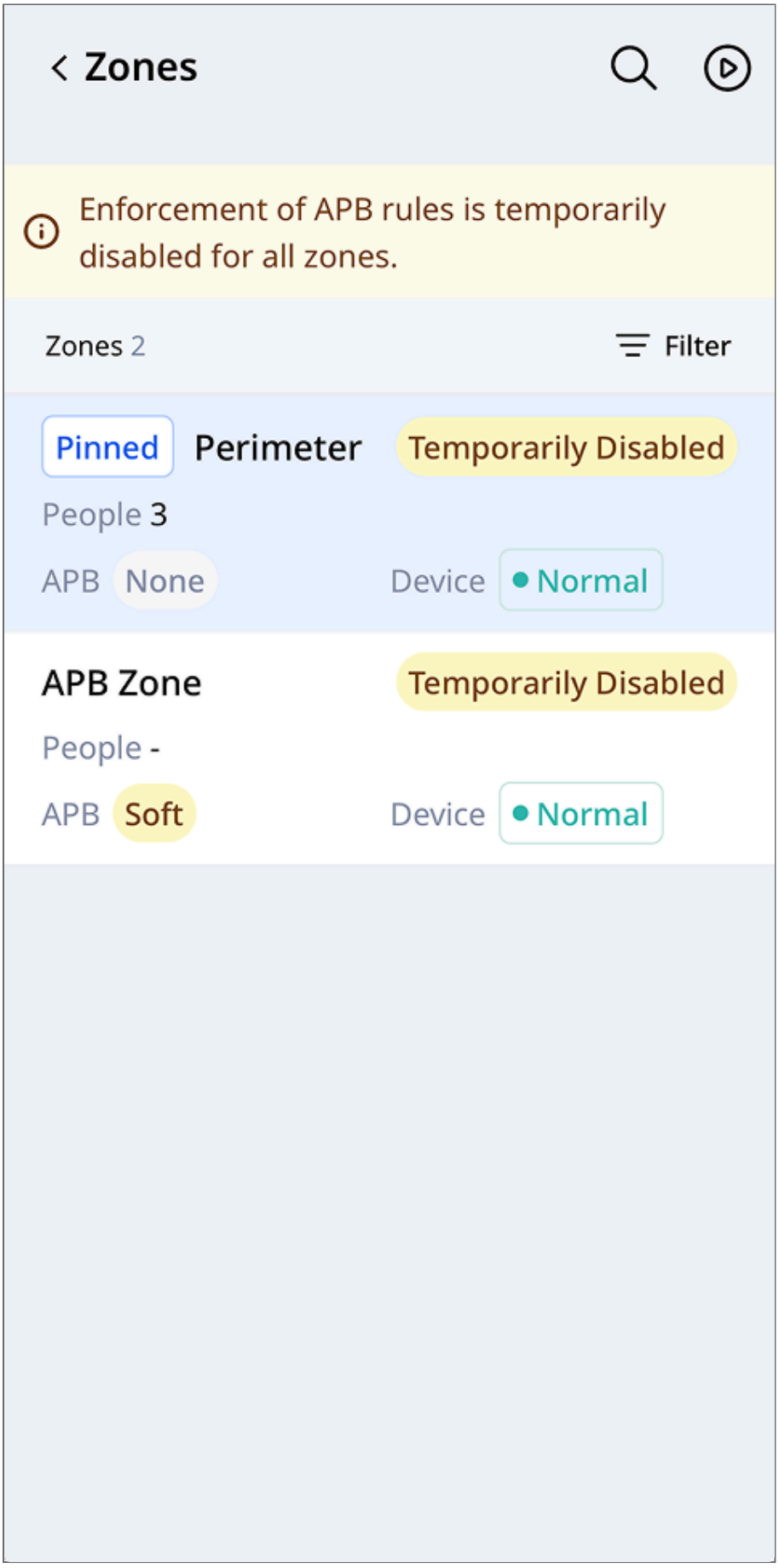
Select **Temporarily Disable APB**(⏸) at the top of the list to pause site-wide APB (for special events or peak traffic). APB pauses for all zones, including perimeter zones. After resuming, each zone returns to its previous state. During the pause, the zone list locks, so do not make other changes.

Click **Resume APB**(▶) to resume the APB mode set for zones.

Web



Mobile

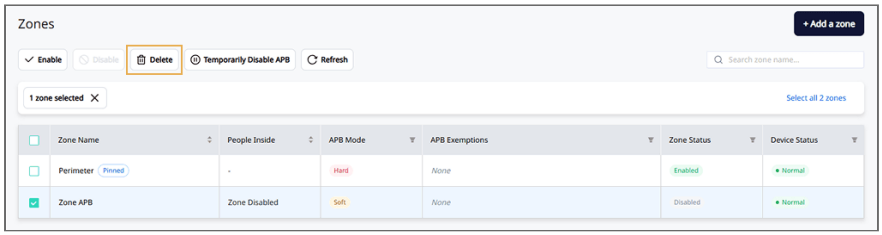

Zones
Enforcement of APB rules is temporarily disabled for all zones.
Zones 2
Filter
Pinned
Perimeter
Temporarily Disabled
People 3
APB None
Device Normal
APB Zone
Temporarily Disabled
People -
APB Soft
Device Normal

You cannot enable an anti-passback zone while an Roll Call is in progress. Try again after Roll Call ends. For more information about Roll Call, see Roll Call.

Delete a zone

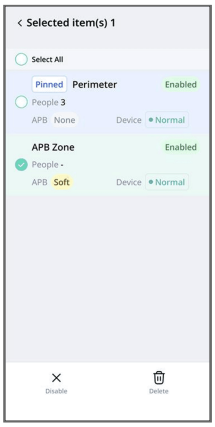
Web

1. Select the checkbox for the zone to delete in the list. Select one or more zones.
2. Click **Delete** at the top of the list.



3. Click the **Delete** button when the confirmation message window appears.

Mobile



1. Touch and hold the zone to delete in the list.
2. Select the zone to delete. Select one or more zones.
3. Tap **Delete** at the bottom of the screen.
4. When the confirmation message appears, click **Delete**.

Info

- **Perimeter** cannot be deleted.
- Only the selected zone is deleted. Doors and devices assigned to the zone remain. Deletion cannot be undone.
- The system cannot delete a zone while assigned devices are offline, syncing, or upgrading firmware. Wait until the devices reconnect, or remove them from the zone, then try again.

Check APB Violations

In the **Zone Management** → **Violations** menu, review users who violate the zone anti-passback (APB) rules and clear violations as needed. If you have not set zones and APB mode yet, first refer to Manage Zones.

When violations occur

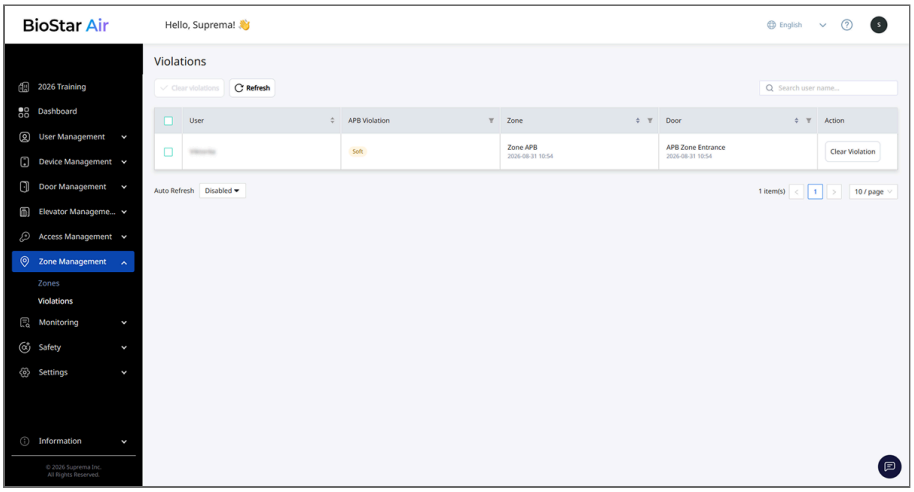
The system records an APB violation when a user tries to enter or exit out of sequence based on the zone's APB mode.

- In zones set to **Hard mode**, an APB violation blocks access, and the system records the violation.
- In zones set to **Soft mode**, the system allows access, but records an APB violation.
- APB rules do not apply to users in the APB exception group, so they do not appear in the violations list.

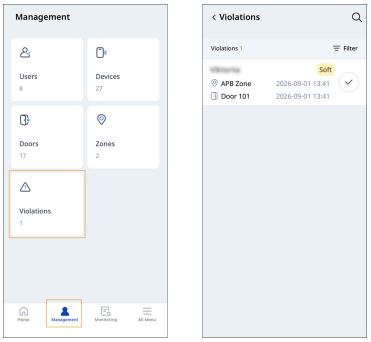
Review the violations list

Web

In the left sidebar, click **Zone Management** → **Violations**.



Mobile



1. Open the BioStar Air app on your mobile device and log in.
2. Tap **Management** at the bottom of the screen.
3. Tap the **Violations** card.

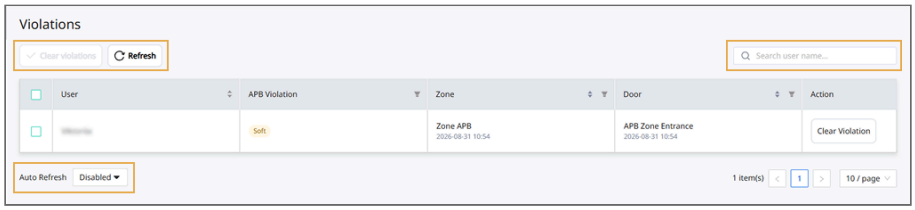
The list shows users with active APB violations. If no active APB violations exist, an empty state screen appears instead of the list.

- **User**: User with a recorded APB violation.
- **APB Violation**: Mode (Hard/Soft) where the APB violation occurred.
- **Zone**: The zone where the APB violation occurred.
- **Door**: The door where the APB violation occurred.
- **Action**: Clear an individual APB violation.

> **Info**
> Review cleared APB violations and past APB violation history in **Monitoring** → **Event Logs**.

Manage the violations list

Use the management features at the top and bottom of the list to perform the following tasks.

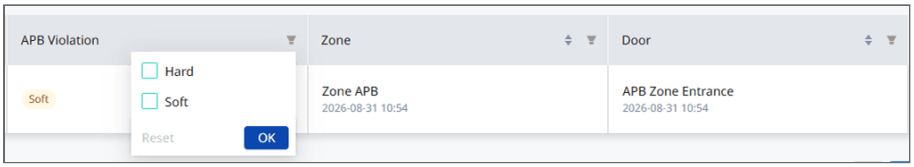


- **Clear Violation**: Clear APB violations for the selected user in the list. For more information, see Clear violations.
- **Refresh**: Refresh the list immediately to show the latest status. In **Auto Refresh** at the bottom of the list, select an auto refresh interval (**Disabled** / **5 Seconds** / **1 Minute**). The list refreshes automatically at the set interval.
- **Search user name...**: Search by user name.

Filter the violation list

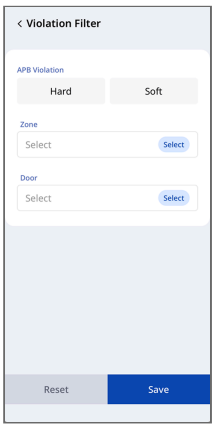
Web

In the list header, click the button in the **APB Violation**, **Zone**, or **Door** column to filter the list by that condition.



> **Info**
> Click **Reset** to clear the filter.

Mobile



1. Tap **Filters** at the top right of the violation list.
2. Select a filter condition in **APB Violation**, **Zone**, or **Door**.
3. Tap **Save** to filter the list by the selected criteria.

> **Info**
> Tap **Reset** to clear the filter.

Clear violations

Clearing an APB violation initializes the user's active APB violation status and restores normal zone access.

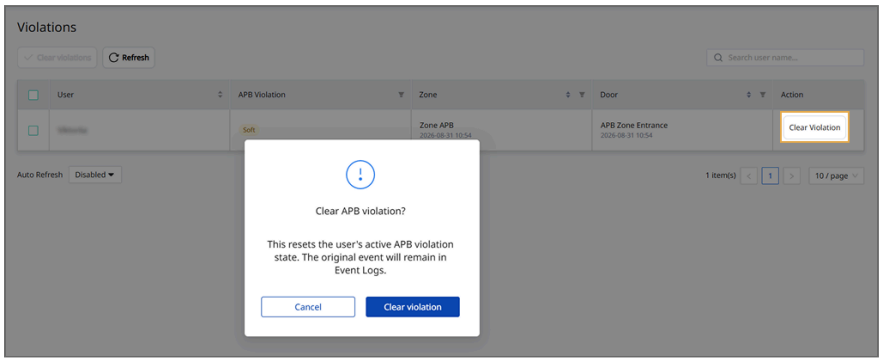
Info

- **Clear Violation** initializes only the user's active APB violation status. The event that triggered the APB violation remains in the event log.
- Existing APB violations remain after the zone is disabled. Clear them in the violation list.
- Users in an APB exception group do not appear in this list, but remain included in the zone presence count.

Clear a violation for an individual user

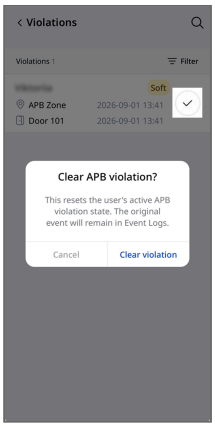
Web

1. In the list, click **Clear Violation** in the **Action** column for the user whose APB violation to clear.



2. When the confirmation message appears, click **Clear Violation**.

Mobile

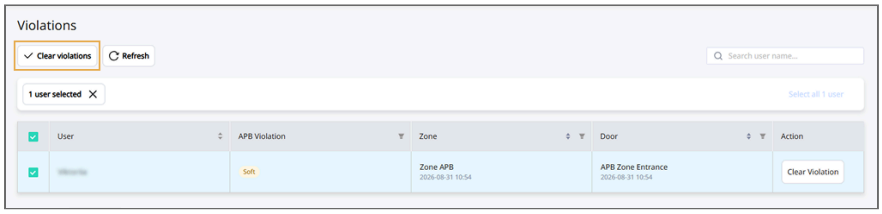


1. In the list, tap in the user's row to clear the APB violation.
2. When the confirmation message appears, tap **Clear Violation**.

Clear violations for multiple users

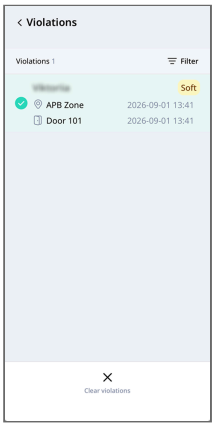
Web

1. Select the checkboxes next to users with APB violations to clear. Select one or more users.
2. Click **Clear violations** at the top of the list.



3. When the confirmation message appears, click **Clear violations**.

Mobile



1. Touch and hold a user in the list.
2. Select users whose violations to clear. Select one or more users.
3. Tap **Clear violations** at the bottom of the screen.
4. When the confirmation message appears, tap **Clear violations**.

Monitoring

Use BioStar Air monitoring to track and manage key system activities in real time. Monitor event and change logs to analyze system activity, check door status in real time and control doors remotely, and comprehensively manage security activity through generated notifications and reports.

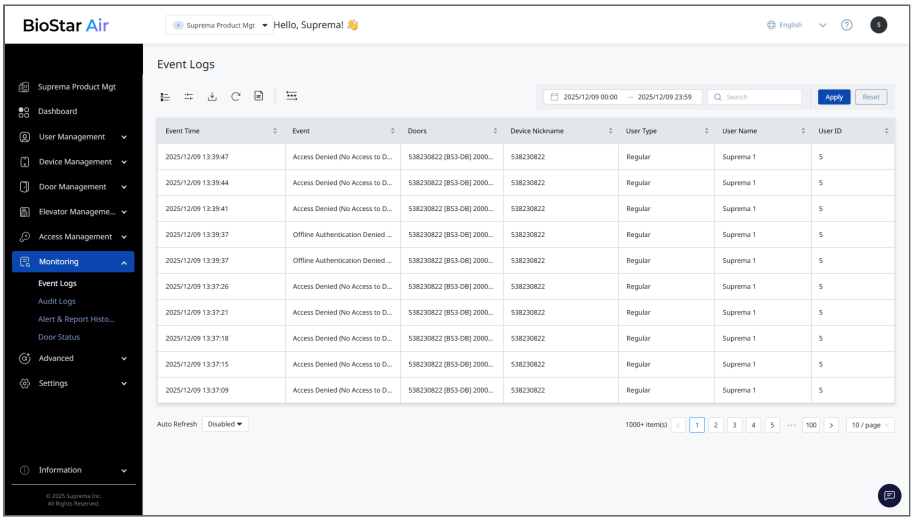
Use Event Logs
One of the key advantages of a cloud access control platform is the ability to monitor site activity anytime, anywhere. This document explains how to monitor and analyze event logs in BioStar Air.

> **Tip**
> Watch the following video for a tutorial on event logs.

View event logs

Web

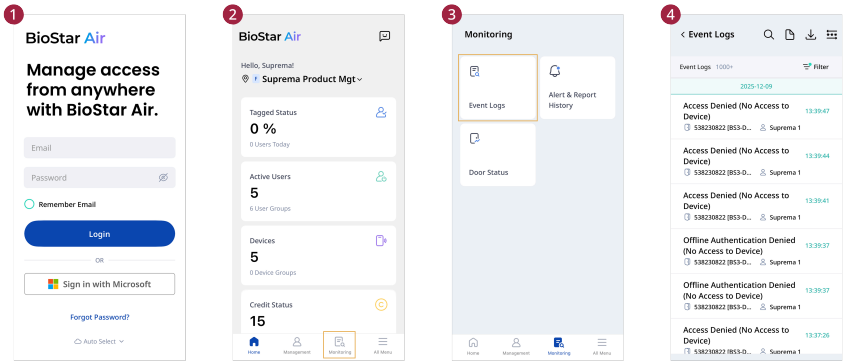
Go to **Event Logs** to view event logs. Click **Monitoring** → **Event Logs** in the left sidebar.



The **Event Logs** screen shows a table with details including event time and name, door name, device alias, user type, and user name.

Mobile

This guide explains how to check the event log in the mobile app.



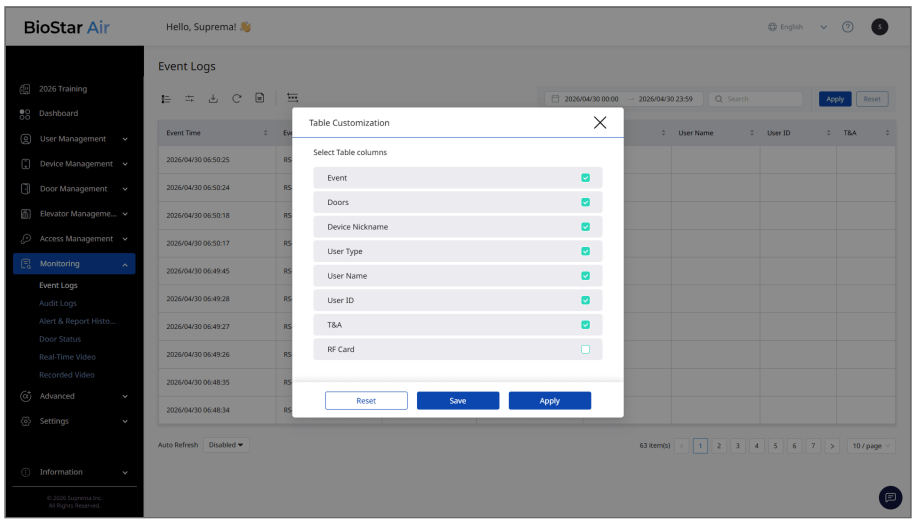
1. Open the BioStar Air app on your mobile device and log in.
2. Tap **Monitoring** at the bottom of the home screen.
3. Tap the **Event Logs** card.
4. Scroll through the event log list to view its contents.

Info

- **Filters**: Filter event logs.
- : Search by specific keywords. Enter one of the following: RF card ID, user ID, email, or name.
- : Generate reports. For more information on report creation, refer to Configure reports.
- : Download reports as CSV or PDF files.
- : Apply personal data masking.

Table Customization

Customize table columns to show or hide information. Reorder columns to place frequently used ones at the front. Click the button at the top of the event log list. The **Table Customization** window appears.



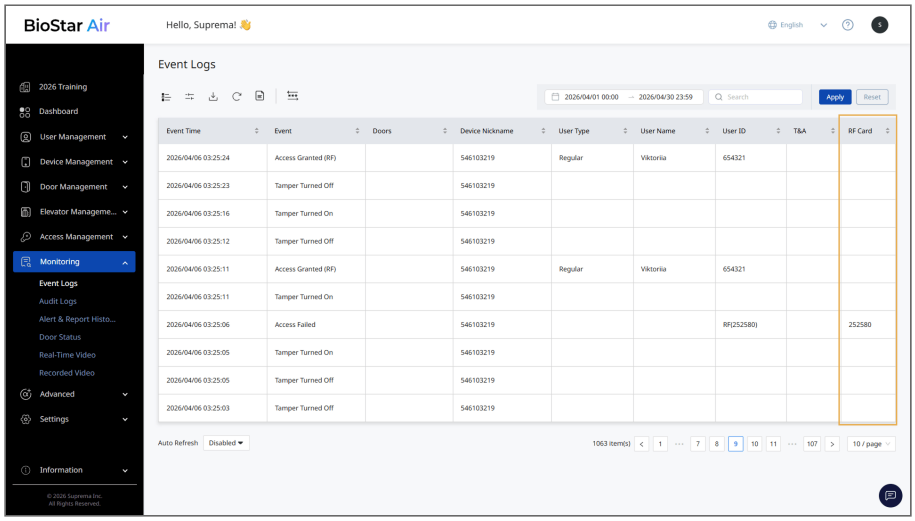
- Select or clear the checkboxes for columns to show or hide.
- To reorder columns, click and drag a column to the desired position.
- Click **Save** to save the **Table Customization** settings.
- Click **Apply** to apply **Table Customization** to the log list without saving.
- Click **Reset** to cancel the changes in **Table Customization** and restore the initial state.

> **Info**
>
> - When you click **Save**, the settings remain even after navigating to another menu. When you click **Apply**, the changes apply only to the current list and revert after you leave the page.
> - **Audit Logs** does not support the **Table Customization** feature.

Show RF card number column

Add the **RF Card** column to the event log to view the RF card number when a user authenticates using an RF card.

1. Click the button at the top of the event log list.
2. When the **Table Customization** window appears, check the **RF Card** checkbox and drag it to the desired position.
3. Click the **Save** or **Apply** button.
4. The **RF Card** column is displayed in the event log list.

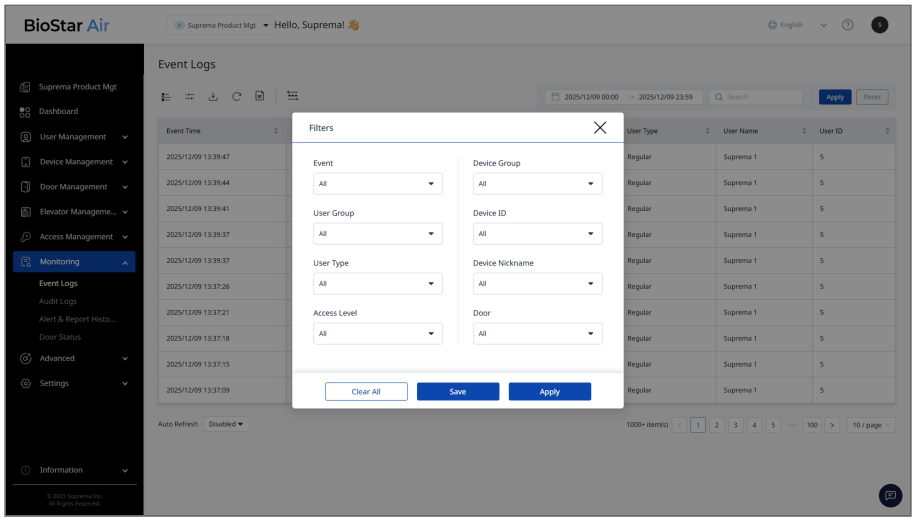


Info

The RF card number is shown in the event log only when a user has a single card assigned. If a user has multiple RF cards assigned, the RF card number will not be shown.

Filter logs

Filter logs to quickly find the information you need. Click at the top of the log list. When the **Filters** window appears, select the desired value for each item.



Info

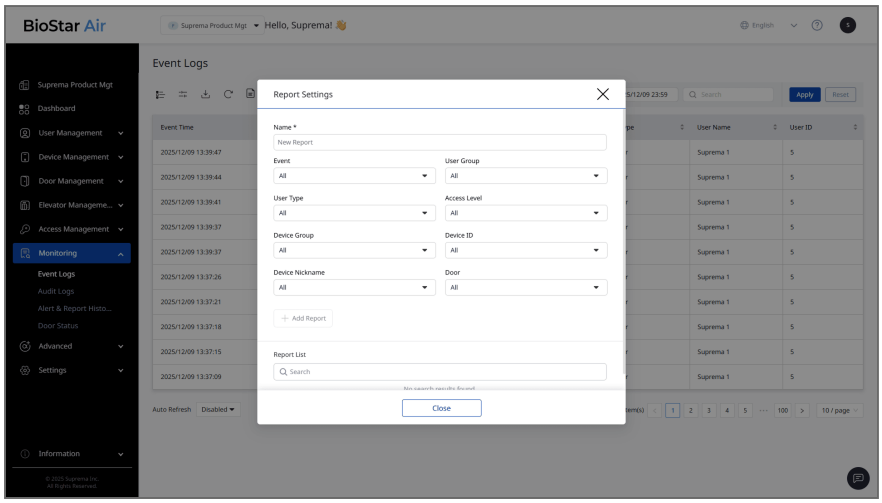
- Click **Save** or **Save Filter** to save the settings so they remain after navigating to another menu. Click **Apply** or **Apply Filter** to apply the changes only to the current list; they will revert when you navigate away.
- **Reset** or **Clear Filters** to cancel the changes and return to the initial state.

Configure reports

Generate reports for events that occurred during a specific period by filtering log data.

1. Click the button at the top of the log list.

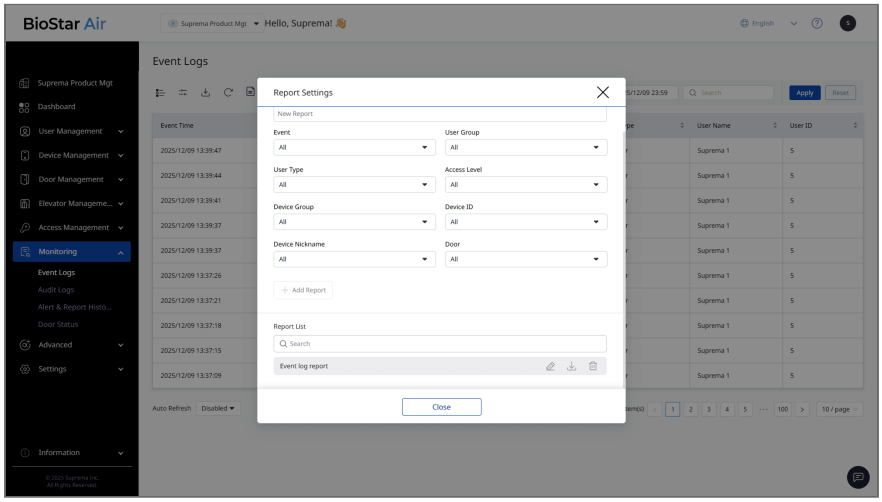
2. When the **Report Settings** window appears, enter a report name.



3. Select the items to include in the report.

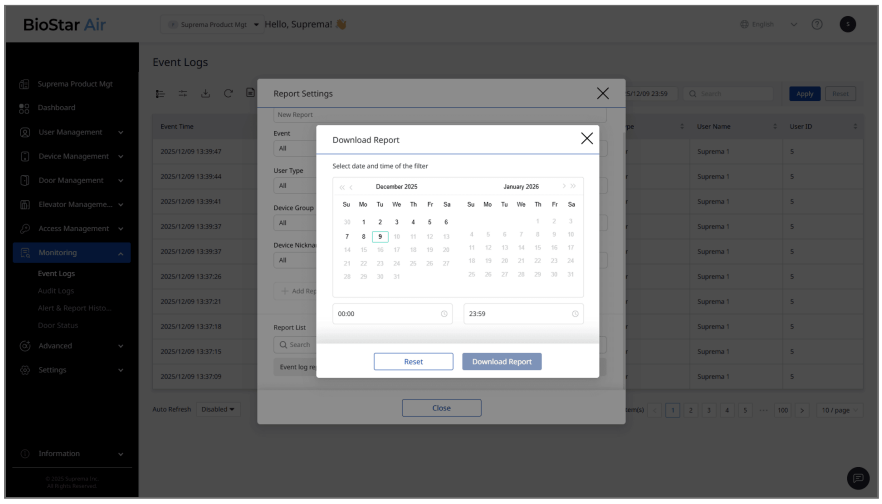
4. Click **Add Report** to save the configured report.

5. A report is created with the name set in **Report List**.



6. To download the generated report, click the button next to the report name.

7. When the **Download Report** window appears, select the period to query events and click **Download Report**.



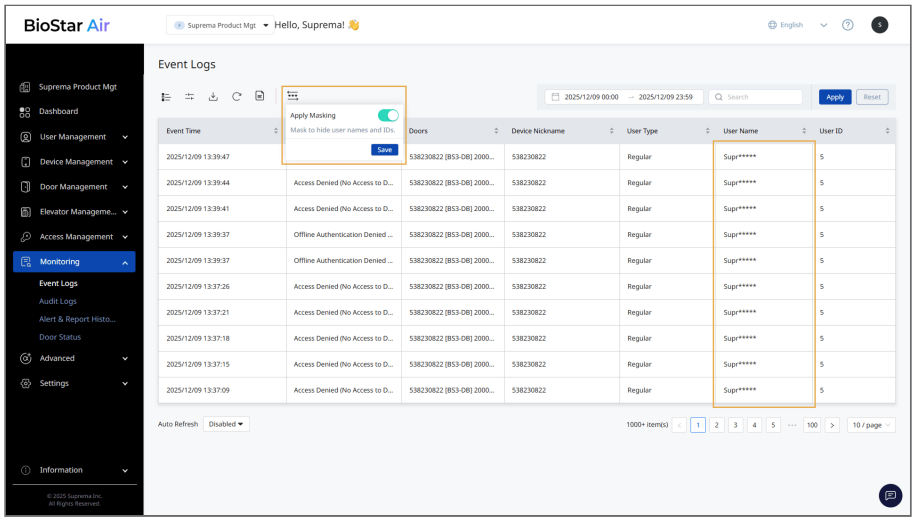
A download link is sent to the administrator's email.

> **Info**
> **Report List** lets you search for, edit, download, or delete the reports created.

Mask personal data

Mask personal data in logs to protect sensitive information. When personal data masking is enabled, information such as user names, email addresses, and phone numbers is partially hidden.

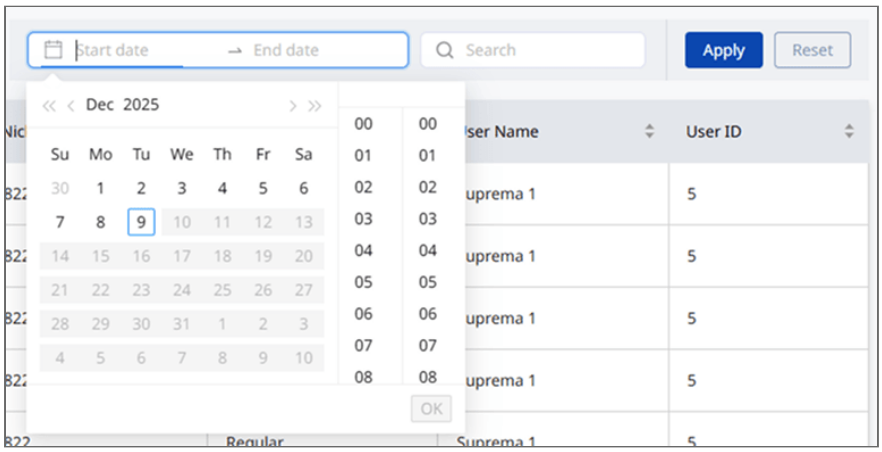
To enable personal data masking, click the button at the top of the log list. In the pop-up menu, enable **Apply Masking** and click **Save**.



Other features

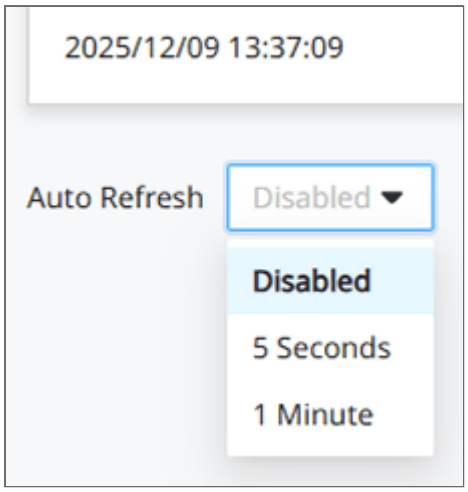
Use the toolbar at the top of the log list to manage logs more efficiently.

- To sort logs by date, select a date and time range, then click **Apply**. Click **Reset** to reset the date.



- In the **Search** input field, enter specific keywords to search logs. Enter one of the following: RF card ID, user ID, email, or name.
- Click to save logs as a CSV or PDF file.
- Click at the top of the list to refresh logs.

- To refresh at a specific interval, select 5 seconds or 1 minute in **Auto Refresh** at the bottom left of the list.



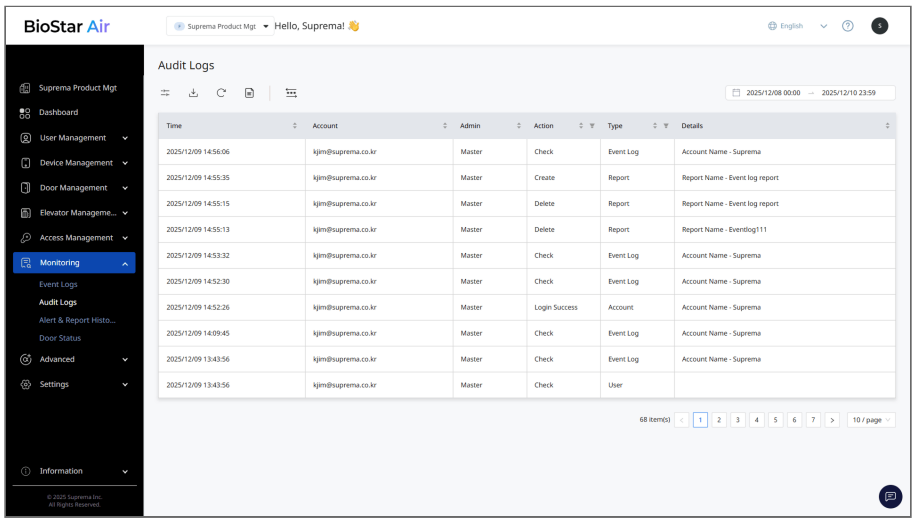
Use Audit Logs

One of the key advantages of a cloud access control platform is the ability to monitor site activity anytime, anywhere. This document explains how to monitor and analyze audit logs in BioStar Air.

> **Tip**
>
> Watch the following video for a tutorial on audit logs.

View audit logs

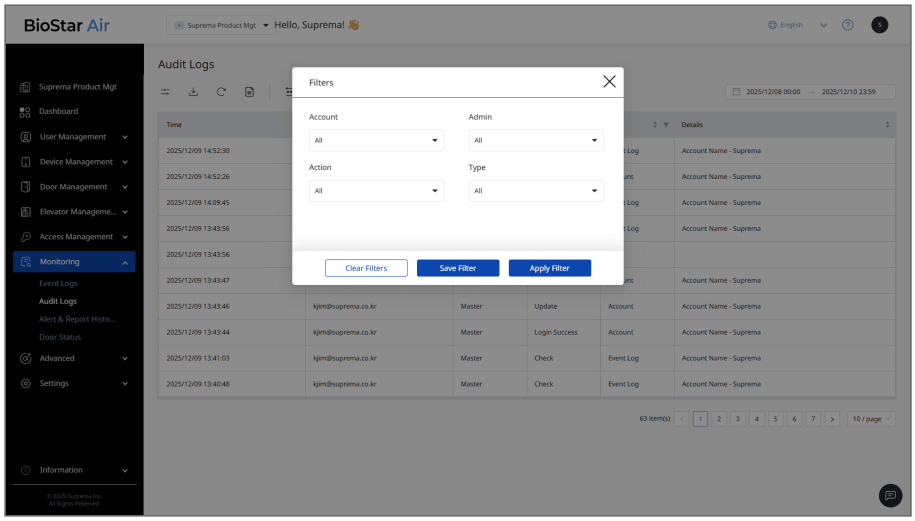
Go to **Audit Logs** to view audit logs. Click **Monitoring** → **Audit Logs** in the left sidebar.



Use **Audit Logs** to track administrator actions. Each log in the list displays a table with information such as operation time, email address, administrator privileges, operation type, menu path, and operation details.

Filter logs

Filter logs to quickly find the information you need. Click ⇥⇤ at the top of the log list. When the **Filters** window appears, select the desired value for each item.



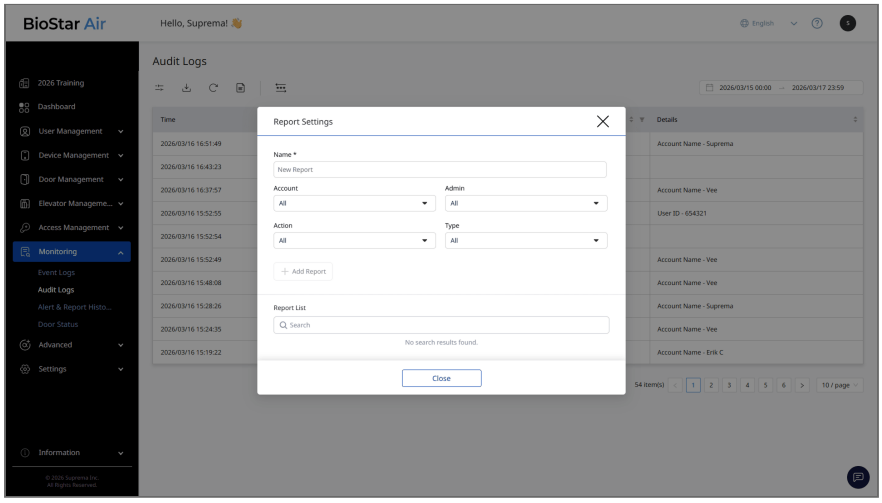
Info

- Click **Save** or **Save Filter** to save the settings so they remain after navigating to another menu. Click **Apply** or **Apply Filter** to apply the changes only to the current list; they will revert when you navigate away.
- **Reset** or **Clear Filters** to cancel the changes and return to the initial state.

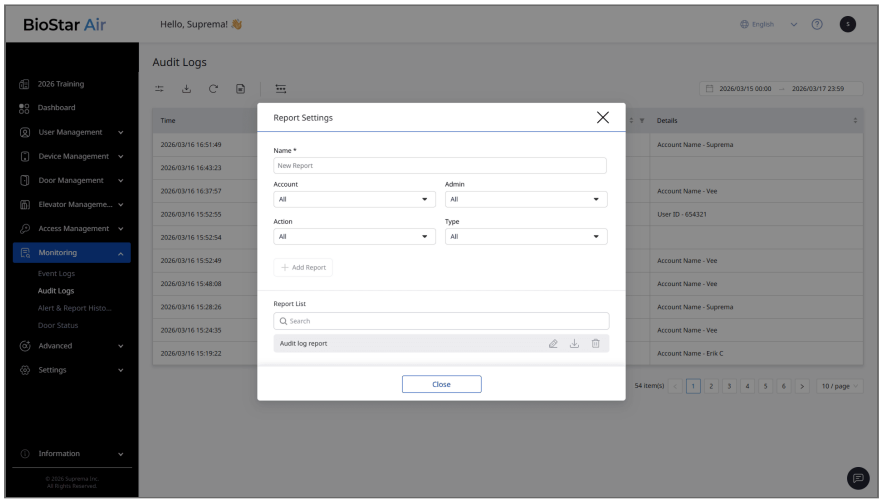
Configure reports

Generate reports for events that occurred during a specific period by filtering log data.

1. Click the button at the top of the log list.
2. When the **Report Settings** window appears, enter a report name.

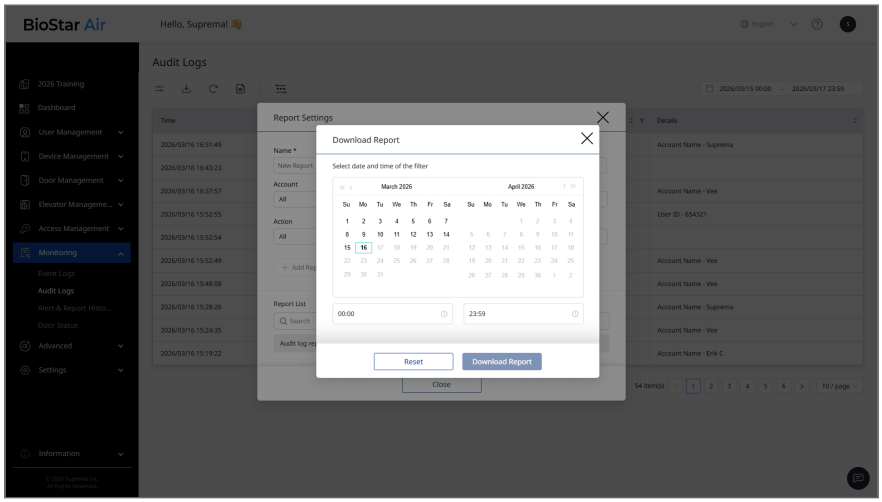


3. Select the items to include in the report.
4. Click **Add Report** to save the configured report.
5. A report is created with the name set in **Report List**.



6. To download the generated report, click the button next to the report name.

7. When the **Download Report** window appears, select the period to query events and click **Download Report**.



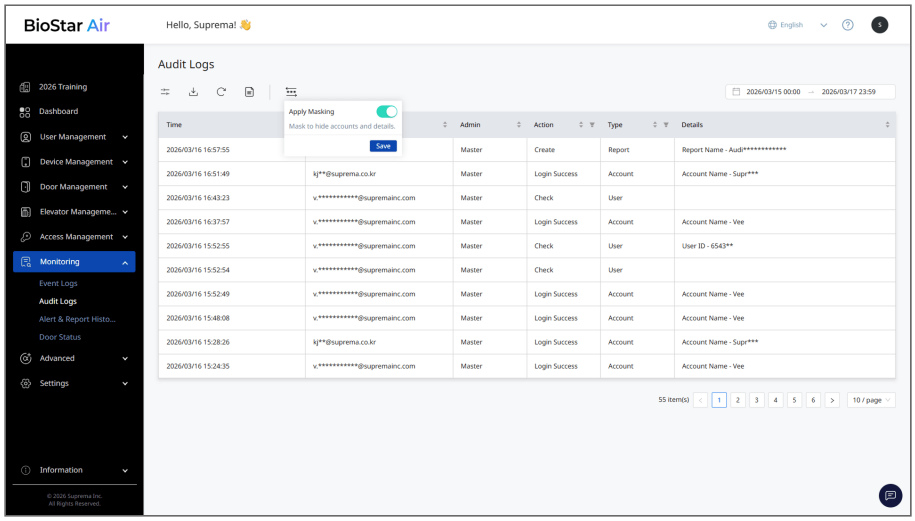
A download link is sent to the administrator's email.

> **Info**
>
> **Report List** lets you search for, edit, download, or delete the reports created.

Mask personal data

Mask personal data in logs to protect sensitive information. When personal data masking is enabled, information such as user names, email addresses, and phone numbers is partially hidden.

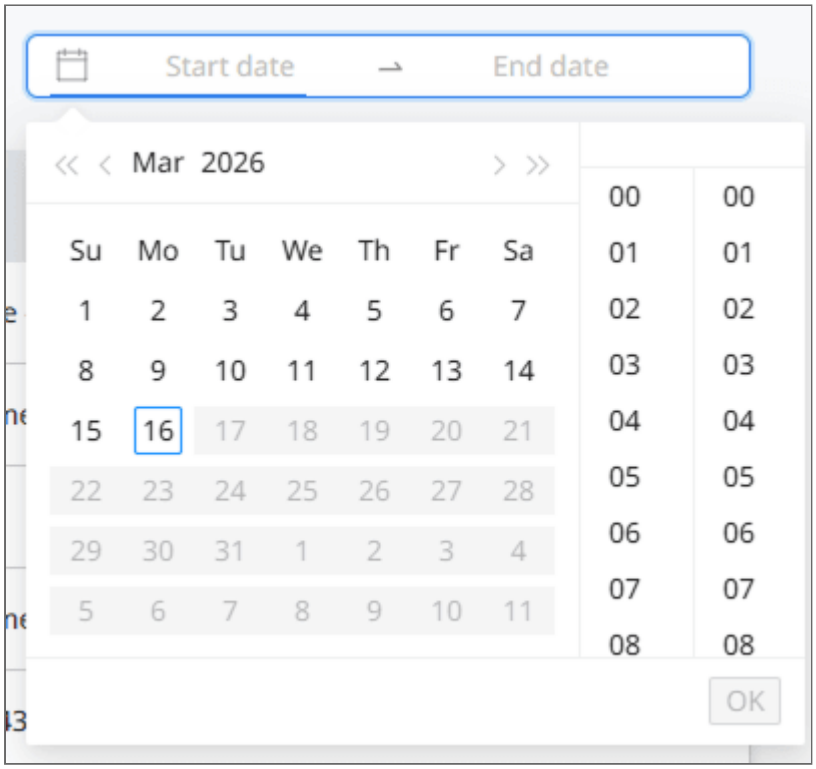
To enable personal data masking, click the button at the top of the log list. In the pop-up menu, enable **Apply Masking** and click **Save**.



Other features

Use the toolbar at the top of the log list to manage logs more efficiently.

- To sort logs by date, select a date and time range, then click **OK**.



- Click ⬇ to save logs as a CSV or PDF file.
- Click ↻ at the top of the list to refresh the log list.

Check Alert & Report History

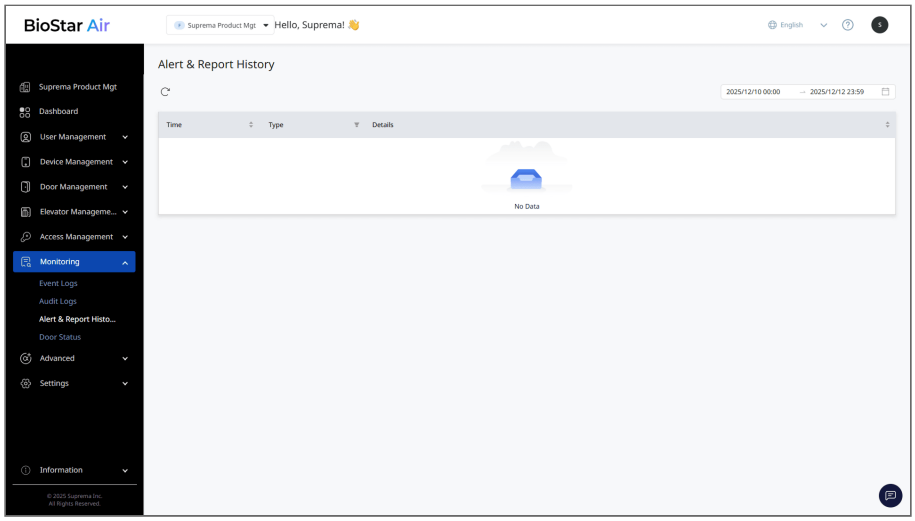
Learn how to check the history of alerts and reports generated in BioStar Air. Administrators can view past alerts and generated reports through the web portal and mobile app.

Before you start

The alert and report history shows only items generated by the alert and report rules configured in **Settings** → **Alert & Report History**. For more information on setting rules for creating alerts and reports, refer to Set Up Alerts and Reports.

Check alert and report history

On the left sidebar, click **Monitoring** → **Alert & Report History**. The alert and report history appears.



- View the time, type, and details of each generated alert or report in the list.
- Click the date range area in the top-right corner of the screen, set the desired period, and filter the alert and report history within that period.
- Click ↻ at the top of the list to refresh the list.

Monitor Door Status

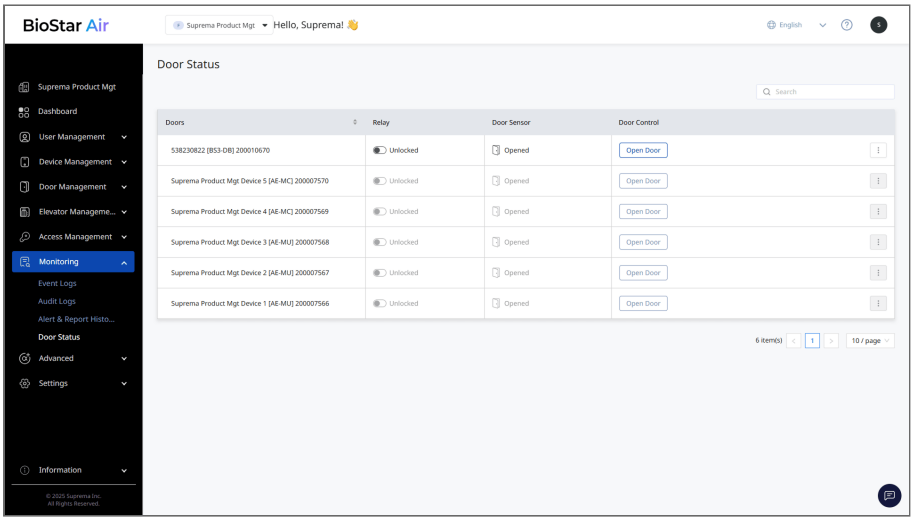
Monitor the status of doors connected to BioStar Air in real time. Check whether a door is locked or unlocked and the status of its relay sensor, and lock or unlock it remotely to control access.

> **Tip**
> Refer to the following video to watch the video guide on monitoring door status.

Door status monitoring

Web

Monitor door status in the BioStar Air web portal. Click **Monitoring** → **Door Status** in the left sidebar. View the list of doors registered to BioStar Air.

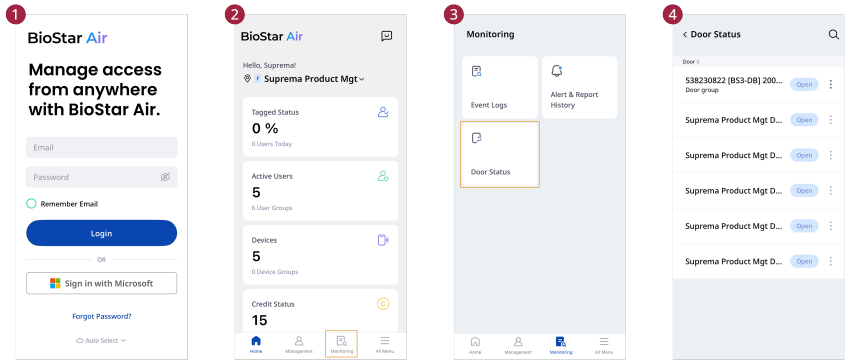


Check the following items for each door.

- **Relay**: Indicates whether the door is locked or unlocked.
- **Door Sensor**: Indicates whether the door is physically open or closed.

Mobile

Monitor door status using the BioStar Air app on a mobile device.



1. Open the BioStar Air app on your mobile device and log in.
2. Tap **Monitoring** at the bottom of the home screen.
3. Tap the **Door Status** card.
4. View the list of doors registered to BioStar Air.

> **Info**
> For more information on door registration and management, refer to Manage Registered Doors.

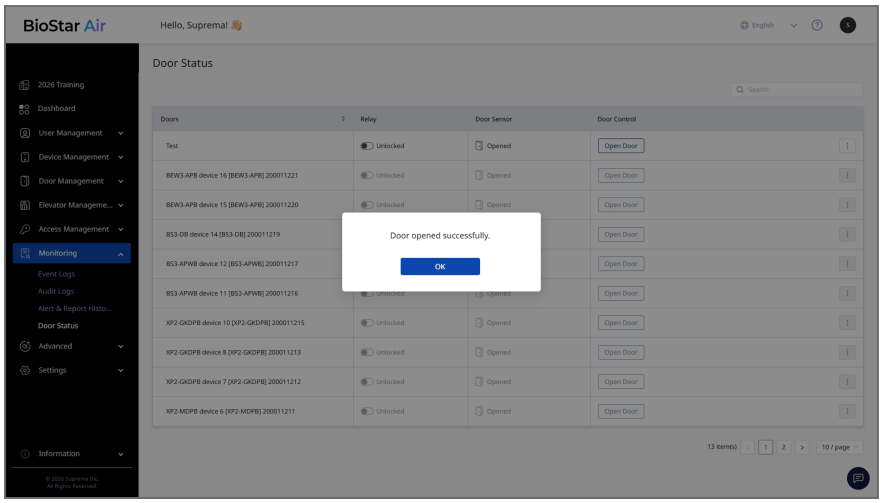
Unlock a door

Unlock the door remotely when it is online and connected to BioStar Air.

Web

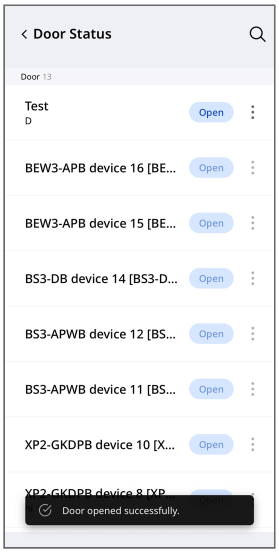
1. In the **Door Control** column, click **Open Door**.

2. The status in the **Relay** column changes to unlocked, and a success message appears.



3. After the configured time elapses, the door returns to locked.

Mobile



1. Tap **Open Door** to remotely unlock the door.
2. A success message will appear at the bottom of the screen.
3. After the configured time elapses, the door returns to locked.

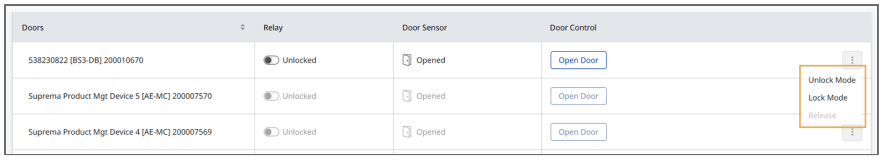
> **Info**
> For information on setting the duration that the door remains open, refer to Manage Registered Doors.

Set always-open mode

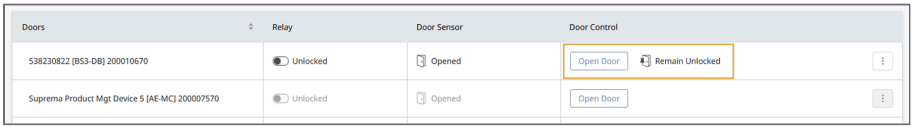
Keep a door unlocked indefinitely. Use this when temporary or visitor access is needed.

Web

1. In the door list, click ⋮ at the far right of the door to keep open.

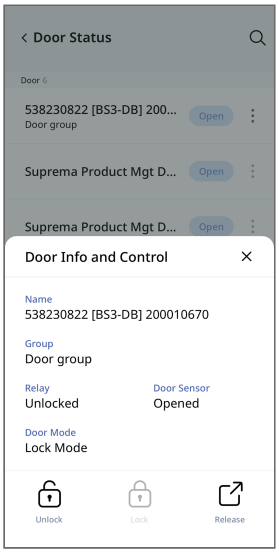


2. Click **Unlock Mode** in the popup menu.
3. The status in the **Door Control** column changes to **Remain Unlocked**.



Click ⋮ → **Release** to return to normal operation.

Mobile



1. Tap ⋮ at the far right of the door.
2. When the **Door Info and Control** option appear, tap **Unlock**.
3. A success message will appear at the bottom of the screen.

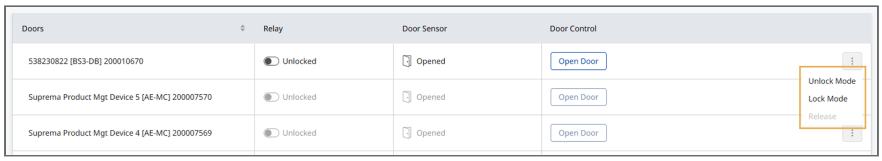
Tap ⋮ → **Release** to return to normal operation.

Set lock mode

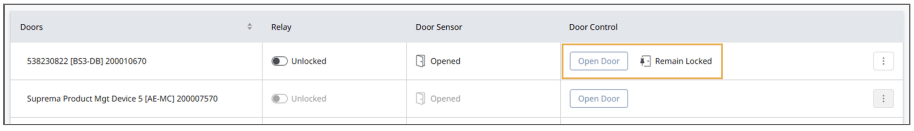
Keep a door locked regardless of the current schedule. Use this when enhanced security is required.

Web

1. In the door list, click ⋮ at the far right of the door to keep locked.

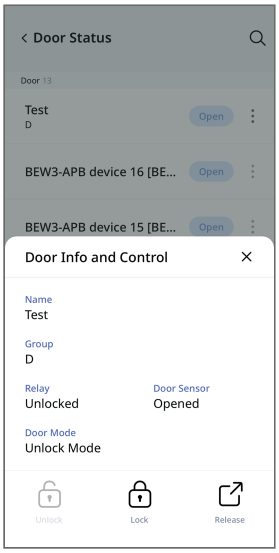


2. Click **Lock Mode** in the pop-up menu.
3. The status in the **Door Control** column changes to **Remain Locked**.



Click ⋮ → **Release** to return to normal operation.

Mobile



1. Tap ⋮ at the far right of the door.
2. When the **Door Info and Control** option appear, tap **Lock Mode**.
3. A success message will appear at the bottom of the screen.

Tap ⋮ → **Release** to return to normal operation.

Safety

BioStar Air's Safety Management features help track people on site during normal operations and manage evacuations during emergencies. Presence, including **On-Site Now** and **Zones**, gives administrators a real-time view of which credential holders are on site and where they are within the site. Administrators can also manually update a person's presence status.

Roll Call supports orderly evacuations by allowing designated administrators to take responsibility for specific muster points and oversee the safety of the people assigned to them. It uses the same on-site presence engine as **On-Site Now**.

Refer to the following documents to learn how to manage Presence and Roll Call in the BioStar Air portal.

Check Presence

The **Safety** → **Presence** menu shows users currently on site in real time. The presence status is calculated based on authentication logs from the entry and exit devices set in **Perimeter**. If Perimeter is not set yet, see Manage Zones first.

How presence status is determined

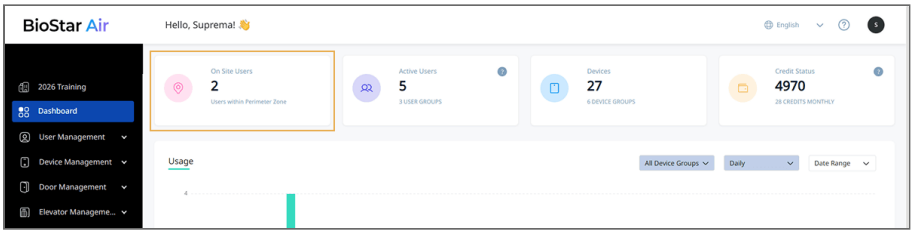
When users authenticate at an entry device in the perimeter zone, their status changes to **On Site**. When they authenticate at an exit device, it changes to **Off Site**.

- For sites without an exit device in the perimeter zone, always set **Off-site timer**. If users are inactive for the set time, their status automatically changes to **Off Site**.
- For how to set entry and exit devices for the perimeter zone and the **Off-site timer** setting, see Manage Zones.
- Administrators can see the list and number of people on site from several menus:
  - **Dashboard** widget
  - **Safety** → **Presence**
  - **Zone Management** → **Zones** → **People Inside** (Perimeter)

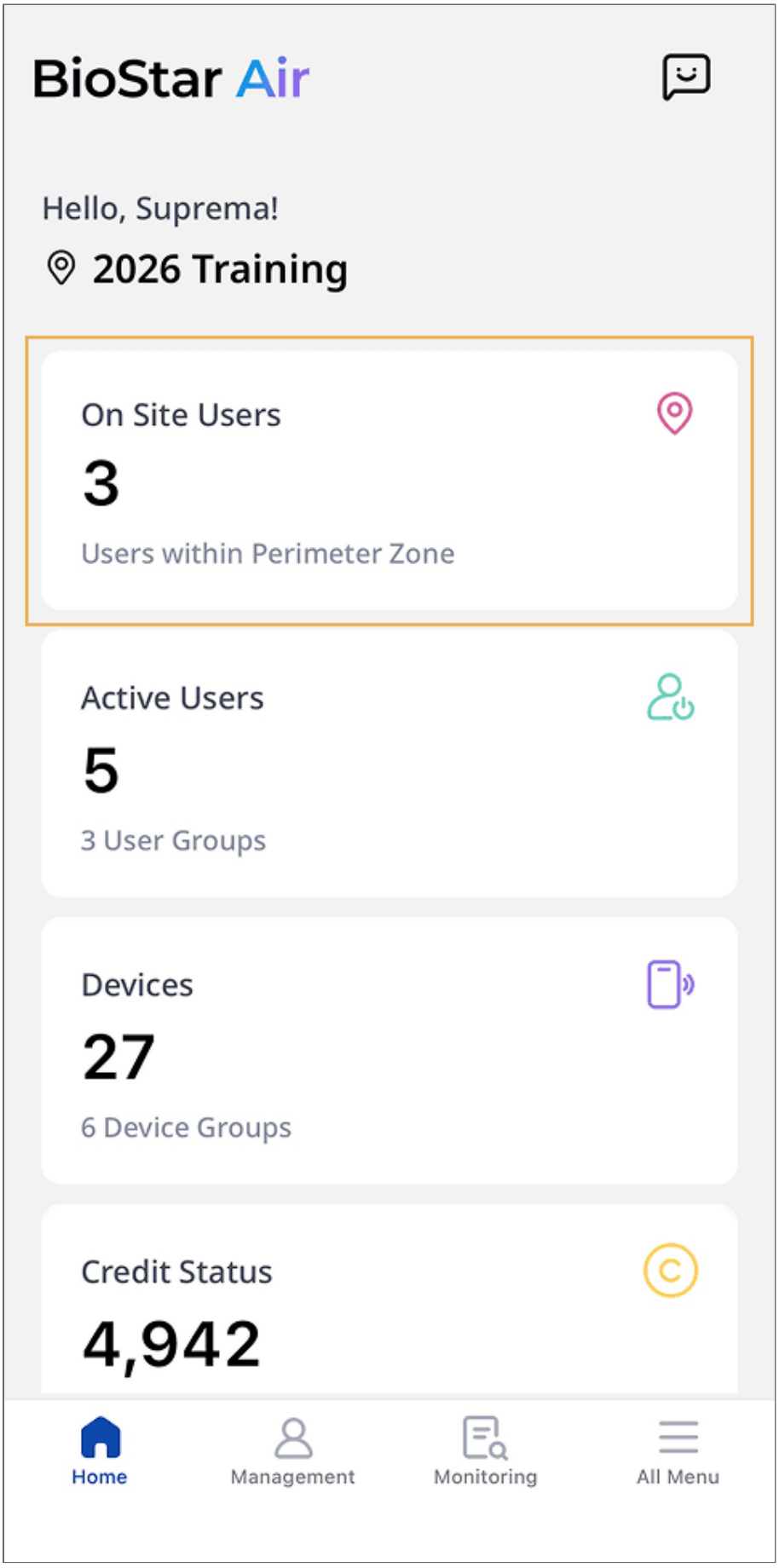
Check on the dashboard

The **Dashboard** menu also shows the number of users currently on site in the **On Site Users** card.

Web


BioStar Air
Hello, Suprema!
English
2026 Training
Dashboard
User Management
Device Management
Door Management
Elevator Manageme...
On Site Users
2
Users within Perimeter Zone
Active Users
5
3 USER GROUPS
Devices
27
6 DEVICE GROUPS
Credit Status
4970
28 CREDITS MONTHLY
Usage
All Device Groups
Daily
Date Range

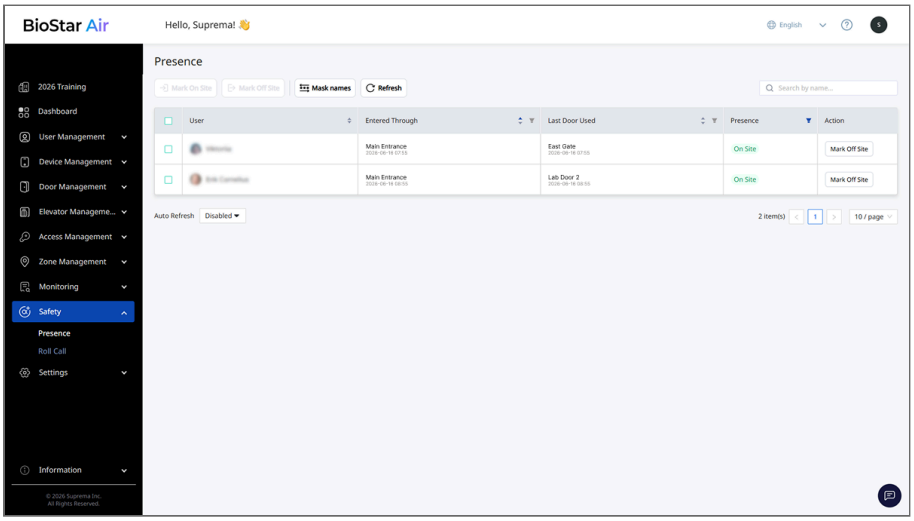
Mobile


BioStar Air
Hello, Suprema!
2026 Training
On Site Users
3
Users within Perimeter Zone
Active Users
5
3 User Groups
Devices
27
6 Device Groups
Credit Status
4,942
Home
Management
Monitoring
All Menu

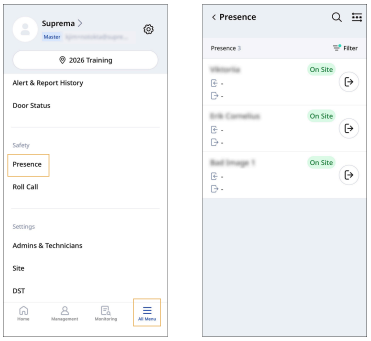
Explore presence list

Web

On the left sidebar, click **Safety** → **Presence**.



Mobile



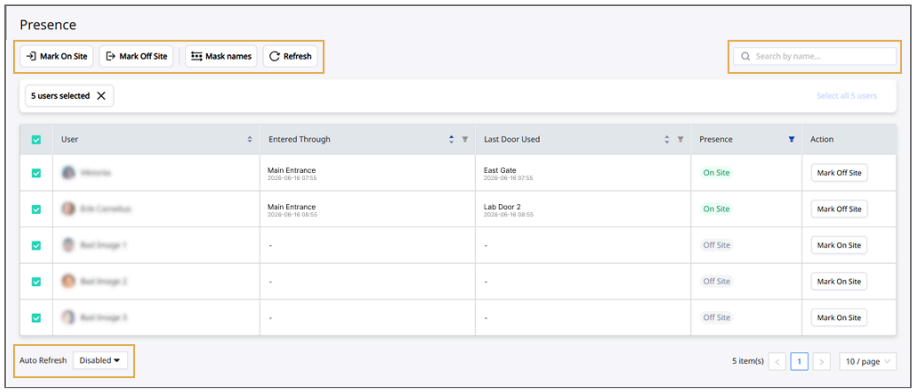
1. Open the BioStar Air app on your mobile device and log in.
2. Tap **All Menu** → **Presence** at the bottom of the screen.

By default, the presence list shows only users with the **On Site** status.

- **User**: The user's profile photo and name.
- **Entered Through**: The entry device and time when the user authenticated to enter the site.
- **Last Door Used**: The most recently used door and time.
- **Presence**: The user's current presence status (**On Site** / **Off Site**).
- **Action**: Change the user's presence status.

Presence list management

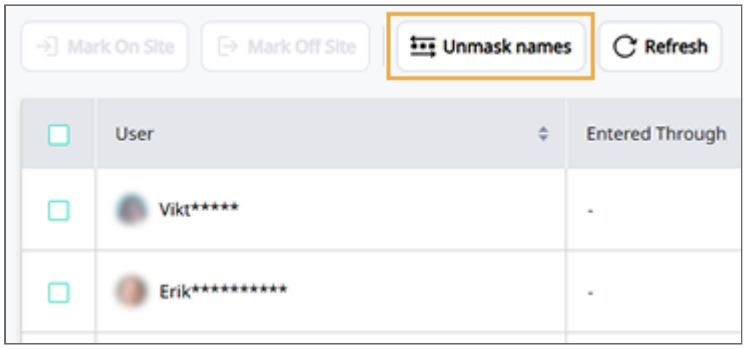
Use the management features at the top and bottom of the list to perform the following tasks.



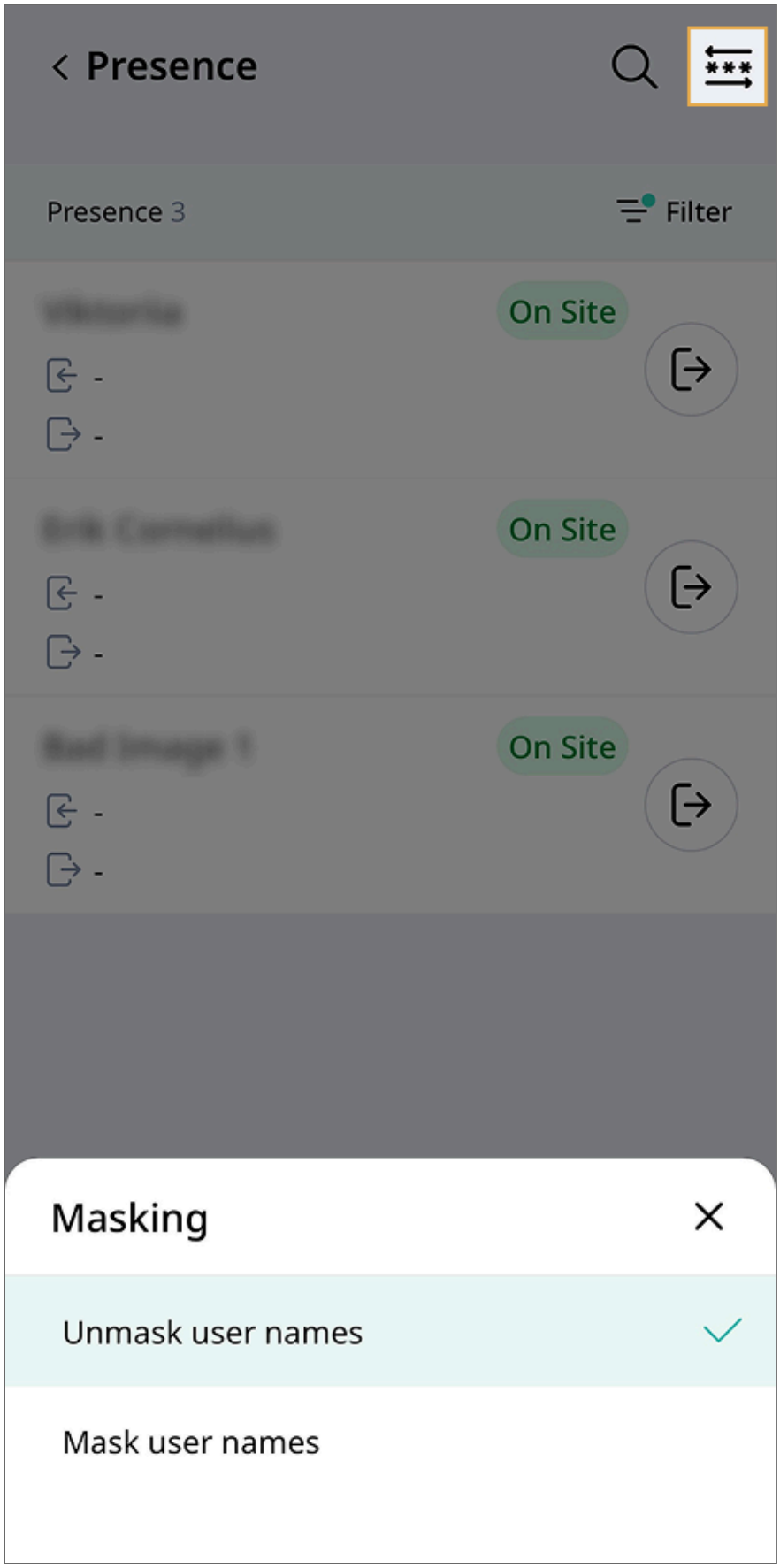
- **Mark On Site** / **Mark Off Site**: Change the user's presence status to On Site or Off Site. For more information, see Manually change presence status.

- **Mask names** / **Unmask names** (***): Hide or show user names. Useful when sharing the screen in sensitive environments.

Web



Mobile

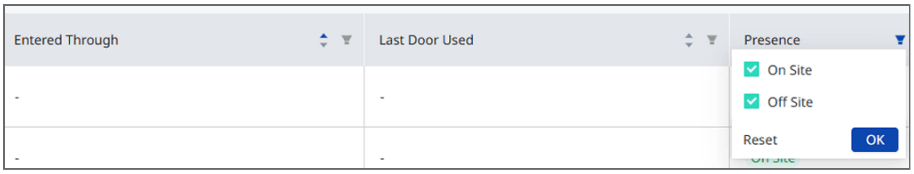


- **Refresh**: Refresh the list immediately to show the latest status. In **Auto Refresh** at the bottom of the list, select an auto refresh interval (**Disabled** / **5 Seconds** / **1 Minute**). The list refreshes automatically at the set interval.
- **Search by name...**: Search the list by user name.

Filter presence list

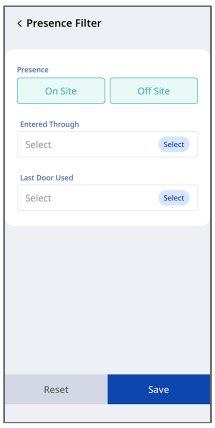
Web

In the **Presence** column, click the button to filter the list by **On Site**, **Off Site**, or all users. Also filter by selected criteria in the **Entered Through** and **Last Door Used** columns.



> **Info**
> Click **Reset** to clear the filter.

Mobile



1. Tap **Filters** at the top right of the presence list.
2. Select **On Site** or **Off Site**, or select both.
3. Select criteria in **Entered Through** and **Last Door Used**.
4. Tap **Save** to filter the list by the selected criteria.

> **Info**
> Tap **Reset** to clear the filter.

> **Info**
>
> - To view all users, select both **On Site** and **Off Site** in the **Presence** column.
> - The presence list shows users in **On Site** status by default.

Manually change presence status

When actual conditions differ from the presence status recorded in the system, an administrator can change the status.

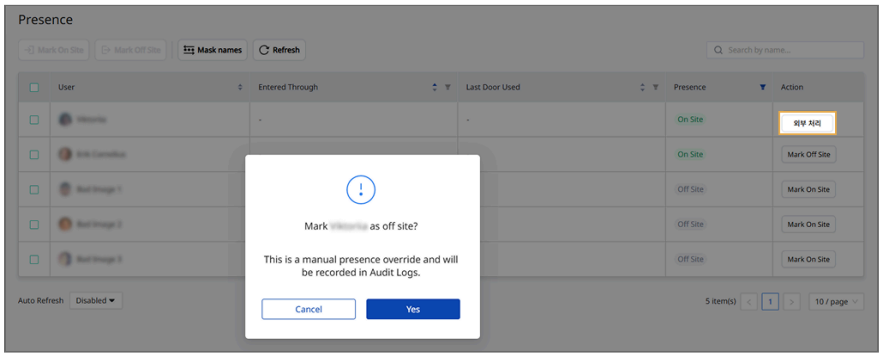
- Presence accuracy varies depending on the site's entry and exit device setup. Sites with clearly defined entry and exit devices provide more reliable presence information.
- If a device goes offline or event delivery is delayed, the presence status may update after synchronization completes.
- Presence status differs from access permissions. Users shown as **On Site** cannot necessarily access every door.
- Users with expired, inactive, or suspended accounts cannot change presence status until the account is active.

> **Info**
>
> Manual changes only update the status recorded in the system. They do not physically verify a user's location. Check the change history in **Monitoring** → **Audit Logs**.

Change a user's presence status

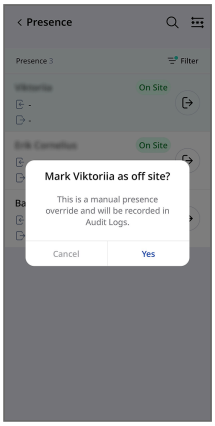
Web

1. In the user's **Action** column, click **Mark On Site** or **Mark Off Site**.



2. When the confirmation message appears, click **Yes**.

Mobile

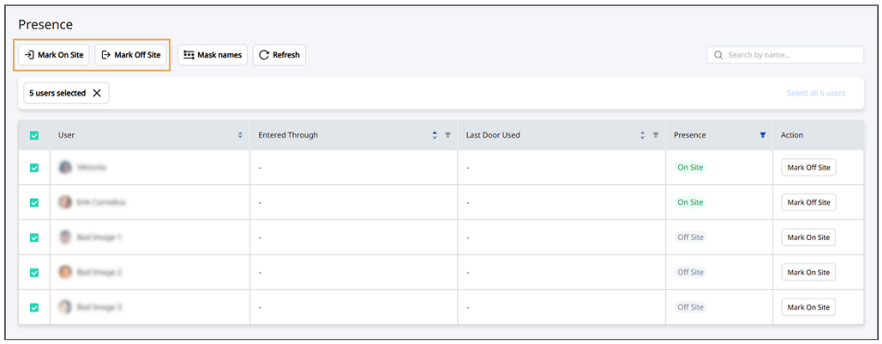


1. In the list, tap ⎋ or ⎆ next to the user to change status.
2. When the confirmation message appears, tap **Yes**.

Change presence status for multiple users

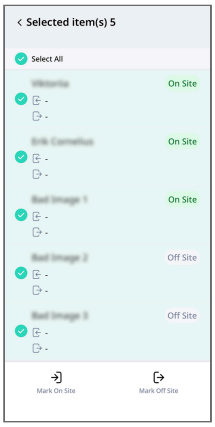
Web

1. Click the checkbox for each user to change presence status. Select one or more users.
2. Click **Mark On Site** or **Mark Off Site** at the top of the list.



3. When the confirmation message appears, click **Yes**.

Mobile



1. Touch and hold the user in the list to change their status.
2. Select the user to change the status. Select one or more users.
3. Tap **Mark On Site**( ) or **Mark Off Site**( ) at the bottom of the screen.
4. When the confirmation message appears, click **Yes**.

Roll Call

With BioStar Air's Roll Call feature, organizations can track which users have safely evacuated during an emergency. Set muster points and run a roll call in the BioStar Air mobile app. Administrators can quickly identify on-site users based on presence information and confirm safety.

Accurate muster lists based on Presence

- Roll call does not assume all users are on site. Using Presence logic, include only users confirmed to be on site at the time of the emergency as roll call targets.
- Assign user groups to muster points and designate dedicated administrators. Safety managers can focus on assigned users.
- The Suprema Pass app guides mobile credential users on site to the correct muster point and warns off-site users not to enter the facility during an emergency.

Info

- Ensure that muster points are correctly assigned to user groups to avoid confusion.
- Regularly test the roll call feature to ensure smooth operation during a real emergency.
- Use access events to verify attendance for safety compliance.

Tip

Watch the following video for a roll call and muster point guide.

Before you start

- Roll call accuracy depends on presence detection. If **Perimeter** is not set correctly, the roll call list may differ from the actual on-site headcount.
- Mobile notifications require the Suprema Pass app. Users who use only RF cards or biometric credentials cannot receive mobile roll call notifications.
- On-site users not assigned to a muster point may not receive guidance.
- If the **Assigned Admins** setting is incorrect, the expected roll call screen may not appear for administrators.
- If a device goes offline or event delivery is delayed, it can affect presence information and roll call accuracy.
- Inactive users do not receive roll call notifications.

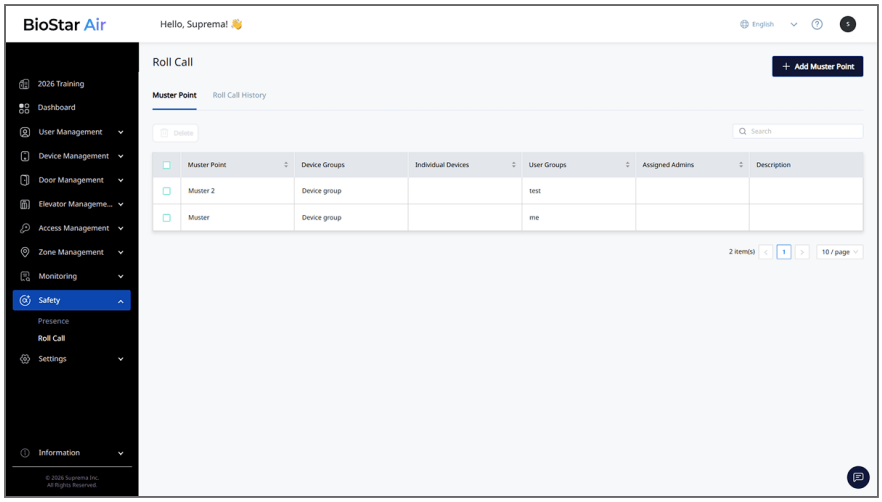
Info

Users and administrators who use earlier versions of the Suprema Pass or BioStar Air app can continue using the legacy roll call method. Update to the latest version to use the new features.

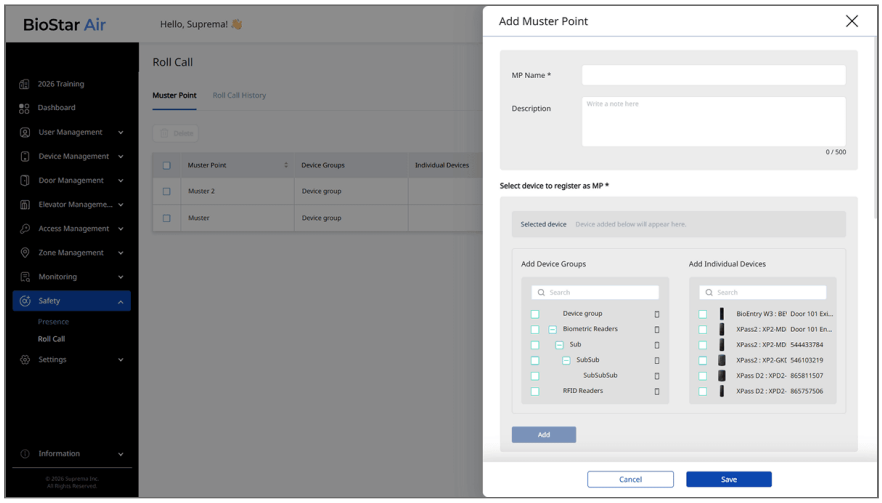
Set muster points

A muster point is a designated location where users authenticate their credentials to indicate they are safe during an emergency.

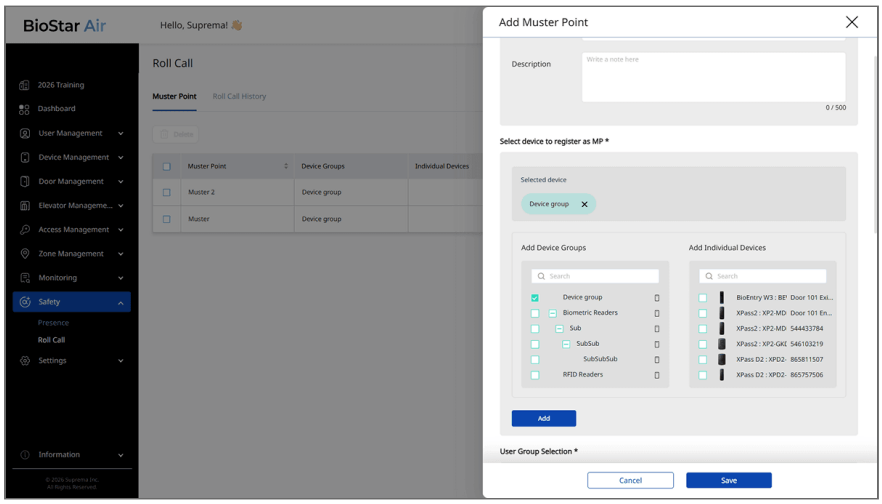
1. Click **Safety** → **Roll Call** on the left sidebar.
2. Click **Add Muster Point** at the top right of the screen.



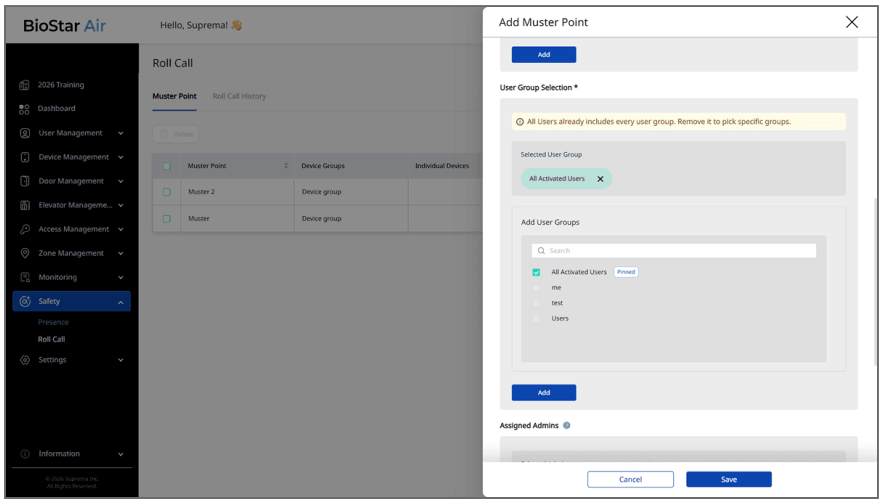
3. Enter the muster point name and description (optional) when the **Add Muster Point** panel appears.



4. In the **Select device to register as MP *** section, add the device group or device to assign to the muster point. Select the checkbox for the device group or device, and click **Add**.

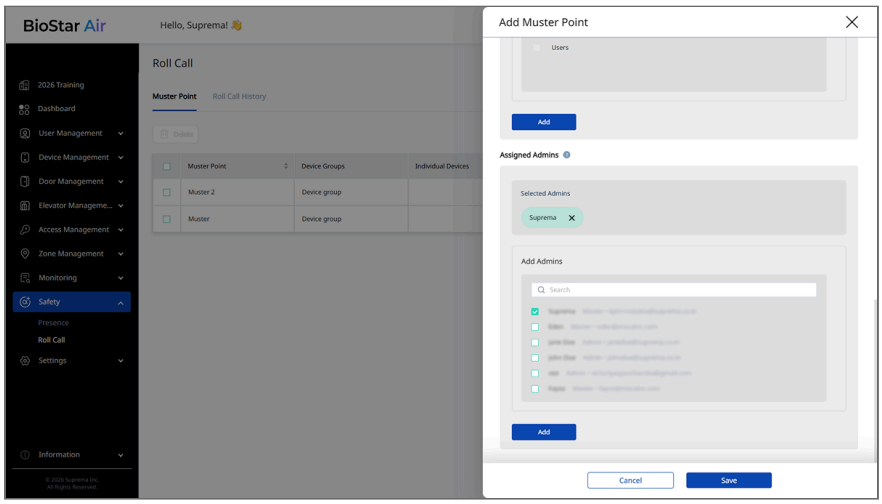


5. In the **User Group Selection *** section, select the user groups that must report when they arrive at the muster point.



- Select the checkbox for the group, and click **Add**.
- **All Activated Users**: Assigns all currently active users on BioStar Air site to a chosen muster point. Running a roll call does not assume all active users are on site. It targets only users with confirmed on site status based on presence detection. Enabling this option disables the ability to choose individual user groups. Disable this option first to select only certain user groups.

6. In the **Assigned Admins** section, select the checkbox for the administrator who will run Roll Call at the muster location, then click **Add**.



- If you select **Assigned Admins**, only the selected administrators can start the Roll Call. During an ongoing Roll Call, they can view and manage only users in their assigned muster points.
- If you do not assign **Assigned Admins**, users with the **Master**, **Admin**, or **Operator** role can start Roll Call.
- An administrator cannot be assigned as the designated administrator for multiple muster points at the same time.

7. Click **Save** to save the muster point settings.

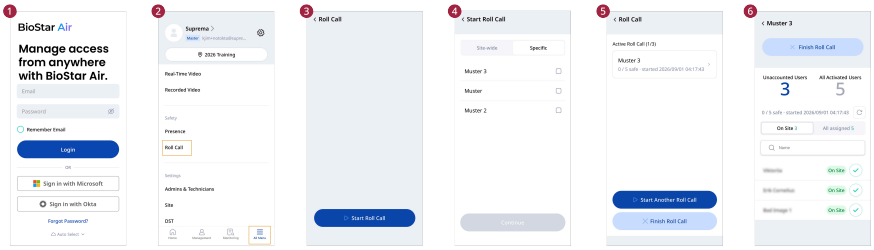
Best practices for muster points

- Make the muster point name and description clear and easy to understand. For example, use names like 'East Parking Lot' or 'Main Building Lobby'.
- When adding multiple devices to a muster point, select a device group instead of individual devices. Device groups let you manage multiple devices at once. For more information on device group management, refer to Manage Device and Panel Groups.
- In a large campus with multiple buildings, assign **only relevant users** to a specific muster point.
- Wired access control devices support both mobile and card authentication, whereas Airfob Tag and Airfob Patch support only mobile credentials.

Start roll call

Start on mobile

Start a roll call and check attendance in the BioStar Air mobile app.



1. Open the BioStar Air app on your mobile device and log in.
2. Tap **All Menu** → **Roll Call** at the bottom of the screen.
3. Tap **Start Roll Call**.
4. Select the muster point to start Roll Call, then tap **Continue**.

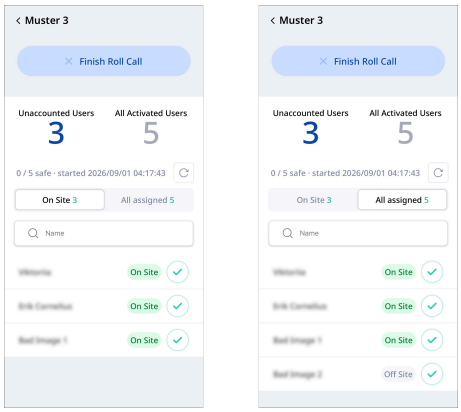
   To run Roll Call in all muster points, select **Site-wide**, then tap **Continue**.
5. Select a muster point in the ongoing Roll Call list.
6. A list of all users who must gather at the muster location appears.

Differences by administrator role

- **Master**, **Admin**, and **Operator** users can view the Roll Call list. This applies when they are not assigned as **Assigned Admins** for the muster point. They start new Roll Calls in the order listed above.
- **Assigned Admins** receives a notification when Roll Call starts in the assigned muster point. Tap the notification to go directly to the progress screen for the assigned muster point.

Explore the active Roll Call screen

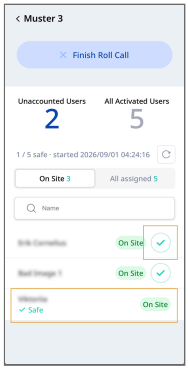
When Roll Call starts, the progress status appears with the muster point name.



- At the top of the screen, check the number of **Unaccounted Users** and **All Activated Users**.

  Below the headcount, **people marked Safe/total people** and the **Roll Call start time** appear. Tap the refresh (↻) button to check the latest status.
- Switch the user range shown in the list.
  - **On Site**: Shows only users whose Presence status is On Site.
  - **All assigned**: Shows all users assigned to this muster point, regardless of Presence status. Users marked Safe move to the bottom of the list.
- Use search to find a certain user.
- On the right of each user in the list, check Presence status (**On Site** / **Off Site**).

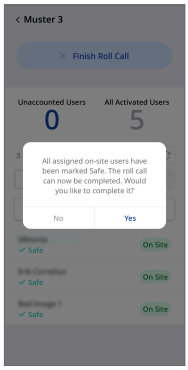
Mark users safe



Administrators or users can mark themselves safe in the following ways.

- An administrator can touch and hold the **check mark** next to a user's name in the mobile app to mark the user safe.
- Users tag their credential on a device at the assigned muster point.

Complete roll call



Complete the roll call when any of the following conditions are met.

- When the completion message window appears because the number of On Site users—that is, **Unaccounted Users**—included in the Roll Call scope becomes 0, tap the **Yes** button
- When the administrator manually marks all users as safe and taps the **Finish Roll Call** button
- 24 hours have passed

End scope by role

- The site master can end Roll Calls individually one by one, select multiple calls to end at once, or end all ongoing Roll Calls at the site at once.
- Admin or Operator selected in **Assigned Admins** can end only Roll Calls for the zones they manage.

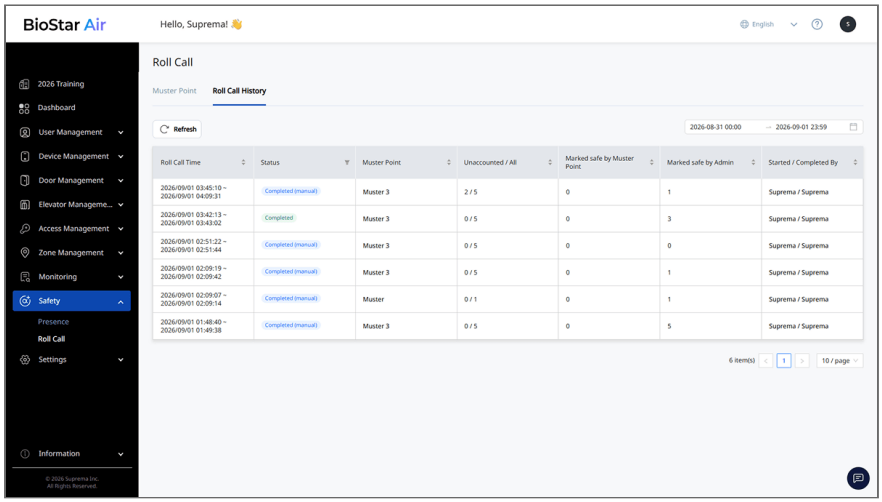
Info

Manually mark users in the **Off Site** status as safe. For example, mark users working from home that day as safe in advance.

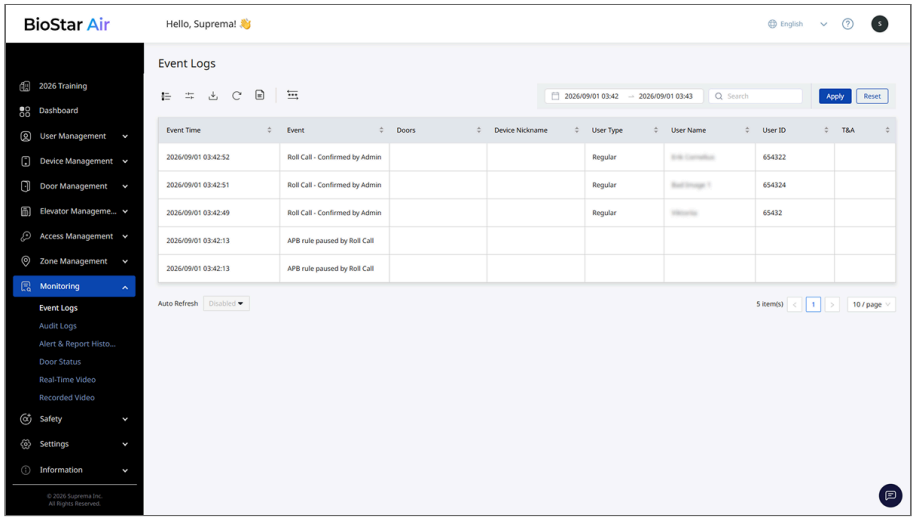
View roll call history

View the history of previous roll calls.

1. Click **Safety** → **Roll Call** on the left sidebar.
2. Click the **Roll Call History** tab.



3. Click a completed roll call entry to view its details.



- View the list of all access events recorded during the roll call.
- Check whether each user was marked safe or unconfirmed.
- Check the start and end times of the roll call.

Configure Site Settings

Manage the basic settings required to operate BioStar Air. Configure the system to meet organizational requirements by managing admin accounts with operating privileges, setting basic organization information, configuring time zones and alerts, customizing email templates, and defining card formats.

Tip

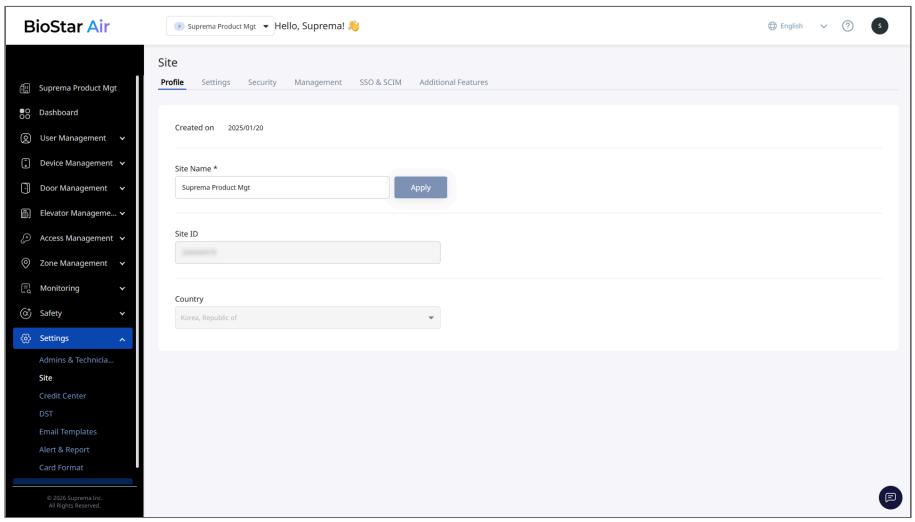
Refer to the following video to watch a guide on site settings.

Profile Settings

Site information is the most basic setting in BioStar Air. This guide explains how to manage basic information, such as the site name and identifier, and how to delete a site when necessary.

Set site information

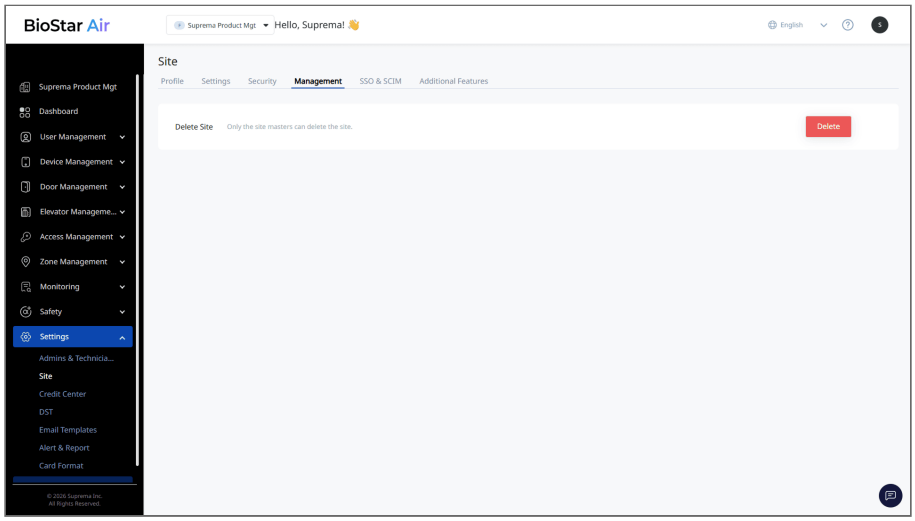
Click **Settings** → **Site** in the left sidebar. Use the **Profile** tab to modify the site's basic information.



- **Site Name**: The site name. Enter a new name and click **Apply**. Change it at any time.
- **Site ID**: A unique identifier required for support requests. Copy and provide the site ID when communicating with the MOCA team.
- **Country**: Set when the site is created and cannot be changed later. Request changes through the BioStar Air Partner Portal.

Delete Site

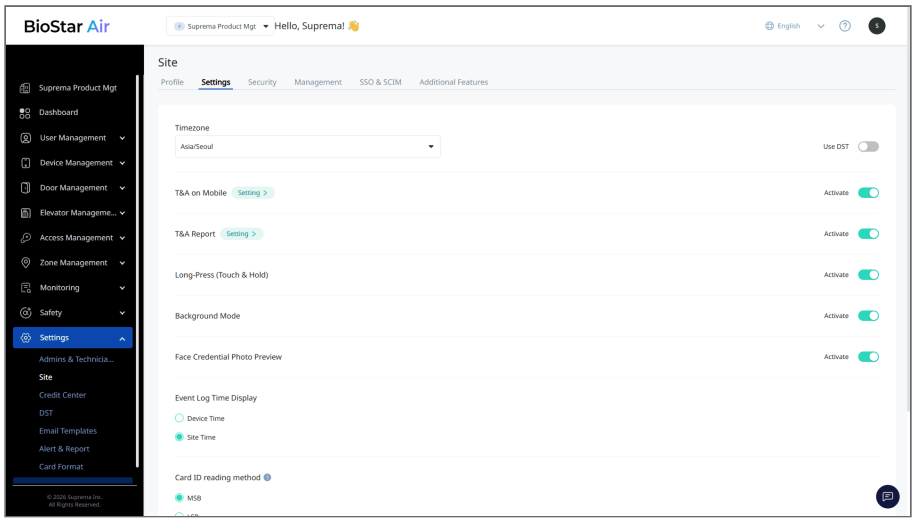
Click **Settings** → **Site** in the left sidebar. The only option available in the **Management** tab is **Delete Site**. This action is irreversible, and only the **master administrator** can delete a site.



Advanced Settings

Configure advanced options to optimize BioStar Air for your organization's work environment. Set the time zone and daylight saving time, enable time and attendance, and adjust mobile authentication methods and how event logs are displayed.

Click **Settings** → **Site** in the left sidebar. Use the **Settings** tab to configure site settings.



- **Timezone**: Change the time zone at any time. The system records logs and events based on the configured time zone. For more information, refer to Daylight Saving Time (DST).
  - **Use DST**: Enable or disable daylight saving time for specific regions.
- **T&A on Mobile**: Enable the time and attendance (T&A) feature. After enabling the T&A feature, click **Setting** to configure detailed settings. For more information, refer to Time & Attendance (T&A).
- **T&A Report**: Generate time and attendance (T&A) reports. After enabling the report feature, click **Setting** to configure report conditions. For more information, refer to Time and Attendance Report.
- **Long-Press (Touch & Hold)**: Enable the Long Touch feature to remotely open doors from a certain distance.
- **Background Mode**: Allow mobile cards while the Suprema Pass app runs in background mode. When enabled, users can open a door without launching the app.
- **Face Credential Photo Preview**: Show a face preview when issuing face credentials.
- **Event Log Time Display**: Set how event log times are displayed.
  - **Device Time**: Show event logs based on each device's time zone.
  - **Site Time**: Show logs according to the site's time zone. Useful when all devices are in one location. See the **Timezone** option.
- **Card ID reading method**: Configure how card data is transmitted when using Airfob Patch with third-party readers.

> This setting applies only to patch devices and can be adjusted to match the type of third-party device to which the patch is attached.

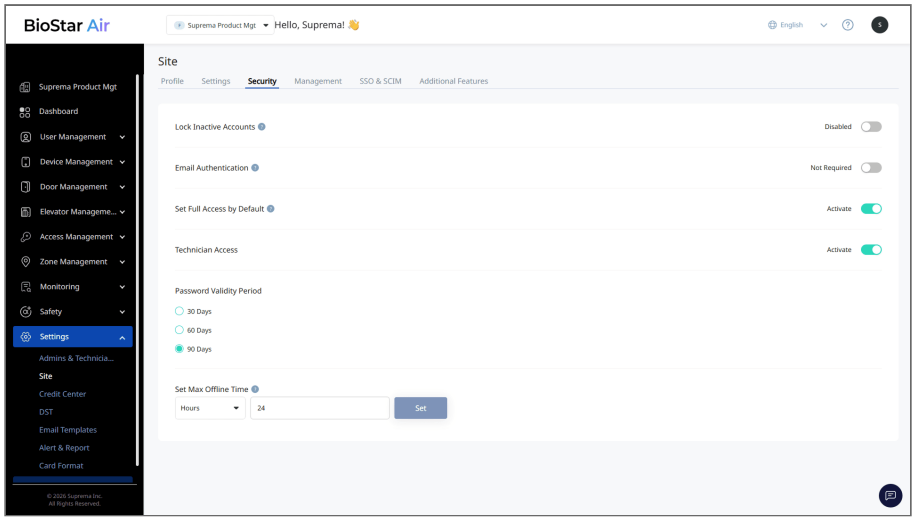
- **Validity Period for Mobile Access Card Activation/Reissue Link**: Set the default validity period for mobile credentials.

> Admins can set a separate expiration date for each user's credentials. For more information, refer to Add Users.

Security Settings

Configure security policies properly to prevent unauthorized access and keep the site secure. You can strengthen site security by locking inactive administrator accounts, enabling email-based 2-factor authentication, and setting password change intervals.

Click **Settings** → **Site** in the left sidebar. Use the **Security** tab to configure site security settings.



- **Lock Inactive Accounts**: Lock administrator accounts that have been inactive for more than 90 days.
- **Email Authentication**: Require email two-factor authentication each time an administrator signs in.
- **Set Full Access by Default**: Grant 'full access' to new users by default when no other access rights are selected. If this setting is disabled, assign access levels manually. Temporary users are not granted full access automatically even if the setting above is enabled.

  > For more information about access levels, see Manage Access Levels.

- **Technician Access**: Allow technician accounts to access the site. If this setting is disabled, technician accounts cannot access the site.

  > For more information on managing site access for technician accounts, see Assign Technicians to a Site.

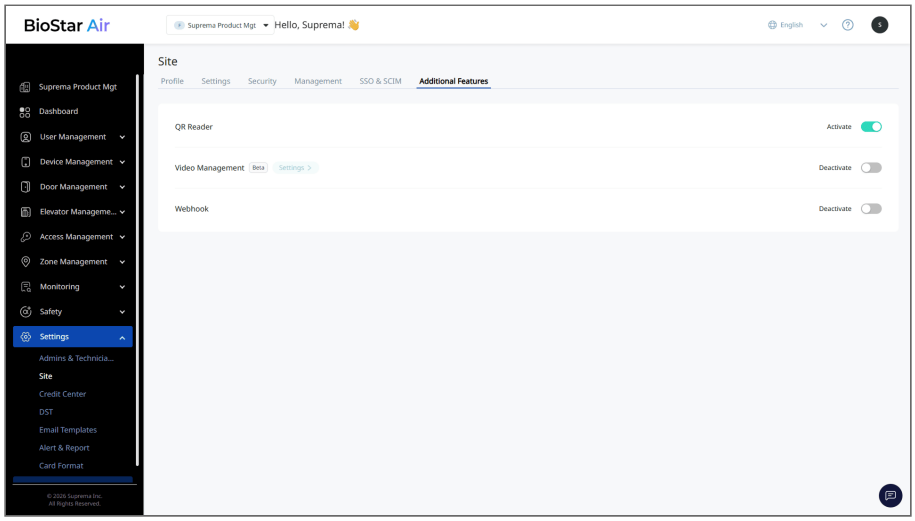
- **Password Validity Period**: Require password reset every 30, 60, or 90 days.
- **Set Max Offline Time**: Set how long mobile credentials remain valid when the device is offline.

  > – The default is 5 minutes and can be set from 1 minute to 8 days.
  > – This helps balance security and convenience, especially at remote sites with limited network connectivity.

Settings for Additional Features

You can enable or disable additional features required for site operation, such as support for QR code readers, ONVIF camera integration, and event forwarding to external systems (webhooks).

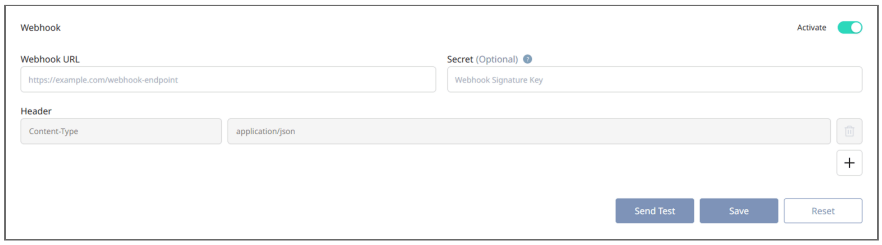
Click **Settings** → **Site** in the left sidebar. Use the **Additional Features** tab to enable or disable additional features.



- **QR Reader**: Supports QR code readers. Disable this option if you do not use a QR reader.
- **Video Management**: Supports ONVIF-compliant IP cameras. Enable this feature to integrate BioStar Air with video surveillance. After enabling the feature, click **Settings** to set the event log playback time.

> For more information about video management, see IP Camera Support and Setup.

- **Webhook**: Enable webhooks to send BioStar Air events to external systems. After enabling the feature, configure the fields below.



  - **Webhook URL**: Enter the endpoint address of the external server that will receive events. Example: `https://example.com/webhook-endpoint`
  - **Secret**: A security token used to verify that the webhook request originated from a trusted server. The sending server encrypts the payload with the security key using SHA-256 and sends it in the `X-Signature` header.
  - **Send Test**: Verify that the webhook works correctly. Send a test message to confirm that the external server receives and responds to the request.

> **Info**
>
> - After entering all required information, click **Save**.
> - Click **Reset** to initialize the entered information.

Manage Administrator Accounts and Roles

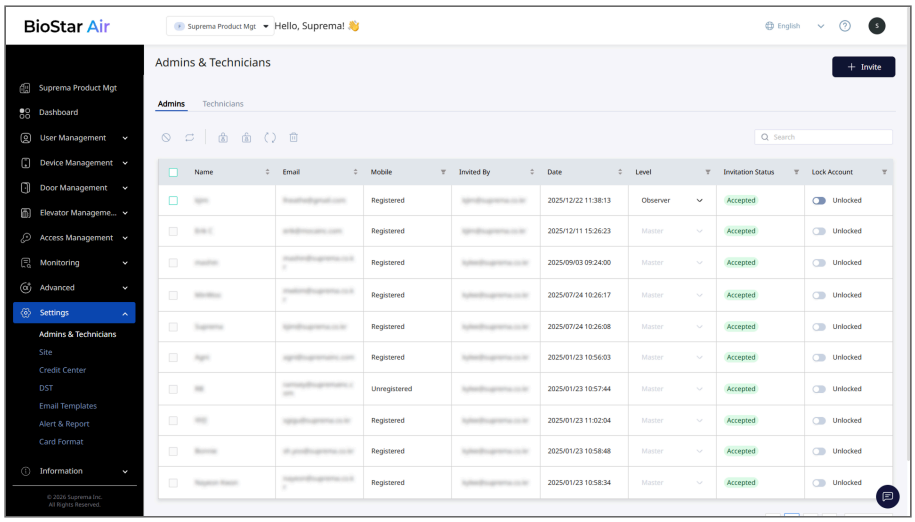
Use BioStar Air's administrator and role management features to effectively control site access. Assign the 4 roles — Observer, Operator, Administrator, and Master — to grant each person only the permissions they need, ensuring both security and operational efficiency.

This document covers the entire administrator account lifecycle, from inviting administrators to assigning roles, managing permissions, and locking accounts.

> **Tip**
> Watch the following video for a guide on managing administrators.

View administrators

Click **Settings** → **Admins & Technicians** in the left sidebar.



> **Info**
> Enabling the **Technician Access** option changes the **Settings** → **Admin** menu to the **Admins & Technicians** menu. The **Admin** and **Technicians** tabs let you manage admin and technician accounts separately.
>
> For more information on how to enable **Technician Access**, see Manage Technician Accounts.

Administrator List

The **Admins & Technicians** menu shows a list of all administrators. The administrator list includes the following information.

- **Name**: The administrator's name.
- **Email**: The administrator's email address.
- **Mobile**: The administrator's phone number.
- **Invited By**: The email address of the person who invited the administrator.
- **Date**: The date the administrator was invited.

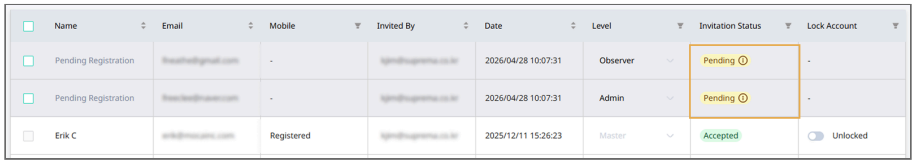
- **Level**: The administrator's permission level. For more information, see Administrator levels.
- **Invitation Status**: The invitation status of the administrator account. For more information, see Invitation status.
- **Lock Account**: The lock status of the administrator account. You can lock or unlock an account. For more information, see Lock or unlock administrators.

Invitation status

The administrator list shows each administrator's invitation status.

Pending sign-up

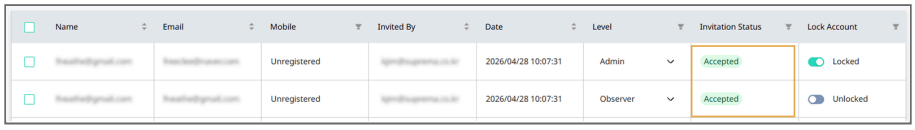
An invited administrator's status appears as **Pending** until they accept the email invitation and complete registration. An invited administrator can accept the invitation by clicking the link in the email to register or sign in to access the site.



> **Info**
>
> An invited administrator has up to 7 days to accept the invitation. After 7 days, the invitation expires and the status changes to **Expired**. If the invitation expires, you can resend the invitation link so the invited account can sign up again. For more information on resending invitation links, see Resend invitation link.

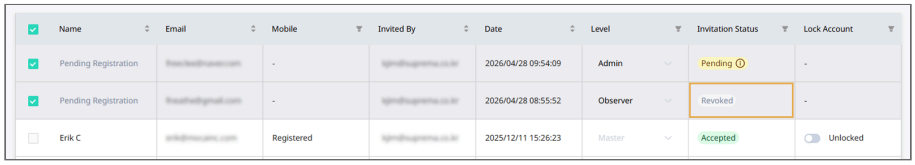
Sign-up complete

When an invited administrator accepts the email invitation and completes registration, the invitation status changes to **Accepted**. After completing registration, an administrator logs in to the site and accesses menus and features based on their assigned role.



Invitation revoked

You can cancel the invitation if the invited administrator's email address is incorrect or if the invitation is no longer needed. If you cancel the invitation, its status changes to **Revoked**. For more information on canceling administrator invitations, see Invitation revoked.



Administrator levels

Each administrator level in BioStar Air has specific permissions, and higher levels inherit the permissions of lower levels.

> **Info**
> Each administrator role has different permissions across BioStar Air. **Observer** has the most restricted access and some menus are hidden.

Compare permissions

Feature	Observer	Operator	Administrator	Master
View Dashboard/Logs	✔	✔	✔	✔
Export Logs and Generate Reports	✔	✔	✔	✔
User Management	✕	✔	✔	✔
Manage User Groups	✕	✔	✔	✔
Manage Access Levels	✕	✔	✔	✔
Manage Schedules	✕	✔	✔	✔
Manage Holiday Groups	✕	✔	✔	✔
Control and Configure Devices	✕	✕	✔	✔
Invite Administrators	✕	✕	✔	✔
Assign Master Role	✕	✕	✕	✔
Edit or Delete Master Administrators	✕	✕	✕	✔
Create Subsites	✕	✕	✕	✔
Configure Site Settings	✕	✕	✕	✔

Observer (Lowest Level)

- **Dashboard** and logs **can be viewed**.
- **Export** logs and generate reports.
- **Cannot modify** settings, users, or devices.
- Access to menus is restricted. Most menus do not appear on the screen.

Operator

- Can manage **Users**, **User Groups**, **Access Levels**, **Schedules**, and **Holiday Groups**.
- **No access** to device control or management settings.

- Suitable for managing everyday user and access configurations.

Admin

- **Can invite** new administrators. However, cannot assign the **Master** role.
- Has **full device control** authority to modify settings and manage connected devices.
- Cannot delete or modify administrators with the **Master** role.
- This role is typically recommended for IT staff responsible for system management.

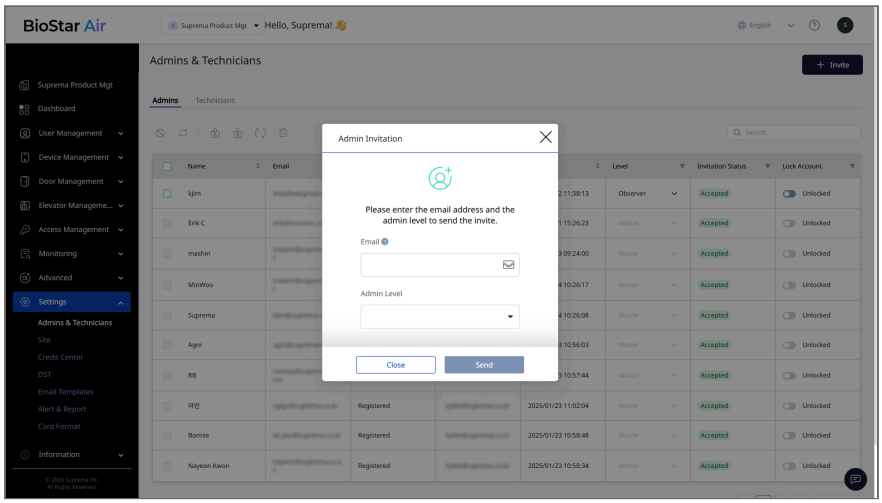
Master (Highest Level)

- Has **full access** to all settings and features.
- Cannot be deleted or modified by **administrators**.
- Can create **subsites** to manage different locations or organizations.
- Can configure **site settings**, including critical system-wide configurations.
- Responsible for accepting the **terms** before other administrators log in.
- Usually assigned to the company owner or a highly trusted executive.

Invite new administrators

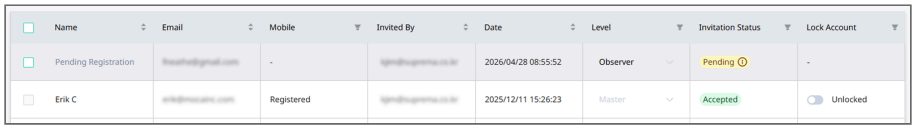
Add new administrators.

1. Click **Settings** → **Admins & Technicians** in the left sidebar.
2. Click **Invite** at the top right of the screen.
3. When the **Admin Invitation** window appears, enter the email address.



4. In **Admin Level**, select the role to assign to the new administrator.
5. Click **Send** to send the invitation.

Invited accounts appear in the administrator list with **Invitation Status** set to **Pending**. When an invited account accepts the invitation by email, its **Invitation Status** changes to **Accepted**.

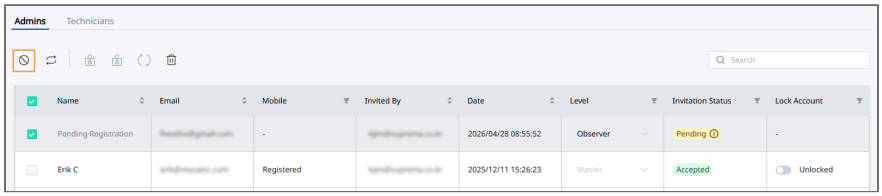


- An invited account can accept the invitation for up to 7 days. If 7 days pass, the invitation expires and the account's status changes to **Expired**.
- Each administrator must have a unique email address. If necessary, use an alias address (for example, erik+training@example.com).
- Click the link in the invitation email. Sign up if the administrator does not have an account. If the administrator already has an account, log in to access the **site** directly.

Invitation revoked

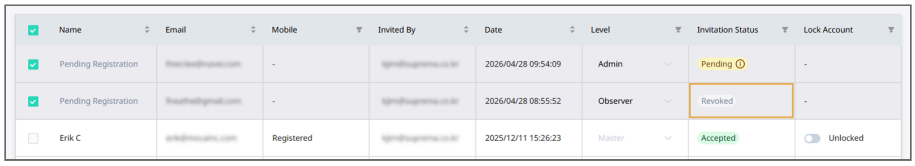
If an invited account hasn't accepted the invitation yet, you can cancel it. Canceling the invitation prevents accounts that are pending sign-up from signing up using the invitation link in the email.

1. Click the checkbox for accounts with invitation status **Pending** in the administrator list. Select 1 or more accounts.
2. Click ⃠ at the top left of the administrator list.



3. When a popup appears, review the message and click **Yes**.

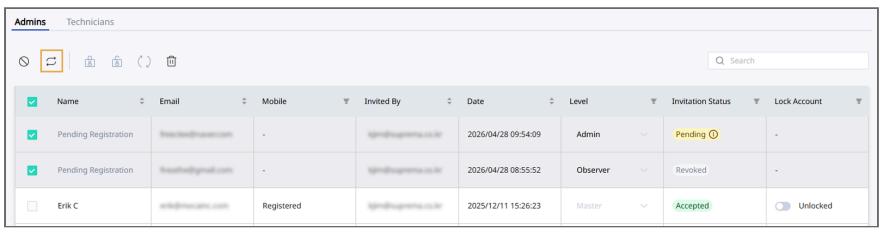
Accounts in the administrator list whose invitations have been revoked change to **Revoked**.



Resend invitation link

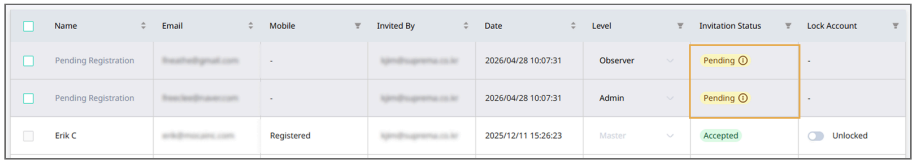
You can resend the invitation link if an invited account didn't receive or lost the invitation email, or if the invitation link has expired. Resending the invitation link lets the user sign up using the new link.

1. Click the checkbox for accounts with invitation status **Pending**, **Expired** or **Revoked** in the administrator list. Select 1 or more accounts.
2. Click ⟲ at the top left of the administrator list.



3. When a popup appears, review the message and click **Yes**.

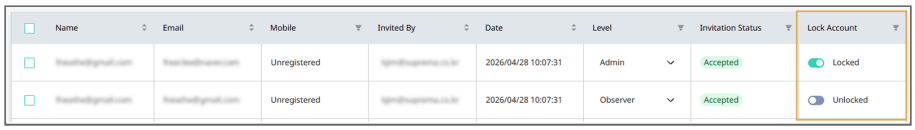
Accounts whose invitation link is resent will change to **Pending**.



Lock or unlock administrators

Use the **Lock Account** option to lock or unlock administrators who have completed sign-up by accepting an email invitation. Locking an account prevents the administrator from logging in. Account information is retained so the account can be reactivated later if needed.

In the **Lock Account** column, locked administrators appear as **Locked**, and unlocked administrators appear as **Unlocked**.

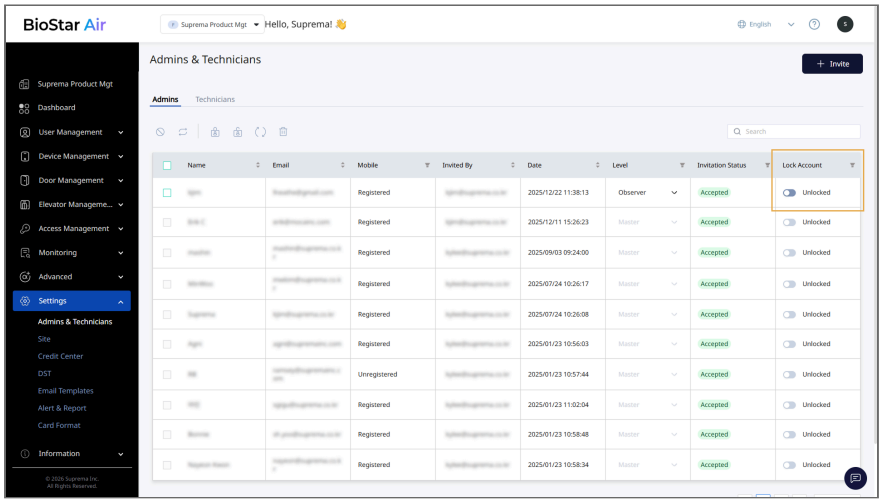


Info

- Only administrator accounts that have completed sign-up can be locked or unlocked.
- The **Lock Account** option may be restricted by the administrator's role. Administrators with the **Master** role cannot lock other administrators with the **Master** role.

Lock or unlock an individual administrator

1. Find the administrator to lock or unlock in the list.
2. Click the toggle switch in the **Lock Account** column.

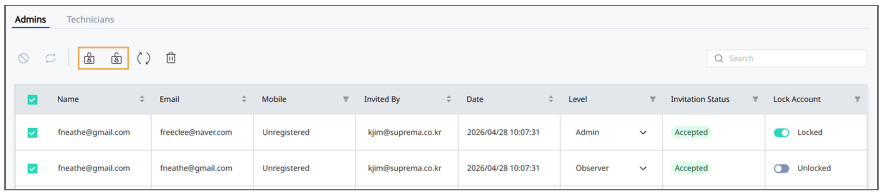


3. When the message window appears, click the **Confirm** button.

Lock or unlock multiple administrators

1. In the administrators list, click the checkbox for the administrator you want to lock or unlock. You can select 1 or more administrators.

2. Click or in the upper left corner of the screen.



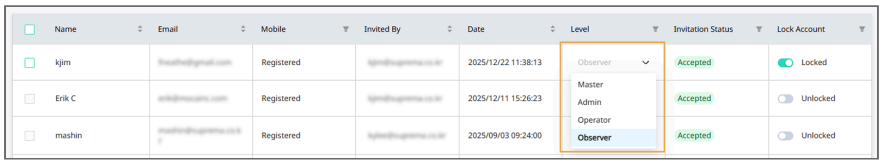
3. When a popup appears, review the message and click **Yes**.

Change an administrator's role

Administrators can change the roles of administrators at a lower level. Adjust roles when employees' duties change, when their responsibilities expand or contract, or during organizational restructuring. Downgrading a role removes an administrator's access to features they previously had.

1. Find the administrator whose role you want to change in the list.

2. Select the new administrator level in the **Level** column.



3. When the message window appears, click the **Confirm** button.

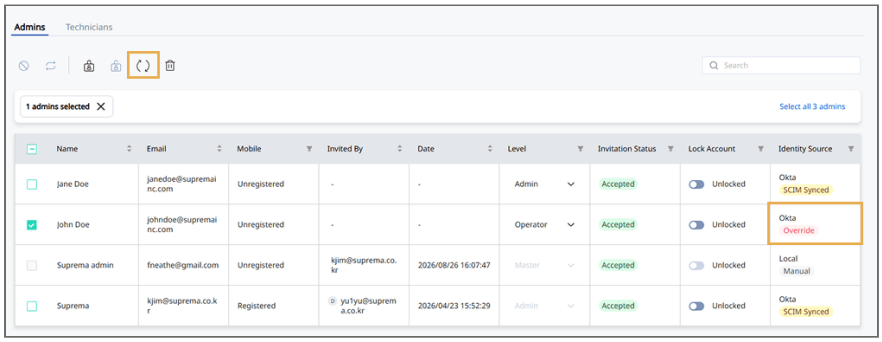
> Only **Master** administrators can assign or modify the **Master** role for other administrators.

Release override status

Manually changing a SCIM-synced administrator’s permissions or lock status locally sets **Override**. Cancel local changes and restore SCIM management.

1. In the administrators list, click the checkbox next to the administrator whose status is **Override**. You can select 1 or more administrators.

2. Click in the upper left of the screen.



3. When a popup appears, review the message and click **Yes**.

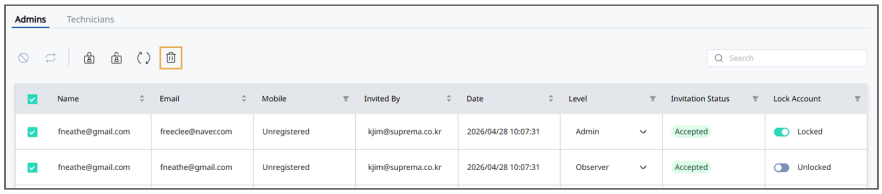
The system clears the **Override** status for the selected administrator account and changes it to **SCIM Synced**.

> **Info**
>
> For more information on SSO & SCIM settings, see Set Up SSO & SCIM.

Delete administrator account

If you delete an administrator account, that administrator will not be able to log in to the site, and the deleted account information cannot be recovered.

1. In the administrators list, click the checkbox for the administrator you want to delete. You can select 1 or more administrators.
2. Click in the upper left of the screen.



3. When a popup appears, review the message and click **Yes**.

Deleted administrator accounts no longer appear in the administrator list.

Manage Technician Accounts

A technician is a professional granted access to a customer site. To manage technician accounts, invite technicians in the Partner Portal, assign them to sites, and set their permission levels.

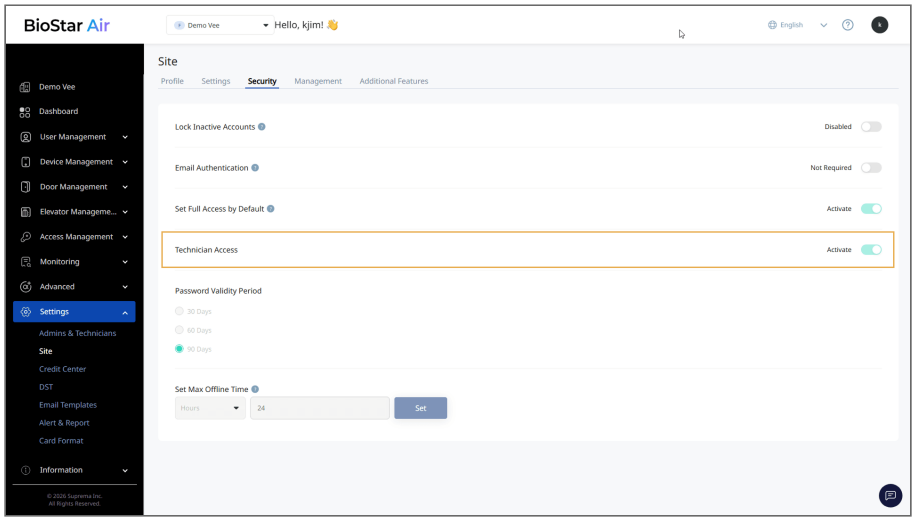
In the BioStar Air portal, modify an invited technician's access permissions or lock/unlock their site access. You can also delete a technician account entirely to remove their site access.

> **Info**
>
> - For more information on inviting technicians in the Partner Portal and assigning them to sites, see Manage Partner Technicians.
> - Activities of invited technicians are recorded per account and can be viewed at **Monitoring** → **Event Logs** / **Audit Logs**.

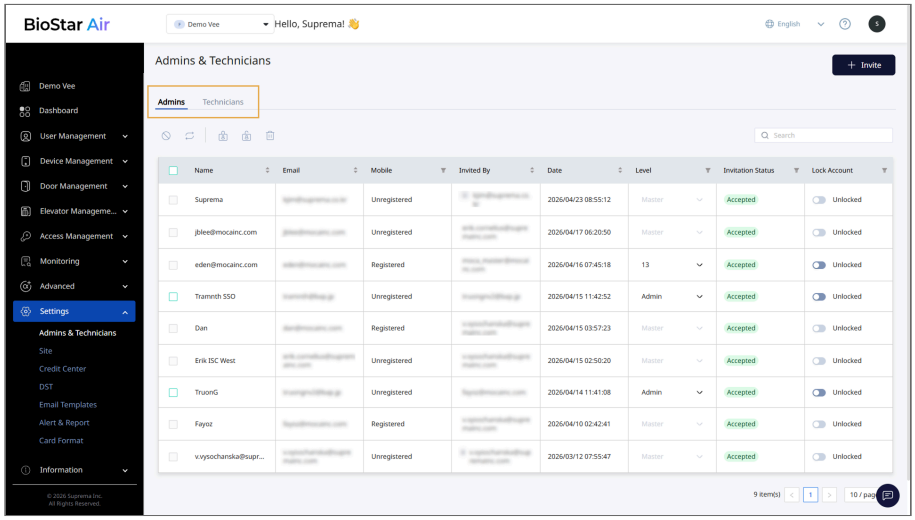
Before you start

Before managing technician accounts, ensure that technician accounts are allowed to access the site in the site security settings. If technician accounts are not allowed to access the site in the site security settings, you won't be able to manage them.

1. Click **Settings** → **Site** in the left sidebar.
2. Click the **Security** tab.
3. Enable the **Technician Access** option.



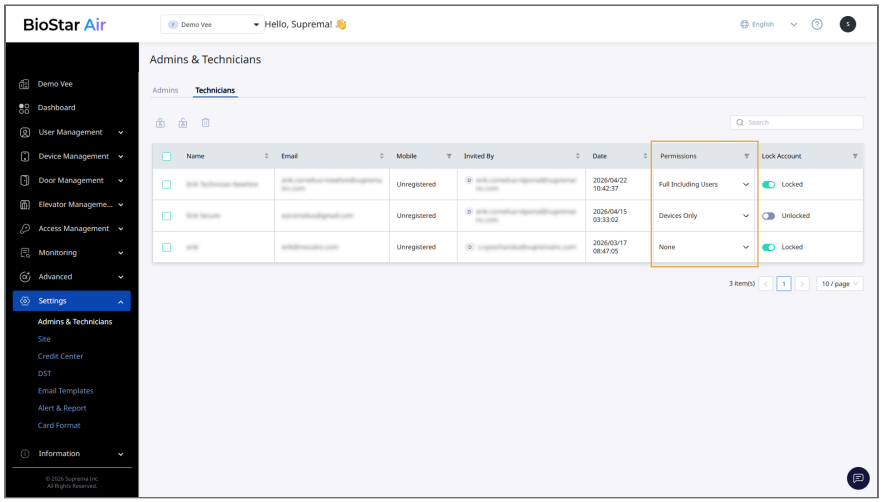
Enabling the **Technician Access** option changes the **Settings** → **Admin** menu to the **Admins & Technicians** menu. The **Admin** and **Technicians** tabs let you manage admin and technician accounts separately.



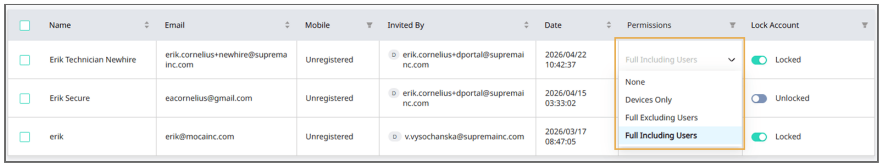
Change technician permissions

Follow the instructions below to change access permissions for technicians invited to the site.

1. Click **Settings** → **Admins & Technicians** in the left sidebar.
2. Click the **Technicians** tab.
3. In the technician list, click the **Permissions** column for the technician whose access permissions you want to change.



4. Select the desired permission level from the access dropdown.



- : Cannot log in to the site.
- **Devices Only**: Provides access only to the **Dashboard** and **Device Management** menus.
- **Full Excluding Users**: Provides access to all menus except **User Management**, but access to certain setting features is restricted.
- **Full Including Users**: Provides access to all menus including **User Management**, but access to certain setting features is restricted.

5. Click **Yes** when the confirmation message window appears.

The technician's access permissions are updated, and a success message appears at the top of the screen.

> **Info**
>
> **Full Excluding Users** and **Full Including Users** have view permission but not edit permission for the following menu paths.
>
> - **Settings** → **Admins & Technicians**
> - **Settings** → **Site**

Lock or unlock technician accounts

If a technician's support is no longer needed, or if site access must be restricted for security reasons, you can lock the technician's account to prevent them from accessing the site. If you need the technician's support again, you can unlock the account to allow them to access the site.

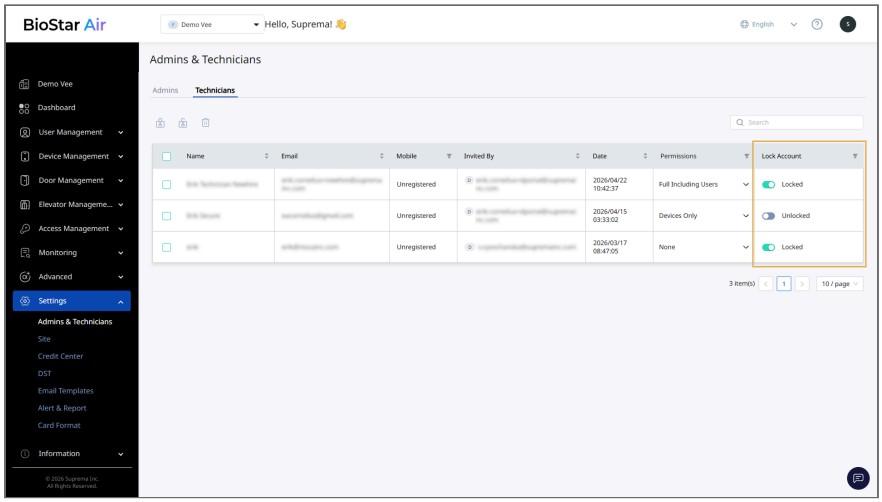
If you lock an invited technician's account, they won't be able to sign in to the site.

Lock or unlock an individual technician account

1. Click **Settings** → **Admins & Technicians** in the left sidebar.

2. Click the **Technicians** tab.

3. In the technician list, click the toggle in the **Lock Account** column for the technician whose account you want to lock or unlock.



4. When a popup appears, review the message and click **Yes**.

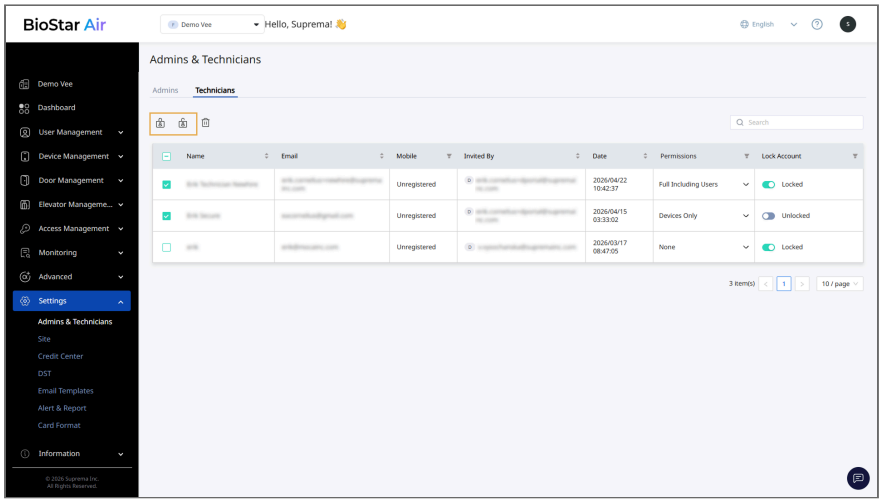
Lock or unlock multiple technician accounts

1. Click **Settings** → **Admins & Technicians** in the left sidebar.

2. Click the **Technicians** tab.

3. In the technician list, click the checkboxes next to the technicians whose accounts you want to lock or unlock. You can select 1 or more technicians.

4. Click  or  at the top of the technician list.



5. When a popup appears, review the message and click **Yes**.

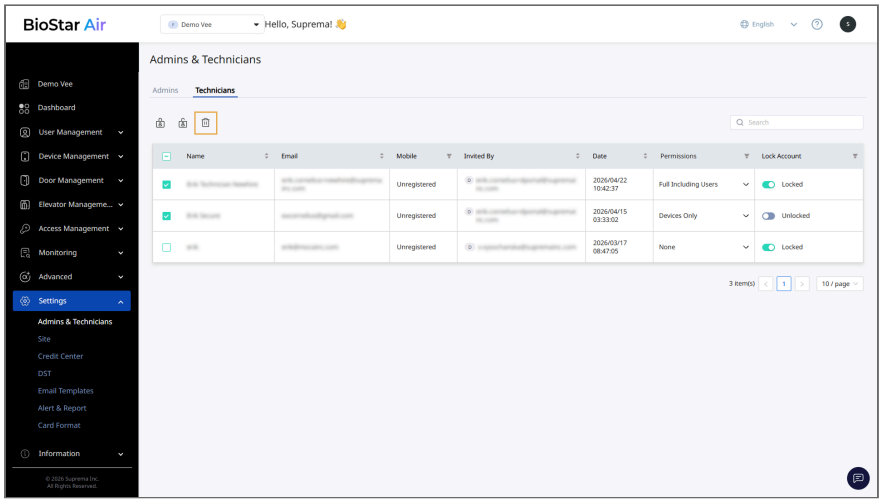
The selected technicians' accounts are locked or unlocked, and a success message appears at the top of the screen.

> **Info**
>
> If selected technicians have mixed lock statuses, a bulk action locks all accounts or unlocks all accounts.

Delete technician accounts

Deleting an invited technician's account completely removes their access to the site.

1. Click **Settings** → **Admins & Technicians** in the left sidebar.
2. Click the **Technicians** tab.
3. In the technician list, click the checkbox next to the technician whose account you want to delete. You can select 1 or more technicians.
4. Click at the top of the technician list.



5. When a popup appears, review the message and click **Yes**.

After the selected technicians' accounts are deleted, a success message appears at the top of the screen, and those technicians no longer appear in the technician list.

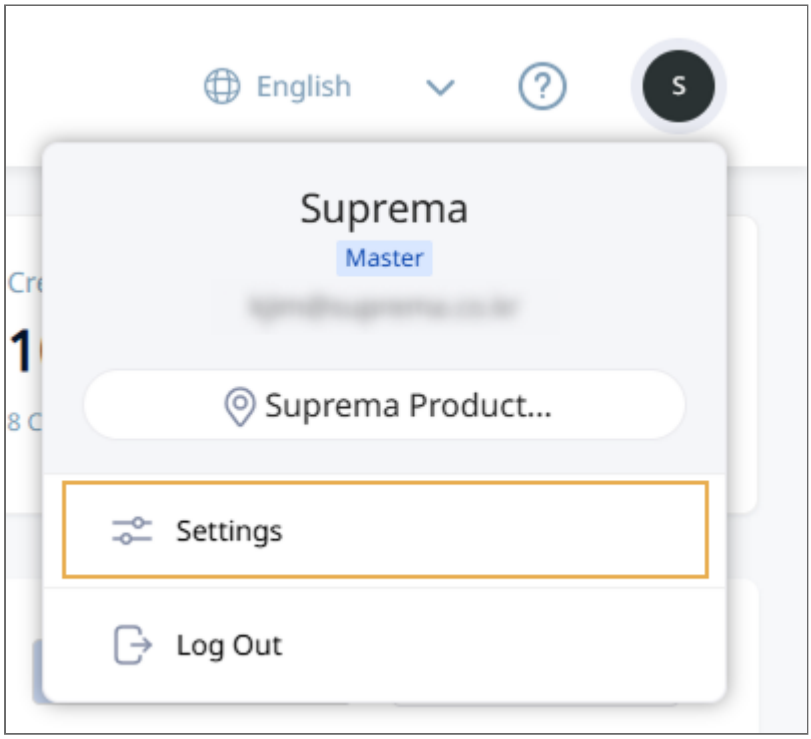
> **Info**
>
> A deleted technician account cannot be recovered. Technicians who have been removed from a site can be reassigned to that site through the Partner Portal. For more information on assigning a technician to a site in the Partner Portal, see Assign Technicians to a Site.

Personal Account Settings

You can manage your personal account settings—such as changing your password, adjusting how you receive alerts, and configuring IP intercom settings. You can leave the site or permanently delete your account.

Access account settings

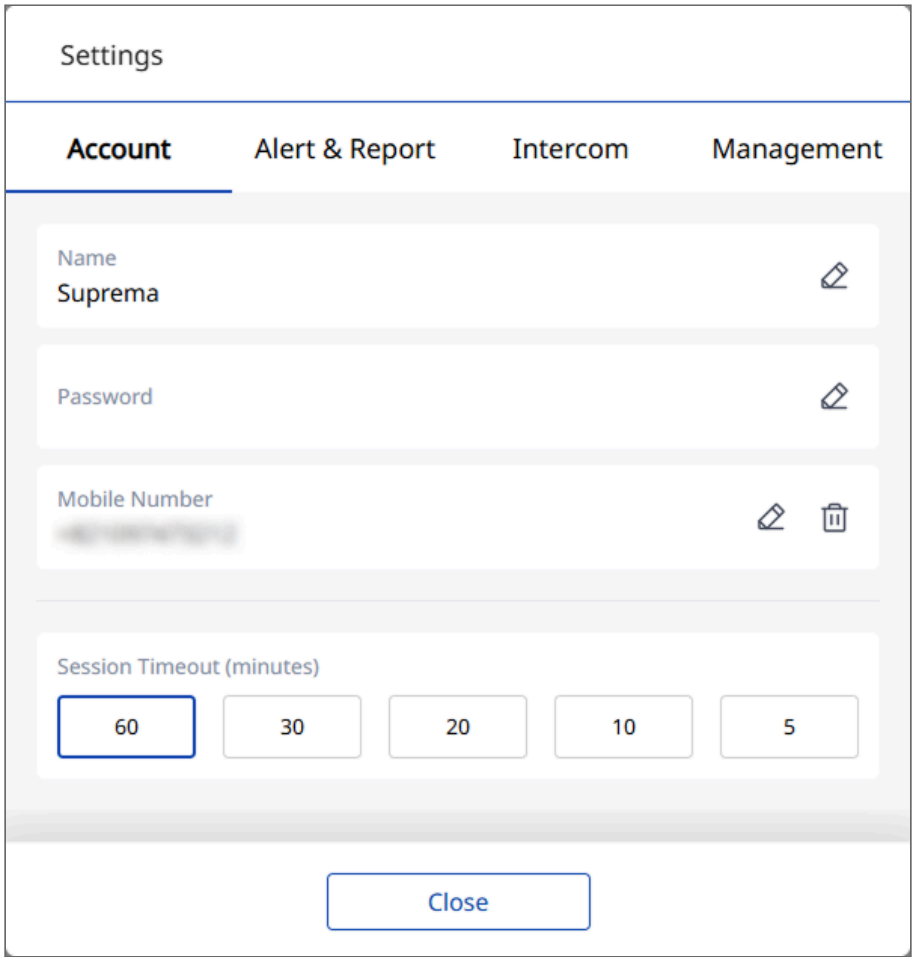
1. Log in to the BioStar Air portal.
2. Click the user profile icon at the top right of the screen.
3. Click **Settings** in the drop-down menu.



4. When the **Settings** window appears, set your desired options.
   - **Account**: Edit the user name, password, and phone number. See Change account information for details.
   - **Alert & Report**: Set how alerts are received. See Set alerts for details.
   - **Intercom**: Manage SIP intercom settings. See Intercom settings for details.
   - **Management**: Leave the site or delete the account. See Leave or delete account for details.

Change account information

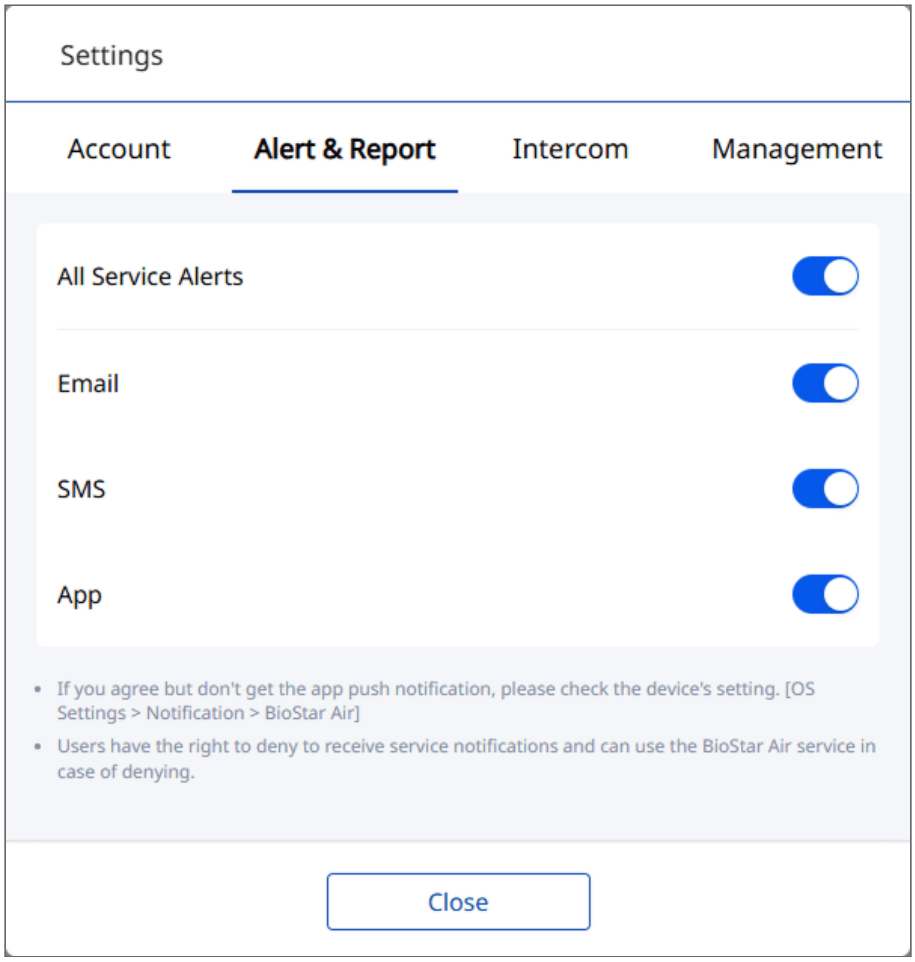
In the **Account** tab, edit information for the currently logged-in user.



- Edit the user name, password, and phone number. Click for each item.
- **Session Timeout (minutes)**: Automatically logs out after the selected time elapses. Select the desired time.

Set alerts

In the **Alert & Report** tab, set how alerts are received. Activate the **All Service Alerts** option to receive all alerts. Disable unwanted alerts individually.

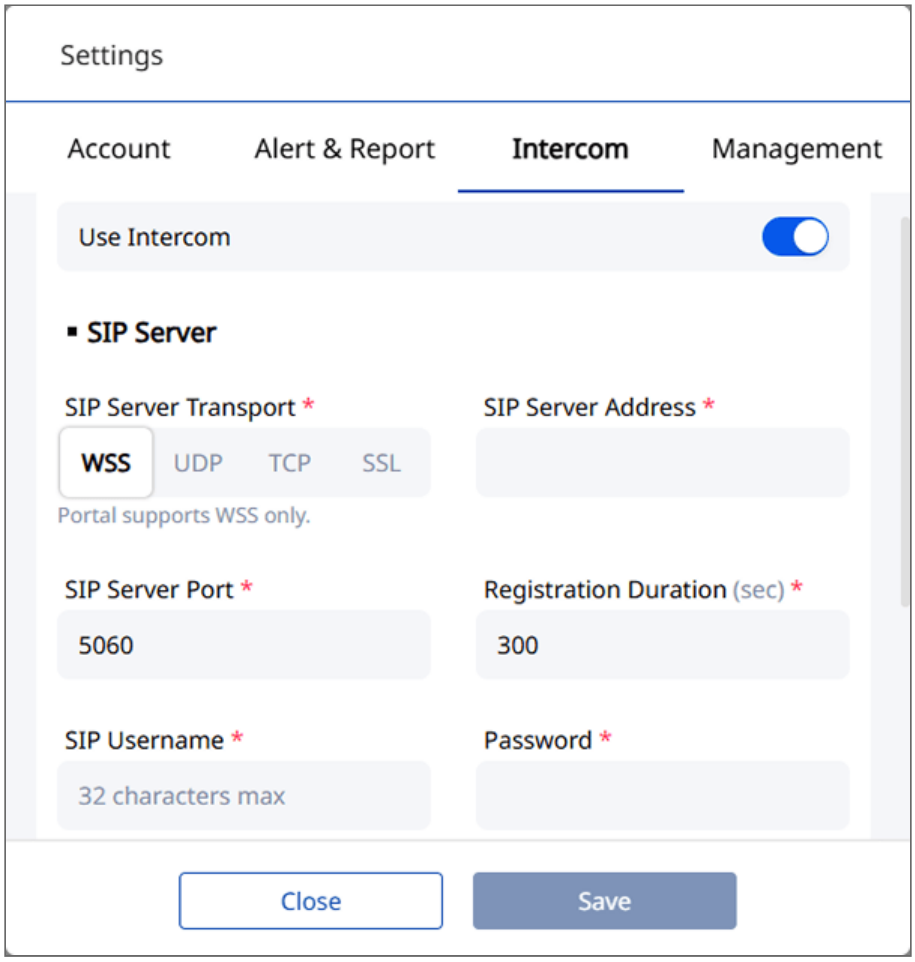


Info

- If you agreed to receive app alerts but none appear, check the mobile settings. App alerts must be allowed on iOS or Android devices.
- Users may refuse to receive service alerts, and doing so does not restrict service use.

Intercom settings

In the **Intercom** tab, manage SIP intercom settings.

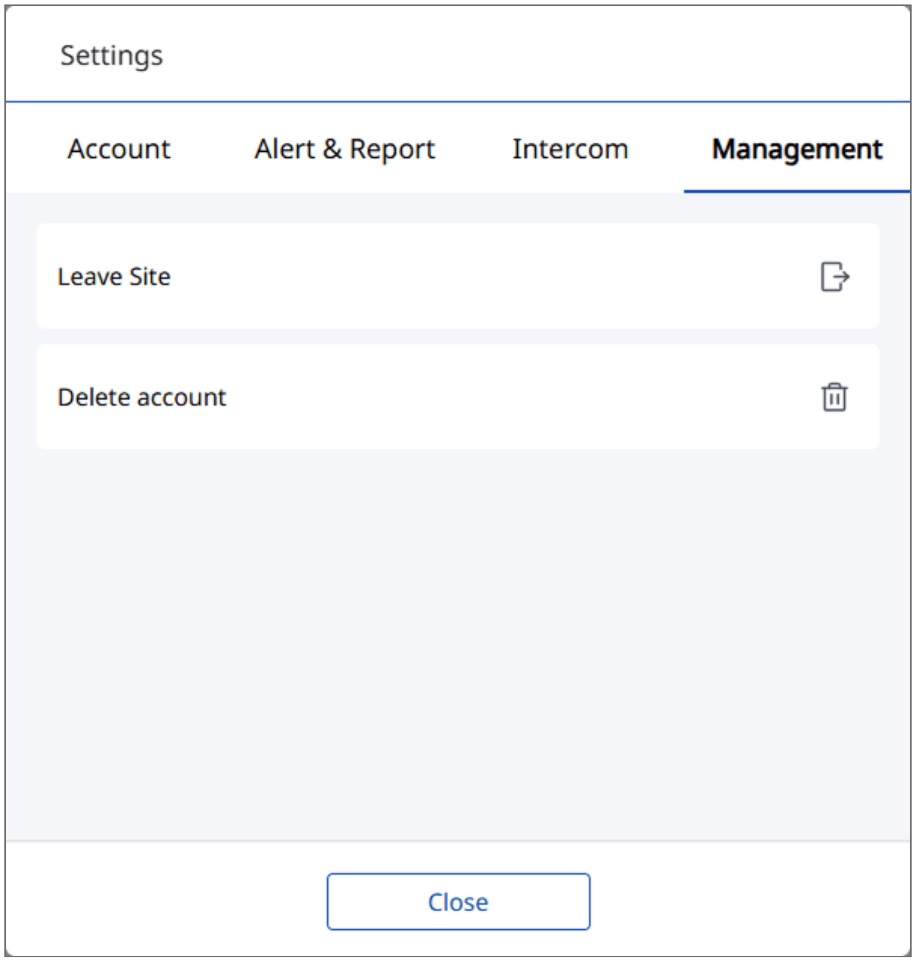


Info

For more information on SIP intercom settings, see Configure SIP Intercom for BioStation 3.

Leave or delete account

In the **Management** tab, leave the site or delete the account.



- **Leave Site**: Leave the site. After leaving a site, you must receive an invitation from the site administrator to join again.
- **Delete account**: Permanently delete the account. Deleting the account permanently deletes all personal information and settings and cannot be recovered.

Set Up SSO & SCIM

Many organizations already manage internal system access with Microsoft Entra ID or Okta, regardless of company size. BioStar Air integrates with these ID providers to centrally manage admin accounts and credential users from a single source.

SSO (Single Sign-On) applies your organization's existing ID policies to BioStar Air admin logins, enhancing security. SCIM (System for Cross-domain Identity Management) automatically creates and deletes user accounts, reducing security risks from accounts left active without access. This reduces repetitive work to create, edit, and delete users, user groups, and admin accounts.

In the left sidebar, click **Settings** → **Site**. On the **SSO & SCIM** tab, select the sign-in policy and identity provider, and configure them. For basic settings, see Enabling SSO & SCIM.

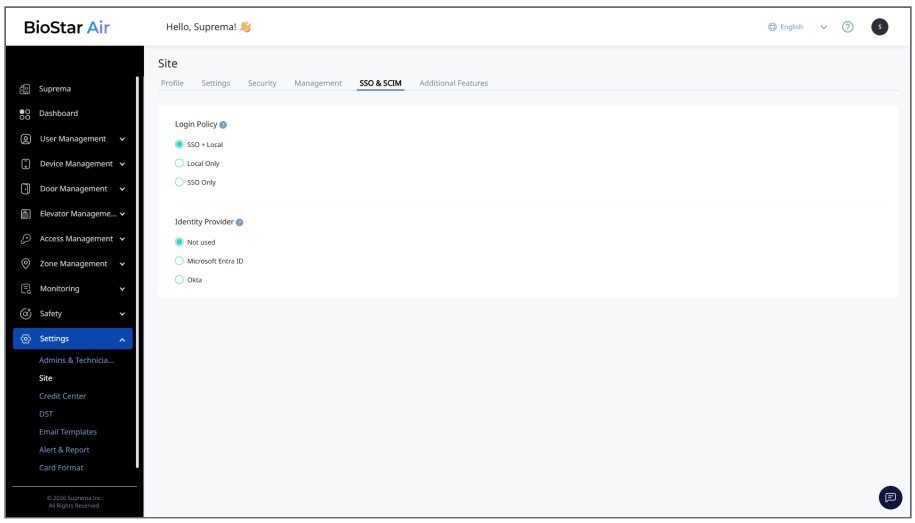
BioStar Air supports site administrator and credential user provisioning through **Microsoft Entra ID** or **Okta**. If you are using one of these identity providers, use the documents below to set up SSO and SCIM for BioStar Air sites.

Minimum requirements

- BioStar Air SSO & SCIM license
- Microsoft Entra AD or Okta active subscription
- Ability to create new applications in IdP
- Ability to create, push, and assign groups in IdP
- Master permissions in BioStar Air

Enabling SSO & SCIM

Click **Settings** → **Site** in the left sidebar. On the **SSO & SCIM** tab, select the login policy and ID provider, or clear them.



Caution

Before changing ID provider settings, keep at least one master administrator account that can log in locally. Otherwise, ID provider integration problems can lock administrators out of the site.

Info

- Only the site master administrator can manage SSO and SCIM settings.
- Credential users do not log in to BioStar Air, so SSO and SCIM settings do not affect them.
- The Partner Portal is not included in the scope of SSO and SCIM settings.

Login policy

In **Login Policy**, set how BioStar Air administrators log in.

- **SSO**: Administrators authenticate through an identity provider.
- **Local**: Administrators authenticate with the email address and password set in BioStar Air.

Select one of the following three options.

- **SSO + Local**: Both SSO login and local login are available.
- **Local Only**: Only local login is available.
- **SSO Only**: Only SSO login is available.

ID provider integration settings

In **Identity Provider**, select an external ID provider for BioStar Air administrator accounts. A site can have only one ID provider active at a time.

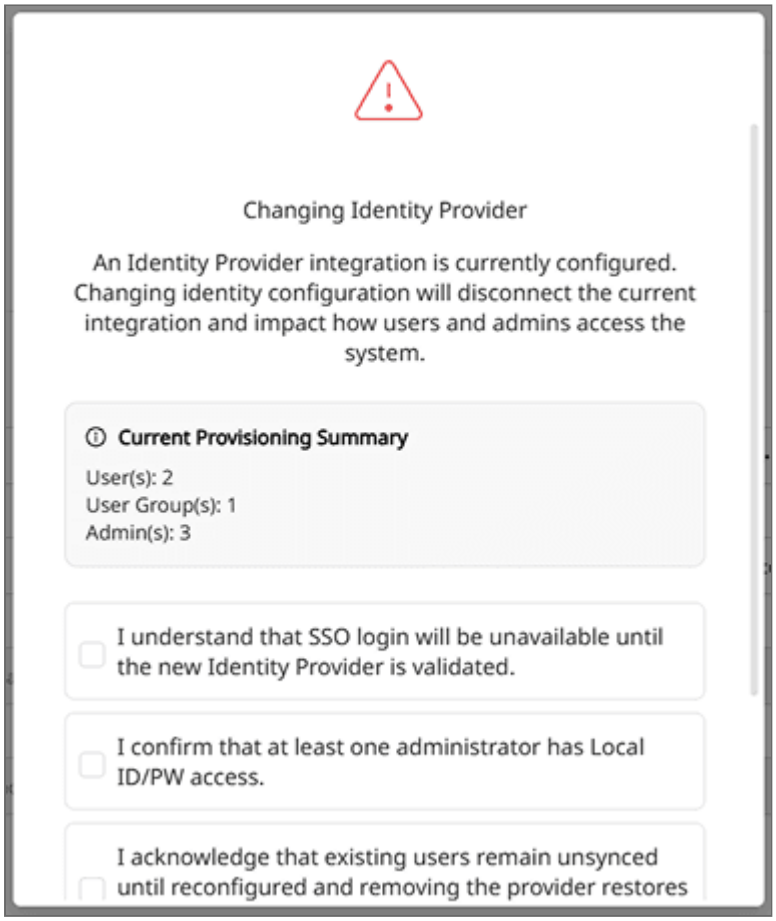
- **Not used**
- **Microsoft Entra ID**: Set Up Microsoft Entra ID Integration
- **Okta**: Set Up Okta Integration

> **Info**
> To change the connected ID provider, select **Not used** to disconnect, then select a new ID provider. Without disconnecting, the site cannot switch directly to another ID provider.

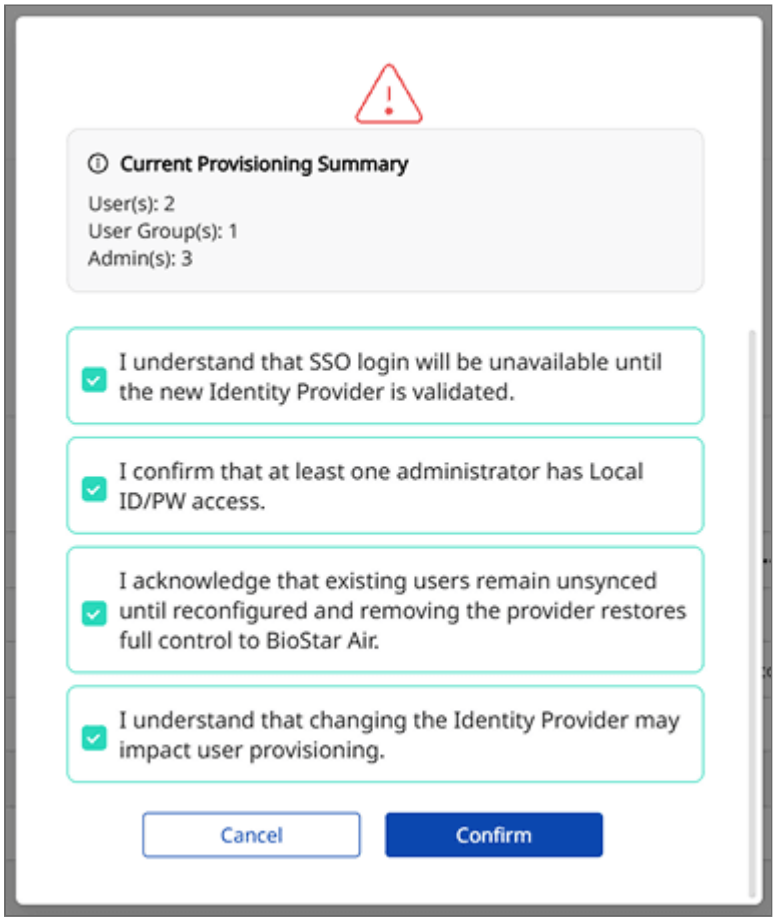
Disable SSO & SCIM settings

Disable ID provider integration.

1. Select **Not used** in the **Identity Provider** section.
2. Review the message in the warning pop-up.



3. Review the impact of the setting change, and click the checkbox.



4. Click **Confirm**.

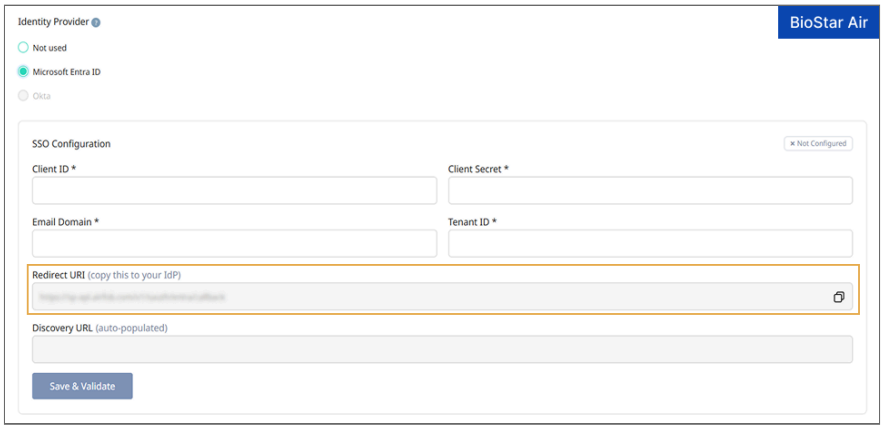
Set Up Microsoft Entra ID Integration

To sign in to BioStar Air with Microsoft Entra ID, an ID administrator creates an app registration in Entra ID. Then the administrator links it to the BioStar Air SSO settings.

Connect Entra ID SSO

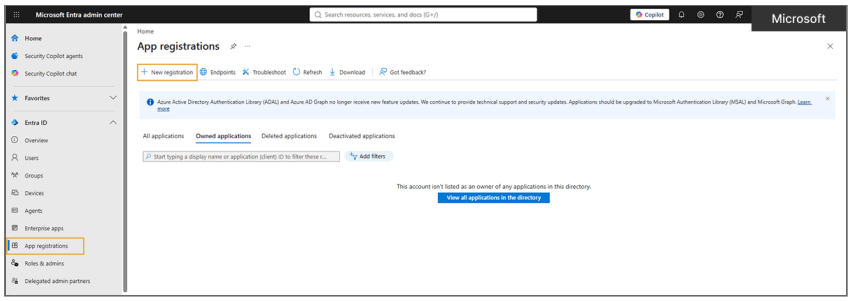
1 BioStar Air: Prepare redirect URI

1. Click **Settings** → **Site** in the left sidebar of BioStar Air.
2. Click the **SSO & SCIM** tab.
3. Under **Identity Provider**, select **Microsoft Entra ID**.
4. Copy the URI value shown in the **Redirect URI** field.



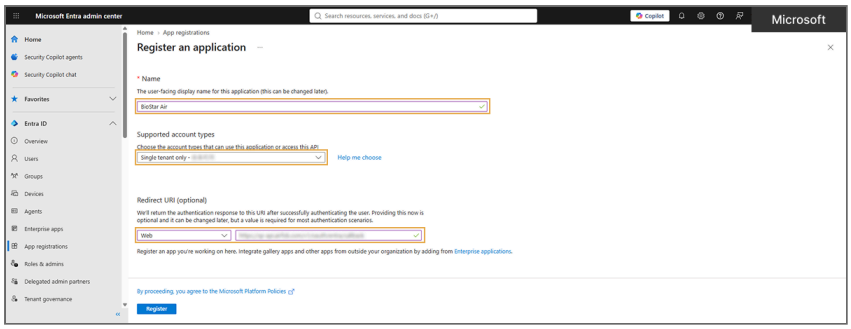
2 Microsoft Entra admin center: Register app

1. Sign in to the Microsoft Entra admin center.
2. Go to **Entra ID** → **App registrations**.
3. Click **New registration**.



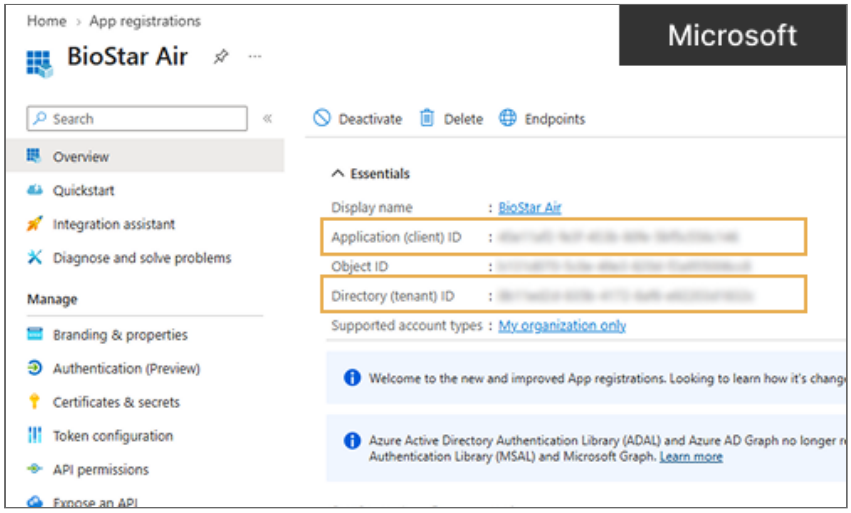
4. Enter 'BioStar Air' for the app name.
5. Under **Supported account types**, select **Single tenant only**.

6. In **Redirect URI**, select **Web**. Paste the URI from step BioStar Air: Prepare redirect URI into the field.



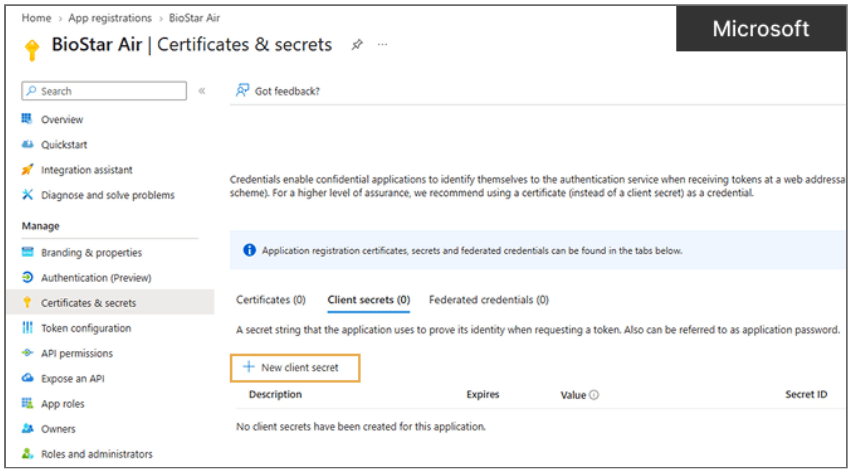
7. Click **Register**.

8. In the BioStar Air app **Overview**, copy the following values.

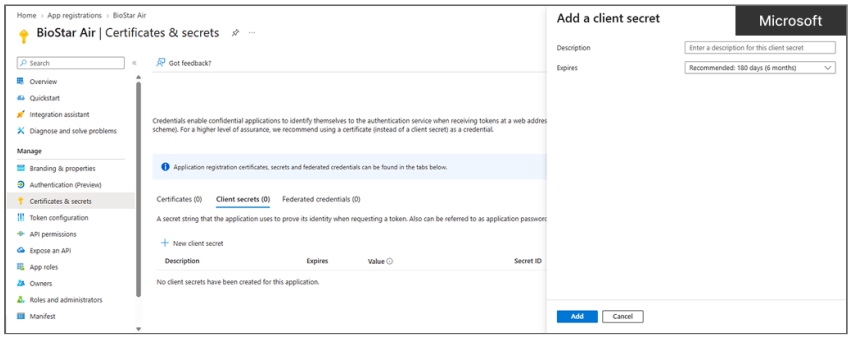


- **Application (client) ID**
- **Directory (tenant) ID**

9. Under **Certificates & secrets** → **Client secrets**, click **New client secret**.

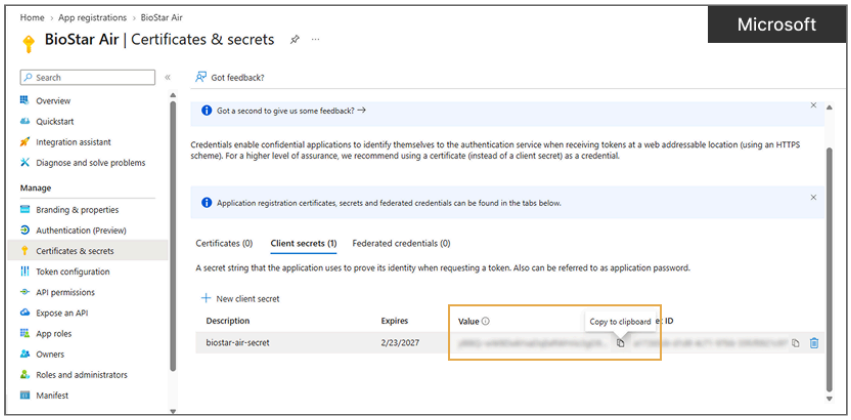


10. Enter a description and select an expiration period.



11. Click **Add**.

12. Copy the **Value** of the generated client secret.



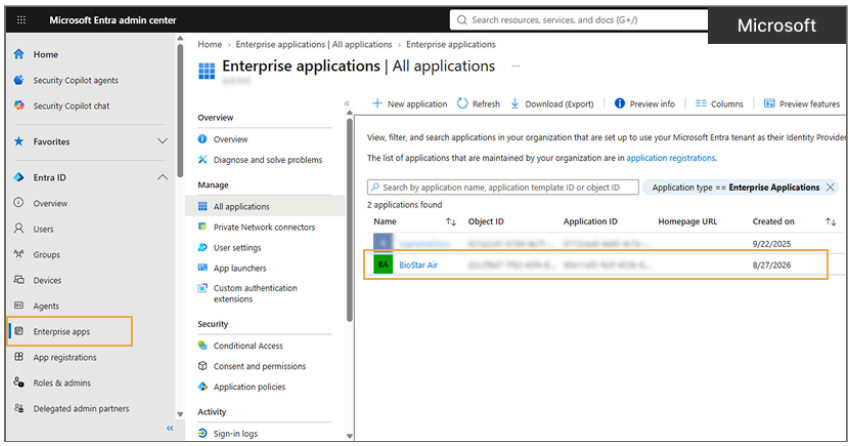
Enter the copied **Application (client) ID**, **Directory (tenant) ID**, and **Value** in the next step.

> **Caution**
> Use **Value**, not **Secret ID**. The **Value** appears only once, so copy it now.

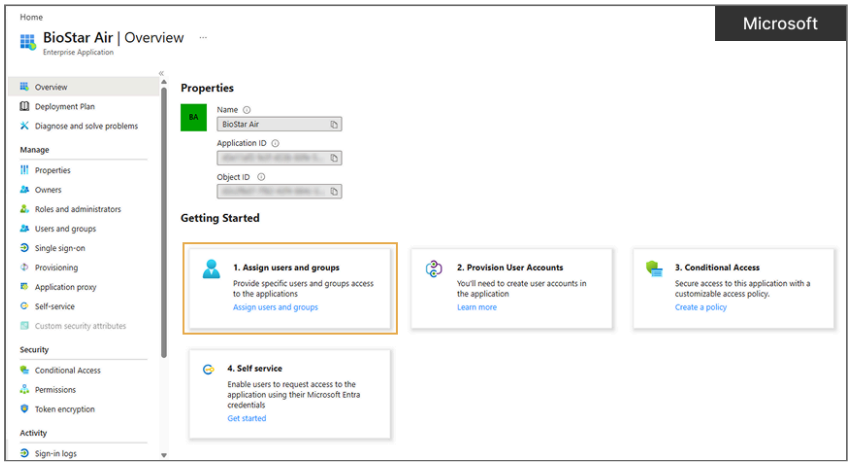
3 Microsoft Entra admin center: Assign users and groups

Create users and groups before assigning them.

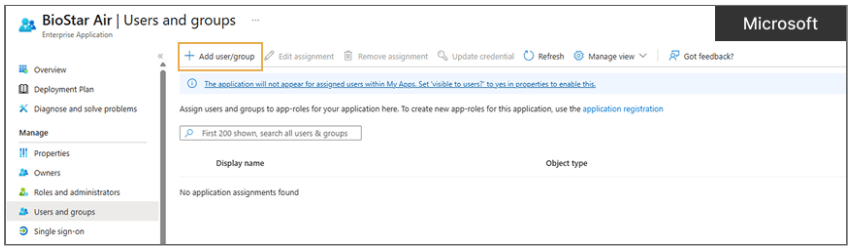
1. In **Enterprise apps**, click the app created earlier (BioStar Air).



2. Click **Assign users and groups**.



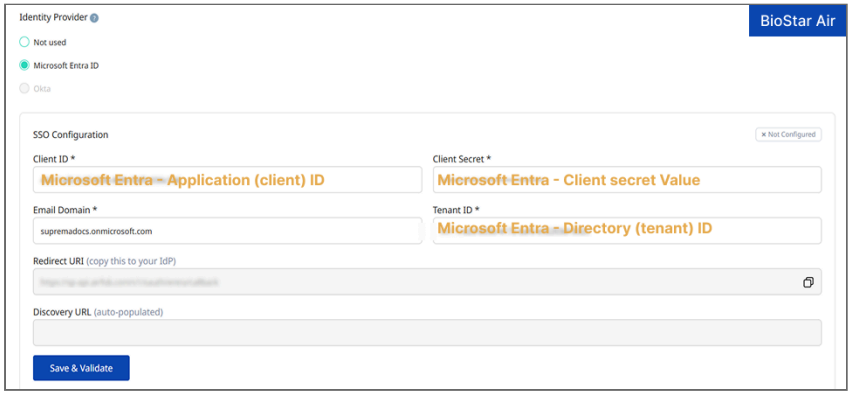
3. Click **Add user/group** to assign users and groups.



4. After assigning users and groups, click **Assign**.

4 BioStar Air: Configure SSO

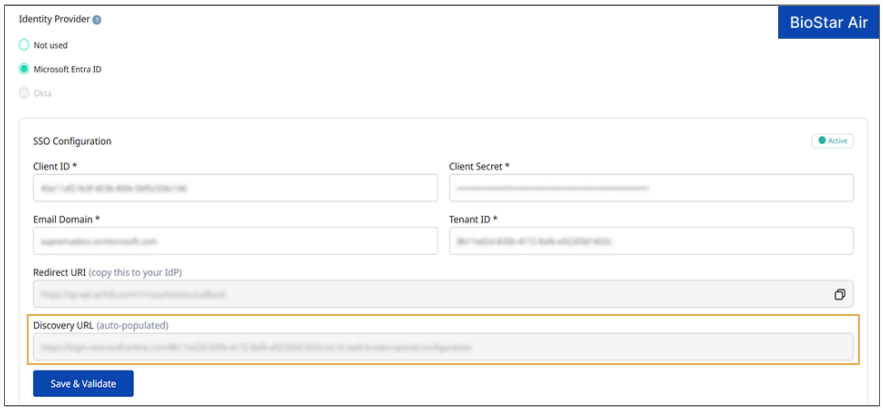
1. Return to the BioStar Air Settings screen and enter the values copied in Microsoft Entra admin center: Register app into each field.



- **Client ID**: Application (client) ID
- **Client Secret**: Value
- **Tenant ID**: Directory (tenant) ID

2. In the **Email Domain** field, enter your organization's email domain.
3. Click **Save & Validate**.

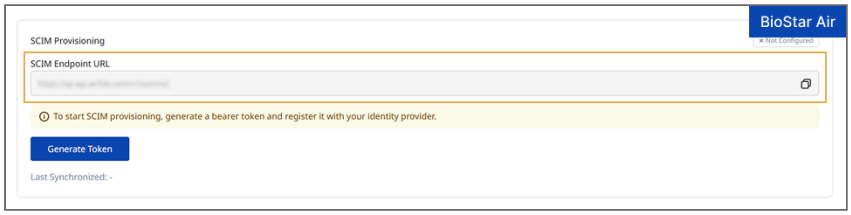
After the system saves and verifies successfully, it automatically generates the value for **Discovery URL**.



Connect Entra ID SCIM provisioning

1 BioStar Air: Copy SCIM token

1. Click **Settings** → **Site** in the left sidebar of BioStar Air.
2. Click the **SSO & SCIM** tab.
3. In the **SCIM Provisioning** section, copy the **SCIM Endpoint URL** value.

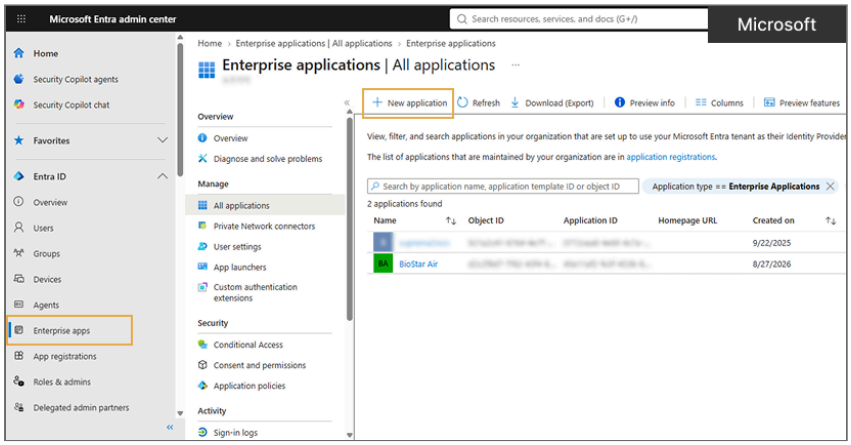


4. Click **Generate Token**.
5. In the Token Generation Complete dialog box, copy the token.

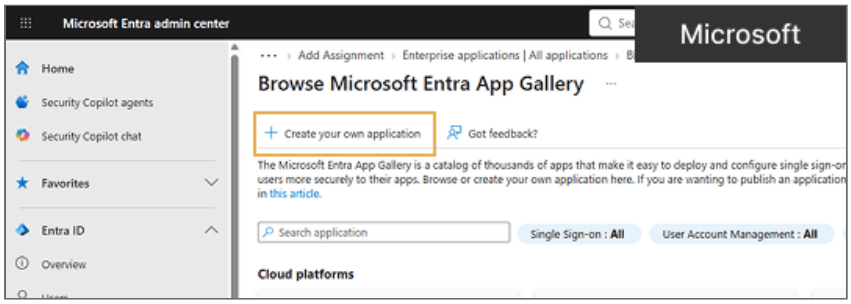
> **Info**
>
> - Copy the generated token immediately. Copy the token only when you generate it. After you close the dialog box, you cannot copy the token again.
> - If you lose the token, click **Rotate Token** to generate a new token. Enter the new token in the identity provider again.
> - In the next step, enter the SCIM endpoint URL and token copied in this step.

2 Microsoft Entra admin center: Create a SCIM provisioning app

1. In **Enterprise apps**, click **New application**.

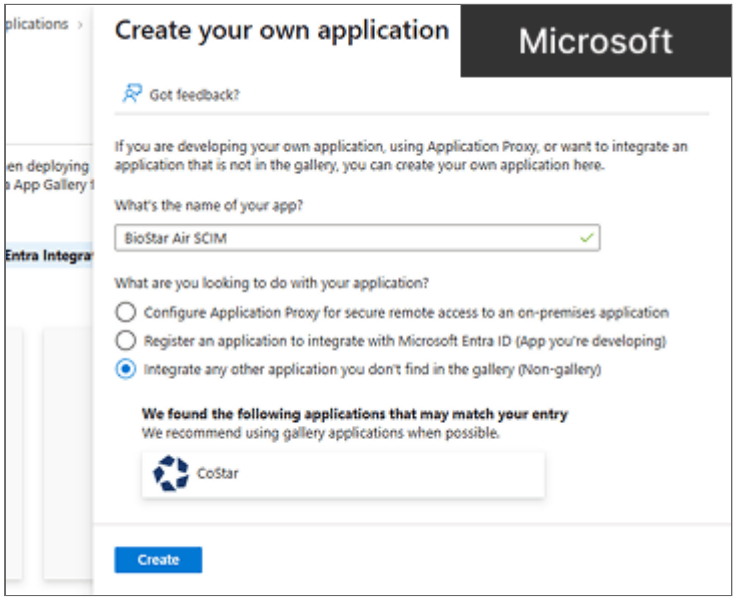


2. Click **Create your own application**.



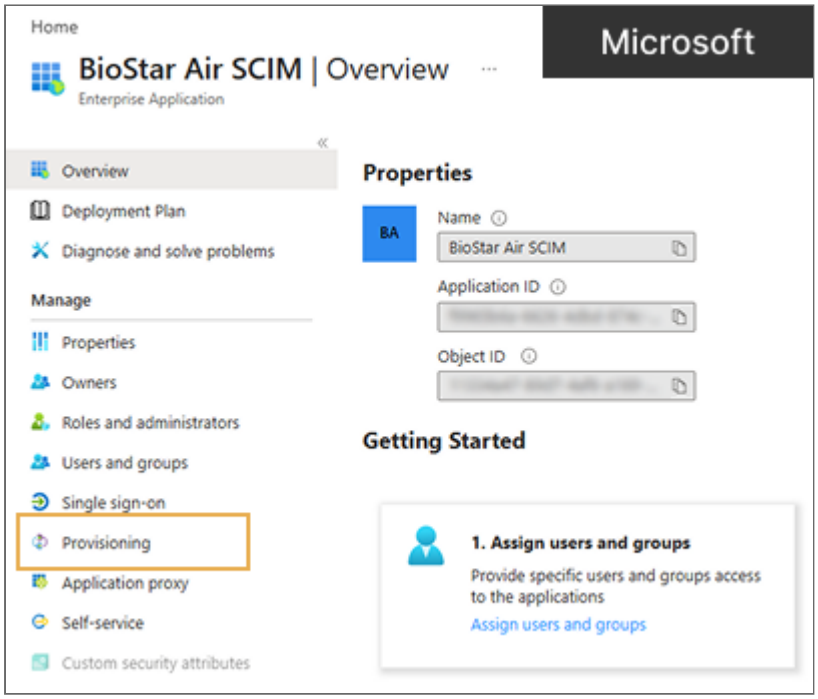
3. Enter the app name as 'BioStar Air SCIM'.

4. Select **Integrate any other application you don't find in the gallery (Non-gallery)**.



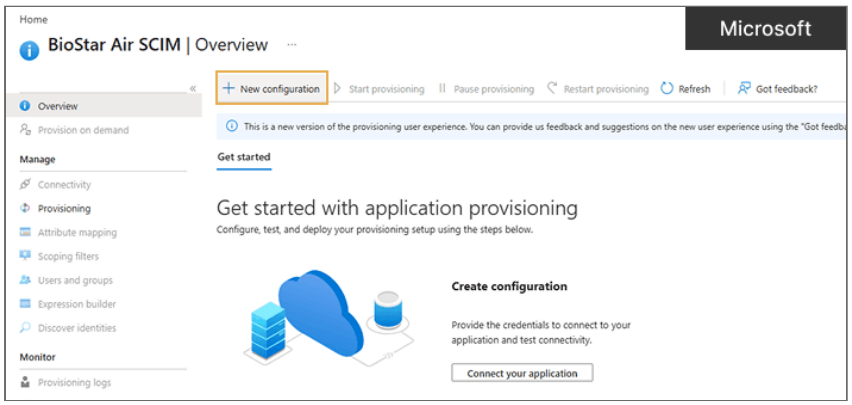
5. Click **Create**.

6. In the BioStar Air SCIM app, click **Manage** → **Provisioning**.

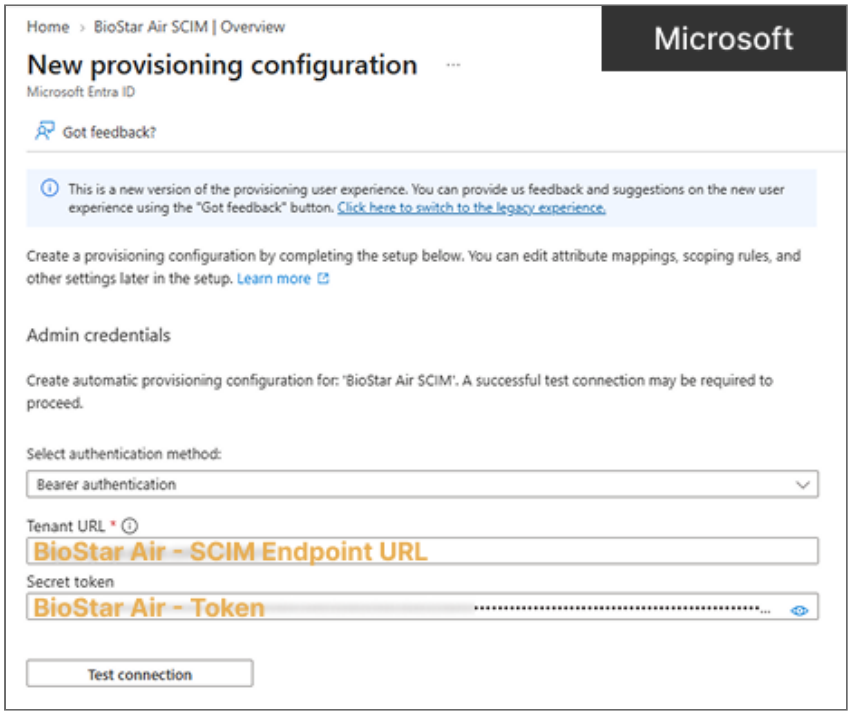


3 Microsoft Entra admin center: Set admin credentials and start provisioning

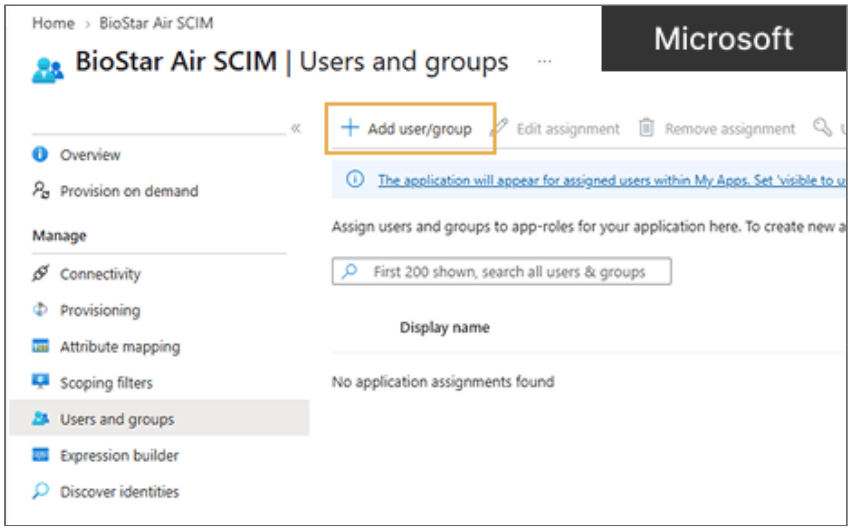
1. Click **New Configuration**.



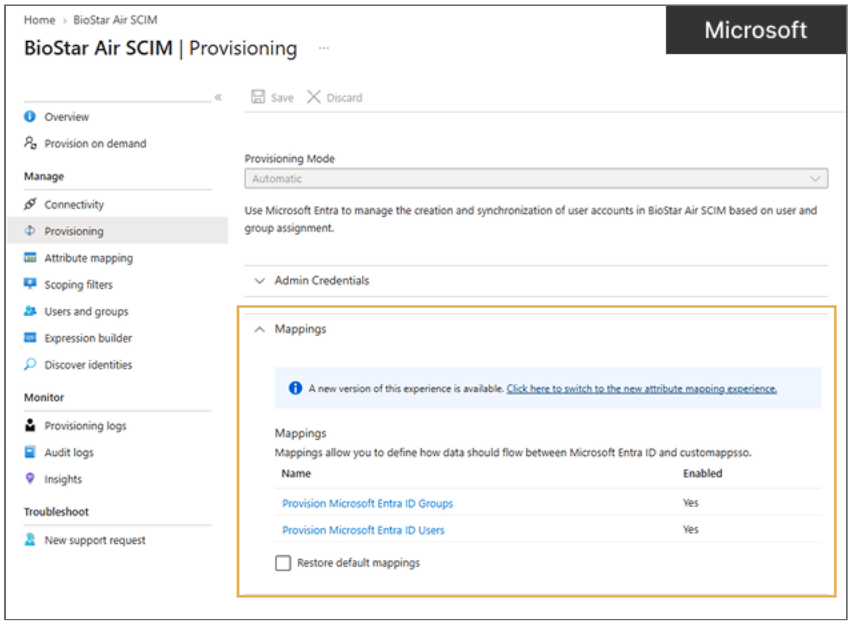
2. In **Admin credentials**, enter the SCIM endpoint URL and token copied in BioStar Air: Copy SCIM token into **Tenant URL** and **Secret token**.



3. Click **Test Connection** to test synchronization.
4. Click **Create**.
5. In **Users and groups**, click **Add user/group**.

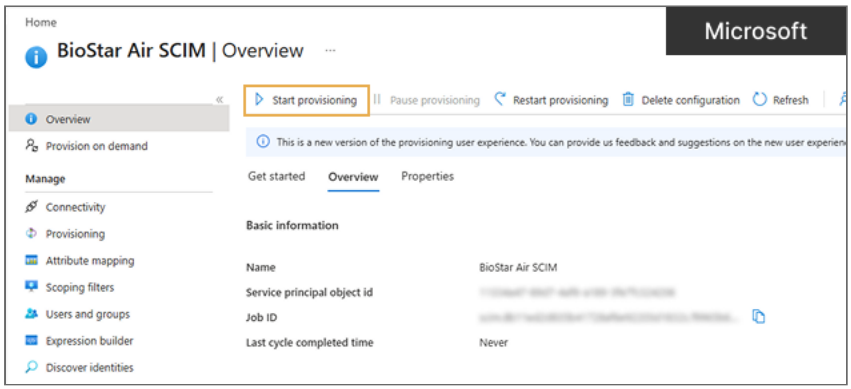


6. Assign the users and security groups to provision.
7. Click **Assign**.
8. Go to **Provisioning** → **Mappings** and confirm that user and group synchronization is enabled.



9. Review the mappings before changing attributes.

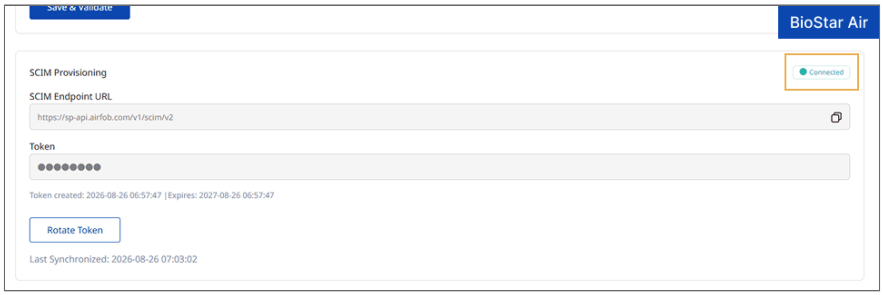
10. In the SCIM app **Overview**, click **Start provisioning**.



> **Info**
>
> It is recommended to start with a small test group. BioStar Air can take up to 40 minutes to reflect group membership changes.

4 BioStar Air: Check the connection

1. Click **Settings** → **Site** in the left sidebar of BioStar Air.
2. Click the **SSO & SCIM** tab.
3. In the **SCIM Provisioning** section, check for the **Connected** indicator.



Group mapping

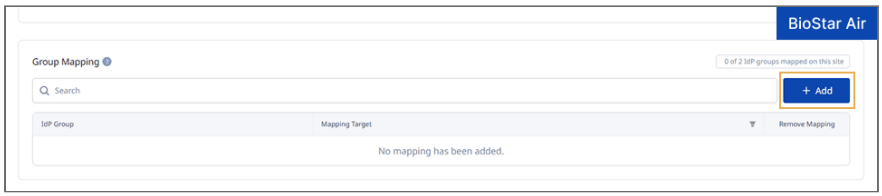
After connecting SSO and SCIM and pushing IdP groups, the site administrator must map them to BioStar Air groups.

Mapping rules

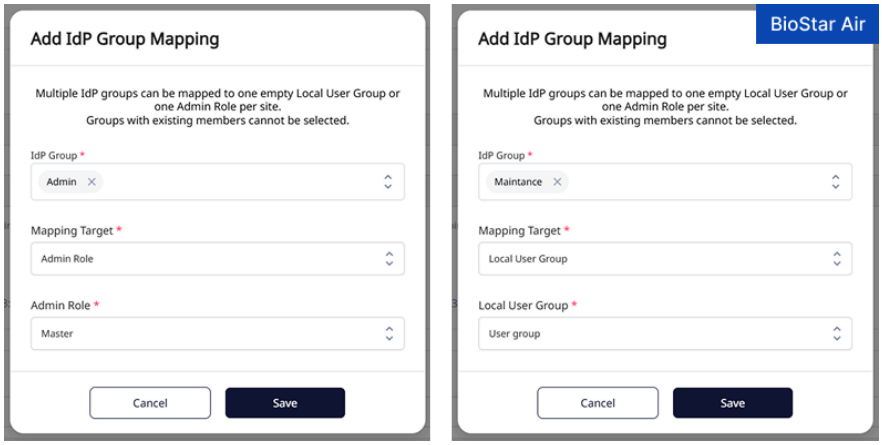
- You can map multiple IdP groups to a single BioStar Air user group.
- A BioStar Air user group must be empty before mapping.
- BioStar Air groups with members cannot serve as mapping targets.
- Only the site master administrator can manage IdP group mapping.
- The system locks the role after mapping an IdP group to the master role.

Map administrator roles and user groups

1. Click **Settings** → **Site** in the left sidebar of BioStar Air.
2. Click the **SSO & SCIM** tab.
3. Go to the **Group Mapping** section and click **Add**.

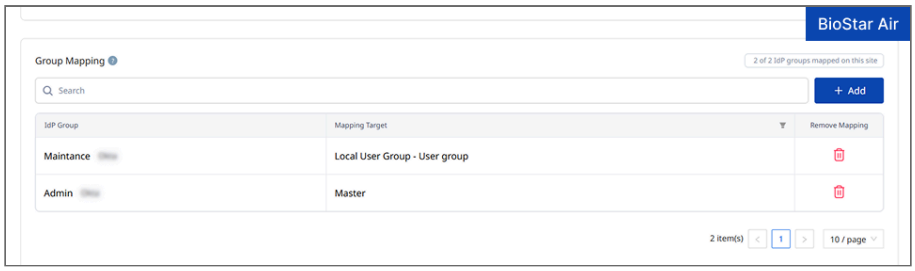


4. From **IdP Group**, select an IdP group.
5. In **Mapping Target**, select **Admin Role** or **Local User Group** based on the selected IdP group.
6. Depending on the mapping target, assign an administrator role or select a user group.



7. Click **Save** to save the mapping.

The **Group Mapping** section shows IdP groups and their mapped BioStar Air groups.

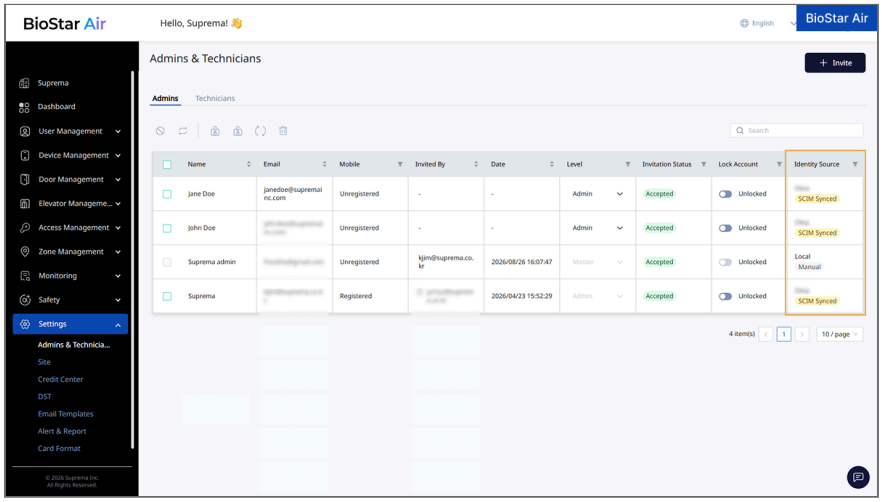


> **Info**
>
> - For more information on administrator roles, see Manage Administrator Accounts and Roles.
> - For more information on user groups, see Manage User Groups.

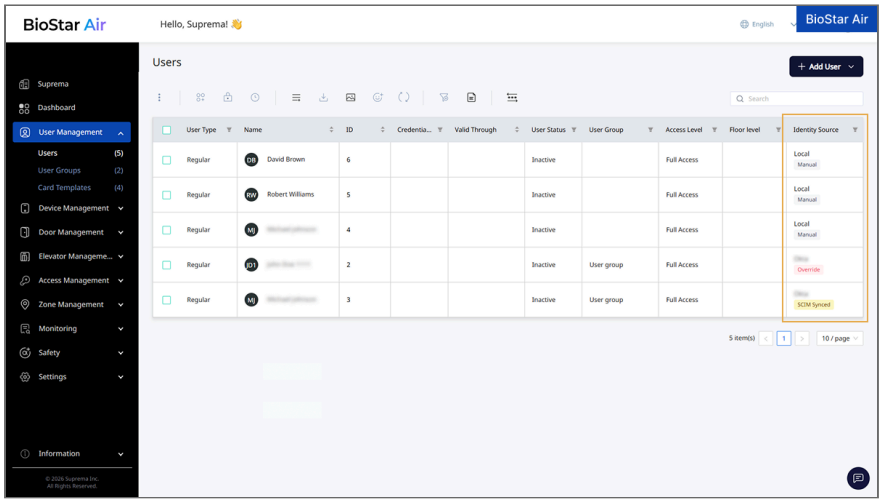
Manage synchronized admins, users, and groups

With provisioning enabled, BioStar Air shows whether each admin, user, and group is local or synchronized from the identity provider.

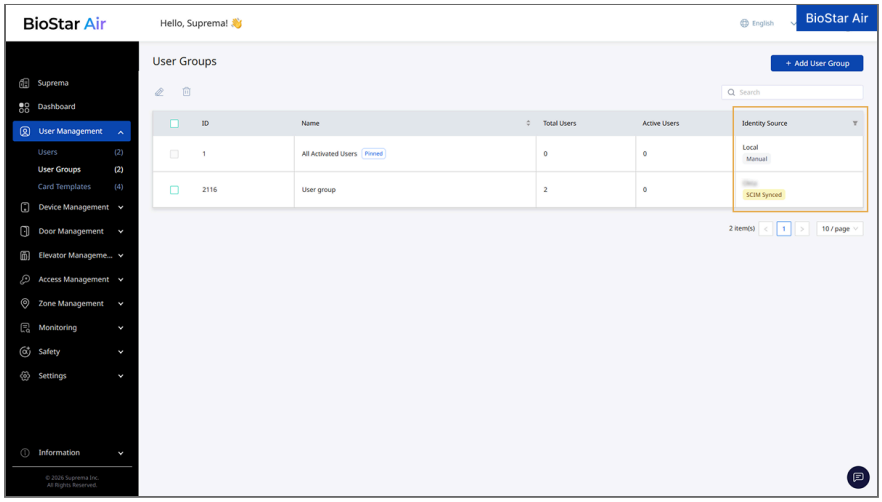
- In **Settings** → **Admins & Technicians**, check the **Identity Source** column in the admin list.



- In **User Management** → **Users**, check the **Identity Source** column in the user list.

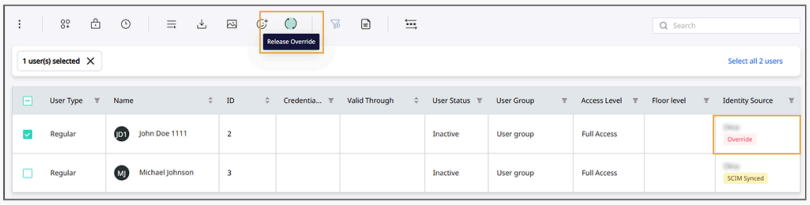


- In **User Management** → **User Groups**, check the **Identity Source** column in the user group list.



How SCIM-synced entries work

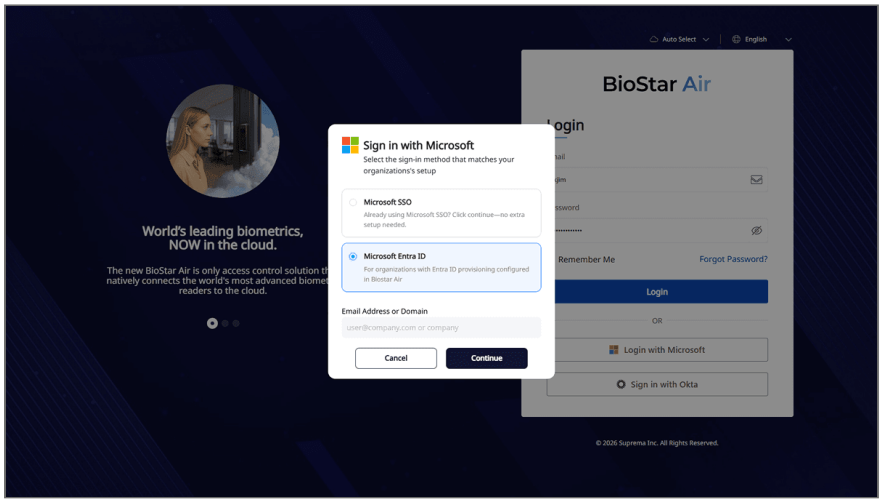
- Manually created users and admins remain manually managed.
- BioStar Air prevents manual deletion of SCIM-synced entries.
- BioStar Air prevents manually adding or removing users from SCIM-synced groups.
- Manually changing a synchronized entry locally sets the status to **Override**. Run **Release Override** to cancel local changes and return the entry to SCIM management.



Sign in with Entra ID

After completing Entra ID SSO connection, users sign in to BioStar Air with a Microsoft account on the sign-in screen.

1. On the BioStar Air sign-in screen, click **Login with Microsoft**.
2. Select **Microsoft Entra ID**.



> If your organization already uses Microsoft SSO, select **Microsoft SSO** to sign in without additional settings.

3. Enter the organization's email address or domain in the **Email Address or Domain** field. (For example, `user@company.com` or `company`)
4. Click **Continue**.
5. On the Microsoft Entra ID sign-in screen, enter your organization's account email address and password.
6. After authentication is complete, you are automatically redirected to BioStar Air, completing the sign-in process.

> **Info**
>
> If Entra ID SSO is not set up for the entered email domain, an error message appears. Contact the site administrator.

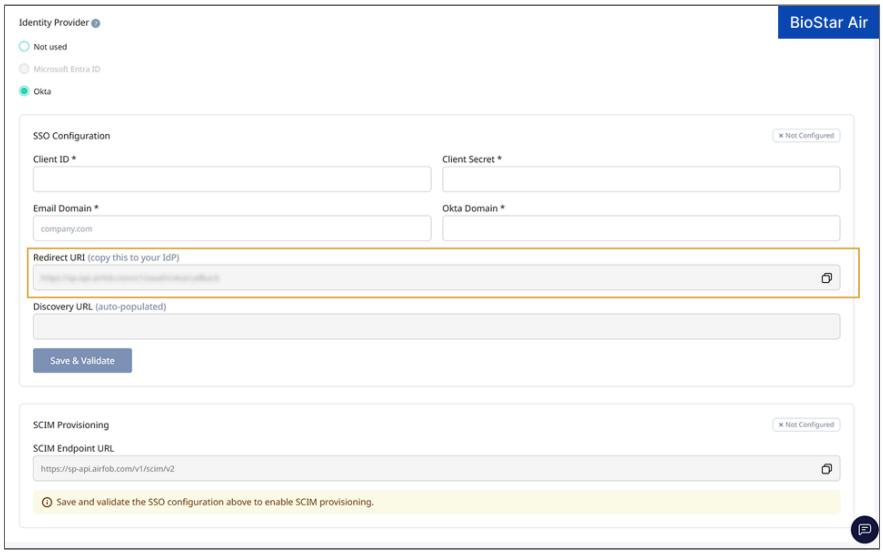
Set Up Okta Integration

To sign in to BioStar Air with Okta, the ID administrator must create an OIDC application in Okta. Link it to the SSO settings in BioStar Air.

Connect Okta SSO

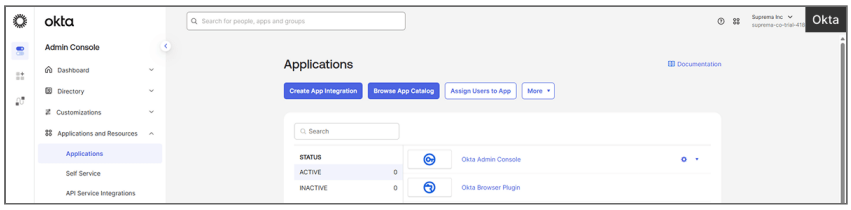
1 BioStar Air: Prepare redirect URI

1. Click **Settings** → **Site** in the left sidebar of BioStar Air.
2. Click the **SSO & SCIM** tab.
3. Select **Okta** under **Identity Provider**.
4. Copy the URI value shown in the **Redirect URI** field.

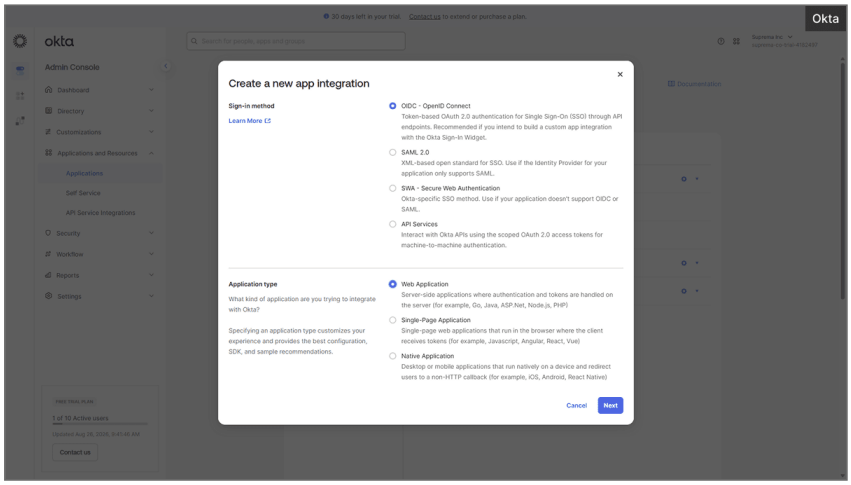


2 Okta: Create an app

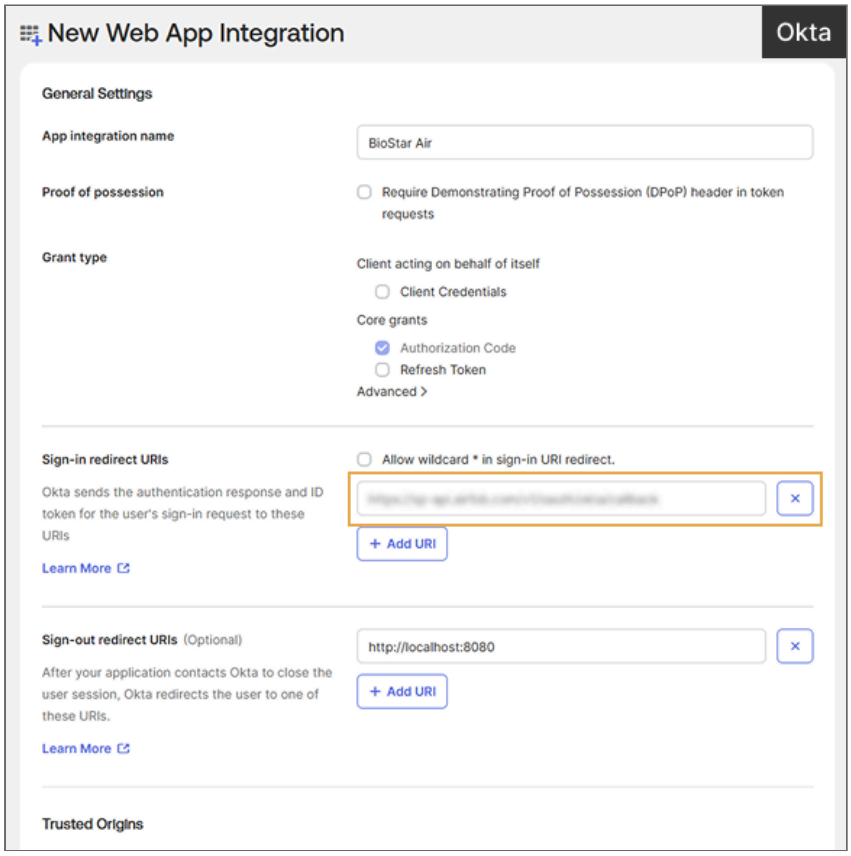
1. Sign in to the **Okta Admin Console**.
2. Go to **Applications and Resources → Applications**.



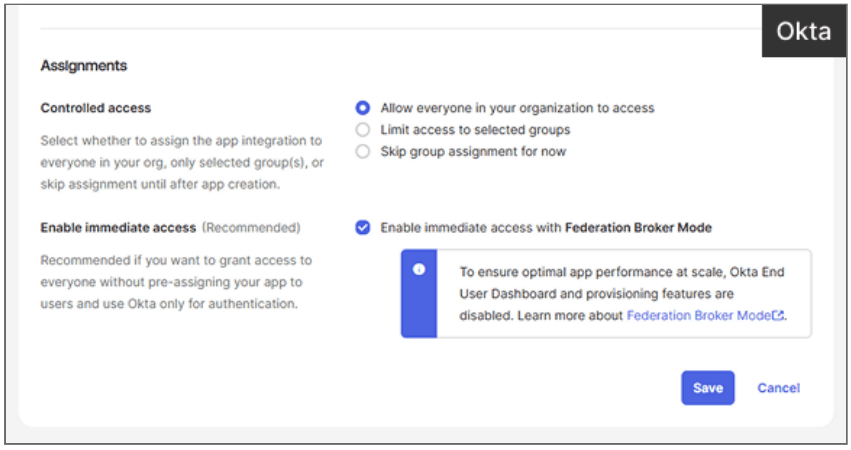
3. Click **Create App Integration**.
4. Under **Sign-in method**, select **OIDC - OpenID Connect**.
5. Under **Application type**, select **Web Application** so you can obtain a client secret.



6. Click **Next**.
7. In **App Integration name**, enter 'BioStar Air'.
8. Paste the URI copied in the BioStar Air: Prepare redirect URI step into the input field under **Sign-in redirect URIs**.



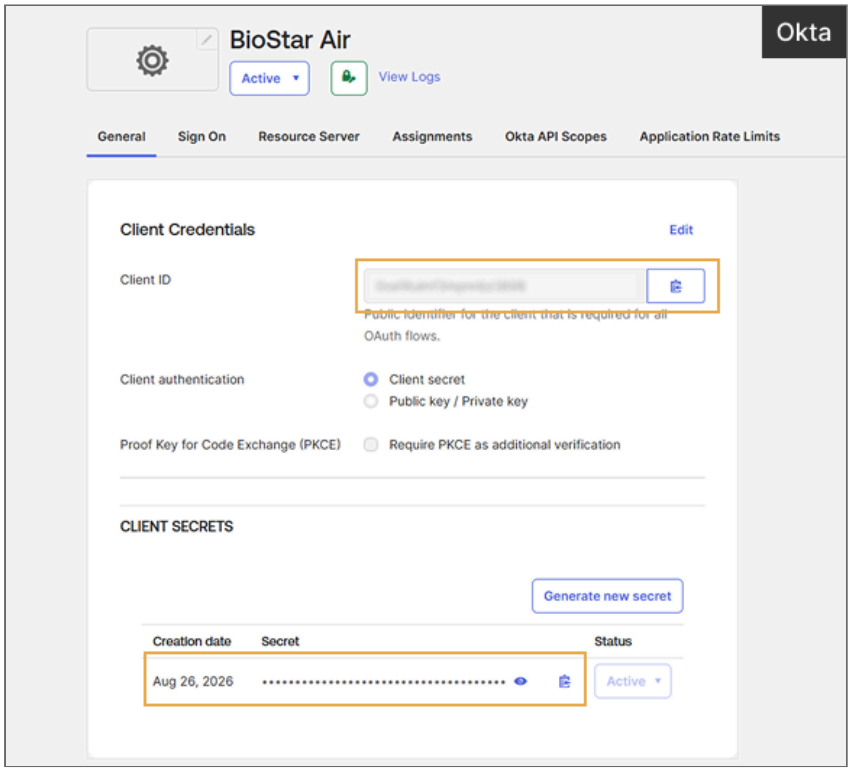
9. Go to **Assignments**, then select **Allow everyone in your organization to access**.



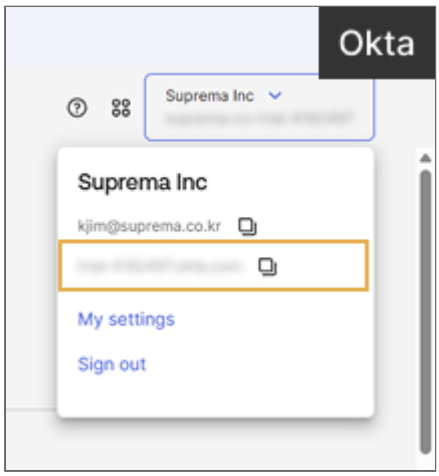
10. Click **Save**.

3 Okta: Copy app client information

1. After creating the application, copy **Client ID** and **Client Secret** from the **General** tab.



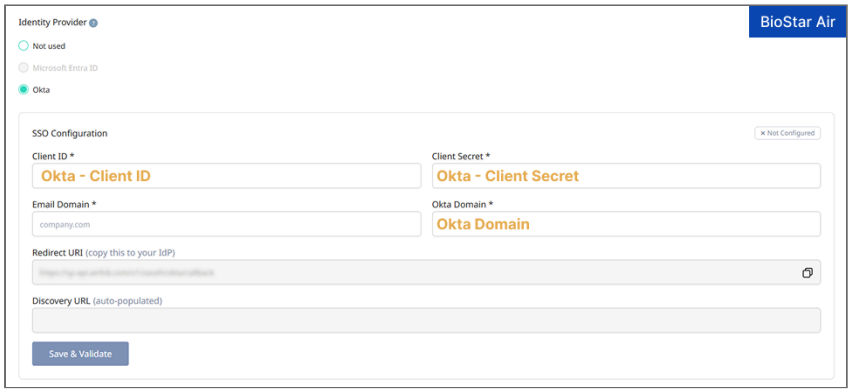
2. Click the profile in the upper-right corner, then copy **Okta Domain**.



Enter the copied **Client ID**, **Client Secret**, and **Okta Domain** in the next step.

4 BioStar Air: Configure SSO

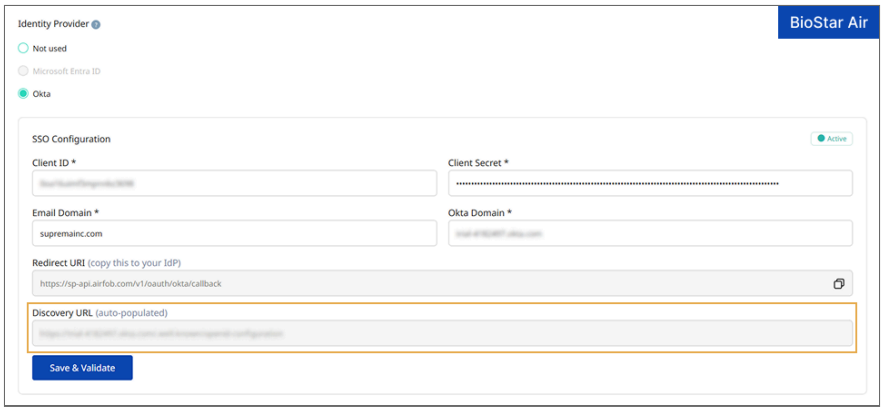
1. Return to the BioStar Air settings page, then enter the values copied in the Okta: Copy app client information step into each field.



- **Client ID**: Client ID
- **Client Secret**: Client Secret
- **Okta Domain**: Okta Domain

2. In the **Email Domain** field, enter your organization's email domain.
3. Click **Save & Validate**.

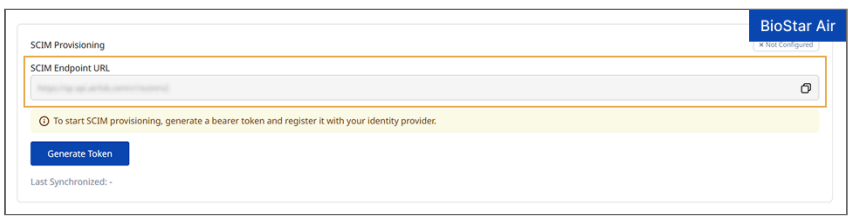
After the system saves and verifies successfully, it automatically generates the value for **Discovery URL**.



Connect Okta SCIM provisioning

1 BioStar Air: Copy SCIM token

1. Click **Settings** → **Site** in the left sidebar of BioStar Air.
2. Click the **SSO & SCIM** tab.
3. In the **SCIM Provisioning** section, copy the **SCIM Endpoint URL** value.



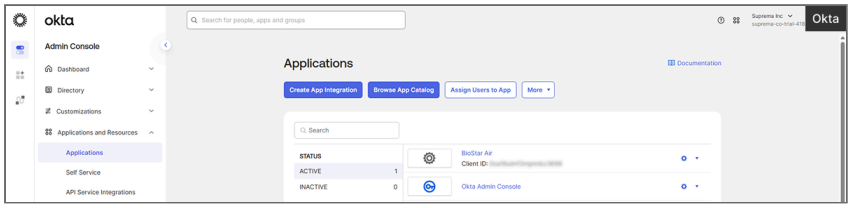
4. Click **Generate Token**.

5. In the Token Generation Complete dialog box, copy the token.

> **Info**
>
> - Copy the generated token immediately. Copy the token only when you generate it. After you close the dialog box, you cannot copy the token again.
> - If you lose the token, click **Rotate Token** to generate a new token. Enter the new token in the identity provider again.
> - In the next step, enter the SCIM endpoint URL and token copied in this step.

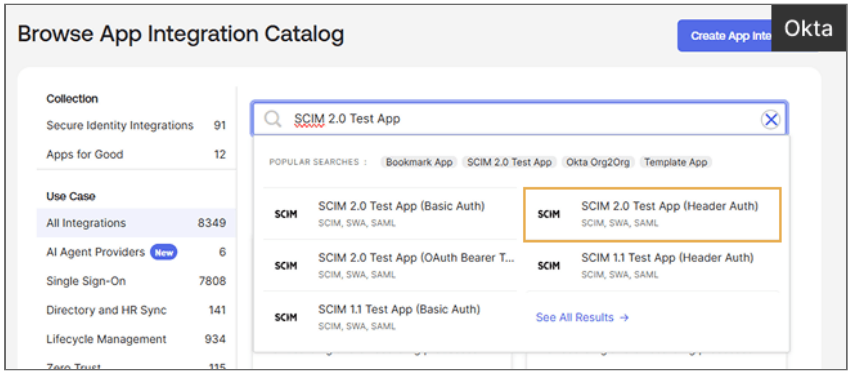
2 Okta: Create a SCIM provisioning app

1. In the **Okta Admin Console**, go to **Applications and Resources** → **Applications**.



2. Click **Browse App Catalog**.

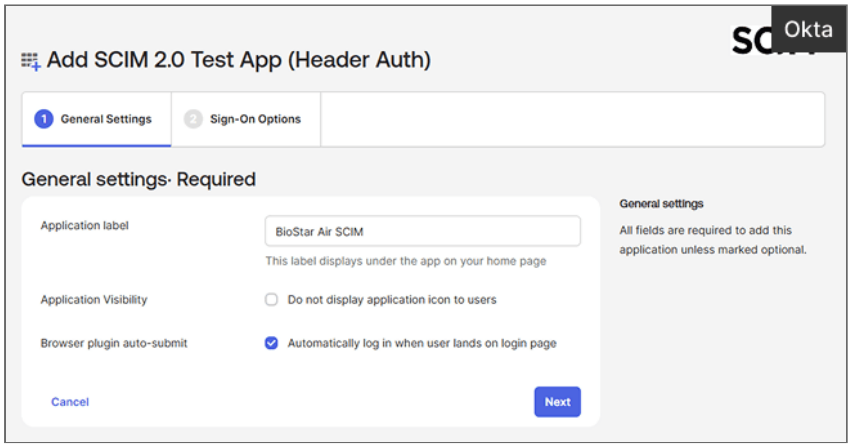
3. Search for 'SCIM 2.0 Test App'.



4. In the search results, select **SCIM 2.0 Test App (Header Auth)**.

5. Click **Add Integration**.

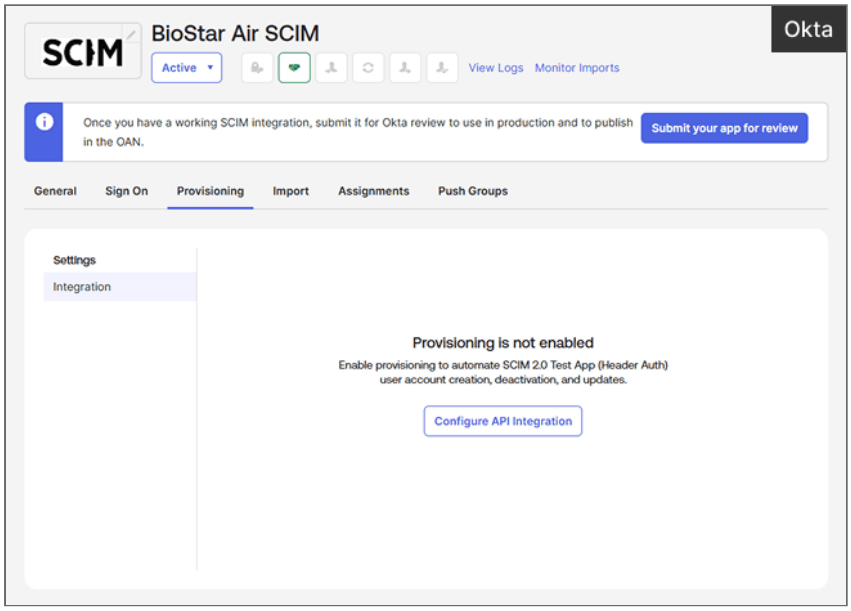
6. In the **Application label** field, enter 'BioStar Air SCIM'.



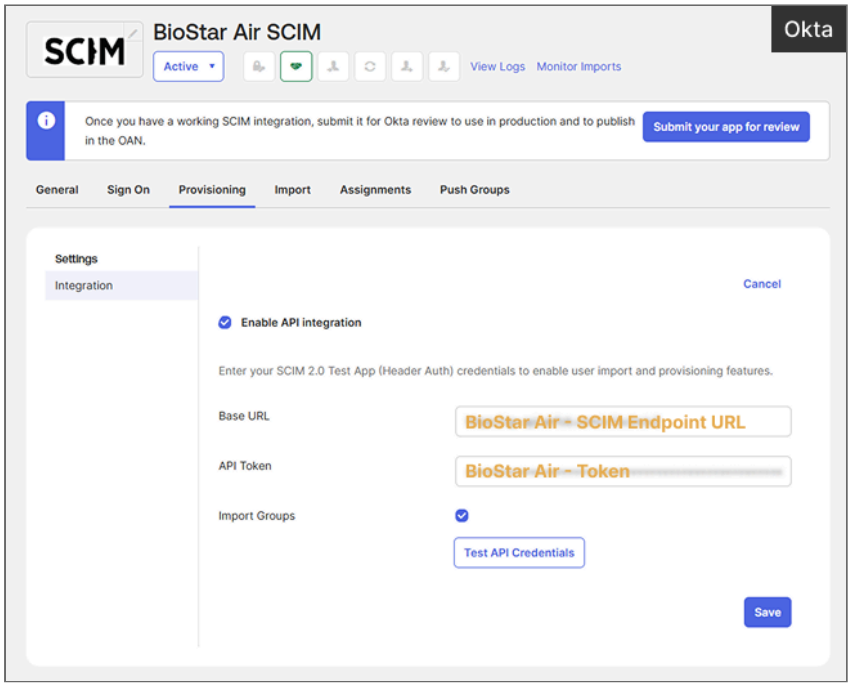
7. Click **Next**.
8. In **Sign-on options**, scroll down without changing settings, and click **Done**.

3 Okta: API integration settings

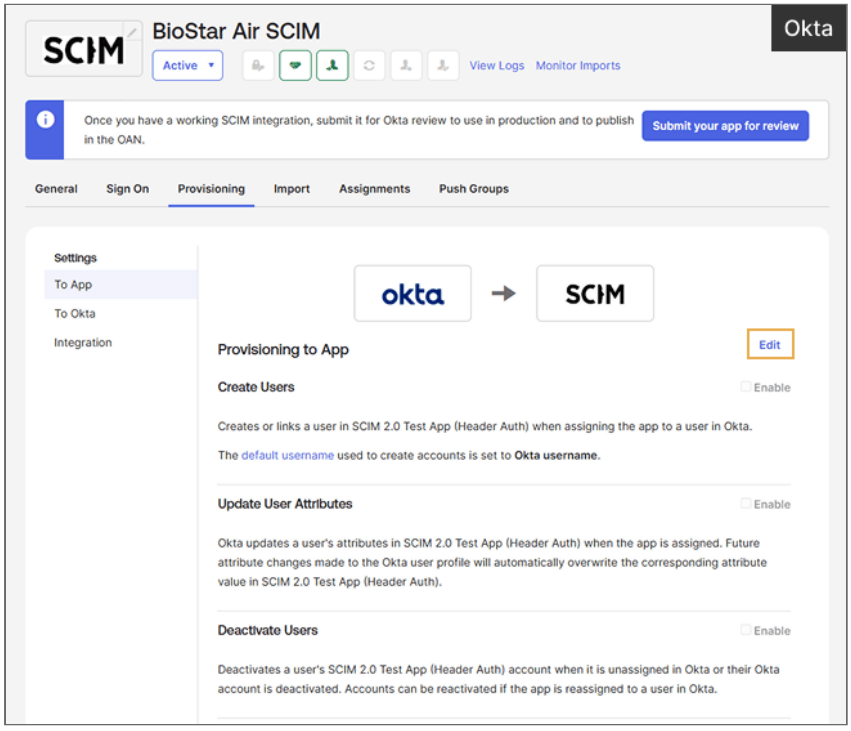
1. After creating the provisioning app, click the **Provisioning** tab.



2. Click **Configure API Integration**.
3. Click **Enable API integration**.
4. Enter the SCIM endpoint URL and SCIM bearer token from BioStar Air: Copy SCIM token into the **Base URL** and **API Token** fields.

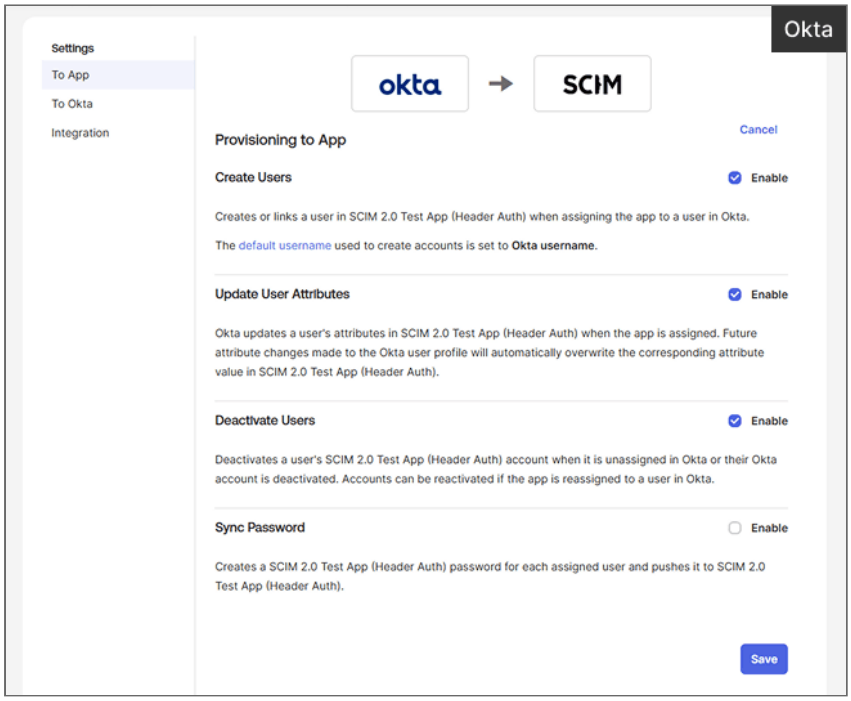


5. To test synchronization, click **Test API Credentials**.
6. Click **Save**.
7. Click the **Provision** tab to set group push behavior.
8. Click **Edit**, then enable the following attributes.



- **Create Users**
- **Update User Attributes**
- **Deactivate Users**

9. Click **Save** to save the changes.

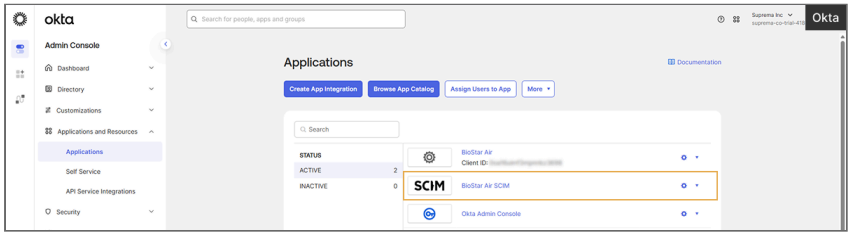


Push IdP groups to BioStar Air

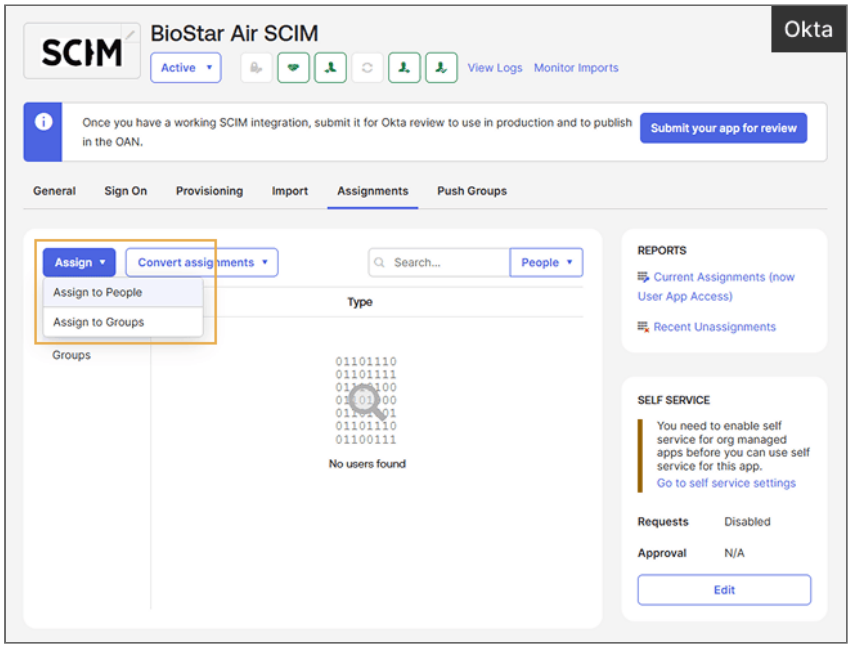
To push IdP groups to BioStar Air, first prepare user groups and users in Okta. After preparing user groups and users, push them to BioStar Air via SCIM.

1 Okta: Assign user groups

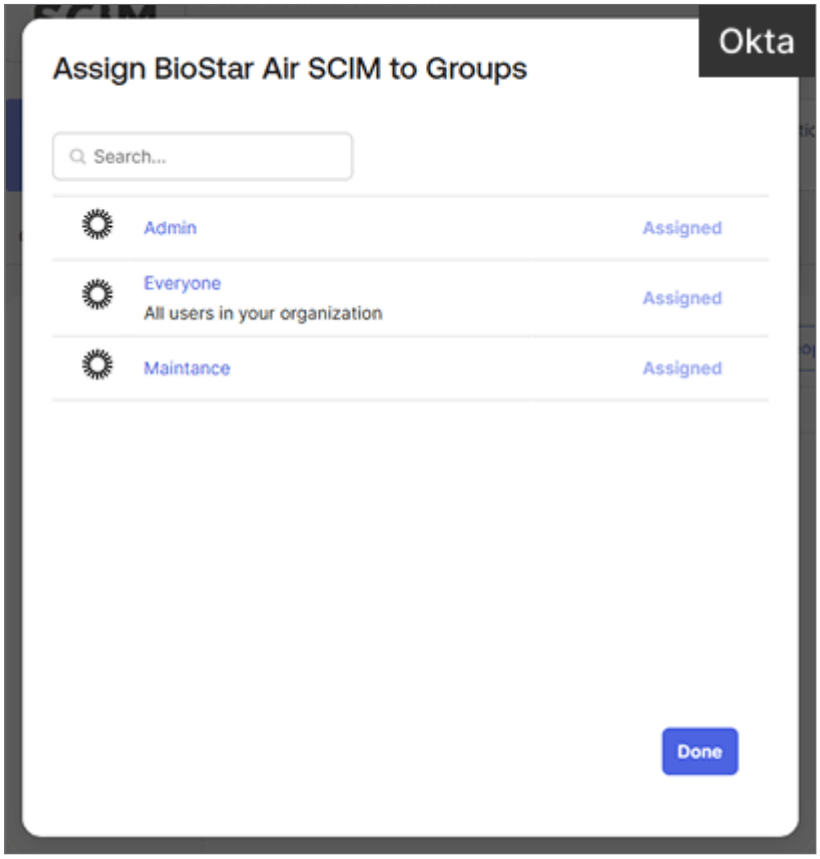
1. Sign in to the **Okta Admin Console**.
2. Go to **Applications and Resources** → **Applications**.
3. Select the SCIM application.



4. Click the **Assignments** tab.
5. Click **Assign** → **Assign to Groups**.

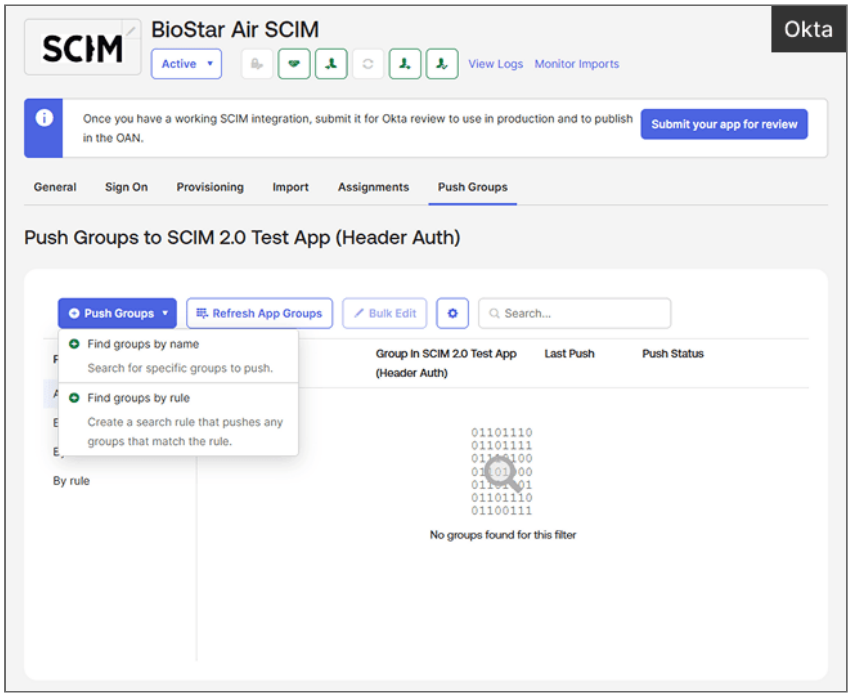


6. In the user group to assign to the SCIM application, click **Assign**.
7. After assigning the group, click **Done**.

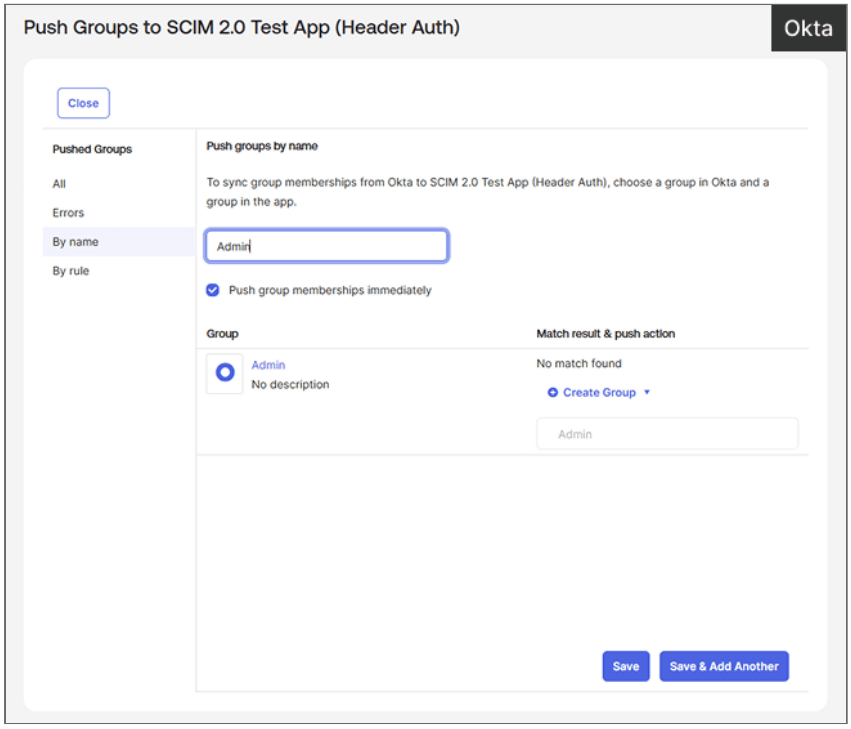


2 Okta: Push user groups

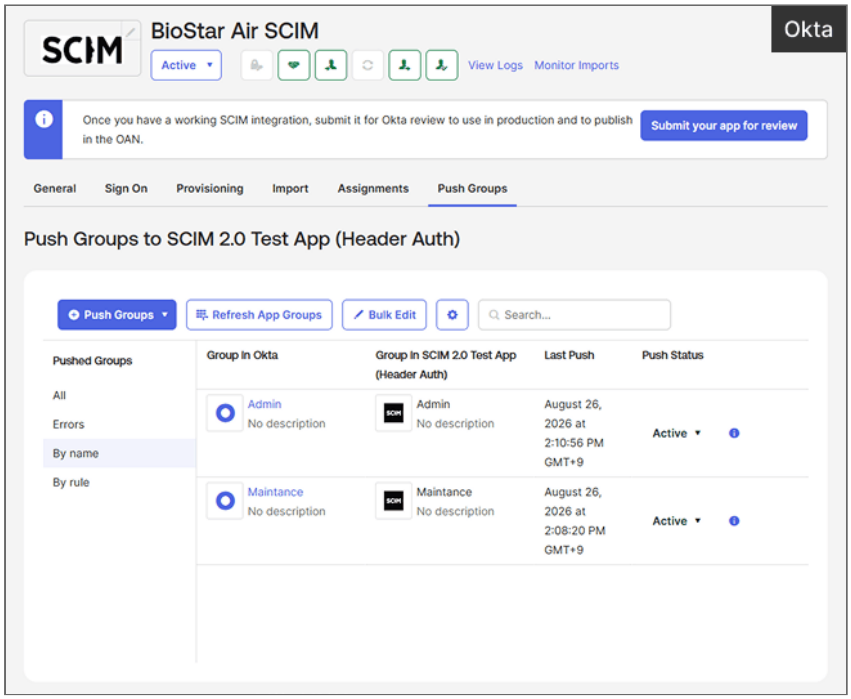
1. Click the **Push Groups** tab.
2. Click **Push Groups** → **Find groups by name**.



3. In the input field, enter the group name to push.
4. When a matching user group appears, select it.

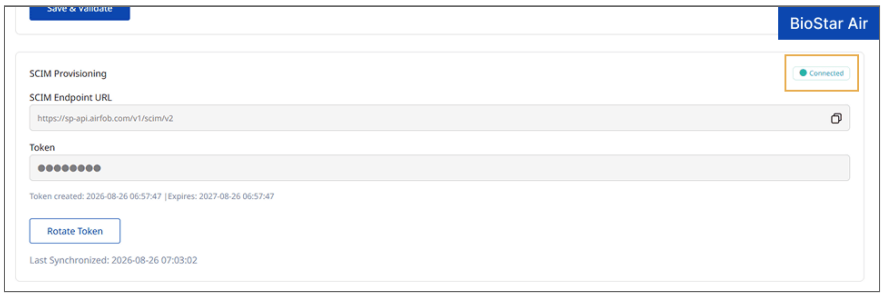


5. After selecting a user group, click **Save** or **Save & Another** to add it.
6. Check the pushed user groups on the **Push Groups** tab.



3 BioStar Air: Check the connection

1. Click **Settings** → **Site** in the left sidebar of BioStar Air.
2. Click the **SSO & SCIM** tab.
3. In the **SCIM Provisioning** section, check for the **Connected** indicator.



Group mapping

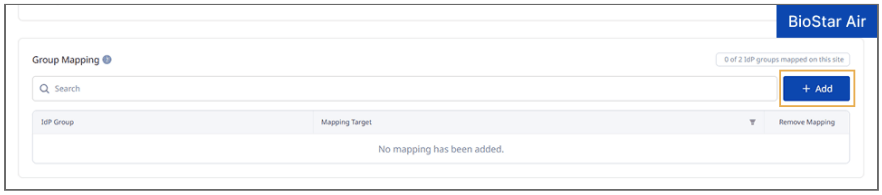
After connecting SSO and SCIM and pushing IdP groups, the site administrator must map them to BioStar Air groups.

Mapping rules

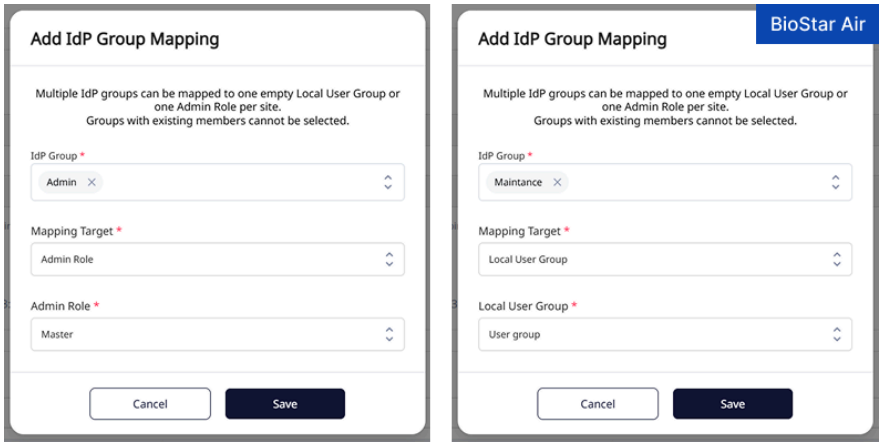
- You can map multiple IdP groups to a single BioStar Air user group.
- A BioStar Air user group must be empty before mapping.
- BioStar Air groups with members cannot serve as mapping targets.
- Only the site master administrator can manage IdP group mapping.
- The system locks the role after mapping an IdP group to the master role.

Map administrator roles and user groups

1. Click **Settings** → **Site** in the left sidebar of BioStar Air.
2. Click the **SSO & SCIM** tab.
3. Go to the **Group Mapping** section and click **Add**.

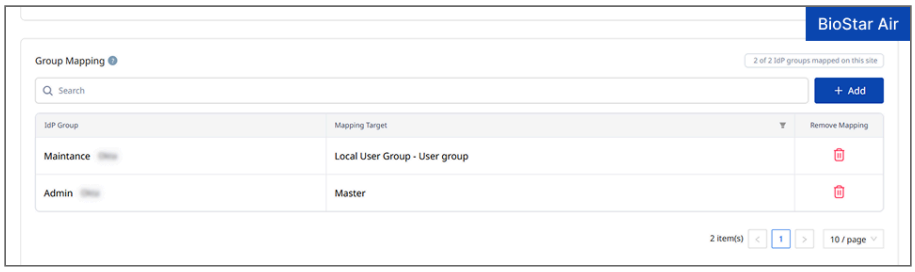


4. From **IdP Group**, select an IdP group.
5. In **Mapping Target**, select **Admin Role** or **Local User Group** based on the selected IdP group.
6. Depending on the mapping target, assign an administrator role or select a user group.



7. Click **Save** to save the mapping.

The **Group Mapping** section shows IdP groups and their mapped BioStar Air groups.

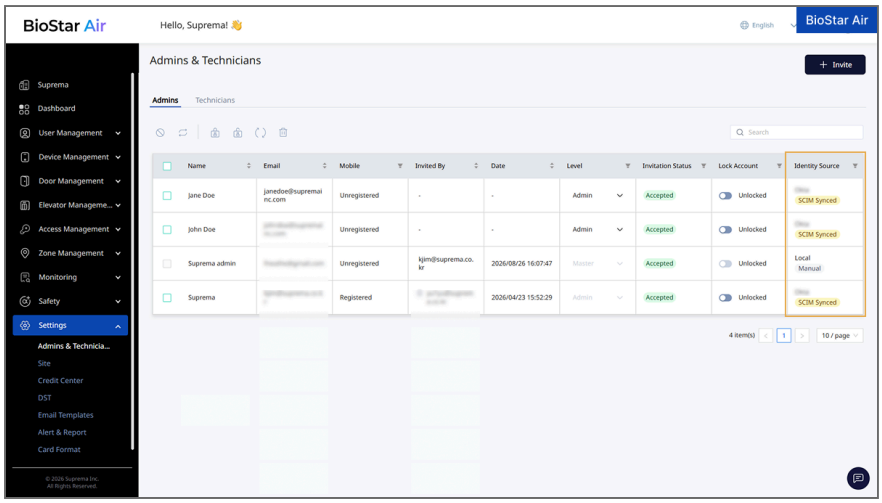


> **Info**
>
> - For more information on administrator roles, see Manage Administrator Accounts and Roles.
> - For more information on user groups, see Manage User Groups.

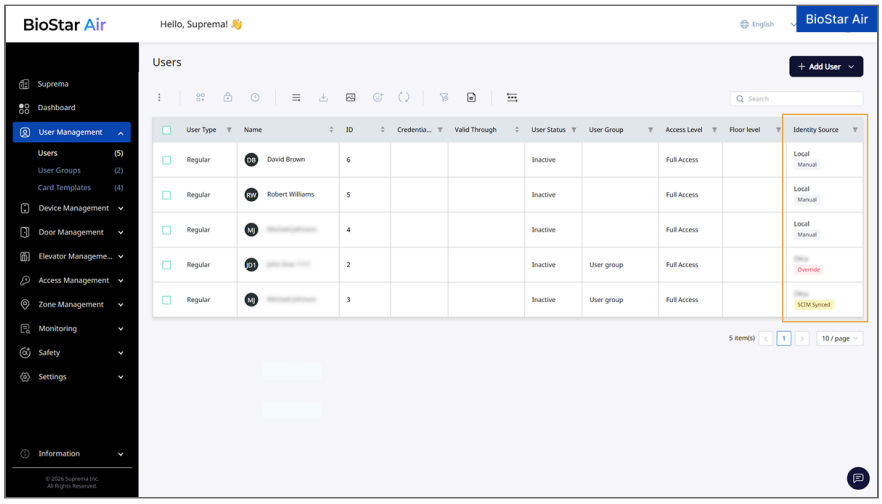
Manage synchronized admins, users, and groups

With provisioning enabled, BioStar Air shows whether each admin, user, and group is local or synchronized from the identity provider.

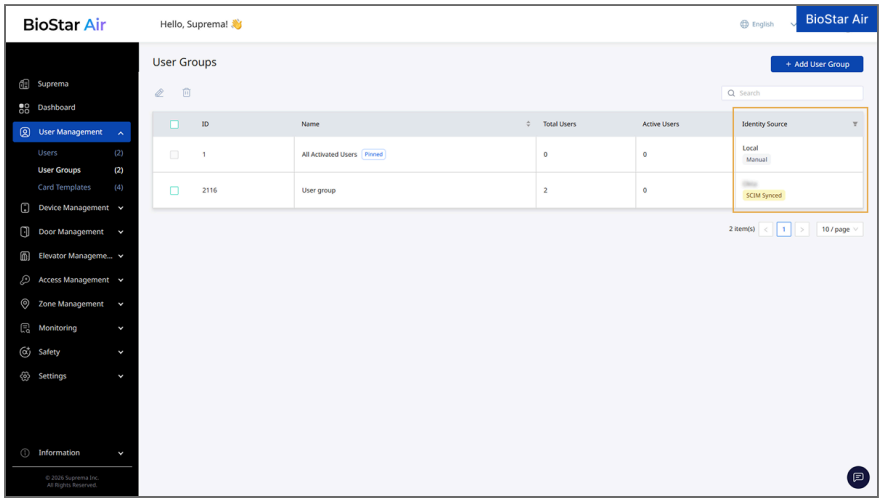
- In **Settings** → **Admins & Technicians**, check the **Identity Source** column in the admin list.



- In **User Management** → **Users**, check the **Identity Source** column in the user list.

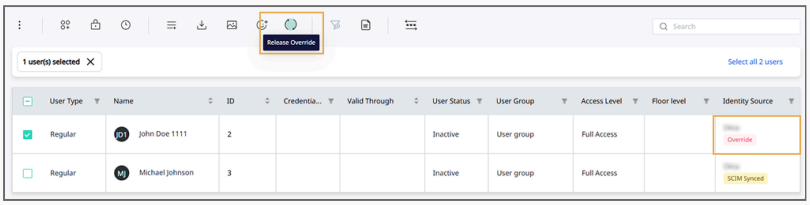


- In **User Management** → **User Groups**, check the **Identity Source** column in the user group list.



How SCIM-synced entries work

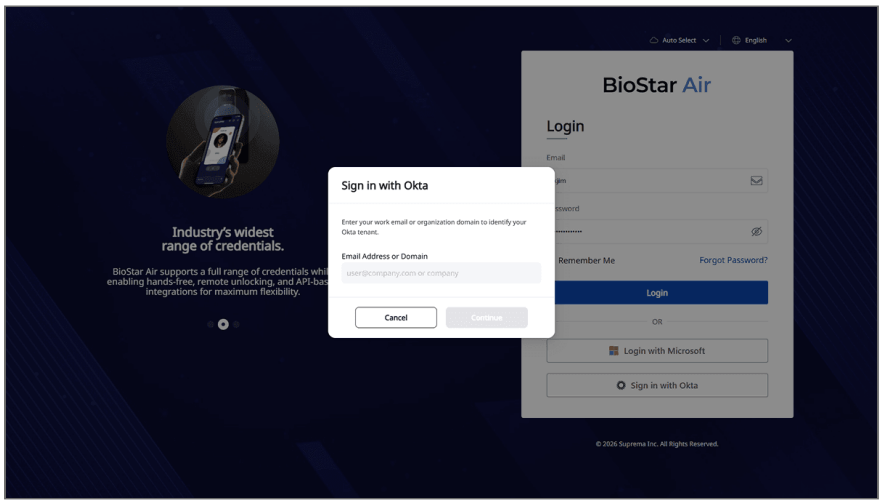
- Manually created users and admins remain manually managed.
- BioStar Air prevents manual deletion of SCIM-synced entries.
- BioStar Air prevents manually adding or removing users from SCIM-synced groups.
- Manually changing a synchronized entry locally sets the status to **Override**. Run **Release Override** to cancel local changes and return the entry to SCIM management.



Sign in to Okta

After completing the Okta SSO connection, users can sign in with their Okta accounts on the BioStar Air login screen.

1. On the BioStar Air login screen, click **Sign in with Okta**.



2. Enter the organization's email address or domain in the **Email Address or Domain** field. (For example, `user@company.com` or `company`)
3. Click **Continue**.
4. When the Okta sign-in page opens, enter the email address and password for the organization account.
5. After authentication is complete, you are automatically redirected to BioStar Air, completing the sign-in process.

Info

If Okta SSO is not set up for the entered email domain, an error message appears. Contact the site administrator.

Additional Site Configuration

In addition to site default settings, you can configure detailed features that affect the BioStar Air service, such as time

policies, email templates, alert delivery methods, and time and attendance records. You can add custom Wiegand card formats or directly configure how time and attendance are managed and how reports are generated.

Daylight Saving Time (DST)

Use the Daylight Saving Time (DST) settings to configure how the site adjusts its time. This is especially important for ensuring consistent and accurate time tracking when managing a site that has devices and records across multiple time zones.

For accurate time management in BioStar Air, **DST settings in three places** are required:

- **DST Profile**: Defines the start and end date and time of DST for each time zone.
- **Site Time**: Set the time zone applied to the site and event logs.
- **Device Time**: Configure each individual reader so it adjusts its clock correctly.

All three settings must be configured correctly for sites located in time zone that observes Daylight Saving Time.

Tip
Watch the following video for a guide to configuring Daylight Saving Time (DST) settings.

Info
Consider the following when reviewing Event Logs.

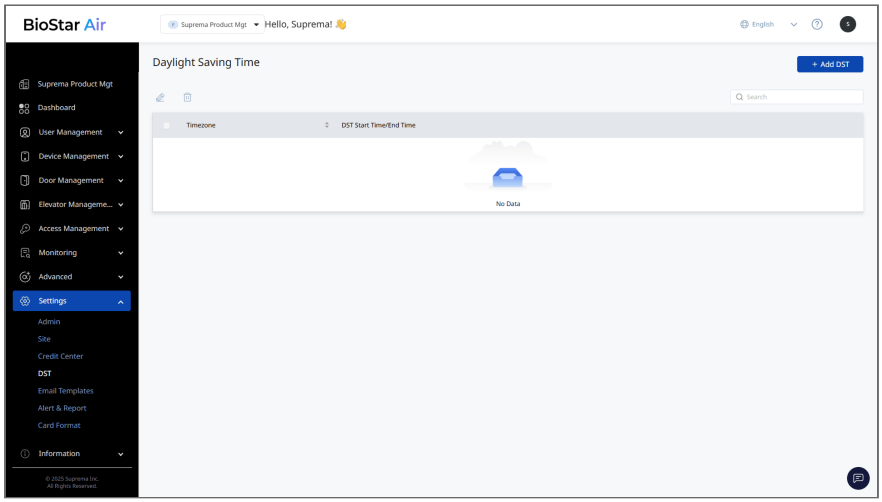
- If device time is configured, event log timestamps adjust to each device's DST time.
- If site time is configured, timestamps adjust according to the site's DST configuration instead of each device.

Step 1: Create DST profile

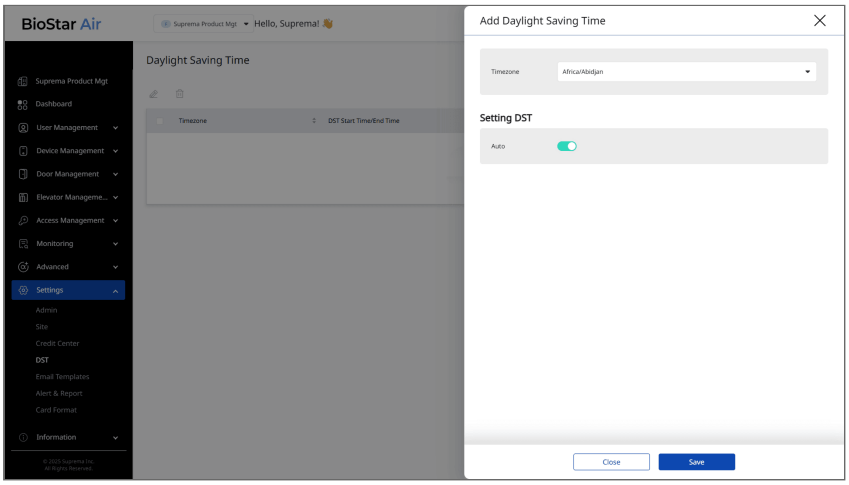
A DST profile defines the date and time when DST starts and ends for a specific time zone. You must create a DST profile for each time zone where the site and readers are located.

Add new profile

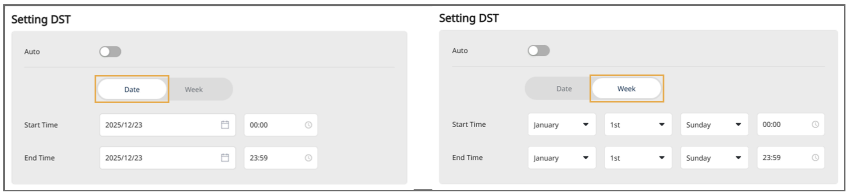
1. Click **Settings** → **DST** in the left sidebar.
2. Click **Add DST** at the top right of the screen.



3. Select the desired item from **Timezone** when the **Add Daylight Saving Time** panel appears.
4. Select automatic or manual configuration in **Setting DST**.
   - **Auto**: The DST configuration for the selected time zone is added automatically. The start and end dates for DST are determined by the standard rules for that time zone.



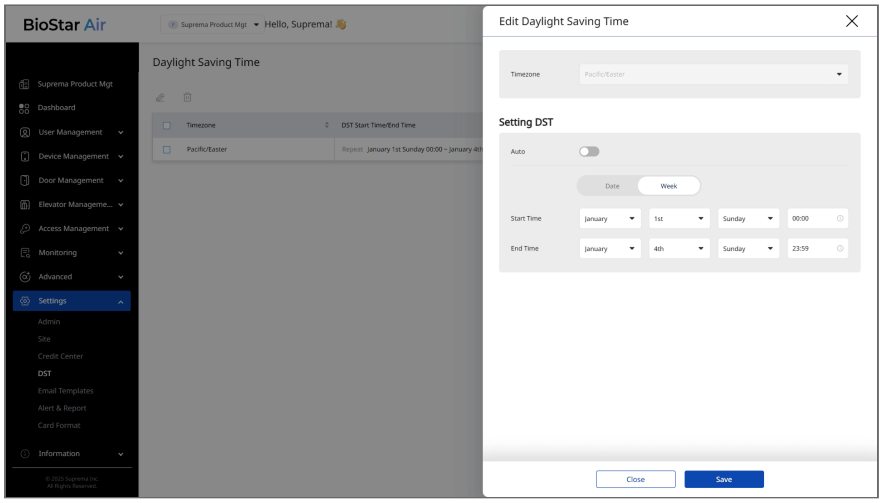
   - **Manual**: Set the appropriate start and end times for the time zone to configure manually.



     – **Date**: Select the dates when DST starts and ends.
     – **Week**: Select the weeks when DST starts and ends.
5. Click **Save** at the bottom to save the DST profile.

Edit existing DST profile

1. Click **Settings** → **DST** in the left sidebar.
2. Click the DST profile you want to edit in the list. Alternatively, select the checkbox and click ✎ at the top.
3. Modify the start and end times when the **Edit Daylight Saving Time** panel appears.



The image above is an example screen and may differ from the actual screen.

4. Click **Save** at the bottom to save the changes.

Delete DST profile

1. Click **Settings** → **DST** in the left sidebar.
2. Click the checkbox for the DST profile you want to delete in the list. You can select one or more profiles.
3. Click 🗑 at the top of the screen.
4. When the message window appears, click the **Yes** button.

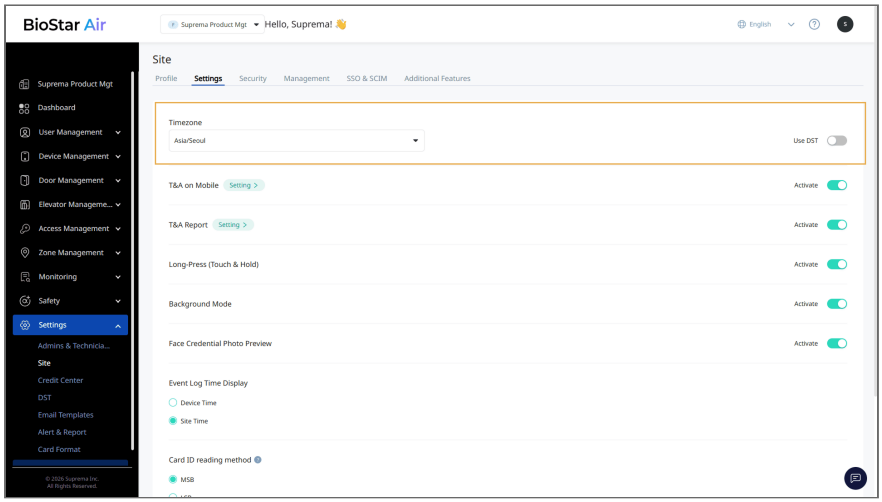
Step 2: Site time settings

The site time determines the default time zone used by the entire system. The following items are affected by this setting:

- Event log timestamps
- Reports and monitoring data
- Default time zone applied when registering a new device

Follow the instructions below to set the site's time zone and enable DST.

1. Click **Settings** → **Site** in the left sidebar.
2. Click **Settings** tab.
3. Select the desired time zone in **Timezone**.



4. Enable **Use DST** to apply daylight saving time to the selected time zone.

> **Caution**
>
> If the **Use DST** option is not enabled in a time zone where DST applies, the system will not automatically adjust the time, and event logs may appear incorrectly.

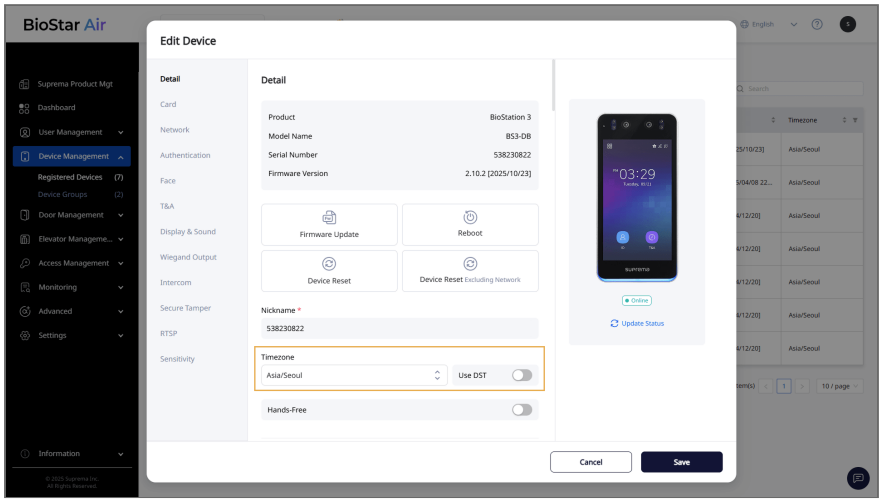
Step 3: Enable DST for devices

Each device connected to BioStar Air maintains its own clock, which is used for access control and attendance records. Configure DST settings for any device located in a time zone where DST applies.

Devices with screens, such as BioStation 3, displays the time. Devices without screens, such as XPass 2, maintain their internal clocks for access control and time and attendance records.

Set DST on all devices, regardless of whether they have a display, to ensure event logs, access records, and attendance data are recorded accurately.

1. Click **Device Management** → **Registered Devices** in the left sidebar.
2. Click the device to which you want to apply the DST settings in the list.
3. Select the desired time zone in the **Timezone** section, and enable the **Use DST** option.



> This setting is enabled by default for time zones where DST applies.

4. Click **Save** at the bottom to save the changes.

> **Info**
> If the device time is not set correctly, the following issues may occur:
>
> - **Access Denied Error**: The access time is set to start at 07:00 AM, but if the device thinks it is 06:00 AM, user entry will be denied.
> - **Schedule error**: The lock/unlock at the scheduled time may not be accurate.
> - **Record error**: The times in the event log and the time and attendance records do not match the actual time.

Checklist

To ensure accurate timekeeping in regions that observe Daylight Saving Time (DST), make sure you have completed all three of the following steps.

- **Create DST profiles**: Have you created the DST profiles needed for each time zone?
- **Site time settings**: Have you set the site's time zone and enabled the **Use DST** option?
- **Device DST settings**: Have you set each device's time zone and enabled the **Use DST** option?

If all three are configured correctly, the event logs, access times, and attendance records will all show the correct time.

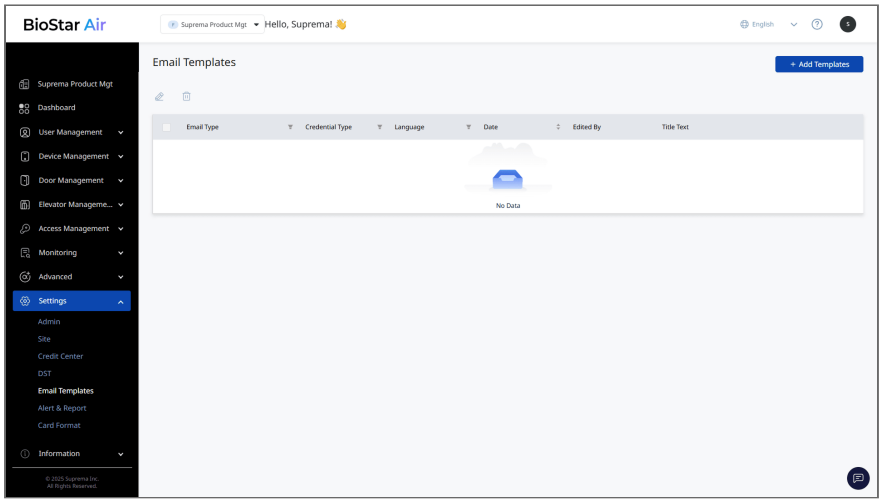
Customize Email Templates

Use the email template feature to customize emails sent to site users so they reflect your company's brand and messaging. Email templates include invitations, activation emails, and other notifications.

> **Tip**
> Watch the following video to learn how to configure email templates.

Add email templates

1. Click **Settings** → **Email Templates** in the left sidebar.
2. Click **Add Templates** at the top right of the screen.

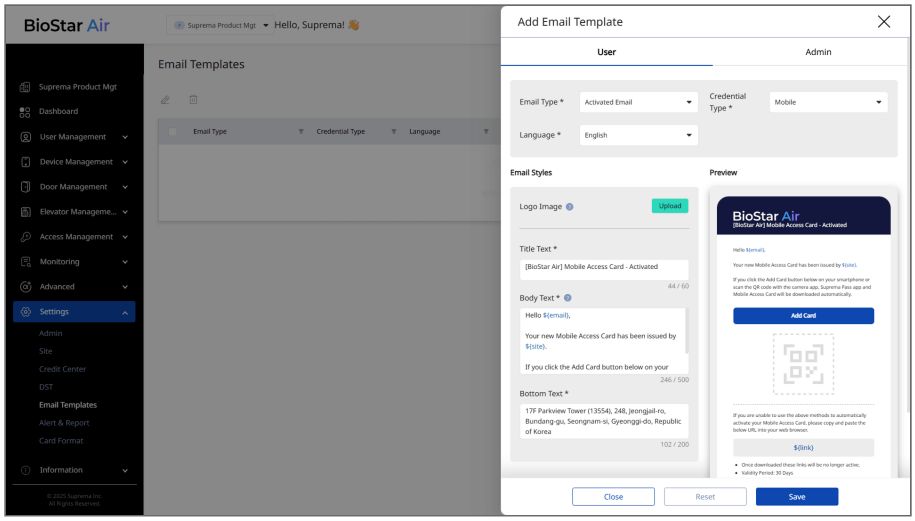


3. When the **Add Email Template** panel appears, set each item. Select the **User** or **Admin** tab to configure user or administrator email templates.

> **Info**
>
> Create separate email templates for each language. Select the language in **Language**. Supported languages are as follows:
>
> > *English, 한국어, 日本語, Nederlands, Español, Português*
>
> More languages will be supported.

User

Customize the email templates sent to users.



- **Email Type**: Select the email template type to create. Available options are as follows:
  - **Activated Email**: Typically used as an invitation to download a mobile card.
  - **Reactivated Email**: Sends a notification to the user that the mobile card has been reactivated.
  - **Reissued Email**: Used when issuing a new mobile card.
  - **Delete Email**: Sends a notification to the user about card deletion.
  - **Suspended Email**: Notifies the user that the card has been suspended.

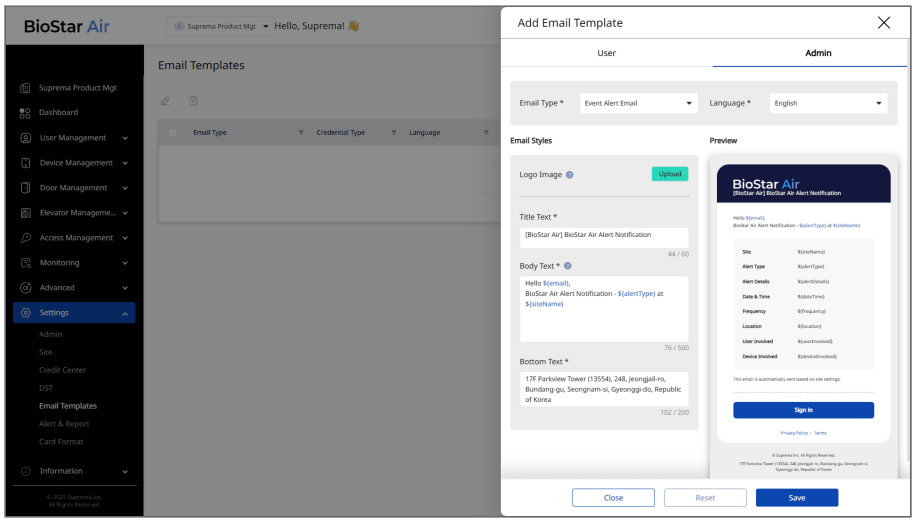
  - **Face Registration Request Email**: Used to request that the user upload a face photo.

- **Credential Type**: Can be selected for email types that allow mobile card downloads, such as **Activated Email** and **Reissued Email**.
  - **Mobile**
  - **Web QR**
  - **Link Pass**

> For more information about credential types, see User Card and Credential Types.

Admin

Customize the email templates sent to administrators.

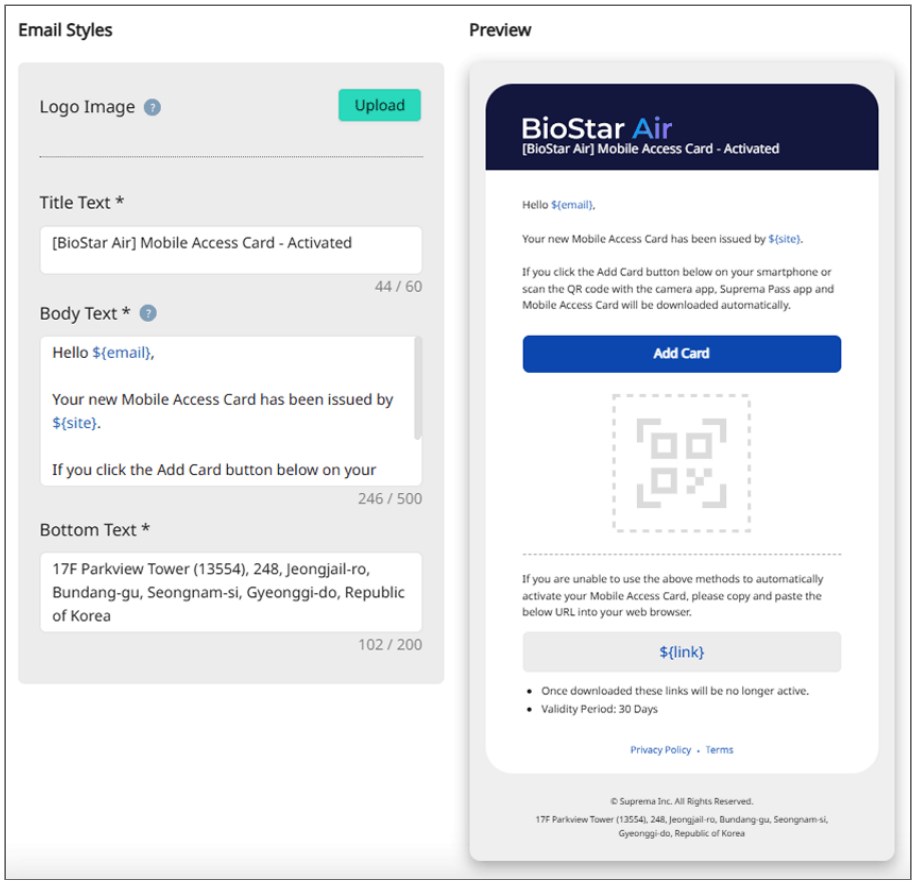


Email Type: Select the email template type to create. Available options are as follows:

- **Event Alert Email**: Sends administrators notifications about events occurring on the site.
- **System Alert Email**: Sends system alerts to administrators.
- **Report Alert Email**: Sends administrators a download link after generating a report.

Email Styles

Customize the email logo and content. View changes in real time in **Preview**.



- **Logo Image**: Upload the logo image to appear in the email.

  - File types: JPG, JPEG, PNG
  - Minimum resolution: 200 x 60
  - File size: 1 MB or less

- **Title Text**: Enter the email subject.
- **Body Text**: Enter the message to display in the email body.

The email body must include HTML keys. Each key is replaced with the recipient's email address, the site name, and other values. Available keys may vary according to the value selected in **Email Type**.

- **User** tab
- `${email}`: Email address
- `${siteName}`: Site name
- **Administrator** tab
- `${email}`: Email address
- `${siteName}`: Site name
- `${alertType}`: Alert type
- `${alertDetails}`: Alert details
- `${frequency}`: Alert frequency
- `${location}`: Alert location
- `${userInvolved}`: User involved in the alert
- `${deviceInvolved}`: Device involved in the alert
- `${dateTime}`: Date and time of the alert

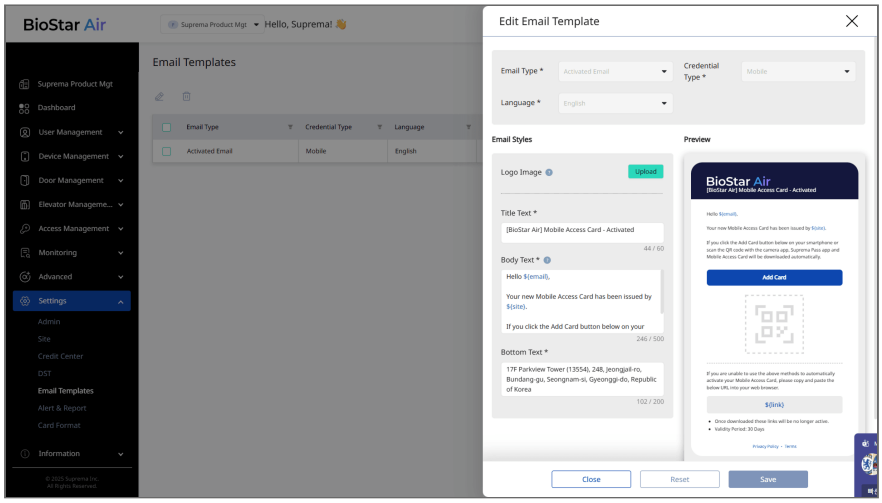
- **Bottom Text**: Enter additional information to appear at the bottom of the email. Add the company address or contact information for compliance or to provide location details to users.

Info

- Verify that the logo image is in the proper format and size so that it appears correctly in the email.
- If the current language is not supported, check future updates. More languages will be added.
- The address field is important for regulatory compliance and clarity, so enter it accurately.
- Click **Save** at the bottom to save the email template.
- Click **Reset** at the bottom to restore the original content after making changes.

Edit email templates

1. Click **Settings** → **Email Templates** in the left sidebar.
2. Click the email template you want to edit from the list. Alternatively, select the checkbox and click at the top.
3. When the **Edit Email Template** panel appears, edit the necessary items.



4. Click **Save** at the bottom to save the changes.

Delete email templates

1. Click **Settings** → **Email Templates** in the left sidebar.
2. Select the checkbox of the email template you want to delete from the list. You can select more than one template.
3. Click at the top of the list.
4. Click **Delete** when the message window appears.

Set Up Alerts and Reports

Setting up alerts and reports enables automatic detection and tracking of system events and security situations. This article explains how to configure alert and report settings in BioStar Air.

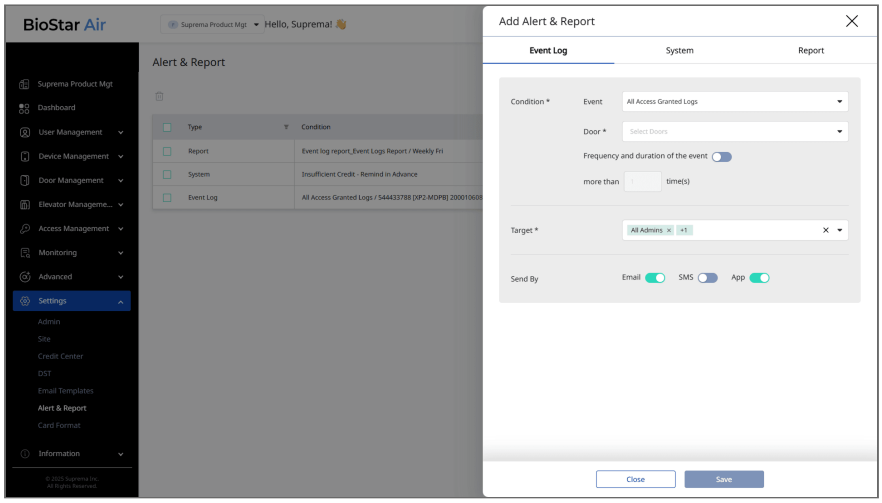
Alert and report settings provide the following benefits.

- Immediately detect security threats or system issues and send real-time alerts to administrators.
- Automatically generate reports on system status and user activity to improve management efficiency.

Add alerts

Configure alerts for specific event logs and system status on the site.

1. Click **Settings** → **Alert & Report** in the left sidebar.
2. Click **Add Alert & Report** at the top right of the screen.
3. When the **Add Alert & Report** panel appears, choose either the **Event Log** or **System** tab.

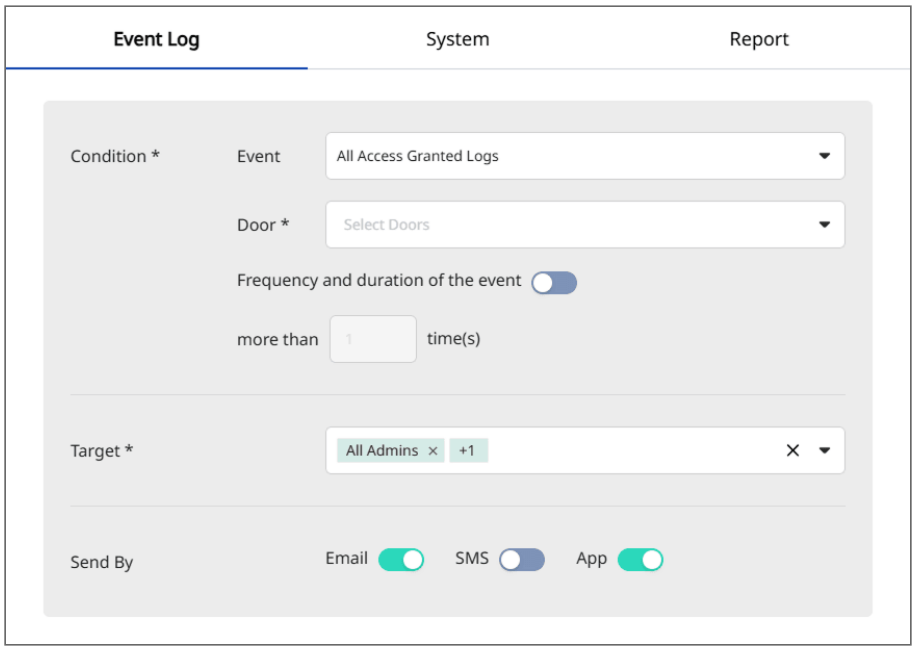


4. After configuring each item, click **Save** to save.

Set conditions

Event log

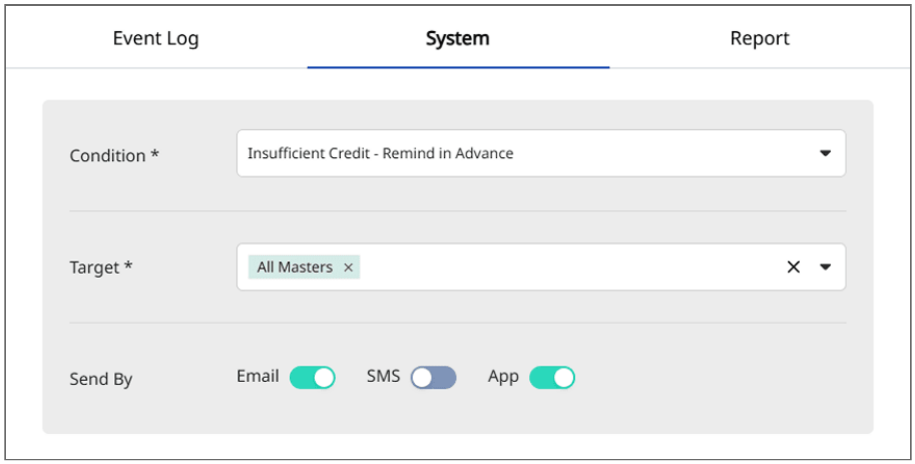
In the **Event Log** tab, set alert conditions by event type.



- **Events**: Select the event types to alert. A predefined **Preset Events** can also be selected.
- **Door**: Select door. Send an alert when an event occurs at the selected door. More than one door can be selected.
- **Frequency and duration of the event**: Send an alert when events occur at a specified frequency within the defined time period. For example, configure the system to send an alert if an event occurs three times within five minutes.

> **Tip**
> In BioStar Air version 2.12 and later, you can configure real-time alerts for device network disconnection events.

System



In the **System** tab, set alert conditions based on system status. The available options are as follows.

- **Insufficient Credit - Remind in Advance**
- **Insufficient Credit - Site Suspended**
- **Insufficient Credit - SMS (Less than 10)**
- **APB battery is low**
- **A new Firmware is available**
- **Network Disconnected (Detected by Device)**

Set alert recipients

Use **Target** to designate alert recipients. Select users by administrator role or select individual users.

Set delivery method

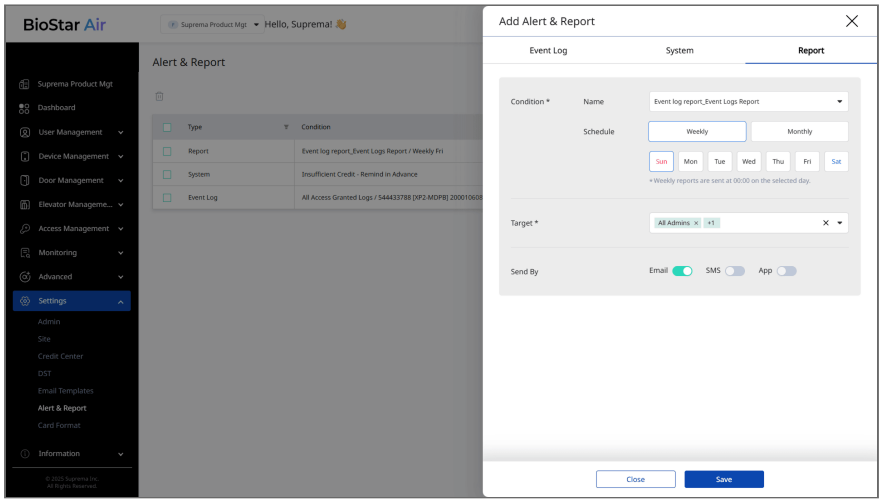
Choose the delivery method in **Send By**. Alerts are delivered by email, SMS, or app push notification.

> **Info**
> You can send text messages only after recharging your SMS credits. Remaining SMS credits can be checked in **Settings** → **Credit Center**.

Generate reports

Automatically generate reports at defined intervals and send them to administrators. Generate reports on event log activity and user status.

1. Click **Settings** → **Alert & Report** in the left sidebar.
2. Click **Add Alert & Report** at the top right of the screen.
3. When the **Add Alert & Report** panel appears, select the **Report** tab.



4. After configuring each item, click **Save** to save.

Set conditions

Configure report type and generation interval.

- **Name**: Select the report type to generate.
  - **T&A Report**: Generates a report on user Time & Attendance status for the selected period.
  - **Audit Logs Report**: Generates a report on audit log status for the selected period.
  - **Event Logs Report**: Generates a report on event log activity for the selected period.
  - **User Report**: Generates a report on user status for the selected period.
- **Schedule**: Select the report generation interval. Choose between **Weekly** and **Monthly**.

Set report recipients

Use **Target** to designate alert recipients. Select users by administrator role or select individual users.

Set delivery method

Choose the delivery method in **Send By**.

> **Info**
> Reports are delivered **by email only**. They are not delivered by SMS or app push notification.

Edit alerts and reports

1. Click **Settings** → **Alert & Report** in the left sidebar.
2. Click the alert or report to edit in the list.
3. When the **Edit Alert** or **Edit Report** panel appears, edit the necessary items.
4. Click **Save** at the bottom to save the changes.

Delete alerts and reports

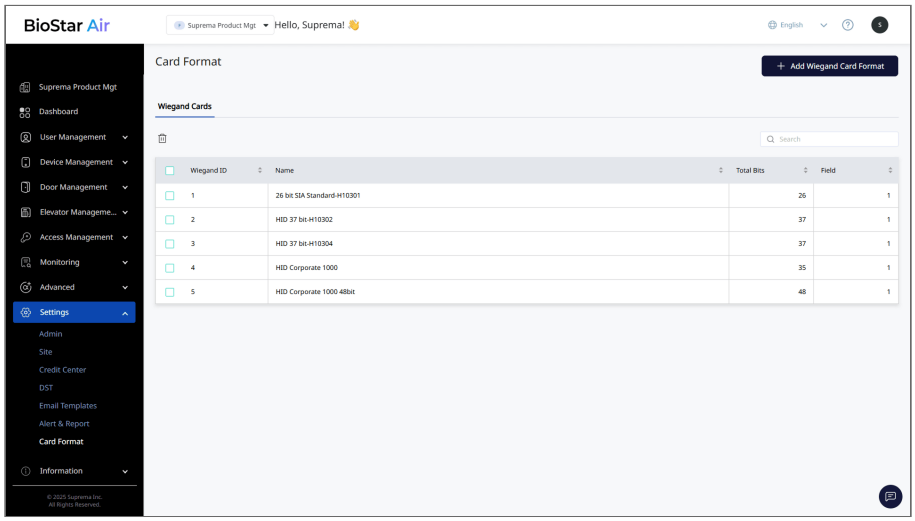
1. Click **Settings** → **Alert & Report** in the left sidebar.
2. Select the checkbox of the alert or report to delete in the list. More than one item can be selected.
3. Click at the top left of the list.
4. Click **Delete** when the message window appears.

Custom Wiegand card format

Create and configure a custom Wiegand card format in BioStar Air v2.10—including facility codes, ID segments, parity bits, and bit assignments—to migrate smoothly from an existing access control system.

Wiegand card format list

Click **Settings** → **Card Format** in the left sidebar. Create, manage, and view special card formats, including Wiegand, SIA, and HID formats. Useful for sites migrating from an existing access control solution with pre-issued cards.

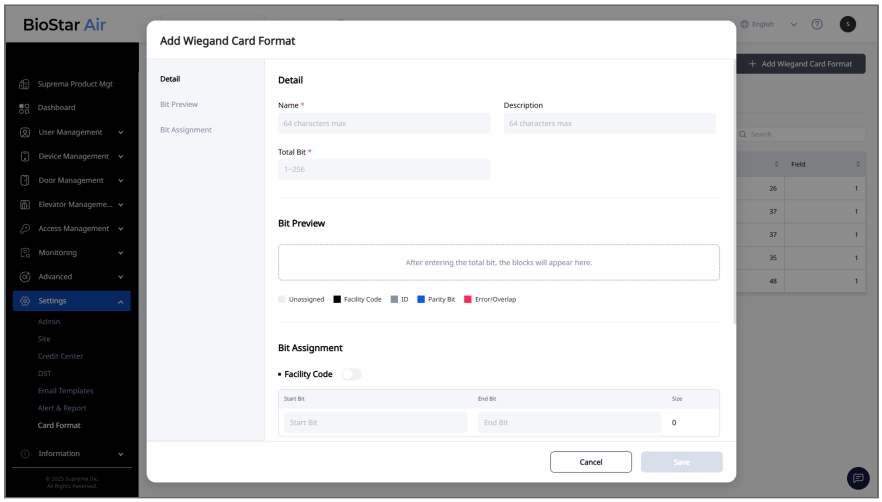


- View all registered Wiegand card formats, including the default formats included in BioStar Air.
- Check the format's name, description, total bits, bit preview, and detailed bit assignments.
- Configure a new custom card format, including its name, description, total bits, and detailed bit assignments. The system provides a bit preview for visual verification.

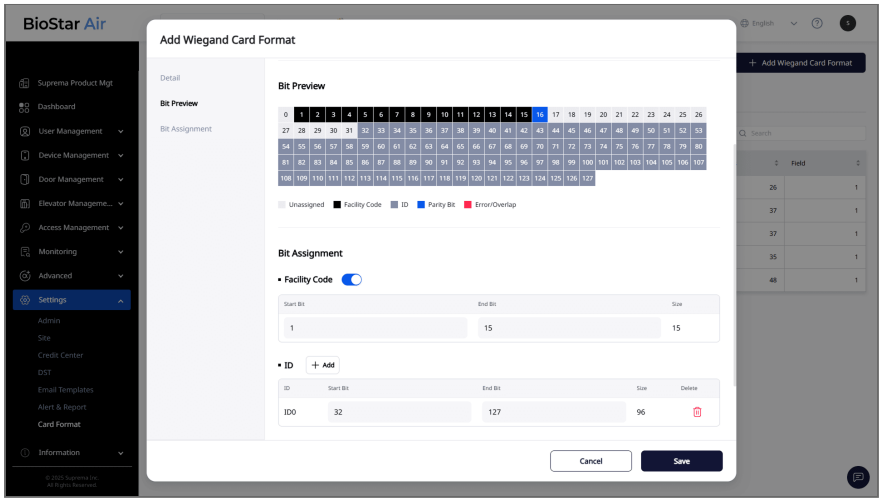
Add a card format

Add a new custom Wiegand card format in addition to the built-in formats.

1. Click **Settings** → **Card Format** in the left sidebar.
2. Click **Add Wiegand Card Format** at the top right of the screen.
3. When the **Add Wiegand Card Format** window appears, enter the name, optional description, and total bits in the **Detail** section.



4. Enter the total bits to activate **Bit Preview**, then configure bit assignment in the **Bit Assignment** section.



The image above is an example screen and may differ from the actual screen.

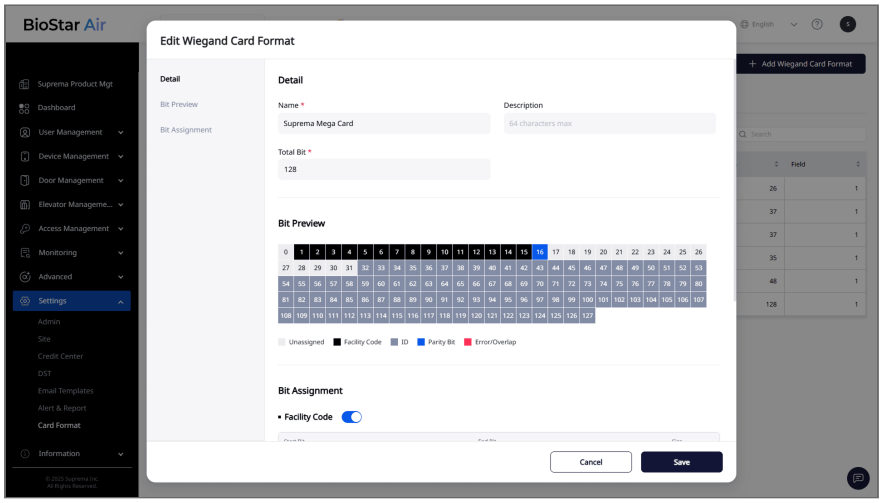
- **Facility Code**: Click the toggle switch to enable the facility code. Enter **Start Bit** and **End Bit**.
- **ID**: Specify start and end bits to add one or more ID segments.
- **Parity Bit**: Specify start and end bits to add odd/even parity bits.

5. Click **Save** to add the new card format.

Edit card format

Follow these steps to edit an existing Wiegand card format.

1. Click **Settings** → **Card Format** in the left sidebar.
2. Click the card format to edit.
3. When the **Edit Wiegand Card Format** window appears, edit the required fields.



4. Click **Save** to save the edited card format.

Delete card format

1. Click **Settings** → **Card Format** in the left sidebar.
2. Click the checkbox for the card format to delete. Select one or more card formats.
3. Click at the top of the list.
4. When the message window appears, click **Yes**.

> **Info**
> The five built-in Wiegand card formats cannot be deleted.

Time & Attendance (T&A)

BioStar Air records shift and break times to provide basic **T&A** tracking and integrates with external T&A systems or exports the data. BioStar Air is not a complete T&A system, but it supports event logging and API integration with payroll and T&A systems. It also generates basic **working hours** reports.

> **Tip**
> Refer to the following video to watch a video guide on T&A configuration.

T&A events

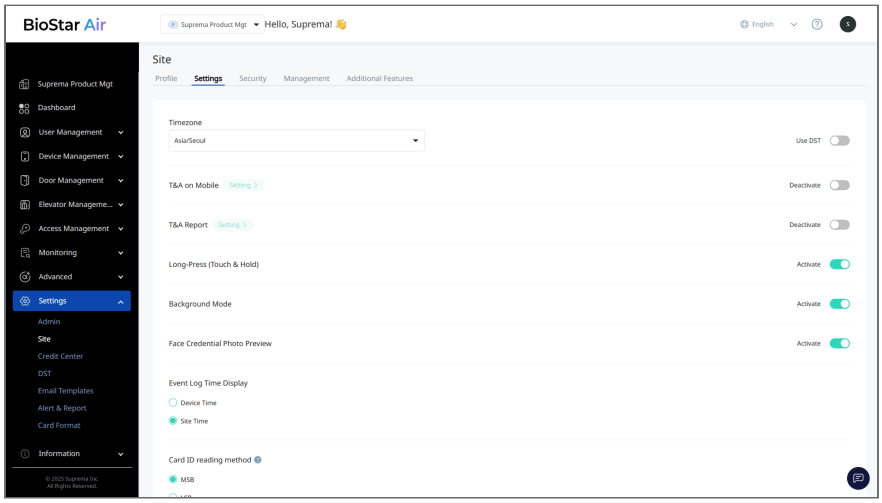
The following T&A events can be recorded. T&A events are logged and can be exported as a CSV file or retrieved through the API.

- **Shift start**
- **Shift end**
- **Break start**
- **Break end**

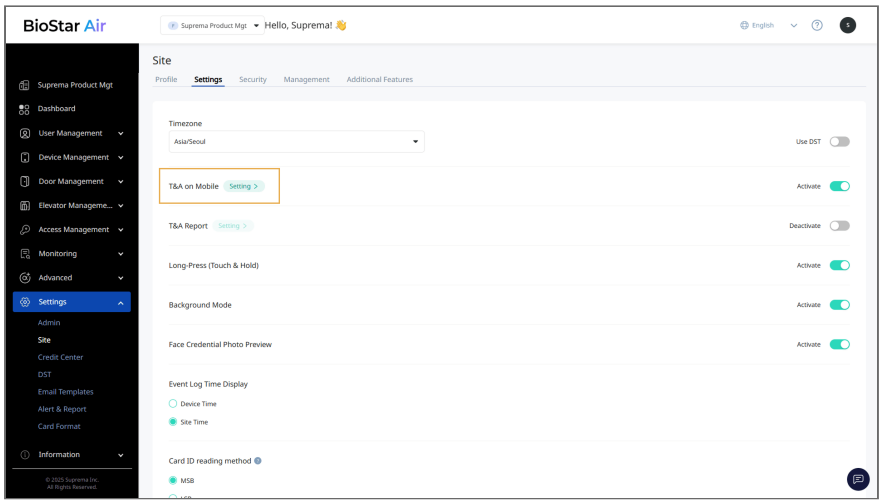
Configure T&A

Follow these steps to enable and configure T&A settings.

1. Click **Settings** → **Site** in the left sidebar.
2. Click **Settings** at the top of the screen.

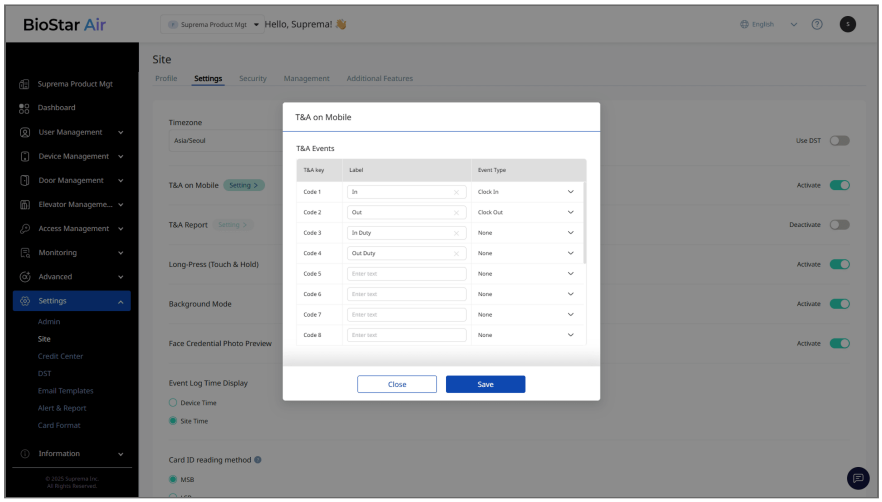


3. Activate **T&A on Mobile**.
4. When the message window appears, click the **Confirm** button.
5. In **T&A on Mobile**, click **Setting**.



6. When the **T&A on Mobile** window appears, set the label for **T&A key**.

> *For example, Shift start, Shift end, Break start, Break end*

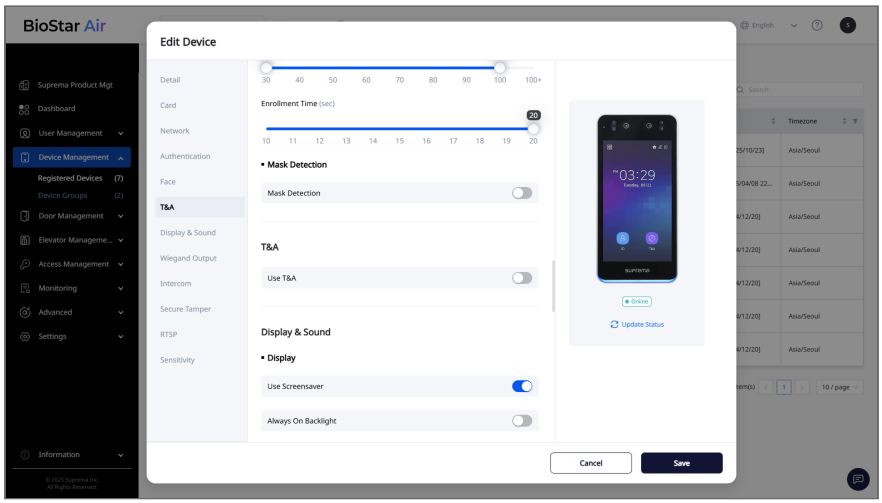


7. Select whether the event type for **T&A key** is **Clock-In** or **Clock-Out**.
8. Click **Save** to save the settings.

Configure T&A on devices

After activating **T&A on Mobile**, specify the devices that will use it.

1. Click **Device Management** → **Registered Devices** in the left sidebar.
2. In the device list, click the device to configure for T&A.
3. When the **Edit Device** window appears, go to the **T&A** section.



The image above is an example screen and may differ from the actual screen.

4. Click the toggle for **Use T&A** to enable T&A.
5. Click **Save** to save the settings.

- When **T&A Mode** is set to **Mobile**, the **T&A is Required** option is available for mandatory T&A selection during access authentication.
- T&A event labels are managed at the **site** level and cannot be changed per device.

T&A Mode

A device records T&A events in several ways. Select the desired attendance mode in **T&A Mode**.

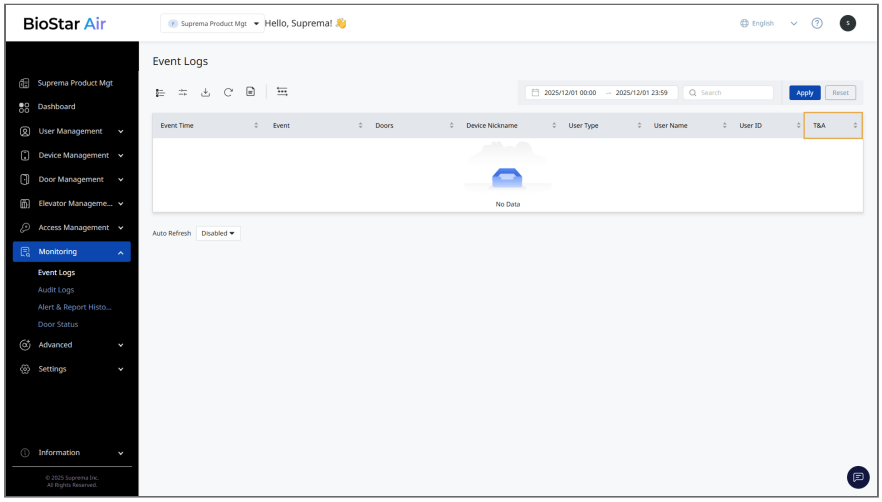
- **User Selects**: When the attendance key appears on the screen, the user selects the attendance event during authentication.
- **By Schedule**: Records clock-in and clock-out times based on the defined schedule. For example, events between 8:00 AM and 12:00 PM are recorded as **Clock-In**, while events between 1:00 PM and 5:00 PM are recorded as **Clock-Out**.
- **Last Choice**: The user continues to use the last selected attendance event.
- **Fixed**: Assigns a fixed T&A code to the device. Each authentication on that device records the same T&A event. Use this option to designate the device for clock-in or clock-out.
- **Mobile**: Requires the user to select a T&A code before authentication. The selected T&A event is recorded with the access log.

> **Info**
>
> Supported attendance management modes may vary depending on the device model. For more information, refer to the device-specific T&A modes in Device and Panel Configuration Options.

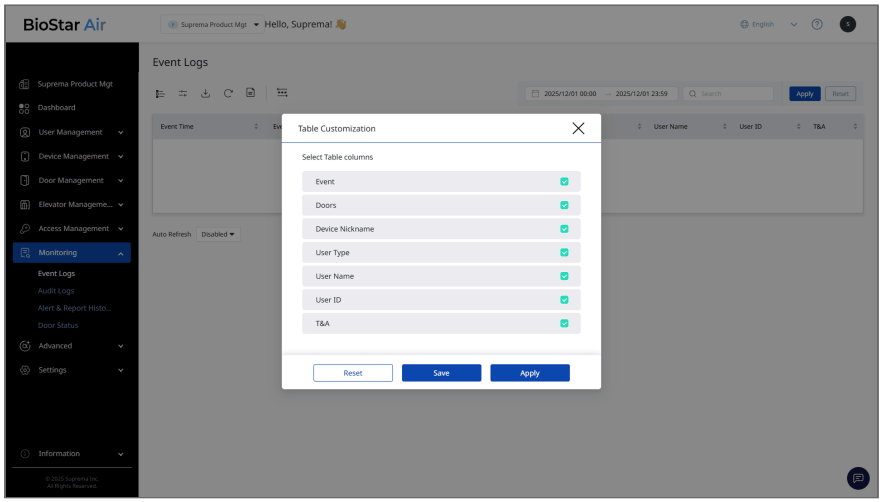
View and export T&A logs

T&A events are saved to the event log and can be reviewed or exported to a CSV file.

1. Click **Monitoring** → **Event Logs** in the left sidebar.
2. Locate the **T&A** column in the log table.



3. Click ☰ at the top of the log table to customize the view and move the **T&A** column for better visibility.



4. Click and select **Download CSV** to download the data as a CSV file.

Time and Attendance Report

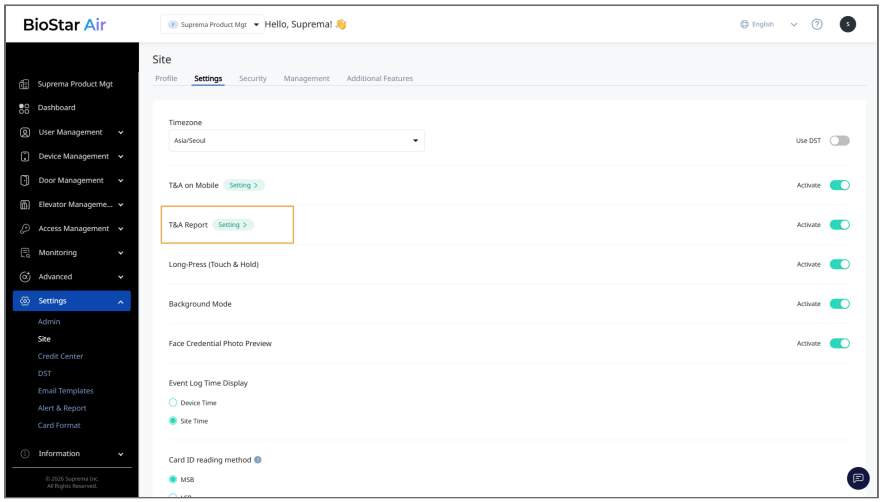
The time and attendance (T&A) report in BioStar Air is a simple **on-site work hour** report. It shows employees' start and end times based on event logs.

This feature is designed for basic reporting without complex configuration options. Time and attendance systems can have various requirements depending on local regulations. If the built-in time and attendance report does not meet your organization's needs, use a third-party T&A solution. Export event logs to **CSV** or integrate directly with third-party T&A software by using the BioStar Air API.

> **Info**
>
> - The built-in time and attendance report is intentionally simple and may not meet all compliance requirements.
> - If complex T&A rules exist (for example, local labor laws or shift patterns), use a third-party T&A solution.
> - Export event logs to CSV for manual processing or use the API to integrate automatically with other systems.

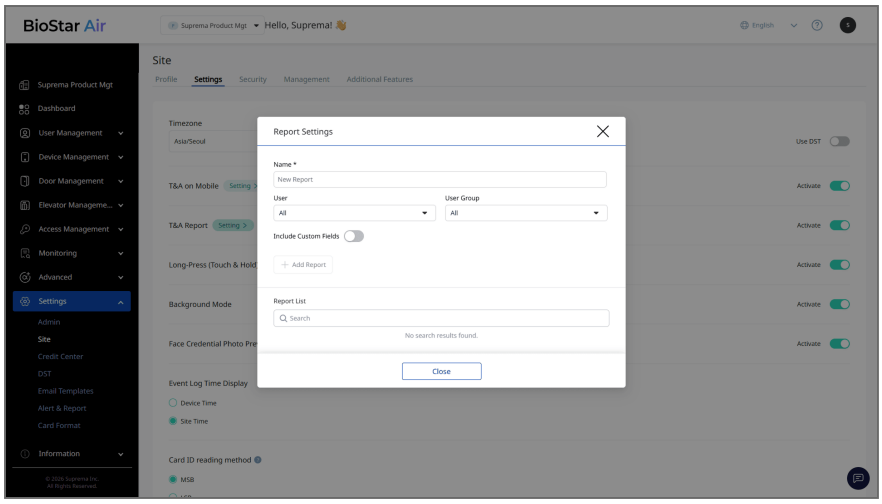
Follow these steps to generate a time and attendance (T&A) report.

1. Click **Settings** → **Site** in the left sidebar.
2. In the **Settings** tab, click **T&A Report** → **Setting**.

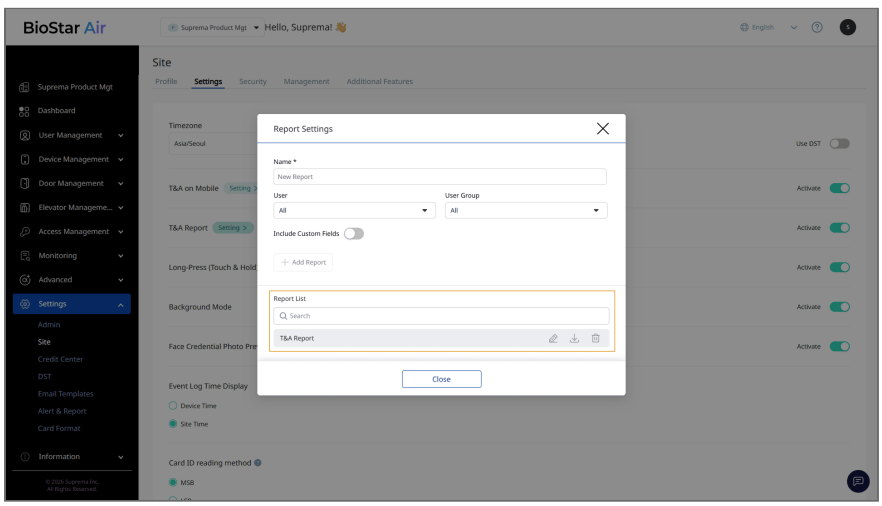


Click the toggle on the right to enable **T&A Report**.

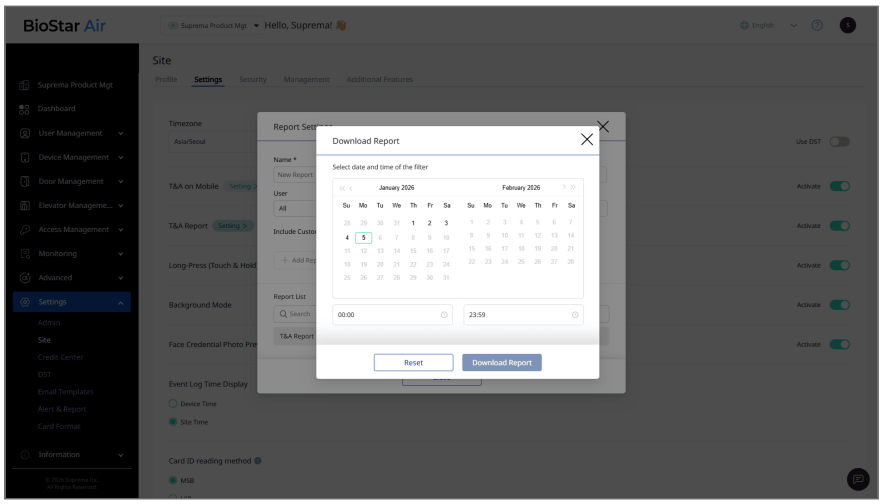
3. When the **Report Settings** window appears, enter a name for the report.



4. Select the users or user groups to include in the report.
5. Click **Add Report**.
6. A downloadable report is generated in **Report List**.



7. Click ⬇ to download the report.
8. When the **Download Report** window appears, select a date and time range.



9. Click **Download Report**.

After the report is generated, a download link is sent to the administrator's email. Download the report from the email in PDF or CSV format.

> **Info**
>
> - Enable **Include Custom Fields** and select the desired template items to include user templates in the report.
> - The report is available for download for 24 hours after the download email is received. After that period, the report is no longer available.
> - Configure an automated schedule in **Alert & Report**. For more information, refer to Set Up Alerts and Reports.

Create and Schedule Reports

Reports in BioStar Air can be configured from different pages depending on the report type. This article explains how to create and schedule user, event log, and audit log reports.

Access report configuration

The entry path differs by report type.

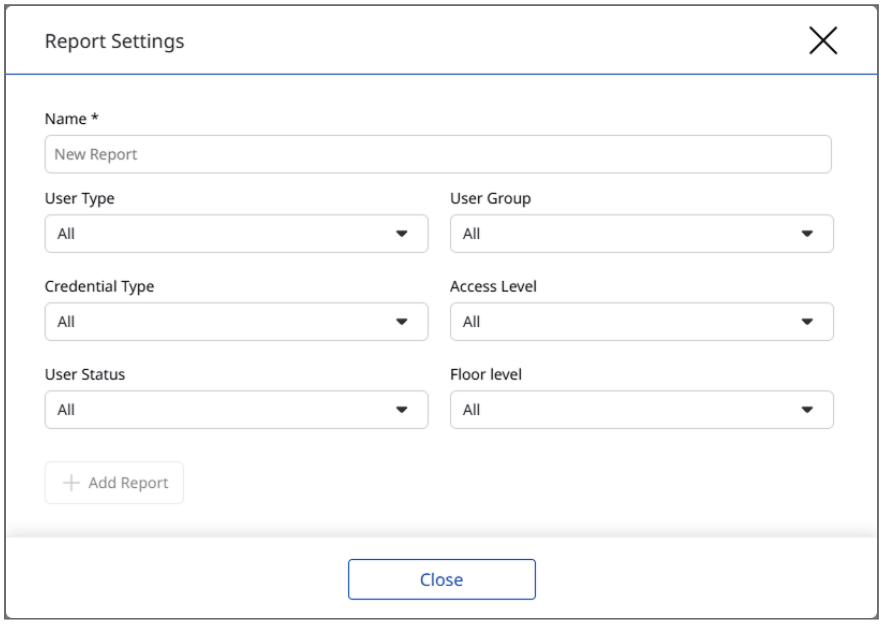
- User report: **User Management** → **Users**
- Event log report: **Monitoring** → **Event Logs**
- Audit log report: **Monitoring** → **Audit Logs**

Click 📄 in the toolbar at the top of the list. The report settings page appears.

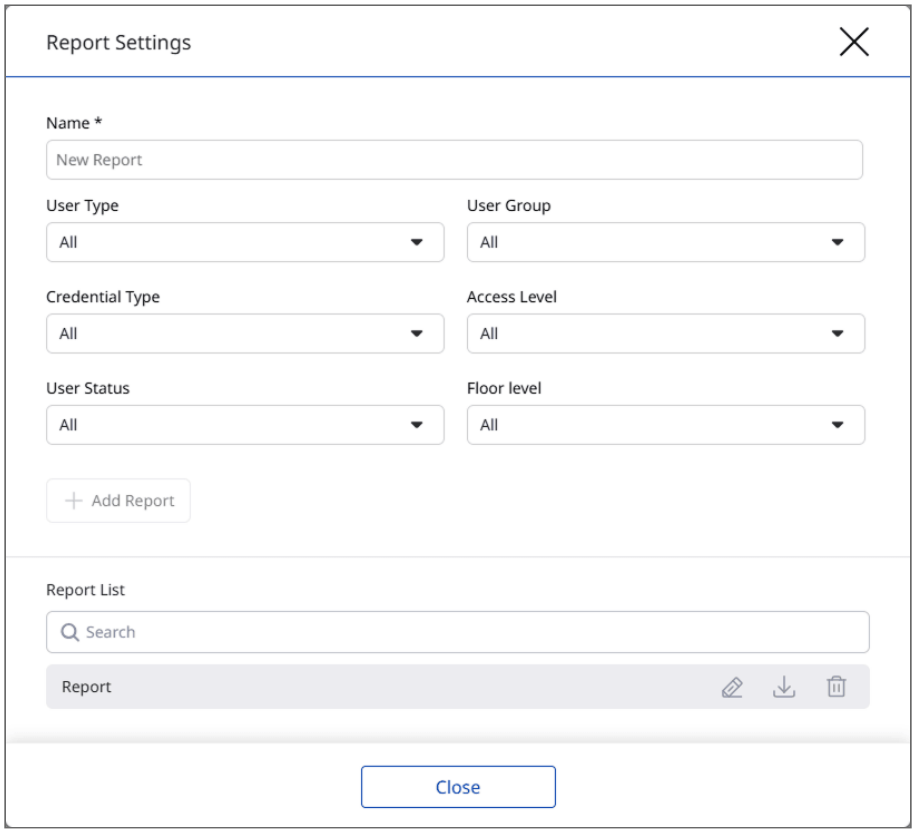
Configure user reports

Configure a user report to view the current status of users registered on the site.

1. Go to **User Management** → **Users** in the left sidebar.
2. In the toolbar at the top of the user list, click .
3. When the **Report Settings** window appears, enter a report name.



4. Select the items to include in the report from each filter option.
5. Click **Add Report** to save the report.
6. A **Report List** is created at the bottom, and a download link is sent to the administrator's email.



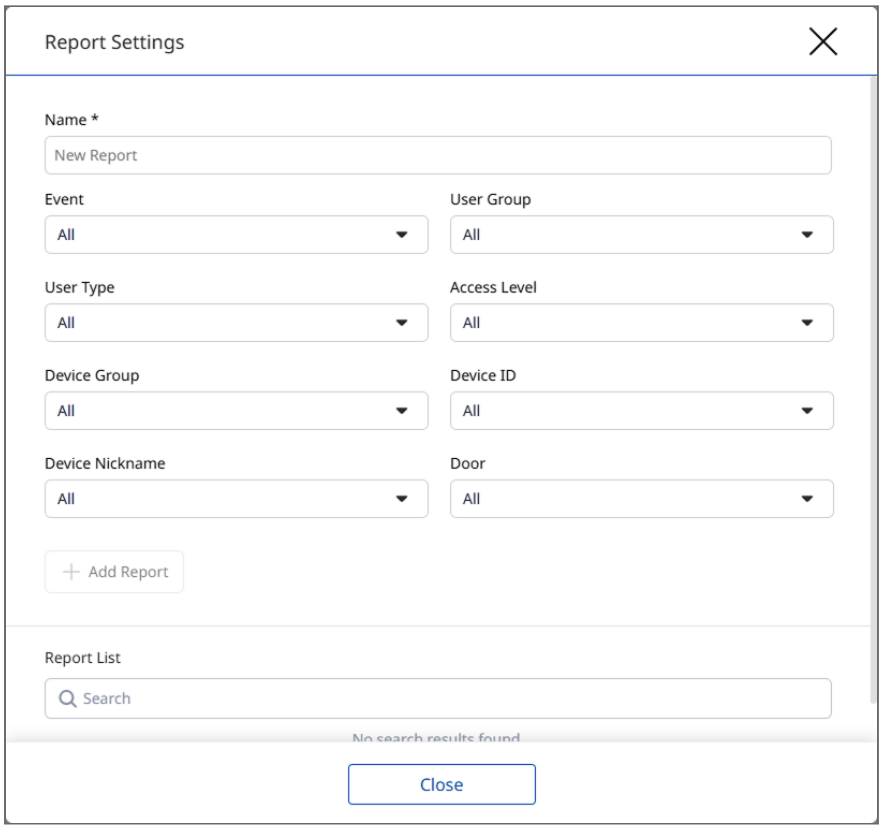
Info

- Click to edit the report.
- Click to export the report as a PDF or CSV file.
- Click to delete the report.
- For more information on user management, refer to Users.

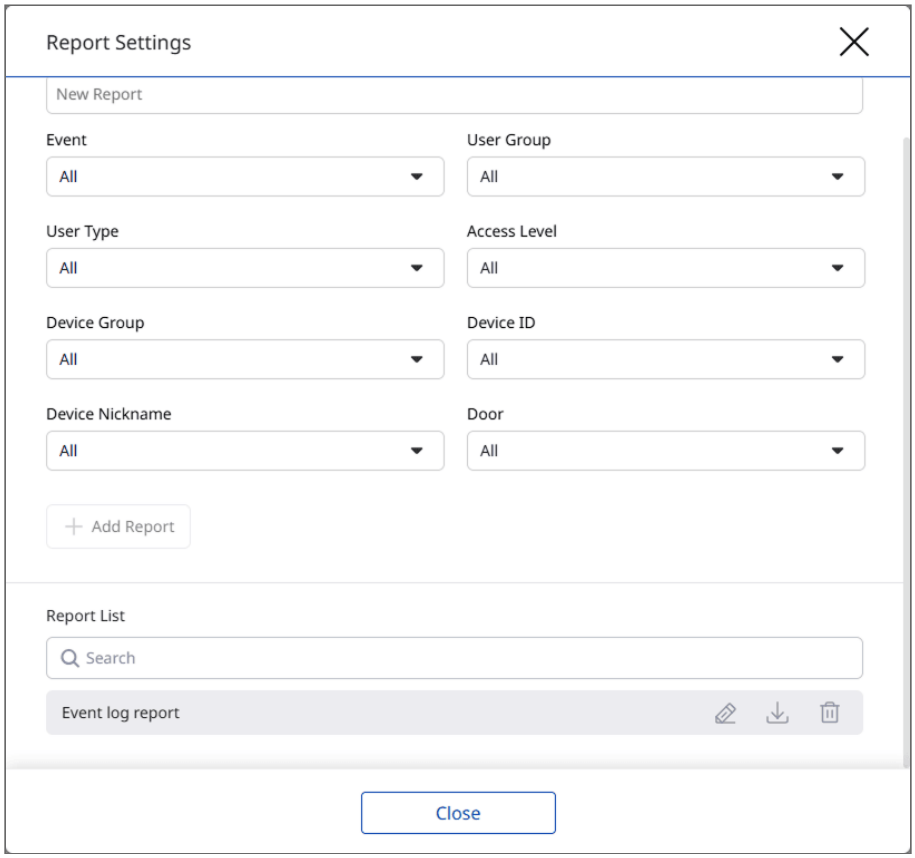
Configure event log reports

Configure a report on event logs generated on the site.

1. Go to **Monitoring** → **Event Logs** in the left sidebar.
2. In the toolbar at the top of the log list, click .
3. When the **Report Settings** window appears, enter a report name.



4. Select the items to include in the report from each filter option.
5. Click **Add Report** to save the report.
6. A **Report List** is created at the bottom, and a download link is sent to the administrator's email.



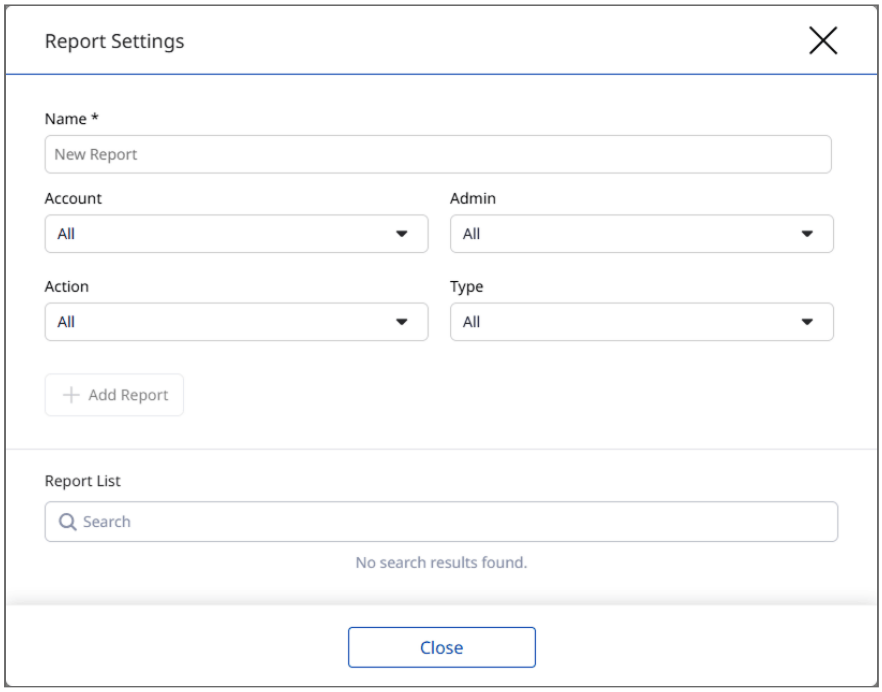
Info

- Click to edit the report.
- Click to export the report as a PDF or CSV file.
- Click to delete the report.
- For more information on event logs, refer to Use Event Logs.

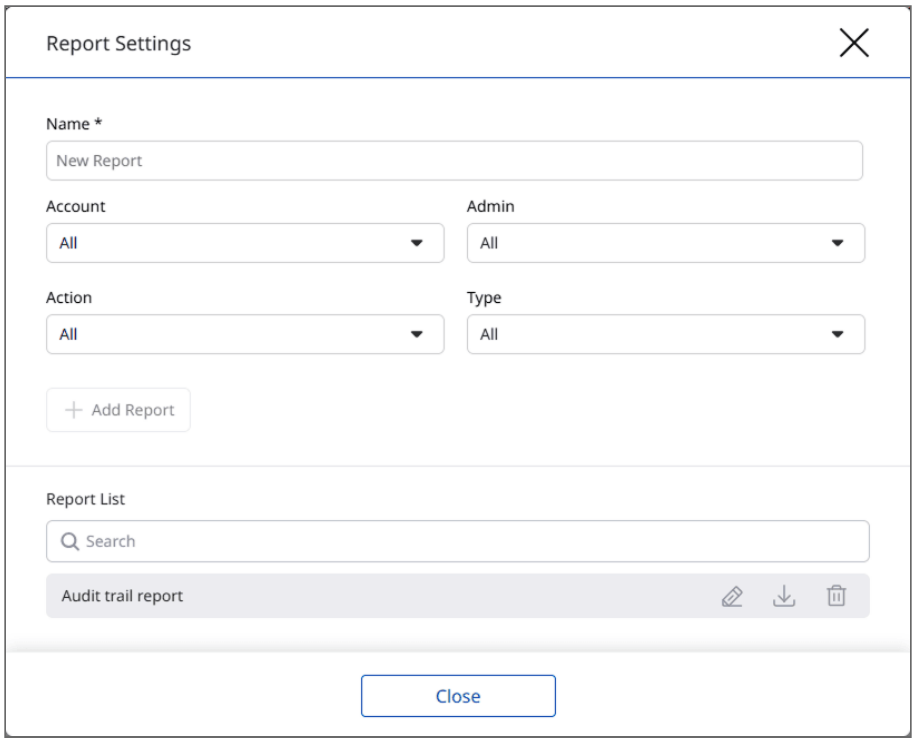
Configure audit log reports

Configure an audit log report on changes made by administrators.

1. Go to **Monitoring** → **Audit Logs** in the left sidebar.
2. In the toolbar at the top of the log list, click .
3. When the **Report Settings** window appears, enter a report name.



4. Select the items to include in the report from each filter option.
5. Click **Add Report** to save the report.
6. A **Report List** is created at the bottom, and a download link is sent to the administrator's email.



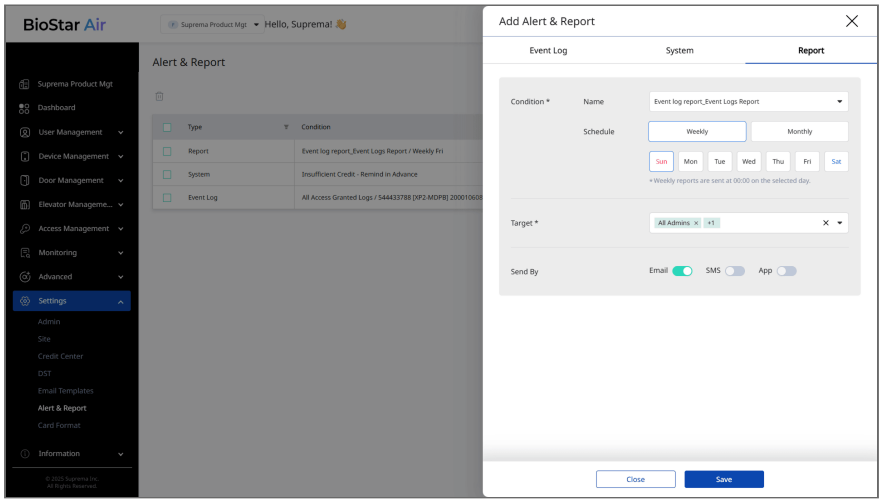
Info

- Click to edit the report.
- Click to export the report as a PDF or CSV file.
- Click to delete the report.
- For more information on audit logs, refer to Use Audit Logs.

Schedule reports

Automatically generate reports at defined intervals and send them to administrators.

1. Go to **Settings** → **Alert & Report** in the left sidebar.
2. Click **Add Alert & Report** at the top right of the screen.
3. When the **Add Alert & Report** panel appears, select the **Report** tab.



4. In the **Condition** section, select the report type to generate from **Name**.
5. Select the report schedule from **Schedules**.
   - Select either **Weekly** or **Monthly**.
   - Select the specific date to send the report.
   - All reports are sent at midnight on the selected day.
6. Select the recipients from **Target**.
   - All administrators of a specific level
   - Individual administrator
7. Choose the delivery method in **Send By**.
   - Reports can only be sent by email.
   - They are not delivered by SMS or app push notification.
8. After configuring each item, click **Save** to save.

Info

For more information on scheduling report generation, refer to Set Up Alerts and Reports.

Partners & Installers

The BioStar Air Partner Portal is a dedicated platform for value-added resellers (VARs) with distribution agreements. Create customer sites, allocate credits, or configure federation sites to centrally manage multiple locations.

Install on-site hardware such as SIP intercoms, IP cameras, and QR scanners, and configure network settings.

Use the Partner Portal

The BioStar Air Partner Portal is an exclusive tool for value-added resellers (VARs) that lets them manage customer sites, distribute credits, and efficiently oversee administrative functions.

Log in to the Partner Portal to perform the following tasks.

- Create new sites for customers.
- Allocate and distribute credits to those sites.

Info

- The Partner Portal is for value-added resellers (VARs) only and not for site administrators or end customers.
- If you do not receive an invitation email, check your spam folder or contact your Partner Portal administrator.
- Verify that the email used for registration is correct. This cannot be changed later.

Tip

Watch the video below for a guide on using the BioStar Air Partner Portal.

Access the Partner Portal

The Partner Portal is available only as a web portal. Visit it through the following link. https://partner.biostarair.com/

Sign up for the Partner Portal

1. After a distribution agreement is signed, an invitation email to sign up for the Partner Portal is sent.
2. Click **Sign Up** in the email.
3. Review and accept the privacy policy and terms of use.
4. When the sign-up screen with your email prefilled appears, enter the required information.
5. Complete the sign-up process and log in to the portal.

Info

- The Partner Portal is for approved resellers only; site administrators and end users cannot access it.
- If the invitation email is not received, check the spam folder or contact the Partner Portal administrator.
- Verify that the email used for registration is correct. It cannot be changed after sign-up.

Manage sites

Log in to the Partner Portal to view the list of sites linked to your account.

- Review site details such as site name, country, and allocated credits.
- Monitor each site's monthly costs to determine when additional credits are needed.
- Track the number of users and registered devices.
- Add notes for internal tracking.

Edit site details

Click the site you want to edit in the site list. On the site edit screen, perform the following actions.

- Update site details, including time zone and country information.
- Add or edit notes related to the site.
- Adjust the number of allocated credits.
- Invite additional administrators to the site.
- Delete the site if necessary.

Track credit history

View all credit changes in the **Credit history** section.

- Set a time range to review credit changes for a specific period.
- Monitor recent credit additions for customer sites.

Manage administrators

Invite other users to the partner portal in the **Admin** section.

1. Select the administrator level.
2. Enter the email address of the user to invite.
3. Click **OK** to send the invitation.

> **Info**
> End customers must not be added to the partner portal. Only value-added resellers (VARs) should manage site creation and credit allocation.

Understand roles and permissions

The partner portal has four permission levels.

- **Observer**: Can view site information but cannot make changes.
- **Operator**: Can set up new sites and allocate credits but cannot modify administrator permissions or invite new administrators.
- **Admin**: Can invite and manage other administrators but cannot remove master level users.
- **Master**: Has full control of the portal, including user management, site creation, and credit allocation. Only master level users can activate the Partner Portal account initially.

> **Info**
> Set up and activate a master account before users with other permission levels can access the portal.

Manage Federated Sites

BioStar Air provides **federated sites**, enabling a primary site to seamlessly manage multiple subsites. This feature is ideal for multi-tenant buildings or organizations with multiple branches and offers centralized control through distributed access management.

By leveraging the federated site feature in BioStar Air, administrators effectively manage access in complex environments and deliver a secure, scalable, and streamlined experience for all stakeholders.

What is a federated site?

Federated sites support a hierarchical structure in which a **primary site** manages one or more **subsites**. An administrator of the primary site—called the **federation administrator**—can directly access and manage subsites from the BioStar Air interface.

Federated sites are useful in the following situations.

Multi-tenant building

For example, in a commercial building where each floor is occupied by a different company, configure the system as follows.

- **Master account** for the building
- **Subaccount** for each tenant company

This setup authorizes only employees with access to a specific floor, simplifying building management.

Multi-branch organization

A company with offices in multiple locations can configure the system as follows.

- Manage global settings through a **master account**
- Create a **subaccount** for each branch

For example, a company with ten offices worldwide can use a federated structure to streamline management.

Set up federated sites

1 Access Partner Portal

URL: https://partner.biostarair.com

- Only partners and installers can use the BioStar Air Partner Portal.
- End customers must contact an installer to configure this feature.

2 Create primary site

1. Log in to the Partner Portal.
2. Click , and select in .
   - This step **must** be performed when first setting up the site.
   - A standard site cannot be converted to a federated site later.
3. Add a federation site administrator on the same screen.
   - A **federation site administrator** added in the Partner Portal can access the primary site and all subsites.
   - A **general administrator** added in BioStar Air can manage only individual sites.

3 Add subsites

1. When the primary site is set as a federated site, the will display an option to create subsites.
2. Click and configure it like any other site.

Important considerations

User and device management

- Add users and devices separately to each subsite.
- A device can be registered to only one site at a time. Select either the primary site or a subsite.

Primary site usage

- Certain customers use the primary site only as an access point for subsite management and do not register any users or devices in the primary site.
- **Example 1**: A company with three branch offices sets up a primary site with no devices and creates a subsite for each branch.
- **Example 2**: A company with headquarters and three branches registers users and devices at headquarters (the primary site) and sets up subsites for the branches.

Billing

- Billing is calculated based on the number of registered devices (readers) per site.
- There is no additional cost to create a primary site without registered devices.

Invite Partner Administrators

Guide on inviting partner administrator accounts, assigning roles, and managing permissions in the Partner Portal. Partner administrators control access to customer sites to enhance security and operational efficiency.

Partner administrators are assigned one of 4 roles — Observer, Operator, Administrator, or Master — each with different access permissions. This document compares the permissions of each role and provides step-by-step guidance from inviting administrator accounts to managing permissions, locking/unlocking accounts, and deleting accounts.

Understand administrator roles and permissions

Administrators in the Partner Portal can be assigned one of the following 4 roles.

- **Observer**: Can view site information but cannot make changes.
- **Operator**: Can set up new sites and allocate credits but cannot modify administrator permissions or invite new administrators.
- **Admin**: Can invite and manage other administrators but cannot remove master level users.
- **Master**: Has full control of the portal, including user management, site creation, and credit allocation. Only master level users can activate the Partner Portal account initially.

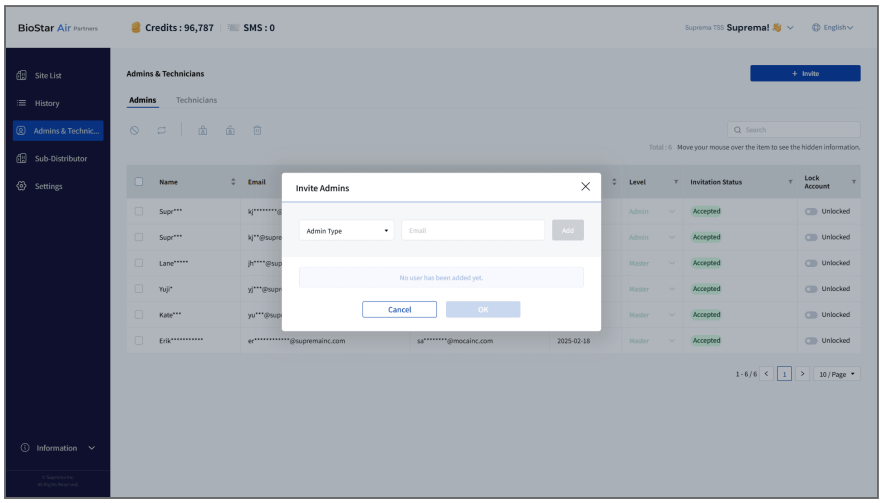
> **Info**
> Set up and activate a master account before users with other permission levels can access the portal.

Invite Administrators

Follow the steps below to invite administrators.

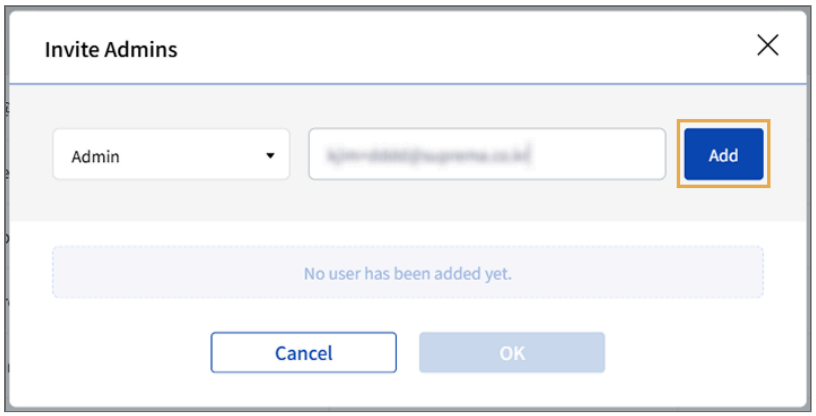
1. Log in to the Partner Portal with an account assigned the **Admin** role or higher.
2. Click in the left sidebar.
3. Click at the top right of the screen.

4. When the window appears, select the administrator role to invite from the field.

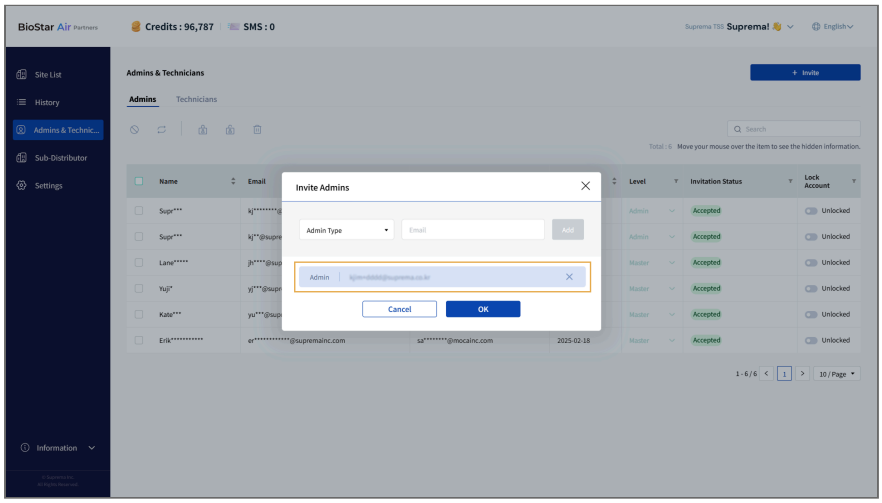


5. Enter the email address of the administrator to invite.

6. Click when it becomes active.



7. Added administrators appear below the email address field. Repeat steps 4–6 to invite additional administrators.



8. After adding all administrators, click **Ok**.

9. When the confirmation message appears, click **Confirm**.

> **Info**
> Inviting administrators to the Partner Portal does not grant site access; invite them to each site separately.

Invitation status

After inviting administrators, check the invitation status of each invited account in the administrators list.

Pending sign-up

Invited administrators remain in the status until they accept the invitation via email and activate their account. Invited administrators can click the link in the email to register their account or log in to the Partner Portal.



> **Info**
> Invited administrators have up to 7 days to accept the invitation; after 7 days the invitation expires and the status changes to . If the invitation expires, you can resend the invitation link so the invited account can sign up again. For more information on resending invitation links, see Resend invitation link.

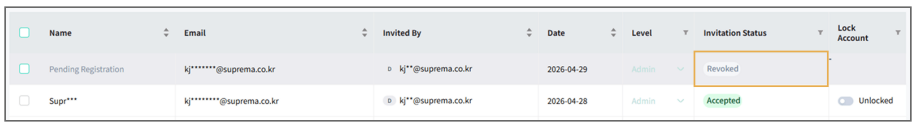
Sign-up complete

When an invited administrator accepts the email invitation and completes registration, the invitation status changes to .



Invitation revoked

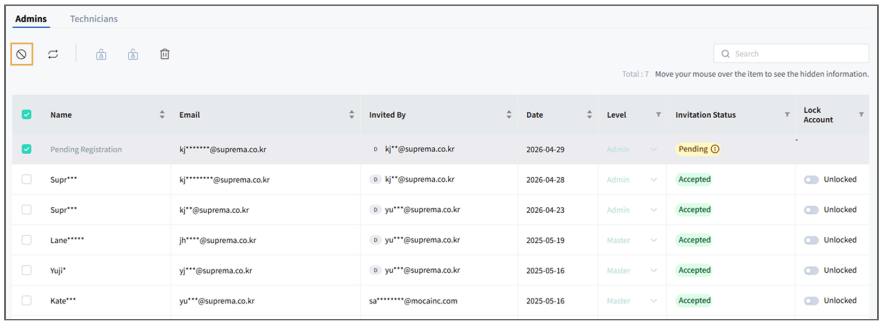
You can cancel the invitation if the invited administrator's email address is incorrect or if the invitation is no longer needed. If you cancel the invitation, its status will change to . For more information on revoking administrator invitations, see Invitation revoked.



Invitation revoked

You can cancel an invitation if a partner entered an administrator's email address incorrectly or if the invitation is no longer needed. After you cancel an invitation, the user will not be able to use the invitation link to sign up.

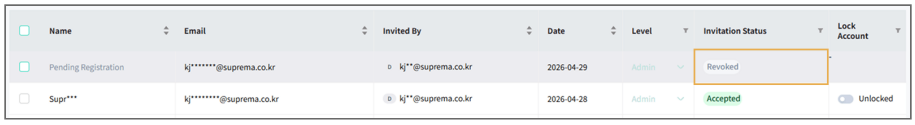
1. In the administrators list, click the checkbox next to the administrator whose invitation status is . You can select 1 or more administrators.
2. Click ⃠ at the top left of the administrator list.



> Only administrators with the status can have their invitations canceled.

3. If a popup message appears, review the message and click .
4. When the success message for the canceled invitation appears, click **Close**.

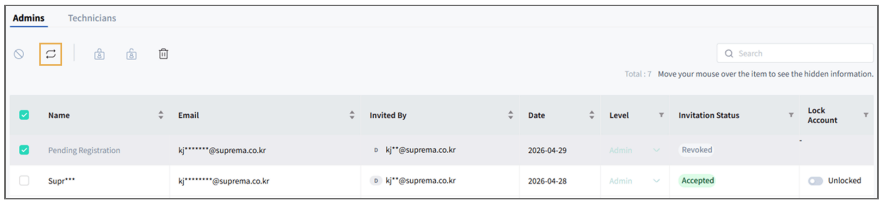
In the administrators list, the invitation status for an administrator whose invitation was canceled changes to .



Resend invitation link

Resend the invitation link if an invited administrator did not receive the invitation email, lost it, or if the invitation link has expired.

1. In the administrators list, click the checkbox next to any administrator whose invitation status is , , or . You can select 1 or more administrators.
2. Click ⟲ at the top left of the administrator list.



3. If a popup message appears, review the message and click .
4. When the success message for resending the invitation link appears, click **Close**.

In the administrators list, the invitation status of an administrator whose invitation link was resent changes to .



Admin management

After an invited administrator accepts the email invitation and completes sign-up, you can manage the administrator in the administrators list. Lock or unlock an administrator's account, or change their role. If an administrator is no longer needed, you can delete their account.

Lock or unlock an administrator account

Lock or unlock an account using the option for administrators who have accepted the email invitation and completed sign-up. When an account is locked, the administrator cannot sign in to the partner portal. Account information is retained so the account can be reactivated later if needed.

For locked administrators, the column shows ; for unlocked administrators it shows .



Info

- Accounts for administrators who have completed sign-up are unlocked by default.
- Accounts with the **Admin** role or higher cannot be locked or unlocked.

Lock or unlock an individual administrator

Click the toggle in the column of the administrators list to lock or unlock individual administrator accounts.

1. Click the toggle in the column of the administrators list.



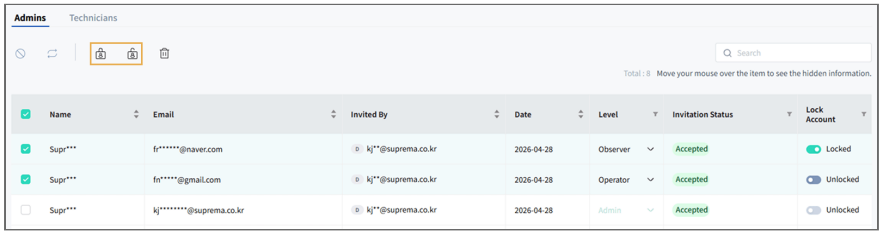
2. If a pop-up message appears, review it and click **Confirm**.

Lock or unlock multiple administrators

To lock or unlock multiple administrator accounts at once, select them in the administrators list.

1. In the administrators list, click the checkbox for the administrator you want to lock or unlock. You can select 1 or more administrators.

2. Click or in the upper left corner of the screen.



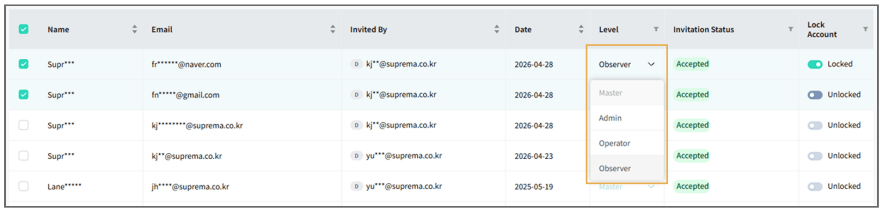
3. If a popup message appears, review the message and click .

4. When the success message confirming the account lock or unlock appears, click **Close**.

Change administrator role

Change an administrator's role. For more information on administrator roles, see Understand administrator roles and permissions.

1. In the administrators list, click the column for the administrator whose role you want to change.



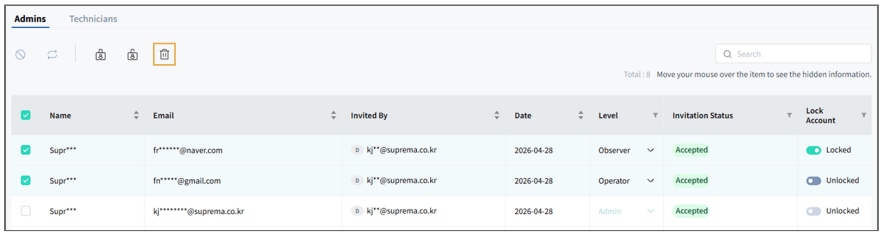
2. Select the permission you want to change from the list.
3. When a pop-up message appears, click **Confirm**.

The user's permissions are updated in the administrators list.

Delete administrator account

You can delete an administrator account when it is no longer needed. Deleting an administrator account prevents the administrator from logging into the partner portal, and the account information is permanently removed and cannot be restored.

1. In the administrators list, click the checkbox for the administrator you want to delete. You can select 1 or more administrators.
2. Click in the upper left of the screen.



3. If a pop-up message appears, review it and click **Confirm**.
4. When the account deletion success message appears, click **Close**.

Deleted administrator accounts no longer appear in the administrator list.

Invite Site Administrator

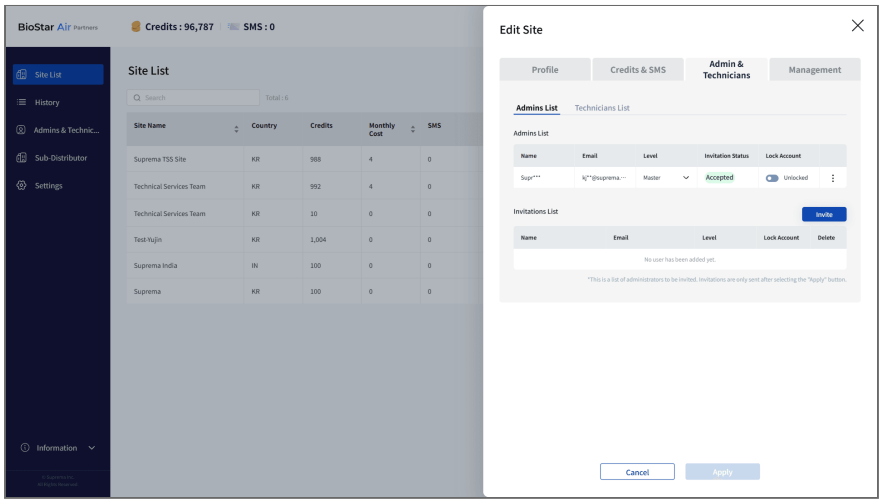
Partners can invite administrators to customer sites and set permissions. Manage granular access levels for each administrator to ensure the security and operational efficiency of customer sites.

> **Info**
>
> - For more information on administrator levels and roles, see Manage Administrator Accounts and Roles.
> - For more information on inviting administrators and setting roles in the BioStar Air portal, see Manage Administrator Accounts and Roles.

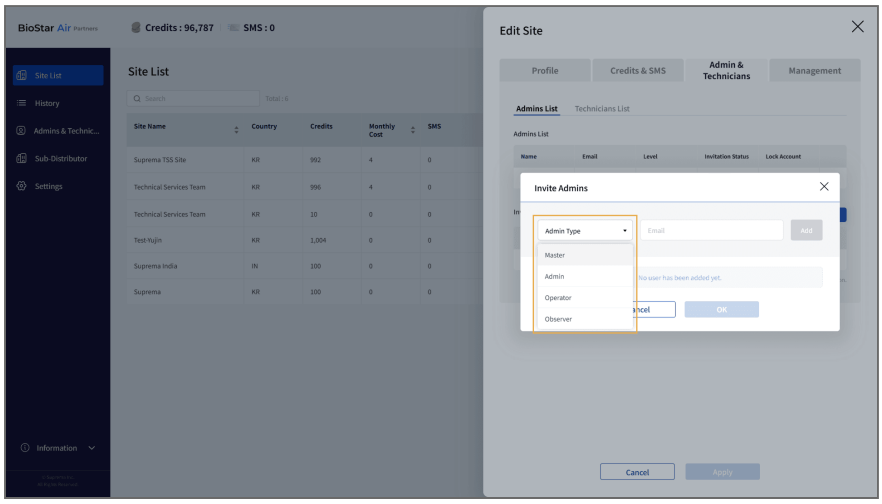
Invite a site administrator

Learn how to invite administrators to customer sites and set permissions in the Partner Portal.

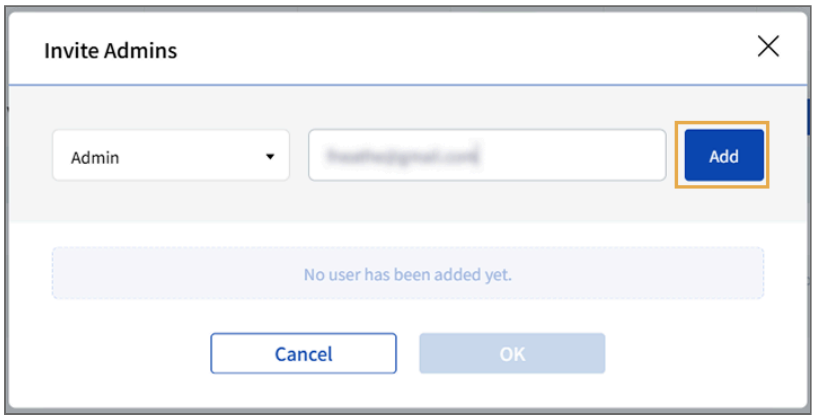
1. Log in to the Partner Portal with an account assigned the **Admin** role or higher.
2. Click in the left sidebar.
3. In the site list, click the site where you want to assign an administrator.
4. When the panel appears, click → in that order.



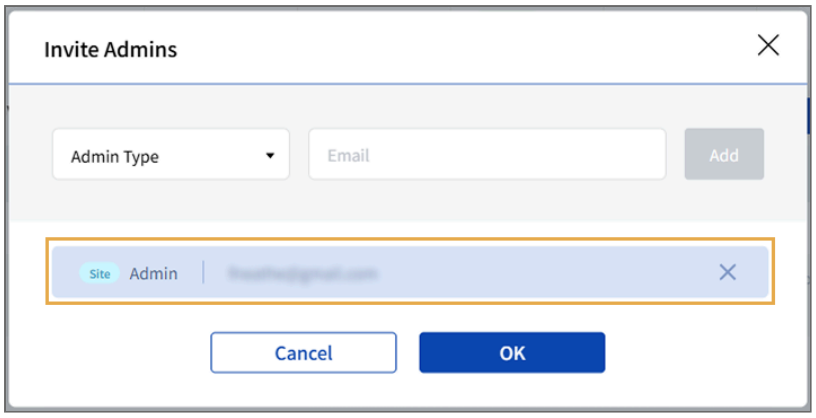
5. Click .
6. When the window appears, select the administrator role to invite from the field.



7. Enter the email address of the administrator to invite.
8. Click when it becomes active.



9. Added administrators appear below the email address field. Repeat steps 6–8 to invite additional administrators.



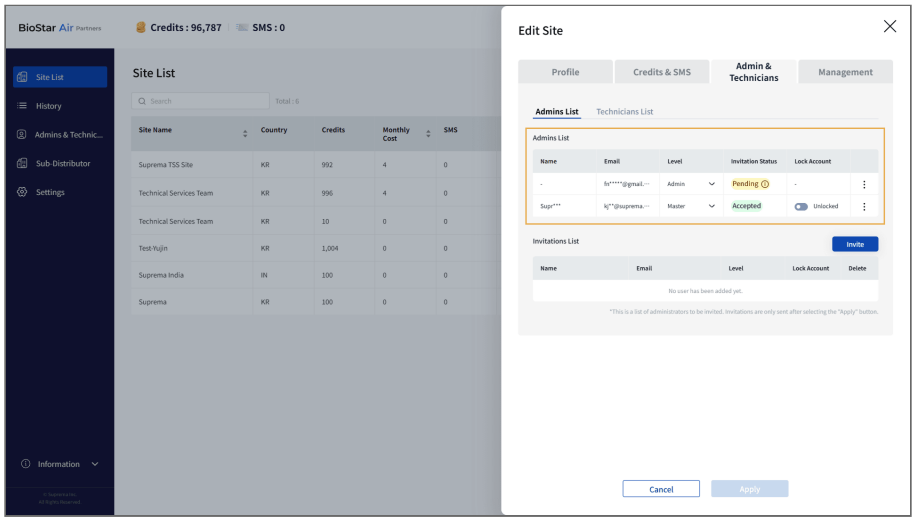
10. After adding all administrators, click **Ok**.
11. Review the administrators added in and then click to send the invitation email.
12. When the success message appears, click **Confirm**.

Check invitation status

Check the invitation status of administrators invited to the site. The invitation status is until the invited administrator accepts the invitation email. Invited administrators have up to 7 days to accept the invitation; after 7 days the invitation expires and the status changes to .

1. In the site list, click the site where you invited an administrator.
2. When the panel appears, click → in that order.
3. Check the invitation status in .

When an invited administrator completes site enrollment, the status changes from to .

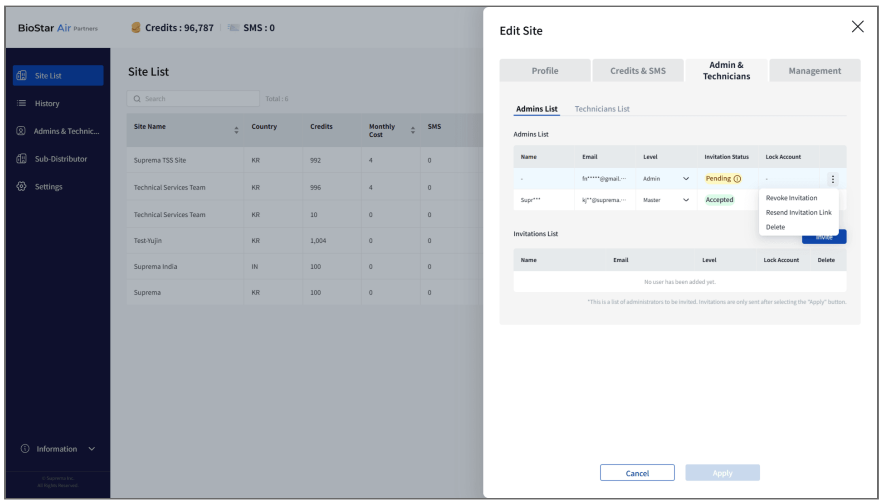


Invitation revoked

Cancel the invitation if the invited administrator's email address was entered incorrectly or the administrator is no longer needed.

1. In the site list, click the site where you invited an administrator.

2. When the panel appears, click → in that order.
3. In , for any administrator with status , click ⋮ on the far right.



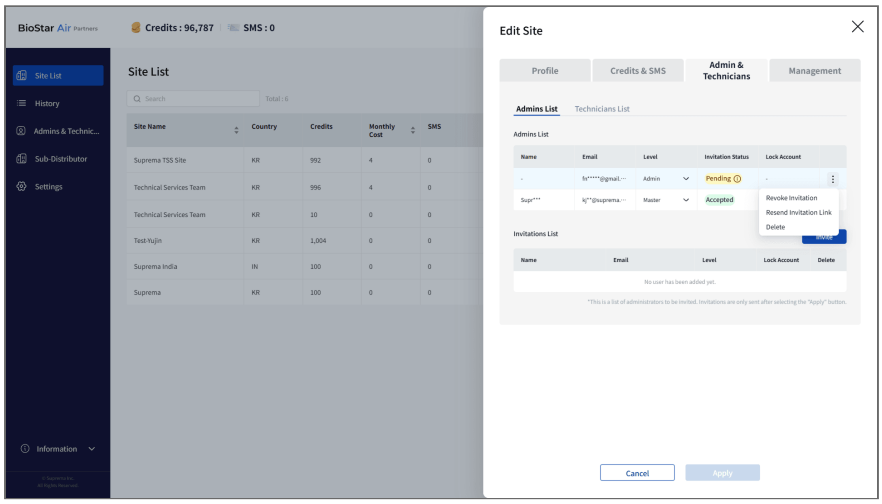
4. Click in the popup menu.
5. If a popup message appears, review the message and click .
6. When the success message for the canceled invitation appears, click **Close**.

When an invitation is canceled, the invitation status changes from to .

Resend invitation link

Resend the invitation link if the invited administrator did not receive the invitation email or has lost it.

1. In the site list, click the site where you invited an administrator.
2. When the panel appears, click → in that order.
3. In , for administrators with status , , or , click ⋮ on the far right.

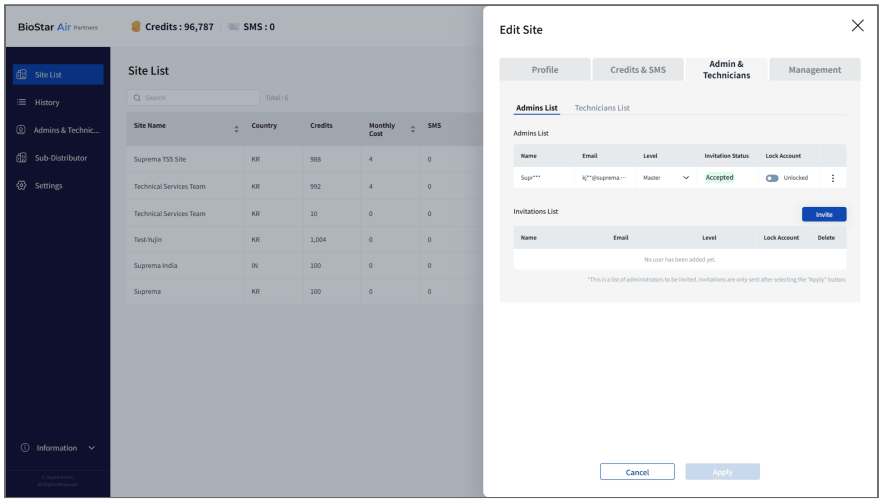


4. Click in the popup menu.
5. If a popup message appears, review the message and click .
6. When the success message for resending the invitation link appears, click **Close**.

Lock or unlock an administrator account

Lock or unlock administrator accounts assigned to a site.

1. Click in the left sidebar.
2. In the site list, click the site where you want to manage administrator access.
3. When the panel appears, click → in that order.

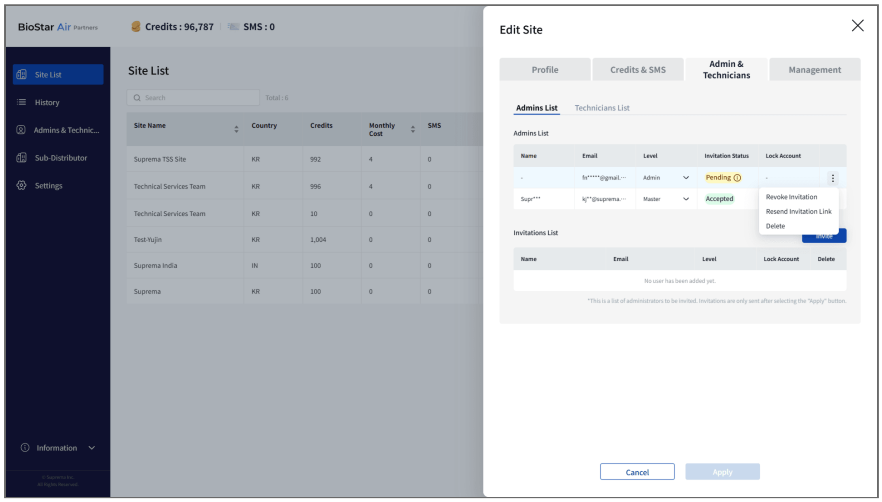


4. In , click the toggle button in the column to lock or unlock an administrator account.
5. Click at the bottom to apply the changes.

Remove administrator

Delete an invited administrator's account. When an administrator's account is deleted, they will no longer be able to sign in to the site, and their access will be fully revoked. Once an administrator account is deleted, it cannot be recovered.

1. In the site list, click the site where you invited an administrator.
2. When the panel appears, click → in that order.
3. In , click ⋮ at the far right of the administrator you want to delete.



4. Click **Delete** in the popup menu.

5. If a pop-up message appears, review it and click **Confirm**.
6. When the success message confirming the administrator's deletion appears, click **Close**.

Manage Partner Technicians

Technician accounts allow partners and installers to support customer sites without sharing an admin account. Partners invite technicians through the partner portal and assign them to specific sites. After assignment, customers and site administrators can activate or update technicians' site permissions in the BioStar Air admin portal. This lets you control partner support access, implement audit trails, and limit access to only the sites that are necessary.

Benefits of technician management

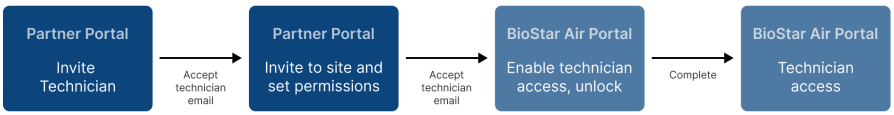
Technician accounts are designed for professionals who provide system installation, maintenance, and technical support across multiple customer sites. Partners can define each technician's role and permission level to implement the following.

- **Enhanced Security**: Reduce the risk of unauthorized access by removing shared admin accounts
- **Compliance**: Meets privacy regulations; option to exclude access to user data
- **Efficient management**: Track and audit individual technicians' activities across multiple sites
- **Flexible permission control**: Granular permissions per technician and per site

Limitations

- **Separate accounts required for the partner portal and the BioStar Air portal**: Each portal requires a separate sign-up process. Passwords are not synchronized between portals.
- **No expiration or time-based access control**: Technician access does not expire automatically. Site administrators must manually lock or remove access.
- **Fixed access permissions**: Only 4 predefined permission levels are available. Custom roles or granular permissions cannot be created.
  - **None** / **Devices Only** / **Full Excluding Users** / **Full Including Users**
- **Customer activation required when assigning technicians**: Technicians assigned by partners must be unlocked by the site administrator before they can access the site. Lack of clear communication may delay support or installation.
- **No bulk assignment**: Technicians must be assigned individually per site.
- **Technician and administrator roles cannot share the same email address**: An email address that is already registered as a technician in the partner portal cannot be invited as an administrator. When changing a role, you must delete the existing account and re-invite the user with the new role.

Overall process



Invite Technicians to the Partner Portal

Using technician accounts, grant partners and installers limited access to sites without a shared admin account. Technicians are managed centrally in the Partner Portal and can be assigned to individual sites.

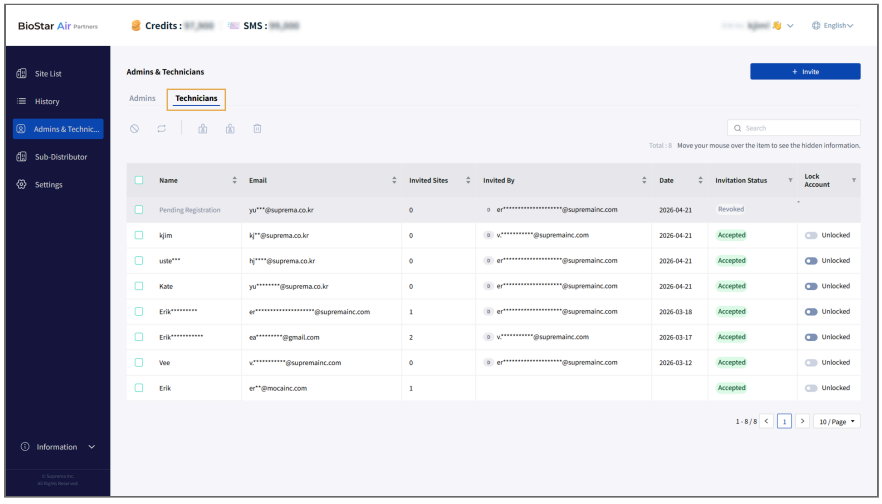
Key Benefits of Technician Accounts

- **Enhanced Security**: Reduce the risk of unauthorized access by removing shared admin accounts
- **Compliance**: Help meet privacy regulations (such as GDPR) and offer an option to restrict access to user data
- **Access Control**: Configure granular permissions from device access to full administrator privileges
- **Audit Trail**: Record individual technician activities in audit logs to track accountability
- **Increased Efficiency**: Assign and manage technicians across multiple sites without login conflicts
- **Immediate Revocation**: Revoke technician access immediately, at any time

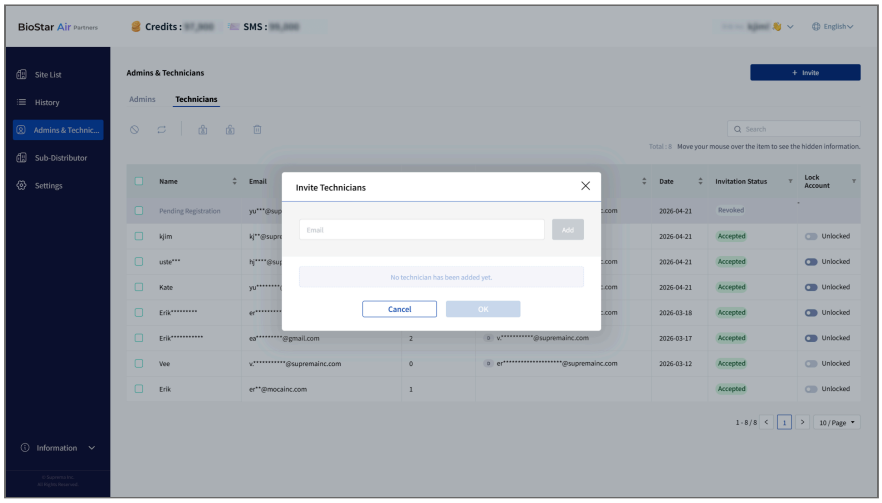
Invite technicians

Partners must invite technicians to create technician accounts before granting site access. Technician accounts are created using an email address. Invited technicians activate their accounts by accepting the invitation sent to their email.

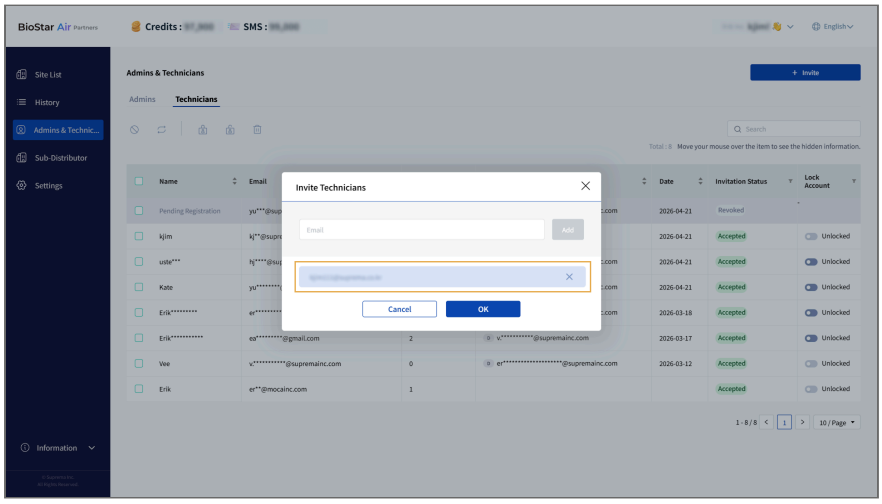
1. Log in to the Partner Portal.
2. Click in the left sidebar.
3. Click the tab.



4. Click at the top right of the screen.
5. When the window appears, enter the email address of the technician you want to invite.



6. Click when it becomes active.
7. Added technicians appear below the email address input field. Repeat steps 5–6 to invite additional technicians.



8. After adding all technicians, click **Ok**.
9. When the confirmation message appears, click **Confirm**.

Info

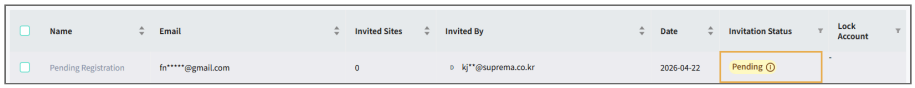
- Inviting technicians to the Partner Portal does not grant them access to sites; you must invite technicians to each site separately. For more information on inviting a technician to a site, see Assign Technicians to a Site.
- Technicians who sign up using the invitation email can sign in to the Partner Portal, but their access to menus is limited. They can only change their own password, delete their account, and set their language.

Invitation status

After inviting technicians, partners can check each technician's invitation status in the technician list.

Pending sign-up

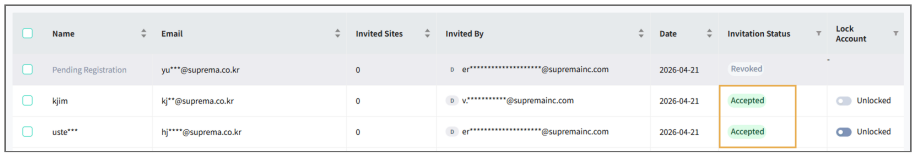
The invitation status is shown as until the invited technician accepts the invitation. Invited technicians can click the link in the email to register an account or sign in to the Partner Portal.



> **Info**
>
> Invited technicians have up to 7 days to accept the invitation. After 7 days, the invitation expires and the status changes to . If an invitation expires, partners can resend the invitation link so the technician can sign up again. For more information on resending invitation links, see Resend invitation link.

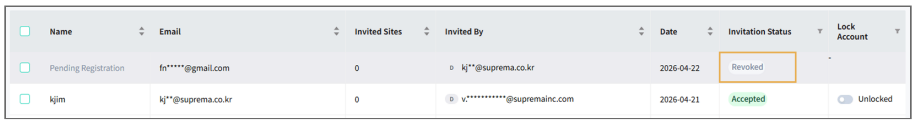
Sign-up complete

When a technician accepts the invitation email and completes sign-up, their invitation status changes to .



Invitation revoked

Partners can cancel an invitation if they entered the technician's email incorrectly, or if the issue has been resolved and the invitation is no longer needed. The invitation status changes to . For more information on revoking a technician's invitation, see Invitation revoked.



Invitation revoked

Partners can cancel an invitation if they entered the technician's email incorrectly, or if the issue has been resolved and the invitation is no longer needed. After you cancel an invitation, the user will not be able to use the invitation link to sign up.

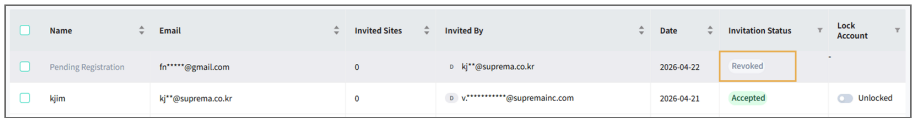
1. In the technician list, select the checkbox for each technician whose invitation status is . You can select 1 or more technicians.
2. Click ⃠ at the top left of the technician list.



> Only technicians with status can have their invitations revoked.

3. If a popup message appears, review the message and click .
4. When the success message for the canceled invitation appears, click **Close**.

The invitation status of a revoked technician changes to in the technician list.



Resend invitation link

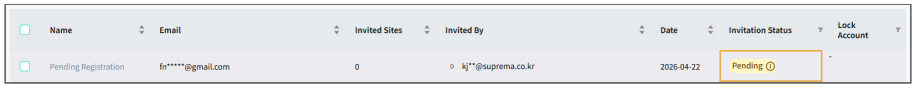
Resend the invitation link if an invited technician did not receive the invitation email, lost it, or the invitation link has expired.

1. In the technician list, select the checkbox for each technician whose invitation status is , , or . You can select 1 or more technicians.
2. Click ↻ at the top left of the technician list.



3. If a popup message appears, review the message and click .
4. When the success message for resending the invitation link appears, click **Close**.

After resending a technician's invitation link, their invitation status changes to in the technician list.



Manage technicians

After the invited technician accepts the email invitation and completes sign-up, partners can manage the following items in the technician list.

- Lock or unlock technician accounts
- Edit site access
- Delete technician accounts

Lock or unlock technician accounts

Partners can lock or unlock technician accounts using the option. Locking a technician account prevents the technician from logging into the Partner Portal and assigned sites. Account information is retained, allowing reactivation when needed.

In the column, locked technicians are shown as , and unlocked technicians are shown as .



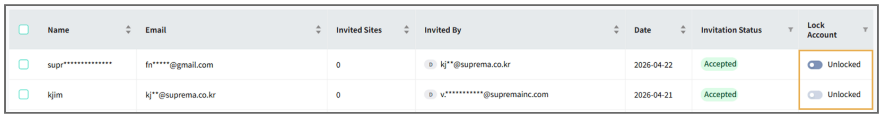
Info

- The accounts of technicians who have completed the sign-up process are unlocked by default.
- Although a Partner Portal admin account may appear in the technician list if it has technician access to certain sites, that admin account cannot be locked or unlocked from the technician list.

Lock or unlock an individual technician account

In the technician list, click the toggle button in the column to lock or unlock an individual technician account.

1. In the technician list, click the toggle in the column.



2. If a popup message appears, review the message and click .
3. When the success message confirming the account lock or unlock appears, click **Close**.

Lock or unlock multiple technician accounts

Select multiple technician accounts in the technician list to lock or unlock them in bulk.

1. In the technician list, click the checkbox for each technician to lock or unlock. You can select 1 or more technicians.
2. Click or in the upper left corner of the screen.

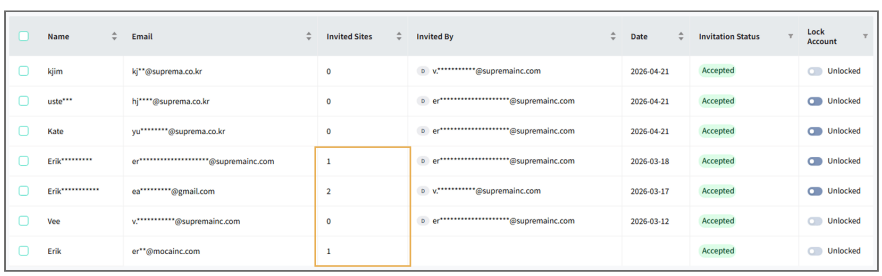


3. If a popup message appears, review the message and click .
4. When the success message confirming the account lock or unlock appears, click **Close**.

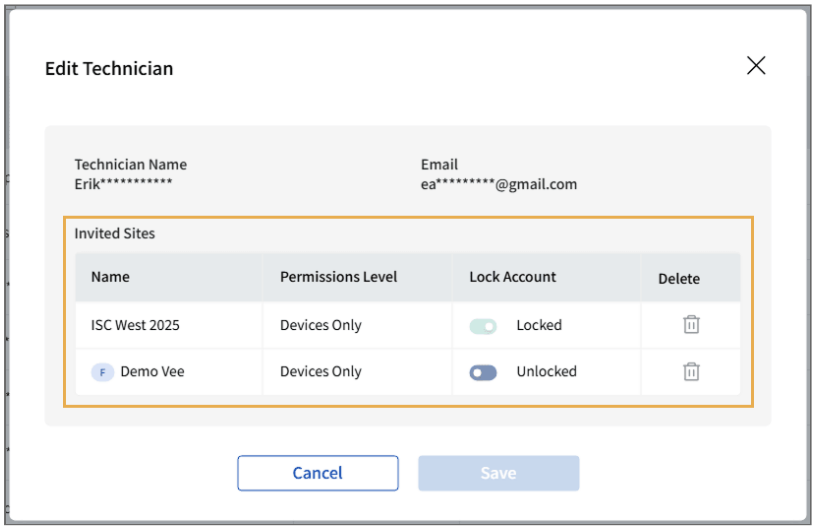
Edit site access

You can modify a technician's site access.

1. In the technician list, click a technician whose column indicates 1 or more sites.



2. When the window appears, check the list of sites the technician is invited to in .



3. Click the toggle button in the column to allow or block site access.
4. Click to save the changes.
5. When a success message appears confirming the site access changes, click **Close**.

> **Info**
>
> - Once a technician is assigned to a site and permissions are set in the Partner Portal, only an administrator account can change those permissions in the BioStar Air admin portal.
> - If a site administrator locks a technician's site access in the BioStar Air portal, it cannot be unlocked from the Partner Portal. To modify a technician's site access, use an account with administrator privileges for that site in the BioStar Air portal.
> - For more information on granting site access to a technician, see Assign Technicians to a Site.

Delete technician accounts

If you no longer need technician's support, you can delete their account. Deleting a technician account prevents the technician from logging in to the Partner Portal and permanently removes all information associated with the account from the system.

1. In the technician list, click the checkbox of the technician you want to delete. You can select 1 or more technicians.
2. Click in the upper left of the screen.



3. If a pop-up message appears, review it and click **Confirm**.
4. When the account deletion success message appears, click **Close**.

Deleted technician accounts no longer appear in the technician list.

Assign Technicians to a Site

Partners can assign technicians to customer sites and set permissions. Manage granular access levels for each technician to protect sensitive personal information.

Key features of assigning technicians to sites

- **Granular access settings**: Flexible options from device access to full administrator rights
- **User data protection**: Comply with privacy regulations by using the option to exclude user data access
- **Efficient management**: Manage technicians at each site according to partner-defined permission levels

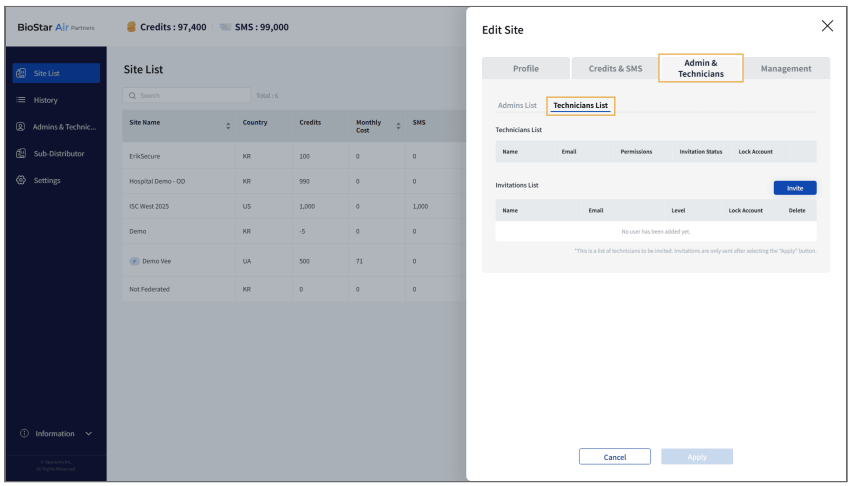
> **Info**
>
> - Before assigning technicians to a site, invite their accounts in the Partner Portal. For more information, see Invite Technicians to the Partner Portal.
> - For more information on assigning technicians to a site in the BioStar Air administrator portal, see Manage Technician Accounts.

Assign technicians to a site

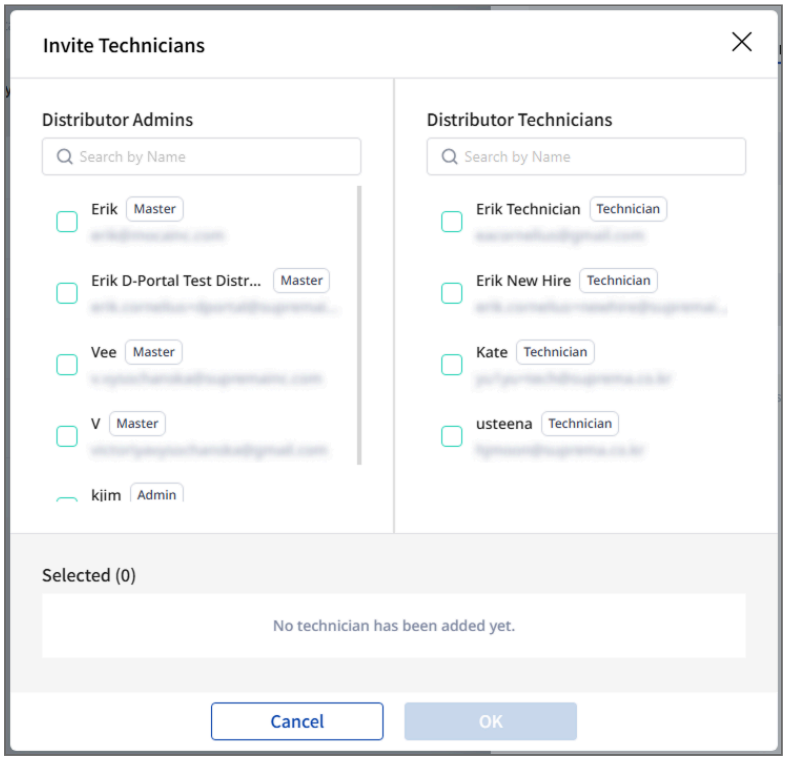
After inviting a technician in the Partner Portal, assign the technician to each individual site so they can access those sites. Follow the steps below to assign a technician to a site.

1 Go to the site list

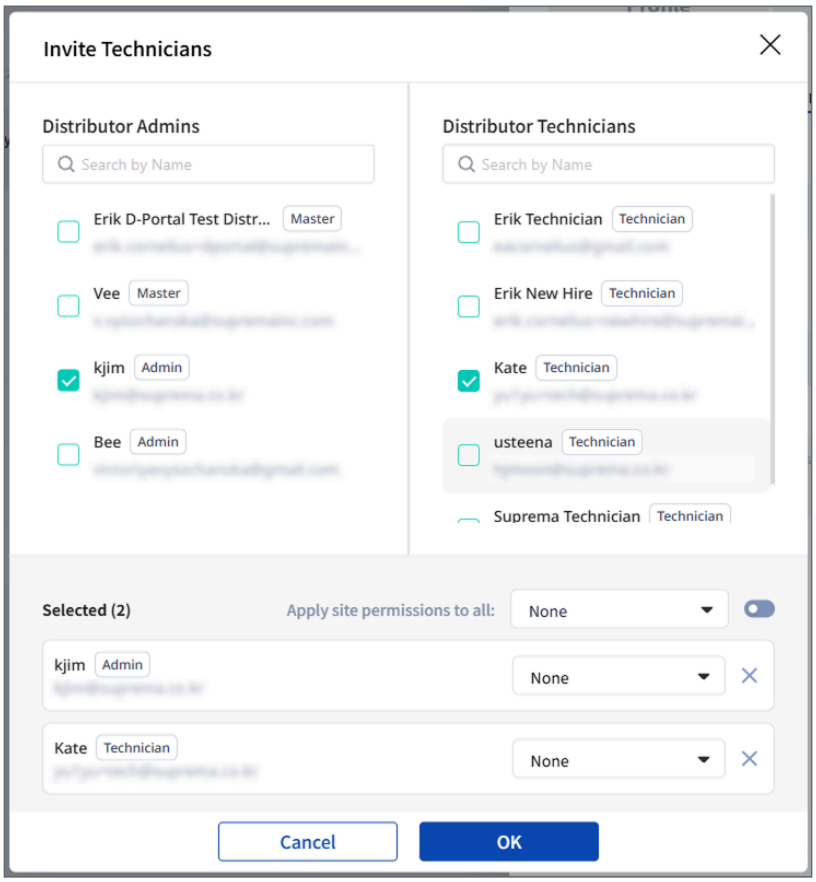
1. Log in to the Partner Portal.
2. Click in the left sidebar.
3. In the site list, click the site to which you want to assign a technician.
4. When the panel appears, select the tab, then the tab.



5. Click .
6. When the window appears, select the desired account from the or list.



Selected accounts appear in the list at the bottom.



Info

- Enter an administrator's or technician's name in the name search field.
- To cancel the selected account, in the list, click ✕ to the right of the account.
- Accounts that are registered as site administrators or already assigned as technicians to the site will not appear in the list.

2 Set site access permissions

After selecting all technicians you want to invite, apply the site access permissions. Available permissions are as follows.

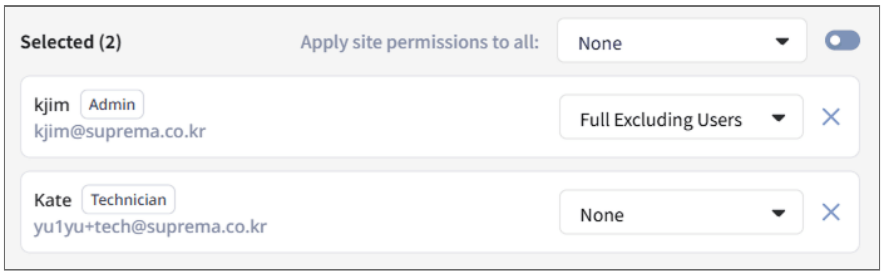
- : Can be added to the site but cannot log in.
- : Can only access the **Dashboard** and **Device Management** menus.
- : Can access all menus except the **User Management** menu, but access to certain settings is restricted.
- : Can access all menus including the **User Management** menu, but access to certain settings is restricted.

Info

- and have view-only access to the following menu path.
  - **Settings** → **Admins & Technicians**
  - **Settings** → **Site**
- Once a technician is assigned to a site and permissions are set in the Partner Portal, only an administrator account can change those permissions in the BioStar Air admin portal.

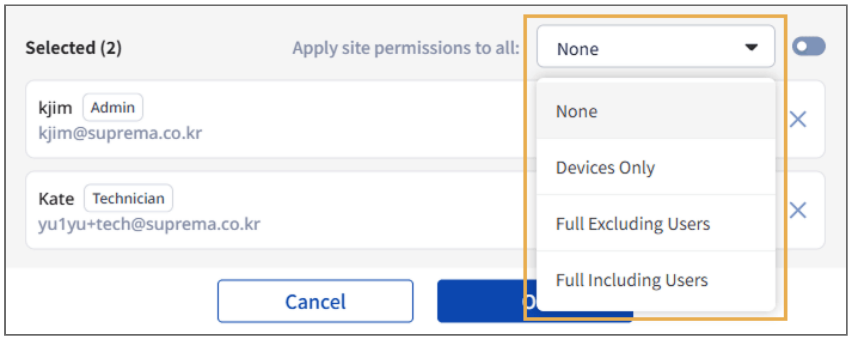
3 Set permissions for individual technicians

Assign different permissions to individual technicians. To the right of each account, select the desired permission level.

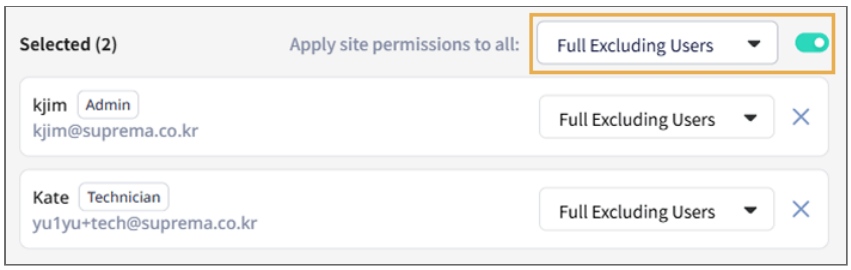


4 Apply the same permissions to all technicians

1. Choose the desired permission level from the option, then click the toggle on the right to apply the same permissions to all selected accounts.

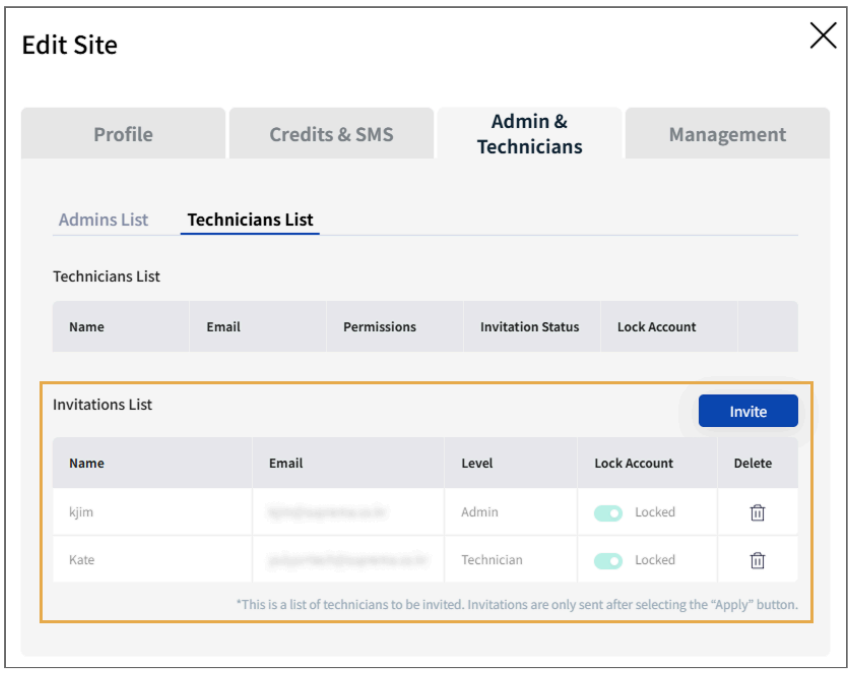


2. When the confirmation message appears, click .
3. The selected permission is applied to all accounts in the list.



5 Technician invitation completed

1. After completing technician invitations and permission settings, click **Confirm** in the window.
2. The window closes, and the invited technicians are listed under in the panel.



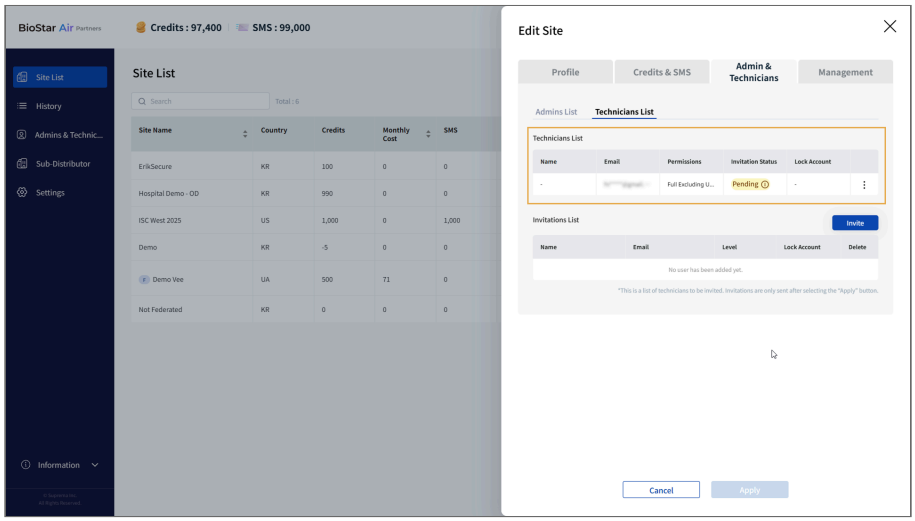
3. To send invitation emails and allow technicians to access the site, click at the bottom of the panel.

Check invitation status

Check the invitation status of technicians invited to the site. The invitation status is shown as until the invited technician accepts the invitation. Invited technicians have up to 7 days to accept the invitation. After 7 days, the invitation expires and the status changes to .

1. In the site list, click the site where you invited the technician.
2. When the panel appears, select the tab, then the tab.
3. : Check the invitation status.

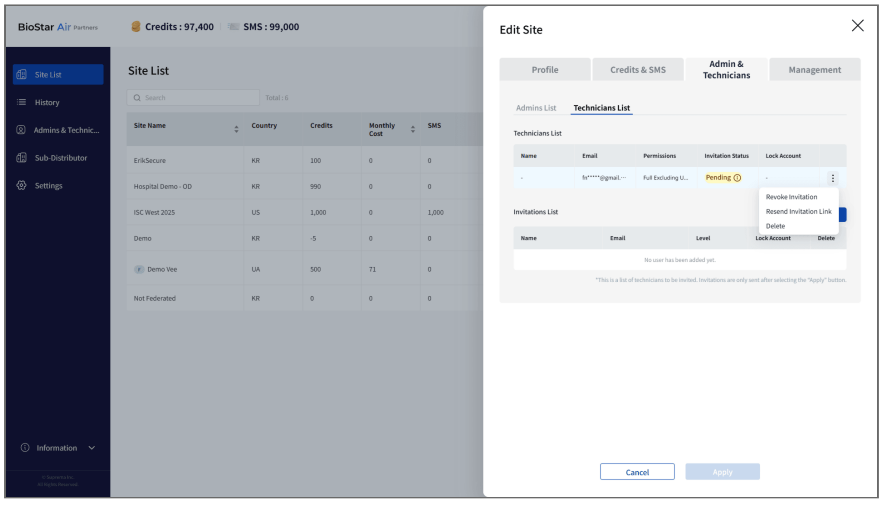
When a technician completes signing up for the site, their status changes from to .



Invitation revoked

You can cancel the invitation if the invited technician's email address was entered incorrectly, or if the issue has been resolved and the invitation is no longer needed.

1. In the site list, click the site where you invited the technician.
2. When the panel appears, select the tab, then the tab.
3. In , for the technician whose status is , click ⋮ at the far right.



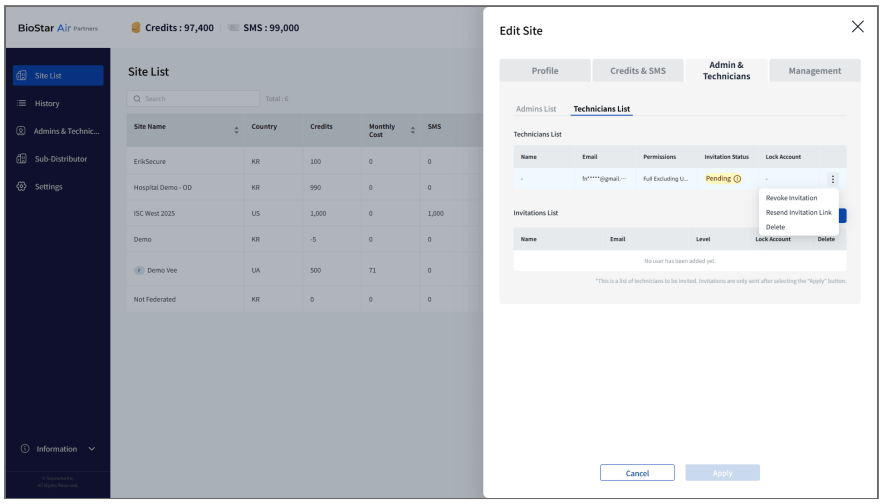
4. Click in the popup menu.
5. If a popup message appears, review the message and click .
6. When the success message for the canceled invitation appears, click **Close**.

When an invitation is canceled, the technician's status changes from to .

Resend invitation link

Resend the invitation link if an invited technician didn't receive the invitation email or has lost it.

1. In the site list, click the site where you invited the technician.
2. When the panel appears, select the tab, then the tab.
3. In , for the technician whose status is , , or , click ⋮ at the far right.

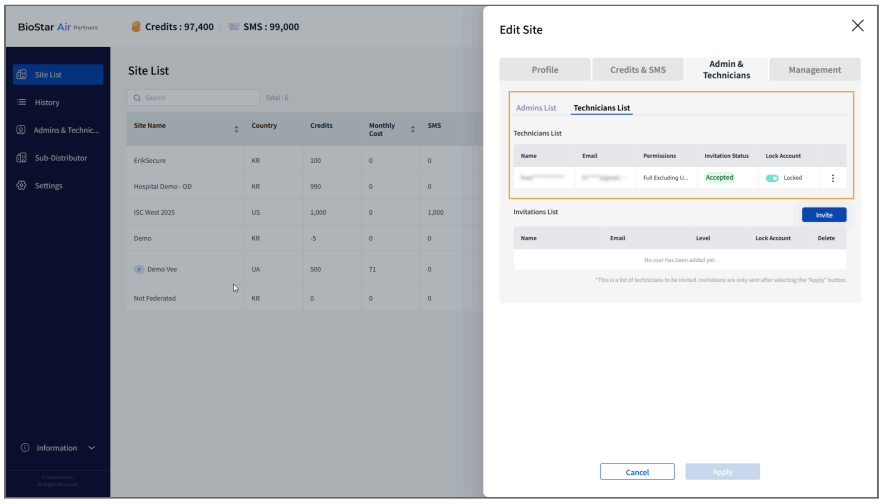


4. Click in the popup menu.
5. If a popup message appears, review the message and click .
6. When the success message for resending the invitation link appears, click **Close**.

Lock or unlock technician accounts

Lock or unlock accounts for technicians assigned to a site.

1. Click in the left sidebar.
2. In the site list, click the site where you want to manage technician access.
3. When the panel appears, select the tab, then the tab.



4. In , click the toggle button in the column to lock or unlock a technician account.

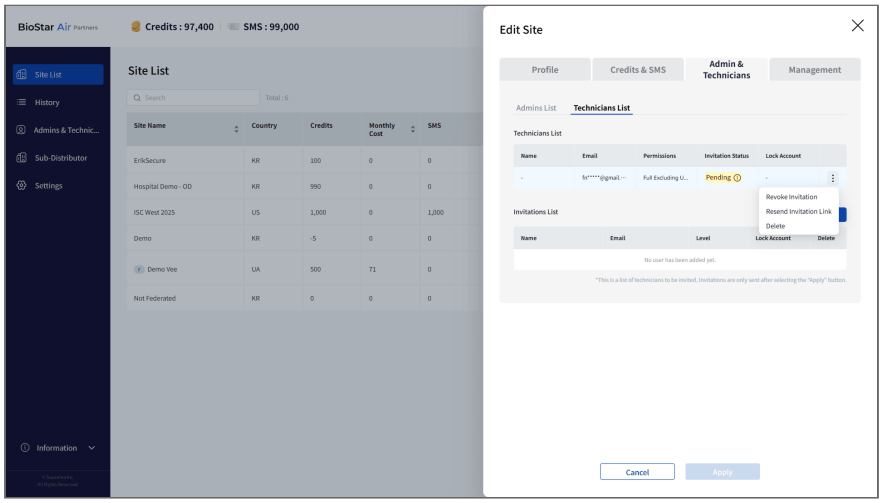
5. Click at the bottom to apply the changes.

> **Info**
> Newly registered technician accounts have site access set to . To unlock the status, use an account with administrator rights for that site in the BioStar Air portal.

Delete technician accounts

You can delete the account of a technician invited to the site. When a technician's account is deleted, they cannot sign in to the site and their access is revoked.

1. In the site list, click the site where you invited the technician.
2. When the panel appears, select the tab, then the tab.
3. On , click ⋮ at the far right of the technician you want to delete.



4. Click **Delete** in the popup menu.
5. If a pop-up message appears, review it and click **Confirm**.
6. When the success message confirming the technician's account deletion appears, click **Close**.

> **Info**
> Deleting a technician account does not remove the account entirely; it only revokes access to that site. Re-invite a deleted technician to the site to restore access.

Installing the Hardware

This is a hardware installation and setup guide for configuring the BioStar Air system correctly. These documents explain how to connect and configure each device, including SIP intercoms, IP cameras, QR scanners, and Airfop Patch, as well as how to set up network ports and security module settings.

Configure SIP Intercom for BioStation 3

As of **BioStar Air v2.10**, **BioStation 3** (BS3) supports the SIP intercom feature. This enables two-way voice calls between the reader and administrators and remote door unlocking.

> **Info**
> A SIP server is required to use this feature; purchase and configure it separately. Suprema does not provide SIP services.

SIP

Session Initiation Protocol (SIP) is a communication protocol widely used to initiate, maintain, and terminate real-time voice and video calls over IP networks. In this context, SIP lets BioStation 3 act as an intercom endpoint that can place and receive calls through a compatible SIP service.

Receive calls

Answer calls received from BioStation 3 in the following ways.

- **BioStar Air Web**: Receive calls directly in a web browser
- **BioStar Air Mobile App** (iOS / Android): Receive calls on the go

Remote door control

When answering a SIP call, use **DTMF commands** to unlock the door:

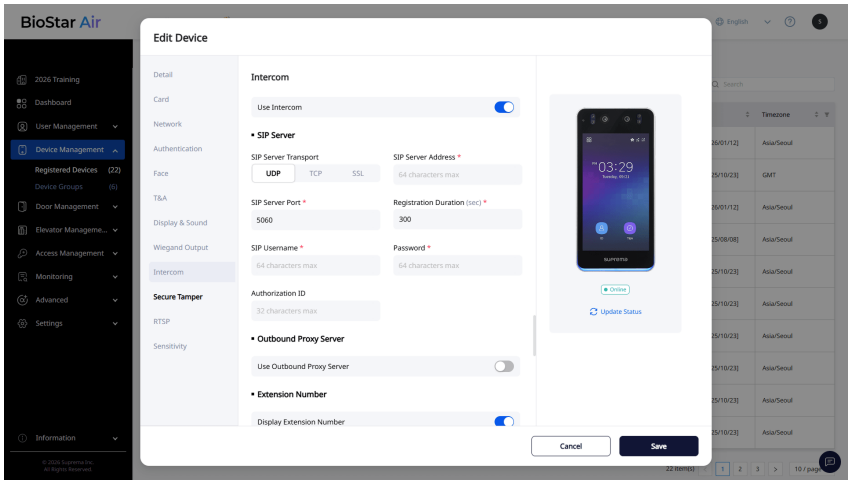
- Hardware SIP phone
- BioStar Air mobile app
- BioStar Air Web interface

Configuration steps

Configure this in device settings and administrator account settings.

1 Device settings

1. Log in to the BioStar Air portal.
2. Click **Device Management** → **Registered Devices** in the left sidebar.
3. In the device list, click **BioStation 3**.
4. Go to the **Intercom** section and enable the **Use Intercom** option.
5. Enter the SIP server information.



The image above is an example screen and may differ from the actual screen.

- **SIP Server Address**
- **SIP Server Port**
- **SIP Username** / **Password**

6. Click **Save** to save the changes.

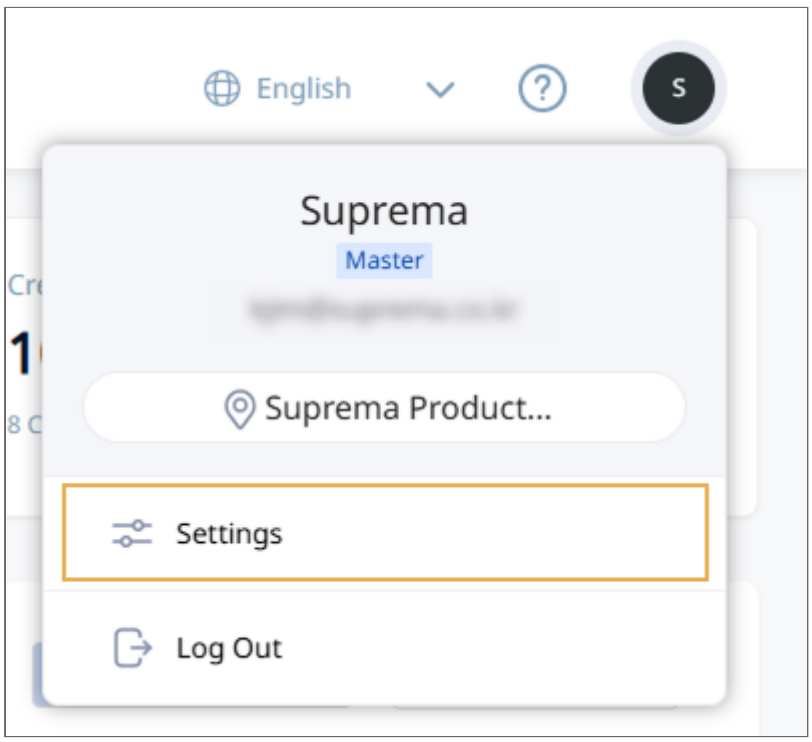
2 Account settings

Route calls from BioStation 3 to a browser or app.

1. For each administrator who needs to receive calls, log in to the BioStar Air portal or mobile app.
2. Go to **Account settings**.

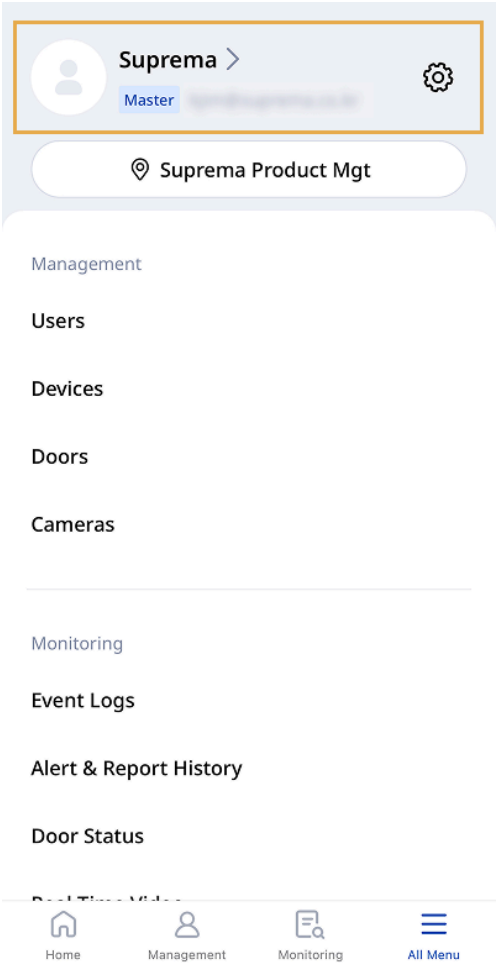
Web

Click the user profile icon at the top right of the screen and select **Settings**.



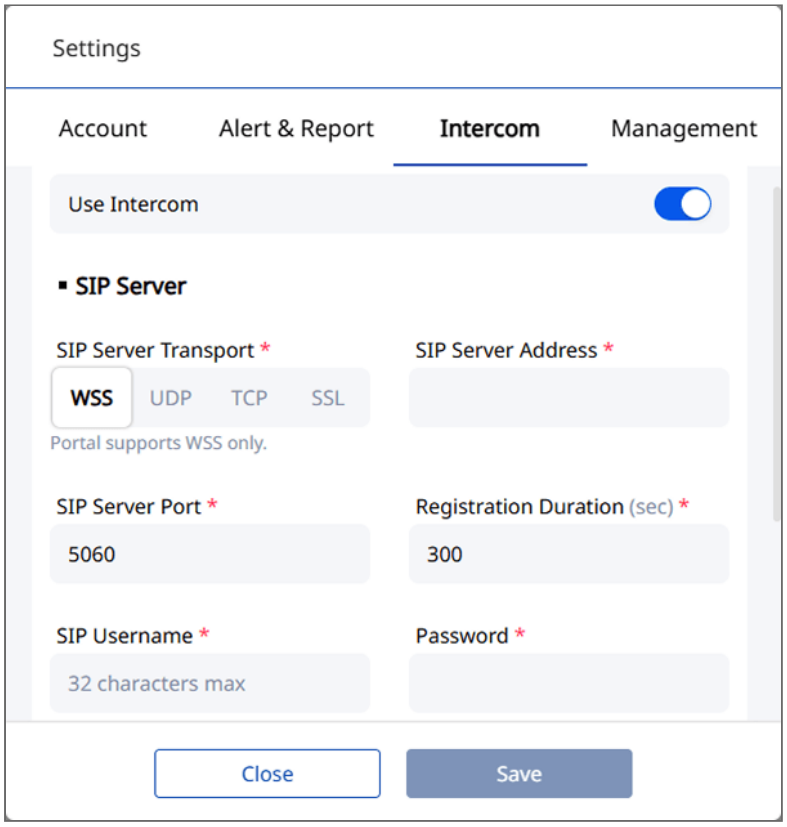
Mobile

On the home screen, tap **All Menu** at the bottom, then tap the user profile area.

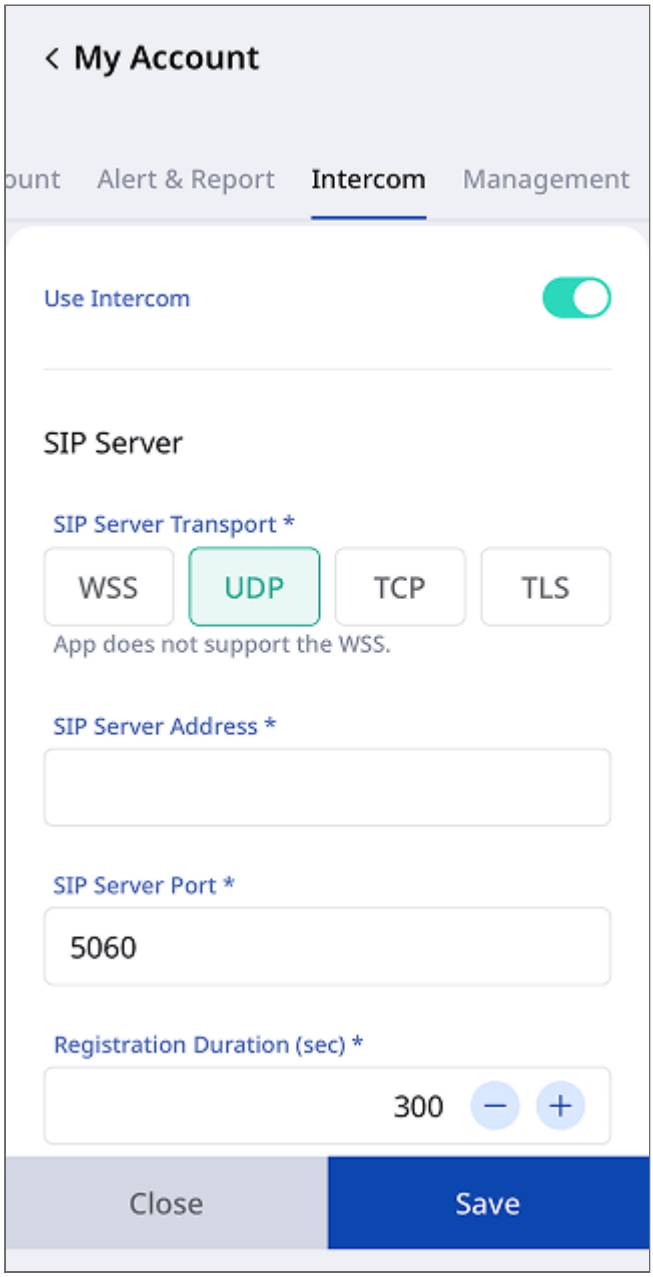


3. When the **Settings** window appears, click the **Intercom** tab and add the SIP server login information.

Web


Settings
Account
Alert & Report
Intercom
Management
Use Intercom
SIP Server
SIP Server Transport *
SIP Server Address *
WSS
UDP
TCP
SSL
Portal supports WSS only.
SIP Server Port *
Registration Duration (sec) *
5060
300
SIP Username *
Password *
32 characters max
Close
Save

Mobile



4. Click **Save** to save the settings.

Verified SIP providers

BioStation 3 has been tested and confirmed to work properly with the providers below.

- RingCentral
- FreePBX
- Linphone
- Linhome

IP Camera Support and Setup

BioStar Air automatically detects IP cameras connected to the same network as readers compatible with BioStar Air. Because the cameras use the device as a gateway, a network video recorder (NVR) is not required. Instead, the cameras use

the built-in SD card storage.

With a reader compatible with BioStar Air installed, BioStar Air can display the following concurrent live view streams.

- Up to two cameras at Full HD resolution (1080p)
- Up to four cameras at HD resolution (720p)

These specifications double when X-Station 2 is used.

> **Info**
> If a recorded video does not play after you register the camera in BioStar Air, see Troubleshoot Video Playback Issues.

Compatibility

- **Onvif profiles**: The IP camera must be compatible with Onvif profile S or G.
  - **Onvif profile S**: Live video streaming
  - **Onvif profile G**: Recorded video stored on the SD card
- **SD card**: The IP camera must have a built-in SD card so that recorded footage can be played back later.

  > Use SanDisk microSDXC Class10 Max Endurance 256 GB or 512 GB.

- **Encoding**: The camera must support H.264 (AVC) and it must be set as the active codec. BioStar Air currently does not support H.265.
- **Recommended brands**: HanwhaVision, Hikvision, and Dahua cameras are highly compatible. Compatibility with other brands may vary depending on Onvif profile compliance. For details on the list of tested and verified devices, see Tested and verified devices list.
- Contact the service team to test other camera brands.

Functionality overview

Perform the following actions in the BioStar Air portal or mobile app.

- View live camera feeds.
- View recorded camera footage.
- Access camera footage related to access events.

Instructions

1 Connect IP cameras

- **Network connection**: Ensure that the IP camera is on the same network as the reader compatible with BioStar Air.

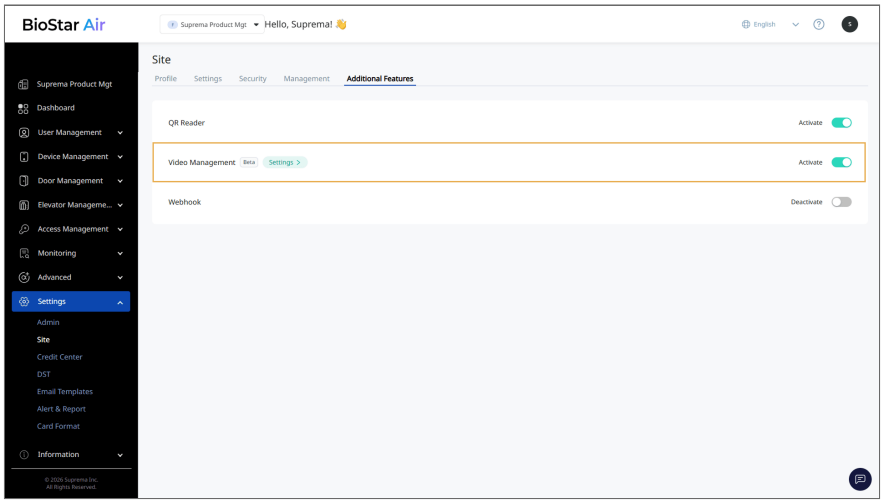
- **Enable Onvif**: Make sure Onvif is enabled on the camera.
- **Device registration**: Make sure the device is registered in the BioStar Air portal.

2 Log in to BioStar Air

Master administrators can change site settings such as enabling Video Management. Log in to the BioStar Air portal with **master** privileges.

3 Enable video management

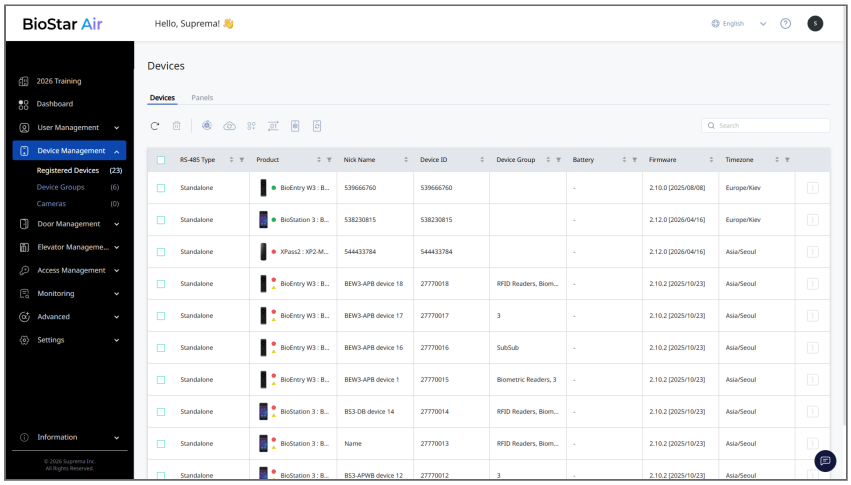
1. Click **Settings** → **Site** in the left sidebar.
2. Click the **Additional Features** tab.
3. Enable **Video Management**.



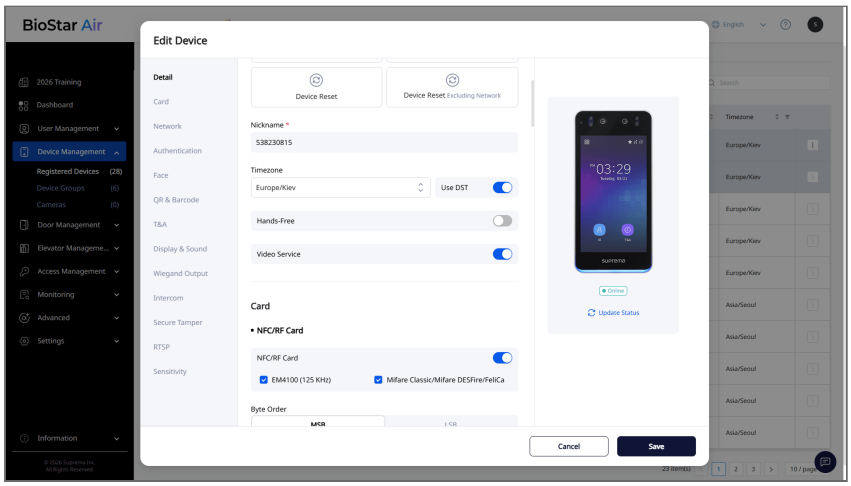
> **Info**
> Only **master**-level administrators can enable this feature.

4 Enable video service

1. Click **Device Management** → **Registered Devices** in the left sidebar.



2. Click the device(e.g. BioStation 3) compatible with BioStar Air in the list.
3. The **Edit Device** window appears.
4. Enable **Video Service** in the **Detail** section.

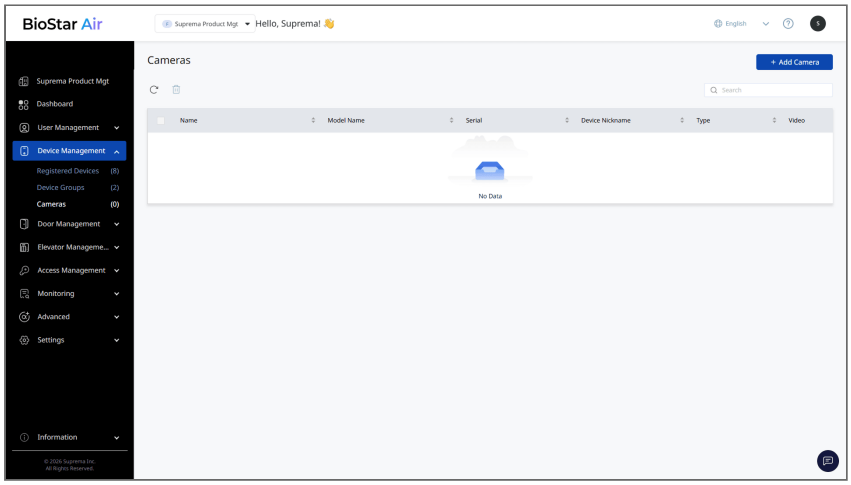


5. Click **Save** at the bottom to save the changes.

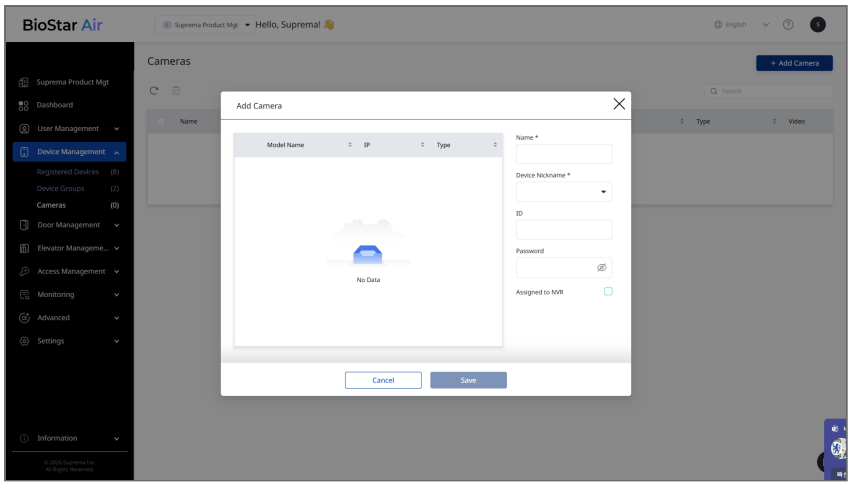
> **Info**
> The device must run firmware version 2.5.1 or later and be on the same network as the camera.

5 Add camera

1. Click **Device Management** → **Cameras** in the left sidebar.



2. Click **Add Camera** at the top right of the screen.
3. When the **Add Camera** window appears, select the device that will act as the gateway.



The image above is an example screen and may differ from the actual screen.

4. Set the following information to add the camera.
   - **Name**: Enter the camera name.
   - **Device Nickname**: Select a name to identify the camera.
   - **ID**: Enter the ID to connect to the camera.
   - **Password**: Enter the password to connect to the camera.
5. Click **Save** to add the selected camera.

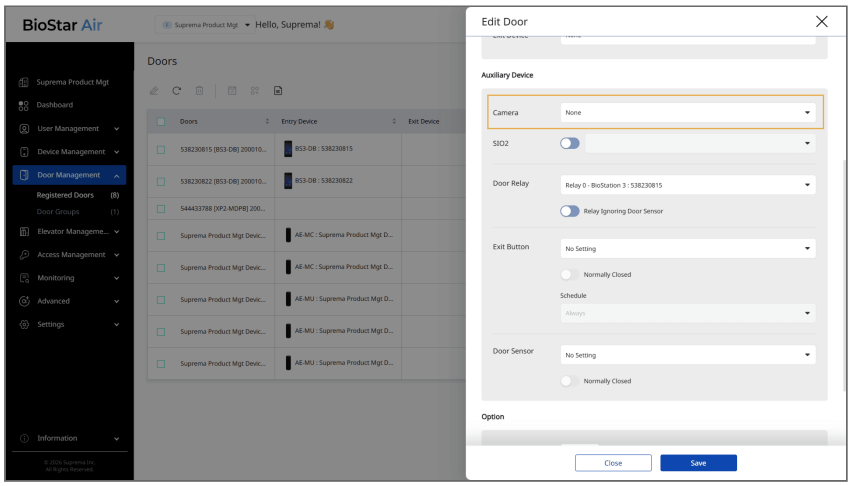
Info

- The device must run firmware version 2.5.1 or later and be on the same network as the camera.
- BioStar Air automatically discovers cameras on the network.

6 Link to a door

Link the added camera to a door to associate video with access events.

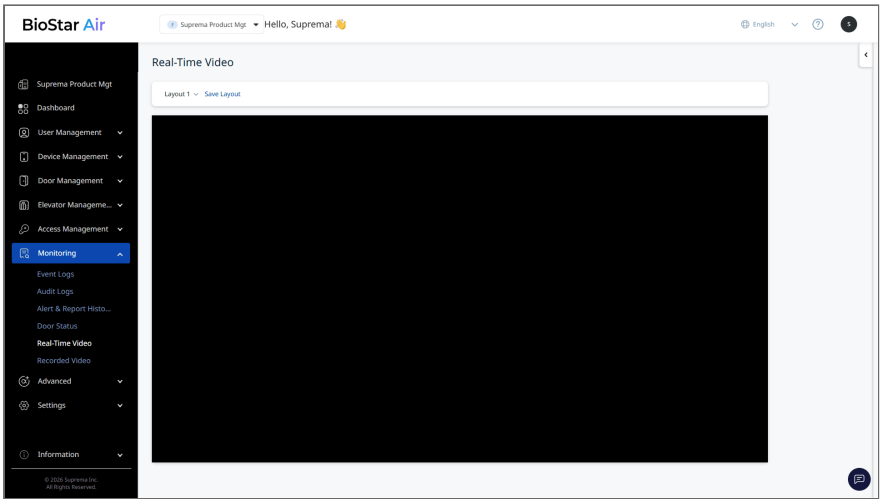
1. Click **Door Management** → **Registered Doors** in the left sidebar.
2. Click the door in the list to assign a camera.
3. When the **Edit Door** panel appears, scroll to **Auxiliary Device**.
4. Select the camera you added from **Camera**.



5. Click **Save** to save the changes.

7 View live camera video

View live video from the added cameras. Click **Monitoring** → **Real-Time Video** in the left sidebar.



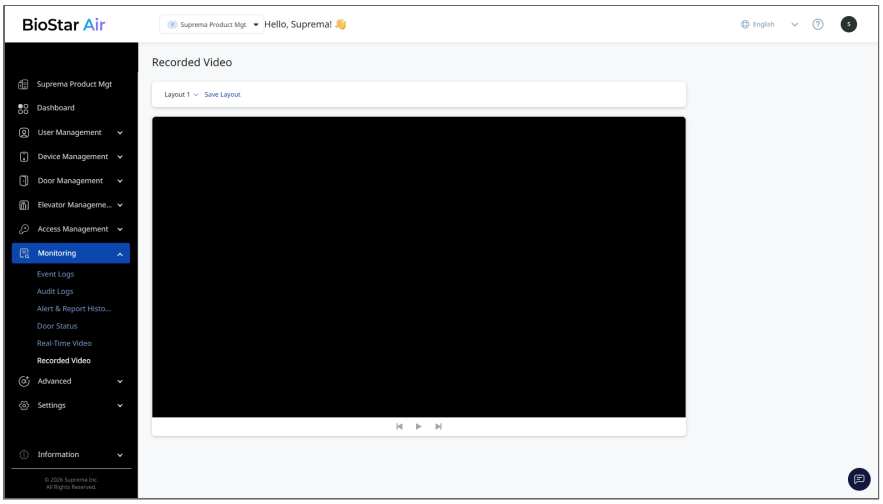
The image above is an example screen and may differ from the actual screen.

- View up to two Full HD (1080p) live streams per installed reader compatible with BioStar Air.
- Add more devices or reduce camera resolution to view more live streams.

> ***Device Management*** → ***Cameras*** → *Click camera in the list* → ***Video Profile***

8 View recorded camera video

View recorded video streams. Click **Monitoring** → **Recorded Video** in the left sidebar.



The image above is an example screen and may differ from the actual screen.

9 View event video

Click **Monitoring** → **Event Logs** in the left sidebar. Find an event log with an associated video clip and click play to watch it.

Tested and verified devices list

No	Manufacturer	Model number	Device type	Onvif profile	Resolution
1	Hanwha Techwin	QNV-C8011R	Camera	S, G, T, M	2592x1944
2	Hanwha Techwin	QND-6022R	Camera	S, G, T	1920x1080
3	Hanwha Techwin	MMI-600R	Camera	S, T	1920x1080
4	HIKVISION	DS-2CD2025FWD-I	Camera	S, G, T	1920x1080
5	HIKVISION	DS-2CD2166G2-I	Camera	S, G, T	3200×1800
6	HIKVISION	DS-2CD1121-I	Camera	S	1920x1080
7	Dahua	DHI-NVR2104HS-P-S3	NVR	S, G, T	12MP
8	Dahua	IPC-HDBW3249E-AS-NI	Camera	S, G, T	1920×1080
9	Dahua	SD22204UEN-GN	Camera	S, G, T	1920×1080
10	Dahua	DH-IPC-HFW1230DT-STW-VN	Camera	S, T	1920×1080
11	Marruy	IPC-A32E-L	Camera	S, T	2304×1296

No	Manufacturer	Model number	Device type	Onvif profile	Resolution
12	TP-Link	Tapo C210	Camera	S	2304×1296

Enable ONVIF on an IP camera

1. Open a web browser and enter the camera's IP address.
2. Authenticate with administrator credentials and log in.
3. Go to the **Network** or **Configuration** section.
4. Enable ONVIF or the open network video interface.
5. Create an ONVIF-only user profile if necessary.
6. Save the settings and test the ONVIF connection in BioStar Air.

Tip

- **Firmware update**: Update the camera and the device to the latest firmware.
- **Port forwarding**: Configure port forwarding for ONVIF if required.
- **Third-party tools**: Use ONVIF Device Manager to verify camera settings and functionality.

Install Airfob Patch

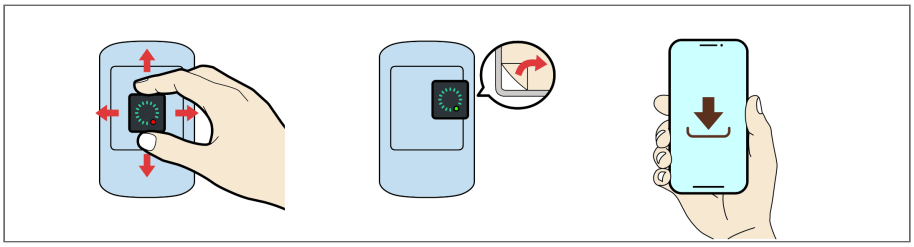
This guide explains how to install Airfob Patch. The Airfob Patch upgrades an existing access control system to work with BioStar Air mobile credentials.

Info

- Airfob Patch is compatible with MIFARE 1K technology but are not compatible with 125 kHz **low-frequency** readers.
- Airfob Patch authenticates encrypted Bluetooth BioStar Air credentials and emulates a MIFARE RFID signal to the reader. It attaches to access control readers with tape and requires no wiring.
- For more information on how to register an Airfob Patch in the BioStar Air app, see Configure Airfob Patch and Tag.

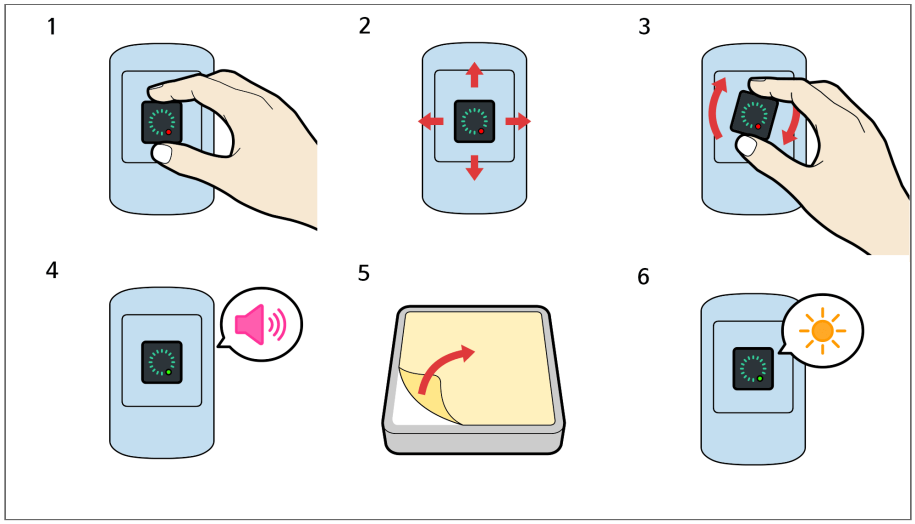
Installation overview

Find the location where the Airfob Patch is powered by the reader's RF field.



Check the Airfob Patch installation location

Before permanently attaching the Airfob Patch to the access control reader with the included adhesive tape, find the best location on the reader by following the actions in the diagram and instructions below.



1. Position Airfob Patch on the access control reader so that they touch each other.
2. Find a spot where the Airfob Patch LED blinks green at least once per second.
3. Hold the Airfob Patch on the reader or temporarily attach it with removable tape. Register the Airfob Patch in using the BioStar Air app. For more information, see Configure Airfob Patch and Tag.
4. Perform at least five test authentications using an Airfob or BioStar Air mobile credential.
5. Remove the protective film of the double-sided adhesive tape on the back of Airfob Patch.
6. Attach Airfob Patch permanently to the access control reader.

Info

- Airfob Patch does not require an additional power supply. Attaching it on access control reader will power on the device.
- When you attach the Airfob Patch to a reader with the included double-sided tape, consider it permanent. Removing the Airfob Patch may destroy it and make reuse impossible.

Troubleshooting

▼ Q. The access control reader does not emit five consecutive beeps.

If the access control reader does not emit five consecutive beeps, reboot the Airfob Patch.

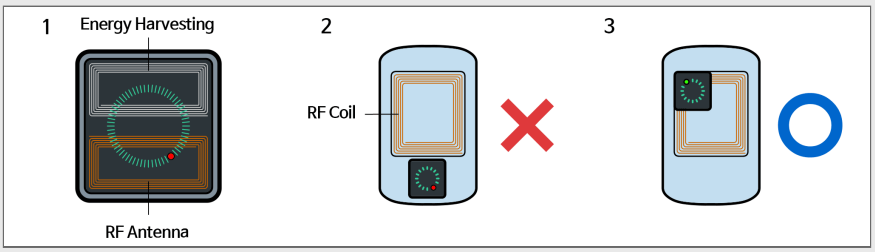
1. Detach the Airfob Patch from the access control reader.
2. When power turns off, the Airfob Patch LED blinks red for about 6 seconds, then turns off.
3. Make sure the Airfob Patch is powered off, then start over.

▼ Q. The Airfob Patch LED blinks red.

If the Airfob Patch LED blinks red, adjust the patch position.

1. Move the Airfob Patch to another location on the access control reader and check whether the LED blinks green.
2. If the power strength is high, the LED blinks at 0.5-second or 1-second intervals.
3. If you change the Airfob Patch position, reboot the Airfob Patch and start over.

▼ Q. The access control reader does not recognize the Airfob Patch.



- The two devices work properly when the access control reader RF coil position matches the Airfob Patch RF antenna position.
- If valid access rights are not granted when you touch the access control reader with a mobile device, adjust or rotate the Airfob Patch to find a location where it works properly.
- The position and orientation of the Airfob Patch may vary depending on the access control reader.
- The operating range of the Airfob Patch may be small or large depending on the RF signal strength of the access control reader and the position and size of the RF coil.

Configure SIO2 Secure Module

SIO2 secure module enhances access control system security by acting as an intermediary between the reader compatible with BioStar Air and relays. It communicates with the reader over an **RS485 cable** and blocks security breaches through encrypted communication.

Caution

Refer to the wiring diagram included in the product package for precise installation instructions for the **SIO2 secure module**. Because installation methods may vary by environment, request professional assistance from a Suprema distributor.

Enable SIO2 in the BioStar Air portal

Enable the **SIO2** option by following these steps to properly integrate the SIO2 secure module and enhance access control system security.

Info

If SIO2 is installed but the settings are not changed in the BioStar Air portal, it may not operate.

1 Register the reader

- Verify that the reader, SIO2, and door relay are connected successfully.

- Register the reader to the site through the **BioStar Air app**.

2 Check the device connection

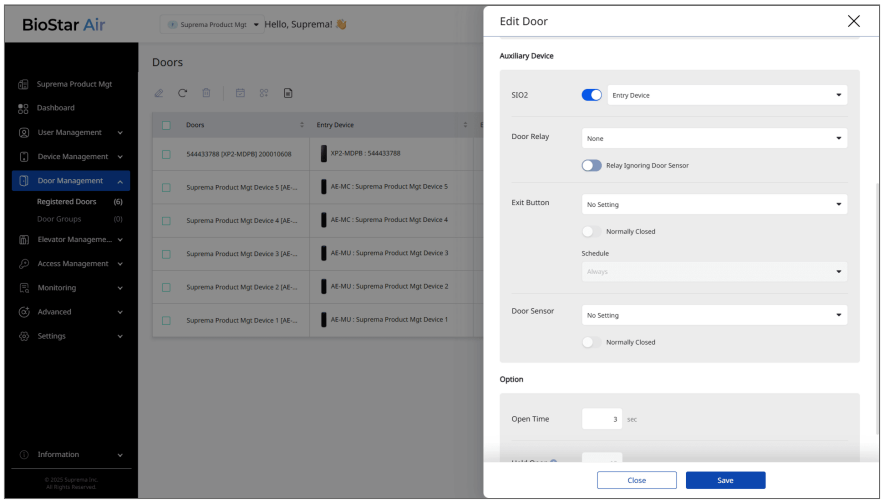
1. Access the BioStar Air portal.
2. Click **Device Management** → **Registered Devices** in the left sidebar.
3. In the device list, verify that the device appears in **green** (🟢) to confirm the connection.

3 Assign SIO2 to a door

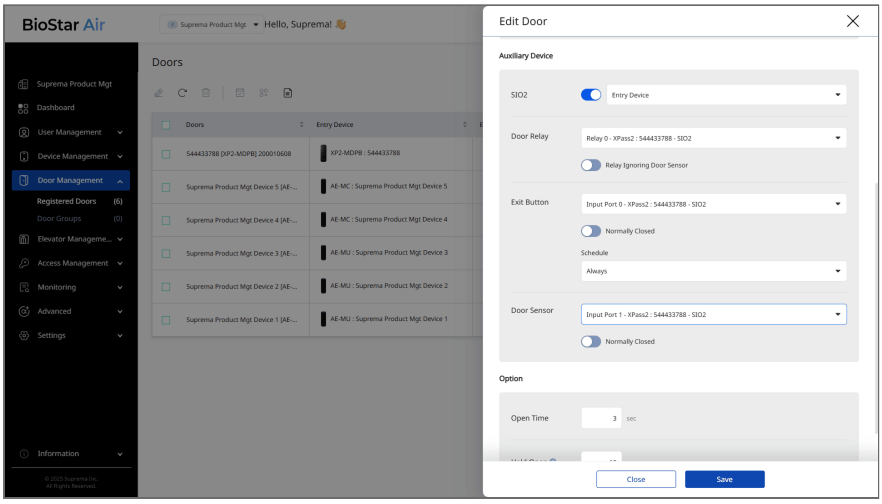
1. Click **Door Management** → **Registered Doors** in the left sidebar.
2. Click the door linked to the device in the list. Registering the device automatically creates a door.

4 Enable SIO2

1. When the **Edit Door** panel appears, go to **Secondary Device**.
2. Enable the **SIO2** option.



5 Configure relay and sensors



The image above is an example screen and may differ from the actual screen.

- For **Door Relay**, select **Relay 0**.

> The SIO2 module has only one door relay port.

- For **Door Sensor**, select the input port number of the connected SIO2.
- If **Exit Button** is connected, select the corresponding input port on the SIO2.
- If another type of exit device is used, select **Exit Device**.

6 Save the settings

- Click **Save** to apply the settings.
- The SIO2 secure module now operates normally.

Wiring and Configuring the E200 QR Scanner

Step 1: Wire

Connect the E200-series QR scanner using the included adapter cable as shown below.

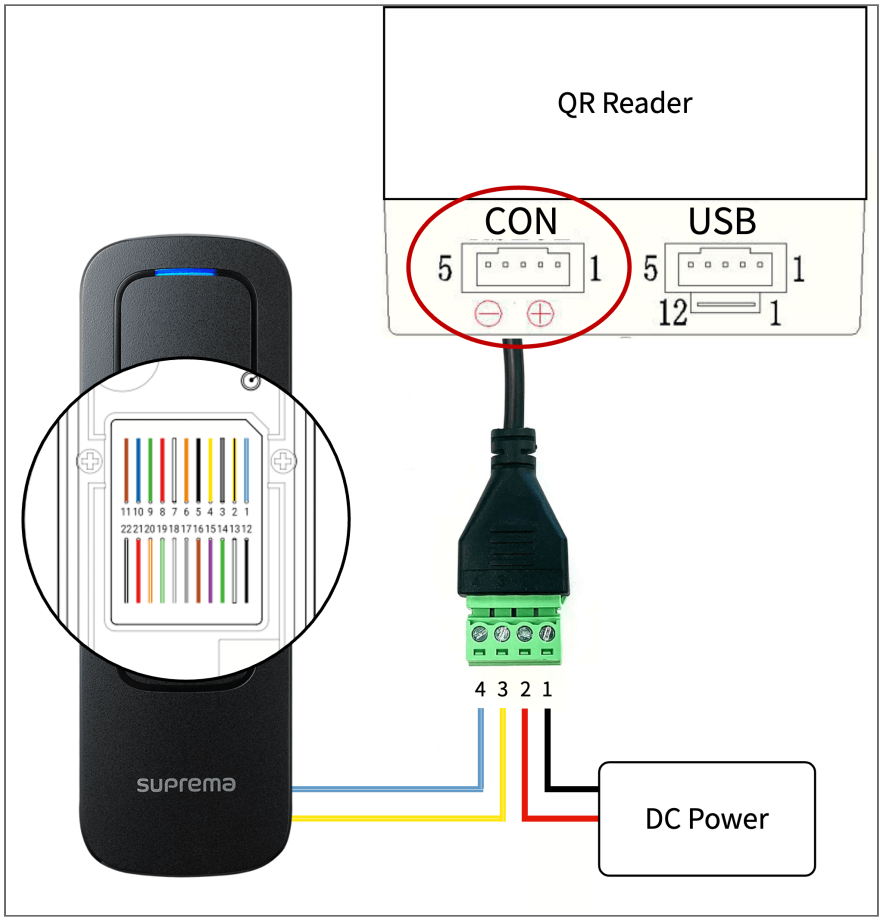
- The green terminal block has pins labeled **1 through 4**, arranged **right-to-left** when you face the front of the connector.

Pin	Wire color	Feature
1	Black	Negative / Ground
2	Red	Positive (V+)
3	Yellow (white stripe)	RS-485 TRXN

Pin	Wire color	Feature
4	Blue (white stripe)	RS-485 TRXP

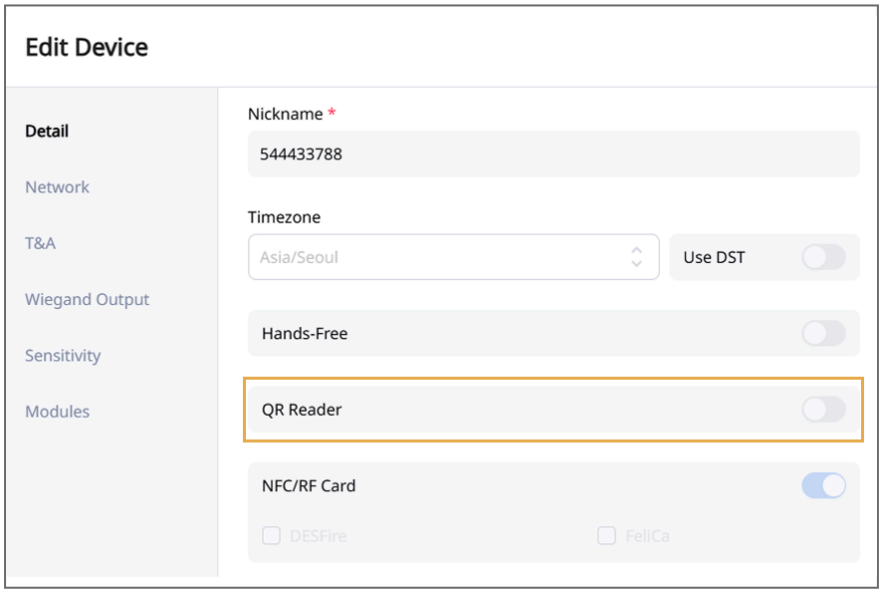
> **Info**
> The wiring direction is the exact opposite of many other connectors. Check the orientation again before wiring.

- Attach the 4-pin connector to the CON port on the bottom of the QR scanner. Because the connector is **polarized** (keyed), it fits only one way.



Step 2: Enable the QR reader

1. Sign in to the BioStar Air portal (web or app).
2. Click **Device Management** → **Registered Devices** in the left sidebar.
3. Click the device that has the connected E200 QR scanner.
4. Enable the **QR Reader** option in the **Detail** section.



5. Click **Save** to save the changes.

> **Info**
> Enabling the QR reader prevents you from using other RS-485 devices (for example, an SIO2) on the same reader.

Step 3: Configure the QR scanner

By default, the **E200 QR scanner** is set to a baud rate of **115,200**. Change the baud rate to **9,600** to use it with Suprema devices.

Connect the QR scanner to the device and **scan the barcode below** to apply the new baud rate.



When the wiring is correct and the Suprema device is connected to the network, use the **dynamic QR credentials** provided through BioStar Air.

Identify Network Ports and Devices

BioStar Air and compatible devices must access specific network ports for seamless connection. Network ports allow secure communication between compatible devices, cloud services, and user applications. Administrators may need to verify a BioStar Air-compatible device's MAC address from its serial number for network configuration tasks.

Required network ports

Verify that the following ports are open on the network firewall.

- **6379**, **6381**: Redis Ports

  Used to synchronize user information, handle fast event logging, manage sessions, and serve as a message broker for signaling between devices and the cloud.

- **5671**: AMQP over TLS (RabbitMQ)

  Provides a secure messaging protocol for real-time communication between services.

- **443**: HTTPS (TLS)

  Used for standard secure web traffic and required for the following services:

  - Access to the management portal web app through a web browser
  - BioStar Air mobile app (iOS/Android)
  - API calls
  - Device firmware updates through the cloud
  - Device login and authentication services

- When using BioStar Air's built-in video management feature:
  - Web-socket domain: eu-wss-api.airfob.com
  - Web-socket Port: 3500
  - TURN/STUN Ports: 80, 443, 3478, 5349

> **Info**
> Verify access to the following endpoints for device login and authentication.
> - https://e-afs-api.airfob.com/v1/device/login (Europe)
> - https://afs-api.airfob.com/v1/device/login (Rest of world)

Check the MAC address from the serial number

In certain cases, administrators need to determine a BioStar Air-compatible reader's MAC address using only its serial number. This is useful for tasks such as adding the device to a whitelist before adding it to the network.

Steps

1. **Find the serial number**:

Locate the 9-digit serial number on the back of the device.

2. **Convert the serial number to hexadecimal**:

   Use a calculator or an online tool to convert the serial number from decimal to hexadecimal.

3. **Extract the last 3 bytes**:

   Take the last six characters from the hexadecimal value. These six characters represent the last 3 bytes.

4. **Build the MAC address**:

   The MAC address always starts with `00:17:FC:`. Append the last 3 bytes (six characters) from the hexadecimal value, separating each pair with a colon.

Example

1. **Serial number**: 546089489
2. **Hexadecimal**: 208CAA11
3. **Last 3 bytes**: 8CAA11
4. **MAC address**: 00:17:FC:8C:AA:11

These steps allow accurate identification of a BioStar Air-compatible reader on the network using its serial number.

MAC address converter

Enter the device's serial number below to get its MAC address instantly.

Credential User

With the Suprema Pass app, you can open doors using just your smartphone. This guide covers the app's key features — from choosing Bluetooth, NFC, or QR code authentication methods and setting up 2-step authentication to adjusting Bluetooth detection sensitivity.

Using Mobile Credentials

Use mobile credentials instead of plastic RFID cards to open doors with the Suprema Pass app. Tag the mobile device via Bluetooth or NFC, touch and hold the card, or scan a QR code to open doors.

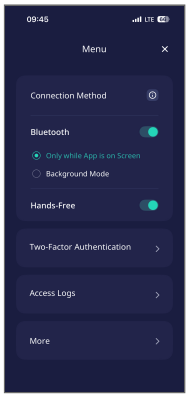
> **Info**
> The Suprema Pass app serves as the user interface for the BioStar Air system and primarily acts as a digital wallet for mobile credentials. Users issue and store mobile access cards in the app to enter secure areas with their mobile devices.

Requirements and preparation

Meet the following requirements to open doors with mobile credentials.

- An access control device compatible with Suprema Pass mobile credentials must be installed.
- Install the Suprema Pass app on the mobile device.
  - iOS
  - Android
- Enable Bluetooth or NFC on the mobile device.
- Enabling two-step authentication disables **Background Mode**.
- The administrator must enable QR authentication in the BioStar Air portal.
- Verify that the site supports the hands-free access method.

> **Info**
> - Location services are required to authenticate with the mobile access card in Suprema Pass. See the related FAQ at Why Am I Being Asked to Enable Location Services?.
> - Follow the provided guidance to troubleshoot the issue if the mobile card authenticates with the device but the door does not open. See the related FAQ at Fix Mobile Card Issues.



Set connection method

Select between two operating modes in the Suprema Pass app. On the Suprema Pass app home screen, tap ☰ in the upper right corner, then select the desired mode in **Connection Method**.

- **Only while App is on Screen**: Open the door only when the app appears on the screen and the mobile card is visible.
- **Background Mode**: Open the door even if the phone is locked when the app is running in the background.

> **Info**
> Regardless of the mode, tag the mobile device on the reader to authenticate.

Open doors

Use the Suprema Pass app to open doors in several ways.

Tag your mobile device to a reader

Bring the mobile device close to a reader compatible with BioStar Air and authenticate via Bluetooth or NFC to open the door.

1. Make sure the Suprema Pass app is running.
2. Hold the Bluetooth or NFC antenna area of the mobile device close to the reader.
3. The door opens when the mobile credential authenticates.

> **Info**
> - Choose between two communication modes. For more information, see Set Up Advanced Features.
>   - **Bluetooth mode**: The mobile device communicates wirelessly with the reader.
>   - **NFC mode**: Available only on Android devices; tag the mobile device on the reader to authenticate.
> - The Bluetooth or NFC antenna location varies by model. Refer to the device specifications for the optimal touch point.

Touch and hold mobile card

Touch and hold the mobile card in the Suprema Pass app to open the door.

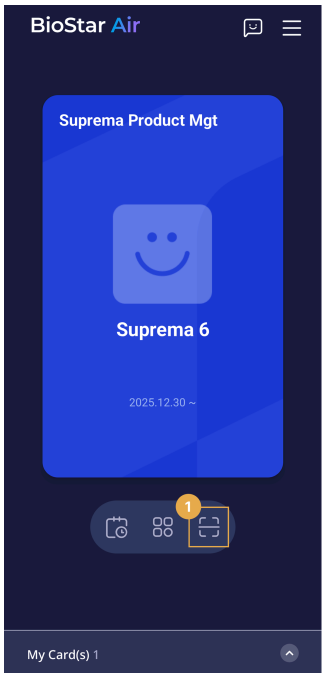
1. Display the home screen of the Suprema Pass app.
2. Touch and hold the mobile card near a reader compatible with BioStar Air for 2–3 seconds.
3. The door opens when the mobile credential authenticates.

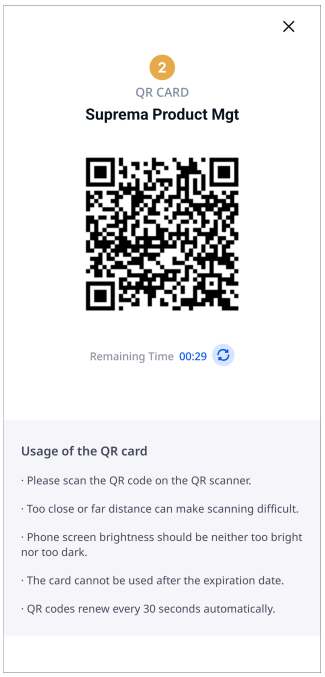
Info

- Select **Background Mode** in **Connection Method** to use this feature. For more information, see Set connection method.
- For security reasons, **the site administrator may disable this feature**.
- **Effective range** varies depending on mobile device Bluetooth strength.
- Nearby access control readers may trigger unintended authentication.

QR authentication

If the administrator enables the **QR Reader** option in the BioStar Air portal, you can open the door by scanning the QR code in the Suprema Pass app with a QR reader. On the home screen of the Suprema Pass app, tap the icon under the mobile card.





Info

- For more information about the **QR Reader** option, see Settings for Additional Features.
- QR authentication is available only at doors equipped with a QR reader.

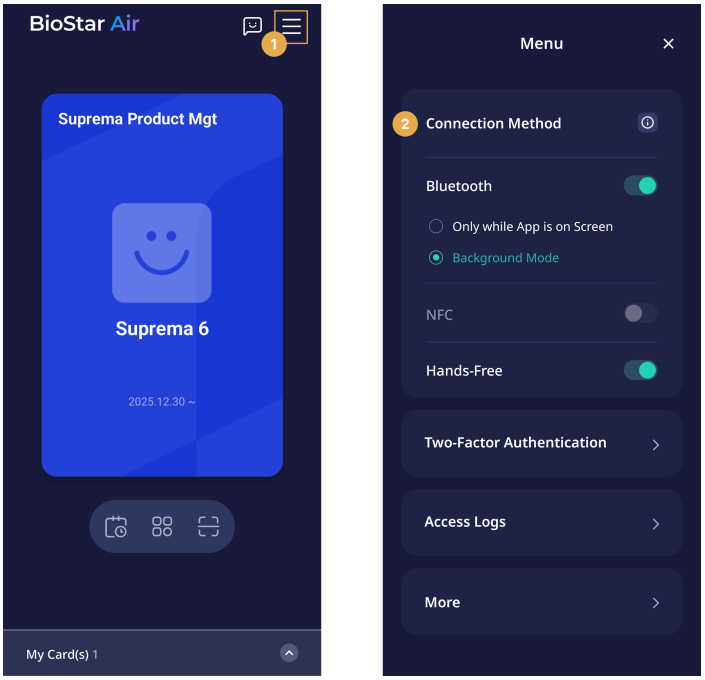
Set Up Advanced Features

The Suprema Pass app includes advanced settings and security options to enhance the user experience and access control features. Users can configure authentication methods, enable two-factor authentication, review access logs, report issues, and use support features.

Configure connection method

Select a preferred connection method to communicate with the access control device. On the Suprema Pass app home

screen, tap ☰ in the upper right corner, then select the desired mode in **Connection Method**.



Bluetooth

Choose between two Bluetooth authentication modes.

- **Only while App is on Screen**: Authenticate with a mobile card only when the app is open on the mobile device. This mode saves battery but requires manually launching the app before approaching the door.
- **Background Mode**: Authenticate with a mobile card even if the device screen is off when the app runs in the background. This mode is more convenient but consumes more battery. If the app closes, relaunch it to resume background functions.

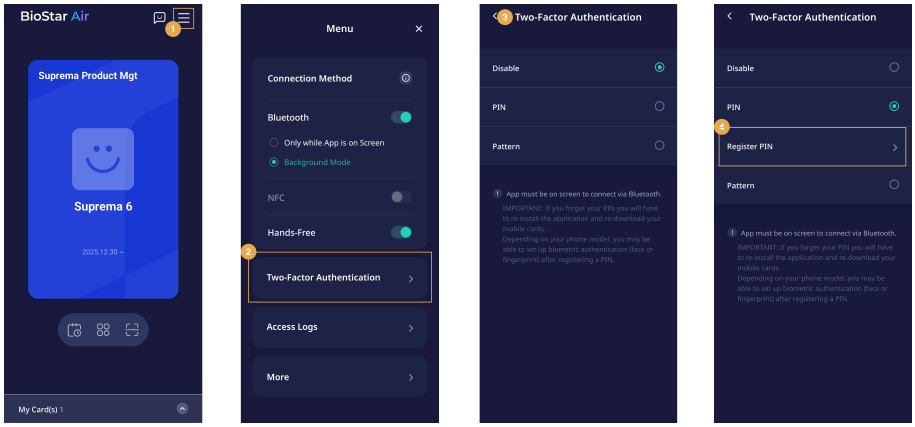
NFC

NFC authentication is available only on Android devices. Use NFC alone or with Bluetooth for faster entry.

> **Info**
> Android users with an NFC-compatible device can use NFC with Bluetooth.

Two-factor authentication (2FA)

Enable two-factor authentication with a **PIN, pattern, or biometric authentication** (face or fingerprint) for additional security.



Info

- This feature is not supported in **Background Mode** connections because the app screen must remain open during access authentication.
- If the PIN or pattern is forgotten, reinstall the app and reactivate the mobile card.
- Supported features may vary depending on the mobile device.

iOS users

1. On the Suprema Pass app home screen, tap ☰ in the upper right corner.
2. Set the connection method to **Only while App is on Screen**.
3. Tap **Two-Factor Authentication**.
4. Tap **Register PIN**.
5. Enter the six-digit PIN.
6. When the success notification appears, tap **OK**.

Info

- Tap **Change PIN**, then enter the new PIN to change the PIN.
- Enable **Biometric Authentication** and follow the setup instructions to use biometrics.

Android users

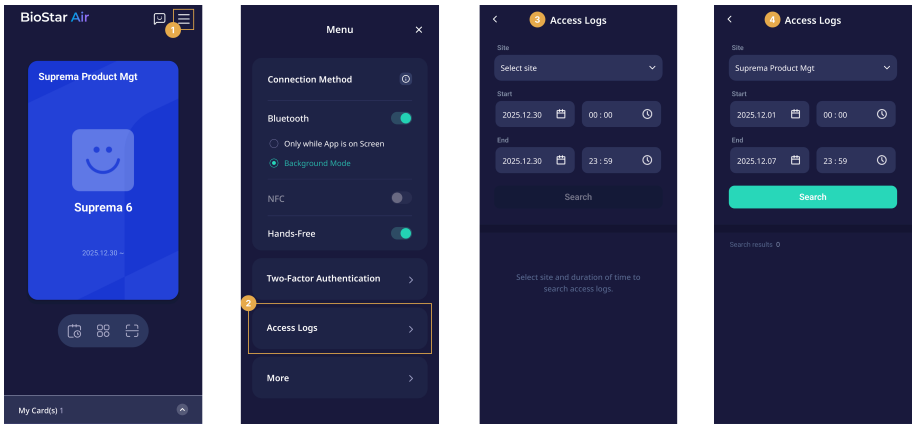
1. On the Suprema Pass app home screen, tap ☰ in the upper right corner.
2. Set the connection method to **Only while App is on Screen** or **NFC**.
3. Tap **Two-Factor Authentication**.
4. Tap **PIN** → **Register PIN** or **Pattern** → **Register Pattern**.
5. Enter the selected PIN or pattern.
6. When the success notification appears, tap **OK**.

Info

- Tap **Change PIN**, then enter the new PIN to change the PIN.
- Tap **Change Pattern**, then enter the new pattern to change the pattern.
- Enable **Biometric Authentication** and follow the setup instructions to use biometrics.

Access logs

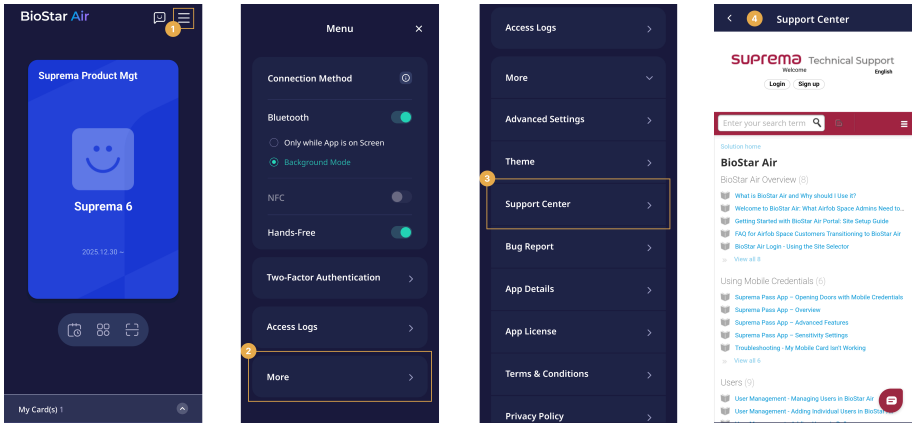
Use access records to track entry attempts and troubleshoot entry-related issues.



1. On the Suprema Pass app home screen, tap ☰ in the upper right corner.
2. Tap **Access Logs**.
3. Select a site, then set the start and end dates.
4. Tap **Search**.

Support center

Go to **Support Center** for additional support.



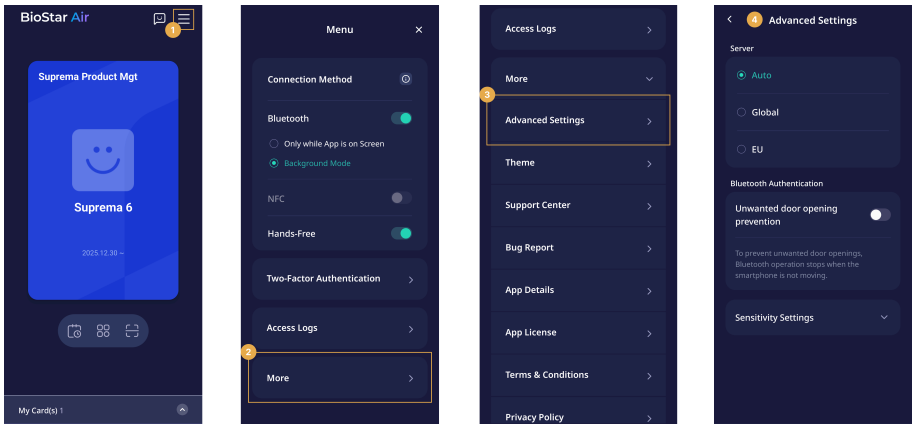
1. On the Suprema Pass app home screen, tap ☰ in the upper right corner.
2. Tap **More**.
3. Tap **Support Center**.

4. Go to the **Suprema Technical Support** page.

> - Search questions or review FAQs.
> - If support is needed, tap the chat icon in the lower right corner to submit a ticket to the MOCA Systems team.

Advanced Settings

Tap ☰ in the upper right corner on the Suprema Pass app home screen, then select **More** → **Advanced Settings** to use the following additional features.



- **Location setting**: Select **Global** or **EU** server based on your location. Select **Auto** to have the app detect your location and choose the appropriate server.
- **Bluetooth Authentication**: Enable **Unwanted door opening prevention** to block Bluetooth authentication when the mobile device is stationary.
- **Sensitivity Settings**: Adjust the Bluetooth sensitivity between the mobile device and the reader compatible with BioStar Air. For more information, see Set Bluetooth Sensitivity.

Additional features

Tap ☰ in the upper right corner on the Suprema Pass app home screen, then select **More** to use the following additional features.

- **Theme**: Set the app's color mode. Select **Light**, **Dark**, or **System** mode.
- **Bug Report**: Write detailed information, such as the error occurrence context and reproduction steps, to submit the bug report to the developer.
- **App Details**: Check the model name, OS version, BLE support and status of the mobile device.
- **App License**: View the open-source license information used in the Suprema Pass app.
- **Terms & Conditions**: View the terms of use for the BioStar Air platform.

Set Bluetooth Sensitivity

With the **Sensitivity Settings** feature, adjust the Bluetooth sensitivity between the mobile device and the reader compatible with BioStar Air. This feature helps ensure smooth authentication and reduces unauthorized access attempts and

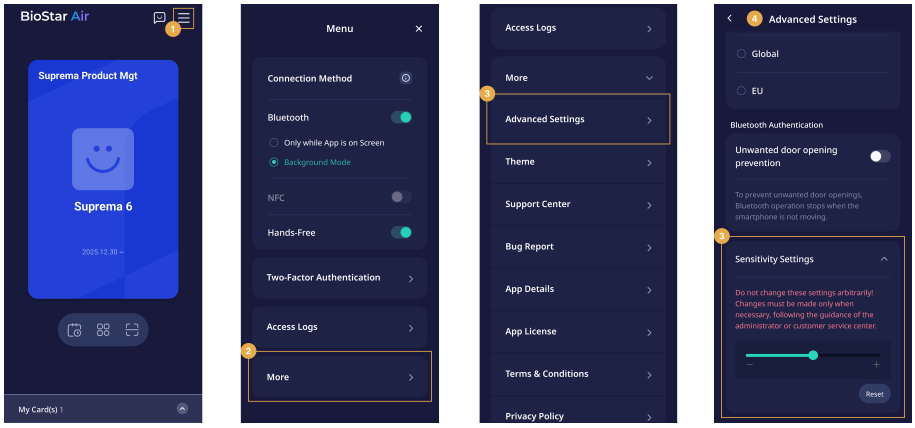
authentication failures.

Info

Because Bluetooth signal strength varies by mobile device model, users may experience different detection ranges. Environmental factors such as walls, interference, or the placement of readers compatible with BioStar Air can also affect Bluetooth detection.

Adjust the sensitivity setting

Users can fine-tune Bluetooth authentication sensitivity based on the mobile device's Bluetooth strength and personal preference.



1. On the Suprema Pass app home screen, tap ☰ in the upper right corner.
2. Tap **More**.
3. Tap **Advanced Settings**.
4. Tap **Sensitivity Settings**, then move the slider to adjust sensitivity.

Info

- Move the slider toward − to lower the sensitivity and block unintended authentication.

  > *For example, when the mobile device is on a desk*

- If authentication fails, move the slider toward + to increase the sensitivity. However, the mobile device must be very close to a reader that is compatible with BioStar Air.

Tip

iOS user tips

If you bring an iPhone with Apple Pay close to a reader compatible with BioStar Air, Apple Pay will launch. This occurs because the mobile device's NFC area is detected along with mobile card authentication.

Solution: Adjust the sensitivity setting toward + so that a reader compatible with BioStar Air detects the mobile device's Bluetooth signal earlier, eliminating the need for physical contact with the device. This allows smooth access while blocking Apple Pay from being triggered.

Developer

BioStar Air provides a cloud-based RESTful API. You can use the API to integrate with external systems, automate the user lifecycle, and manage credentials. Set up a demo environment and understand the authentication flow, then implement integration with the user management API.

Quick Start

This guide shows how to set up the BioStar Air demo site, connect and register compatible devices, and test cloud API integration. If you have worked with BioStar 2 before, many concepts will feel familiar. BioStar Air is fully cloud-based.

Prerequisites

Before you start, check the following.

- Prepare a **BioStar Air-compatible device** with factory-initialized firmware.
  - XP2-AIR, XS2-AIR, BEW3-AIR, BS3-AIR, BLN2-AIR
  - Devices can be purchased through authorized Suprema distributors.
- The device must be connected to the internet via Ethernet.
- Allow outbound access on the network.
  - Port 443 (HTTPS)
  - Port 5671 (MQTT over TLS)

Set up the demo environment and API key

1 Sign up and log in

1. Go to BioStar Air Developer.
2. Click **Sign Up**, complete the form, and wait for approval.
3. After approval, log in using your Developer Portal user email address and password.

> **Info**
> The email address and password used for the Developer Portal cannot be used on the Demo Portal.

2 Create a demo application

1. Go to **API** → **Management**.

2. Click **+ Register**.
3. Select **Demo** as the application type.
4. Enter an application name and click **Register**.
5. After registering the demo application, you can download the *site_info.csv* file.

> **Info**
>
> - The *site_info.csv* file contains the alias email and password.
> - When logging in to the demo portal, be sure to use this alias email and password.
> - **Do not use the email and password for the Developer Portal on the demo portal.**

3 Generate an API key

1. Go to **API → Management**.
2. Click the application you registered.
3. Scroll to **API Management**.
4. Click **Add**.
5. Enter a name and confirm.
6. Copy the generated API key and store it securely.

This API key is used to authenticate API calls to the demo environment.

4 Log in to the demo portal

1. Click **Demo Portal** in the Developer Portal menu or go directly to https://demo.airfobspace.com/login.
2. Log in with the alias email and password from the *site_info.csv* file.

> **Info**
>
> **Do not use the email and password for the Developer Portal on the demo portal.**

Register devices

Use the BioStar Air Demo App (Android only) on your mobile device.

1. Go to the BioStar Air Developers link and download the demo app.
2. Launch the demo app and log in with the alias email and password from the *site_info.csv* file.
3. Move your Android device near the reader (within BLE range).

- In **All Menu** → **Devices**, tap the + button in the upper right.
- Search for the device and tap **Register**.

4. The device beeps, reboots, and appears in the registered device list.

> **Info**
> Devices can only be registered through the mobile app. You cannot register devices from the web portal. API-based registration requires an encryption certificate that is not provided to partners.

Device Management

Manage devices from the demo app or the demo web portal.

- **BioStar Air Demo App**
- **Demo Web Portal:** https://demo.airfobspace.com/login

Demo vs Production

- A **Demo** site for testing is created through the Developer Portal.
- A **Production** site is created through the Partner Portal and requires a site ID, user email, and password. Only authorized resellers or Suprema branches can create a production site.

> **Info**
> - User IDs and account IDs are different. Do not confuse them.
> - If you manage multiple sites, store passwords securely.
> - Always use the latest Bearer token.
> - A Bearer token copied from the browser can be reused in Postman.

Need help?

Open a ticket in the Suprema Technical Support Portal. https://support.supremainc.com

API Authentication

The BioStar Air Cloud API uses Bearer token (JWT)-based authentication. You must obtain a token through the login process before calling the API, and include it in the Authorization header of every request.

API Base URLs

Environment	Base URL	Description
Demo (TEST)	https://sp-demo-api.airfob.com/v1	When the application type is registered as a "Demo", you can download the demo environment site and site master account information as a csv file.
Production (LIVE)	https://sp-api.airfob.com/v1	(**Auto-Routing**) Automatically selects the global or EU server based on the client region.
	https://sp-a-api.airfob.com/v1	(**Global Dedicated**) Connects to the global server environment.
	https://sp-e-api.airfob.com/v1	(**EU Dedicated**) Connects to the EU(Europe) server environment.

> **Auto-Routing** environment may result in unexpected routing based on region detection.

API login flow

Make API calls with Postman or programmatically.

Log in

- **Endpoint:** `login`
- **Payload:**

```
{
  "username": "your_email",
  "password": "your_password"
}
```

Returns a Bearer token (JWT).

Get account information

- **Endpoint:** `getSelfAccounts`
- **Authorization:** Bearer Token

Returns a list of accessible sites and accounts.

Log in to an account

- **Endpoint:** `loginAccount`
- **Authorization:** Bearer Token

Returns a site-specific token.

How to get a Bearer token from a web browser

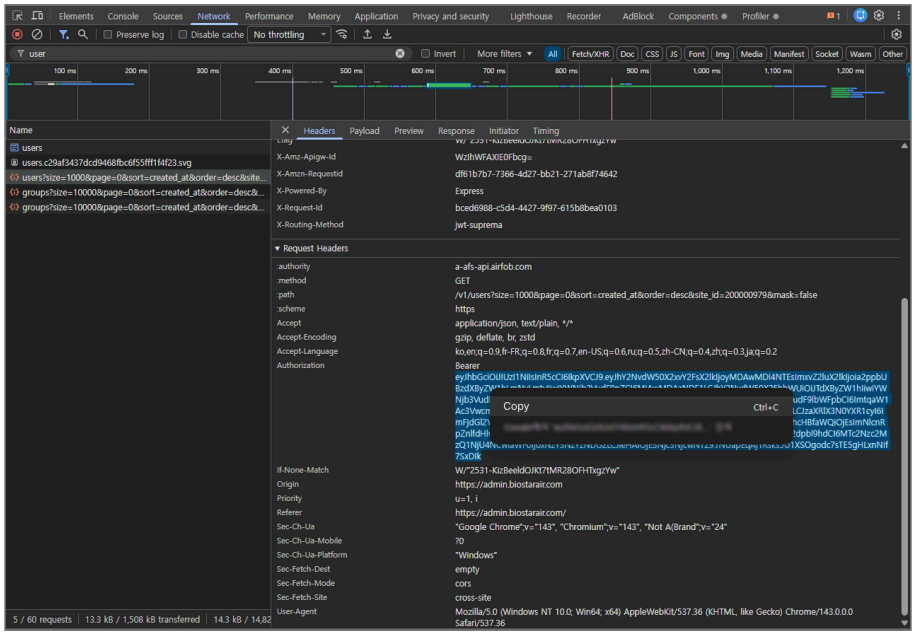
You can obtain the Bearer token directly from your browser using the developer tools, without Postman.

Chrome/Edge (Windows or Mac)

1. In the web browser, press `F12` or `Ctrl/Cmd + Shift + I`.
2. Go to the **Network** tab.
3. Refresh the page.
4. Search for API calls.

   > *e.g.,* `groups`, `login`

5. Click the request in the list.
6. Go to the **Headers** tab.
7. In the request headers, find `Authorization: Bearer ...`.
8. Right-click the token and copy it.



Safari (Mac)

1. Enable the **Developer** menu. In Safari, go to Preferences → Advanced and check **Show Develop menu**.
2. Go to **Develop** → **Show Web Inspector**.

3. Go to the **Network** tab.
4. Refresh the page.
5. Filter and inspect API calls.
6. Copy the `Authorization: Bearer` token from the request headers.

> **Info**
> A Bearer token copied from the browser can be reused in Postman. Always use the latest Bearer token.

Using the User Management API

After obtaining an authentication token, you can manage the user lifecycle through the API. Use endpoints to retrieve, create, update, and deactivate users to automate user management on your BioStar Air site.

Recommended API integration scope

Limit your API integration to the scope below whenever possible.

- User lifecycle management (create/update/delete)
- Credential management (mobile, RF card, biometric)

Allow administrators to continue using the existing BioStar Air web and mobile management apps.

- Access Level
- Schedules
- Door and device settings
- Site settings

User management API calls

After logging in, use the following endpoints to manage users.

- `getUsers`
- `createUser`
- `updateUser`
- `suspendUsers`

Always include a Bearer token in the Authorization header.

> To activate a user, assign at least one credential type.
>
> > *e.g., RF card, mobile, LinkPass*

Sample application

The following sample code is a Python app that uploads a CSV file via the API and bulk deactivates users.

Python

```
import requests
import csv
import getpass
from pathlib import Path

def select_server():
    servers = {
        "1": ("Demo", "https://demo-afs-api.airfob.com/v1"),
        "2": ("Global", "https://a-afs-api.airfob.com/v1"),
        "3": ("EU", "https://e-afs-api.airfob.com/v1")
    }

    print("Please select a server:")
    for key, (name, _) in servers.items():
        print(f"{key}: {name}")

    choice = input("Enter server number: ").strip()
    return servers.get(choice, (None, None))[1]

def login(base_url, username, password):
    url = f"{base_url}/login"
    payload = {"username": username, "password": password}
    response = requests.post(url, json=payload)
    response.raise_for_status()
    data = response.json()
    token = data.get("access_token")
    if not token:
        raise ValueError("Login succeeded but no access_token returned.")
    print("✅ Login successful.")
    return token

def login_to_account(base_url, token, account_id):
    url = f"{base_url}/login/{account_id}"
    headers = {"Authorization": f"Bearer {token}"}
    response = requests.post(url, headers=headers)
    response.raise_for_status()
    new_token = response.json().get("access_token")
    if new_token:
        print(f"✅ Switched to account ID: {account_id}")
        return new_token
    return token

def get_accounts(base_url, token):
    url = f"{base_url}/accounts/self"
    headers = {"Authorization": f"Bearer {token}"}
    response = requests.get(url, headers=headers)
    response.raise_for_status()
    accounts = response.json().get("accounts", [])
    return [{"id": acc["id"], "name": acc["site"]["name"]} for acc in accounts]

def suspend_users_from_csv(base_url, csv_path, token):
    if not Path(csv_path).exists():
        print(f"❌ File not found: {csv_path}")
        return

    headers = {"Authorization": f"Bearer {token}"}
```

```
    with open(csv_path, newline='', encoding='utf-8-sig') as f:
        reader = csv.DictReader(f)

        # Normalize headers
        reader.fieldnames = [field.strip().lower() for field in reader.fieldnames]
        if 'email' not in reader.fieldnames:
            print("❌ Missing required 'email' column in CSV.")
            return

        for row in reader:
            email = row.get("email")
            if not email:
                print("⚠️ Skipping row with missing email.")
                continue

            # Search user
            search_url = f"{base_url}/users/search"
            payload = {"filters": [{"field": "email", "equals": email}]}
            search_resp = requests.post(search_url, headers=headers, json=payload)
            if search_resp.status_code != 200:
                print(f"❌ Failed to search user {email}: {search_resp.text}")
                continue

            users = search_resp.json().get("users", [])
            if not users:
                print(f"❌ No user found with email: {email}")
                continue

            user_id = users[0]["id"]

            # Suspend user
            suspend_url = f"{base_url}/users/suspend"
            suspend_payload = {
                "ids": [user_id],
                "certify_by": "none",
                "use_site_template": True
            }
            suspend_resp = requests.post(suspend_url, headers=headers, json=suspend_payload)
            if suspend_resp.status_code == 200:
                print(f"✅ Suspended user: {email}")
            else:
                print(f"❌ Failed to suspend user {email}: {suspend_resp.text}")

def main():
    base_url = select_server()
    if not base_url:
        print("❌ Invalid selection. Exiting.")
        return

    print("\n🔑 BioStar Air Login")
    username = input("Email: ")
    password = getpass.getpass("Password: ")

    token = login(base_url, username, password)
    accounts = get_accounts(base_url, token)

    print("\n🌐 Available Sites:")
```

```
    for i, acc in enumerate(accounts):
        print(f"{i}: {acc['name']} (ID: {acc['id']})")

    selected = int(input("\nSelect site number to log into: "))
    account_id = accounts[selected]["id"]
    token = login_to_account(base_url, token, account_id)

    csv_path = input("Enter path to CSV file with user emails: ").strip()
    suspend_users_from_csv(base_url, csv_path, token)

if __name__ == "__main__":
    main()
```

Troubleshooting

Have you encountered an unexpected problem while using BioStar Air? This document identifies common issues you may encounter when using BioStar Air and explains how to resolve them.

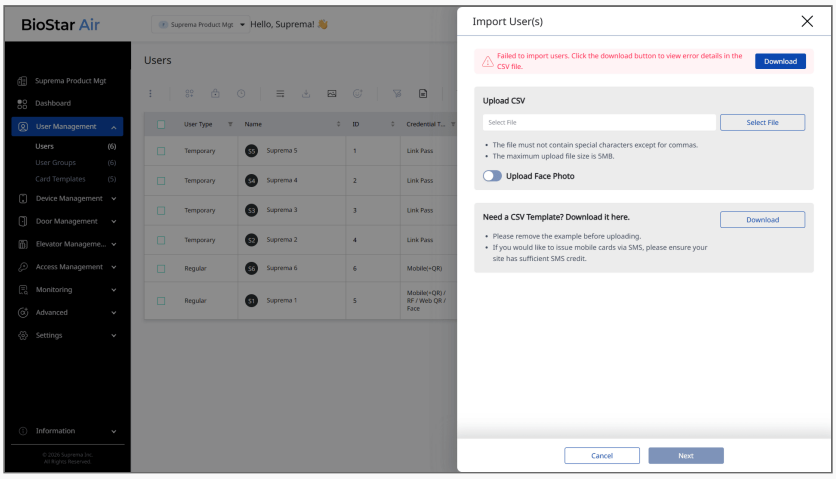
Select a problem below to view step-by-step solutions.

Fix Bulk User Addition Issues

Several customers and partners have reported issues when adding user lists in bulk. Most issues arise from incorrectly formatted CSV files. Follow the instructions below exactly to ensure the bulk addition feature works as expected.

Info

Starting with v2.10, BioStar Air returns a validation report when a CSV file containing invalid entries is uploaded. Correct the errors, and then upload the file again.



Prepare the CSV file

Download the CSV template

1. Go to **User Management** → **Users** in the left sidebar.
2. Click **Add User** → **Import User(s)** at the top right of the screen.
3. When the **Import User(s)** panel appears, click **Download**.
4. Save the CSV template file (*biostar-import-user-csv-example.csv*) locally.

Use the exact CSV template format

- **Do not manually add or delete columns**. An unexpected column can cause an error.
- If you need to include additional fields (for example, employee ID or department), use the **User Template**( ) feature

at the top of the user list to add them. When a field is added, the downloaded CSV file automatically includes the corresponding column.

Enter data correctly by referring to the requirements of each column.

User Key

- A unique numeric ID for each user.
- The **User Key** column **can be left blank**, and the system assigns a value automatically.
- If you enter user IDs manually
  - Use **numbers only**.
  - Use a **unique value**.
  - Do not include letters, spaces, hyphens, or special characters.

> **Caution**
> If you need to use a company-specific employee ID that includes letters, do not use the **User Key** field. Instead, create a custom user field with the **User Template** feature.

Email

- Use a valid email format. Refer to the validation formulas to verify the email format.
  - No spaces are allowed.
  - It must include the at sign (`@`).
  - The domain must include a period (`.`) and a top-level domain.

    > *Example: example.com, gmail.com, suprema.co.kr*
  - There must be no additional period after the address.
  - No special or hidden characters are allowed.
  - It must be an email address. Errors such as 'Not provided' may occur.
- The email address **must be unique**. Duplicates are not allowed within the file or among existing users.
- An email address is required when issuing the credentials below.
  - **Mobile Card**
  - **Web QR**
  - **Link Pass**
- Users with only an RFID card do not need to enter an email address.

Mobile

- Providing a phone number is optional when the credential is not delivered via mobile SMS.
- Like the email address, it **must be unique**, and duplicates are not allowed within the file or among existing users.

- Use email to deliver credentials when possible. SMS messages incur additional charges.

Dates (**Start Date** / **End Date**)

All date fields must follow the exact format shown below.

```
YYYY-MM-DDTHH:MM:SS.sssZ

Example:
1995-05-09T00:00:00.000Z
```

Even minor differences—such as omitting the 'Z', using slashes (`/`) instead of dashes (`—`), or leaving out the time—can cause the upload to fail.

Credential requirements

Credential type	Email or phone number
RF Card Only	No.
Mobile Card / **Web QR** / **Link Pass**	Yes, one is required.

- Credentials must be delivered by email address or phone number.
- Both can be provided, but **mobile credentials require at least one**.
- Email is free. SMS is charged.

Excel formulas for pre-validation

Before uploading data, use the following formulas in **helper columns** to verify the data.

Duplicate email or phone number validation

Detect Duplicate Emails or Phone Numbers

```
=IF(E2="", "", IF(COUNTIF(E$2:E2, E2)>1, "Duplicate", "First Occurrence"))
```

Date format validation

Validate ISO 8601 Date Format (Column Q)

```
=IF(Q2="", "", IF(AND(LEN(Q2)=24,
  ISNUMBER(VALUE(MID(Q2,1,4))), MID(Q2,5,1)="-",
  ISNUMBER(VALUE(MID(Q2,6,2))), MID(Q2,8,1)="-",
  ISNUMBER(VALUE(MID(Q2,9,2))), MID(Q2,11,1)="T",
  ISNUMBER(VALUE(MID(Q2,12,2))), MID(Q2,14,1)=":",
  ISNUMBER(VALUE(MID(Q2,15,2))), MID(Q2,17,1)=":",
  ISNUMBER(VALUE(MID(Q2,18,2))), MID(Q2,20,1)=".",
  ISNUMBER(VALUE(MID(Q2,21,3))), RIGHT(Q2,1)="Z"),
  "Valid", "Invalid"))
```

Email format validation

Validate Email Format (Column E)

```
=IF(TRIM(E2)="", "", IF(AND(
  ISNUMBER(FIND("@", E2)),
  ISNUMBER(FIND(".", E2)),
  FIND("@", E2) > 1,
  FIND(".", E2, FIND("@", E2)) > FIND("@", E2) + 1,
  LEN(E2) - LEN(SUBSTITUTE(E2, "@", "")) = 1,
  ISERROR(FIND(" ", E2))
), "Valid", "Invalid"))
```

Encountering errors?

- Did you download the correct template and not add additional columns?
- Are all required fields completed for users receiving a mobile credential?
- Are the email address and phone number unique between the file and existing users?
- Are the date and email formats correct as specified above?

Info

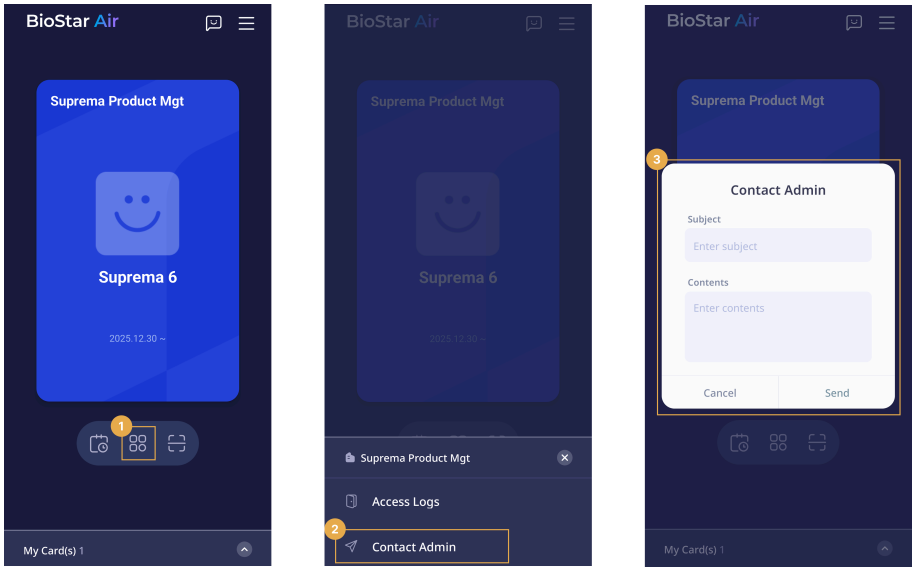
- The service team does not provide file-editing services. If the file fails to upload, use the validation tools above to identify and resolve the issue.
- This document is designed to enable successful uploads without manual troubleshooting by the service team.

Fix Mobile Card Issues

If the mobile card authenticates with the device but the door does not open, follow these steps to resolve the issue.

Contact your BioStar Air administrator

The site administrator can help with mobile card reissuance, temporary mobile device issues, and setting issues.



1. In the Suprema Pass app on your mobile device, tap the icon below the mobile card.
2. When the bottom panel appears, tap **Contact Admin**.
3. When the pop-up window appears, enter a title and message.
4. Tap **Send** to send a message to the administrator.

Was the mobile card deleted?

If you changed your mobile device or reinstalled the Suprema Pass app, all mobile cards were deleted for security reasons. Contact the following for mobile card reissuance.

- **Company Spaces**: HR, IT, security, or operations team
- **Shared Spaces**: regional administrator or customer service team

> **Info**
> When an administrator reissues a user's credentials in BioStar Air, previously issued mobile credentials, QR codes, and LinkPasses are revoked and replaced. The user will receive an email or SMS, depending on site settings, containing a link to the updated credentials. The user must follow the link to download the new mobile credential into the Suprema Pass app or access the new QR code or LinkPass. Access attempts using revoked mobile credentials, QR codes, or LinkPasses will fail.

Step-by-step troubleshooting guide

1 Did an error message appear in the Suprema Pass app?

- If the door does not open, try authenticating again in the Suprema Pass app.
- If an error message appears, capture a screenshot and share it with your site administrator.

2 Is Bluetooth enabled on your mobile device?

The mobile card relies on Bluetooth communication between the mobile device and the access controller.

- Make sure Bluetooth is enabled.
- Turn Bluetooth off and back on.
- Restart the mobile device if necessary.

3 Allow location permission for the Suprema Pass app

Bluetooth and NFC authentication require location permission.

1. Go to **Settings** → **Apps** on the mobile device.
2. Select the **Suprema Pass** app.
3. Under **Permissions** → **Location**, set location access to **Allow all the time** or **Allow only while using the app**.

4 Check cellular network and Wi-Fi connections

A stable cellular network or Wi-Fi connection is required for mobile card authentication.

5 Are you using the selected connection method?

Check the connection method in the Suprema Pass app.

- On the Suprema Pass app home screen, tap ☰ in the upper right corner.
- Check authentication mode in **Connection Method**.
- Keep the app open in the background when using **Background Mode**.

6 Did the mobile device vibrate during authentication?

- If the mobile device vibrated but the door did not open, open the Suprema Pass app and try authenticating again.
- If an error message appears, capture a screenshot and share it with your site administrator.

Why Am I Being Asked to Enable Location Services?

Location services are required to authenticate with the mobile access card in Suprema Pass. This ensures secure Bluetooth communication between the mobile device and the access control device.

Q. Do I need to switch from Airfob Space to BioStar Air?

No. If you are an existing Airfob Space customer, you can continue using the platform as-is. There is no forced

migration at this time.

Q. Will my devices or data be affected?

No. Both platforms share the same backend. Devices, user data, and configurations remain fully compatible across both services.

Q. Should I start using Suprema Pass instead of the Airfob Space app?

There is no need to migrate existing mobile credential users over to BioStar Air. If you use the app.airfobspace.com URL or Airfob Pro app to manage users and issue mobile credentials, those users will receive an invitation that points to the Airfob Space app. If you use admin.biostarair.com or the BioStar Air app to manage users and issue mobile credentials, those users will receive an invitation that points to the Suprema Pass app.

Q. Will support or billing change?

No immediate changes will occur in your support or billing processes. Over time, however, BioStar Air will become the primary brand used for documentation, support, and feature announcements.

Q. Can I switch to BioStar Air if I want to?

Yes. Since the backend is shared, transitioning is simple, but some branding and feature availability differences may apply. Simply start using admin.biostarair.com and the BioStar Air app to manage your site. Existing administrator login credentials from app.airfobspace.com will work seamlessly.

Q. What are the benefits of BioStar Air?

BioStar Air is the future-facing brand. It will receive ongoing enhancements, such as improved integrations, UI/UX updates, and new features that may not be backported to Airfob Space.

Q. Will future features work with Airfob Space?

Some will, but not all. New features may be exclusive to BioStar Air going forward. For the best experience and support, new deployments should use BioStar Air.

Troubleshoot Video Playback Issues

Follow these steps to diagnose and resolve the issue when recorded video does not play after you register a camera in BioStar Air. These steps resolve video playback issues and ensure proper operation in BioStar Air.

Info

For more information on camera registration, refer to IP Camera Support and Setup.

Q. Do I need to switch from Airfob Space to BioStar Air?

No. If you are an existing Airfob Space customer, you can continue using the platform as-is. There is no forced migration at this time.

Q. Will my devices or data be affected?

No. Both platforms share the same backend. Devices, user data, and configurations remain fully compatible across both services.

Q. Should I start using Suprema Pass instead of the Airfob Space app?

There is no need to migrate existing mobile credential users over to BioStar Air. If you use the app.airfobspace.com URL or Airfob Pro app to manage users and issue mobile credentials, those users will receive an invitation that points to the Airfob Space app. If you use admin.biostarair.com or the BioStar Air app to manage users and issue mobile credentials, those users will receive an invitation that points to the Suprema Pass app.

Q. Will support or billing change?

No immediate changes will occur in your support or billing processes. Over time, however, BioStar Air will become the primary brand used for documentation, support, and feature announcements.

Q. Can I switch to BioStar Air if I want to?

Yes. Since the backend is shared, transitioning is simple, but some branding and feature availability differences may apply. Simply start using admin.biostarair.com and the BioStar Air app to manage your site. Existing administrator login credentials from app.airfobspace.com will work seamlessly.

Q. What are the benefits of BioStar Air?

BioStar Air is the future-facing brand. It will receive ongoing enhancements, such as improved integrations, UI/UX updates, and new features that may not be backported to Airfob Space.

Q. Will future features work with Airfob Space?

Some will, but not all. New features may be exclusive to BioStar Air going forward. For the best experience and support, new deployments should use BioStar Air.

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.