BioStar X

Administrator Guide

Version 1.0.0

English

EN 102.00.BSX

suprema
SECURITY & BIOMETRICS

BioStar X

Welcome to the BioStar X User Guide

BioStar X is Suprema's next-generation integrated security platform that combines AI-based access control with intelligent video analytics. An innovative platform that can effectively integrate and manage overall security operations beyond simple access control. **BioStar X**, the culmination of AI-based access control and intelligent video analysis, is designed to utilize AI technology to perform real-time access management, video monitoring, and abnormal behavior detection all on a single platform. In addition to access control, it is equipped with various AI-based video analysis features such as intrusion detection, loitering detection, and fall detection, allowing for proactive responses.

This document provides various features and configuration methods of **BioStar X**. We provide extensive and diverse guidance to help you make the most out of all the features of **BioStar X**. Follow the step-by-step guide to easily and quickly implement **BioStar X**.

Overview → 2 items

This guide provides an overview of the key features of BioStar X, essential considerations before implementation, and the applicability across various environments. Understand the key technologies and advantages of BioStar X, such as AI-based access control, intelligent video analytics, and integrated security management, and review in advance whether implementation is optimized for your security infrastructure.

- Before Start
- System Minimum Requirements

↳ 2 items

Getting Started → 8 items

This is a collection of guide documents that walk you through the basic procedures required for the installation, upgrade, and initial setup of BioStar X step by step.

- Check Network Priority
- Express Installation
- Custom Installation

↳ 8 items

Server Management → 5 items

This document guides you on how to manage the services of the BioStar X server, change ports, and modify the database using the BioStar X Service Manager.

- Start and Stop Server
- Service Settings
- Change the Port

↳ 5 items

Launcher → Read more

This guide describes the user interface of the launcher page.

User → 13 items

This guide covers the features available on the User page, one of BioStar X's core features.

- Manage User Groups
- Register Users
- Enter Basic User Information

↳ 13 items

Monitoring → 5 items

This guide covers the features available on the Monitoring page, one of BioStar X's core features.

- Monitoring Doors
- Monitor Map
- Monitor Device

↳ 5 items

Data → 3 items

You can query user information or events that meet specific criteria, and generate reports on a regular schedule.

- Generate Report
- Automatic Report Schedule
- Settings

↳ 3 items

Dashboard → 3 items

The dashboard can be customized to suit individual preferences by allowing each user to select the information they want, add widgets, and freely configure and arrange the widgets.

- Add Widgets
- Edit Widget
- Delete Widget

↳ 3 items

Settings → 20 items

This guides you through various features that can be configured on the settings page of BioStar X.

- Manage Devices
- Device Settings
- Image Log Settings

↳ 20 items

Advanced Settings → 8 items

Guide for advanced settings feature available when activating a license of Advanced or higher.

- Managing Elevators
- Advanced Access Control Settings
- Video Settings

↳ 8 items

Plugins → 2 items

BioStar X plugins enhance the BioStar X platform with additional features to meet specific customer requirements or integrate with existing systems.

- How to Use Time & Attendance
- Manage Visitors

↳ 2 items

Explore UI → 5 items

Explore the UI of each page of BioStar X and guide on how to use it.

- Learn Common UI
- User
- Monitoring

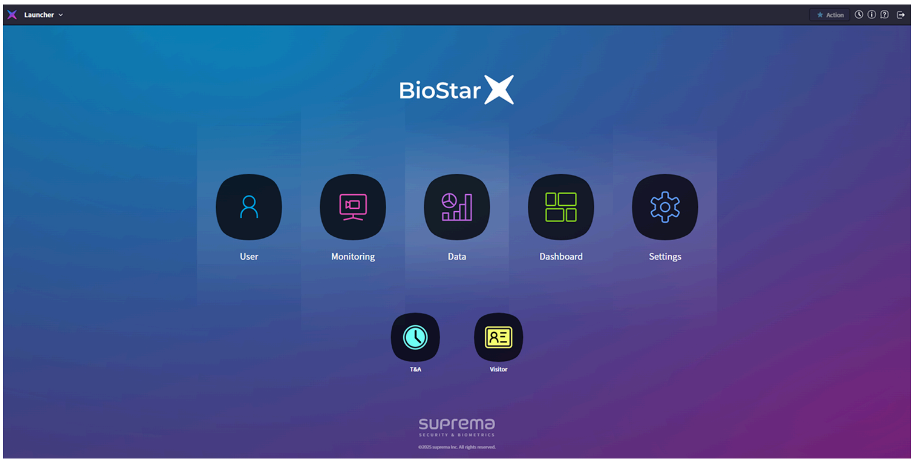
↳ 5 items

License Policy → Read more

This guide provides detailed information about the licensing policy of BioStar X, which is designed with a modular structure.

Overview

BioStar X is Suprema's next-generation integrated security platform that combines AI-based access control with intelligent video analytics. An innovative platform that can effectively integrate and manage overall security operations beyond simple access control.



BioStar X, the culmination of AI-based access control and intelligent video analysis, is designed to utilize AI technology to perform real-time access management, video monitoring, and abnormal behavior detection all on a single platform. In addition to access control, it is equipped with various AI-based video analysis features such as intrusion detection, loitering detection, and fall detection, allowing for proactive responses.

In addition, it supports more sophisticated security monitoring in large facilities through people counting, tailgating detection, blacklist detection, and missing person search functionalities. This functionality can be effectively utilized not only in multi-use facilities such as schools, shopping malls, airports, and hospitals but also in smart buildings.

Enhanced operational efficiency and security

BioStar X supports the integrated management of all security elements in real-time from a single platform. This allows security personnel to efficiently monitor and control individual systems from a single interface without the need to manage them separately.

Additionally, the integrated operating method optimizes security monitoring personnel and reduces costs and time spent on maintenance. Without the need to add a separate individual security system, leveraging the flexible scalability of **BioStar X** allows you to easily add the required functionalities, thereby creating a safer and more efficient security environment.

Provides strong scalability and stability

In enterprise environments such as large corporations or public institutions, the scalability and stability of security systems are essential. **BioStar X** supports the registration of tens of thousands of users and enables stable operation even when connecting various devices.

Additionally, it supports intuitive management of complex security operations by providing a customized UI·UX for users. You can directly configure the interface layout of the monitoring screen, allowing you to quickly and effectively check the information you need.

Essential security solution BioStar X

With the increasing variety of security threats and the growing complexity of security operations, **BioStar X**, which combines AI with integrated security technology, is establishing itself as an essential security solution. If your organization requires both strong security and efficient operations, **BioStar X** is the optimal choice.

Before Start

> **TIP**
>
> This guide provides important information you should know before starting **BioStar X**. **BioStar X** supports 64-bit operating systems. Check the system requirements of the PC where you want to install **BioStar X**, then install it.

Pre-installation Notes

Before installing **BioStar X**, check the following and proceed with the installation.

- **BioStar X** can only be installed on a 64bit operating system.
- If you are using MS SQL 2012 Express, refer to the following link to install the Service Pack 3.
- If you are using MS SQL 2014 Express, refer to the following link to install Service Pack 2.
- If you are using MS SQL Server, set the `Collation` option of the server and each table to CI (Case-insensitive).
- When backing up a database from an older version of **BioStar X**, disable all services before proceeding. Furthermore, if you do not back up and restore the AC database and the TA database together, you will not be able to use the TA database.
- If you want to back up the database of **BioStar X**, be sure to also back up the *enckey* in the *\Program Files\BioStar X\util* folder and the *system.conf* and *setting.conf* file in the *\Program Files\BioStar X* folder. Otherwise, the database will be unavailable.
- Refer to the following for the default port used by **BioStar X**. If another program occupies the same port, **BioStar X** may not work properly.

Check the database

If you are using a user-configured database, check the items below before installing **BioStar X**.

MariaDB

1. Please change the options below under the `[mysql]` section in the *my.cnf* file.

   my.cnf

   ```
   character-set-server=utf8
   collation-server=utf8_unicode_ci
   max_connections = 600
   ```

2. Please add the options below under the `[mysql]` section in the *my.cnf* file.

   my.cnf

   ```
   log_bin_trust_function_creators = 1
   group_concat_max_len = 102400
   ```

3. Connect to MariaDB with root privileges and execute the command below.

   SQL

   ```
   GRANT SUPER ON . TO user_id@'localhost' IDENTIFIED BY "password";
   GRANT SUPER ON . TO user_id@'%' IDENTIFIED BY "password";
   ```

MS SQL Server

> **INFO**
>
> - Set the `Collation` options for all databases and tables to be case-insensitive (CI).
> - Database names can only contain numbers, English letters (case-sensitive), and special symbols `-` `_`.

Setting the port

- Run **SQL Server Configuration Manager** and set **TCP/IP Protocol** for **Protocols for SQLEXPRESS** to the desired port number.
- Restart the **SQL Server Services** to apply the settings.

Creating the user and database

1. Log in with the **sa** account using **SQL Server Authentication** in **SQL Server Management Studio**.
2. Right-click on **Security** and click **New Login**.
3. Enter the desired name in the **Login Name** field and select **SQL Server Authentication**.
4. Enter the desired password in the **Password** and **Confirm password** fields, then uncheck **Enforce password policy**.
5. Click **OK** to save the settings.
6. Right-click on **Database** and click **New Database**.
7. Enter the desired name in the Database Name field.
8. Enter the login name set in step **3** in the **Owner** field.

TIP

It is recommended to set up the **Database Files** section as shown below.

- **Initial Size (MB)**: 3000
- **Autogrowth/Maxsize**: 10MB, **Unlimited**

CAUTION

In environments with many transactions, backup the logs periodically to ensure that the size of the log files does not increase.

Setting the Windows Authentication database

1 Presetting

If you are using **Microsoft Windows Active Directory**, complete the presets as below before setting up the Windows Authentication database.

1. Log in as an administrator account in **SQL Server Management Studio**.
2. Right-click on **Security** and click **New Login**.
3. Select **Windows Authentication** and then click **Search**.
4. Click on the location in the **Select a user or group** window, select the Active Directory path, and click **OK**.
5. Enter the user name in the **Enter object name to select** field, then click **Check Names** > **OK**.
6. Click on **Server Roles** in the **Select a page**.
7. Select **sysadmin** and then click **OK**.
8. Click on **User Mapping** in the **Select page**.
9. Select **ac**, **master**, **ta**, **ve** and set the **Default Schema** to **dbo**.
10. Click **OK** to save the settings.

2 Settings for using MS SQL with Windows Authentication through Active Directory

1. Run *services.msc*.
2. In the **Properties** > **Logon** window of the SQL Server database, select **Specify account** and log in as a domain user.
3. Add port 1433 as an exception in the Windows Firewall.

4. Create empty **ac**, **ta**, **ve** databases in SQL Server with **sysadmin** authentication.
5. Set the domain user to use Windows Authentication for SQL Server and assign all permissions except **sysadmin** to the **ac**, **ta**, **ve** databases.
6. Connect all services except the local computer in *services.msc*.
7. Set the domain user as an administrator on the local service computer.
8. Connect to MS SQL ODBC.

3 Setting the database

1. After running the **SQL Server Configuration Manager**, click on **Client Protocol** under **SQL Native Client**.
2. Select **TCP/IP** and check the default port.
3. Click on the **Protocols for SQL EXPRESS** under **SQL Server Network Configuration**.
4. Check if the ODBC port in **TCP/IP** is set to the same value as the default port.
5. Log in as an administrator account in **SQL Server Management Studio**.
6. Click on **Security** > **Log In**, then double-click **NT AUTHORITY\SYSTEM**.
7. Click on **Server Roles** in the **Select a page**.
8. Select **public** and **sysadmin**, then click **OK**.
9. Click on **User Mapping** in the **Select page**.
10. Select the **ac**, **ta**, **ve** database and click **OK** to save.

System Minimum Requirements

BioStar X provides a reliable and scalable integrated security management solution for large enterprise environments. The system can efficiently manage over a thousand devices through a distributed architecture consisting of a main server and a communication server.

The main server manages the core management features of the system, while the communication server is responsible for device communication, distributing the load and optimizing performance. Additionally, administrators can access the system via a web browser on client PCs and perform all management tasks. Check the system requirements below to configure the optimal environment for your organization size.

> **INFO**
>
> For more information on license configuration and optimization, contact Suprema Technical Support.

Main server

The main server is the server where the central management system of **BioStar X** is installed. The user accesses the system through a web browser to manage it and handle all tasks such as setting user information or access permissions. It is also responsible for monitoring the overall status of the system and managing event logs or alarms.

Item		Small	Mid-sized organization	Enterprise
Usage Environment	Total Devices	1 to 50	51 to 100	101 to 1,000
System Requirement	Operating System	Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, Windows Server 2022		
	Database	MariaDB 11.4.4, MS SQL Server 2012 SP3, MS SQL Server 2014 SP2, MS SQL Server 2016 SP1, MS SQL Server 2017, MS SQL Server 2019, MS SQL Server 2022		
	CPU	2.3 GHz 6-core	2.3 GHz 8-core	Minimum 2.3 GHz Recommended 4.0 GHz 16-core
	RAM	16 GB	32 GB	Minimum 64 GB Recommended 128 GB
	SSD	512 GB	512 GB	1 TB
	HDD	When using the **Image Log** feature, 200 GB is required for 10 million image logs.		

ⓘ **INFO**

- **BioStar X** can only be installed on 64-bit operating systems.
- MS SQL Server communication security supports TLS 1.2.
- If MS SQL Server and **BioStar X** are installed on different PCs, you should install the Microsoft OLE DB Driver for SQL Server on a PC with **BioStar X** installed.
- For enterprise environment, it is recommended to install an MS SQL Server database.
- If you are using an MS SQL Server database and **BioStar X T&A**, you will need to install the Microsoft ODBC Driver 17 for SQL Server appropriate for your environment.
- The Windows virtual environment provided by Boot Camp on macOS is not supported.

SQL Server license requirements

If using SQL Server as the database, a proper SQL Server license is required depending on the number of connected devices for stable operation of **BioStar X**. Refer to the recommended license configurations for each environment to select a license suitable for the size and needs of your organization.

ⓘ **INFO**

For more information on SQL Server licenses, refer to Microsoft SQL Server Licensing.

General usage

Organization	Total Devices	Number of cores	SQL Server license
Small	1 to 50	4 - 6	SQL Server Standard Edition (Core-based)
Mid-sized organization	50 - 300 devices	8 - 12	
Enterprise	300 - 1,000 devices	16 - 24	

Using the BioStar X API

Organization	Total Devices	Number of cores	SQL Server license
Small	1 to 50	4 - 6	SQL Server Standard Edition (Core-based)
Mid-sized organization	50 - 300 devices	8 - 12	
Enterprise	300 - 1,000 devices	16 - 24	

Communication server

The communication server is a server dedicated to communication with access control devices. It helps to manage many devices reliably by installing separately from the main server. A single communication server can connect up to 1,000 devices, and you can add multiple communication servers as needed.

Item		Specification
System Requirement	Operating System	Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, Windows Server 2022
	CPU	Minimum 2.3 GHz, recommended 4.0 GHz 16-core
	RAM	Minimum 64 GB, recommended 128 GB
	SSD	1 TB

Client

The client is the PC where administrators access **BioStar X** through a web browser to operate the system.

Item		Small	Mid-sized organization	Enterprise
System Requirement	CPU	2.5 GHz	2.5 GHz	Minimum 2.5 GHz
	RAM	16 GB	32 GB	Minimum 32 GB
	GPU	Minimum NVIDIA GeForce RTX 4060 when using VMS		
	web browser	Google Chrome version 100 or higher		

ⓘ **INFO**

- **BioStar X** is optimized for Google Chrome.
- The web interface of **BioStar X** does not provide support for mobile browsers.

Getting Started

Essential setup guide for first-time users of **BioStar X**. Step by step guide to the key procedures necessary for successfully building and operating **BioStar X**, from choosing installation methods to license registration.

Check Network Priority

Instructions for checking and setting the server's network priority before installing BioStar X.

Express Installation

This guide provides steps to quickly install BioStar X by automatically creating the embedded MariaDB server and database.

Custom Installation

This guides the user on how to set up a custom installation to integrate with a database that the user has already installed.

Upgrade

This document guides the procedure for upgrading BioStar 2 to BioStar X and the requirements to check before the upgrade.

Install Communication Server

This document guides the process of installing the communication server.

How to Log in

Access **BioStar X** through a web browser.

Register License Key

Activate the BioStar X license to use additional features.

Initial Setup Guide

This document provides step-by-step instructions for the initial setup and operation of the BioStar X access control system.

Check Network Priority

Instructions for checking and setting the server's network priority before installing **BioStar X**.

When is it needed?

You need to check and set network priority in the following situations.

- When two or more network adapters are installed on the server
- When a specific network adapter must be used for the **BioStar X** service
- To prevent network connection issues after installing **BioStar X**

> ⓘ **INFO**
>
> If none of the above situations apply, there is no need to change the network priority. Skip this step and proceed with the installation of **BioStar X**. For more information on installing **BioStar X**, refer to the following.

> ⚠ **WARNING**
>
> A network adapter with a lower metric (higher priority) will be automatically selected during the installation of **BioStar X**. Since it may be difficult to change this setting after installation, be sure to check and adjust the network priority before installation.

Check Network Priority

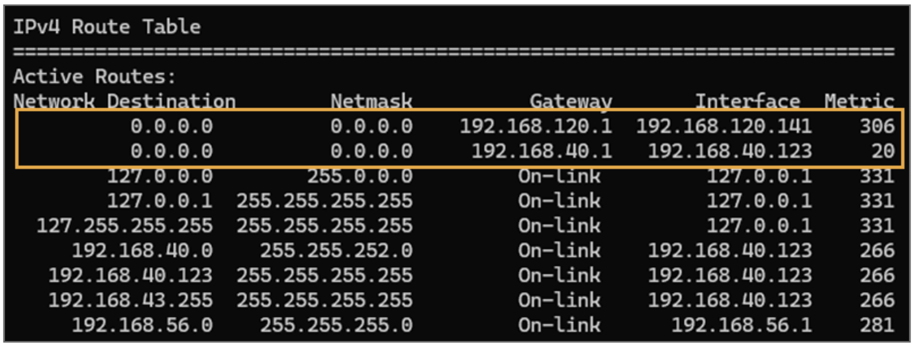
Check in command prompt

1. Search for `cmd` in the **Start** menu and run **Command Prompt**.
2. Enter the following command.

   ```
   route print
   ```

3. Look for entries in the **IPv4 Route Table** section where **Network Destination** is `0.0.0.0`.
4. Check the value in the **Metric** column. The lower the value, the higher the priority.

Example output:



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.120.1  192.168.120.141    306
          0.0.0.0          0.0.0.0     192.168.40.1   192.168.40.123     20
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     192.168.40.0    255.255.252.0         On-link    192.168.40.123    266
   192.168.40.123  255.255.255.255         On-link    192.168.40.123    266
   192.168.43.255  255.255.255.255         On-link    192.168.40.123    266
     192.168.56.0    255.255.255.0         On-link      192.168.56.1    281
```

In the above example, the `192.168.40.123` interface has a metric value of **20**, resulting in a higher priority.

Check network adapter information

Verify which network adapter corresponds to each interface.

1. In the **Command Prompt** window, enter the command below.

```
ipconfig /all
```

2. Match each network adapter's **IPv4 address** with the **Gateway** address identified earlier to identify which adapter it is.

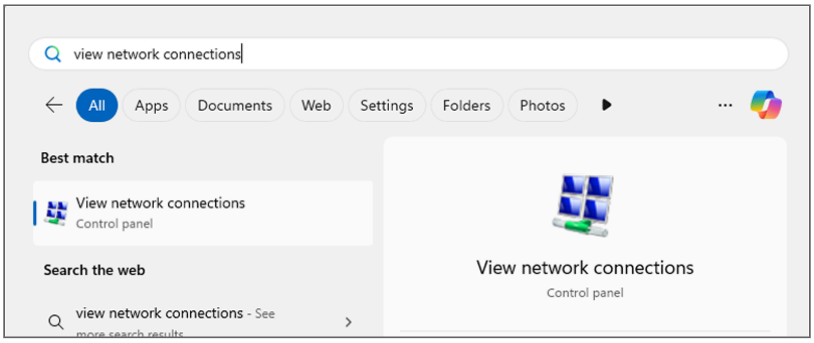
Change network priority

To raise the priority of the desired network adapter, follow the steps below.

> ⓘ **INFO**
>
> The following steps are based on Windows 11. The menu location may vary depending on the version of Windows you are using.

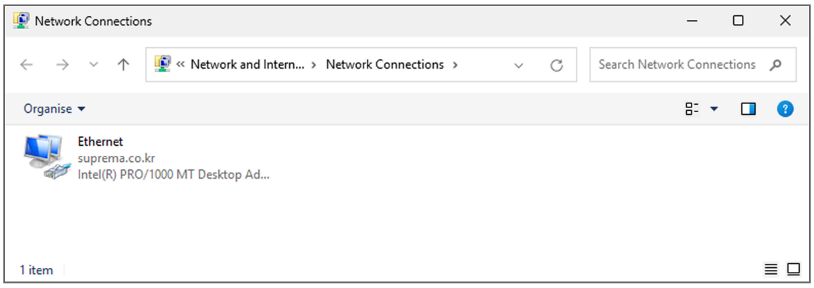
1 Open network settings

1. In the **Start** menu, type **View Network Connections**.



view network connections

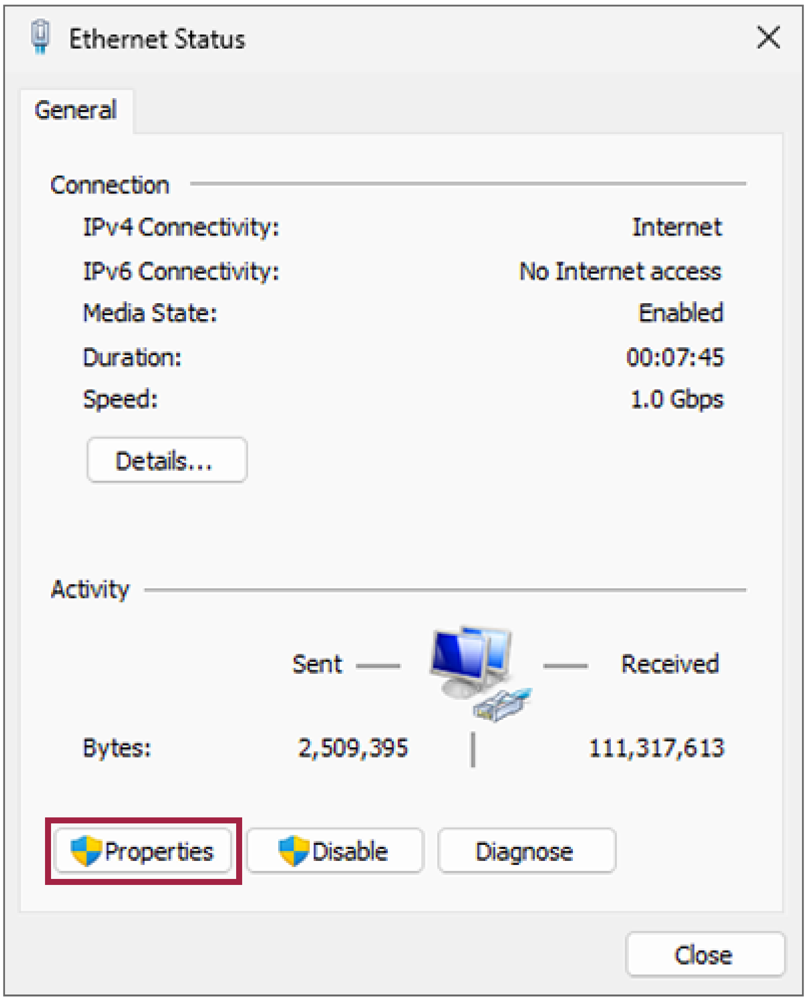
2. Click **View Network Connections** from the search results.
3. Double-click on the adapter connected to the internet from the list.



Network Connections
« Network and Intern... › Network Connections ›
Search Network Connections
Organise ▾
Ethernet
suprema.co.kr
Intel(R) PRO/1000 MT Desktop Ad...
1 item

2 Open adapter options

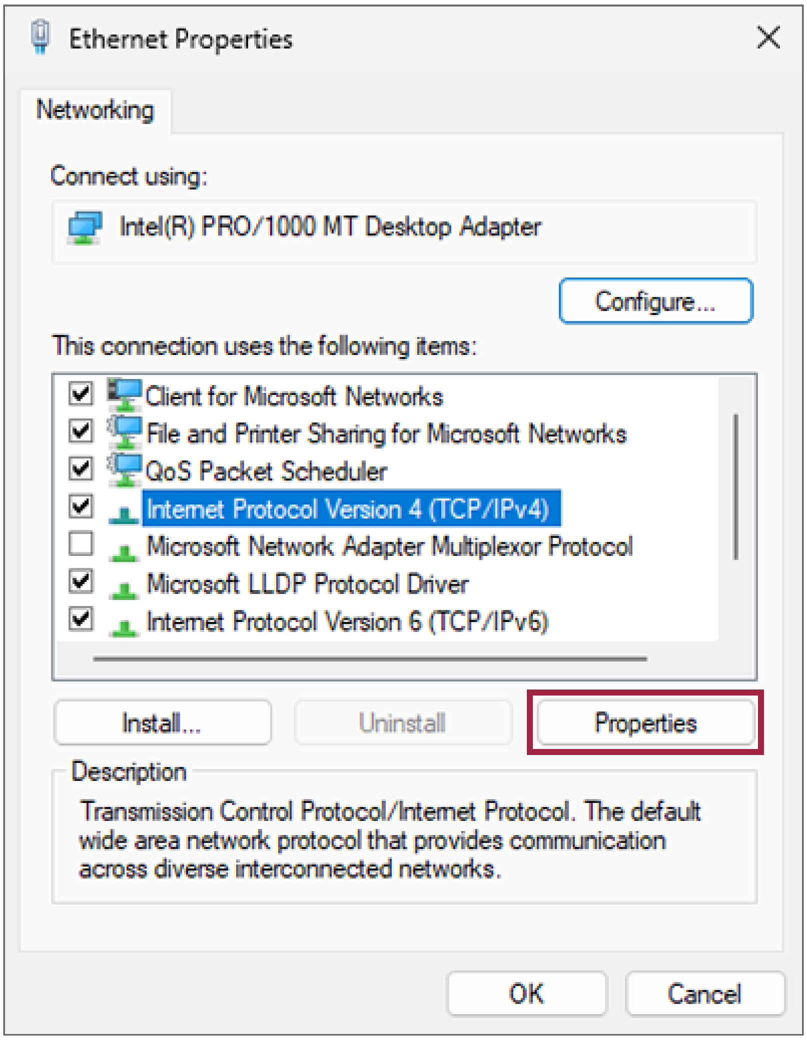
1. When the **Ethernet Status** window appears, click the **Properties** button.



IPv4 Connectivity: Internet
IPv6 Connectivity: No Internet access
Media State: Enabled
Duration: 00:07:45
Speed: 1.0 Gbps

Bytes: 2,509,395 | 111,317,613

2. When the Ethernet Properties window appears, select **Internet Protocol Version 4 (TCP/IPv4)** from the list.



Ethernet Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Desktop Adapter

This connection uses the following items:

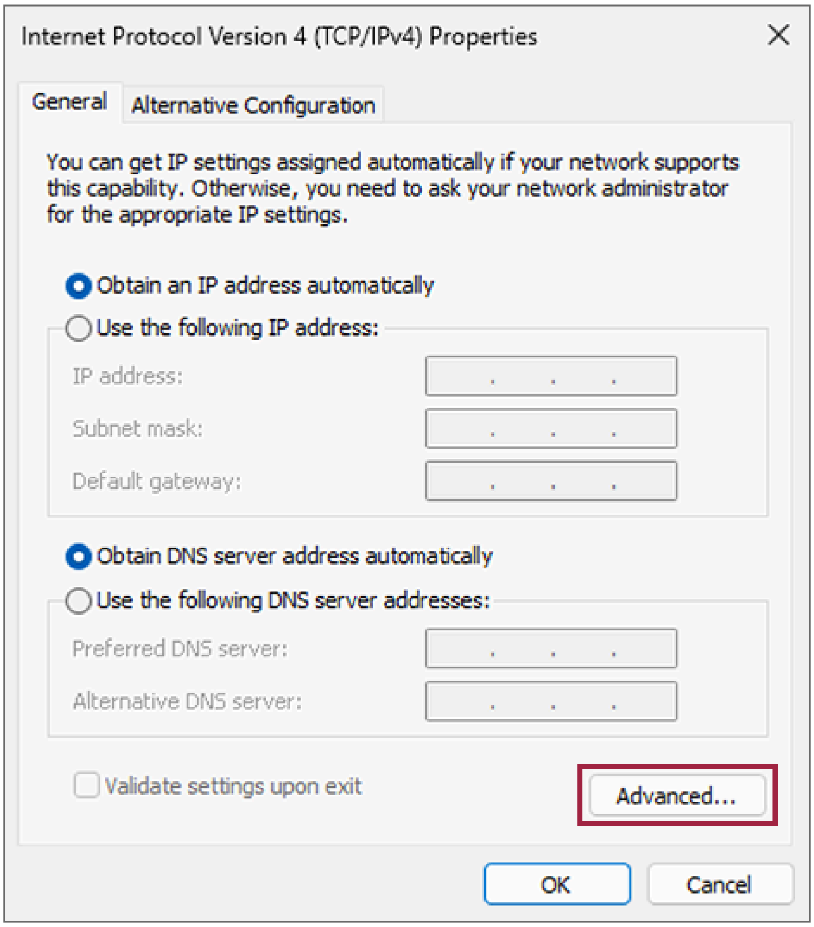
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

3. Click the **Properties** button.

4. When the **Internet Protocol Version 4 (TCP/IPv4) Properties** window appears, click the **Advanced** button.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

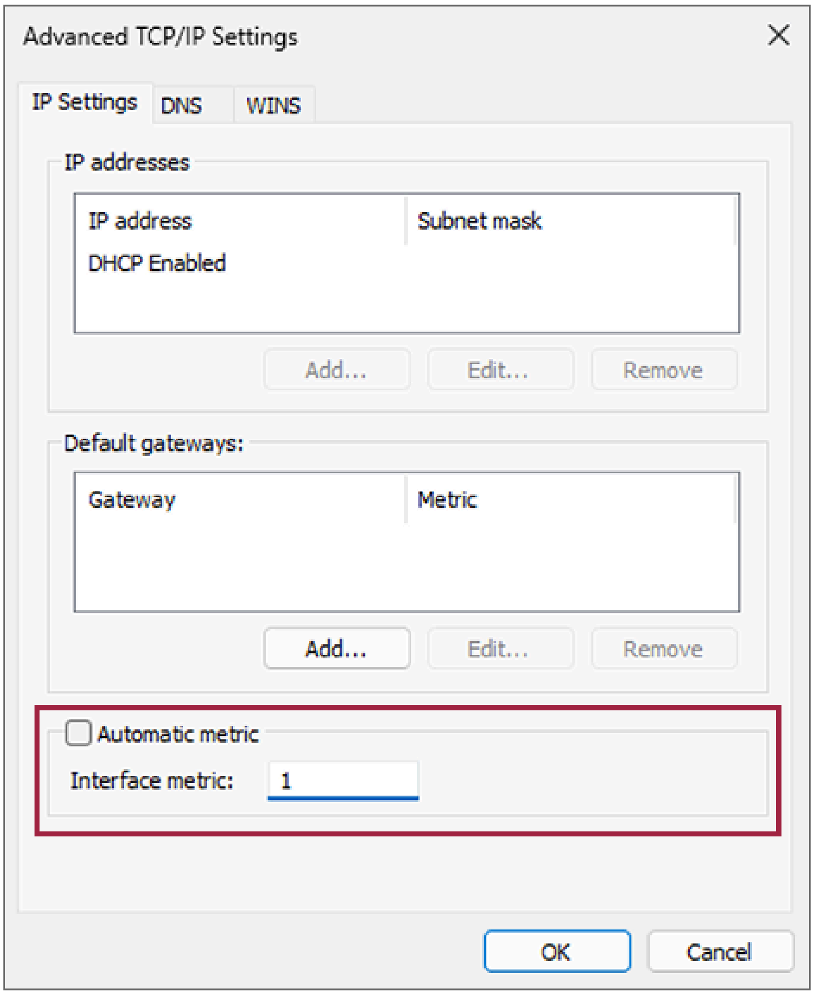
Alternative DNS server: . . .

□ Validate settings upon exit

3

Metric settings

1. Uncheck the **Automatic Metric** checkbox.



Advanced TCP/IP Settings

□ Automatic metric

Interface metric: 1

2. Enter the desired value in the **Interface Metric** field.
   - If you want the highest priority, enter `1`.
   - If you want a higher priority than other adapters, enter a number smaller than the metric values of other adapters.
3. To save the settings and close all windows, click the **OK** button.

> **INFO**
>
> The values you can enter for **Interface Metric** range from `1` to `9999`. The lower the value, the higher the priority.

4

Check settings

1. Reopen **Command Prompt** and execute the `route print` command.

2. Check whether the metric value has changed.

Troubleshooting

- If the settings are not applied, restart your computer or disable and then re-enable the network adapter.
- If the network connection is lost, revert to the original settings and re-enable the **Automatic Metric** option. Contact your network administrator to verify the correct settings.

> **INFO**
>
> If you need to change network settings after installing **BioStar X**, it's recommended to completely uninstall the program and then reinstall it.

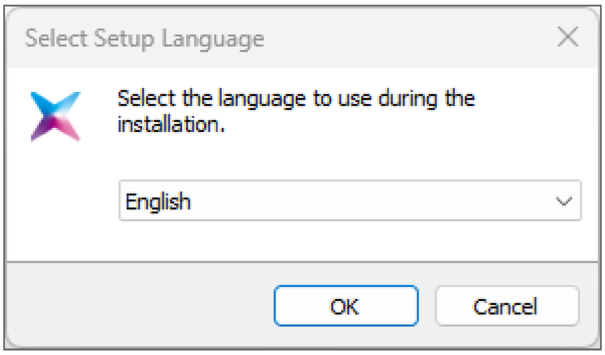
Express Installation

This procedure guides you step-by-step to install **BioStar X** using **Express installation**. **Express installation** automatically installs the embedded MariaDB server and creates the database, allowing for quick installation without separate database configuration.

> **INFO**
>
> To proceed with **Custom installation** to connect with an already installed database, refer to the following.

Installation guide

1. Go to the Suprema Download Center, log in, and download the installation package (*BioStar X Setup.X.Y.Z.BB.exe*).
2. Run the downloaded installation file.
3. Select the language to use and select the **OK** button.

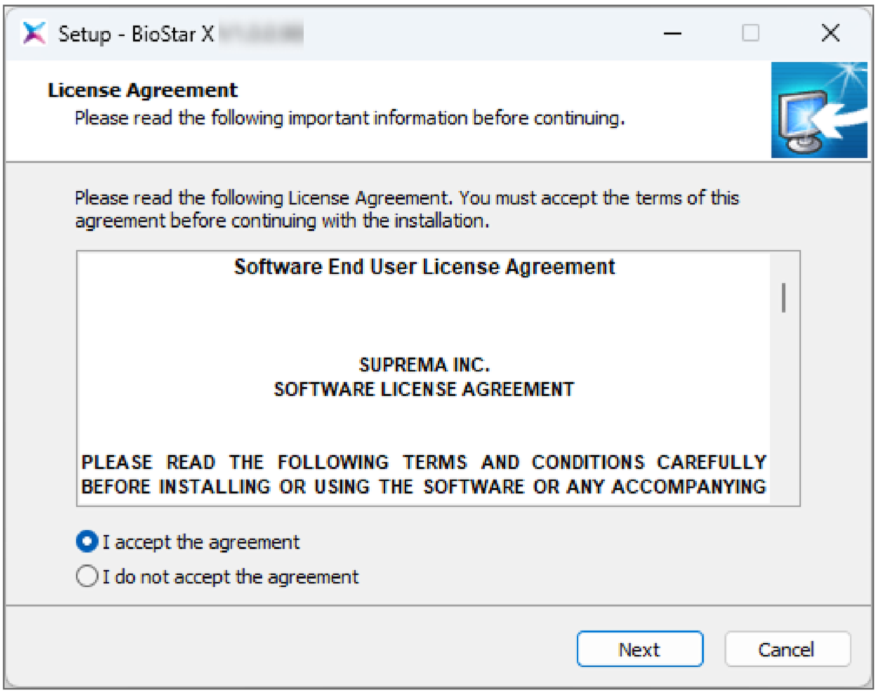


Select Setup Language

Select the language to use during the installation.

English

4. To continue the installation, select **I accept the agreement** and click the **Next** button.



Setup - BioStar X [redacted]

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

Software End User License Agreement

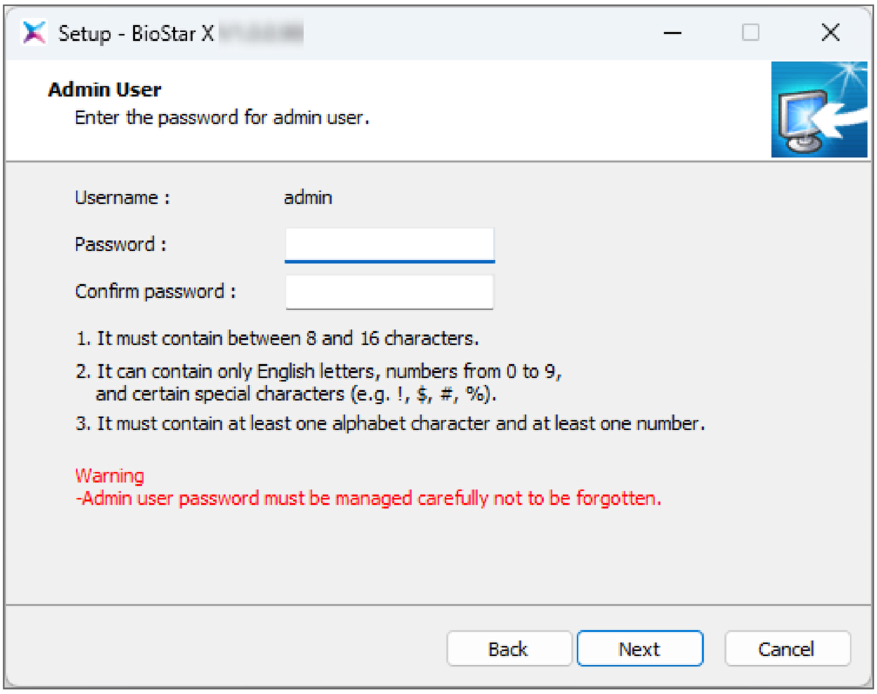
SUPREMA INC.
SOFTWARE LICENSE AGREEMENT

PLEASE READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE INSTALLING OR USING THE SOFTWARE OR ANY ACCOMPANYING

● I accept the agreement

○ I do not accept the agreement

5. Enter the administrator account password and click the **Next** button.



Setup - BioStar X [redacted]

Admin User

Enter the password for admin user.

Username : admin

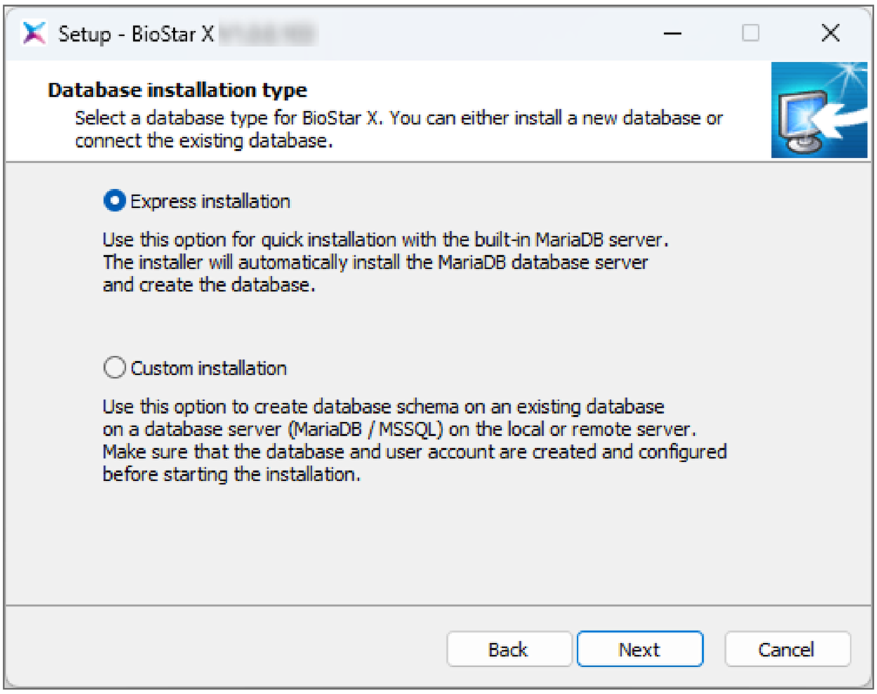
Password :

Confirm password :

1. It must contain between 8 and 16 characters.
2. It can contain only English letters, numbers from 0 to 9, and certain special characters (e.g. !, $, #, %).
3. It must contain at least one alphabet character and at least one number.

Warning
-Admin user password must be managed carefully not to be forgotten.

6. Select **Express installation** and click the **Next** button.



Database installation type

Select a database type for BioStar X. You can either install a new database or connect the existing database.

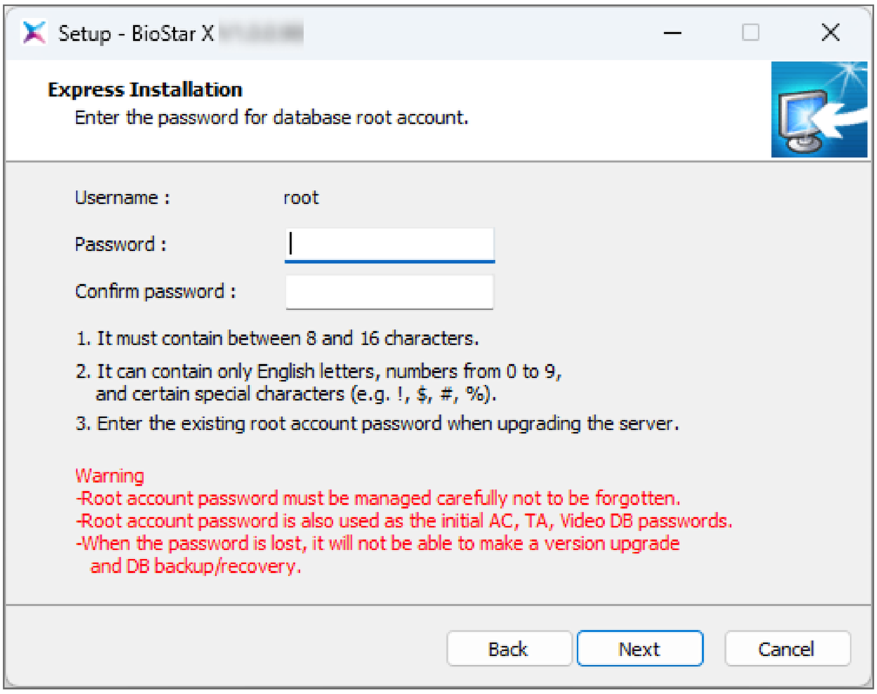
● Express installation

Use this option for quick installation with the built-in MariaDB server. The installer will automatically install the MariaDB database server and create the database.

○ Custom installation

Use this option to create database schema on an existing database on a database server (MariaDB / MSSQL) on the local or remote server. Make sure that the database and user account are created and configured before starting the installation.

7. Enter the root account password for the database and click the **Next** button.



Express Installation

Enter the password for database root account.

Username : root

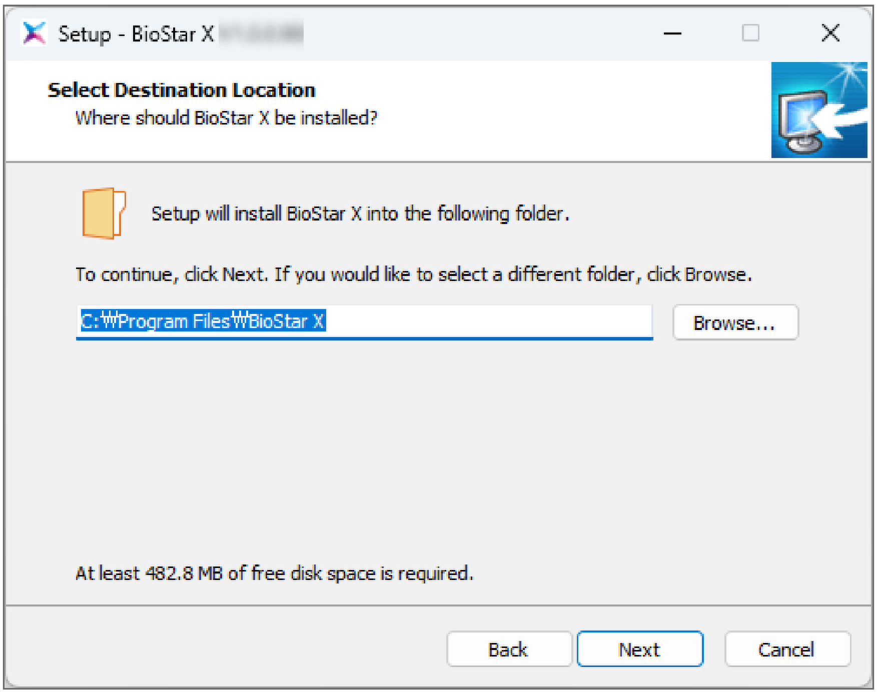
Password :

Confirm password :

1. It must contain between 8 and 16 characters.
2. It can contain only English letters, numbers from 0 to 9, and certain special characters (e.g. !, $, #, %).
3. Enter the existing root account password when upgrading the server.

Warning
-Root account password must be managed carefully not to be forgotten.
-Root account password is also used as the initial AC, TA, Video DB passwords.
-When the password is lost, it will not be able to make a version upgrade and DB backup/recovery.

8. Set the installation path for **BioStar X** and click the **Next** button.



Setup - BioStar X

Select Destination Location

Where should BioStar X be installed?

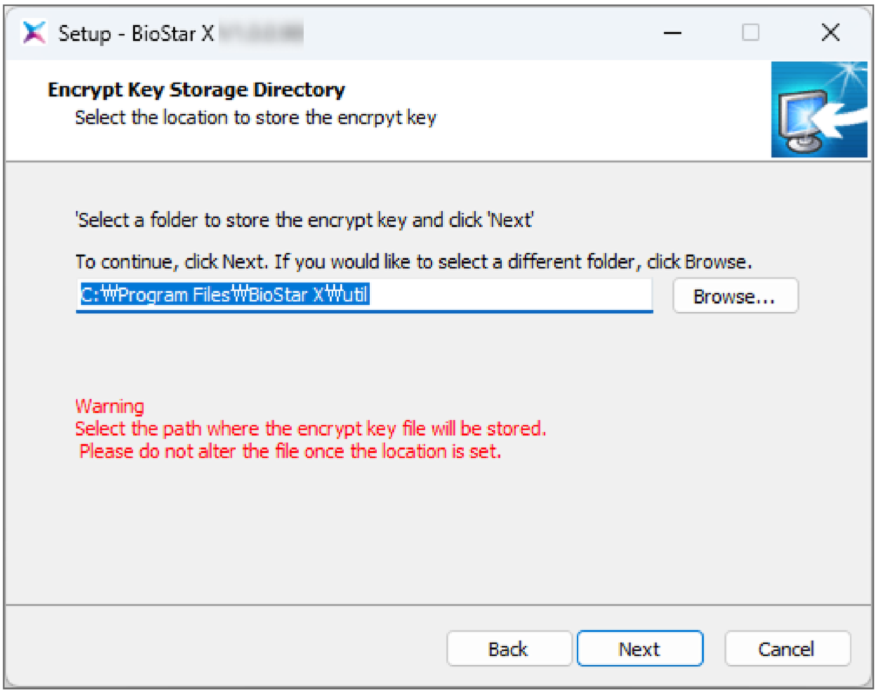
Setup will install BioStar X into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:₩Program Files₩BioStar X

At least 482.8 MB of free disk space is required.

9. Set the path to store the encryption key and click the **Next** button.



Setup - BioStar X

Encrypt Key Storage Directory

Select the location to store the encrpyt key

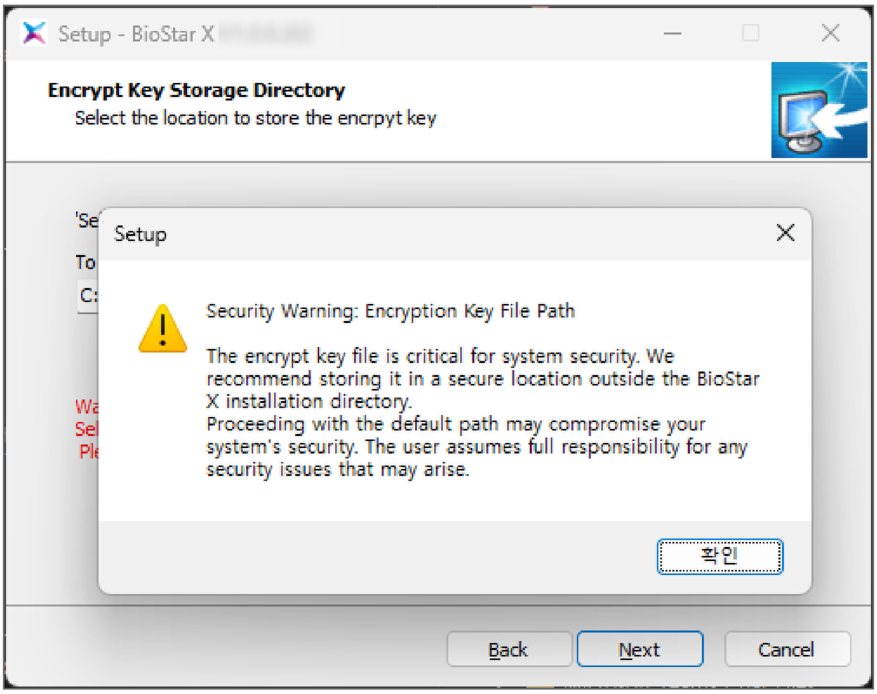
'Select a folder to store the encrypt key and click 'Next'

To continue, click Next. If you would like to select a different folder, click Browse.

C:₩Program Files₩BioStar X₩util

Warning
Select the path where the encrypt key file will be stored.
Please do not alter the file once the location is set.

10. Check the contents of the security warning message and click **OK**.



Setup - BioStar X [redacted]

Encrypt Key Storage Directory

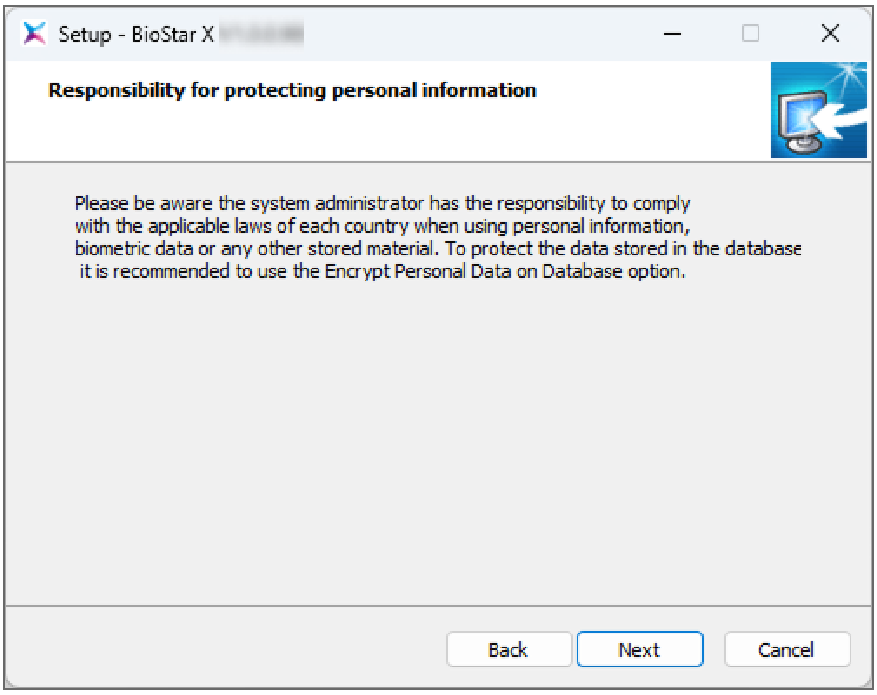
Select the location to store the encrpyt key

Setup

Security Warning: Encryption Key File Path

The encrypt key file is critical for system security. We recommend storing it in a secure location outside the BioStar X installation directory.
Proceeding with the default path may compromise your system's security. The user assumes full responsibility for any security issues that may arise.

11. Read the information about the management and responsibility of personal information stored in the database, and click the **Next** button to continue the installation.

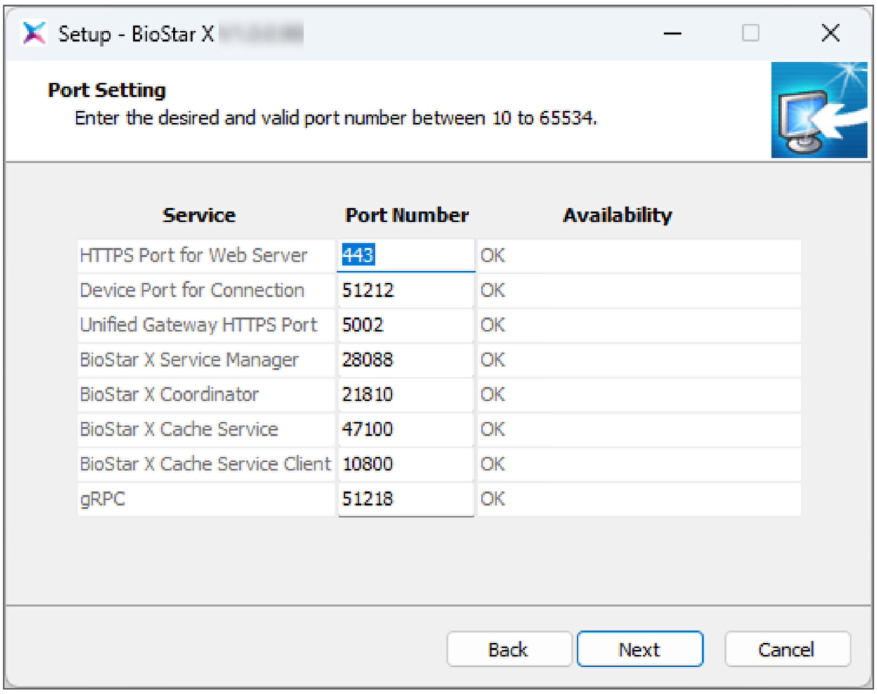


Setup - BioStar X [redacted]

Responsibility for protecting personal information

Please be aware the system administrator has the responsibility to comply with the applicable laws of each country when using personal information, biometric data or any other stored material. To protect the data stored in the database it is recommended to use the Encrypt Personal Data on Database option.

12. Set the port for **BioStar X** communication and click the **Next** button.



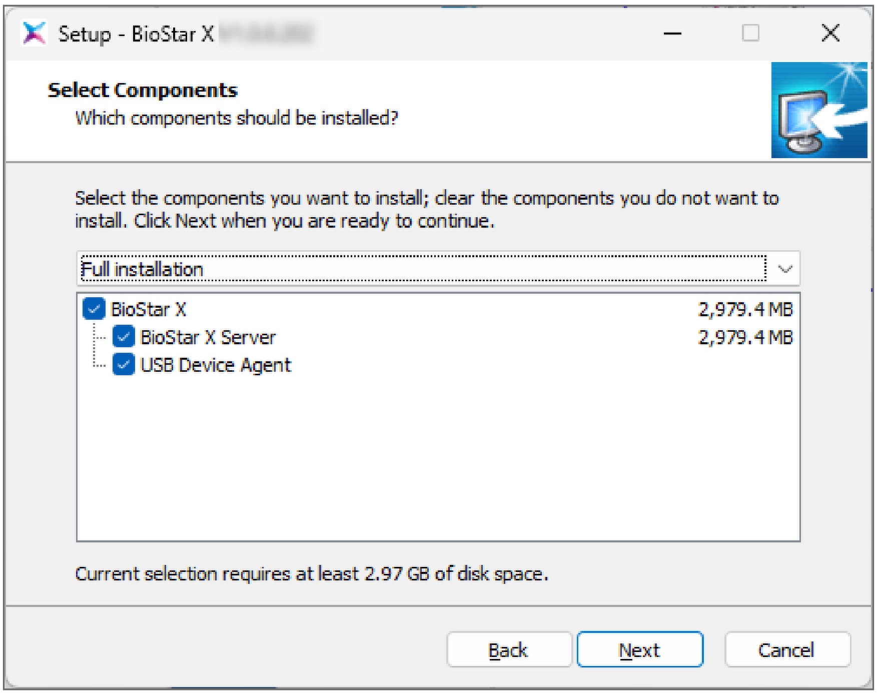
Setup - BioStar X

Port Setting

Enter the desired and valid port number between 10 to 65534.

Service	Port Number	Availability
HTTPS Port for Web Server	443	OK
Device Port for Connection	51212	OK
Unified Gateway HTTPS Port	5002	OK
BioStar X Service Manager	28088	OK
BioStar X Coordinator	21810	OK
BioStar X Cache Service	47100	OK
BioStar X Cache Service Client	10800	OK
gRPC	51218	OK

13. Select the components of **BioStar X** and click the **Next** button. If you select **USB Device Agent**, the USB Agent and driver for using BioMini, BioMini Plus 2, BioMini Slim 2, and DUALi DE-620 will be installed together.



Setup - BioStar X

Select Components

Which components should be installed?

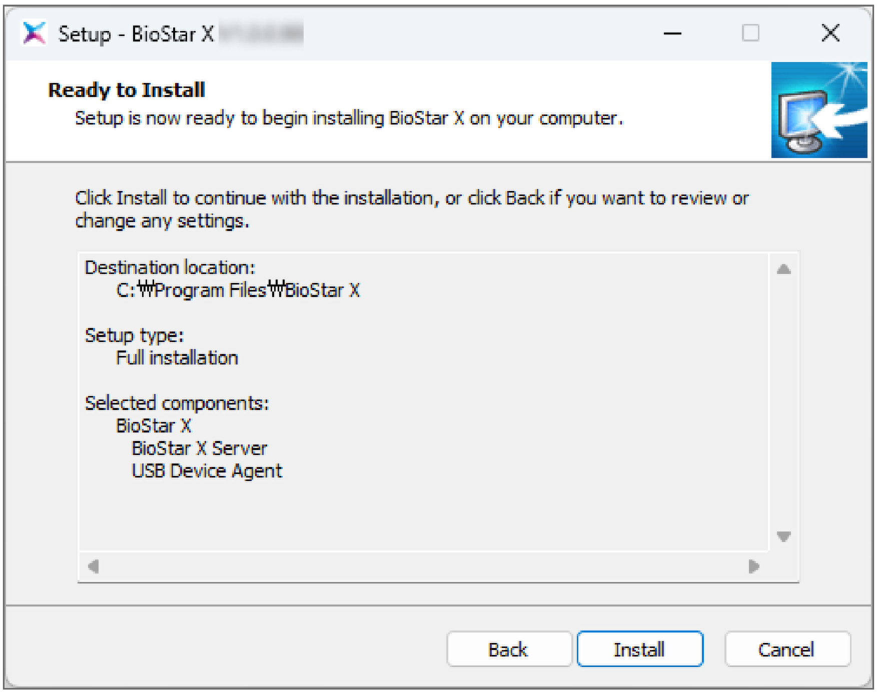
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Full installation

☑ BioStar X 2,979.4 MB
- ☑ BioStar X Server 2,979.4 MB
- ☑ USB Device Agent

Current selection requires at least 2.97 GB of disk space.

14. When all preparations for installation are complete, click the **Install** button.



Setup - BioStar X

Ready to Install

Setup is now ready to begin installing BioStar X on your computer.

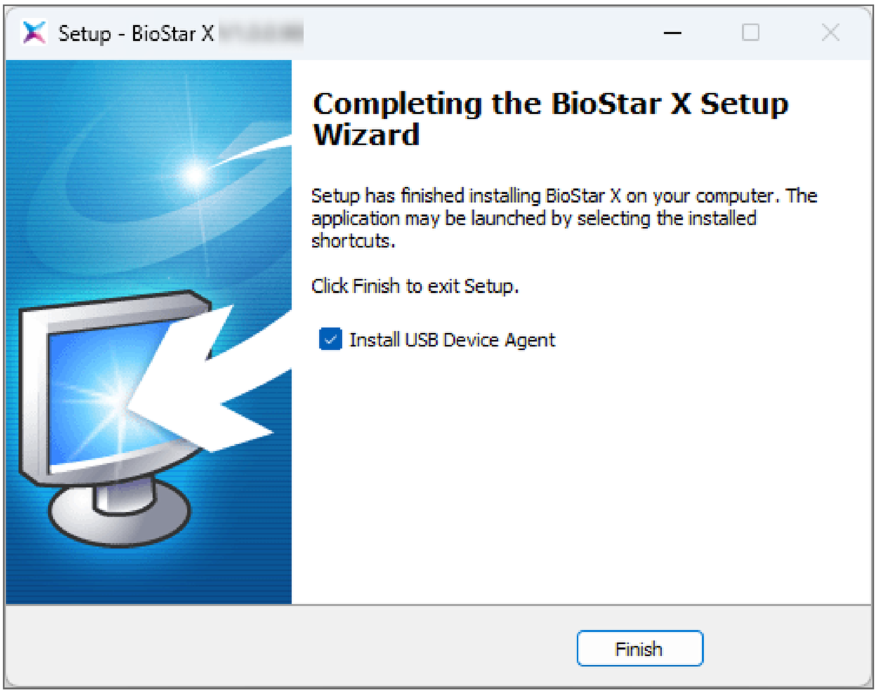
Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:₩Program Files₩BioStar X

Setup type:
Full installation

Selected components:
BioStar X
BioStar X Server
USB Device Agent

15. Select whether to install additional programs and click the **Finish** button.



Setup - BioStar X

Completing the BioStar X Setup Wizard

Setup has finished installing BioStar X on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

☑ Install USB Device Agent

16. Complete the installation of **USB Device Agent** by following the instructions on the installation screen.

ⓘ **INFO**

- In the downloaded file name, X.Y.Z is the version information and BB is the build number.
- The administrator account password is used when logging in for the first time after installing **BioStar X**.
- The root account password for the database is used as the initial password for AC, TA, and Video DB.
- The storage path for the encryption key can be changed. If you modify or move the encryption key file after changing the path, a system error may occur.
- When **BioStar X** is deleted, the encryption key file is also deleted.
- The provided USB Device Agent certificate can only be applied to the local network.
- If another program is using port 443, the BioStar X Setting program runs automatically and allows you to change the port number. For details on changing the port number, refer to the following.
- For more information about changing database settings, refer to the following.

⚠ **WARNING**

- Be careful not to lose the administrator or root account password for the database.
- If you lose the password, version upgrade and DB backup/restore may not be possible.

Custom Installation

This document provides a step-by-step guide on how to install **BioStar X** using the **Custom installation** method. **Custom installation** creates a database schema in conjunction with an existing database (MariaDB, MS SQL Server) installed on a local or remote server. Prepare the database and user account to be linked before starting the installation.

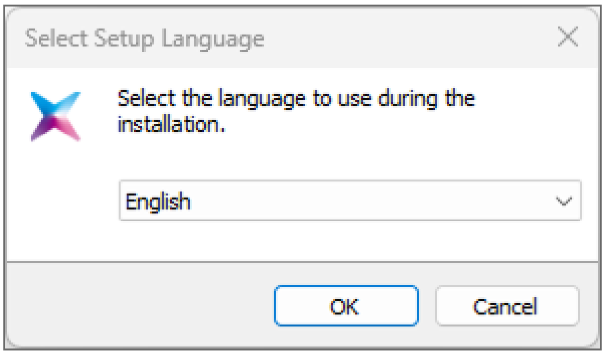
Before starting

- The databases that can be used in integration with **BioStar X** are as follows.
  - MariaDB 11.4.4
  - MS SQL Server 2012 SP3
  - MS SQL Server 2014 SP2
  - MS SQL Server 2016 SP1
  - MS SQL Server 2017
  - MS SQL Server 2019
  - MS SQL Server 2022
- MS SQL Server communication security supports TLS 1.2.
- If the database table creation fails when MS SQL Server is set as the Database Type, you can create the table by executing the script in *C:\Program Files\BioStar X\dbscript\mssql* folder.
- When installing with **Custom installation**, **AC DB name**, **TA DB name**, and **VE DB name** cannot be set the same.
- To use Windows authentication, Microsoft ODBC Driver 17 for SQL Server is required. Please install the driver first.

Installation guide

1. Go to the Suprema Download Center, log in, and download the installation package (*BioStar X Setup.X.Y.Z.BB.exe*).
2. Run the downloaded installation file.

3. Select the language to use and select the **OK** button.

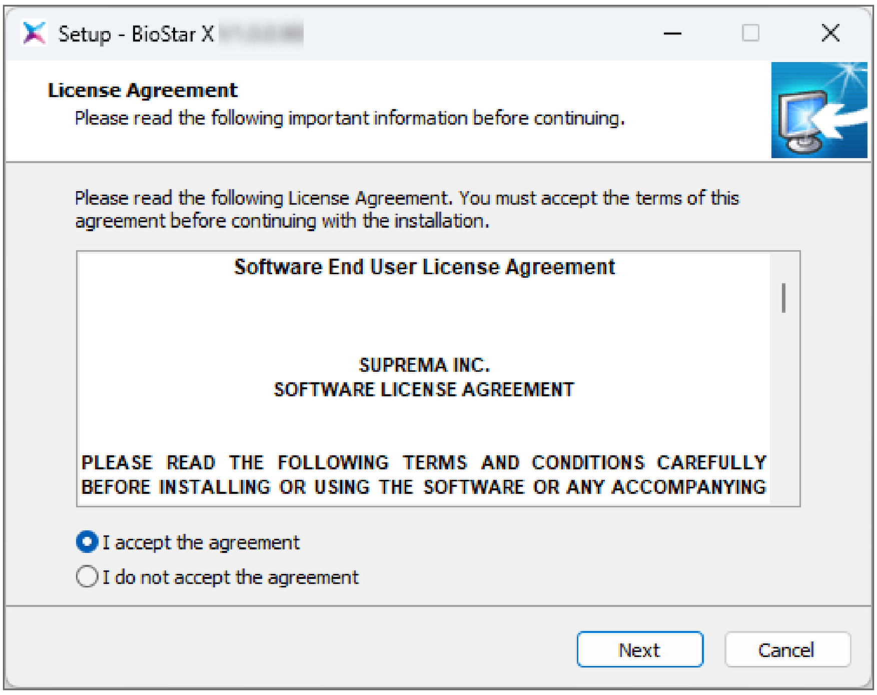


Select Setup Language

Select the language to use during the installation.

English

4. To continue the installation, select **I accept the agreement** and click the **Next** button.



Setup - BioStar X [redacted]

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

Software End User License Agreement

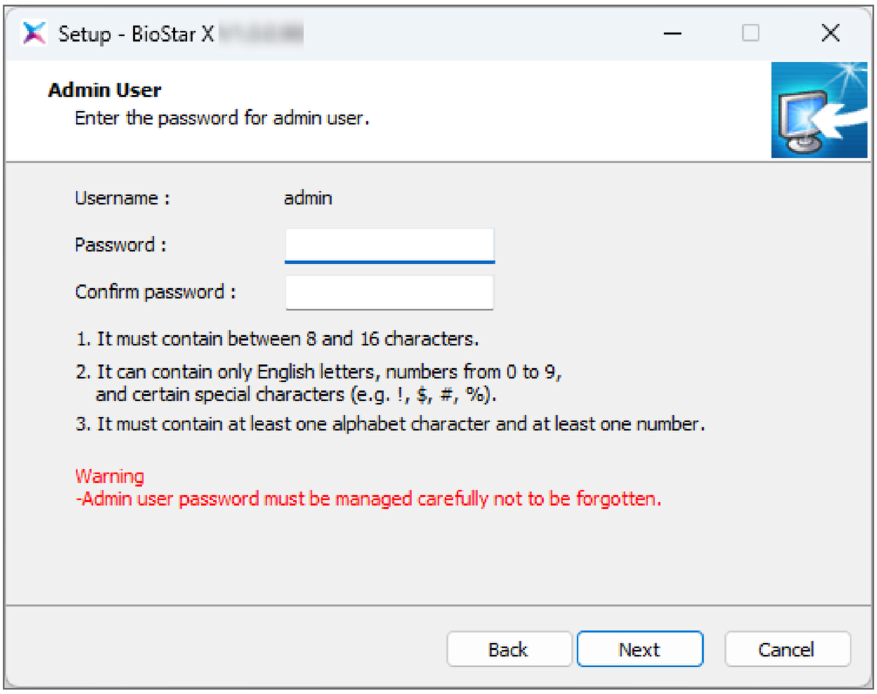
SUPREMA INC.
SOFTWARE LICENSE AGREEMENT

PLEASE READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE INSTALLING OR USING THE SOFTWARE OR ANY ACCOMPANYING

● I accept the agreement

○ I do not accept the agreement

5. Enter the administrator account password and click the **Next** button.


Setup - BioStar X [redacted]

Admin User

Enter the password for admin user.

Username : admin

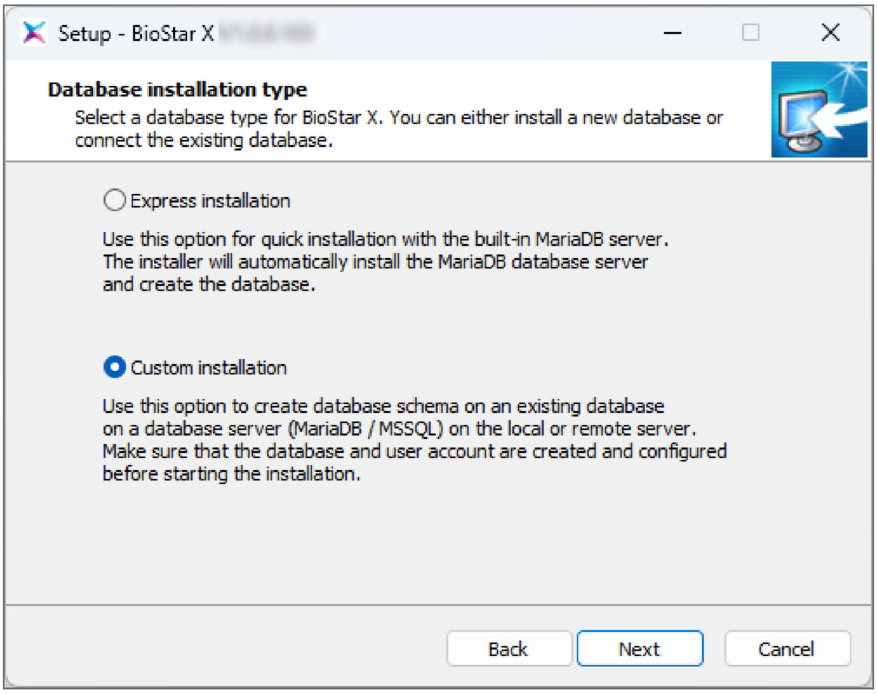
Password :

Confirm password :

1. It must contain between 8 and 16 characters.
2. It can contain only English letters, numbers from 0 to 9, and certain special characters (e.g. !, $, #, %).
3. It must contain at least one alphabet character and at least one number.

Warning
-Admin user password must be managed carefully not to be forgotten.

6. Select **Custom installation** and click the **Next** button.


Setup - BioStar X [redacted]

Database installation type

Select a database type for BioStar X. You can either install a new database or connect the existing database.

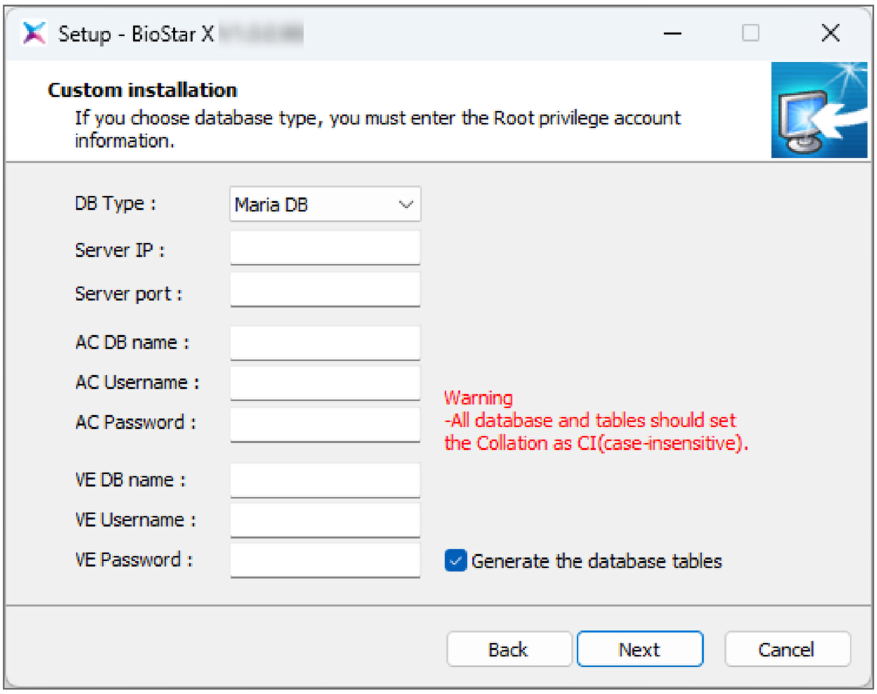
○ Express installation

Use this option for quick installation with the built-in MariaDB server. The installer will automatically install the MariaDB database server and create the database.

● Custom installation

Use this option to create database schema on an existing database on a database server (MariaDB / MSSQL) on the local or remote server. Make sure that the database and user account are created and configured before starting the installation.

7. Enter the details of the pre-configured database and click the **Next** button.



Setup - BioStar X [redacted]

Custom installation

If you choose database type, you must enter the Root privilege account information.

DB Type : Maria DB

Server IP :

Server port :

AC DB name :

AC Username :

AC Password :

VE DB name :

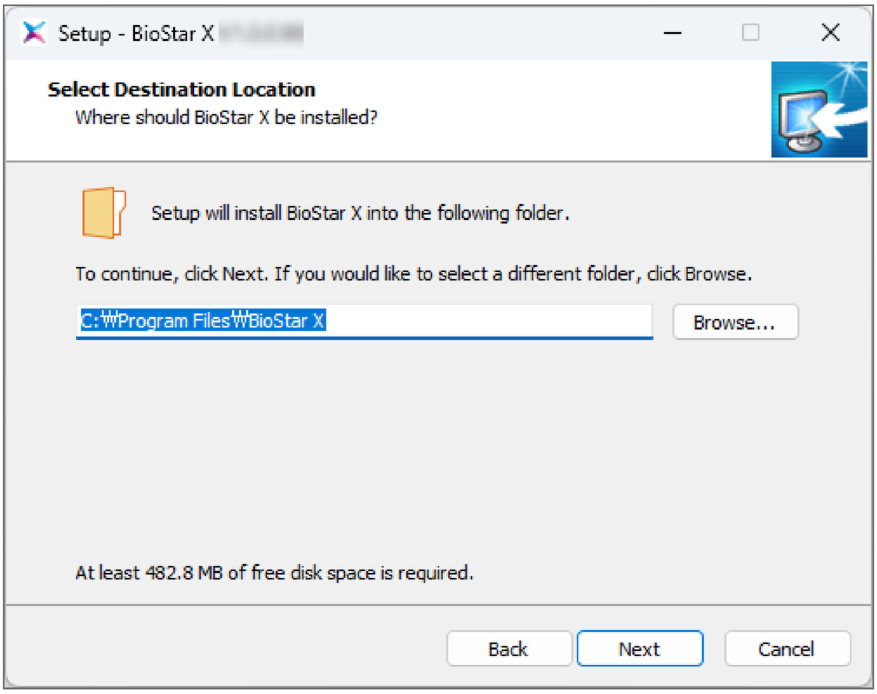
VE Username :

VE Password :

Warning
-All database and tables should set the Collation as CI(case-insensitive).

☑ Generate the database tables

8. Set the installation path for **BioStar X** and click the **Next** button.



Setup - BioStar X [redacted]

Select Destination Location

Where should BioStar X be installed?

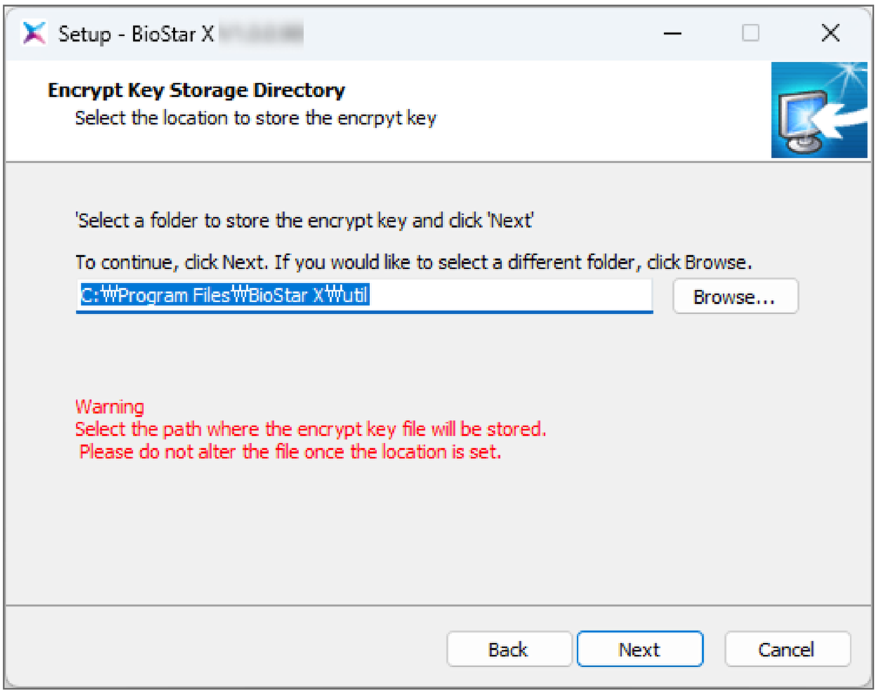
Setup will install BioStar X into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:₩Program Files₩BioStar X

At least 482.8 MB of free disk space is required.

9. Set the path to store the encryption key and click the **Next** button.



Setup - BioStar X

Encrypt Key Storage Directory

Select the location to store the encrpyt key

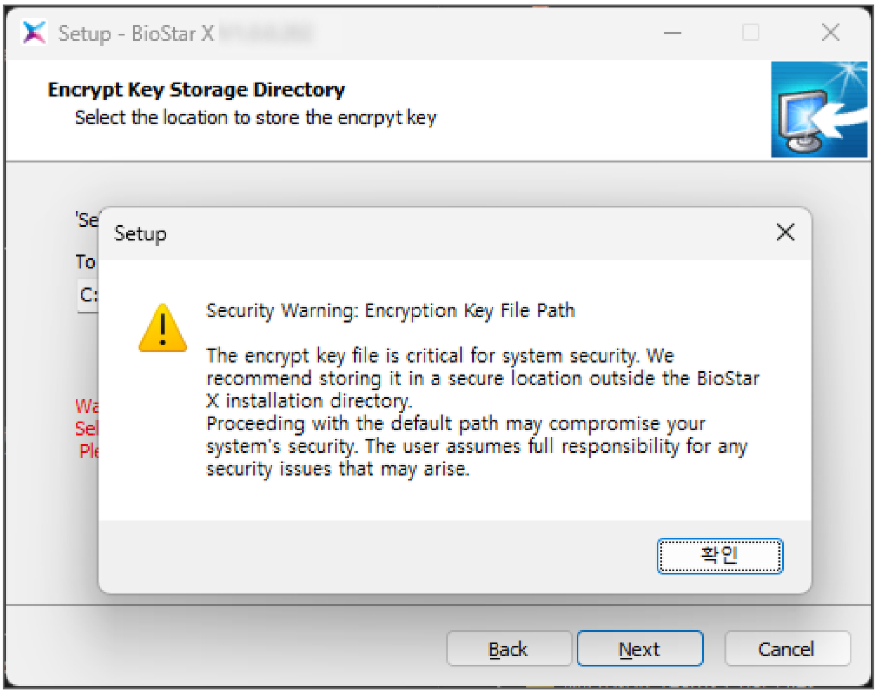
'Select a folder to store the encrypt key and click 'Next'

To continue, click Next. If you would like to select a different folder, click Browse.

C:₩Program Files₩BioStar X₩util

Warning
Select the path where the encrypt key file will be stored.
Please do not alter the file once the location is set.

10. Check the contents of the security warning message and click **OK**.



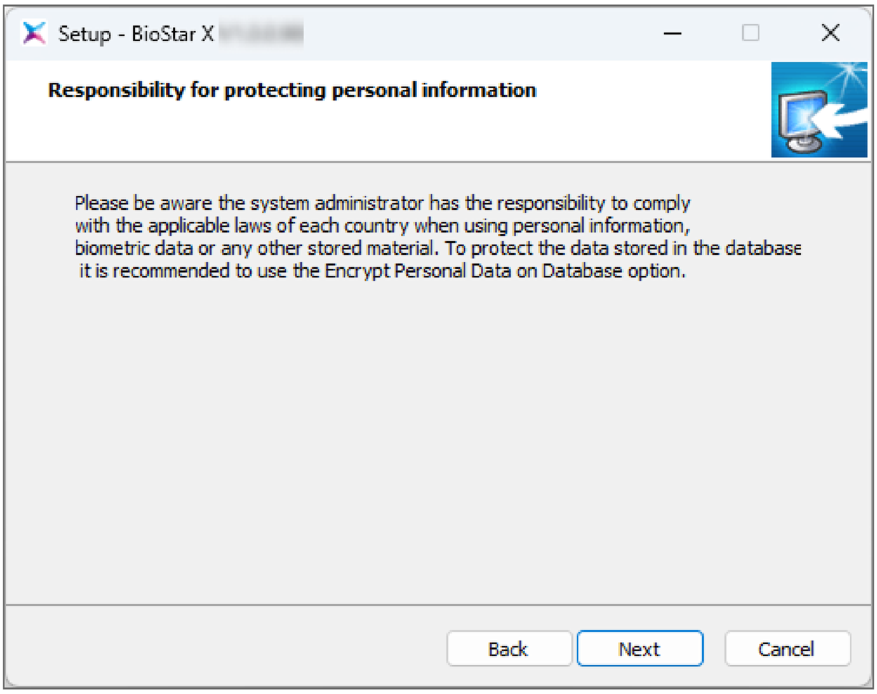
Setup

Security Warning: Encryption Key File Path

The encrypt key file is critical for system security. We recommend storing it in a secure location outside the BioStar X installation directory.
Proceeding with the default path may compromise your system's security. The user assumes full responsibility for any security issues that may arise.

Setup - BioStar X
Encrypt Key Storage Directory
Select the location to store the encrpyt key
확인
Back
Next
Cancel

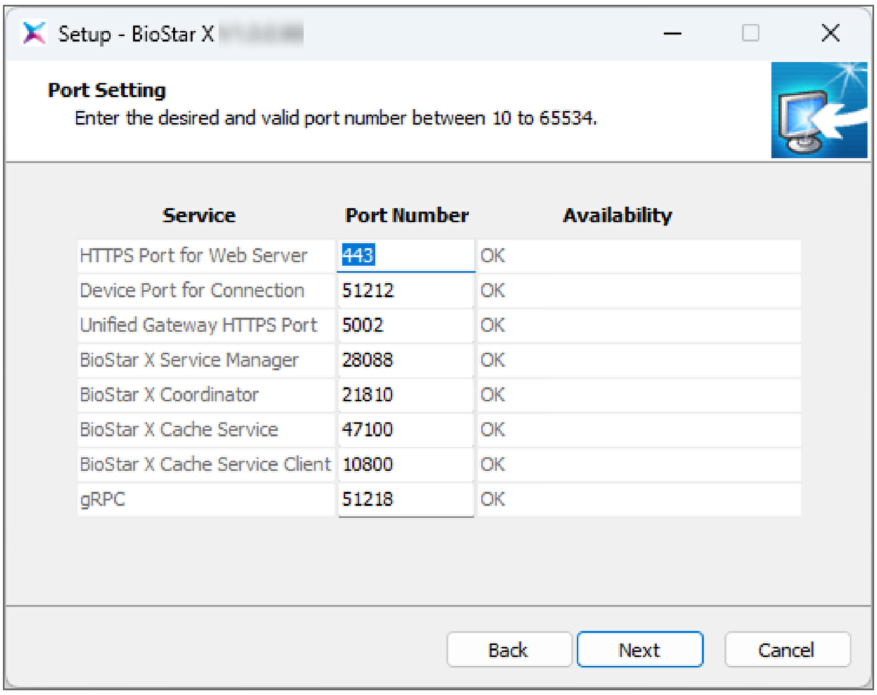
11. Read the information about the management and responsibility of personal information stored in the database, and click the **Next** button to continue the installation.



Responsibility for protecting personal information

Please be aware the system administrator has the responsibility to comply with the applicable laws of each country when using personal information, biometric data or any other stored material. To protect the data stored in the database it is recommended to use the Encrypt Personal Data on Database option.

12. Set the port for **BioStar X** communication and click the **Next** button.

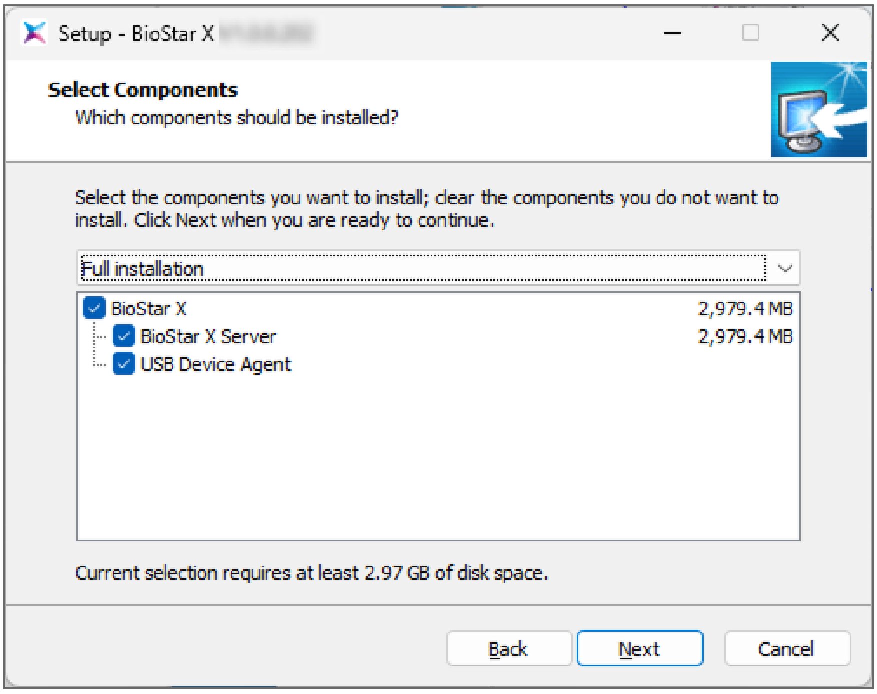


Port Setting

Enter the desired and valid port number between 10 to 65534.

Service	Port Number	Availability
HTTPS Port for Web Server	443	OK
Device Port for Connection	51212	OK
Unified Gateway HTTPS Port	5002	OK
BioStar X Service Manager	28088	OK
BioStar X Coordinator	21810	OK
BioStar X Cache Service	47100	OK
BioStar X Cache Service Client	10800	OK
gRPC	51218	OK

13. Select the components of **BioStar X** and click the **Next** button. If you select **USB Device Agent**, the USB Agent and driver for using BioMini, BioMini Plus 2, BioMini Slim 2, and DUALi DE-620 will be installed together.



Select Components

Which components should be installed?

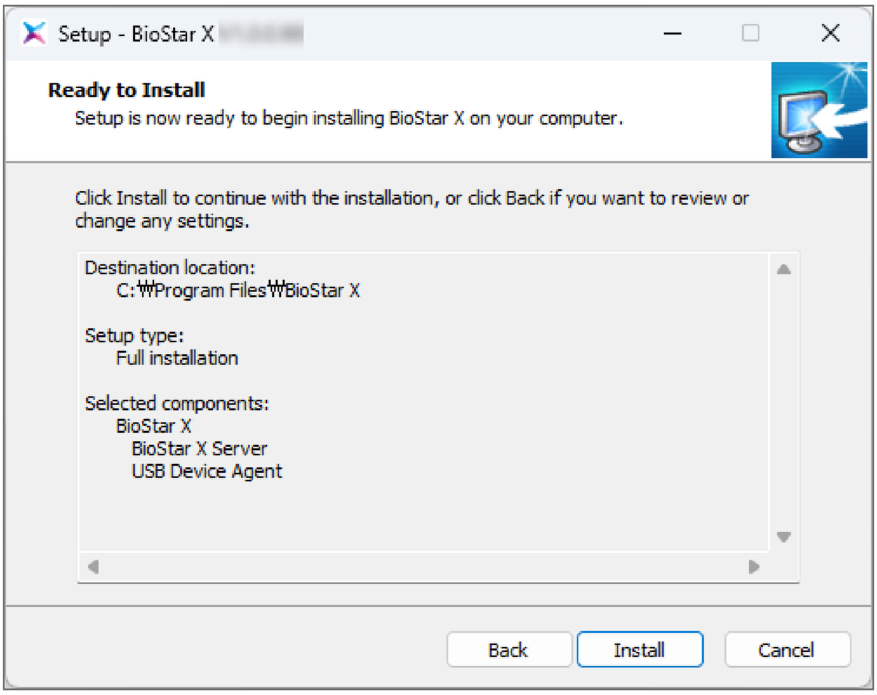
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Full installation

- ☑ BioStar X 2,979.4 MB
  - ☑ BioStar X Server 2,979.4 MB
  - ☑ USB Device Agent

Current selection requires at least 2.97 GB of disk space.

14. When all preparations for installation are complete, click the **Install** button.



Ready to Install

Setup is now ready to begin installing BioStar X on your computer.

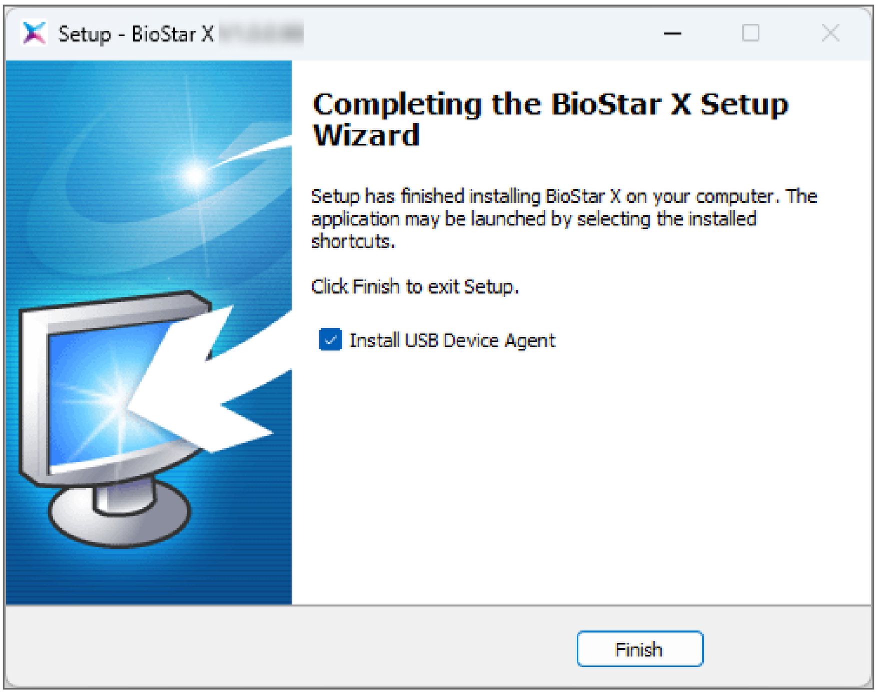
Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:₩Program Files₩BioStar X

Setup type:
Full installation

Selected components:
BioStar X
BioStar X Server
USB Device Agent

15. Select whether to install additional programs and click the **Finish** button.



Completing the BioStar X Setup Wizard

Setup has finished installing BioStar X on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

☑ Install USB Device Agent

16. Complete the installation of **USB Device Agent** by following the instructions on the installation screen.

INFO

- In the downloaded file name, X.Y.Z is the version information and BB is the build number.
- The administrator account password is used when logging in for the first time after installing **BioStar X**.
- The root account password for the database is used as the initial password for AC, TA, and Video DB.
- The storage path for the encryption key can be changed. If you modify or move the encryption key file after changing the path, a system error may occur.
- When **BioStar X** is deleted, the encryption key file is also deleted.
- The provided USB Device Agent certificate can only be applied to the local network.
- If another program is using port 443, the BioStar X Setting program runs automatically and allows you to change the port number. For details on changing the port number, refer to the following.
- For more information about changing database settings, refer to the following.

WARNING

- Be careful not to lose the administrator or root account password for the database.
- If you lose the password, version upgrade and DB backup/restore may not be possible.

Upgrade

This document provides a step-by-step guide on how to upgrade BioStar 2 to **BioStar X**. Check the system requirements and precautions before starting the upgrade.

Before starting

Check the following before upgrading from **BioStar 2** to **BioStar X**.

Minimum requirements

- If you are in an environment of BioStar 2 v2.9.11 or higher, you can upgrade to **BioStar X**.
  - If you are using a version of BioStar 2 lower than v2.6.4, you must upgrade sequentially up to v2.9.11 before upgrading. For instructions on upgrading BioStar 2 step-by-step, refer to the **BioStar 2 Admin Guide**.
  - You cannot upgrade on versions of BioStar 2 below v2.9.10.
- If the following devices are connected to BioStar 2, the upgrade to **BioStar X** is not supported.
  - XPass S2, XPass, BioEntry W, BioEntry Plus, BioLite Net

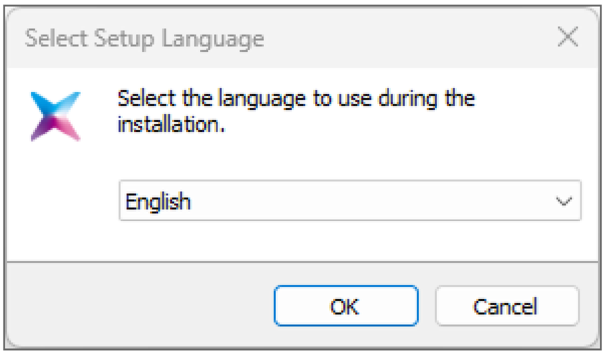
License

- You must contact your dealer to prepare at least one BioStar X license before upgrading to **BioStar X**.
- A different licensing policy applies when upgrading to **BioStar X** compared to BioStar 2.
- If you upgrade while having an Advanced or higher grade license of BioStar 2 AC license activated, the following service features and settings will be deleted.
  - Graphic Map
  - Cloud
- To use the BioStar 2 T&A service on **BioStar X**, you must purchase the **BioStar X T&A** license separately.

Upgrade installation guide

1. Go to the Suprema Download Center, log in, and download the installation package (*BioStar X Setup.X.Y.Z.BB.exe*).
2. Run the downloaded installation file.

3. Select the language to use and select the **OK** button.

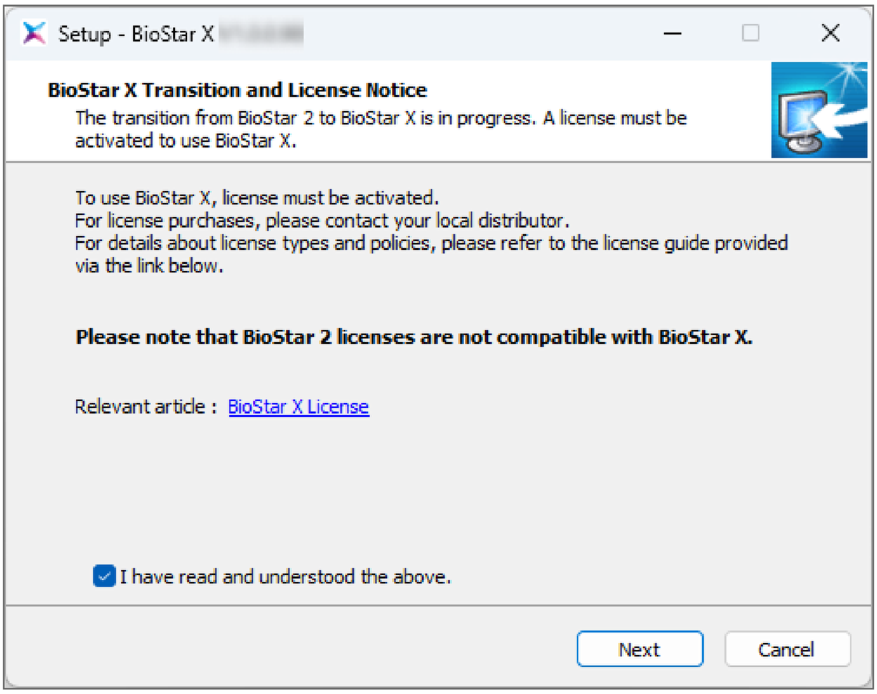


Select Setup Language

Select the language to use during the installation.

English

4. Agree to the licensing policy of transitioning from BioStar 2 to **BioStar X**. Click the checkbox and select the **Next** button.



Setup - BioStar X

BioStar X Transition and License Notice

The transition from BioStar 2 to BioStar X is in progress. A license must be activated to use BioStar X.

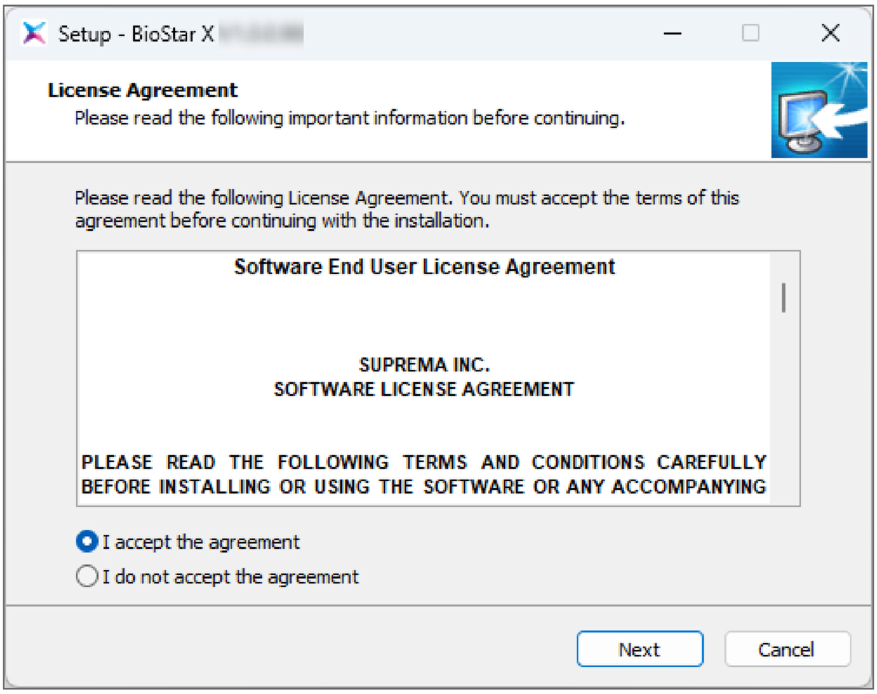
To use BioStar X, license must be activated.
For license purchases, please contact your local distributor.
For details about license types and policies, please refer to the license guide provided via the link below.

Please note that BioStar 2 licenses are not compatible with BioStar X.

Relevant article : BioStar X License

☑ I have read and understood the above.

5. To continue the installation, select **I accept the agreement** and click the **Next** button.



Setup - BioStar X [redacted]

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

Software End User License Agreement

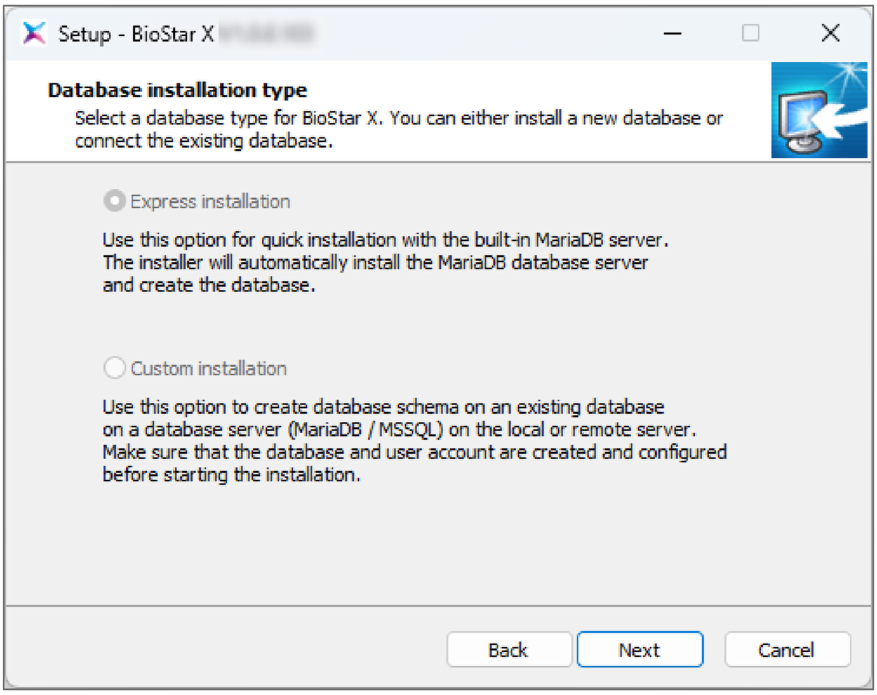
SUPREMA INC.
SOFTWARE LICENSE AGREEMENT

PLEASE READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE INSTALLING OR USING THE SOFTWARE OR ANY ACCOMPANYING

● I accept the agreement

○ I do not accept the agreement

6. When upgrading from BioStar 2, the existing database will be connected to proceed with the installation. Click the **Next** button.



Setup - BioStar X [redacted]

Database installation type

Select a database type for BioStar X. You can either install a new database or connect the existing database.

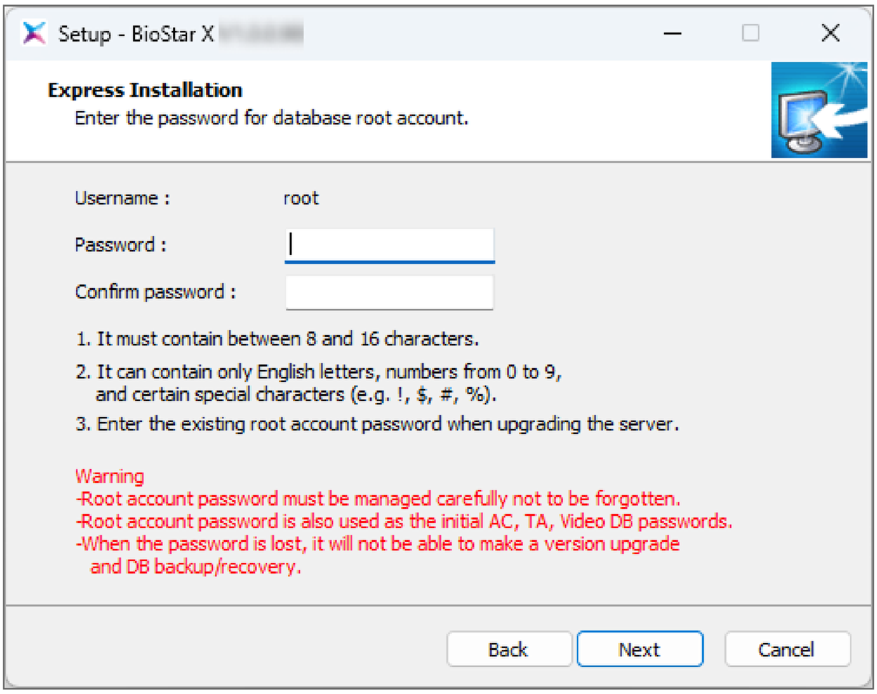
● Express installation

Use this option for quick installation with the built-in MariaDB server. The installer will automatically install the MariaDB database server and create the database.

○ Custom installation

Use this option to create database schema on an existing database on a database server (MariaDB / MSSQL) on the local or remote server. Make sure that the database and user account are created and configured before starting the installation.

7. Enter the root account password of the existing database and click the **Next** button.



Express Installation
Enter the password for database root account.

Username : root

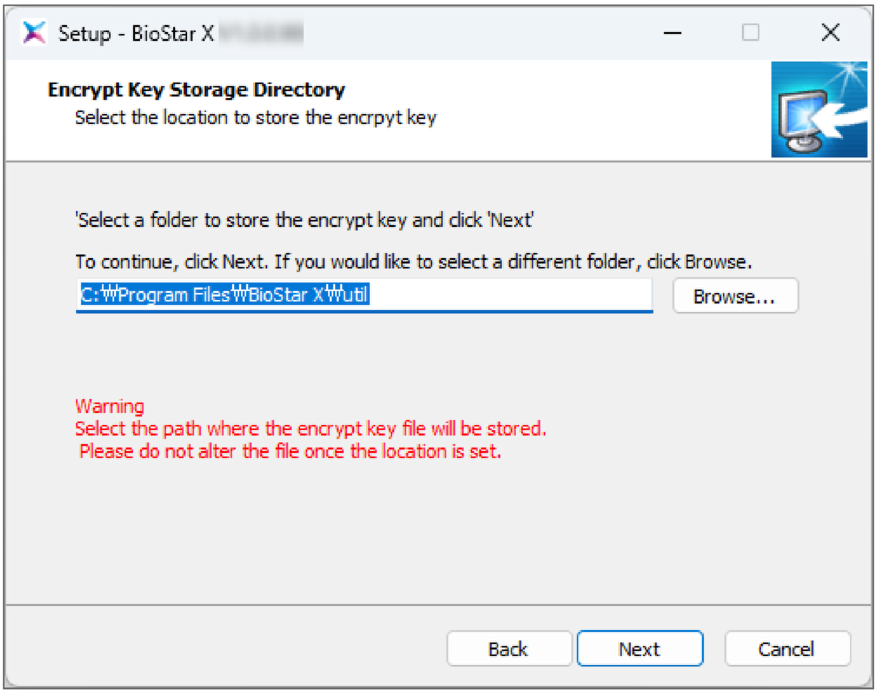
Password :

Confirm password :

1. It must contain between 8 and 16 characters.
2. It can contain only English letters, numbers from 0 to 9, and certain special characters (e.g. !, $, #, %).
3. Enter the existing root account password when upgrading the server.

Warning
-Root account password must be managed carefully not to be forgotten.
-Root account password is also used as the initial AC, TA, Video DB passwords.
-When the password is lost, it will not be able to make a version upgrade and DB backup/recovery.

8. Set the path to store the encryption key and click the **Next** button.



Encrypt Key Storage Directory
Select the location to store the encrpyt key

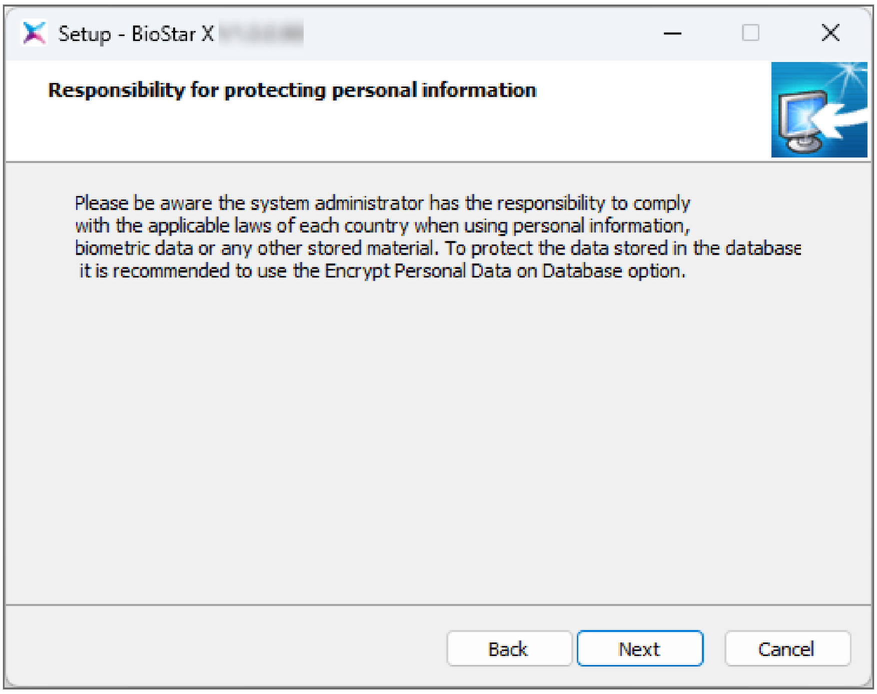
'Select a folder to store the encrypt key and click 'Next'

To continue, click Next. If you would like to select a different folder, click Browse.

C:₩Program Files₩BioStar X₩util

Warning
Select the path where the encrypt key file will be stored.
Please do not alter the file once the location is set.

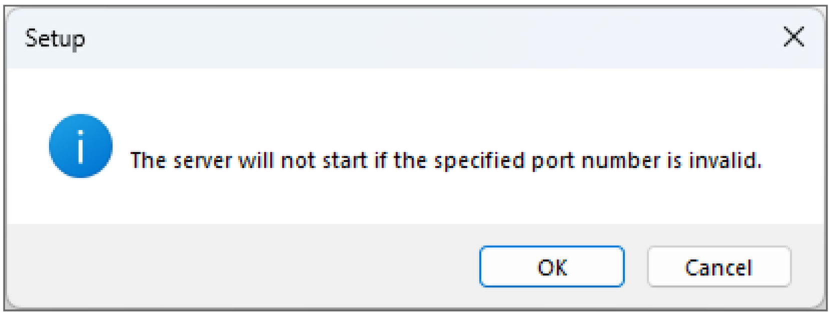
9. Read the information about the management and responsibility of personal information stored in the database, and click the **Next** button to continue the installation.



Responsibility for protecting personal information

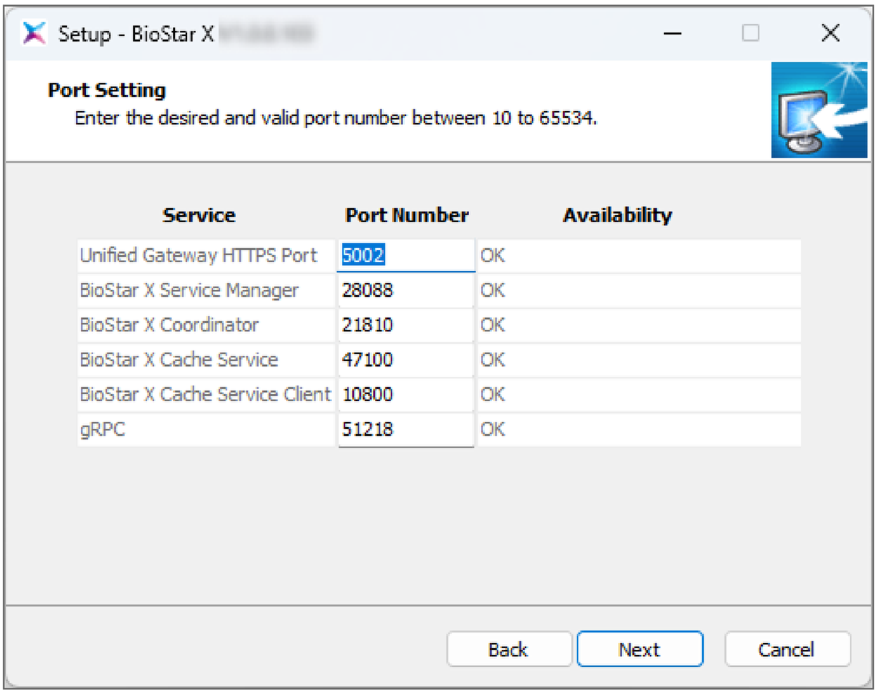
Please be aware the system administrator has the responsibility to comply with the applicable laws of each country when using personal information, biometric data or any other stored material. To protect the data stored in the database it is recommended to use the Encrypt Personal Data on Database option.

10. If a port number related message appears, click **OK**.



The server will not start if the specified port number is invalid.

11. Set the port for **BioStar X** communication and click the **Next** button.

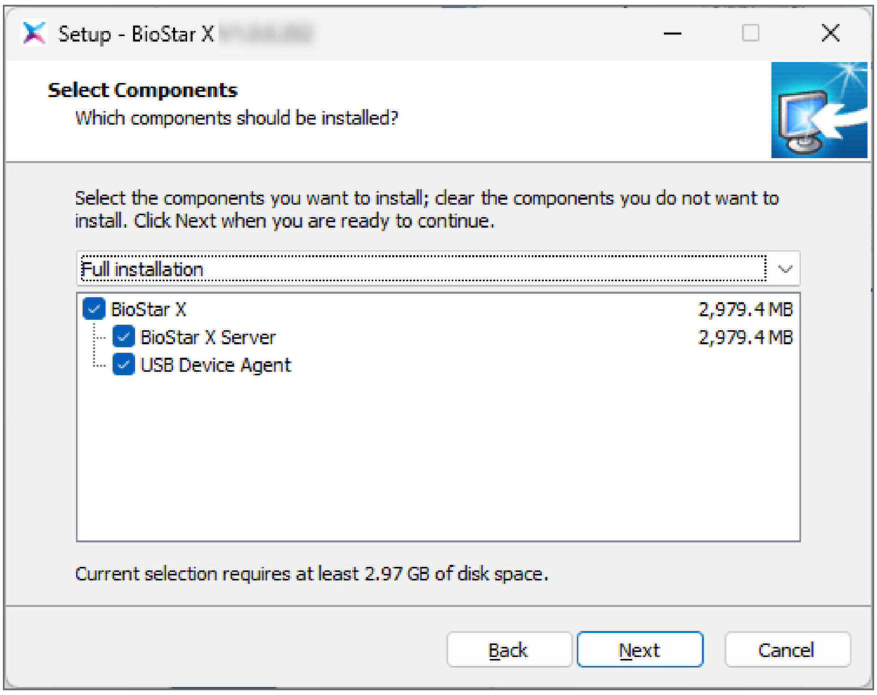


Port Setting

Enter the desired and valid port number between 10 to 65534.

Service	Port Number	Availability
Unified Gateway HTTPS Port	5002	OK
BioStar X Service Manager	28088	OK
BioStar X Coordinator	21810	OK
BioStar X Cache Service	47100	OK
BioStar X Cache Service Client	10800	OK
gRPC	51218	OK

12. Select the components of **BioStar X** and click the **Next** button. If you select **USB Device Agent**, the USB Agent and driver for using BioMini, BioMini Plus 2, BioMini Slim 2, and DUALi DE-620 will be installed together.



Select Components

Which components should be installed?

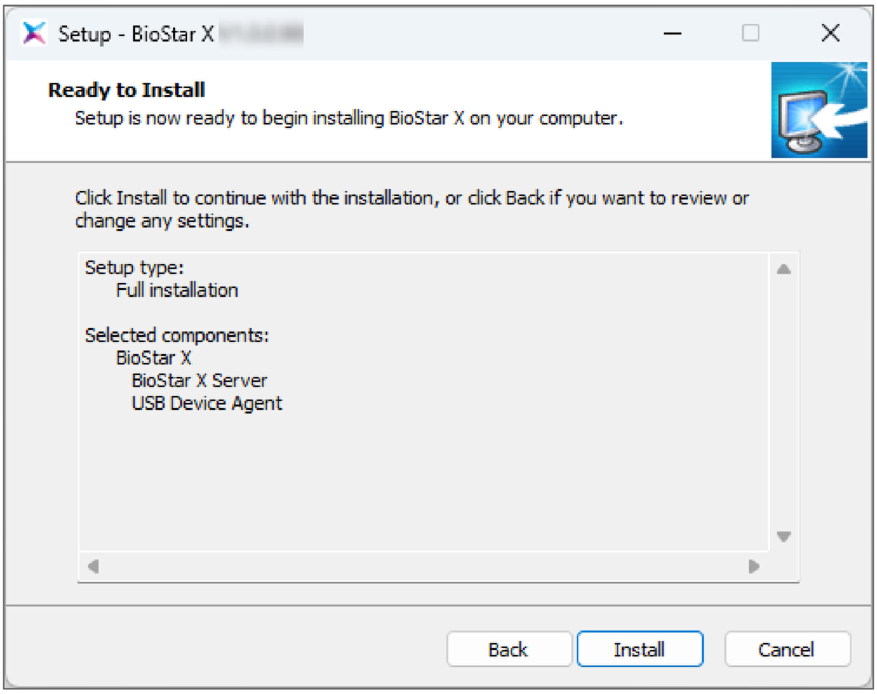
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Full installation

☑ BioStar X	2,979.4 MB
☑ BioStar X Server	2,979.4 MB
☑ USB Device Agent	

Current selection requires at least 2.97 GB of disk space.

13. When all preparations for installation are complete, click the **Install** button.



Setup - BioStar X

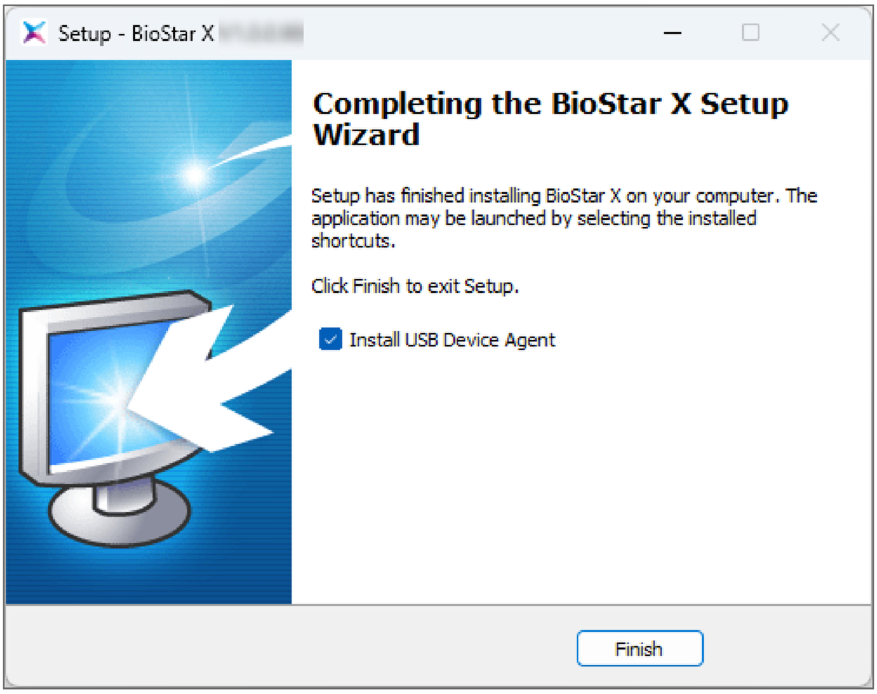
Ready to Install

Setup is now ready to begin installing BioStar X on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Setup type:
    Full installation

Selected components:
    BioStar X
        BioStar X Server
        USB Device Agent
```

14. Select whether to install additional programs and click the **Finish** button.



Setup - BioStar X

Completing the BioStar X Setup Wizard

Setup has finished installing BioStar X on your computer. The application may be launched by selecting the installed shortcuts.

Click Finish to exit Setup.

☑ Install USB Device Agent

15. Complete the installation of **USB Device Agent** by following the instructions on the installation screen.

ⓘ **INFO**

- In the downloaded file name, X.Y.Z is the version information and BB is the build number.
- The administrator account password is used when logging in for the first time after installing **BioStar X**.
- The root account password for the database is used as the initial password for AC, TA, and Video DB.
- The storage path for the encryption key can be changed. If you modify or move the encryption key file after changing the path, a system error may occur.
- When **BioStar X** is deleted, the encryption key file is also deleted.
- The provided USB Device Agent certificate can only be applied to the local network.
- If another program is using port 443, the BioStar X Setting program runs automatically and allows you to change the port number. For details on changing the port number, refer to the following.
- For more information about changing database settings, refer to the following.

⚠ **WARNING**

- Be careful not to lose the administrator or root account password for the database.
- If you lose the password, version upgrade and DB backup/restore may not be possible.

Install Communication Server

This document explains how to install the **Communication Server** of **BioStar X**.

The communication server is a server dedicated to communication with access control devices. It helps to manage many devices reliably by installing separately from the main server. A single communication server can connect up to 1,000 devices, and you can add multiple communication servers as needed.

Before starting

Before installing the communication server, check the following items.

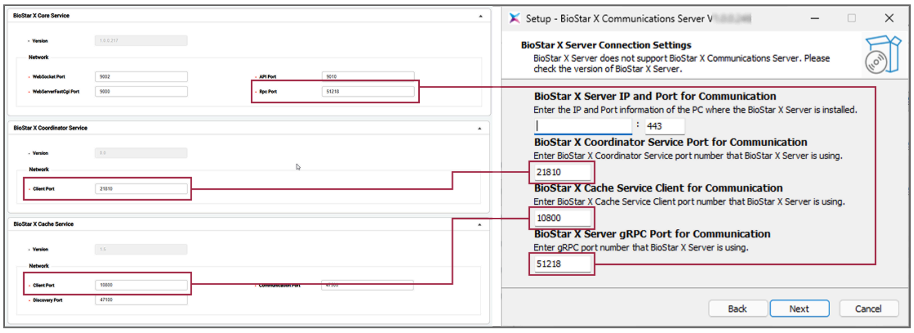
- The communication server cannot be installed on the same server as the **BioStar X** server.
- The communication server can only be installed on a 64-bit operating system. For more information on the system minimum requirements, refer to the following.
- A multi-communication server license is required to install and connect the communication server. For more information on licensing policy, refer to the following.

Pre-installation checks

Before installing the communication server, run **BioStar X Service Manager** to check the information needed during installation.

1. Click **Start** ⊞ → **BioStar X** → **BioStar X Service Manager** on Windows.
2. The **BioStar X Service Manager** window appears.
3. Click **SERVICE SETTINGS**.

Below is the information required when installing the communication server. Review and prepare each item.



BioStar X Core Service

- Version: 1.0.0.217
- Network
- WebSocket Port: 9002
- API Port: 9010
- WebServerFastCgi Port: 9000
- Rpc Port: 51218

BioStar X Coordinator Service

- Version: 0.0
- Network
- Client Port: 21810

BioStar X Cache Service

- Version: 1.5
- Network
- Client Port: 10800
- Communication Port
- Discovery Port: 47100

Setup - BioStar X Communications Server V

BioStar X Server Connection Settings

BioStar X Server does not support BioStar X Communications Server. Please check the version of BioStar X Server.

BioStar X Server IP and Port for Communication

Enter the IP and Port information of the PC where the BioStar X Server is installed.

: 443

BioStar X Coordinator Service Port for Communication

Enter BioStar X Coordinator Service port number that BioStar X Server is using.

21810

BioStar X Cache Service Client for Communication

Enter BioStar X Cache Service Client port number that BioStar X Server is using.

10800

BioStar X Server gRPC Port for Communication

Enter gRPC port number that BioStar X Server is using.

51218

BioStar X Service Manager	Information required for communication server installation
BioStar X Core Service → RPC Port	**BioStar X Server gRPC Port for Communication**
BioStar X Coordinator Service → Client Port	**BioStar X Coordinator Service Port for**

BioStar X Service Manager	Information required for communication server installation
	Communication
BioStar X Cache Service → Client Port	**BioStar X Cache Service Client for Communication**

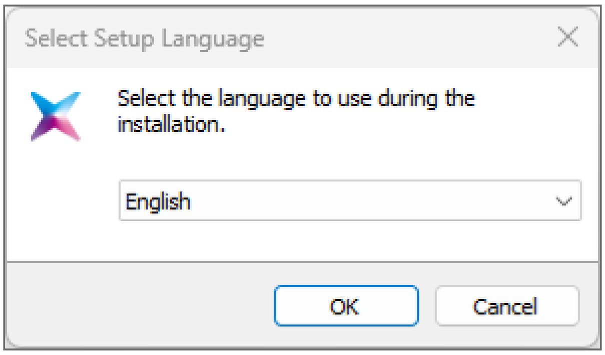
ⓘ **INFO**

For more information on **SERVICE SETTINGS**, refer to the following.

Installation guide

Follow the steps below to install the communication server.

1. Access the Suprema Download Center, log in, and download the installation package (*BioStar X Communications Server.X.Y.X.BB.exe*).
2. Run the downloaded installation file.
3. Select the language to use and select the **OK** button.

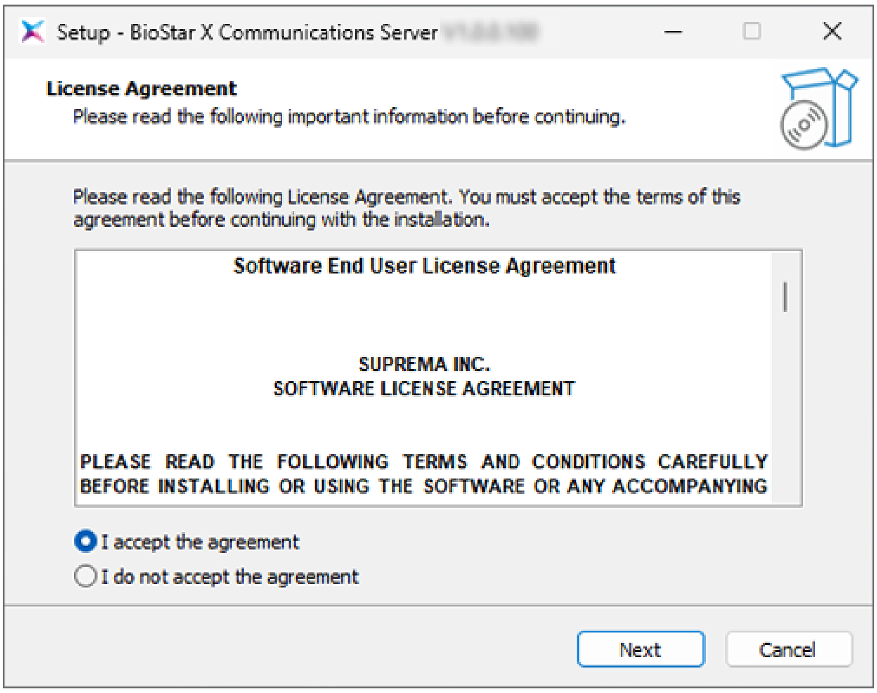


Select Setup Language

Select the language to use during the installation.

English

4. To continue the installation, select **I accept the agreement** and click the **Next** button.



Setup - BioStar X Communications Server

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

Software End User License Agreement

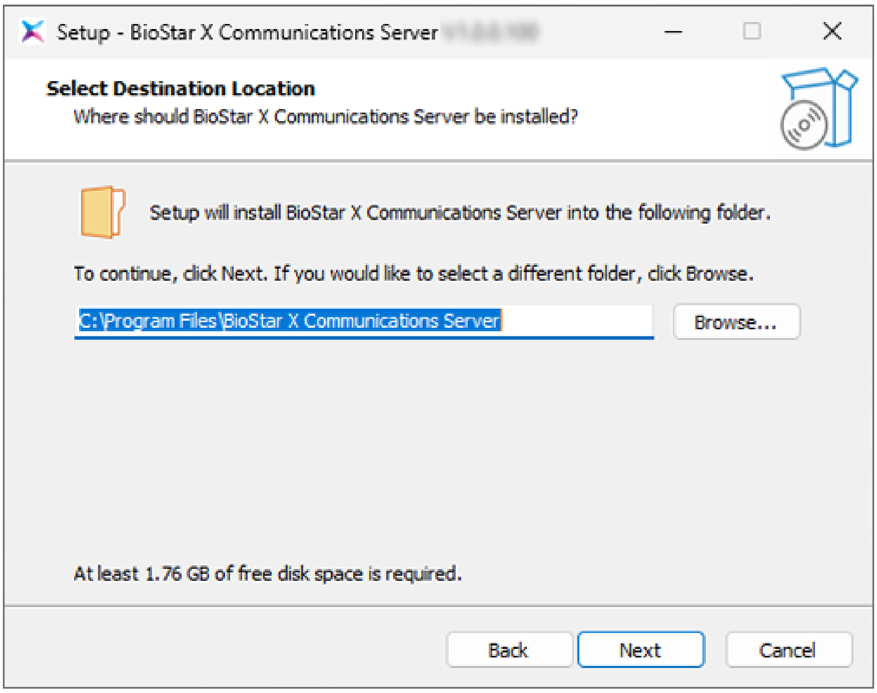
SUPREMA INC.
SOFTWARE LICENSE AGREEMENT

PLEASE READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE INSTALLING OR USING THE SOFTWARE OR ANY ACCOMPANYING

● I accept the agreement

○ I do not accept the agreement

5. Set the path where the communication server will be installed and click **Next**.



Setup - BioStar X Communications Server

Select Destination Location

Where should BioStar X Communications Server be installed?

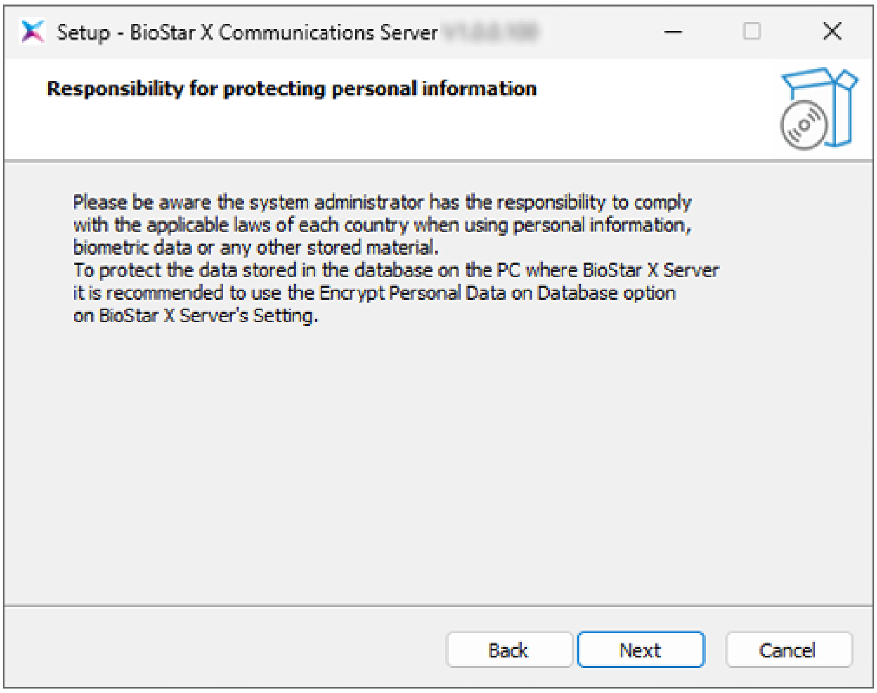
Setup will install BioStar X Communications Server into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\BioStar X Communications Server

At least 1.76 GB of free disk space is required.

6. Review the permissions and responsibilities regarding personal information and click **Next** to continue the installation.

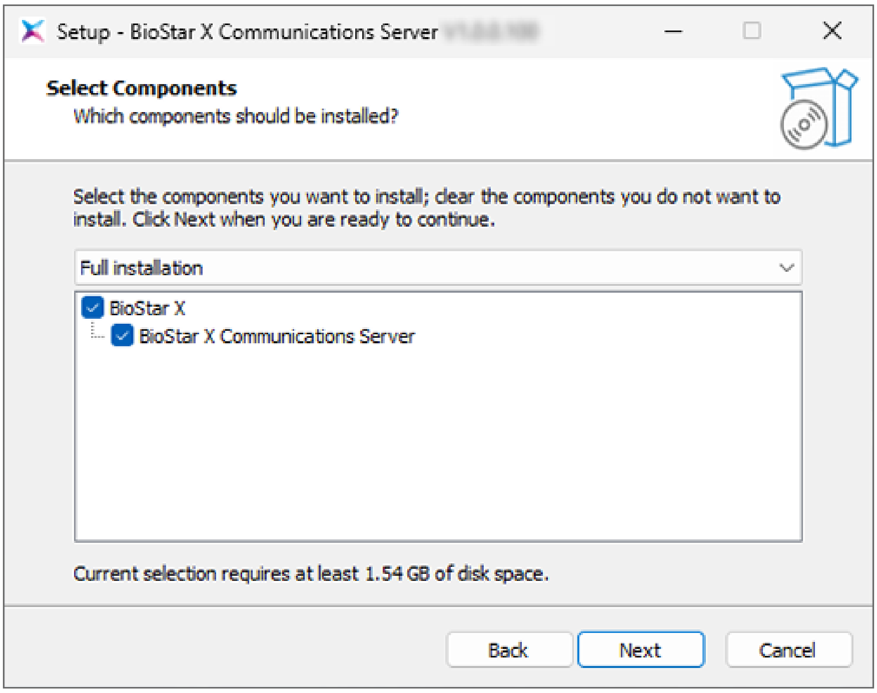


Setup - BioStar X Communications Server

Responsibility for protecting personal information

Please be aware the system administrator has the responsibility to comply
with the applicable laws of each country when using personal information,
biometric data or any other stored material.
To protect the data stored in the database on the PC where BioStar X Server
it is recommended to use the Encrypt Personal Data on Database option
on BioStar X Server's Setting.

7. Select the components of the communication server and click **Next**.



Setup - BioStar X Communications Server

Select Components

Which components should be installed?

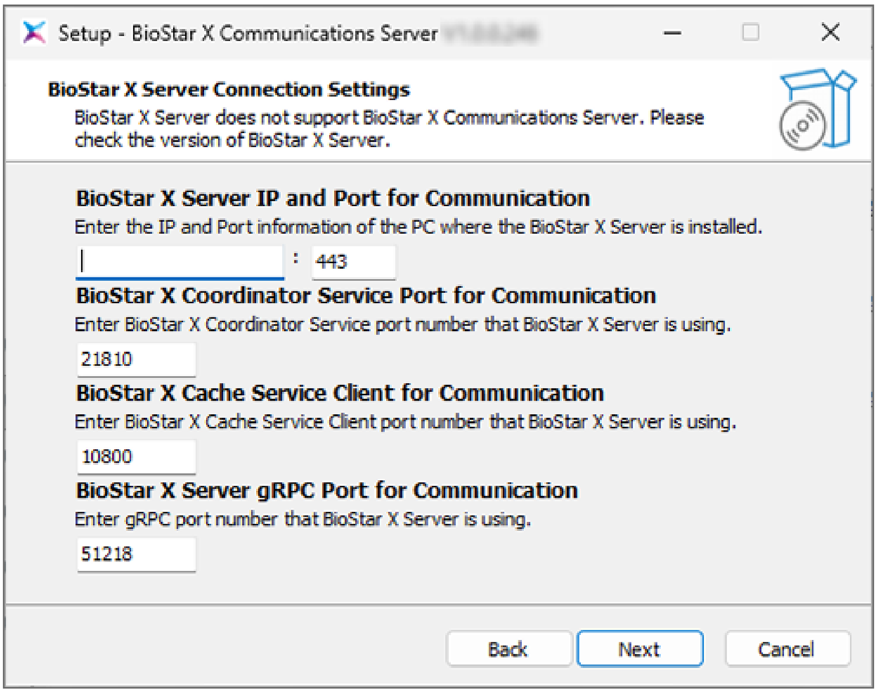
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Full installation

- ☑ BioStar X
  - ☑ BioStar X Communications Server

Current selection requires at least 1.54 GB of disk space.

8. Enter the IP address and port number of the **BioStar X** server, and input details for connection to the **BioStar X** server. Complete your settings and click **Next**.



Setup - BioStar X Communications Server

BioStar X Server Connection Settings

BioStar X Server does not support BioStar X Communications Server. Please check the version of BioStar X Server.

BioStar X Server IP and Port for Communication

Enter the IP and Port information of the PC where the BioStar X Server is installed.

: 443

BioStar X Coordinator Service Port for Communication

Enter BioStar X Coordinator Service port number that BioStar X Server is using.

21810

BioStar X Cache Service Client for Communication

Enter BioStar X Cache Service Client port number that BioStar X Server is using.

10800

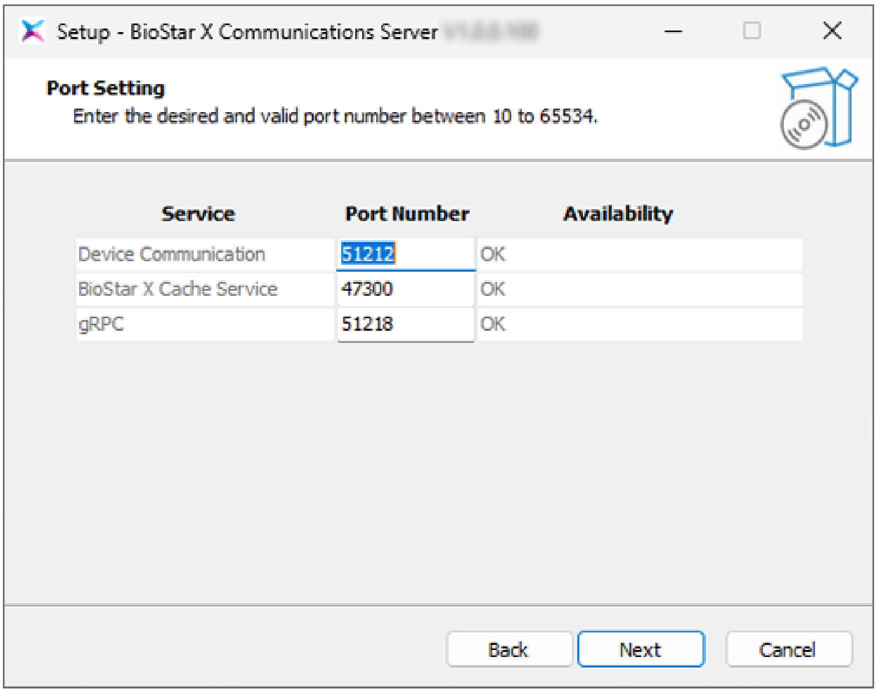
BioStar X Server gRPC Port for Communication

Enter gRPC port number that BioStar X Server is using.

51218

For more information on each entry item, refer to the following.

9. Set the port for communication and click **Next**.



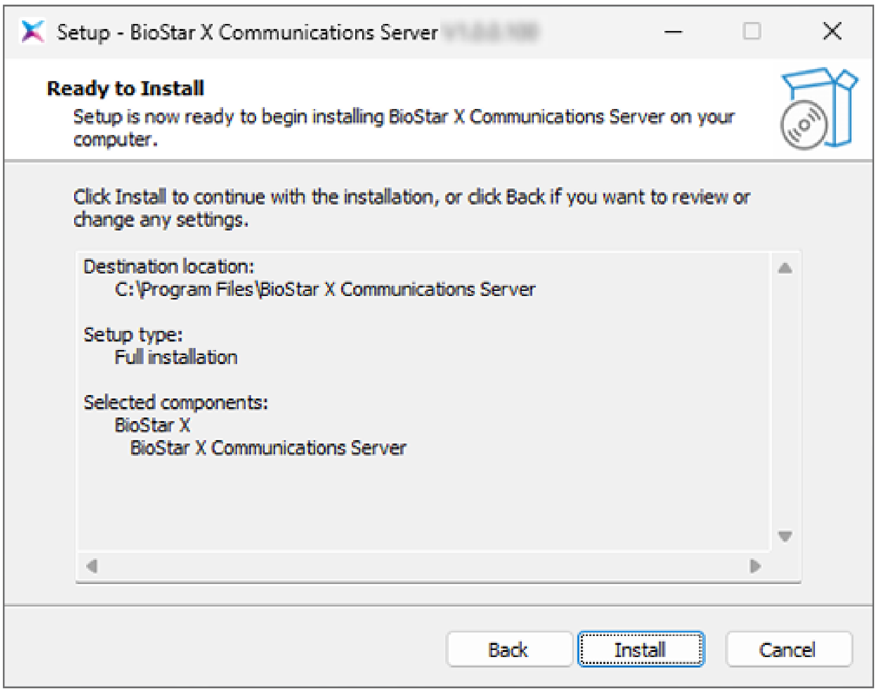
Setup - BioStar X Communications Server

Port Setting

Enter the desired and valid port number between 10 to 65534.

Service	Port Number	Availability
Device Communication	51212	OK
BioStar X Cache Service	47300	OK
gRPC	51218	OK

10. When all preparations for installation are complete, click the **Install** button. Proceed with the installation.



Setup - BioStar X Communications Server [redacted]

Ready to Install

Setup is now ready to begin installing BioStar X Communications Server on your computer.

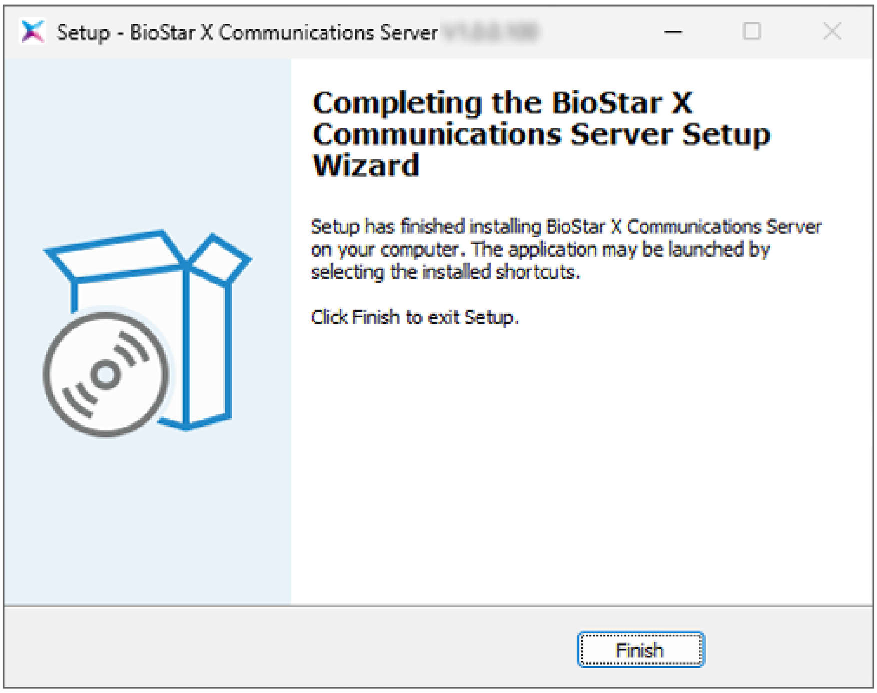
Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:\Program Files\BioStar X Communications Server

Setup type:
Full installation

Selected components:
BioStar X
BioStar X Communications Server

11. Check the installation completion message and click **Finish**.



Setup - BioStar X Communications Server [redacted]

Completing the BioStar X Communications Server Setup Wizard

Setup has finished installing BioStar X Communications Server on your computer. The application may be launched by selecting the installed shortcuts.

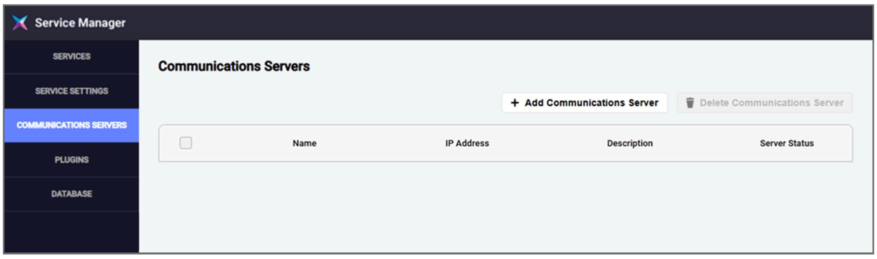
Click Finish to exit Setup.

Complete the installation of the communication server. Once the installation is complete, verify the connection between the communication server and the **BioStar X** main server.

Post-installation checks

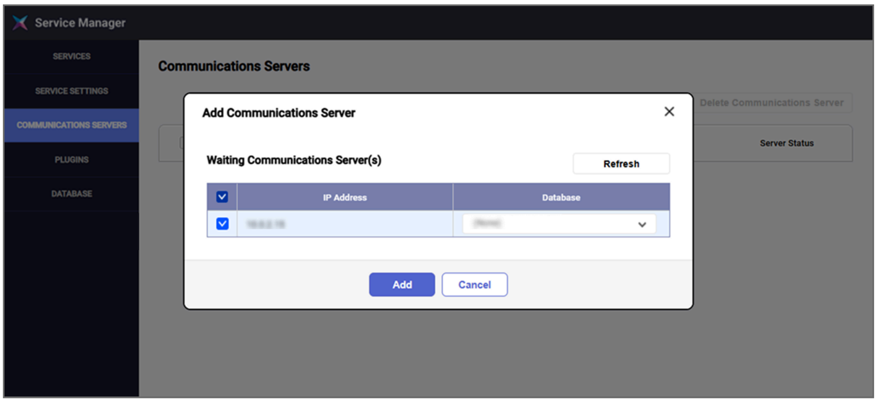
After completing the installation of the communication server, you need to connect the main server and the communication server through **BioStar X Service Manager**.

1. Click **Start** → **BioStar X** → **BioStar X Service Manager** on Windows.
2. The **BioStar X Service Manager** window appears.
3. In the left sidebar, click the **COMMUNICATIONS** menu.



□	Name	IP Address	Description	Server Status

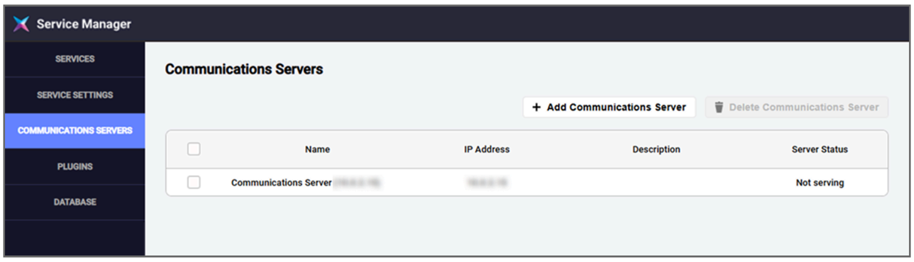
4. Click the **Add Communication Server** button in the upper right corner of the screen.
5. When the **Add Communication Server** window appears, check the box for the item that matches the IP address of the installed communication server, and select the database to use from the **Database** column.



☑	IP Address	Database
☑	[illegible]	(None)

6. Click the **Add** button.

In the communication server list, check if the **Server Status** column of the added communication server is in **Connected** status.



□	Name	IP Address	Description	Server Status
□	Communications Server [illegible]	[illegible]		Not serving

INFO

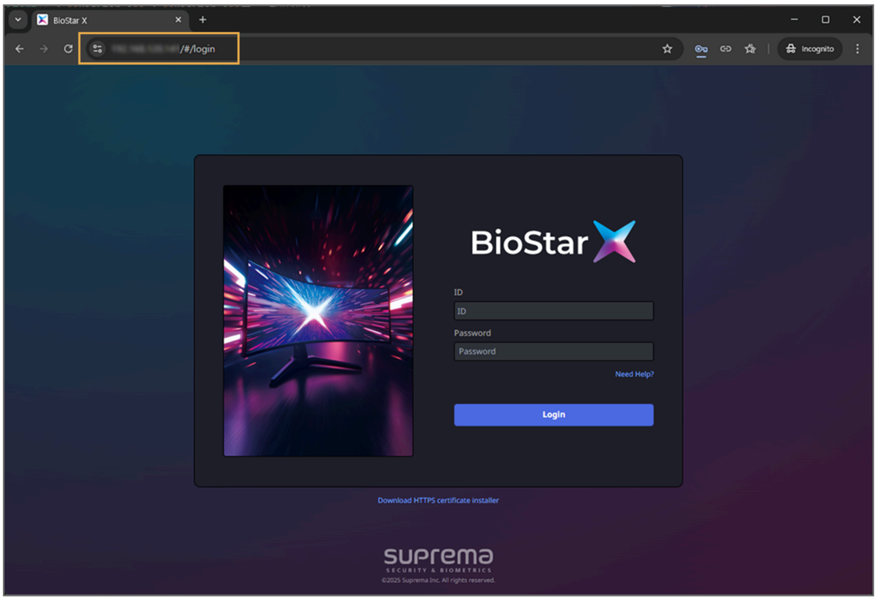
- The **COMMUNICATIONS** menu can be used when the multi-communication server license is activated. For more information on licensing policy, refer to the following.
- To delete the communication server, check the box of the server to be deleted in the list and click the **Delete Communication Server** button in the upper right corner of the screen.
- When adding a communication server, you can also add a secondary database to reduce the load on the main server. For more information on adding a secondary database, refer to the following.

How to Log in

If you have completed the installation of **BioStar X** through the installation package, access it via a web browser to check if it is functioning properly. **BioStar X** provides a web-based service that allows access anytime and anywhere.

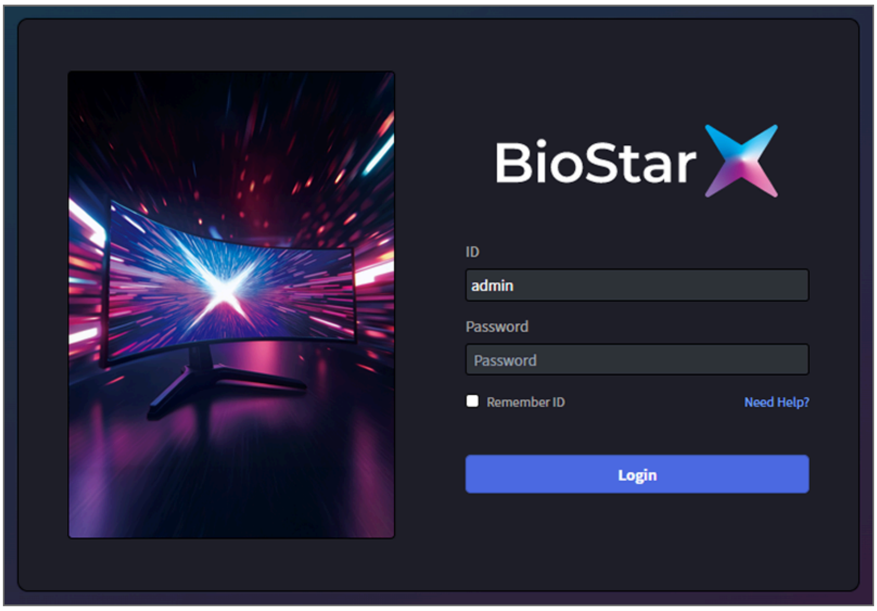
Log in from a web browser

1. Click **Start** → **BioStar X** → **BioStar X** on Windows.
2. Connect to **BioStar X** via a web browser.



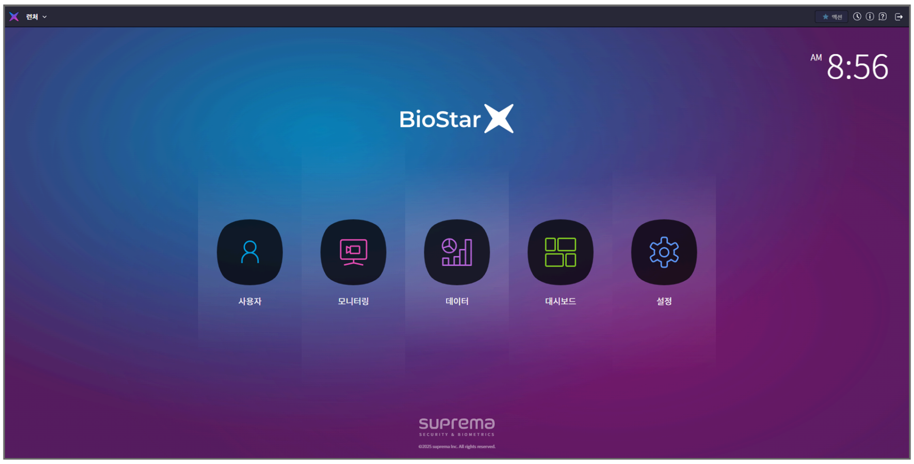
- Check the access address of **BioStar X** in the web browser's address bar.
- If you installed **BioStar X** on another PC, enter the IP address of that PC. e.g. https://192.168.0.1
- Do not use 'localhost' as the **BioStar X** access address.
- **BioStar X** processes all requests through the Unified Gateway. Thus, web access and API calls are made through the Unified Gateway port (default 443).

3. When the login screen appears, log in with the administrator account.



- The admin ID is **admin**.
- If you see a **Not Secure** warning in the web browser's address bar, you need to install the HTTPS certificate. For more information on installing the certificate, refer to the following.

After logging in, you can view the Launcher screen.



INFO

- It is recommended to use a browser version of Chrome 100 or higher.
- The external IP address of the PC where **BioStar X** is installed can be checked by visiting this link.
- **BioStar X** uses **port 443** by default. If there is a program using port **443**, close it and try connecting again. If you cannot close the program, run the **BioStar X Service Manager** to change the port number. For more information, refer to the following.

Register License Key

If you purchased the BioStar X license, you can register the license key and use more features.

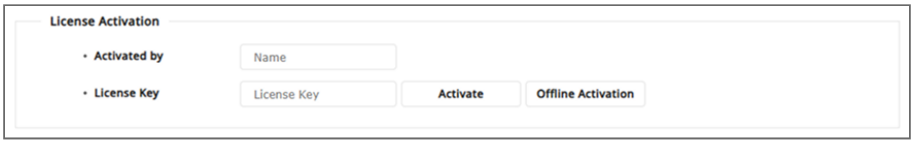
Go to **License** → **BioStar X License** menu.

The method to activate **BioStar X License** varies depending on your network environment. Check your network status and activate your license according to the provided instructions.

> ⓘ **INFO**
>
> - For more information on the **License** menu, refer to the following.
> - For more information about the license policy, refer to the following.
> - For more information about license error codes, refer to the following link.

Registering in an online state

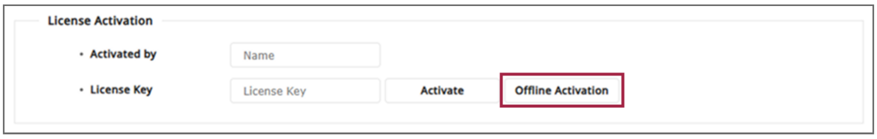
To activate the **BioStar X** license while online with an internet connection, enter your name and the received license key, then click **Activate**.



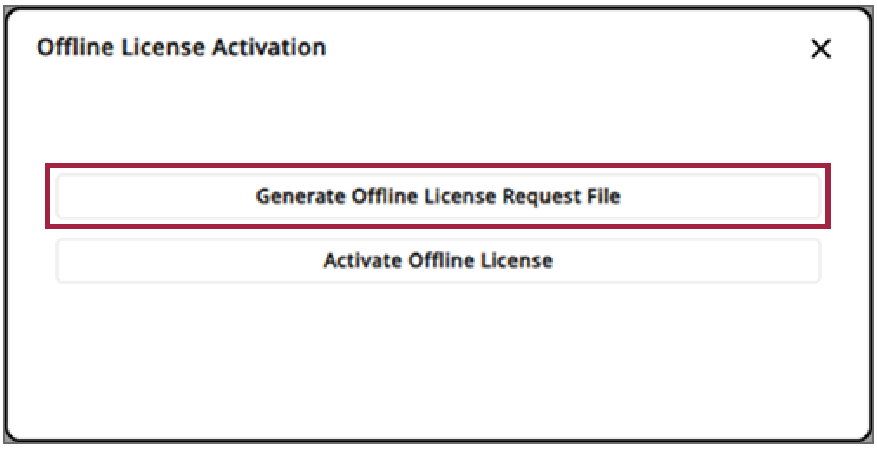
Registering in offline

To activate the **BioStar X** license in a closed network environment or in an offline state with limited internet access, please follow the instructions below.

1. In the **License Activation** section, click **Offline Activation**.

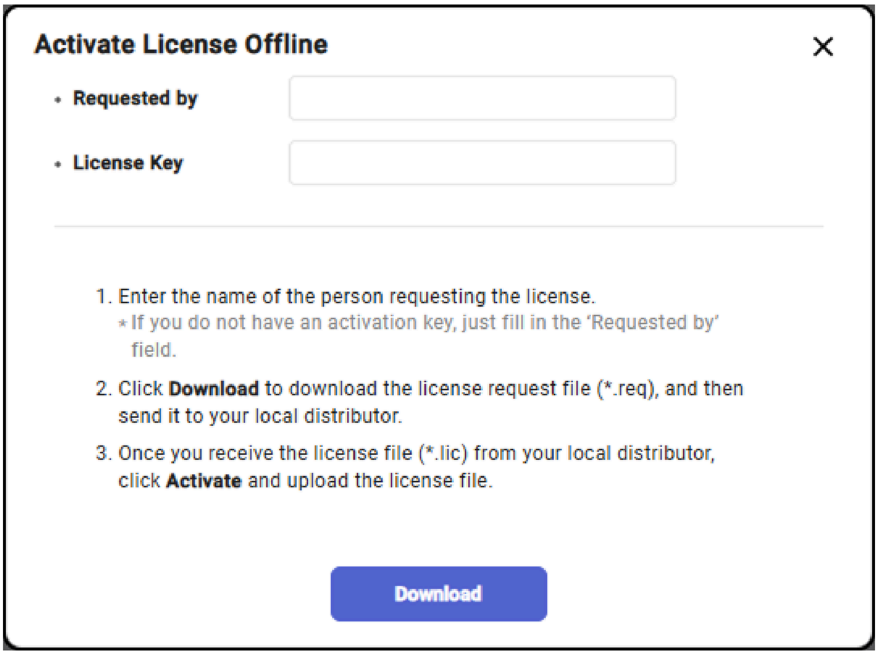


2. When the **Activate License Offline** window appears, click **Generate Offline License Request File**.



Offline License Activation

3. When the dialog appears, enter **Requested by** and **License Key**.



Activate License Offline

- Requested by
- License Key

1. Enter the name of the person requesting the license.
   * If you do not have an activation key, just fill in the 'Requested by' field.
2. Click **Download** to download the license request file (*.req), and then send it to your local distributor.
3. Once you receive the license file (*.lic) from your local distributor, click **Activate** and upload the license file.

4. Click the **Download** button to download the license request file (**.req*).

5. Send it to the purchase location.

Once you receive the license file (**.lic*) from the purchase location, click the **Offline License Activation** button to upload the license file.

> ⓘ **INFO**
>
> If you do not have a license key, only enter **Requested by**.

Initial Setup Guide

Step-by-step settings are provided to ensure the proper operation of **BioStar X** after initial installation. Follow each step sequentially to build an efficient access control environment.

1 Register device

Register a device to connect to **BioStar X**. Configure separate authentication modes based on the devices or assign administrators to each device.

Additionally, set actions based on various events generated by the device (such as authentication failure, duress fingerprint authentication, anti-passback violations, etc.).

- Manage Device Groups
- Register Device
- Register Wiegand Credentials
- Register Slave
- Device Settings

2 Door enrollment and settings

Register the door information where the devices are installed. Configure relay, anti-passback, dual authentication, alarms, and more.

- Manage Door Group
- Register Door

3 Access level settings

Access levels are created by combining door and schedule information, allowing multiple doors and schedules to be registered under a single access level.

Manage Access Levels

4 Access group settings

Access groups are created by combining access levels (doors, schedules) and user information, enabling multiple access levels and users to be registered under a single access group.

Manage Access Groups

5

Register users

Register information such as user information and credentials to be used for access control. User information can be registered directly on the device or in **BioStar X**. In addition, user information registered on the device can be imported to **BioStar X**, or user information registered in **BioStar X** can be sent to the device.

- Manage User Groups
- Manage Users
- Register Users
- Enroll User's Credential

6

Advanced access control settings

Configure anti-passback and fire alarm, allowing settings for local and global.

- Advanced Access Control Settings
- Monitor Map

> **INFO**
>
> Available only with an **Advanced** or higher license. For more information about the license policy, refer to the following.

7

Monitoring

Manage the access control system in real time through various monitoring features such as doors, devices, and events.

- Monitor Doors
- Monitor Device
- Monitor Event

Server Management

After installing BioStar X, users can efficiently operate the system through various server management features. This document guides you on the server management features of BioStar X.

Start and Stop Server

Learn how to start and stop services of the BioStar X server using BioStar X Service Manager.

Service Settings

In the Service Settings of BioStar X Service Manager, you can configure and manage the core services of the system.

Change the Port

Guide to change the port when the default port (443) of BioStar X is unavailable.

Change the Database

Change the database setting.

Add Auxiliary Database

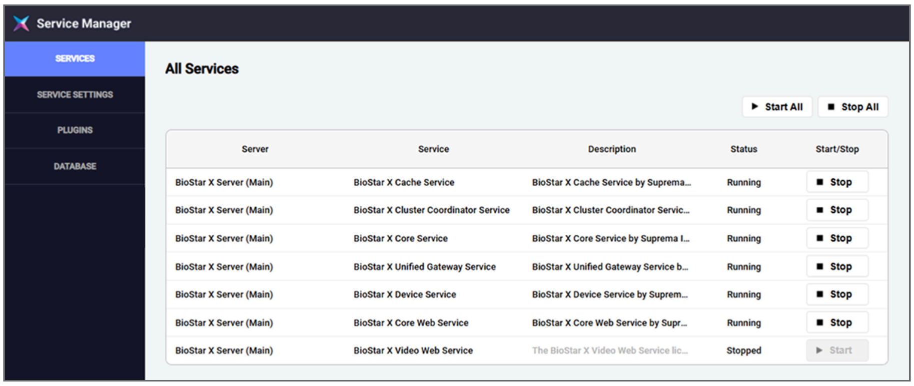
When adding a communication server, add and connect an auxiliary database to reduce the load on the main server.

Start and Stop Server

Check how to manage services of the BioStar X server using **BioStar X Service Manager**. You can start or stop individual services.

Manage BioStar X service

Provides a tool to manage the status of the **BioStar X** server. Click **Start** ⊞ → **BioStar X** → **BioStar X Service Manager** on Windows. The BioStar X Service Manager window appears.



All Services

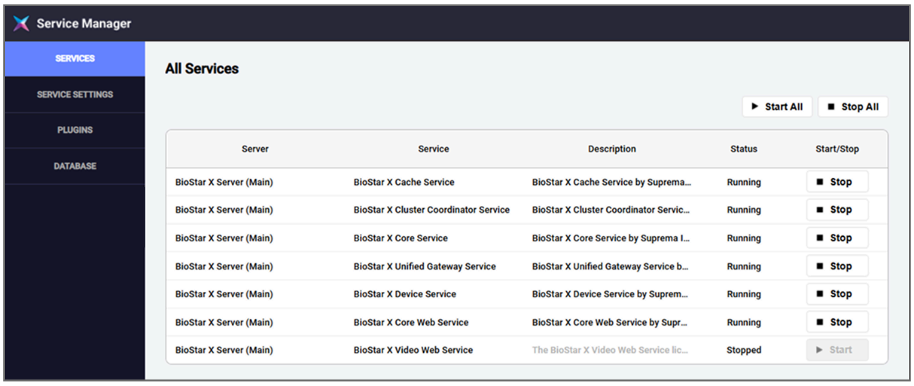
Server	Service	Description	Status	Start/Stop
BioStar X Server (Main)	BioStar X Cache Service	BioStar X Cache Service by Suprema...	Running	■ Stop
BioStar X Server (Main)	BioStar X Cluster Coordinator Service	BioStar X Cluster Coordinator Servic...	Running	■ Stop
BioStar X Server (Main)	BioStar X Core Service	BioStar X Core Service by Suprema I...	Running	■ Stop
BioStar X Server (Main)	BioStar X Unified Gateway Service	BioStar X Unified Gateway Service b...	Running	■ Stop
BioStar X Server (Main)	BioStar X Device Service	BioStar X Device Service by Suprem...	Running	■ Stop
BioStar X Server (Main)	BioStar X Core Web Service	BioStar X Core Web Service by Supr...	Running	■ Stop
BioStar X Server (Main)	BioStar X Video Web Service	The BioStar X Video Web Service lic...	Stopped	▶ Start

ⓘ **INFO**

If you do not restart, **BioStar X** may not operate properly. If you have changed the time settings of the **BioStar X** server, stop and restart the **BioStar X Core Service**.

End service

To shut down **BioStar X**, click the Stop button for individual services in the SERVICES menu.

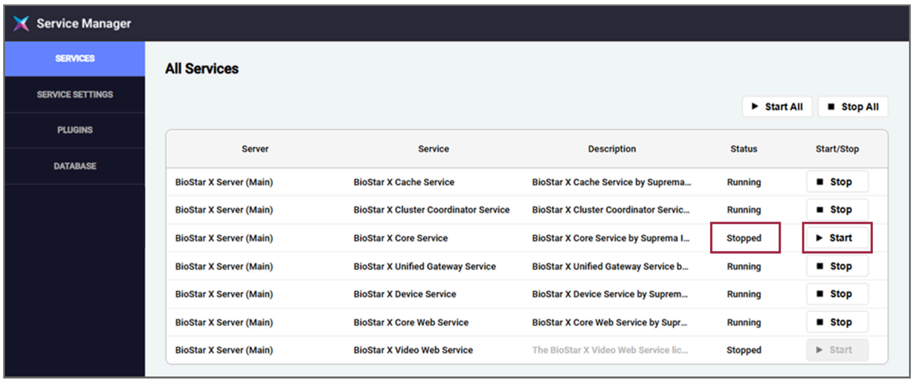


All Services

Server	Service	Description	Status	Start/Stop
BioStar X Server (Main)	BioStar X Cache Service	BioStar X Cache Service by Suprema...	Running	■ Stop
BioStar X Server (Main)	BioStar X Cluster Coordinator Service	BioStar X Cluster Coordinator Servic...	Running	■ Stop
BioStar X Server (Main)	BioStar X Core Service	BioStar X Core Service by Suprema I...	Running	■ Stop
BioStar X Server (Main)	BioStar X Unified Gateway Service	BioStar X Unified Gateway Service b...	Running	■ Stop
BioStar X Server (Main)	BioStar X Device Service	BioStar X Device Service by Suprem...	Running	■ Stop
BioStar X Server (Main)	BioStar X Core Web Service	BioStar X Core Web Service by Supr...	Running	■ Stop
BioStar X Server (Main)	BioStar X Video Web Service	The BioStar X Video Web Service lic...	Stopped	▶ Start

Start the server

To restart **BioStar X**, click Start for the service in the SERVICES menu with a Stopped status in the Status column.



All Services

Server	Service	Description	Status	Start/Stop
BioStar X Server (Main)	BioStar X Cache Service	BioStar X Cache Service by Suprema...	Running	■ Stop
BioStar X Server (Main)	BioStar X Cluster Coordinator Service	BioStar X Cluster Coordinator Servic...	Running	■ Stop
BioStar X Server (Main)	BioStar X Core Service	BioStar X Core Service by Suprema I...	Stopped	▶ Start
BioStar X Server (Main)	BioStar X Unified Gateway Service	BioStar X Unified Gateway Service b...	Running	■ Stop
BioStar X Server (Main)	BioStar X Device Service	BioStar X Device Service by Suprem...	Running	■ Stop
BioStar X Server (Main)	BioStar X Core Web Service	BioStar X Core Web Service by Supr...	Running	■ Stop
BioStar X Server (Main)	BioStar X Video Web Service	The BioStar X Video Web Service lic...	Stopped	▶ Start

Service Settings

In the **Service Settings** menu of **BioStar X Service Manager**, you can configure and manage the core services of the system. Each service is configured independently, and you can check network ports and version information.

Service Settings consists of the following major services.

- **BioStar X Core Web Service**: Web interface service
- **BioStar X Core Service**: Core system functionalities and API communication service
- **Unified Gateway Service**: Reverse proxy-based integrated gateway service
- **BioStar X Coordinator Service**: Management of distributed system configuration information and service synchronization
- **BioStar X Server (Main)**: Main server service
- **BioStar X Cache Service**: Data caching and enhanced system performance

Situations where configuration changes are needed

You may need to change the service settings in the following situations.

- **Resolving port conflicts**: When another application uses the same port and causes conflicts
- **Compliance with security policies**: When only specific ports are allowed according to the organization's network security policy
- **Firewall settings**: When you need to change to ports allowed by your corporate firewall
- **Server environment changes**: When changing the server IP address or network configuration
- **Performance optimization**: When separation of ports is needed for traffic distribution or load balancing

How to change settings

1. Click the **SERVICE SETTINGS** menu in **BioStar X Service Manager**.
2. Go to the section of the service you want to change.
3. Modify the required port number or address.
4. To apply changes, click the **Apply** button in the upper right corner of the screen.

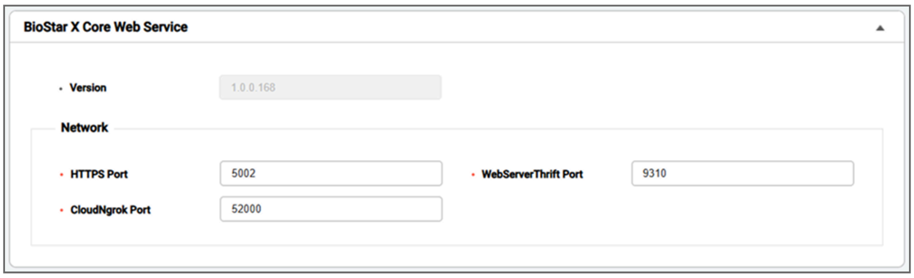
> ⓘ After changing the service settings, restart the related services to apply the changes.

> ⚠ **CAUTION**
>
> When changing port numbers, make sure there are no conflicts with other services or applications.

Service composition

BioStar X Core Web Service

This service is responsible for the web-based user interface.



BioStar X Core Web Service

- Version: 1.0.0.168

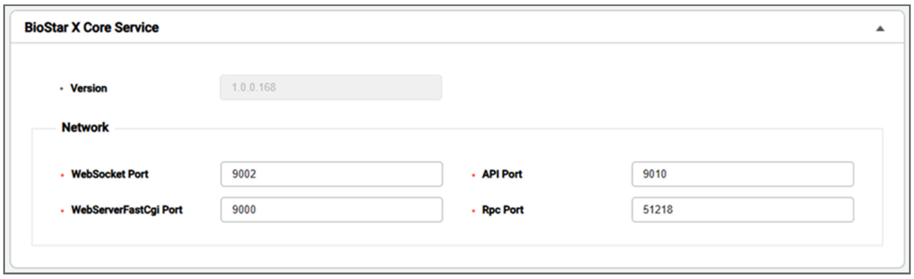
Network

- HTTPS Port: 5002
- WebServerThrift Port: 9310
- CloudNgrok Port: 52000

- **HTTPS Port**: Web interface access port (default: 5002)
- **WebServerThrift Port**: Web server communication port based on the Thrift protocol (default: 9310)
- **CloudNgrok Port**: Cloud tunneling service communication port (default: 52000)

BioStar X Core Service

This is the main service that handles core functionalities of the system and external API communications.



BioStar X Core Service

- Version: 1.0.0.168

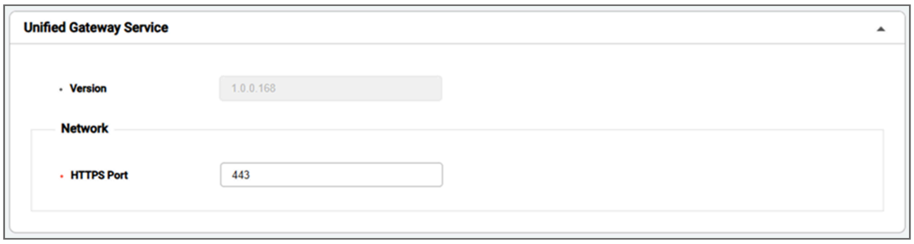
Network

- WebSocket Port: 9002
- API Port: 9010
- WebServerFastCgi Port: 9000
- Rpc Port: 51218

- **WebSocket Port**: WebSocket port for real-time bidirectional communication (default: 9002)
- **API Port**: REST API communication port (default: 9010)
- **WebServerFastCgi Port**: Web server communication port based on FastCGI protocol (default: 9000)
- **Rpc Port**: Remote Procedure Call (RPC) communication port (default: 51218)

Unified Gateway Service

Efficiently process requests to the **BioStar X** server through reverse proxy, improve the security vulnerabilities of iframes, and minimize SSL certificate errors.



Unified Gateway Service

- Version: 1.0.0.168

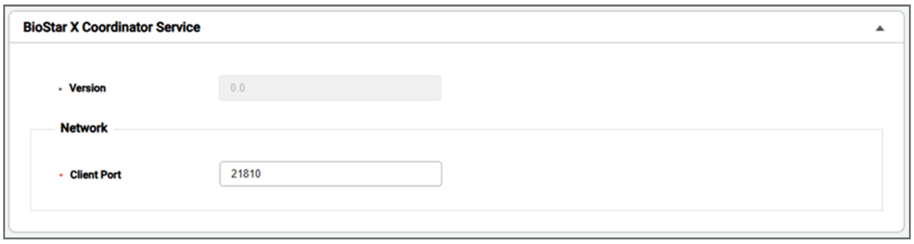
Network

- HTTPS Port: 443

- **HTTPS Port**: Integrated gateway HTTPS communication port (default: 443)

BioStar X Coordinator Service

This service is responsible for managing configuration information of the distributed system, monitoring service status, and synchronizing services.



BioStar X Coordinator Service

- Version: 0.0

Network

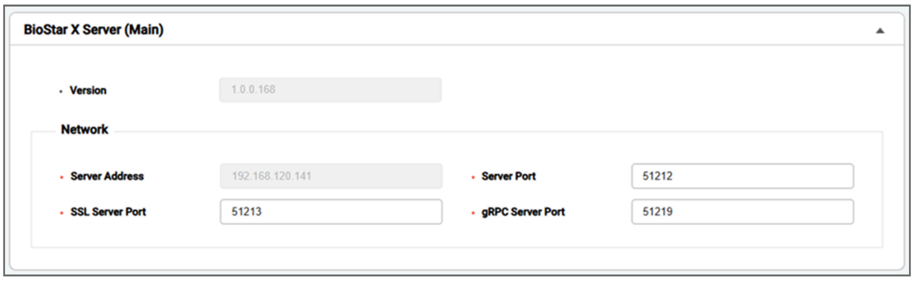
- Client Port: 21810

- **Client Port**: Communication port for client connections (default: 21810)

> **INFO**
>
> - Change the value of **Client Port**, then manually restart the **BioStar X Coordinator Service** in **Windows Services**(*services.msc*).
> - After restarting the **BioStar X Coordinator Service**, go to **BioStar X Service Manager** → **SERVICES** and restart all services.
>   Click **Stop All** in the top right corner of the screen. After all services are stopped, when the **Start All** button is enabled, click the button.

BioStar X Server (Main)

This is the core service that serves as the main server of the system.



BioStar X Server (Main)

- Version: 1.0.0.168

Network

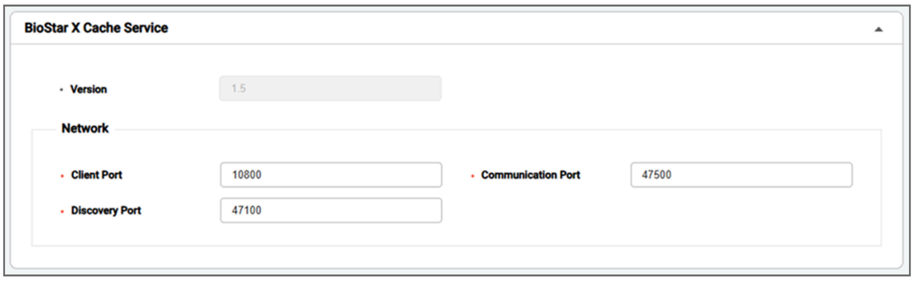
- Server Address: 192.168.120.141
- Server Port: 51212
- SSL Server Port: 51213
- gRPC Server Port: 51219

- **Server Address**: IP address of the main server
- **Server Port**: General server communication port (default: 51212)

- **SSL Server Port**: SSL secure encrypted communication port (default: 51213)
- **gRPC Server Port**: High-performance communication port based on gRPC protocol (default: 51219)

BioStar X Cache Service

This service improves the system's data processing speed and performance by storing frequently used data in memory.



BioStar X Cache Service

- Version: 1.5

Network

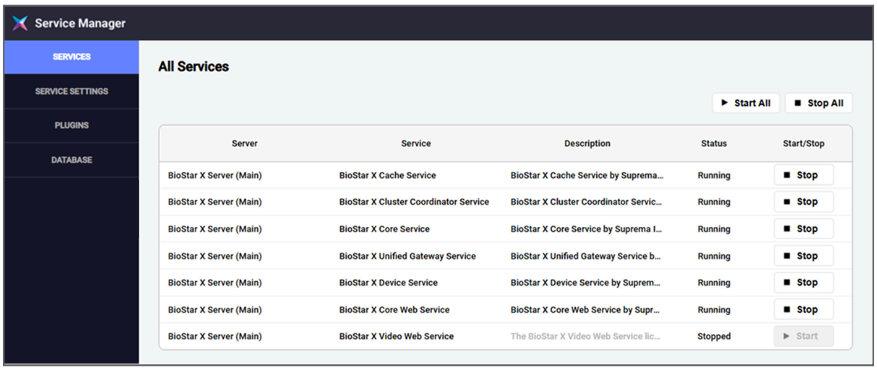
- Client Port: 10800
- Communication Port: 47500
- Discovery Port: 47100

- **Client Port**: Cache service client connection port (default: 10800)
- **Communication Port**: Internal communication port between cache nodes (default: 47500)
- **Discovery Port**: Port for automatic discovery of distributed cache nodes (default: 47100)

Change the Port

This guide explains how to change the port when the default port (443) of **BioStar X** is unavailable.

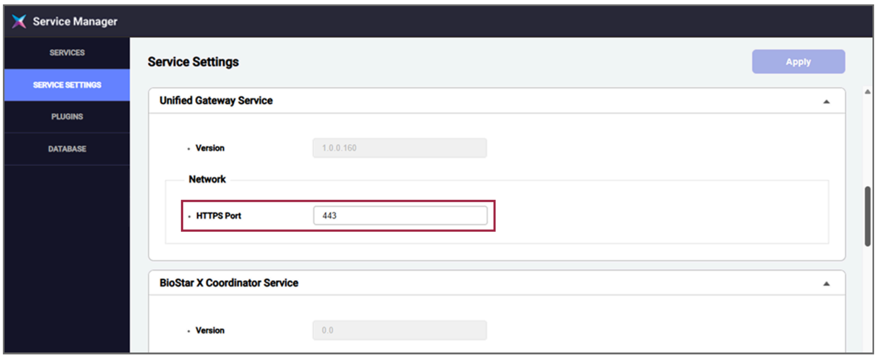
1. Click **Start** ⊞ → **BioStar X** → **BioStar X Service Manager** on Windows.
2. When the **BioStar X Service Manager** window appears in the web browser, click the **SERVICES** menu.
3. Click the **Stop** button for all services.



All Services

Server	Service	Description	Status	Start/Stop
BioStar X Server (Main)	BioStar X Cache Service	BioStar X Cache Service by Suprema...	Running	■ Stop
BioStar X Server (Main)	BioStar X Cluster Coordinator Service	BioStar X Cluster Coordinator Servic...	Running	■ Stop
BioStar X Server (Main)	BioStar X Core Service	BioStar X Core Service by Suprema I...	Running	■ Stop
BioStar X Server (Main)	BioStar X Unified Gateway Service	BioStar X Unified Gateway Service b...	Running	■ Stop
BioStar X Server (Main)	BioStar X Device Service	BioStar X Device Service by Suprem...	Running	■ Stop
BioStar X Server (Main)	BioStar X Core Web Service	BioStar X Core Web Service by Supr...	Running	■ Stop
BioStar X Server (Main)	BioStar X Video Web Service	The BioStar X Video Web Service lic...	Stopped	▶ Start

4. Click **SERVICE SETTINGS** in the left sidebar.
5. Enter the port number to change in the **HTTPS Port** input field in the **Unified Gateway Service** section.



Service Settings

Unified Gateway Service

- Version: 1.0.0.160

Network

- HTTPS Port: 443

BioStar X Coordinator Service

- Version: 0.0

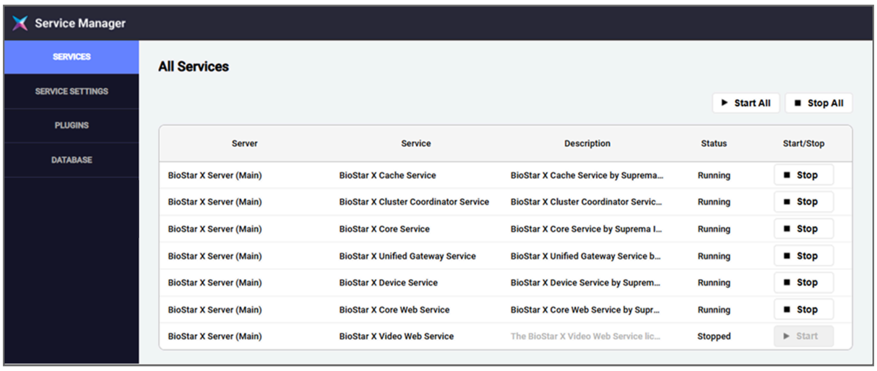
6. Click **Apply** in the upper right corner of the screen.
7. When the confirmation message appears, click **OK**.
8. Navigate to **SERVICES** and click the **Start** button for all services.
9. Access **BioStar X** through your web browser.

> ⓘ **INFO**
>
> - If you changed the port number to 450, enter `https://{ip_address}:450` in the address bar.

Change the Database

You can change the database settings.

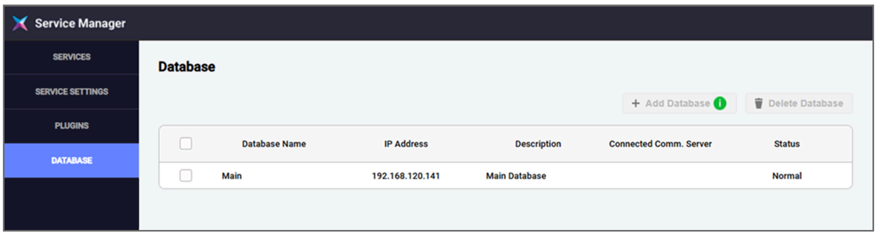
1. Click **Start** → **BioStar X** → **BioStar X Service Manager** on Windows.
2. When the **BioStar X Service Manager** window appears in the web browser, click the **SERVICES** menu.
3. Click Stop for all services.



Server	Service	Description	Status	Start/Stop
BioStar X Server (Main)	BioStar X Cache Service	BioStar X Cache Service by Suprema...	Running	■ Stop
BioStar X Server (Main)	BioStar X Cluster Coordinator Service	BioStar X Cluster Coordinator Servic...	Running	■ Stop
BioStar X Server (Main)	BioStar X Core Service	BioStar X Core Service by Suprema I...	Running	■ Stop
BioStar X Server (Main)	BioStar X Unified Gateway Service	BioStar X Unified Gateway Service b...	Running	■ Stop
BioStar X Server (Main)	BioStar X Device Service	BioStar X Device Service by Suprem...	Running	■ Stop
BioStar X Server (Main)	BioStar X Core Web Service	BioStar X Core Web Service by Supr...	Running	■ Stop
BioStar X Server (Main)	BioStar X Video Web Service	The BioStar X Video Web Service lic...	Stopped	▶ Start

> ⓘ Click Stop All to stop all services at once.

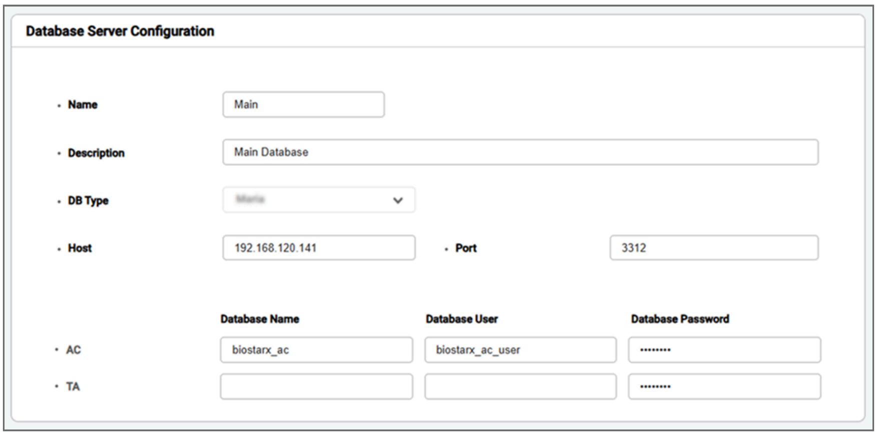
4. Click the **DATABASE** menu in the left sidebar.



□	Database Name	IP Address	Description	Connected Comm. Server	Status
□	Main	192.168.120.141	Main Database		Normal

5. Select the database desired to change the settings for from the database list.

6. In the **Database Server Configuration** section, you can change the following settings:



Database Server Configuration

- Name: Main
- Description: Main Database
- DB Type: Maria
- Host: 192.168.120.141
- Port: 3312

	Database Name	Database User	Database Password
AC	biostarx_ac	biostarx_ac_user	••••••••
TA			••••••••

- **Name**: Enter the database name.
- **Description**: Enter the database description.
- **DB Type**: Select the database type. (MariaDB, MS SQL)
- **Host**: Enter the hostname or IP address of the database server.
- **Port**: Enter the port number of the database server.
- **AC** / **TA** / **Video**: Enter the name, user, and password for the AC, TA, and Video databases.

7. Click Test Connection at the top right of the screen to check if the database is connected normally.

8. Click Save at the top right of the screen to save settings.

Add Auxiliary Database

When adding a communication server, add and connect an auxiliary database to reduce the load on the main server.

> ⓘ **INFO**
>
> - You need a **multi-communication server** license to add an auxiliary database. For more information on licensing policy, refer to the following.
> - For more information on installing a communication server, refer to the following.

Before start

If you are using a domain or hostname instead of an IP address for communication between databases in a MariaDB environment, be sure to check the following guidance.

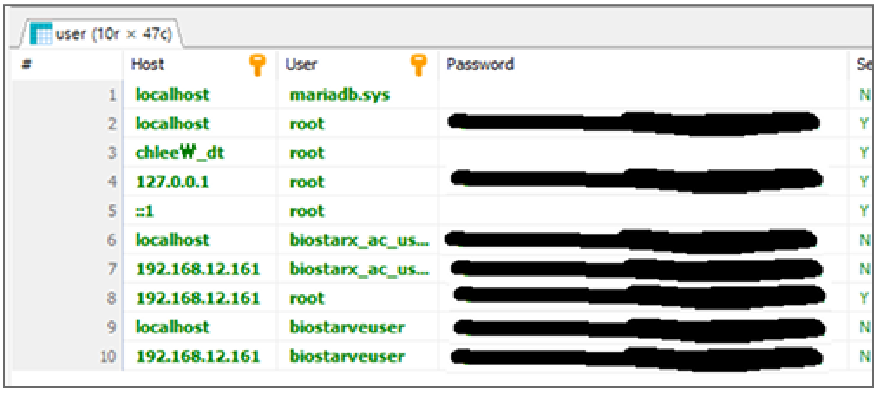
- If you do not use an IP address, Create user or Grant enrollment may not be possible.
- If you are communicating using a domain or hostname, ensure that user and permissions are registered for localhost.
- If you installed BioStar X using the convenient installation method, the root account is registered only for localhost, so you must add the server's IP address or *127.0.0.1*.

Registration method

Check if a password is set for the account with Host *127.0.0.1* and User root; if not set, be sure to establish a password and grant permissions.

1. Check if a password is set for the account with Host *127.0.0.1* and User root.

```
SELECT * FROM mysql.user;
```



user (10r × 47c)

#	Host	User	Password	Se
1	localhost	mariadb.sys		N
2	localhost	root	[redacted]	Y
3	chlee₩_dt	root		Y
4	127.0.0.1	root	[redacted]	Y
5	::1	root		Y
6	localhost	biostarx_ac_us...	[redacted]	N
7	192.168.12.161	biostarx_ac_us...	[redacted]	N
8	192.168.12.161	root	[redacted]	Y
9	localhost	biostarveuser	[redacted]	N
10	192.168.12.161	biostarveuser	[redacted]	N

If blank, the password is not set, so be sure to run the query in the following items to add a password and grant permissions.

2. Set a password and grant permissions for the account with Host *127.0.0.1* and User root.

```
ALTER USER 'root'@'127.0.0.1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO 'root'@'127.0.0.1';

CREATE USER '<Main DB AC User>'@'127.0.0.1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB AC User>'@'127.0.0.1';
CREATE USER '<Main DB AC User>'@'::1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB AC User>'@'::1';

CREATE USER '<Main DB TA User>'@'127.0.0.1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB TA User>'@'127.0.0.1';
CREATE USER '<Main DB TA User>'@'::1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB TA User>'@'::1';

CREATE USER '<Main DB VE User>'@'127.0.0.1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB VE User>'@'127.0.0.1';
CREATE USER '<Main DB VE User>'@'::1' IDENTIFIED BY '<Main DB AC Schema Password>';
GRANT ALL PRIVILEGES ON *.* TO '<Main DB VE User>'@'::1';

FLUSH PRIVILEGES;
```

Example

```
ALTER USER 'root'@'127.0.0.1' IDENTIFIED BY 'admin1234!';
GRANT ALL PRIVILEGES ON *.* TO 'root'@'127.0.0.1';
FLUSH PRIVILEGES;
```

IP address communication settings

The following settings can force communication via IP address.

1. After installing **BioStar X**, move to the following path.

> C:\Program Files\BioStar X\ta\mariadb-11.4.4-winx64

2. Open the *my.cnf* file with the owner's permissions and add the `skip-name-resolve` option to the [mysqld] section.

```
[mysqld]
port = 3312
character-set-server=utf8
collation-server=utf8_unicode_ci
socket = /tmp/mysql.sock
skip-external-locking
key_buffer_size = 32M
max_allowed_packet = 64M
...
skip-name-resolve
```

3. Restart the MariaDB service.

Add auxiliary database

This section provides guidance on adding an auxiliary database. Depending on the type of database being used, there are two methods: MariaDB and SQL Server.

MariaDB

1 Main database

Grant the account and permissions to access the main database from the new auxiliary database.

```
CREATE USER '<Main DB AC Schema User>'@'<Sub DB IP>' IDENTIFIED BY '<Main DB AC Schema Password>';

GRANT ALL PRIVILEGES ON <Main DB AC Schema>.* TO '<Main DB AC Schema User>'@'<Sub DB IP>';
FLUSH PRIVILEGES;
```

Example

```
CREATE USER 'biostarx_ac_user'@'192.168.12.42' IDENTIFIED BY 'password';

GRANT ALL PRIVILEGES ON biostar2_ac.* TO 'biostarx_ac_user'@'192.168.12.42';
FLUSH PRIVILEGES;
```

2 Auxiliary database

Grant the account and permissions to access the new auxiliary database from the main database.

```
CREATE USER '<Sub DB AC Schema User>'@'<Main DB IP>' IDENTIFIED BY '<Sub DB AC Schema Password>';

GRANT ALL PRIVILEGES ON <Sub DB AC Schema>.* TO '<Sub DB AC Schema User>'@'<Main DB IP>';
FLUSH PRIVILEGES;
```

Example

```
CREATE USER 'biostarx_ac_user'@'192.168.12.161' IDENTIFIED BY 'password';

GRANT ALL PRIVILEGES ON biostar2_ac.* TO 'biostarx_ac_user'@'192.168.12.161';
FLUSH PRIVILEGES;
```

3 Check for FederatedX usage

Run the command below in both the main and auxiliary databases to check if the FederatedX storage engine is enabled.

```
SHOW ENGINES;
```

If the query result shows `Engine : FEDERATED, Support : YES`, it is already installed. If the FederatedX storage engine is not installed, execute the query below.

```
INSTALL PLUGIN federated SONAME 'ha_federatedx';
```

> **INFO**
>
> Check if the *ha_federatedx.dll* file exists in the *lib/plugin* folder under the path where MariaDB is installed. Typically, the dll file exists at *C:\Program Files\MariaDB {version}\lib\plugin* path.

4 Register server alias

Register a server alias to allow the federatedX table created in the auxiliary database to access the source table in the main database.

```
CREATE SERVER 'default' FOREIGN DATA WRAPPER mysql OPTIONS (HOST '<Main DB IP>', PORT <Main DB
PORT>, DATABASE '<Main DB AC Schema>', USER '<Main DB AC USER>', PASSWORD '<Main DB AC USER
Password>');

-- Confirm registration
SELECT * FROM mysql.servers;
```

If you need to change information about Host, Port, DB, User, or Password for the existing registered server name, it can be modified using the `Alter` statement. You may also change certain information only.

```
ALTER SERVER 'default' OPTIONS (HOST '<Main DB IP>', PORT <Main DB PORT>, DATABASE '<Main DB AC
Schema>', USER '<Main DB AC USER>', PASSWORD '<Main DB AC USER Password>');
```

Example

```
CREATE SERVER 'default' FOREIGN DATA WRAPPER mysql OPTIONS (HOST '192.168.12.161', PORT 3312,
DATABASE 'biostar2_ac', USER 'biostarx_ac_user', PASSWORD 'password');

ALTER SERVER 'default' OPTIONS (HOST '192.168.12.161', PORT 3312, DATABASE 'biostar2_ac', USER
'biostarx_ac_usermt__fttid__', PASSWORD 'password');
```

5 Table link settings

Follow the steps below to link the necessary tables in the auxiliary database to the tables in the main database.

- The following is the query to generate `CREATE TABLE` statements in the main database.

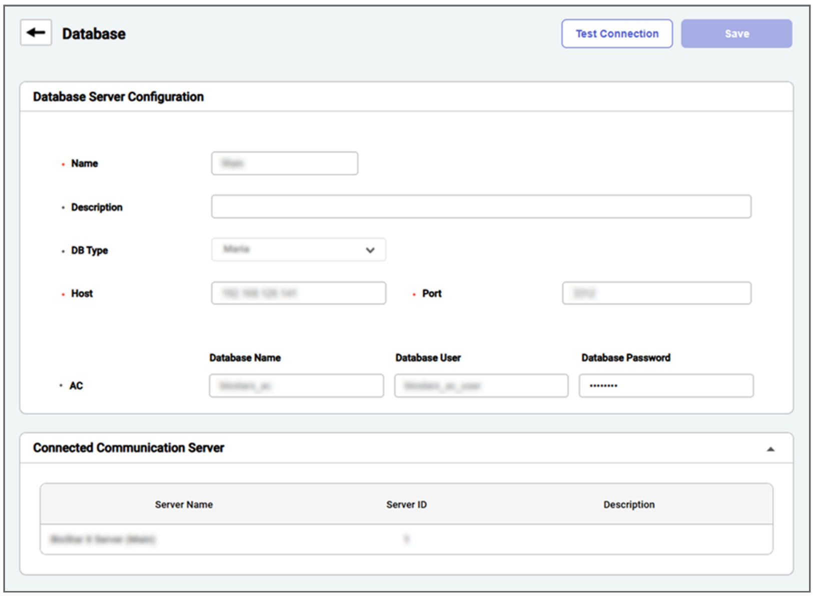
```
select
  concat(
     'CREATE TABLE IF NOT EXISTS <SubDB_AC_Database_Schema>.', table_name,
     ' ENGINE=FEDERATED ',
     'CONNECTION="default/', table_name, '";'
  ) as create_table_sql
from information_schema.TABLES
where TABLE_SCHEMA = '<MainDB_AC_Database_Schema>'
    AND TABLE_TYPE = 'BASE TABLE'
    AND NOT TABLE_NAME REGEXP '^t_lg[0-9]{6}$'
    AND NOT TABLE_NAME REGEXP '^t_almevt[0-9]{6}$'
    AND NOT TABLE_NAME REGEXP '^t_lgalmtrstrc[0-9]{6}$'
ORDER BY TABLE_NAME;
```

> **INFO**
>
> Due to the nature of FederatedX, it is recommended to set `Table_type` to 'BASE TABLE'. `VIEW type` is also possible but not recommended.

6 Service Manager settings

1. Run **BioStar X Service Manager**. (**Start** ⊞ → **BioStar X** → **BioStar X Service Manager**)
2. Click the **DATABASE** menu in the left sidebar.
3. Click the **+ Add Database** button in the upper right corner of the screen.

4. Enter each item in the database addition screen.



- **Name**: Enter the database name.
- **Description**: Enter the database description.
- **DB Type**: Select the database type. (Maria, MS SQL)
- **Host**: Enter the hostname or IP address of the database server.
- **Port**: Enter the port number of the database server.
- **AC** / **TA**: Enter the name, user, and password of the AC, TA databases.

5. Click Test Connection at the top right of the screen to check if the database is connected normally.
6. Click Save at the top right of the screen to save settings.

SQL Server

1 Grant permissions for the main database

Grant the following permissions on the main database with an account that has sysadmin privileges.

```
GRANT ALTER ANY LINKED SERVER TO [<MAIN DATABASE AC USER>];
GRANT ALTER ANY LOGIN TO [<MAIN DATABASE AC USER>];
```

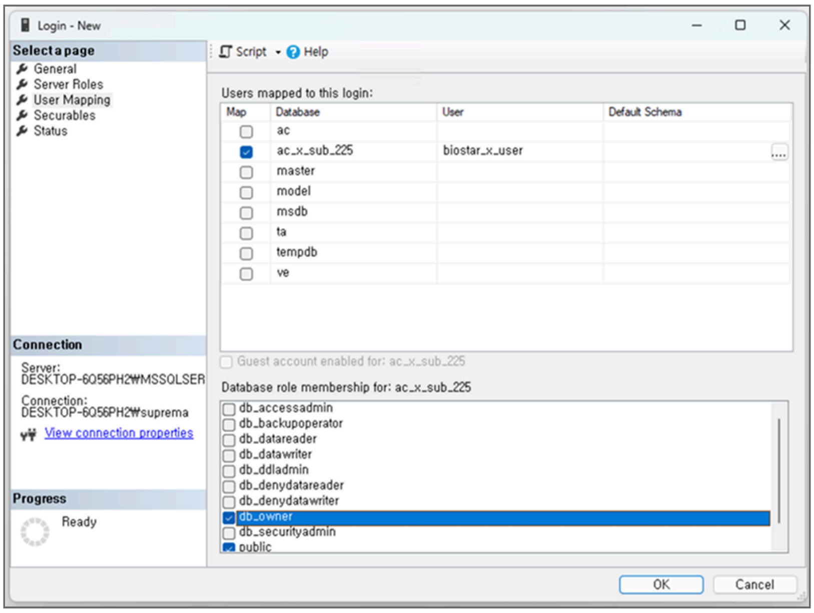
Example

```
GRANT ALTER ANY LINKED SERVER TO [biostar_x_user];
```

2

Grant permissions for the auxiliary database

1. Connect User Mapping for tables and users in the auxiliary database with an account that has sysadmin privileges. At this time, adding the db_owner role is necessary.



Server:
DESKTOP-6Q56PH2₩MSSQLSER

Connection:
DESKTOP-6Q56PH2₩suprema

Users mapped to this login:

Map	Database	User	Default Schema
□	ac		
☑	ac_x_sub_225	biostar_x_user	
□	master		
□	model		
□	msdb		
□	ta		
□	tempdb		
□	ve		

□ Guest account enabled for: ac_x_sub_225

Database role membership for: ac_x_sub_225

- □ db_accessadmin
- □ db_backupoperator
- □ db_datareader
- □ db_datawriter
- □ db_ddladmin
- □ db_denydatareader
- □ db_denydatawriter
- ☑ db_owner
- □ db_securityadmin
- ☑ public

2. Grant the following permissions to the database to be added.

```
GRANT ALTER ANY LINKED SERVER TO [<SUB DATABASE AC USER>];
GRANT ALTER ANY LOGIN TO [<SUB DATABASE AC USER>];
```

Example

```
GRANT ALTER ANY LINKED SERVER TO [biostar_x_user_sub];
GRANT ALTER ANY LOGIN TO [biostar_x_user_sub];
```

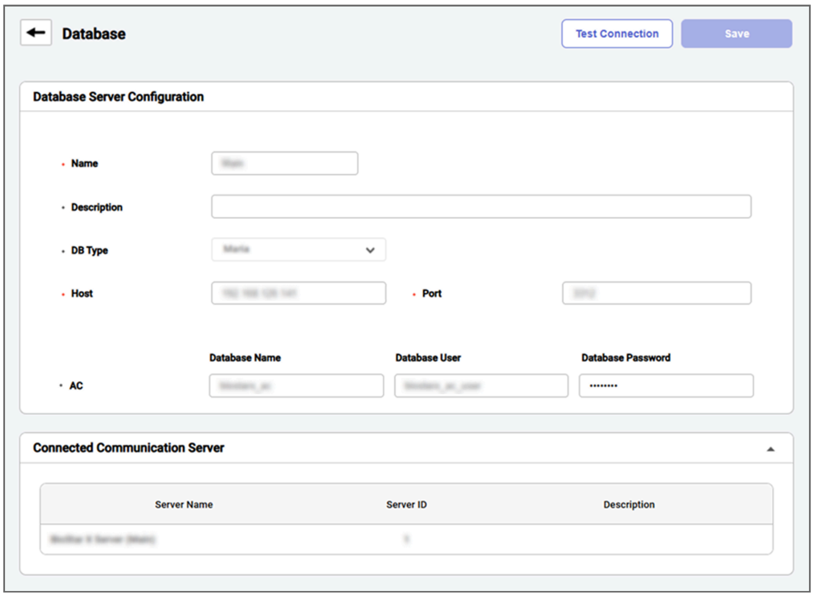
3

Service Manager settings

Use **BioStar X Service Manager** to add the auxiliary database.

1. Run **BioStar X Service Manager**. (**Start** ⊞ → **BioStar X** → **BioStar X Service Manager**)
2. Click the DATABASE menu in the left sidebar.
3. Click the **+ Add Database** button in the upper right corner of the screen.

4. Enter each item in the database addition screen.



Database Server Configuration

- Name [redacted]
- Description
- DB Type [redacted]
- Host [redacted] · Port [redacted]

	Database Name	Database User	Database Password
· AC	[redacted]	[redacted]	••••••••

Connected Communication Server

Server Name	Server ID	Description
[redacted]	[redacted]	

- **Name**: Enter the database name.
- **Description**: Enter the database description.
- **DB Type**: Select the database type. (Maria, MS SQL)
- **Host**: Enter the hostname or IP address of the database server.
- **Port**: Enter the port number of the database server.
- **AC** / **TA**: Enter the name, user, and password of the AC, TA databases.

5. Click Test Connection at the top right of the screen to check if the database is connected normally.

6. Click Save at the top right of the screen to save settings.

> **INFO**
>
> - After completing the settings, Linked Server settings for both main and auxiliary databases will be automatically applied.
> - Even when modifying database information, the Linked Server settings will be automatically changed. When modifying the main database, the changes will reflect in the Linked Server settings of all registered auxiliary databases. When modifying the auxiliary database, only changes for the main database and that auxiliary database will be reflected.

4 Generate Linked Temp Table query

Run the query below in the main database to generate the Linked Temp Table query to be created in the auxiliary database.

```
USE [<AC Schema>];
GO
DECLARE @LinkedServer  sysname = N'default';
DECLARE @SourceSchema  sysname = N'dbo';
DECLARE @TargetSchema  sysname = N'dbo';

SELECT
    'IF OBJECT_ID(N''' + QUOTENAME(@TargetSchema,'''') + '.' + QUOTENAME(t.name,'''') + ''', ''SN'') IS NOT NULL '
  + 'DROP SYNONYM ' + QUOTENAME(@TargetSchema) + '.' + QUOTENAME(t.name) + ';'
  + 'CREATE SYNONYM ' + QUOTENAME(@TargetSchema) + '.' + QUOTENAME(t.name)
  + ' FOR ' + QUOTENAME(@LinkedServer) + '.' + QUOTENAME(DB_NAME()) + '.' + QUOTENAME(s.name) + '.' +
QUOTENAME(t.name) + ';'
  AS recreate_synonym_sql
FROM sys.tables AS t
JOIN sys.schemas AS s
  ON s.schema_id = t.schema_id
WHERE s.name = @SourceSchema
  AND t.is_ms_shipped = 0
  AND t.name NOT LIKE 't_lg[0-9][0-9][0-9][0-9][0-9][0-9]'
  AND t.name NOT LIKE 't_almevt[0-9][0-9][0-9][0-9][0-9][0-9]'
  AND t.name NOT LIKE 't_lgalmtrstrc[0-9][0-9][0-9][0-9][0-9][0-9]'
ORDER BY t.name;
```

Example

```
-- Example
USE [main_ac_x_215];
GO
DECLARE @LinkedServer  sysname = N'default';  -- Linked Server name set in the sub DB
DECLARE @SourceSchema  sysname = N'dbo';      -- Schema to target in the main DB
DECLARE @TargetSchema  sysname = N'dbo';      -- Schema to create synonyms in the sub DB (reflected in
the output string)

SELECT
    'IF OBJECT_ID(N''' + QUOTENAME(@TargetSchema,'''') + '.' + QUOTENAME(t.name,'''') + ''', ''SN'') IS NOT NULL '
  + 'DROP SYNONYM ' + QUOTENAME(@TargetSchema) + '.' + QUOTENAME(t.name) + ';'
  + 'CREATE SYNONYM ' + QUOTENAME(@TargetSchema) + '.' + QUOTENAME(t.name)
  + ' FOR ' + QUOTENAME(@LinkedServer) + '.' + QUOTENAME(DB_NAME()) + '.' + QUOTENAME(s.name) + '.' +
QUOTENAME(t.name) + ';'
  AS recreate_synonym_sql
FROM sys.tables AS t
JOIN sys.schemas AS s
  ON s.schema_id = t.schema_id
WHERE s.name = @SourceSchema
  AND t.is_ms_shipped = 0
  AND t.name NOT LIKE 't_lg[0-9][0-9][0-9][0-9][0-9][0-9]'
  AND t.name NOT LIKE 't_almevt[0-9][0-9][0-9][0-9][0-9][0-9]'
```

5

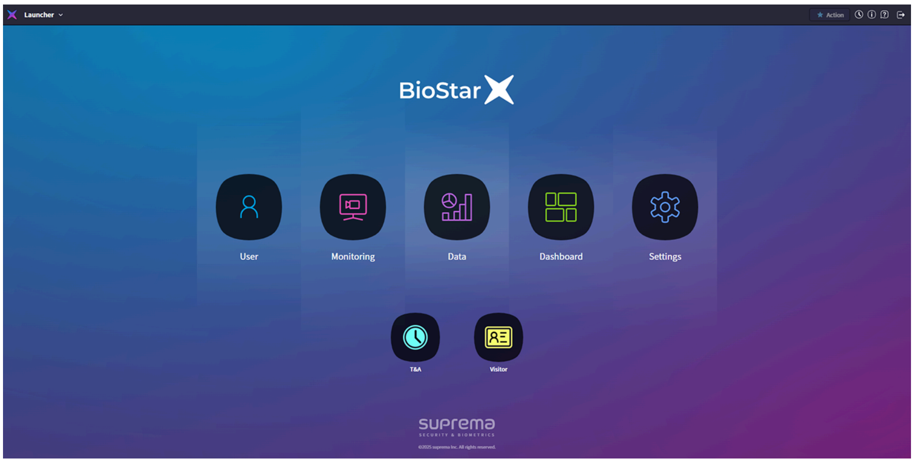
Execute query in the auxiliary database.

Copy the previously generated `CREATE SYNONYM` query in full. Connect to the auxiliary database server to be added, write the query as below, and execute it. It will be stored in Synonyms in the AC schema of the auxiliary database.

```
use [<Sub DB AC Database>];

IF OBJECT_ID(N'[dbo].[T_ACSGR]', 'SN') IS NOT NULL DROP SYNONYM [dbo].[T_ACSGR];CREATE SYNONYM
[dbo].[T_ACSGR] FOR [default].[main_ac_x_215].[dbo].[T_ACSGR];
IF OBJECT_ID(N'[dbo].[T_ACSGRLVLS]', 'SN') IS NOT NULL DROP SYNONYM [dbo].[T_ACSGRLVLS];CREATE
SYNONYM [dbo].[T_ACSGRLVLS] FOR [default].[main_ac_x_215].[dbo].[T_ACSGRLVLS];
IF OBJECT_ID(N'[dbo].[T_ACSGRSENT]', 'SN') IS NOT NULL DROP SYNONYM [dbo].[T_ACSGRSENT];CREATE
SYNONYM [dbo].[T_ACSGRSENT] FOR [default].[main_ac_x_215].[dbo].[T_ACSGRSENT];
IF OBJECT_ID(N'[dbo].[T_ACSGRUSS]', 'SN') IS NOT NULL DROP SYNONYM [dbo].[T_ACSGRUSS];CREATE
SYNONYM [dbo].[T_ACSGRUSS] FOR [default].[main_ac_x_215].[dbo].[T_ACSGRUSS];
...
```

Launcher

The **Launcher** page is the initial **BioStar X** home page users encounter after logging in, serving as a central hub for accessing **BioStar X**'s main features. This page is designed to allow users to easily navigate and use all features of **BioStar X**. The UI components of the launcher page are as follows.



The **Launcher** page provides links to the **User**, **Monitoring**, **Data**, **Dashboard**, and **Settings** pages.

- **User**: Efficiently manage users through various features such as user group management, user management, user template management, and checking users by access permissions, thereby enhancing security through permissions. For more information, refer to the following.
- **Monitoring**: Monitor doors, devices, video, and events in various ways. Control related features and monitor through real-time video. For more information, refer to the following.
- **Data**: Query user information or events based on desired criteria, and generate reports on a set schedule. For more information, refer to the following.
- **Dashboard**: Users can add and arrange widgets based on data selected from the various data provided by **BioStar X** to create their desired dashboard. For more information, refer to the following.
- **Settings**: Configure **BioStar X** optimized for user environments through various settings for devices, access control, user permissions, language, and time. For more information, refer to the following.

> **INFO**
>
> - For more information about the header area at the top of the screen, refer to the following.
> - At the bottom of the screen, features installed through additional plugins can be accessed. A plugin license is required to use plugin features.
>   - For more information on using plugins, refer to the following.
>   - For more information about the license policy, refer to the following.

User

This guide covers the features available on the User page, one of BioStar X's core features. This page introduces various features to effectively manage users through user group management, user management, user template management, and user verification by access permissions, as well as methods to enhance security through permissions. Use the various features to make the most of **BioStar X**.

Click User on the Launcher page or select User from the shortcut list at the top left of the screen.

Manage User Groups → Read more

Enhance management efficiency, scalability by leveraging user groups and optimize access control operations.

Register Users → Read more

Guidelines for registering new users.

Enter Basic User Information → Read more

This section describes how to enter basic user information.

Enroll User's Credential → 8 items

You can enroll credentials such as fingerprint, face, card information, and PIN.

- Set Security Level
- Authentication Mode Settings
- Enroll Fingerprint

↳ 8 items

Setting User Permissions → Read more

This guide explains how to set the administrator privileges and access permissions for BioStar X users.

Configure User Advanced Settings → Read more

Learn how to set messages to display on the device when the user enters and how to exclude directory integration features.

Explore Users → Read more

This guide explains how to use the features for viewing, searching, sorting, and managing the user list.

Manage Users → 5 items

Guides user management features such as modifying and deleting user information, device synchronization, tracking access history, and exporting/importing data.

- Edit User Information
- Delete User
- Transfer User Information to the Device

↳ 5 items

Manage Access Groups → Read more

This guide shows how to query users by access group and explore the access permission structure.

Login in with Multi-Factor Authentication → Read more

Using multi-factor authentication when logging into BioStar X can enhance the security of your account.

Batch Enroll Faces → Read more

Learn how to batch enroll users' faces.

Face Migration → Read more

You can upgrade the faces enrolled in the previous version of BioStar X to enhance recognition performance using the latest algorithm.

Set Emergency Open Permissions → Read more

This guide explains how to grant emergency open permissions to card credentials for specific users to open all doors in emergency situations.

Manage User Groups

User groups can share common properties and permissions. When a user becomes a member of a group, they are automatically granted all properties of that group. A user can belong to only one user group.

- Instead of setting access permissions for individual users, you can create user groups by department or role and apply the same access permissions at once.
- Modifying the group's access permissions will automatically apply to all users belonging to that group, reducing the administrative workload. You can quickly adjust permissions when there are organizational changes or new projects.
- You can prevent unnecessary access and increase security by setting permissions by group.
- You can separately analyze the access logs of specific groups, making security audits and log management easier.
- User groups can apply detailed policies such as access limit times and restricted areas in integration with the access level.

Add group

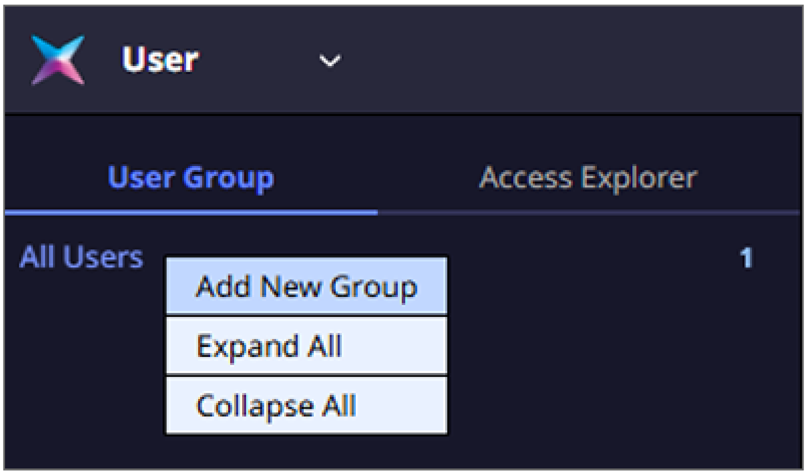
Create groups to efficiently manage multiple users. By registering a name such as the organization the user belongs to, it can be managed conveniently.

> **INFO**
>
> - Registering the group name as the name of the organization or department that the user belongs to makes management easier.
> - You can create sub-groups of the group sequentially up to 8 levels.
> - The user group name can be up to 48 characters long.
> - If you select a group from the user group list, only users belonging to that group will be displayed in the user list.

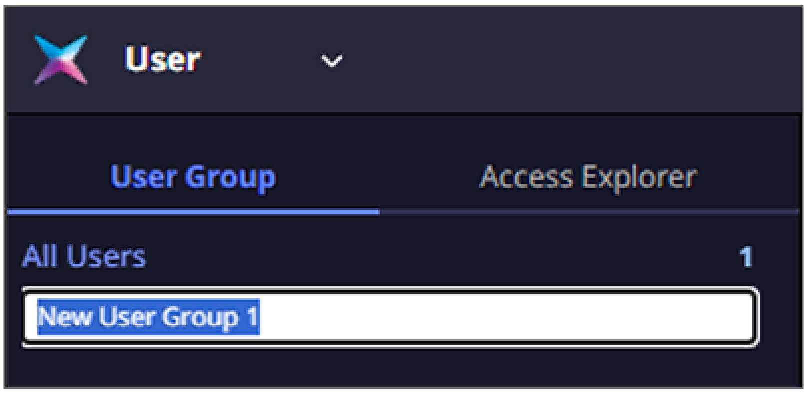
Create top-level group

1. Click **User** on the **Launcher** page.

2. In the left sidebar of the screen, select **All Users** from the **User Group** tab and right-click.

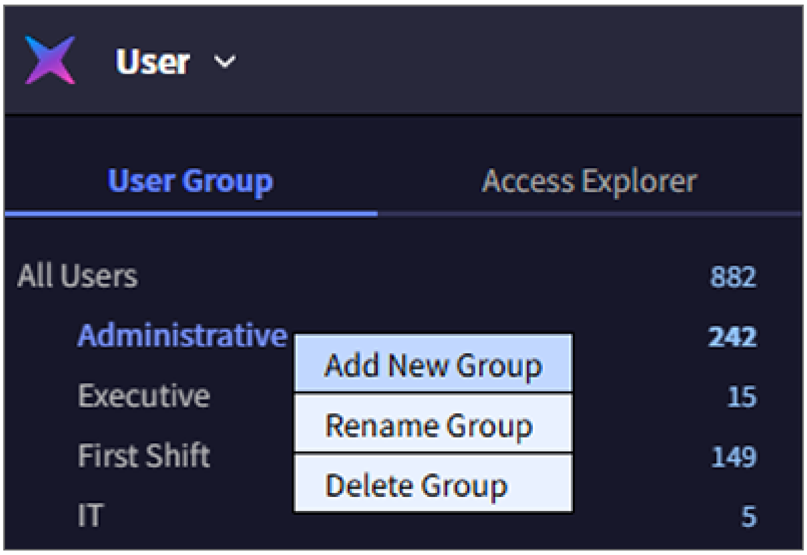


3. Click **Add New Group** in the popup menu.
4. When the group is created, enter your desired group name.



Create lower group

1. In the **User Group** tab of the left sidebar on the screen, select the parent group and right-click.



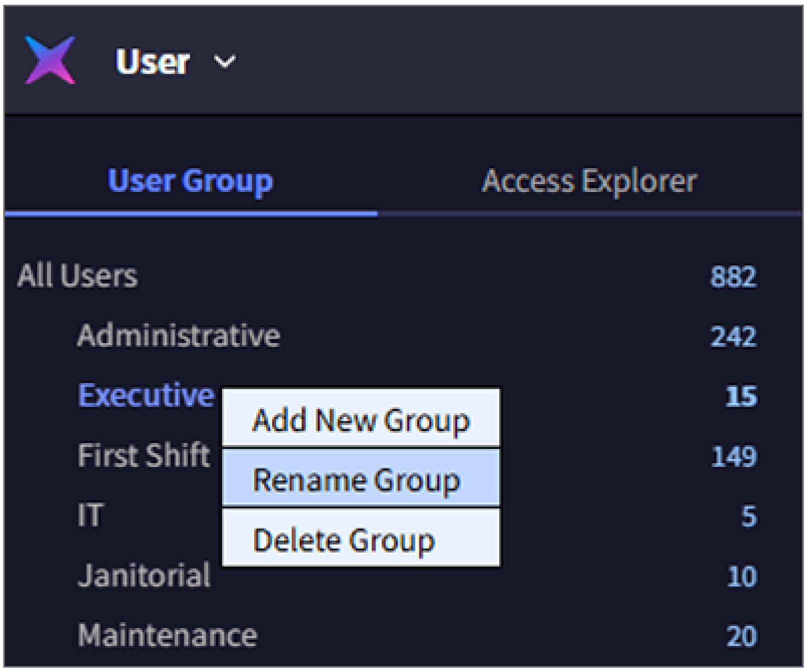
2. Click **Add New Group** in the popup menu.
3. When the group is created, enter your desired group name.

> **INFO**
>
> - You must select a parent group when creating a sub-group, and you can create up to 8 levels.
> - You can set a group as a subgroup of the target group by dragging the group to another group. Moving a group to **All Users** can set it as the top-level group.

Change group name

You can change the name of the group to which the user belongs. It is recommended to change the group name when the name of the organization or department changes.

1. Click **User** on the **Launcher** page.
2. Select the group you want to rename from the **User Group** list of the left sidebar and right-click.



3. Click **Rename Group** in the popup menu.
4. Change the desired group name.

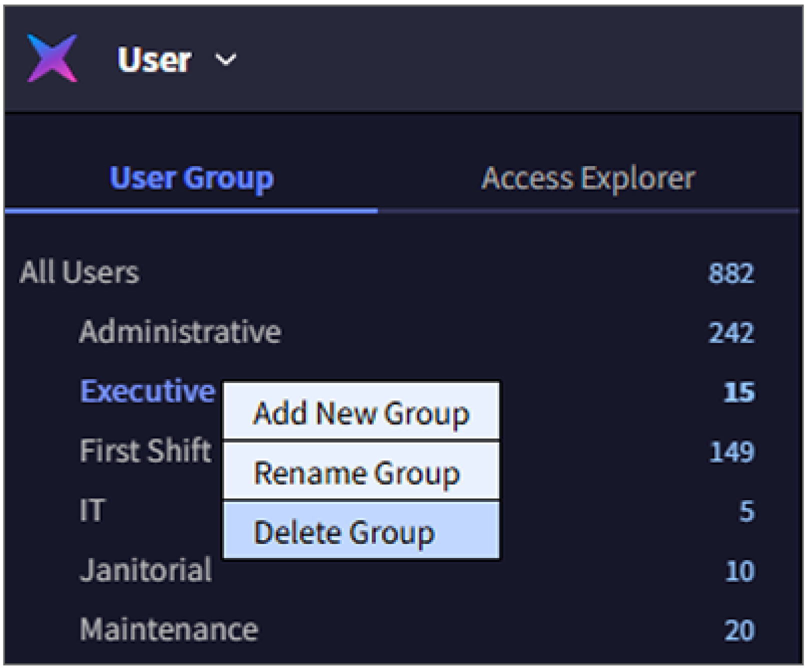
Check for changes in the **User Group** list.

> **INFO**
>
> The user group name can be up to 48 characters long.

Delete group

You can delete the group to which the user belongs.

1. Click **User** on the **Launcher** page.
2. Select the group to delete from the **User Group** list of the left sidebar and right-click.
3. Click **Delete Group** in the popup menu.

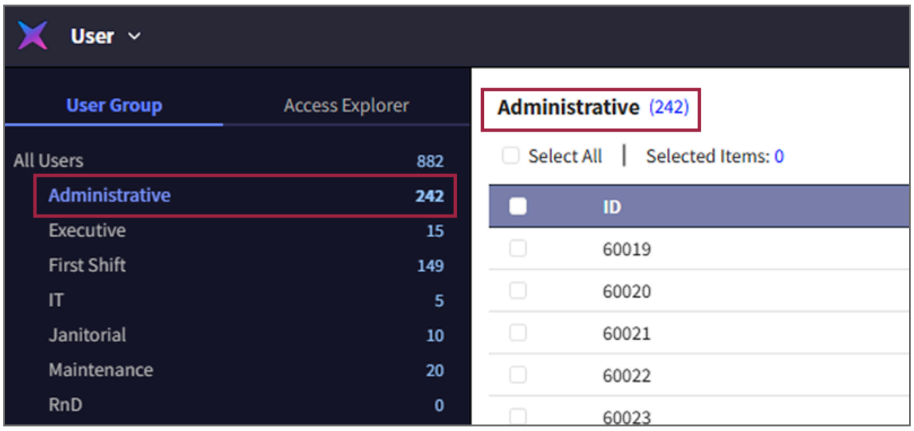


4. When the confirm message appears, click the **Yes** button.

In the **User Group** list, confirm that the selected group has been deleted.

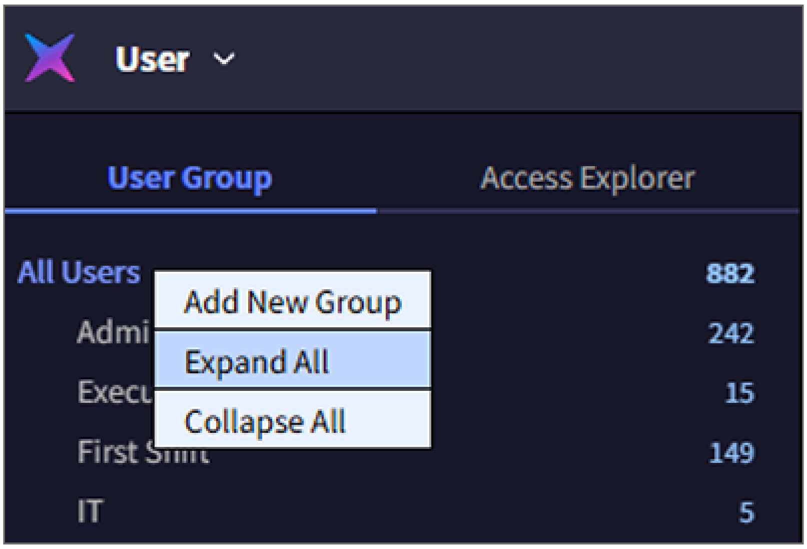
View users by group

You can see users belonging to the user group. In the **User** page, select the desired user group from the left sidebar. Users from the selected user group will be displayed in the list.

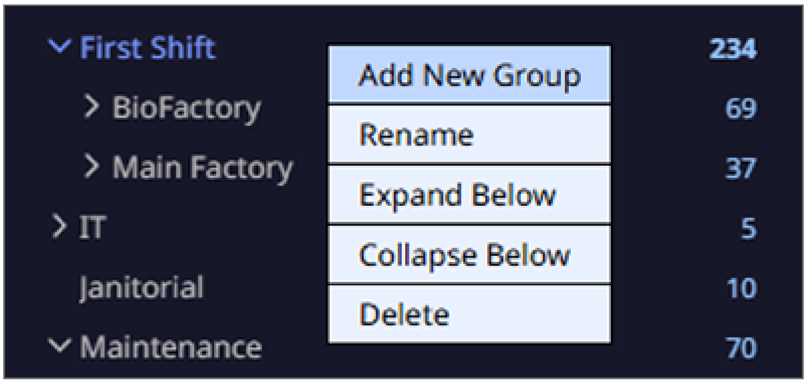


Expand/collapse group list

You can expand or collapse the user group list. In the **User Group** tab, select **All Users** and right-click. In the popup menu, click **Expand All** or **Collapse All**.



If there are subgroups within the group, you can expand or collapse them. Select the parent group and right-click. In the popup menu, click **Expand Below** or **Collapse Below**.

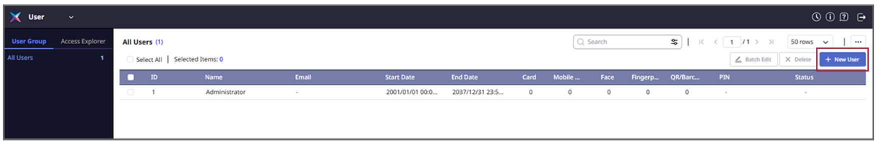


Register Users

Guidelines for registering new users. You can enter information such as the user's photo, name, email, and phone number, and set the user's access permissions and biometric information.

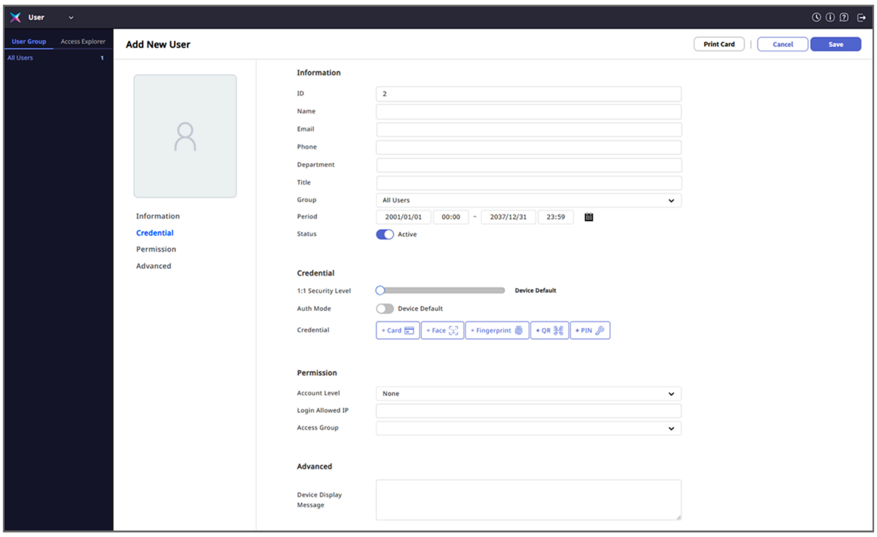
Enter user information and set access permissions, then enroll credentials.

1. Click **User** on the **Launcher** page.
2. Click the **New User** button in the upper right corner of the **User** page.



ID	Name	Email	Start Date	End Date	Card	Mobile ...	Face	Fingerp...	QR/Barc...	PIN	Status
1	Administrator	-	2001/01/01 00:0...	2037/12/31 23:5...	0	0	0	0	0	-	-

3. Enter user information on the **Add New User** screen.



Information

ID: 2
Name:
Email:
Phone:
Department:
Title:
Group: All Users
Period: 2001/01/01 00:00 ~ 2037/12/31 23:59
Status: Active

Credential

1:1 Security Level: Device Default
Auth Mode: Device Default
Credential:

Permission

Account Level: None
Login Allowed IP:
Access Group:

Advanced

Device Display Message:

4. Enter the user's basic information in the **Information** section.
5. Enroll the user's biometric information in the **Credential** section.
6. Set **BioStar X** operation and access permissions for the user in the **Permission** section.
7. In the **Advanced** section, you can enter a message to display on the device when the user accesses it.
8. Enter all information and click **Save** in the upper right corner of the screen.

The registered user appears in the user list. For detailed information on input and settings by section, refer to the below.

ⓘ **INFO**

- Access permissions and biometric information are optional. You can modify or add after saving the basic information.
- To print user information as a card using the card template, click **Print Card** at the top right of the screen. For more information, refer to the following.
- Click **Cancel** at the top right of the screen to cancel user registration.

Enter Basic User Information

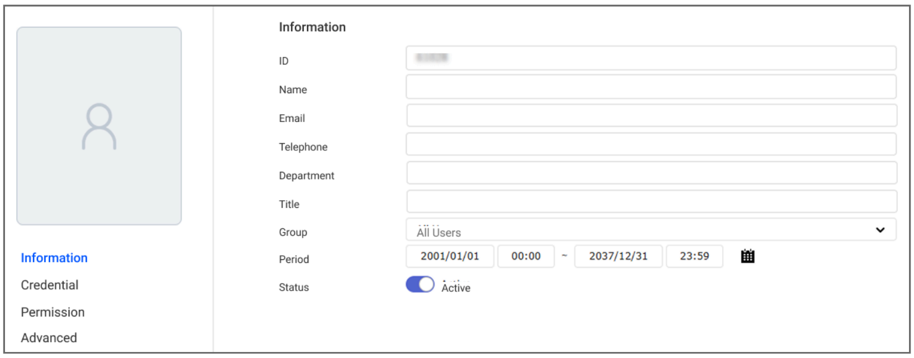
This section describes how to enter basic user information. The entered user information is used for search and management. Managing user information clearly helps comply with the organization's security and privacy policies.

- When you systematically enter basic information such as name, department, position, and group, you can easily search for, classify, and manage users.
- You can refine the access rights based on the user's affiliation, position, and group information.
- It is advantageous for security and auditing because it allows for accurate tracking of activities, access logs, etc. by user.

Go to the **Launcher** → **User** page. You can enter user information in the two ways below.

- **New User**: Click the **New User** button at the top right of the screen. The **New User** window appears.
- **Existing User**: Double-click a user in the user list. Or, click the user and click the **See More** button in the preview screen displayed on the right side of the screen. A window for editing user information appears.

The fields that can be set in the **Information** section are as follows. Please enter user information by referring to the description for each field.

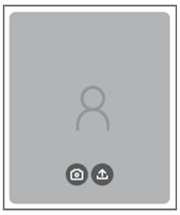


Information

ID	[redacted]
Name	
Email	
Telephone	
Department	
Title	
Group	All Users
Period	2001/01/01 00:00 ~ 2037/12/31 23:59
Status	Active

Information
Credential
Permission
Advanced

- **Photo**: Register the user's photo. You can take a photo with the webcam or upload a photo from your PC. When you hover over the profile, the tools available will be displayed.



  - 📷: If a webcam is connected to the PC, you can click the button to take and register a photo.
  - ⤒: You can upload an image file saved on your PC.

  For more information on details, refer to the following.

- **ID**: Enter the unique ID to assign to the user.
- **Name**: Enter the user's name.
- **Email**: Enter the email address.
- **Phone**: Enter the phone number.
- **Department**: Enter the department to which the user belongs.

- **Title**: Enter the user's position.
- Select **Group**: Select the user's group. For more information about adding and managing user groups, refer to the following.
- **Period**: Set a period for using the user account. You can either click on the date and time area to enter them manually or click 📅 to select the desired date and time.
- **Status**: You can temporarily disable the user account.

Click **Save** in the upper right corner of the screen to save the basic information you entered.

INFO

- **ID** may have different values that can be set according to the **Server** menu under **Settings** → **User ID Type** option. For more information on details, refer to the following.
  - **Number**: Enter a number from 1 to 4294967294.
  - **Alphanumeric**: Enter a combination of letters and numbers.
- Spaces cannot be included with the value of **ID**.
- The username can be up to 48 characters, including special characters.

  > Special characters: ~ ! @ # $ % ^ & ( ) - _ = + [ ] { } ; `

- To display the user's photo, department, and position on the mobile access card, ensure to add a photo and enter the department and position.
- Position and department names can be entered up to 64 characters, including special characters, spaces, and _.
- If using a mobile access card, be sure to enter the user's email when sending via email.
- To use face mobile enrollment or BioStar X QR, be sure to enter the user's email address.

TIP

In addition to the basic input fields provided by **BioStar X**, you can add custom fields using the **Custom User Field** feature to enter additional user information. **Custom User Field** is a useful feature that allows you to expand user information according to the organization's requirements.

For more information on how to add **Custom User Field**, refer to the following.

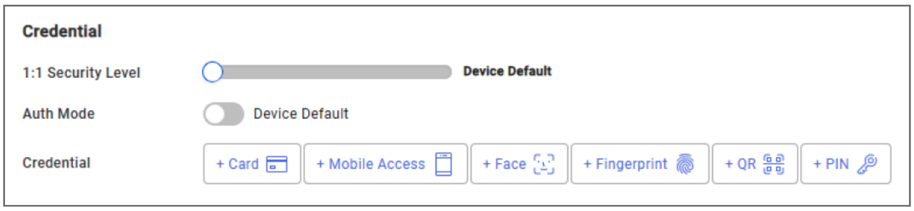
Enroll User's Credential

This document provides guidance on how to enroll user credentials. Users can enroll their fingerprints, faces, card information, and PINs as credentials. Credentials can be added or modified when registering or updating a user.

Go to the **Launcher** → **User** page and enroll, add, or modify credentials in the following two ways:

- **New User**: Click the **New User** button at the top right of the screen. The **New User** window appears.
- **Existing User**: Double-click a user in the user list. Or, click the user and click the **See More** button in the preview screen displayed on the right side of the screen. A window for editing user information appears.

In the **Credential** section, the following items can be set. Refer to the descriptions for each item to set appropriate user permissions.



Credential

1:1 Security Level: Device Default

Auth Mode: Device Default

Enroll credentials and set the appropriate security level in **1:1 Security Level**. A higher security level may lead to a lower authentication rate or a higher false rejection rate (FRR).

> ⓘ **Credential**: Data used to identify users. Digital signatures, smart cards, biometric data, user names, passwords, etc. are common examples of credentials.

> ⓘ **INFO**
>
> - Mobile access cards must be linked with the AirPop portal to be used. For more information regarding the Airfob Portal and mobile access card use, refer to the following.

Eroll credentials

The method to enroll user credentials is as follows. Credentials can be enrolled in various forms such as fingerprints, faces, cards, and passwords.

Set Security Level → Read more

You can grant separate security levels to users regardless of the biometric 1:N security level set on the device.

Authentication Mode Settings → Read more

Set the device default or individual private authentication mode to apply different authentication methods for each user.

Enroll Fingerprint → Read more

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

Enroll Face → Read more

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

Enroll Access Card → Read more

Guide users on how to enroll CSN, Wiegand, and smart cards.

Enroll Mobile Access Cards → Read more

Integrating with Suprema's Airfob Portal enables issuing mobile access cards to users.

Enroll QR/Barcode → Read more

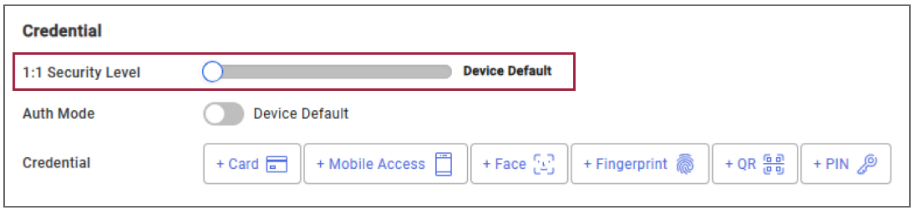
Guide to registering BioStar X QR generation and external issuance QR/Barcode as user authentication methods.

Enroll PIN → Read more

Guide users on how to individually enroll a PIN or bulk enroll via CSV import.

Set Security Level

You can grant separate security levels to users regardless of the biometric 1:N security level set on the device. If users frequently fail authentication when the device's 1:N security level is set high, consider lowering the **1:1 Security Level** to mitigate failed authentications.



Credential

1:1 Security Level: Device Default

Auth Mode: Device Default

Set the desired level in the **1:1 Security Level** field. The available values are as follows:

- **Device Default**
- **Lowest**
- **Low**
- **Normal**
- **High**
- **Highest**

Click **Save** in the upper right corner of the screen to save the settings.

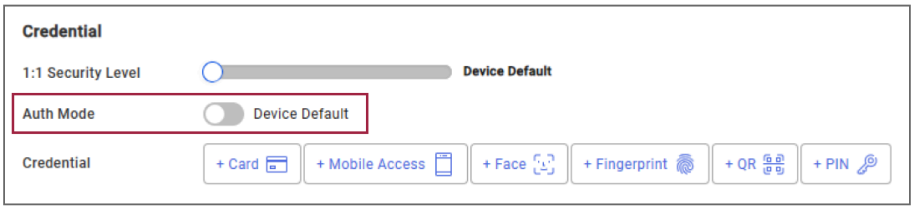
> ⓘ **INFO**
>
> - If you set **Private Auth Mode** in the **Credential** section to **Biometrics**, you cannot apply the 1:1 security level as the input user cannot be identified, and you can only apply the 1:1 security level when a card or ID that allows user identification is set in the authentication mode. For more information about **Private Auth Mode**, refer to the following.
> - Set an appropriate security level. A higher security level may result in lower fingerprint authentication rates or higher False Rejection Rates (FRR).

Authentication Mode Settings

Users can flexibly set authentication methods. You can use the default authentication method set on the device or designate individual authentication modes tailored to each user. Additionally, the extended authentication mode, which includes both facial and fingerprint authentication, enhances security levels.

Device defaults

Setting the **Auth Mode** option to **Device Default** allows for authentication based on the method configured on the device.



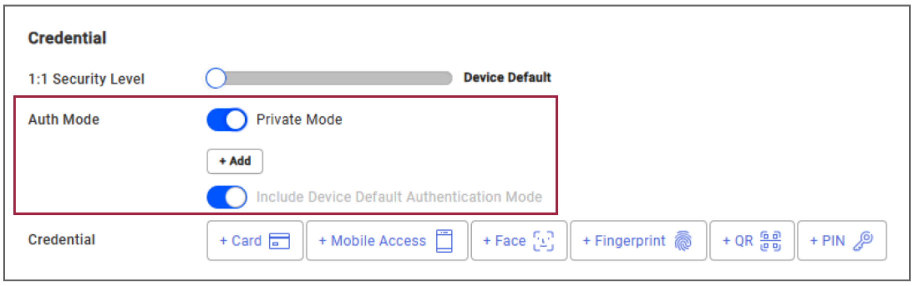
Credential

1:1 Security Level: Device Default

Auth Mode: Device Default

Private authentication mode

Setting the **Auth Mode** option to **Private Mode** enables different authentication methods for each user.



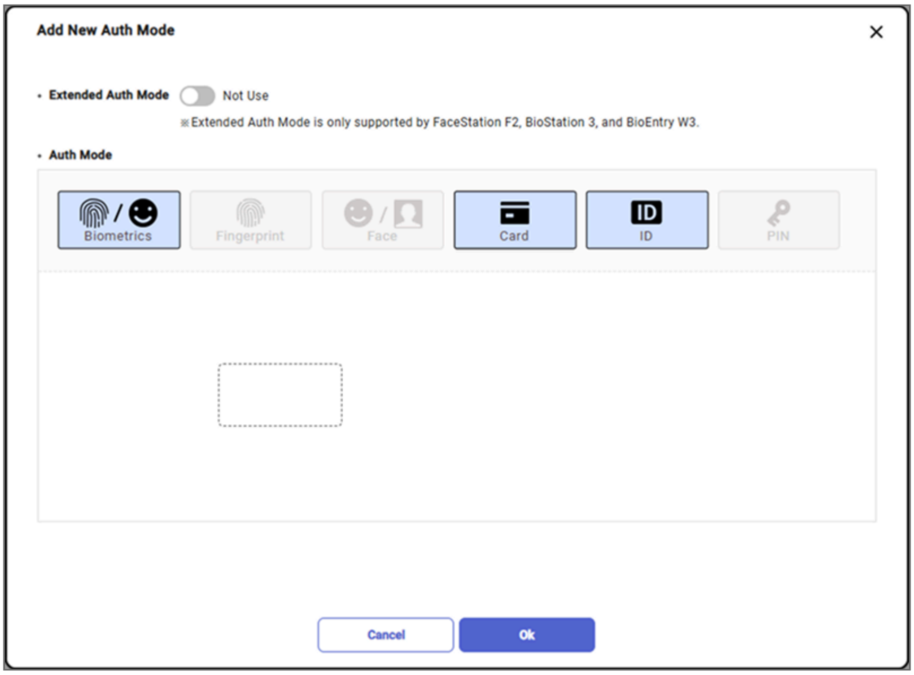
Credential

1:1 Security Level: Device Default

Auth Mode: Private Mode

Include Device Default Authentication Mode

Click the **+ Add** button to open the **Add New Auth Mode** window. Configure the desired authentication methods.



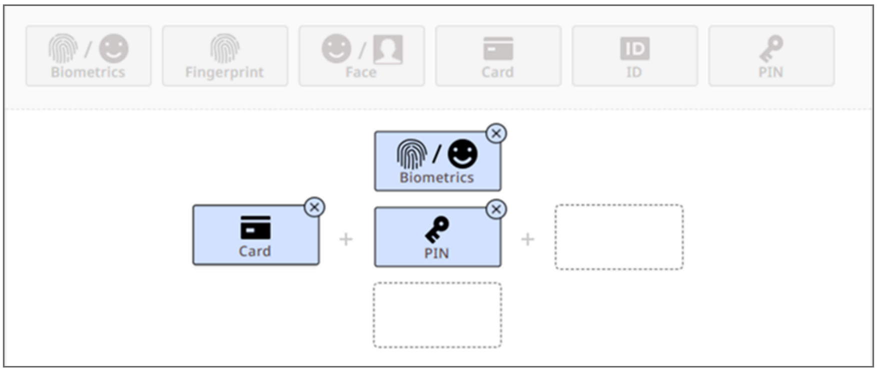
Add New Auth Mode

- Extended Auth Mode: Not Use

※Extended Auth Mode is only supported by FaceStation F2, BioStation 3, and BioEntry W3.

- Auth Mode

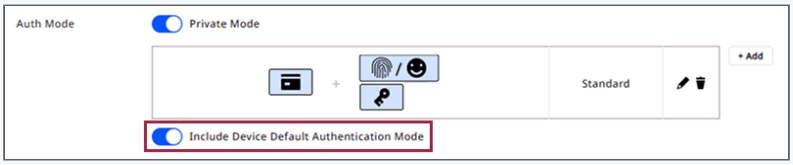
- **Extended Auth Mode**: Set whether to use the extended authentication mode. The extended authentication mode allows for a combination of facial and fingerprint authentication methods.
- **Auth Mode**: Set the authentication methods using drag and drop.



To enroll the configured authentication methods, click the **Apply** button.

INFO

- The **Extended Auth Mode** option is supported on the FaceStation F2, BioStation 3, and BioEntry W3.
- Setting **Include Device Default Authentication Mode** allows the use of both the authentication modes set on the device and the private authentication modes configured in **BioStar X**.



Auth Mode: Private Mode

Include Device Default Authentication Mode

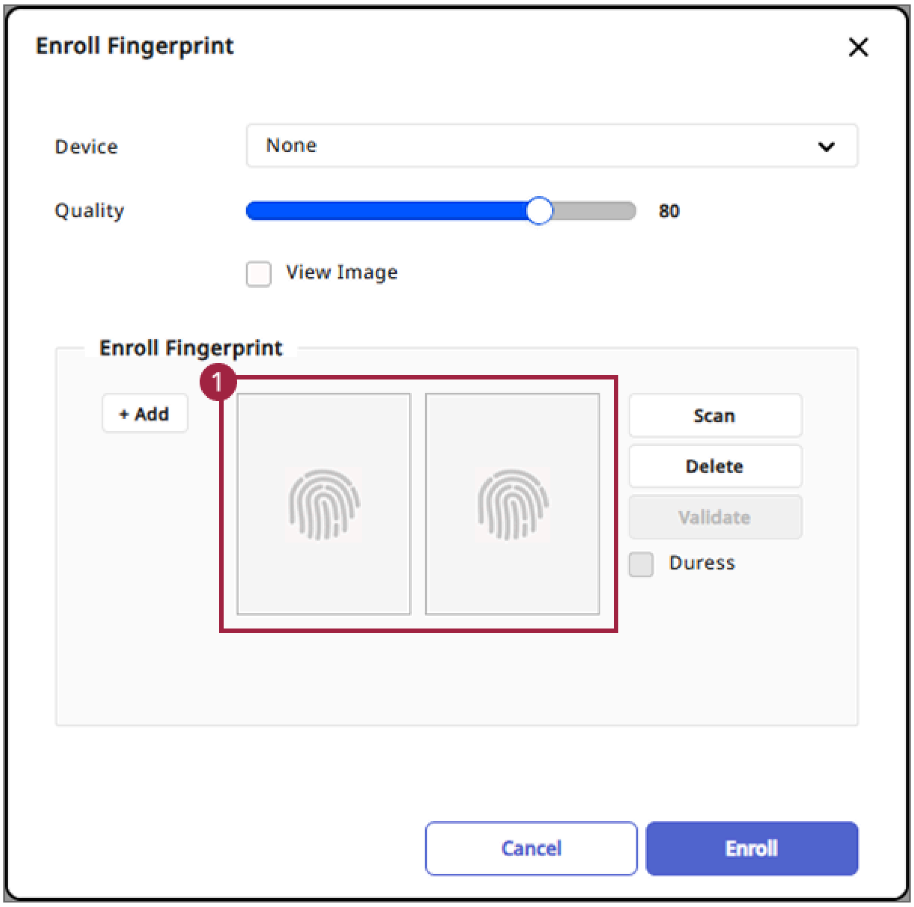
- Setting **Exclude Device Default Authentication Mode** allows only the private authentication modes set in **BioStar X** to be used.

Enroll Fingerprint

You can enroll the user's fingerprint as a means of authentication for access control. Enroll the user's fingerprint information through a device that supports fingerprint authentication. Fingerprints can be scanned on devices equipped with fingerprint scanners.

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

In the **Credential** section, click the **+ Fingerprint** button. When the **Enroll Fingerprint** window appears, configure each item and click the **Enroll** button.



Enroll Fingerprint

Device: None

Quality: 80

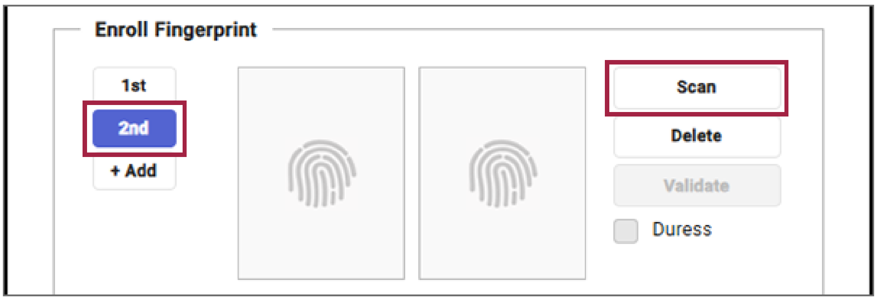
□ View Image

Enroll Fingerprint

□ Duress

- **Device**: Select the device for enrolling the fingerprint.
- **Quality**: You can adjust the fingerprint enrollment quality. Cannot enroll fingerprint information if it does not meet the configured quality level.
- **View Image**: The original image of the scanned fingerprint can be viewed in area 1.
- **+ Add**: Click the button to add a fingerprint. A maximum of 10 fingerprints can be enrolled.
- **Scan**: Select the added fingerprint number and click the button. Place your finger on the fingerprint scanner or

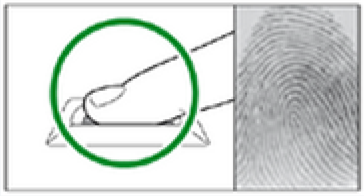
device sensor to scan the fingerprint.

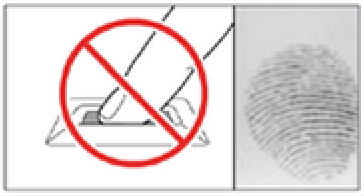


- **Delete**: This allows deleting an enrolled fingerprint. Select the fingerprint number to delete and click the button.
- **Validate**: You can check if it is a previously enrolled fingerprint.
- **Duress**: To enroll a fingerprint as a duress fingerprint, select this option and scan the fingerprint. If you are threatened or forced to open the door, you can use that fingerprint to send a notification.

INFO

- Do not use the fingerprint you use for everyday access as a threat fingerprint.
- When activating the **View Image** option, you can view the fingerprint image, but it is not stored in **BioStar**.
- If the fingerprint authentication rate is low, delete the fingerprint and enroll a new fingerprint.
- To achieve good quality fingerprint, ensure your finger covers the entire surface of the fingerprint recognition sensor. Use the fingerprints of the index or middle finger.





Enroll Face

You can enroll the user's face as a means of authentication for access control. Facial enrollment is an authentication method that captures the user's face with a camera. The user's facial information captured by the camera can be enrolled remotely on a mobile device.

Precautions when enrolling face

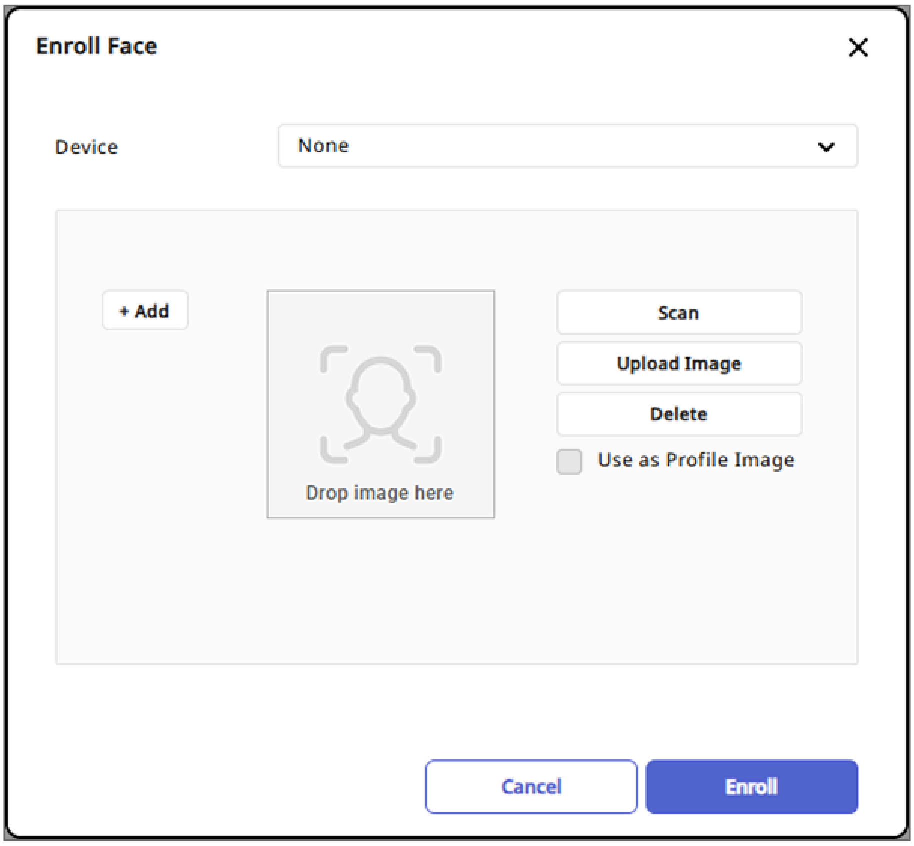
- Keep the distance between the device and your face at 60-100cm when enrolling your face.
- Do not change your face expression.
- Do not wear masks, hats, or eye patches.
- Do not enroll a face wearing a mask. It may increase the False Acceptance Rate (FAR) if both faces with and without a mask are enrolled.
- Do not raise head up or lower head.
- Do not wear thick makeup.
- Do not close your eyes.
- Make sure that both of your shoulders correctly appear on the screen.
- Stand still and enroll your face by staring at the screen.
- Be careful not to display two faces on the screen. Enroll one person at a time.
- If you do not follow the instructions on the screen, the face enrollment may take longer or may fail.

INFO

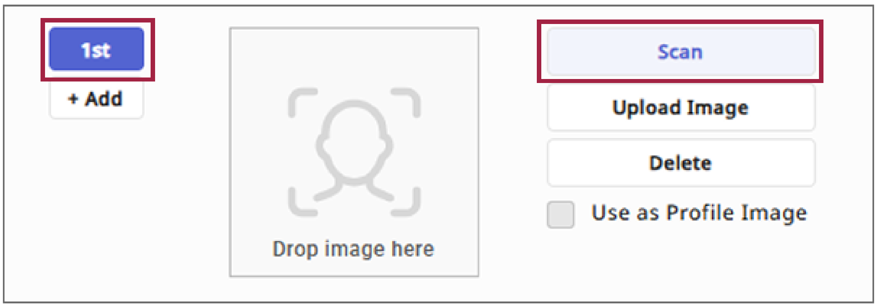
You can use the import from CSV feature or enroll multiple users' faces at once, or send an email link to multiple users for them to enroll their faces directly on a mobile device. For more information, refer to the following.

Enroll by device

Click **+ Face** in the **Credential** section. When the **Enroll Face** window appears, set each item and click **Enroll**.



- **Device**: Select the device for enrolling the face.
- **+ Add**: Click to enroll the face. A maximum of 2 faces can be added.
- **Scan**: Click the added **N-th** button to scan the face. Follow the on-screen instructions to scan the face.



- **Upload Image**: You can upload a face image without scanning.

> ⓘ
> – The maximum file size for supported image types is 10MB.
>
> – Supported image formats include JPG, JPEG, and PNG.

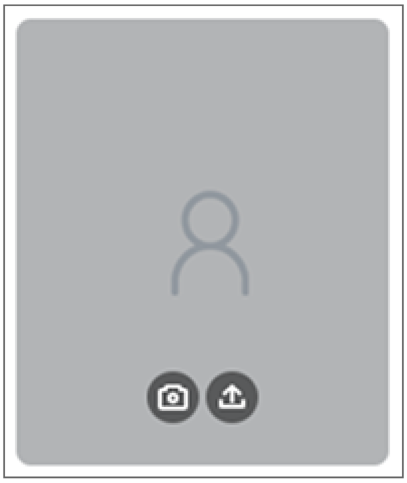
- **Use as profile image**: Check this option if you want to use the scanned face image as a profile image.
- **Delete**: You can delete the face credential. Select the number to delete and click the button.

> **INFO**
>
> - Devices that can enroll faces are as follows:
>   - FaceStation F2
>   - BioStation 3
>   - BioEntry W3
> - If the face authentication rate is low, delete face information and enroll a new face.

Enroll with a webcam or photo image

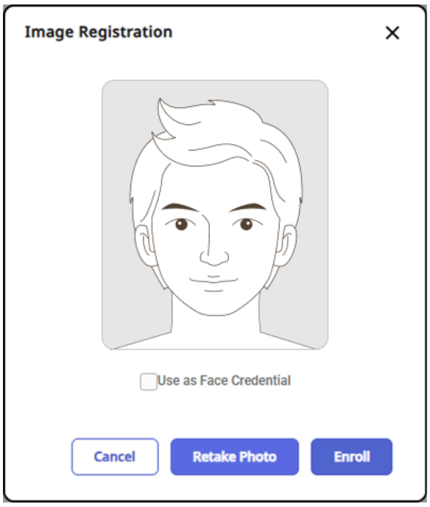
You can take a photo with a webcam connected to your PC, set the captured photo as a user profile picture, and enroll the face as a credential. Or you can enroll the uploaded photo as a face credential.

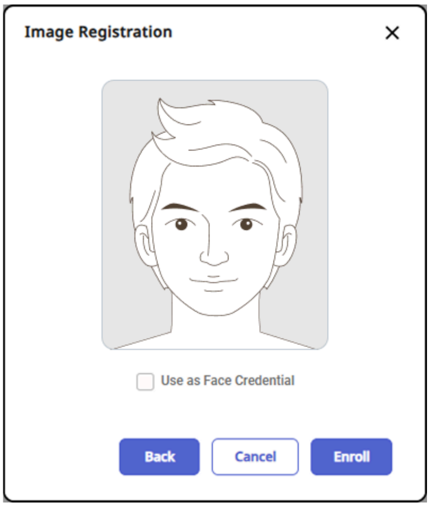
1. Connect the webcam to the PC.
2. Hover over the profile image area at the top right of the screen and click the 📷 button that appears. To upload an image saved on your PC, click the ⭱ button.



3. When the **Image Registration** window appears, click **Take photo** or **Upload photo**.

4. If you take a photo with the webcam, the photo displays, and if you upload a photo from the PC, it displays the uploaded photo.





5. To enroll the photo taken with the webcam or the uploaded photo as a face credential, click the checkbox for the **Use as Face Credential** option.

6. To complete facial enrollment, click **Enroll**.

ⓘ **INFO**

- If you are using the webcam for the first time, a pop-up asking for camera permission from the browser appears. To utilize the webcam functionality, granting permission for the browser's camera is required.
- The process of allowing camera access may differ depending on the browser.
- It may take a few seconds to click the **Take photo** button and take the photo.
- It is recommended to use Google Chrome version 100 or higher.
- The maximum size for an image file to upload is 10MB.
- Supported image formats include JPG, JPEG, and PNG.
- Cautions for enrolling a visual face with a webcam
  - Maintain a reasonable distance from the webcam.
  - Enroll your face straight ahead without moving.
  - Do not change your face expression.
  - Do not wear masks, hats, or eye patches.
  - Do not raise head up or lower head.
  - Do not wear thick makeup.
  - Do not close your eyes.
  - Make sure both shoulders are visible.
  - Be careful not to display two faces on the screen. Enroll one person at a time.

Enroll Access Card

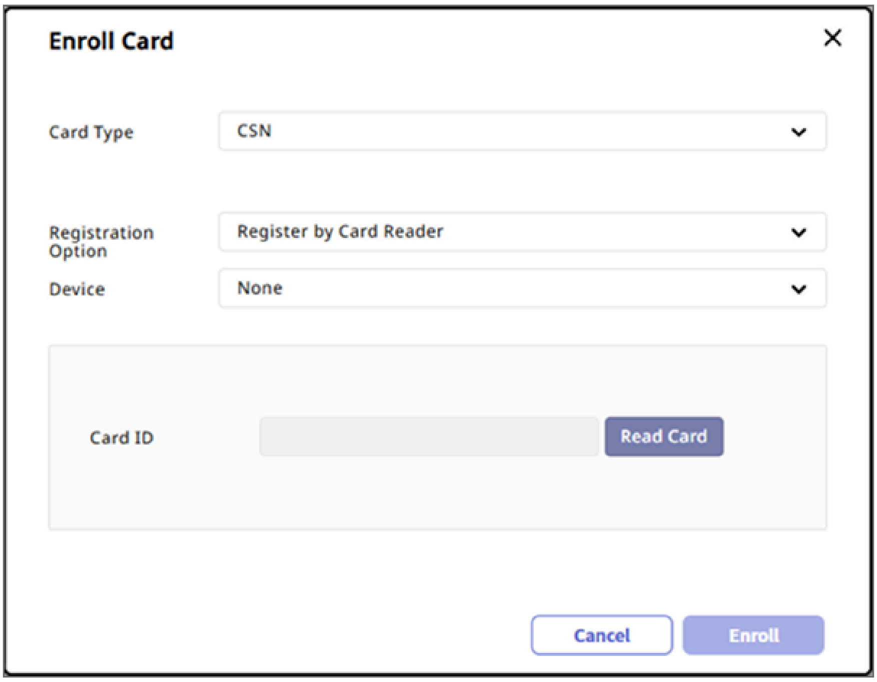
Guide users on how to enroll access cards. Explain the enrollment methods for CSN cards, Wiegand cards, and smart cards, as well as the card reading/formatting features. Refer to the manual of the device for the types of cards supported by the device.

Card enrollment using a USB agent

Card Type	CSN	Wiegand	Smart Card
EM	❌	❌	❌
MIFARE	✅	❌	✅
DESFire	✅	❌	✅
FeliCa	✅	❌	❌
HID Prox	❌	❌	❌
HID iCLASS	❌	❌	❌

CSN card

1. In the **Credential** section, click the **+ Card** button.
2. When the **Enroll Card** window appears, select **CSN** from the **Card Type** options.



Enroll Card

Card Type: CSN

Registration Option: Register by Card Reader

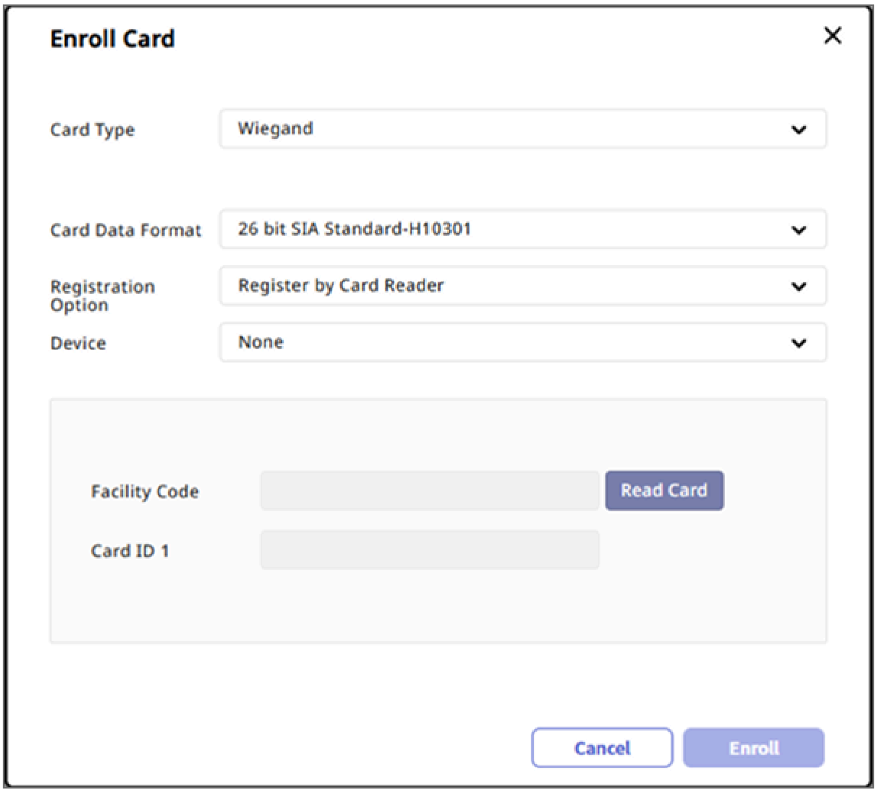
Device: None

Card ID

3. Select your desired card enrollment method from the **Registration Option** field.
   - **Register by Card Reader**: Select the device from the **Device** list to scan the card and click the **Read Card** button.
   - **Assign Card**: Select the card you want to assign to the user from the list. You can search through the input field.
   - **Enter Manually**: Enter the card number manually or click the **Use User ID** button.
4. Click the **Enroll** button.

Wiegand card

1. In the **Credential** section, click the **+ Card** button.
2. When the **Enroll Card** window appears, select **Wiegand** from the **Card Type** options.



Enroll Card

Card Type: Wiegand

Card Data Format: 26 bit SIA Standard-H10301

Registration Option: Register by Card Reader

Device: None

Facility Code

Card ID 1

3. Select the desired format from the **Card Data Format** field.
4. Select your desired card enrollment method from the **Registration Option** field.
   - **Register by Card Reader**: Select the device from the **Device** list to scan the card and click the **Read Card** button.
   - **Assign Card**: Select the card you want to assign to the user from the list. You can search through the input field.
   - **Enter Manually**: Enter the facility code and card ID manually.
5. Click the **Enroll** button.

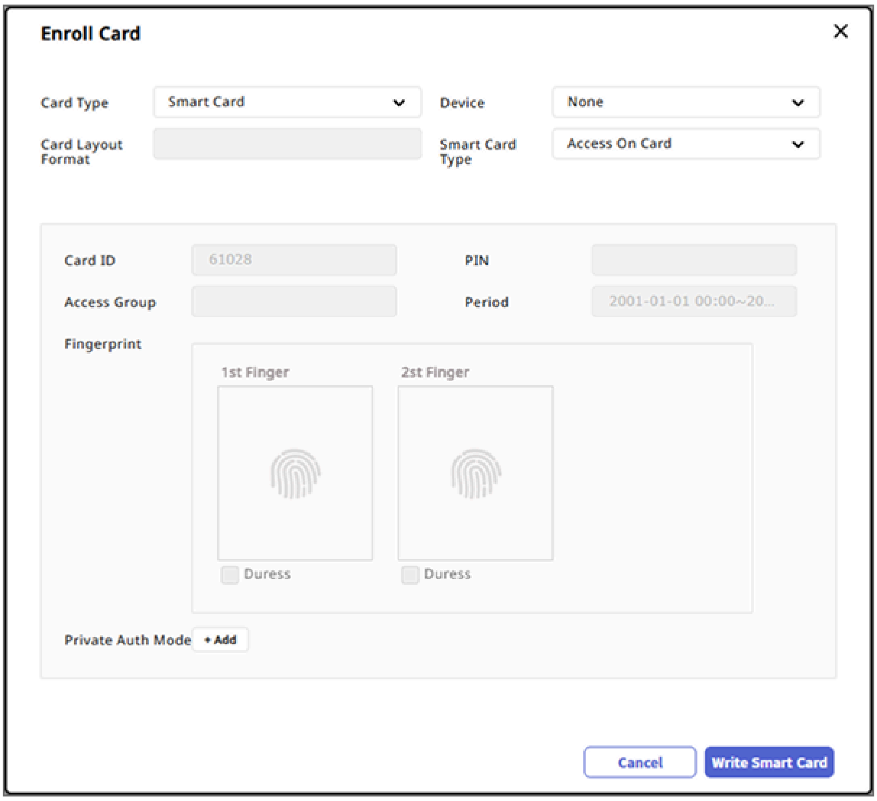
INFO

If the desired card data format is not available in the **Card Data Format** options, refer to the following.

Smart card

Enroll a security credential card, access-on card, or custom smart card.

1. In the **Credential** section, click the **+ Card** button.
2. When the **Enroll Card** window appears, select **Smart Card** from the **Card Type** options.



Enroll Card

Card Type: Smart Card

Device: None

Card Layout Format:

Smart Card Type: Access On Card

Card ID: 61028

PIN:

Access Group:

Period: 2001-01-01 00:00~20...

Fingerprint

3. Select the device for card enrollment from the **Device** field.
4. Once selected, the card layout format set in the **Card Layout Format** field will be displayed.
5. Select the desired card type from **Smart Card Type**.
   - **Secure Credential Card**: User information (card ID, PIN, access group, duration, fingerprint template, face template, private authentication mode) can be stored on the card.
   - **Access On Card**: User information (card ID, PIN, fingerprint template, face template) can be stored on the card.
   - **Custom Smart Card**: Enroll a smart card issued by a third party. Click the **Read Card** button to enroll the card ID.
6. Select the desired fingerprint template.
7. Click the **Write Smart Card** button.

ⓘ **INFO**

- To issue a smart card, the correct card type must be set. For more information about card types, refer to the following.
- The user information stored on the smart card uses information stored in **BioStar X**. Failure to store updated user information may result in incorrect information being stored on the smart card. Additionally, if the updated user information is not synchronized with the device, the device may fail to perform authentication.
- To use a face template, select **Use Face Template** in the **Layout** section when adding a new smart card in the **Settings** → **Credential** → **Card Format** menu. For more information, refer to the following.
- Access On Card cannot set the card ID manually.
- For devices and firmware versions supporting Custom Smart Card, refer to the list below.

  View devices and firmware versions that support custom smart cards

  – XPass D2 firmware version 1.7.1 or higher

  – BioEntry P2 firmware version 1.5.1 or higher

  – BioEntry W2 firmware version 1.8.0 or higher

  – BioStation 2a firmware version 1.1.0 or higher

  – X-Station 2 firmware version 1.3.0 or higher

  – BioStation 3 firmware version 1.3.0 or higher

  – BioEntry W3 firmware version 1.0.0 or higher

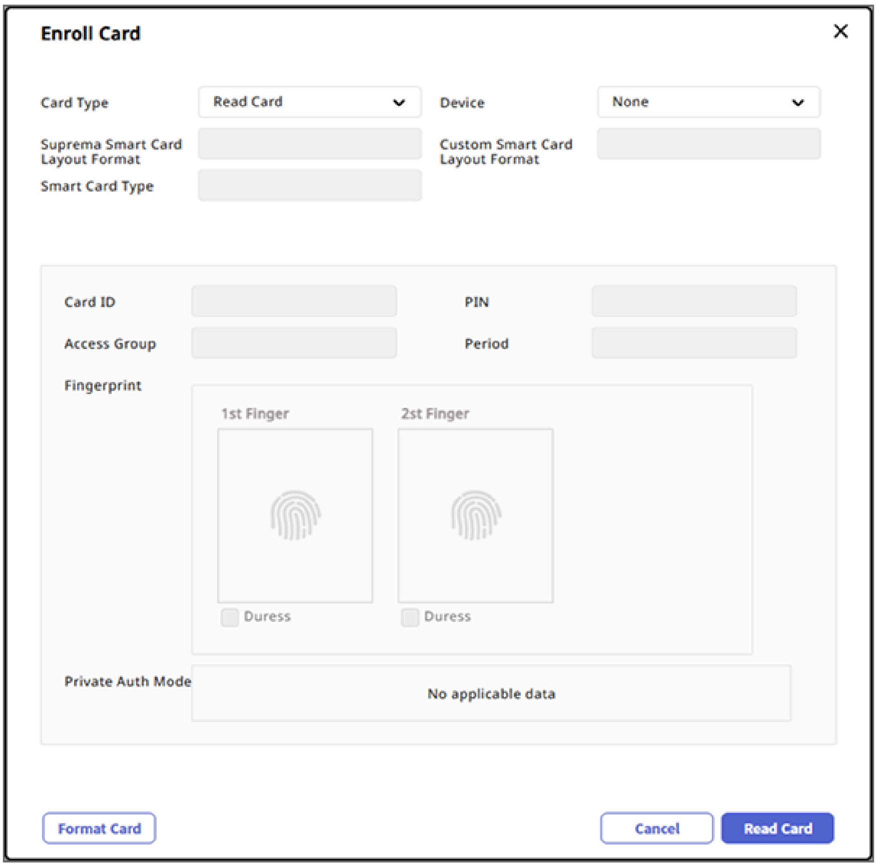
  – BioLite N2 firmware version 1.6.2 or higher
- To set up the smart card layout, refer to the following.
- To format the smart card and rewrite information, refer to the following.

Reading card/format

You can format smart cards and rewrite information.

1. In the **Credential** section, click the **+ Card** button.

2. When the **Enroll Card** window appears, select **Read Card** from the **Card Type** options.



Enroll Card

Card Type: Read Card

Device: None

Private Auth Mode: No applicable data

3. Select the device capable of reading smart cards from the **Device** field.

4. Select the **Smart Card Type**.

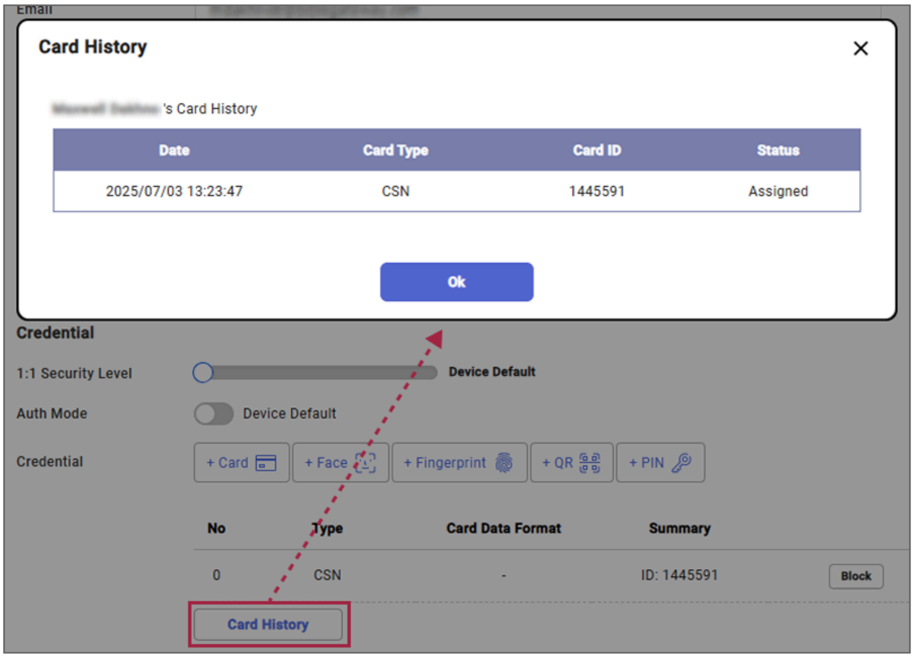
5. Click the **Read Card** button.

6. Verify the card information and click the **Format Card** button.

> **INFO**
>
> - The list of devices in the **Device** field will only display devices with the smart card layout set. For more information about setting this up, refer to the following.
> - Custom smart cards cannot be formatted.

Assigned card information confirmation

To view the assigned card information for the user, click the **Card History** button in the **Credential** section. You can check the date of card assignment, card type, card ID, and status.



Card History

's Card History

Date	Card Type	Card ID	Status
2025/07/03 13:23:47	CSN	1445591	Assigned

Credential

1:1 Security Level: Device Default

Auth Mode: Device Default

No	Type	Card Data Format	Summary
0	CSN	-	ID: 1445591

Enroll Mobile Access Cards

Integrating with Suprema's Airfob Portal enables issuing mobile access cards to users. Users can enroll mobile access cards individually or use the CSV import feature to enroll multiple users at once.

You need to enter the user's email according to the method of sending mobile access cards set up in the AirPop portal.

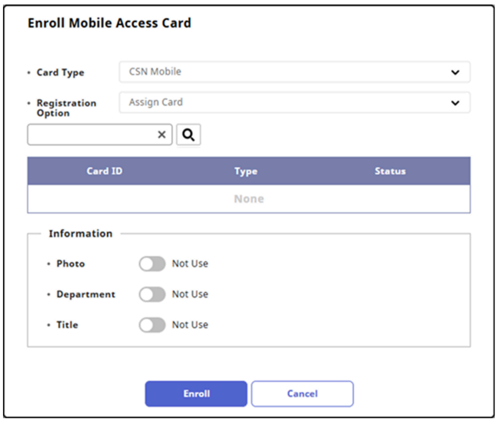
> **INFO**
>
> - Only one of the **CSN Mobile Card** or the **Template on Mobile** can be used.
> - This feature can only be used when linked with the Airfob portal. For more information regarding the Airfob Portal and mobile access card use, refer to the following.

CSN mobile

You can issue CSN mobile access cards to users.

Card assignment

1. Click the **Mobile Access** button in the **Credential** section.
2. When the **Enroll Mobile Access Card** window appears, select **Card Type** option and select **CSN Mobile**.
3. In the **Registration Option** options, select **Assign Card**.



Enroll Mobile Access Card

Card Type: CSN Mobile

Registration Option: Assign Card

Card ID	Type	Status
None		

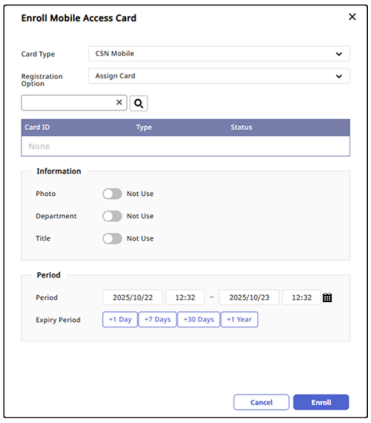
Information

Photo: Not Use

Department: Not Use

Title: Not Use

Airfob portal site: Regular



Enroll Mobile Access Card

Card Type: CSN Mobile

Registration Option: Assign Card

Card ID	Type	Status
None		

Information

Photo: Not Use

Department: Not Use

Title: Not Use

Period

Period: 2025/10/22 12:32 ~ 2025/10/23 12:32

Airfob portal site: Dynamic

> The **Period** item is activated when setting a **dynamic** site upon site creation in the AirPop portal. You can set the expiration duration and usage period for the mobile access cards. For more information about the Airfob Portal, refer to the following link.

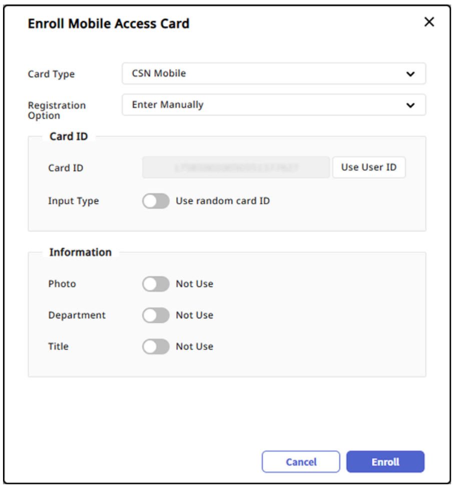
4. Select or search for the card desired to assign from the card list.

5. Set the Info and Period.
6. Click the Enroll button.

> **INFO**
>
> - If you have enabled the Photo, Department, and Title options in the Info section, that information can be displayed on the user's mobile access card. The items displayed at this time are based on the information entered by the user. For more information on entering user basic information, refer to the following.

Enter manually

1. Click the Mobile Access button in the Credential section.
2. When the Enroll Mobile Access Card window appears, select Card Type option and select CSN Mobile.
3. Select Enter Manually from the Registration Option options.



Enroll Mobile Access Card

Card Type: CSN Mobile

Registration Option: Enter Manually

Card ID

Card ID: Use User ID

Input Type: Use random card ID

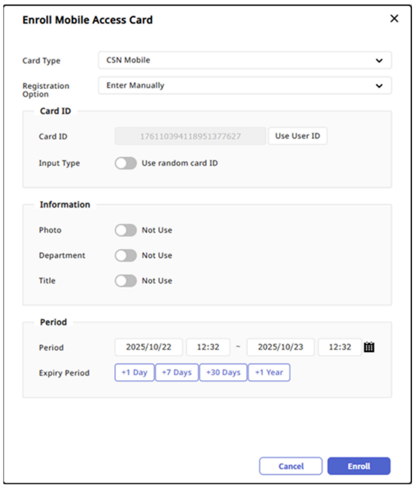
Information

Photo: Not Use

Department: Not Use

Title: Not Use

Airfob portal site: Regular



Enroll Mobile Access Card

Card Type: CSN Mobile

Registration Option: Enter Manually

Card ID

Card ID: 176110394118951377627 Use User ID

Input Type: Use random card ID

Information

Photo: Not Use

Department: Not Use

Title: Not Use

Period

Period: 2025/10/22 12:32 ~ 2025/10/23 12:32

Expiry Period: +1 Day +7 Days +30 Days +1 Year

Airfob portal site: Dynamic

> The Period item is activated when setting a **dynamic** site upon site creation in the AirPop portal. You can set the expiration duration and usage period for the mobile access cards. For more information about the Airfob Portal, refer to the following link.

4. Select Input Type.
   - Use random card ID: Automatically generate a card ID.
   - Use User ID: Uses the user ID as the card ID.
   - Enter manually: Allows manual entry of the card ID.
5. Set the Info and Period.
6. Click the Enroll button.

ⓘ **INFO**

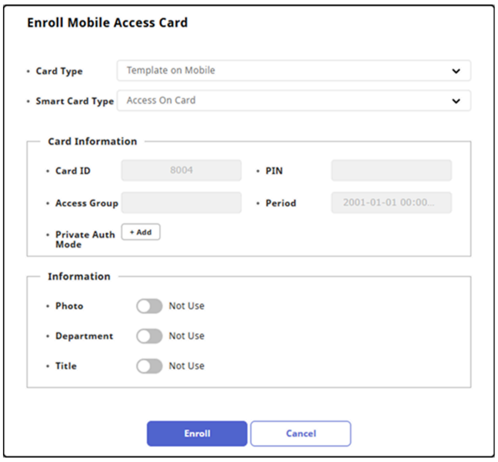
- If you have enabled the **Photo**, **Department**, and **Title** options in the **Info** section, that information can be displayed on the user's mobile access card. The items displayed at this time are based on the information entered by the user. For more information on entering user basic information, refer to the following.
- If the user has lost or deleted the activation link sent via email, click the **resend** button to reissue the activation link.
- For more information about the CSN mobile application, refer to the following link.

Template on Mobile

Template on Mobile is a mobile access card that stores the user's biometric template on a mobile device. It can authenticate biometrically without storing user data on the **BioStar X** server or the AirPop portal (Airfob Portal) and device.

This feature is useful for environments that want to use biometrics as credentials but cannot store biometric information on the server and device due to privacy concerns. Since the issuance of **Template on Mobile** and the biometric template registration process are conducted separately, users can enroll their face directly on **Template on Mobile** supported devices without facing an administrator.

1. Click the **Mobile Access** button in the **Credential** section.
2. When the **Enroll Mobile Access Card** window appears, select **Card Type** option and select **Template on Mobile**.



Enroll Mobile Access Card

- Card Type: Template on Mobile
- Smart Card Type: Access On Card

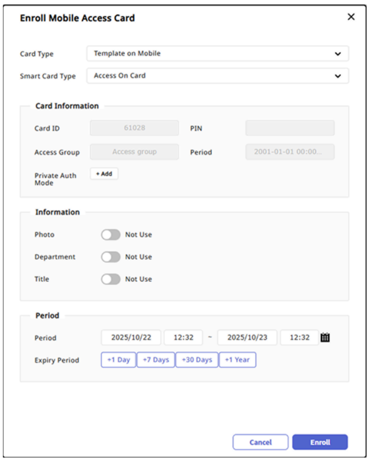
Card Information

- Card ID: 8004
- PIN:
- Access Group:
- Period: 2001-01-01 00:00...
- Private Auth Mode: + Add

Information

- Photo: Not Use
- Department: Not Use
- Title: Not Use

Airfob portal site: Regular



Enroll Mobile Access Card

Card Type: Template on Mobile
Smart Card Type: Access On Card

Card Information

Card ID: 61028
PIN:
Access Group: Access group
Period: 2001-01-01 00:00...
Private Auth Mode: + Add

Information

Photo: Not Use
Department: Not Use
Title: Not Use

Period

Period: 2025/10/22 12:32 ~ 2025/10/23 12:32
Expiry Period: +1 Day, +7 Days, +30 Days, +1 Year

Airfob portal site: Dynamic

ⓘ The **Period** item is activated when setting a **dynamic** site upon site creation in the AirPop portal. You can set the expiration duration and usage period for the mobile access cards. For more information about the Airfob Portal, refer to the following link.

3. Select the desired card type from **Smart Card Type**.
   - **Access On Card**: User information (card ID, PIN, access group, duration, private authentication mode) can be stored on the card.
   - **Secure Credential Card**: Secure credential card. User card ID and PIN data can be stored.

4. Set the **Info** and **Period**.
5. Click the **Enroll** button.

An issuance email will be sent to the registered user's email address. The user must install the Airfob Pass application through the link in the email to complete the issuance of the **Template on Mobile**.

> **TIP**
>
> **How to Template on Mobile Authentication**
>
> The user tags the mobile device that issued the **Template on Mobile** against the auth device and follows the on-screen prompts to authenticate their face.

> **INFO**
>
> - If you have enabled the **Photo**, **Department**, and **Title** options in the **Info** section, that information can be displayed on the user's mobile access card. The items displayed at this time are based on the information entered by the user. For more information on entering user basic information, refer to the following.
> - For devices and firmware versions that support **Template on Mobile**, refer to the list below.
>   - BioStation 3 firmware version 1.2.0 or higher
>   - BioEntry W3 firmware version 1.0.0 or higher
>   - FaceStation F2 Firmware version 2.2.0 or higher
> - Only one mobile access card can be issued: either **CSN mobile card** or **Template on Mobile**.

Enroll QR/Barcode

Guide to registering QR code or barcode as user authentication methods. You can enroll QR codes generated directly by **BioStar X** and QR/barcodes issued externally.

INFO

- Devices that include scanners capable of QR/Barcode authentication are listed below.
  - X-Station 2 (XS2-QDPB, XS2-QAPB)
- Devices that include cameras capable of QR/Barcode authentication are included in the list below.
  - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) firmware version 1.2.0 or higher
  - BioStation 3 (BS3-DB, BS3-APWB) firmware version 1.1.0 or higher
  - A separate device license is required to use QR/Barcode authentication with a camera. For more information, refer to the following.

BioStar X QR

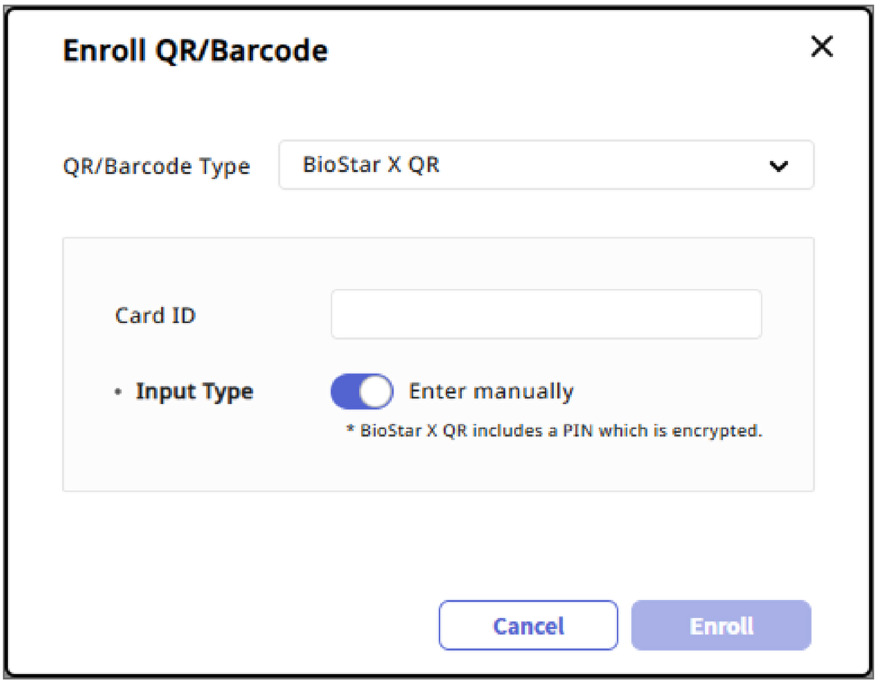
You can issue a QR code containing an encrypted PIN to allow user access.

Before you start

- Complete the email information settings, including SMTP configuration, before using **BioStar QR**. For more information, refer to the following.
- To issue **BioStar QR**, you must register an email address in the user information. For more information, refer to the following.

1. Click **+ QR/Barcode** in the **Credential** section.

2. When the **Enroll QR/Barcode** window appears, select **BioStar QR** from the **QR/Barcode Type**.



3. Select **Input Type**.
    - **Use random card ID**: Automatically generate a card ID.
    - **Enter manually**: Enter the card ID manually.
4. Click the **Enroll** button.

Then, when a user authenticates access, QR codes are issued and sent to the email address registered with user information. The user can scan the QR code included in the email on the device to gain access.

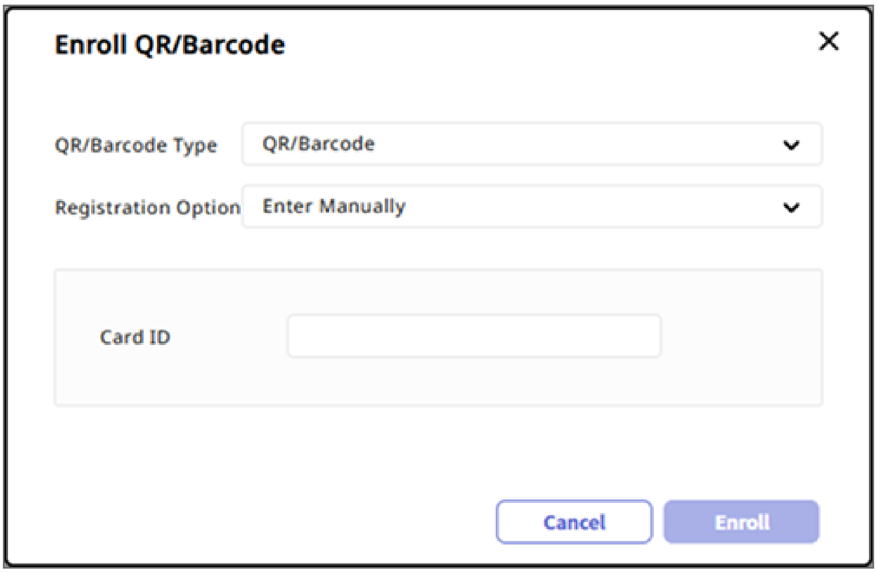
> **INFO**
>
> To prevent duplicate card ID creation, it is recommended to set **Input Type** to **Use random card ID**.

QR/Barcode

Register a QR/barcode issued by other external issuers for users.

1. Click **+ QR/Barcode** in the **Credential** section.

2. When the **Enroll QR/Barcode** window appears, select **QR/Barcode** from the **QR/Barcode Type** options.



Enroll QR/Barcode

QR/Barcode Type: QR/Barcode

Registration Option: Enter Manually

Card ID

3. Select **Enter Manually** from the **Registration Option** options.
4. Enter the previously issued QR/barcode ID directly in the **Card ID** option.
5. Click the **Enroll** button.

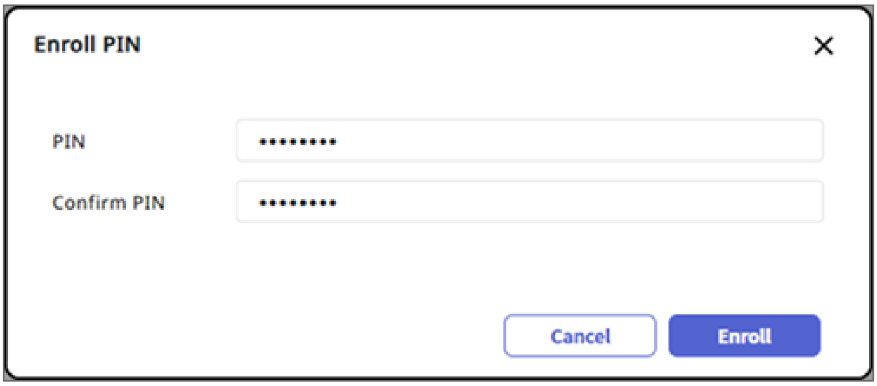
> **INFO**
>
> In the **Card ID** option, you can input up to 32 characters, including English letters, numbers, and special characters.

Enroll PIN

Guide the user on how to enroll a PIN so they can access by entering it on the device. You can enroll a PIN for individual users or bulk enroll multiple users via CSV import.

Enroll PIN

1. Click **PIN** in the **Credential** section.



PIN ••••••••

Confirm PIN ••••••••

2. Once the input field is activated, enter the password.
3. Enter the same password in **Confirm PIN**.
4. Click the **Enroll** button.

> **INFO**
>
> - The PIN must be at least 8 characters long and can only contain numbers.
> - You can enroll a maximum of one PIN credential per user.

Enroll PIN via CSV import

Use the CSV import feature to enroll multiple users at once.

1. Add a `pin` column to the CSV file to be imported.
2. Enter the user's PIN in the `pin` column and save the CSV file.
3. Navigate to the **User** page.
4. Click ⋯ at the top right of the screen and select **Import** → **CSV**.
5. Follow the prompts on the screen to select the CSV file and set the import options.

INFO

- You can enroll a maximum of one PIN credential per user.
- For more information about the CSV import feature, refer to the following.

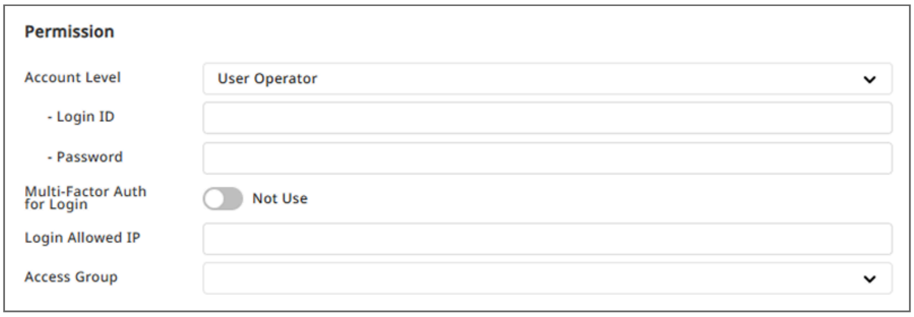
Setting User Permissions

According to the organization's security policy, you can differentiate user-specific operational privileges and access permissions for **BioStar X**. Restrict access to main menus through administrator levels and control access to physical spaces through access groups. You can also enhance security through IP address restrictions and multi-factor authentication.

Go to the **User** page and set access permissions using the two methods below.

- **New User**: Click the **New User** button at the top right of the screen. The **New User** window appears.
- **Existing User**: Double-click a user in the user list. Or, click the user and click the **See More** button in the preview screen displayed on the right side of the screen. A window for editing user information appears.

In the **Permission** section, the following items can be set. Refer to the descriptions for each item to set appropriate user permissions.



Permission

Account Level	User Operator
- Login ID	
- Password	
Multi-Factor Auth for Login	Not Use
Login Allowed IP	
Access Group	

Select administrator level

The menus accessible will be limited based on the selected administrator level. Select the user's administrator level in the **Permission** section, under the **Account Level** item. Refer to the list below for the administrator levels that can be assigned to users.

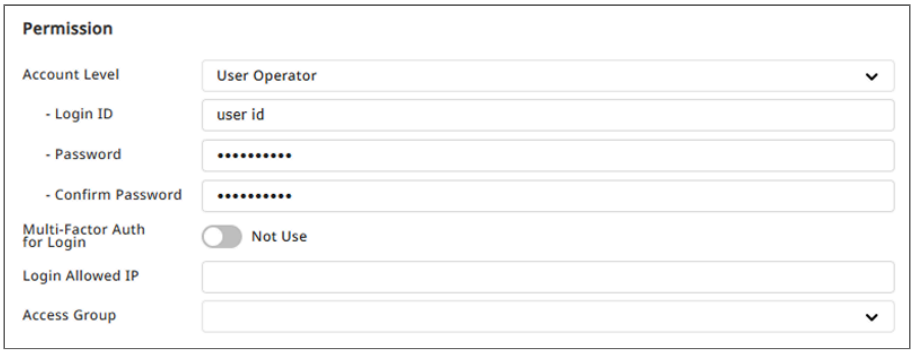
- **Administrator**: This is an administrator level that can use all menus.
- **User Operator**: **User** menu has **read** and **write** permissions.
- **Monitoring Operator**: **Monitoring**, **Data**, and **Dashboard** menus have **read** and **write** permissions.
- **T&A Operator**: **TIME ATTENDANCE** menu has **read** and **write** permissions.
- **Visitor Operator**: **VISITOR** menu has **read** and **write** permissions.

INFO

- Select **None** if you do not want to set an admin level. In this case, the user cannot log in to **BioStar X**.
- To add new user permissions other than the predefined ones, refer to the following.
- The permissions of the default accounts cannot be modified or deleted.
- Levels such as **T&A Operator** and **Visitor Operator** require separate licenses. For more information on licensing policy, refer to the following.

Set login ID and password

If you selected an administrator level, you must set the ID and password to be used when the user logs in to **BioStar X**.



Permission

Account Level	User Operator
- Login ID	user id
- Password	••••••••••
- Confirm Password	••••••••••
Multi-Factor Auth for Login	Not Use
Login Allowed IP	
Access Group	

INFO

Precautions when setting ID and password

- Set the ID to a combination of letters and numbers between 8 and 32 characters.
- For more information on password policy configuration, refer to the following.
- Avoid using passwords that are vulnerable to security.
  - Consecutive characters or numbers (e.g., abcd, 1234)
  - Common words or patterns (e.g., qwerty, password)

Multi-Factor Authentication Setting

Enabling **Multi-Factor Auth for Login** allows users to log into **BioStar X** with added fingerprint authentication.

INFO

For more information about the multi-factor authentication settings, refer to this document.

Login settings with user IP address

If you register a user IP address, you can log in to the PC only when the IP information matches the one registered to your account. This enhances security. Enter the user's IP address in the **Login Allowed IP** field of the **Permission** section.

> ⓘ **INFO**
>
> - IP addresses can be entered in the format xxx.xxx.xxx.xxx, and each octet must contain a number in the range of 0–255.
> - If the IP address is not registered, PC login will be allowed regardless of IP information.

Select access group

Set the user's access group to restrict access by organization or department. In the **Permission** section, select the access group from **Access Group**.

> ⓘ **INFO**
>
> For more information about adding and managing access groups, refer to the following.

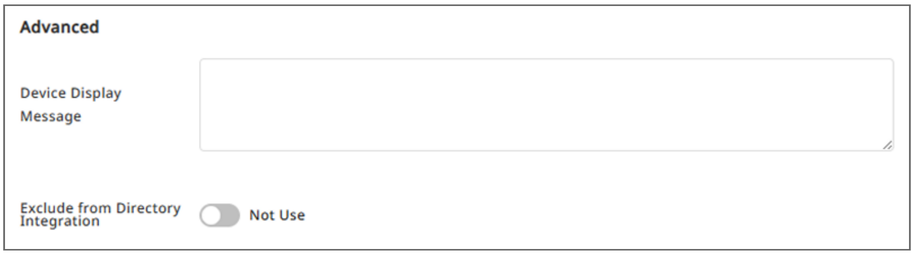
Configure User Advanced Settings

You can set messages to display on the device when the user enters or exclude the user from synchronization during Directory Service integration. This feature can be set when adding or editing a user.

Go to the **User** page and set access permissions using the two methods below.

- **New User**: Click the **New User** button at the top right of the screen. The **New User** window appears.
- **Existing User**: Double-click a user in the user list. Or, click the user and click the **See More** button in the preview screen displayed on the right side of the screen. A window for editing user information appears.

The items that can be set in the **Advanced** section are as follows.



Advanced

Device Display Message

Exclude from Directory Integration: Not Use

- **Device Display Message**: You can enter a message to display on the device when the user enters. You can enter up to 128 characters for the message.
- **Exclude from Directory Integration**: You can exclude the user from synchronization during Directory Service integration.

> **INFO**
>
> - The **Exclude from Directory Integration** option is available through additional options for **Advanced** or higher licenses. For more information on licensing policy, refer to the following.
> - For more information on directory integration settings, refer to the following.

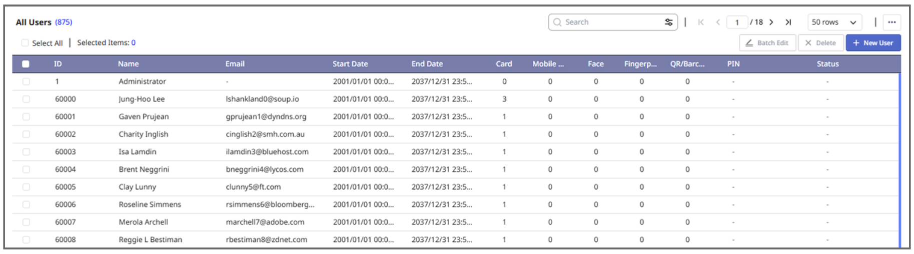
Explore Users

This guide explains how to view and manage registered users on the user list page. You can quickly find desired users through general and advanced searches, and use features like list sorting, column settings, and printing.

To access the **User** page, click **User** in the **Launcher** or select **User** from the menu at the top left of the screen.

View user list

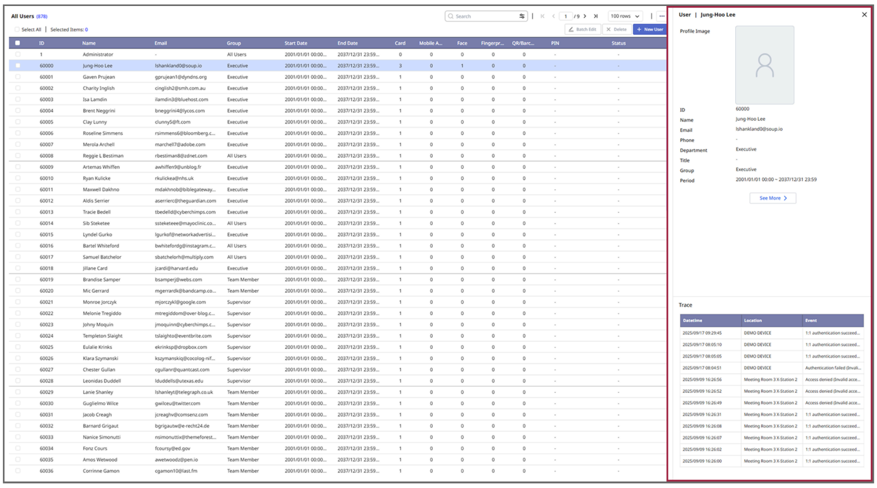
On the user list page, you can check the basic information and status of users, and view or edit the detailed information of each user.



ID	Name	Email	Start Date	End Date	Card	Mobile ...	Face	Fingerp...	QR/Barc...	PIN	Status
1	Administrator	-	2001/01/01 00:0...	2037/12/31 23:5...	0	0	0	0	0	-	-
60000	Jung-Hoo Lee	lshankland0@soup.io	2001/01/01 00:0...	2037/12/31 23:5...	3	0	0	0	0	-	-
60001	Gaven Prujean	gprujean1@dyndns.org	2001/01/01 00:0...	2037/12/31 23:5...	1	0	0	0	0	-	-
60002	Charity Inglish	cinglish2@smh.com.au	2001/01/01 00:0...	2037/12/31 23:5...	1	0	0	0	0	-	-
60003	Isa Lamdin	ilamdin3@bluehost.com	2001/01/01 00:0...	2037/12/31 23:5...	1	0	0	0	0	-	-
60004	Brent Neggrini	bneggrini4@lycos.com	2001/01/01 00:0...	2037/12/31 23:5...	1	0	0	0	0	-	-
60005	Clay Lunny	clunny5@ft.com	2001/01/01 00:0...	2037/12/31 23:5...	1	0	0	0	0	-	-
60006	Roseline Simmens	rsimmens6@bloomberg...	2001/01/01 00:0...	2037/12/31 23:5...	1	0	0	0	0	-	-
60007	Merola Archell	marchell7@adobe.com	2001/01/01 00:0...	2037/12/31 23:5...	1	0	0	0	0	-	-
60008	Reggie L Bestiman	rbestiman8@zdnet.com	2001/01/01 00:0...	2037/12/31 23:5...	1	0	0	0	0	-	-

The user list displays all registered users, and you can check each user's ID, name, email address, duration, status of enrolled credentials. Users are listed in order by their ID.

- To view the detailed information of an individual user, click on the desired user in the user list. User profile information will be displayed on the right side of the screen. Click the **See More** button in the user profile information to navigate to the page where you can edit detailed user information.



ID	Name	Email	Group	Start Date	End Date	Card	Mobile A...	Face	Fingerpr...	QR/Barc...	PIN	Status
1	Administrator	-	All Users	2001/01/01 00:00...	2037/12/31 23:59...	0	0	0	0	0	-	-
60000	Jung-Hoo Lee	lshankland0@soup.io	Executive	2001/01/01 00:00...	2037/12/31 23:59...	3	0	1	0	0	-	-
60001	Gaven Prujean	gprujean1@dyndns.org	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60002	Charity Inglish	cinglish2@smh.com.au	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60003	Isa Lamdin	ilamdin3@bluehost.com	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60004	Brent Neggrini	bneggrini4@lycos.com	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60005	Clay Lunny	clunny5@ft.com	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60006	Roseline Simmens	rsimmens6@bloomberg.c...	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60007	Merola Archell	marchell7@adobe.com	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60008	Reggie L Bestiman	rbestiman8@zdnet.com	All Users	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60009	Artemas Whiffen	awhiffen9@unblog.fr	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60010	Ryan Kulicke	rkulickea@nhs.uk	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60011	Maxwell Dakhno	mdakhnob@biblegateway...	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60012	Aldis Serrier	aserrierc@theguardian.com	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60013	Tracie Bedell	tbedelld@cyberchimps.com	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60014	Sib Steketee	ssteketeee@mayoclinic.co...	All Users	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60015	Lyndel Gurko	lgurkof@networkadvertisi...	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60016	Bartel Whiteford	bwhitefordg@instagram.c...	All Users	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60017	Samuel Batchelor	sbatchelorh@multiply.com	All Users	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60018	Jillane Card	jcardi@harvard.edu	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60019	Brandise Samper	bsamperj@webs.com	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60020	Mic Gerrard	mgerrardk@bandcamp.co...	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60021	Monroe Jorczyk	mjorczykl@google.com	Supervisor	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60022	Melonie Tregiddo	mtregiddom@over-blog.c...	Supervisor	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60023	Johny Moquin	jmoquinn@cyberchimps.c...	Supervisor	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60024	Templeton Slaight	tslaighto@eventbrite.com	Supervisor	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60025	Eulalie Krinks	ekrinksp@dropbox.com	Supervisor	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60026	Klara Szymanski	kszymanskiq@cocolog-nif...	Supervisor	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60027	Chester Gullan	cgullanr@quantcast.com	Supervisor	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60028	Leonidas Duddell	lduddells@utexas.edu	Supervisor	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60029	Lanie Shanley	lshanleyt@telegraph.co.uk	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60030	Guglielmo Wilce	gwilceu@twitter.com	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60031	Jacob Creagh	jcreaghv@comsenz.com	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60032	Barnard Grigaut	bgrigautw@e-recht24.de	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60033	Nanice Simonutti	nsimonuttix@themeforest...	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60034	Fonz Cours	fcoursy@ed.gov	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60035	Amos Wetwood	awetwoodz@pen.io	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
60036	Corrinne Gamon	cgamon10@last.fm	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-

ID: 60000
Name: Jung-Hoo Lee
Email: lshankland0@soup.io
Phone: -
Department: Executive
Title: -
Group: Executive
Period: 2001/01/01 00:00 ~ 2037/12/31 23:59

Datetime	Location	Event
2025/09/17 09:29:45	DEMO DEVICE	1:1 authentication succeed...
2025/09/17 08:05:10	DEMO DEVICE	1:1 authentication succeed...
2025/09/17 08:05:05	DEMO DEVICE	1:1 authentication succeed...
2025/09/17 08:04:51	DEMO DEVICE	Authentication failed (Invali...
2025/09/09 16:26:56	Meeting Room 3 X-Station 2	Access denied (Invalid acce...
2025/09/09 16:26:52	Meeting Room 3 X-Station 2	Access denied (Invalid acce...
2025/09/09 16:26:49	Meeting Room 3 X-Station 2	Access denied (Invalid acce...
2025/09/09 16:26:31	Meeting Room 3 X-Station 2	1:1 authentication succeed...
2025/09/09 16:26:08	Meeting Room 3 X-Station 2	1:1 authentication succeed...
2025/09/09 16:26:07	Meeting Room 3 X-Station 2	1:1 authentication succeed...
2025/09/09 16:26:02	Meeting Room 3 X-Station 2	1:1 authentication succeed...
2025/09/09 16:26:00	Meeting Room 3 X-Station 2	1:1 authentication succeed...

- To edit the detailed information of a user, double-click on the desired user in the user list. Go to the page where you can edit the user's detailed information.

ⓘ **INFO**

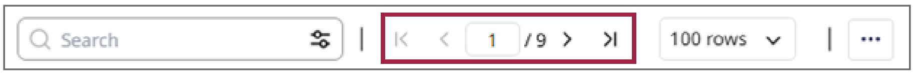
- For more information about user information modification, refer to the following.
- You can change the column layout in the user list. For more information on changing column layouts, refer to the following.

Select view options

You can change the display options for the user list using the tool button in the upper right corner of the screen.

Go to the user list

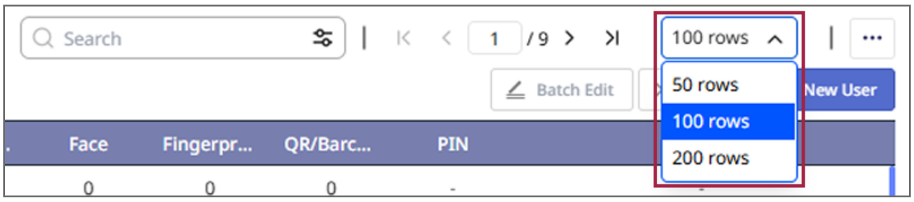
The user list displays a default of 10 users. You can click the button at the top of the screen to go to another page.



- |< : Go to the first page of the user list.
- < : Go to the previous page of the user list.
- > : Go to the next page of the user list.
- >| : Go to the last page of the user list.
- Go to the desired page, enter the page number in the number input field and press the Enter.

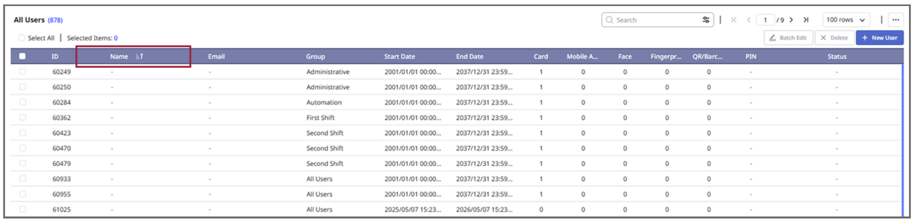
Change the number of users displayed on the list

You can change the number of users displayed in the user list. Select the desired number of users from the list box at the top right of the screen. Available options are 50, 100, or 200 users.



Sort user list

You can change the sorting criteria of the user list. Clicking the column header at the top of the list allows you to sort in ascending or descending order. For example, clicking the column header **First Name** will sort the users' names in ascending or descending order. The clicked item will show either an ascending (≡↑) or descending (≡↓) icon.



□	ID	Name	Email	Group	Start Date	End Date	Card	Mobile A...	Face	Fingerpr...	QR/Barc...	PIN	Status
□	60249	-	-	Administrative	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60250	-	-	Administrative	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60284	-	-	Automation	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60362	-	-	First Shift	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60423	-	-	Second Shift	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60470	-	-	Second Shift	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60479	-	-	Second Shift	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60933	-	-	All Users	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60955	-	-	All Users	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	61025	-	-	All Users	2025/05/07 15:23...	2026/05/07 15:23...	0	0	0	0	0	-	-

> **INFO**
>
> There may be items that cannot be sorted depending on the column type.

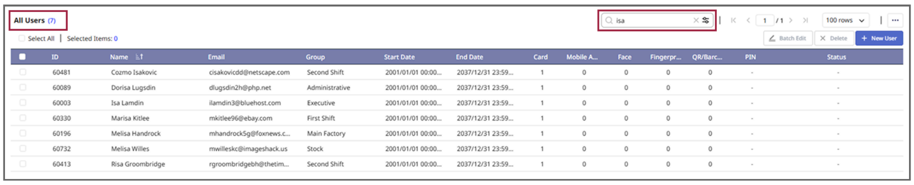
Search user

Provides guidance on how to search for specific users. You can quickly find the desired users using the search feature on the user list page.

> **INFO**
>
> - Search terms are case-insensitive.
> - User’s basic information must be entered to search for users. For more information about user information input, refer to the following.

General search

You can search based on the user's ID, name, or email. Enter the desired keywords in the search input field at the top of the screen and press the Enter. Users matching the specified keyword will be displayed in the list. You can check the number of search results at the very top of the list.

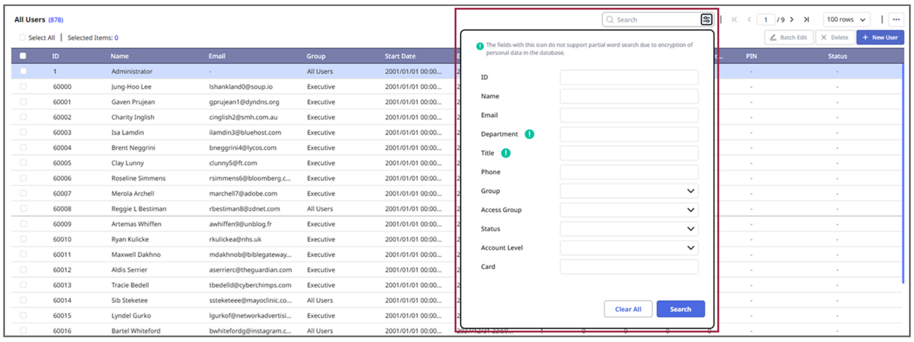


□	ID	Name	Email	Group	Start Date	End Date	Card	Mobile A...	Face	Fingerpr...	QR/Barc...	PIN	Status
□	60481	Cozmo Isakovic	cisakovicdd@netscape.com	Second Shift	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60089	Dorisa Lugsdin	dlugsdin2h@php.net	Administrative	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60003	Isa Lamdin	ilamdin3@bluehost.com	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60330	Marisa Kitlee	mkitlee96@ebay.com	First Shift	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60196	Melisa Handrock	mhandrock5g@foxnews.c...	Main Factory	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60732	Melisa Willes	mwilleskc@imageshack.us	Stock	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60413	Risa Groombridge	rgroombridgebh@thetim...	Second Shift	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-

Advanced search

You can search for specific user IDs, names, email addresses, and so on.

1. Click the button next to the search input field at the top of the screen.
2. When the advanced search window opens, enter your desired search criteria and click **Search**.



The fields with this icon do not support partial word search due to encryption of personal data in the database.

ID	Name	Email	Group	Start Date	PIN	Status
1	Administrator	-	All Users	2001/01/01 00:00...	-	-
60000	Jung-Hoo Lee	lshankland0@soup.io	Executive	2001/01/01 00:00...	-	-
60001	Gaven Prujean	gprujean1@dyndns.org	Executive	2001/01/01 00:00...	-	-
60002	Charity Inglish	cinglish2@smh.com.au	Executive	2001/01/01 00:00...	-	-
60003	Isa Lamdin	ilamdin3@bluehost.com	Executive	2001/01/01 00:00...	-	-
60004	Brent Neggrini	bneggrini4@lycos.com	Executive	2001/01/01 00:00...	-	-
60005	Clay Lunny	clunny5@ft.com	Executive	2001/01/01 00:00...	-	-
60006	Roseline Simmens	rsimmens6@bloomberg.c...	Executive	2001/01/01 00:00...	-	-
60007	Merola Archell	marchell7@adobe.com	Executive	2001/01/01 00:00...	-	-
60008	Reggie L Bestiman	rbestiman8@zdnet.com	All Users	2001/01/01 00:00...	-	-
60009	Artemas Whiffen	awhiffen9@unblog.fr	Executive	2001/01/01 00:00...	-	-
60010	Ryan Kulicke	rkulickea@nhs.uk	Executive	2001/01/01 00:00...	-	-
60011	Maxwell Dakhno	mdakhnob@biblegateway...	Executive	2001/01/01 00:00...	-	-
60012	Aldis Serrier	aserrierc@theguardian.com	Executive	2001/01/01 00:00...	-	-
60013	Tracie Bedell	tbedelld@cyberchimps.com	Executive	2001/01/01 00:00...	-	-
60014	Sib Steketee	ssteketeee@mayoclinic.co...	All Users	2001/01/01 00:00...	-	-
60015	Lyndel Gurko	lgurkof@networkadvertisi...	Executive	2001/01/01 00:00...	-	-
60016	Bartel Whiteford	bwhitefordg@instagram.c...	All Users	2001/01/01 00:00...	-	-

INFO

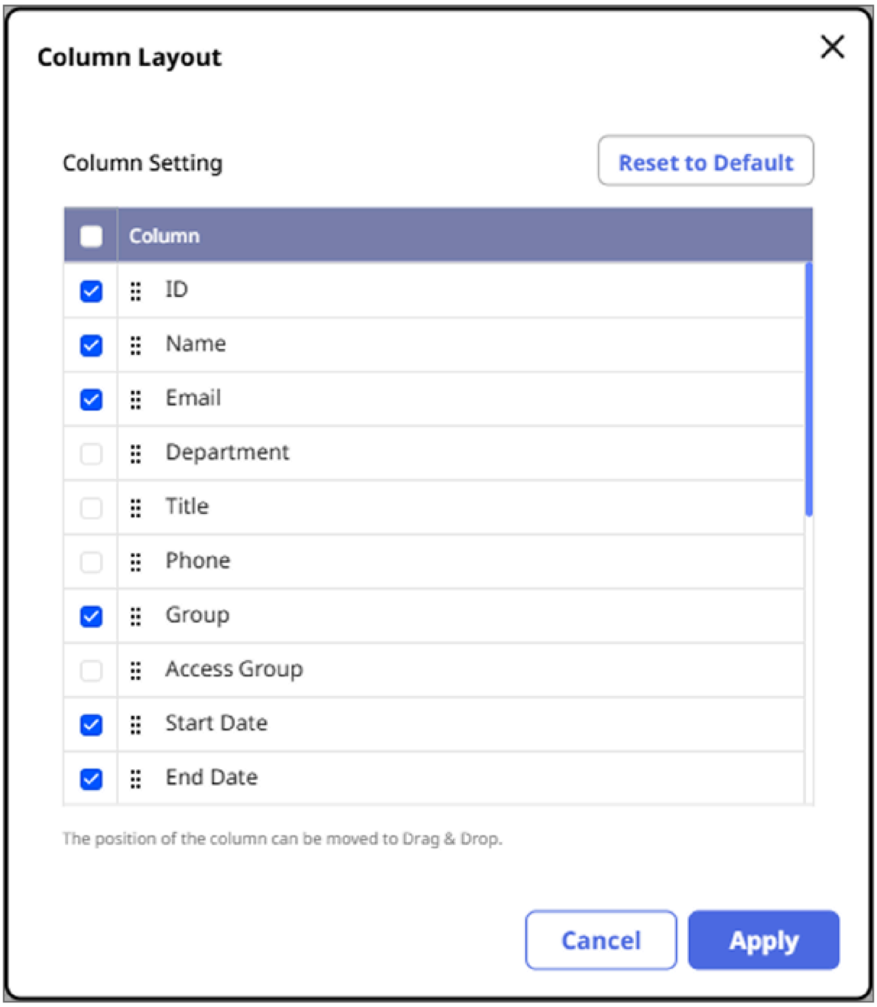
- The fields with ! icon do not support partial word search due to encryption of personal data in the database.
- To reset the criteria entered the advanced search window, click the **Clear All** button.
- Advanced search supports searching for **Custom User Field**. For more information on **Custom User Field**, refer to the following.

User list column settings

You can change the column settings displayed in the user list. Through column settings, you can select the columns to be displayed or change the order of the columns.

1. Click the ··· button at the top right of the user list screen.
2. Click **Column Layout**.

3. When the **Column Layout** window appears, select or deselect the desired columns.



Column Layout ×

Column Setting

□	Column
☑	ID
☑	Name
☑	Email
□	Department
□	Title
□	Phone
☑	Group
□	Access Group
☑	Start Date
☑	End Date

The position of the column can be moved to Drag & Drop.

4. To change the order of the columns, click and drag the desired column to change its position.
5. To save the settings, click the **Apply** button.

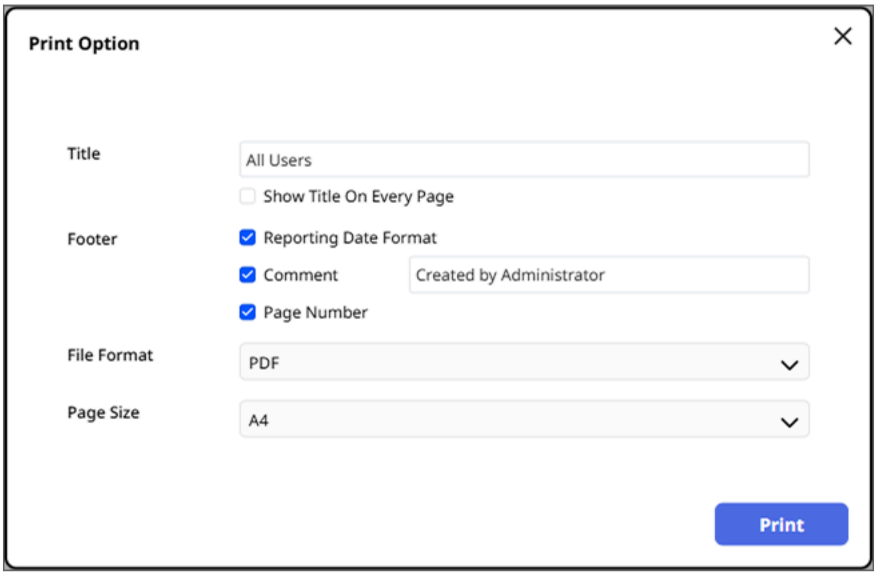
> **INFO**
>
> - Column settings are saved for each user account.
> - To reset the column layout settings, click the **Default Column** button.

Print user list

You can save the user list you are currently viewing as a PDF or SVG file.

1. Click the ••• button at the top right of the user list screen.
2. Click **Print**.

3. When the **Print Option** window appears, select your desired format in the **File Format** options and set the other options.



Print Option

Title: All Users

□ Show Title On Every Page

Footer:

☑ Reporting Date Format

☑ Comment: Created by Administrator

☑ Page Number

File Format: PDF

Page Size: A4

4. Click the **Print** button.

You can print the PDF or SVG file that opens through the browser.

Manage Users

Guides how to effectively manage registered users. Explains key features necessary for user management step by step, including modifying and deleting user information, data synchronization with devices, tracking access history, and exporting/importing user data.

Edit User Information

Guide the process of modifying the information of individual users or multiple users and changing access permissions.

Delete User

Describes how to delete a registered user.

Transfer User Information to the...

This guides on how to transfer user information to the registered device.

Track User Access History

This guide explains how to track and verify user access logs.

Export/Import User Information

You can utilize user information from a previous version or a different server by exporting or importing user data.

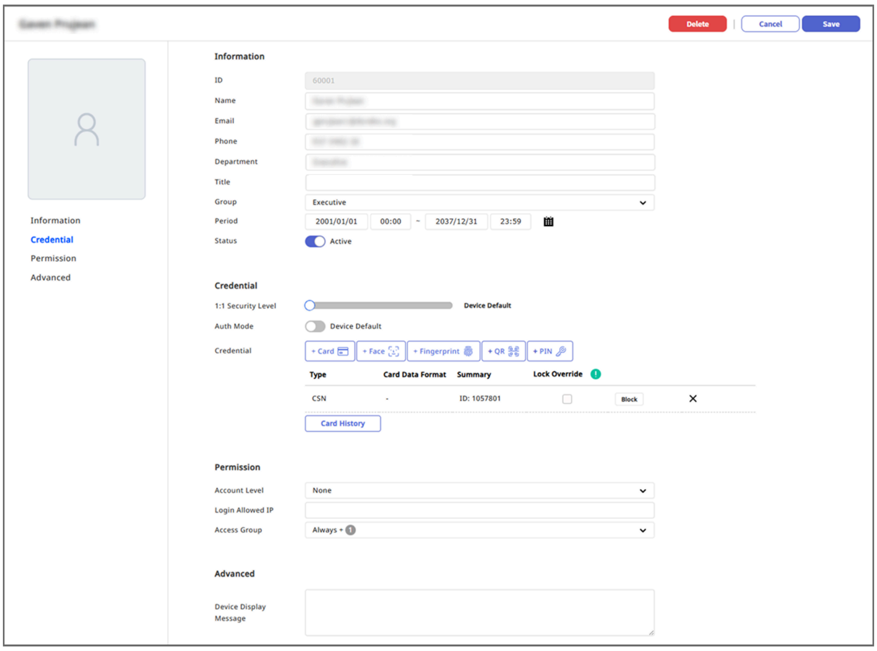
Edit User Information

Guide how to modify the information of registered users. Modify basic information, access permissions, or credentials of individual users or batch modify the information of multiple users.

> ⓘ **INFO**
>
> A user with the original ID of `1` cannot be modified by other administrators. Only the user logged in to this account can modify their own information.

Edit user information

1. Click **User** on the **Launcher** page.
2. Select the user to edit from the user list.
3. Double-click the user or click the **See More** button when the user's profile information appears on the right side of the screen.
4. A window for editing user information appears.



[redacted]

Information

ID: 60001

Name: [redacted]

Email: [redacted]

Phone: [redacted]

Department: [redacted]

Title:

Group: Executive

Period: 2001/01/01 00:00 ~ 2037/12/31 23:59

Status: Active

Credential

1:1 Security Level: Device Default

Auth Mode: Device Default

Credential:

Type	Card Data Format	Summary	Lock Override		
CSN	-	ID: 1057801	□	Block	×

Permission

Account Level: None

Login Allowed IP:

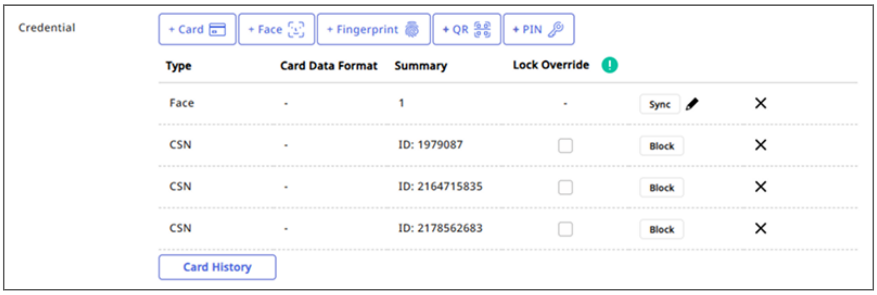
Access Group: Always + 1

Advanced

Device Display Message:

5. Modify the desired items.

6. To modify credential items, click the ✎ button, and to delete, click the ✕ button.



Type	Card Data Format	Summary	Lock Override		
Face	-	1	-	Sync ✎	✕
CSN	-	ID: 1979087	☐	Block	✕
CSN	-	ID: 2164715835	☐	Block	✕
CSN	-	ID: 2178562683	☐	Block	✕

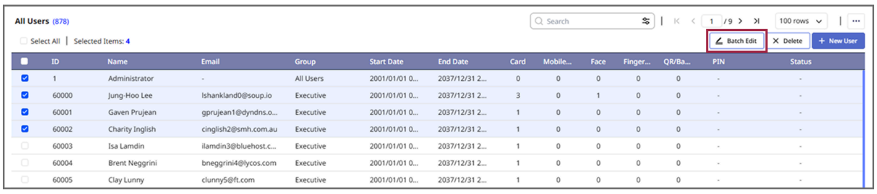
7. To save changes, click the **Save** button in the upper right corner of the screen.

> **INFO**
>
> - For more information about each field in the **Information** section, refer to the following.
> - For more information about each field in the **Credential** section, refer to the following.
> - For more information about each field in the **Permission** section, refer to the following.
> - You can enter the user's personal message in the **Advanced** section.

Batch edit user information

You can edit the information or access permissions of multiple users at once. This feature is useful when setting the same access permissions or groups for multiple users.

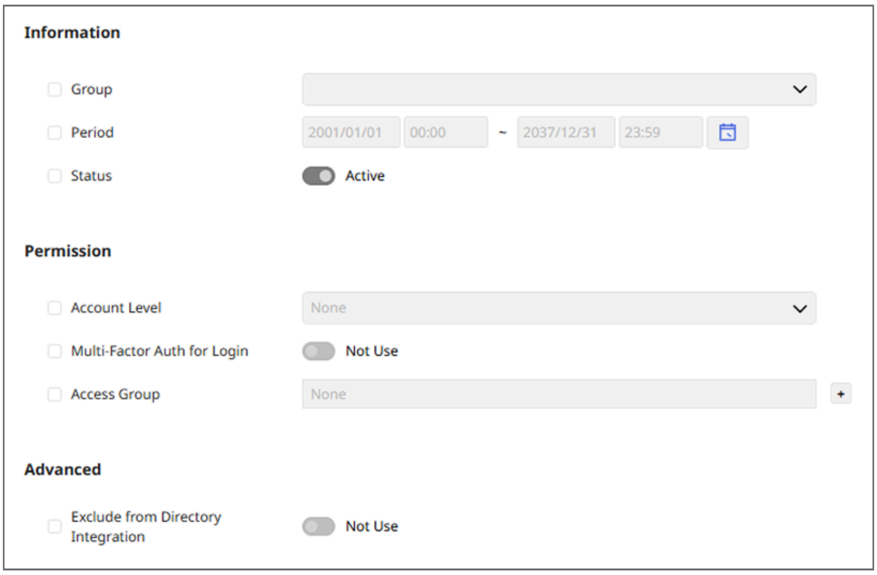
1. Click **User** on the **Launcher** page.
2. Click the checkbox to the left of the user you want to edit in the user list. Select two or more users.
3. Click **Batch Edit** at the top right of the screen.



☐ Select All | Selected Items: 4

☐	ID	Name	Email	Group	Start Date	End Date	Card	Mobile...	Face	Finger...	QR/Ba...	PIN	Status
☑	1	Administrator	-	All Users	2001/01/01 0...	2037/12/31 2...	0	0	0	0	0	-	-
☑	60000	Jung-Hoo Lee	lshankland0@soup.io	Executive	2001/01/01 0...	2037/12/31 2...	3	0	1	0	0	-	-
☑	60001	Gaven Prujean	gprujean1@dyndns.o...	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-
☑	60002	Charity Inglish	cinglish2@smh.com.au	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-
☐	60003	Isa Lamdin	ilamdin3@bluehost.c...	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-
☐	60004	Brent Neggrini	bneggrini4@lycos.com	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-
☐	60005	Clay Lunny	clunny5@ft.com	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-

4. When the **Batch Edit** screen appears, click the checkbox for the item you want and make modifications.



Information

□ Group

□ Period 2001/01/01 00:00 ~ 2037/12/31 23:59

□ Status Active

Permission

□ Account Level None

□ Multi-Factor Auth for Login Not Use

□ Access Group None +

Advanced

□ Exclude from Directory Integration Not Use

5. To save the edited information, click the **Save** button at the top right of the screen.

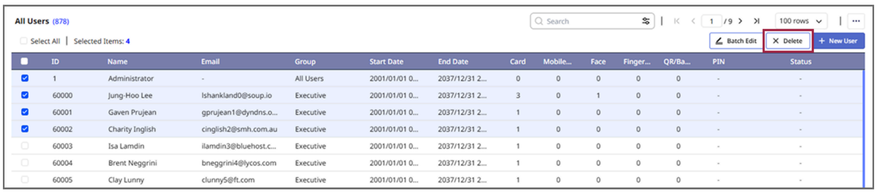
INFO

- User's ID, name, email, phone number, and credentials cannot be batch edited.
- To cancel the edited information, click the **Cancel** button at the top right of the screen.

Delete User

If you need to delete a user registered in **BioStar X** due to resignation, contract termination, or security violation, follow the steps below.

1. Click **User** on the **Launcher** page.
2. Click the checkbox to the left of the user you want to delete from the user list. You can select more than one user.
3. Click **Delete** at the top right of the screen.



☑	ID	Name	Email	Group	Start Date	End Date	Card	Mobile...	Face	Finger...	QR/Ba...	PIN	Status
☑	1	Administrator	-	All Users	2001/01/01 0...	2037/12/31 2...	0	0	0	0	0	-	-
☑	60000	Jung-Hoo Lee	lshankland0@soup.io	Executive	2001/01/01 0...	2037/12/31 2...	3	0	1	0	0	-	-
☑	60001	Gaven Prujean	gprujean1@dyndns.o...	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-
☑	60002	Charity Inglish	cinglish2@smh.com.au	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-
□	60003	Isa Lamdin	ilamdin3@bluehost.c...	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-
□	60004	Brent Neggrini	bneggrini4@lycos.com	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-
□	60005	Clay Lunny	clunny5@ft.com	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-

4. Click **Delete** to confirm the message appears.

Confirm that the selected user has been deleted from the user list.

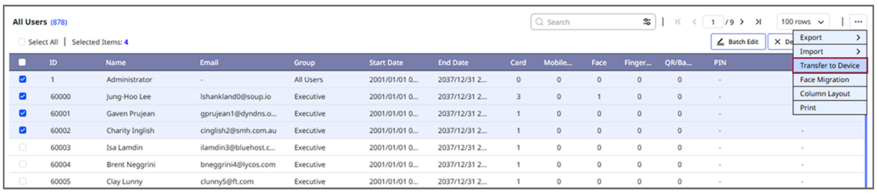
INFO

- User with ID `1` cannot be deleted.
- For more information on how to delete user information from the device, refer to the following.

Transfer User Information to the Device

Provides a feature to transmit user information registered on the **BioStar X** server to the device for access control. When user information is sent to the device, the device will use the user data to determine access permissions and can perform authentication even in offline environments.

1. Click **User** on the **Launcher** page.
2. Click the checkbox to the left of the user whose information you want to send from the user list. You can select more than one user.
3. Select the ••• button in the top right corner of the screen and click **Transfer to Device**.

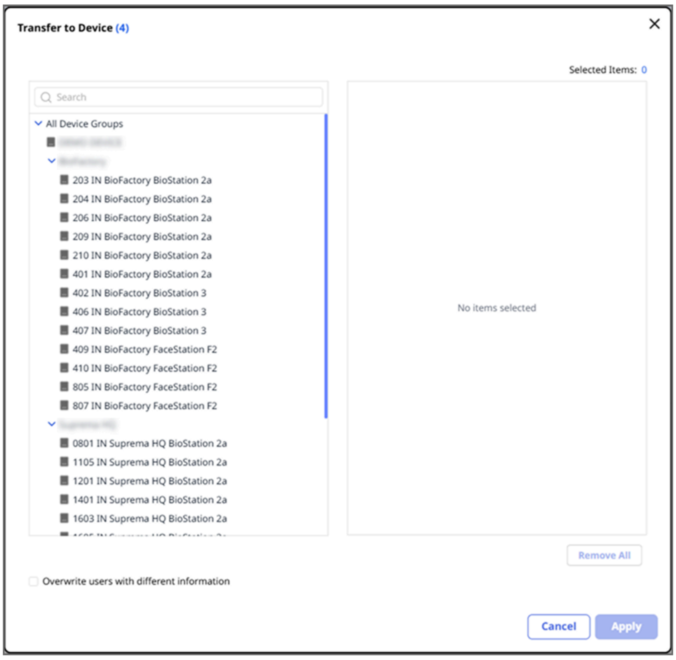


All Users (878)

□ Select All | Selected Items: 4

☐	ID	Name	Email	Group	Start Date	End Date	Card	Mobile...	Face	Finger...	QR/Ba...	PIN	
☑	1	Administrator	-	All Users	2001/01/01 0...	2037/12/31 2...	0	0	0	0	0	-	
☑	60000	Jung-Hoo Lee	lshankland0@soup.io	Executive	2001/01/01 0...	2037/12/31 2...	3	0	1	0	0	-	
☑	60001	Gaven Prujean	gprujean1@dyndns.o...	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	
☑	60002	Charity Inglish	cinglish2@smh.com.au	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-
☐	60003	Isa Lamdin	ilamdin3@bluehost.c...	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-
☐	60004	Brent Neggrini	bneggrini4@lycos.com	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-
☐	60005	Clay Lunny	clunny5@ft.com	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-

4. When the **Transfer to Device** window appears, select the device from the list to which you want to transfer user information.



Transfer to Device (4)

Selected Items: 0

All Device Groups
- 203 IN BioFactory BioStation 2a
- 204 IN BioFactory BioStation 2a
- 206 IN BioFactory BioStation 2a
- 209 IN BioFactory BioStation 2a
- 210 IN BioFactory BioStation 2a
- 401 IN BioFactory BioStation 2a
- 402 IN BioFactory BioStation 3
- 406 IN BioFactory BioStation 3
- 407 IN BioFactory BioStation 3
- 409 IN BioFactory FaceStation F2
- 410 IN BioFactory FaceStation F2
- 805 IN BioFactory FaceStation F2
- 807 IN BioFactory FaceStation F2
- 0801 IN Suprema HQ BioStation 2a
- 1105 IN Suprema HQ BioStation 2a
- 1201 IN Suprema HQ BioStation 2a
- 1401 IN Suprema HQ BioStation 2a
- 1603 IN Suprema HQ BioStation 2a

No items selected

□ Overwrite users with different information

5. If the information is different for the same ID, click the checkbox for the **Overwrite users with different information** option to overwrite with the contents of the **BioStar X** server.
6. If you have selected all the devices to transfer, click **Apply**.

Transferring user information to the selected device.

ⓘ **INFO**

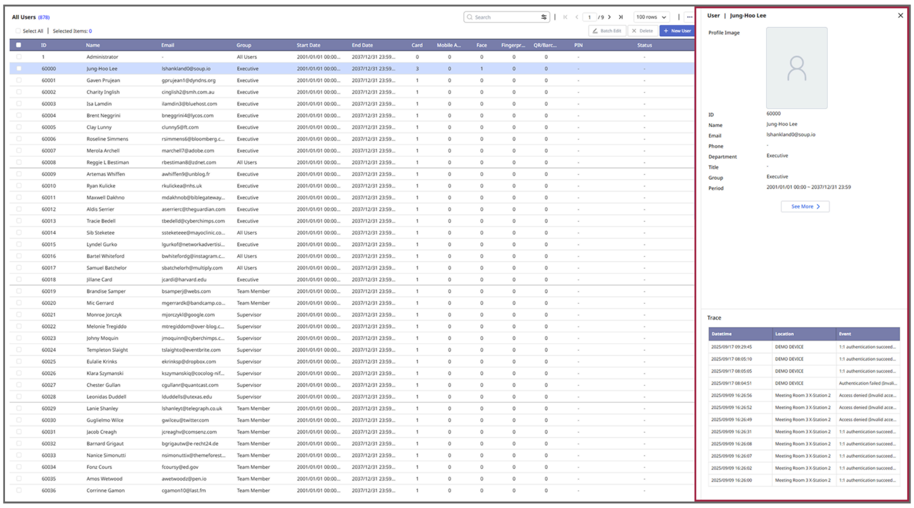
- You can also search for devices by entering keywords in the search input field.
- To transfer user information, the device must be connected to the **BioStar X** server.
- If you change information for a user who is already registered on the device, you must resend the user information to reflect the changes on the device. To use the option for synchronizing user information with the device, refer to the following.
- There is a limit to the number of users that can be registered on each device. Check the number of users that can be registered to the device.

Track User Access History

Tracking and verifying user access history is crucial for enhancing security and improving operational efficiency. You can prevent security threats and optimize operations through access history. You can identify users attempting to access restricted areas or at unauthorized times. This allows for a quick response to security threats. By identifying abnormal signs such as repeated authentication failures or access from unusual time zones, security threats can be detected early.

You can check the user's access history according to the following steps.

1. Click **User** on the **Launcher** page.
2. Click on the user whose access history you want to check from the user list.
3. The selected user's profile information will be displayed on the right side of the screen.



All Users (878)

□ Select All | Selected Items: 0

□	ID	Name	Email	Group	Start Date	End Date	Card	Mobile A...	Face	Fingerpr...	QR/Barc...	PIN	Status
□	1	Administrator	-	All Users	2001/01/01 00:00...	2037/12/31 23:59...	0	0	0	0	0	-	-
□	60000	Jung-Hoo Lee	lshankland0@soup.io	Executive	2001/01/01 00:00...	2037/12/31 23:59...	3	0	1	0	0	-	-
□	60001	Gaven Prujean	gprujean1@dyndns.org	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60002	Charity Inglish	cinglish2@smh.com.au	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60003	Isa Lamdin	ilamdin3@bluehost.com	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60004	Brent Neggrini	bneggrini4@lycos.com	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60005	Clay Lunny	clunny5@ft.com	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60006	Roseline Simmens	rsimmens6@bloomberg.c...	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60007	Merola Archell	marchell7@adobe.com	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60008	Reggie L Bestiman	rbestiman8@zdnet.com	All Users	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60009	Artemas Whiffen	awhiffen9@unblog.fr	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60010	Ryan Kulicke	rkulickea@nhs.uk	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60011	Maxwell Dakhno	mdakhnob@biblegateway...	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60012	Aldis Serrier	aserrierc@theguardian.com	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60013	Tracie Bedell	tbedelld@cyberchimps.com	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60014	Sib Steketee	ssteketeee@mayoclinic.co...	All Users	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60015	Lyndel Gurko	lgurkof@networkadvertisi...	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60016	Bartel Whiteford	bwhitefordg@instagram.c...	All Users	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60017	Samuel Batchelor	sbatchelorh@multiply.com	All Users	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60018	Jillane Card	jcardi@harvard.edu	Executive	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60019	Brandise Samper	bsamperj@webs.com	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60020	Mic Gerrard	mgerrardk@bandcamp.co...	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60021	Monroe Jorczyk	mjorczykl@google.com	Supervisor	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60022	Melonie Tregiddo	mtregiddom@over-blog.c...	Supervisor	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60023	Johny Moquin	jmoquinn@cyberchimps.c...	Supervisor	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60024	Templeton Slaight	tslaighto@eventbrite.com	Supervisor	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60025	Eulalie Krinks	ekrinksp@dropbox.com	Supervisor	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60026	Klara Szymanski	kszymanskiq@cocolog-nif...	Supervisor	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60027	Chester Gullan	cgullanr@quantcast.com	Supervisor	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60028	Leonidas Duddell	lduddells@utexas.edu	Supervisor	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60029	Lanie Shanley	lshanleyt@telegraph.co.uk	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60030	Guglielmo Wilce	gwilceu@twitter.com	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60031	Jacob Creagh	jcreaghv@comsenz.com	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60032	Barnard Grigaut	bgrigautw@e-recht24.de	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60033	Nanice Simonutti	nsimonuttix@themeforest...	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60034	Fonz Cours	fcoursy@ed.gov	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60035	Amos Wetwood	awetwoodz@pen.io	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-
□	60036	Corrinne Gamon	cgamon10@last.fm	Team Member	2001/01/01 00:00...	2037/12/31 23:59...	1	0	0	0	0	-	-

User | Jung-Hoo Lee

Profile Image	
ID	60000
Name	Jung-Hoo Lee
Email	lshankland0@soup.io
Phone	-
Department	Executive
Title	-
Group	Executive
Period	2001/01/01 00:00 ~ 2037/12/31 23:59

Trace

Datetime	Location	Event
2025/09/17 09:29:45	DEMO DEVICE	1:1 authentication succeed...
2025/09/17 08:05:10	DEMO DEVICE	1:1 authentication succeed...
2025/09/17 08:05:05	DEMO DEVICE	1:1 authentication succeed...
2025/09/17 08:04:51	DEMO DEVICE	Authentication failed (Invali...
2025/09/09 16:26:56	Meeting Room 3 X-Station 2	Access denied (Invalid acce...
2025/09/09 16:26:52	Meeting Room 3 X-Station 2	Access denied (Invalid acce...
2025/09/09 16:26:49	Meeting Room 3 X-Station 2	Access denied (Invalid acce...
2025/09/09 16:26:31	Meeting Room 3 X-Station 2	1:1 authentication succeed...
2025/09/09 16:26:08	Meeting Room 3 X-Station 2	1:1 authentication succeed...
2025/09/09 16:26:07	Meeting Room 3 X-Station 2	1:1 authentication succeed...
2025/09/09 16:26:02	Meeting Room 3 X-Station 2	1:1 authentication succeed...
2025/09/09 16:26:00	Meeting Room 3 X-Station 2	1:1 authentication succeed...

You can check the access history of the user in the **Trace** section below the preview screen.

> **INFO**
>
> - You can check real-time access events on the **Monitoring** page. For more information, refer to the following.
> - Past access events can be viewed on the **Data** page. For more information, refer to the following.

Export/Import User Information

You can utilize user information from a previous version or a different server by exporting or importing user data.

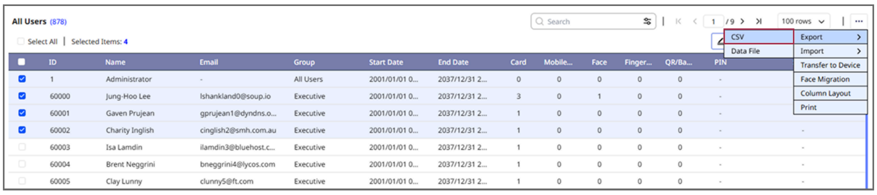
CSV export/import

Save selected user information as a CSV file, or load saved CSV files. This allows for easy transfer of user information using CSV files.

> **INFO**
>
> - If there are custom user fields not added to **BioStar X**, the CSV file cannot be imported correctly. For more information on adding custom user fields, refer to the following.
> - If user information is entered in a language other than English or Korean, save the CSV file in UTF-8 format.

CSV export

1. Click **User** on the **Launcher** page.
2. Click the checkbox next to the users you want to save as a CSV file from the user list. You can select more than one user.
3. Click the ··· button in the upper right corner of the screen and select **Export** → **CSV**.



□ Select All | Selected Items: 4

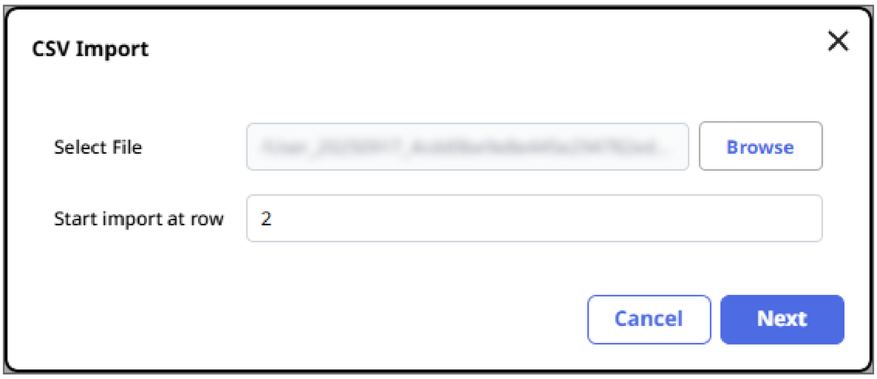
□	ID	Name	Email	Group	Start Date	End Date	Card	Mobile...	Face	Finger...	QR/Ba...	PIN	
☑	1	Administrator	-	All Users	2001/01/01 0...	2037/12/31 2...	0	0	0	0	0	-	
☑	60000	Jung-Hoo Lee	lshankland0@soup.io	Executive	2001/01/01 0...	2037/12/31 2...	3	0	1	0	0	-	
☑	60001	Gaven Prujean	gprujean1@dyndns.o...	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	
☑	60002	Charity Inglish	cinglish2@smh.com.au	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-
□	60003	Isa Lamdin	ilamdin3@bluehost.c...	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-
□	60004	Brent Neggrini	bneggrini4@lycos.com	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-
□	60005	Clay Lunny	clunny5@ft.com	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-

4. Click the **Download** button when the **CSV Export** window appears.
5. Save the CSV file to your desired location on your local path.

CSV import

1. Click **User** on the **Launcher** page.
2. Click ··· at the top right of the screen and select **Import** → **CSV**.
3. Select the CSV file saved locally.

4. Set **Start import at row** in the **CSV Import** window and click the **Next** button.

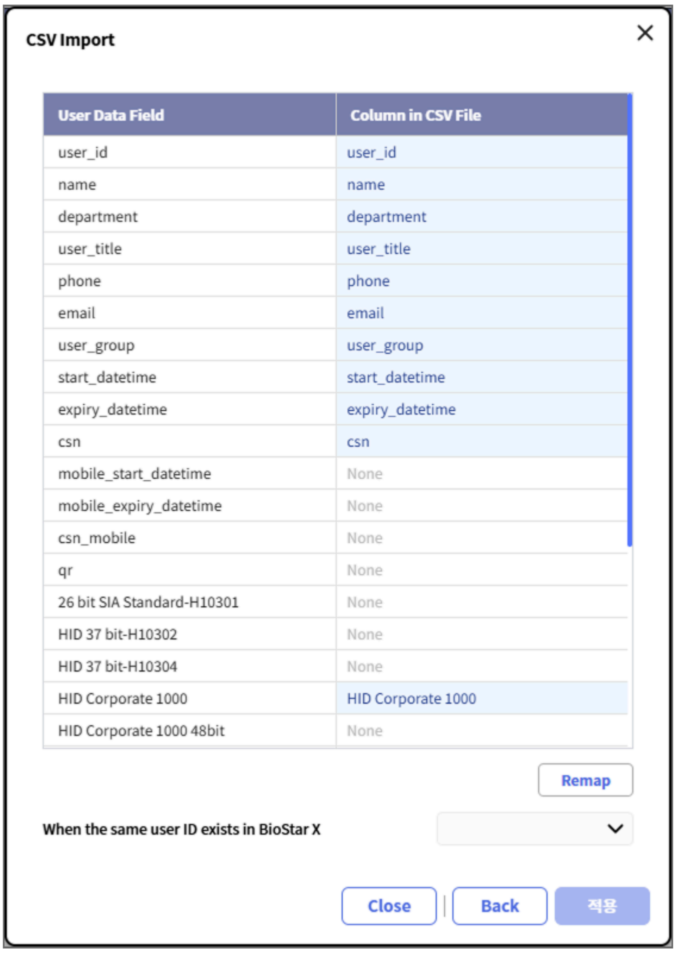


CSV Import

Select File

Start import at row: 2

5. User data fields from the CSV file will automatically map to user data fields in **BioStar X**. Click **Remap** to remap fields with the same name.

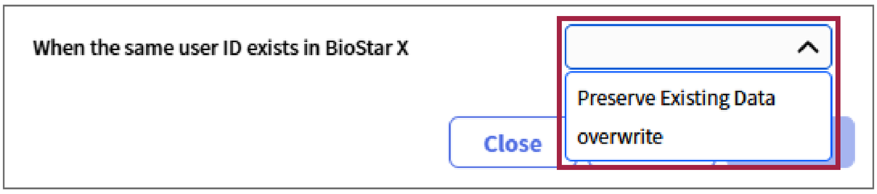


CSV Import

User Data Field	Column in CSV File
user_id	user_id
name	name
department	department
user_title	user_title
phone	phone
email	email
user_group	user_group
start_datetime	start_datetime
expiry_datetime	expiry_datetime
csn	csn
mobile_start_datetime	None
mobile_expiry_datetime	None
csn_mobile	None
qr	None
26 bit SIA Standard-H10301	None
HID 37 bit-H10302	None
HID 37 bit-H10304	None
HID Corporate 1000	HID Corporate 1000
HID Corporate 1000 48bit	None

When the same user ID exists in BioStar X

6. Choose whether to keep user data already registered with user IDs in **BioStar X** or to overwrite it with the information from the CSV file and click **Apply**.



When the same user ID exists in BioStar X

If an error occurs while importing information from the CSV file, you can review and upload only the erroneous CSV data.

ⓘ **INFO**

- Mobile access cards can be issued through CSV import. When using the regular site, one credit will be deducted from the Airfob Portal for each mobile access card issued upon completion of the import. To avoid issuing mobile access cards, disable mapping.
- If the CSV file contains identical data to mobile access cards already issued to users registered in **BioStar X**, you can choose to maintain or overwrite the data, in which case existing mobile access cards will be retained.
- If the CSV file contains different data from mobile access cards issued to users registered in **BioStar X**, maintaining the data will keep existing mobile access cards, while overwriting will issue new mobile access cards to the respective users.
- When issuing mobile access cards through CSV import on a dynamic site, ensure to input values for the `mobile_start_datetime` and `mobile_expiry_datetime` fields.
- **BioStar X** QR cannot be issued through CSV import.
- User facial data can be enrolled through CSV import. For more information, refer to the following.
- User PINs can be enrolled through CSV import. For more information, refer to the following.
- If you add columns that do not match the saved CSV file, you cannot import the file into **BioStar X**.

Data file export/import

User information can be stored on external storage (USB) for import into **BioStar X** or devices. Up to 500,000 user records can be transferred from the server to devices or between devices.

INFO

- Data exported from devices using outdated firmware cannot be imported into **BioStar X**. Always use the latest version of the firmware.
- Data cannot be imported if different fingerprint template formats are used. For example, data exported from devices using the Suprema fingerprint template format cannot be imported into devices using the ISO fingerprint template format.
- When importing user data, if fingerprint and face credentials stored on the **BioStar X** server already exist, it will be overwritten by the existing data.
- Data cannot be imported from devices with outdated firmware versions. Upgrade the device firmware to a compatible version.

  View compatible devices and firmware versions

  – BioStation 2 Firmware version 1.9.0 or higher

  – BioStation A2 Firmware version 1.8.0 or higher

  – FaceStation 2 firmware version 1.4.0 or higher

  – FaceStation F2 Firmware version 2.2.0 or higher

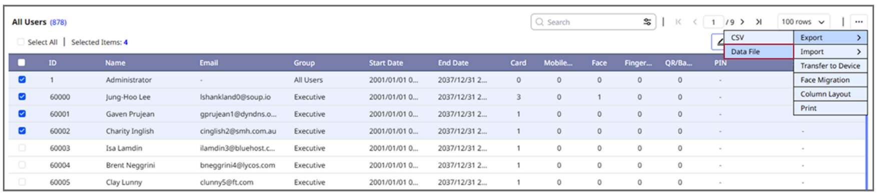
  – X-Station 2 firmware 1.0.0 or higher

  – BioStation 3 Firmware version 1.3.1 or higher

  – BioStation 2a Firmware version 1.0.0 or higher

Data export

1. Click **User** on the **Launcher** page.
2. Click the checkbox next to the users you want to export from the user list. You can select more than one user.
3. Click ••• in the top right corner of the screen, then select **Export** → **Data File**.

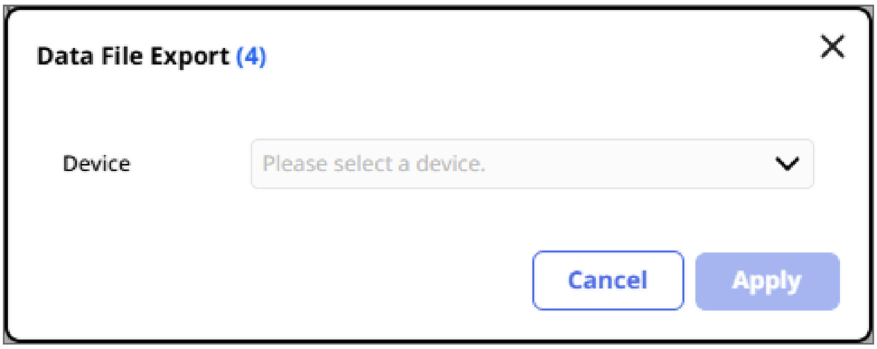


All Users (878)

□ Select All | Selected Items: 4

□	ID	Name	Email	Group	Start Date	End Date	Card	Mobile...	Face	Finger...	QR/Ba...	PIN	
☑	1	Administrator	-	All Users	2001/01/01 0...	2037/12/31 2...	0	0	0	0	0	-	
☑	60000	Jung-Hoo Lee	lshankland0@soup.io	Executive	2001/01/01 0...	2037/12/31 2...	3	0	1	0	0	-	
☑	60001	Gaven Prujean	gprujean1@dyndns.o...	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	
☑	60002	Charity Inglish	cinglish2@smh.com.au	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-
□	60003	Isa Lamdin	ilamdin3@bluehost.c...	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-
□	60004	Brent Neggrini	bneggrini4@lycos.com	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-
□	60005	Clay Lunny	clunny5@ft.com	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-	-

4. Select the device to apply the data file in the **Data File Export** window and click the **Apply** button.



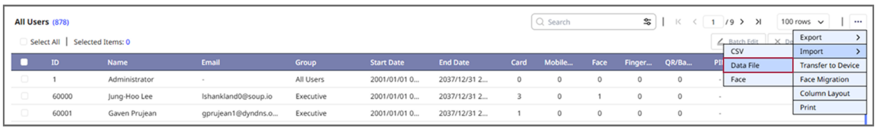
5. Save the data file in your desired local path.

> **INFO**
>
> - The data file export includes user profile photos, IDs, names, validity periods, access groups, PINs, private authentication modes, credentials (face, fingerprint, card, mobile card, face, QR/Barcode), and one-to-one security level information.
> - Selecting the incorrect device to apply the data file may cause it to be unrecognized by that device.

Data import

1. Click **User** on the **Launcher** page.

2. Click ••• in the top right corner of the screen, then select **Import** → **Data File**.


All Users (878)

□ Select All | Selected Items: 0

□	ID	Name	Email	Group	Start Date	End Date	Card	Mobile...	Face	Finger...	QR/Ba...	PI
□	1	Administrator	-	All Users	2001/01/01 0...	2037/12/31 2...	0	0	0	0	0	-
□	60000	Jung-Hoo Lee	lshankland0@soup.io	Executive	2001/01/01 0...	2037/12/31 2...	3	0	1	0	0	-
□	60001	Gaven Prujean	gprujean1@dyndns.o...	Executive	2001/01/01 0...	2037/12/31 2...	1	0	0	0	0	-

3. Select the data file (*.tgz*) saved locally.

A message will appear on the screen if the data file is successfully imported.

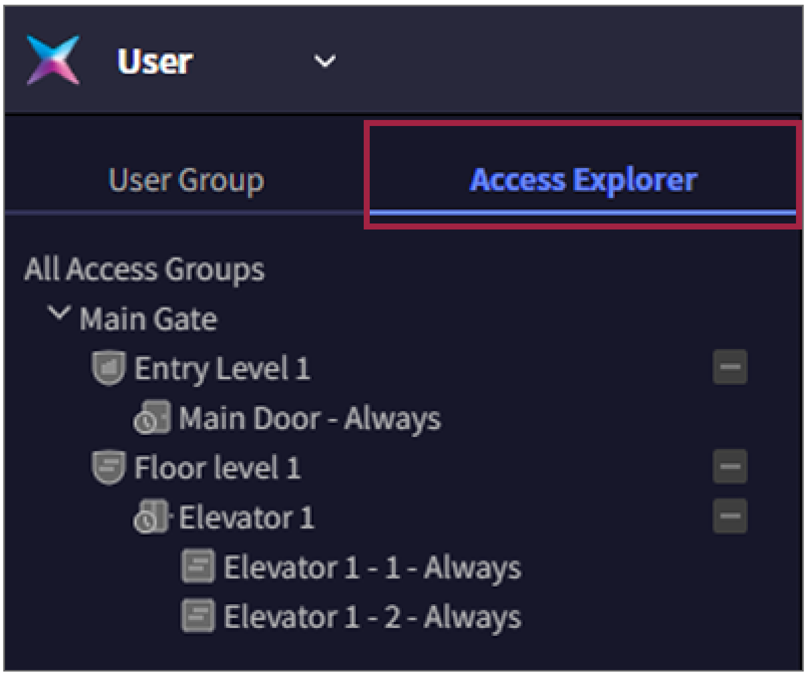
Manage Access Groups

This guide shows how to query and manage users based on access groups. Use **Access Explorer** to check registered users by access group and explore the access permission hierarchy through the tree structure.

> **INFO**
>
> To check access doors or floors belonging to an access group in **Access Explorer**, you must first set up the access control feature. For more information, refer to the following.

Check users by access group

1. Click **User** on the **Launcher** page.
2. Click the **Access Explorer** tab in the tree structure menu.



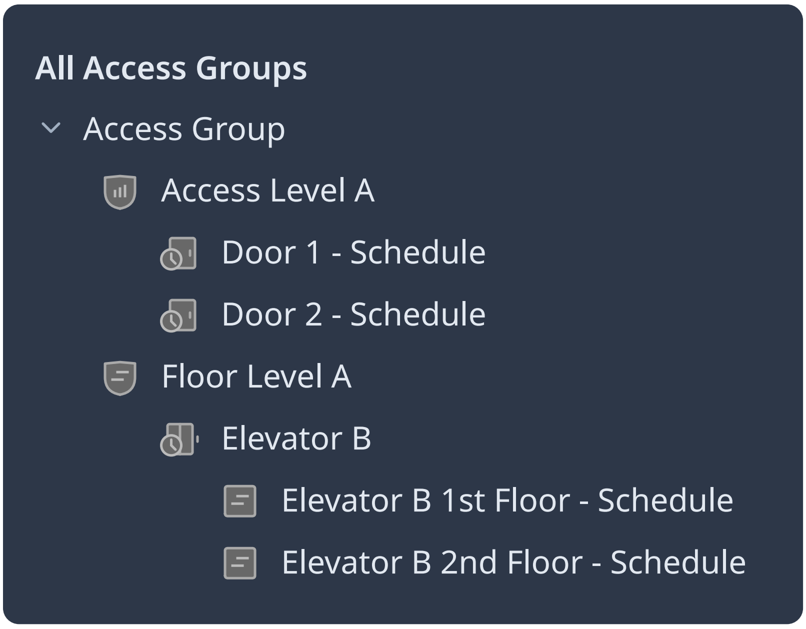
3. Click the desired access permission group in **All Access Groups**.

You can view users belonging to the selected access permission group in the user list.

> **INFO**
>
> To expand or collapse access levels or floor levels under the access group, click + or −.

Learn about the tree structure

The tree structure menu is composed of the following structure.



All Access Groups

- Access Group
  - Access Level A
    - Door 1 - Schedule
    - Door 2 - Schedule
  - Floor Level A
    - Elevator B
      - Elevator B 1st Floor - Schedule
      - Elevator B 2nd Floor - Schedule

- **Access group** is the upper layer that includes access levels, floor levels, user groups, and users. You can manage access permissions through the **access group**. For more information on creating access groups, refer to the following.
- **Access level** sets the times when users can enter and grants permission to access doors during this time. For more information on creating access levels, refer to the following.
- You can manage the floors users can access via elevators through the **floor level**. For more information on creating floor levels, refer to the following.
- **Schedule** is a feature that efficiently operates access control and attendance management by setting access and holiday schedules. For more information on registering schedules, refer to the following.
- You can register elevators and manage the floors accessible via the elevators. For more information about elevator enrollment, refer to the following.

> **INFO**
>
> The elevator registration feature is available through additional options for **Advanced** licenses and above. For more information on licensing policy, refer to the following.

Login in with Multi-Factor Authentication

You can use the **Multi-Factor Authentication** feature to enhance security when logging into **BioStar X**. Enabling **Multi-Factor Auth for Login** adds a fingerprint authentication step through a fingerprint scanner to the combination of user ID and password.

ⓘ **INFO**

- Users who want to use the **Multi-Factor Auth for Login** feature must enroll their fingerprint and set their username, password, and operator level.
- To use the **Multi-Factor Auth for Login** feature, a fingerprint scanner that supports multi-factor authentication login must be connected to the **BioStar X** client PC. Please refer to the list below for devices supported by the fingerprint scanner.
  - BioMini
  - BioMini Plus 2
  - BioMini Slim 2
- If you use the Directory Service account with the **Use for BioStar X Login** option, you cannot use the **Multi-Factor Auth for Login** feature.
- Administrators who set **Multi-Factor Auth for Login** cannot authenticate with **BioStar X** services (attendance management and video) other than access control. To use the service, log in after disabling the **Multi-Factor Auth for Login** setting. You can then reactivate the **Multi-Factor Auth for Login** setting.

⚠ **CAUTION**

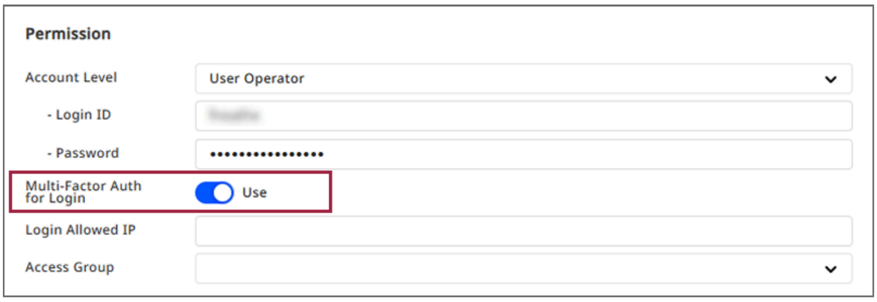
- After setting up the multi-factor authentication feature for the main admin account (ID 1), be aware that you will not be able to log in with that account if the fingerprint authentication becomes unavailable.
- If login becomes impossible due to fingerprint issues, contact Suprema Technical Support.

Multi-Factor authentication setting

Follow the steps below to set **Multi-Factor Auth for Login**.

1. Click **User** on the **Launcher** page.
2. Double click on the user who wants to set **Multi-Factor Auth for Login** from the user list.
   Alternatively, select a user and click the **See More** button in the profile displayed on the right screen.

3. When the user preview screen appears, set the **Multi-Factor Auth for Login** item to **Use** in the **Permission** section.



Permission

Account Level	User Operator
- Login ID	[redacted]
- Password	••••••••••••••••
Multi-Factor Auth for Login	Use
Login Allowed IP	
Access Group	

4. Click **Save** at the top right of the screen.

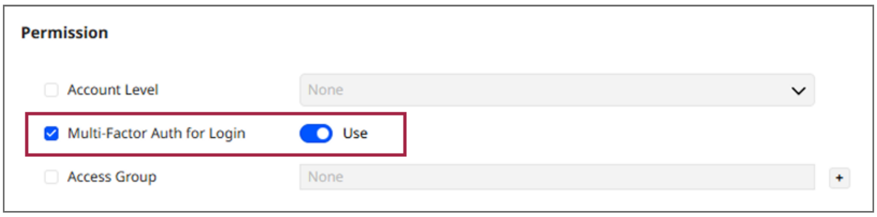
Completing multi-factor authentication setup.

Multi-Factor authentication batch setting

> **Before you start**
>
> To use the multi-authentication login feature, you must meet the following conditions.
>
> - The user must have a registered fingerprint authentication method.
> - **Operator**, **Login ID**, and **Password** must be set. Please refer to the following for details.

You can use the batch edit feature to apply the **Multi-Factor Auth for Login** feature to multiple users.

1. Click **User** on the **Launcher** page.
2. Click the checkbox to the left of the user you want to set up multi-factor authentication for in the user list.
3. Click **Batch Edit** at the top right of the screen.
4. When the batch edit window appears, click the checkbox for the **Multi-Factor Auth for Login** option in the **Permission** section and set it to **Use**.



Permission

□ Account Level	None
☑ Multi-Factor Auth for Login	Use
□ Access Group	None

5. Click **Save** at the top right of the screen.

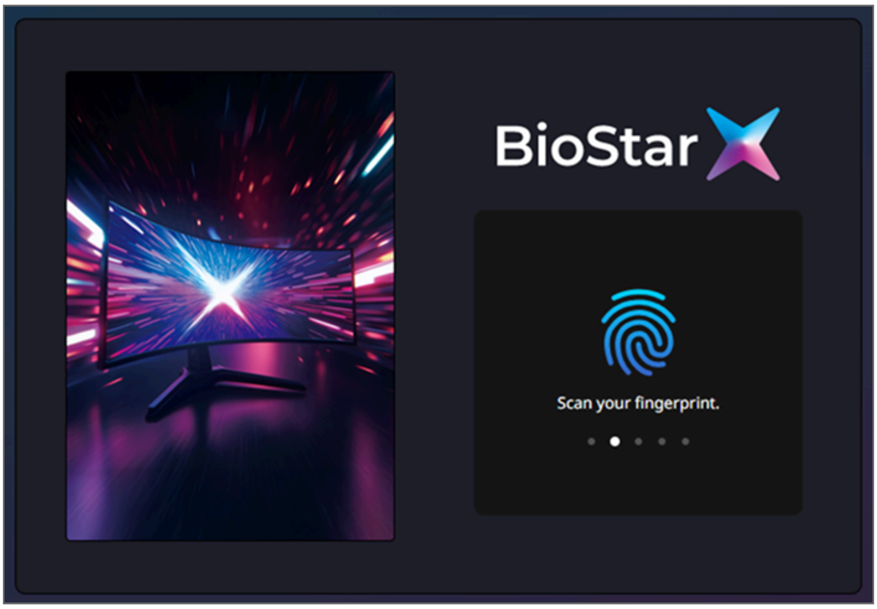
Completing the multi-factor authentication setup for multiple selected users.

INFO

Users among the selected who do not meet the conditions required to activate the **Multi-Factor Auth for Login** feature can be confirmed through the popup message of **Not applicable user(s)**. Please check the conditions required for the settings and try again.

Log in with Multi-Factor authentication

1. Access **BioStar X** log in screen through a web browser.
2. Enter your user ID and password, then click the **Login** button.
3. When the fingerprint input screen appears, scan your fingerprint using the fingerprint scanner.



Completing the login.

INFO

- The scan time limit is fixed at 18 seconds and cannot be changed.
- Fingerprint scanning can be attempted up to three times consecutively. If the fingerprint is not accurately scanned within these three attempts, authentication will fail.
- If authentication fails, click the **Retry** button to retry fingerprint authentication. Up to two retry attempts are allowed. If authentication fails after retry attempts, the process will revert to the ID and Password login step.

Batch Enroll Faces

Learn how to batch enroll users' faces. You can enroll faces of multiple users at once by using the import feature with a CSV file or by loading face pictures with file names that match user IDs. Alternatively, you can send face enrollment links via email to multiple users, allowing them to enroll faces directly from their mobile devices.

Before start

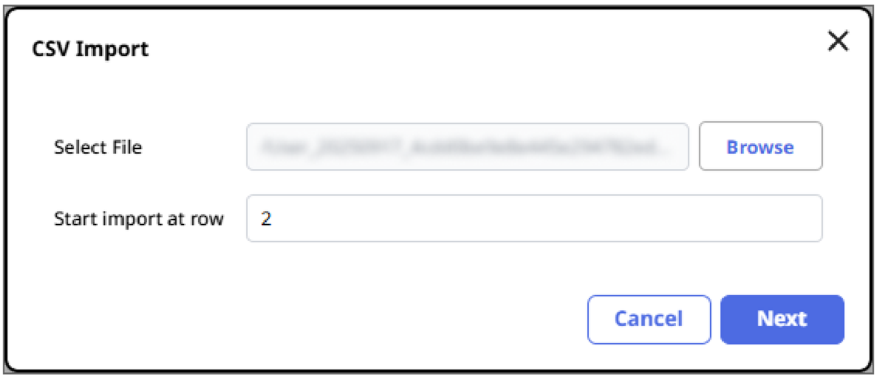
Prepare user face images before starting batch enrollment.

- Face image files must be stored in one folder. Face image file names must match user IDs.
- The maximum file size for supported image types is 10MB.
- Supported image formats include JPG, JPEG, and PNG.

Enroll with CSV file import

You can enroll users' faces in bulk using the CSV import feature.

1. Click **User** on the **Launcher** page.
2. In the user list, check the checkbox of the user whose face you want to enroll. You can select more than one user.
3. Click the ••• button in the upper right corner of the screen and select **Export** → **CSV**.
4. When the CSV export window appears, click **Download**.
5. Save the CSV file to your desired location on your local path.
6. Open the CSV file and add `face_image_file1`, `face_image_file2` columns.
7. Enter the filenames of the face images, including the extensions, in the added columns and save.
8. Click ••• at the top right of the screen and select **Import** → **CSV**.
9. Select the modified CSV file.
10. When the CSV import window appears, set **Start import at row** and click **Next**.

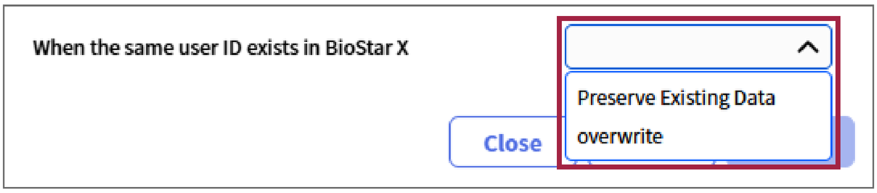


CSV Import

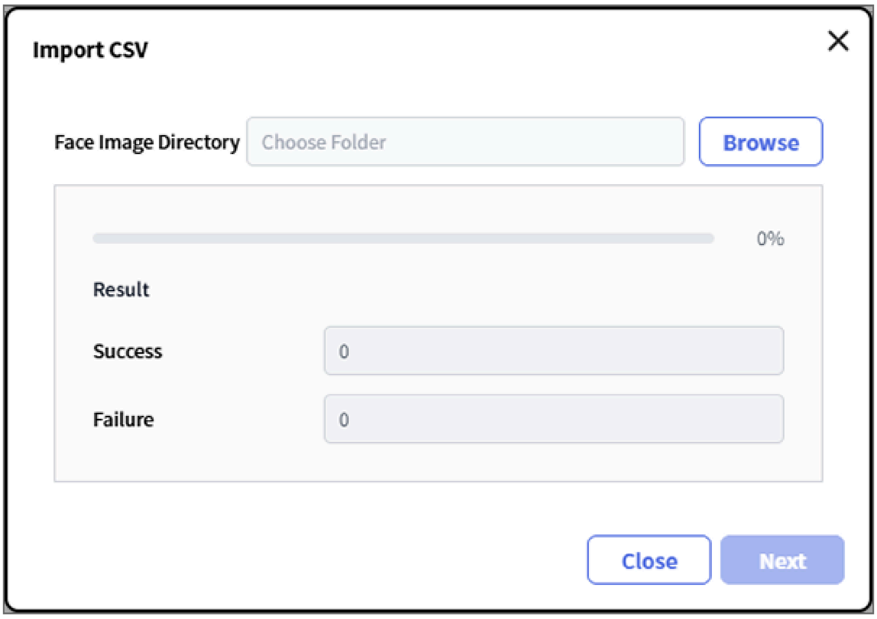
Select File

Start import at row: 2

11. Choose whether to overwrite user data already registered in **BioStar X** with the information from the CSV file, and click **Apply**.


When the same user ID exists in BioStar X

12. Click the **Browse** button in **Face Image Directory**.


Import CSV

Face Image Directory: Choose Folder

0%

Result

Success: 0

Failure: 0

13. Select the path where the face images are stored and click **Upload**.
14. To complete CSV import, click **Next**.

If an error occurs while importing the CSV file, you can recheck and upload only the CSV data that caused the error.

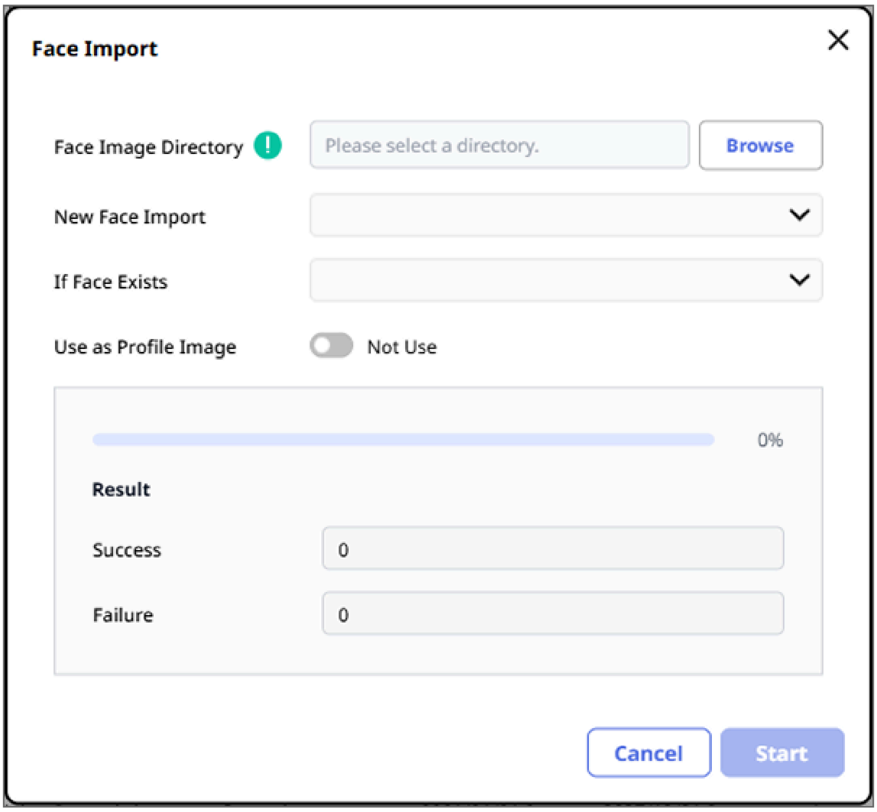
> ⓘ **INFO**
>
> It is recommended to use the same path for the CSV file and the face image files to be imported.

Import face

You can import face images with file names matching user IDs and enroll them for face authentication. Prepare user face image files before starting. Face image file names must match user IDs.

1. Click **User** on the **Launcher** page.
2. Click the ••• button in the upper right corner and select **Import** → **Face**.

3. When the **Face Import** window appears, click the **Browse** button.



Face Import

Face Image Directory: Please select a directory.

New Face Import:

If Face Exists:

Use as Profile Image: Not Use

0%

Result

Success: 0

Failure: 0

4. Select the path where the face images are stored.
5. Select the method to load face images in the **New Face Import** option.
   - **Import image files whose name matches user ID**: Loads images with filenames matching the user IDs.
   - **Import image files whose name matches user ID + Add new user by using file name as user ID**: If registered user IDs match the face image filenames, the images are loaded; if they do not match, a new user is created using the file name as the user ID and enrolled as a face authentication method.
6. In the **If Face Exists** option, select **Preserve data** or **Overwrite**.
   - **Preserve**: Preserves the face images of registered users.
   - **Overwrite**: Overwrites the face images of registered users with the newly imported face images.
7. To use the imported face images as profile images, click the **Use as Profile Image** option to enable it.
8. Click **Start**.

If an error occurs while importing a face image file, a list of photos with errors appears. Check the list and try again.

> ⓘ **INFO**
>
> A maximum of 1 face image can be imported per user ID.

Facial enrollment via mobile device

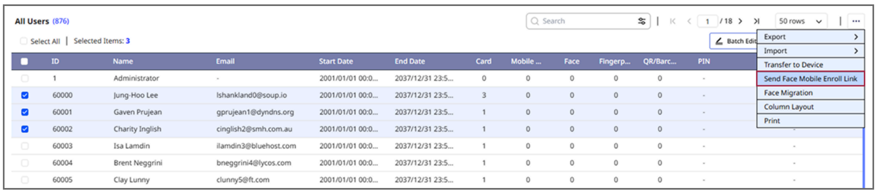
You can send face enrollment links to users via email. Users can access the link on their mobile devices to enroll faces directly.

Before start

- Complete the email information settings, including SMTP settings, before using the mobile face enrollment feature. For more information, refer to the following.
- You must enable the **Remote Access** feature to use the mobile face enrollment feature. For more information on **Remote Access** refer to the following.

Send face enrollment link

1. Click **User** on the **Launcher** page.
2. In the user list, check the checkbox of the user whose face you want to enroll. You can select more than one user.
3. Click the ••• button in the upper right corner of the screen and select **Send Face Mobile Enroll Link**.

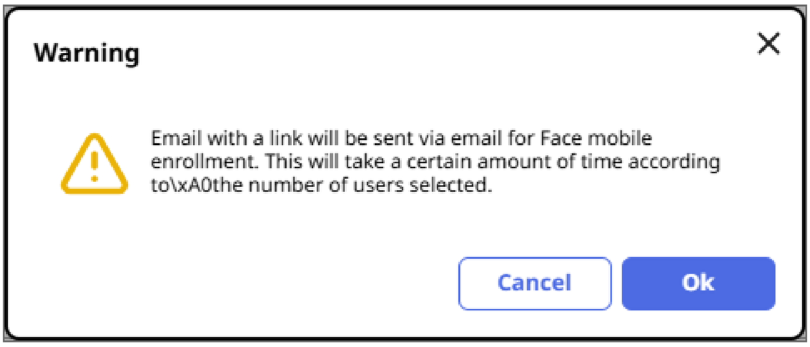


All Users (876)

□ Select All | Selected Items: 3

□	ID	Name	Email	Start Date	End Date	Card	Mobile ...	Face	Fingerp...	QR/Barc...	PIN	
□	1	Administrator	-	2001/01/01 00:0...	2037/12/31 23:5...	0	0	0	0	0	-	
☑	60000	Jung-Hoo Lee	lshankland0@soup.io	2001/01/01 00:0...	2037/12/31 23:5...	3	0	0	0	0	-	
☑	60001	Gaven Prujean	gprujean1@dyndns.org	2001/01/01 00:0...	2037/12/31 23:5...	1	0	0	0	0	-	
☑	60002	Charity Inglish	cinglish2@smh.com.au	2001/01/01 00:0...	2037/12/31 23:5...	1	0	0	0	0	-	-
□	60003	Isa Lamdin	ilamdin3@bluehost.com	2001/01/01 00:0...	2037/12/31 23:5...	1	0	0	0	0	-	-
□	60004	Brent Neggrini	bneggrini4@lycos.com	2001/01/01 00:0...	2037/12/31 23:5...	1	0	0	0	0	-	-
□	60005	Clay Lunny	clunny5@ft.com	2001/01/01 00:0...	2037/12/31 23:5...	1	0	0	0	0	-	-

4. When the message window appears, click the **Ok** button.



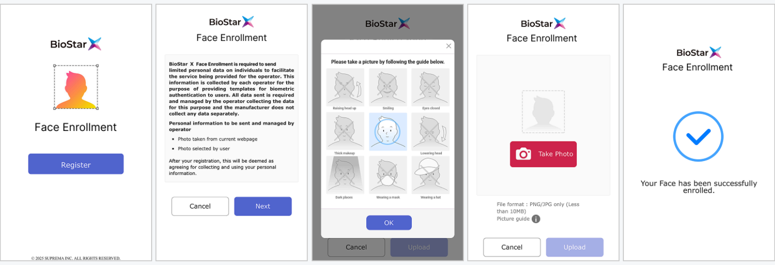
Warning

Email with a link will be sent via email for Face mobile enrollment. This will take a certain amount of time according to\xA0the number of users selected.

The face enrollment link is sent to the email of the selected users. Once the users complete the upload, their face credential is added to their user profiles.

INFO

- You can check the email sending status in **Audit Trail**. For more information, refer to the following.
- The language displayed on the page accessed via the face enrollment mobile link follows the language settings of the browser used on the mobile device.
- When the user accesses the sent face enrollment mobile link, the face enrollment service will be executed as shown below. Follow the instructions on the screen.



BioStar X Face Enrollment is required to send limited personal data on individuals to facilitate the service being provided for the operator. This information is collected by each operator for the purpose of providing templates for biometric authentication to users. All data sent is required and managed by the operator collecting the data for this purpose and the manufacturer does not collect any data separately.

Personal information to be sent and managed by operator

- Photo taken from current webpage
- Photo selected by user

After your registration, this will be deemed as agreeing for collecting and using your personal information.

Please take a picture by following the guide below.

File format : PNG/JPG only (Less than 10MB)

Your Face has been successfully enrolled.

© 2025 SUPREMA INC. ALL RIGHTS RESERVED.

- The maximum file size for supported image types is 10MB.
- Supported image formats include JPG, JPEG, and PNG.
- The sent face enrollment mobile link will expire after 24 hours.
- Once the Face Mobile Enrollment process is successful after uploading a face picture, an enrollment success message appears on the screen. If enrollment fails, a failure message and reason are displayed, and the user can retry the Visual Face Enrollment again using a different face picture.

Face Migration

You can upgrade the faces enrolled in the previous version of **BioStar X** to enhance recognition performance using the latest algorithm. The synchronization protocol has been improved to only transmit templates, excluding the actual images during user synchronization. Additionally, this helps significantly reduce synchronization time and prevent privacy-related issues.

Before start

Before running the face migration feature, check the following items.

> **What is face migration?**
>
> It is a feature that generates two types of face templates from user images already stored on the BioStar X server. To synchronize only the template for facial authentication during user synchronization, proceed with Face Migration.

Supported device and firmware version

Please refer to the list below for the devices that can synchronize the face with the template.

- FaceStation F2 firmware v2.2.0 or later
- BioStation 3 firmware v1.3.1 or later
- BioEntry W3 firmware v1.0.0 or later

Notice on FaceStation F2 v1.x.x Firmware Support Discontinuation

BioStar X optimized synchronization performance by changing to send only templates when synchronizing the user's face to the device. Therefore, support for the FaceStation F2 v1.x.x firmware, which can only extract templates from the device, will be discontinued. If you are currently using FaceStation F2 firmware version 1.x.x, upgrade to the latest firmware to use **BioStar X** with FaceStation F2.

The latest firmware can be downloaded from the Suprema Download Center.

Notes on face template types

Differences in face template types for FaceStation F2, BioStation 3, and BioEntry W3.

- **NPU Type**: BioStation 3, BioEntry W3
- **GPU Type**: FaceStation F2

- **Synchronization Time Between Devices with Different Face Template Types**
  Before proceeding with Face Migration, if you synchronize by adding BioStation 3 or BioEntry W3 to an environment that only used FaceStation F2, the template type will differ, and the NPU type template will be extracted from the image, which may take considerable time depending on the number of faces enrolled on the server.

- **Face Enrollment Recommendations in BioStar X**
  When enrolling faces without using the option to **Store Face Image** on the device, only the template is synchronized with **BioStar X**. As a result, it cannot be synchronized to devices with different face template types. Therefore, it is recommended to enroll faces through **BioStar X**.

Device related notices

The user data file exported from **BioStar X** contains only templates without images, so the user data file cannot be imported into FaceStation F2 and BioStation 3 that are using existing firmware.

When data file export from FaceStation F2 and BioStation 3, the data files can only be exported using firmware versions above the following:

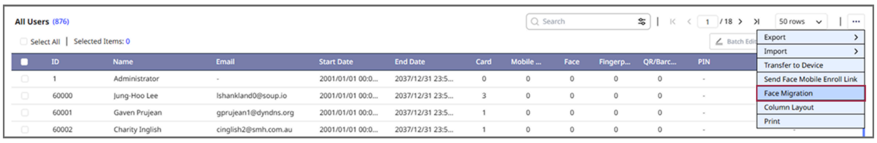
- FaceStation F2 firmware v2.2.0 or later
- BioStation 3 firmware v1.3.1 or later

CAUTION

When using FaceStation F2 or BioStation 3, it is recommended to upgrade to the latest firmware version. The latest firmware can be downloaded from the Suprema Download Center.

How to face migration

1. Click User on the Launcher page.
2. Select the ••• button at the top right of the screen and click the Face Migration button.

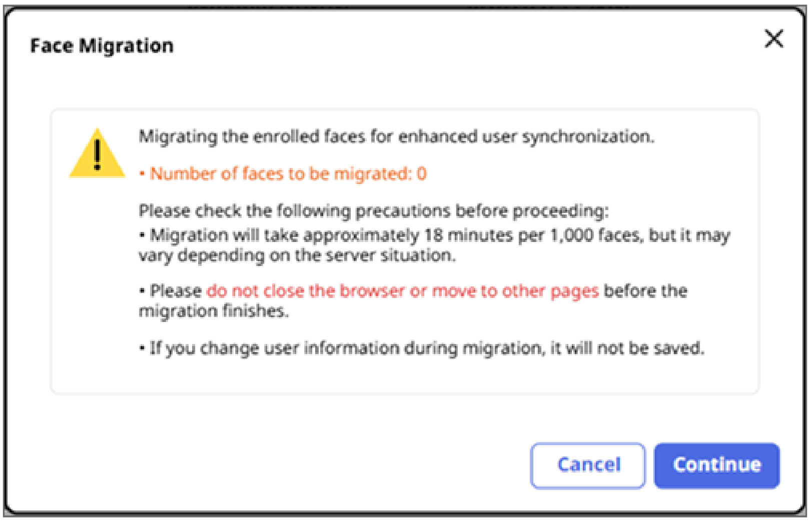


All Users (876)

□ Select All | Selected Items: 0

□	ID	Name	Email	Start Date	End Date	Card	Mobile ...	Face	Fingerp...	QR/Barc...	PIN
□	1	Administrator	-	2001/01/01 00:0...	2037/12/31 23:5...	0	0	0	0	0	-
□	60000	Jung-Hoo Lee	lshankland0@soup.io	2001/01/01 00:0...	2037/12/31 23:5...	3	0	0	0	0	-
□	60001	Gaven Prujean	gprujean1@dyndns.org	2001/01/01 00:0...	2037/12/31 23:5...	1	0	0	0	0	-
□	60002	Charity Inglish	cinglish2@smh.com.au	2001/01/01 00:0...	2037/12/31 23:5...	1	0	0	0	0	-

3. Check the contents of the warning popup and click **Continue**.



Face Migration

Migrating the enrolled faces for enhanced user synchronization.

• Number of faces to be migrated: 0

Please check the following precautions before proceeding:
• Migration will take approximately 18 minutes per 1,000 faces, but it may vary depending on the server situation.

• Please do not close the browser or move to other pages before the migration finishes.

• If you change user information during migration, it will not be saved.

Proceeding with face migration. When face migration is complete, a result pop-up will appear. It will show the total number of faces enrolled, as well as the number of faces that were successfully migrated and those that failed.

- After a successful migration, sync the user information to the device to apply the changes. For more information about how to send user information to the device, refer to the following.
- If face migration fails, you can download a list of failed users as a CSV file. To delete all faces that failed migration, click the **Delete** button.

INFO

- Only the admin account with user ID **1** can use this feature.
- Do not navigate away from the current page while the migration is in progress.
- The larger the size of the enrolled face images for each user, the longer it may take to generate the templates.
- For approximately 1,000 faces, the process takes about 18 minutes, although this may vary depending on server performance.
- For more information about how to save only the template without saving the user's facial image to the server, refer to the following.

Set Emergency Open Permissions

You can set emergency open permissions to allow specific users to access all doors in emergency situations. If a door is opened with a card that has emergency access permission set, that door remains open, allowing anyone to enter.

Before start

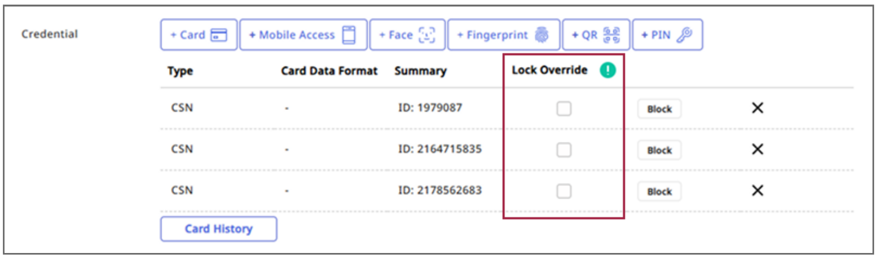
You must first add the card credentials before setting the emergency open permissions. For more information on how to add card credentials, refer to the following.

INFO

- Other credentials besides card credentials are not supported.
- All card credentials are supported except smart cards (AoC) and ToM mobile access cards (ToM AoC).
- Depending on the device, emergency open functionality may not be supported. Refer to the supported devices and firmware versions below.
  - BioStation 3 firmware v1.4.0 or higher

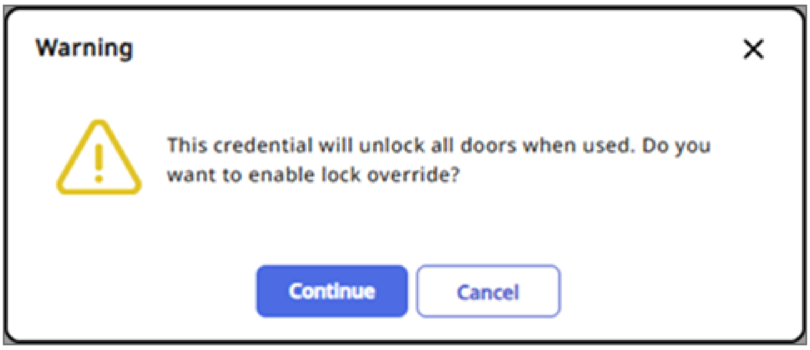
Set emergency open permissions

1. Click **User** on the **Launcher** page.
2. Double click the user you wish to set emergency open permissions for in the user list.
   Alternatively, select a user and click the **See More** button in the profile displayed on the right screen.
3. When the user detail screen appears, go to the **Credential** section.
4. Click the checkbox in the **Lock Override** item for the card credentials you want to allow for emergency open.



Type	Card Data Format	Summary	Lock Override		
CSN	-	ID: 1979087	□	Block	×
CSN	-	ID: 2164715835	□	Block	×
CSN	-	ID: 2178562683	□	Block	×

5. When a warning message appears, check the content and click **Continue**.



Warning

This credential will unlock all doors when used. Do you want to enable lock override?

6. Click **Save** at the top right of the screen.

Complete the setting of emergency open permissions.

⚠ CAUTION

Users can open all doors with an access card configured with emergency access permission.

ⓘ INFO

- You can select one or more card credentials to grant emergency access permission.
- To revoke emergency access permission, click the checkbox of the selected card credential's **Lock Override** item again.

Monitoring

This guide covers the features available on the Monitoring page, one of **BioStar X**'s core features.

Click Monitoring on the Launcher page or select Monitoring from the shortcut list at the top left of the screen.

Monitoring Doors → 5 items

Monitor doors, elevators, and advanced access control. Guides how to control related features and monitor in real time through live video.

- Check Door Status
- Door Control
- Control Slave Devices

↳ 5 items

Monitor Map → Read more

This guide explains how to monitor and control the real-time status of doors and cameras by zone and floor using the map monitoring feature. Visually manage areas and floor structures linked to the GIS map, utilizing various features such as access control and camera video playback.

Monitor Device → Read more

Monitor devices and cameras connected to all areas and doors in real time. Efficient management is possible through various features, including checking the status of devices and cameras, viewing detailed information, and playing camera video.

Monitor Video → Read more

This document provides step-by-step instructions for the main operations of the video monitoring feature, including adding video, resizing, repositioning, and checking alarms.

Monitor Event → Read more

This guide provides methods for monitoring and managing real-time events through the event monitoring feature. Utilize various functions such as alarm events, warning events, filtering, and status management to efficiently handle events.

Monitor Doors

Monitoring the door is one of the core features of the security system, allowing real-time checking and control of the door status. This document guides how to monitor and control doors, elevators, and advanced access control. This enables efficient security management and rapid response.

Check Door Status

You can monitor the status of the entrance door in real-time to operate the security system reliably. You can also check the abnormal status of the device assigned to the entrance door.

Door Control

Control the door and check the detailed information.

Control Slave Devices

This guides how to control devices connected to the entrance door.

Control Elevators

Control elevators and check detailed information.

Control Advanced Access Control

Control advanced access control and check detailed information.

Check Door Status

You can monitor the status of the entrance door in real-time to operate the security system reliably. Check the abnormal status of the device assigned to the entrance door at a glance through the status icon provided in **Monitoring** and respond immediately when a problem occurs.

Click **Monitoring** on the **Launcher** page or select **Monitoring** from the shortcut list at the top left of the screen. You can check the status of each entrance door in the **Door** tab located in the left sidebar of the screen.

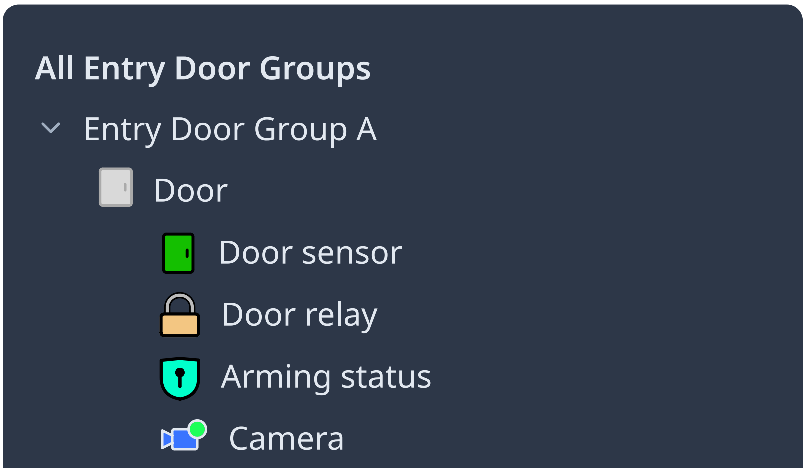
Before start

Ensure that the devices connected to the door are correctly configured. It is important to check if the device is connected to the network and updated with the latest firmware. In case of an issue, it is advisable to first check the power status and network connection of the device.

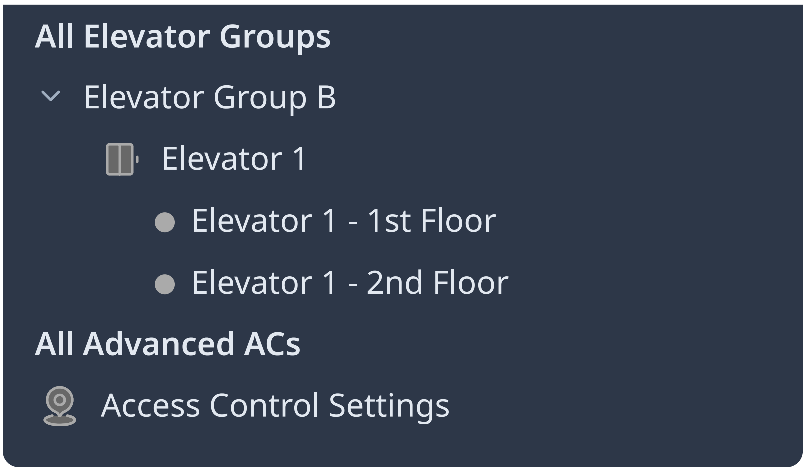
> **INFO**
>
> - For more information about adding and configuring devices, refer to the following.
> - For more information about adding and configuring doors, refer to the following.
> - The **Log Upload** feature must be enabled to monitor or control the status of the access door. This feature can be enabled in the **Settings** → **Server** → **Server** menu path under the **General** section.
> - The feature to connect cameras to the door through the VMS server is available as an additional option with an **Advanced** license or higher. For more information on licensing policy, refer to the following.

Learn about the tree structure

The tree structure in the **Door** tab of the left sidebar is organized as follows.



All Entry Door Groups
Entry Door Group A
Door
Door sensor
Door relay
Arming status
Camera



All Elevator Groups

Elevator Group B

Elevator 1

Elevator 1 - 1st Floor

Elevator 1 - 2nd Floor

All Advanced ACs

Access Control Settings

INFO

- For more information about adding and configuring devices, refer to the following.
- For more information about adding and configuring doors, refer to the following.
- For more information about adding and configuring elevators, refer to the following.
- For more information on advanced access control settings, refer to the following.
- To link the door and the camera, refer to the following.

Check status

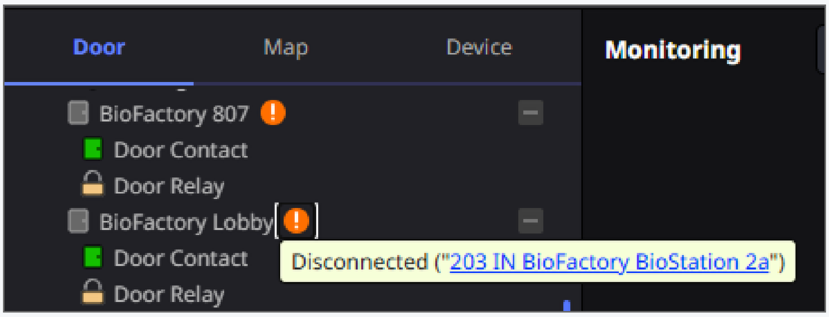
Check connection errors and alarms

You can check the status of the door or elevator to verify proper operation. Refer to the information below for the status of each icon.

Status Icon	Description
❗	Displays device abnormal statuses such as disconnection, communication server errors, and synchronization errors.
🚨	Displays the status when entrance door alarms (forced door opening, prolonged door opening, APB, fire alarms, emergency openings) or AI video analysis alarms (loitering detection, intrusion detection, etc.) occur.

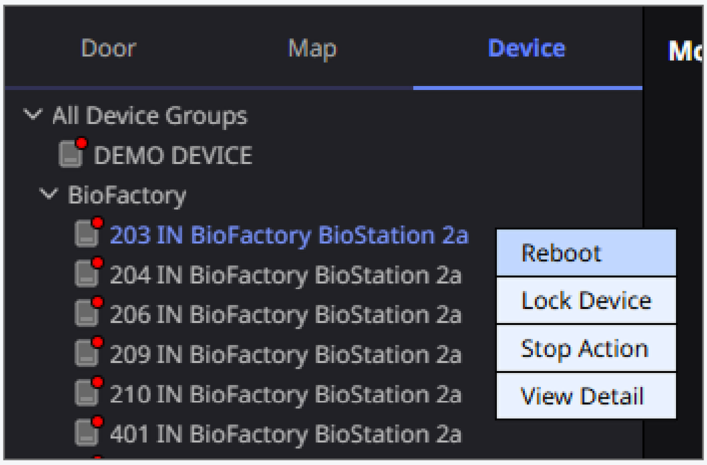
TIP

Click a status icon to view detailed information in a tooltip. Click the link in the tooltip error message to navigate to the list of devices connected to the door or elevator.



Disconnected ("203 IN BioFactory BioStation 2a")

Right-click on the device and select the **Reconnect** or **Reboot** option.


Door
Map
Device
Mo
All Device Groups
DEMO DEVICE
BioFactory
203 IN BioFactory BioStation 2a
204 IN BioFactory BioStation 2a
206 IN BioFactory BioStation 2a
209 IN BioFactory BioStation 2a
210 IN BioFactory BioStation 2a
401 IN BioFactory BioStation 2a
Reboot
Lock Device
Stop Action
View Detail

INFO

- Alarms occurring from the door or elevator can be configured through the following settings.
  - Door alarm settings
  - Elevator alarm settings
  - Advanced access control settings
- You can connect the entrance door and the camera in video rules to set alarms. For more information on video rule settings, refer to the following.
- When linked with the VMS server, AI event alarms for videos can be sent to **BioStar X**. For more information, refer to the manual for the VMS server.
- For more information on acknowledging alarms, refer to the following.

Checking door lock status

You can check the locking status of the door through the door relay status. Refer to the following for the status of the door relay.

Status Icon	Description
🔒	The entrance door is locked.
🔓	The door is open.

Checking camera status

Check the camera status to verify that the camera is operating normally. Refer to the following for camera status.

Status Icon	Description
📹🟢	The camera is connected.
📹❌	The camera is off or disconnected.

Checking arming status

You can check the security status of the entrance door or advanced access control settings.

Status Icon	Description
⊘	This is the icon for inactive settings. Inactive settings do not generate alarms.
🛡	The door is armed.
🛡⃠	The door is disarmed.

> ⓘ **INFO**
>
> The security status is displayed only when the entrance door is set to **guard**. For more information on security settings, refer to the following.

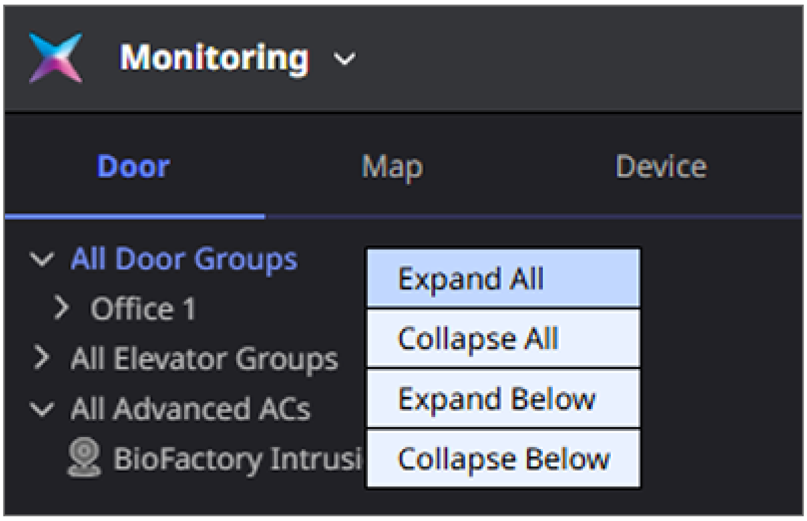
Check elevator status

You can check the floor access control status via the elevator.

Status Icon	Description
●	The corresponding floor is locked via the elevator.
🟢	The corresponding floor is unlocked via the elevator.

Expand/collapse group list

You can expand or collapse the list through the top-level group or sub-group.



Top-level group

1. In the **Door** tab, select **All Door Groups** or **All Elevator Groups**, **All Advanced ACs** and right-click.
2. Choose **Expand All** or **Collapse All** from the popup menu.

All sub-lists can be expanded or collapsed based on the selected top-level group.

Sub-group

1. To expand or collapse the list of sub-groups in each top-level group, select the sub-group and right-click.
2. Select **Expand Below** or **Collapse Below** option from the popup menu.

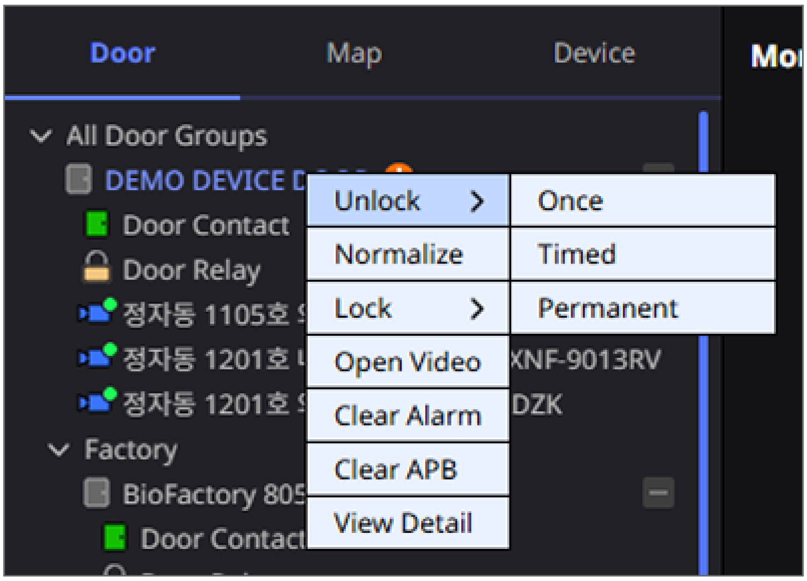
You can expand or collapse the list of the selected sub-group.

Door Control

This guide describes how to control doors. You can lock the door for a certain period of time, check the camera connected to the door and clear alarms that have occurred.

- Control the door remotely to manage access. You can set the door to be open or locked for a specific period of time.
- You can monitor access situations in real-time through the camera connected to the door.
- The anti-passback feature prevents unauthorized access and accurately manages access logs.

Click **Monitoring** on the **Launcher** page or select **Monitoring** from the shortcut list at the top left of the screen. Select the door you want to control and right-click. You can select the desired feature from the popup menu.



ⓘ **INFO**

- The **Log Upload** feature must be enabled to monitor or control the status of the access door. This feature can be enabled in the **Settings** → **Server** → **Server** menu path under the **General** section.
- The **Open Video** option is linked with the VMS and requires integration with the access door and camera to be used. Additionally, this feature can be used through purchase of add-on options with an **advanced** license or higher. For more information about the license policy, refer to the following.

Door open

The opened door can be accessed by anyone. Click **Unlock** in the popup menu and select the desired option.

- **Once**: Unlocks the door once.
- **Timed**: Opens the door for a certain time. Enter the desired time in seconds.
- **Permanent**: Unlocks the door regardless of time.

When the access door opens, the access door relay icon changes from 🔒 to 🔓 status.

> **TIP**
>
> The door can be temporarily opened for the convenience of external guests when they visit. After opening the door, be sure to switch to **Normalize** mode.

Door normalize

Changing the door to **Normalize** status will allow only authorized users to access. Click **Normalize** in the popup menu.

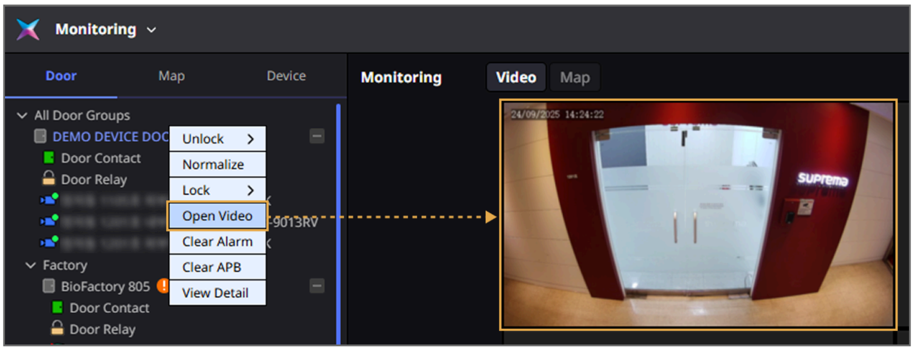
Door lock

Changing the door to **Lock** status will prevent anyone from access. Click **Lock** in the popup menu and select the desired option.

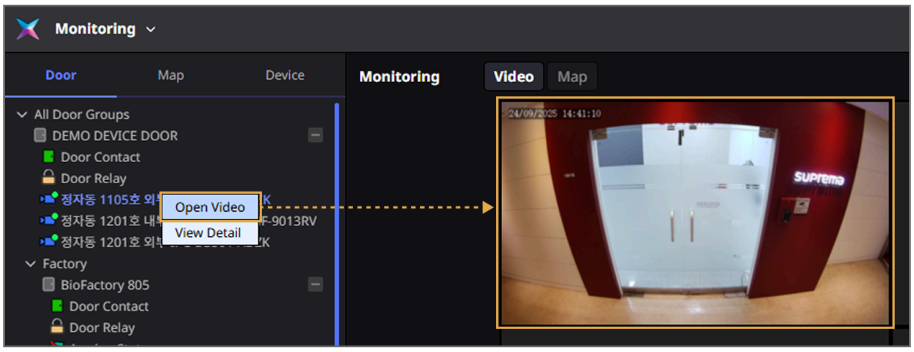
- **Timed**: Changes the door to a locked state for a certain period of time. Enter the desired time in seconds.
- **Permanent**: Changes the door to a locked state regardless of time.

Check door camera

You can check the camera connected to the door. Click **Open Video** in the popup menu. You can add and play footage from the selected camera in the video tile section of **Monitoring**.



Or select the desired camera and click the right mouse button. Click **Open Video** in the popup menu to add and play footage from the selected camera.



INFO

- If there is more than one camera connected to the access door, the first connected camera appears in the video tile.
- Video tiles are added in order from the top left of the screen. If there is no space to add more, an error message appears.
- For more information about video monitoring, refer to the following.
- This feature is available with additional options on the **Advanced** license or higher. For more information on licensing policy, refer to the following.

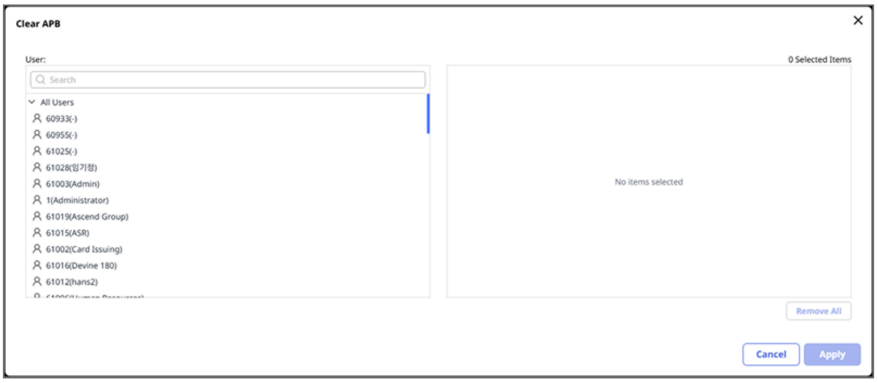
Clear alarm

You can deactivate the alarm that occurred at the door. Click **Clear Alarm** in the popup menu. An alarm message appears in the upper right corner of the screen.

Clear Anti Pass Back

You can deactivate the APB alarm when an anti-passback violation occurs.

1. Click **Clear APB** in the popup menu.
2. When the **Clear APB** window appears, check the list of users who have violated anti-passback.



3. Select a user and click the **Apply** button.

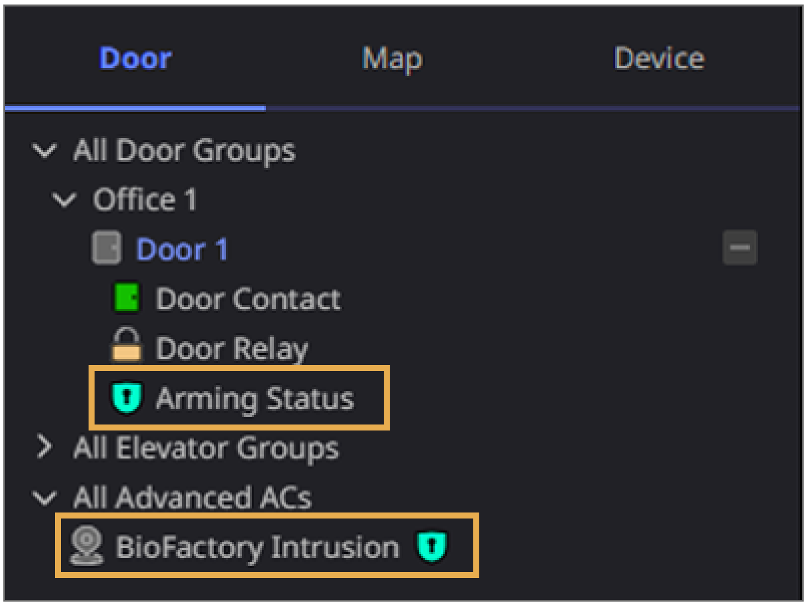
A completion message appears in the upper right corner of the screen.

ⓘ **INFO**

- **APB (Anti-passback)**: A structural method used to control access. This function uses access control devices installed both inside and outside the door, so that authentication is required for access to the zone. In the case of card-based access control systems, if a person enters a zone following the person in front without swiping their card on the reader, the door does not open when the person attempts to leave the zone, and subsequently an anti-passback event occurs. Anti-passback is categorized into hard APB and soft APB. If the anti-passback is violated, the anti-passback event is created immediately and hard APB does not permit access to the user while soft APB still permits access to the user.
- For more information on how to set up **anti-passback** at the door, refer to the following.

Set or unset the alarm

If the door is set to security, you can set or disable the security. Click **Arm** or **Disarm** in the popup menu.



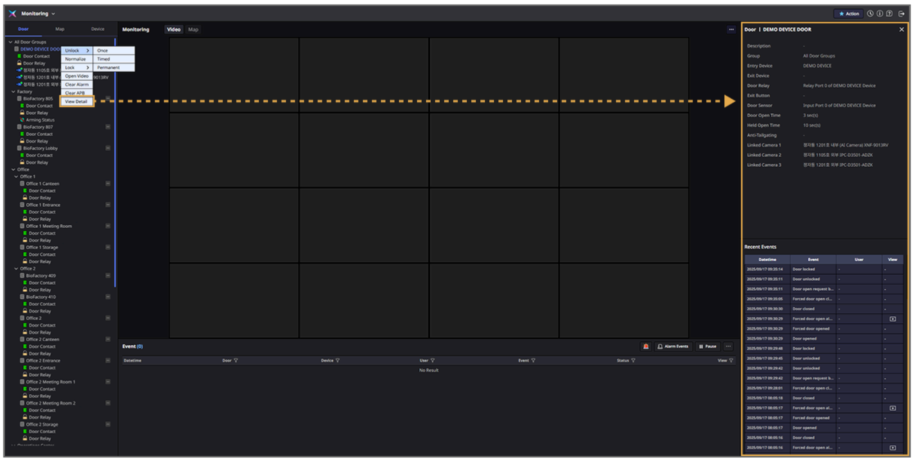
An access door in alarm status changes the alarm status icon from 🛡 to 🛡. At this time, the 🛡 icon is also applied to the corresponding access control setting.

ⓘ **INFO**

This feature can be used by purchasing additional options with an **advanced** license or higher, or with an **enterprise** license or higher. For more information about the license policy, refer to the following.

View details

You can check detailed information about the door and the event history. Click **View Detail** in the popup menu. Detailed information and event history for the door appear on the right side of the screen.



Door | DEMO DEVICE DOOR

Description	-
Group	All Door Groups
Entry Device	DEMO DEVICE
Exit Device	-
Door Relay	Relay Port 0 of DEMO DEVICE Device
Exit Button	-
Door Sensor	Input Port 0 of DEMO DEVICE Device
Door Open Time	3 sec(s)
Held Open Time	10 sec(s)
Anti-Tailgating	-
Linked Camera 1	정자동 1201호 내부 (AI Camera) XNF-9013RV
Linked Camera 2	정자동 1105호 외부 IPC-D3501-ADZK
Linked Camera 3	정자동 1201호 외부 IPC-D3501-ADZK

Recent Events

Datetime	Event	User	View
2025/09/17 09:35:14	Door locked	-	-
2025/09/17 09:35:11	Door unlocked	-	-
2025/09/17 09:35:11	Door open request b...	-	-
2025/09/17 09:35:05	Forced door open cl...	-	-
2025/09/17 09:30:30	Door closed	-	-
2025/09/17 09:30:29	Forced door open al...	-	▶
2025/09/17 09:30:29	Forced door opened	-	-
2025/09/17 09:30:29	Door opened	-	-
2025/09/17 09:29:48	Door locked	-	-
2025/09/17 09:29:45	Door unlocked	-	-
2025/09/17 09:29:42	Door unlocked	-	-
2025/09/17 09:29:42	Door open request b...	-	-
2025/09/17 09:28:01	Forced door open cl...	-	-
2025/09/17 08:05:18	Door closed	-	-
2025/09/17 08:05:17	Forced door open al...	-	▶
2025/09/17 08:05:17	Forced door opened	-	-
2025/09/17 08:05:17	Door opened	-	-
2025/09/17 08:05:16	Door closed	-	-
2025/09/17 08:05:16	Forced door open al...	-	▶

- **Door Detail Information**: You can check the name, location, status, and information of connected sub-devices of the door.
- **Recent Events**: You can check the recent event list that occurred at the selected access door.

> **INFO**
>
> For more information about each item in the door's details section, refer to the following.

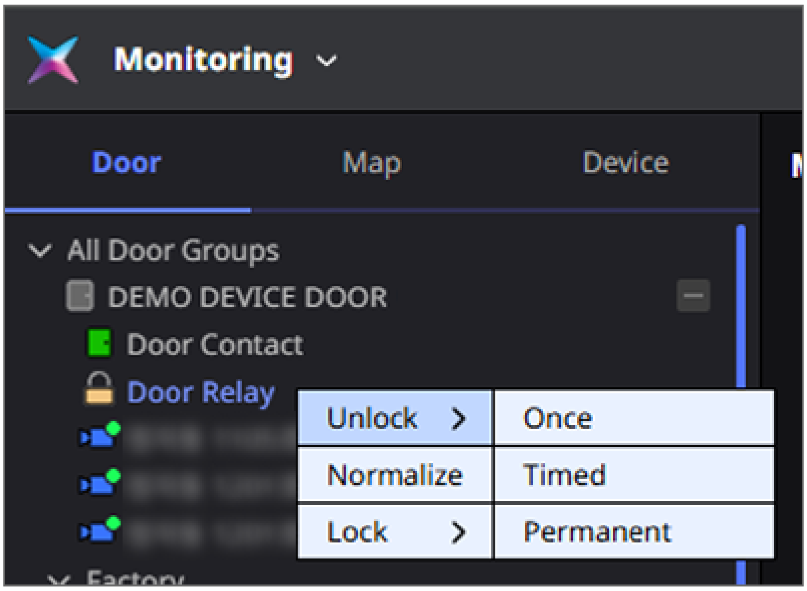
Control Slave Devices

This document provides guidance on controlling devices by model for easy control of devices connected to the entrance door. Various features are available, such as locking/unlocking via door relay, checking camera video and detailed information, and managing security status.

1. Click **Monitoring** on the **Launcher** page or select **Monitoring** from the shortcut list at the top left of the screen.
2. In the **Door** tab, select a door.
3. Select the connected device from the sublist and click the right mouse button. You can select the desired feature from the popup menu.

Controlling door relay

You can control the relay connected to the door. Right-click on the relay device. You can select the desired feature from the popup menu.



ⓘ **INFO**

Relay: A control device that auto-executes the opening and closing of the electric circuit according to changes in the current, voltage, frequency, etc. of another electric circuit.

Relay unlock

You can unlock the door through the relay device connected to the door. The opened door can be accessed by anyone. Click **Unlock** in the popup menu and select the desired option.

- **Once**: Unlocks the door once.
- **Timed**: Opens the door for a certain time. Enter the desired time in seconds.

- **Permanent**: Unlocks the door regardless of time.

Opening the door relay changes the door relay icon from 🔒 to 🔓.

> **TIP**
>
> The door can be temporarily opened for the convenience of external guests when they visit. After opening the door, be sure to switch to **Normalize** mode.

Relay normalize

Change the door to **Normalize** status using the relay so that only authorized users can access. Click **Normalize** in the popup menu.

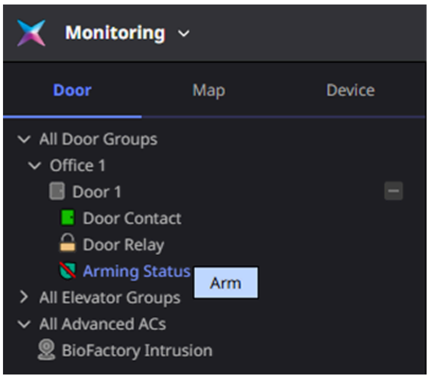
Relay lock

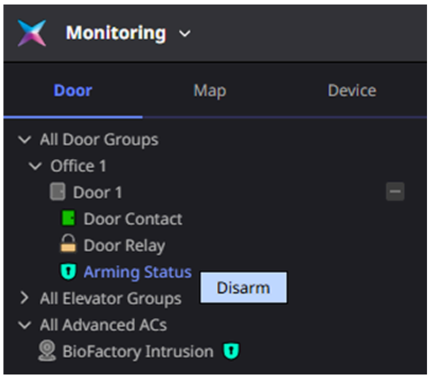
Change the door to **Lock** status using the relay connected to the door will prevent anyone from access. Click **Lock** in the popup menu and select the desired option.

- **Timed**: Changes the door to a locked state for a certain period of time. Enter the desired time in seconds.
- **Permanent**: Changes the door to a locked state regardless of time.

Controlling security device

You can set or unset the door in armed state through the security device connected to the door. Click **Arm** or **Disarm** in the popup menu.

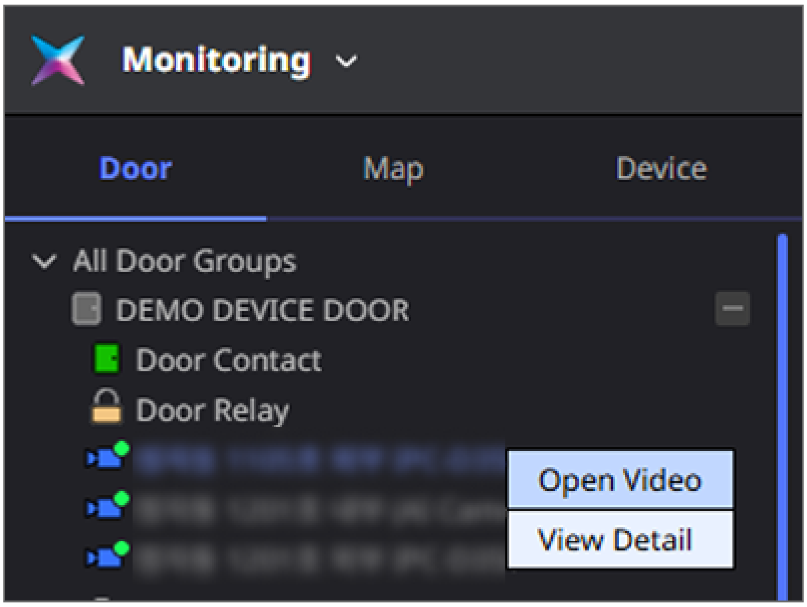




> **INFO**
>
> This feature can be used by purchasing additional options with an **advanced** license or higher, or with an **enterprise** license or higher. For more information about the license policy, refer to the following.

Controlling door camera device

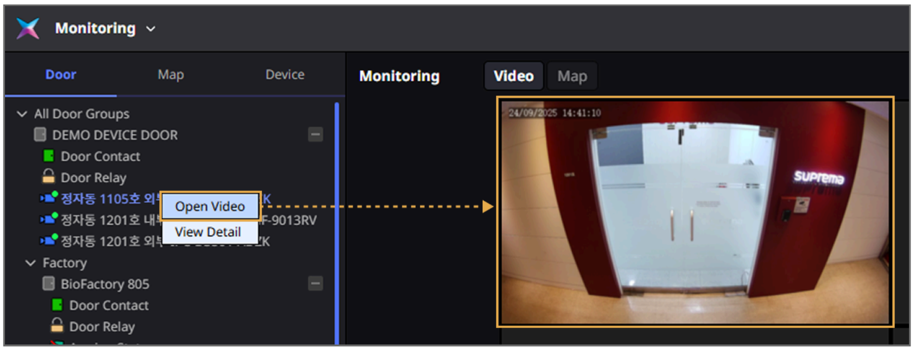
You can control the camera device connected to the door. You can view the camera video in real time or view details.



> **INFO**
>
> - This feature requires the door to be connected to a camera in order to be used. Refer to the following for how to integrate the door with the camera.
> - This feature is available with additional options on the **Advanced** license or higher. For more information on licensing policy, refer to the following.

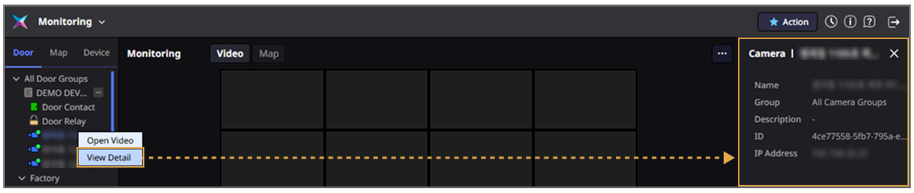
Checking camera video

To view the camera feed in real-time, click **Open Video** from the pop-up menu. You can add and play footage from the selected camera in the video tile section of **Monitoring**.



View camera details

To view the camera details, click **View Detail** in the popup menu. Camera details appear on the right side of the screen.



Name	[redacted]
Group	All Camera Groups
Description	-
ID	4ce77558-5fb7-795a-e...
IP Address	[redacted]

Control Elevators

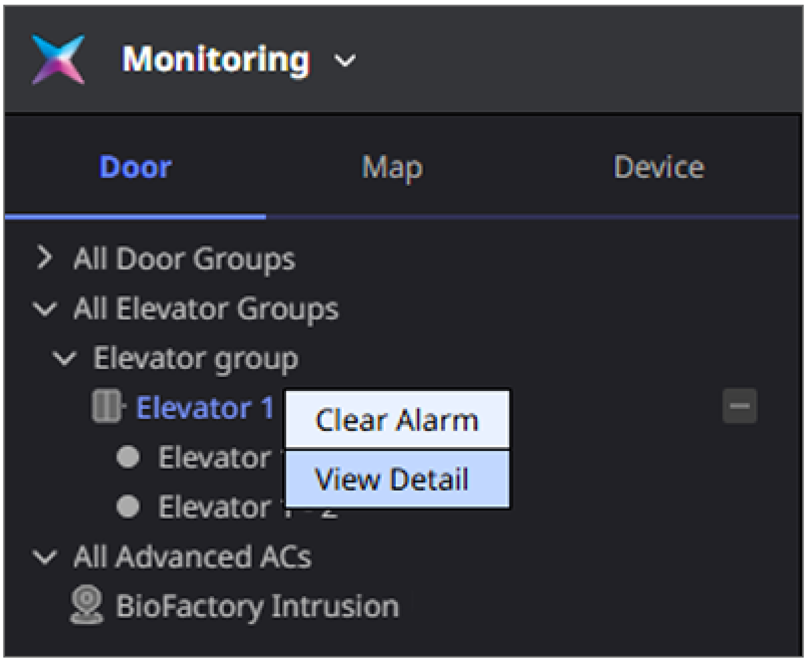
This guide describes how to control the elevator. You can control the elevator or check detailed information through the provided features.

1. Click **Monitoring** on the **Launcher** page or select **Monitoring** from the shortcut list at the top left of the screen.
2. In the **Door** tab on the left sidebar, go to **All Elevator Groups**.
3. Select the elevator in the desired group and right-click. You can select the desired feature from the popup menu.

> **INFO**
>
> For more information about how to set up the elevator and configuring groups, refer to the following.

Control Elevators

You can acknowledge or check details of alarms triggered by the elevator.

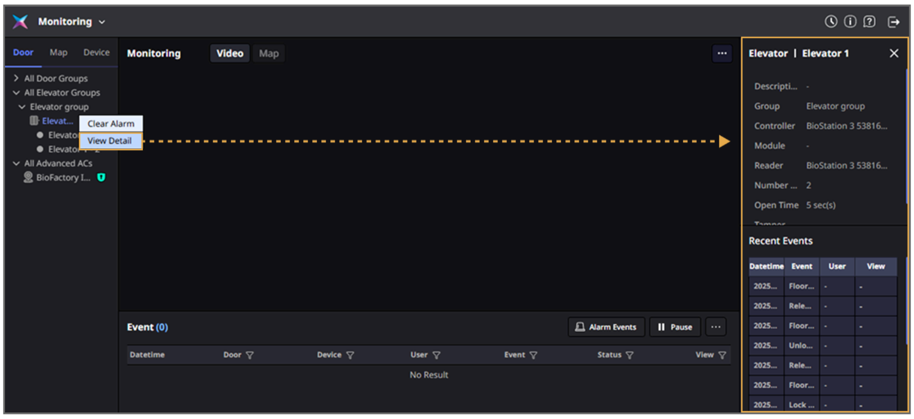


Clear alarm

You can deactivate the alarm that occurred at this elevator. Click **Clear Alarm** in the popup menu. A completion message appears in the upper right corner of the screen.

View details

You can check detailed information about the elevator and the event history. Click **View Detail** in the popup menu. Detailed information and event history for the elevator appear on the right side of the screen.



Elevator | Elevator 1

Descripti...	-
Group	Elevator group
Controller	BioStation 3 53816...
Module	-
Reader	BioStation 3 53816...
Number ...	2
Open Time	5 sec(s)

Recent Events

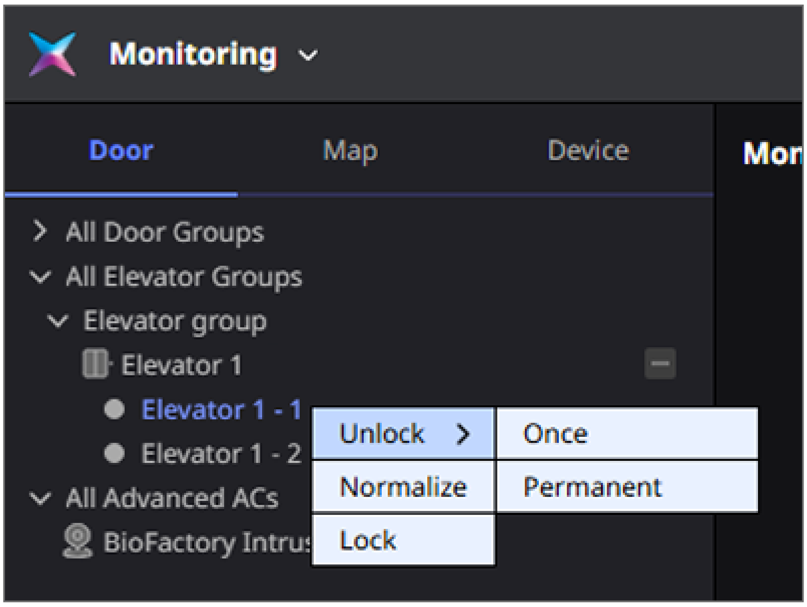
Datetime	Event	User	View
2025...	Floor...	-	-
2025...	Rele...	-	-
2025...	Floor...	-	-
2025...	Unlo...	-	-
2025...	Rele...	-	-
2025...	Floor...	-	-
2025...	Lock ...	-	-

- **View Details**: You can check the name, location, status information, and more for the elevator.
- **Recent Events**: You can check the recent event list that occurred at the selected elevator.

> **INFO**
>
> For more information about each item in the elevator's details section, refer to the following.

Floor access control

You can control the floors that can be accessed by the elevator. Click on the relay for the floor set in the elevator and right-click. Select the desired feature from the pop-up menu.



Floor open

The opened floor can be accessed by anyone. Click **Unlock** in the popup menu and select the desired option.

- **Once**: Opens the floor once.
- **Permanent**: Opens the floor regardless of time.

> **TIP**
>
> The floor can be temporarily opened for the convenience of external guests when they visit. After opening the floor, be sure to switch to **Normalize** mode.

Normalize floor

Changing the floor to **Normalize** status will allow only authorized users to access. Click **Normalize** in the popup menu.

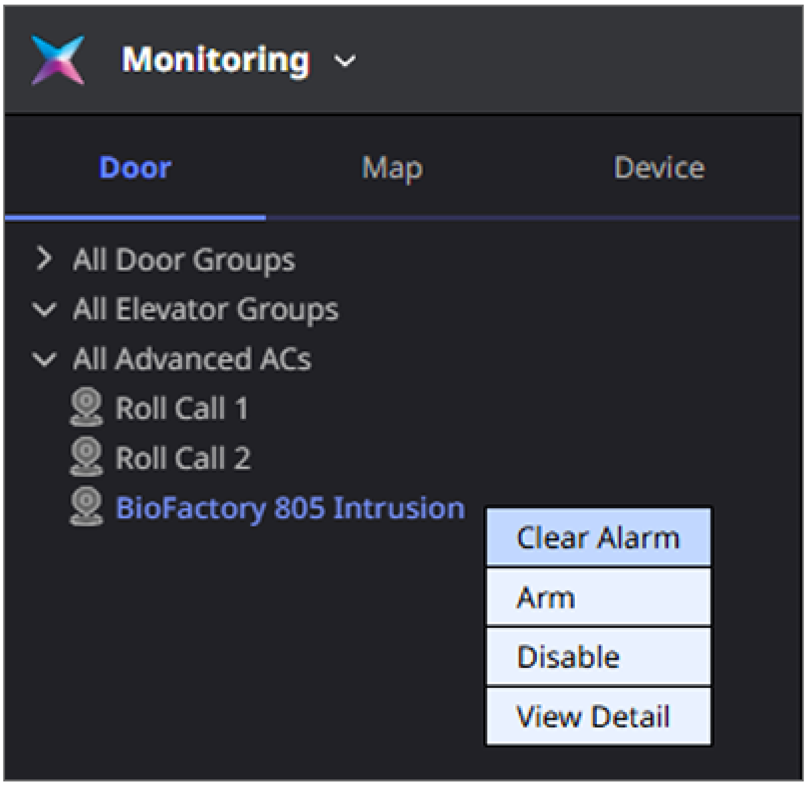
Lock floor

Changing the floor to **Lock** status will prevent anyone from access. Click **Lock** in the popup menu.

Control Advanced Access Control

This guides how to control doors or devices set with advanced access control. The features provided enable quick responses and efficient management in case of issues.

1. Click **Monitoring** on the **Launcher** page or select **Monitoring** from the shortcut list at the top left of the screen.
2. Move to **Door** tab under the left sidebar on the screen and select **All Advanced ACs**.
3. Select the configured advanced access control and right-click. You can select the desired feature from the popup menu.



> **INFO**
>
> The features offered vary depending on the type of advanced access control. The types of advanced access control are as follows.
>
> - **Anti-Passback**
> - Fire Alarm
> - Scheduled Lock/Unlock
> - Intrusion Alarm
> - Interlock
> - Muster
> - Occupancy Limit Zone
> - Roll Call
>
> For more information on each advanced access control, refer to the following.

Clear anti pass back

You can clear the APB alarm for the door or device set to **Anti-Passback**. Click **Clear APB** in the popup menu. A completion message appears at the top of the screen.

> **INFO**
>
> - The **Clear APB** feature is only available for **Anti-Passback**.
> - For more information about **Anti-Passback** settings, refer to the following.
> - For more information about **Anti-Passback**, refer to the following.

Clear alarm

You can clear the alarm that occurred at the door or device. Click **Clear Alarm** in the popup menu. A completion message appears at the top of the screen.

> **INFO**
>
> **Clear Alarm** cannot be used in the occupancy limit feature.

Activate/Deactivate

You can activate advanced access control or disable unused features. Deactivated advanced access control displays the ⊘ icon. Click **Enable** or **Disable** in the popup menu.

Security/Disarm

You can set or clear the security for the door or device. Click **Arm** or **Disarm** in the popup menu.

> ⓘ **INFO**
>
> - **Arm** or **Disarm** can only be used on advanced access control set for security.
> - For more information on security settings, refer to the following.

View muster report

To check the report on musters, click **Muster Report**. In the new window, you can check user entry and exit times and whether the stay time has exceeded through the user list and devices set with the muster feature.

> ⓘ **INFO**
>
> - The **Muster Report** feature is only available in musters.
> - For more information about the muster feature, refer to the following.

Monitoring occupancy limit

You can check the status of devices set with the occupancy limit feature. Click **Occupancy Monitoring** in the popup menu. In the new window, go to **Settings** → **Advanced AC** menu. You can check the status in the **Occupancy Limit** list.

> ⓘ **INFO**
>
> - The **Occupancy Monitoring** feature is only available for items set with the occupancy limit feature.
> - For more information on the occupancy limit settings, refer to the following.

View details

You can check detailed information and event occurrence history of advanced access control. Click **View Detail** in the popup menu. Detailed information and event occurrence history are displayed in the right panel of the screen.

- **Detailed Information**: You can check the name and status of the advanced access control feature, device information, etc.
- **Recent Events**: You can check the list of recent events occurred in the selected advanced access control.

ⓘ **INFO**

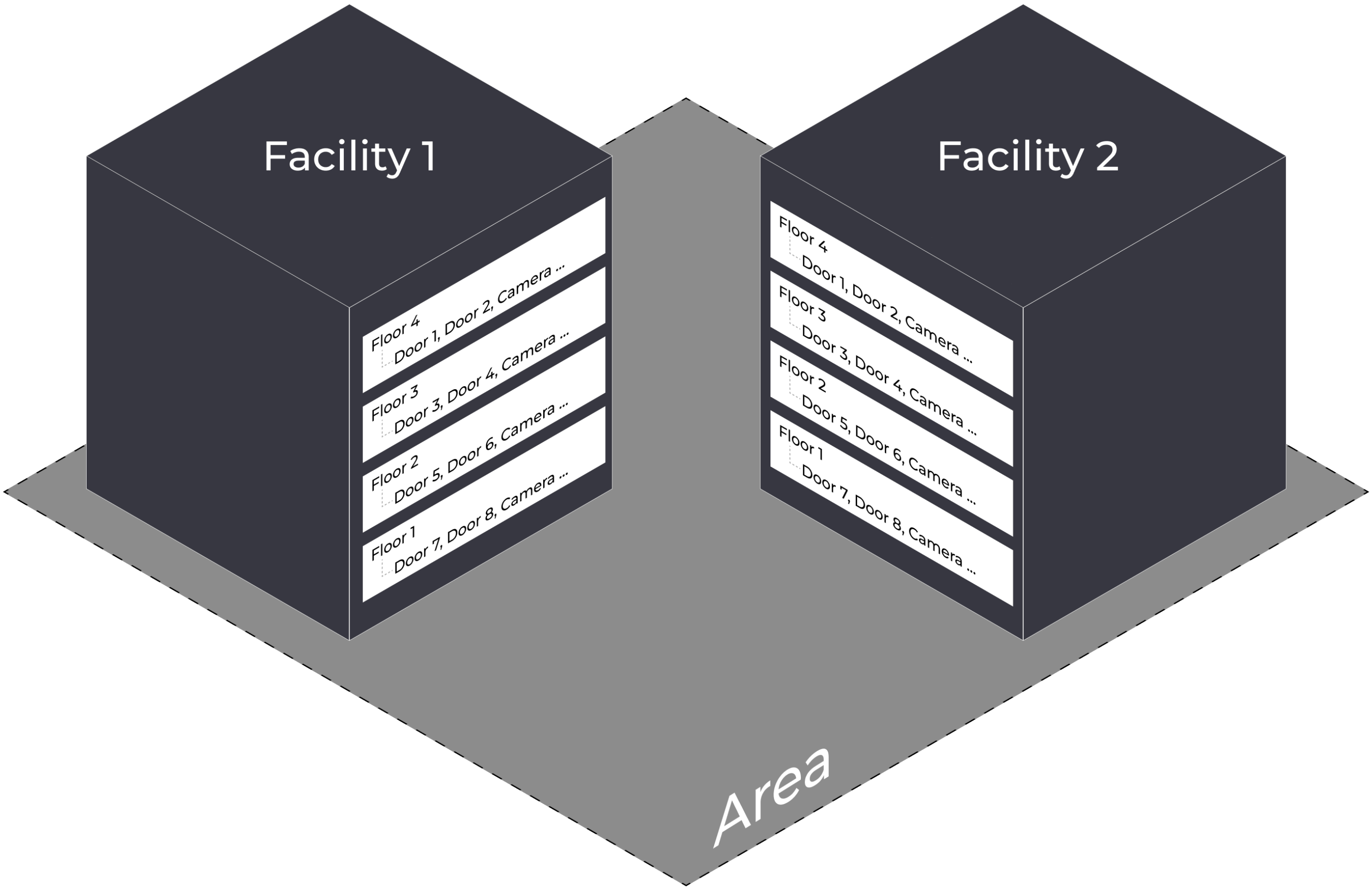
For more information on each item in the advanced access control details section, refer to the following.

Monitor Map

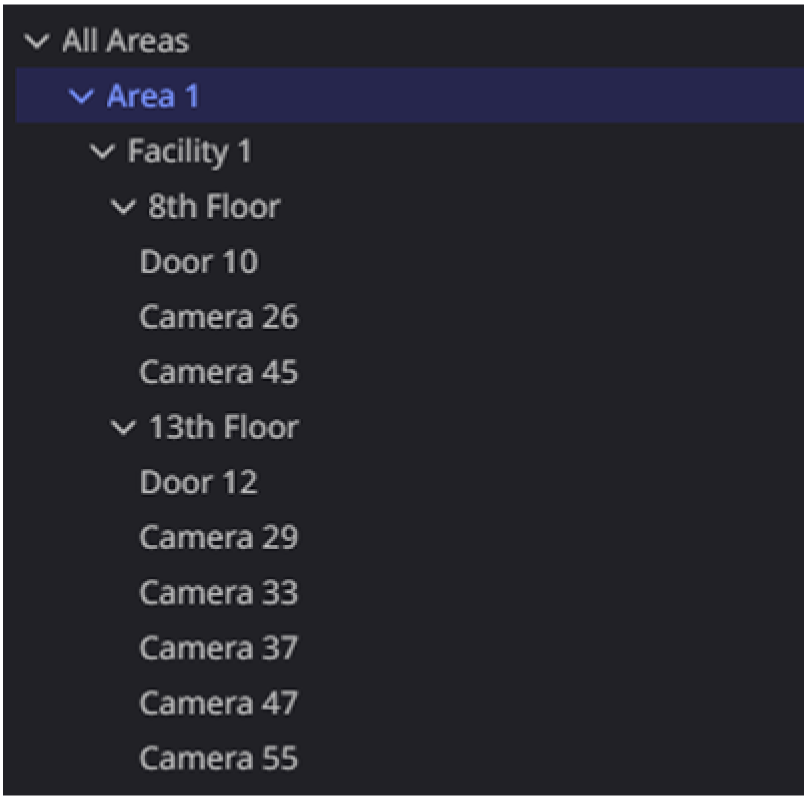
This guide explains how to monitor and control the real-time status of doors and cameras by zone and floor using the map monitoring feature. Map monitoring allows for easy navigation of areas and floors through a visual interface integrated with Google Maps, enabling various features such as access door control and camera video playback.

To access the **Monitoring** page, click **Monitoring** in the **Launcher** or select **Monitoring** from the menu at the top left of the screen.

Multiple facilities can be configured within a single area in **BioStar X**. Each facility can have multiple floors configured. In one floor, you can set up the door and camera based on the drawing for monitoring. Please refer to the below.


Facility 1
Floor 4
Door 1, Door 2, Camera ...
Floor 3
Door 3, Door 4, Camera ...
Floor 2
Door 5, Door 6, Camera ...
Floor 1
Door 7, Door 8, Camera ...
Facility 2
Floor 4
Door 1, Door 2, Camera ...
Floor 3
Door 3, Door 4, Camera ...
Floor 2
Door 5, Door 6, Camera ...
Floor 1
Door 7, Door 8, Camera ...
Area

You can access the configured area on the GIS map in the order of Area → Facility → Floor, as shown in the image, to monitor and control doors and cameras. This structure can also be seen in the sidebar of the **Monitoring** page.



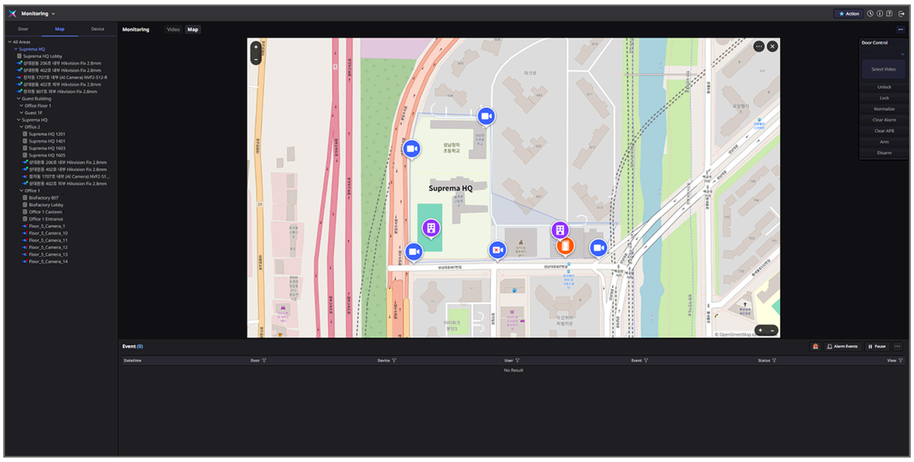
- All Areas
  - Area 1
    - Facility 1
      - 8th Floor
        - Door 10
        - Camera 26
        - Camera 45
      - 13th Floor
        - Door 12
        - Camera 29
        - Camera 33
        - Camera 37
        - Camera 47
        - Camera 55

> **INFO**
>
> For more information on how to configure the map, refer to the following.

Components and options

Component

Components displayed on the map include the area, facilities, and cameras connected to the facilities. You can access the floor through the facility. You can check the door and camera on the floor.



Component	Description
🏢	**Facility**: Click on a facility placed on the map to enter the corresponding configured floor.
🚪	**Door**: Click on a door placed on the map to display a popup menu for controlling that door. For more information about the provided features, refer to the following.
📹	**Camera**: Click on the camera to play the video of the corresponding facility or floor.
✕ 📹	**Camera Error**: This message appears when the camera is not connected or powered off.
🔓	**Open Door**: The door placed on the floor is in an open state.
🔒	**Locked Door**: The door placed on the floor is in a locked state.

Options

The options feature provided in the map or layer is as follows.

Feature	Description
+ − / + −	You can zoom in and out by clicking the buttons located at the top left and bottom right of the map. You can also use the mouse wheel to zoom in or out of the map.
+ 100% −	You can zoom in and out by clicking the buttons located at the bottom right of the floor.
•••	Click the button to access additional features.
✕	To close the map or floor positioned on the video tile, click the button at the top right.
✥	By clicking and dragging while holding down the icon, you can move the map to another location.

ⓘ **INFO**

- You can move the position by dragging the mouse while clicking on the map. You can zoom in or out using the mouse wheel.
- Double-click the map to expand it to full screen. Double-click again or press the ESC key to return to the original size.

Check status

In the left sidebar, you can check the status of each door and camera for the facilities or floors. Refer to the information below for the status of each icon.

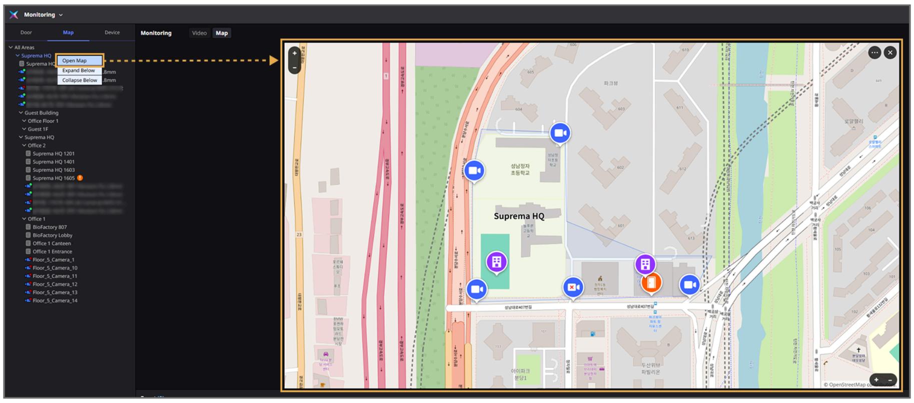
Status Icon	Description
❗	There is a communication server error or the connection is lost.
🚨	An alarm has occurred at the door. If loitering or intrusion is detected, the corresponding icon will be displayed.
📹🟢	The camera is connected.
📹❌	The camera is off or disconnected.

Open map

If the area is linked to the GIS map, you can display the map in the **Monitoring** section.

1. In the left sidebar, select the facility to view on the map.
2. Right-click.
3. Click **Open Map** in the popup menu.

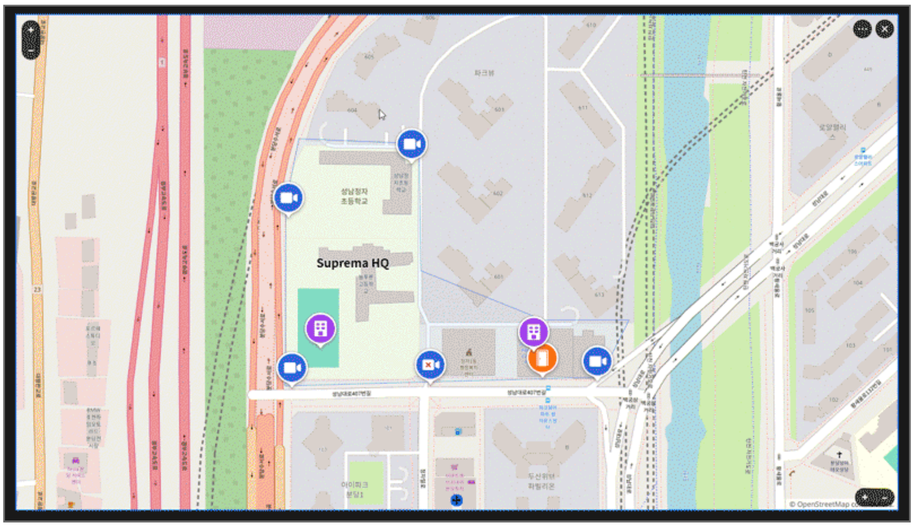
The map of the selected area will be displayed in the video tile of the **Monitoring** section.



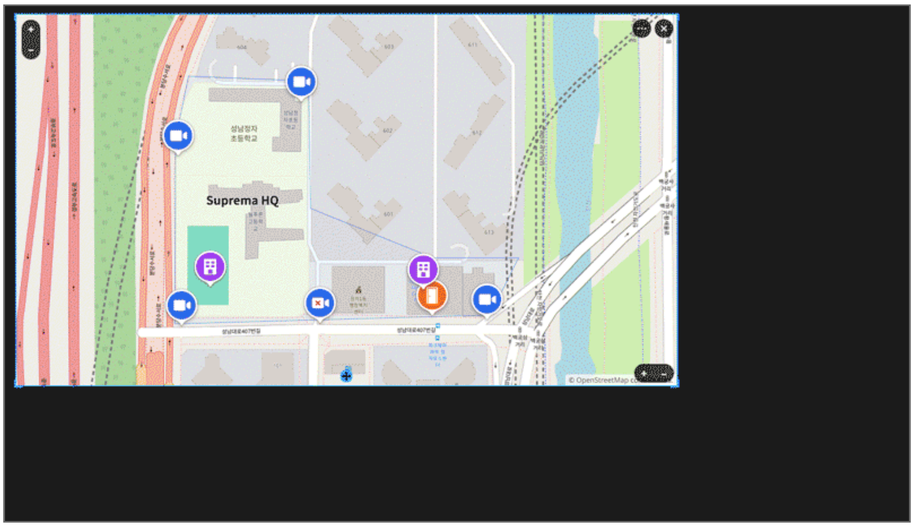
> **INFO**
>
> - You can also open the map by double-clicking the corresponding facility in the left sidebar.
> - The image is an example screen. The actual screen may differ.
> - For more information on how to configure areas linked to the GIS map, refer to the following.

Map size adjustment and relocation

To adjust the size of the map, click on an empty area on the map. Handles for resizing will appear at each corner. Click and drag the handle to adjust to the desired size.



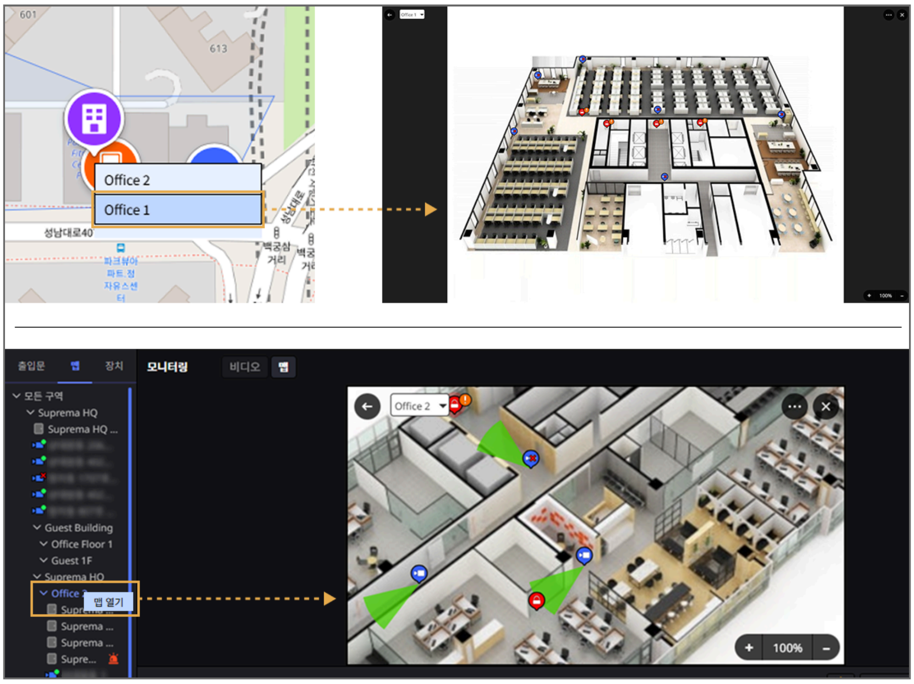
To move the map to another location while resizing, click on the ✥ icon over the map and drag it to the desired position.



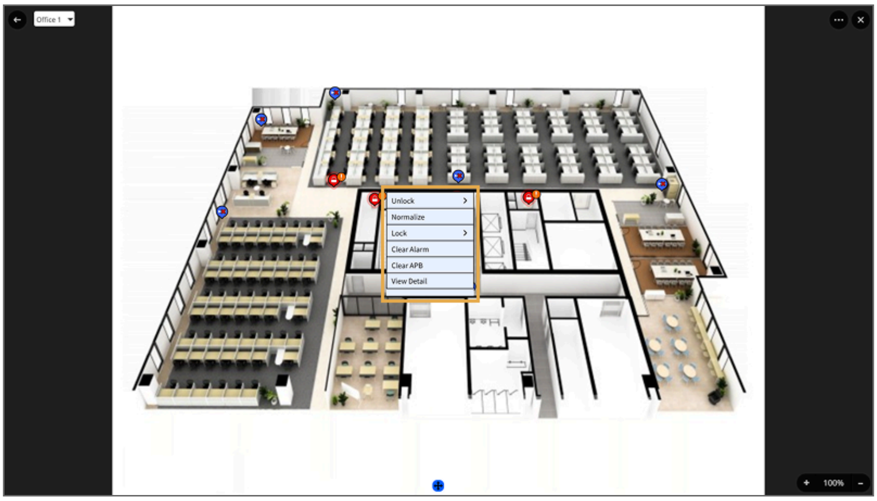
Enter the floor

To enter a floor on the map, click on the facility. When the list of floors accessible from the popup menu is displayed, select the desired floor. You can check the drawings, doors, and cameras on the selected floor.

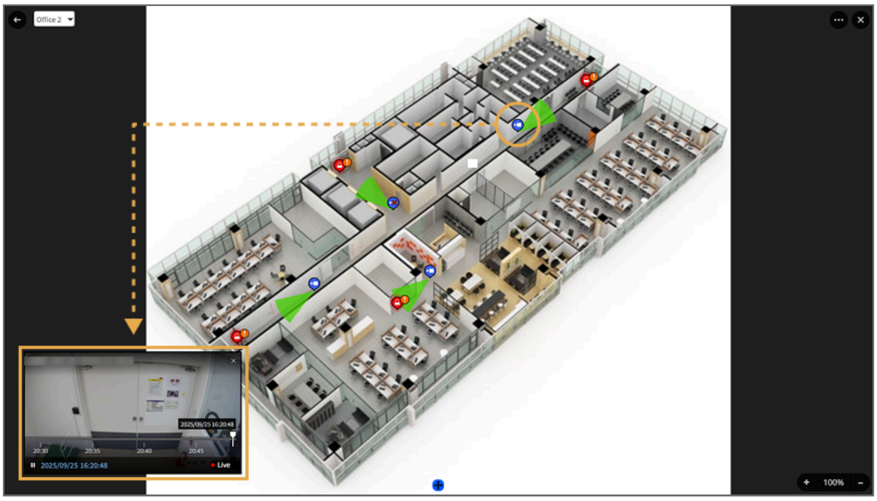
Or, double-click the floor in the left sidebar or right-click it and select **Open Map** from the popup menu.



- Clicking the door will display a popup menu that allows you to control that door. For more information about the provided features, refer to the following.



- Double-clicking the camera allows you to play the live feed.

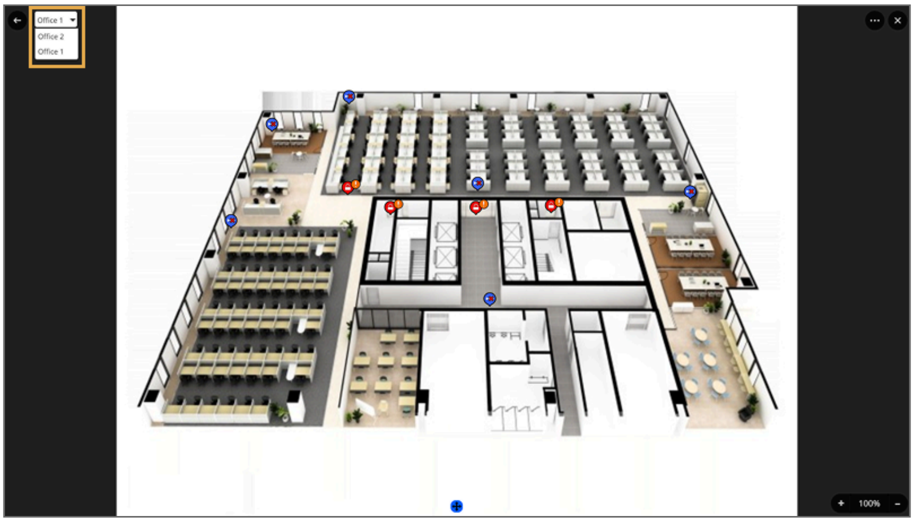


INFO

- For more information on how to set up doors and cameras in the floor, refer to the following.
- To navigate to the map displaying the facility, click the ← button at the top left.
- For more information about video control methods and the tools displayed in the video, refer to the following.
- The image is an example screen. The actual screen may differ.

Move to another floor

To move to a different floor, click on the selection option in the upper left corner of the map and select the floor you want to move to.

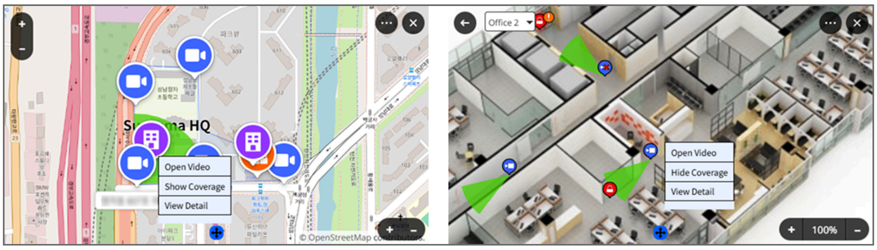


ⓘ **INFO**

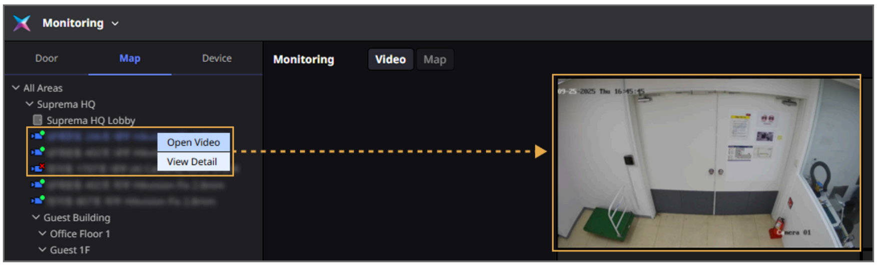
- To navigate to the map displaying the facility, click the ← button at the top left.
- The floor selection option at the top left of the map displays only the floors configured for the facility. If the floor is not configured in the facility, it will not be displayed in the list. For more information on how to configure floors in the facility, refer to the following.

Controlling camera

- To control the camera on the map or floor, click the camera icon. Select the desired feature from the pop-up menu.



  - **Open Video**: You can check the camera video in real-time.
  - **Show Coverage** / **Hide Coverage**: You can display or hide the shooting range of the camera.
  - **View Detail**: You can check detailed information about the camera. Displays the name, group, ID, IP address, etc., of the camera in the right panel.
- To place and play the camera feed on the video tile, double-click the camera in the **Map** list on the left sidebar of the screen. Or right-click and select **Open Video** from the popup menu.



To view detailed information such as the camera's name and group, click **View Detail** from the popup menu.

INFO

- Video tiles are added in order from the top left of the screen. If there is no space to add more, an error message appears.
- For more information about video control methods and the tools displayed in the video, refer to the following.

Monitor Device

This document provides guidance on using the device and camera monitoring features. You can check the status of devices and cameras, view detailed information, and play camera video in real-time, among various other features. Additionally, review recent events to efficiently manage the status of devices and cameras.

To access the **Monitoring** page, click **Monitoring** in the **Launcher** or select **Monitoring** from the menu at the top left of the screen.

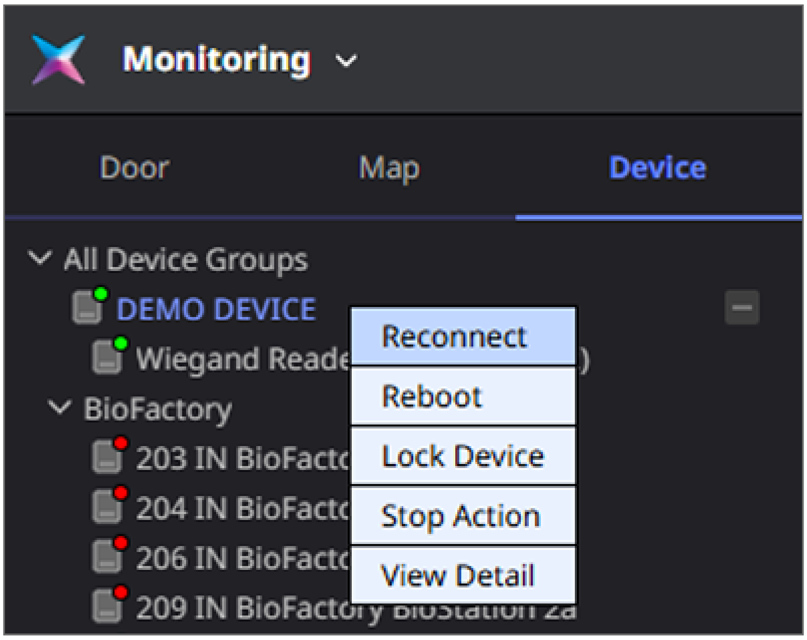
Checking device and camera status

Click the **Device** tab on the left sidebar. You can check the status of all devices and cameras. Refer to the following for the status of devices and cameras.

Status Icon	Description
🟢	The device is connected properly.
🟠	The device is off or disconnected.
📹🟢	The camera is connected.
📹❌	The camera is off or disconnected.

Device control

Select the desired device from the list on the left sidebar and right-click. You can select the desired feature from the popup menu.



Reconnect device

If the device is off or disconnected, click **Reconnect** in the popup menu. When the device reconnects, the status icon changes to

●.

> **INFO**
>
> The **Reconnect** feature is not supported for devices connected via **Device** ▶ **Server Connection** option. For more information on registering devices, refer to the following.

Restart device

To restart the device, click **Reboot** in the popup menu.

Lock device

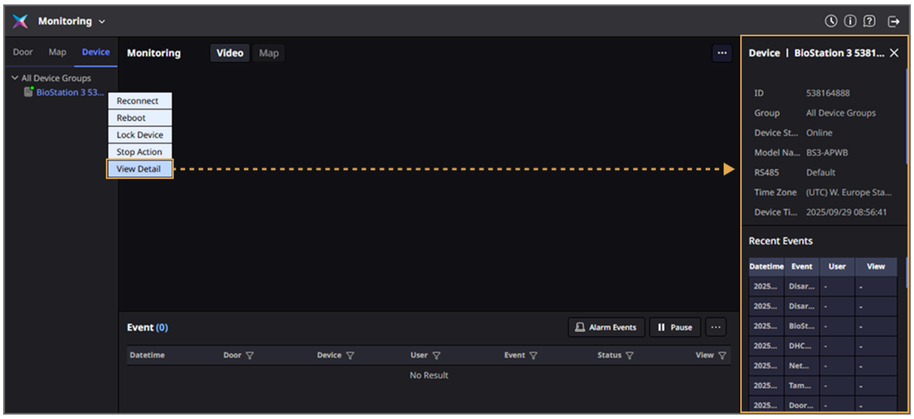
- To lock the device, click **Lock Device** in the popup menu. A message will appear at the top of the screen indicating that the device lock is in progress. When the lock is completed, the message will disappear.
- To unlock the device, click **Unlock Device** in the popup menu. A message will appear at the top of the screen indicating that the device unlock is in progress. When the unlock is completed, the message will disappear.

Stop action

To stop an ongoing action, click **Stop Action** in the popup menu. A success message for stopping the action will appear at the top of the screen. When the action stop is completed, the message will disappear.

Device detailed view

To view detailed information about the device, click **View Detail** in the popup menu. Or double-click the device. The detailed information of the device will appear on the right side of the screen.



Datetime	Door	Device	User	Event	Status	View
No Result						

ID	538164888
Group	All Device Groups
Device St...	Online
Model Na...	BS3-APWB
RS485	Default
Time Zone	(UTC) W. Europe Sta...
Device Ti...	2025/09/29 08:56:41

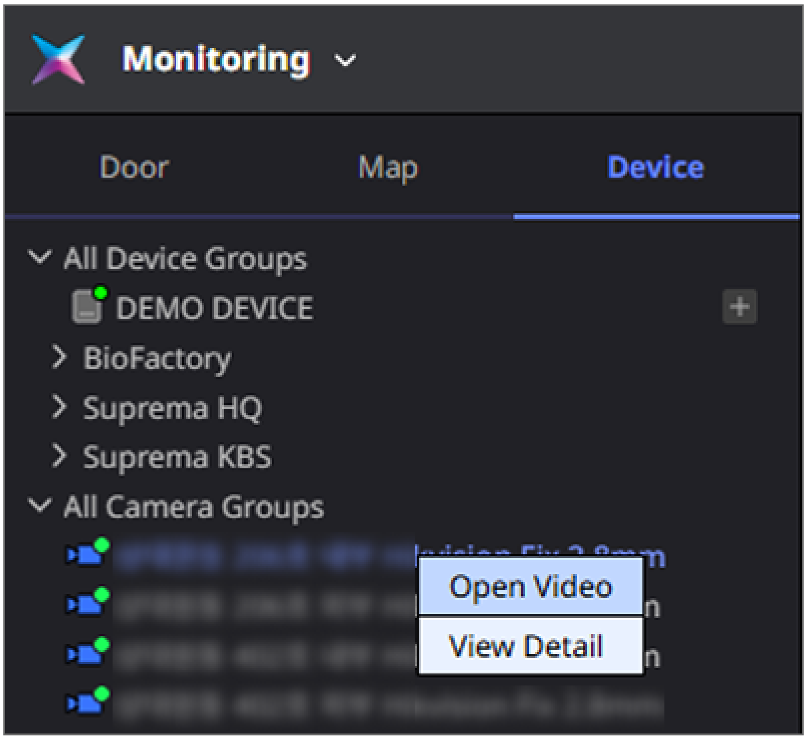
Recent Events

Datetime	Event	User	View
2025...	Disar...	-	-
2025...	Disar...	-	-
2025...	BioSt...	-	-
2025...	DHC...	-	-
2025...	Net...	-	-
2025...	Tam...	-	-
2025...	Door...	-	-

You can view the device's ID, group, model name, uptime, IP address, and other details. The **Recent Events** list at the bottom shows recent events in reverse chronological order.

Camera control

Select the desired camera from the list on the left sidebar and right-click. You can select the desired feature from the popup menu.



Playing camera video

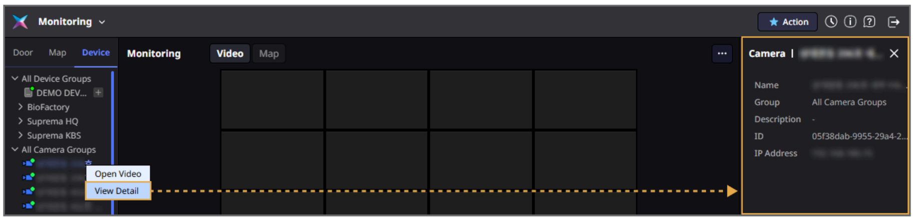
To place the camera video in the video tile and monitor in real-time, click **Open Video** in the popup menu.

> Adding camera video to video tiles can also be done in the following ways:
>
> - Double-click the camera to play the video from the camera in the left sidebar.
> - You can also add video by dragging and dropping the camera into the video tile area.

> **INFO**
>
> - Video tiles are added in order from the top left of the screen. If there is no space to add more, an error message appears.
> - For detailed information on how to control the video and the tools displayed on the video, refer to the following.

Camera detailed view

To view the camera details, click **View Detail** in the popup menu. You can check the camera's group, description, ID, and IP address.



Camera | [redacted]

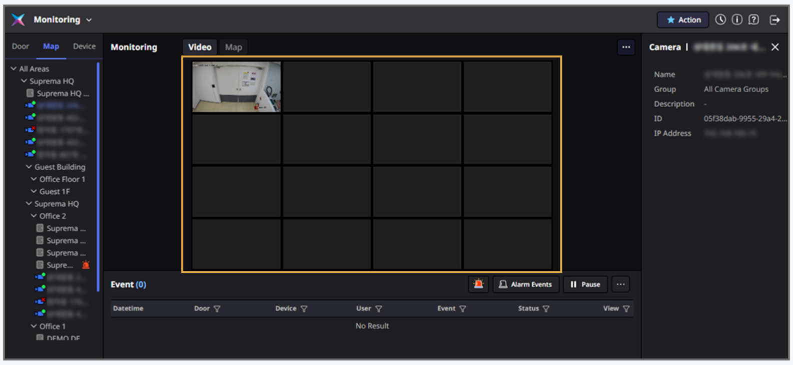
Name [redacted]
Group All Camera Groups
Description -
ID 05f38dab-9955-29a4-2...
IP Address [redacted]

Monitor Video

You can monitor and control camera videos linked to doors, areas, and devices in real-time through the video monitoring feature. This document provides guidance on how to utilize video tiles to add camera videos, resize, reposition, view in full screen, and perform various tasks. Additionally, it supports rapid response to security situations through management features such as checking and clearing alarm statuses.

INFO

- **Video Tile** is the area in the center of the screen where the camera video appears. It is an interface component that allows simultaneous placement and monitoring of multiple camera videos. Users can resize or reposition the video in the video tile and close or switch to full screen as needed.



Camera | [redacted]

Name [redacted]
Group All Camera Groups
Description -
ID 05f38dab-9955-29a4-2...
IP Address [redacted]

- For information on how to integrate with VMS and add and manage cameras, refer to the following.

- If a load error occurs when playing back recordings from VMS, install the certificate on the VMS server, and install the VMS server's certificate on the client PC. For more information, refer to the followings.

  – Install the certificate on the VMS server

  – Install the VMS server certificate on the client PC

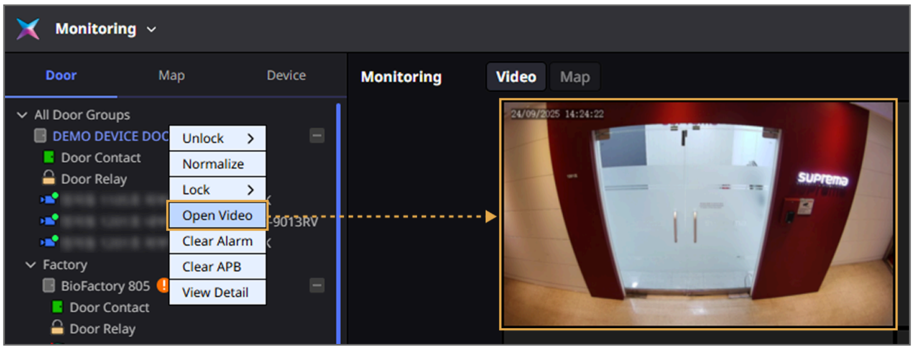
- Video monitoring is available with additional options for **Advanced** licenses and higher. For more information on licensing policy, refer to the following.

Play video

You can add camera videos to the video tile for monitoring. The video tile is located in the center of the screen and allows for simultaneous monitoring of multiple camera videos.

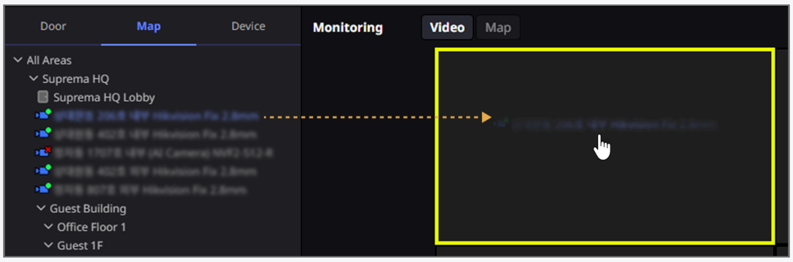
1. Select the camera device you wish to view from the **Door** or **Map**, **Device** tabs in the left sidebar.
2. Right-click.
3. Click **Open Video** in the popup menu.

The selected camera video can be placed in the video tile in the center of the screen.



ⓘ **INFO**

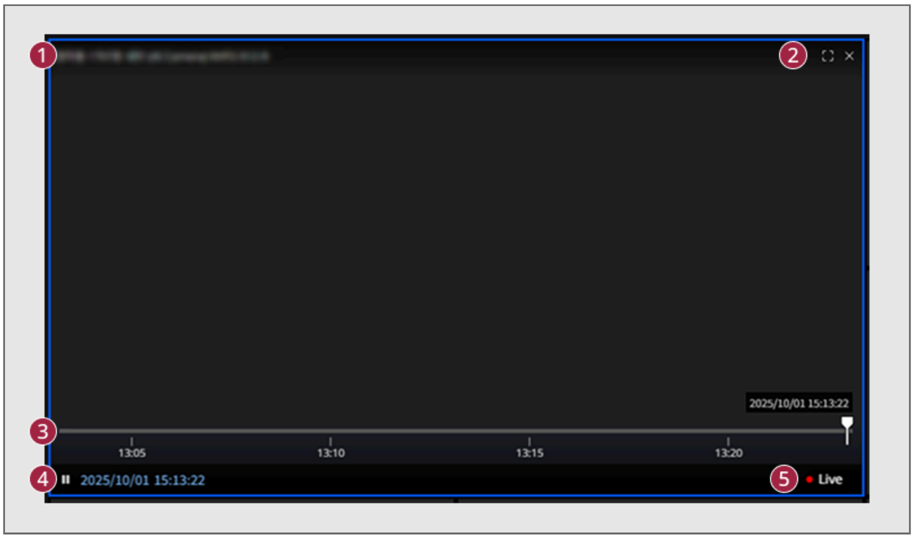
- You can also select cameras from the list in the sidebar and drag and drop them into the video tile area.



- Video tiles are added in order from the top left of the screen. If there is no space to add more, an error message appears.

Control video

The videos placed in the video tile are played in real-time by default. You can adjust the playback of the video or view recordings from the past using the playback tools.



1 This is the name of the camera device.

2 This is a button that allows you to play the video in full screen (⛶) or exclude it from the video tile (✕).

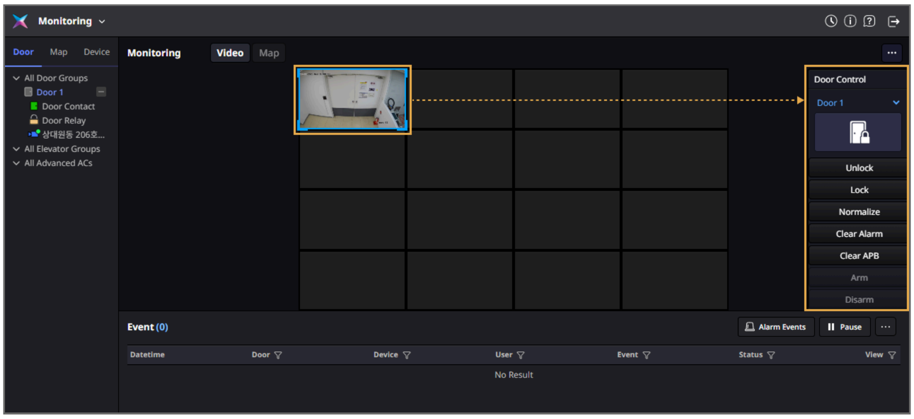
3 This is a slider that allows you to adjust the playback position of the video. Dragging the slider allows you to view past video.

4 To play or pause the video, click the ▶ or ⏸ button.

5 This icon indicates that the current video is being played in real-time. To switch back to live video when playing back video from the past, click this icon.

Door control tool

After adding a video, use the **Door Control** tool for additional actions. Selecting the camera linked to the door from the video tile activates the **Door Control** tool that can control the door. You can use functions such as open or lock the door, unlock, and disable the alarm.



Datetime	Door	Device	User	Event	Status	View

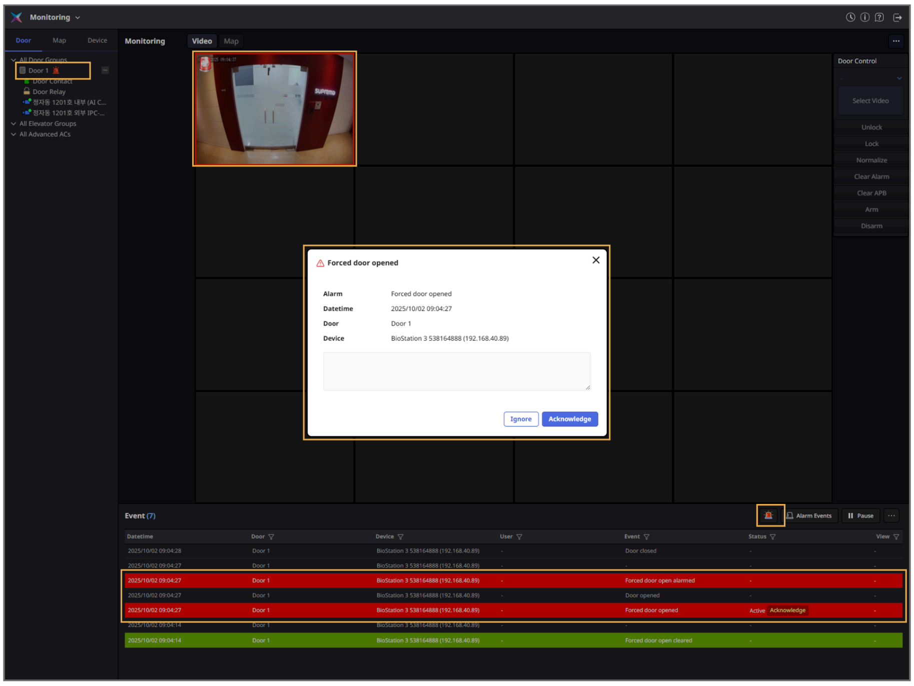
No Result

ⓘ **INFO**

- The **Door Control** tool can be used when there is nothing open in the right panel. If the detailed information is open in the right panel, use it while it is closed.
- This feature requires a camera to be linked to the door. For information on linking doors and cameras, refer to the following.
- For more information about the features available in the **Door Control** tool, refer to the following.

Check video alarm

When an alarm state is triggered for one of the doors linked to the camera, an alarm icon appears on the video. All alarms linked to the door must be cleared for the alarm icon to disappear.



Forced door opened

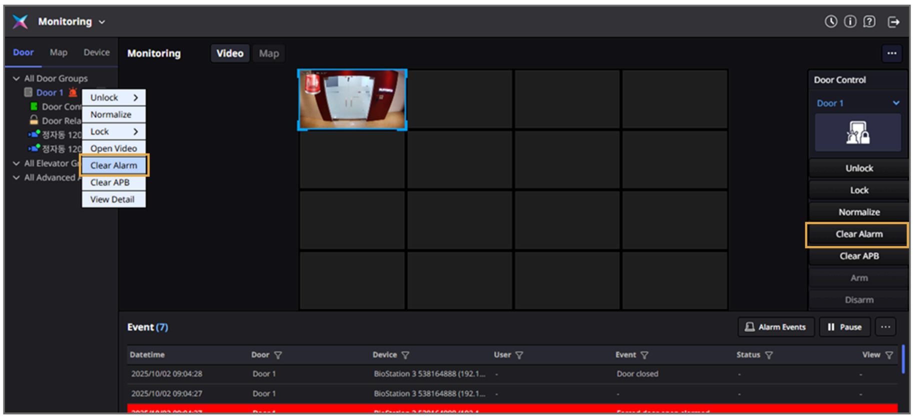
Alarm	Forced door opened
Datetime	2025/10/02 09:04:27
Door	Door 1
Device	BioStation 3 538164888 (192.168.40.89)

Ignore Acknowledge

Event (7)

Datetime	Door	Device	User	Event	Status	View
2025/10/02 09:04:28	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Door closed	-	-
2025/10/02 09:04:27	Door 1	BioStation 3 538164888 (192.168.40.89)	-	-	-	-
2025/10/02 09:04:27	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Forced door open alarmed	-	-
2025/10/02 09:04:27	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Door opened	-	-
2025/10/02 09:04:27	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Forced door opened	Active Acknowledge	-
2025/10/02 09:04:14	Door 1	BioStation 3 538164888 (192.168.40.89)	-	-	-	-
2025/10/02 09:04:14	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Forced door open cleared	-	-

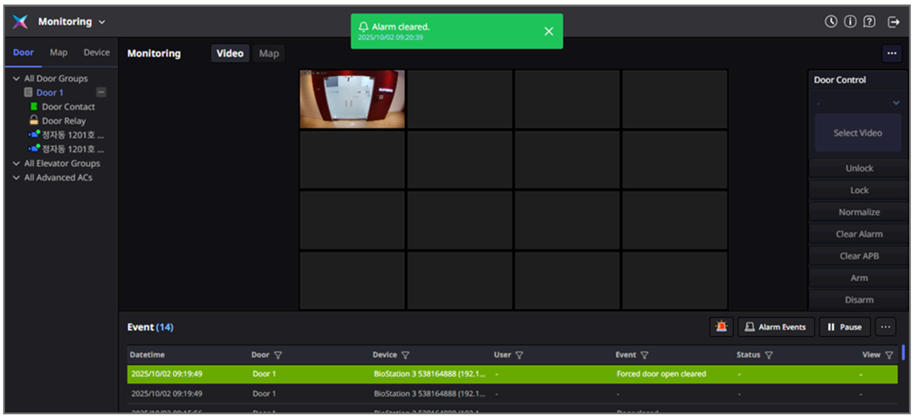
To clear the door alarm, right-click on the door in the list and click **Clear Alarm** in the popup menu. Alternatively, click **Door Control** tool, then click **Clear Alarm**.



Event (7)

Datetime	Door	Device	User	Event	Status	View
2025/10/02 09:04:28	Door 1	BioStation 3 538164888 (192.1...	-	Door closed	-	-
2025/10/02 09:04:27	Door 1	BioStation 3 538164888 (192.1...	-	-	-	-

A success or failure message will appear at the top of the screen.



Alarm cleared.
2025/10/02 09:20:39

Event (14)

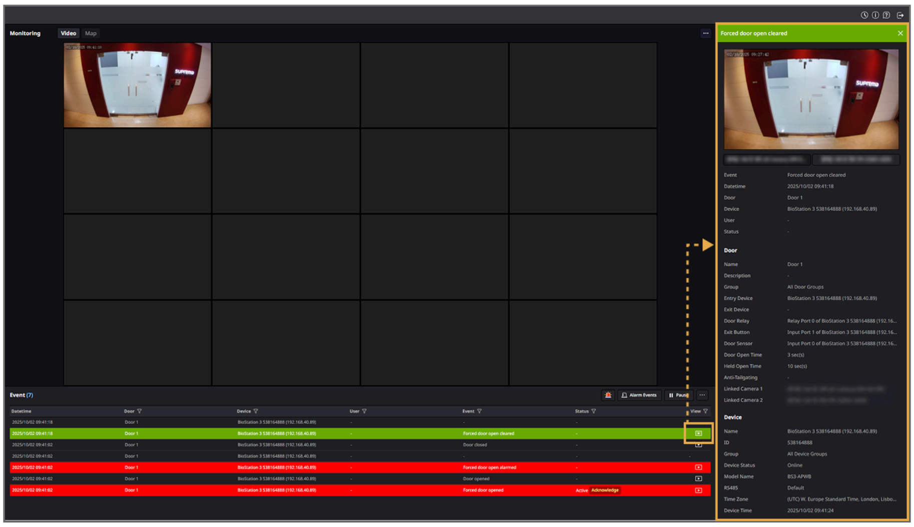
Datetime	Door	Device	User	Event	Status	View
2025/10/02 09:19:49	Door 1	BioStation 3 538164888 (192.1...	-	Forced door open cleared	-	-
2025/10/02 09:19:49	Door 1	BioStation 3 538164888 (192.1...	-	-	-	-

ⓘ **INFO**

For more information about the **Event** section at the bottom of the screen, refer to the following.

Check video log

When a specific event occurs at a door set by a rule, the corresponding event item in the **Event** section list will display a video log (▶) icon. Clicking on the event item with the video log icon will show detailed information on the right side of the screen, allowing you to view video from the time the specific event occurred. You can check the video of the time a specific event occurred.



Event (7)

Datetime	Door	Device	User	Event	Status	View
2025/10/02 09:41:18	Door 1	BioStation 3 538164888 (192.168.40.89)	-	-	-	
2025/10/02 09:41:18	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Forced door open cleared	-	▶
2025/10/02 09:41:02	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Door closed	-	▶
2025/10/02 09:41:02	Door 1	BioStation 3 538164888 (192.168.40.89)	-	-	-	-
2025/10/02 09:41:02	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Forced door open alarmed	-	▶
2025/10/02 09:41:02	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Door opened	-	▶
2025/10/02 09:41:02	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Forced door opened	Active Acknowledge	▶

Event	Forced door open cleared
Datetime	2025/10/02 09:41:18
Door	Door 1
Device	BioStation 3 538164888 (192.168.40.89)
User	-
Status	-

Door

Name	Door 1
Description	-
Group	All Door Groups
Entry Device	BioStation 3 538164888 (192.168.40.89)
Exit Device	-
Door Relay	Relay Port 0 of BioStation 3 538164888 (192.16...
Exit Button	Input Port 1 of BioStation 3 538164888 (192.16...
Door Sensor	Input Port 0 of BioStation 3 538164888 (192.16...
Door Open Time	3 sec(s)
Held Open Time	10 sec(s)
Anti-Tailgating	-
Linked Camera 1	[redacted]
Linked Camera 2	[redacted]

Device

Name	BioStation 3 538164888 (192.168.40.89)
ID	538164888
Group	All Device Groups
Device Status	Online
Model Name	BS3-APWB
RS485	Default
Time Zone	(UTC) W. Europe Standard Time, London, Lisbo...
Device Time	2025/10/02 09:41:24

ⓘ **INFO**

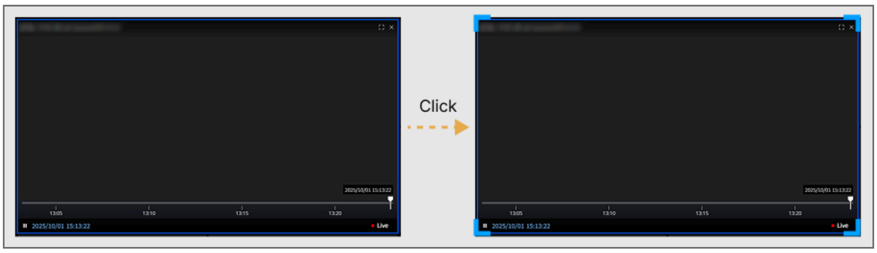
- The video log icon is displayed only when a camera is linked to the door. For information on linking cameras and doors, refer to the following.
- The first connected camera is prioritized for playback based on event setting rules. To view the video on a larger screen, double-click on it.
- You can link up to 4 cameras to a door and can click the camera button at the bottom of the video to play the desired camera's video. If only one camera is linked, the camera button will not be displayed.
- For more information about the **Event** section at the bottom of the screen, refer to the following.

Set video tile layout

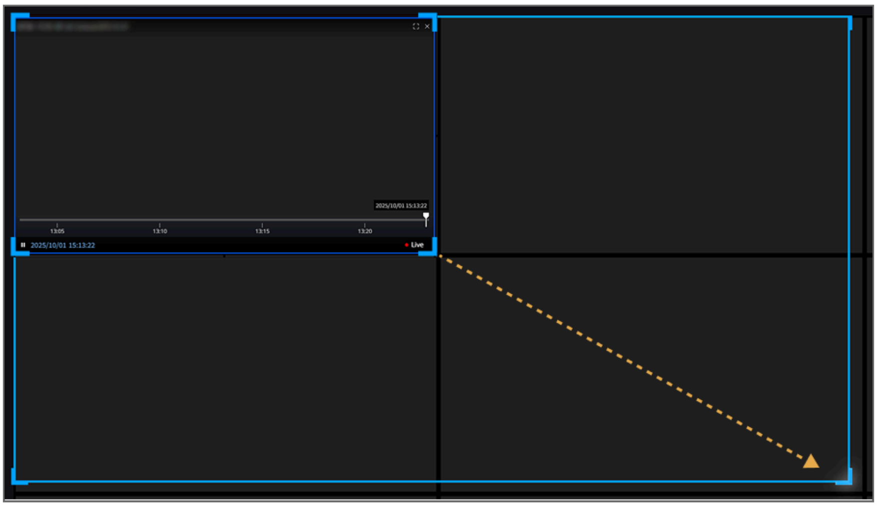
You can resize the video placed in the video tile or reposition it as desired. Adjust the size and position of the video based on its importance for monitoring.

Change video size

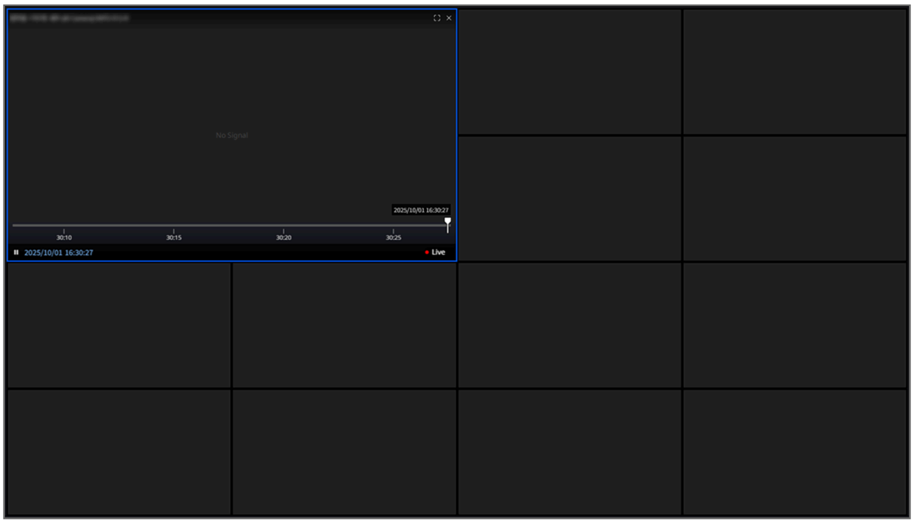
1. Click on the video whose size you want to change to activate the frame of the selected video.



2. Hover the mouse cursor over the edges of the frame to change the cursor shape to one that can resize.
3. Click on a corner and drag to the desired size.

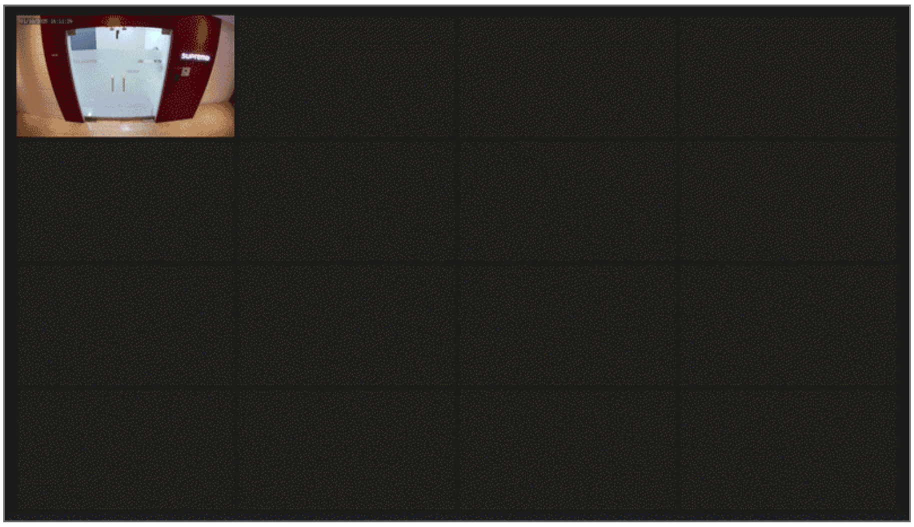


You can resize the video proportionally to the size of the placed tile. Conversely, you can also reduce the size of the video.



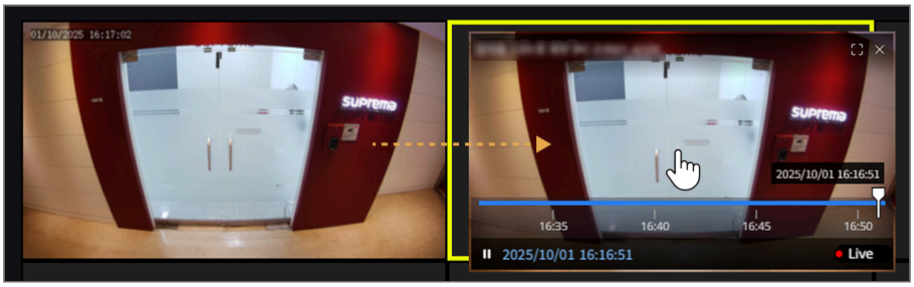
Enlarge video size

To enlarge the video to the entire size of the video tile, double-click on the video. The video will expand to the size of the video tile.

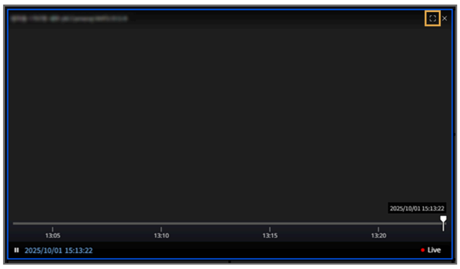


Change video location

Click on the video to move and drag it to the desired location. You can change the position of the selected video.



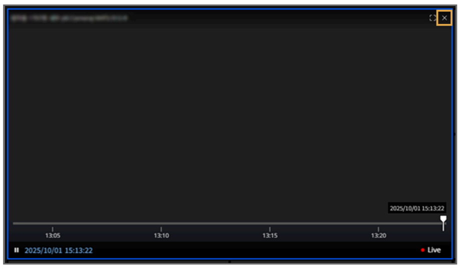
Full screen view



To view the video in full screen, click ⛶ at the upper right corner of the video.

To exit full screen, click the ⤡ button at the top right of the screen. Or press the ESC key on the keyboard.

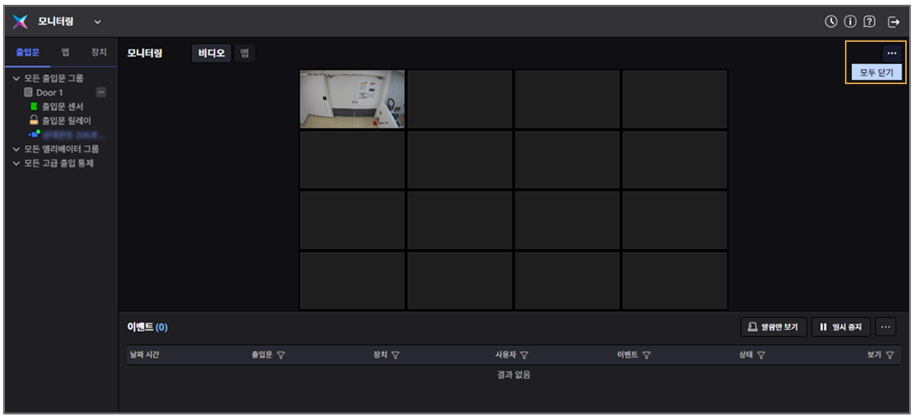
Close video



To close the video placed in the video tile, click ✕ at the upper right of the video.

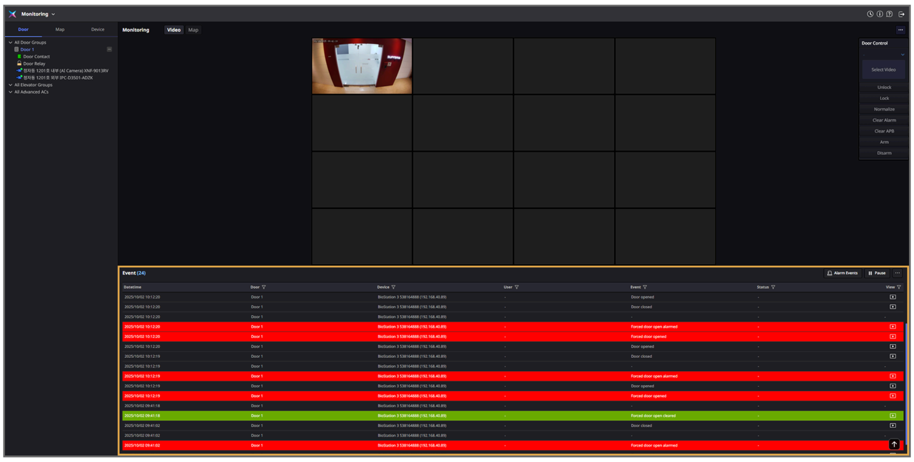
Close all videos

To close all videos placed in the video tile, click ⋯ at the upper right corner of the screen. Click **Close All** in the popup menu.



Monitor Event

In the **Event** section at the bottom of the monitoring page, you can check and manage real-time events. Efficient event management is possible through various features such as event status, alarm event handling, filtering, and color coding. Specifically, you can monitor events related to doors, devices, and users in real time and take prompt actions as needed.

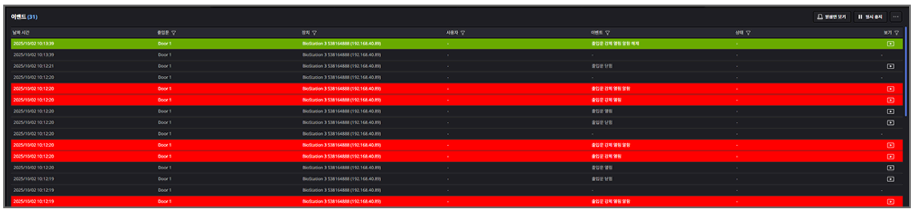


Event (24)

Datetime	Door	Device	User	Event	Status	View
2025/10/02 10:12:20	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Door opened	-	▶
2025/10/02 10:12:20	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Door closed	-	▶
2025/10/02 10:12:20	Door 1	BioStation 3 538164888 (192.168.40.89)	-	-	-	-
2025/10/02 10:12:20	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Forced door open alarmed	-	▶
2025/10/02 10:12:20	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Forced door opened	-	▶
2025/10/02 10:12:20	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Door opened	-	▶
2025/10/02 10:12:19	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Door closed	-	▶
2025/10/02 10:12:19	Door 1	BioStation 3 538164888 (192.168.40.89)	-	-	-	-
2025/10/02 10:12:19	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Forced door open alarmed	-	▶
2025/10/02 10:12:19	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Door opened	-	▶
2025/10/02 10:12:19	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Forced door opened	-	▶
2025/10/02 09:41:18	Door 1	BioStation 3 538164888 (192.168.40.89)	-	-	-	-
2025/10/02 09:41:18	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Forced door open cleared	-	▶
2025/10/02 09:41:02	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Door closed	-	▶
2025/10/02 09:41:02	Door 1	BioStation 3 538164888 (192.168.40.89)	-	-	-	-
2025/10/02 09:41:02	Door 1	BioStation 3 538164888 (192.168.40.89)	-	Forced door open alarmed	-	

Checking the event list

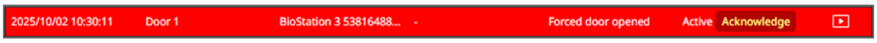
In the **Event** section, you can view events as they occur in real time. Each event includes the following information:



이벤트 (31)

날짜 시간	출입문	장치	사용자	이벤트	상태	보기
2025/10/02 10:13:39	Door 1	BioStation 3 538164888 (192.168.40.89)	-	출입문 강제 열림 알람 해제	-	▶
2025/10/02 10:13:39	Door 1	BioStation 3 538164888 (192.168.40.89)	-	-	-	-
2025/10/02 10:12:21	Door 1	BioStation 3 538164888 (192.168.40.89)	-	출입문 닫힘	-	▶
2025/10/02 10:12:20	Door 1	BioStation 3 538164888 (192.168.40.89)	-	-	-	-
2025/10/02 10:12:20	Door 1	BioStation 3 538164888 (192.168.40.89)	-	출입문 강제 열림 알람	-	▶
2025/10/02 10:12:20	Door 1	BioStation 3 538164888 (192.168.40.89)	-	출입문 강제 열림	-	▶
2025/10/02 10:12:20	Door 1	BioStation 3 538164888 (192.168.40.89)	-	출입문 열림	-	▶
2025/10/02 10:12:20	Door 1	BioStation 3 538164888 (192.168.40.89)	-	출입문 닫힘	-	▶
2025/10/02 10:12:20	Door 1	BioStation 3 538164888 (192.168.40.89)	-	-	-	-
2025/10/02 10:12:20	Door 1	BioStation 3 538164888 (192.168.40.89)	-	출입문 강제 열림 알람	-	▶
2025/10/02 10:12:20	Door 1	BioStation 3 538164888 (192.168.40.89)	-	출입문 강제 열림	-	▶
2025/10/02 10:12:20	Door 1	BioStation 3 538164888 (192.168.40.89)	-	출입문 열림	-	▶
2025/10/02 10:12:19	Door 1	BioStation 3 538164888 (192.168.40.89)	-	출입문 닫힘	-	▶
2025/10/02 10:12:19	Door 1	BioStation 3 538164888 (192.168.40.89)	-	-	-	-
2025/10/02 10:12:19	Door 1	BioStation 3 538164888 (192.168.40.89)	-	출입문 강제 열림 알람	-	▶

- **Datetime**: The date and time the event occurred.
- **Door**: The door where the event occurred.
- **Device**: The device on which the event occurred.
- **User**: The user who triggered the event.
- **Event**: Detailed information about the event.
- **Status**: The event status. Active events are displayed as **Active**. Alarm events have a **Acknowledge** button displayed. Click **Acknowledge** to resolve the event.



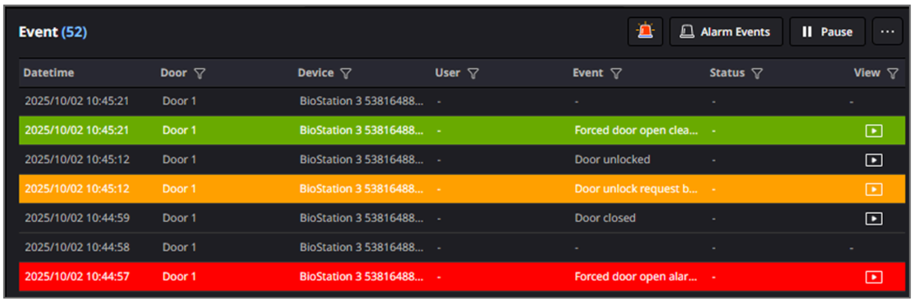
2025/10/02 10:30:11 Door 1 BioStation 3 53816488... - Forced door opened Active Acknowledge ▶

- **View**: If the event includes video information from the camera connected to the door, a video icon (▶) is displayed. Clicking this icon lets you view the video.

> ⓘ **INFO**
>
> - Clicking on an individual event will display detailed information on the right side of the screen. This detailed information includes the time of the event, area, door, device, user group, user, port, and event details.
> - If the event includes video or image information from a camera connected to the door, you can also view video and image logs.

Distinguishing events by color

Events in the event list can be distinguished by color:



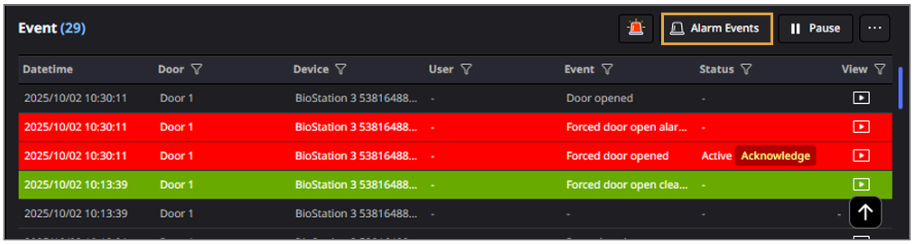
Event (52)

Datetime	Door	Device	User	Event	Status	View
2025/10/02 10:45:21	Door 1	BioStation 3 53816488...	-	-	-	-
2025/10/02 10:45:21	Door 1	BioStation 3 53816488...	-	Forced door open clea...	-	▶
2025/10/02 10:45:12	Door 1	BioStation 3 53816488...	-	Door unlocked	-	▶
2025/10/02 10:45:12	Door 1	BioStation 3 53816488...	-	Door unlock request b...	-	▶
2025/10/02 10:44:59	Door 1	BioStation 3 53816488...	-	Door closed	-	▶
2025/10/02 10:44:58	Door 1	BioStation 3 53816488...	-	-	-	-
2025/10/02 10:44:57	Door 1	BioStation 3 53816488...	-	Forced door open alar...	-	▶

- **No Color**: Normal event.
- **Orange**: Caution event. This indicates events that need attention, such as unauthorized access attempts in restricted areas or doors being left open.
- **Red**: Alarm event. This indicates a warning event requiring action within the system.
- **Green**: Resolved alarm event.

Checking alarm events

Only alarm events can be viewed in the **Event** section. Click the **Alarm Events** button in the upper right corner of the **Event** section. The event list will display only alarm events, which are indicated in red. Alarm events are displayed in red.



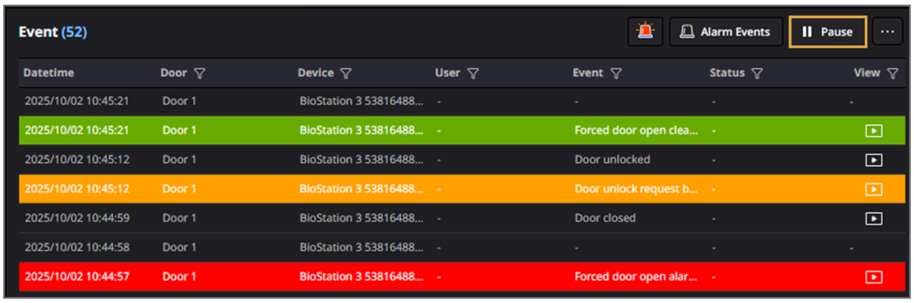
Event (29)

Datetime	Door	Device	User	Event	Status	View
2025/10/02 10:30:11	Door 1	BioStation 3 53816488...	-	Door opened	-	▶
2025/10/02 10:30:11	Door 1	BioStation 3 53816488...	-	Forced door open alar...	-	▶
2025/10/02 10:30:11	Door 1	BioStation 3 53816488...	-	Forced door opened	Active Acknowledge	▶
2025/10/02 10:13:39	Door 1	BioStation 3 53816488...	-	Forced door open clea...	-	▶
2025/10/02 10:13:39	Door 1	BioStation 3 53816488...	-	-	-	-

> ⓘ **INFO**
>
> To view all events, click the **All Events** button in the upper right corner of the **Event** section.

Real-time events

The event list in the **Event** section allows you to check events as they occur in real time. To stop real-time events, click ⏸ **Pause** in the upper right corner of the **Event** section. Click ▶ **Play** to resume real-time events.



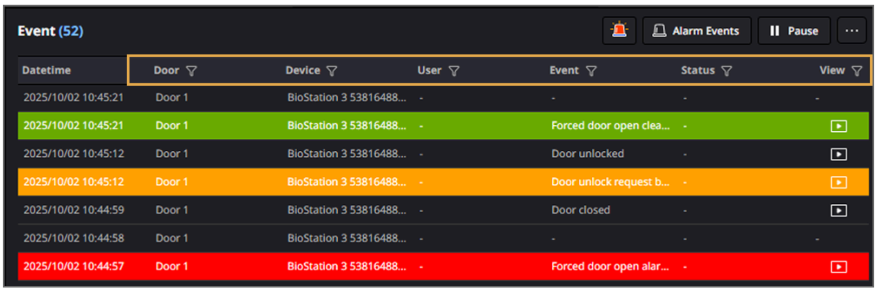
Datetime	Door	Device	User	Event	Status	View
2025/10/02 10:45:21	Door 1	BioStation 3 53816488...	-	-	-	-
2025/10/02 10:45:21	Door 1	BioStation 3 53816488...	-	Forced door open clea...	-	▶
2025/10/02 10:45:12	Door 1	BioStation 3 53816488...	-	Door unlocked	-	▶
2025/10/02 10:45:12	Door 1	BioStation 3 53816488...	-	Door unlock request b...	-	▶
2025/10/02 10:44:59	Door 1	BioStation 3 53816488...	-	Door closed	-	▶
2025/10/02 10:44:58	Door 1	BioStation 3 53816488...	-	-	-	-
2025/10/02 10:44:57	Door 1	BioStation 3 53816488...	-	Forced door open alar...	-	▶

Filtering events

Applying filters

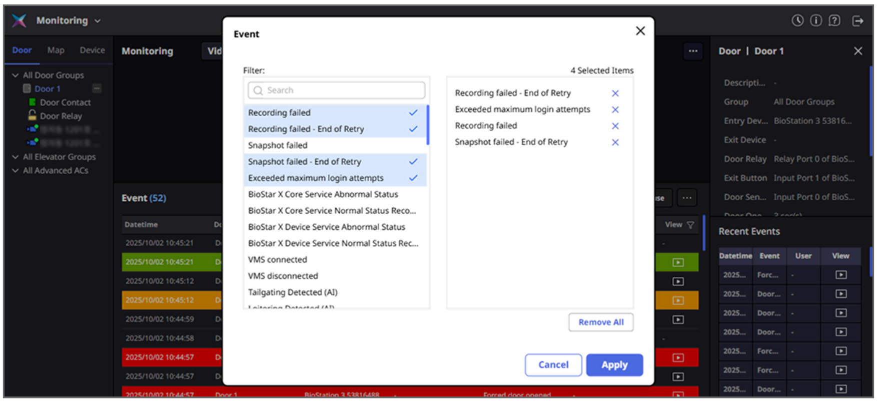
Users can filter the event list according to their desired criteria, allowing for quick identification of relevant events. This allows you to quickly check events based on the desired conditions.

1. Click ▽ on each header column in the **Event** section.



Datetime	Door	Device	User	Event	Status	View
2025/10/02 10:45:21	Door 1	BioStation 3 53816488...	-	-	-	-
2025/10/02 10:45:21	Door 1	BioStation 3 53816488...	-	Forced door open clea...	-	▶
2025/10/02 10:45:12	Door 1	BioStation 3 53816488...	-	Door unlocked	-	▶
2025/10/02 10:45:12	Door 1	BioStation 3 53816488...	-	Door unlock request b...	-	▶
2025/10/02 10:44:59	Door 1	BioStation 3 53816488...	-	Door closed	-	▶
2025/10/02 10:44:58	Door 1	BioStation 3 53816488...	-	-	-	-
2025/10/02 10:44:57	Door 1	BioStation 3 53816488...	-	Forced door open alar...	-	▶

2. When the filter window appears, select the desired item from the left list.



Event

Filter:

Search

- Recording failed ✓
- Recording failed - End of Retry ✓
- Snapshot failed
- Snapshot failed - End of Retry ✓
- Exceeded maximum login attempts ✓
- BioStar X Core Service Abnormal Status
- BioStar X Core Service Normal Status Reco...
- BioStar X Device Service Abnormal Status
- BioStar X Device Service Normal Status Rec...
- VMS connected
- VMS disconnected
- Tailgating Detected (AI)
- Loitering Detected (AI)

4 Selected Items

- Recording failed - End of Retry ✕
- Exceeded maximum login attempts ✕
- Recording failed ✕
- Snapshot failed - End of Retry ✕

Remove All

Cancel Apply

To deselect an item, click ✕. To clear all items, click **Remove All**.

3. Once all settings are complete, click **Apply**.

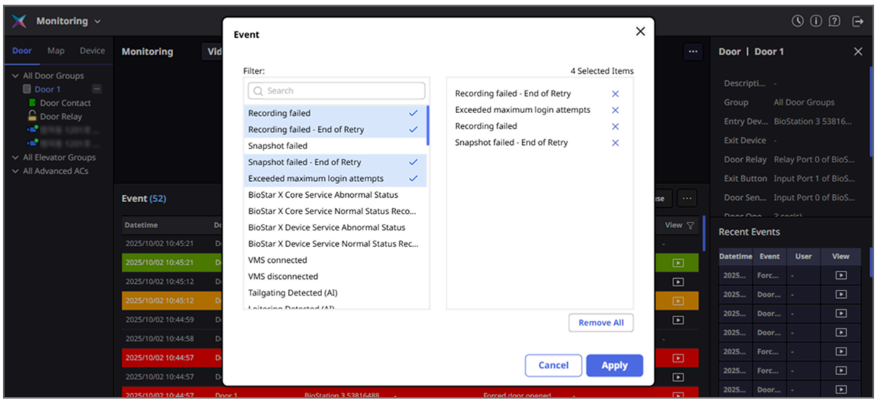
Only events that meet the set conditions will be displayed in the event list.

> **INFO**
>
> - You can also quickly search for desired items using the search input field in the filter window.
> - Multiple conditions can be set for each header column, applying an `AND` condition if more than one condition is specified. When setting more than one condition, apply the `AND` condition.
> - The items that can be filtered may vary by header column.
> - When filtering conditions are applied, the ▽ icon color in the header column changes to blue.

Removing filters

You can clear the applied filter conditions.

1. Click ▽ on the header column where filters were applied in the **Event** section.
2. When the filter window appears, click ✕ next to the item you wish to remove from the right list. To clear all filters, click **Remove All**.


Monitoring
Door
Map
Device
Monitoring
All Door Groups
Door 1
Door Contact
Door Relay
All Elevator Groups
All Advanced ACs
Event (52)
Datetime
Event
Filter:
4 Selected Items
Search
Recording failed ✓
Recording failed - End of Retry ✓
Snapshot failed
Snapshot failed - End of Retry ✓
Exceeded maximum login attempts ✓
BioStar X Core Service Abnormal Status
BioStar X Core Service Normal Status Reco...
BioStar X Device Service Abnormal Status
BioStar X Device Service Normal Status Rec...
VMS connected
VMS disconnected
Tailgating Detected (AI)
Recording failed - End of Retry ✕
Exceeded maximum login attempts ✕
Recording failed ✕
Snapshot failed - End of Retry ✕
Remove All
Cancel
Apply
Door | Door 1
Descripti... -
Group All Door Groups
Entry Dev... BioStation 3 53816...
Exit Device -
Door Relay Relay Port 0 of BioS...
Exit Button Input Port 1 of BioS...
Door Sen... Input Port 0 of BioS...
Recent Events
Datetime
Event
User
View

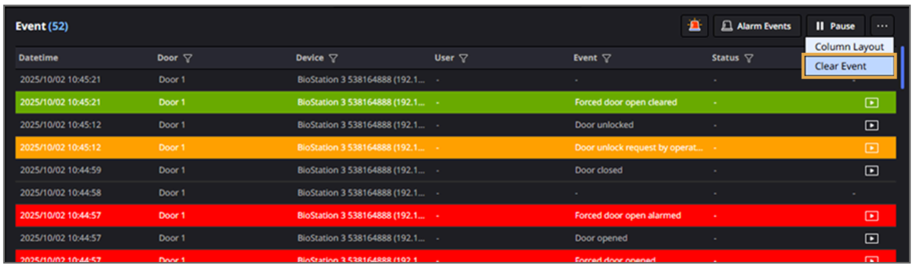
3. Once all conditions to be cleared are set, click **Apply**.

> **INFO**
>
> - You can also quickly search for desired items using the search input field in the filter window.
> - When filtering conditions are cleared, the icon color in the header column will revert to its original state.

Clearing the event list

In the **Event** section, you can clear events. Click ··· in the upper right corner of the **Event** section and select **Clear Event** from the popup menu. If there are many unnecessary events accumulated in the event list, you can use the

Clear Event feature to clean up.

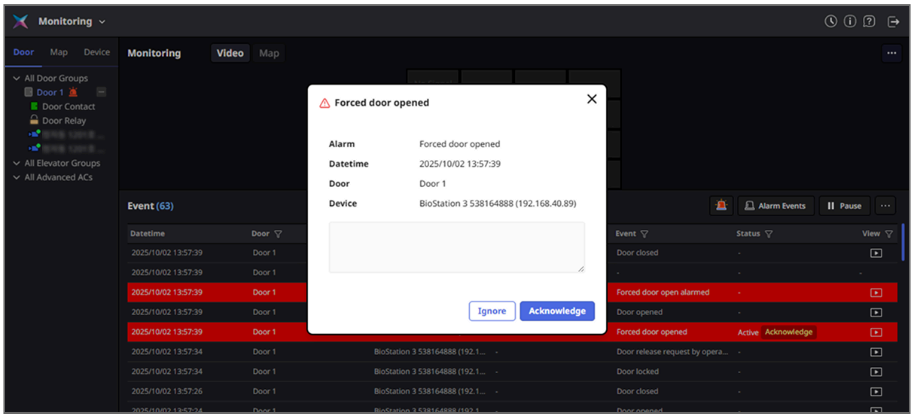


Event (52)

Datetime	Door	Device	User	Event	Status
2025/10/02 10:45:21	Door 1	BioStation 3 538164888 (192.1...	-	-	-
2025/10/02 10:45:21	Door 1	BioStation 3 538164888 (192.1...	-	Forced door open cleared	-
2025/10/02 10:45:12	Door 1	BioStation 3 538164888 (192.1...	-	Door unlocked	-
2025/10/02 10:45:12	Door 1	BioStation 3 538164888 (192.1...	-	Door unlock request by operat...	-
2025/10/02 10:44:59	Door 1	BioStation 3 538164888 (192.1...	-	Door closed	-
2025/10/02 10:44:58	Door 1	BioStation 3 538164888 (192.1...	-	-	-
2025/10/02 10:44:57	Door 1	BioStation 3 538164888 (192.1...	-	Forced door open alarmed	-
2025/10/02 10:44:57	Door 1	BioStation 3 538164888 (192.1...	-	Door opened	-
2025/10/02 10:44:57	Door 1	BioStation 3 538164888 (192.1	-	Forced door opened	-

Check alarm and record action

When an alarm event, such as forced opening of the door, occurs, an alarm message window appears. The alarm message window includes detailed information about the triggered alarm event. At this time, the administrator can record their acknowledgement of the triggered alarm event and any actions taken.



Forced door opened

Alarm	Forced door opened
Datetime	2025/10/02 13:57:39
Door	Door 1
Device	BioStation 3 538164888 (192.168.40.89)

Event (63)

Datetime	Door			Event	Status	View
2025/10/02 13:57:39	Door 1			Door closed	-	
2025/10/02 13:57:39	Door 1			-	-	-
2025/10/02 13:57:39	Door 1			Forced door open alarmed	-	
2025/10/02 13:57:39	Door 1			Door opened	-	
2025/10/02 13:57:39	Door 1			Forced door opened	Active Acknowledge	
2025/10/02 13:57:34	Door 1	BioStation 3 538164888 (192.1...	-	Door release request by opera...	-	
2025/10/02 13:57:34	Door 1	BioStation 3 538164888 (192.1...	-	Door locked	-	
2025/10/02 13:57:26	Door 1	BioStation 3 538164888 (192.1...	-	Door closed	-	
2025/10/02 13:57:24	Door 1	BioStation 3 538164888 (192.1	-	Door opened	-	

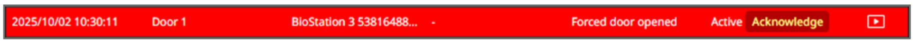
> **INFO**
>
> The Ignore All button is displayed only when two or more alarm events occur.

Record action for alarm event

Enter actions regarding the alarm event in the message input field. You can enter up to 500 characters. Enter actions and click the Acknowledge button. Records acknowledgement and actions regarding the alarm event. The alarm message window will close.

Pending acknowledgment of alarm event

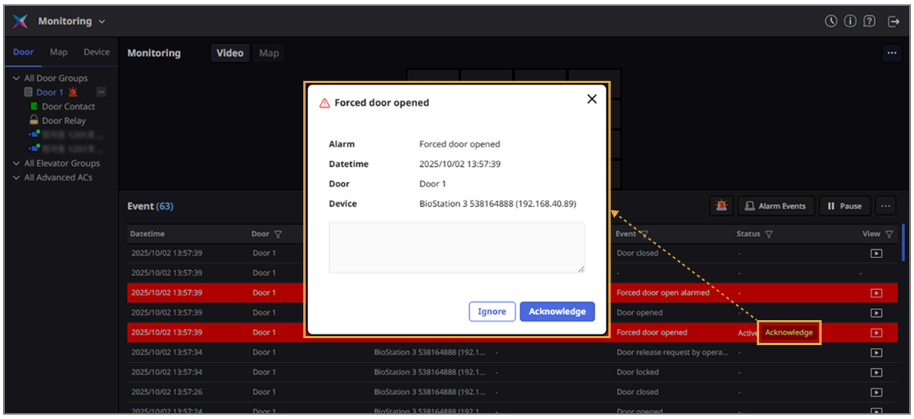
You can also defer acknowledgement of the alarm event by clicking the Ignore button. Actions taken can be recorded. The alarm message window will close. Deferred alarm events are displayed in the event list as Active status, and the Acknowledge button can be used.



2025/10/02 10:30:11	Door 1	BioStation 3 53816488...	-	Forced door opened	Active Acknowledge

Checking alarm events in the event list

Clicking the **Acknowledge** button displayed in the **Status** column of the event list allows recording of the acknowledgement and actions regarding the triggered alarm events. Complete your entry and click the **Acknowledge** button.



Forced door opened

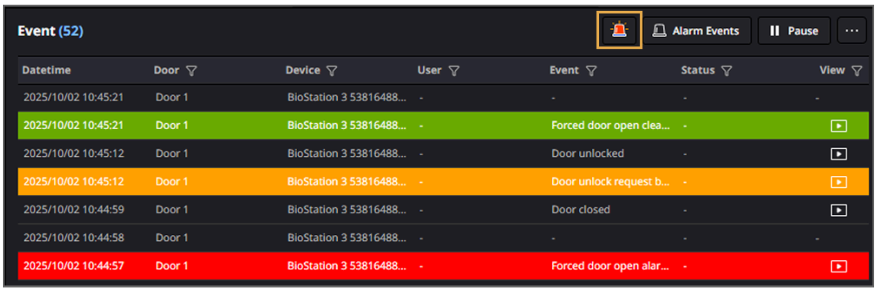
Alarm	Forced door opened
Datetime	2025/10/02 13:57:39
Door	Door 1
Device	BioStation 3 538164888 (192.168.40.89)

Datetime	Door			Event	Status	View
2025/10/02 13:57:39	Door 1			Door closed	-	▶
2025/10/02 13:57:39	Door 1			-	-	-
2025/10/02 13:57:39	Door 1			Forced door open alarmed	-	▶
2025/10/02 13:57:39	Door 1			Door opened	-	▶
2025/10/02 13:57:39	Door 1			Forced door opened	Active Acknowledge	▶
2025/10/02 13:57:34	Door 1	BioStation 3 538164888 (192.1...	-	Door release request by opera...	-	▶
2025/10/02 13:57:34	Door 1	BioStation 3 538164888 (192.1...	-	Door locked	-	▶
2025/10/02 13:57:26	Door 1	BioStation 3 538164888 (192.1...	-	Door closed	-	▶
2025/10/02 13:57:24	Door 1	BioStation 3 538164888 (192.1...	-	Door opened	-	▶

Viewing unacknowledged alarm events

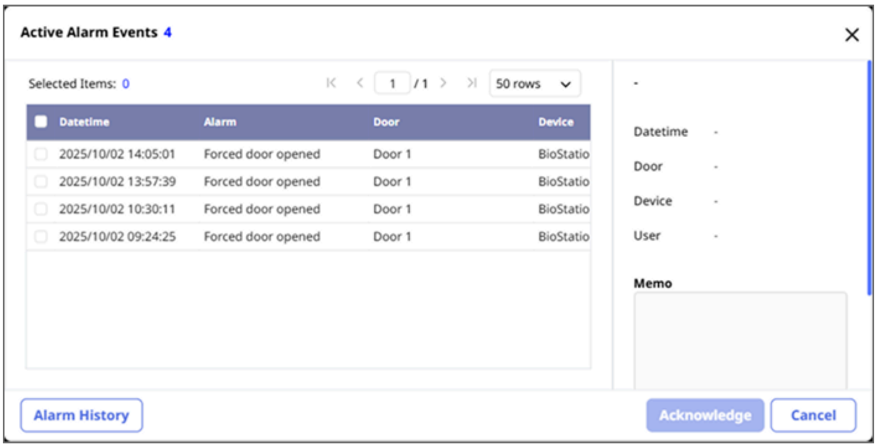
This feature allows you to view unacknowledged alarm events at once and record actions taken. It is especially useful when multiple identical alarm events occur.

1. Click the 🚨 button in the upper right corner of the **Event** section.



Datetime	Door	Device	User	Event	Status	View
2025/10/02 10:45:21	Door 1	BioStation 3 53816488...	-	-	-	-
2025/10/02 10:45:21	Door 1	BioStation 3 53816488...	-	Forced door open clea...	-	▶
2025/10/02 10:45:12	Door 1	BioStation 3 53816488...	-	Door unlocked	-	▶
2025/10/02 10:45:12	Door 1	BioStation 3 53816488...	-	Door unlock request b...	-	▶
2025/10/02 10:44:59	Door 1	BioStation 3 53816488...	-	Door closed	-	▶
2025/10/02 10:44:58	Door 1	BioStation 3 53816488...	-	-	-	-
2025/10/02 10:44:57	Door 1	BioStation 3 53816488...	-	Forced door open alar...	-	▶

2. When the **Active Alarm Events** window appears, select the alarm event to record actions from the left list. To select all events, click the checkbox on the far left of the header column.



□ Datetime	Alarm	Door	Device
□ 2025/10/02 14:05:01	Forced door opened	Door 1	BioStatio
□ 2025/10/02 13:57:39	Forced door opened	Door 1	BioStatio
□ 2025/10/02 10:30:11	Forced door opened	Door 1	BioStatio
□ 2025/10/02 09:24:25	Forced door opened	Door 1	BioStatio

Datetime	-
Door	-
Device	-
User	-

3. Enter actions regarding the alarm event in the **Memo** input field.
4. Click **Acknowledge**.

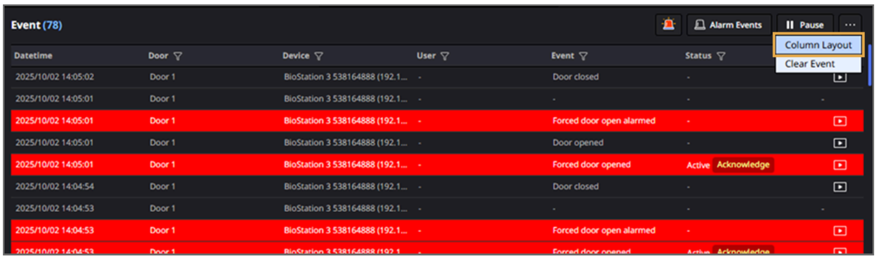
Click **Acknowledge** for the alarm event. A popup window will appear where you can enter your acknowledgement of the alarm event and any actions taken.

> **INFO**
>
> You must select more than one event from the alarm event list for the **Acknowledge** button to be activated.

Event list column settings

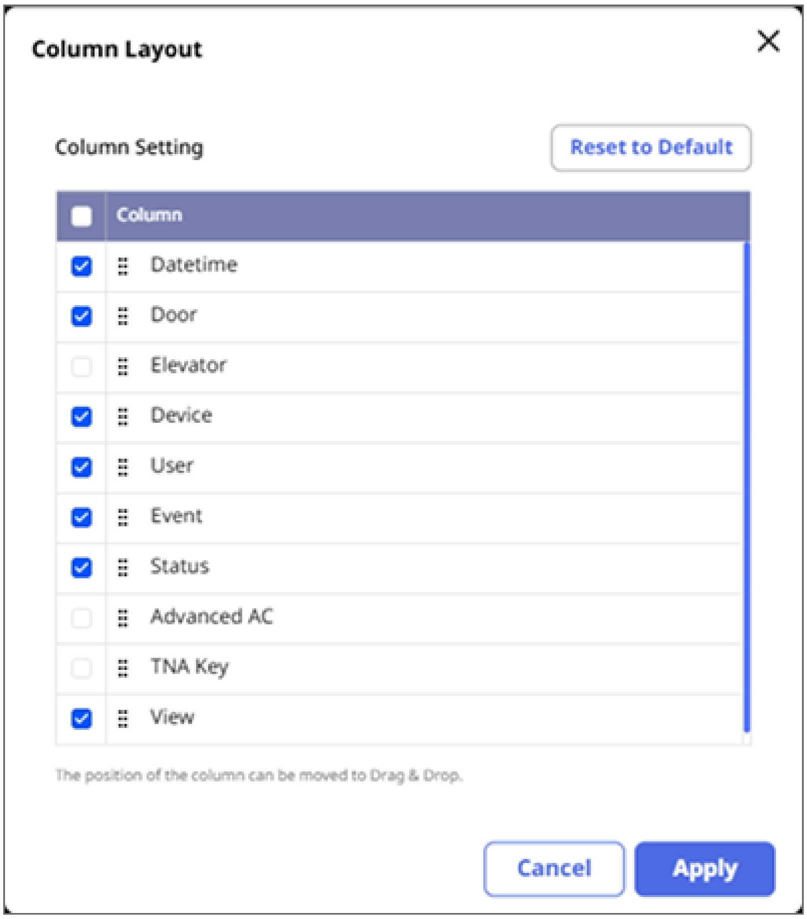
You can add columns to display in the event list, rearrange them, and set them to hidden.

1. Click ••• → **Column Layout** at the upper right of the **Event** section.



Datetime	Door	Device	User	Event	Status	
2025/10/02 14:05:02	Door 1	BioStation 3 538164888 (192.1...	-	Door closed	-	▶
2025/10/02 14:05:01	Door 1	BioStation 3 538164888 (192.1...	-	-	-	-
2025/10/02 14:05:01	Door 1	BioStation 3 538164888 (192.1...	-	Forced door open alarmed	-	▶
2025/10/02 14:05:01	Door 1	BioStation 3 538164888 (192.1...	-	Door opened	-	▶
2025/10/02 14:05:01	Door 1	BioStation 3 538164888 (192.1...	-	Forced door opened	Active Acknowledge	▶
2025/10/02 14:04:54	Door 1	BioStation 3 538164888 (192.1...	-	Door closed	-	▶
2025/10/02 14:04:53	Door 1	BioStation 3 538164888 (192.1...	-	-	-	-
2025/10/02 14:04:53	Door 1	BioStation 3 538164888 (192.1...	-	Forced door open alarmed	-	▶
2025/10/02 14:04:53	Door 1	BioStation 3 538164888 (192.1...	-	Forced door opened	Active Acknowledge	▶

2. When the **Column Layout** window appears, you can click the checkboxes of the columns to display them or set them as hidden. You can also change the order of columns via drag and drop.



Column Layout

Column Setting

☐	Column
☑	Datetime
☑	Door
☐	Elevator
☑	Device
☑	User
☑	Event
☑	Status
☐	Advanced AC
☐	TNA Key
☑	View

The position of the column can be moved to Drag & Drop.

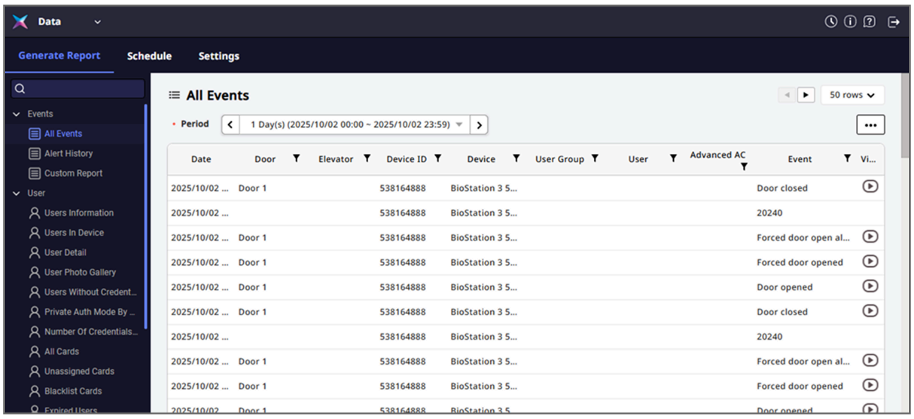
3. After making all changes to column settings, click the **Apply** button.

> **INFO**
>
> To initialize the column settings, click the **Default Column** button.

Data

Using the **Data** menu, you can query user information registered in **BioStar X** or events that meet specific criteria, and generate reports on a regular schedule. You can automatically generate the desired report on a regular schedule if needed, and the generated report can be exported as CSV or PDF files or printed.

Click **Data** or select **Data** from the shortcut list at the top left of the screen on the **Launcher** page.



Date	Door	Elevator	Device ID	Device	User Group	User	Advanced AC	Event	Vi...
2025/10/02 ...	Door 1		538164888	BioStation 3 5...				Door closed	▶
2025/10/02 ...			538164888	BioStation 3 5...				20240	
2025/10/02 ...	Door 1		538164888	BioStation 3 5...				Forced door open al...	▶
2025/10/02 ...	Door 1		538164888	BioStation 3 5...				Forced door opened	▶
2025/10/02 ...	Door 1		538164888	BioStation 3 5...				Door opened	▶
2025/10/02 ...	Door 1		538164888	BioStation 3 5...				Door closed	▶
2025/10/02 ...			538164888	BioStation 3 5...				20240	
2025/10/02 ...	Door 1		538164888	BioStation 3 5...				Forced door open al...	▶
2025/10/02 ...	Door 1		538164888	BioStation 3 5...				Forced door opened	▶
2025/10/02 ...	Door 1		538164888	BioStation 3 5...				Door opened	▶

Generate Report → Read more

Reports are created in the desired format.

Automatic Report Schedule → Read more

Set a schedule to automatically generate custom reports created by setting the DYNAMIC period.

Settings → Read more

Set the path where the report will be saved if you have set up an auto-generated schedule.

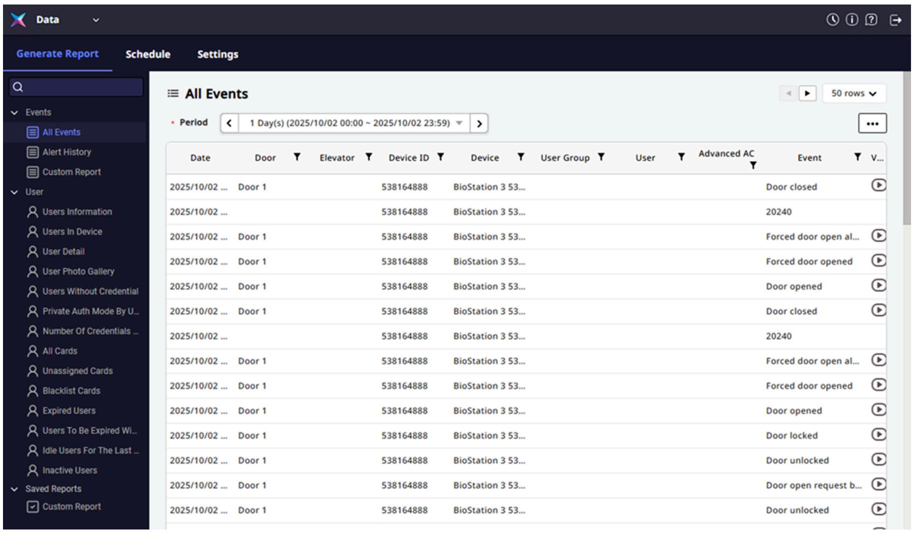
Generate Report

You can view all events that occurred in **BioStar X** or just the alarm history. You can filter and generate custom reports according to user-defined conditions.

Click **Data** or select **Data** from the shortcut list at the top left of the screen on the **Launcher** page.

View all events

You can view all events that occurred in **BioStar X**. Click **Events** → **All Events** on the left sidebar of the screen.

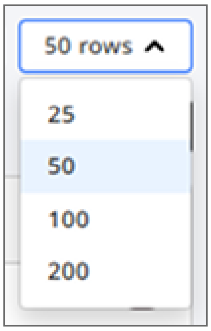


All Events

Period 1 Day(s) (2025/10/02 00:00 ~ 2025/10/02 23:59)

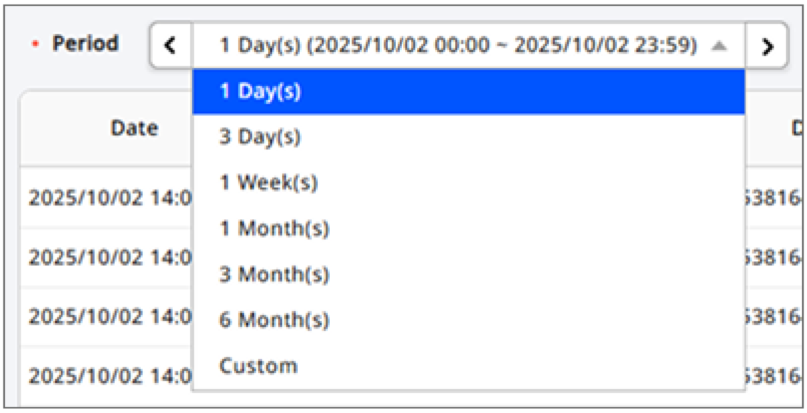
Date	Door	Elevator	Device ID	Device	User Group	User	Advanced AC	Event	V...
2025/10/02 ...	Door 1		538164888	BioStation 3 53...				Door closed	▶
2025/10/02 ...			538164888	BioStation 3 53...				20240	
2025/10/02 ...	Door 1		538164888	BioStation 3 53...				Forced door open al...	▶
2025/10/02 ...	Door 1		538164888	BioStation 3 53...				Forced door opened	▶
2025/10/02 ...	Door 1		538164888	BioStation 3 53...				Door opened	▶
2025/10/02 ...	Door 1		538164888	BioStation 3 53...				Door closed	▶
2025/10/02 ...			538164888	BioStation 3 53...				20240	
2025/10/02 ...	Door 1		538164888	BioStation 3 53...				Forced door open al...	▶
2025/10/02 ...	Door 1		538164888	BioStation 3 53...				Forced door opened	▶
2025/10/02 ...	Door 1		538164888	BioStation 3 53...				Door opened	▶
2025/10/02 ...	Door 1		538164888	BioStation 3 53...				Door locked	▶
2025/10/02 ...	Door 1		538164888	BioStation 3 53...				Door unlocked	▶
2025/10/02 ...	Door 1		538164888	BioStation 3 53...				Door open request b...	▶
2025/10/02 ...	Door 1		538164888	BioStation 3 53...				Door unlocked	▶

- To check the previous or next page from the listed results, click ◀ or ▶ at the top right of the screen.
- To change the number of rows displayed in the list, click the dropdown menu at the top right of the screen and select your desired value. You can select from a minimum of 25 rows to a maximum of 200 rows.



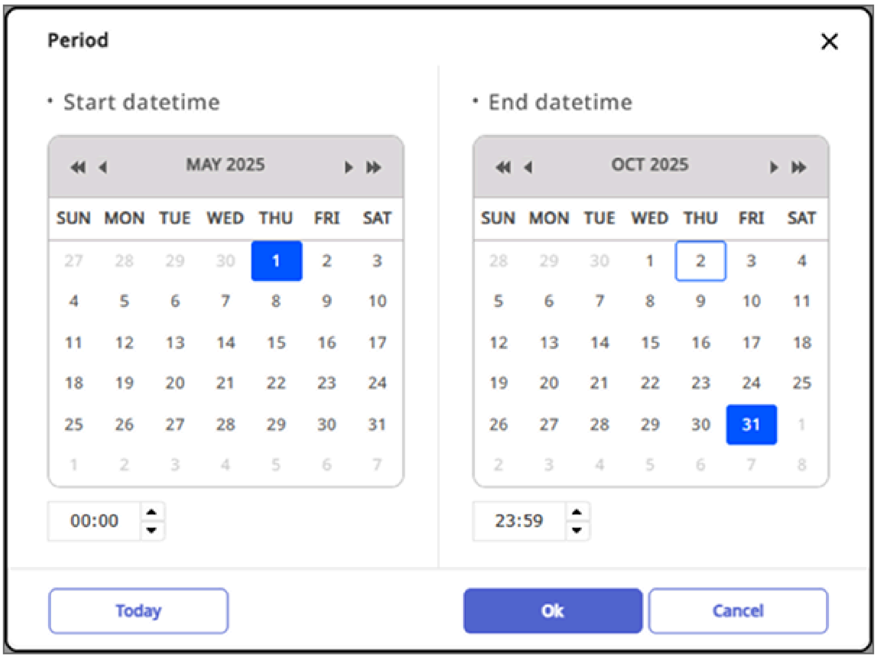
Set period

You can set the desired period in the **Period** option at the top left of the screen. Click the date area.



Period: 1 Day(s) (2025/10/02 00:00 ~ 2025/10/02 23:59)

- You can select predefined periods from today ranging from the 1st to 6 months. The events that occurred during the selected period will be automatically displayed in the list.
- By selecting **User Defined**, you can also manually set your desired period. When the period selection window appears, set the start date, end date, and time, then click **Ok**. The events that occurred during the set period will automatically appear in the list.



Period

Start datetime: MAY 2025, 1, 00:00

End datetime: OCT 2025, 31, 23:59

INFO

To select today's date, click **Today**.

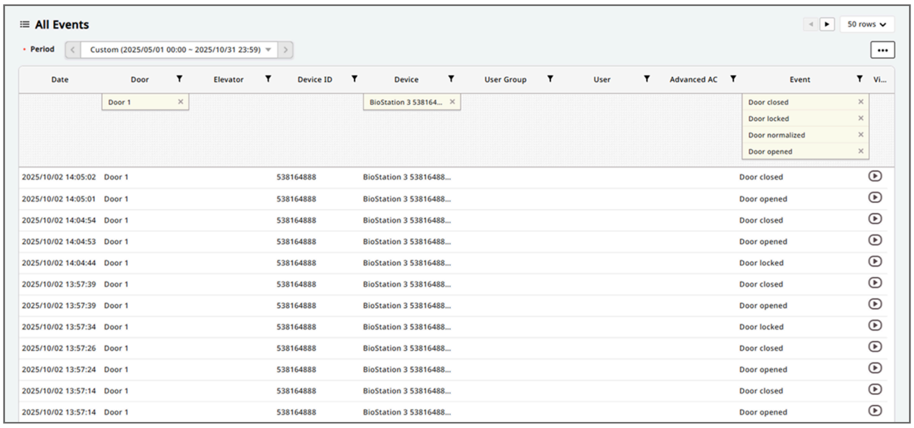
Set query conditions

You can filter the list by setting your desired conditions in the header section of the query list. You can set conditions for all items except for dates.

1. In the header section of the event list, click the ▼ button for the desired column.
2. When the filter condition window appears, select your desired items.

3. Once your selections are complete, click the **Add Condition** button.

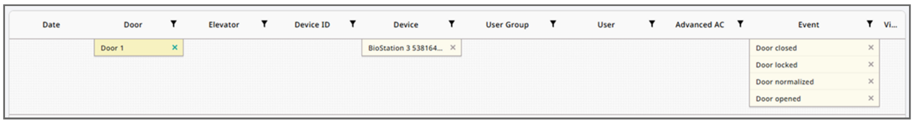
Only events matching the selected conditions will be displayed in the list.



Date	Door	Elevator	Device ID	Device	User Group	User	Advanced AC	Event	Vi...
	Door 1 ×			BioStation 3 538164... ×				Door closed × Door locked × Door normalized × Door opened ×	
2025/10/02 14:05:02	Door 1		538164888	BioStation 3 53816488...				Door closed	▶
2025/10/02 14:05:01	Door 1		538164888	BioStation 3 53816488...				Door opened	▶
2025/10/02 14:04:54	Door 1		538164888	BioStation 3 53816488...				Door closed	▶
2025/10/02 14:04:53	Door 1		538164888	BioStation 3 53816488...				Door opened	▶
2025/10/02 14:04:44	Door 1		538164888	BioStation 3 53816488...				Door locked	▶
2025/10/02 13:57:39	Door 1		538164888	BioStation 3 53816488...				Door closed	▶
2025/10/02 13:57:39	Door 1		538164888	BioStation 3 53816488...				Door opened	▶
2025/10/02 13:57:34	Door 1		538164888	BioStation 3 53816488...				Door locked	▶
2025/10/02 13:57:26	Door 1		538164888	BioStation 3 53816488...				Door closed	▶
2025/10/02 13:57:24	Door 1		538164888	BioStation 3 53816488...				Door opened	▶
2025/10/02 13:57:14	Door 1		538164888	BioStation 3 53816488...				Door closed	▶
2025/10/02 13:57:14	Door 1		538164888	BioStation 3 53816488...				Door opened	▶

Clear query conditions

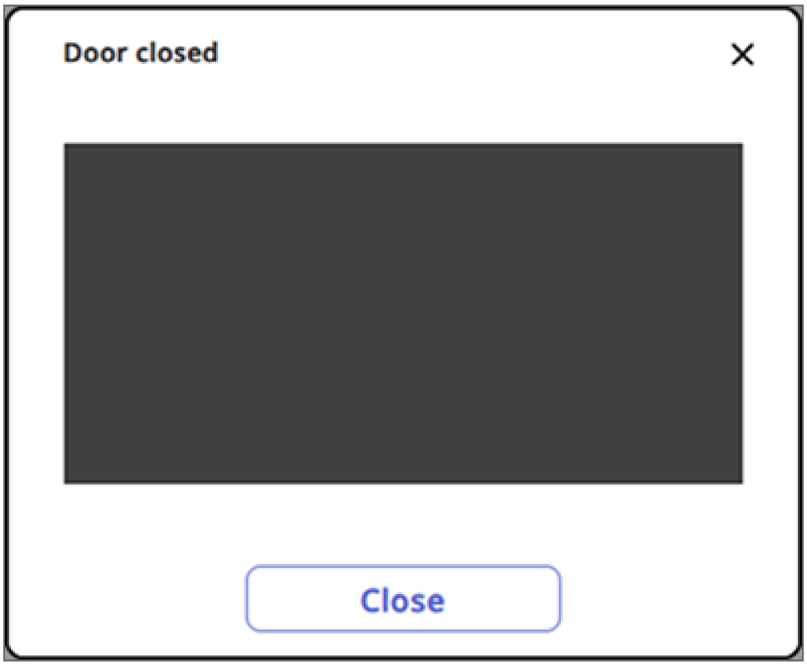
To clear the set query conditions, click the × button in the conditions set below the header section. The set conditions will be cleared, and all events will be displayed in the list again.



Date	Door	Elevator	Device ID	Device	User Group	User	Advanced AC	Event	Vi...
	Door 1 ×			BioStation 3 538164... ×				Door closed × Door locked × Door normalized × Door opened ×	

Check event video

If a camera is connected to a device where a specific event occurred in the event list, an **View** column will show the ▶ icon for that event. By clicking the icon, you can view the video at the time the event occurred through a pop-up window.



ⓘ **INFO**

- If you have connected more than one camera in the camera rule settings, it will play the video from the first camera. For more information about camera rule settings, refer to the following.
- This feature is available with additional options on the **Advanced** license or higher. For more information on licensing policy, refer to the following.
- For information on linking doors and cameras, refer to the following.

Export to CSV

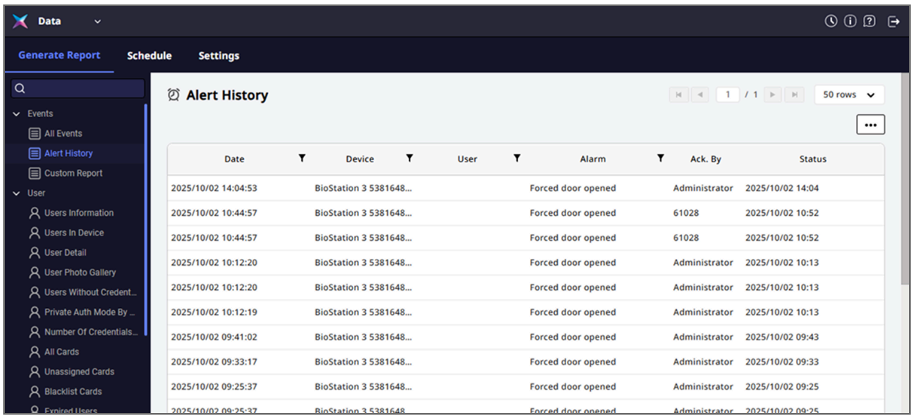
You can export the queried event list as a CSV file. Click ••• → **CSV Export** at the top right of the screen. You can download the CSV file to your PC.

ⓘ **INFO**

The name format of the CSV file is `Report_YYYYMMDD_hash.csv`. (For example, *Report_20251002_94a85b7519664378b4b39b879f1e81b7.csv*)

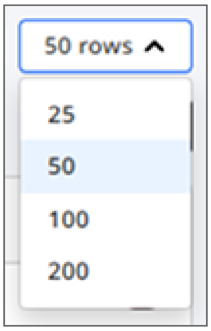
View alarm history

You can only view alarm (alert) history. Click **Events** → **Alert History** on the left sidebar of the screen.



Date	Device	User	Alarm	Ack. By	Status
2025/10/02 14:04:53	BioStation 3 5381648...		Forced door opened	Administrator	2025/10/02 14:04
2025/10/02 10:44:57	BioStation 3 5381648...		Forced door opened	61028	2025/10/02 10:52
2025/10/02 10:44:57	BioStation 3 5381648...		Forced door opened	61028	2025/10/02 10:52
2025/10/02 10:12:20	BioStation 3 5381648...		Forced door opened	Administrator	2025/10/02 10:13
2025/10/02 10:12:20	BioStation 3 5381648...		Forced door opened	Administrator	2025/10/02 10:13
2025/10/02 10:12:19	BioStation 3 5381648...		Forced door opened	Administrator	2025/10/02 10:13
2025/10/02 09:41:02	BioStation 3 5381648...		Forced door opened	Administrator	2025/10/02 09:43
2025/10/02 09:33:17	BioStation 3 5381648...		Forced door opened	Administrator	2025/10/02 09:33
2025/10/02 09:25:37	BioStation 3 5381648...		Forced door opened	Administrator	2025/10/02 09:25
2025/10/02 09:25:37	BioStation 3 5381648...		Forced door opened	Administrator	2025/10/02 09:25

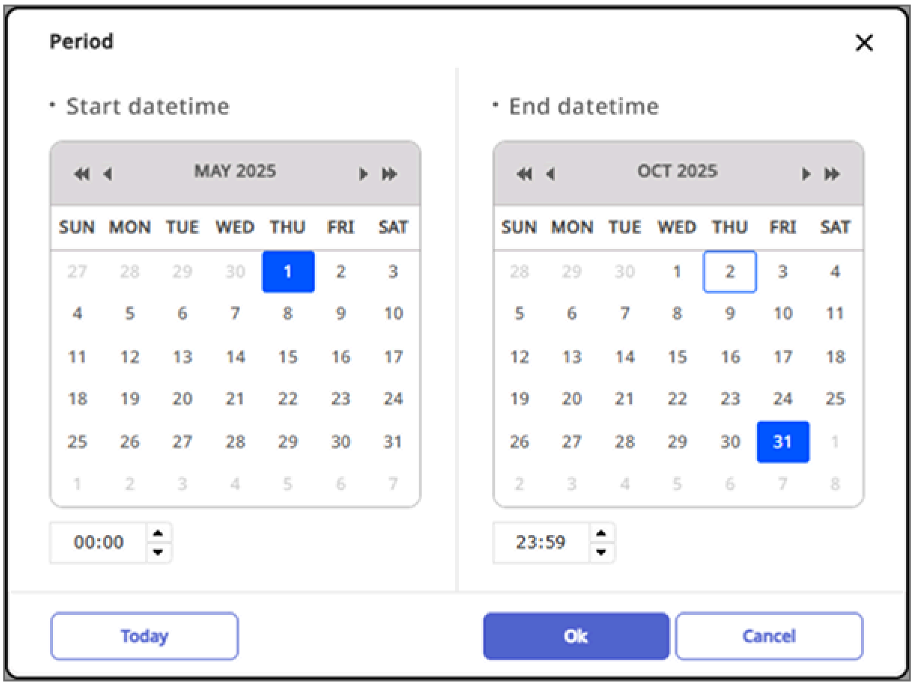
- To check the previous or next page from the listed results, click ◀ or ▶ at the top right of the screen.
- To go to the first or last page of the queried list, click ⏮ or ⏭ at the top right of the screen.
- To change the number of rows displayed in the list, click the dropdown menu at the top right of the screen and select your desired value. You can select from a minimum of 25 rows to a maximum of 200 rows.



> **INFO**
>
> For more information about checking alarm (alert) events in event monitoring, refer to the following.

Set period

You can set the desired period and query the alarm history that occurred during that period. In the **Date** column of the queried list, click the ▼ button. When the period selection window appears, set the start date, end date, and time, then click **Ok**. The events that occurred during the set period will automatically appear in the list.



Start datetime

MAY 2025

SUN	MON	TUE	WED	THU	FRI	SAT
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

00:00

End datetime

OCT 2025

SUN	MON	TUE	WED	THU	FRI	SAT
28	29	30	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

23:59

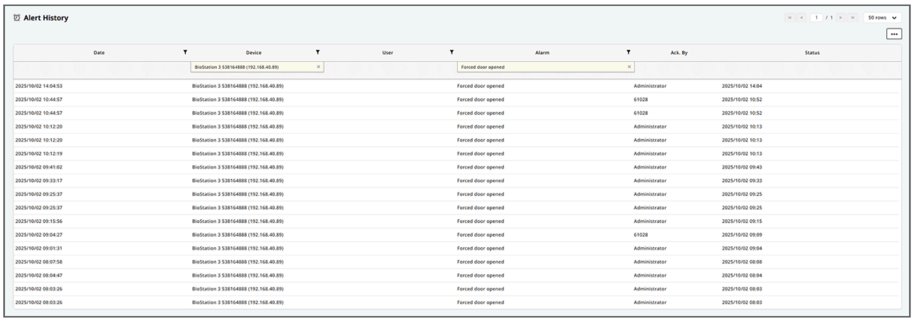
> **INFO**
>
> To select today's date, click **Today**.

Set query conditions

You can filter the list by setting your desired conditions in the header section of the query list. You can set conditions for all items except for dates.

1. In the header section of the event list, click the ▼ button for the desired column.
2. When the filter condition window appears, select your desired items.
3. Once your selections are complete, click the **Add Condition** button.

Only events matching the selected conditions will be displayed in the list.

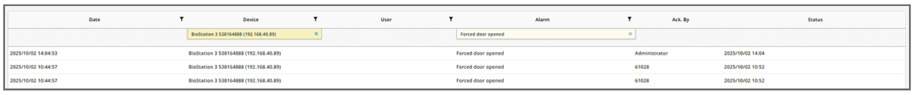


Alert History

Date	Device	User	Alarm	Ack. By	Status
	BioStation 3 538164888 (192.168.40.89)		Forced door opened		
2025/10/02 14:04:53	BioStation 3 538164888 (192.168.40.89)		Forced door opened	Administrator	2025/10/02 14:04
2025/10/02 10:44:57	BioStation 3 538164888 (192.168.40.89)		Forced door opened	61028	2025/10/02 10:52
2025/10/02 10:44:57	BioStation 3 538164888 (192.168.40.89)		Forced door opened	61028	2025/10/02 10:52
2025/10/02 10:12:20	BioStation 3 538164888 (192.168.40.89)		Forced door opened	Administrator	2025/10/02 10:13
2025/10/02 10:12:20	BioStation 3 538164888 (192.168.40.89)		Forced door opened	Administrator	2025/10/02 10:13
2025/10/02 10:12:19	BioStation 3 538164888 (192.168.40.89)		Forced door opened	Administrator	2025/10/02 10:13
2025/10/02 09:41:02	BioStation 3 538164888 (192.168.40.89)		Forced door opened	Administrator	2025/10/02 09:43
2025/10/02 09:33:17	BioStation 3 538164888 (192.168.40.89)		Forced door opened	Administrator	2025/10/02 09:33
2025/10/02 09:25:37	BioStation 3 538164888 (192.168.40.89)		Forced door opened	Administrator	2025/10/02 09:25
2025/10/02 09:25:37	BioStation 3 538164888 (192.168.40.89)		Forced door opened	Administrator	2025/10/02 09:25
2025/10/02 09:15:56	BioStation 3 538164888 (192.168.40.89)		Forced door opened	Administrator	2025/10/02 09:15
2025/10/02 09:04:27	BioStation 3 538164888 (192.168.40.89)		Forced door opened	61028	2025/10/02 09:09
2025/10/02 09:01:31	BioStation 3 538164888 (192.168.40.89)		Forced door opened	Administrator	2025/10/02 09:04
2025/10/02 08:07:58	BioStation 3 538164888 (192.168.40.89)		Forced door opened	Administrator	2025/10/02 08:08
2025/10/02 08:04:47	BioStation 3 538164888 (192.168.40.89)		Forced door opened	Administrator	2025/10/02 08:04
2025/10/02 08:03:26	BioStation 3 538164888 (192.168.40.89)		Forced door opened	Administrator	2025/10/02 08:03
2025/10/02 08:03:26	BioStation 3 538164888 (192.168.40.89)		Forced door opened	Administrator	2025/10/02 08:03

Clear query conditions

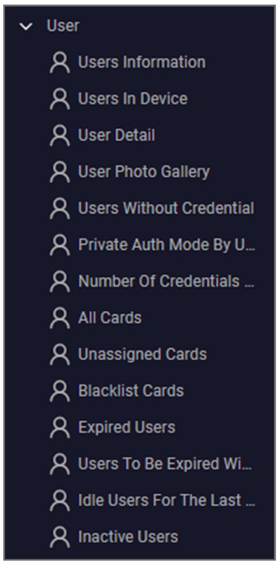
To clear the set query conditions, click the ✕ button in the conditions set below the header section. The set conditions will be cleared, and all events will be displayed in the list again.



Date	Device	User	Alarm	Ack. By	Status
	BioStation 3 538164888 (192.168.40.89)		Forced door opened		
2025/10/02 14:04:53	BioStation 3 538164888 (192.168.40.89)		Forced door opened	Administrator	2025/10/02 14:04
2025/10/02 10:44:57	BioStation 3 538164888 (192.168.40.89)		Forced door opened	61028	2025/10/02 10:52
2025/10/02 10:44:57	BioStation 3 538164888 (192.168.40.89)		Forced door opened	61028	2025/10/02 10:52

User report query

You can select user-related templates to generate reports. In the left sidebar of the screen, click the desired template under **User**.



- **Users Information**: You can view detailed user information in a list format.
- **Users In Device**: You can view information of users registered to the device.
- **User Detail**: You can view detailed user information in a card format.
- **User Photo Gallery**: You can view user profile pictures in a gallery format.
- **Users Without Credential**: You can view users who have not set credentials.
- **Private Auth Mode By User**: You can view user-specific private authentication mode settings.
- **Number Of Credentials By User**: You can view the number of credentials set for the user.
- **All Cards**: You can view users based on enrolled

cards.

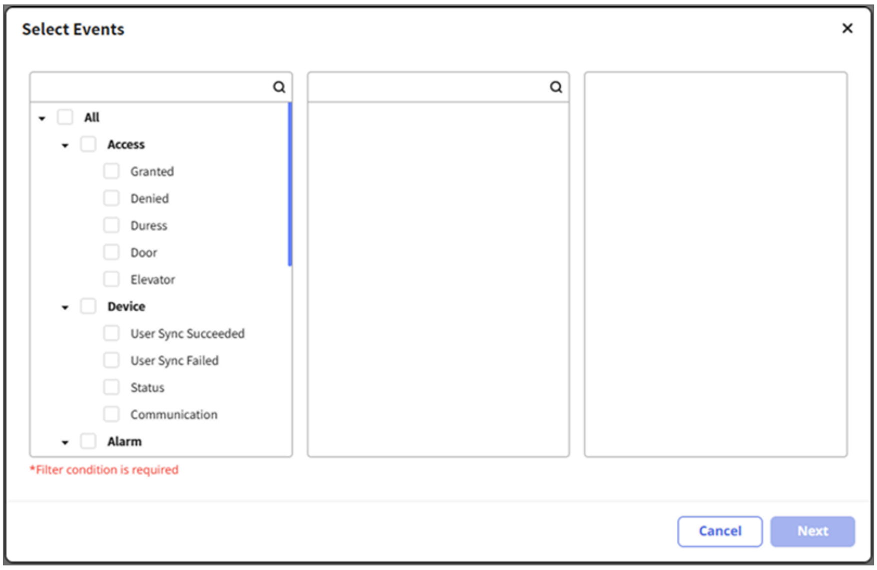
- **Unassigned Cards**: You can view cards that have not been assigned to users.
- **Blacklist Cards**: You can view disabled cards.
- **Expired Users**: You can view users whose expiration date has passed.
- **Users To Be Expired Within X Days**: You can view users whose expiration date is approaching within N days. You can directly input the number of days before generating the report.
- **Idle users for the last N months**: You can view users who have had no access records for the past N months. You can directly input the number of months before generating the report.
- **Inactive Users**: You can view inactive users.

> **INFO**
>
> - The generated report can be saved under **Saved Reports**. Click the **Save Report** button at the top left of the report.
> - For more information about report management, refer to the following.

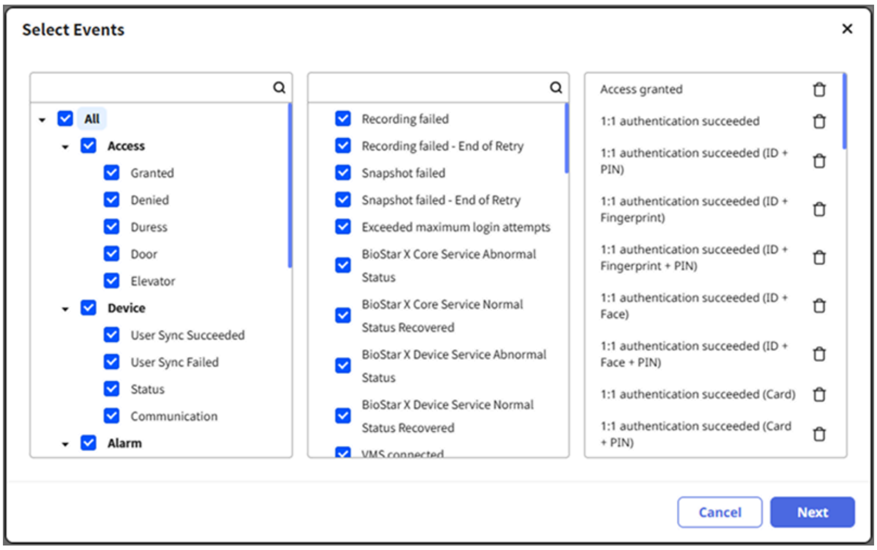
Generate custom report

You can filter and generate custom reports according to your desired conditions. The generated report can be saved as a template for convenient use when generating reports with the same conditions in the future.

1. Click **Events** → **Custom Report** on the left sidebar of the screen.
2. In the **Select Events** window, select the desired events.



3. Once you have completed your desired event selection, click the **Next** button.



Select Events

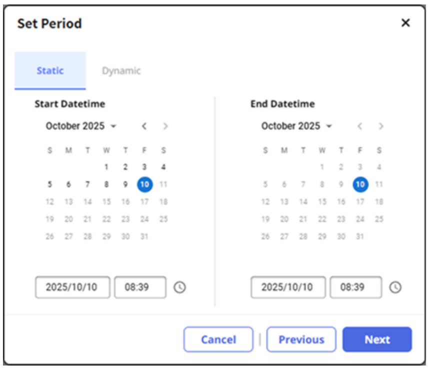
- ☑ All
  - ☑ Access
    - ☑ Granted
    - ☑ Denied
    - ☑ Duress
    - ☑ Door
    - ☑ Elevator
  - ☑ Device
    - ☑ User Sync Succeeded
    - ☑ User Sync Failed
    - ☑ Status
    - ☑ Communication
  - ☑ Alarm

- ☑ Recording failed
- ☑ Recording failed - End of Retry
- ☑ Snapshot failed
- ☑ Snapshot failed - End of Retry
- ☑ Exceeded maximum login attempts
- ☑ BioStar X Core Service Abnormal Status
- ☑ BioStar X Core Service Normal Status Recovered
- ☑ BioStar X Device Service Abnormal Status
- ☑ BioStar X Device Service Normal Status Recovered
- ☑ VMS connected

- Access granted
- 1:1 authentication succeeded
- 1:1 authentication succeeded (ID + PIN)
- 1:1 authentication succeeded (ID + Fingerprint)
- 1:1 authentication succeeded (ID + Fingerprint + PIN)
- 1:1 authentication succeeded (ID + Face)
- 1:1 authentication succeeded (ID + Face + PIN)
- 1:1 authentication succeeded (Card)
- 1:1 authentication succeeded (Card + PIN)

- In the search (🔍) input field, you can search for desired items.
- By clicking the 🗑 button in the rightmost list, you can exclude the selected items.

4. Set the query period and click the **Next** button.

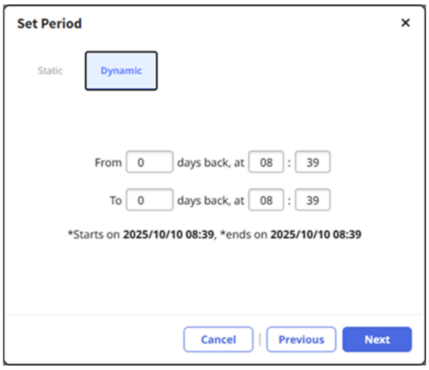


Set Period

Static | Dynamic

Start Datetime: 2025/10/10 08:39

End Datetime: 2025/10/10 08:39



Set Period

Static | Dynamic

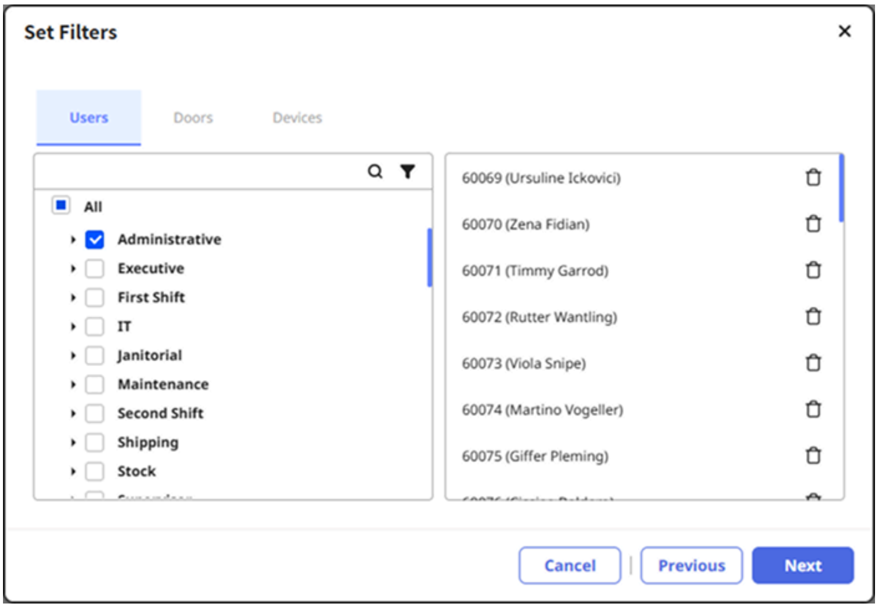
From 0 days back, at 08 : 39

To 0 days back, at 08 : 39

*Starts on **2025/10/10 08:39**, *ends on **2025/10/10 08:39**

- **Static**: You can set a specific date and time to set the query period.
- **Dynamic**: You can set the start date, end date, and time based on today. It is useful when generating reports for a specific period iteratively.

5. You can set conditions based on users, doors, and devices, either grouped or individually.

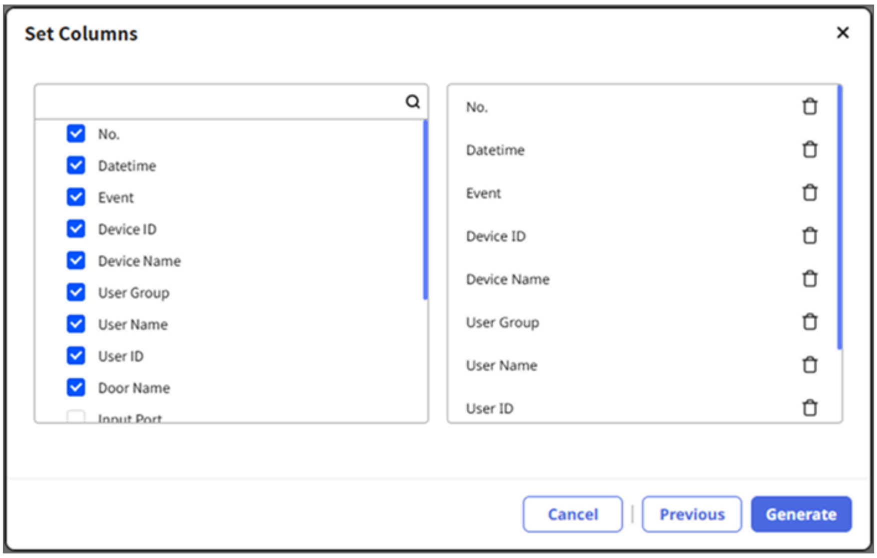


- ■ All
  - ☑ Administrative
  - ☐ Executive
  - ☐ First Shift
  - ☐ IT
  - ☐ Janitorial
  - ☐ Maintenance
  - ☐ Second Shift
  - ☐ Shipping
  - ☐ Stock

60069 (Ursuline Ickovici)
60070 (Zena Fidian)
60071 (Timmy Garrod)
60072 (Rutter Wantling)
60073 (Viola Snipe)
60074 (Martino Vogeller)
60075 (Giffer Pleming)

- By clicking the 🗑 button in the right list, you can exclude the selected items.

6. Select your desired conditions and click the **Next** button.
7. In the column settings window, select the columns to be displayed in the report.

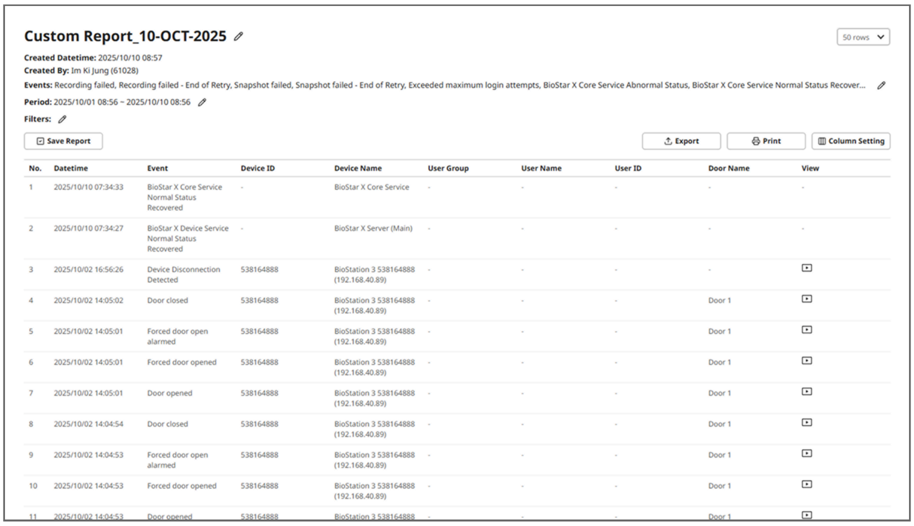


☑ No.
☑ Datetime
☑ Event
☑ Device ID
☑ Device Name
☑ User Group
☑ User Name
☑ User ID
☑ Door Name
☐ Input Port

No.
Datetime
Event
Device ID
Device Name
User Group
User Name
User ID

8. Once you have finished selecting your desired columns, click the **Generate** button.

Complete the creation of the custom report.



Custom Report_10-OCT-2025 🖉

Created Datetime: 2025/10/10 08:57

Created By: Im Ki Jung (61028)

Events: Recording failed, Recording failed - End of Retry, Snapshot failed, Snapshot failed - End of Retry, Exceeded maximum login attempts, BioStar X Core Service Abnormal Status, BioStar X Core Service Normal Status Recover... 🖉

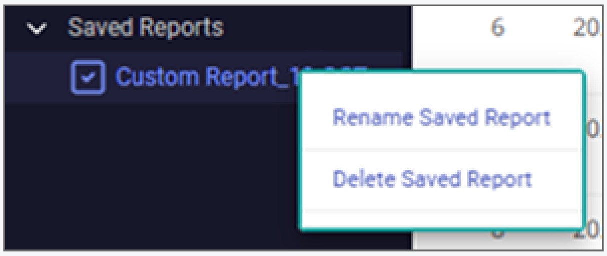
Period: 2025/10/01 08:56 ~ 2025/10/10 08:56 🖉

Filters: 🖉

No.	Datetime	Event	Device ID	Device Name	User Group	User Name	User ID	Door Name	View
1	2025/10/10 07:34:33	BioStar X Core Service Normal Status Recovered	-	BioStar X Core Service	-	-	-	-	-
2	2025/10/10 07:34:27	BioStar X Device Service Normal Status Recovered	-	BioStar X Server (Main)	-	-	-	-	-
3	2025/10/02 16:56:26	Device Disconnection Detected	538164888	BioStation 3 538164888 (192.168.40.89)	-	-	-	-	▶
4	2025/10/02 14:05:02	Door closed	538164888	BioStation 3 538164888 (192.168.40.89)	-	-	-	Door 1	▶
5	2025/10/02 14:05:01	Forced door open alarmed	538164888	BioStation 3 538164888 (192.168.40.89)	-	-	-	Door 1	▶
6	2025/10/02 14:05:01	Forced door opened	538164888	BioStation 3 538164888 (192.168.40.89)	-	-	-	Door 1	▶
7	2025/10/02 14:05:01	Door opened	538164888	BioStation 3 538164888 (192.168.40.89)	-	-	-	Door 1	▶
8	2025/10/02 14:04:54	Door closed	538164888	BioStation 3 538164888 (192.168.40.89)	-	-	-	Door 1	▶
9	2025/10/02 14:04:53	Forced door open alarmed	538164888	BioStation 3 538164888 (192.168.40.89)	-	-	-	Door 1	▶
10	2025/10/02 14:04:53	Forced door opened	538164888	BioStation 3 538164888 (192.168.40.89)	-	-	-	Door 1	▶
11	2025/10/02 14:04:53	Door opened	538164888	BioStation 3 538164888	-	-	-	Door 1	▶

INFO

- To modify the report title, event items, period, and filter conditions, click the 🖉 button at the top of the report.
- The report title can also be changed under **Saved Reports** in the left sidebar of the screen. Select the custom report for which you want to change the title and right-click. Select **Rename Saved Report** from the pop-up menu.

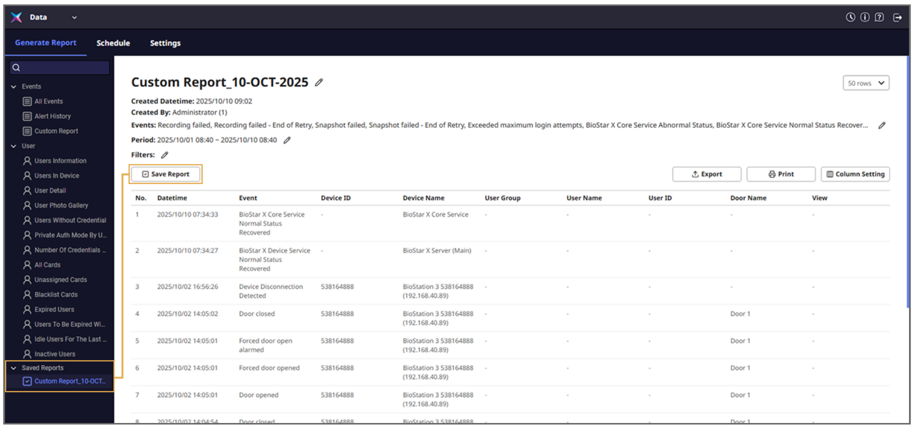


- For more information about report management, refer to the following.

Report management

Report Save

To save the generated report as a template, click the **Save Report** button. Saved reports can be viewed under **Saved Reports** in the left sidebar of the screen.



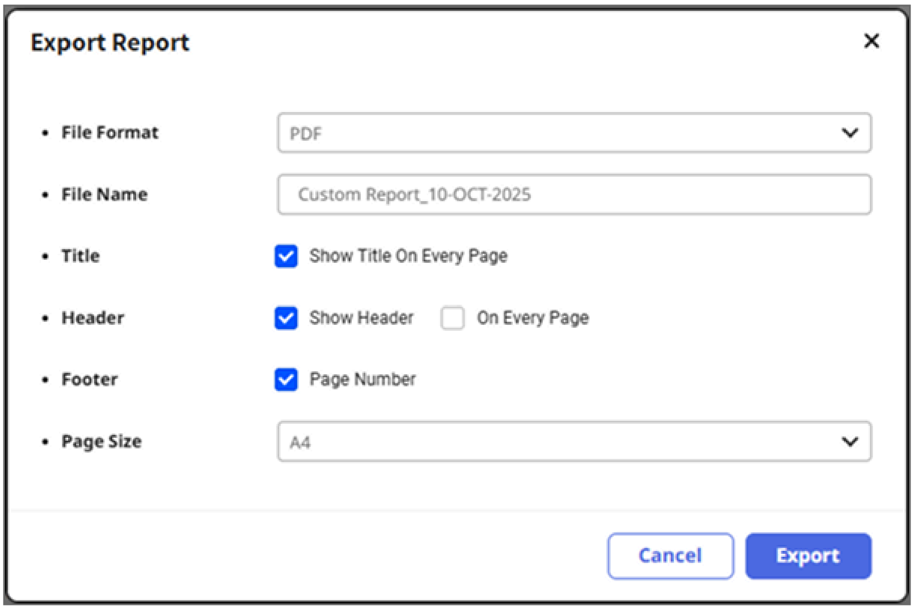
Custom Report_10-OCT-2025

Created Datetime: 2025/10/10 09:02
Created By: Administrator (1)
Events: Recording failed, Recording failed - End of Retry, Snapshot failed, Snapshot failed - End of Retry, Exceeded maximum login attempts, BioStar X Core Service Abnormal Status, BioStar X Core Service Normal Status Recover...
Period: 2025/10/01 08:40 ~ 2025/10/10 08:40
Filters:

No.	Datetime	Event	Device ID	Device Name	User Group	User Name	User ID	Door Name	View
1	2025/10/10 07:34:33	BioStar X Core Service Normal Status Recovered	-	BioStar X Core Service	-	-	-	-	-
2	2025/10/10 07:34:27	BioStar X Device Service Normal Status Recovered	-	BioStar X Server (Main)	-	-	-	-	-
3	2025/10/02 16:56:26	Device Disconnection Detected	538164888	BioStation 3 538164888 (192.168.40.89)	-	-	-	-	-
4	2025/10/02 14:05:02	Door closed	538164888	BioStation 3 538164888 (192.168.40.89)	-	-	-	Door 1	-
5	2025/10/02 14:05:01	Forced door open alarmed	538164888	BioStation 3 538164888 (192.168.40.89)	-	-	-	Door 1	-
6	2025/10/02 14:05:01	Forced door opened	538164888	BioStation 3 538164888 (192.168.40.89)	-	-	-	Door 1	-
7	2025/10/02 14:05:01	Door opened	538164888	BioStation 3 538164888 (192.168.40.89)	-	-	-	Door 1	-
8	2025/10/02 14:04:54	Door closed	538164888	BioStation 3 538164888	-	-	-	Door 1	-

Save report file

To export the report as a PDF or CSV file, click the **Export** button. When the **Export Report** window appears, set each item and click the **Export** button.

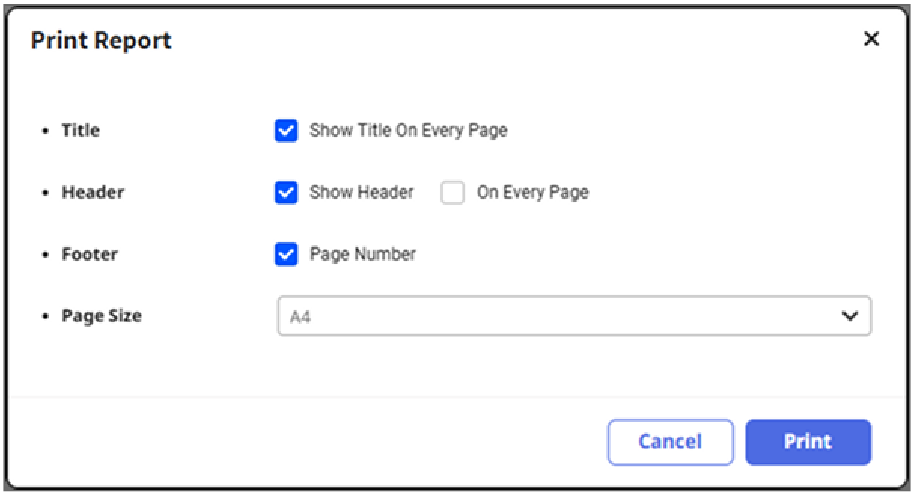


Export Report

- File Format: PDF
- File Name: Custom Report_10-OCT-2025
- Title: ☑ Show Title On Every Page
- Header: ☑ Show Header ☐ On Every Page
- Footer: ☑ Page Number
- Page Size: A4

Print report

To print the report using a printer connected to your PC, click the **Print** button. When the **Print Report** window appears, set each item and click the **Print** button.



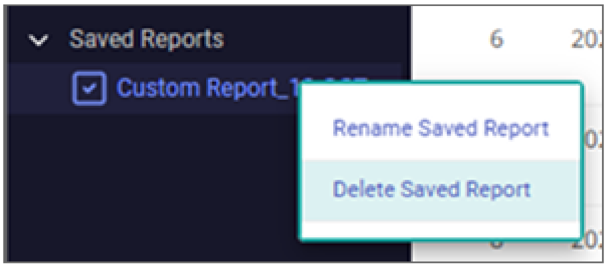
Print Report ×

- Title ☑ Show Title On Every Page
- Header ☑ Show Header □ On Every Page
- Footer ☑ Page Number
- Page Size A4

The print preview screen will appear in a new tab of your web browser. Click the print button at the top right of the screen to start printing.

Delete report

To delete a saved report, select the report to be deleted under **Saved Reports** in the left sidebar and right-click. Select **Delete Saved Report** from the pop-up menu.

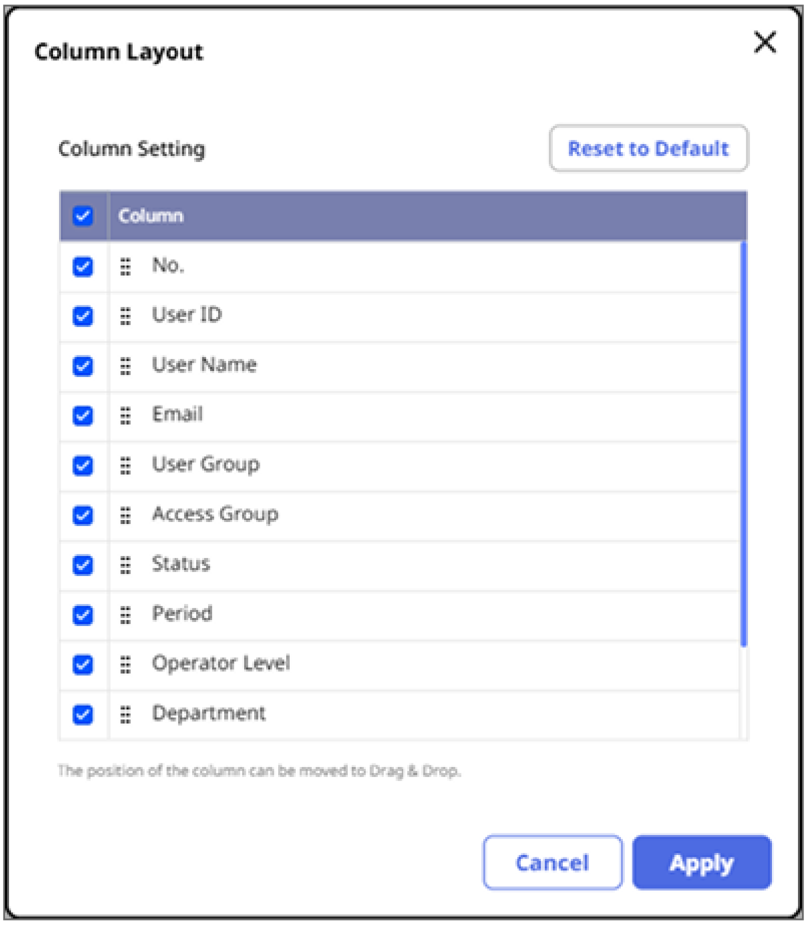


Set columns

You can change the column settings displayed in the report. Through column settings, you can select the columns to be displayed or change the order of the columns.

1. Click the **Set Columns** button at the top right of the report.

2. When the **Column Layout** window appears, select or deselect the desired columns.



- ☑ Column
- ☑ No.
- ☑ User ID
- ☑ User Name
- ☑ Email
- ☑ User Group
- ☑ Access Group
- ☑ Status
- ☑ Period
- ☑ Operator Level
- ☑ Department

The position of the column can be moved to Drag & Drop.

3. To change the order of the columns, click and drag the desired column to change its position.

4. To save the settings, click the **Apply** button.

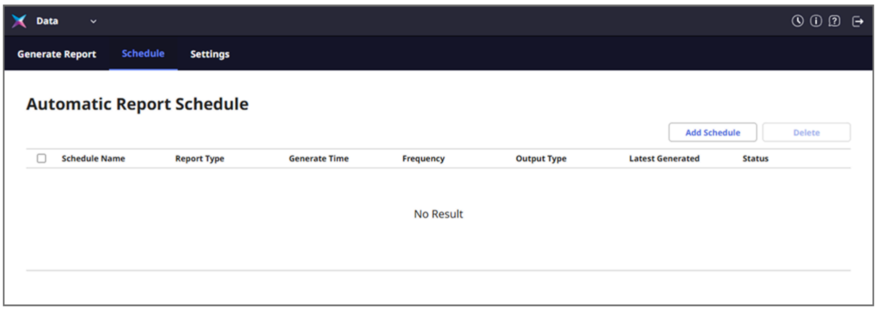
> **INFO**
>
> - To reset the column layout settings, click the **Default Column** button.
> - Depending on the generated report, the columns that can be selected or deselected may vary.

Automatic Report Schedule

Set a schedule to automatically generate **Custom Report** created by setting the DYNAMIC period.

Add auto-generated schedule

1. Click **Data** or select **Data** from the shortcut list at the top left of the screen on the **Launcher** page.
2. Click **Schedule** tab.
3. Click **Add Schedule** at the top right of the screen.

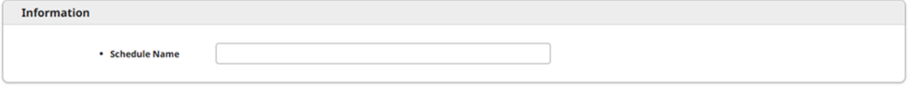


□	Schedule Name	Report Type	Generate Time	Frequency	Output Type	Latest Generated	Status
				No Result			

4. When the **Add Automatic Report Schedule** screen appears, set each item.

Information setting

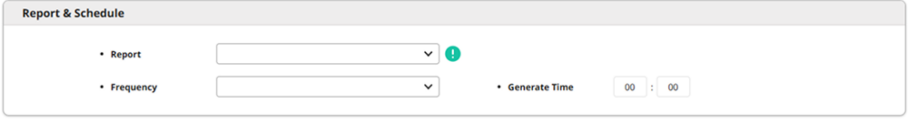
Set basic information of Automatic Report Schedule.



- **Schedule Name**: Enter the schedule name.

Report and schedule settings

Set the schedule to be automatically generated for each report.

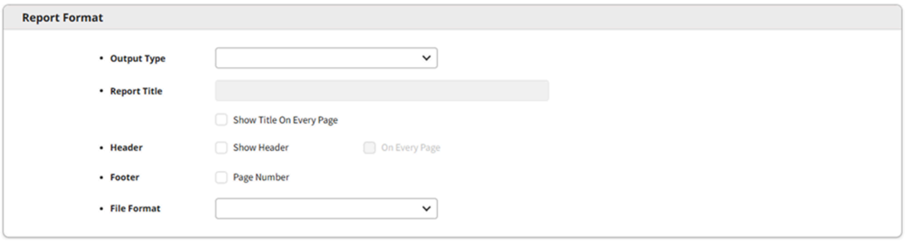


- **Report**: Select a custom report to automatically generate. Only custom reports set to DYNAMIC period will appear.
- **Frequency**: Set the frequency to automatically generate reports.
- **Generate Time**: Set the time to automatically generate reports.

> **INFO**
>
> For more information about creating custom reports, refer to the following.

Report format settings

Set the format for each report.



- **Output Type**: Set the automatically generate method of reports.
- **Report Title**: Select **Show Title On Every Page** to display the report name as the title on every page.
- **Header**: If **Show Header** is selected, the header is displayed when the report is created. Select **On Every Page** to display the header on every page.

  > **INFO**
  >
  > The header may vary depending on the reports.

- **Footer**: Set whether to display page numbers.
- **File Format**: Set the file format for exporting reports.

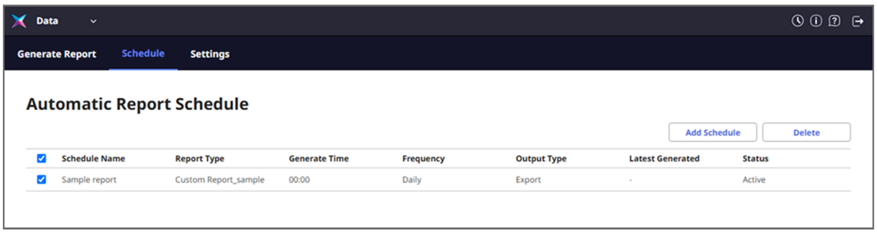
3. Click **Apply** to save the settings.

> **INFO**
>
> If all settings are complete, set the path to save the report. For more information, refer to the following.

Delete auto-generated schedule

1. Click **Data** or select **Data** from the shortcut list at the top left of the screen on the **Launcher** page.
2. Click **Schedule** tab.

3. Click the checkbox of the schedule to delete from the auto schedule list.



Automatic Report Schedule

☑	Schedule Name	Report Type	Generate Time	Frequency	Output Type	Latest Generated	Status
☑	Sample report	Custom Report_sample	00:00	Daily	Export	-	Active

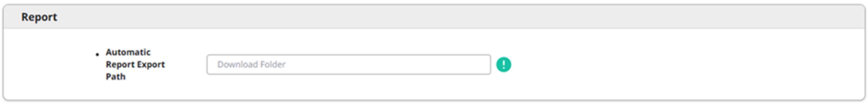
4. Click **Delete** at the top right of the screen.

Settings

Set the path where the report will be saved if you have set **Schedule**.

1. Click **Settings**.

2. Enter the path where you want to save the report.



Report

- Automatic Report Export Path: Download Folder

   - **Automatic Report Export Path**: The report will be saved to the specified path, and if no path is entered, it will be automatically saved in the *Documents\BioStarX* folder on the user's PC.

3. Click **Apply** to save the settings.

Dashboard

The dashboard can be customized to suit individual preferences by allowing each user to select the information they want, add widgets, and freely configure and arrange the widgets.

INFO

- Each user can configure **Dashboard** individually.
- The information available on **Dashboard** may vary depending on **Account Level**.

Add Widgets

The dashboard is a customizable monitoring screen where users can freely arrange the information they want.

Edit Widget

Edit widgets added to the dashboard.

Delete Widget

Delete widgets added to the dashboard.

Add Widgets

The **BioStar X** dashboard is a customizable monitoring screen where users can freely arrange the information they want. By adding various widgets, you can configure the key information of the access control system according to your work environment.

The types of widgets that can be added are as follows.

- **Chart**: Visualize access event data in bar, line, or pie charts
- **Counter**: Display the number of events per day/week in numbers
- **Real-time events**: Monitor all events occurring in **BioStar X** in real-time
- **Real-time access monitoring**: Display authentication success user information for specific devices in real-time
- **System usage status**: Display registration status of users, devices, access points, etc. in numbers
- **Door control**: Check the status of selected access points and control them remotely
- **Text**: Place custom text such as announcements or widget titles

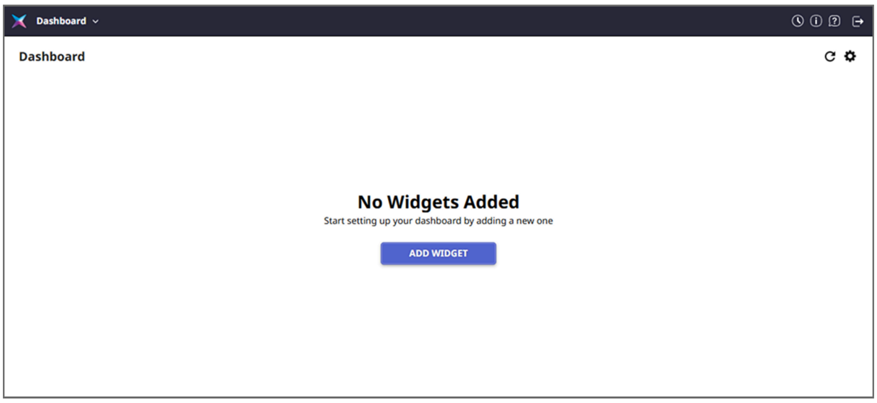
You can gain the following advantages from the widgets placed on the dashboard.

- **Customized configuration**: Select only the information needed for work and arrange it on one screen
- **Real-time monitoring**: Instantly check access events and system status
- **Intuitive visualization**: Visual representation of data through charts and counters
- **Efficient management**: Improve work efficiency by integrating monitoring and control features

Add widgets

You can add widgets to **Dashboard** to check the information you want.

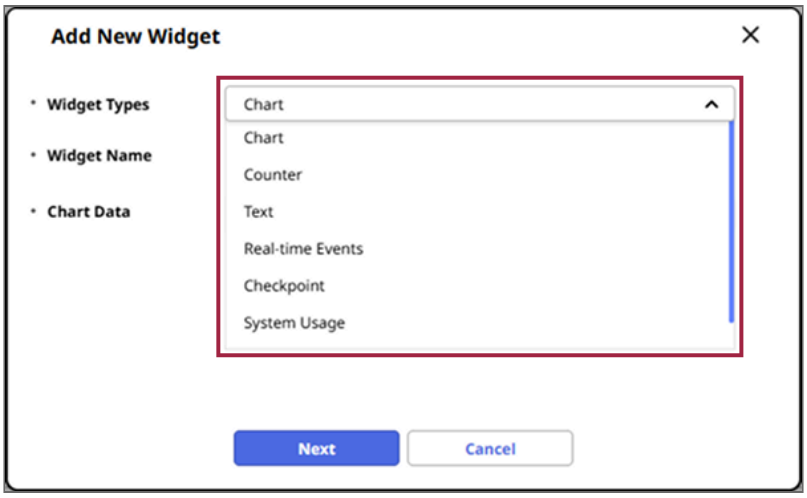
1. Click **Dashboard** in the **Launcher** page.
2. Click the **Add Widget** button.



No Widgets Added

Start setting up your dashboard by adding a new one

3. When the **Add New Widget** window appears, select the desired item in **Widget Type** and enter or set the required fields.

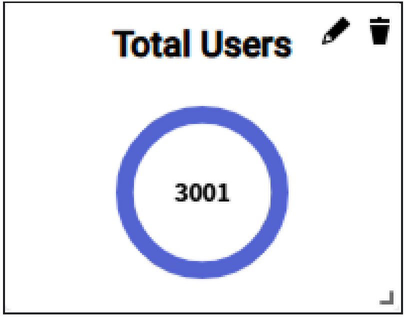


4. Complete the widget settings and click the **Apply** button.
5. When the widget is created in the widget display area, adjust its size or place it in the desired location.
6. Once you have completed all settings, click the **Apply** button in the upper right corner of the screen.

> ⓘ **INFO**
>
> If a widget has already been added, click the ⚙ icon in the upper right corner of the screen. Once you enter **Dashboard Settings** mode, click the **Add Widget** button.

Types of widgets

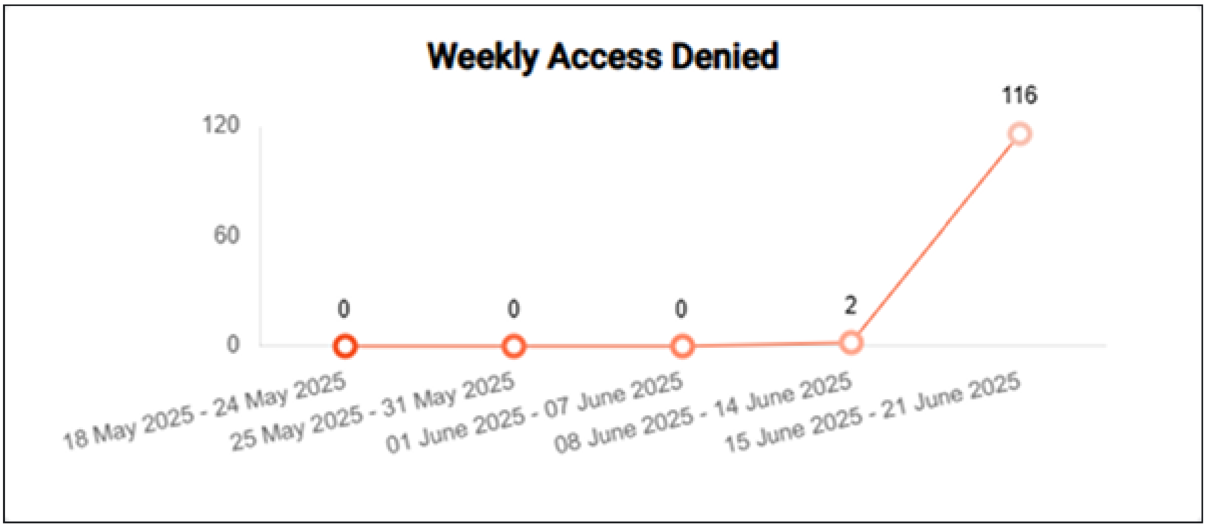
- The default widget size is set differently for each widget and is optimized to look best at the default.
- All widgets can be resized by dragging the lower-right corner.



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

Chart

Selecting desired chart data enables the display of the number of events that occurred in a chart.



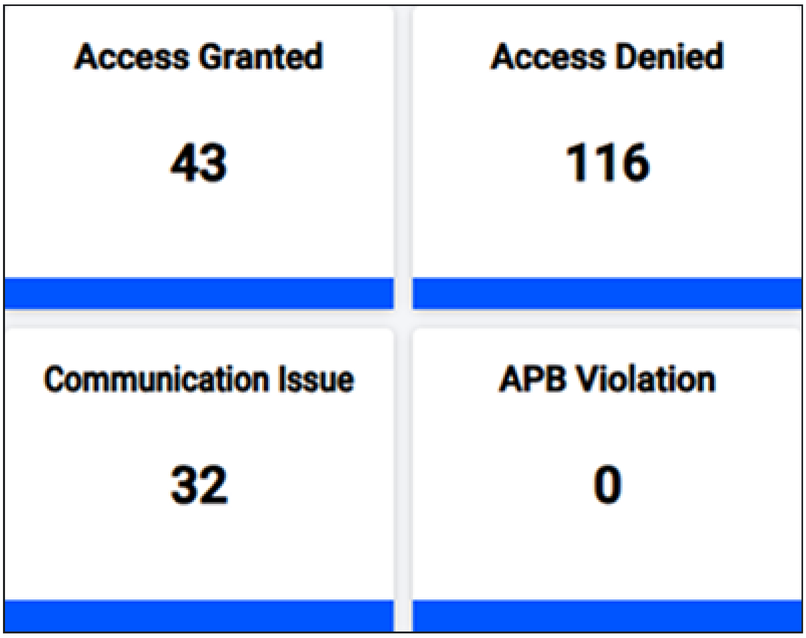
The image above is an example screen and may differ from the actual screen.

- **Chart Data**: From the daily or weekly event list, select the desired chart data.
  - **Daily Access Granted**, **Daily Access Denied**, **Daily Communication Issue**, **Daily APB Violation**, **Weekly Access Granted**, **Weekly Access Denied**, **Weekly Communication Issue**, **Weekly APB Violation**
- **Chart Type**: Select the desired type among **Vertical Bar**, **Horizontal Bar**, **Line**, and **Pie**.
- **Color Schemes**: Select the desired color among 5 color schemes.

> **INFO**
>
> The charts shown when selecting **Color Schemes** are random values for preview, not actual values.

Counter

Selecting desired counter data enables the display of the number of events that occurred as a number.

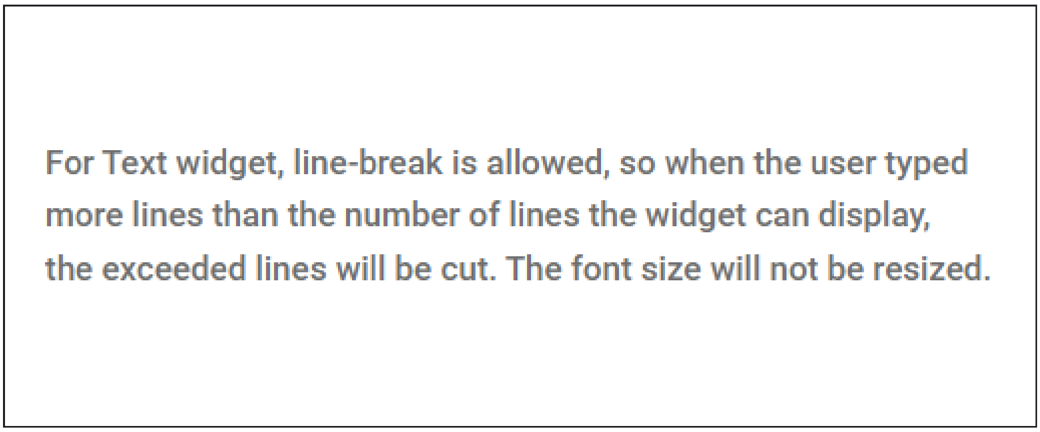


The image above is an example screen and may differ from the actual screen.

- **Counter Data**: From the daily or weekly event list, select the desired counter data.
  - **Daily Access Granted**, **Daily Access Denied**, **Daily Communication Issue**, **Daily APB Violation**, **Weekly Access Granted**, **Weekly Access Denied**, **Weekly Communication Issue**, **Weekly APB Violation**

Text

You can input and place the desired text in the widget area of **Dashboard**. After creation, you can place it in the required location and use it as a title for a widget or as a notice.



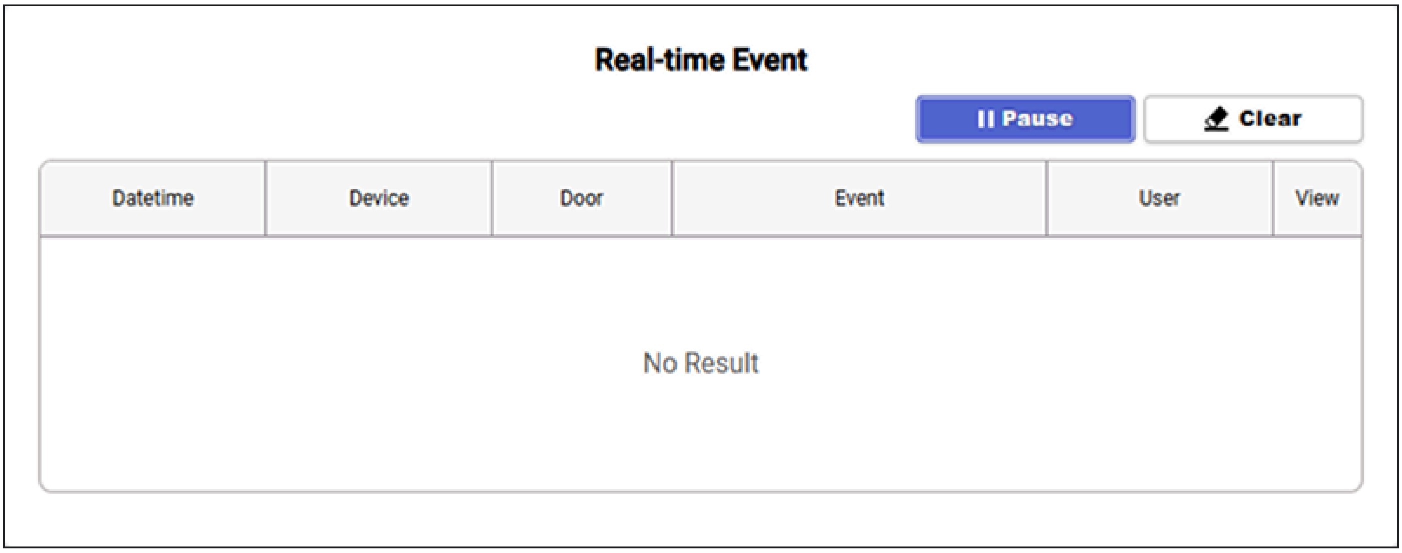
For Text widget, line-break is allowed, so when the user typed more lines than the number of lines the widget can display, the exceeded lines will be cut. The font size will not be resized.

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

> **INFO**
>
> If you select the **Remove Background** option while creating a **Text** widget, transparency will be applied to the background.

Real-time events

Shows events occurring in **BioStar X** in real-time. You can check events by filtering specific events, users, doors, and devices.



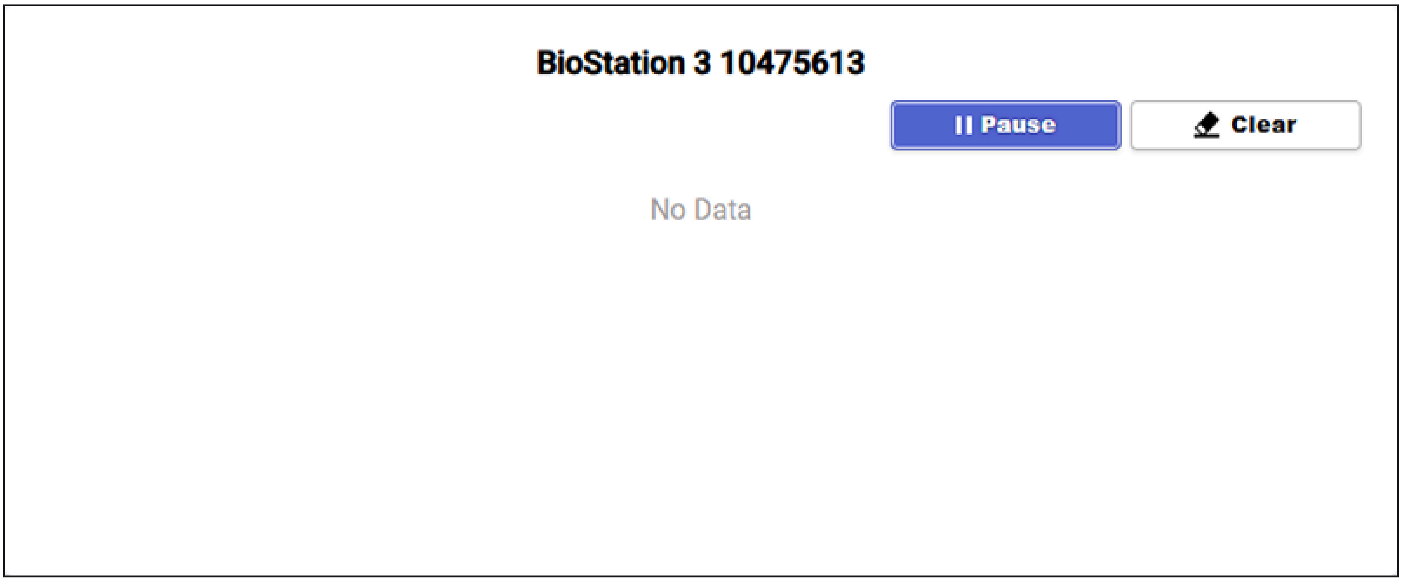
The image above is an example screen and may differ from the actual screen.

- **Pause**: To pause the real-time event.
- **Play**: Resume a real-time event that stopped.
- **Clear**: The entire captured record will be removed.

> **INFO**
>
> If you navigate to another page and then return to **Dashboard**, the list will be cleared and events will be recorded again.

Real-time access monitoring

Select one device and display the profile photo and information (**User**, **Date**, **Device**) of the user who successfully authenticated to the selected device in real time.



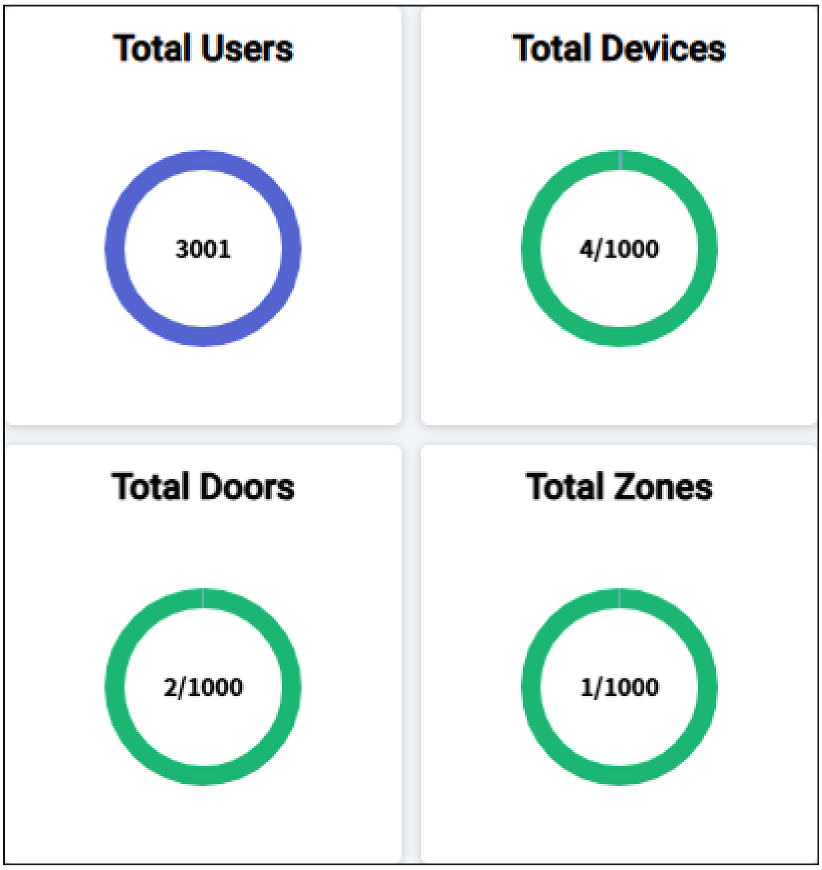
The image above is an example screen and may differ from the actual screen.

- **Pause**: To pause the checkpoint.
- **Play**: To resume the checkpoint that paused.
- **Clear**: The entire captured record will be removed.

> **INFO**
>
> **Checkpoint** are recorded for up to 5 people.

System usage status

The various usage statuses of BioStar X are displayed in numbers.

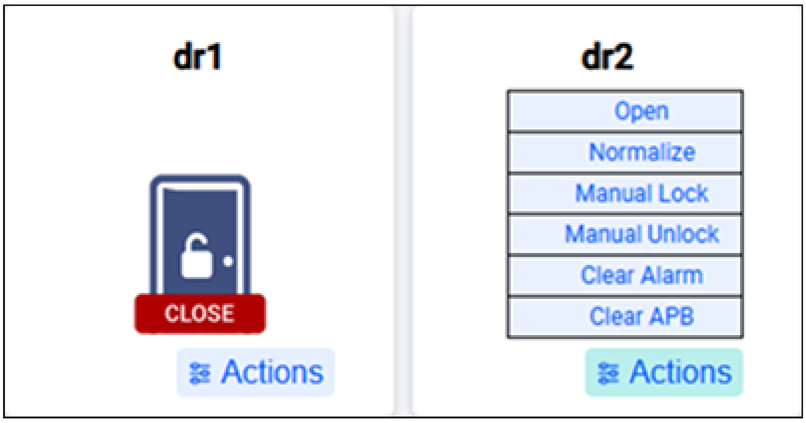


The image above is an example screen and may differ from the actual screen.
The **System Usage** that can be displayed is as follows:

- **Total Users**, **Total Cards**, **Total Fingerprints**, **Total Faces**, **Total Faces**, **Total QR/Barcode**, **Total Mobile Access**, **Total Devices**, **Total Doors**, **Total Zones**, **Total Access Groups**, **Total User Groups**, **Total Device Groups**

Door control

Select one door to check and control its status.



The image above is an example screen and may differ from the actual screen.
The following items can be controlled with the **Actions** buttons:

- **Open**, **Normalize**, **Manual Lock**, **Manual Unlock**, **Clear Alarm**, **Clear APB**

> **INFO**
>
> The name of the **Door Control** widget is automatically assigned to the name of the door and cannot be modified.

Set widget data refresh interval

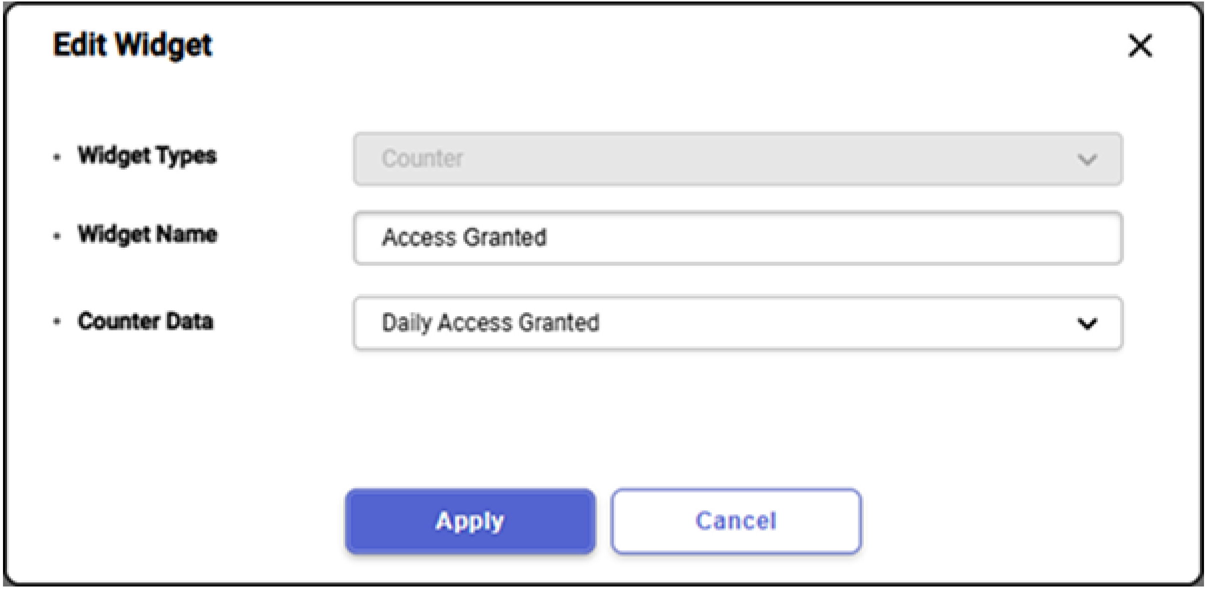
You can set the data refresh interval of widgets added to the dashboard.

1. Click **Dashboard** in the **Launcher** page.
2. Click the ⚙ icon in the upper right corner of the screen.
3. Once you enter **Dashboard Settings** mode, set **Auto Refresh Interval** in the general settings at the bottom of the screen.

Edit Widget

Edit widgets added to the dashboard.

1. Click **Dashboard** in the **Launcher** page.
2. Click the ⚙ icon in the upper right corner of the screen.
3. Click ✎ at the top right of the **Widget** you want to modify in **Dashboard Settings** mode.
4. When the **Edit Widget** window appears, modify your desired items.



Edit Widget

- Widget Types: Counter
- Widget Name: Access Granted
- Counter Data: Daily Access Granted

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

5. Click **Apply** after completing your modifications.
6. Click **Apply** in the upper right of the **Dashboard Settings** screen.

Confirm that the changes made on the dashboard are reflected.

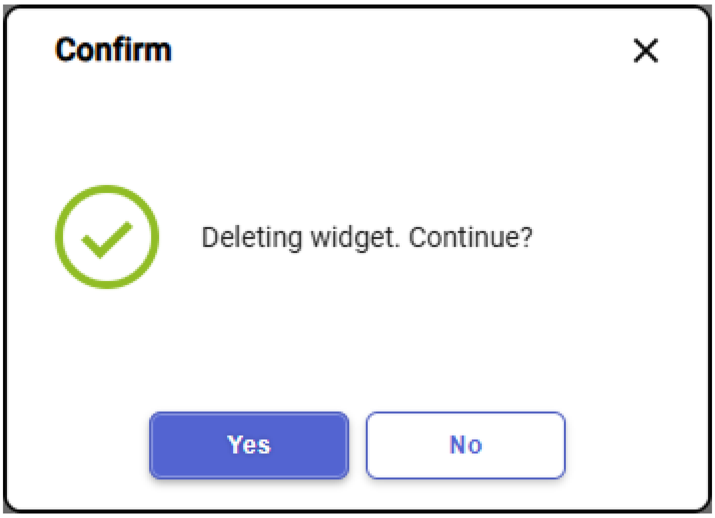
ⓘ **INFO**

- The **Widget Types** cannot be changed in the **Edit Widget**.
- **Text**, **System Usage**, and **Door Control** that use a specific name cannot modify the **Widget Name**.

Delete Widget

Delete widgets added to the dashboard.

1. Click **Dashboard** in the **Launcher** page.
2. Click the ⚙ icon in the upper right corner of the screen.
3. When you enter **Dashboard Settings** mode, click the 🗑 button in the upper right corner of the **Widget** you want to delete.
4. Check the delete confirmation popup and click the **Yes** button.



Confirm

Deleting widget. Continue?

5. Click **Apply** in the upper right corner of the **Dashboard Settings** screen.

Confirm that the changes made on the dashboard are reflected.

Settings

This guides you through the various features that can be set on the **Settings** page of **BioStar X**. You can add devices and explore various options for customizing the user environment, such as permissions, language, date and time, and access card management.

Click **Settings** on the **Launcher** page or select **Settings** from the shortcut list at the top left of the screen.

> **INFO**
>
> The features that can be configured may differ based on the user's permissions. Some features can only be used by users with administrator permission. For more information about user permission-based accessible menus, refer to the following.

Manage Devices → 7 items

This guide describes hot to manage addition, deletion, and modification of devices.

- Manage Device Groups
- Register Device
- Register Wiegand Credentials

↳ 7 items

Device Settings → 7 items

This provides guidance on how to set and manage the detailed features of the registered device.

- Basic Information Setting
- Network Settings
- Authentication Settings

↳ 7 items

Image Log Settings → Read more

This document provides instructions for setting events and schedules to generate image logs, options for deleting image logs, and methods for configuring storage paths.

USB Agent Settings → Read more

This document provides instructions for using the USB fingerprint enrollment device and card enrollment device when accessing BioStar X on the client PC.

Device Connection Management Settings → Read more

This document provides guidance on connecting and managing a large number of devices through the communication server in BioStar X. You can manage up to 3,000 network devices by distributing them across multiple servers.

Manage Doors → 4 items

This guide describes how to set up and manage the access door information for the registered device.

- Manage Door Group
- Register Door
- Modify Door Information

↳ 4 items

Manage Operation Permissions → 1 item

This guide describes how to assign operator permissions and add and configure custom permissions to registered users.

- Add Custom Permissions

↳ 1 item

Access Control Settings → 4 items

This guide describes how to set up access control system

- Manage Access Levels
- Manage Access Groups
- Manage Floor Levels

↳ 4 items

Schedule Settings → Read more

Set entry and holiday schedules to efficiently manage access control and attendance.

Trigger and Action Settings → Read more

You can set the device or BioStar X to perform the desired action when a certain event occurs at the device, entrance, or area.

Import Event Logs → Read more

Learn how to import event logs.

Alert Settings → Read more

Set the types of alert and messages to appear on the screen when events occur in the device, door, or area.

Manage Credentials → 4 items

This guide describes how to manage credentials for access authentication.

- Manage Cards
- Set Wiegand Card Format
- Set Smart Card Format

↳ 4 items

Card Printer → Read more

You can print cards with the desired design by integrating BioStar X and cardPresso.

Email Setting → Read more

You can configure information such as the subject line of the email that will send the mobile link for face enrollment, the company name, company logo, and contact details.

How to Use the Quick Action → Read more

You can add Quick Action button to the main screen.

Server Settings → 2 items

Provides various methods for configuring essential server settings in BioStar X, including basic server information, user and device management, automatic upgrades, and HTTPS certificates.

- Server Detailed Settings
- Install HTTPS Certificate

↳ 2 items

Activate License → 2 items

Activate BioStar X license and device license.

- BioStar X License
- Device License

↳ 2 items

System Settings → 5 items

Learn how to configure key system settings in the BioStar X platform.

- Audit Trail
- System Backup
- System Restore

↳ 5 items

Configure Settings → Read more

This guide covers how to set the language and time zone, date/time format, and notification sound when you first install BioStar X or change your usage environment.

Manage Devices

This guide describes hot to manage addition, deletion, and modification of devices. Import user information registered on the device to the **BioStar X** server or upgrade firmware remotely.

Manage Device Groups

This guide describes to the device group feature for efficiently managing multiple devices.

Register Device

This guide describes how to register a device in BioStar X.

Register Wiegand Credentials

This guide outlines how to add a Wiegand device to the registered master or slave device.

Register Slave

This provides guidance on adding a slave to the master.

Manage Users Registered on Dev...

This document provides guidance on managing users stored in the device.

Upgrade Firmware

Instructions for upgrading the firmware of devices connected to BioStar X.

Use Device Management Feature

Instructions for reconnecting the device, synchronizing, and batch editing functionality.

Manage Device Groups

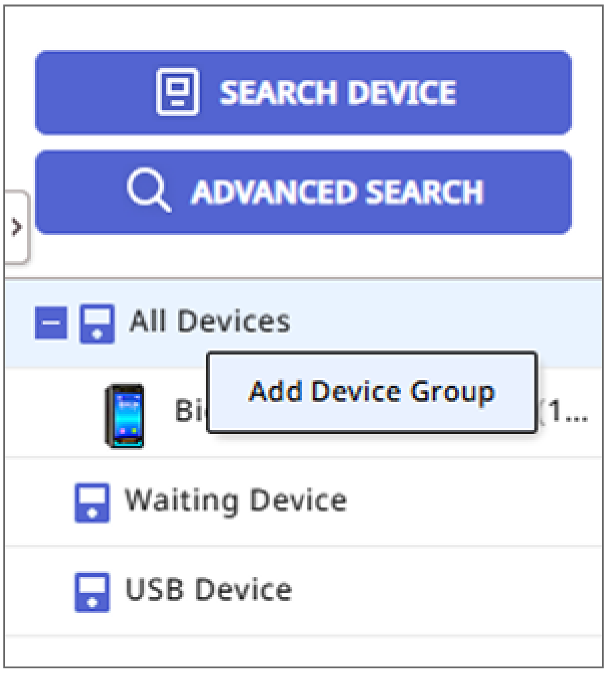
This guide describes to the device group feature for efficiently managing multiple devices. This document provides guidance on the device group feature that allows for efficient management of multiple devices.

TIP

Naming device groups based on the location or purpose of the devices makes management easier. For example, groups can be designated as '1st Floor Entrance', '2nd Floor Office', 'Conference Room', etc.

Create a device group

1. Click **Settings** on the **Launcher** page.
2. Click **Device** in the left sidebar.
3. Right-click **All Devices** in the device list.



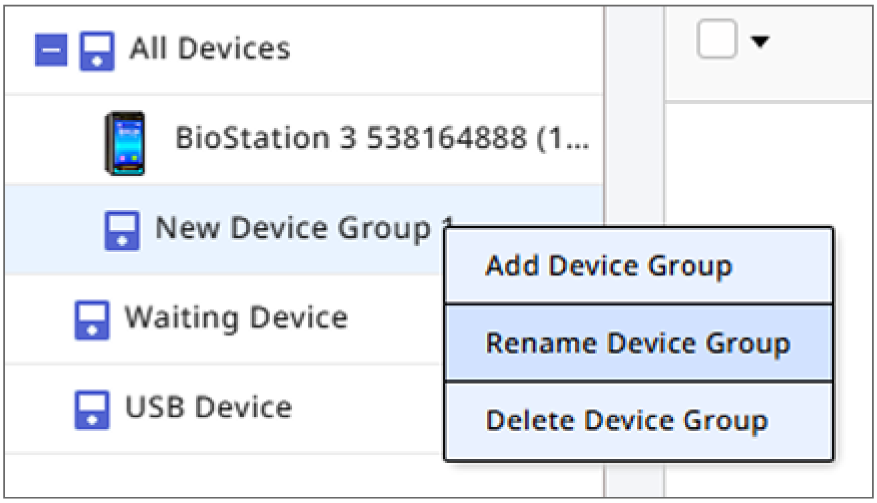
4. Click **Add Device Group** in the popup menu.
5. Enter your desired group name.

INFO

- You can create device groups with up to 8 levels of subgroups.
- Device group names can be up to 48 characters long.
- Selecting a device group from the device list will display only the devices belonging to that group.

Modify a device group name

1. Click **Settings** on the **Launcher** page.
2. Click **Device** in the left sidebar.
3. From the sublist of **All Devices**, select the device group whose name you want to change and right-click.



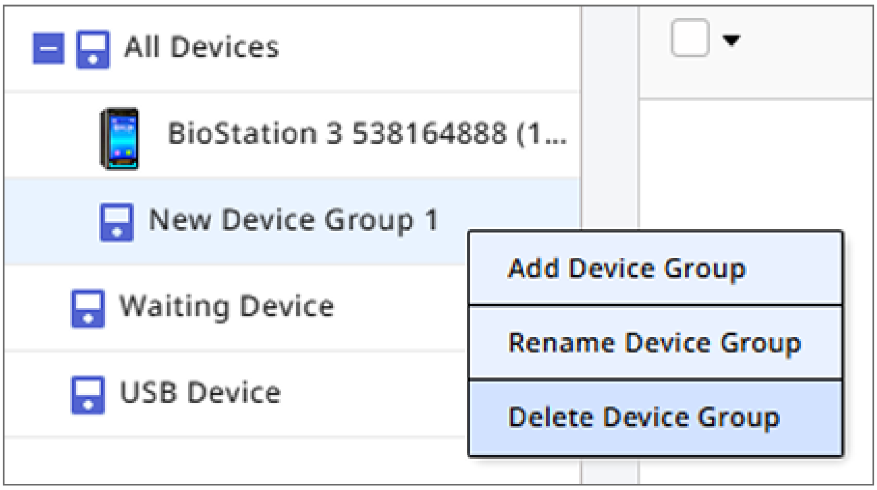
4. Click **Rename Device Group** in the popup menu.
5. Enter the new name for the group.

> **INFO**
>
> Device group names can be up to 48 characters long.

Deleting a device group

1. Click **Settings** on the **Launcher** page.
2. Click **Device** in the left sidebar.

3. From the sublist of **All Devices**, select the device group you want to delete and right-click.



4. Click **Delete Device Group** in the pop-up menu.

> ⚠ **CAUTION**
>
> Deleting a device group will remove all devices belonging to that group.

Register Device

This guide explains how to register a device in **BioStar X**. Registering a device allows **BioStar X** to monitor and manage the status of that device. Ensure the device is properly connected before searching for it. It’s convenient to know the location, ID, IP address, and other details in advance when adding multiple devices at once.

> **INFO**
>
> - When registering a new device, change the device key value to the server's data encryption key value. All user data on the device will be deleted during the key conversion.
> - To delete all setting information and user data stored on the device and resend them, click **Delete Data & Sync Device**. You can find the **Delete Data & Sync Device** option by selecting the device from the device list and clicking the ⋯ button.
> - To register all devices in the **Waiting Device** group, right-click the group name and click **Add All Waiting Devices**. To register devices individually, right-click on the device name and click **Add Waiting Device**.
> - If the user ID type on **BioStar X** differs from the device, change the device settings according to **BioStar X**’s user ID configuration.
> - If the user ID type on **BioStar X** is set to alphanumeric, some devices may not be usable or may have restrictions. For more information on details, refer to the following.
> - Refer to the following to register a device and configure its details.

Before start

Check the following before registering the device.

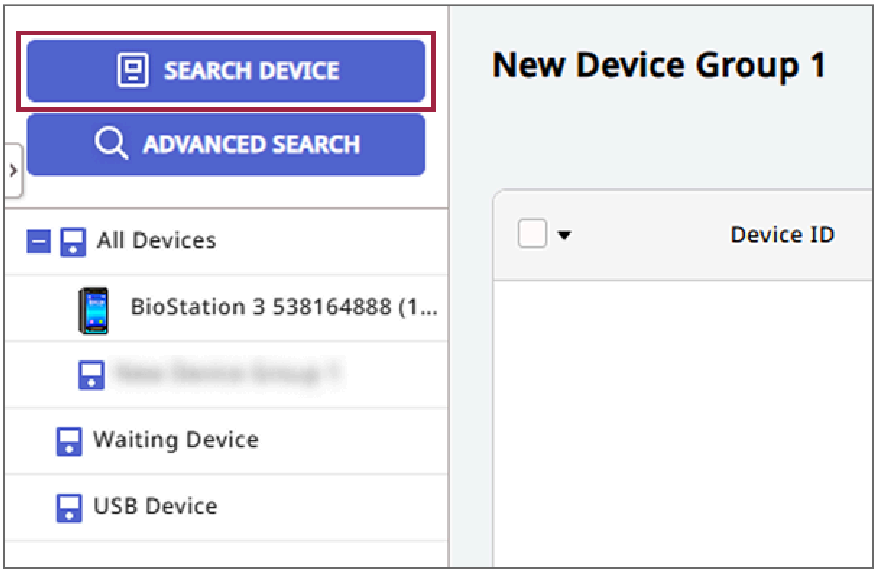
- Set access levels, access groups, and floor levels for access control. For more information, refer to the following.
- Create a group to manage devices efficiently. Refer to the following for more information.

Quick registration

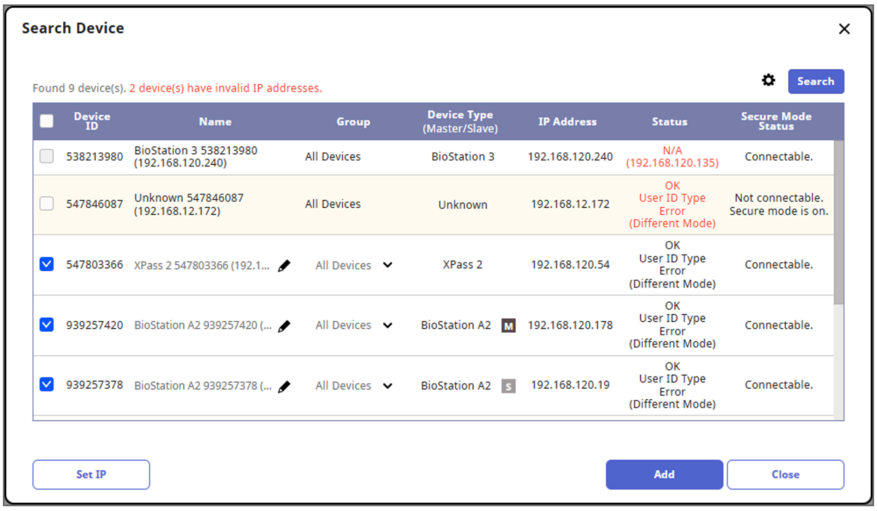
Devices on the same network as **BioStar X** can be automatically searched and registered.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** in the left sidebar.

3. Click **Search Device** in the device list.



4. When the **Search Device** window appears, a list of all devices that can be registered will be displayed. If the desired device is not in the list, click **Search** in the top right corner.

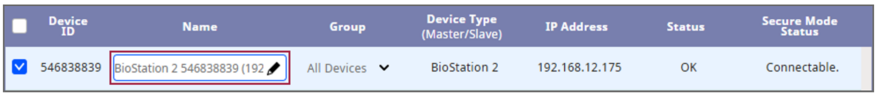


Found 9 device(s). 2 device(s) have invalid IP addresses.

☐	Device ID	Name	Group	Device Type (Master/Slave)	IP Address	Status	Secure Mode Status
☐	538213980	BioStation 3 538213980 (192.168.120.240)	All Devices	BioStation 3	192.168.120.240	N/A (192.168.120.135)	Connectable.
☐	547846087	Unknown 547846087 (192.168.12.172)	All Devices	Unknown	192.168.12.172	OK User ID Type Error (Different Mode)	Not connectable. Secure mode is on.
☑	547803366	XPass 2 547803366 (192.1...	All Devices	XPass 2	192.168.120.54	OK User ID Type Error (Different Mode)	Connectable.
☑	939257420	BioStation A2 939257420 (...	All Devices	BioStation A2 M	192.168.120.178	OK User ID Type Error (Different Mode)	Connectable.
☑	939257378	BioStation A2 939257378 (...	All Devices	BioStation A2 S	192.168.120.19	OK User ID Type Error (Different Mode)	Connectable.

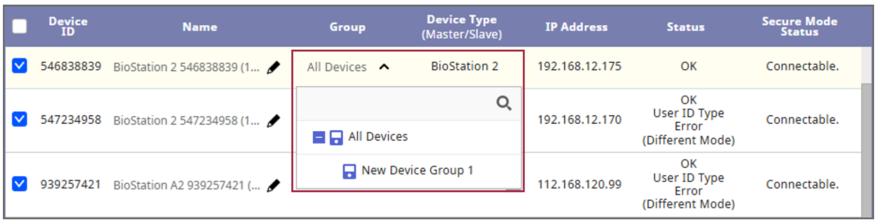
5. Select the devices to register from the device list or deselect devices to not register.

6. To change the name of the device to be registered, click ✎ in the **Name** column and make the change.



☐	Device ID	Name	Group	Device Type (Master/Slave)	IP Address	Status	Secure Mode Status
☑	546838839	BioStation 2 546838839 (192	All Devices	BioStation 2	192.168.12.175	OK	Connectable.

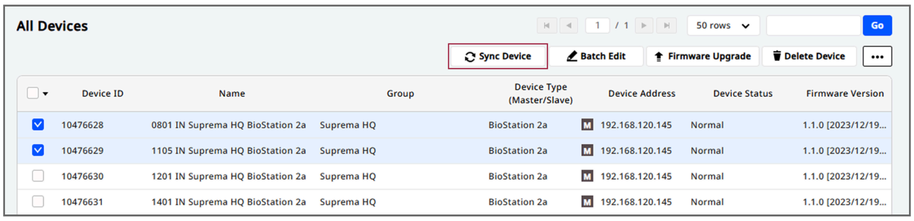
7. To specify the group for the device to be registered, select it in the **Group** column.



☐	Device ID	Name	Group	Device Type (Master/Slave)	IP Address	Status	Secure Mode Status
☑	546838839	BioStation 2 546838839 (1...	All Devices	BioStation 2	192.168.12.175	OK	Connectable.
☑	547234958	BioStation 2 547234958 (1...			192.168.12.170	OK User ID Type Error (Different Mode)	Connectable.
☑	939257421	BioStation A2 939257421 (...			112.168.120.99	OK User ID Type Error (Different Mode)	Connectable.

8. Once all settings for the selected devices are complete, click **Add**.

The added devices will appear in the device list. Select the added device and click **Sync Device**.

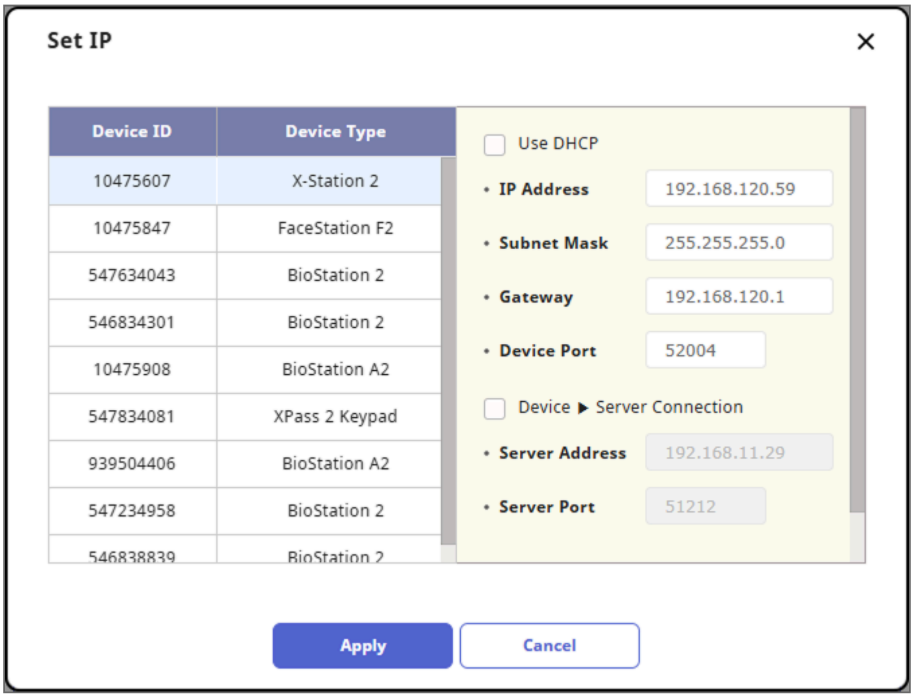


□	Device ID	Name	Group	Device Type (Master/Slave)	Device Address	Device Status	Firmware Version
☑	10476628	0801 IN Suprema HQ BioStation 2a	Suprema HQ	BioStation 2a	M 192.168.120.145	Normal	1.1.0 [2023/12/19...
☑	10476629	1105 IN Suprema HQ BioStation 2a	Suprema HQ	BioStation 2a	M 192.168.120.145	Normal	1.1.0 [2023/12/19...
□	10476630	1201 IN Suprema HQ BioStation 2a	Suprema HQ	BioStation 2a	M 192.168.120.145	Normal	1.1.0 [2023/12/19...
□	10476631	1401 IN Suprema HQ BioStation 2a	Suprema HQ	BioStation 2a	M 192.168.120.145	Normal	1.1.0 [2023/12/19...

> **INFO**
>
> Devices for which the IP address is unavailable or needs to be changed can be modified by clicking **Set IP**. Refer to the following for more information.

IP address setting

You can change the IP address of the device to be registered. Click **Set IP** at the bottom left of the **Search Device** window. When the **Set IP** window appears, select the device to change the IP address.



Device ID	Device Type
10475607	X-Station 2
10475847	FaceStation F2
547634043	BioStation 2
546834301	BioStation 2
10475908	BioStation A2
547834081	XPass 2 Keypad
939504406	BioStation A2
547234958	BioStation 2
546838839	BioStation 2

□ Use DHCP

- IP Address: 192.168.120.59
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.120.1
- Device Port: 52004

□ Device ▶ Server Connection

- Server Address: 192.168.11.29
- Server Port: 51212

- **Use DHCP**: Select this option to allow the device to automatically obtain an IP address via DHCP. Selecting this option may result in the IP address changing each time the device connects to the network.

  > To manually enter the IP address, subnet mask, gateway, etc., deselect this option.

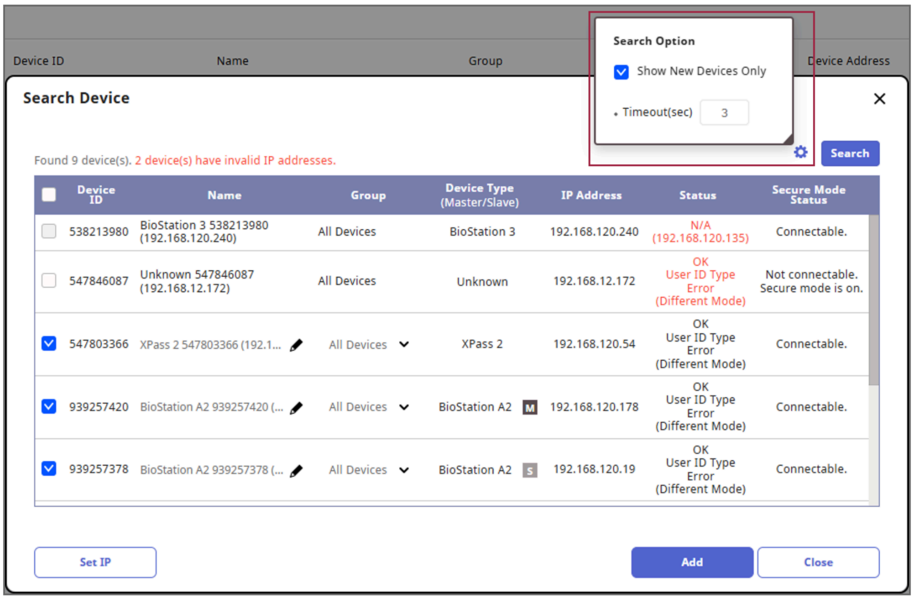
- **Device ▶ Server Connection**: Select this option to configure the device to connect to the **BioStar X** server. You will need to enter the IP address and port number of the server where **BioStar X** is installed.

ⓘ **INFO**

After completing all IP settings and saving changes, click **Apply**. To cancel changes, click **Cancel**.

Device search options

You can set device search options by clicking ⚙ at the top right of the **Search Device** window.



Search Option

☑ Show New Devices Only

Timeout(sec) 3

Search Device

Found 9 device(s). 2 device(s) have invalid IP addresses.

□	Device ID	Name	Group	Device Type (Master/Slave)	IP Address	Status	Secure Mode Status
□	538213980	BioStation 3 538213980 (192.168.120.240)	All Devices	BioStation 3	192.168.120.240	N/A (192.168.120.135)	Connectable.
□	547846087	Unknown 547846087 (192.168.12.172)	All Devices	Unknown	192.168.12.172	OK User ID Type Error (Different Mode)	Not connectable. Secure mode is on.
☑	547803366	XPass 2 547803366 (192.1...	All Devices	XPass 2	192.168.120.54	OK User ID Type Error (Different Mode)	Connectable.
☑	939257420	BioStation A2 939257420 (...	All Devices	BioStation A2 M	192.168.120.178	OK User ID Type Error (Different Mode)	Connectable.
☑	939257378	BioStation A2 939257378 (...	All Devices	BioStation A2 S	192.168.120.19	OK User ID Type Error (Different Mode)	Connectable.

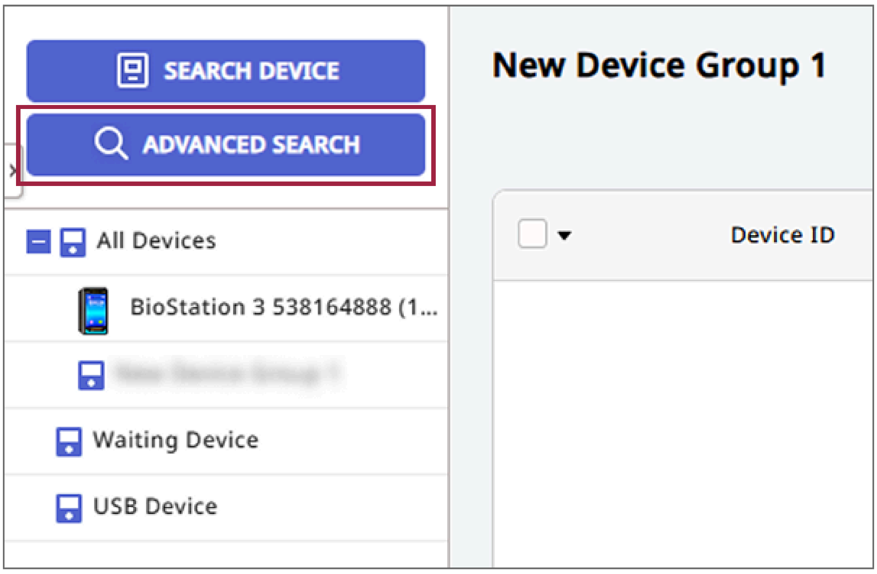
- **Show New Devices Only**: Select this option to display only newly discovered devices in the search list.
- **Timeout(sec)**: Set the desired time to exclude devices that do not respond for a certain period from the search list. This can be set in seconds, with a default of 3 seconds.

Advanced search

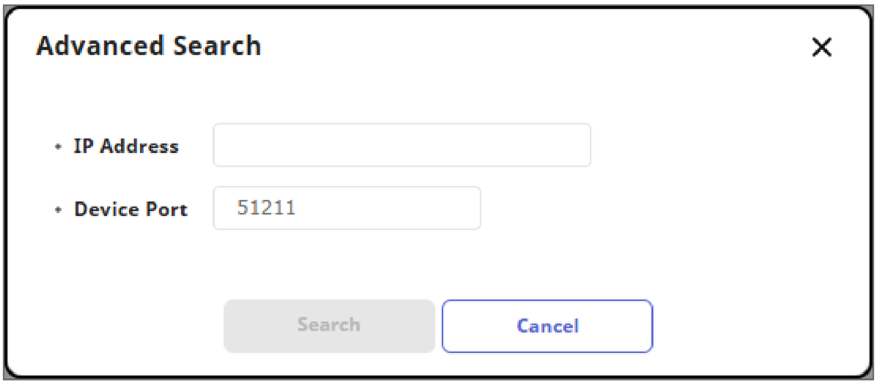
You can specify the IP address and port number of a specific device to registrer it.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** in the left sidebar.

3. Click **ADVANCED SEARCH** in the device list.

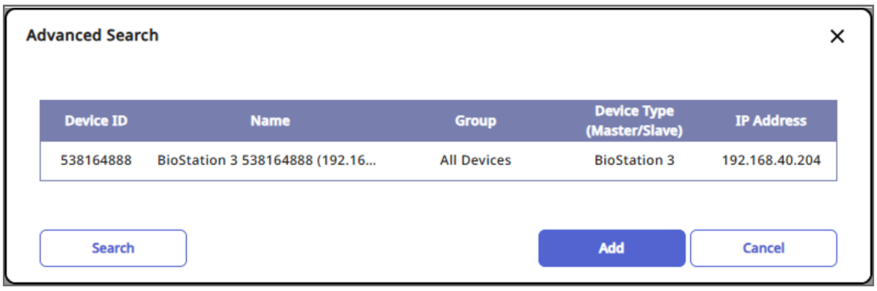


4. When the **ADVANCED SEARCH** window appears, enter the IP address and port number of the device to be registered.


Advanced Search

- IP Address
- Device Port 51211

5. Click **Search** to display devices matching the entered criteria.


Advanced Search

Device ID	Name	Group	Device Type (Master/Slave)	IP Address
538164888	BioStation 3 538164888 (192.16...	All Devices	BioStation 3	192.168.40.204

6. To register the device, click **Add**.

The added devices will appear in the device list. Select the added device and click **Sync Device**.

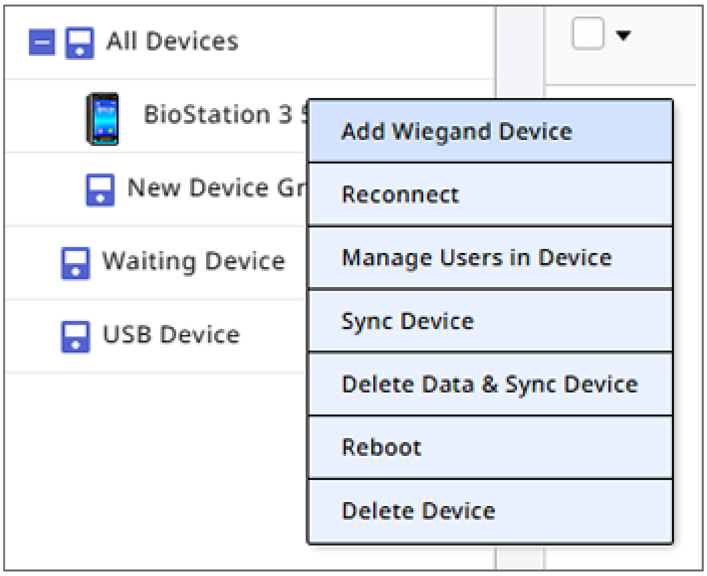
Register Wiegand Credentials

This guide outlines how to add a Wiegand device to the registered master or slave device.

ⓘ **INFO**

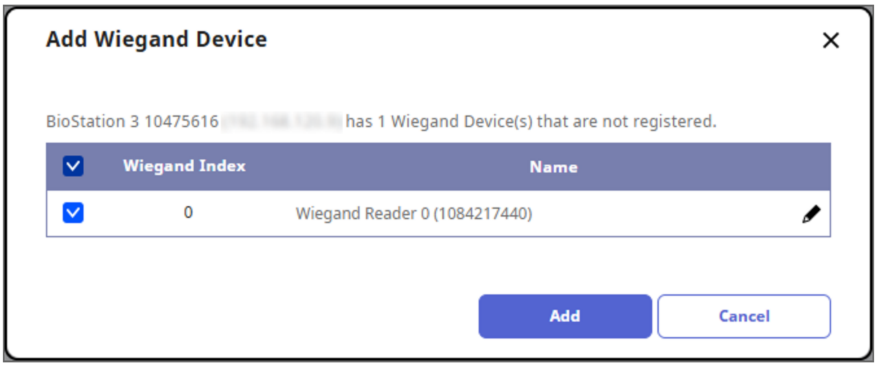
- **Master device**: Among the devices that are connected through RS-485, the device that plays the role of a controller. It processes data by periodically monitoring the slave device. It is also called a host device.
- **Slave device**: Among devices connected through RS-485, the device that only performs the input and output functions. It does not contain user information and is controlled by the master device.
- **Wiegand**: A method that transfers a small amount of data using D0 and D1. Generally it is used as a method of communication between the reader and controller of an access control device.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** in the left sidebar.
3. Right-click on the master or slave device in the All Devices list.



4. Click **Add Wiegand Device** in the popup menu.

5. When the list of Wiegand devices connected to the master device appears, select the device to register.



Add Wiegand Device

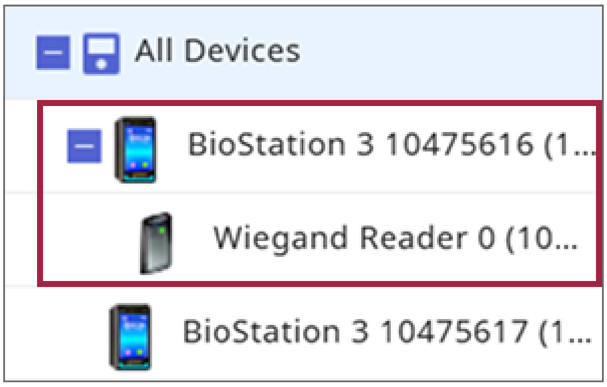
BioStation 3 10475616 [redacted] has 1 Wiegand Device(s) that are not registered.

☑	Wiegand Index	Name
☑	0	Wiegand Reader 0 (1084217440)

6. Click **Add**.

7. When the device registration confirmation message appears, click **Apply**.

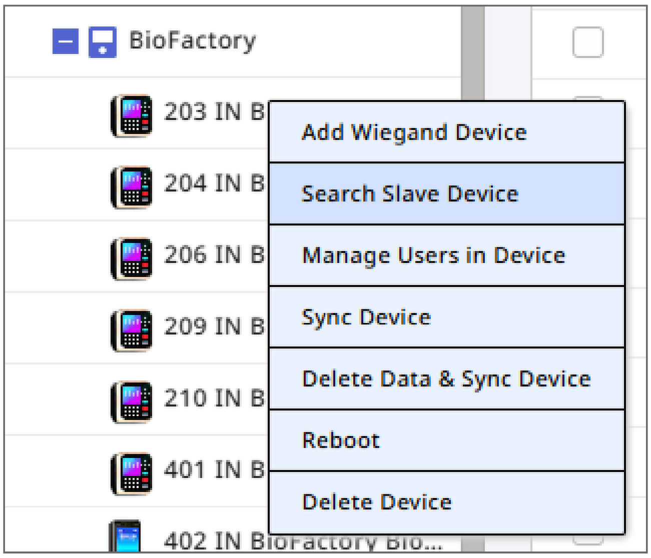
The registered Wiegand device will appear under the selected device.



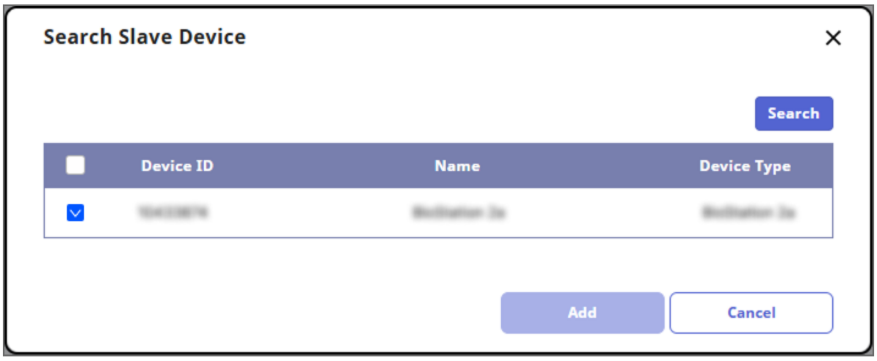
Register Slave

You can easily expand the access control system network by adding a slave device to the registered master device. The master and slave devices can be connected via RS-485 communication. In addition to devices, add-on devices such as Secure I/O 2 can also be connected and used.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** in the left sidebar.
3. Right-click on the master or slave device in the **All Devices** list.



4. Click **Search Slave Device** in the popup menu.
5. When the list of slave devices connected to the master device appears, select the device to register. If the desired device is not listed, click **Search** in the upper right corner.



6. Click **Add**.
7. When the device registration confirmation message appears, click **Apply**.

The registered slave device will appear under the selected device.

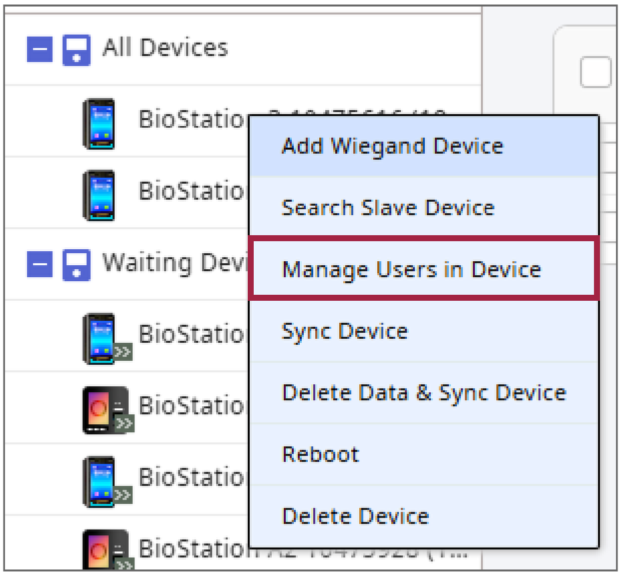
INFO

- You cannot add a facial authentication device as a slave when the master device is a fingerprint authentication device.
- You cannot add a facial authentication device as a slave if the master device is a facial authentication device and another slave device has already been added.
- Only one facial authentication device can be added as a slave when connecting a facial authentication device as the master.
- When connecting a facial authentication device as the master, you can additionally connect one Secure I/O 2 and one DM-20.
- The maximum number of slave devices available to connect varies according to the authentication method, number of users, and number of devices. Also note that the number of slave devices affects the authentication performance.

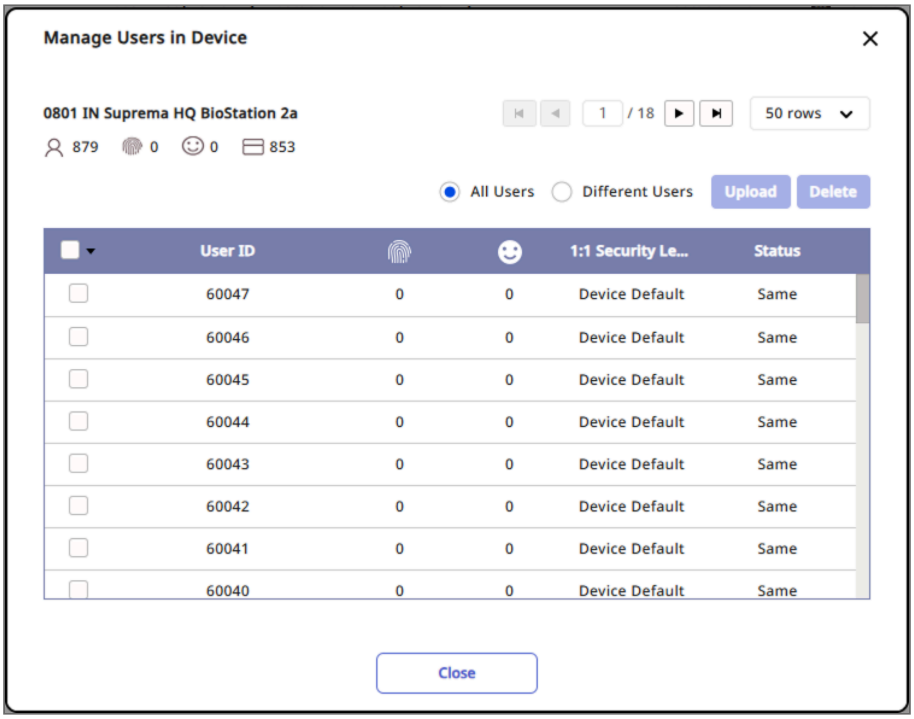
Manage Users Registered on Device

You can check the number of users, fingerprints, faces, and cards stored on the device. Information about users not registered on **BioStar X** can be compared with registered user information, and you can send or delete this information on the **BioStar X** server.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** in the left sidebar.
3. Select the device from the **All Devices** list and right-click.
4. Click **Manage Users in Device** from the pop-up menu.



When the **Manage Users in Device** window appears, you can compare the user information registered on the device with the user information registered on **BioStar X**.



Manage Users in Device

0801 IN Suprema HQ BioStation 2a

879 0 ☺ 0 853

1 / 18 ▶ ⏭ 50 rows

● All Users ○ Different Users Upload Delete

□	User ID		☺	1:1 Security Le...	Status
□	60047	0	0	Device Default	Same
□	60046	0	0	Device Default	Same
□	60045	0	0	Device Default	Same
□	60044	0	0	Device Default	Same
□	60043	0	0	Device Default	Same
□	60042	0	0	Device Default	Same
□	60041	0	0	Device Default	Same
□	60040	0	0	Device Default	Same

Close

Refer to the values displayed in the **Status** column to choose whether to delete user information from the device or send it to the **BioStar X** server. The values in the **Status** column are as follows:

- **Same**: User with the same information registered on the **BioStar X** server
- **Different**: User with information different from that registered on the **BioStar X** server
- **New User**: **BioStar X** user not stored on the server

To delete specific user information from the device, select the user to delete and click the **Delete** button. To send user information to the **BioStar X** server, click the **Upload** button.

INFO

- The **Manage Users in Device** feature can only be used with one device selected.
- When clicking the **Upload** button, if there is a user on the **BioStar X** server with the same ID, it can be updated with the device’s information.
- Deleted user information is removed only from the device and will be retained on the **BioStar X** server.
- For more information about the device's settings, refer to the following.

Upgrade Firmware

Devices connected to **BioStar X** can easily upgrade their firmware without additional connections or operations. Keeping the device firmware up to date resolves security vulnerabilities and allows access to new features.

Before start

Before upgrading the device firmware, prepare the new version of the firmware file. Save the downloaded firmware file in the following path. Create a new folder if the *firmware* folder does not exist.

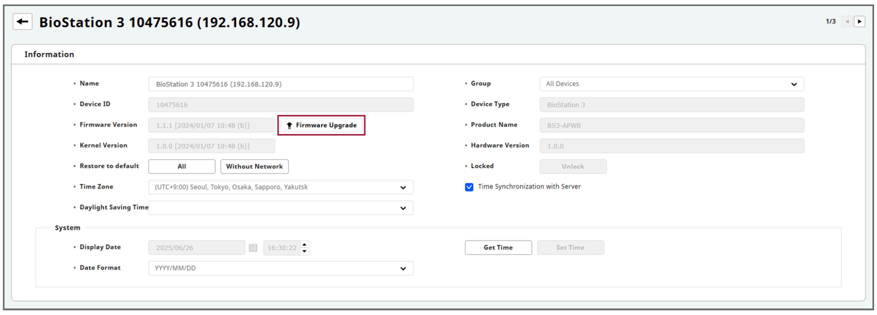
> *C:\Program Files\BioStar X\firmware*

> **INFO**
>
> Search for your device model name on the Suprema Download Center to download the latest version of the firmware file.

Firmware upgrade

Upgrade firmware for a single device

1. Click **Settings** on the **Launcher** page.
2. Click **Device** in the left sidebar.
3. Click the device in the device list that you want to upgrade.
4. Click the **Firmware Upgrade** button in the **Information** section of the device details screen.



BioStar Station 3 10475616 (192.168.120.9)

Information

- Name: BioStation 3 10475616 (192.168.120.9)
- Device ID: 10475616
- Firmware Version: 1.1.1 [2024/01/07 10:48 (b)]
- Kernel Version: 1.0.0 [2024/01/07 10:48 (b)]
- Restore to default
- Time Zone: (UTC+9:00) Seoul, Tokyo, Osaka, Sapporo, Yakutsk
- Daylight Saving Time
- Group: All Devices
- Device Type: BioStation 3
- Product Name: BS3-APWB
- Hardware Version: 1.0.0
- Locked
- ☑ Time Synchronization with Server

System

- Display Date: 2025/06/26 16:30:22
- Date Format: YYYY/MM/DD

This initiates the firmware upgrade for the device.

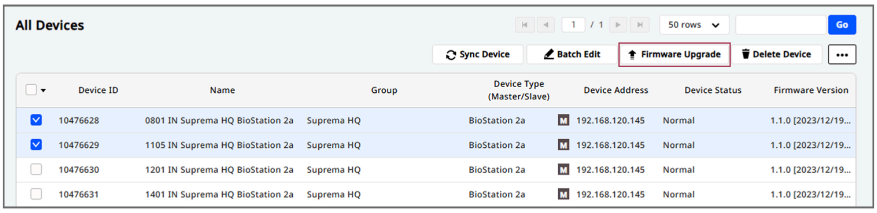
Upgrade firmware for multiple devices

1. Click **Settings** on the **Launcher** page.

2. Click **Device** in the left sidebar.

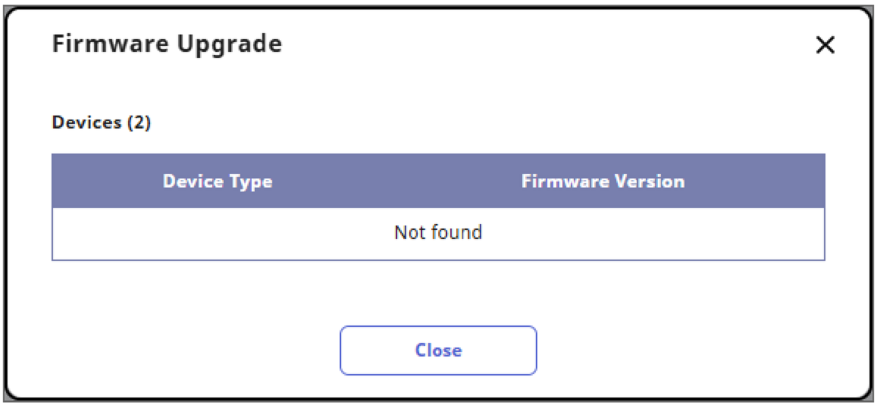
3. Select the checkbox on the far left of the devices you want to upgrade in the device list. You can select multiple devices.

4. Click the **Firmware Upgrade** button at the top right of the device list.



□	Device ID	Name	Group	Device Type (Master/Slave)	Device Address	Device Status	Firmware Version
☑	10476628	0801 IN Suprema HQ BioStation 2a	Suprema HQ	BioStation 2a M	192.168.120.145	Normal	1.1.0 [2023/12/19...
☑	10476629	1105 IN Suprema HQ BioStation 2a	Suprema HQ	BioStation 2a M	192.168.120.145	Normal	1.1.0 [2023/12/19...
□	10476630	1201 IN Suprema HQ BioStation 2a	Suprema HQ	BioStation 2a M	192.168.120.145	Normal	1.1.0 [2023/12/19...
□	10476631	1401 IN Suprema HQ BioStation 2a	Suprema HQ	BioStation 2a M	192.168.120.145	Normal	1.1.0 [2023/12/19...

5. When the **Firmware Upgrade** window appears, click the firmware version.



Devices (2)

Device Type	Firmware Version
Not found	

This initiates the firmware upgrade for the selected devices.

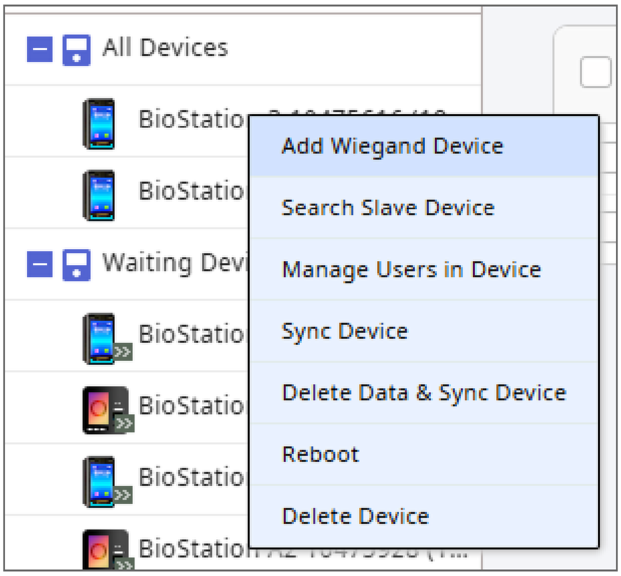
INFO

- The **Firmware Upgrade** button is activated only after selecting a device from the device list.
- Devices with the same RS-485 mode can be upgraded simultaneously in groups. For example, master devices can upgrade multiple master devices at once, and slave devices can upgrade multiple slave devices at once.
- Master devices or slaves without a master can be upgraded simultaneously in groups.
- Slave devices connected to the same master device cannot be upgraded simultaneously.

Use Device Management Feature

This guide explains how to use additional features of **BioStar X**. It provides options for reconnecting the device, synchronization, batch information editing, and deleting the device.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** in the left sidebar.
3. Select the device from the **All Devices** list and right-click.
4. Select the desired feature from the pop-up menu.



Refer to the features available through the pop-up menu below: The features provided may vary depending on the device.

- **Reconnect**: Reconnect the selected device. This option is available when one device is selected. Use this feature when the connection to **BioStar X** is lost.

> **INFO**
>
> This feature is not supported by devices connected with the **Device** ▶ **Server Connection** option. For more information on registering devices, refer to the following.

- **Sync Device**: Synchronize all user information registered on the device with **BioStar X**. This synchronization is based on the **BioStar X** database, and user information registered only on the device will be deleted. Use the **Manage Users in Device** feature to upload user information to **BioStar X**.
- **Delete Data & Sync Device**: Delete all setting information and user information stored on the device and resend it. This feature can also be accessed by selecting the device from the list and clicking the ··· button.
- **Manage Users in Device**: Upload or delete user information registered on the device in **BioStar X**. For more information, refer to the following.
- **Firmware Upgrade**: Easily upgrade the device firmware. For more information, refer to the following.

- **Reboot**: Restart the selected device. Use this feature when the device is not operating normally.
- **Delete Device**: Delete the selected device from the list. Devices set as doors or zones cannot be deleted.

> ⓘ **INFO**
>
> - For more information about the **Add Wiegand Device** feature, refer to the following.
> - For more information about the **Search Slave Device** feature, refer to the following.

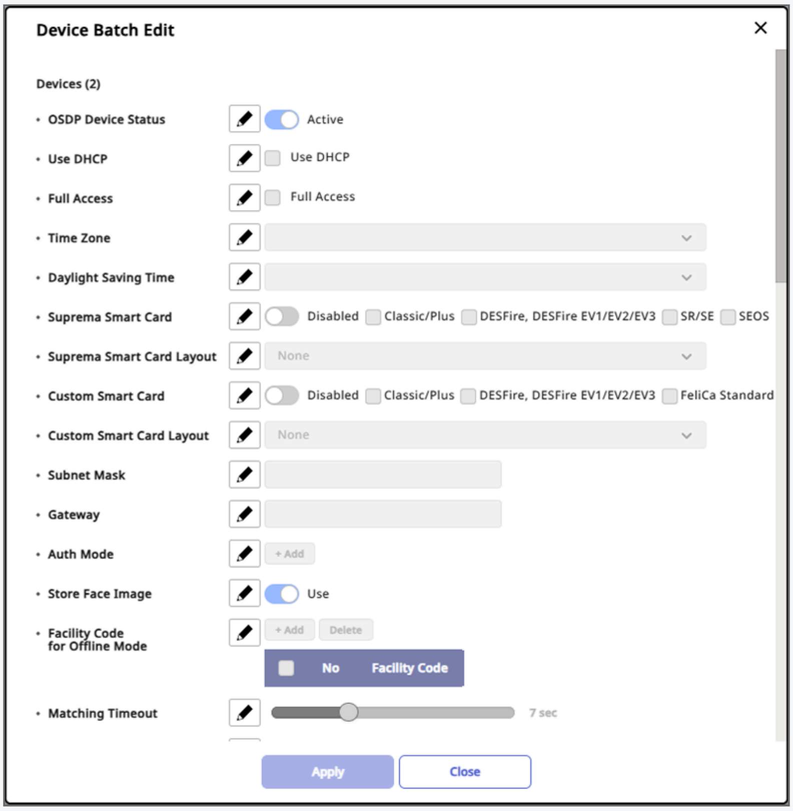
Device Settings

This provides guidance on how to set and manage the detailed features of the registered device. You can set details such as device information, network settings, authentication, and advanced settings. Details may vary based on RS-485 connection types or device models.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** in the left sidebar.
3. Select the device you want to configure from the device list.
4. Reference the details in each section to configure the device information.
   - **Information**: Verify and modify the device's name and group, time zone, hardware, and firmware versions. For more information, refer to the following.
   - **Network**: Configure the network settings of the device for TCP/IP, RS-485, and server communication. For more information, refer to the following.
   - **Authentication**: Configure options related to user authentication for the device. For more information, refer to the following.
   - **Advanced**: You can configure Master Administrator, Device Management, Display/Sound, Operating Conditions, and Actions. For more information, refer to the following.
   - **Thermal & Mask** / **Mask**: Configure details related to thermal camera and mask usage. For more information, refer to the following.
   - **Intercom**: Configure details for using the IP intercom. For more information, refer to the following.
   - **RTSP**: Set details for **Real Time Streaming Protocol** (RTSP) streaming. For more information, refer to the following.
5. Once all configurations are complete, click the **Apply** button at the bottom of the screen.

INFO

- You can also modify the information of multiple devices at once. Select two or more devices, then click **Batch Edit** in the upper right corner of the screen.



Device Batch Edit

Devices (2)

- OSDP Device Status: Active
- Use DHCP: □ Use DHCP
- Full Access: □ Full Access
- Time Zone
- Daylight Saving Time
- Suprema Smart Card: Disabled □ Classic/Plus □ DESFire, DESFire EV1/EV2/EV3 □ SR/SE □ SEOS
- Suprema Smart Card Layout: None
- Custom Smart Card: Disabled □ Classic/Plus □ DESFire, DESFire EV1/EV2/EV3 □ FeliCa Standard
- Custom Smart Card Layout: None
- Subnet Mask
- Gateway
- Auth Mode: + Add
- Store Face Image: Use
- Facility Code for Offline Mode: + Add, Delete

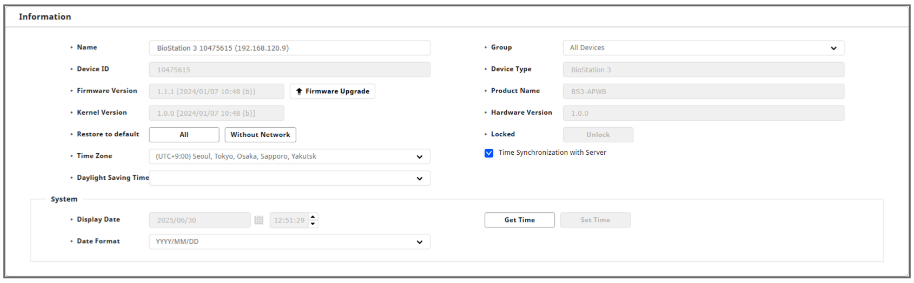
□	No	Facility Code

- Matching Timeout: 7 sec

- The details displayed in the **Device Batch Edit** window may vary depending on the selected device types.
- When selecting a master device and slave devices simultaneously for batch editing, only certain items within **Authentication** and **Display/Sound** can be modified.
- **Auth Mode** can only be batch edited when devices with the same model name are selected.

Basic Information Setting

The **Information** section allows you to set the basic information of the device. You can check the device's name and group, time zone, hardware, and firmware versions. You can change the device's name and group or upgrade the device's firmware.



Information

- Name: BioStation 3 10475615 (192.168.120.9)
- Device ID: 10475615
- Firmware Version: 1.1.1 [2024/01/07 10:48 (b)]
- Kernel Version: 1.0.0 [2024/01/07 10:48 (b)]
- Restore to default
- Time Zone: (UTC+9:00) Seoul, Tokyo, Osaka, Sapporo, Yakutsk
- Daylight Saving Time:
- Group: All Devices
- Device Type: BioStation 3
- Product Name: BS3-APWB
- Hardware Version: 1.0.0
- Locked
- ☑ Time Synchronization with Server

System

- Display Date: 2025/06/30 12:51:29
- Date Format: YYYY/MM/DD

Below are the default information settings for the device that cannot be modified by the user.

- **Device ID**: You can check the device ID.
- **Device Type**: You can check the type of device.
- **Product Name**: You can check the model name of the device.
- **Kernel Version**: You can check the device's kernel version.
- **Hardware Version**: You can check the hardware version of the device.

> **INFO**
>
> If the user has made any arbitrary changes, click the **Apply** button. Changes will not be applied to the device if not saved.

Change the device name

You can change the default device name. Enter your desired device name in the **Name** field. You can enter a device name up to 48 characters. The device name can be up to 48 characters long and is used to identify the device in the device list.

Change the device group

You can change the group to which the device belongs. Select the desired device group in the **Group** field.

> **INFO**
>
> For more information about creating a new device group, changing, or deleting group names, refer to the following.

Firmware upgrade

You can check the device's firmware version in the **Firmware Version** section. To upgrade the firmware, click the **Firmware Upgrade** button.

> **INFO**
>
> For more information about upgrading the device's firmware, refer to the following.

Set the device's date and time

You can set the device's date and time using the options below.

- **Time Zone**: You can select the standard time zone where the device is located.
- **Time Synchronization with Server**: You can synchronize the device's time information with the **BioStar X** server.
- **Daylight Saving Time**: You can apply the user's configured daylight saving time to the device. Refer to the following to add a new daylight saving time.
- **Display Date**: You can manually set the device's date and time. After setting both date and time, click the **Set Time** button.

  > This feature can be used when the **Time Synchronization with Server** option is not selected.

- **Date Format**: You can select the date format displayed on the device.
- **Get Time**: You can get the time set on the device.

> **CAUTION**
>
> The set date and time will be recorded in the event log and in real time. If the device's date and time are incorrect, log records may be inaccurate.

Unlock the device

When the device is locked due to operating conditions and actions, click the **Locked Unlock** button to unlock the device. You can unlock the device.

> **INFO**
>
> For more information on operating conditions and action settings, refer to the following.

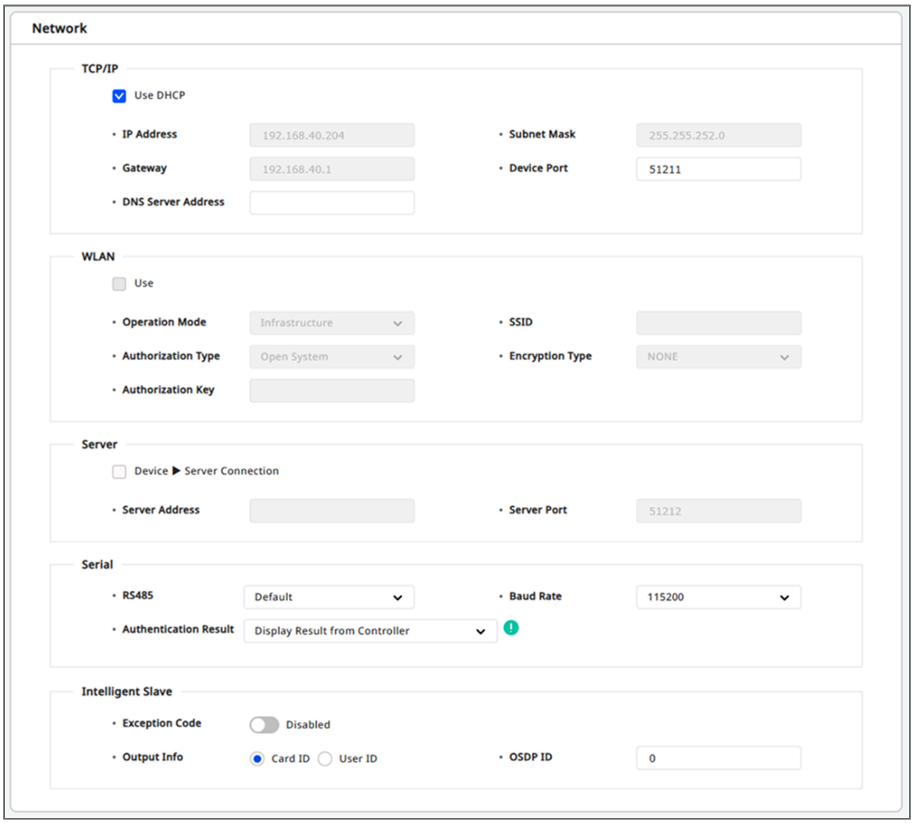
Initialize the device

To initialize the device settings, select one of the following features in the **Restore to default** field.

- **All**: Initializes all settings of the device.
- **Without Network**: Maintains network settings and initializes other settings.

Network Settings

Here are the network settings for the registered device. In the **Network** section, you can set the device's TCP/IP, RS-485, and server communication network.



Network

TCP/IP

☑ Use DHCP

- IP Address: 192.168.40.204
- Subnet Mask: 255.255.252.0
- Gateway: 192.168.40.1
- Device Port: 51211
- DNS Server Address:

WLAN

□ Use

- Operation Mode: Infrastructure
- SSID:
- Authorization Type: Open System
- Encryption Type: NONE
- Authorization Key:

Server

□ Device ▶ Server Connection

- Server Address:
- Server Port: 51212

Serial

- RS485: Default
- Baud Rate: 115200
- Authentication Result: Display Result from Controller

Intelligent Slave

- Exception Code: Disabled
- Output Info: ● Card ID ○ User ID
- OSDP ID: 0

INFO

- The available network options may differ depending on the device type.
- If the user has made any arbitrary changes, click the **Apply** button. Changes will not be applied to the device if not saved.

TCP/IP settings

In the **TCP/IP** group, you can set the device's IP address.

INFO

For more information about IP address settings during device registration, refer to the following.

Dynamic IP settings

To set the device to use dynamic IP, click the checkbox for the **Use DHCP** option. The device will automatically receive an IP address from the DHCP server, which may change. In this case, the IP address of the device may change.

Static IP settings

To set the device's IP address statically, uncheck the checkbox for the **Use DHCP** option. You can enter the device's network information in the details below.

- **OSDP ID**: Enter the OSDP address of the device. This should be a number between 0 and 126.
- **Subnet Mask**: Enter the device's subnet mask.
- **Gateway**: Enter the device's gateway address.
- **Device Port**: Enter the device's port number.
- **DNS Server Address**: Enter the device's DNS server address.

View devices and firmware versions that can accept DNS server addresses

- BioStation L2 firmware 1.0.0 or higher
- BioStation A2 firmware 1.0.0 or higher
- BioStation 2 firmware 1.2.0 or higher
- BioLite Net firmware 2.2.0 or higher
- BioEntry Plus firmware 2.2.0 or higher
- BioEntry W firmware 2.2.0 or higher
- XPass firmware 2.2.0 or higher
- XPass S2 firmware 2.2.0 or higher
- FaceStation 2 firmware 1.0.0 or higher
- BioLite N2 firmware 1.0.0 or higher
- FaceLite firmware 1.0.0 or higher
- XPass 2 firmware 1.0.0 or higher
- FaceStation F2 firmware 1.0.0 or higher
- X-Station 2 firmware 1.0.0 or higher
- BioStation 3 firmware 1.0.0 or higher
- BioEntry W3 firmware version 1.0.0 or higher

Wireless LAN settings

In the **WLAN** group, you can enable or disable the device's wireless LAN settings. Detailed settings are available in the device's user guide.

> **INFO**
>
> Refer to the following devices that support wireless LAN settings:
>
> - BioStation 2
> - BioStation A2
> - FaceStation 2
> - BioStation 3

Server communication settings

In the **Server** group, you can configure how the device communicates with the **BioStar X** server.

- **Device ▶ Server Connection**: Selecting this option allows you to enter the IP address and port number of the **BioStar X** server the device will connect to.
- **Server Address**: Enter the IP address or domain name of the **BioStar X** server.
- **Server Port**: Enter the port number of the **BioStar X** server.

> **TIP**
>
> This feature is useful when the IP address of the **BioStar X** server changes. By pre-configuring this option on multiple devices before changing the server's IP address, the devices will automatically connect to the updated IP address.

View devices and firmware versions that allow entering domain names in **Server Address**

- BioStation L2 firmware 1.0.0 or higher
- BioStation A2 firmware 1.0.0 or higher
- BioStation 2 firmware 1.2.0 or higher
- BioEntry W2 firmware 1.0.0 or higher
- BioEntry P2 firmware 1.0.0 or higher
- FaceStation 2 firmware 1.0.0 or higher
- FaceLite firmware 1.0.0 or higher
- FaceStation F2 firmware 1.0.0 or higher
- BioLite N2 firmware 1.0.0 or higher
- BioLite Net firmware 2.2.0 or higher
- BioEntry Plus firmware 2.2.0 or higher
- BioEntry W firmware 2.2.0 or higher
- XPass firmware 2.2.0 or higher
- XPass S2 firmware 2.2.0 or higher
- XPass 2 firmware 1.0.0 or higher
- X-Station 2 firmware 1.0.0 or higher
- BioStation 3 firmware 1.0.0 or higher
- BioEntry W3 firmware version 1.0.0 or higher

Serial communication settings

In the **Serial** group, you can set the mode, transmission performance, and display authentication results for devices connected via RS-485.

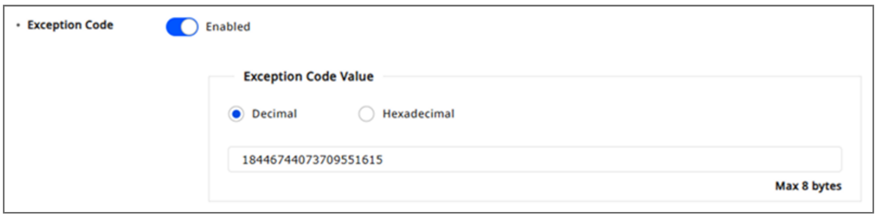
- **RS485**: Set the RS-485 mode.
- **Baud Rate**: Set the RS-485 communication performance.
- **Authentication Result**: Choose the authentication result to display on the device's screen when using the device with a third-party controller.
  - **Display Result from Controller**: You can display the authentication result from the third-party controller on the device.
  - **Display Device Matching Result**: You can display the device's authentication result.

> **INFO**
>
> The **Authentication Result** option is enabled when the **RS485** option is set to **Slave** or **Default**.

Intelligent slave settings

In the **Intelligent Slave** group, when a user authenticates using a fingerprint in an environment where Suprema devices are connected to third-party controllers, the authentication result is sent as Open Supervised Device Protocol (OSDP) card data to support numerous 1:1 or 1:N matching.

- **Exception Code**: When using the intelligent slave, if an exception occurs such as authentication failure, enter the exception code in decimal (0-18446744073709551615) or hexadecimal (0-FFFFFFFFFFFFFFFF) format to record an accurate log. Hexadecimal can be input using numbers or letters.



- Exception Code Enabled

Exception Code Value

● Decimal ○ Hexadecimal

18446744073709551615

Max 8 bytes

- **Output Info**: You can output the card ID or user ID upon successful authentication.
- **OSDP ID**: Enter the OSDP address of the device. This should be a number between 0 and 126.

> **INFO**
>
> - You can input data of up to 8 bytes for **Exception Code**.
> - The **Intelligent Slave** option is enabled when the **RS485** option is set to **Default**.

View devices and firmware versions that support the **Intelligent Slave** option

- BioEntry W2 firmware 1.6.3 or higher
- BioStation L2 firmware 1.6.1 or higher
- BioEntry P2 firmware 1.4.1 or higher
- XPass 2 firmware 1.2.3 or higher
- X-Station 2 firmware 1.1.0 or higher
- BioLite N2 firmware 1.4.1 or higher
- FaceStation F2 firmware 1.1.2 or higher
- BioStation 3 firmware 1.0.0 or higher
- BioEntry W3 firmware version 1.0.0 or higher

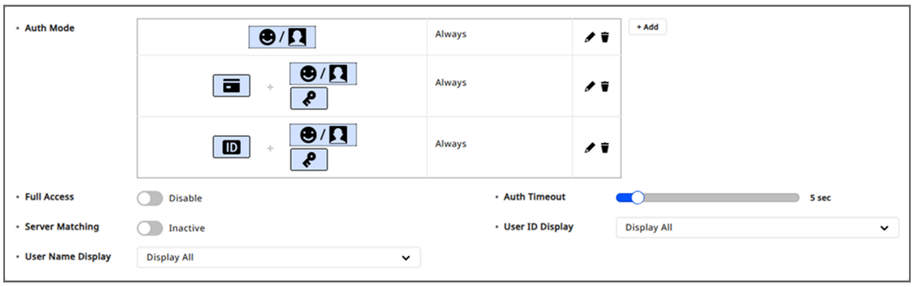
Authentication Settings

Instructions for various settings related to user authentication on the device are provided. **Authentication** section provides step-by-step information on authentication methods and key authentication options supported by the device. Note that changes to settings will be applied to the actual device, and configure the authentication policy according to your environment by referring to the features and precautions of each option.

> **INFO**
>
> - The available network options may differ depending on the device type.
> - If the user has made any arbitrary changes, click the **Apply** button. Changes will not be applied to the device if not saved.

Authentication method settings

You can set the device's authentication mode, permissions, server matching, and authentication timeout.



- Auth Mode: Always; Always; Always
- Full Access: Disable
- Server Matching: Inactive
- User Name Display: Display All
- Auth Timeout: 5 sec
- User ID Display: Display All

- **Auth Mode**: Set the authentication mode of the device by combining one or more credentials. For more information, refer to the following.
  - Click the ✎ button to modify the added authentication mode.
  - Click the 🗑 button to delete the added authentication mode.
- **Full Access**: Users registered on the device can be granted all access permissions without defining access group settings.

  > **INFO**
  >
  > When this option is set to **Use**, the device cannot be registered in **Access Level** and **Floor Level**.

- **Auth Timeout**: This is the timeout for authenticating the second credential when multiple credentials are used in **Auth Mode** option. If the credential is not authenticated within the specified time, authentication will fail.
- **Server Matching**
  - **Active**: Activates server matching. Configure the server matching feature to authenticate using user information stored on the server where **BioStar X** is installed.
  - **Inactive**: Deactivates server matching. In this case, authentication is performed using the user information

registered on the device.

View devices and firmware versions supporting **Server Matching** feature

- CoreStation firmware version 1.0.0 or higher
- BioEntry P2 firmware 1.0.0 or higher
- BioEntry W2 firmware 1.0.0 or higher
- BioStation L2 firmware 1.0.0 or higher
- BioStation A2 firmware 1.0.0 or higher
- BioStation 2 firmware 1.2.0 or higher
- BioLite Net firmware 2.2.0 or higher
- BioEntry Plus firmware 2.2.0 or higher
- BioEntry W firmware 2.2.0 or higher
- XPass firmware 2.2.0 or higher
- XPass S2 firmware 2.2.0 or higher
- BioLite N2 firmware 1.0.0 or higher
- XPass D2 firmware version 1.0.0 or higher
- XPass 2 firmware 1.0.0 or higher
- FaceStation 2 firmware version 1.4.0 or higher
- FaceStation F2 firmware 1.0.0 or higher
- X-Station 2 firmware 1.0.0 or higher
- BioStation 3 firmware 1.0.0 or higher
- BioEntry W3 firmware version 1.0.0 or higher
- FaceLite does not support server matching feature.
- FaceStation F2, BioStation 3, BioEntry W3 devices cannot use server matching for facial authentication.

- **Face Detection Level**: Set the algorithm steps for recognizing faces using the built-in camera when the user authenticates.
  - **Normal**: Detects faces at a distance equivalent to the length of a person's arm.
  - **High**: Requires the user to be closer than the length of a person's arm to detect a face.
  - **Not Use**: Does not use facial recognition functionality.

> ⓘ **INFO**
>
> This option is supported on the BioStation A2.

- **User ID Display**: Control whether to display or hide the user ID shown on the device when authentication is successful.

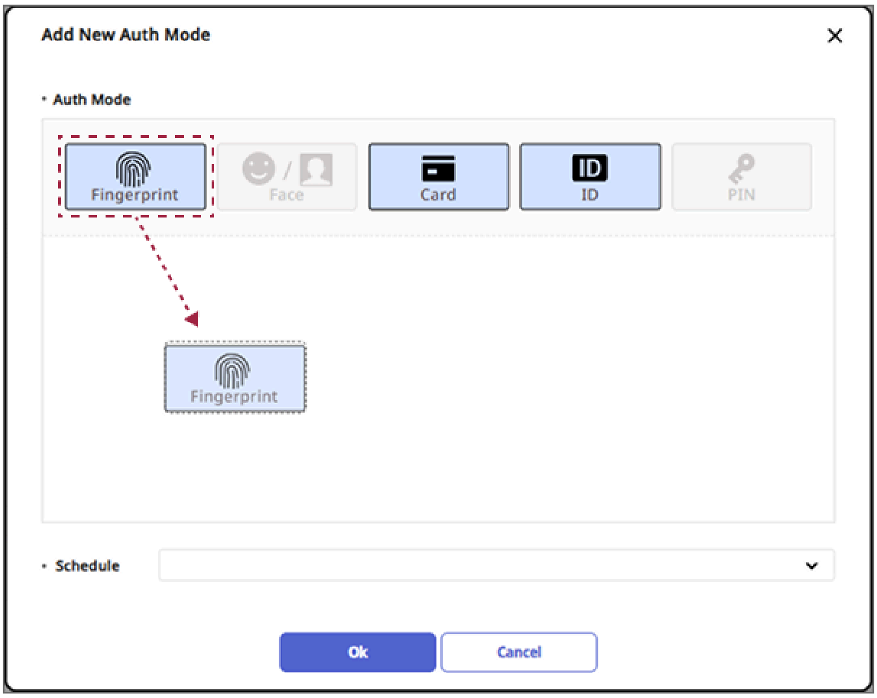
  - **Display All** / **Mask All but First Letter** / **Hide All**

- **User Name Display**: Control whether to display or hide the user name shown on the device when authentication is successful.
  - **Display All** / **Mask All but First Letter** / **Hide All**

Add authentication mode

Set the device's authentication mode in the **Auth Mode** option. You can configure the authentication mode by combining credentials such as fingerprint, ID, card, PIN, and face.

1. In the **Auth Mode** option, click the + **Add** button.
2. When the **Add New Auth Mode** window appears, drag the desired authentication mode to the center area.



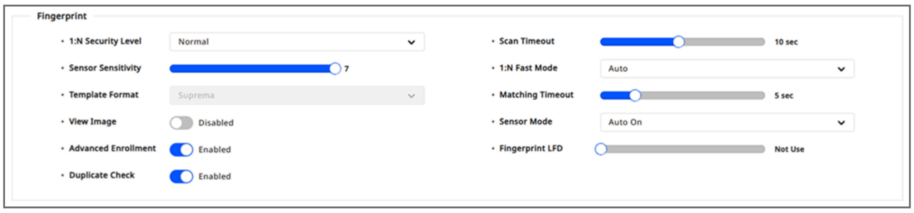
   You can add up to five desired authentication modes.

3. Select the desired item in the **Schedule** option.
4. Once all settings are completed, click the **Apply** button.

> **INFO**
>
> If the desired schedule is not available in the **Schedule** option, click + **Add New Schedule** to add a new schedule. You can add a new schedule. For more information about schedule settings, refer to the following.

Fingerprint authentication settings

In the **Fingerprint** group, you can configure details related to the device's fingerprint authentication.



Fingerprint

- 1:N Security Level: Normal
- Sensor Sensitivity: 7
- Template Format: Suprema
- View Image: Disabled
- Advanced Enrollment: Enabled
- Duplicate Check: Enabled
- Scan Timeout: 10 sec
- 1:N Fast Mode: Auto
- Matching Timeout: 5 sec
- Sensor Mode: Auto On
- Fingerprint LFD: Not Use

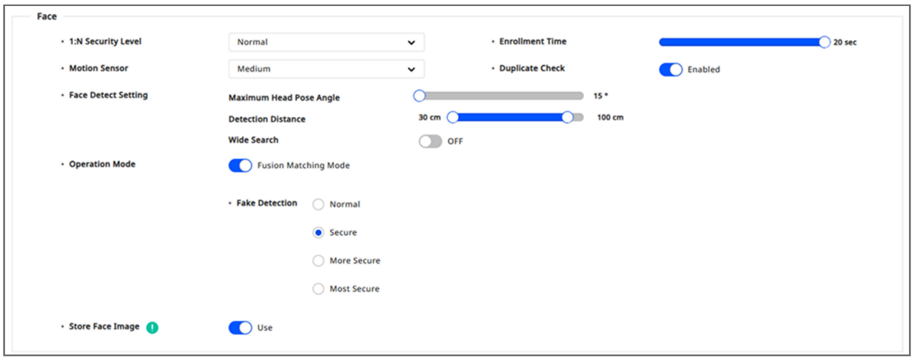
- **1:N Security Level**: Set the security level used for authenticating fingerprints. Higher security levels increase the False Rejection Rate (FRR) but decrease the False Acceptance Rate (FAR).
- **Scan Timeout**: Set the timeout for fingerprint scanning. Failure to scan within the time set will result in authentication failure.
- **Sensor Sensitivity**: Set the sensitivity of the fingerprint recognition sensor. Set the sensitivity higher to obtain precise fingerprint information.
- **1:N Fast Mode**: Set the speed of fingerprint authentication. When **Automatic** is selected, it sets the authentication performance according to the total fingerprint templates registered on the device.
- **Template Format**: View the configured fingerprint template format.
- **Matching Timeout**: Set the timeout for fingerprint matching. If authentication is not completed within the specified time, it will fail.
- **View Image**: Display fingerprint images on the screen during authentication.
- **Sensor Mode**: Set the operating mode of the fingerprint sensor.
  - **Auto On**: The fingerprint sensor turns on by recognizing the user's finger.
  - **Always On**: The fingerprint sensor remains always on.
- **Advanced Enrollment**: Assess the quality of scanned fingerprints to save high-quality fingerprint information. Set to **Use** to notify the user if the fingerprint quality is low, helping to scan fingerprints correctly.
- **Fingerprint LFD**: Set the level for fake fingerprint detection. Higher levels for fake fingerprint detection may also increase rejection rates for actual people’s fingerprints.
- **Duplicate Check**: Check for duplicate registrations when enrolling fingerprints.

ⓘ **INFO**

- The options available for configuration may vary depending on the type of device.
- Changing the **Template Format** option in fingerprint authentication settings will render all previously stored fingerprints unusable. Make sure to select a template in the **Template Format** option before enrolling users' fingerprints.
- The **View Image** option is supported on BioStation 2, BioStation A2, BioStation L2, BioLite N2, FaceStation F2 (FSF2-ODB), and X-Station 2 (XS2-ODPB, XS2-OAPB) models.
- The **Fingerprint LFD** option is supported on BioStation A2, BioStation L2, BioEntry W2, BioLite N2, FaceStation F2 (FSF2-ODB), and X-Station 2 (XS2-ODPB, XS2-OAPB) models.

Facial authentication settings

In the **Face** group, you can configure details related to the device's facial authentication.



Face

- 1:N Security Level: Normal
- Motion Sensor: Medium
- Face Detect Setting
  - Maximum Head Pose Angle: 15 °
  - Detection Distance: 30 cm – 100 cm
  - Wide Search: OFF
- Operation Mode: Fusion Matching Mode
  - Fake Detection: ○ Normal ● Secure ○ More Secure ○ Most Secure
- Store Face Image: Use
- Enrollment Time: 20 sec
- Duplicate Check: Enabled

- **1:N Security Level**: Set the security level used for authenticating faces. Higher security levels increase the False Rejection Rate (FRR) but decrease the False Acceptance Rate (FAR).
- **Enrollment Time**: If the user's face is not enrolled within the set time when registering, the face enrollment will be canceled.
- **Motion Sensor**: Set the sensitivity for detecting movement around the device.
- **Ambient Brightness**: The device can detect ambient brightness and adjust the intensity of the IR LED.
- **Enhanced fake face enrollment block**: Set the level for fake face detection. Increasing the level for detecting fake face registrations may heighten the rejection rates for actual faces.
- **Light Brightness**: Manually adjust the brightness of the device's light. Set brightness by choosing **Normal** or **High**, or select **Not Use** to turn off the light.
- **Quick Enrollment**: Set whether to enable quick face enrollment.
  - **Enable**: Configures the face enrollment procedure to one step.
  - **Disabled**: Sets the face enrollment procedure to 3 steps. Set to **Disabled** for high-quality face template enrollment.
- **Duplicate Check**: Check for duplicate registrations when enrolling faces.
- **Face Detect Setting**: Configure the environmental settings for recognizing the user's face during

authentication.

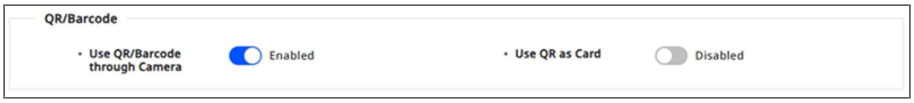
- **Maximum Head Pose Angle**: Set the maximum rotation angle permitted for the face.
- **Detection Distance**: Set the minimum and maximum distances for recognizing the face.
- **Wide Search**: Set to **ON** to allow facial recognition across the entire camera view.

- **Operation Mode**: Set the operation mode of the device during facial authentication.
  - **Fusion Matching Mode**: Perform both visual and infrared matching to enhance the accuracy of facial authentication.
  - **Fast Matching Mode**: Allows for rapid authentication of users walking within the device's authentication range.
- **Fake Detection**: Prevent user authentication using fake faces such as photos. This is activated when the **Operation Mode** option is set to **Fusion Matching Mode**.

> **INFO**
>
> - The options available for configuration may vary depending on the type of device.
> - The **Ambient Brightness**, **Enhanced fake face enrollment block**, and **Quick Enrollment** options are supported in the FaceStation 2 and FaceLite models.
> - The **Light Brightness** option is supported on FaceStation F2 firmware version 1.1.0 or higher.
> - The **Face Detect Setting** and **Operation Mode** options are supported in FaceStation F2 and BioStation 3 models.

QR/Barcode settings

In the **QR/Barcode** group, you can configure details for QR/barcode authentication on the device.



QR/Barcode

- Use QR/Barcode through Camera: Enabled
- Use QR as Card: Disabled

- **Use QR/Barcode through Camera**: Set whether to use QR/barcode authentication through the device's camera.
- **Camera Timeout**: Set the camera scan timeout. If a QR/barcode is not scanned within the specified time, authentication will fail.
- **Use QR as Card**: Set to authenticate QR codes with the same data as CSN cards or Wiegand cards issued to users.
- **Motion Sensor**: Set the sensitivity for detecting movement to initiate camera scanning.
- **Use QR/Barcode through Scanner**: Set whether to use the device's scanner for QR/barcode authentication.
- **Scanner Timeout**: Set the scanning timeout. If a QR/barcode is not scanned within the specified time, authentication will fail.

INFO

- The **Use QR/Barcode through Camera** option requires a separate device license. For more information, refer to the following.
- The devices supporting **Use QR/Barcode through Camera**, **Camera Timeout**, **Use QR as Card**, and **Motion Sensor** options are as follows.
  - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) firmware version 1.2.0 or higher
  - BioStation 3 (BS3-DB, BS3-APWB) firmware version 1.1.0 or higher
- The devices supporting **Use QR/Barcode through Scanner** and **Scanner Timeout** options are as follows.
  - X-Station 2 (XS2-QDPB, XS2-QAPB)

Card authentication settings

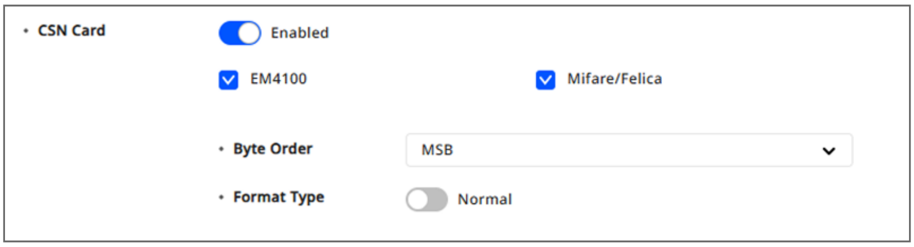
In the **Card Type** group, you can set the types of cards to be used on the device.

INFO

Only card types supported by the device will be displayed in the **Card Type** group.

CSN Card

You can select the types of CSN cards and formats and set the byte order.

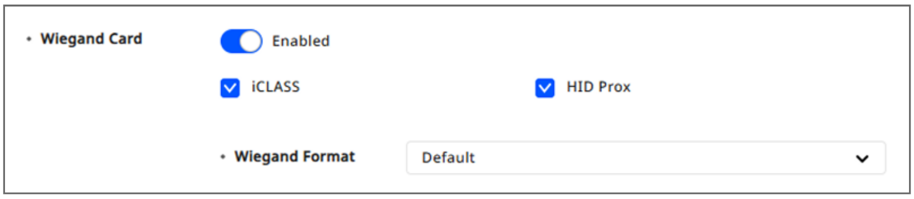


- CSN Card: Enabled
  - ☑ EM4100 ☑ Mifare/Felica
  - Byte Order: MSB
  - Format Type: Normal

- **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).
- **Format Type**
  - **General**: Reads and expresses the card's serial number (CSN) without separate conversion.
  - **Wiegand**: Transforms and expresses the card's serial number (CSN) according to user-defined Wiegand format. For information about how to set a new Wiegand format, refer to the following.

Wiegand Card

Select the types of Wiegand cards and set the Wiegand formats. Choose the Wiegand format to be used in the **Wiegand Format** option.



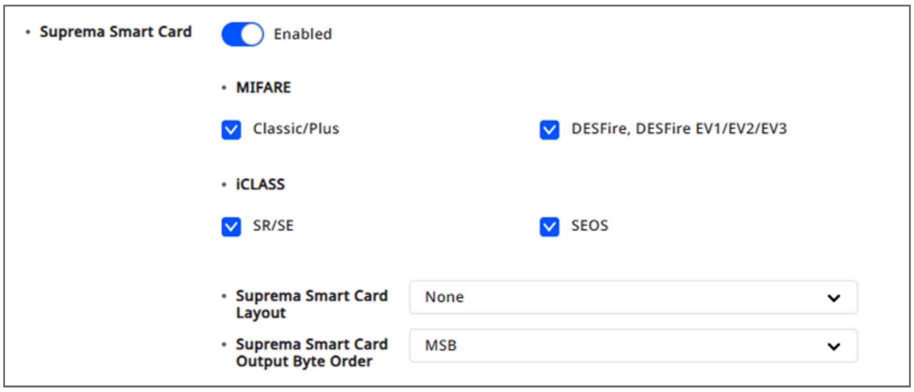
- Wiegand Card: Enabled
  - ☑ iCLASS
  - ☑ HID Prox
  - Wiegand Format: Default

INFO

For information about how to set a new Wiegand format, refer to the following.

Suprema Smart Card

Select the types of Suprema smart cards and set the card layout and byte order.

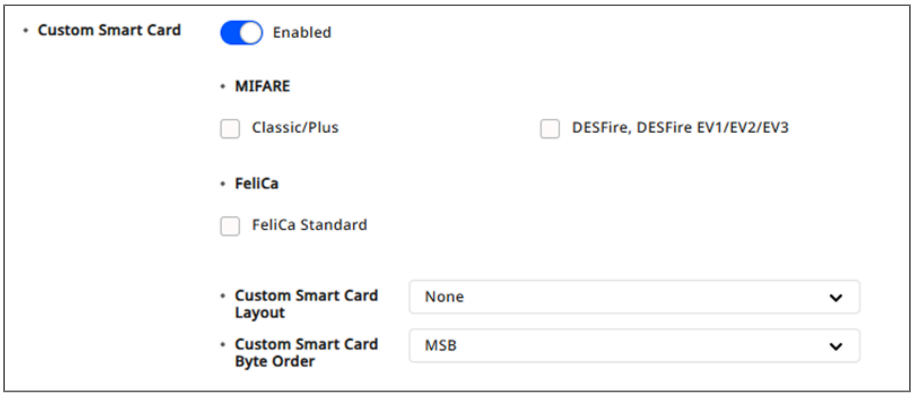


- Suprema Smart Card: Enabled
  - MIFARE
    - ☑ Classic/Plus
    - ☑ DESFire, DESFire EV1/EV2/EV3
  - iCLASS
    - ☑ SR/SE
    - ☑ SEOS
  - Suprema Smart Card Layout: None
  - Suprema Smart Card Output Byte Order: MSB

- **Suprema Smart Card Layout**: Choose the Suprema smart card layout. For information about how to set a new smart card layout, refer to the following.
- **Suprema Smart Card Output Byte Order**
  - **MSB**: Processes card data in order from large byte units to small byte units.
  - **LSB**: Processes card data in order from small byte units to large byte units.

Custom Smart Card

Select types of custom smart cards issued by third parties and set the card layout and byte order.



- Custom Smart Card ● Enabled
- MIFARE
  □ Classic/Plus □ DESFire, DESFire EV1/EV2/EV3
- FeliCa
  □ FeliCa Standard
- Custom Smart Card Layout: None
- Custom Smart Card Byte Order: MSB

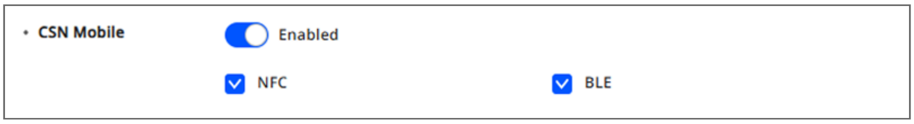
- **Custom Smart Card Layout**: Choose the custom smart card layout. For information about how to set a new smart card layout, refer to the following.
- **Custom Smart Card Byte Order**
  - **MSB**: Processes card data in order from large byte units to small byte units.
  - **LSB**: Processes card data in order from small byte units to large byte units.

View devices and firmware versions supporting custom smart cards

- XPass D2 firmware version 1.7.1 or higher
- BioEntry P2 firmware version 1.5.1 or higher
- BioEntry W2 firmware version 1.8.0 or higher
- BioStation 2a firmware version 1.1.0 or higher
- X-Station 2 firmware version 1.3.0 or higher
- BioStation 3 firmware version 1.3.0 or higher
- BioEntry W3 firmware version 1.0.0 or higher
- BioLite N2 firmware version 1.6.2 or higher

CSN Mobile

You can set the method for recognizing mobile cards.

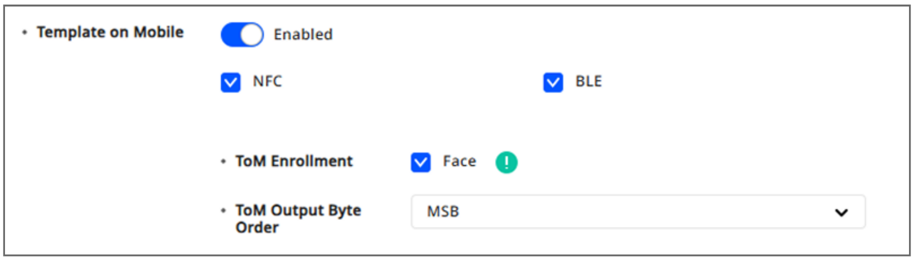


- CSN Mobile ● Enabled
  ☑ NFC ☑ BLE

- **NFC**: Recognizes mobile cards through NFC communication from mobile devices.
- **BLE**: Recognizes mobile cards through Bluetooth Low Energy (BLE) communication.

Template on Mobile

You can specify how recognition works on the Template on Mobile and set the byte order for biometrics enrolled directly by the user on the device.



- Template on Mobile: Enabled
  ☑ NFC ☑ BLE
  - ToM Enrollment: ☑ Face
  - ToM Output Byte Order: MSB

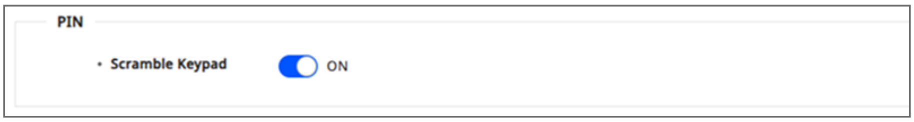
- **ToM Output Byte Order**
  - **MSB**: Processes card data in order from large byte units to small byte units.
  - **LSB**: Processes card data in order from small byte units to large byte units.

View devices and firmware versions supporting templates on mobile

- BioStation 3 firmware version 1.2.0 or higher
- BioEntry W3 firmware version 1.0.0 or higher

PIN authentication settings

In the **PIN** group, you can turn the **Scramble Keypad** option on or off for the device's PIN authentication.



PIN
- Scramble Keypad: ON

> **INFO**
>
> The **Scramble Keypad** option is only available on Suprema products that support user interfaces through the LCD screen.

Advanced Settings

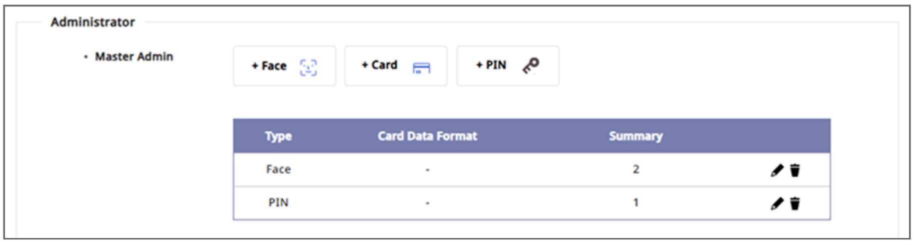
This section provides guidance on configuring items in the **Advanced** settings. You can check how to configure various advanced features such as Master Administrator, administrator permission management, attendance events, screen and sound, operating conditions and actions, image logs, Wiegand, security tamper, and the meaning of each option. Apply settings suitable for your environment to effectively manage the device.

> **INFO**
>
> - The available network options may differ depending on the device type.
> - If the user has made any arbitrary changes, click the **Apply** button. Changes will not be applied to the device if not saved.

Add master administrator

Master Admin feature enhances the overall administrator permissions of the device to improve security and prevent unauthorized access and settings changes. A new device must register a Master Administrator through this feature, and only the registered Master Administrator can enter the administrator menu and change settings.

Select two types of desired credentials to enroll from the **Advanced** → **Administrator Master Admin** menu.



Type	Card Data Format	Summary	
Face	-	2	✎ 🗑
PIN	-	1	✎ 🗑

The credentials that can be enrolled as **Master Admin** are as follows:

Credential Type	Number of Enrollments	Conditions
card	Up to 4	Supports only CSN and Wiegand types, and cannot enrollmnet duplicates of the same type.
Face	Up to 2	Can only enroll on devices equipped with the same algorithm.
Fingerprint	Up to 2	*
PIN	1	Must enter at least 8 digits.

- To change the enrolled credential, click the ✎ button to the right of that credential.
- To delete the enrolled credential, click the 🗑 button to the right of that credential.

Enrollment conditions

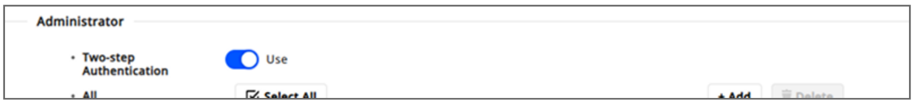
- You must enroll at least two types of credentials.
- The same conditions apply to both new devices and firmware upgrade devices.
- All credentials supported by the device can be used as authentication means.

INFO

- This feature is only available on Suprema products that support user interfaces via LCD screens.
- Existing devices that have been upgraded will not show the **Master Admin** menu in BioStar 2's device settings.
- Existing devices that have been upgraded do not provide **Master Admin** settings, however, you can enhance the overall administrator permissions to improve device security using the **Two-step Authentication** option. For more information about how to set **Two-step Authentication**, refer to the following.
- For more information about devices and firmware versions that support this feature, refer to the following.

Two-step authentication setting

Existing devices that have been upgraded do not provide **Master Admin** settings, however, you can enhance the overall administrator permissions to improve device security using the **Two-step Authentication** option.



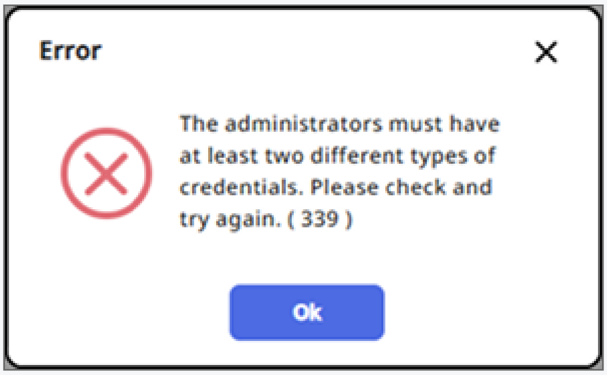
Administrator

- Two-step Authentication: Use
- All

If you set the **Two-step Authentication** option to **Use**, you must use two or more credentials for overall administrator authentication on the device. For example, if both a card and PIN are enrolled, you must scan the card and enter the PIN to authenticate successfully during overall administrator authentication.

ⓘ **INFO**

If there are not two types of credentials enrolled for all administrators, activation fails and an error message is displayed. Enroll two types of credentials for all administrators and try again.

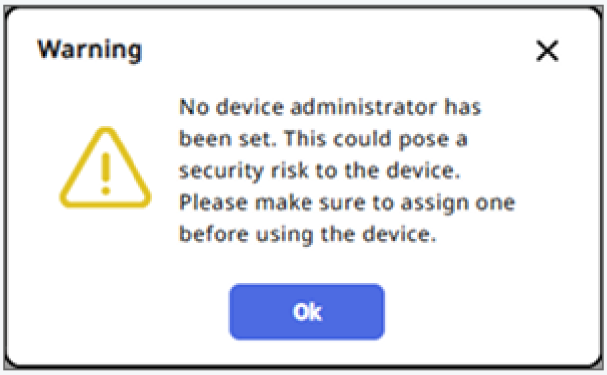


Error

The administrators must have at least two different types of credentials. Please check and try again. (339)

⚠ **CAUTION**

If the overall administrator is not set on the device, the following popup message will appear. Add administrators for all permissions in **Advanced** → **Administrator**.



Warning

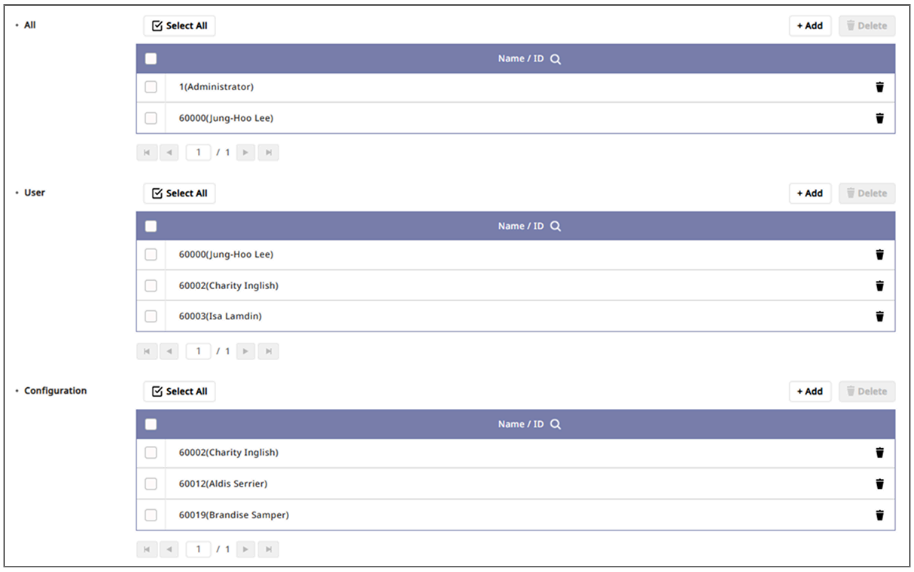
No device administrator has been set. This could pose a security risk to the device. Please make sure to assign one before using the device.

⚠ **WARNING**

If you activate **Two-step Authentication** and then delete all administrators' credentials to less than two types, you will not be able to access the administrator menu on the device when unable to connect to **BioStar X**. Therefore, you need to be particularly careful when deleting administrator credentials.

Add administrators

In the **Administrator** group, you can manage the device's administrators by permission level.



- All

☑ Select All + Add 🗑 Delete

□	Name / ID 🔍	
□	1(Administrator)	🗑
□	60000(Jung-Hoo Lee)	🗑

1 / 1

- User

☑ Select All + Add 🗑 Delete

□	Name / ID 🔍	
□	60000(Jung-Hoo Lee)	🗑
□	60002(Charity Inglish)	🗑
□	60003(Isa Lamdin)	🗑

1 / 1

- Configuration

☑ Select All + Add 🗑 Delete

□	Name / ID 🔍	
□	60002(Charity Inglish)	🗑
□	60012(Aldis Serrier)	🗑
□	60019(Brandise Samper)	🗑

1 / 1

To add an administrator by permission level, click the **+ Add** button. When the user list appears, select the desired user. You can also search for the desired user by clicking the 🔍 button in the user list.

Refer to the permissions for each level below.

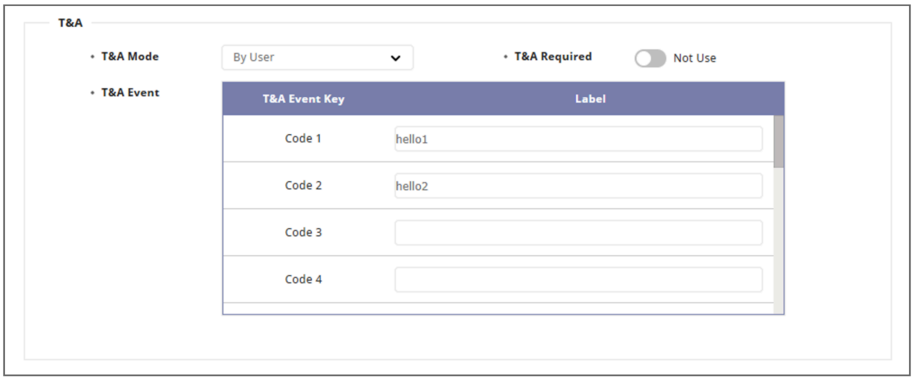
Level	User Information Management	Device Settings
All	✓	✓
User	✓	✗
Configuration	✗	✓

ⓘ **INFO**

- Up to 1,000 administrators can be added. The number of administrators that can be added may vary depending on the device firmware version.
- To search for the registered user, click the 🔍 button in **Name / ID**.
- **Device Settings** allows changes to settings for screen and sound, network, RS-485, etc.
- To delete an administrator, click the 🗑 button to the right of the administrator.
- Administrators set for each device do not affect **BioStar X** permissions.

Attendance management

The **T&A** group allows you to change attendance event names or set attendance modes.



T&A

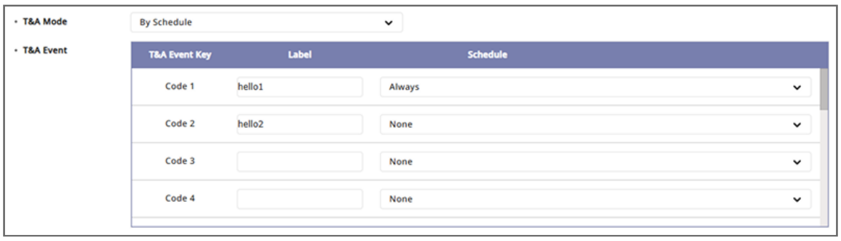
- T&A Mode: By User
- T&A Required: Not Use
- T&A Event

T&A Event Key	Label
Code 1	hello1
Code 2	hello2
Code 3	
Code 4	

- **T&A Mode**: Set how attendance events are registered.
  - **Not Use**: Attendance events cannot be recorded.
  - **By User**: The user can select the desired attendance event when authenticating.
  - **By Schedule**: Attendance events automatically change according to a set schedule. You can select a schedule to apply to attendance events.
  - **Last Choice**: The last used attendance event can continue to be used.
  - **Fixed**: Only the selected attendance event can be used. Choose the fixed attendance event to use.
- **T&A Required**: Set it to require the user to register an attendance event when authenticating.

> This option can be used when the **T&A Mode** option is set to **By User**.

- **T&A Event**: You can modify the names of attendance events or add schedules used when the **T&A Mode** option is set to **By Schedule**.
  - **T&A Event Key**: This is a list of keys that can be used to register attendance.
  - **Label**: You can change the name of the attendance event based on **T&A Event Key**.
  - **Schedule**: You can set a schedule for automatic changes when the **T&A Mode** option is set to **By Schedule**.



- T&A Mode: By Schedule
- T&A Event

T&A Event Key	Label	Schedule
Code 1	hello1	Always
Code 2	hello2	None
Code 3		None
Code 4		None

> **INFO**
>
> - Devices without an LCD screen can set attendance modes to **Fixed** and **By Schedule** and can register fixed attendance events or attendance events that change according to a pre-set schedule. The supported devices are BioEntry P2, BioEntry W2, XPass D2, XPass 2.
> - For more information about setting new schedules, refer to the following.

Screen and sound settings

You can change settings related to the device's screen and sound. Available options may vary depending on the device.

BioEntry P2, BioEntry W2, XPass D2, XPass 2

- **Sound**: You can turn the sound on or off.
- **LED/Buzzer**: Select and set the event items that will activate the LED or buzzer.
- **Keypad Backlight**: You can turn the keypad backlight on or off. When this option is activated, the light behind the keypad turns on, making it easier to identify keys in dark environments. You can easily identify keys even in dark environments.

> ⓘ The **Keypad Backlight** option is available on XPass D2 hardware V02M and firmware version 1.7.1 or higher.

BioStation 2, BioStation L2, BioLite N2, FaceLite

- **Language**: Set the language to be displayed on the device's screen. Click the **Update Resource** button to send language resource files to the device.
- **Device Volume**: Set the default sound level produced by the device.
- **Menu Timeout**: Set the time it takes to switch from the menu screen to the idle screen.
- **Theme**: Change the style of the home screen of the device.
- **Backlight Timeout**: Set the time before the screen light automatically turns off.
- **Message Timeout**: Set the time before messages automatically disappear.
- **Voice Instruction**: You can use voice guidance instead of notification tones.
- **Background**: Set items to be displayed in the device's home screen background.
  - **Logo**: Users can display images they registered on the device's home screen. Click the **Add** button to register an image.
  - **Notice**: Administrators can display their input on the home screen.
  - **Slide Show**: Users can display up to 10 registered images as a slideshow on the home screen. Click the **Add** button to register an image.

> ⓘ
> - To reflect changes in real time on the device, click the **Update** button.
> - If you change the type of background wallpaper, clicking the **Update** button will not apply it to the device. At the bottom of the screen, click the **Apply** button.
> - The options **Notice** and **Slide Show** are supported by the BioStation 2 model.

- **Sound**: Set sound effects to play upon starting, successful authentication, and authentication failure events. Select **.wav* files up to 500Kb in file size. Click the **Browse** button.

> ⓘ To reflect changes in real time on the device, click the **Update** button.

BioStation 3, BioStation A2, FaceStation 2, FaceStation F2, X-Station 2

- **Language**: Set the language to be displayed on the device's screen. Click the **Update Resource** button to send language resource files to the device.
- **Device Volume**: Set the default sound level produced by the device.
- **Intercom Speaker Volume**: Set the volume of sound output from the device when using the IP intercom feature.
- **Intercom Microphone Volume**: Set the volume of sound input into the device when using the IP intercom feature.
- **Menu Timeout**: Set the time it takes to switch from the menu screen to the idle screen.
- **Backlight Timeout**: Set the time before the screen light automatically turns off.
- **Message Timeout**: Set the time before messages automatically disappear.
- **Server Private Message**: Set whether to use a private message that will be displayed on the screen when the user authenticates.
- **Screensaver**: Reduces unnecessary power consumption by reducing LCD screen brightness when the device is not in use. If this feature is not enabled, even if the **Screensaver** option is enabled on the device, authentication success messages will not be displayed.

  > ⓘ This option is supported by the FaceStation 2, FaceStation F2, X-Station 2, and BioStation 3 models.

- **Voice Instruction**: You can use voice guidance instead of notification tones.
- **Home Screen**: Set items to be displayed in the device's home screen background.
  - **Normal**: Displays the default image on the home screen.
  - **Logo**: Users can display images they registered on the device's home screen. Click the **Add** button to register an image.
  - **Notice**: Administrators can display their input on the home screen.

  > ⓘ
  > - To reflect changes in real time on the device, click the **Update** button.
  > - If you change the type of background wallpaper, clicking the **Update** button will not apply it to the device. At the bottom of the screen, click the **Apply** button.
  > - Setting the home screen as **Logo** and **Slide Show** allows displaying up to 10 images as a slideshow on the home screen. Click the **Add** button to register an image.

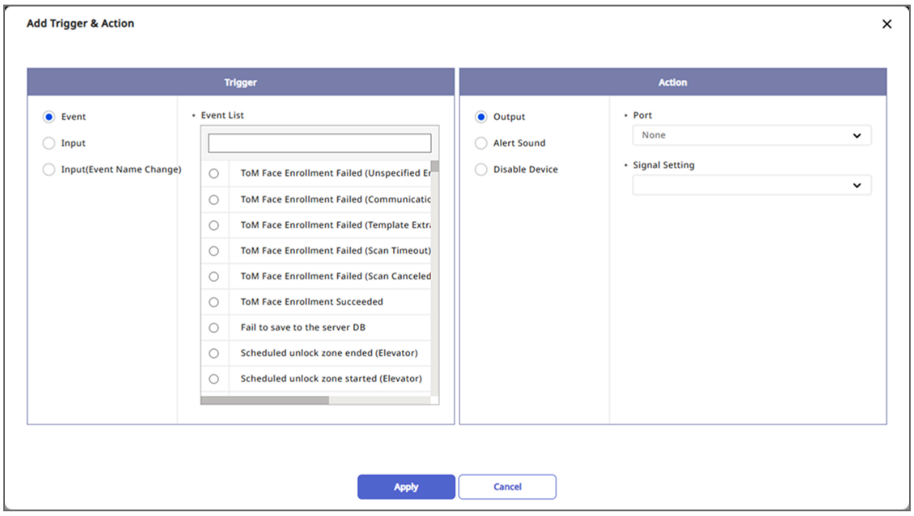
- **Sound**: Set sound effects to play upon starting, successful authentication, and authentication failure events. Select **.wav* files up to 500Kb in file size. Click the **Browse** button.

  > ⓘ To reflect changes in real time on the device, click the **Update** button.

Trigger conditions and actions settings

In the **Trigger & Action** group, you can set action conditions and actions based on specific situations. For example, you can configure all alarms to sound when authentication fails or the device becomes unusable if the RS-485 connection is lost.

You can register events by selecting them for action conditions and actions or set conditions and actions according to user preferences. Click the **Trigger & Action** group and then click the + **Add** button on the right.


Add Trigger & Action
×
Trigger
● Event
○ Input
○ Input(Event Name Change)
• Event List
○ ToM Face Enrollment Failed (Unspecified Er
○ ToM Face Enrollment Failed (Communicatic
○ ToM Face Enrollment Failed (Template Extr
○ ToM Face Enrollment Failed (Scan Timeout)
○ ToM Face Enrollment Failed (Scan Canceled
○ ToM Face Enrollment Succeeded
○ Fail to save to the server DB
○ Scheduled unlock zone ended (Elevator)
○ Scheduled unlock zone started (Elevator)
Action
● Output
○ Alert Sound
○ Disable Device
• Port
None
• Signal Setting
Apply
Cancel

Trigger

You can select predefined events or add custom conditions.

- **Event**: Select a predefined event.
- **Input**: Set custom conditions by selecting each item within the option.
- **Input(Event Name Change)**: Set custom conditions by selecting each item within the option. You can configure it to only detect inputs without separate actions.

> **INFO**
>
> - When **Trigger** is set to **Event**, you can select only one event from the event list.
> - When selecting the **Input** or **Input(Event Name Change)** options to set custom conditions, if your desired schedule is not available, click **+ Add Schedule**. For more information about schedule settings, refer to the following.
> - If the desired event name is not available when selecting the **Input(Event Name Change)** option to set custom conditions, click **Add Event Name**. When this event occurs, the event name will be displayed in the event log and real-time log.
> - Event names can be entered with a maximum of 64 characters.

Action

You can select predefined actions or add custom actions.

> **INFO**
>
> - If you select the **Output** option to set custom actions and your desired signal setting is not available, click **+ Add Signal** to configure it.
> - If you selected **Trigger** as **Input(Event Name Change)**, you can set **Action** as **Port None**.

Image log settings

In the **Image Log** group, you can set image log events and schedules used by the device.

1. Set the **Image Log** option to **Use**.
2. Click **Configuration** and then click **+ Add** to set your desired events and schedules.

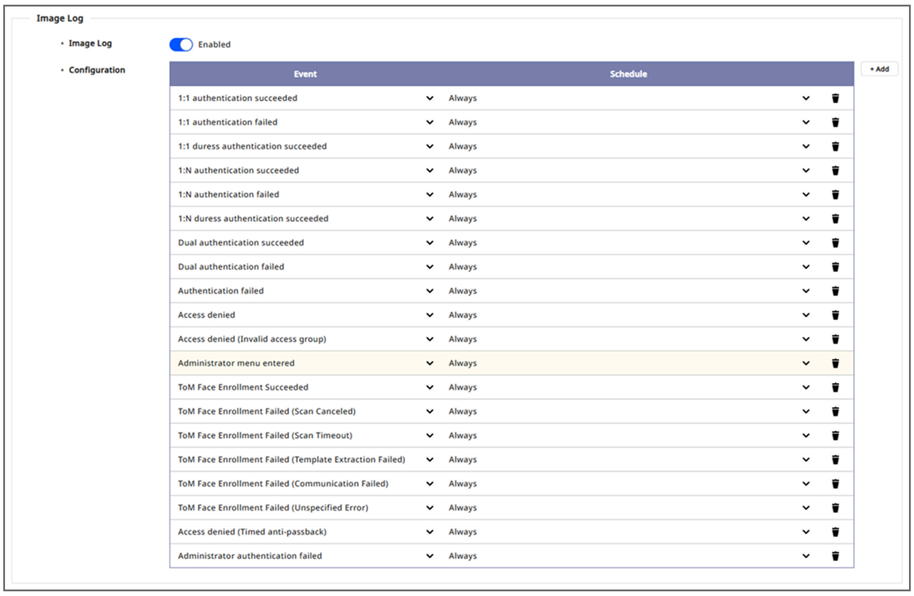


Image Log

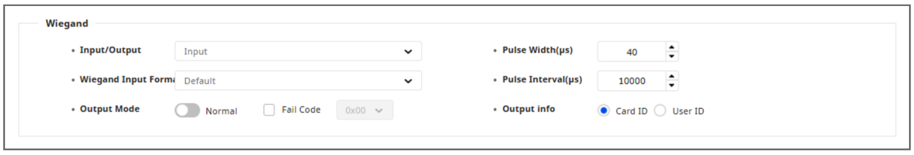
- Image Log: Enabled
- Configuration

Event	Schedule
1:1 authentication succeeded	Always
1:1 authentication failed	Always
1:1 duress authentication succeeded	Always
1:N authentication succeeded	Always
1:N authentication failed	Always
1:N duress authentication succeeded	Always
Dual authentication succeeded	Always
Dual authentication failed	Always
Authentication failed	Always
Access denied	Always
Access denied (Invalid access group)	Always
Administrator menu entered	Always
ToM Face Enrollment Succeeded	Always
ToM Face Enrollment Failed (Scan Canceled)	Always
ToM Face Enrollment Failed (Scan Timeout)	Always
ToM Face Enrollment Failed (Template Extraction Failed)	Always
ToM Face Enrollment Failed (Communication Failed)	Always
ToM Face Enrollment Failed (Unspecified Error)	Always
Access denied (Timed anti-passback)	Always
Administrator authentication failed	Always

> **INFO**
>
> - This feature is supported by the BioStation A2, FaceStation 2, FaceStation F2, X-Station 2, and BioStation 3 models.
> - For more information about the default settings of image logs, refer to the following.

Wiegand settings

In the **Wiegand** group, you can configure input and output details related to Wiegand devices.



Wiegand

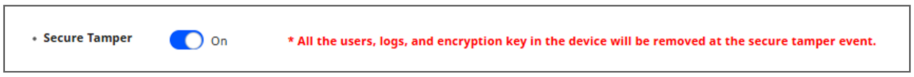
- Input/Output: Input
- Wiegand Input Forma: Default
- Output Mode: Normal □ Fail Code 0x00
- Pulse Width(μs): 40
- Pulse Interval(μs): 10000
- Output info: ● Card ID ○ User ID

- **Input/Output**: Select the input and output mode.
- **Pulse Width(μs)**: Set the pulse width for the Wiegand signal.
- **Wiegand Input Format**: Change the Wiegand format designated for the device.
- **Pulse Interval(μs)**: Set the pulse interval for the Wiegand signal.
- **Output Mode**: Configure the Wiegand signal output mode.
  - **Normal**: Scan cards using the configured Wiegand format. You can set error codes and select values to be sent if Wiegand card authentication fails.
  - **Bypass**: Send CSN regardless of Wiegand authentication. Set this if you are using it as a device without door control functionality.
- **Output info**: Select the information that will be output to the device during authentication.

> **INFO**
>
> For more information about Wiegand format settings, refer to the following.

Security tamper settings

If a tamper event occurs on the device, you can set it to delete all user information, logs, and security keys stored on the device. To activate the **Secure Tamper** feature, set it to **On**.



- Secure Tamper: On * All the users, logs, and encryption key in the device will be removed at the secure tamper event.

Analog intercom settings

You can set whether to use an analog intercom. To use the intercom connected to the device, click **Interphone** group and select **Use**.

> **INFO**
>
> This feature is supported only by the BioStation 2 model.

Camera settings

You can set the camera frequency. Incorrectly setting the frequency in environments with fluorescent lights can cause flickering in images. Set the frequency for the local area in the **Camera** group.

INFO

- This feature is supported by the FaceStation F2 and BioStation A2 models with firmware version 2.1.4 or higher.
- Camera frequencies vary by geographic location. The USA typically uses 60Hz, while most other regions use 50Hz. For the camera frequency in your area, consult your dealer.

Thermal and Mask Settings

In the **Thermal & Mask** or **Mask** sections, you can set detailed parameters for the thermal camera and mask usage.

- The thermal camera can be linked to Suprema's facial authentication device to measure the temperature of users passing through the door and restrict access for users exceeding the threshold temperature.
- The system detects masks and restricts access for users not wearing a mask.

> ⓘ **INFO**
>
> - The **Thermal Camera** setting feature is supported by FaceStation 2 and FaceStation F2 models. Refer to the thermal cameras supported below.
>   - TCM10-FS2
>   - TCM10-FSF2
> - The **Mask Detection** setting feature is supported by FaceStation F2, BioStation 3, and BioEntry W3.
> - If the user has made any arbitrary changes, click the **Apply** button. Changes will not be applied to the device if not saved.

Mask settings

In the **Mask Configuration** group, you can set whether to use mask detection.

- **Mask Detection**: Select whether to use mask detection.
  - **Use (Deny access when failed to detect mask)**: Users without masks are denied authentication, and events of mask unwear recorded.
  - **Use (Allow access after leaving log when failed to detect mask)**: Users without masks can authenticate, but events of mask unwear are recorded.
  - **Not Use**: Mask detection is not used.
- **Mask Detect Level**: Select the mask detection sensitivity.

Thermal camera settings

In the **Thermal Camera** group, you can set the use of the thermal camera and its parameters.

- **Thermal Camera Use**: Set whether to use the thermal camera.
  - **Use (Deny access when exceeded threshold temperature)**: Users exceeding the threshold temperature are denied authentication, and events of exceeding the threshold temperature are recorded.
  - **Use (Allow access after leaving log when exceeded threshold temperature)**: Users exceeding the threshold temperature can authenticate, but events of exceeding the threshold temperature are recorded.

- **Celsius/Fahrenheit**: Set the temperature display unit.
- **Threshold Temp. (℃)** / **Threshold Temp. (℉)**: Set the minimum and maximum values for the threshold temperature that restricts access.
  Users with a surface temperature below the **Low** value or above the **High** value will be restricted from entry according to the **Thermal Camera Use** option. You can set the range from 1℃ to 45℃, and the **Low** value cannot be higher than the **High** value.
- **Save Temp. Data**: Set whether to save the user's temperature log.
  - **Enabled**: Logs both authentication success and the user's temperature value.
  - **Disable**: Only logs authentication success.
- **Temp. Fail Sound**: Set whether to notify authentication failure due to exceeding the threshold temperature.
- **Show Infrared Image**: Set whether to display infrared images on the device screen.
- **Camera Configuration**: Set detailed options for the thermal camera.
  - **Temp. Correction (℃)**: Adjust the temperature to measure consistently higher or lower based on the product usage environment. For example, if temperatures are consistently measured 0.1℃ higher, set the temperature compensation value to -0.1℃.
  - **Distance(cm)**: Set the distance between the user and the thermal camera.
  - **Emissivity**: Set the infrared emissivity.
  - **Dynamic ROI**: If other lighting is present in the environment, configure the thermal camera to measure the user's temperature automatically without interference from nearby lights.
  - **ROI X(%)** / **ROI Y(%)** / **ROI Width(%)** / **ROI Height(%)**: If the **Dynamic ROI** option is set to **Disable**, manually set the ROI (Region of Interest). Adjust the ROI location and size to specify the area where the thermal camera will measure temperature.

ⓘ **INFO**

- The settings for the **Threshold Temp.** option's **Low** and **High** values are supported from the firmware versions below.
  - FaceStation 2 firmware version 1.4.2 and above
  - FaceStation F2 firmware version 1.0.2 and above
- For optimal performance, it is advised to use the default settings for the sub-options in **Camera Configuration**. The default values for each device's options are listed below.

Item	FaceStation 2	FaceStation F2
Distance(cm)	100	100
Emissivity	0.98	0.98
ROI X(%)	47	30
ROI Y(%)	45	25
ROI Width(%)	15	50
ROI Height(%)	10	55

Thermal and mask verification methods

Thermal & Mask Check Mode group allows settings to determine the verification method based on the device's purpose when **Mask Detection** or **Thermal Camera Use** options are set to **Use**.

- **Check after authentication**: Checks the user's mask usage or measures temperature after authentication.
- **Check before authentication**: Checks the user's mask usage or measures temperature before authentication. In this case, users not wearing a mask or exceeding the threshold temperature cannot authenticate.
- **Check without authentication**: The device can only be used to check for mask usage or measure temperature. Users wearing a mask or having a temperature below the threshold can enter regardless of authentication.

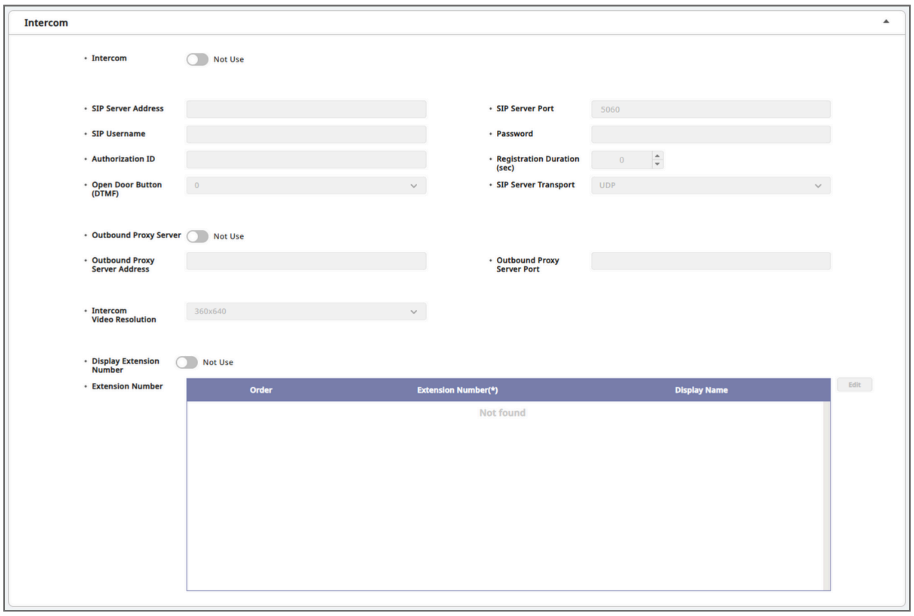
Intercom Settings

In the **Intercom** section, you can set detailed options for using the intercom.

> **INFO**
>
> - This feature is supported on the BioStation 3, FaceStation 2, and BioStation A2.
> - If the user has made any arbitrary changes, click the **Apply** button. Changes will not be applied to the device if not saved.

Intercom settings

Set each option to register the device with the Session Initiation Protocol (SIP) server.



Intercom

- Intercom: Not Use
- SIP Server Address:
- SIP Server Port: 5060
- SIP Username:
- Password:
- Authorization ID:
- Registration Duration (sec): 0
- Open Door Button (DTMF): 0
- SIP Server Transport: UDP
- Outbound Proxy Server: Not Use
- Outbound Proxy Server Address:
- Outbound Proxy Server Port:
- Intercom Video Resolution: 360x640
- Display Extension Number: Not Use
- Extension Number:

Order	Extension Number(*)	Display Name
Not found		

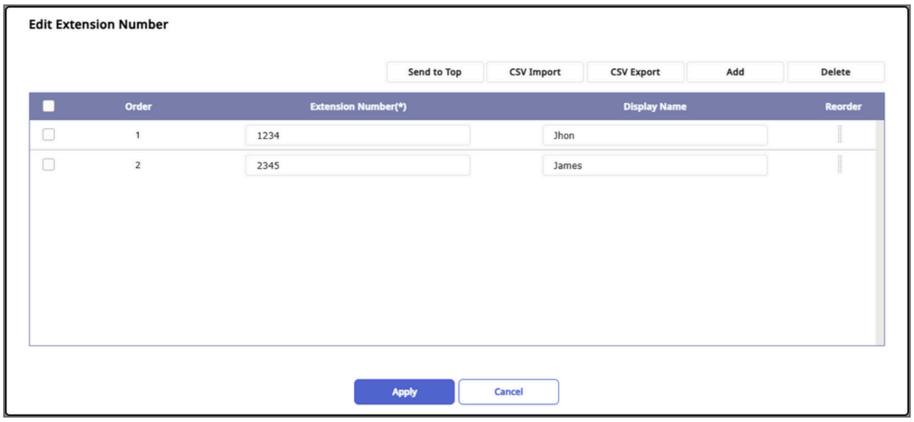
- **Intercom**: To use the device as an intercom, set to **Enabled**.
- **SIP Server Address**: Enter the address of the SIP server.
- **SIP Server Port**: Enter the port of the SIP server. The default is 5060.
- **SIP Username**: Enter the username for the SIP account.
- **Password**: Enter the password for the SIP account.
- **Authorization ID**: Enter the authorization ID for the SIP account.
- **Registration Duration (sec)**: Enter the registration duration in seconds. The device attempts to register with the SIP server every time the registration duration expires.
- **Open Door Button (DTMF)**: Specify a button to open the entrance door during a call.
- **SIP Server Transport**: Choose the SIP transport method when configuring the intercom's SIP server settings.

- **Outbound Proxy Server**: Set to **Enabled** if using SIP services via a separate outbound proxy server.
  - **Outbound Proxy Server Address**: Enter the address of the outbound proxy server.
  - **Outbound Proxy Server Port**: Enter the port of the outbound proxy server.
- **Intercom Video Resolution**: Select the resolution of the video output when using the intercom. The default is **360 x 640**.
- **Display Extension Number**: Set to **Disable** to prevent the device from displaying the extension number. Without displaying the extension number, you cannot distinguish the recipient on the calling screen.
- **Extension Number**: You can register up to 128 extension numbers. To add or edit extension numbers, click the **Edit** button. For more information, refer to the following.

> **INFO**
>
> - The options **SIP Username** and **Authorization ID** can only include numbers, English letters (case sensitive), and special characters.
> - The **Registration Duration (sec)** option can be set between 60 and 600 seconds.
> - The **SIP Server Transport** and **Intercom Video Resolution** options are supported on firmware version 1.3.0 and above of BioStation 3.
> - **Session Initiation Protocol** (SIP) is a communication protocol based on internet protocols for various multimedia communications, such as VoIP and video conferencing. The SIP server manages such communications and establishes connections.

Edit extension numbers

Guidance on the features provided in the **Edit Extension Number** window.



Edit Extension Number

□	Order	Extension Number(*)	Display Name	Reorder
□	1	1234	Jhon	
□	2	2345	James	

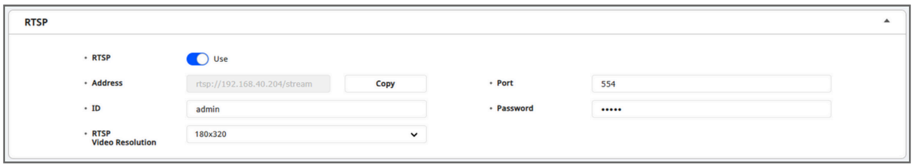
- **Send to Top**: Move the selected extension number to the top of the list.
- **CSV Import**: Import a CSV file that contains the extension numbers.
- **CSV Export**: Export the saved extension numbers to a CSV file.
- **Add**: Add an extension number.
- **Delete**: Delete an extension number.

- **Reorder**: Change the order of the extension numbers by dragging them with the mouse.

> **INFO**
>
> - The FaceStation 2 and BioStation A2 models can save up to 16 extension numbers.
> - You cannot import a CSV file that contains more extension numbers than the maximum supported.
> - Extension numbers can only include numbers, English letters (case sensitive), and special characters.

RTSP Settings

In the **RTSP** section, you can configure the details for **Real Time Streaming Protocol** (RTSP) streaming. The device's camera can stream live video.



RTSP

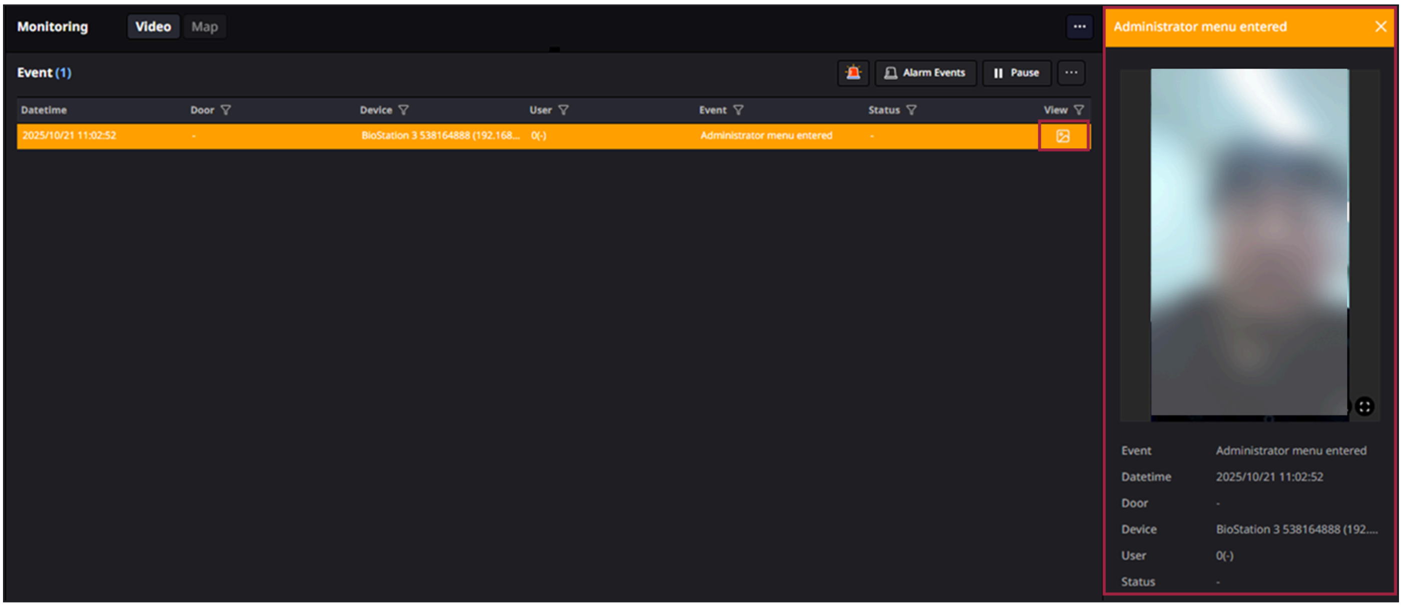
- RTSP: Use
- Address: rtsp://192.168.40.204/stream Copy
- Port: 554
- ID: admin
- Password: •••••
- RTSP Video Resolution: 180x320

- **RTSP**: Enable RTSP streaming by setting **Enabled**.
- **Address**: The RTSP server address is fixed. Click the **Copy** button to copy the RTSP address.
- **Port**: Set the RTSP port.
- **ID**: Enter the RTSP server ID.
- **Password**: Enter the RTSP server password.
- **RTSP Video Resolution**: Select the resolution of the video output when using RTSP. The default is **180 x 320**.

> **INFO**
>
> - This feature supports BioStation 3 and BioEntry W3 models.
> - The **RTSP Video Resolution** option is supported on BioStation 3 firmware version 1.3.0 or higher.
> - If the user has made any arbitrary changes, click the **Apply** button. Changes will not be applied to the device if not saved.

Image Log Settings

Image Log allows for image verification of events that occur on devices with cameras. It can record face images of users passing through doors or situations during event occurrences using the device's camera. The recorded images can be viewed through real-time events on the **Monitoring** page.



Event (1)

Datetime	Door	Device	User	Event	Status	View
2025/10/21 11:02:52	-	BioStation 3 538164888 (192.168...	0(-)	Administrator menu entered	-	🖼

Administrator menu entered

Event	Administrator menu entered
Datetime	2025/10/21 11:02:52
Door	-
Device	BioStation 3 538164888 (192....
User	0(-)
Status	-

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

When you set up image logging, an image log for the event will be created in the **Event** list. Click the 🖼 button at the far right of the event item. You can view the image captured when the event occurred in the right panel.

> **INFO**
>
> - This feature is supported by the BioStation A2, FaceStation 2, FaceStation F2, X-Station 2, and BioStation 3 models.
> - For detailed information on viewing event logs on the **Monitoring** page, refer to the following.
> - The settings configured in the **Settings** → **Device** → **Image Log** menu do not reflect on the device. For detailed information on the device's **Image Log** settings, refer to the following.

Add basic settings

You can set events and schedules to generate image logs on the device. An image log will be generated if the conditions of events and schedules are met.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Image Log** in the left sidebar.

3. Click the **+ Add** button to the right of the **Preset** section.

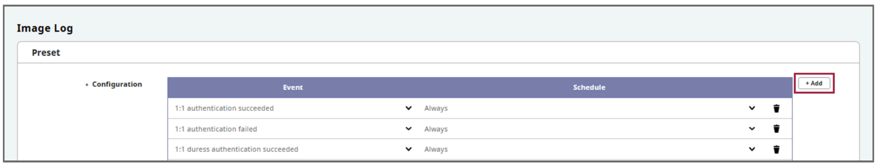
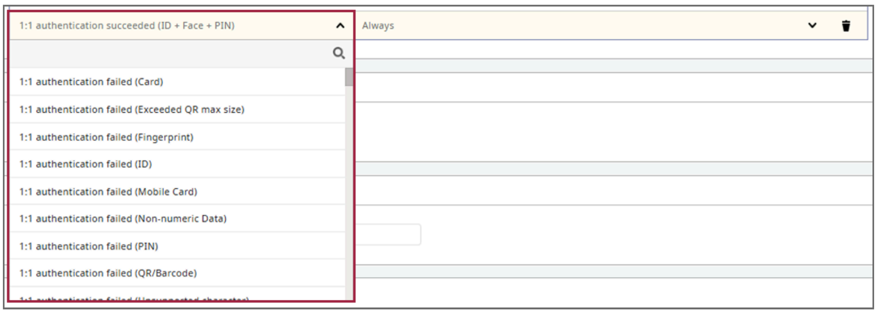
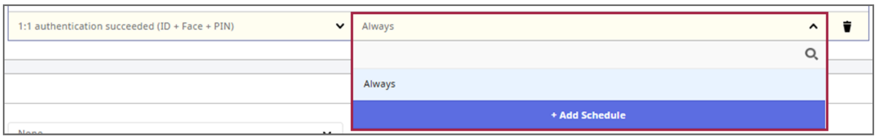


Image Log
Preset
• Configuration
Event
Schedule
+ Add
1:1 authentication succeeded
Always
1:1 authentication failed
Always
1:1 duress authentication succeeded
Always

4. When an event is added at the bottom of the list, click the ⌄ button for the desired event and select your options.


1:1 authentication succeeded (ID + Face + PIN)
Always
1:1 authentication failed (Card)
1:1 authentication failed (Exceeded QR max size)
1:1 authentication failed (Fingerprint)
1:1 authentication failed (ID)
1:1 authentication failed (Mobile Card)
1:1 authentication failed (Non-numeric Data)
1:1 authentication failed (PIN)
1:1 authentication failed (QR/Barcode)

5. Click the ⌄ button in the schedule for the selected event and choose the preferred option.



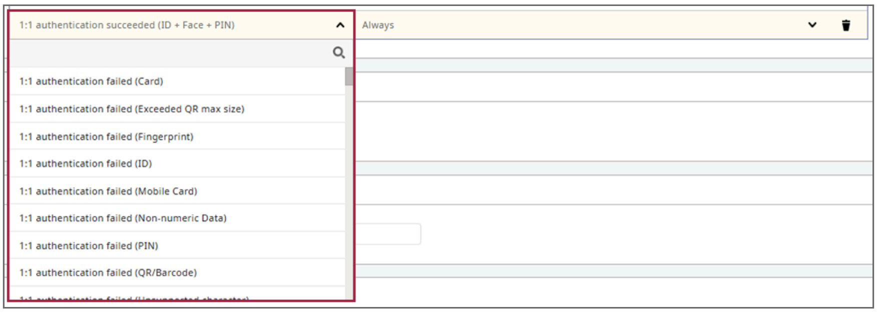
6. Click **Apply** at the bottom of the screen to save the settings.

> ⓘ **INFO**
>
> If the desired schedule is not available, click **+ Add Schedule** to add one. For more information about schedule settings, refer to the following.

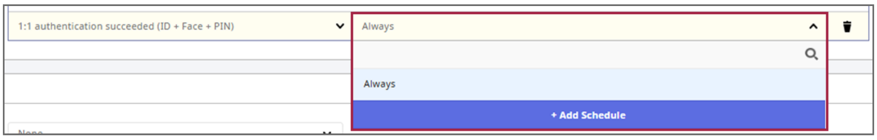
Modify basic settings

You can change the events and schedules of existing image logs.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Image Log** in the left sidebar.
3. In the list of the **Preset** section, click the ⌄ button for the event you want to modify and select your options.


1:1 authentication succeeded (ID + Face + PIN)
Always
1:1 authentication failed (Card)
1:1 authentication failed (Exceeded QR max size)
1:1 authentication failed (Fingerprint)
1:1 authentication failed (ID)
1:1 authentication failed (Mobile Card)
1:1 authentication failed (Non-numeric Data)
1:1 authentication failed (PIN)
1:1 authentication failed (QR/Barcode)

4. Click the ⌄ button in the schedule for the selected event and choose the preferred option.



1:1 authentication succeeded (ID + Face + PIN) | Always

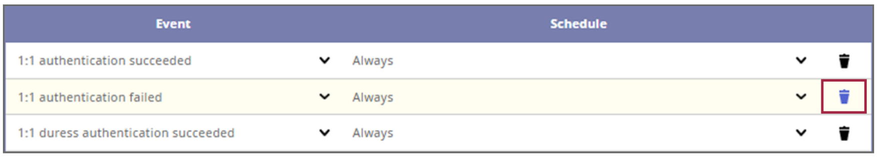
5. Click **Apply** at the bottom of the screen to save the settings.

> **INFO**
>
> If the desired schedule is not available, click **+ Add Schedule** to add one. For more information about schedule settings, refer to the following.

Delete basic settings

You can delete events and schedules of existing image logs.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Image Log** in the left sidebar.
3. In the list of the **Preset** section, click the 🗑 button for the event you want to delete.



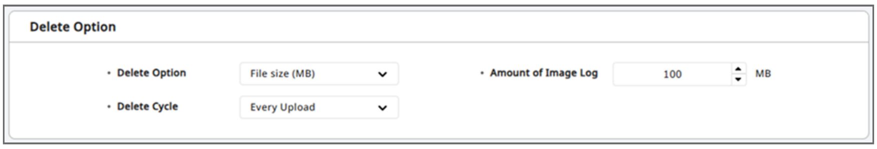
Event	Schedule	
1:1 authentication succeeded	Always	🗑
1:1 authentication failed	Always	🗑
1:1 duress authentication succeeded	Always	🗑

4. Click **Apply** at the bottom of the screen to save the settings.

Delete Option

You can set delete options so that image log files do not take up space on the **BioStar X** server. Image logs that exceed the set file size or duration will be automatically deleted.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Image Log** in the left sidebar.
3. Set the conditions for deleting image logs in the **Delete Option** section.



Delete Option

- Delete Option: File size (MB)
- Delete Cycle: Every Upload
- Amount of Image Log: 100 MB

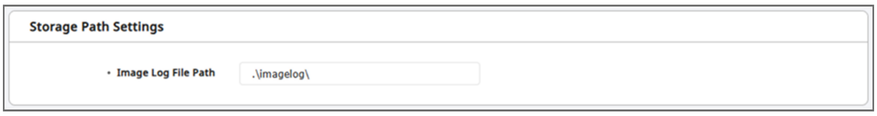
- **Delete Option**: Choose the file size unit (**MB**/**GB**) or duration unit (**Day**/**Week**/**Month**).
- **Amount of Image Log**: Set the unit of the condition defined in **Delete Option**.
- **Delete Cycle**: Choose the cycle for deleting image logs.

4. Click **Apply** at the bottom of the screen to save the settings.

Storage Path Settings

You can set the path where image logs are stored.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Image Log** in the left sidebar.
3. Enter the path for storing image logs in the **Image Log File Path** input field of the **Storage Path Settings** section.



Storage Path Settings

- Image Log File Path: .\imagelog\

4. Click **Apply** at the bottom of the screen to save the settings.

INFO

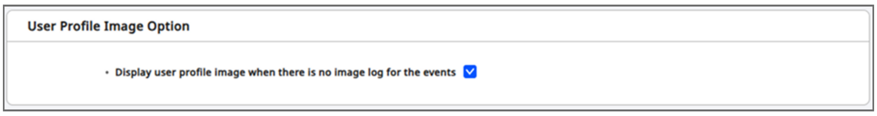
- The storage path is not created automatically, so it must be created in advance for storing image logs.
- For example, entering `.\imagelog\` will store image logs under the path where BioStar X is installed.

  > *C:\Program Files\BioStar X\imagelog\*

User Profile Image Option

You can configure the device to display the user's profile picture when monitoring event logs and real-time logs if the device cannot shoot image logs.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Image Log** in the left sidebar.
3. Check the checkbox for the **Display user profile image when there is no image log for the events** item in the **User Profile Image Option** section.



User Profile Image Option

- Display user profile image when there is no image log for the events ☑

4. Click **Apply** at the bottom of the screen to save the settings.

INFO

- When this option is enabled, if an image log occurs, the user profile picture will not be shown, and the recorded image log will be displayed instead.
- For detailed information on viewing event logs on the **Monitoring** page, refer to the following.

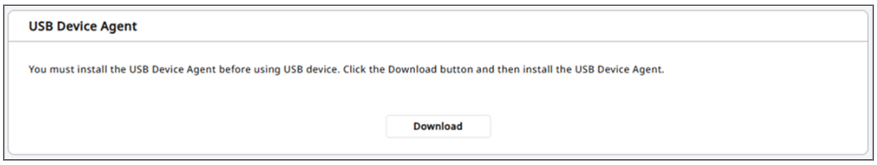
USB Agent Settings

When accessing **BioStar X** from a client PC, ensure the USB fingerprint and card enrollment devices are available. To do this, install the USB Device Agent. This document provides guidance on how to install and set up the USB Device Agent.

Install the USB device agent

To access **BioStar X** from a client PC and use the USB fingerprint and card enrollment devices, the USB Device Agent must be installed.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **USB Agent** in the left sidebar.
3. Click the **Download** button in the **USB Device Agent** section.



USB Device Agent

You must install the USB Device Agent before using USB device. Click the Download button and then install the USB Device Agent.

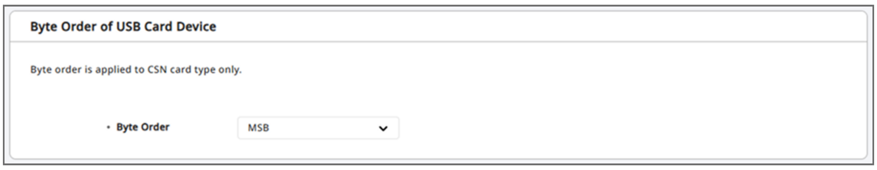
4. Run the downloaded file and follow the on-screen instructions to complete the installation.

> **INFO**
>
> If **User Account Control** is enabled in Windows, the USB Agent cannot be auto-launched. Disable User Account Control or run it directly with administrative privileges.

Set the USB card device byte order

You can set the byte order for the USB card device.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **USB Agent** in the left sidebar.
3. Setting the **Byte Order of USB Card Device** option in the **Byte Order** section.



Byte Order of USB Card Device

Byte order is applied to CSN card type only.

- Byte Order: MSB

- **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).

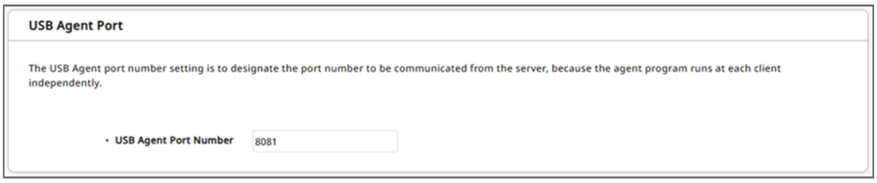
4. Once all configurations are complete, click the **Apply** button at the bottom of the screen.

> ⓘ **INFO**
>
> The **Byte Order** option applies only to CSN cards.

Set the USB agent port

You can set the port used by the USB Agent.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **USB Agent** in the left sidebar.
3. Enter the port number in the **USB Agent Port Number** input field in the **USB Agent Port** section.



USB Agent Port

The USB Agent port number setting is to designate the port number to be communicated from the server, because the agent program runs at each client independently.

- USB Agent Port Number: 8081

4. Once all configurations are complete, click the **Apply** button at the bottom of the screen.

> ⓘ **INFO**
>
> The USB Agent is a program that operates per client, and the port number setting is for the server to communicate via that port number.

Device Connection Management Settings

BioStar X's **Device Connection Manager** is a feature designed to efficiently manage a large number of devices in companies or large buildings. Previously, a single server could connect a maximum of 1,000 devices, but now you can install multiple **communication** servers on several computers to manage up to 3,000 network devices.

> ⓘ **INFO**
>
> - This feature requires the **Device Manager** license to be activated. For more information about the license policy, refer to the following.
> - For specifications and installation of the communication server, refer to the followings:
>   - Communication Server Specifications
>   - Install Communication Server

Key features

- **Server Expansion**: Install communication servers on additional computers besides the main computer to connect more devices.
- **Multiple Server Operation**: Use up to three servers together to support a total of 3,000 devices.
- **Convenient Device Management**: When adding new devices, choose which server to connect to, and you can also move existing devices to another server.
- **Large Environment Support**: Operate a large number of devices reliably in large business sites or buildings.

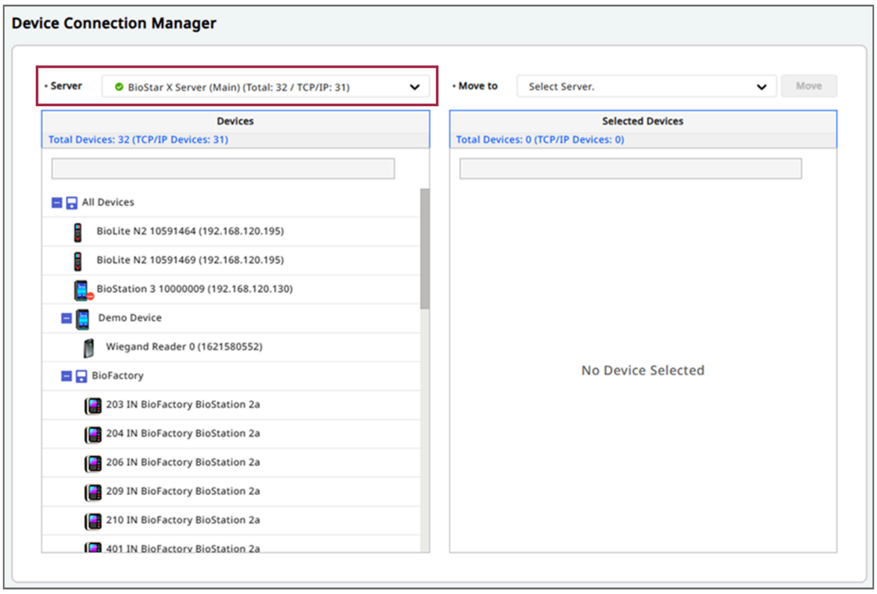
The communication server is a dedicated service that separates the connection functionality with devices from the integrated server of BioStar X. It focuses solely on reliable communication with devices, enhancing the performance of the overall system.

Move devices to another server

You can move devices registered on the main server or other communication servers to another communication server. This feature helps maintain the connection status of the devices while moving them between servers.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Device Connection Manager** on the left sidebar

3. From the **Server** section on the left, select the server where the device you want to move is registered.



Device Connection Manager

• Server: BioStar X Server (Main) (Total: 32 / TCP/IP: 31)

• Move to: Select Server.

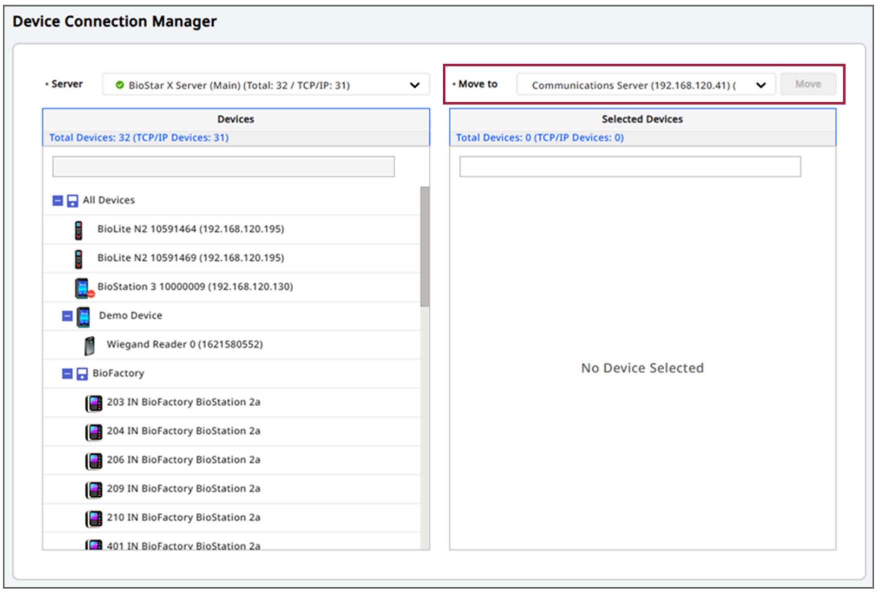
Devices
Total Devices: 32 (TCP/IP Devices: 31)

- All Devices
  - BioLite N2 10591464 (192.168.120.195)
  - BioLite N2 10591469 (192.168.120.195)
  - BioStation 3 10000009 (192.168.120.130)
  - Demo Device
    - Wiegand Reader 0 (1621580552)
  - BioFactory
    - 203 IN BioFactory BioStation 2a
    - 204 IN BioFactory BioStation 2a
    - 206 IN BioFactory BioStation 2a
    - 209 IN BioFactory BioStation 2a
    - 210 IN BioFactory BioStation 2a
    - 401 IN BioFactory BioStation 2a

Selected Devices
Total Devices: 0 (TCP/IP Devices: 0)

No Device Selected

4. In the **Move to** section on the right, select the target server to which you want to move the devices.



Device Connection Manager

• Server: BioStar X Server (Main) (Total: 32 / TCP/IP: 31)

• Move to: Communications Server (192.168.120.41) (

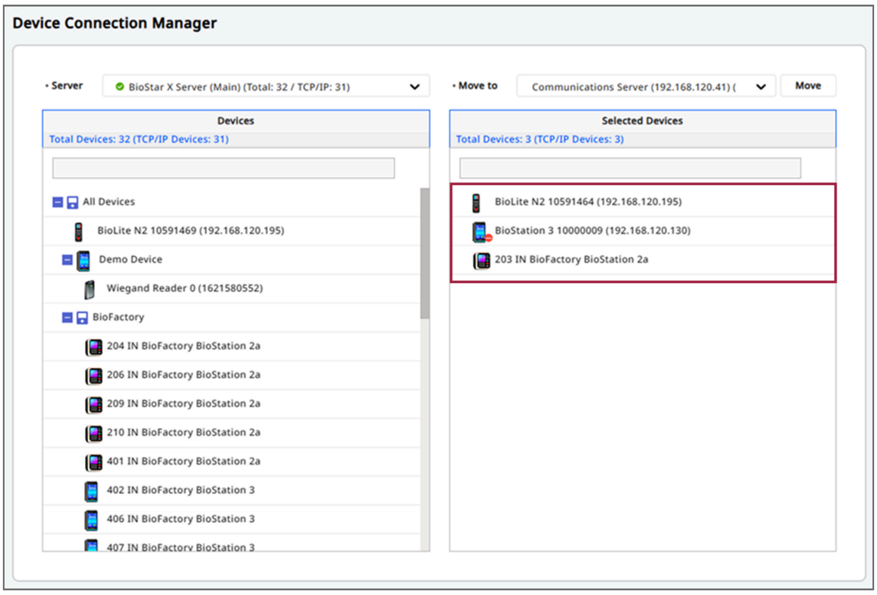
Devices
Total Devices: 32 (TCP/IP Devices: 31)

- All Devices
  - BioLite N2 10591464 (192.168.120.195)
  - BioLite N2 10591469 (192.168.120.195)
  - BioStation 3 10000009 (192.168.120.130)
  - Demo Device
    - Wiegand Reader 0 (1621580552)
  - BioFactory
    - 203 IN BioFactory BioStation 2a
    - 204 IN BioFactory BioStation 2a
    - 206 IN BioFactory BioStation 2a
    - 209 IN BioFactory BioStation 2a
    - 210 IN BioFactory BioStation 2a
    - 401 IN BioFactory BioStation 2a

Selected Devices
Total Devices: 0 (TCP/IP Devices: 0)

No Device Selected

5. Select the device(s) you want to move from the device list. You can select multiple devices.



Device Connection Manager

• Server: BioStar X Server (Main) (Total: 32 / TCP/IP: 31)

• Move to: Communications Server (192.168.120.41) (

Move

Devices
Total Devices: 32 (TCP/IP Devices: 31)

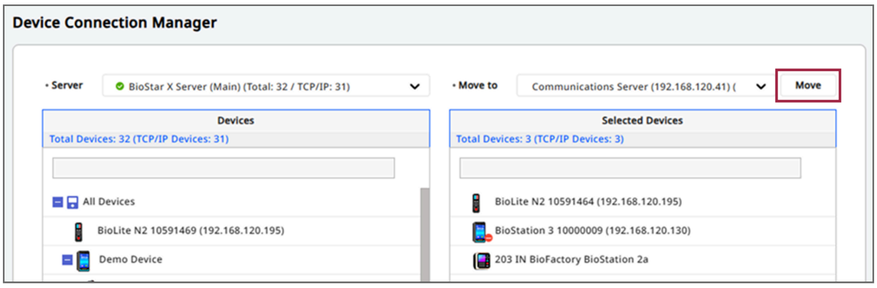
- All Devices
  - BioLite N2 10591469 (192.168.120.195)
  - Demo Device
    - Wiegand Reader 0 (1621580552)
  - BioFactory
    - 204 IN BioFactory BioStation 2a
    - 206 IN BioFactory BioStation 2a
    - 209 IN BioFactory BioStation 2a
    - 210 IN BioFactory BioStation 2a
    - 401 IN BioFactory BioStation 2a
    - 402 IN BioFactory BioStation 3
    - 406 IN BioFactory BioStation 3
    - 407 IN BioFactory BioStation 3

Selected Devices
Total Devices: 3 (TCP/IP Devices: 3)

- BioLite N2 10591464 (192.168.120.195)
- BioStation 3 10000009 (192.168.120.130)
- 203 IN BioFactory BioStation 2a

> ⓘ To search for a specific device, enter keywords in the input field at the top. You can search by device name or serial number.

6. Click **Move** to move the device to the target server.



Device Connection Manager

• Server: BioStar X Server (Main) (Total: 32 / TCP/IP: 31)

• Move to: Communications Server (192.168.120.41) (

Move

Devices
Total Devices: 32 (TCP/IP Devices: 31)

- All Devices
  - BioLite N2 10591469 (192.168.120.195)
  - Demo Device

Selected Devices
Total Devices: 3 (TCP/IP Devices: 3)

- BioLite N2 10591464 (192.168.120.195)
- BioStation 3 10000009 (192.168.120.130)
- 203 IN BioFactory BioStation 2a

7. Check the total number of devices to move, the number of TCP/IP connected devices, the name of the server to move to, and the IP address in the message window.

8. Click **Yes**.

Once the move is complete, you can check the total number of devices moved, the number of TCP/IP connected devices, and the name and IP address of the moved server in the message window.

If there are devices that failed to move, the message window will show the number of devices that failed to move and the number of TCP/IP connected devices. To view a list of devices that failed to move and the reasons for failure in a CSV file, click the **Download** button.

ⓘ **INFO**

- If there are no connected extension servers, **Move to** on the right side of the screen will not be displayed.
- When selecting a server, you can see all registered devices, including Wiegand and RS-485 connected devices on that server.
- Selecting a device or device group will also move the subordinate devices connected to the device and the devices included in the group.
- Devices that are not connected via TCP/IP cannot be moved.

Manage Doors

This guide describes how to set up and manage the access door information for the registered device. You can set information regarding the device's relays, dual authentication, anti-passback, forced door opening, and long door opening alarms, and the configured door information will be used as components of access levels.

Manage Door Group

This guide describes how to set up groups to easily manage multiple doors.

Register Door

Set the door for access control. Select the entrance/exit device based on the door or set up anti-passback to enhance security, and configure alarms.

Modify Door Information

This guide describes how to modify the settings information of the registered access door.

Delete Door

This guide describes how to delete registered doors.

Manage Door Group

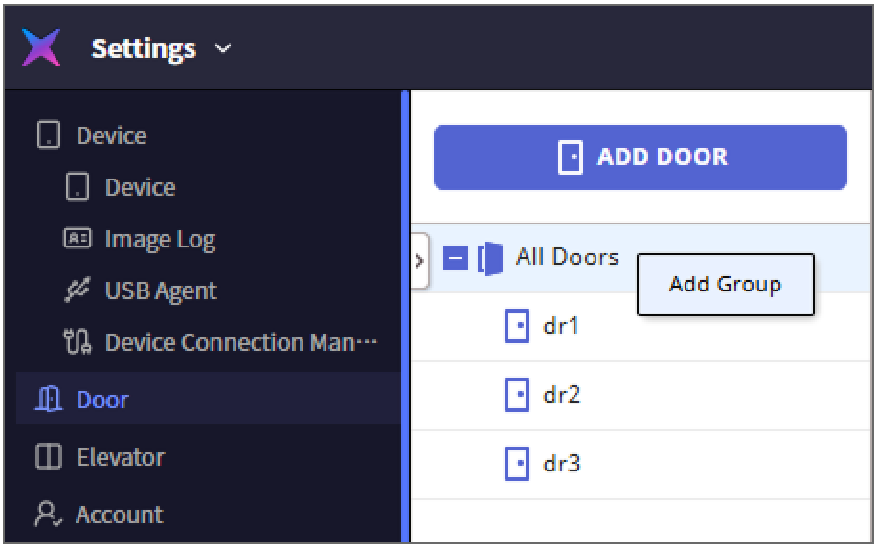
This guide describes how to set up groups to easily manage multiple doors. This guide describes how to set up groups for easy management of multiple doors. A door group is a feature that allows you to manage several doors as one group.

TIP

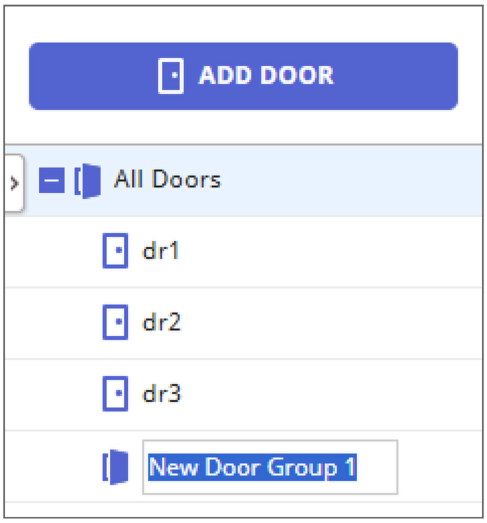
Register group names using door locations or office names for easier management.

Add door group

1. Click **Settings** on the **Launcher** page.
2. Click **Door** in the left sidebar.
3. Right-click on **All Doors** from the door list.



4. Click **Add Group** in the popup menu.



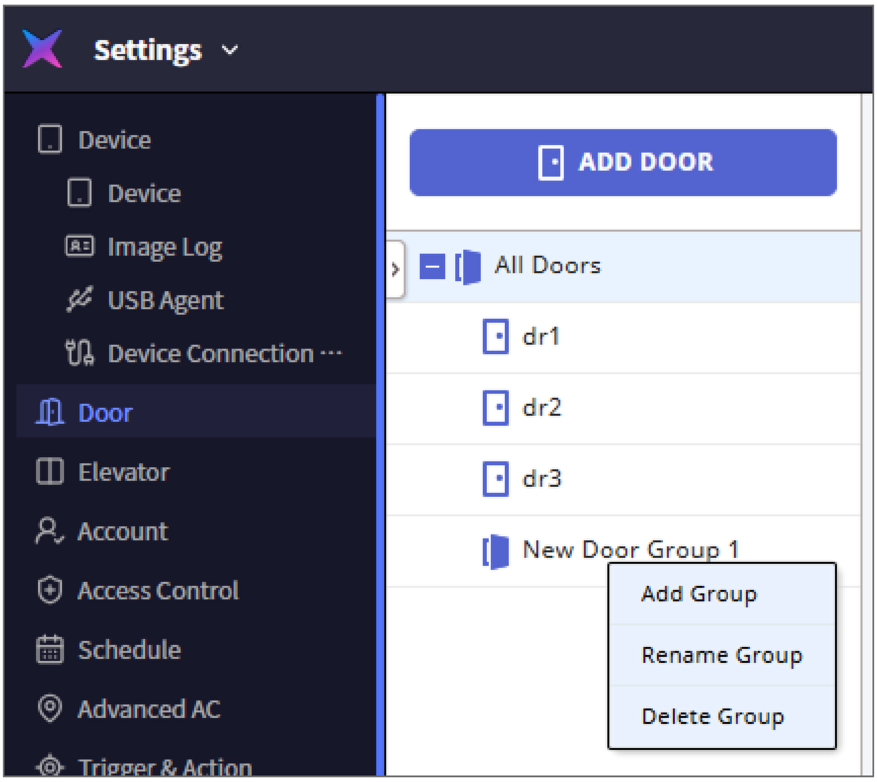
5. Enter your desired group name.

> **INFO**
>
> - You can create up to 8 levels of door groups.
> - The door group name can be up to 48 characters long.

Rename door group

1. Click **Settings** on the **Launcher** page.
2. Click **Door** in the left sidebar.

3. Right-click on the group you want to rename from the door list.



4. Click **Rename Group** in the popup menu.

5. Enter the new group name.

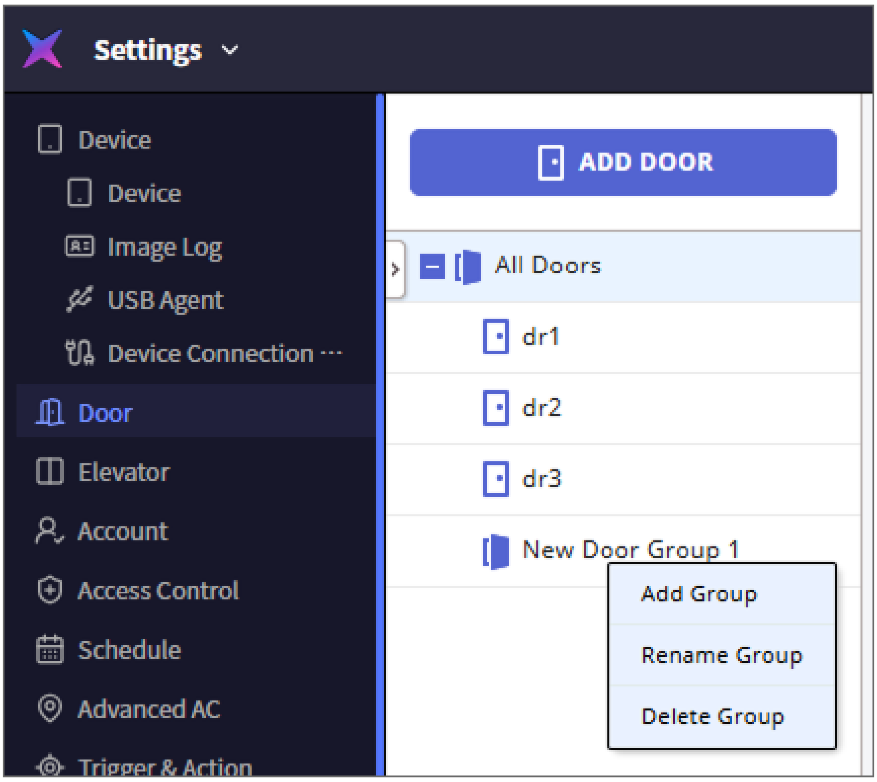
> **INFO**
>
> The door group name can be up to 48 characters long.

Delete door group

1. Click **Settings** on the **Launcher** page.

2. Click **Door** in the left sidebar.

3. Right-click on the group you want to delete from the door list.



4. Click **Delete Group** in the popup menu.

> ⚠ **CAUTION**
>
> Deleting a door group removes all doors included in the group. To avoid deleting the doors, move them to another group before deleting the group.

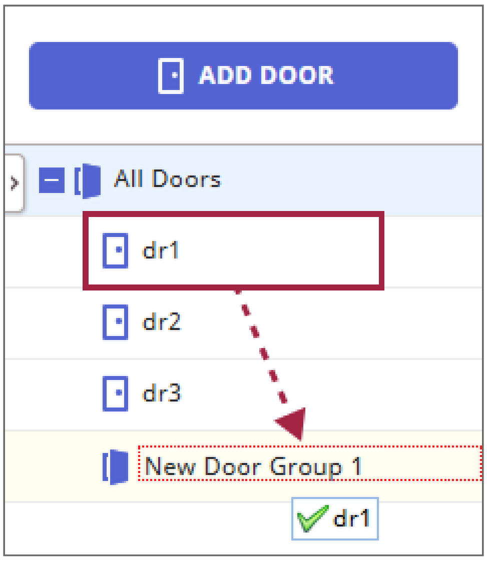
Add door to group

Add from door list

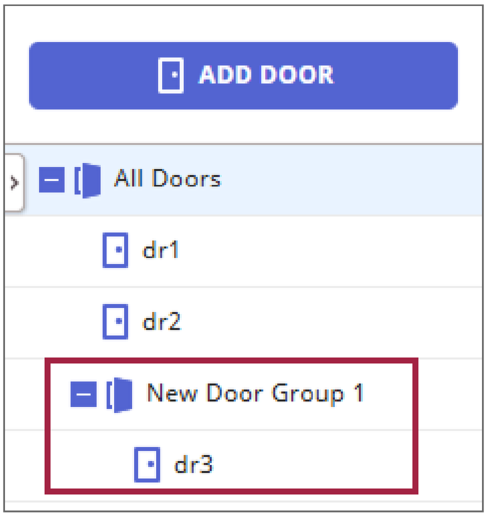
1. Click **Settings** on the **Launcher** page.

2. Click **Door** in the left sidebar.

3. Select the door you want to add to a group from the door list and drag it to the desired group.

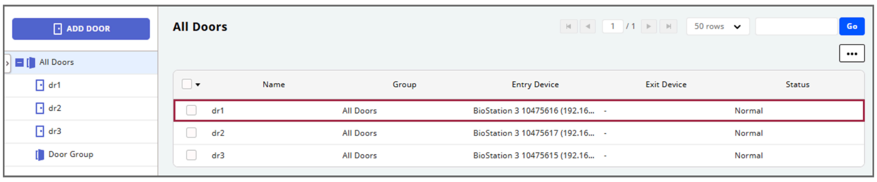


The selected door moves to the group.



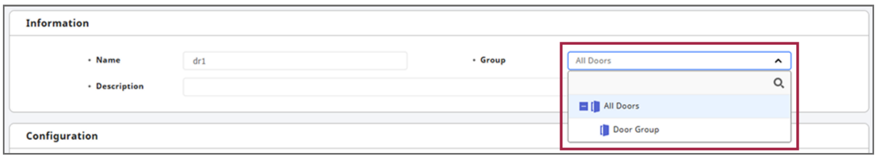
Add from door information

1. Click **Settings** on the **Launcher** page.
2. Click **Door** in the left sidebar.
3. Click the door you want to add to a group from the list on the right side of the screen.



□	Name	Group	Entry Device	Exit Device	Status
□	dr1	All Doors	BioStation 3 10475616 (192.16...	-	Normal
□	dr2	All Doors	BioStation 3 10475617 (192.16...	-	Normal
□	dr3	All Doors	BioStation 3 10475615 (192.16...	-	Normal

4. When the door information edit screen appears, click the **Group** option in the **Information** section.



Information

- Name: dr1
- Description:
- Group: All Doors

5. Select the desired group.

6. Click **Apply** at the bottom of the screen.

Register Door

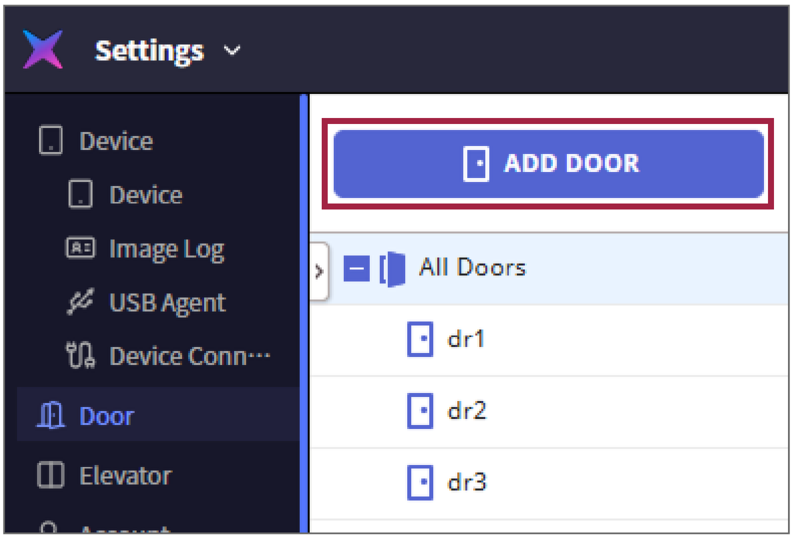
This guide describes how to register and set up doors. Connect entry and exit devices for each door, and configure security features such as anti-passback and dual authentication to establish a systematic access management environment. Additionally, configure alarms based on the door status to prevent security incidents in advance.

Before start

- Set access levels, access groups, and floor levels for access control before registering doors. For more information, refer to the following.
- Register devices before registering doors. For more information about device registration, refer to the following.
  - Register Device
  - Register Wiegand Credentials
  - Register Slave

Register door

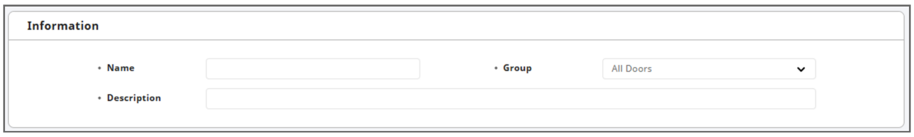
1. Click **Settings** on the **Launcher** page.
2. Click **Door** in the left sidebar.
3. Click **ADD DOOR**.



4. When the **Add New Door** screen appears, set each section item in order.
    - **Information**: Set the basic information of the door. For more information, refer to the following.
    - **Configuration**: Set devices connected to the door, and entry and exit buttons along with door sensors. For more information, refer to the following.
    - **Option**: Set additional options. For more information, refer to the following.
    - **Anti PassBack**: Set the anti-passback feature to manage access history and enhance security. For more information, refer to the following.
    - **Timed Anti PassBack**: Set the initialization time for the anti-passback feature. For more information, refer to the following.
    - **Alarm**: You can set the alarm to trigger or block device usage when an anti-passback violation occurs. For more information, refer to the following.
5. Once all configurations are complete, click the **Apply** button at the bottom of the screen.

Set basic information

In the **Information** section, you can input or change the door's name, group, and description.



Information

- Name
- Group: All Doors
- Description

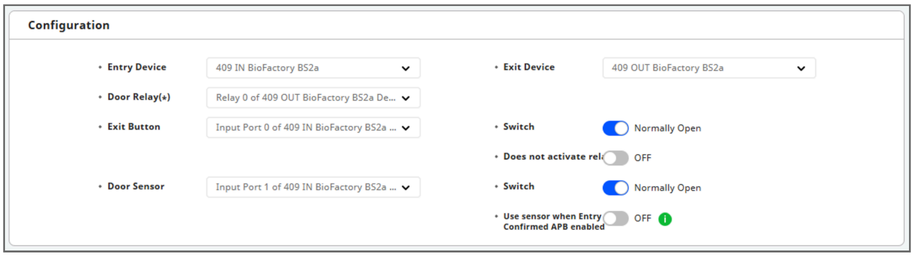
- **Name**: Enter the door name. Enter a name that can be specified for convenient management.
- **Group**: Select the door group.
- **Description**: Enter a brief description of the door.

INFO

- The door name can be up to 48 characters long.
- For more information about registering door groups, refer to the following.

Set door configuration

In the **Configuration** section, you can set the devices connected to the door, exit buttons, and door sensors.



Configuration

- Entry Device: 409 IN BioFactory BS2a
- Exit Device: 409 OUT BioFactory BS2a
- Door Relay(*): Relay 0 of 409 OUT BioFactory BS2a De...
- Exit Button: Input Port 0 of 409 IN BioFactory BS2a ...
- Switch: Normally Open
- Does not activate rel: OFF
- Door Sensor: Input Port 1 of 409 IN BioFactory BS2a ...
- Switch: Normally Open
- Use sensor when Entry Confirmed APB enabled: OFF

- **Entry Device**: Select the device to be used for entry. If the device is not listed, register the device first.

- **Door Relay**: Choose the relay that will function as the door lock mechanism.
- **Exit Button**: Select the port to be used as the exit button.
  - **Switch**: Can be set to **N/C** (Normally Closed) or **N/O** (Normally Open).
  - **Does not activate relay**: Configure so that an exit button input generates a door open request log without triggering the relay.
- **Door Sensor**: Choose the port to confirm the door's status. Setting it to **None** will disable the use of the **Alarm** section.
  - **Switch**: Can be set to **N/C** (Normally Closed) or **N/O** (Normally Open).
  - **Use sensor when Entry Confirmed APB enabled**: Set whether to use the door sensor when using the **Entry Confirmed APB** option.

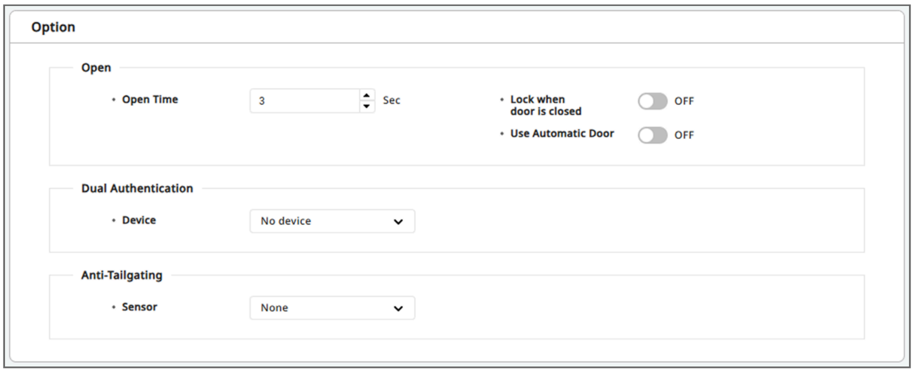
  > If **Timed Anti PassBack** is enabled, the **Use sensor when Entry Confirmed APB enabled** option cannot be used.

- **Exit Device**: Select the device to be used for exit.

> **INFO**
>
> - If you selected a wireless door lock for **Entry Device**, you must also select a wireless door lock for **Exit Device**.
> - If you selected a wireless door lock for **Entry Device**, you cannot use the **Door Relay** option.
> - CoreStation models cannot be used as entry or exit devices.

Set additional options

In the **Option** section, you can set additional options for the door.



Option

Open

- Open Time: 3 Sec
- Lock when door is closed: OFF
- Use Automatic Door: OFF

Dual Authentication

- Device: No device

Anti-Tailgating

- Sensor: None

- **Open**: Set options for door opening.
  - **Open Time**: Set the duration for which the door remains open after authentication is complete. The door will automatically lock after this time.
  - **Lock when door is closed**: The door will lock when the door sensor detects it has closed. If set to **On**, the

option **Use Automatic Door** cannot be used.

- **Use Automatic Door**: If using an automatic door as the door, the relay can operate regardless of the door sensor's status. If set to **Lock when door is closed**, the option cannot be used.

> ⓘ **INFO**
>
> The **Open Time** may vary depending on the type of door locking device being used.

- **Dual Authentication**: Set to require two people (a regular user and an administrator) to authenticate credentials to open the door.
  - **Device**: Select the device to use for dual authentication. **Device**: Select the device for dual authentication.
  - **Schedule**: Select the schedule for using dual authentication. If the desired schedule is not available, click **+ Add Schedule** to add one.
  - **Approval Type**: Set the order of administrator authentication.
    - **None**: Two authentications are required regardless of the authentication group.
    - **Last**: The general user must authenticate first, followed by an authenticated user included in the set authentication group.
  - **Approval Group**: Set the group to which the administrator belongs. This option can be used when **Approval Type** is set to **Last**.
  - **Timeout**: Set the waiting time between the first and second authentications. **Timeout**: Set the waiting time until the second authentication after the first authentication.

> ⓘ **INFO**
>
> - To change the dual authentication of the device configured with the occupant limit setting, modify the settings in the following menu. **Settings** → **Advanced AC** → **Occupancy Limit** For more information about **Occupancy Limit** settings, refer to the following.
> - For more information about schedule settings, refer to the following.

- **Anti-Tailgating**: Set to detect tailgating where an unauthorized person follows an authorized person to enter.
  - **Sensor**: Select a sensor to detect tailgating.

Set anti-passback

Anti-passback is used to manage access history and enhance security. It can prevent cases where a user hands over their entry card to another user after entering and stop outsiders from entering when they follow users with access privileges.

Refer below to complete the settings in the **Anti PassBack** section.

- **Type**: Choose the type of anti-passback.
  - **None**: Does not utilize the anti-passback feature.
  - **Soft APB**: During an anti-passback violation, entry is allowed but will trigger an alarm or create a log in

BioStar X.

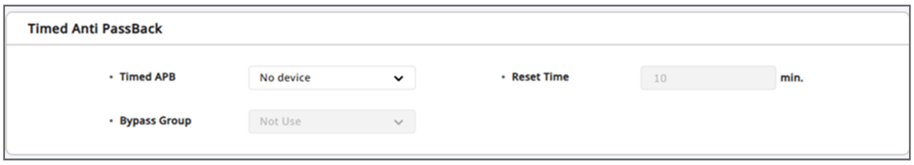
- **Hard APB**: During an anti-passback violation, entry is not allowed, and an alarm will sound or a log will be created in **BioStar X**.

- **Reset Time**: Set the time until the anti-passback feature resets. This can be set for up to 7 days (10080 minutes), and if set to 0, it will not reset.

> **INFO**
>
> - This can be used when both entry and exit devices are installed, and setting **Exit Device** option to **None** in the **Configuration** section will render it unusable. For the exit device setup method, refer to the following.
> - The **Anti PassBack** section requires a master device configured via RS-485 and a slave device.
> - If **Timed Anti PassBack** section is enabled, **Anti PassBack** cannot be used.

Set timed anti-passback

When a user attempts to re-authenticate on the same device after entry authentication, the anti-passback feature will prevent immediate re-authentication. The **Timed Anti PassBack** section sets the initialization time for the anti-passback feature to effectively limit frequent entries by users.



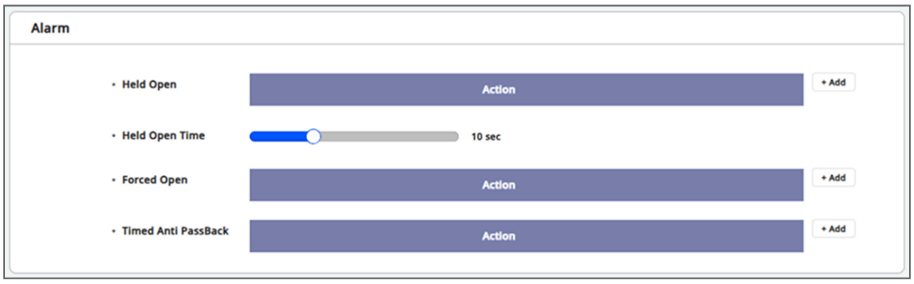
Timed Anti PassBack

- Timed APB: No device
- Reset Time: 10 min.
- Bypass Group: Not Use

- **Timed APB**: Select the device to use the timed anti-passback feature.
- **Reset Time**: Set the time until the anti-passback feature resets. The input unit is minutes (min), with a default of 10 minutes. It can be set for a maximum of 60 minutes.
- **Bypass Group**: Select access groups that can always pass without being subject to timed anti-passback.

Set alarms

In the **Alarm** section, you can configure to sound an alarm or block device usage when the door is forcibly opened, left open, or when an anti-passback violation occurs. Click the **+ Add** button for the item to add an alarm.



Alarm

- Held Open
- Held Open Time: 10 sec
- Forced Open
- Timed Anti PassBack

- **Held Open**: Configure alarm actions when the door is left open.
- **Held Open Time**: Set the time for the alarm to sound when the door has been open for an extended period.

Determine the maximum time the door may remain open.

- **Forced Open**: Configure alarm actions when the door is forcibly opened.
- **Anti PassBack** / **Timed Anti PassBack**: Set alarm actions for anti-passback or timed anti-passback violations.

> ⓘ **INFO**
>
> The **Anti PassBack** option can only be set if the exit device is registered.

Modify Door Information

This guide describes how to modify the settings information of the registered access door. Change detailed settings for individual doors or select multiple doors to modify common items in bulk.

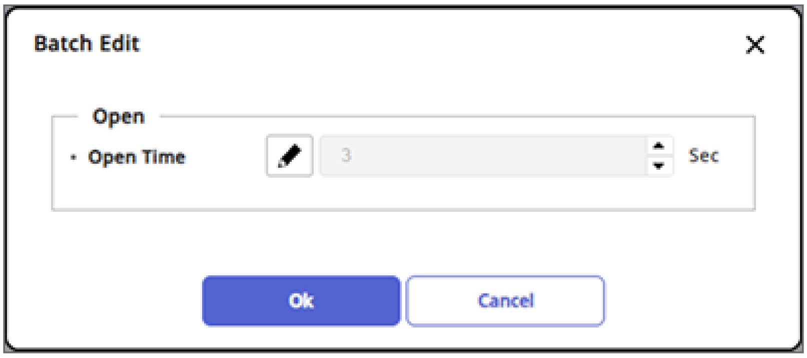
Modify information for a door

1. Click **Settings** on the **Launcher** page.
2. Click **Door** in the left sidebar.
3. Click the door you wish to modify in the door list.
4. Modify the details in each section.
5. Once all configurations are complete, click the **Apply** button at the bottom of the screen.

> **INFO**
>
> For detailed information on each section of the door modification screen, refer to the following.

Batch edit multiple doors

1. Click **Settings** on the **Launcher** page.
2. Click **Door** in the left sidebar.
3. Click the checkboxes for the doors you wish to modify in the door list. Select two or more doors.
4. Click **Batch Edit** at the top right of the screen.
5. When the **Batch Edit** window appears, set your desired options.



Batch Edit

Open

- Open Time: 3 Sec

   - **Open Time**: Set the duration for which the door remains open after authentication is complete. The door will automatically lock after this time.

6. After completing all settings, click **Apply**.

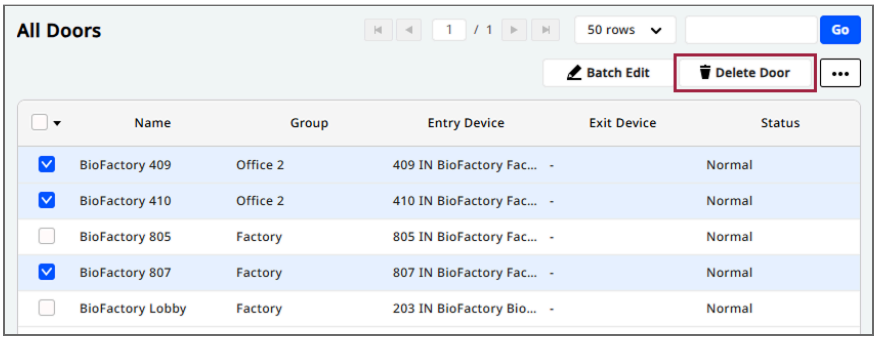
INFO

Batch Edit is activated only when two or more doors are selected from the door list.

Delete Door

This guide describes how to delete registered doors.

1. Click **Settings** on the **Launcher** page.
2. Click **Door** in the left sidebar.
3. Click the checkbox of the door you want to delete from the list.
4. Click the **Delete Door** button at the top right of the screen.



□	Name	Group	Entry Device	Exit Device	Status
☑	BioFactory 409	Office 2	409 IN BioFactory Fac...	-	Normal
☑	BioFactory 410	Office 2	410 IN BioFactory Fac...	-	Normal
□	BioFactory 805	Factory	805 IN BioFactory Fac...	-	Normal
☑	BioFactory 807	Factory	807 IN BioFactory Fac...	-	Normal
□	BioFactory Lobby	Factory	203 IN BioFactory Bio...	-	Normal

5. Click the **Yes** button when the confirmation message window appears.

The selected door will be deleted. Deleted doors cannot be recovered.

> **INFO**
>
> The **Delete Door** button is enabled only when one or more doors are selected from the access door list.

Manage Operation Permissions

This guide describes how to assign operator permissions and add and configure custom permissions to registered users. Operator permissions control the tasks a user can perform on **Biostar X**. **Custom permissions** allow the setting of additional permissions beyond the default operator permissions.

Check permission types

Click **Settings** on the **Launcher** page. Click **Account** on the left sidebar. Refer to the provided accounts based on permission levels.

- **Administrator**: This is an administrator level that can use all menus.
- **User Operator**: **User** menu has **read** and **write** permissions.
- **Monitoring Operator**: **Monitoring**, **Data**, and **Dashboard** menus have **read** and **write** permissions.
- **T&A Operator**: **TIME ATTENDANCE** menu has **read** and **write** permissions.
- **Visitor Operator**: **VISITOR** menu has **read** and **write** permissions.

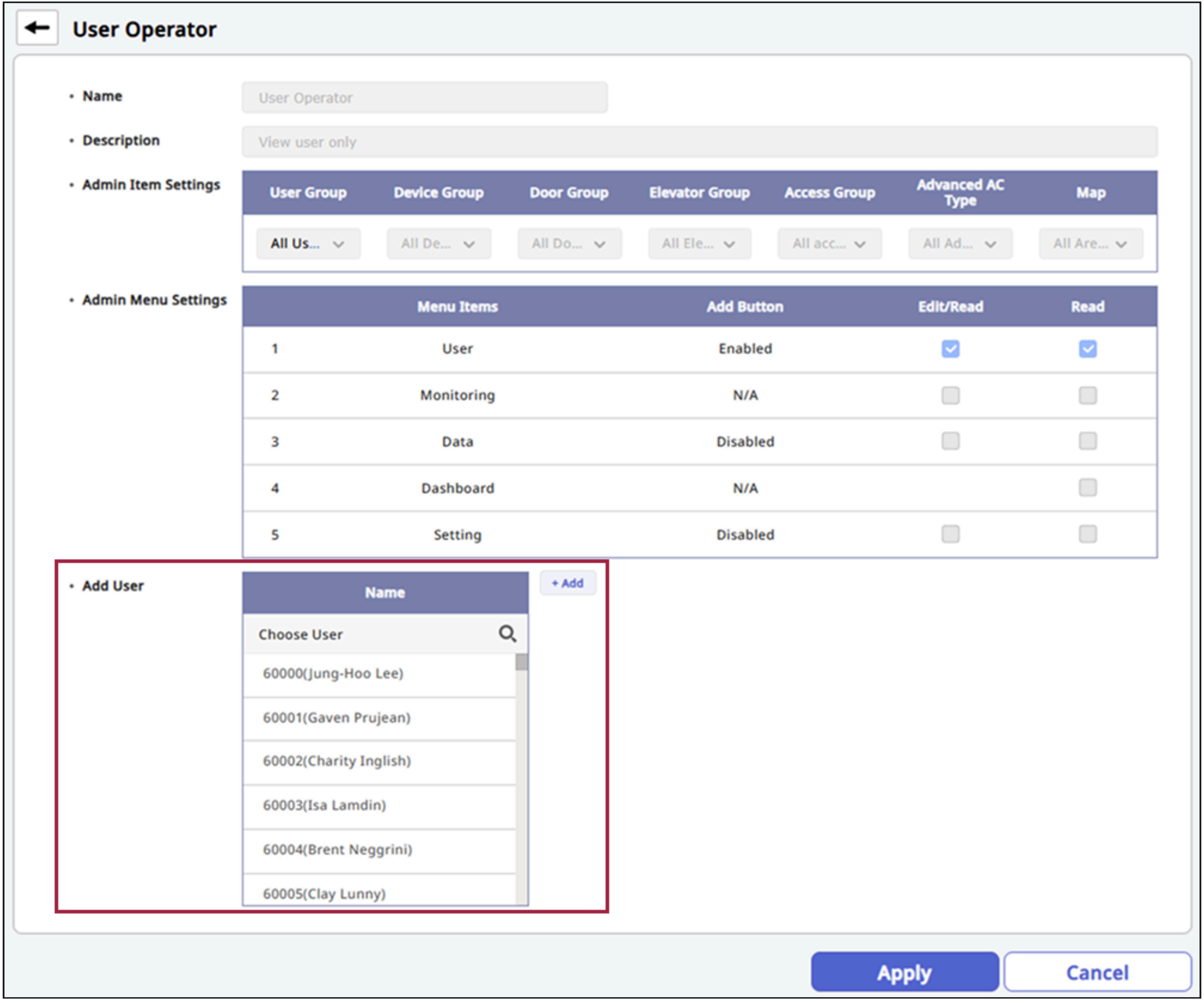
> ⓘ **INFO**
>
> - To add new user permissions other than the predefined ones, refer to the following.
> - The permissions of the default accounts cannot be modified or deleted.
> - Levels such as **T&A Operator** and **Visitor Operator** require separate licenses. For more information on licensing policy, refer to the following.

Granting operator permissions to users

Guide on granting operator permissions to general users.

1. Click **Settings** on the **Launcher** page.
2. Click **Account** on the left sidebar.
3. Click the desired item from the account list.

4. Click **+ Add** in the **Add User** option.



User Operator

- Name: User Operator
- Description: View user only
- Admin Item Settings

User Group	Device Group	Door Group	Elevator Group	Access Group	Advanced AC Type	Map
All Us...	All De...	All Do...	All Ele...	All acc...	All Ad...	All Are...

- Admin Menu Settings

	Menu Items	Add Button	Edit/Read	Read
1	User	Enabled	☑	☑
2	Monitoring	N/A	☐	☐
3	Data	Disabled	☐	☐
4	Dashboard	N/A		☐
5	Setting	Disabled	☐	☐

- Add User

Name
Choose User
60000(Jung-Hoo Lee)
60001(Gaven Prujean)
60002(Charity Inglish)
60003(Isa Lamdin)
60004(Brent Neggrini)
60005(Clay Lunny)

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

5. Select the user to whom you want to grant operator permissions from the user list.

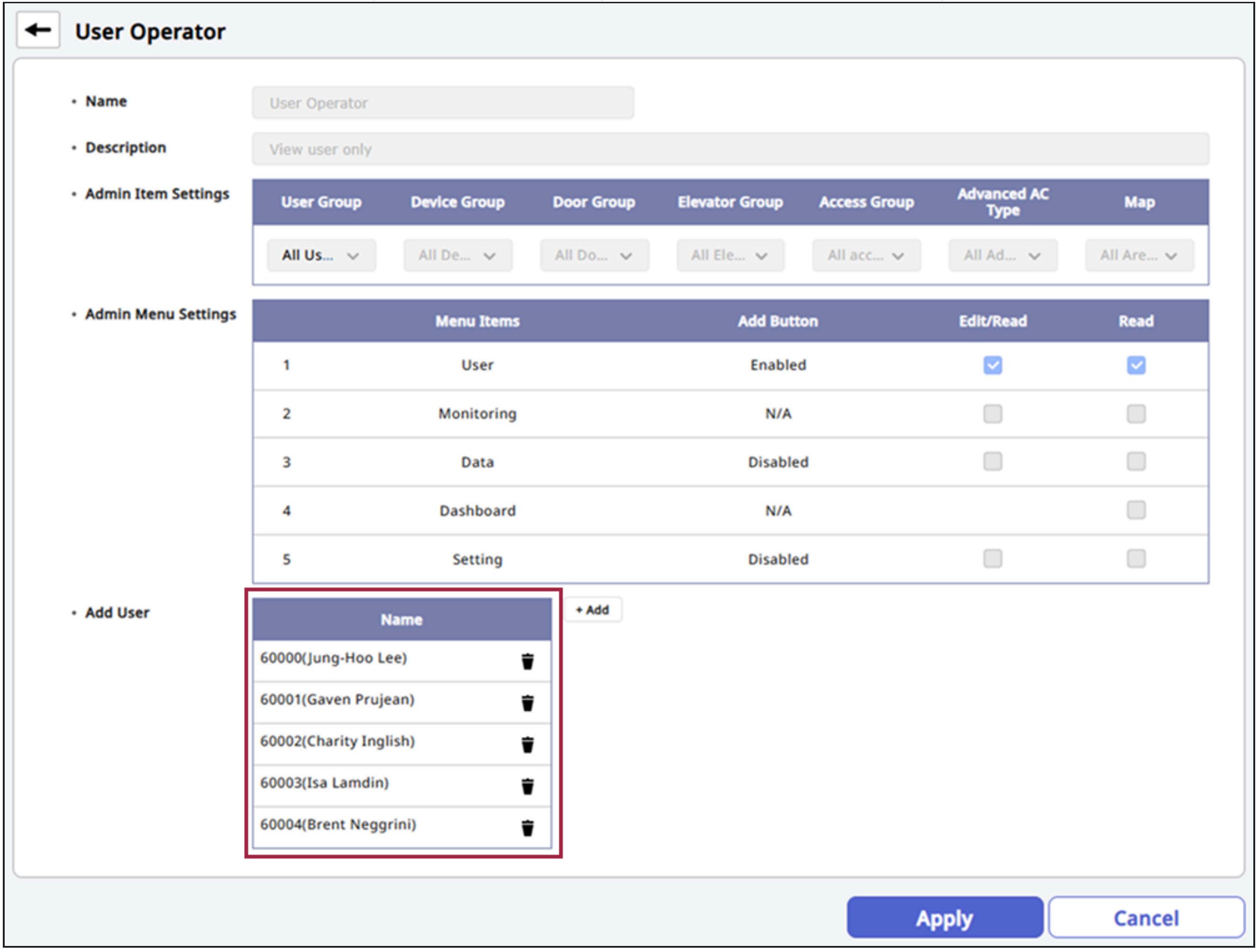
6. After selecting all desired users, click **Apply** at the bottom of the screen.

> **INFO**
>
> - If it's difficult to find users due to their quantity, click 🔍 to search and select the desired user.
> - Operator permissions can also be granted when adding or modifying user information. Please refer to the following for details.
> - If permissions have already been set when adding or modifying user information, they will be included in the **Add User** option.

Excluding operator permissions

Guide on excluding operator permissions granted to users.

1. Click **Settings** on the **Launcher** page.
2. Click **Account** on the left sidebar.
3. Click the desired account type from the account list.
4. Click 🗑 for the user from whom you wish to exclude permissions in the **Add User** option.



User Operator

- Name: User Operator
- Description: View user only
- Admin Item Settings

User Group	Device Group	Door Group	Elevator Group	Access Group	Advanced AC Type	Map
All Us...	All De...	All Do...	All Ele...	All acc...	All Ad...	All Are...

- Admin Menu Settings

	Menu Items	Add Button	Edit/Read	Read
1	User	Enabled	☑	☑
2	Monitoring	N/A	□	□
3	Data	Disabled	□	□
4	Dashboard	N/A		□
5	Setting	Disabled	□	□

- Add User

Name	
60000(Jung-Hoo Lee)	🗑
60001(Gaven Prujean)	🗑
60002(Charity Inglish)	🗑
60003(Isa Lamdin)	🗑
60004(Brent Neggrini)	🗑

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

5. Click **Apply** at the bottom of the screen to save the settings.

Checking operator permission details

Click the account in the account list in the **Account** menu to view the details of the operational permissions for that account.

- **Name**: The name of the selected operator permission.

- **Description**: A brief description of the permission.
- **Admin Item Settings**: Can view the groups granted permissions item by item.
- **Admin Menu Settings**: Can view the permissions granted to access the menu.
  - **Edit/Read**: Grants permission to add, edit, or delete items in the menu.
  - **Read**: Grants permission to enter the menu and only view the settings.
- **Add User**: Can view users granted permissions.

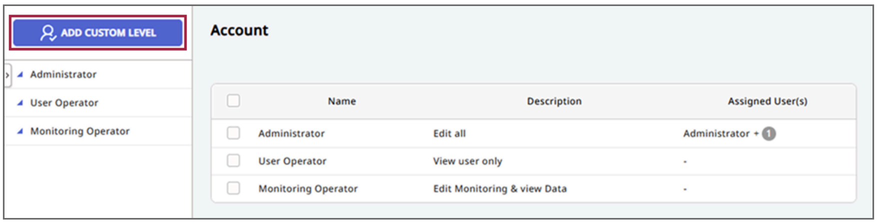
> ⓘ **INFO**
>
> For methods to grant permissions to specific users, refer to the following.

Add Custom Permissions

This guide describes how to add the desired permission level. Custom permissions are user-customizable features that allow for additional permissions beyond the default operational permissions.

Add custom permissions

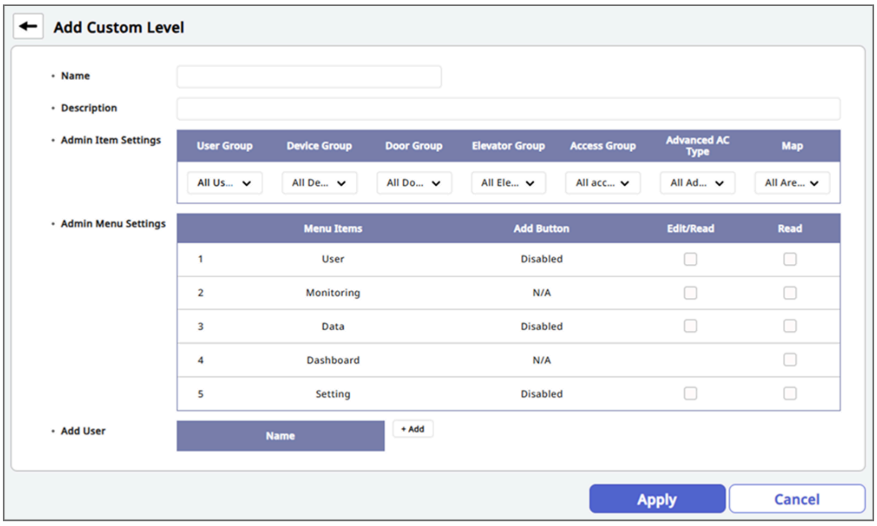
1. Click **Settings** on the **Launcher** page.
2. Click **Account** on the left sidebar.
3. Click **Add Custom Level**.



Account

□	Name	Description	Assigned User(s)
□	Administrator	Edit all	Administrator + 1
□	User Operator	View user only	-
□	Monitoring Operator	Edit Monitoring & view Data	-

4. Enter a name and description for the newly created permission.



Add Custom Level

- Name
- Description
- Admin Item Settings

User Group	Device Group	Door Group	Elevator Group	Access Group	Advanced AC Type	Map
All Us...	All De...	All Do...	All Ele...	All acc...	All Ad...	All Are...

- Admin Menu Settings

	Menu Items	Add Button	Edit/Read	Read
1	User	Disabled	□	□
2	Monitoring	N/A	□	□
3	Data	Disabled	□	□
4	Dashboard	N/A		□
5	Setting	Disabled	□	□

- Add User

Name

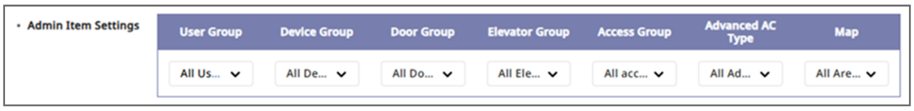
5. Fill in or select each of the remaining items.
6. Click **Apply** at the bottom of the screen to save the settings.

INFO

- The types of **Admin Menu Settings** settings you can configure may vary depending on the activated license type.
- For more information about **Admin Item Settings**, refer to the following.
- For more information about **Admin Menu Settings**, refer to the following.
- For more information about **Add User**, refer to the following.

Admin Item Settings

Set detailed permissions for items. You can select groups to grant edit and view permissions for each menu. You can set item permissions for **User Group**, **Device Group**, **Door Group**, **Access Group** based on the information of already created groups in each menu.



- Admin Item Settings

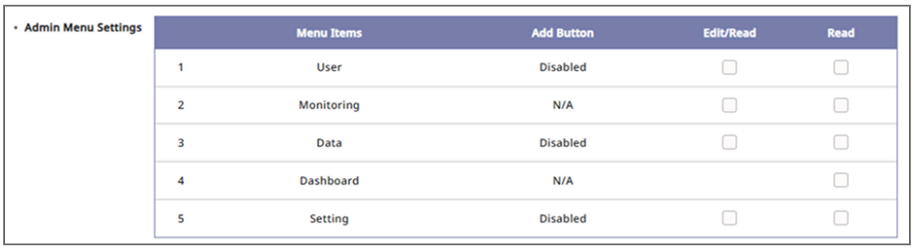
User Group	Device Group	Door Group	Elevator Group	Access Group	Advanced AC Type	Map
All Us...	All De...	All Do...	All Ele...	All acc...	All Ad...	All Are...

INFO

- If your desired group is not available, go to the appropriate menu to add a new group. For more information about adding groups, refer to the followings:
  - User group management
  - Device group management
  - Door group management
  - Elevator group management
  - Register and manage access groups
- The permissions for **Elevator Group**, **Advanced AC Type**, **Map** are available with an **Advanced** license or higher. For more information on the licensing policy, refer to the following.

Admin Menu Settings

Set **edit** and **view** permissions for individual menus. Different permissions can be configured for each menu.



- Admin Menu Settings

	Menu Items	Add Button	Edit/Read	Read
1	User	Disabled	□	□
2	Monitoring	N/A	□	□
3	Data	Disabled	□	□
4	Dashboard	N/A		□
5	Setting	Disabled	□	□

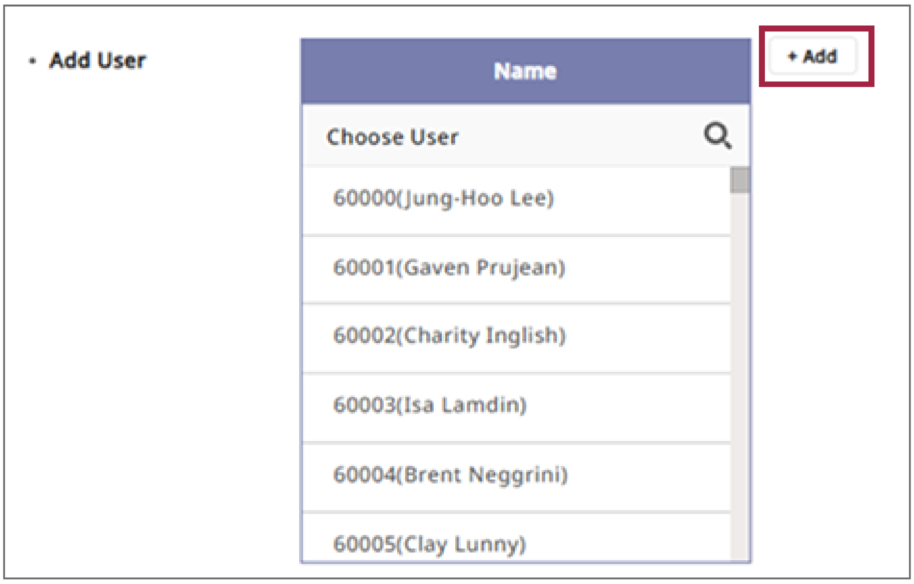
- **Edit/Read**: Grants permission to add, edit, or delete items in the menu.

- **Read**: Grants permission to enter the menu and only view the settings.

> **INFO**
>
> Granting **edit** permissions for each menu activates the **Add** button. However, for the **Dashboard** and **Settings** menus, since there are no additional features, they will be displayed as **N/A**. For the **Access Control** menu, the **Admin Item Settings** must have **Access Group** set to **All access groups** and **edit** permissions granted in order for the **Add** button to be activated.

Add User

You can add or verify user information for granting permissions. Click the **+ Add** button to add a user. Select the user to grant permissions from the user list.



60000(Jung-Hoo Lee)

60001(Gaven Prujean)

60002(Charity Inglish)

60003(Isa Lamdin)

60004(Brent Neggrini)

60005(Clay Lunny)

> **INFO**
>
> Clicking 🗑 next to a user in the user list will exclude that user from permissions.

Access Control Settings

This guide describes how to set up access control system Set entry points and entry times to create access levels, and configure access groups using access levels and user group information. Use the configured access groups for access control configuration.

Manage Access Levels

Set the time periods during which a user may access a door and register them as an access level.

Manage Access Groups

Set access groups using access levels and user group information.

Manage Floor Levels

Set floor levels using the configured elevator and floor information.

Check Access Permission Status

Check the list of doors that users can access.

Manage Access Levels

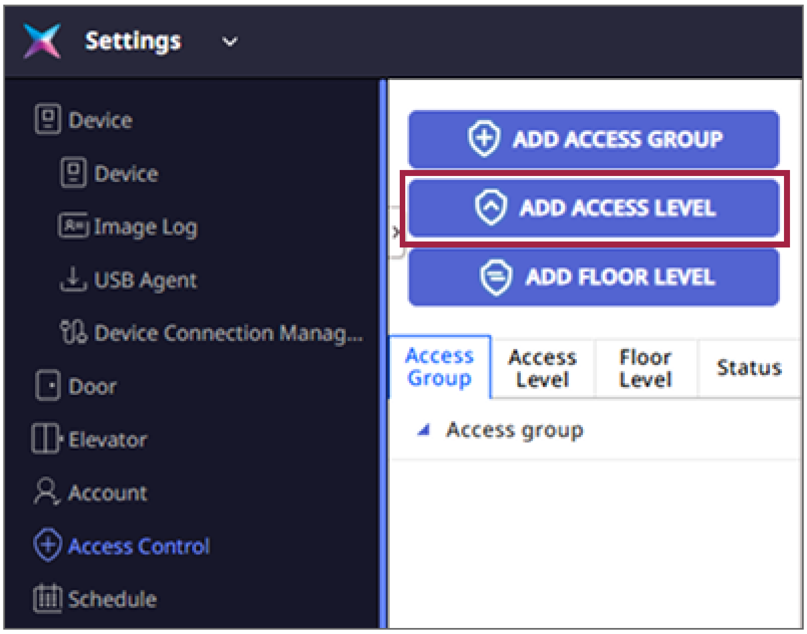
Access levels enable users to set times for entry and grant permission to access doors during those times. Access levels are a key element for configuring access groups.

Before start

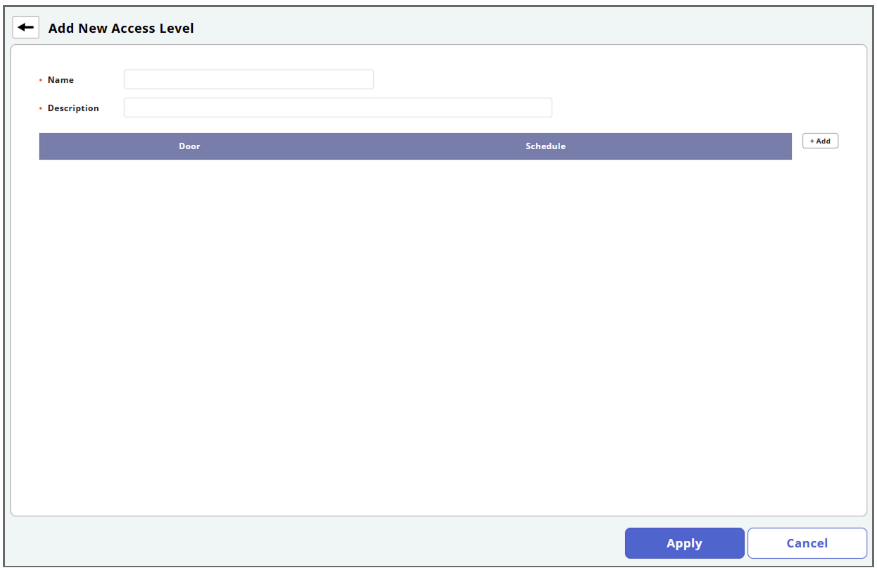
- Initialize doors before enrolling access levels. For more information about door enrollment, refer to the following.
- You can predefine time to apply to access levels through schedule settings. For more information about schedule settings, refer to the following.

Register access level

1. Click **Settings** on the **Launcher** page.
2. Click **Access Control** on the left sidebar.
3. Click **ADD ACCESS LEVEL**.



4. Enter **Name** and **Description** in the **Add New Access Level** screen.



5. Select the door to apply the access level in the **Door** field.

6. Select the schedule to apply the access level in the **Schedule** field.

7. Click **Apply** at the bottom of the screen to register the access level.

ⓘ **INFO**

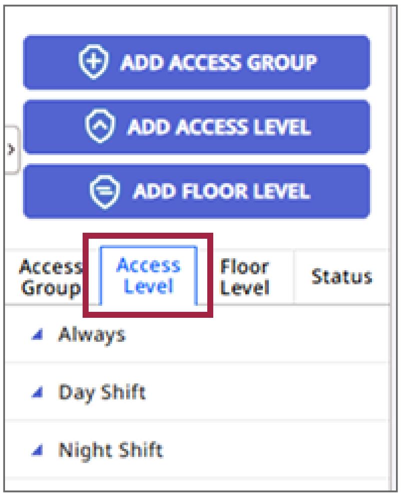
- Up to 128 access levels can be registered per access group.
- Click 🔍 in the **Door** and **Schedule** fields to search for the desired doors and schedules.
- Click 🗑 to delete items added in the **Door** and **Schedule** fields.
- If the desired door is not available, you need to register a new door. For more information about door enrollment, refer to the following.
- If the desired schedule is not available, click **+ Add Schedule** to add one. For more information about schedule settings, refer to the following.

Modify access level

1. Click **Settings** on the **Launcher** page.

2. Click **Access Control** in the left sidebar.

3. Click the **Access Level** tab.



4. Click the access level you wish to modify from the access level list.

5. Modify the desired items.

6. Once modifications are complete, click **Apply** at the bottom of the screen.

Delete access level

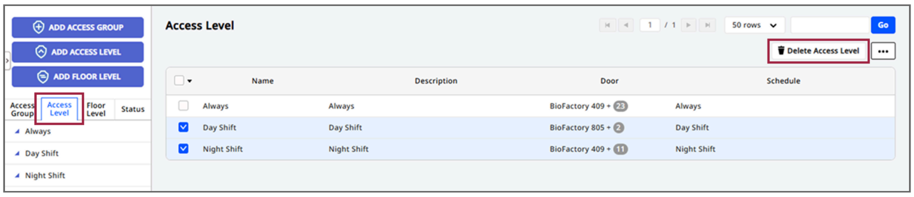
1. Click **Settings** on the **Launcher** page.

2. Click **Access Control** in the left sidebar.

3. Click the **Access Level** tab.

4. Check the checkbox of the access level you wish to delete from the access level list.

5. Click **Delete Access Level** at the top right of the screen.



□	Name	Description	Door	Schedule
□	Always	Always	BioFactory 409 + 23	Always
☑	Day Shift	Day Shift	BioFactory 805 + 2	Day Shift
☑	Night Shift	Night Shift	BioFactory 409 + 11	Night Shift

Manage Access Groups

This guide describes how to set up access groups using access levels and user group information. Access groups are crucial elements that define permission for accessing doors. Setting up access groups enables management of user permissions to access doors.

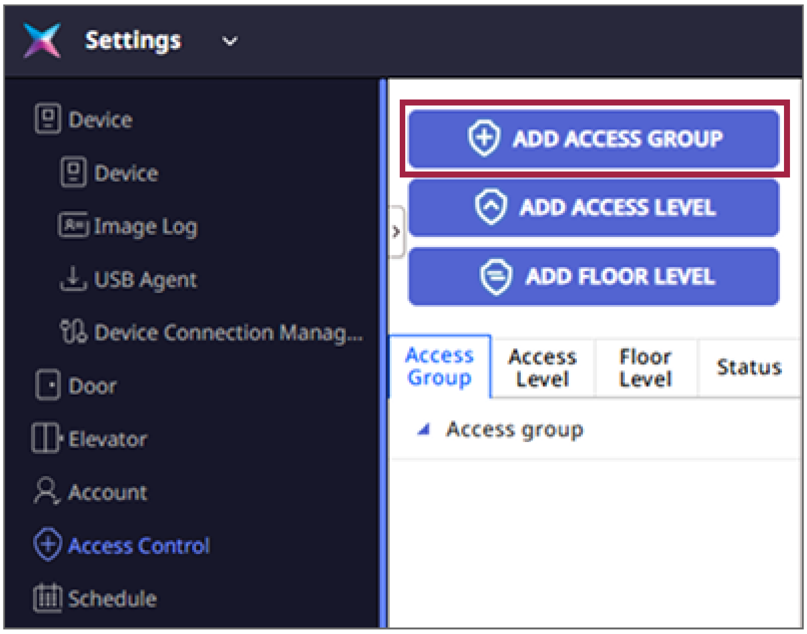
Before start

Confirm the following before registering access groups.

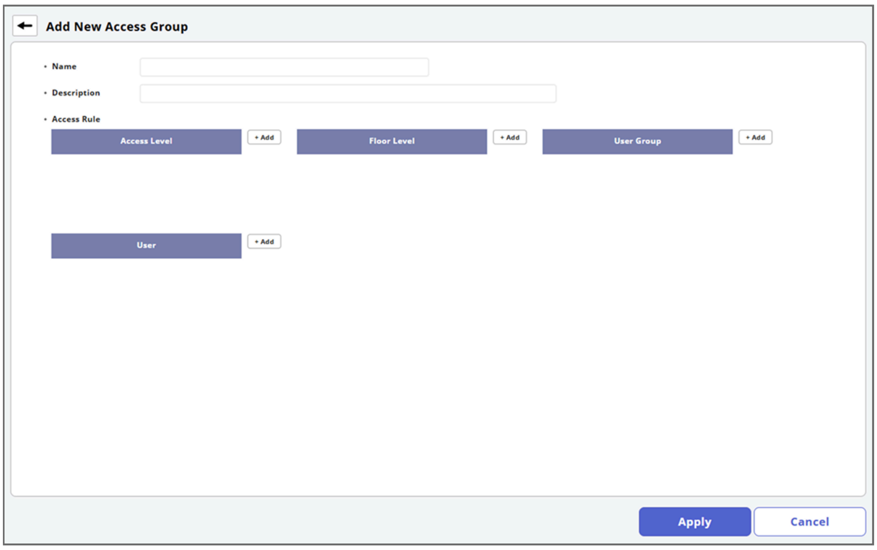
- Set up access levels. For more information about registering access levels, refer to the following.
- Set up floor levels. For more information about the floor levels, refer to the following.
- Set up user groups. For more information about registering user groups, refer to the following.

Register access groups

1. Click **Settings** on the **Launcher** page.
2. Click **Access Control** in the left sidebar.
3. Click **ADD ACCESS GROUP**.



4. On the **Add New Access Group** screen, enter **Name** and **Description**.



5. In the **Access Level** field, click **+ Add** to select the access levels to apply to the access group.

6. In the **Floor Level** field, click **+ Add** to select the floor levels to apply to the access group.

7. In the **User Group** field, click **+ Add** to select the user groups to apply to the access group.

8. In the **User** field, click **+ Add** to select users for the access group.

9. To register the access group, click **Apply** at the bottom of the screen.

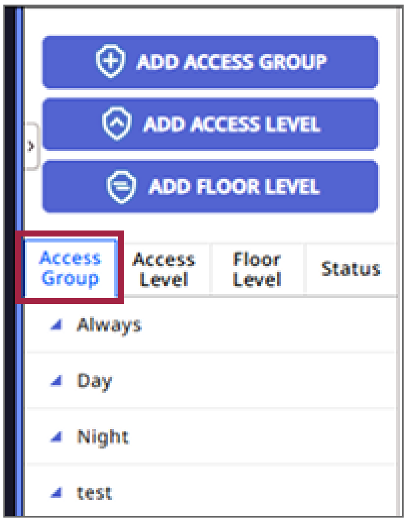
> **INFO**
>
> - If the desired access level is not available, you will need to register a new access level. For more information about registering access levels, refer to the following.
> - If the desired floor level is not available, you will need to register a new floor level. For more information about the floor levels, refer to the following.
> - To delete added items, click 🗑.
> - To search for a desired item, click 🔍.

Edit access groups

1. Click **Settings** on the **Launcher** page.

2. Click **Access Control** in the left sidebar.

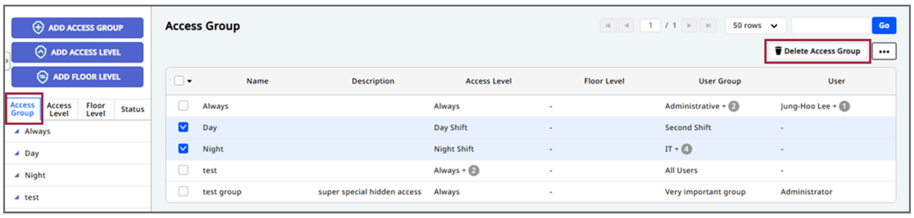
3. Click the **Access Group** tab.



4. Click the access group you want to edit from the list.
5. Modify the desired items.
6. Once modifications are complete, click **Apply** at the bottom of the screen.

Delete access groups

1. Click **Settings** on the **Launcher** page.
2. Click **Access Control** in the left sidebar.
3. Click the **Access Group** tab.
4. Check the checkbox for the access group you wish to delete from the list.
5. Click **Delete Access Group** in the upper right corner of the screen.



Access Group

□	Name	Description	Access Level	Floor Level	User Group	User
□	Always		Always	-	Administrative + 2	Jung-Hoo Lee + 1
☑	Day		Day Shift	-	Second Shift	-
☑	Night		Night Shift	-	IT + 4	-
□	test		Always + 2	-	All Users	-
□	test group	super special hidden access	Always	-	Very important group	Administrator

Manage Floor Levels

This guide describes how to set floor levels using the configured elevator and floor information. Floor levels are important elements that can be applied to access groups. By setting floor levels, you can manage the floors users are allowed to access via the elevator.

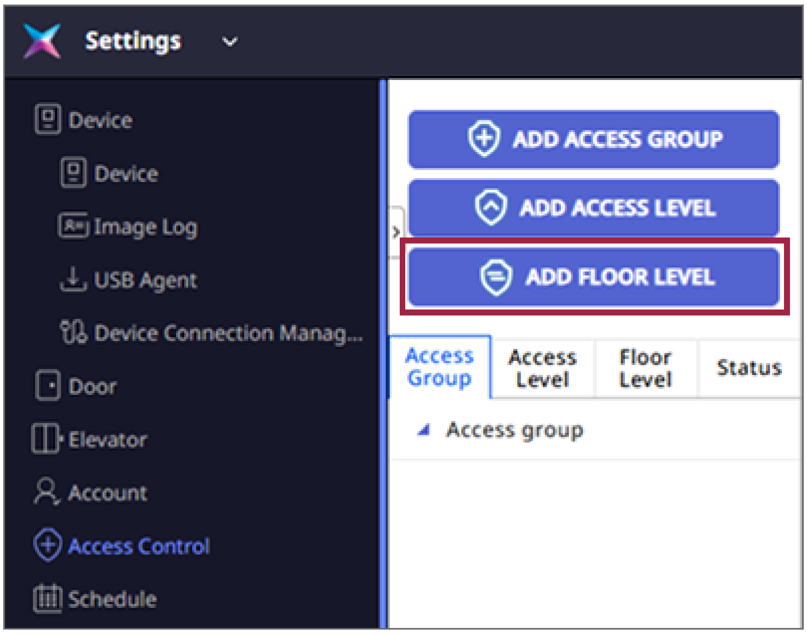
> **INFO**
>
> You can only use the **Floor Level** tab and **ADD FLOOR LEVEL** button with a license of **Advanced** or higher. For more information about the license policy, refer to the following.

Before start

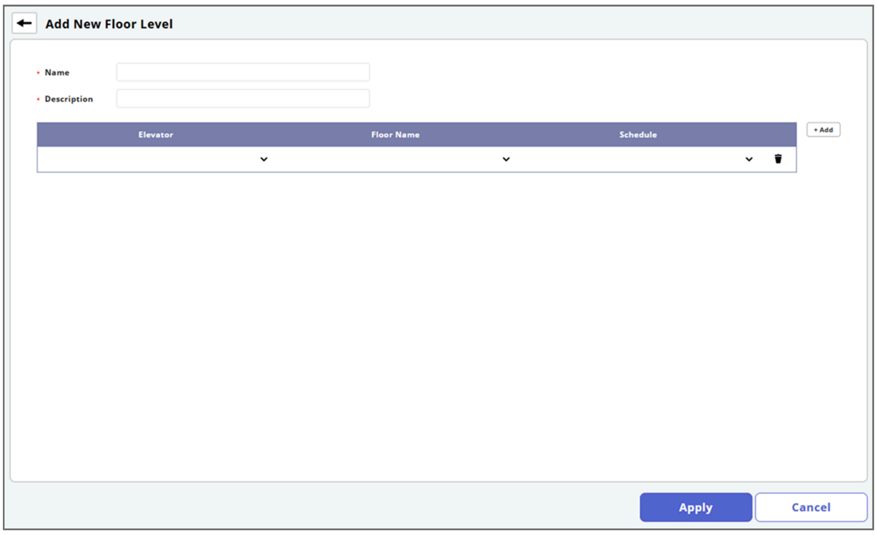
- You must set up the elevator before enrolling floor levels. For more information about elevator enrollment, refer to the following.
- You can define the time to apply to the floor grade in advance through schedule settings. For more information about schedule settings, refer to the following.

Register floor levels

1. Click **Settings** on the **Launcher** page.
2. Click **Access Control** on the left sidebar.
3. Click **ADD FLOOR LEVEL**.



4. In the **Add New Floor Level** screen, enter **Name** and **Description**.



5. Select the elevator to apply to the floor grade in the **Elevator** item.

6. Select the floor to apply to the floor grade in the **Floor Name** item.

7. Select the schedule to apply to the floor grade in the **Schedule** item.

8. Click **Apply** at the bottom of the screen to register the floor level.

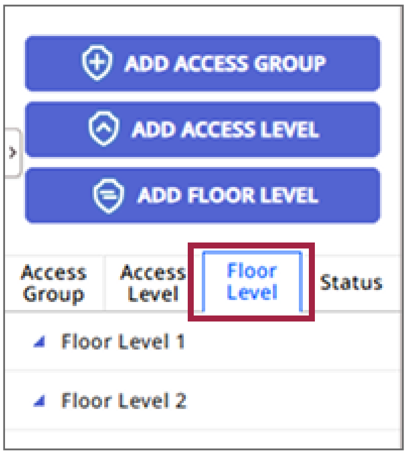
> **INFO**
>
> - If the desired access level is not available, you will need to register a new access level. For more information about registering access levels, refer to the following.
> - If the desired elevator is not available, you need to register a new elevator. For more information about elevator enrollment, refer to the following.
> - If the desired schedule is not available, click **+ Add Schedule** to add one. For more information about schedule settings, refer to the following.
> - To delete added items, click 🗑.
> - To search for a desired item, click 🔍.

Edit floor levels

1. Click **Settings** on the **Launcher** page.

2. Click **Access Control** in the left sidebar.

3. Click the **Floor Level** tab.



4. Click the floor level you want to edit from the floor level list.

5. Modify the desired items.

6. Once modifications are complete, click **Apply** at the bottom of the screen.

Delete floor levels

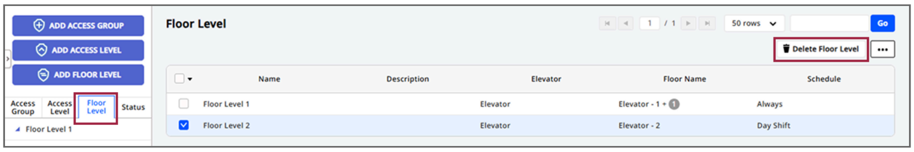
1. Click **Settings** on the **Launcher** page.

2. Click **Access Control** in the left sidebar.

3. Click the **Floor Level** tab.

4. Click the checkbox of the floor level you want to delete from the floor level list.

5. Click **Delete Floor Level** at the top right of the screen.



Floor Level

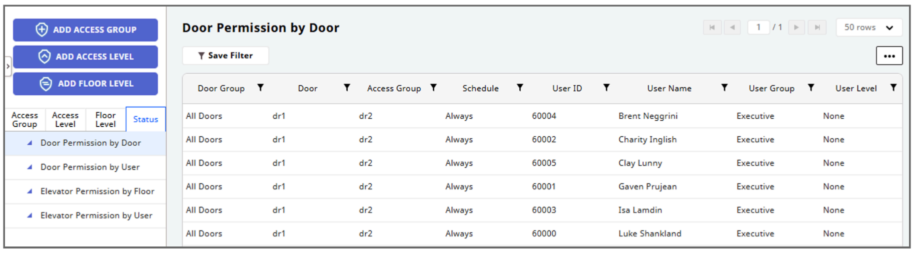
□	Name	Description	Elevator	Floor Name	Schedule
□	Floor Level 1		Elevator	Elevator - 1 + 1	Always
☑	Floor Level 2		Elevator	Elevator - 2	Day Shift

Check Access Permission Status

This guide explains how to check the list of doors accessible by users. By checking the access permission status, you can manage the doors a user can access and the permissions for those doors. Use the filter feature to sort the desired results, and you can save the list as a CSV file.

Check access permission status

Access permissions can be viewed by door or floor, or by user.



Door Permission by Door

Door Group	Door	Access Group	Schedule	User ID	User Name	User Group	User Level
All Doors	dr1	dr2	Always	60004	Brent Neggrini	Executive	None
All Doors	dr1	dr2	Always	60002	Charity Inglish	Executive	None
All Doors	dr1	dr2	Always	60005	Clay Lunny	Executive	None
All Doors	dr1	dr2	Always	60001	Gaven Prujean	Executive	None
All Doors	dr1	dr2	Always	60003	Isa Lamdin	Executive	None
All Doors	dr1	dr2	Always	60000	Luke Shankland	Executive	None

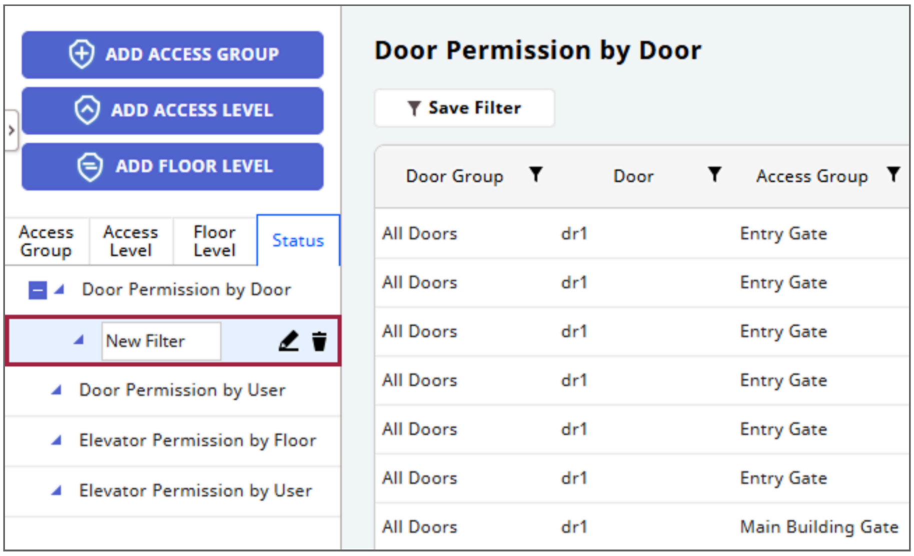
1. Click **Settings** on the **Launcher** page.
2. Click **Access Control** on the left sidebar.
3. Click the **Status** tab.
4. Click the desired item from the list of statuses under the **Status** tab.
   - **Door Permission by Door**
   - **Door Permission by User**
   - **Elevator Permission by Floor**
   - **Elevator Permission by User**

You can check the access permission status for the selected item.

Save filter

To sort the desired results, click the ▼ button in the header of the access permission list table. You can add filter conditions.

After setting the filter, you can save it. Click **Save Filter**. The saved filter can be checked in the status list under the **Status** tab.



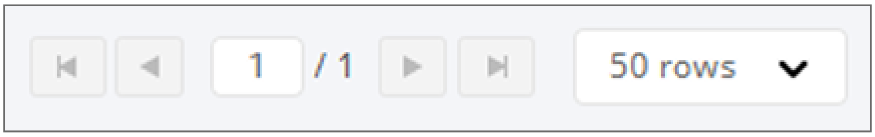
Door Permission by Door

Door Group	Door	Access Group
All Doors	dr1	Entry Gate
All Doors	dr1	Entry Gate
All Doors	dr1	Entry Gate
All Doors	dr1	Entry Gate
All Doors	dr1	Entry Gate
All Doors	dr1	Entry Gate
All Doors	dr1	Main Building Gate

- Click ✎ to rename the filter.
- Click 🗑 to delete the filter.

Navigate the list page

Move between pages or set the number of items to appear on each page. Use the page navigation tool in the top right corner of the screen.



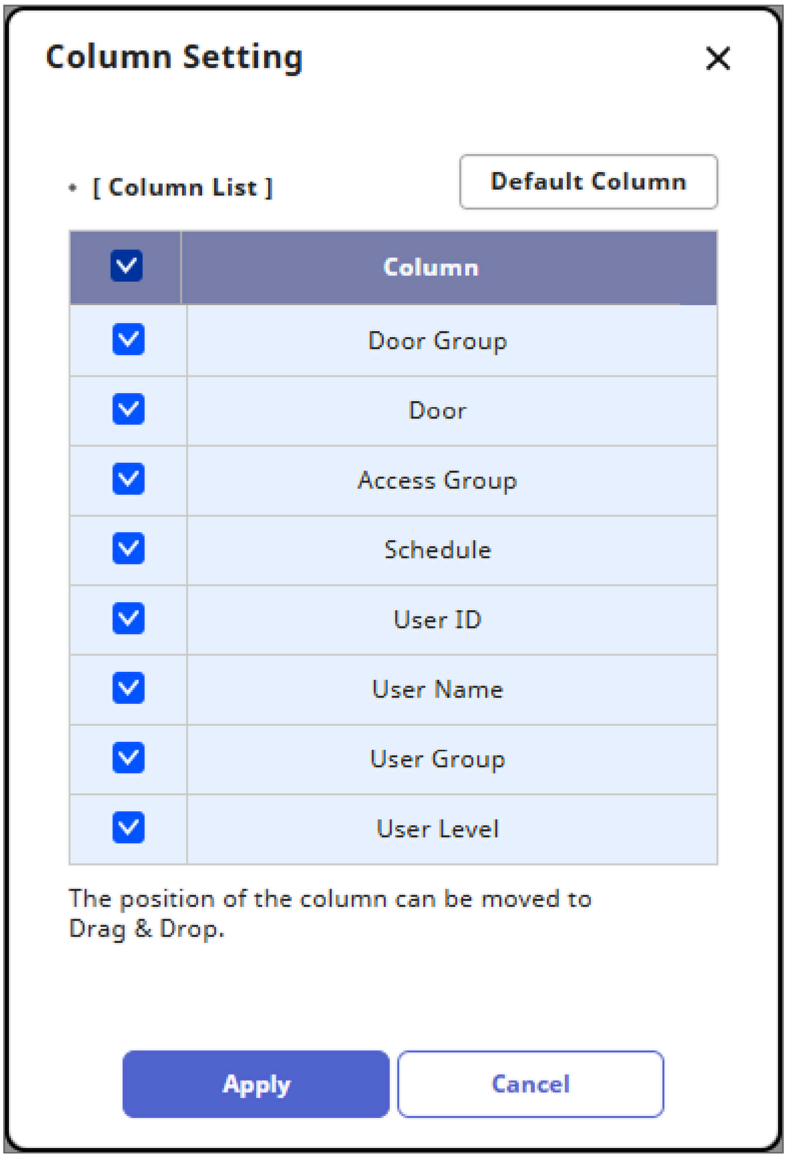
- ⏮: Move to the first page.
- ◀: Move to the previous page.
- ▶: Move to the next page.
- ⏭: Move to the last page.
- Enter the page number in the input field to move to the desired page.
- Click the row selection box to set the number of items displayed on each page.

Export to CSV

You can export the current access permission status list as a CSV file. Click ⋯ at the top right of the screen and select **CSV Export**.

Set columns

You can hide or display desired columns in the current access permission status list table. Click ⋯ at the top right of the screen and select **Column Setting**.



Column Setting

• [Column List]

☑	Column
☑	Door Group
☑	Door
☑	Access Group
☑	Schedule
☑	User ID
☑	User Name
☑	User Group
☑	User Level

The position of the column can be moved to Drag & Drop.

- Select the columns to display from **Column List**. The selected columns will appear in the list table. The unselected columns will be hidden from the list table.
- Click **Default Column** to initialize the settings.

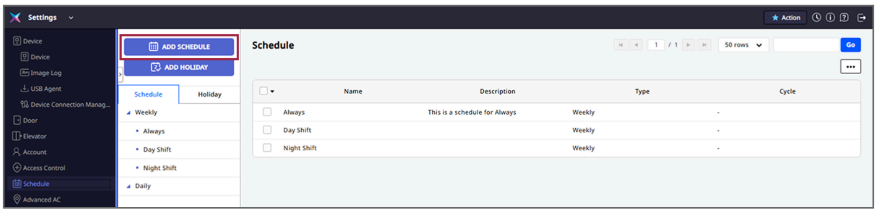
Once all settings are complete, click **Apply**.

Schedule Settings

This guide describes how to efficiently operate access control and attendance management by setting up access and holiday schedules. Schedules are an important factor that can be applied to access control, allowing management of user access times and holidays.

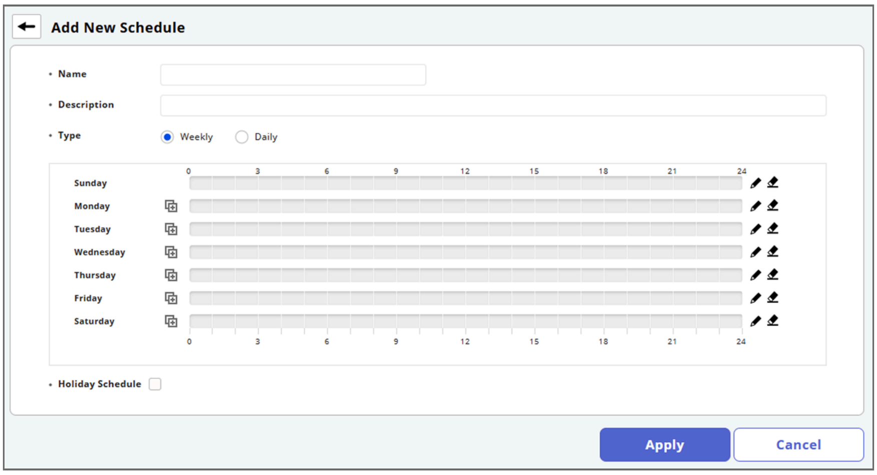
Register schedule

1. Click **Settings** on the **Launcher** page.
2. Click **Schedule** in the left sidebar.
3. Click the **ADD SCHEDULE** button at the top left of the screen.



Name	Description	Type	Cycle
Always	This is a schedule for Always	Weekly	-
Day Shift		Weekly	-
Night Shift		Weekly	-

4. Enter or set each item on the **Add New Schedule** screen.



Type ● Weekly ○ Daily

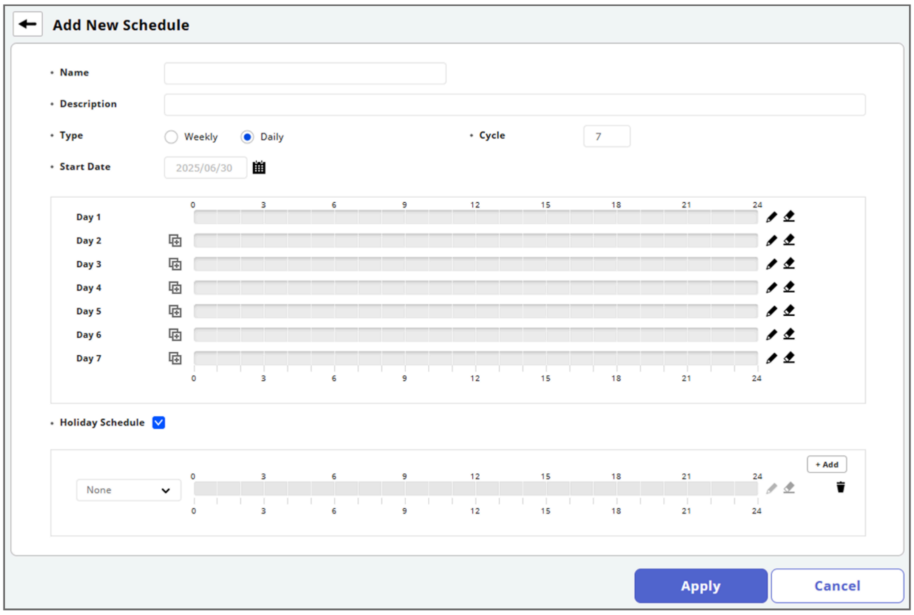
Holiday Schedule □

5. Once all settings are complete, click the **Apply** button at the bottom of the screen.

> **INFO**
>
> For detailed information about individual items on the **Add New Schedule** screen, refer to the following.

New schedule addition options guide

Guide to individual items that can be set on the **Add New Schedule** screen.



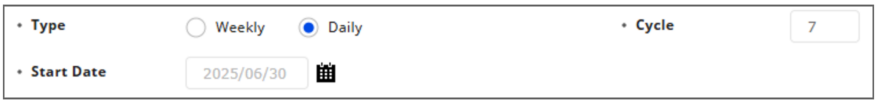
Add New Schedule

- Name
- Description
- Type ○ Weekly ● Daily
- Cycle 7
- Start Date 2025/06/30

- Holiday Schedule ☑

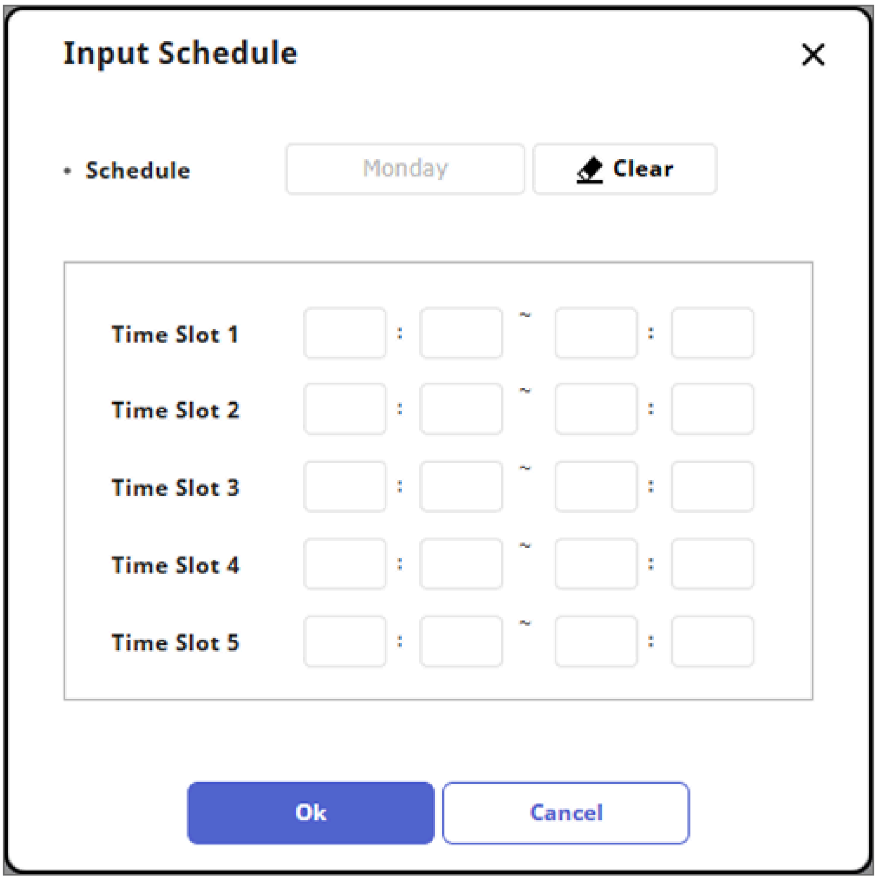
Apply Cancel

- **Name**: Enter the schedule name.
- **Description**: Enter a brief description of the schedule.
- **Type**: Choose a weekly or daily schedule. Selecting **Daily** will allow you to select **Cycle** and **Start Date**.



- Type ○ Weekly ● Daily
- Cycle 7
- Start Date 2025/06/30

- Click the **Time segment** in the middle area to set the desired time. Once completed, click the **Apply** button.



Input Schedule

- Schedule Monday Clear

Time Slot 1		:		~		:	
Time Slot 2		:		~		:	
Time Slot 3		:		~		:	
Time Slot 4		:		~		:	
Time Slot 5		:		~		:	

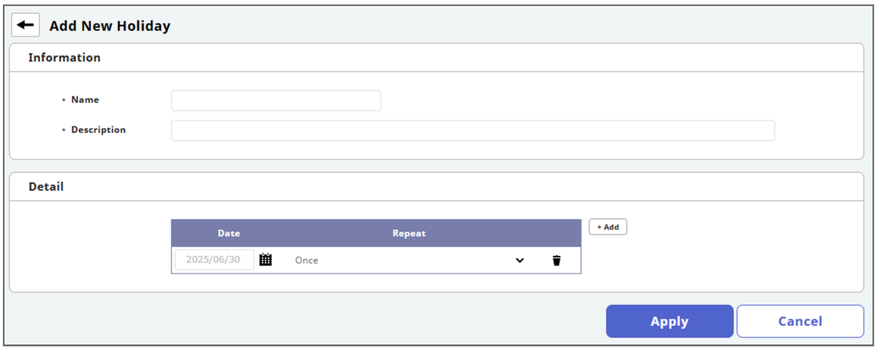
Ok Cancel

  - You can set up to 5 time slots per day or weekly.
  - To copy the time slots set above, schedule them and click the ⧉ button.
  - Click the ✎ button to modify a time slot. Click the ⌫ button to delete a set time slot.
- **Holiday Schedule**: Choose whether to apply holiday schedules. Selecting an item allows for detailed settings.
  - Select the **None** checkbox to choose pre-set holidays. To add more holidays, click **+ Add** and set the holidays.
  - **Holiday Time Slots**: Click the time slots to set the time slots to be applied on holidays.

> ⓘ **INFO**
>
> - Click the ✎ button to modify a time slot. Click the ⌫ button to delete a set time slot.
> - To delete added holidays, click 🗑.
> - For detailed information on adding holiday schedules, refer to the following.

Add holiday schedule

1. Click **Settings** on the **Launcher** page.
2. Click **Schedule** in the left sidebar.
3. Click **ADD HOLIDAY** at the top left of the screen.
4. Enter **Name** and **Description** on the **Add New Holiday** screen.



Add New Holiday

Information

- Name
- Description

Detail

Date	Repeat
2025/06/30	Once

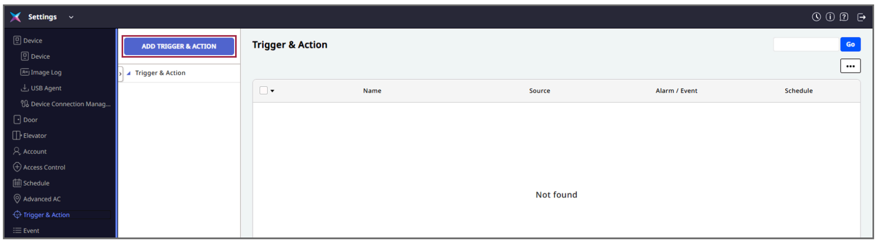
5. Click **+ Add** in the **Detail** section.
6. Click 📅 to select the date and set the number of repetitions and duration.
7. Click **Apply** to register the set holiday schedule.

> ⓘ **INFO**
>
> To delete a holiday schedule, click 🗑.

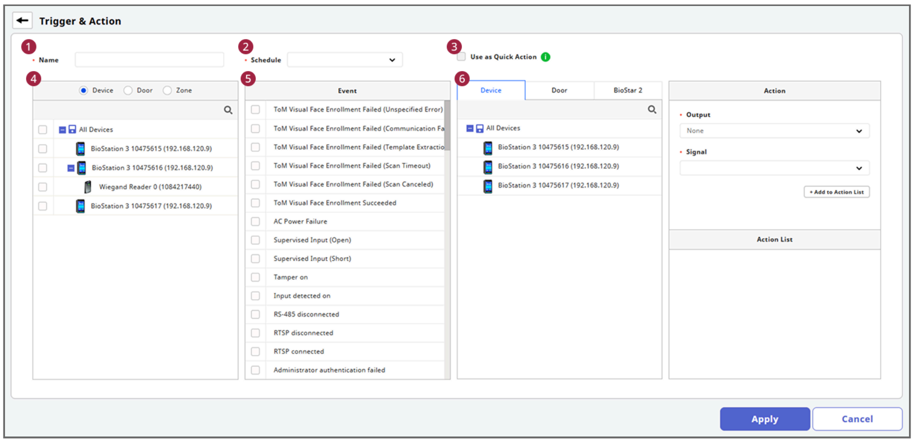
Trigger and Action Settings

You can configure the device or **BioStar X** to perform desired actions when specific events occur at a device, door, or area.

1. Click **Settings** on the **Launcher** page.
2. Click **Trigger & Action** in the left sidebar of the screen.
3. Click **ADD TRIGGER & ACTION** at the top left of the screen.



Follow the instructions on the screen to set the details.


Trigger & Action
1
Name
2
Schedule
3
Use as Quick Action
4
Device
Door
Zone
All Devices
BioStation 3 10475615 (192.168.120.9)
BioStation 3 10475616 (192.168.120.9)
Wiegand Reader 0 (1084217440)
BioStation 3 10475617 (192.168.120.9)
5
Event
ToM Visual Face Enrollment Failed (Unspecified Error)
ToM Visual Face Enrollment Failed (Communication Fa
ToM Visual Face Enrollment Failed (Template Extractio
ToM Visual Face Enrollment Failed (Scan Timeout)
ToM Visual Face Enrollment Failed (Scan Canceled)
ToM Visual Face Enrollment Succeeded
AC Power Failure
Supervised Input (Open)
Supervised Input (Short)
Tamper on
Input detected on
RS-485 disconnected
RTSP disconnected
RTSP connected
Administrator authentication failed
6
Device
Door
BioStar 2
All Devices
BioStation 3 10475615 (192.168.120.9)
BioStation 3 10475616 (192.168.120.9)
BioStation 3 10475617 (192.168.120.9)
Action
Output
None
Signal
+ Add to Action List
Action List
Apply
Cancel

1 Enter name

Name: Enter the name for the action conditions and actions.

2 Set schedule

Schedule: Set the schedule for when the action conditions and actions will apply.

ⓘ **INFO**

- Click **+ Add Schedule** to set a schedule if there is no desired schedule when selecting **Input** to create custom conditions.
- For more information about schedule settings, refer to the following.

3 Use as Quick Action

Setting **Quick Action** allows you to control multiple doors at once using the **Quick Action** button on the **BioStar X** main screen. Click the **Use as Quick Action** checkbox.

ⓘ **INFO**

- This feature is only available when the **Schedule** option is set to **Always**.
- **Quick Action** can be set in **Settings** → **Custom Interface**. For more information about **Quick Action**, refer to the following.

4 Select device, door, advanced access control

Select the items to send event signals. Multiple devices can be selected, and they will operate independently even if the connection with **BioStar X** is lost.

ⓘ **INFO**

The **Advanced Access Control** option is only available with an **Advanced** or higher license. For more information about the license policy, refer to the following.

5 Set event conditions

Set the condition events. You must select one or more events.

ⓘ **INFO**

Depending on the options selected in the previous step, different event lists will be activated.

6 Set actions

Select the device that will perform the actions. You can choose actions for devices, doors, or **BioStar X**.

In the **Action** section, you can set the signals to send when the selected condition events occur. To receive

> logs via email, this can be set in **BioStar X**.
>
> > **INFO**
> >
> > - Clicking on **Device**, **Door**, or **BioStar X** will change the contents of the actions section.
> > - To set the email server information, click the ⚙ icon on the **BioStar X** tab. When the **SMTP Option** window appears, enter the email server information and click the **Apply** button. For more information, refer to the following.
> > - For detailed information on email server settings, contact your system administrator.

Once all settings are completed, click the **Apply** button.

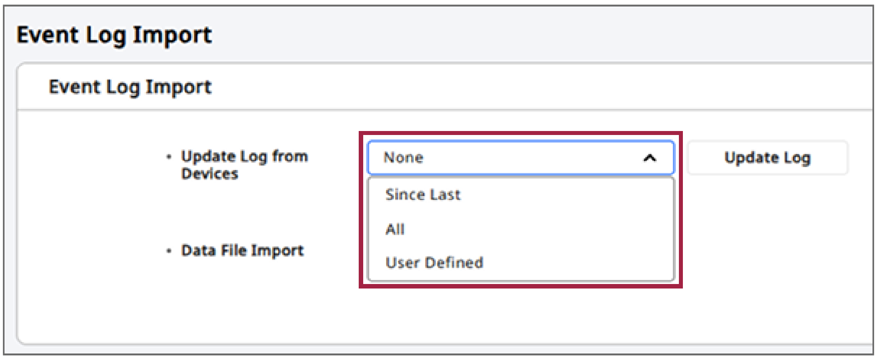
Import Event Logs

You can import the logs of the device to the **BioStar X** server to check events. This feature is available when the **Log Upload** option is set to **Manual** in the **Server** settings.

> **INFO**
>
> For more information on the **Log Upload** option, refer to the following.

Import manually

1. Click **Settings** on the **Launcher** page.
2. Click **Event** → **Event Log Import** in the left sidebar of the screen.
3. Select the period for fetching logs in **Update Log from Devices**.



Event Log Import

Event Log Import

- Update Log from Devices: None
- Data File Import

   - **Since Last**: Imports logs since the date of the last log saved to the **BioStar X** server.
   - **All**: Imports all logs from the device.
   - **User Defined**: You can select the start and end dates to import logs.

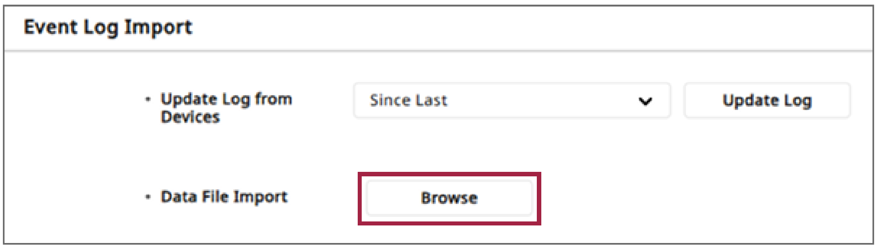
4. Click the **Update Log** button to import the logs.

Import from external storage

You can load event logs stored on an external storage device (USB) into **BioStar X**.

1. Click **Settings** on the **Launcher** page.
2. Click **Event** → **Event Log Import** in the left sidebar of the screen.

3. Click the **Browse** button for the **Data File Import** item.



4. Select the data file (.*tgz*) saved locally.

A message will appear on the screen if the data file is successfully imported.

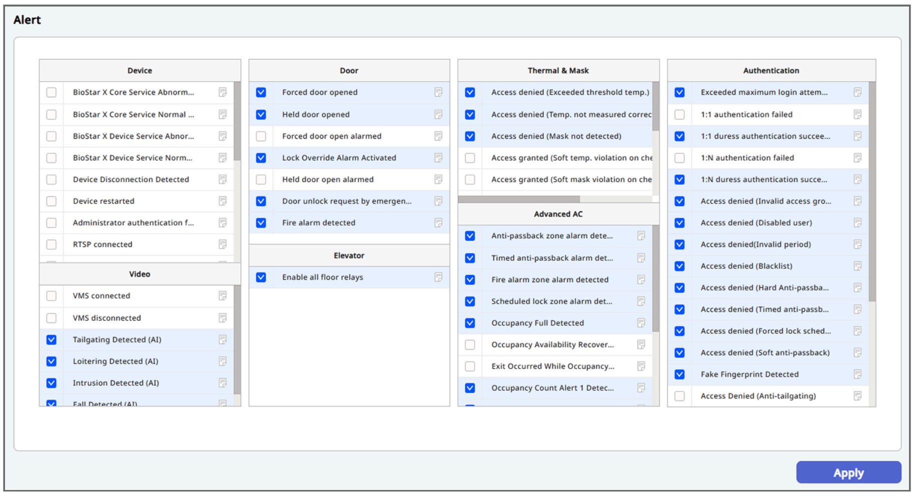
> **INFO**
>
> - Data exported from devices using an outdated firmware version cannot be imported into **BioStar X**. Always use the latest version of the firmware.
> - Only data files exported from FaceStation F2, FaceStation 2, FaceLite, BioStation A2, BioStation 2, X-Station 2, BioStation 3 models can be imported.
> - If the imported event logs are not from access points, elevators, or zones set in the **BioStar X** system, some information may appear blank.

Alert Settings

Set the types of alert and messages to appear on the screen when events occur in the device, door, or area. Additionally, you can configure it to play a sound file uploaded by the user when the alert occurs.

Alert Settings

1. Click **Settings** on the **Launcher** page.
2. Click **Event** → **Alert** in the left sidebar of the screen.
3. Select the event to display on the screen from the event list in each category.
4. Once all settings are completed, click the **Apply** button.



Alert

Device
- ☐ BioStar X Core Service Abnorm...
- ☐ BioStar X Core Service Normal ...
- ☐ BioStar X Device Service Abnor...
- ☐ BioStar X Device Service Norm...
- ☐ Device Disconnection Detected
- ☐ Device restarted
- ☐ Administrator authentication f...
- ☐ RTSP connected

Video
- ☐ VMS connected
- ☐ VMS disconnected
- ☑ Tailgating Detected (AI)
- ☑ Loitering Detected (AI)
- ☑ Intrusion Detected (AI)
- ☑ Fall Detected (AI)

Door
- ☑ Forced door opened
- ☑ Held door opened
- ☐ Forced door open alarmed
- ☑ Lock Override Alarm Activated
- ☐ Held door open alarmed
- ☑ Door unlock request by emergen...
- ☑ Fire alarm detected

Elevator
- ☑ Enable all floor relays

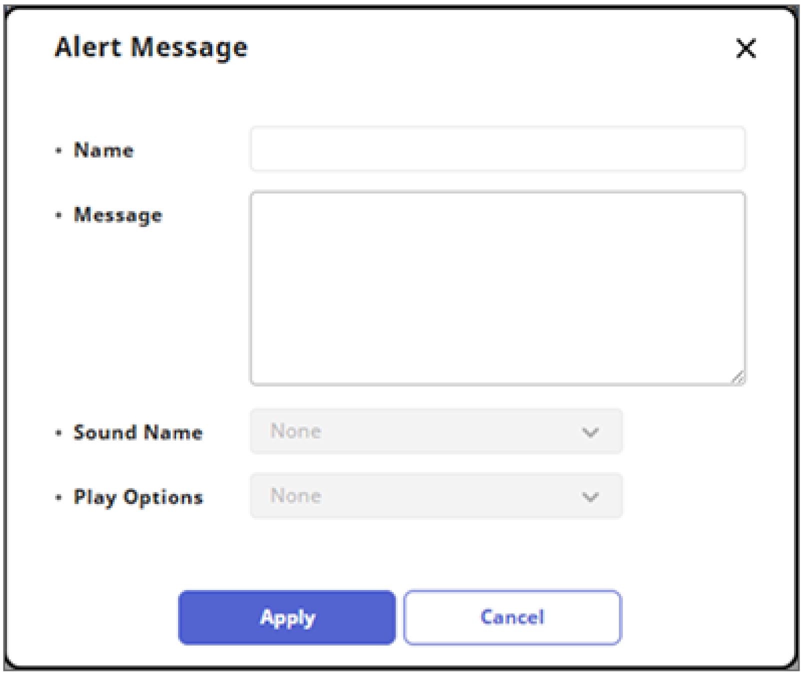
Thermal & Mask
- ☑ Access denied (Exceeded threshold temp.)
- ☑ Access denied (Temp. not measured correc
- ☑ Access denied (Mask not detected)
- ☐ Access granted (Soft temp. violation on che
- ☐ Access granted (Soft mask violation on che

Advanced AC
- ☑ Anti-passback zone alarm dete...
- ☑ Timed anti-passback alarm det...
- ☑ Fire alarm zone alarm detected
- ☑ Scheduled lock zone alarm det...
- ☑ Occupancy Full Detected
- ☐ Occupancy Availability Recover...
- ☐ Exit Occurred While Occupancy...
- ☑ Occupancy Count Alert 1 Detec...

Authentication
- ☑ Exceeded maximum login attem...
- ☐ 1:1 authentication failed
- ☑ 1:1 duress authentication succee...
- ☐ 1:N authentication failed
- ☑ 1:N duress authentication succe...
- ☑ Access denied (Invalid access gro...
- ☑ Access denied (Disabled user)
- ☑ Access denied(Invalid period)
- ☑ Access denied (Blacklist)
- ☑ Access denied (Hard Anti-passba...
- ☑ Access denied (Timed anti-passb...
- ☑ Access denied (Forced lock sched...
- ☑ Access denied (Soft anti-passback)
- ☑ Fake Fingerprint Detected
- ☐ Access Denied (Anti-tailgating)

Edit alert message

Click 📄 in the event list to edit the alert message. When the **Alert Message** window appears, set each item and click **Apply**.



- **Name**: Change the alert message name.
- **Message**: Enter the message to display on the screen.
- **Sound Name**: If you have uploaded a sound file to play for the event, you can select it from the list.
- **Play Options**: If you have selected a sound file, choose the number of times to play it.

> **INFO**
>
> If there are no sound files to play, refer to the following to upload.

Manage Credentials

This guide describes how to manage credentials for access authentication. You can check card issuance status, user possession, and blacklist, and set card formats. You can also check how to set up mobile access cards.

Manage Cards

This guide explains how to check card issuance status, change Wiegand card data format, and manage the deletion history for CSN mobile cards.

Set Wiegand Card Format

This guide describes how to set Wiegand card format.

Set Smart Card Format

Set layout of smart cards such as MIFARE, iCLASS, DESFire, iCLASS Seos.

Manage Mobile Access Cards

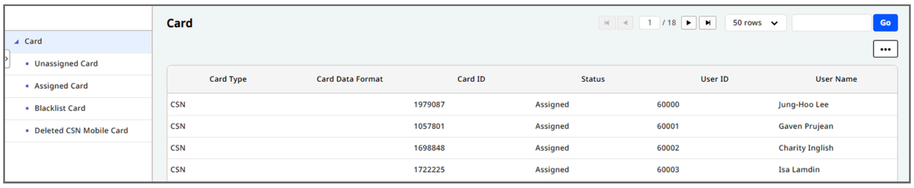
This guide describes how to manage mobile access cards for users in BioStar X by integrating Airfob Portal.

Manage Cards

You can check the issuance status of the card, change the Wiegand card data format, and manage the deletion history of CSN mobile cards.

Card Management

1. Click **Settings** on the **Launcher** page.
2. Click **Credential** → **Card** in the left sidebar.
3. You can see the enrolled cards on the card list screen.



Card Type	Card Data Format	Card ID	Status	User ID	User Name
CSN		1979087	Assigned	60000	Jung-Hoo Lee
CSN		1057801	Assigned	60001	Gaven Prujean
CSN		1698848	Assigned	60002	Charity Inglish
CSN		1722225	Assigned	60003	Isa Lamdin

Click the issuance status on the left side of the screen to filter by card issuance status. The card issuance statuses are as follows:

- **Unassigned Card**: Card that is not assigned to any user.
- **Assigned Card**: Card assigned to a specific user. You can check the ID and name of the assigned user on the card list.
- **Blacklist Card**: Card registered on the blacklist. The cardholder cannot authenticate for access.
- **Deleted CSN Mobile Card**: Deleted mobile access card.

> **INFO**
>
> If you have blocked a user's card, you can check the card information in the **Blacklist Card** list. To unblock, select the desired card and click **Unblocked**.

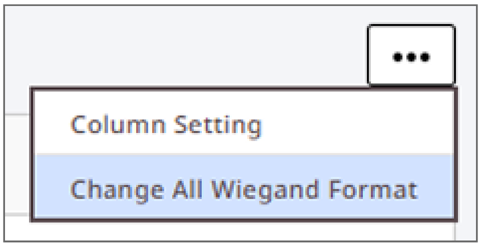
Change Wiegand card data format

You can change the Wiegand card data format in use all at once.

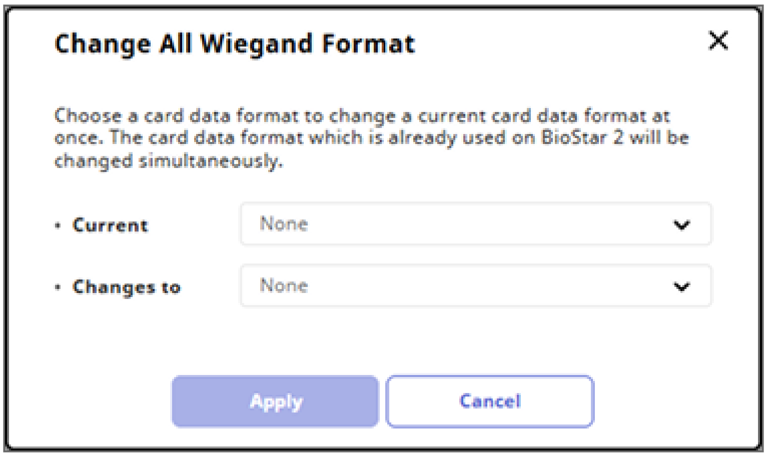
> **CAUTION**
>
> Changing the data format of cards already assigned to users will also occur, so be cautious.

1. Click **Settings** on the **Launcher** page.
2. Click **Credential** → **Card** in the left sidebar.

3. Click ••• at the top right of the card list and select **Change All Wiegand Format**.



4. When the **Change All Wiegand Format** window appears, select the card data format you want to change from the **Current** list.


Change All Wiegand Format

Choose a card data format to change a current card data format at once. The card data format which is already used on BioStar 2 will be changed simultaneously.

- Current: None
- Changes to: None

5. Select the desired card data format from the **Changes to** list.

6. Click **Apply** to change the card data format.

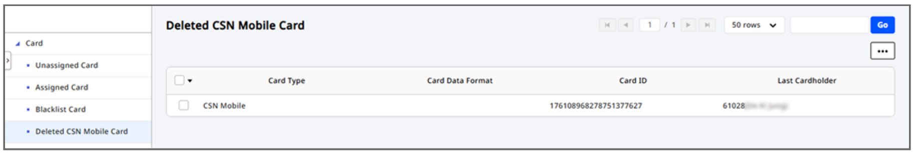
CSN Mobile Card Deletion Management Guidelines

When using CSN mobile cards integrated with the Airfob Portal Regular Site in **BioStar X**, if a user deletes a card, the same card ID could be reissued to another user. However, this could lead to an issue where the original cardholder could still access the premises even after the card has been reissued.

To address this issue, **BioStar X** provides the feature to manage deletion history after deleting CSN mobile cards.

Separate management of deleted CSN mobile cards

Deleted CSN mobile cards are recorded in the **Settings** → **Card** → **Deleted CSN Mobile Card** list. In this list, you can view the **Card Type**, **Card Data Format**, **Card ID**, and **Last Cardholder**.



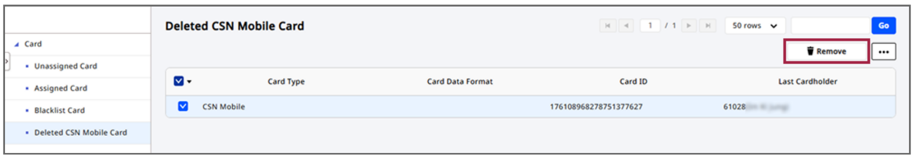
Deleted CSN Mobile Card

□	Card Type	Card Data Format	Card ID	Last Cardholder
□	CSN Mobile		176108968278751377627	61028[redacted]

Preventing reissuance of deleted card IDs

If there is a history of deletion for a CSN mobile card, the system will prevent that card ID from being reissued to another user.

If you wish to issue a card with a deleted card ID, you can only do so after excluding the corresponding CSN mobile card from the **Deleted CSN Mobile Card** list.



Deleted CSN Mobile Card

☑	Card Type	Card Data Format	Card ID	Last Cardholder
☑	CSN Mobile		17610896827875137627	61028[redacted]

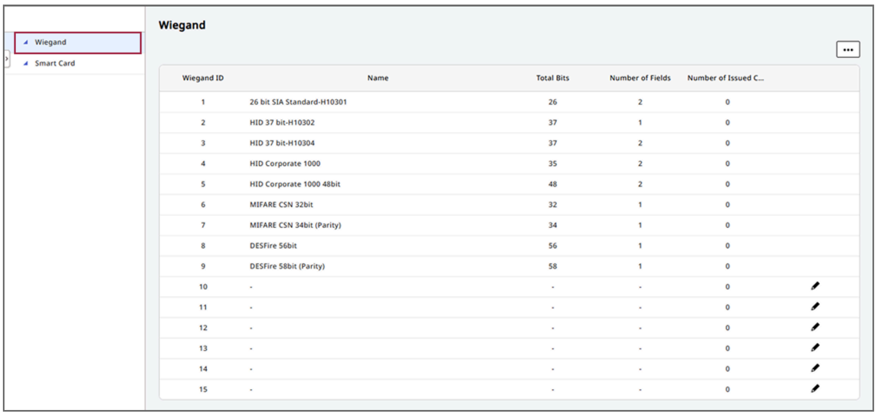
> **INFO**
>
> CSN mobile cards included in the **Deleted CSN Mobile Card** list cannot be deleted from the **Unassigned Card** list.
>
> To delete a card from the **Unassigned Card** list, first remove the card from the **Deleted CSN Mobile Card** list and then proceed with the deletion.

Set Wiegand Card Format

Set the card data reading format. Card data is processed according to the configured Wiegand format.

Set Wiegand card format

1. Click **Settings** on the **Launcher** page.
2. Click **Credential** → **Card Format** on the left sidebar.
3. Click **Wiegand** in the left card format list.



Wiegand

Wiegand ID	Name	Total Bits	Number of Fields	Number of Issued C...	
1	26 bit SIA Standard-H10301	26	2	0	
2	HID 37 bit-H10302	37	1	0	
3	HID 37 bit-H10304	37	2	0	
4	HID Corporate 1000	35	2	0	
5	HID Corporate 1000 48bit	48	2	0	
6	MIFARE CSN 32bit	32	1	0	
7	MIFARE CSN 34bit (Parity)	34	1	0	
8	DESFire 56bit	56	1	0	
9	DESFire 58bit (Parity)	58	1	0	
10	-	-	-	0	✎
11	-	-	-	0	✎
12	-	-	-	0	✎
13	-	-	-	0	✎
14	-	-	-	0	✎
15	-	-	-	0	✎

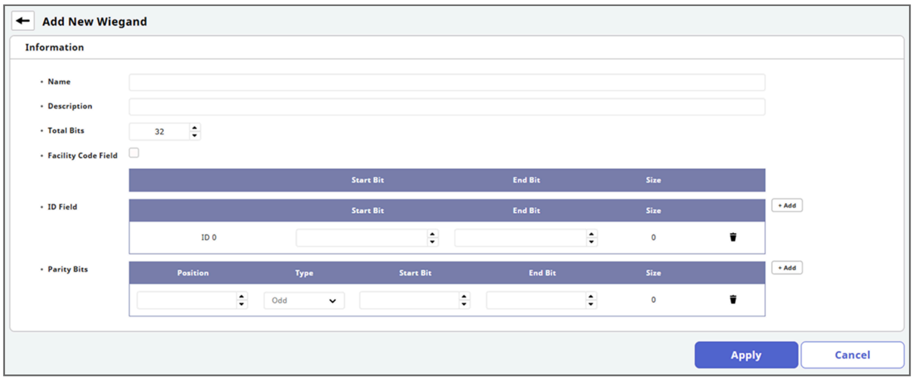
4. Click the ✎ button for the unnamed item in the Wiegand format list.
5. When the **Add New Wiegand** screen appears, set each item. For more information, refer to the following.
6. Click **Apply** to add the configured Wiegand format.

INFO

- Up to 15 Wiegand formats can be used.
- Predefined formats cannot be modified or deleted.

Setting options guide

Reference the items below to set the bit configuration when adding or editing a Wiegand card format.



- Name
- Description
- Total Bits: 32
- Facility Code Field: □

	Start Bit	End Bit	Size

- ID Field

	Start Bit	End Bit	Size
ID 0			0

- Parity Bits

Position	Type	Start Bit	End Bit	Size
	Odd			0

- **Name**: Enter the Wiegand format name.
- **Description**: Enter a brief description of the Wiegand format.
- **Total Bits**: Enter the total number of bits.
- **Facility Code Field**: Set whether to use the identification code. To use the identification code, click the checkbox and enter **Start Bit** and **End Bit**.
- **ID Field**: Enter the **Start Bit** and **End Bit** for the ID you want to use. Click **+ Add** to add an ID field.
- **Parity Bits**: Click **+ Add** to enter the number of parity bits. Enter the position of the parity bits and the start and end bits.

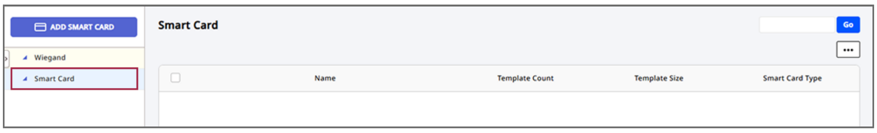
> ⓘ **INFO**
>
> To add parity bits, the **Total Bits** option must be entered.

Set Smart Card Format

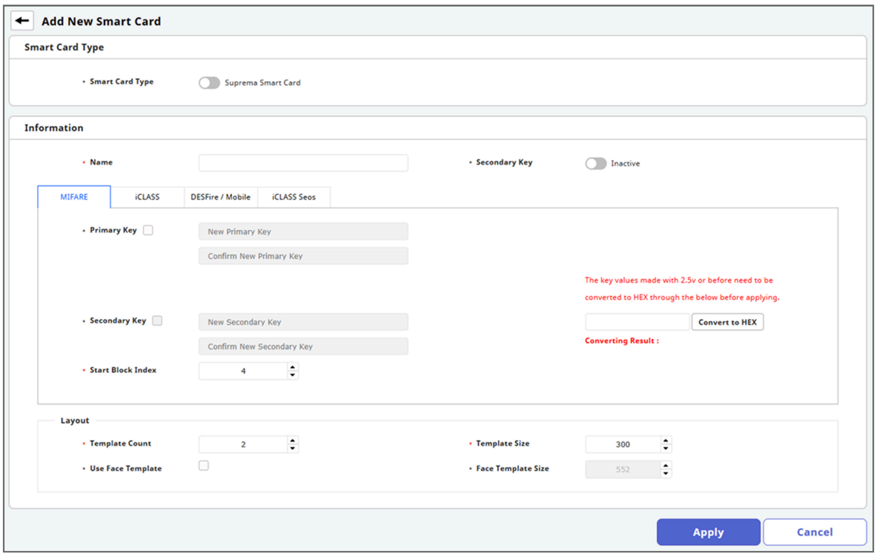
Set layout of smart cards such as MIFARE, iCLASS, DESFire, iCLASS Seos.

Add smart card

1. Click **Settings** on the **Launcher** page.
2. Click **Credential** → **Card Format** on the left sidebar.
3. Click **Smart Card** in the left card format list.



4. Click **Add Smart Card** in the top left of the screen.
5. When the **Add New Smart Card** screen appears, configure each item. For more information, refer to the following.



Smart Card Type: Suprema Smart Card

Name:

Secondary Key: Inactive

Primary Key □

Secondary Key □

Start Block Index: 4

The key values made with 2.5v or before need to be converted to HEX through the below before applying.

Converting Result :

Template Count: 2

Template Size: 300

Use Face Template □

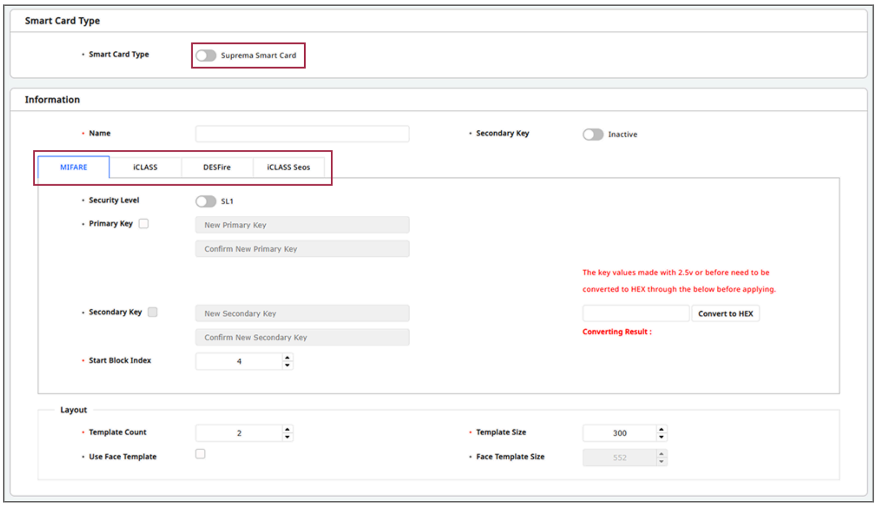
Face Template Size: 552

6. Once all settings are completed, click **Apply**.

Smart card types

You can set the desired smart card type in the **Smart Card Type** option.

- **Suprema Smart Card**



Smart Card Type

- Smart Card Type: Suprema Smart Card

Information

- Name:
- Secondary Key: Inactive

- Security Level: SL1
- Primary Key □: New Primary Key / Confirm New Primary Key
- Secondary Key □: New Secondary Key / Confirm New Secondary Key
- Start Block Index: 4

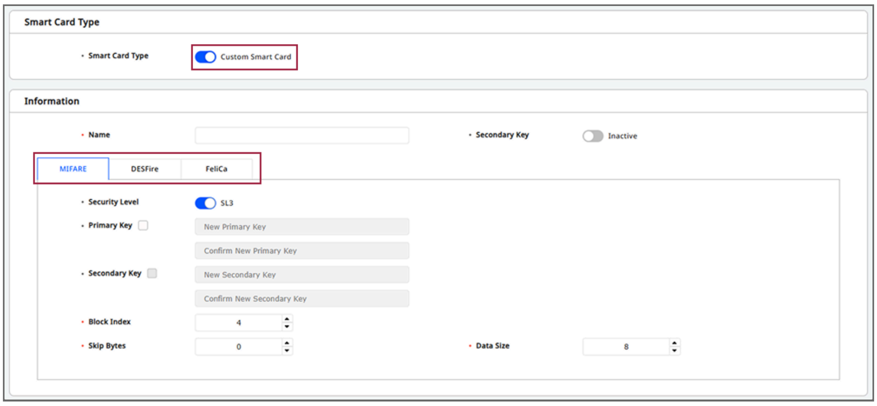
The key values made with 2.5v or before need to be converted to HEX through the below before applying.

Converting Result :

Layout

- Template Count: 2
- Template Size: 300
- Use Face Template: □
- Face Template Size: 552

- **Custom Smart Card**



Smart Card Type

- Smart Card Type: Custom Smart Card

Information

- Name:
- Secondary Key: Inactive

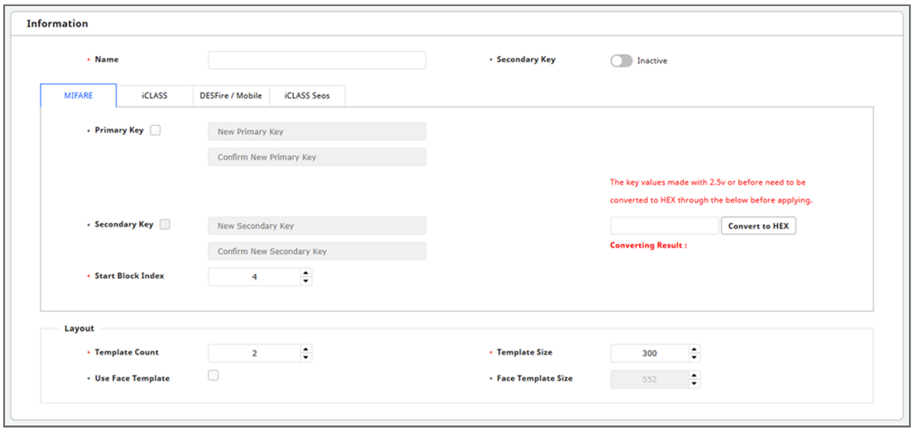
- Security Level: SL3
- Primary Key □: New Primary Key / Confirm New Primary Key
- Secondary Key □: New Secondary Key / Confirm New Secondary Key
- Block Index: 4
- Skip Bytes: 0
- Data Size: 8

INFO

- Custom smart cards only support MIFARE, DESFire, and FeliCa.
- FeliCa is only supported on BioStation 3 firmware version 1.3.0 or higher.

Setting options guide

Set the card layout in the **Info** section.

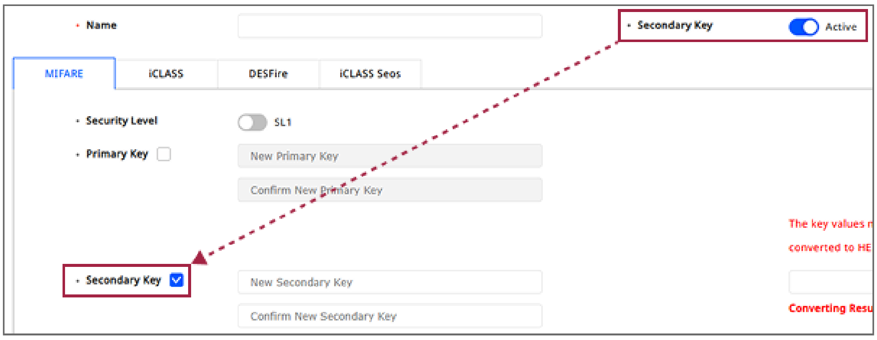


The key values made with 2.5v or before need to be converted to HEX through the below before applying.

> **INFO**
>
> - The **Primary Key** and **Secondary Key** support only hexadecimal. Enter the key values to be used in the right field and click **Convert to HEX**. Use the converted value as the site key.
> - **Convert to HEX** is only available when the **Smart Card Type** option is **Suprema Smart Card**.

Set basic information

- **Name**: Enter the smart card name.
- **Secondary Key**: Configure whether to use a secondary site key. Set to **Active** to enable secondary site key configuration. When a secondary site key is set, it will be used for authentication when the card's primary site key does not match.



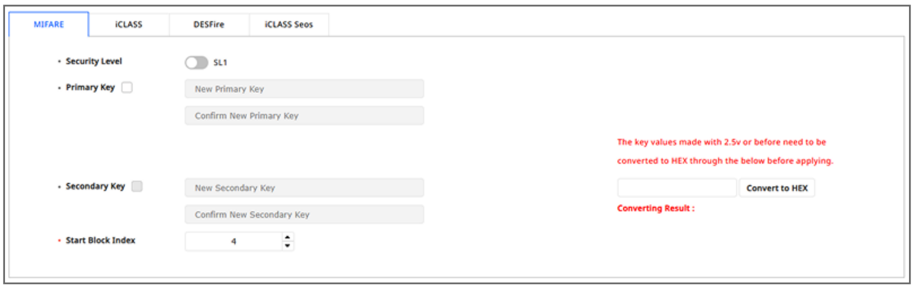
Set smart card

You can set the structure of the smart card.

Suprema smart card

The **Primary Key** and **Secondary Key** support only hexadecimal. Enter the key value for each input field and click **Convert to HEX**. Use the converted value as the site key.

MIFARE



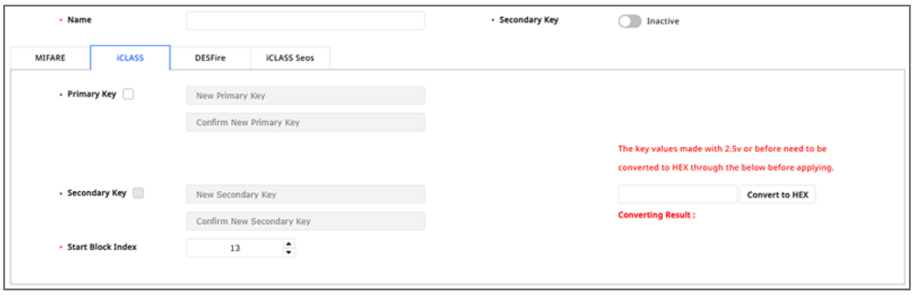
- Security Level: SL1
- Primary Key □ New Primary Key / Confirm New Primary Key
- Secondary Key □ New Secondary Key / Confirm New Secondary Key
- Start Block Index: 4

The key values made with 2.5v or before need to be converted to HEX through the below before applying.

Converting Result :

- **Security Level**: Set encryption type to **SL1** or **SL3**.
- **Primary Key**: The key that encrypts communications between the smart card and the card reader.
- **Secondary Key**: Used for authentication when the card's primary site key does not match. The secondary site key can only be entered after activating the **Secondary Key** option at the top of the section.
- **Start Block Index**: Select the starting block where each template will be saved. This block is the index of the block where user information is stored; set it to a storable block if the user is already using the smart card.

iCLASS



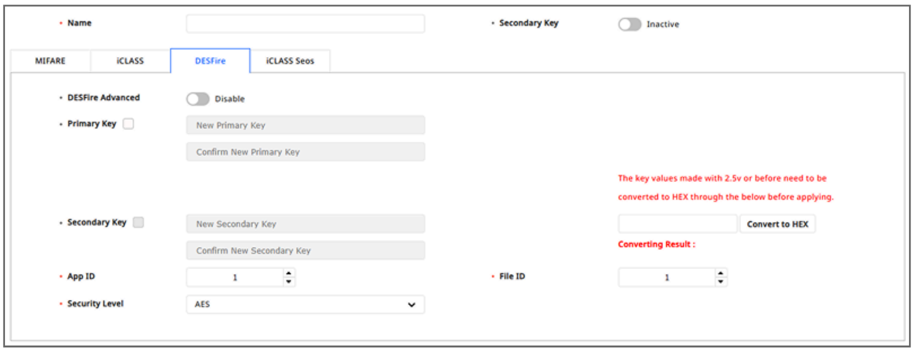
- Name
- Secondary Key: Inactive
- Primary Key □ New Primary Key / Confirm New Primary Key
- Secondary Key □ New Secondary Key / Confirm New Secondary Key
- Start Block Index: 13

The key values made with 2.5v or before need to be converted to HEX through the below before applying.

Converting Result :

- **Primary Key**: The key that encrypts communications between the smart card and the card reader.
- **Secondary Key**: Used for authentication when the card's primary site key does not match. The secondary site key can only be entered after activating the **Secondary Key** option at the top of the section.
- **Start Block Index**: Select the starting block where each template will be saved. This block is the index of the block where user information is stored; set it to a storable block if the user is already using the smart card.

DESFire



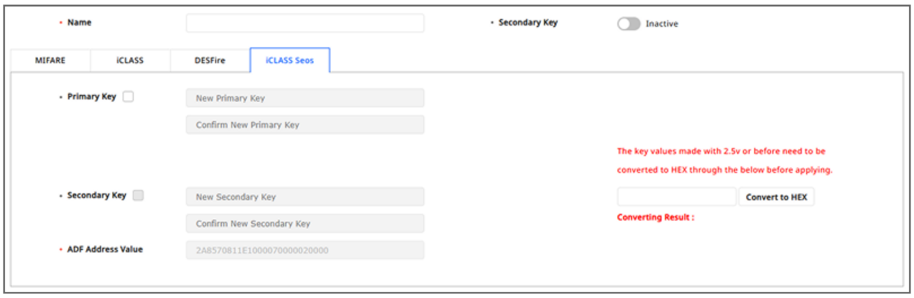
- Name
- Secondary Key: Inactive
- DESFire Advanced: Disable
- Primary Key □
- Secondary Key □
- App ID: 1
- File ID: 1
- Security Level: AES

The key values made with 2.5v or before need to be converted to HEX through the below before applying.

Converting Result :

- **DESFire Advanced**: You can use DESFire cards issued by third parties. Only DESCire can be configured.
- **Primary Key**: The key that encrypts communications between the smart card and the card reader.
- **Secondary Key**: Used for authentication when the card's primary site key does not match. The secondary site key can only be entered after activating the **Secondary Key** option at the top of the section.
- **ID Field**: Configure to read a specific area on the card. Acts as a directory containing **File ID**.
- **File ID**: Set the file ID.
- **Security Level**: Set the encryption type to **DES/3DES** or **AES**.

iClass Seos



- Name
- Secondary Key: Inactive
- Primary Key □
- Secondary Key □
- ADF Address Value: 2A8570811E1000070000020000

The key values made with 2.5v or before need to be converted to HEX through the below before applying.

Converting Result :

- **Primary Key**: The key that encrypts communications between the smart card and the card reader.
- **Secondary Key**: Used for authentication when the card's primary site key does not match. The secondary site key can only be entered after activating the **Secondary Key** option at the top of the section.
- **ADF Address Value**: The ADF address where digital credentials are stored.

Layout

You can modify the layout that records user information, facial, and fingerprint information.

- **Template Count**: Set the number of fingerprint templates to include in the layout.
- **Template Size**: Set the number of bytes used by each fingerprint template.
- **Use Face Template**: Choose whether to use the face template.

- **Face Template Size**: Set the number of bytes used by the face template.

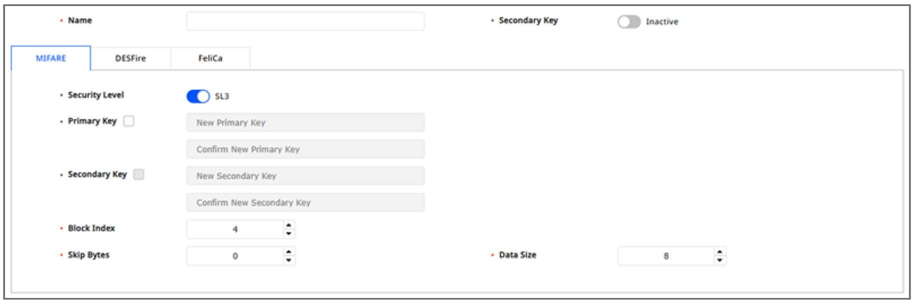
> **INFO**
>
> **Use Face Template** is available on FaceStation F2, BioStation 3, and BioEntry W3 models.

Custom smart card

Custom smart cards only support MIFARE, DESFire, and FeliCa.

> **INFO**
>
> FeliCa is only supported on BioStation 3 firmware version 1.3.0 or higher.

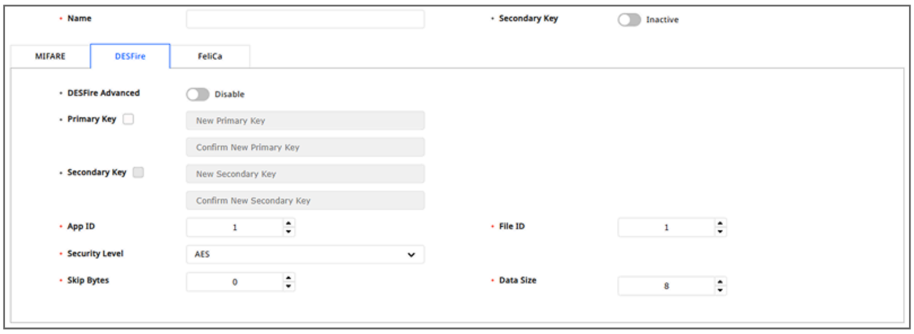
MIFARE



- Name
- Secondary Key: Inactive
- Security Level: SL3
- Primary Key □
- Secondary Key □
- Block Index: 4
- Skip Bytes: 0
- Data Size: 8

- **Security Level**: Set encryption type to **SL1** or **SL3**.
- **Primary Key**: The key that encrypts communications between the smart card and the card reader.
- **Secondary Key**: Used for authentication when the card's primary site key does not match. The secondary site key can only be entered after activating the **Secondary Key** option at the top of the section.
- **Block Index**: Select the starting block where each template will be saved. This block is the index of the block where user information is stored; set it to a storable block if the user is already using the smart card.
- **Skip Bytes**: Set the starting point for reading the card number.
- **Data Size**: (When the set **Primary Key** and **Secondary Key** values are the same as the card's configuration) Configure the data size of the card to be read.

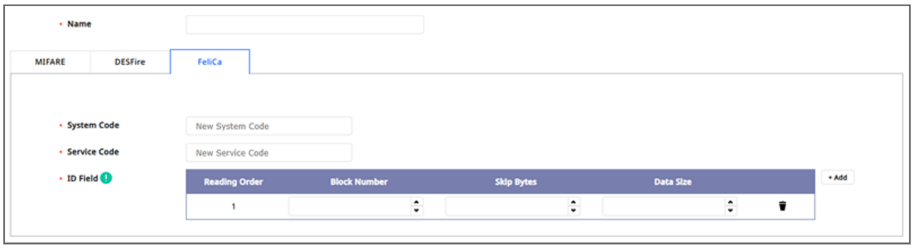
DesFire



- Name
- Secondary Key: Inactive
- DESFire Advanced: Disable
- Primary Key □: New Primary Key / Confirm New Primary Key
- Secondary Key □: New Secondary Key / Confirm New Secondary Key
- App ID: 1
- File ID: 1
- Security Level: AES
- Skip Bytes: 0
- Data Size: 8

- **DESFire Advanced**: You can use DESFire cards issued by third parties. Only DESCire can be configured.
- **Primary Key**: The key that encrypts communications between the smart card and the card reader.
- **Secondary Key**: Used for authentication when the card's primary site key does not match. The secondary site key can only be entered after activating the **Secondary Key** option at the top of the section.
- **ID Field**: Configure to read a specific area on the card. Acts as a directory containing **File ID**.
- **File ID**: Set the file ID.
- **Security Level**: Set the encryption type to **DES/3DES** or **AES**.
- **Skip Bytes**: Set the starting point for reading the card number.
- **Data Size**: (When the set **Primary Key** and **Secondary Key** values are the same as the card's configuration) Configure the data size of the card to be read.

Felica



- Name
- System Code: New System Code
- Service Code: New Service Code
- ID Field

Reading Order	Block Number	Skip Bytes	Data Size
1			

- **System Code**: Enter the system code to read FeliCa cards in hexadecimal, with a maximum of 4 characters.
- **Service Code**: Enter the service code to read FeliCa cards in hexadecimal, with a maximum of 4 characters.
- **App ID**: Set the application ID, serving as a type of directory that includes **File ID**. You can set up to 8 blocks to read by clicking **+ Add**.
  Block Number: Set the block to read from the card. (0-150)

Manage Mobile Access Cards

Integrate the Airfob Portal to issue or delete mobile access cards for users in **BioStar X**.

Users can receive mobile access cards via a link sent to their email without signing up for the Airfob Portal or separately enrolling for mobile access cards.

ⓘ **INFO**

- Only one of the **CSN Mobile** card or **Template on Mobile** can be used for mobile access cards.
- Refer to the following for devices and firmware versions that support the **CSN Mobile** card.

  View devices and firmware versions supporting the **CSN Mobile** card

  - XPass 2 firmware version 1.1.0 or higher
  - XPass D2 (Rev 2) firmware version 1.4.0 or higher
  - BioLite N2 firmware version 1.3.0 or higher
  - BioEntry W2 (Rev 2) firmware version 1.6.0 or higher
  - FaceStation 2 firmware version 1.4.0 or higher
  - FaceStation F2 firmware 1.0.0 or higher
  - BioStation 2 firmware version 1.9.0 or higher (NFC supported model)
  - BioStation A2 firmware version 1.8.0 or higher (NFC supported model)
  - FaceLite firmware version 1.2.0 or higher
  - X-Station 2 firmware 1.0.0 or higher
  - BioStation 3 firmware 1.0.0 or higher
  - BioEntry W3 firmware version 1.0.0 or higher
- Refer to the following for devices and firmware versions that support **Template on Mobile**.
  - BioStation 3 firmware version 1.2.0 or higher
  - BioEntry W3 firmware version 1.0.0 or higher

Set whether to use mobile access cards and manage settings related to Airfob Portal integration. You can also register devices that will use mobile access cards. After signing up for the Airfob Portal, you can manage mobile access cards in **BioStar X**.

1 Sign up for Airfob Portal and create Site

Set up mobile access cards and registered devices in the Airfob Portal, and manage your site and credits.

1. Access the Airfob Portal.
2. Click **Get Started** to proceed with membership registration and site creation.
3. Enter the Airfob Portal administrator's email address in the email input field, then click **Get Started**. A verification code will be sent to the entered email address.
4. Enter the verification code received via email into the verification code input field, then click **Confirm**.

> ⓘ The verification code is a 6-digit number.

5. Review the privacy policy and terms, then click **Agree**.
6. Set a password and nickname for the Airfob Portal, then click **Create Account**. Account creation will be completed.
7. Once account creation is completed, click **Sign In**.
8. Enter your email and password, then click **Sign In**.
9. Click **Create Site** to proceed with site creation.

> ⓘ **Site** refers to the organization or company using mobile access cards.

10. Set the site name and country, then click **Next**.
11. Select the site type.

> ⓘ You can select the card type as **Dynamic** or **Regular** depending on the site type.
>
> - **Dynamic**: A type that deducts credits based on device and usage duration, allowing management actions such as revocation, suspension, reissuance, and expiration date designation even after the card is issued. This type is suitable for membership facilities like fitness clubs or study rooms, as well as co-working spaces.
> - **Regular**: A type that deducts credits based on the number of cards issued, available permanently until the administrator removes the cards in **BioStar X**. This type is suitable for companies or groups to use as employee IDs and access cards.

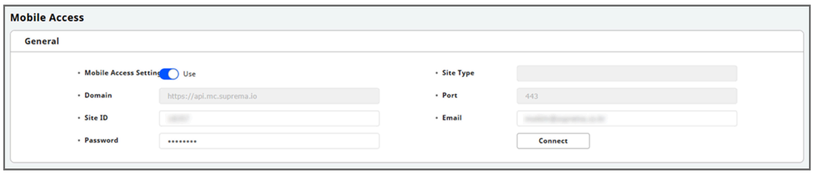
12. Click **Create**. Site creation will be completed.
13. Click the site name to access the Airfob Portal for that site.

> **INFO**
>
> For more information about using the Airfob Portal, refer to the following link.

2 Configure mobile access card in BioStar X

After signing up for the Airfob Portal, you can manage mobile access cards in **BioStar X**. To use Suprema mobile access cards, sign up for the Airfob Portal and create a site.

1. Click **Settings** on the **Launcher** page.
2. Click **Credential** → **Mobile Access** in the left sidebar.
3. Edit the necessary fields.



Mobile Access

General

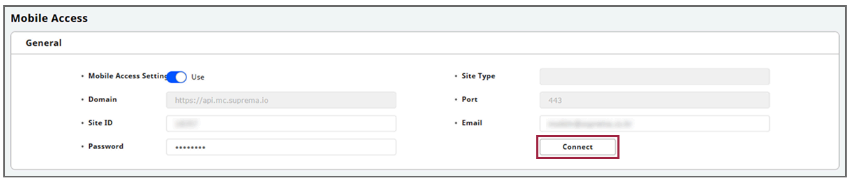
- Mobile Access Setting: Use
- Domain: https://api.mc.suprema.io
- Site ID: [redacted]
- Password: ••••••••
- Site Type:
- Port: 443
- Email: [redacted]

   - **Mobile Access Setting**: You can set whether to use mobile access cards. Set to **Use** to issue mobile access cards to users.
   - **Site ID**: Enter the site ID created in the Airfob Portal. The site ID can be found in the Airfob Portal pathway **Settings** → **Site**.
   - **Email**: Enter the email address of the mobile access card administrator account.
   - **Password**: Enter the password of the mobile access card administrator account.
4. Click **Connect** when all settings are complete.

> **INFO**
>
> To use mobile access cards in **BioStar X**, complete the sign-up and initial setup of the Airfob Portal first. For more information, refer to the following.

3 Register device

You can register devices that will use mobile access cards directly from the Airfob Pass application or **BioStar X**.



Mobile Access

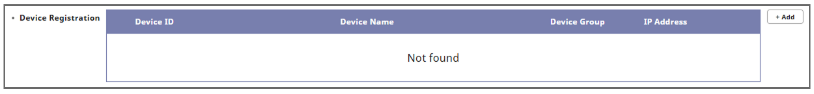
General

- Mobile Access Setting: Use
- Domain: https://api.mc.suprema.io
- Site ID: [redacted]
- Password: ••••••••
- Site Type:
- Port: 443
- Email: [redacted]

Once the settings for integration with the Airfob Portal are completed, click **Connect**. The **Device**

Registration option will be available.

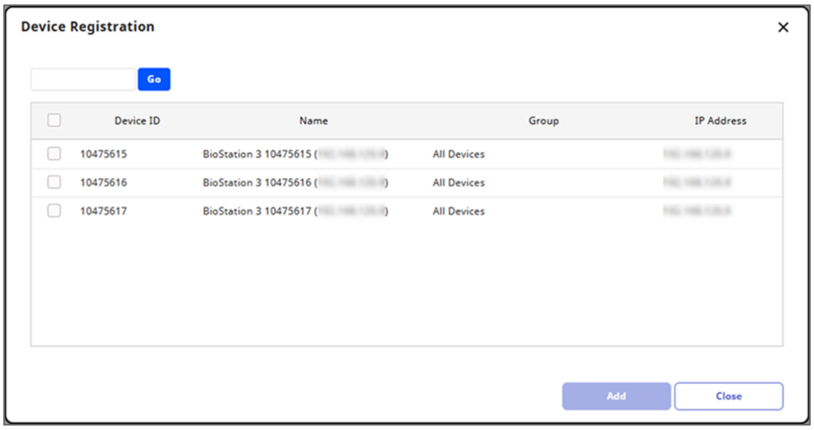
1. To add a device that will use mobile access cards, click **+ Add**.



• Device Registration

Device ID	Device Name	Device Group	IP Address
Not found			

2. In the device list of the **Device Registration** window, click the checkbox for the device that will use the mobile access card.



Device Registration

□	Device ID	Name	Group	IP Address
□	10475615	BioStation 3 10475615 ([redacted])	All Devices	[redacted]
□	10475616	BioStation 3 10475616 ([redacted])	All Devices	[redacted]
□	10475617	BioStation 3 10475617 ([redacted])	All Devices	[redacted]

3. After selecting all devices, click **Add**.

You can verify the added devices in the device list.

- To resend the mobile access card certificate, click ⟳.
- To delete a registered device, click 🗑.

INFO

- Refer to the following for devices and firmware versions that can use mobile access cards.

  View devices and firmware versions that can use mobile access cards

  - XPass 2 firmware version 1.1.0 or higher
  - XPass D2 (Rev 2) firmware version 1.4.0 or higher
  - BioLite N2 firmware version 1.3.0 or higher
  - BioEntry W2 (Rev 2) firmware version 1.6.0 or higher
  - FaceStation 2 firmware version 1.4.0 or higher
  - FaceStation F2 firmware 1.0.0 or higher
  - BioStation 2 firmware version 1.9.0 or higher (NFC supported model)
  - BioStation A2 firmware version 1.8.0 or higher (NFC supported model)
  - FaceLite firmware version 1.2.0 or higher
  - X-Station 2 firmware 1.0.0 or higher
  - BioStation 3 firmware 1.0.0 or higher
  - BioEntry W3 firmware version 1.0.0 or higher
- You can also register devices using the Airfob Pass application.
- Deleting a registered device will remove the mobile access card certificate sent to that device.

4 Issue mobile access card

You can issue mobile access cards to users registered in **BioStar X**. To issue a mobile access card to a user, essential user information based on the method of sending the mobile access card must be entered. For more information, refer to the followings.

- User Information Registration
- Mobile Access Card Enrollment

Card Printer

You can print cards with the desired design by integrating **BioStar X** and cardPresso. cardPresso is professional software for card design and printing. Using cardPresso, you can create various card templates and arrange user information accordingly.

Before start

To use the card printer feature of **BioStar X**, install the cardPresso program and connect it to **BioStar X**. To use the web printing server function of the cardPresso program, a cardPresso XXL edition license is required.

> ⓘ **INFO**
>
> - For more information on the license types of the cardPresso program, refer to the following link.
> - The web printing server function is supported only on Windows operating systems.

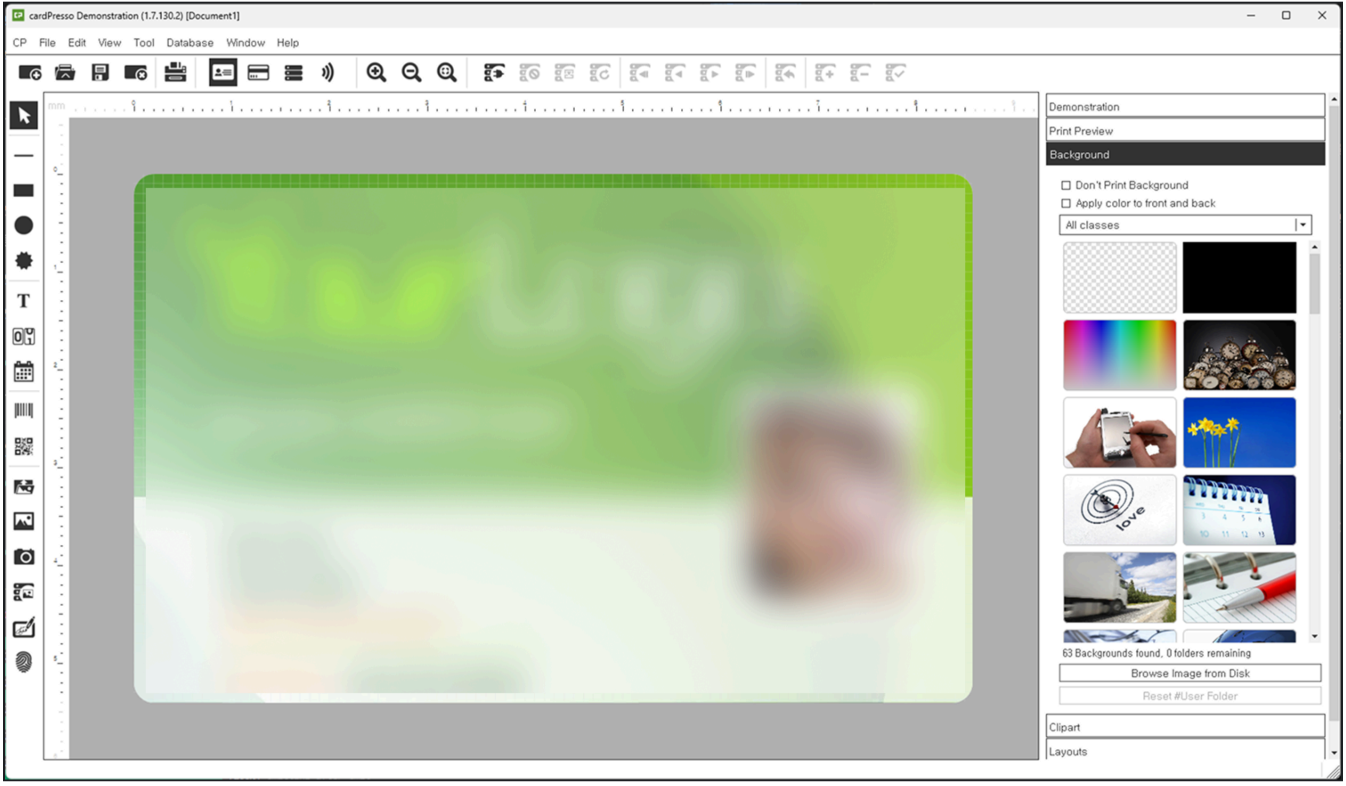
Installing and configuring the cardPresso

Follow the steps below to install the cardPresso program and set up the web printing server.

> ⓘ The menu path or screen may vary depending on the installation version.

1. Download the latest version of cardPresso compatible with the operating system of the PC to be operated as a web printing server from cardPresso Download.
2. Install the program and activate the license issued by cardPresso.

3. After running cardPresso, create a card template.



□ Don't Print Background
□ Apply color to front and back

63 Backgrounds found, 0 folders remaining

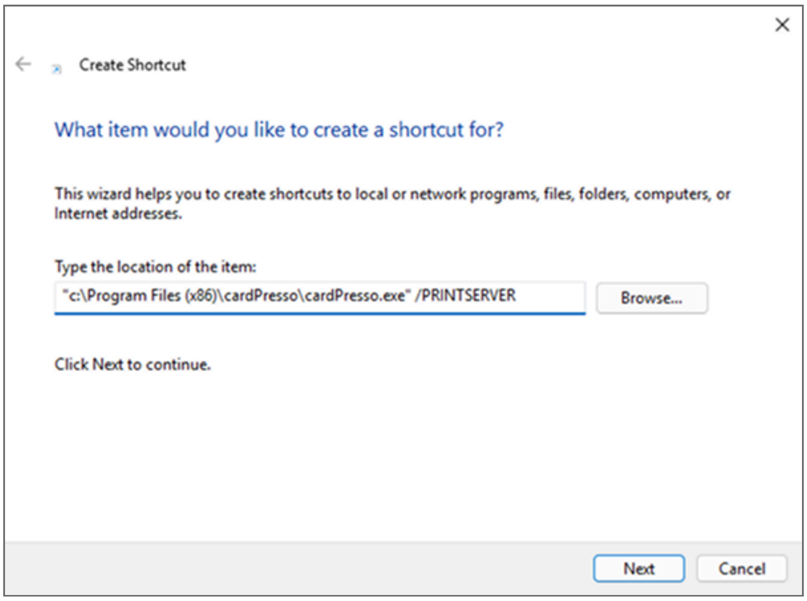
The image above is an example screen and may differ from the actual screen.

4. Save the created card template to a desired location on the server where **BioStar X** is installed. (ex. *C:\template\example.card*)

5. Right-click on the desktop of the PC where cardPresso is installed, then click **New** → **Shortcut** from the popup menu.

6. Enter the following in the **Item Location** field, then click the **Next** button.

```
"C:\Program Files (x86)\cardPresso\cardPresso.exe" /PRINTSERVER
```



Create Shortcut

What item would you like to create a shortcut for?

This wizard helps you to create shortcuts to local or network programs, files, folders, computers, or Internet addresses.

Type the location of the item:

"c:\Program Files (x86)\cardPresso\cardPresso.exe" /PRINTSERVER

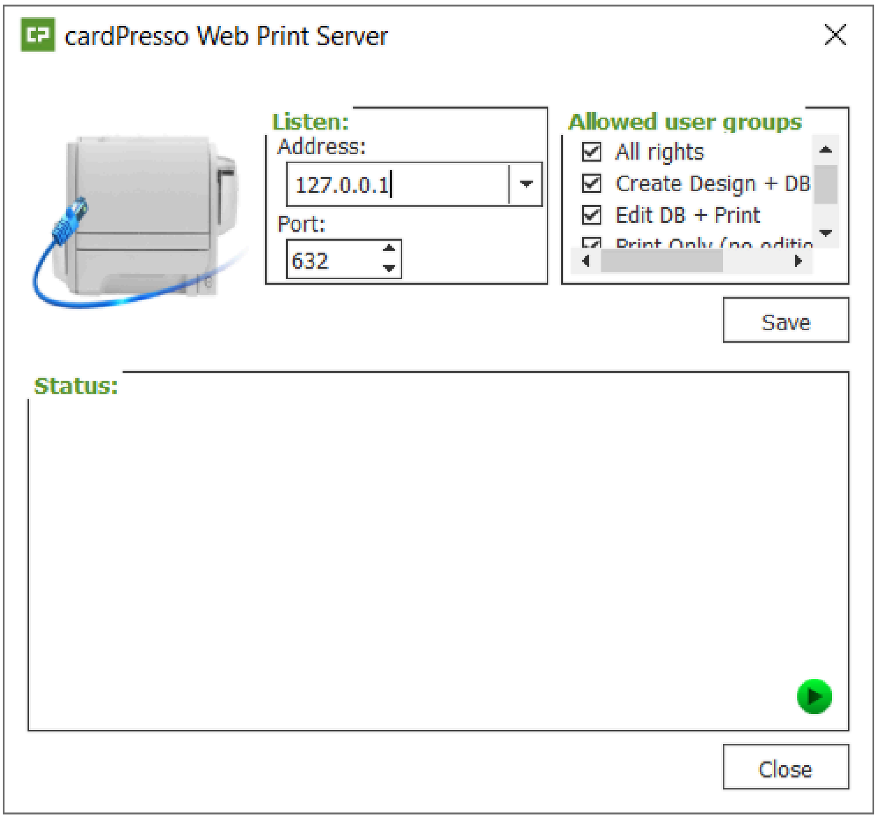
Click Next to continue.

> ⓘ The path where cardPresso is installed may differ based on the installation environment. After confirming the path where cardPresso is installed, modify it appropriately according to the above path.

7. Enter a name for the shortcut, then click the **Finish** button.

8. Double-click the cardPresso web printing server shortcut icon created on the desktop to run it.

9. When the cardPresso web printing server window appears, click the **Settings** icon.



Address: 127.0.0.1

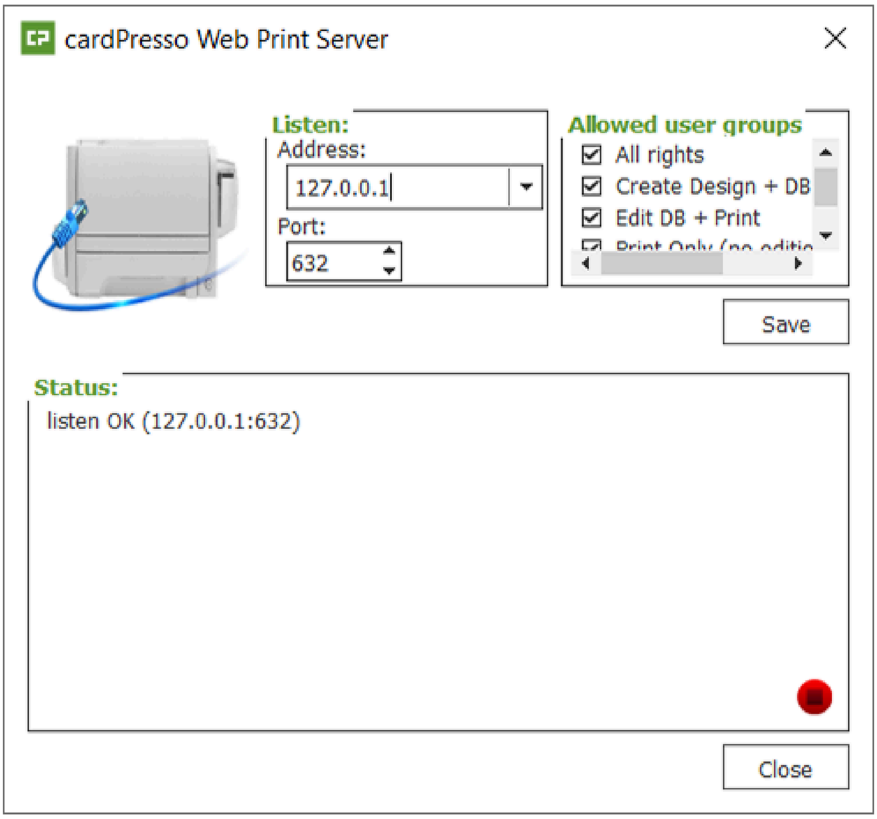
Port: 632

☑ All rights
☑ Create Design + DB
☑ Edit DB + Print
☑ Print Only (no editio

- **Address**: Enter the IP address of the computer acting as the Web Print Server.
- **Port**: Port number on which cardPresso receive print operations.
- **Allowed user groups**: Select a user group that has access to the Web Print Server.

10. Click **Save** when the configuration is complete.

11. Click the ▶ in the bottom right corner to start the service. If properly set, the icon changes to ■ and a **listen OK** message appears.



cardPresso Web Print Server

Listen:
Address: 127.0.0.1
Port: 632

Allowed user groups
☑ All rights
☑ Create Design + DB
☑ Edit DB + Print
☑ Print Only (no editio

Status:
listen OK (127.0.0.1:632)

> ⓘ Do not close the window until card printing is complete.

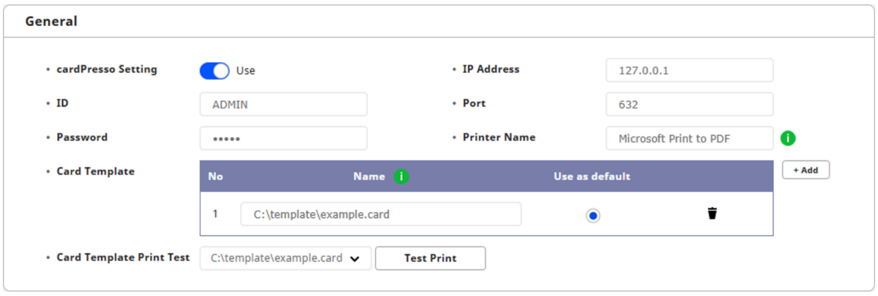
Connecting cardPresso to BioStar X

To connect cardPresso to **BioStar X**, set it up as shown below.

1. Click **Settings** on the **Launcher** page.

2. In the left sidebar, click **Card Printer**.

3. Activate the **cardPresso Setting** to **Use**, then enter each item.



General

- cardPresso Setting: Use
- ID: ADMIN
- Password: •••••
- Card Template:

No	Name	Use as default
1	C:\template\example.card	●

- IP Address: 127.0.0.1
- Port: 632
- Printer Name: Microsoft Print to PDF
- Card Template Print Test: C:\template\example.card

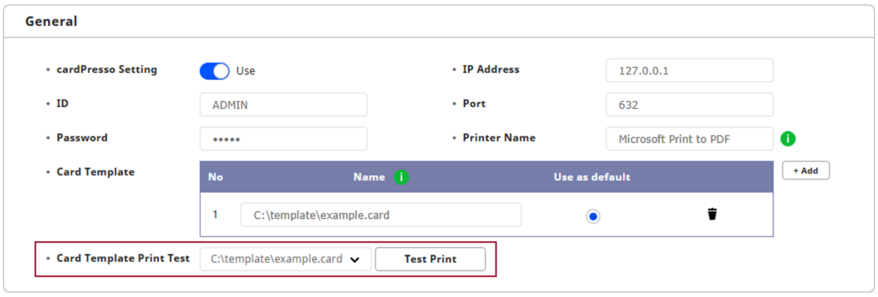
- **ID**: Enter your cardPresso login ID. (default: ADMIN)
- **Password**: Enter your cardPresso login password. (default: admin)
- **IP Address**: Enter the IP address of the PC that runs the cardPresso web print server.
- **Port**: Enter the port number used by cardPresso to receive print operations.
- **Printer Name**: Enter the name of the printer to be used as a card printer. It can be found in the Windows **Control Panel** → **Devices and printers**.
- **Card Template**: Click **+ Add** to add a **Card Template**. In the **Name** item, enter the full path including the filename and extension of the card template.
  - The file name of the card template can be entered using alphanumeric, and special characters.
  - Up to 20 card templates are supported.
  - Example path: C:\template\example.card
- **Card Template Print Test**: Test print the card template.

4. Once you complete the settings, click **Apply**.

Test printing the card template

Test print a card template with Administrator information.

1. Click **Settings** on the **Launcher** page.
2. In the left sidebar, click **Card Printer**.
3. Select the card template you want to print, then click the **Test Print** button.



General

- cardPresso Setting: Use
- ID: ADMIN
- Password: •••••
- Card Template:

No	Name	Use as default
1	C:\template\example.card	●

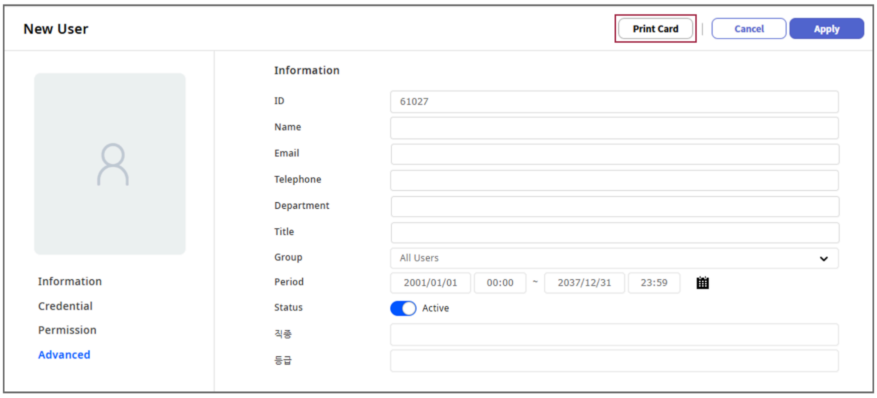
- IP Address: 127.0.0.1
- Port: 632
- Printer Name: Microsoft Print to PDF
- Card Template Print Test: C:\template\example.card

4. Card template with Administrator information is printed.

Print card templates by user

Print cards with per-user card templates.

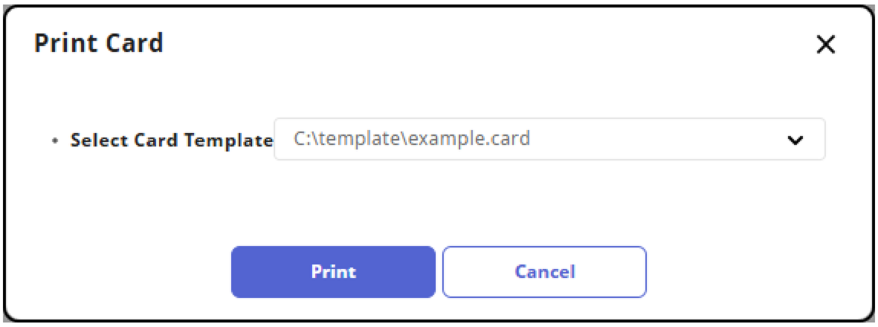
1. Click **User** on the **Launcher** page.
2. Click the **New User** button at the top right of the screen. The **New User** window appears.
3. Fill out the form and click the **Print Card** button.
   - Each item can be entered with alphanumeric and special characters.



Information

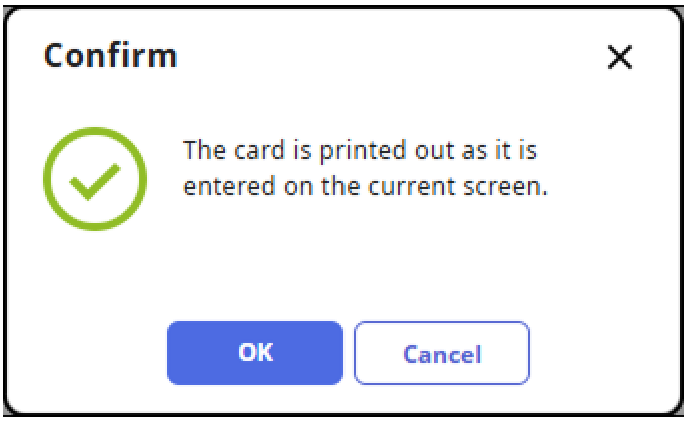
ID: 61027
Name:
Email:
Telephone:
Department:
Title:
Group: All Users
Period: 2001/01/01 00:00 ~ 2037/12/31 23:59
Status: Active
직종:
등급:

4. Select the card template you want to print and click the **Print** button.



Select Card Template: C:\template\example.card

5. When the popup window asking whether to print the card appears, click the **OK** button.



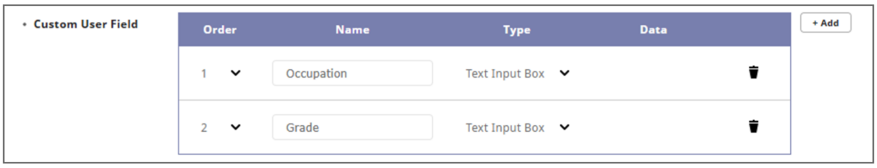
The card is printed out as it is entered on the current screen.

New user will be created and a card is printed as a card template with user information.

Add custom user fields

Print a card with a card template with custom user field added.

1. Click **Settings** on the **Launcher** page.
2. Click **Server** → **Server** in the left sidebar.
3. In the **User/Device Management** section, click the **+ Add** button to enter **Name** and select **Type**. The order of the **Custom User Field** adds decides the element **ID** of the card template.



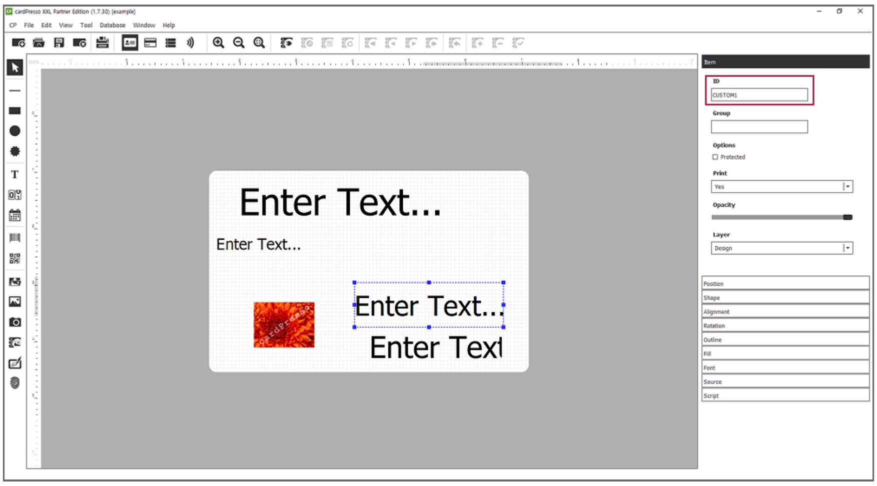
• Custom User Field

+ Add

Order	Name	Type	Data
1	Occupation	Text Input Box	
2	Grade	Text Input Box	

   Based on the BioStar X element ID, **Order 1** is the same as **CUSTOM1**. For more information on the BioStar X attribute ID, refer to the following.

4. Once you complete the settings, click the **Apply** button at the very bottom of the screen.
5. Open the card template file by clicking **File** → **Open Template** in the cardPresso program. Add a new element and enter the **ID** as the **XML item ID name** in the BioStar X element ID order.



cardPresso XXL Partner Edition (1.7.30) [example]

Item

ID: CUSTOM1

Group:

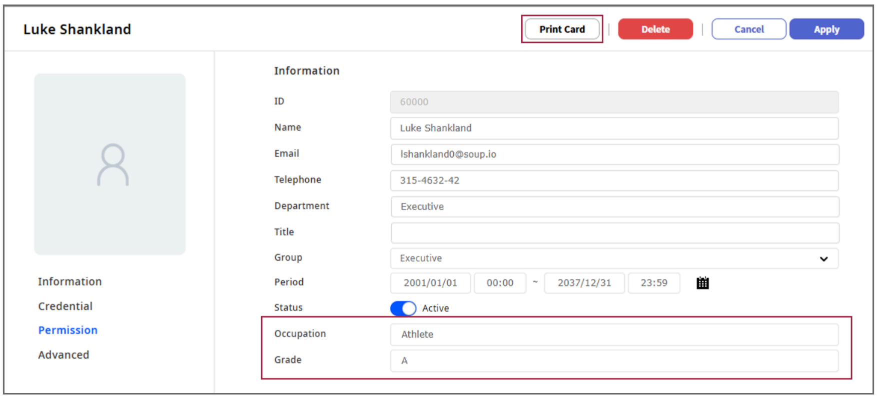
Options: □ Protected

Print: Yes

Layer: Design

6. Click **File** → **Save** when the configuration is complete.
7. Return to **BioStar X** and select the user to apply the card template on the **User** page.

8. You can check the custom user fields you added. Fill in accordance with the form and click the **Print Card** button.

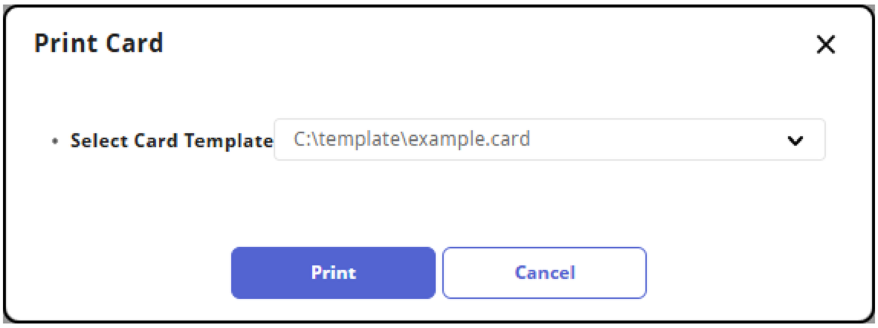


Luke Shankland

Information

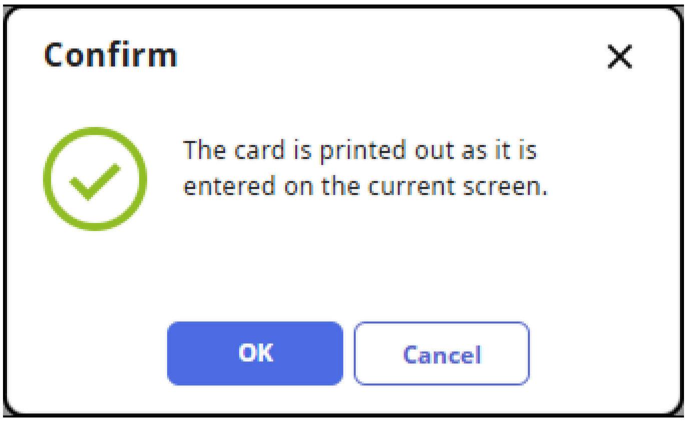
ID	60000
Name	Luke Shankland
Email	lshankland0@soup.io
Telephone	315-4632-42
Department	Executive
Title	
Group	Executive
Period	2001/01/01 00:00 ~ 2037/12/31 23:59
Status	Active
Occupation	Athlete
Grade	A

9. Select the card template you want to print and click the **Print** button.



- Select Card Template: C:\template\example.card

10. When the popup window asking whether to print the card appears, click the **OK** button.



The card is printed out as it is entered on the current screen.

User information is saved and the card is printed as a card template with custom user fields added.

Card template attribute ID

The supported attribute IDs in **BioStar X** are as follows. Make sure to enter **XML item ID name** as element ID when creating a card template.

Index	BioStar X User Data	XML item ID name
1	User ID	ID
2	User Name	NAME
3	Email	EMAIL
4	Department	DEPARTMENT
5	Telephone	TELEPHONE
6	User Group	GROUP
7	Profile Photo	PHOTO
8	Custom Field 1	CUSTOM1
9	Custom Field 2	CUSTOM2
10	Custom Field 3	CUSTOM3
11	Custom Field 4	CUSTOM4
12	Custom Field 5	CUSTOM5
13	Custom Field 6	CUSTOM6
14	Custom Field 7	CUSTOM7
15	Custom Field 8	CUSTOM8
16	Custom Field 9	CUSTOM9
17	Custom Field 10	CUSTOM10

Email Setting

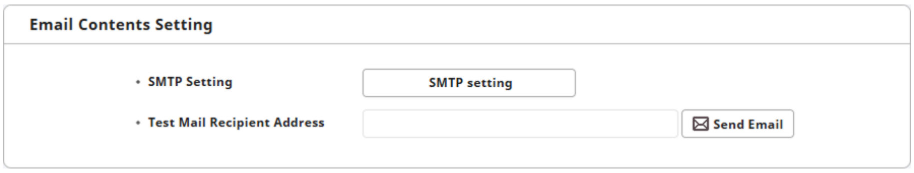
You can configure information such as the subject line of the email that will send the mobile link for face enrollment, the company name, company logo, and contact details.

> **INFO**
>
> - You must register the user's email address in the user information to send the mobile link for face enrollment or issue a QR/Barcode. For more information about user information, refer to the following.
> - The devices that can perform **facial authentication** are as follows.
>   - FaceStation F2, BioStation 3, BioEntry W3
> - The devices that can use **Use QR/Barcode through Scanner** are as follows.
>   - X-Station 2 (XS2-QDPB, XS2-QAPB)
> - The devices that can use **Use QR/Barcode through Camera** are as follows.
>   - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) firmware version 1.2.0 or higher
>   - BioStation 3 (BS3-DB, BS3-APWB) firmware version 1.1.0 or higher
>   - Using **Use QR/Barcode through Camera** requires a separate device license. For more information about device license, refer to the following.

1. Click **Settings** on the **Launcher** page.
2. In the left sidebar, click the **EMAIL SETTING**.
3. Edit the necessary fields.
4. Click **Apply** to save the settings.

Set up email content

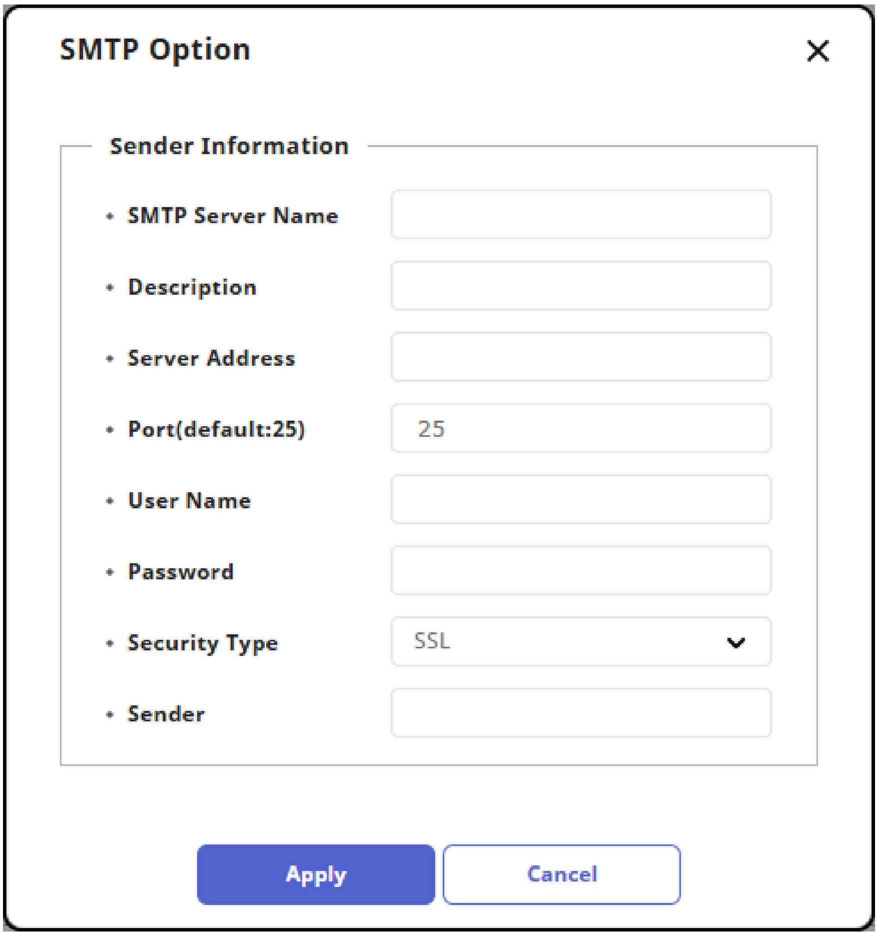
Enter the SMTP server information for sending emails.



Email Contents Setting

- SMTP Setting: SMTP setting
- Test Mail Recipient Address: Send Email

- **SMTP Setting**: Set the SMTP(Simple Mail Transfer Protocol) for sending emails. Click **SMTP setting** to open the **SMTP Setting** settings window.



SMTP Option

Sender Information

- SMTP Server Name
- Description
- Server Address
- Port(default:25) 25
- User Name
- Password
- Security Type SSL
- Sender

- **SMTP Server Name**: Enter the SMTP server name.
- **Description**: Enter the description.
- **Port(default:25)**: Enter the port number of the SMTP server. The SMTP server address is in the format `smtp.{email-service-provider}.com`, and you can confirm it on the settings screen of the email used as the SMTP server.
- **Server Address**: Enter the SMTP server address. Email Service Provider.com', and you can check it on the settings screen of email to use as an SMTP.
- **User Name**: Enter the account of the SMTP service.
- **Password**: Enter the password of the SMTP service.
- **Security Type**: Select security type.
- **Sender**: Enter the email address of the sender.

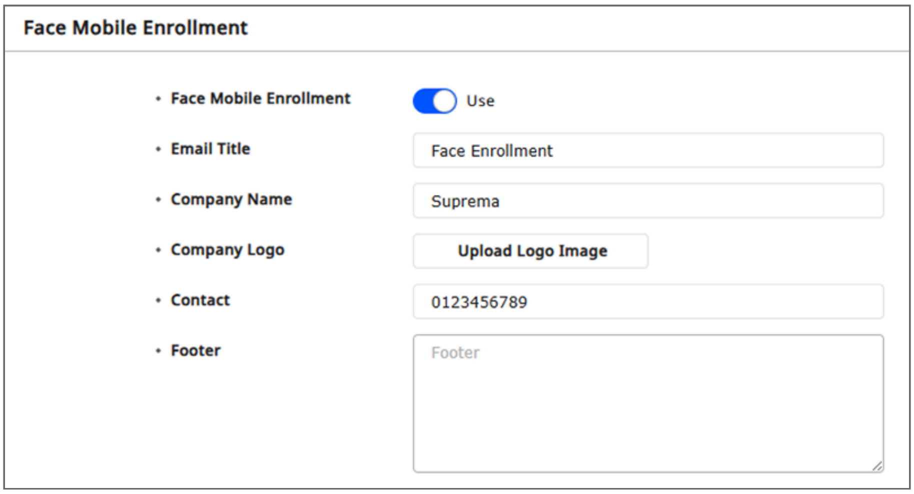
ⓘ **INFO**

- For more information about SMTP information, contact your system administrator.
- When using the SMTP server as an email account with two-factor authentication and change the password of the account, note the following: Once you set up two-factor authentication, the SMTP password is the same as the app password generated using two-factor authentication, not the password of the email account.
  - When you set up two-step authentication, the SMTP password uses the app password generated by two-step authentication, not the password for the email account.
  - At this time, if the password of the email account is changed, the app password is automatically deleted, and the SMTP password is no longer available.
  - When changing the password for the email account, regenerate the app password and then set the SMTP password again.

- To check if there are any issues with the SMTP settings, enter the email address to receive the email and click **Send Email**.

Set up mobile link for face enrollment

Set to **Use** to send a facial enrollment mobile link to the user via email.



Face Mobile Enrollment

Face Mobile Enrollment	Use
Email Title	Face Enrollment
Company Name	Suprema
Company Logo	Upload Logo Image
Contact	0123456789
Footer	Footer

- **Email Title**: Enter the subject line of the email to send the mobile link for face enrollment.
- **Company Name**: Enter the company name.
- **Company Logo**: Upload the company logo image.

ⓘ **INFO**

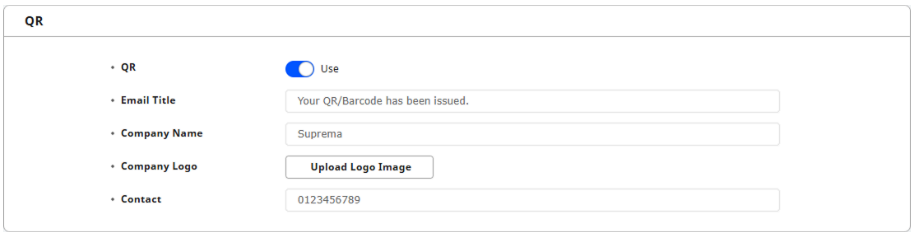
- Supported image file formats are GIF, JPG, JPEG, JPE, JFIF, PNG.
- Supported image file size is up to 5MB.

- **Contact**: Enter the contact information of the person in charge.
- **Footer**: Enter the content to be notified to users enrolling their face, such as legal notices. It will be displayed at the bottom of the email sent with the mobile link for face enrollment.

> **INFO**
>
> Footer can be up to 5,000 characters in length.

QR/Barcode setting

To use the QR/Barcode set it as **Use**.



QR

- QR: Use
- Email Title: Your QR/Barcode has been issued.
- Company Name: Suprema
- Company Logo: Upload Logo Image
- Contact: 0123456789

- **Email Title**: Enter the title of the email.
- **Company Name**: Enter the company name.
- **Company Logo**: Upload the company logo image.

> **INFO**
>
> – Supported image file formats are GIF, JPG, JPEG, JPE, JFIF, PNG.
>
> – Supported image file size is up to 5MB.

- **Contact**: Enter the contact information of the person in charge.

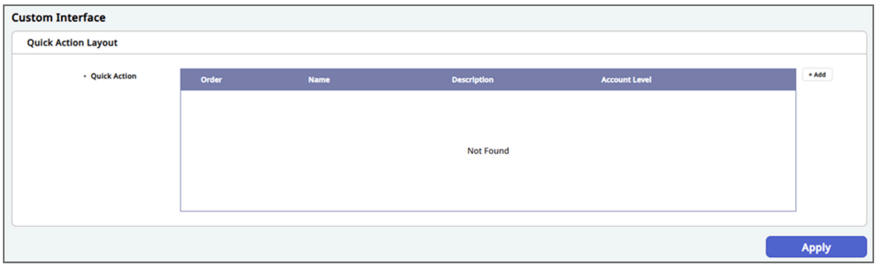
How to Use the Quick Action

Adding a quick action button in the **Custom Interface** menu allows you to easily control multiple access points at once by clicking the quick action button on the **BioStar X** main screen.

> ⓘ **INFO**
>
> To add a **Trigger & Action** for Quick Action, refer to the following.

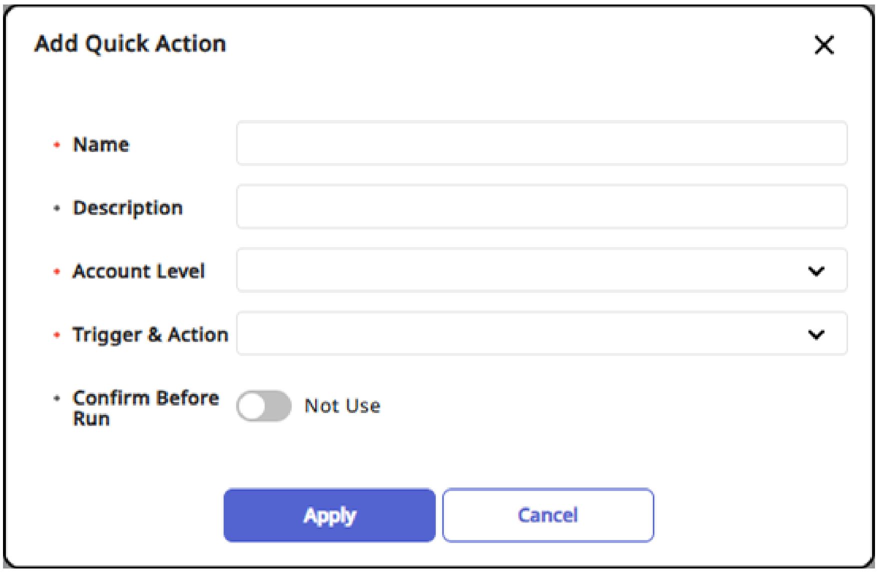
Add quick action button

1. Click **Settings** on the **Launcher** page.
2. In the left sidebar, click the **Custom Interface**.



3. Click **Quick Action Layout** button in the section.

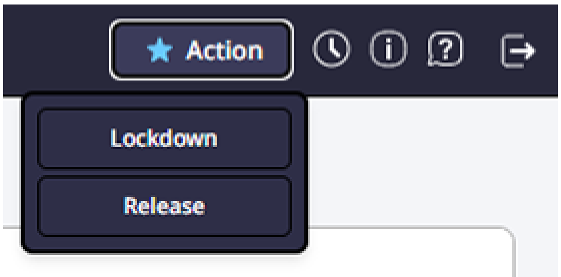
4. When the **Add Quick Action** window appears, enter and set each item.



- **Account Level**: Select the **Account Level** that can execute the quick action you want to add. You can select multiple options.
- **Trigger & Action**: Select the **Trigger & Action** to execute. You can select multiple options.
- **Confirm Before Run**: Enabling this option will prompt a confirmation popup when you press the **Quick Action** button to ask if you want to execute it.

5. Click **Apply** button to save the settings.
6. Click Apply at the bottom right of the screen.

The **Quick Action** button added in the upper right header area of the **BioStar X** screen will be created. Click the created **Quick Action** button to verify it works as configured in **Trigger & Action**.

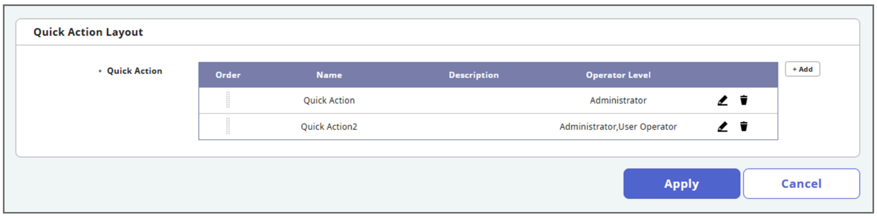


INFO

- You can add up to four **Quick Action** buttons in the upper header area of the screen. It is fixed for use on any page.
- The **Quick Action** buttons available may differ depending on the settings configured for the user **Account Level**.

Editing the Quick Action buttons

1. Click **Settings** on the **Launcher** page.
2. In the left sidebar, click the **Custom Interface**.
3. Click the ✎ button on the right side of the quick action button you want to modify.



Quick Action Layout

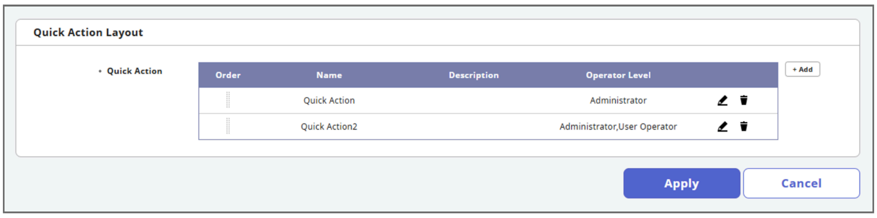
- Quick Action

Order	Name	Description	Operator Level	
	Quick Action		Administrator	✎ 🗑
	Quick Action2		Administrator,User Operator	✎ 🗑

4. When the popup for editing appears, modify the desired item and click the **Apply** button.
5. To save the modifications, click the **Apply** button at the bottom right of the screen.

Deleting the Quick Action button

1. Click **Settings** on the **Launcher** page.
2. In the left sidebar, click the **Custom Interface**.
3. Click the 🗑 button to the right of the quick action button you want to delete.

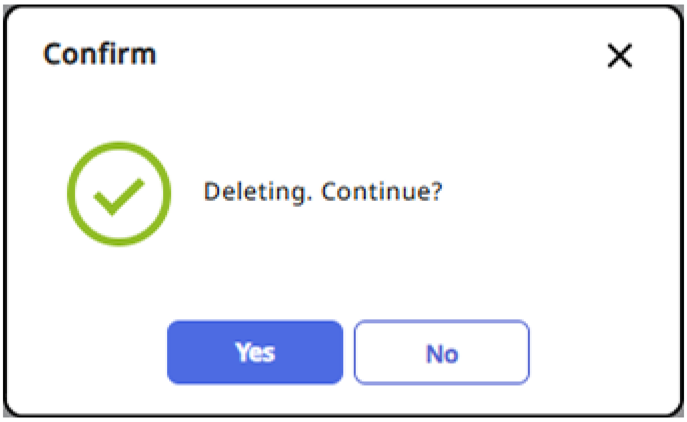


Quick Action Layout

- Quick Action

Order	Name	Description	Operator Level	
	Quick Action		Administrator	✎ 🗑
	Quick Action2		Administrator,User Operator	✎ 🗑

4. Check the deletion confirmation pop-up and click **Yes**.



Confirm

Deleting. Continue?

5. To reflect the deleted items, click the **Apply** button at the bottom right of the screen.

Server Settings

This guide provides various methods for server operations such as basic information about the **BioStar X** server, user and device management, automatic upgrades, and HTTPS certificate.

Server Detailed Settings

Guidance on the basic information of the BioStar X server, user and device management, server matching, system log levels, and settings for saving facial images.

Install HTTPS Certificate

To connect BioStar X via HTTPS, you must register the IP address of the server where BioStar X is installed to install the certificate.

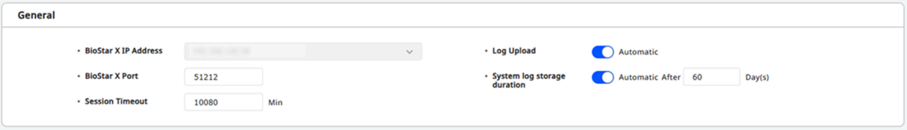
Server Detailed Settings

You can change the basic information settings of the BioStar X server, user and device management, server matching, system log levels, and settings for saving facial images.

1. Click **Settings** on the **Launcher** page.
2. Click **Server** → **Server** in the left sidebar.
3. Set the desired items in each section.
   - **General**: You can set the IP address, port number, session expiration time, event log upload method, and log retention period.
   - **User/Device Management**: You can change user and device management settings.
   - **System Log Level Settings**: You can change system log level settings.
   - **Expert Settings**: You can set it to save both the actual image and the template of the face or save only the template without storing the actual image.
4. Click **Apply** at the bottom right of the screen to save the settings.

Basic information settings

You can check or set basic information for **BioStar X** in the **General** section.



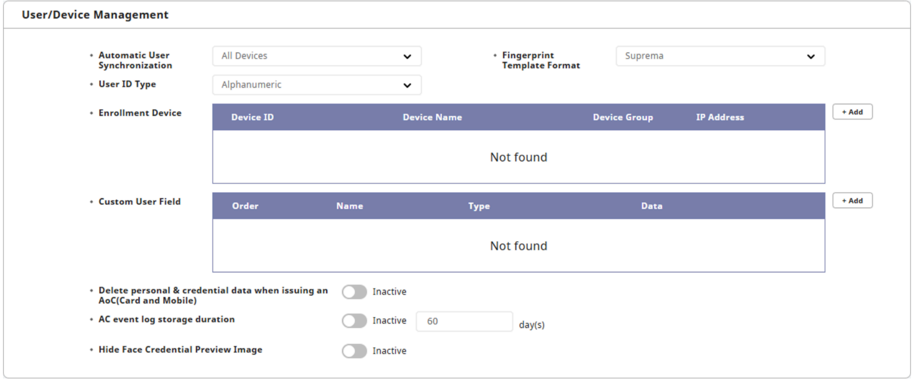
General

- BioStar X IP Address [redacted]
- BioStar X Port 51212
- Session Timeout 10080 Min
- Log Upload ● Automatic
- System log storage duration ● Automatic After 60 Day(s)

- **BioStar X IP Address**: You can check the server IP address.
- **Log Upload**: Select an event log upload method. If real-time communication with the server is difficult, set this to **Manual**.
- **BioStar X Port**: You can change the server port. Enter the desired port number.
- **System log storage duration**: The log retention period can be set from 1 to 120 days.
- **Session Timeout**: Set a session timeout period. If there is no operation after logging into BioStar X for the configured time, you will be automatically logged out.

User and device management

In the **User/Device Management** section, you can set the synchronization and authentication methods between users and devices.



User/Device Management

- Automatic User Synchronization: All Devices
- Fingerprint Template Format: Suprema
- User ID Type: Alphanumeric
- Enrollment Device

Device ID	Device Name	Device Group	IP Address
Not found			

- Custom User Field

Order	Name	Type	Data
Not found			

- Delete personal & credential data when issuing an AoC(Card and Mobile): Inactive
- AC event log storage duration: Inactive 60 day(s)
- Hide Face Credential Preview Image: Inactive

Automatic User Synchronization

In the **Automatic User Synchronization** option, you can choose how to synchronize user information between the server and devices.

- **All Devices**: User information is synchronized automatically between the server and all registered devices.
- **All Devices(Including user update from device)**: User information from the server is synchronized with all devices registered on the server. However, user information modified on the device is not synchronized to the server, and only user information added on the device is synchronized to the server.
- **Specific Devices(Only devices belonging to the access group)**: Only devices belonging to an access group with changes are automatically synchronized with the server.

> **INFO**
>
> - If you select the **Specific Devices(Only devices belonging to the access group)** option, users saved on devices that do not belong to the access group cannot be managed by the server. To use this option, go to **Settings** → **Device** to select each device, and then click **Delete Data & Sync Device** to proceed with synchronization. For more information about the **Delete Data & Sync Device** feature, refer to the following.
> - Even if you select the **Specific Devices(Only devices belonging to the access group)** option, special access groups designated for specific purposes will synchronize regardless of the device access group.
>   - Dual authentication access group set up in the Devices and Elevators.
>   - Always pass group for anti-passback setting
>   - Always pass group for schedule lock setting
>   - Open authentication access group for schedule open setting
>   - Access/Deactivate group for guard setting
> - Even if you select the **Specific Devices(Only devices belonging to the access group)** option, users designated as device administrators will synchronize regardless of the access group.

Fingerprint Template Format

In the **Fingerprint Template Format** option, you can choose the fingerprint template format. Select from the following items.

- **SUPREMA**: Suprema fingerprint template format. Used when enrolling fingerprints on Suprema devices.
- **ISO**: ISO international fingerprint template format.
- **ANSI378**: Fingerprint template format defined by the American National Standards Institute (ANSI).

> ⓘ **INFO**
>
> If there are existing user fingerprint templates on the device, they cannot be changed to another format.

User ID Type

In the **User ID Type** option, you can select the user ID type as **Number** or **Alphanumeric**. Check the list of devices registered in the **BioStar X** server and select compatible settings.

View devices and firmware versions that can change **User ID Type**

- CoreStation firmware version 1.0.0 or higher
- FaceStation 2 firmware 1.0.0 or higher
- FaceLite firmware 1.0.0 or higher
- BioEntry W2 FW 1.1.0 or later
- BioStation L2 FW 1.2.0 or later
- BioStation A2 FW 1.3.0 or later
- BioStation 2 FW 1.4.0 or later
- BioLite N2 firmware 1.0.0 or higher
- BioEntry P2 firmware 1.0.0 or higher
- BioEntry R2 FW 1.0.0 or later
- XPass 2 firmware 1.0.0 or higher
- XPass D2 firmware version 1.0.0 or higher
- X-Station 2 firmware 1.0.0 or higher
- BioStation 3 firmware 1.0.0 or higher

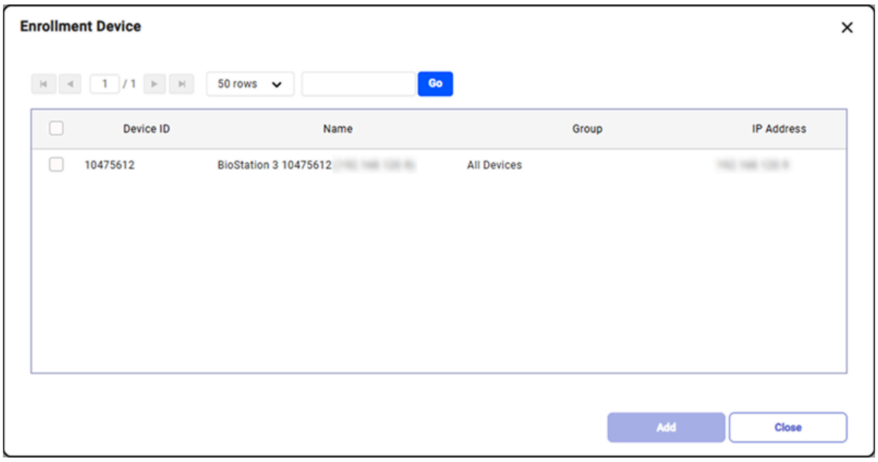
ⓘ **INFO**

Changing from **Alphanumeric** to **Number** requires deleting all user information registered in **BioStar X**.

Enrollment Device

You can add frequently used devices for enrolling fingerprints, faces, or cards in the **Enrollment Device** option for convenience.

1. Click the **+ Add** button to add a device.
2. When the **Enrollment Device** window appears, click the checkbox of the desired device from the list.



Enrollment Device

□	Device ID	Name	Group	IP Address
□	10475612	BioStation 3 10475612 [redacted]	All Devices	[redacted]

3. Click the **Add** button to add the selected device.
4. Click **Apply** at the bottom right of the screen to save the added device settings.

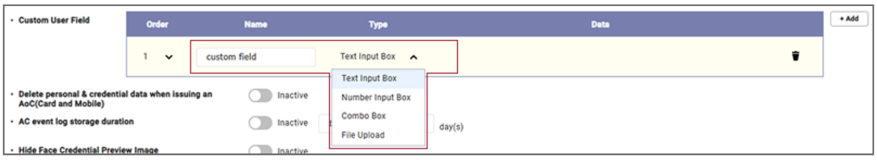
ⓘ **INFO**

- If you find it difficult to locate a registered device from the list due to the large number, enter keywords in the search input field to find devices. You can enter the device ID, device name, device group, and IP address.
- For more information on enrolling fingerprints or face, card credentials, refer to the followings:
  - Enroll Fingerprint
  - Enroll Face
  - Enroll Access Card
  - Enroll Mobile Access Cards

Custom field settings

In the **Custom User Field** option, you can add fields to input additional information about the user. The added fields will be displayed on the user information screen.

1. To add a custom user field, click the **+ Add** button.
2. Enter the name of the custom user field and select the desired item type.

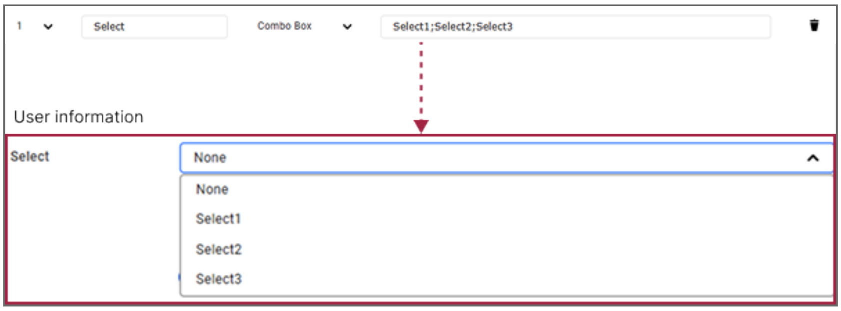


- Custom User Field

Order	Name	Type	Data
1	custom field	Text Input Box	

- Delete personal & credential data when issuing an AoC(Card and Mobile): Inactive
- AC event log storage duration: Inactive day(s)
- Hide Face Credential Preview Image: Inactive

- **Number Input Box**: Allows entry of values from 0 to 4294962795; characters cannot be entered.
- **Text Input Box**: Allows entry of up to 32 characters of numbers and letters.
- **Combo Box**: Allows addition of up to 20 items of 32 characters; each item is separated by a semicolon (;). (e.g., Select1;Select2;Select3)



1 | Select | Combo Box | Select1;Select2;Select3

User information

Select: None

- **File Upload**: You can add a field for file uploads.

> – The maximum file size is 1MB.
>
> – The file name can be a minimum of 1 character and a maximum of 120 characters.
>
> – File name requirements: The file name must use alphanumeric characters, underscores (_), and hyphens (-), and use a period (.) to separate the extension.

3. Click the **Apply** button at the bottom right of the screen to save the added custom user field.

> **INFO**
>
> - To change the order of the custom user fields, change the numbers in the **Order** column. The position of that field will change.
> - After modifying the custom user fields, click the **Apply** button at the bottom right of the screen.
> - Click the 🗑 button to delete a custom user field. Deleted fields cannot be recovered.
> - For more information on user information registration and modification, refer to the following.
> - User information with added custom user fields can be printed on a card. For more information, refer to the following link.

AoC card settings

To issue an Access on Card (AoC) credential that stores user credentials on a card, enable the **Delete personal & credential data when issuing an AoC(Card and Mobile)** option to delete personal information and credential data from the **BioStar X** server.

ⓘ **INFO**

View devices and firmware versions that support **NFC mobile cards**

- Mobile device OS: Android 5.0 Lollipop or later, Android 10 or earlier
- BioStar X Mobile 1.0.0 or higher
- XPass S2: XPS2M-V2 FW 2.4 or later
- BioStation 2: BS2-OMPW, BS2-OIPW FW 1.4 or later, FW 1.8 or earlier
- BioStation A2: BSA2-OMPW, BSA2-OIPW FW 1.3 or later, FW 1.7.1 or earlier
- BioStation L2: BSL2-OM FW 1.2 or later
- BioEntry W2: BEW2-OAP, BEW2-ODP FW 1.1 or later, FW 1.5 or earlier
- FaceStation 2: FS2-D, FS2-AWB FW 1.3.1 or earlier
- BioLite N2: BLN2-ODB, BLN2-OAB, BLN2-PAB FW 1.2 or earlier
- XPass D2: XPD2-MDB, XPD2-GDB, XPD2-GKDB FW 1.3 or earlier
- FaceLite: FL-DB FW 1.1 or earlier
- XPass 2: XP2-MDPB, XP2-GDPB, XP2-GKDPB, XP2-MAPB FW 1.0 or later
- BioEntry P2: BEP2-OD, BEP2-OA FW 1.0 or later
- BioEntry R2: BER2-OD FW v1.1.0 or later

View devices and firmware versions that support **BLE mobile cards**

- Mobile device OS: Android 5.0 Lollipop or later, Android 10 or earlier / iOS 9.0 or later
- BioStar X Mobile 1.0.0 or higher
- FaceStation 2: FS2-AWB FW 1.3.1 or earlier
- BioLite N2: BLN2-ODB, BLN2-OAB, BLN2-PAB FW 1.2 or earlier
- XPass D2: XPD2-MDB, XPD2-GDB, XPD2-GKDB FW 1.3 or earlier
- FaceLite: FL-DB FW 1.1 or earlier
- XPass 2: XP2-MDPB, XP2-GDPB, XP2-GKDPB, XP2-MAPB FW 1.0 or later
- **Use Server Matching**: Activates/Deactivates server matching.

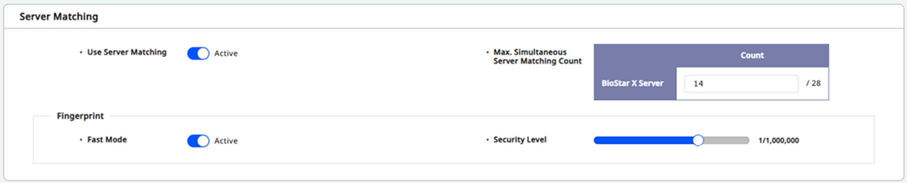
Other settings

- **AC event log storage duration**: Set the retention period for access control event logs.

- **Hide Face Credential Preview Image**: To protect users' personal information, the preview image can be hidden during the registration of face credentials. When this option is enabled, the preview screen will not be provided when enrolling users' face credentials.

Server matching

In the **Server Matching** section, you can set up the server matching feature to authenticate user information on **BioStar X** without authenticating on the device.



Server Matching

- Use Server Matching: Active
- Max. Simultaneous Server Matching Count

	Count
BioStar X Server	14 / 28

Fingerprint

- Fast Mode: Active
- Security Level: 1/1,000,000

- **Use Server Matching**: Activates/Deactivates server matching.
- **Max. Simultaneous Server Matching Count**: You can configure how many matchings can be done simultaneously.

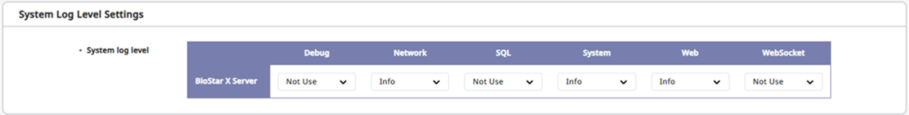
> This option may vary depending on the CPU performance of the server PC where **BioStar X** is installed.

- **Fast Mode**: You can configure the fingerprint matching speed.
- **Security Level**: You can set the security level for server matching for fingerprints. The higher the security level is set, the more the false rejection rate (FRR) can occur.

> **INFO**
>
> **Server Matching** is available when feature add-ons are enabled with an **Advanced** or higher license. For more information about the license policy, refer to the following.

System log level settings

In the **System Log Level Settings** section, you can set the level of system logs stored in the database.



System Log Level Settings

- System log level

	Debug	Network	SQL	System	Web	WebSocket
BioStar X Server	Not Use	Info	Not Use	Info	Info	Not Use

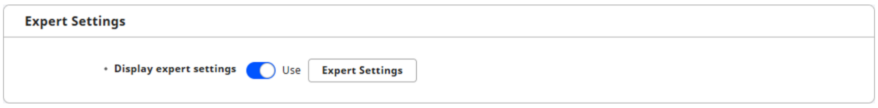
System logs are managed according to predefined categories, and the log levels are classified into **Trace**, **Debug**, **Info**, **Warning**, and **Error**. The high level contains all lower level logs. For example, if you select **Trace**, it will include and save all lower levels of **Debug**, **Info**, **Warning**, and **Error** logs.

Saving facial images

When enrolling a face as a credential, you can set it to save both the actual image and template, or to save only the template without the actual image.

> **Before using**
>
> Before activating the **Display expert settings** option, if any changes have been made in the **Server** menu, be sure to save those changes first. Click Apply at the bottom right of the screen.

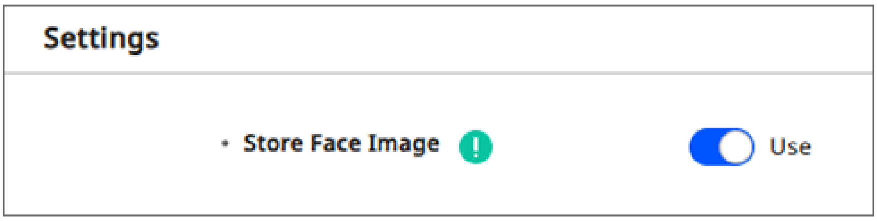
1. In the **Expert Settings** section, set the **Display expert settings** option to **Use**.



Expert Settings

- Display expert settings: Use

2. Click the **Expert Settings** button.
3. When you enter the **Expert Settings** screen, set the **Store Face Image** option.



Settings

- Store Face Image: Use

- **Use**: This is the default setting. Saves both the actual image and the template of the face credential.
- **Not Use**: Does not save the actual image of the face credential and saves only the template. Read the warning popup that appears when you select this option carefully before setting it.

4. Click **Apply** to save the settings.

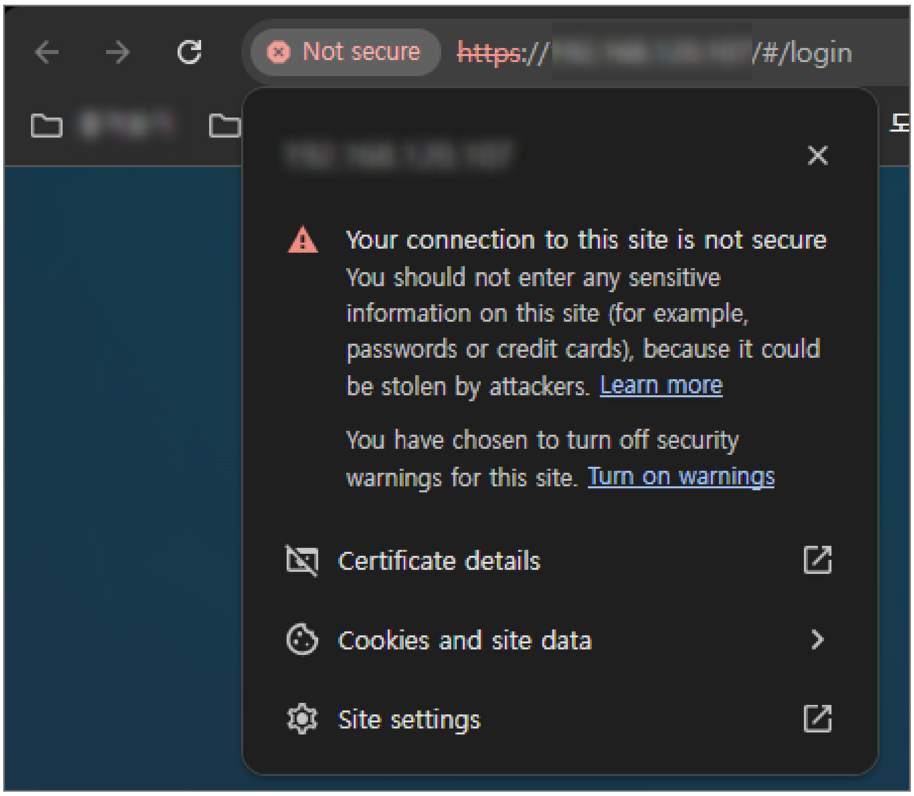
> **CAUTION**
>
> **Precautions when disabling the Store Face Image option**
>
> - If you disable this feature, all stored facial images will be deleted, and future enrolled facial images will only save the templates excluding the images.
> - This feature cannot be disabled if the enrolled facial images do not have both types of templates. For more information about the **Face Migration** feature, refer to the following.
> - After disabling this feature, if you include invalid face image templates in the **Data File Import**, you will not be able to import the data file. To resolve this issue, temporarily enable this feature before importing the data file.

Install HTTPS Certificate

To connect **BioStar X** via HTTPS, you must register the IP address of the server where **BioStar X** is installed to install the certificate.

When certificate installation is required

If you access **BioStar X** without the HTTPS certificate installed, a security warning like the following will appear in your web browser.



Your connection to this site is not secure
You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to turn off security warnings for this site. Turn on warnings

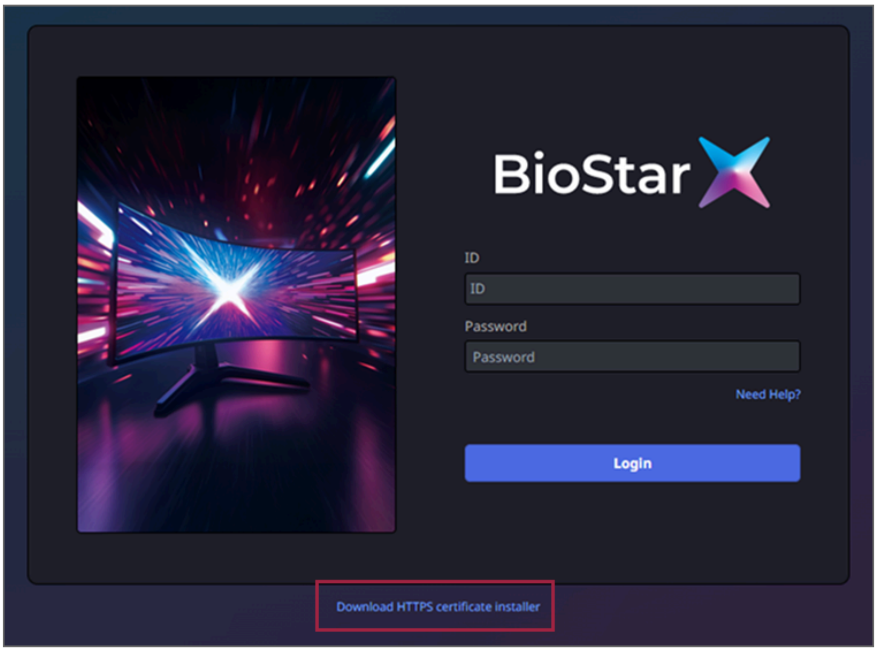
These warnings appear because the browser cannot verify the identity of the server. Installing the certificate will make the browser trust the **BioStar X** server, allowing for a secure HTTPS connection without security warnings.

Certificate installation

Install the certificate before using **BioStar X** for correct network connectivity.

1. Access the **BioStar X** login page.

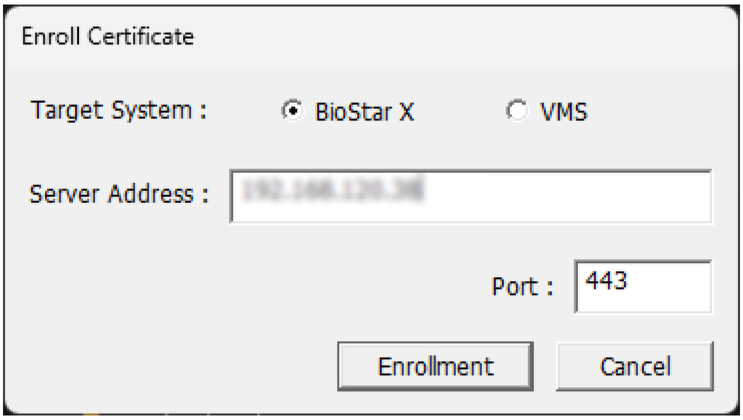
2. Click the **Download HTTPS certificate installer** link at the bottom of the screen.



3. Save the *cert-register.zip* file locally.

4. Extract the downloaded file and run the *cert-register.exe* file. The **Enroll Certificate** program runs.

5. Select **BioStar X** for **Target System**, enter the IP address of the PC where **BioStar X** is installed in **Server Address**, and click **Enrollment**.



Enroll Certificate

Target System : ● BioStar X ○ VMS

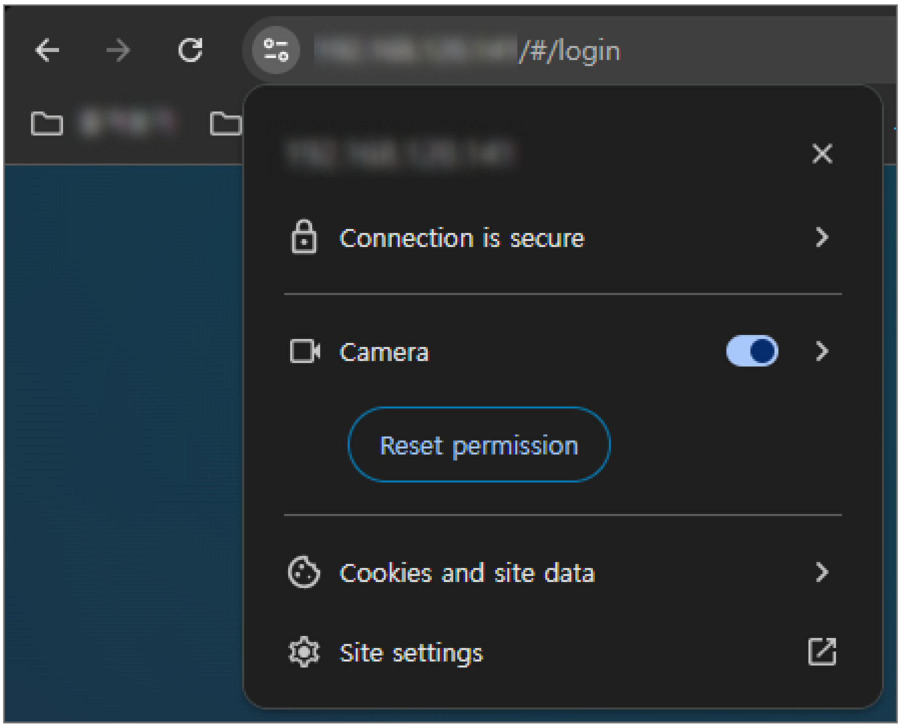
Server Address : [redacted]

Port : 443

> ⓘ The default port number for **BioStar X** is 443. If you changed the port number, enter the new port number in **Port**.

6. Check the security warning message and click **Yes**.

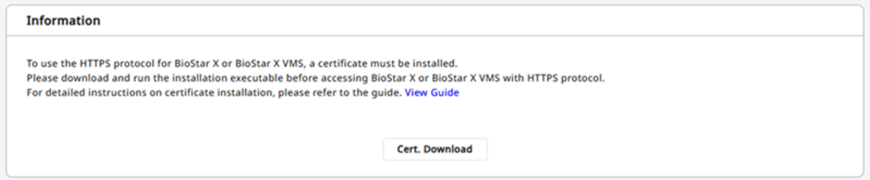
Restart the web browser and enter the registered IP address to navigate to the **BioStar X** page. When you click the icon to the left of the address bar, the message **This connection is secure** will appear.



> **INFO**
>
> The IP address entered in **Enroll Certificate** must be the same as the IP address set in **BioStar X**. You can check it in the menu path Settings → Server → Server under BioStar X IP Address.

Certificate installation in server settings

1. Click Settings on the Launcher page.
2. Click Server → HTTPS in the left sidebar of the screen.
3. Click Cert. Download.

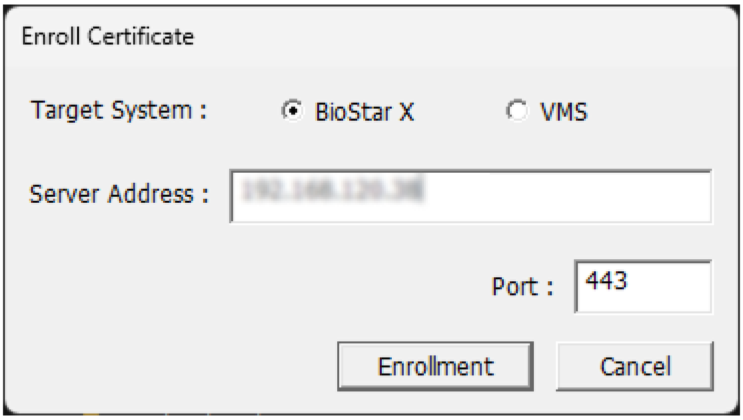


Information

To use the HTTPS protocol for BioStar X or BioStar X VMS, a certificate must be installed.
Please download and run the installation executable before accessing BioStar X or BioStar X VMS with HTTPS protocol.
For detailed instructions on certificate installation, please refer to the guide. View Guide

4. Save the *cert-register.zip* file locally.
5. Unzip the downloaded file and run **cert-register.exe** file. The **Enroll Certificate** program runs.

6. Select **BioStar X** for **Target System**, enter the IP address of the PC where **BioStar X** is installed in **Server Address**, and click **Enrollment**.



Enroll Certificate

Target System : ● BioStar X ○ VMS

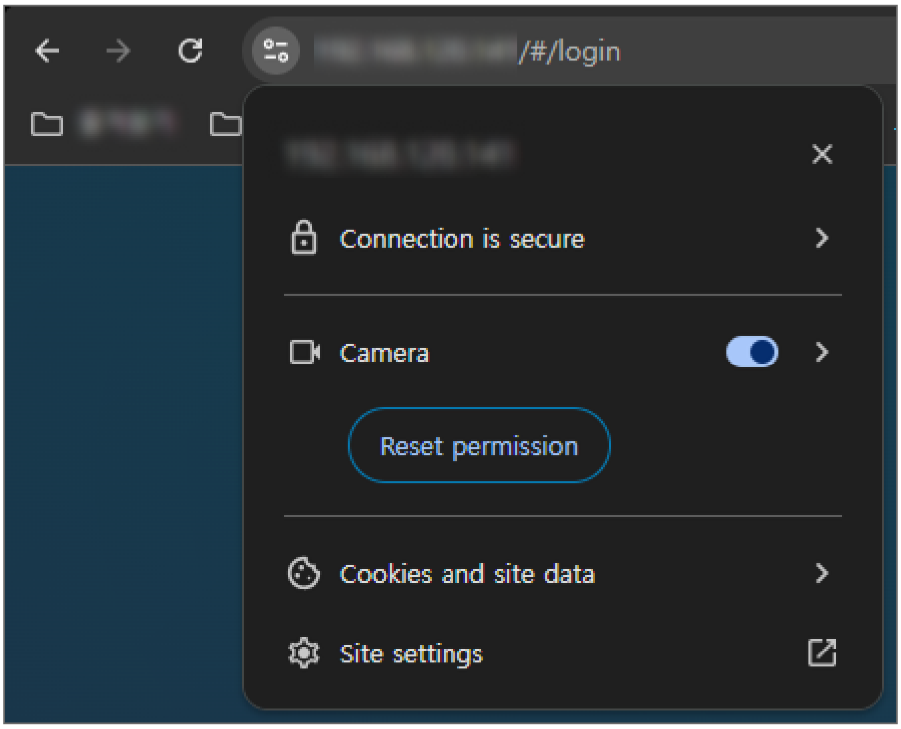
Server Address : [redacted]

Port : 443

> ⓘ The default port number for **BioStar X** is 443. If you changed the port number, enter the new port number in **Port**.

7. Check the security warning message and click **Yes**.

Restart the web browser and enter the registered IP address to navigate to the **BioStar X** page. When you click the icon to the left of the address bar, the message **This connection is secure** will appear.



[redacted]/#/login

[redacted]

Connection is secure

Camera

Certificate installation for VMS server

If the following situations occur, you can install the certificate from the VMS server onto the client PC to resolve the issue.

- When accessing **Video Management System** (VMS) through the browser, and a 'Not secure' warning appears

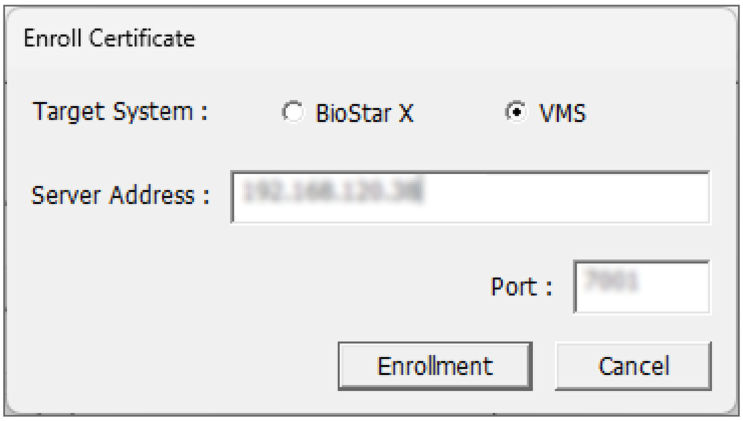
- When real-time video plays on the **Monitoring** page but recorded video does not play
- When installing the VMS server and **BioStar X** on the same server

INFO

- Refer to the following for how to install the certificate on the VMS server.
- The function to integrate with the VMS server must be purchased separately in an additional options package. For more information about the license policy, refer to the following.

Certificate installation on client PC

1. Download the HTTPS certificate installer (*cert-register.zip*) from the login screen or **Settings** → **Server** → **HTTPS** on the client PC where **BioStar X** is installed.
2. Unzip the downloaded file and run **cert-register.exe** file. The **Enroll Certificate** program runs.
3. Select **VMS** for **Target System** and enter the following information.



Enroll Certificate

Target System : ○ BioStar X ● VMS

Server Address : [redacted]

Port : [redacted]

   - **Server Address**: IP address of the VMS server
   - **Port**: Port number of the VMS server
4. Click the **Enrollment** button.
5. Check the security warning message and click **Yes**.

Restart the web browser and check if the recorded video from the VMS server plays normally on the **Monitoring** page.

Activate License

You can activate **BioStar X** license and device licenses.

BioStar X License

You can activate the purchased BioStar X license.

Device License

Activating a device license issued by Suprema allows using specific features corresponding to the license.

BioStar X License

You can activate the purchased **BioStar X** license.

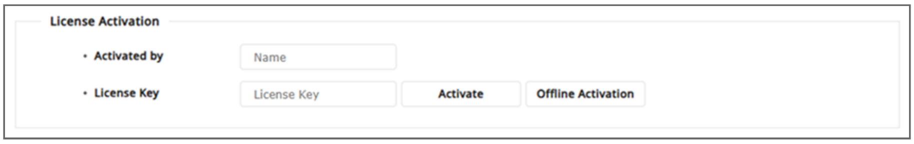
The method to activate BioStar X License varies depending on your network environment. Check your network status and activate your license according to the provided instructions.

1. Click Settings on the Launcher page.
2. Click License → BioStar X License in the left sidebar.

> ⓘ **INFO**
>
> - For more information about the license policy, refer to the following.
> - For more information about license error codes, refer to the following link.

Registering in an online state

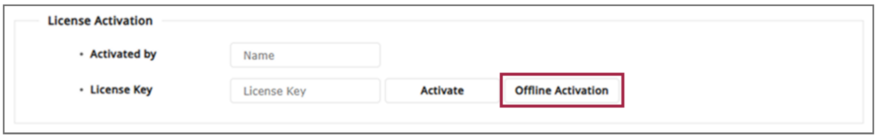
To activate the **BioStar X** license while online with an internet connection, enter your name and the received license key, then click Activate.



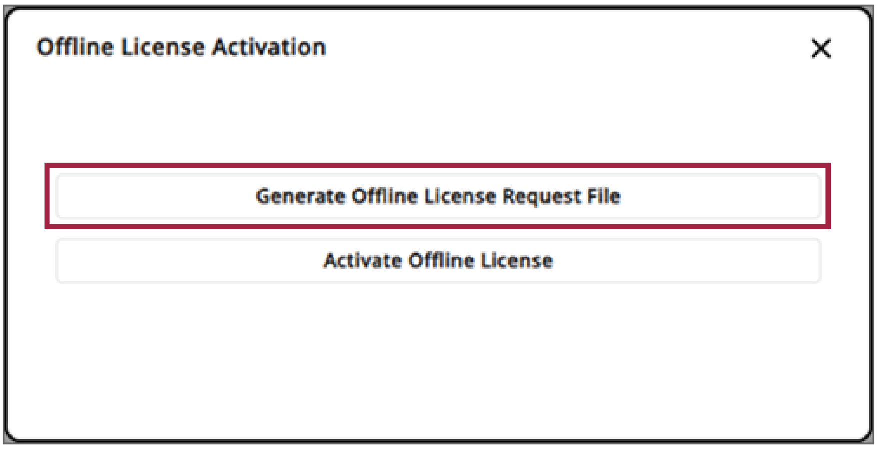
Registering in offline

To activate the **BioStar X** license in a closed network environment or in an offline state with limited internet access, please follow the instructions below.

1. In the License Activation section, click Offline Activation.

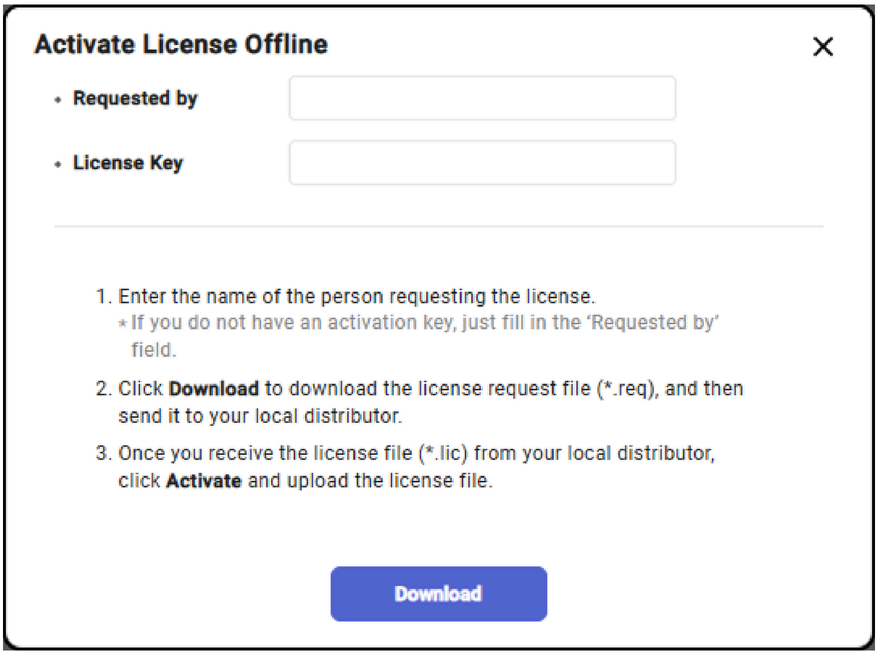


2. When the **Activate License Offline** window appears, click **Generate Offline License Request File**.



Offline License Activation
Generate Offline License Request File
Activate Offline License

3. When the dialog appears, enter **Requested by** and **License Key**.



1. Enter the name of the person requesting the license.
   * If you do not have an activation key, just fill in the 'Requested by' field.
2. Click **Download** to download the license request file (*.req), and then send it to your local distributor.
3. Once you receive the license file (*.lic) from your local distributor, click **Activate** and upload the license file.

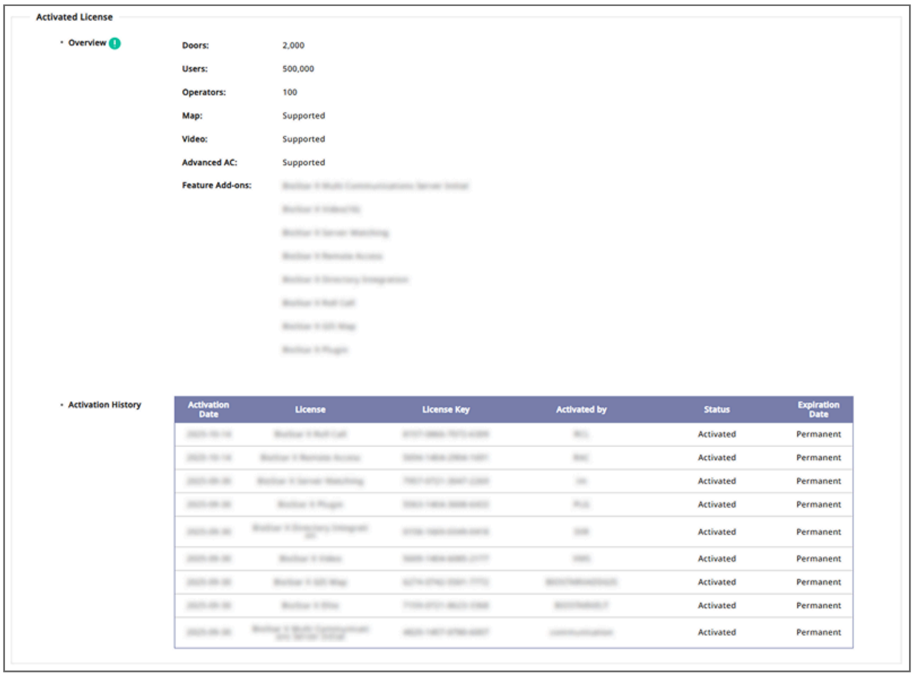
4. Click the **Download** button to download the license request file (**.req*).
5. Send it to the purchase location.

Once you receive the license file (**.lic*) from the purchase location, click the **Offline License Activation** button to upload the license file.

> **INFO**
>
> If you do not have a license key, only enter **Requested by**.

Verify activated license

You can check the information of the activated **BioStar X** license at **Activated License**.



Activated License

- Overview

Doors:	2,000
Users:	500,000
Operators:	100
Map:	Supported
Video:	Supported
Advanced AC:	Supported
Feature Add-ons:	[redacted]

- Activation History

Activation Date	License	License Key	Activated by	Status	Expiration Date
[redacted]	[redacted]	[redacted]	[redacted]	Activated	Permanent
[redacted]	[redacted]	[redacted]	[redacted]	Activated	Permanent
[redacted]	[redacted]	[redacted]	[redacted]	Activated	Permanent
[redacted]	[redacted]	[redacted]	[redacted]	Activated	Permanent
[redacted]	[redacted]	[redacted]	[redacted]	Activated	Permanent
[redacted]	[redacted]	[redacted]	[redacted]	Activated	Permanent
[redacted]	[redacted]	[redacted]	[redacted]	Activated	Permanent
[redacted]	[redacted]	[redacted]	[redacted]	Activated	Permanent
[redacted]	[redacted]	[redacted]	[redacted]	Activated	Permanent

Device License

Activate the **Device License** issued by Suprema to use specific features associated with the license.

Device License can activate the device license using **BioStar X** and a USB memory stick.

> **INFO**
>
> - Contact the place of purchase to issue a device license.
> - One feature is available per device license.
> - You can include multiple device licenses in one device license file. (Supports up to 100)
> - The device license file is an encrypted file and cannot be modified arbitrarily.
> - Device licenses are issued based on device ID. If the device ID is changed in an unusual way, the warranty service for the license is not provided.
> - For more information about license error codes, refer to the following link.

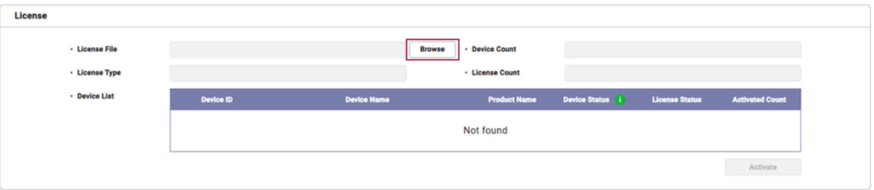
Before start

Before activating the device license, check the following.

- Prepare a valid device license file. Contact the place of purchase for the device license file.
- Ensure the target device is registered in **BioStar X**. For more information about device enrollment, refer to the following.

Apply device license

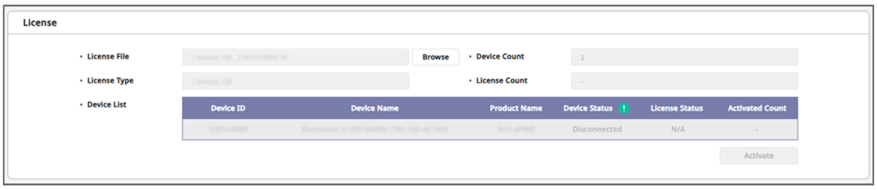
1. Click **Settings** on the **Launcher** page.
2. Click **License** → **Device License** in the left sidebar.
3. Click **Browse**.



Device ID	Device Name	Product Name	Device Status	License Status	Activated Count
Not found					

4. Load the device license file from the path where the device license is saved.

5. The information corresponding to the loaded license appears in **License Type**, **Device Count**, **Device List**.



License

- License File: [illegible] Browse
- License Type: Camera QR
- Device Count: 1
- License Count: -
- Device List

Device ID	Device Name	Product Name	Device Status	License Status	Activated Count
[illegible]	[illegible]	[illegible]	Disconnected	N/A	-

6. Check **Device List**, and to activate the device license, click the **Activate** button.

> **INFO**
>
> If license activation fails, an error message will appear. Try to activate the license again.

Device license information

When you load the device license file, the following information appears.

- **License Type**: Check the type of license included in the device license file.
  - **Camera QR**

    > Devices that can use **Camera QR** are as follows.
    >
    > - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) firmware version 1.2.0 or higher
    > - BioStation 3 (BS3-DB, BS3-APWB) firmware version 1.1.0 or higher

  - **Wireless Door Lock**

    > - Supported OSDP antenna and wireless door lock are as below:
    >   - U&Z OSDP Antenna: CX8936
    >   - U&Z Wireless Door Lock: CX217x (Handle), CX212x (Knob)
    > - You can issue a device license for up to 12 devices, equal to the number of wireless door locks you want to connect.
    > - The maximum number of wireless door locks that can be connected with a device license is 12. Even if you activate multiple device licenses, you cannot exceed 12 devices.

- **Device Count**: Check the number of devices included in the device license file.
- **License Count**: Check the number of Wireless Door Locks that can be activated with a device license.
- **Device List**: You can check detailed information of the devices included in the device license file.
  - **Device ID**: This is the unique ID that identifies the device.
  - **Device Name**: This is the name of the device.
  -

Product Name: This is the model name of the device.

- **Device Status**: This is the current status of the device. Only devices in **Normal** state can activate licenses.
  - **Normal**, **Disconnected**, **Not Supported**, **Unregistered**

  > ⓘ If the device is a model that does not support the license feature or if the firmware version is low, **Device Status** will be displayed as **Not Supported**. Check the supported models and firmware versions for that feature.

- **License Status**: This indicates whether the license is activated. Only **Not Activated** devices can activate licenses.
  - **Not Activated**, **Activated**, **N/A**
- **Activated Count**: This shows the connection status of the wireless door lock.

> **INFO**
>
> - Values for **License Count**, **Activated Count** will only appear when the wireless door lock device license is loaded.

System Settings

Guidelines for configuring major system settings of the **BioStar X** platform.

Audit Trail

You can track not only user access information but also all information changed in the system.

System Backup

You can back up key information such as the database of **BioStar X**, various settings, and keys using the system backup menu.

System Restore

This guide explains how to restore the database, settings, licenses, etc. of BioStar X to a previous state using a system backup file.

Enhance System Security

Enhance system security by configuring the password policy, personal data encryption, and communication security between devices in BioStar X.

Daylight Saving Time

You can set Daylight Saving Time (DST) to automatically adjust system time to local legal time.

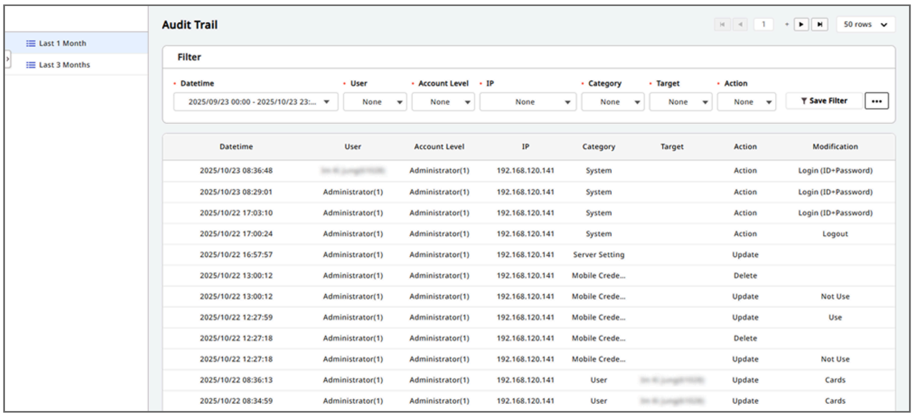
Audit Trail

The **Audit Trail** feature records and tracks all activities occurring in the system. All activities such as user login/ logout, setting changes, and system administration tasks are recorded and can be utilized for security audits and system monitoring.

- **Security audit**: Detect unauthorized access attempts or privilege abuse.
- **Troubleshooting**: Track the occurrence of system errors and setting change history.
- **Compliance**: Retain access logs and generate audit reports.

Use audit trail

1. Click **Settings** on the **Launcher** page.
2. Click **System** → **Audit Trail** on the left sidebar.
3. The audit trail list appears on the screen.



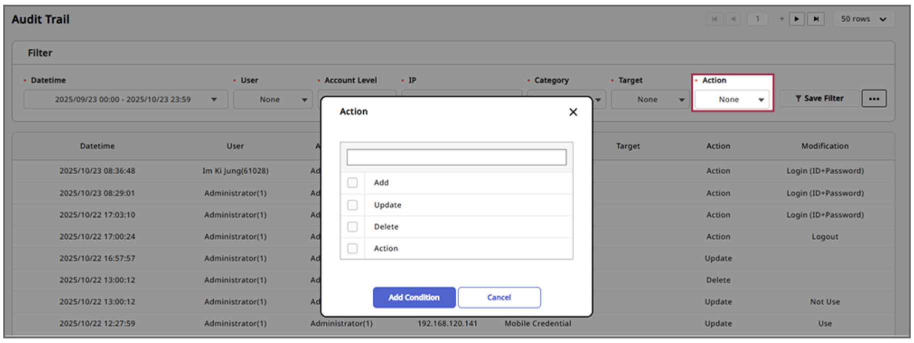
Datetime: 2025/09/23 00:00 - 2025/10/23 23:...
User: None
Account Level: None
IP: None
Category: None
Target: None
Action: None

Datetime	User	Account Level	IP	Category	Target	Action	Modification
2025/10/23 08:36:48	[redacted]	Administrator(1)	192.168.120.141	System		Action	Login (ID+Password)
2025/10/23 08:29:01	Administrator(1)	Administrator(1)	192.168.120.141	System		Action	Login (ID+Password)
2025/10/22 17:03:10	Administrator(1)	Administrator(1)	192.168.120.141	System		Action	Login (ID+Password)
2025/10/22 17:00:24	Administrator(1)	Administrator(1)	192.168.120.141	System		Action	Logout
2025/10/22 16:57:57	Administrator(1)	Administrator(1)	192.168.120.141	Server Setting		Update	
2025/10/22 13:00:12	Administrator(1)	Administrator(1)	192.168.120.141	Mobile Crede...		Delete	
2025/10/22 13:00:12	Administrator(1)	Administrator(1)	192.168.120.141	Mobile Crede...		Update	Not Use
2025/10/22 12:27:59	Administrator(1)	Administrator(1)	192.168.120.141	Mobile Crede...		Update	Use
2025/10/22 12:27:18	Administrator(1)	Administrator(1)	192.168.120.141	Mobile Crede...		Delete	
2025/10/22 12:27:18	Administrator(1)	Administrator(1)	192.168.120.141	Mobile Crede...		Update	Not Use
2025/10/22 08:36:13	Administrator(1)	Administrator(1)	192.168.120.141	User	[redacted]	Update	Cards
2025/10/22 08:34:59	Administrator(1)	Administrator(1)	192.168.120.141	User	[redacted]	Update	Cards

For more information on major tracking items, refer to the following.

Types of tracked actions

Click **Action** option in the **Filter** section to categorize audit trails by the following action types.



Datetime: 2025/09/23 00:00 - 2025/10/23 23:59
User: None
Account Level
IP
Category
Target: None
Action: None

- ☐ Add
- ☐ Update
- ☐ Delete
- ☐ Action

Datetime	User	A			Target	Action	Modification
2025/10/23 08:36:48	Im Ki Jung(61028)	Ad				Action	Login (ID+Password)
2025/10/23 08:29:01	Administrator(1)	Ad				Action	Login (ID+Password)
2025/10/22 17:03:10	Administrator(1)	Ad				Action	Login (ID+Password)
2025/10/22 17:00:24	Administrator(1)	Ad				Action	Logout
2025/10/22 16:57:57	Administrator(1)	Ad				Update	
2025/10/22 13:00:12	Administrator(1)	Ad				Delete	
2025/10/22 13:00:12	Administrator(1)	Ad				Update	Not Use
2025/10/22 12:27:59	Administrator(1)	Administrator(1)	192.168.120.141	Mobile Credential		Update	Use

- **Add**: Create new item

- **Update**: Modify existing item
- **Delete**: Remove item
- **Action**: Execute system functions (login, device control, etc.)

Classification by permission level

Audit trails can be categorized according to admin level. Click **Account Level** option in the **Filter** section to filter by the following permission levels.

- **Administrator(1)**: Access all system functions
- **User Operator(2)**: User management functions
- **Monitoring Operator(3)**: Monitoring functions
- **Video Operator(253)**: Video-related functions
- **TA Operator(254)**: Attendance management functions

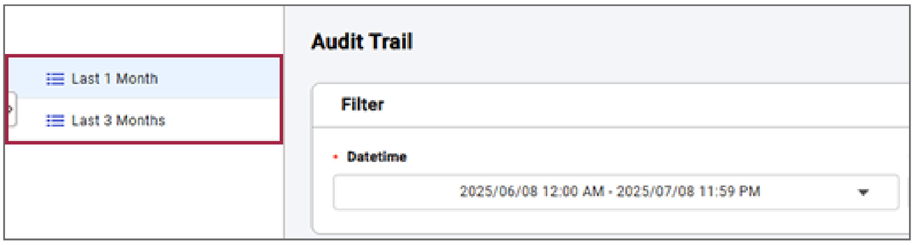
> **INFO**
>
> **Video Operator(253)** and **TA Operator(254)** permission levels are available through additional options for **Advanced** license or higher. For more information on licensing policy, refer to the following.

Period setting query

Set the period to check the audit trail history for a specific duration.

Query with predefined periods

Select **Last 1 Month** or **Last 3 Months** from the filter list on the left screen.



Audit Trail

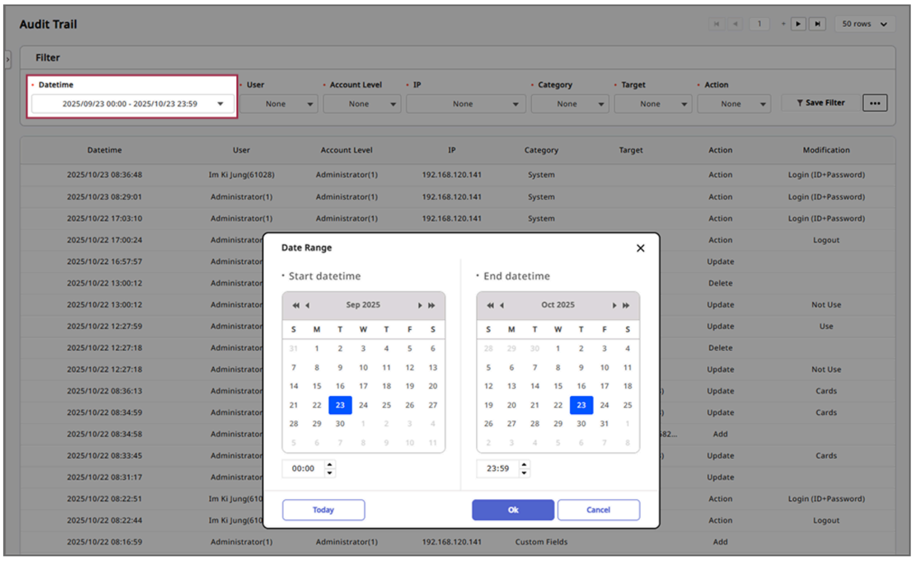
Filter

Datetime

2025/06/08 12:00 AM - 2025/07/08 11:59 PM

Query with custom periods

For detailed period settings, set the start date and end date in the **Filter** section under the **Datetime** option.



Datetime	User	Account Level	IP	Category	Target	Action
2025/09/23 00:00 - 2025/10/23 23:59	None	None	None	None	None	None

Datetime	User	Account Level	IP	Category	Target	Action	Modification
2025/10/23 08:36:48	Im Ki Jung(61028)	Administrator(1)	192.168.120.141	System		Action	Login (ID+Password)
2025/10/23 08:29:01	Administrator(1)	Administrator(1)	192.168.120.141	System		Action	Login (ID+Password)
2025/10/22 17:03:10	Administrator(1)	Administrator(1)	192.168.120.141	System		Action	Login (ID+Password)
2025/10/22 17:00:24	Administrator					Action	Logout
2025/10/22 16:57:57	Administrator					Update	
2025/10/22 13:00:12	Administrator					Delete	
2025/10/22 13:00:12	Administrator					Update	Not Use
2025/10/22 12:27:59	Administrator					Update	Use
2025/10/22 12:27:18	Administrator					Delete	
2025/10/22 12:27:18	Administrator					Update	Not Use
2025/10/22 08:36:13	Administrator				)	Update	Cards
2025/10/22 08:34:59	Administrator				)	Update	Cards
2025/10/22 08:34:58	Administrator				582...	Add	
2025/10/22 08:33:45	Administrator				)	Update	Cards
2025/10/22 08:31:17	Administrator					Update	
2025/10/22 08:22:51	Im Ki Jung(610					Action	Login (ID+Password)
2025/10/22 08:22:44	Im Ki Jung(610					Action	Logout
2025/10/22 08:16:59	Administrator(1)	Administrator(1)	192.168.120.141	Custom Fields		Add	

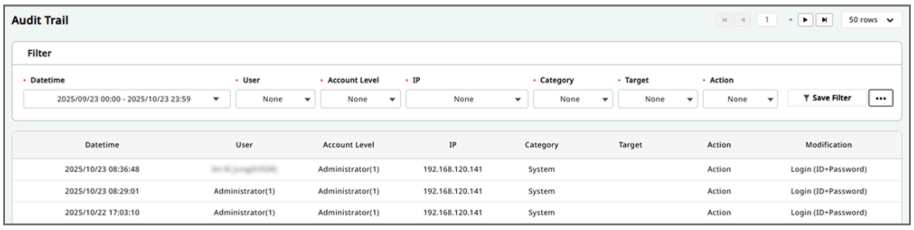
Date Range

• Start datetime: Sep 2025, 23, 00:00

• End datetime: Oct 2025, 23, 23:59

Filter settings

Filter the audit trail list efficiently using various criteria.



Datetime	User	Account Level	IP	Category	Target	Action
2025/09/23 00:00 - 2025/10/23 23:59	None	None	None	None	None	None

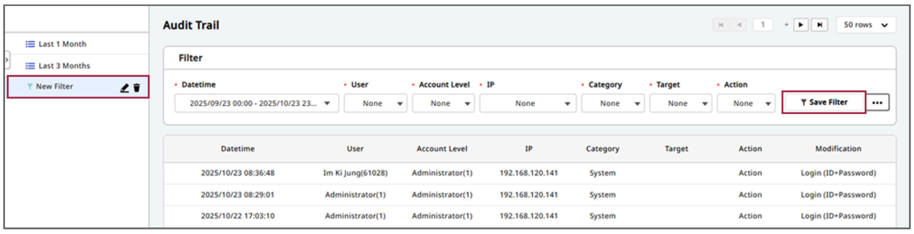
Datetime	User	Account Level	IP	Category	Target	Action	Modification
2025/10/23 08:36:48	[redacted]	Administrator(1)	192.168.120.141	System		Action	Login (ID+Password)
2025/10/23 08:29:01	Administrator(1)	Administrator(1)	192.168.120.141	System		Action	Login (ID+Password)
2025/10/22 17:03:10	Administrator(1)	Administrator(1)	192.168.120.141	System		Action	Login (ID+Password)

In the **Filter** section, you can set the following options. Filter options match the column items of the audit trail list. However, the **Modification** column cannot be filtered.

- **Datetime**: Date and time when the event occurred
- **USER**: User ID of the user who performed the event
- **Account Level**: User's permission level
- **IP**: IP address from which the user accessed
- **Category**: Menu category of the modified item
- **Target**: Modified target
- **Action**: Performed action
- **Modification**: Details during the event occurrence

Save filter

Set the filter and click the **Filter** section's **Save Filter** button to save the filter you set to the filter list on the left screen.



Datetime: 2025/09/23 00:00 - 2025/10/23 23...
User: None
Account Level: None
IP: None
Category: None
Target: None
Action: None

Datetime	User	Account Level	IP	Category	Target	Action	Modification
2025/10/23 08:36:48	Im Ki Jung(61028)	Administrator(1)	192.168.120.141	System		Action	Login (ID+Password)
2025/10/23 08:29:01	Administrator(1)	Administrator(1)	192.168.120.141	System		Action	Login (ID+Password)
2025/10/22 17:03:10	Administrator(1)	Administrator(1)	192.168.120.141	System		Action	Login (ID+Password)

- Click ✎ to edit the filter name. Enter the filter name and press Enter to change the filter name.
- Click 🗑 to delete the filter. The filter will be removed from the filter list.

Page navigation

Move between pages or set the number of items to appear on each page.

- ⏮: Go to the first page.
- ◀: Go to the previous page.
- 1 / 2: Enter the page number to navigate to and press Enter to go to that page.
- ▶: Go to the next page.
- ⏭: Go to the last page.
- 50 rows ⌄: You can select the number of items to display per page.

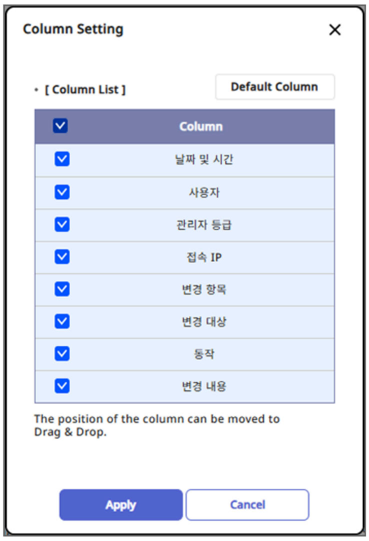
Export to CSV

Export the audit trail list to a CSV file for use with external analysis tools.

1. In the **Filter** section, set filters if needed.
2. Click ••• → **CSV Export** on the right side of the section.

> **TIP**
>
> If you have set filtering, only the filtered results will be exported to the CSV file.

Set columns



Column Setting

- [Column List]

☑	Column
☑	날짜 및 시간
☑	사용자
☑	관리자 등급
☑	접속 IP
☑	변경 항목
☑	변경 대상
☑	동작
☑	변경 내용

The position of the column can be moved to Drag & Drop.

You can change the positions of columns or hide them in the audit trail list. Click ••• → **Column Setting** on the far right of the **Filter** section.

- Uncheck the checkbox of the item you wish to hide from the column list.
- To change the order of the columns, you can drag the desired items to a new position.
- To initialize the column settings, click the **Default Column** button.

Click the **Apply** button to save the settings.

Major tracking items

All activities recorded in the audit trail are organized by category. Click each item to check the details.

System Access

- **Login**: Login (ID+Password)
- **Multi-factor login**: Login (ID+Password+Fingerprint)
- **Logout**: Logout
- **Exceeded login attempts**: Exceeded maximum login attempts

User Information

- **Basic Info**: Name, User ID, Login ID, Email, Phone
- **Authentication Information**: Password, PIN, Fingerprint Template, Face, Cards
- **Permissions and Groups**: Account Level, Access Groups, User Group, Private Auth Modes
- **User Status**: Status, Start Datetime, Expiry Datetime
- **Data Management**: CSV Import, CSV Export, Data file Import, Data file export
- **Device Integration**: Transfer To Device, Delete From Device
- **Others**: Photo, Custom Fields, 1:1 Security Level, Print
- **Management**: CSV Export Long-term Idle Users, Delete Long-term Idle Users, Face Migration, Face Import
- **Email Functions**: Sending Email Succeeded, Sending Email Failed

Access Control

- **Door Settings**: Name, Description, Door Group
- **Door Devices**: Entry Device, Exit Device, Relay, Door Sensor, Exit Button
- **Door Control**: Door Open Duration, Door Open Once, Door Open Timeout, Dual Authentication, Use Automatic Door
- **Door Actions**: Lock, Unlock, Release, Open, Clear Alarm, Clear APB, Clear APB, Clear Timed APB
- **Access Groups**: Name, Description, Access Levels, User Groups, Users
- **Access Levels**: Name, Description, Access Level
- **Elevator Settings**: Name, Description, Elevator Group, Floors, Open Time
- **Elevator Devices**: Controller, Reader, Module, Tamper
- **Elevator Control**: Dual Authentication, Trigger & Action
- **Elevator Actions**: Lock, Unlock, Release, Open, Clear Alarm, Clear APB
- **Floor Levels**: Name, Description, ID, Floor Level

Device Management

- **Device Basic Settings**: Name, Device Group, Time Zone
- **Authentication Settings**: Authentication, Fingerprint, Face, Card
- **Interface Settings**: Display, Image Log, Image Log
- **Communication Settings**: TCP/IP, Device to Server Connection, RS485, WLan, Wiegand, Wiegand IO, USB, VOIP
- **Function Settings**: System, TNA, Trigger & Action, Camera Frequency
- **User Management**: Manage Users
- **Device Control**: Connect, Disconnect, Sync Device, Delete Data & Sync Device, Discover Wiegand Device
- **System Management**: Factory Default, Reboot, Firmware Upgrade, Time Sync with Server, Send License File
- **Device Status**: Locked, Clear Alarm, Delete

Advanced Access Control

- **Advanced Access Control Basic Settings**: Name, Description, Zone Type, Active/Inactive, Mode
- **Anti-passback**: APB, Clear APB, Clear APB
- **Fire Alarm**: Fire Alarm
- **Schedule Control**: Scheduled Lock, Scheduled UnLock
- **Occupancy Management**: Count +1, Count -1, Count Modified
- **Advanced Access Control Actions**: Lock, Unlock, Release, Open, Clear Alarm

System Settings

- **Server Settings**: BioStar X IP Address, BioStar X Port, Web Server Protocol, Session Timeout
- **Security Settings**: Secure communication with device, Password Level, Server Matching
- **Sync Settings**: Log Upload, Automatic User Synchronization
- **Device Settings**: Enrollment Device, Fingerprint Template Format, Mobile Card Enrollment, Use User Photo
- **Licenses**: License
- **Default settings**: Language, Date Format, Time Format, Time Zone
- **Schedule settings**: Name, Description, ID, Schedule, Holiday, Start Date, Type, Cycle
- **Holiday settings**: Name, Description, Holiday
- **Alert settings**: On, Off
- **Image log settings**: Preset, Delete Option
- **Mobile credentials**: Use, Not Use

Advanced security settings

- **Smart card - DESFire**: DESFire App ID, DESFire File ID, DESFire Encryption Type, DESFire Primary Key, DESFire Secondary Key
- **Smart card - iClass**: iClass Primary Key, iClass Secondary Key, iClass Start Block Index
- **Smart card - MIFARE**: MIFARE Primary Key, MIFARE Secondary Key, MIFARE Start Block Index, Use MIFARE Primary Key, Use MIFARE Secondary Key
- **Smart card - Mobile**: Mobile Primary Key, Mobile Secondary Key
- **Smart card - Standard**: Name, Number of Template, Template Size, Use Secondary Key
- **Wiegand settings**: Name, Description, ID, Total Bits, ID Fields, Parity Bits, Parity Position, Parity Type, Facility Code
- **Trigger conditions and actions**: Name, Trigger, Action, Schedule
- **Custom permissions**: Name, Description, ID, Operator, Permission
- **Custom fields**: Name, ID
- **Signal settings**: Name, Delay, Count, On, Off

Data management

- **System backup**: System Backup
- **Video management**: Camera, Rule
- **Visitor management**: Visitor, Visitor Setting
- **Port management**: Port
- **Daylight saving time**: Daylight Saving Time
- **Custom interface**: Custom Interface

System Backup

You can back up key information such as the database of **BioStar X**, various settings, and keys. Use the **System Backup** feature to prevent data loss on the server or when transferring to a new PC.

The supported backup methods are as follows.

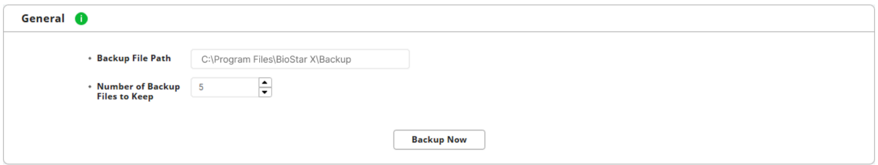
- **Manual Backup**: The user manually creates the backup file.
- **Automatic Backup**: The system automatically creates backup files at predefined intervals.

> **INFO**
>
> - When restoring **BioStar X** from a backup file created on a previous PC to a new PC, you need to reissue the license.
> - If the SQL Server database and **BioStar X** are installed on different servers, you cannot use **BioStar X** system backup and restore.
> - For more information on system restore, refer to the following.

Manual backup

Users can create backup files manually.

1. Click **Settings** on the **Launcher** page.
2. Click **System** → **System Backup** on the left sidebar of the screen.
3. In the **General** section, set the path to save the backup file and the maximum number of backup files.



General

- Backup File Path: C:\Program Files\BioStar X\Backup
- Number of Backup Files to Keep: 5

   - **Backup File Path**: Enter the path to save the backup file. Enter a directory path that has already been created for the save path.
   - **Number of Backup Files to Keep**: Set the maximum number of backup files.

4. To create a backup file, click the **Backup Now** button.

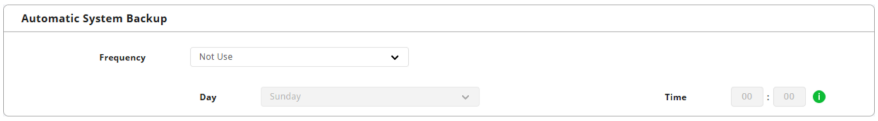
Backup files are saved in *zip* format at the path specified in the **Backup File Path** option. The file name is generated in the format `BioStar_X_Backup_YYYYMMDD_HHMMSS.zip`. Here, `YYYYMMDD` represents the backup date, and `HHMMSS` represents the backup time.

> **INFO**
>
> - If the maximum number of backups are exceeded, the oldest backup files are automatically deleted.
> - **Number of Backup Files to Keep**, only numbers between 1 and 100 are entered.

Automatic backup settings

When you set automatic backup, the system creates backup files at predefined intervals.

1. Click **Settings** on the **Launcher** page.
2. Click **System** → **System Backup** on the left sidebar of the screen.
3. In the **Automatic System Backup** section, select the **Frequency** option.



Automatic System Backup

Frequency: Not Use

Day: Sunday

Time: 00 : 00

   - **Daily**: Automatically backs up daily. Set the backup time in the **Time** option.
   - **Weekly**: Automatically backs up weekly. Set the day to automatically back up in the **Day** option, and set the backup time in the **Time** option.
   - **Monthly**: Automatically backs up monthly. Set the date for automatic backup in the **Date** option, and set the backup time in the **Time** option.

4. Click **Apply** to save the settings.

Backup files are saved in *zip* format at the path specified in the **General** section's **Backup File Path** option. The file name is generated in the format `BioStar_X_Backup_YYYYMMDD_HHMMSS.zip`. Here, `YYYYMMDD` represents the backup date, and `HHMMSS` represents the backup time.

> **INFO**
>
> - If you select the automatic backup frequency as **Monthly** and set the date to 29, 30, or 31, automatic backups will not occur in months without that date.
> - The time is based on the standard time zone set in **Preferences**. For more information on setting the time zone, refer to the following.

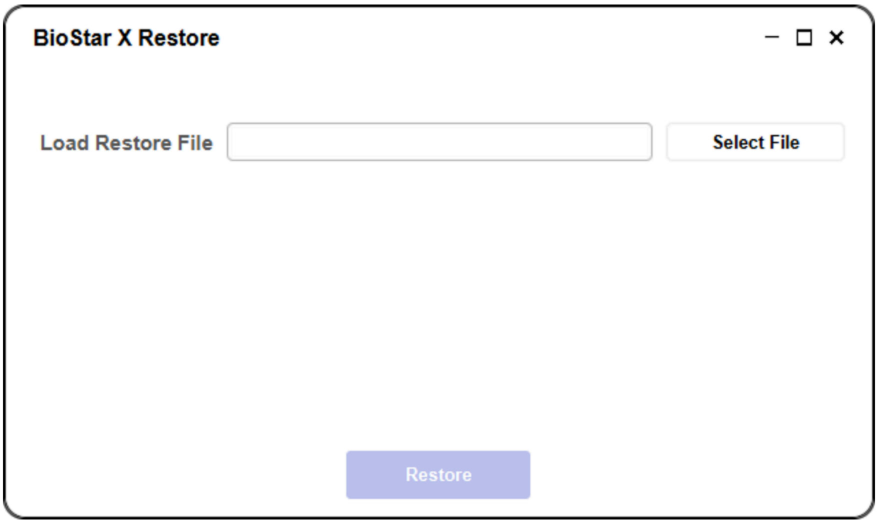
System Restore

You can restore using a system backup file when there is an issue with **BioStar X** or you need to revert to a previous state. The restore feature enables you to return the database, various settings, and license information to the state at the time of backup.

> ⚠ **CAUTION**
>
> - Proceeding with the restore operation returns the current data to the backup point. It is recommended to create a backup of the current state before restoring. To create a backup of the current state, refer to the following.
> - If the server IP address of the restore target differs from the backup server IP address during the restore operation, the restore process may fail. Verify the server IP address before proceeding with the restore operation.

> ⓘ **INFO**
>
> If the SQL Server database and **BioStar X** are installed on different servers, you cannot use **BioStar X** system backup and restore.

1. In Windows, run **Start** ⊞ → **BioStar X** → **BioStar X Restore**.
   - Program path: *C:\Program Files\BioStar X\biostar-restore.exe*
2. Click the **Select File** button and choose the backup file to restore.

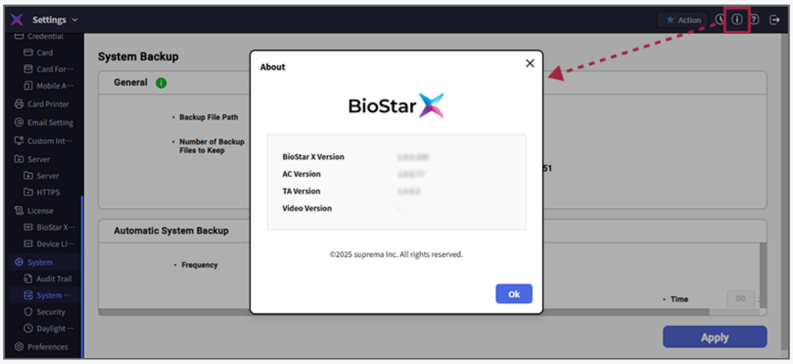


3. To start the restoration, click the **Restore** button.

When the message **Starting Biostar services...Done** appears, the restoration is complete. Access **BioStar X** to verify the restored data.

ⓘ **INFO**

- Restoration cannot proceed if the version of **BioStar X** at the time of the backup is different from the current version. To check the version of **BioStar X**, click the ⓘ button at the top right of the screen.



About

BioStar X Version

AC Version

TA Version

Video Version

©2025 suprema Inc. All rights reserved.

- To check the version of **BioStar X** at the time of the backup, extract the backup file and check the `biostarVersion` value in the *sysbackup.conf* file.

Enhance System Security

Configure the security settings of **BioStar X** according to your organization's security policy. You can selectively set password policy, personal data encryption, communication security between devices, and concurrent access control.

> **INFO**
>
> Check your organization's security policy and regulations before enhancing system security.

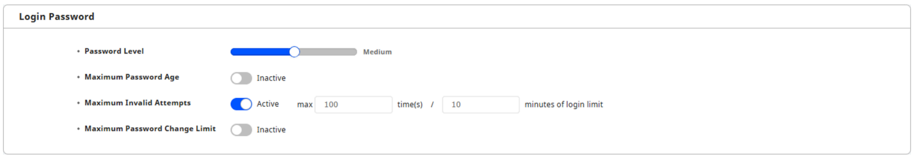
Use system security

1. Click **Settings** on the **Launcher** page.
2. Click **System** → **Security** on the left sidebar.
3. Set each item related to security.
   - **Login Password**: Set the security level related to login password. For more information, refer to the following section.
   - **Advanced Security Settings**: Enhance communication security between personal information and devices. For more information, refer to the following section.
   - **Session Security**: Enhance session security. For more information, refer to the following section.
4. Click **Apply** at the bottom right of the screen to save your settings.

> **INFO**
>
> Only the first administrator account with ID **1** can use the **Advanced Security Settings** menu.

Set password policy

The **Login Password** section sets the security level related to the login password. Set the password policy according to your organization's security requirements.



Login Password

- Password Level: Medium
- Maximum Password Age: Inactive
- Maximum Invalid Attempts: Active max 100 time(s) / 10 minutes of login limit
- Maximum Password Change Limit: Inactive

Set password complexity

You can set the complexity of user passwords. Adjust the slider for the **Password Level** option to set the security level.

- **Low**: You can enter up to 32 characters.

- **Medium**: When setting a password, a combination of 8 to 32 alphabetic characters (uppercase or lowercase) and numbers is required.
- **Strong**: When setting a password, a combination of 10 to 32 alphabetic characters (uppercase and lowercase, including at least one uppercase letter), numbers, and special characters is required.

Set password change cycle

To limit the usage period of passwords, toggle the button in the **Maximum Password Age** option to **Active** state. Users must change their password periodically as set. If the password change cycle is exceeded, a password change request message will appear during login.

> **INFO**
>
> It can be set from 1 to 180 days.

Set login failure limit

You can set the number of allowed password input failures and the login restriction time. If you exceed the number of attempts set in the **Maximum Invalid Attempts** option, you cannot log in for a limited time after incorrectly entering the password.

> **INFO**
>
> This option is activated by default, and login is restricted for 10 minutes after 100 failures. You can adjust the values or disable them as needed.

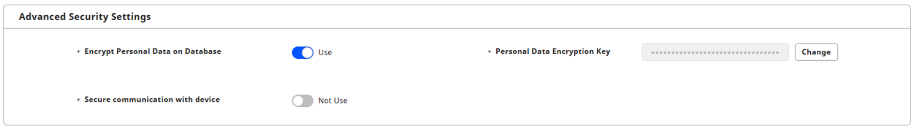
Set password change limit

To limit the number of password changes a user can make in a day, toggle the button in the **Maximum Password Change Limit** option to **Active** state. Users can change the password up to the specified number of times.

> **INFO**
>
> It can be set to a maximum of 10 times.

Advanced security settings

In the **Advanced Security Settings** section, you can enhance personal information and communication security between devices.



Advanced Security Settings

- Encrypt Personal Data on Database: Use
- Personal Data Encryption Key: ••••••••••••••••••••••••••••••••
- Secure communication with device: Not Use

Enhance personal data protection

To minimize the risk of data breaches, set the options below to encrypt sensitive personal information.

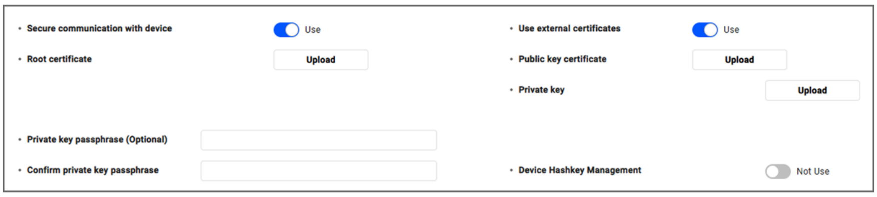
- **Encrypt Personal Data on Database**
  - **Use**: Encrypt and store user personal data, including credential data.
  - **Not Use**: Store user personal information without encryption. Data that is already encrypted will be stored decrypted, and new data will not be encrypted.
- **Personal Data Encryption Key**: Used to encrypt or decrypt information stored in the database to securely protect user personal information. Click the **Change** button and set a new encryption key value. Changing the encryption key re-encrypts the data that was previously encrypted.

> ⓘ **INFO**
>
> - Do not forcefully start the server during the personal data DB encryption or decryption process. Errors such as login failure or data corruption may occur. It may take some time depending on the size of the database and the performance of the server.
>
>   View personal data encryption items
>
>   - Profile image
>   - User ID
>   - Name
>   - Phone number
>   - User IP
>   - Email information for sender ans recipients
>   - Login ID
>   - Login password
>   - Face template
>   - Fingerprint template
>   - Card ID
>   - Smart card layout key
>   - Custom information for user and visitor
>   - Image log files
> - **Personal Data Encryption Key** can be entered using alphanumeric characters and symbols for a total of 32 characters.

Set communication security between devices

Set up secure communication between the **BioStar X** server and access control devices.

- **Secure communication with device**: Communication between the **BioStar X** server and access control devices can be protected with certificates. If you set this option to **Use**, the server automatically generates a certificate to send to the devices, and all communication is encrypted thereafter. Devices can use this certificate to establish a secure channel when exchanging data with the **BioStar X** server.
  To use external certificates, enable the **Use external certificates** option and upload the root certificate, public key certificate, and private key file.



- Secure communication with device: Use
- Root certificate: Upload
- Private key passphrase (Optional)
- Confirm private key passphrase
- Use external certificates: Use
- Public key certificate: Upload
- Private key: Upload
- Device Hashkey Management: Not Use

- **Device Hashkey Management**: You can redefine the data encryption key and administrator password.

INFO

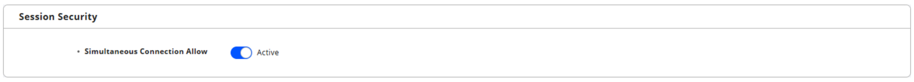
- **BioStar X** generates or deletes certificates according to the configuration status of device and secure communication settings, and does not recreate the same certificate as before. For example, if the setting of Secure communication with device is changed in the order of **Use** → **Not Use**, the created certificate will be deleted automatically. When the setting is changed in the order of **Use** → **Not Use** → **Use**, the operation of **Create A certificate** → **Delete A certificate** → **Create B certificate** is carried out.
- If you set the **Secure communication with device** option to **Not Use** while the device is physically separated from the network, the certificate stored in the device will be deleted. In this case, the device cannot be reconnected. To connect it again, the certificate saved in the device must be deleted or the device must be reset to factory default. For more information, refer to the manual of the device.

View supported devices and firmware versions for **Secure communication with device** feature

- FaceStation 2 FW 1.1.0 or later
- BioStation A2 FW 1.5.0 or later
- BioStation 2 FW 1.6.0 or later
- BioStation L2 FW 1.3.0 or later
- BioLite N2 firmware 1.0.0 or higher
- BioEntry P2 FW 1.1.0 or later
- BioEntry W2 FW 1.2.0 or later
- FaceLite firmware 1.0.0 or higher
- XPass 2 firmware 1.0.0 or higher
- CoreStation FW 1.1.0 or later
- X-Station 2 firmware 1.0.0 or higher
- BioStation 3 firmware 1.0.0 or higher

Concurrent access control

In the **Session Security** section, you can limit duplicate logins for the same account to enhance security. Set the **Simultaneous Connection Allow** option to **Inactive**. When there are concurrent login attempts for the same account, existing users logged in will be logged out.



Session Security

- Simultaneous Connection Allow ● Active

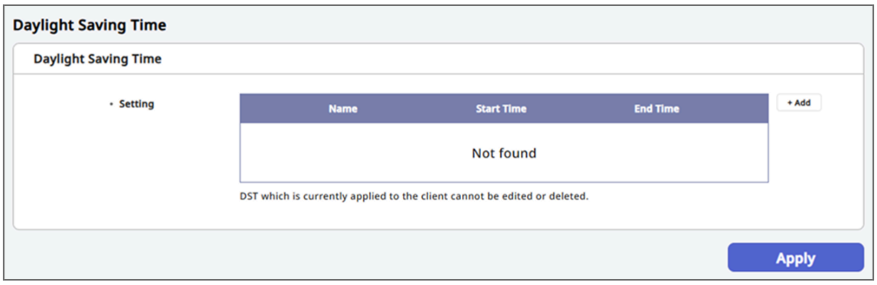
Daylight Saving Time

Set Daylight Saving Time (DST) to automatically adjust system time to local legal time. This ensures the accuracy of access logs and prevents time synchronization issues with other systems.

> **INFO**
>
> Set Daylight Saving Time in the following cases.
>
> - If you operate the system in countries or regions that adopt Daylight Saving Time
> - If you need to record accurate access times integrated with attendance management systems
> - If you manage a consolidated security system operating across multiple time zones

Add daylight saving time

1. Click **Settings** on the **Launcher** page.
2. Click **System** → **Daylight Saving Time** on the left sidebar.
3. Click **+ Add**.



Daylight Saving Time

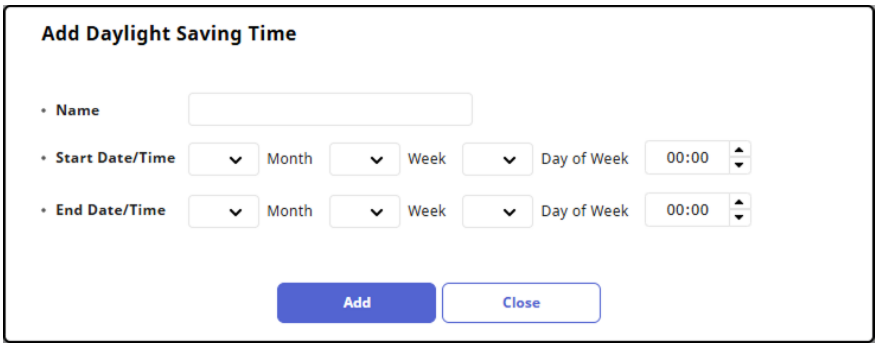
Daylight Saving Time

• Setting

Name	Start Time	End Time
Not found		

DST which is currently applied to the client cannot be edited or deleted.

4. Set each item and click **Add**.



Add Daylight Saving Time

• Name

• Start Date/Time Month Week Day of Week 00:00

• End Date/Time Month Week Day of Week 00:00

5. Click **Apply** at the bottom right of the screen to save the added settings.

INFO

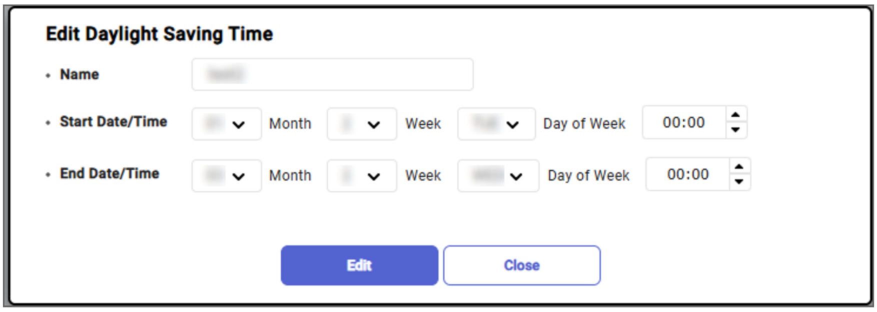
- The current Daylight Saving Time settings cannot be modified or deleted. You can check the current Daylight Saving Time settings in **Settings** → **Preference** menu.
- For more information on applying the added Daylight Saving Time settings to the system, refer to the following.

Edit daylight saving time

INFO

The currently used settings cannot be modified. To modify, first uncheck the selection in **Settings** → **Preference** menu under **Language / Time Zone** section.

1. Click **Settings** on the **Launcher** page.
2. Click **System** → **Daylight Saving Time** on the left sidebar.
3. Click the ✎ button for the item you want to modify from the Daylight Saving Time list.
4. When the **Edit Daylight Saving Time** window appears, modify the desired item.



Edit Daylight Saving Time

- Name
- Start Date/Time: Month, Week, Day of Week, 00:00
- End Date/Time: Month, Week, Day of Week, 00:00

5. When you finish editing, click **Edit**.
6. Click **Apply** at the bottom right of the screen to save the modified settings.

INFO

For more information on applying Daylight Saving Time settings to the system, refer to the following.

Delete daylight saving time

Delete the unused Daylight Saving Time settings.

1. Click **Settings** on the **Launcher** page.
2. Click **System** → **Daylight Saving Time** on the left sidebar.
3. Click the 🗑 button for the item you want to delete from the Daylight Saving Time list.

4. When the confirmation message appears, click **Yes**.
5. Click **Apply** at the bottom right of the screen to save the deleted settings.

Configure Settings

To effectively use **BioStar X**, the appropriate settings for your usage environment are necessary. Below are the required settings for various situations.

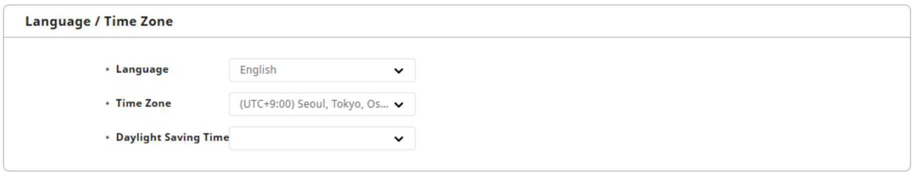
- Initial settings for the newly installed **BioStar X**
- Change to the preferred language
- Set time according to local time zone
- Customize event notification sound

Access default settings

1. Click **Settings** on the **Launcher** page.
2. Click **Preferences** in the left sidebar.
3. Set desired options in each section.
   - **Language / Time Zone**: Interface language and time zone, daylight saving time
   - **Date/Time**: Date and time format
   - **Sound**: Event notification sound
4. After completing all settings, click **Apply** at the bottom right of the screen.

Set language and standard time zone

You can set the interface language for **BioStar X**, the time zone, and daylight saving time rules.



Language / Time Zone

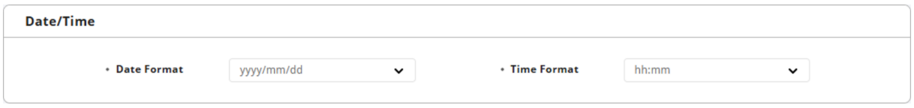
- Language: English
- Time Zone: (UTC+9:00) Seoul, Tokyo, Os...
- Daylight Saving Time:

- **Language**: Select the interface language you want to use.
- **Time Zone**: Select the time zone that corresponds to your current location.
- **Daylight Saving Time**: Choose the daylight saving time rules to apply to the **BioStar X** server. If the desired item is not available, you can refer to the following to add it.

Click **Apply** at the bottom right of the screen to save the settings.

Set date and time display format

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



Date/Time

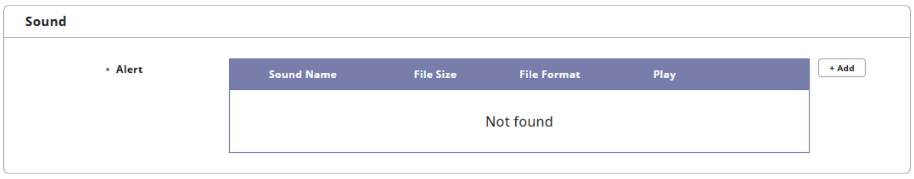
- Date Format: yyyy/mm/dd
- Time Format: hh:mm

- Date Format: You can change the date format.
  - **mm/dd/yyyy**: 01/31/2025
  - **yyyy/mm/dd**: 2025/01/31
  - **dd/mm/yyyy**: 31/01/2025
- Time Format: You can change the time format.
  - **hh:mm**: 23:59, 24-hour format
  - **hh:mm a**: 11:59 PM, 12-hour format
  - **a hh:mm**: PM 11:59, 12-hour format

Click Apply at the bottom right of the screen to save the settings.

Set event notification sound

You can upload a sound file to be used when an event occurs.

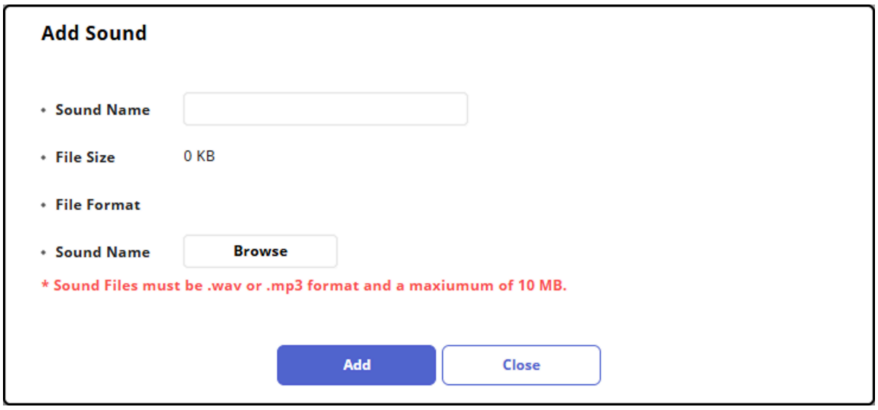


Sound

- Alert

Sound Name	File Size	File Format	Play
Not found			

1. Click + Add.
2. When the Add Sound window appears, click Browse.



Add Sound

- Sound Name
- File Size 0 KB
- File Format
- Sound Name Browse

* Sound Files must be .wav or .mp3 format and a maxiumum of 10 MB.

3. Select the *.wav* or *.mp3* file you want to upload and click **Open**.
4. Click the Add button to upload the sound file.

Click Apply at the bottom right of the screen to save the settings.

INFO

- Only *.wav* or *.mp3* file formats can be uploaded for sound files.
- A maximum file size is 10MB.
- For how to apply the uploaded sound file when an event occurs, refer to the following.

Advanced Settings

Guide for advanced settings feature available when activating a license of Advanced or higher.

Managing Elevators → 4 items

This guide describes how to group register and manage elevators.

- Manage Elevator Group
- Register Elevator
- Edit Elevator Information

↳ 4 items

Advanced Access Control Settings → 9 items

You can control access through advanced access control settings.

- Anti-passback
- Fire Alarm
- Scheduled Lock

↳ 9 items

Video Settings → 3 items

Step-by-step guidance on how to build an integrated video security management system by linking BioStar X and VMS. Covers the entire process from VMS server integration to camera settings and rule configuration.

- Integrate VMS
- Set up the camera
- Set Video Rules

↳ 3 items

Manage Map → 3 items

Guide how to set and manage floors, facilities, and areas.

- Configure Floors
- Configure Facility
- Configure Area

↳ 3 items

Set Visitor → Read more

You can configure visiting sites and PCs. You can also set the terms and conditions for visitors. And You can create the information fields that you want to know from the visitors by using the Custom Visitor Field.

Directory Integration Settings → Read more

This document provides guidance on synchronizing and managing users by integrating Microsoft Entra ID or Active Directory with BioStar X.

Set up Remote Access → Read more

This guide explains how to set up remote access via the ngrok service.

Integrate Virtual Device Event Log → Read more

This guide explains how to enroll a virtual device and log events that occur in external systems to BioStar X.

Manage Elevators

This guide describes how to group register and manage elevators. Control access rights to specific floors through access control settings related to elevators. This enhances security and convenience.

Manage Elevator Group

This guide describes how to set up groups to manage multiple elevators easily.

Register Elevator

This guide describes how to register an elevator for floor control.

Edit Elevator Information

This guide describes how to edit the setting information of the registered elevator.

Delete Elevator

This guide describes how to delete registered elevators.

Manage Elevator Group

This guide describes how to set up groups to manage multiple elevators easily. This guide describes how to configure group settings to easily manage multiple elevators. Elevator groups allow for managing several elevators as one unit.

> **TIP**
>
> Registering the group name based on elevator location makes management convenient.

Add elevator group

1. Click **Settings** on the **Launcher** page.
2. Click **Elevator** in the left sidebar.
3. Select **All Elevators** in the elevator list and right-click.
4. Click **Add Group** in the popup menu.
5. Register the desired group name.

> **INFO**
>
> - A maximum of 8 levels can be created for elevator groups.
> - The elevator group name can be up to 48 characters long.

Change elevator group name

1. Click **Settings** on the **Launcher** page.
2. Click **Elevator** in the left sidebar.
3. Select the group whose name you want to change from the elevator list and right-click.
4. Click **Rename Group** in the popup menu.
5. Enter the new group name.

> **INFO**
>
> The elevator group name can be up to 48 characters long.

Delete elevator group

1. Click **Settings** on the **Launcher** page.
2. Click **Elevator** in the left sidebar.
3. Select the group you want to delete from the elevator list and right-click.
4. Click **Delete Group** in the popup menu.

> ⚠ **CAUTION**
>
> Deleting an elevator group will remove all elevators included in the group. To avoid deleting elevators, first move them to another group before deleting the group.

Add elevator to group

Adding from the elevator list

1. Click **Settings** on the **Launcher** page.
2. Click **Elevator** in the left sidebar.
3. Select the elevator to add to the group from the elevator list and drag it to the desired group.

The selected elevator moves to the group.

Adding from elevator information

1. Click **Settings** on the **Launcher** page.
2. Click **Elevator** in the left sidebar.
3. Click the elevator to add to the group from the elevator list on the right side.
4. When the elevator information modification screen appears, click the **Group** option in the **Information** section.
5. Select the desired group.
6. Click **Apply** at the bottom of the screen.

Register Elevator

This document provides guidance on how to register and set up an elevator. The elevator is used for floor control and forms part of the access control system along with the entrance door. Registering the elevator allows control over access permissions for specific floors.

Before start

- Set the access level, access group, and floor level for access control before registering the elevator. For more information, refer to the following.
- Register the device before registering the elevator. For more information about device registration, refer to the following.
  - Register Device
  - Register Wiegand Credentials
  - Register Slave

Register elevator

1. Click **Settings** on the **Launcher** page.
2. Click **Elevator** in the left sidebar.
3. Once the **Add New Elevator** screen appears, set each section item in order.
   - **Information**: Set the basic information for the elevator. For more information, refer to the following.
   - **Detail**: Set the detailed information for the elevator. For more information, refer to the following.
   - **Option**: Set additional options. For more information, refer to the following.
   - **Alarm**: You can set the alarm to trigger or block device usage when an anti-passback violation occurs. For more information, refer to the following.
4. Once all configurations are complete, click the **Apply** button at the bottom of the screen.

Set basic information

In the **Information** section, you can enter or change the elevator's name, group, and description.

- **Name**: Enter the elevator's name. It is convenient to enter a name that specifies the elevator's location for easier management.
- **Group**: Select the elevator group.
- **Description**: Enter a brief description of the elevator.

> **INFO**
>
> - The elevator name can be up to 48 characters long.
> - For more information about registering elevator groups, refer to the following.

Set detailed information

In the **Detail** section, you can set the elevator's detailed information, such as devices connected to the elevator and floor information. Set the device and floor information to connect to the elevator.

- **Controller**: Select the device that will control access permissions for the elevator.
- **Reader**: Select the device to be used for authentication.
- **Module**: Select the device that will control the elevator button relay.
- **Total Number of Floors**: Enter the total number of floors the elevator can access. You can enter up to 192 floors.
- **Auto-mapping**: Select whether to use automatic mapping. Automatic mapping assigns relay numbers sequentially.
- **Floor Settings**: Set the floor names and relay numbers that will control the floors.

> **INFO**
>
> - Only master devices can be selected for the **Controller** option.
> - For the **Reader** option, only master devices, slave devices, and Wiegand devices can be selected, with a maximum of 4 selections allowed.
>   The OM-120 model cannot be set as a reader.
> - For the **Module** option, only the OM-120, DM-20, IM-120, and SIO2 models can be selected.

Set additional options

In the **Option** section, you can set the additional options for the elevator.

- **Relay Control**: Set options for the floor button relay.
  - **Open Time**: 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.
- **Dual Authentication**: You can set it so that two people (a general user and an administrator) must authenticate their credentials to activate the floor button.
  - **Device**: Select the device to use for dual authentication. To not use dual authentication, select **None**.
  - **Schedule**: Select the schedule for using dual authentication. If the desired schedule is not available, click **+ Add Schedule** to add one.
  - **Approval Type**: Set the order of administrator authentication.

    - **None**: Two authentications are required regardless of the authentication group.
    - **Last**: The general user must authenticate first, followed by an authenticated user included in the set authentication group.
  - **Approval Group**: Set the group to which the administrator belongs. This option can be used when **Approval Type** is set to **Last**.
  - **Timeout**: Set the waiting time between the first and second authentications. If the second authentication is not completed within the set time, the floor button will not be activated.

> **INFO**
>
> - Modify settings in the following menu to change the dual authentication of the device configured for occupancy limit settings. **Settings** → **Advanced AC** → **Occupancy Limit**
>   For more information about **Occupancy Limit** settings, refer to the following.
> - For more information about schedule settings, refer to the following.

- **Tamper**: Set the port to output the tamper signal.

Set alarms

In the **Alarm** section, you can set actions to be performed when tamper inputs or separate input signals are detected.

- **Trigger**: Set the detection of tamper inputs or separate input signals.
- **Action**: Set the actions to be performed based on the conditions set. You can activate all elevator floor buttons or output specific signals.

Edit Elevator Information

This guide describes how to edit the setting information of the registered elevator. You can change the detailed settings of individual elevators or select multiple elevators to make bulk changes to common items.

Edit a elevator info

1. Click **Settings** on the **Launcher** page.
2. Click **Elevator** in the left sidebar.
3. Click the elevator you want to edit in the elevator list.
4. Modify the details in each section.
5. Once all configurations are complete, click the **Apply** button at the bottom of the screen.

> ⓘ **INFO**
>
> For more information about each section of the elevator information edit screen, refer to the following.

Batch edit multiple elevators

1. Click **Settings** on the **Launcher** page.
2. Click **Elevator** in the left sidebar.
3. Click the checkboxes of the elevators you want to edit from the elevator list. Select two or more elevators.
4. Click **Batch Edit** at the top right of the screen.
5. When the **Batch Edit** window appears, set your desired options.
6. After completing all settings, click **Apply**.

> ⓘ **INFO**
>
> **Batch Edit** will be activated only when two or more elevators are selected from the elevator list.

Delete Elevator

This guide describes how to delete registered elevators.

1. Click **Settings** on the **Launcher** page.
2. Click **Elevator** in the left sidebar.
3. Click the checkbox of the elevator you want to delete from the elevator list.
4. Click **Delete** at the top right of the screen.

The selected elevator will be deleted. Deleted elevators cannot be recovered.

> ⓘ **INFO**
>
> **Delete** is activated only when one or more elevators are selected from the elevator list.

Advanced Access Control Settings

You can control access through advanced access control settings. You can set various advanced access control features according to security requirements and operational environments. Prevent unauthorized re-entry with anti-passback, respond to emergencies such as fires or intrusions, automatically control doors based on schedules, and restrict and monitor personnel in specific locations.

Anti-passback → Read more

Guidelines for setting up anti-passback. Anti-passback provides enhanced features compared to anti-passback generated based on doors or devices.

Fire Alarm → Read more

Guidelines on how to set up fire alarms. The fire alarm is a feature that allows you to set all access doors or elevators to open or lock when a fire occurs.

Scheduled Lock → Read more

Guidance on how to set up schedule lock. Schedule lock provides the ability to lock doors at specific times.

Scheduled Unlock → Read more

Guidelines for schedule unlock settings. Schedule unlock provides the feature of opening doors at specific times.

Intrusion Alarm → Read more

This guides you on how to set up security. The intrusion alarm feature provides capabilities to lock doors or trigger alarms when intrusion is detected.

Interlock → Read more

Guidance on how to set interlock. Interlock is a method of access control that enhances security by blocking access to other doors when one door is open among multiple doors.

Muster → Read more

This guide describes how to configure muster settings. Set the location where users will gather in case of an emergency and monitor the number of people in that specific location.

Occupancy Limit → Read more

This guide describes how to set occupancy limit settings. Monitor occupancy status and limit the maximum number of occupants in certain places.

Roll Call → Read more

This guides how to set up roll call.

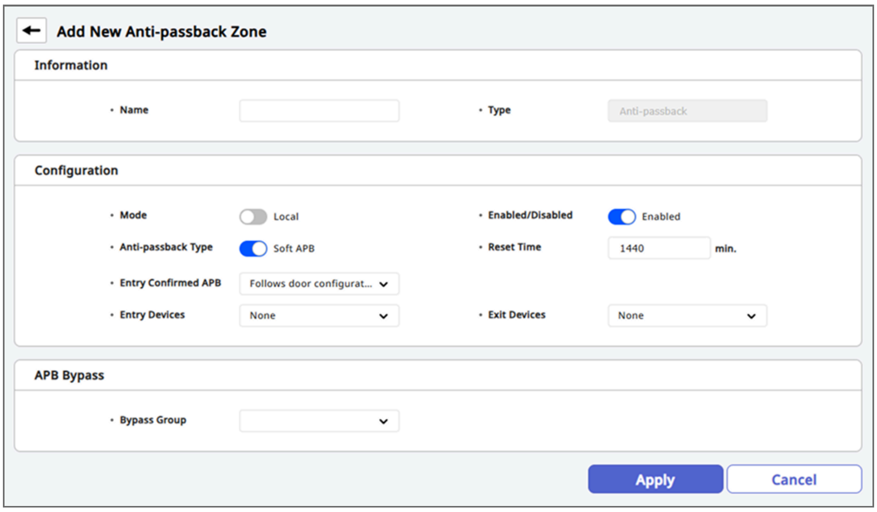
Anti-passback

Anti-passback provides enhanced features compared to anti-passback generated based on doors or devices. Set up anti-passback to force users to use designated doors and devices upon entry and exit. This prevents unauthorized re-entry and enhances security.

> **INFO**
>
> **APB (Anti-passback)**: A structural method used to control access. This function uses access control devices installed both inside and outside the door, so that authentication is required for access to the zone. In the case of card-based access control systems, if a person enters a zone following the person in front without swiping their card on the reader, the door does not open when the person attempts to leave the zone, and subsequently an anti-passback event occurs. Anti-passback is categorized into hard APB and soft APB. If the anti-passback is violated, the anti-passback event is created immediately and hard APB does not permit access to the user while soft APB still permits access to the user.

Register anti-passback

1. Click **Settings** on the **Launcher** page.
2. Click **Advanced AC** in the left sidebar.
3. Click **ADD ADVANCED AC**.
4. Select **Anti-passback** and click **Apply**.
5. Enter the name of the additional anti-passback feature in the **Info** section.



Add New Anti-passback Zone

Information

- Name:
- Type: Anti-passback

Configuration

- Mode: Local
- Enabled/Disabled: Enabled
- Anti-passback Type: Soft APB
- Reset Time: 1440 min.
- Entry Confirmed APB: Follows door configurat...
- Entry Devices: None
- Exit Devices: None

APB Bypass

- Bypass Group:

6. Set the details of the anti-passback feature in the **Settings** section. For more information, refer to the following.
7. Set the actions to perform when an anti-passback violation occurs in the **Alarm** section.
8. Select the entry groups that can bypass anti-passback in the **APB Bypass** section. Users belonging to this group can bypass anti-passback.
9. After completing all settings, click **Apply** at the bottom of the screen.

ⓘ **INFO**

The Alarm section can only be used after configuring both Entry Devices and Exit Devices.

Setting options guide

The details for anti-passback settings are as follows.

- Mode: Set the application range.
  - Local: Can be set with entry devices connected via RS-485.
  - Global: Can be set to all devices registered in **BioStar X**.
- Enabled/Disabled: You can activate or temporarily deactivate the settings.
- Anti-passback Type: Select the type of anti-passback.
  - Hard APB: Creates anti-passback events and cannot enter.
  - Soft APB: Creates anti-passback events and can enter.
- Reset Time: Set the waiting time until re-entry is allowed after a user violates anti-passback rules. After the specified time has passed following an alarm, the user's access is automatically allowed.
  - Can be set within the range of **1** minute to **10080** minutes (7 days).
  - Setting to **0** minutes will prevent the alarm from clearing automatically until the administrator clears it manually.
- Entry Confirmed APB: Set the scope in which anti-passback rules apply.
  - ON: Anti-passback rules apply according to the actual operation of the entry and exit devices.
  - OFF: Rules apply based on user authentication regardless of the door's operation.
  - Follows door configuration: When using APB based on entry for the corresponding door, the anti-passback rules apply according to the sensor usage option setting.
- Entry Devices: Select the device to be used when entering. You can choose from the list of registered devices.
- Exit Devices: Select the device to be used when exiting. You can choose from the list of registered devices.
- Network Failure Action: Set the door action when communication with devices configured with anti-passback in **BioStar X** is interrupted. This feature is available when the Mode option is set to Global.
  - Open by auth: The door opens when the user is authenticated normally.
  - Open by auth & record APB log: An anti-passback violation alarm occurs and the door opens.
  - Door locked & record APB log: An anti-passback violation alarm occurs and the door does not open.

INFO

For more information about device registration, refer to the following.

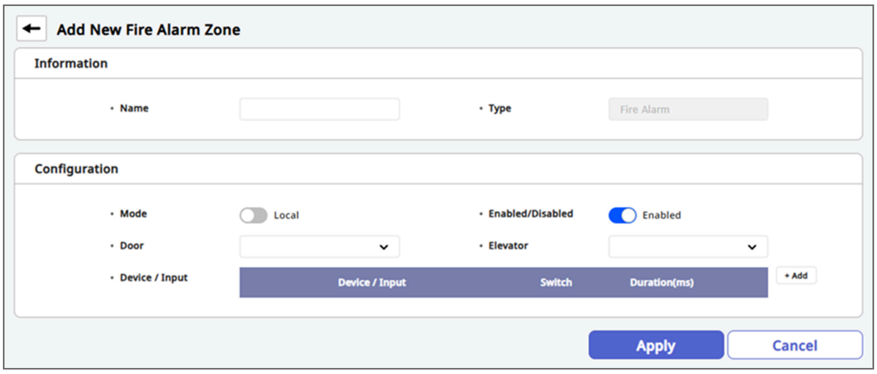
- Register Device
- Register Wiegand Credentials
- Register Slave

Fire Alarm

Guidelines on how to set up fire alarms. The fire alarm is a feature that allows you to set all access doors or elevators to open or lock when a fire occurs.

Register fire alarm

1. Click **Settings** on the **Launcher** page.
2. Click **Advanced AC** in the left sidebar.
3. Click **ADD ADVANCED AC**.
4. Select **Fire Alarm** and click **Apply**.
5. Enter the name of the fire alarm to add in the **Info** section.



Add New Fire Alarm Zone

Information

- Name
- Type: Fire Alarm

Configuration

- Mode: Local
- Enabled/Disabled: Enabled
- Door
- Elevator
- Device / Input

Device / Input	Switch	Duration(ms)

6. Set the details of the fire alarm in the **Settings** section. For more information, refer to the following.
7. Set the actions to be performed when a fire alarm occurs in the **Alarm** section.
8. After completing all settings, click **Apply** at the bottom of the screen.

> **INFO**
>
> The **Alarm** section must set **Door** to be usable.

Setting options guide

The details for setting the fire alarm are as follows.

- **Mode**: Set the application range.
  - **Local**: Can only be set to devices connected via RS-485 with entering devices.
  - **Global**: Can be set to all devices registered in **BioStar X**.
- **Enabled/Disabled**: You can activate or temporarily deactivate the settings.

- Select the access door to designate the fire alarm rules in **Door**.
- Select the elevator to designate the fire alarm rules in **Elevator**.
- Click **+ Add** and set the devices to trigger fire alarm signals with **Device / Input**.

INFO

- Setting the **Mode** option to **Local** allows you to set the fire alarm function on only one access door or elevator.
- Setting the **Mode** option to **Global** allows you to set the fire alarm function on both access doors and elevators simultaneously.
- For more information about device registration, refer to the following.
  - Register Device
  - Register Wiegand Credentials
  - Register Slave

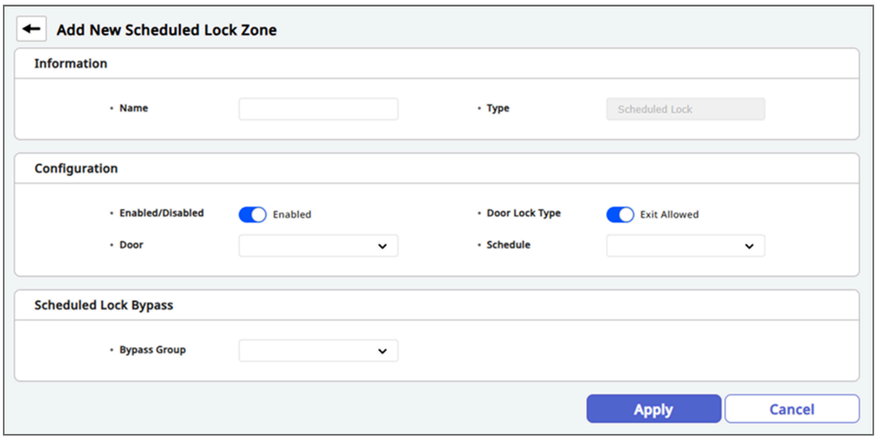
Scheduled Lock

Guidance on how to set up schedule lock. Schedule lock provides the ability to lock doors at specific times. This feature enhances access control and is useful for restricting access during certain periods.

> **INFO**
>
> Schedule lock settings only support **Local** mode.

Register scheduled lock

1. Click **Settings** on the **Launcher** page.
2. Click **Advanced AC** in the left sidebar.
3. Click **ADD ADVANCED AC**.
4. Select **Scheduled Lock** and click **Apply**.
5. Enter the name of the schedule lock feature to add in the **Info** section.



Add New Scheduled Lock Zone

Information

- Name
- Type: Scheduled Lock

Configuration

- Enabled/Disabled: Enabled
- Door Lock Type: Exit Allowed
- Door
- Schedule

Scheduled Lock Bypass

- Bypass Group

6. Set the details of the schedule lock feature in the **Settings** section. For more information, refer to the following.
7. Set the action to take when a schedule lock violation occurs in the **Alarm** section.
8. Select the access group that can bypass the schedule lock in the **Scheduled Lock Bypass** section. Users in this group can bypass the schedule lock.
9. After completing all settings, click **Apply** at the bottom of the screen.

> **INFO**
>
> The **Alarm** section must set **Door** to be usable.

Setting options guide

The details for setting schedule lock are as follows.

- **Enabled/Disabled**: You can activate or temporarily deactivate the settings.
- **Door Lock Type**: You can set it to lock only the entrance device or to lock both entrance and exit devices.
- **Door**: Select the doors to specify schedule lock rules.
- **Schedule**: Select a schedule. If the desired schedule is not available, click **+ Add Schedule** to add one.

> ⓘ **INFO**
>
> - You can select multiple doors to configure schedule lock functionality in **Local** mode.
> - For more information about schedule settings, refer to the following.

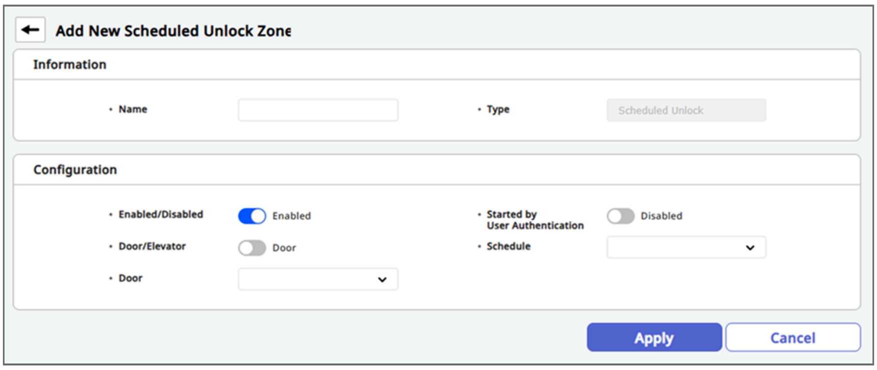
Scheduled Unlock

Guidelines for schedule unlock settings. Schedule unlock provides the feature of opening doors at specific times. This feature enhances access control and is useful for allowing access during certain time periods.

> **INFO**
>
> Schedule unlock supports only **Local** mode.

Register scheduled unlock

1. Click **Settings** on the **Launcher** page.
2. Click **Advanced AC** in the left sidebar.
3. Click **ADD ADVANCED AC**.
4. Select **Scheduled Unlock** and click **Apply**.
5. Enter the name of the schedule unlock feature to be added in the **Info** section.



Add New Scheduled Unlock Zone

Information

- Name
- Type: Scheduled Unlock

Configuration

- Enabled/Disabled: Enabled
- Started by User Authentication: Disabled
- Door/Elevator: Door
- Schedule
- Door

6. Set the details of the schedule unlock feature in the **Settings** section. For more information, refer to the following.
7. Select the access group that can start the scheduled unlock in the **Scheduled Unlock Authentication** section.
8. After completing all settings, click **Apply** at the bottom of the screen.

Setting options guide

The details for schedule unlock settings are as follows.

- **Enabled/Disabled**: You can activate or temporarily deactivate the settings.
- **Started by User Authentication**: If set to **Enabled**, the **Scheduled Unlock Authentication** section will appear. Users from the selected user group in **Access Group** must authenticate according to the specified schedule to start the schedule unlock.
- **Door/Elevator**: Select the door or elevator to which the schedule unlock feature will be applied.

- Selecting **Door** activates the list of doors. Select the door to which the schedule unlock feature will be applied. Multiple doors can be selected.
- Selecting **Elevator** activates the list of elevators. Select the elevator to which the schedule unlock feature will be applied. Multiple elevators can be selected.

> ⓘ The **Door/Elevator** option appears when an elevator is registered. If no elevators are registered, only the **Door** option will appear. For more information about elevator enrollment, refer to the following.

- **Schedule**: Select a schedule. If the desired schedule is not available, click **+ Add Schedule** to add one.
- **Floor**: You can select the floors for the selected elevator.

> **INFO**
>
> - In **Local** mode, you can select multiple doors to configure the schedule unlock feature.
> - If you select an elevator that is already part of another schedule unlock setting, you cannot duplicate settings on the same floor.
> - For more information about schedule settings, refer to the following.

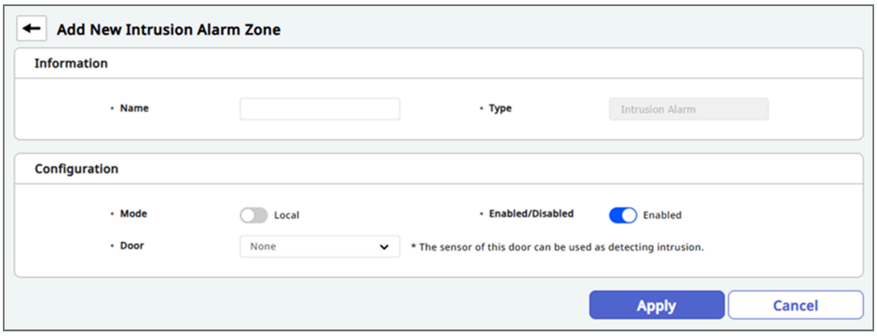
Intrusion Alarm

This guides you on how to set up security. The intrusion alarm settings provide capabilities to lock doors or trigger alarms when intrusion is detected.

> **INFO**
>
> **Intrusion Alarm Zone**: A zone set to emit a warning sound or relay signal if an unauthorized person attempts an intrusion after Arm. This zone normally begins monitoring after the day's work, and emits a preset alarm or signal when an intrusion attempt is detected.

Add intrusion alarm

1. Click **Settings** on the **Launcher** page.
2. Click **Advanced AC** in the left sidebar.
3. Click **ADD ADVANCED AC**.
4. Select **Intrusion Alarm** and click **Apply**.
5. Enter the name of the intrusion alarm setting to add in the **Info** section.



Add New Intrusion Alarm Zone

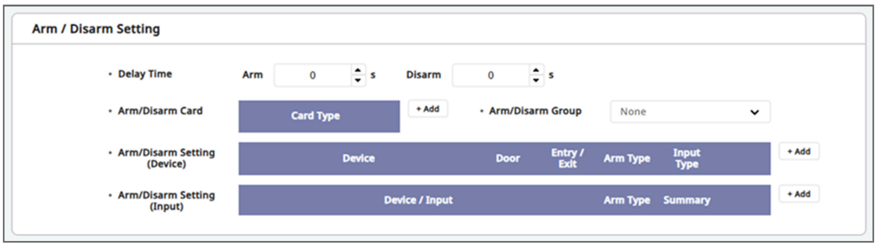
Information

- Name
- Type: Intrusion Alarm

Configuration

- Mode: Local
- Enabled/Disabled: Enabled
- Door: None
- * The sensor of this door can be used as detecting intrusion.

6. Set the details of the intrusion alarm settings in the **Settings** section. For more information, refer to the following.
7. Add authentication settings for arming and disarming in the **Arm / Disarm Setting** section. For more information, refer to the following.

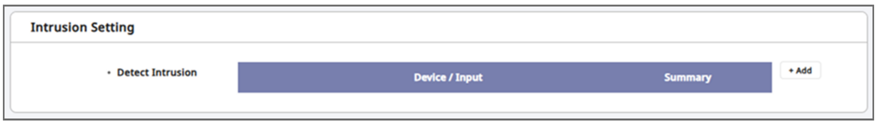


Arm / Disarm Setting

- Delay Time: Arm 0 s Disarm 0 s
- Arm/Disarm Card: Card Type
- Arm/Disarm Group: None
- Arm/Disarm Setting (Device): Device | Door | Entry / Exit | Arm Type | Input Type
- Arm/Disarm Setting (Input): Device / Input | Arm Type | Summary

> The **Arm / Disarm Setting** section appears when you select a door in the **Info** section.

8. Set up intrusion detection signals in the **Intrusion Setting** section. For more information, refer to the following.



9. Set the actions to be performed when specific events occur in the **Alarm** section.

10. After completing all settings, click **Apply** at the bottom of the screen.

> **INFO**
>
> The **Arm / Disarm Setting**, **Intrusion Setting**, and **Alarm** sections are available only if the **Door** option is set in the **Settings** section.

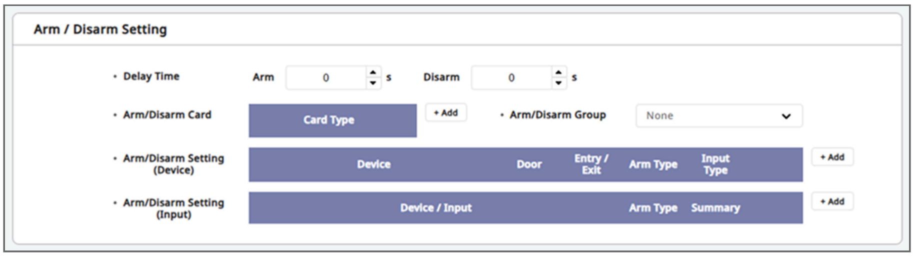
Setting options guide

The details for intrusion alarm settings are as follows.

- **Mode**: Set the application range. The intrusion alarm settings only support the **Local** mode and can only be set with devices connected via RS-485 and entry devices.
- **Enabled/Disabled**: You can activate or temporarily deactivate the settings.
- Select the door to apply the intrusion alarm function at **Door**.

Arming or disarming settings

You can add authentication settings for arming and disarming.

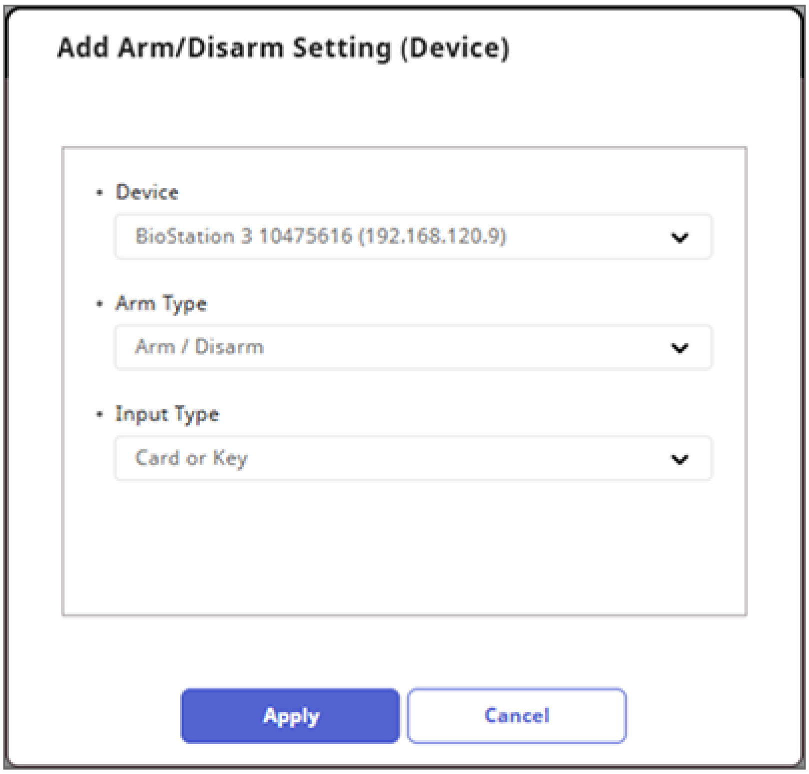


- Set the delay time until arming or disarming with **Delay Time**. This means that the arming is the delay time after authentication until the alarm starts, and the disarming is the delay time before the alarm is triggered after an intrusion is detected.
- Add cards authorized for arming or disarming with **Arm/Disarm Card**. You can register up to 128 arming/disarming cards.
- Select groups authorized for arming or disarming with **Arm/Disarm Group**. You can register up to 128 arming/disarming groups.
- Set the arming/disarming by the device or input signal with **Arm/Disarm Setting**. Click the **+ Add** button and configure each item.

Add arming/disarming by device

Click the **+ Add** button in the **Arm/Disarm Setting** (**Device**) option. Select the device to control the intrusion alarm feature and choose **Arm Type**.

Input Type can select **Card**, **Key**, or **Card or Key**. Devices without an LCD screen can only use **Card** for input type.



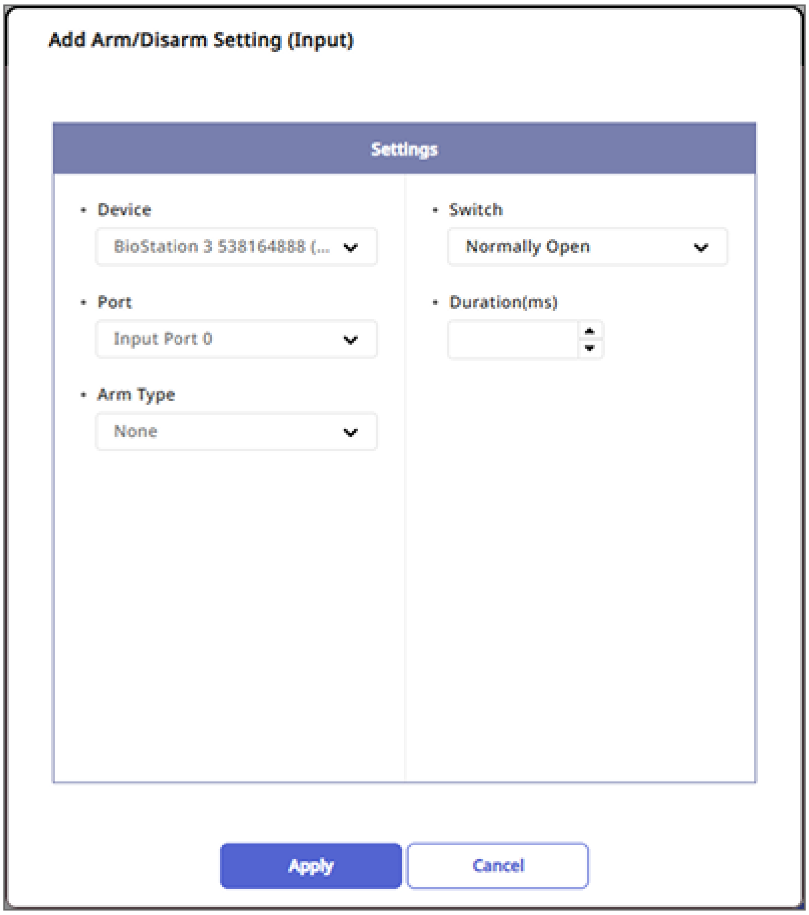
Add Arm/Disarm Setting (Device)

- Device: BioStation 3 10475616 (192.168.120.9)
- Arm Type: Arm / Disarm
- Input Type: Card or Key

Add arming/disarming by input signal

Click the **+ Add** button in the **Arm/Disarm Setting** (**Input**) option. Select the device to control the intrusion alarm feature. Click **Port** to choose the input port of the selected device.

After choosing **Arm Type**, set the type of switch and the duration of the signal.



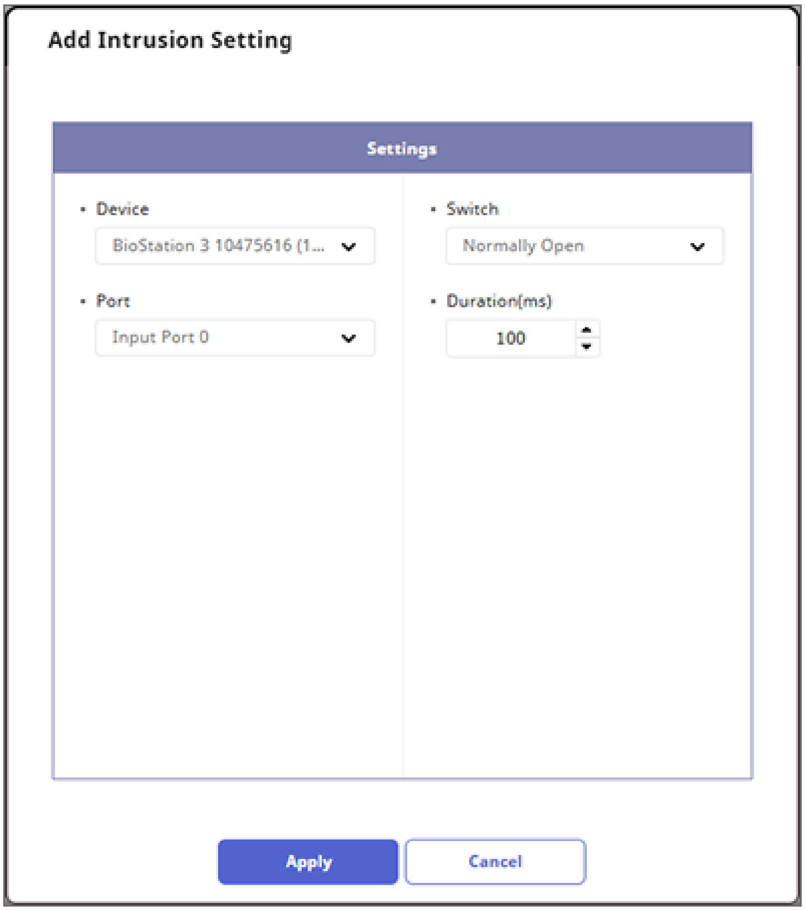
Add Arm/Disarm Setting (Input)

Settings

- Device: BioStation 3 538164888 (...
- Port: Input Port 0
- Arm Type: None
- Switch: Normally Open
- Duration(ms):

Intrusion detection settings

You can set up the intrusion detection signals. Click **+ Add** and set it as shown below to recognize an intrusion when an N/O sensor connected to input port 0 of the BioStation 3 device sends a signal for 100(ms).



Add Intrusion Setting

Settings

- Device: BioStation 3 10475616 (1...
- Port: Input Port 0
- Switch: Normally Open
- Duration(ms): 100

Interlock

Interlock is an access control method used in areas where security is important. When interlock is set up in a location with two or more doors, it operates as follows.

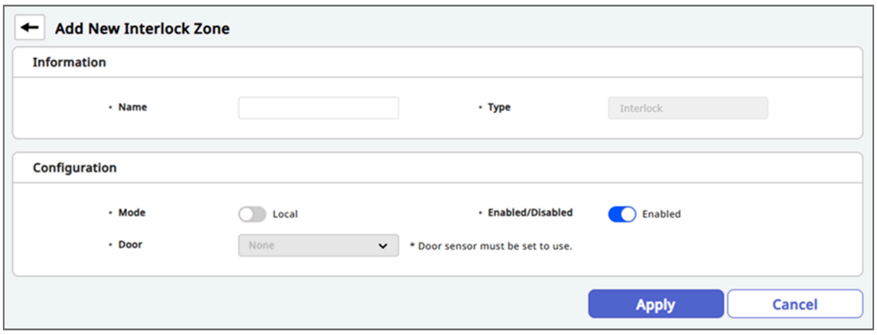
- Monitor the status of each door in real-time via door sensors and relays.
- If one door is open or unlocked, all other doors automatically enter a locked state.
- You can set it to block additional access while a user is present at the location.

This method enhances security by preventing multiple doors from being opened simultaneously.

> **INFO**
>
> - A single interlock setting can consist of up to 4 doors.
> - Only doors composed of devices connected to CoreStation can have interlock set up.
> - Devices set as interlock cannot be used in other interlock settings.
> - Doors set as interlock cannot be used in other settings, except fire alarm settings.

Interlock registration

1. Click **Settings** on the **Launcher** page.
2. Click **Advanced AC** in the left sidebar.
3. Click **ADD ADVANCED AC**.
4. Select **Interlock** and click **Apply**.
5. Enter the name of the interlock setting to be added in the **Info** section.



Add New Interlock Zone

Information

- Name:
- Type: Interlock

Configuration

- Mode: Local
- Enabled/Disabled: Enabled
- Door: None
  * Door sensor must be set to use.

6. Set the details of the interlock setting in the **Settings** section. For more information, refer to the following.
7. You can set it up so that access is not allowed when a user is present in the **Option** section.
8. In the **Alarm** section, set the actions to be performed when specific events occur in the interlock setting.

INFO

The **Option** and **Alarm** sections can only be used if **Settings** and **Door** are set in the **Settings** section.

Setting options guide

The details for interlock settings are as follows.

- **Mode**: Set the application range. Interlock settings only support **Local** mode and can only be set with devices connected to CoreStation via RS-485.
- **Enabled/Disabled**: You can activate or temporarily deactivate the settings.
- **Door**: Select the door to be designated as an interlock. You must select at least 2 or more doors, and only doors with connected door sensors can be added.

Muster

The muster is a necessary setting for effective personnel management and safety assurance during emergencies. This feature allows administrators to designate a specific location as a gathering point to predefine where users will gather during emergencies.

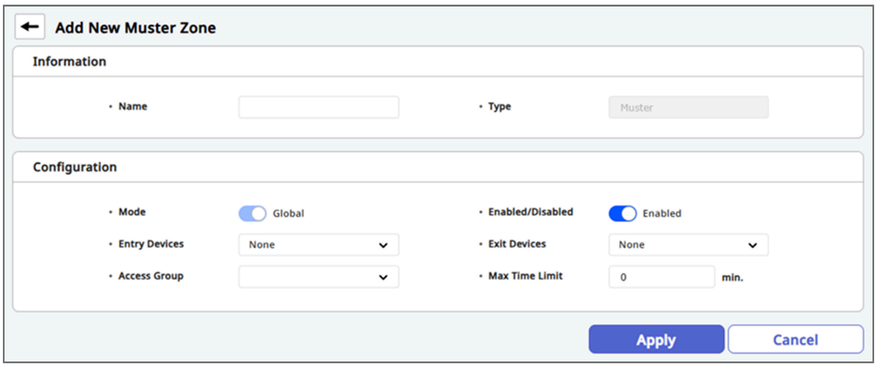
The muster setting serves the following purposes:

- **Emergency response**: Designate a location where users can safely gather in case of emergencies, such as fires or earthquakes.
- **Personnel monitoring**: Check the current number of people and the list of entrants in real-time in a specific location.
- **Long stay detection**: Detect users remaining in a specific location beyond the set time and send notifications to the administrator.
- **Enhanced security**: Continuously monitor access to sensitive locations to improve security levels.

Through these features, administrators can establish a more systematic and efficient security management framework.

Register muster

1. Click **Settings** on the **Launcher** page.
2. Click **Advanced AC** in the left sidebar.
3. Click **ADD ADVANCED AC**.
4. Select **Muster** and click **Apply**.
5. Enter the name of the muster setting to be added in the **Info** section.



Add New Muster Zone

Information

- Name
- Type: Muster

Configuration

- Mode: Global
- Enabled/Disabled: Enabled
- Entry Devices: None
- Exit Devices: None
- Access Group
- Max Time Limit: 0 min.

6. Set the details of the muster settings in the **Settings** section. For more information, refer to the following.
7. Configure the actions to be taken when specific events occur in the muster settings in the **Alarm** section.
8. After completing all settings, click **Apply** at the bottom of the screen.

INFO

The **Alarm** section can only be used after configuring both **Entry Devices** and **Exit Devices**.

Setting options guide

The details for muster settings are as follows:

- **Mode**: You can check the scope of application. The muster setting only supports **Global** mode and can be set up with all devices registered in **BioStar X**.
- **Enabled/Disabled**: You can activate or temporarily deactivate the settings.
- **Entry Devices**: Select the device to be used when entering. You can choose from the list of registered devices.
- **Exit Devices**: Select the device to be used when exiting. You can choose from the list of registered devices.
- **Access Group**: Set the access group for users who will stay in the gathering location. You can set up to 16 access groups.
- **Max Time Limit**: You can set the maximum time allowed to stay in the gathering location. It can be set for a maximum of 4320 minutes, and an alarm will occur if a user stays in the gathering location beyond the specified time.

INFO

For more information about device registration, refer to the following.

- Register Device
- Register Wiegand Credentials
- Register Slave

Occupancy Limit

The occupancy limit feature is a key access control function to ensure the safety and efficiency of spaces. This feature allows administrators to set a maximum number of occupants that can enter simultaneously for each location, preventing overcrowding and enabling more systematic space management.

The main applications of the occupancy limit setting are as follows.

- **Safety Management**: Prevention of safety incidents by limiting the maximum number of occupants based on fire safety regulations or building capacity limits.
- **Space Efficiency**: Optimization of the work environment by maintaining appropriate occupancy in meeting rooms, laboratories, and workspaces.
- **Infectious Disease Response**: Management of personnel in situations requiring social distancing or crowd density restrictions.
- **Real-time monitoring**: Check the current occupancy and entry/exit status for each location in real time.
- **Automatic Alerts**: Immediate notifications to administrators upon reaching the set occupancy limit, enabling swift responses.

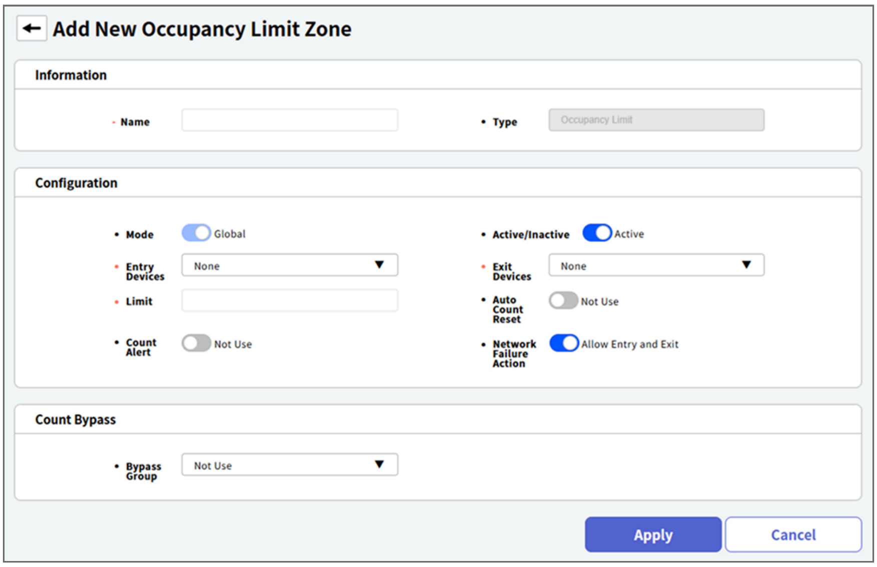
By utilizing these features, administrators can establish tailored personnel management policies suited to the characteristics of each space, ensuring safe and efficient facility operations.

> ⓘ **INFO**
>
> - You can add up to 100 occupancy limit settings.
> - The devices and firmware versions that can be configured for the occupancy limit setting are as follows.
>   - FaceStation F2 firmware version 1.1.0 or higher
>   - FaceStation 2 firmware version 1.5.0 or higher

Occupancy limit registration

1. Click **Settings** on the **Launcher** page.
2. Click **Advanced AC** in the left sidebar.
3. Click **ADD ADVANCED AC**.
4. Select **Occupancy Limit** and click **Apply**.

5. Enter the name of the occupancy limit setting to add in the **Info** section.



Add New Occupancy Limit Zone

Information

- Name
- Type: Occupancy Limit

Configuration

- Mode: Global
- Active/Inactive: Active
- Entry Devices: None
- Exit Devices: None
- Limit
- Auto Count Reset: Not Use
- Count Alert: Not Use
- Network Failure Action: Allow Entry and Exit

Count Bypass

- Bypass Group: Not Use

6. Configure the details of the occupancy limit setting in the **Configuration** section. For more information, refer to the following.

7. In the **Count Bypass** section, you can select access groups that can always bypass the occupancy limit setting. For more information, refer to the following.

8. After completing all settings, click **Apply** at the bottom of the screen.

> **INFO**
>
> **Name** can accept up to 48 characters and cannot be set with the same name as other settings.

Setting options guide

The details for the occupancy limit setting are as follows.

- **Mode**: You can check the scope of application. The occupancy limit setting supports only **Global** mode and can be set for all devices registered to **BioStar X**.

- **Active/Inactive**: You can activate or temporarily deactivate the settings.

- **Entry Devices**: Select the device to be used when entering. You can choose from the list of registered devices.

- **Exit Devices**: Select the device to be used when exiting. You can choose from the list of registered devices.

- **Limit**: Enter the number of persons to limit for entry. Entry is restricted if the number of individuals reaches the set occupancy limit. You can enter a number from 0 to 10,000, and setting it to 0 allows access without limits.

- **Auto Count Reset**: You can set the time to automatically initialize the stored occupancy count. Every day at the set time, the occupancy count and the number of always-passing individuals will be reset.

- **Count Alert**: You can send an alert to the administrator or log an event before the number of entrants reaches the set limit. When occupancy pre-alerts are enabled, the **Alert 1** input field becomes active. To set **Alert 2**, click the ⊞ button.

- **Network Failure Action**: You can determine whether to allow entry and exit when a network error occurs with the configured device. When set to allow entry and exit, the entry restriction stops when the device loses network connection, and users can enter even if the actual number of entrants exceeds the limit.

> ⓘ **INFO**
>
> - The same device cannot be set for both **Entry Devices** and **Exit Devices** at the same time.
> - You can select up to 128 devices for **Entry Devices** and **Exit Devices**.
> - Devices configured with **Dual Authentication** cannot be set as **Entry Devices** and **Exit Devices**.
> - Set the time for the **Auto Count Reset** option while considering the standard time zone of the actual location. For example, if a **BioStar X** server is located in a UTC+1:00 region and the auto-reset time is set to 00:00, the **BioStar X** client in the UTC+2:00 region will have the occupancy automatically reset at 01:00.
> - You can set up to 2 **Count Alert** limits, and only numbers smaller than the limit can be entered. **Alert 1** and **Alert 2** cannot be set to the same value.
> - For more information about device registration, refer to the following.
>   - Register Device
>   - Register Wiegand Credentials
>   - Register Slave

Always-pass personnel setting

You can select access groups that can always bypass the occupancy limit setting. Users who belong to the always bypass group can enter and exit regardless of the occupancy count and will not be counted in the occupancy numbers. Currently active members who are always bypassing can be seen in the always bypass occupants column in the occupancy limit settings list.

> ⓘ **INFO**
>
> - When using a thermal camera connected to the device, setting **Thermal & Mask Check Mode** to **Check without authentication** will not work even if always-pass individuals are set.
> - You can set up to 16 **Bypass Group** groups.

Check occupancy list status

You can check the occupancy limit settings list. You can check the status of each setting and the occupancy count, and change the settings as needed.

- **Name**: You can check the name.
- **Status**: You can check the status.

  - **Normal**: Indicates that the number of users in the zone is less than the number set by **Limit**, **Count Alert**(**Alert 1**, **Alert 2**). Users can enter this location.
  - **Count Alert**: Indicates that the number of users present has reached the value set in **Alert 1** or **Alert 2**.
  - **Full**: Indicates that the number of users present has reached the limit set. Further entries are restricted.
- **Count/Limit**: Check the current number of occupants compared to the capacity. If there is a discrepancy between the recorded occupancy and the actual number of users present due to situations like network errors, the administrator can click ⊞ or ⊟ or click the occupancy count to directly modify the count.
- **Count Bypass**: Check the number of users currently in the always-pass group.
- **Device Status**: Check the status of the configured devices.
  - **Normal**: The network of all configured devices is functioning normally.
  - **Network Failure**: Indicates that one or more devices are experiencing network errors.
- **Full Screen**: You can view the status of the occupancy limit settings in full screen.

> **INFO**
>
> When **Limit** is set, you can enter occupancy counts up to a maximum of 50,000. If **Limit** is not set, you can enter counts up to a maximum of 999,999. You cannot enter numbers exceeding the maximum input value, and if the actual occupancy exceeds this value, the excess will not be recorded in the database.

Initialize occupancy

You can reset the occupancy count and the number of always-pass individuals. Proceeding with the occupancy reset will delete all user's entry and exit information, and the accuracy of the occupancy count may vary depending on the network connection status.

1. Click **Settings** on the **Launcher** page.
2. Click **Advanced AC** in the left sidebar.
3. Click **Occupancy Limit** in the list.
4. Click the checkbox for the setting you want to initialize from the occupancy limit settings list.
5. Click **Reset Count** at the top right of the screen.
6. When a confirmation message appears, click **Apply**.

Activate/deactivate

You can activate a deactivated occupancy limit setting or deactivate an activated setting. Deactivating the settings will reset **Current Occupancy** and **Bypass Count**.

1. Click **Settings** on the **Launcher** page.
2. Click **Advanced AC** in the left sidebar.

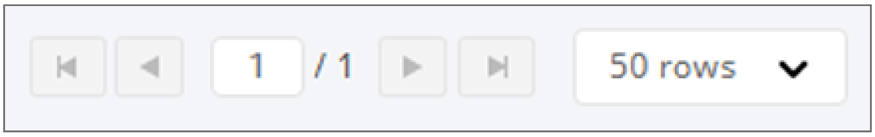
3. Click **Occupancy Limit** in the list.
4. Click the checkbox for the item in the occupancy limit settings list to activate or deactivate.
5. Click **Activate** or **Deactivate** at the top right of the screen.

Delete

1. Click **Settings** on the **Launcher** page.
2. Click **Advanced AC** in the left sidebar.
3. Click **Occupancy Limit** in the list.
4. Click the checkbox for the item you want to delete from the occupancy limit settings list.
5. Click **Delete** at the top right of the screen.
6. When a confirmation message appears, click **Apply**.

Navigate the list page

Move between pages or set the number of items to appear on each page. Use the page navigation tool in the top right corner of the screen.



- ⏮: Move to the first page.
- ◀: Move to the previous page.
- ▶: Move to the next page.
- ⏭: Move to the last page.
- Enter the page number in the input field to move to the desired page.
- Click the row selection box to set the number of items displayed on each page.

Roll Call

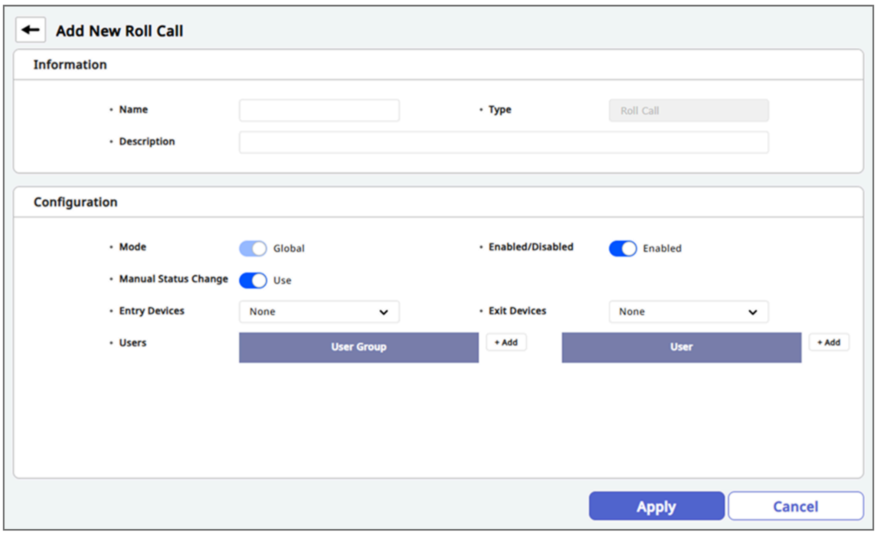
Roll call is a feature that quickly generates a list of personnel based on entry records at a specific time and place, allowing for real-time tracking of current locations. In the event of an emergency, the user can determine whether they have arrived at the roll call location by authenticating through entry or exit devices at a pre-designated location.

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

> **INFO**
>
> Roll call settings can be used through additional options available with an **Advanced** license or above. For more information on licensing policy, refer to the following.

Register roll call

1. Click **Settings** on the **Launcher** page.
2. Click **Advanced AC** in the left sidebar.
3. Click **ADD ADVANCED AC**.
4. Select **Roll Call** and click **Apply**.
5. Enter the name and description of the roll call setting to be added in the **Info** section.



Add New Roll Call

Information

- Name
- Type: Roll Call
- Description

Configuration

- Mode: Global
- Enabled/Disabled: Enabled
- Manual Status Change: Use
- Entry Devices: None
- Exit Devices: None
- Users

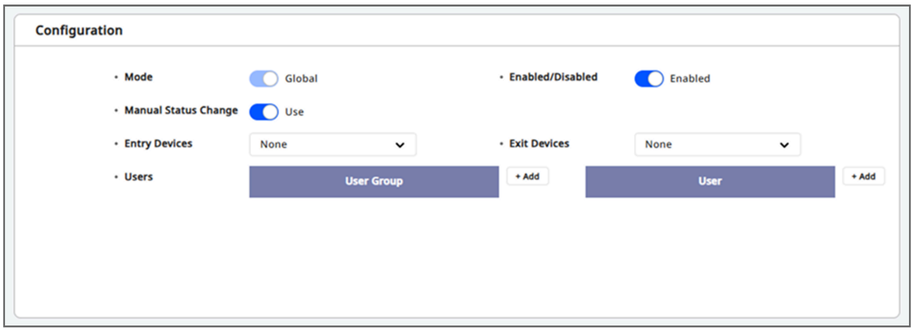
6. Set details in the **Configuration** section. For more information, refer to the following.
7. After completing all settings, click **Apply** at the bottom of the screen.

INFO

Name can accept up to 48 characters and cannot be set with the same name as other settings.

Setting options guide

The details for roll call settings are as follows.



Configuration

- Mode: Global
- Enabled/Disabled: Enabled
- Manual Status Change: Use
- Entry Devices: None
- Exit Devices: None
- Users

- **Mode**: You can check the scope of application. Roll call settings are supported only in **Global** mode, and can be configured for all devices registered in **BioStar X**.
- **Enabled/Disabled**: You can activate or temporarily deactivate the settings.
- **Manual Status Change**: You can set it to change the status manually.
- **Entry Devices**: Select the device to be used when entering. You can choose from the list of registered devices.
- **Exit Devices**: Select the device to be used when exiting. You can choose from the list of registered devices.
- **Users**: You can select user groups or individual users who are allowed to enter.

INFO

- The same device cannot be set for both **Entry Devices** and **Exit Devices** at the same time.
- You can select up to 10 devices for **Entry Devices** and **Exit Devices**.
- Devices configured with **Dual Authentication** cannot be set as **Entry Devices** and **Exit Devices**.
- For more information about device registration, refer to the following.
  - Register Device
  - Register Wiegand Credentials
  - Register Slave

Activate/deactivate

You can activate disabled roll call settings or deactivate activated settings.

1. Click **Settings** on the **Launcher** page.

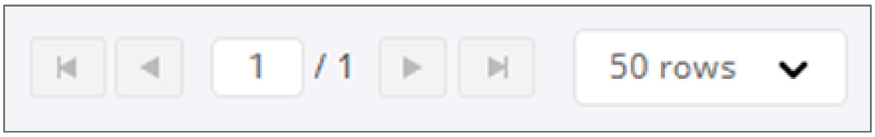
2. Click **Advanced AC** in the left sidebar.
3. Click **Roll Call** from the list.
4. Click the checkbox for the item you want to activate or deactivate in the roll call settings list.
5. Click the **Enable** or **Disable** button in the upper right corner of the screen.

Delete

1. Click **Settings** on the **Launcher** page.
2. Click **Advanced AC** in the left sidebar.
3. Click **Roll Call** from the list.
4. Click the checkbox for the item you want to delete from the roll call settings list.
5. Click the **Delete Advanced AC** button in the upper right corner of the screen.
6. When the warning message appears, click the **Continue** button.

Navigate the list page

Move between pages or set the number of items to appear on each page. Use the page navigation tool in the top right corner of the screen.



- ⏮: Move to the first page.
- ◀: Move to the previous page.
- ▶: Move to the next page.
- ⏭: Move to the last page.
- Enter the page number in the input field to move to the desired page.
- Click the row selection box to set the number of items displayed on each page.

Start roll call

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

INFO

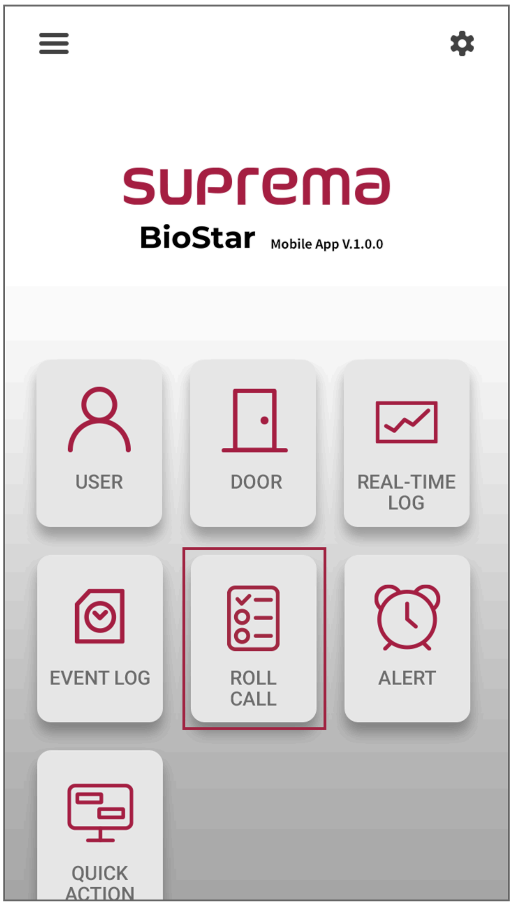
You can install the **BioStar X** mobile app via the following links.

- iOS: Apple App Store
- Android: Google Play

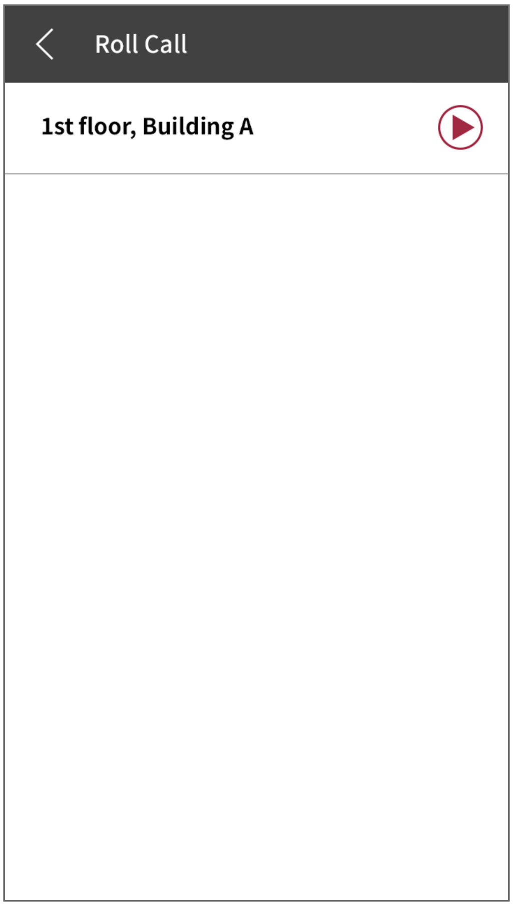
Start roll call in the mobile app

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

1. Launch the **BioStar X** mobile app on your mobile device.
2. Tap the **Roll Call** button on the app's home screen.

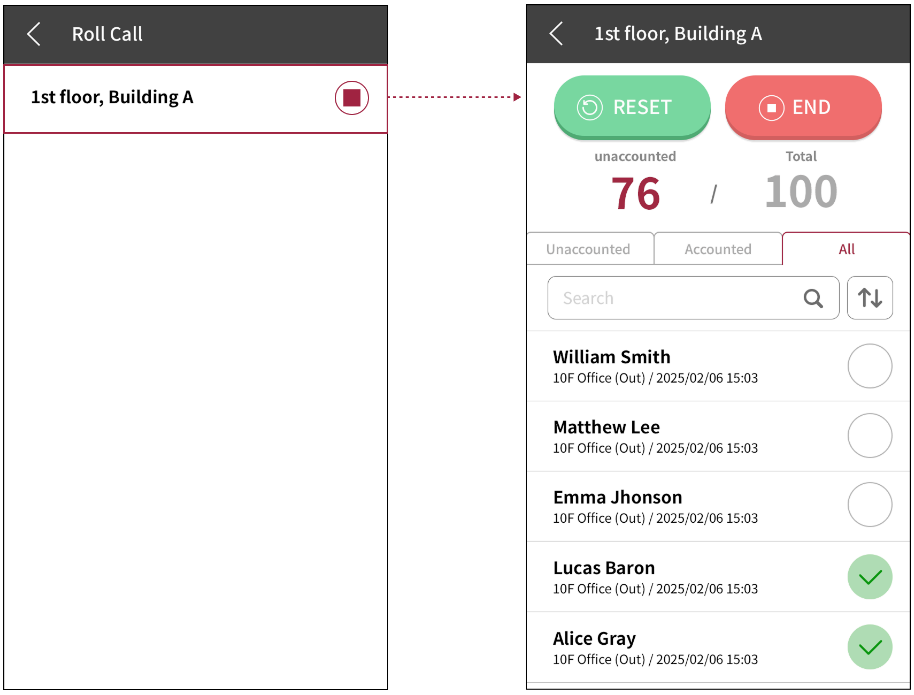


3. In the Roll Call list, tap the ▶ button for the item you want to execute roll call.



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

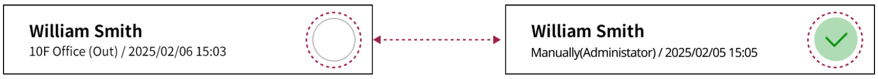
Roll call will start, and by tapping on the ongoing roll call item, you can check the status of the roll call.



Roll Call
1st floor, Building A
1st floor, Building A
RESET
END
unaccounted
Total
76
/
100
Unaccounted
Accounted
All
Search
William Smith
10F Office (Out) / 2025/02/06 15:03
Matthew Lee
10F Office (Out) / 2025/02/06 15:03
Emma Jhonson
10F Office (Out) / 2025/02/06 15:03
Lucas Baron
10F Office (Out) / 2025/02/06 15:03
Alice Gray
10F Office (Out) / 2025/02/06 15:03

Ongoing roll call control

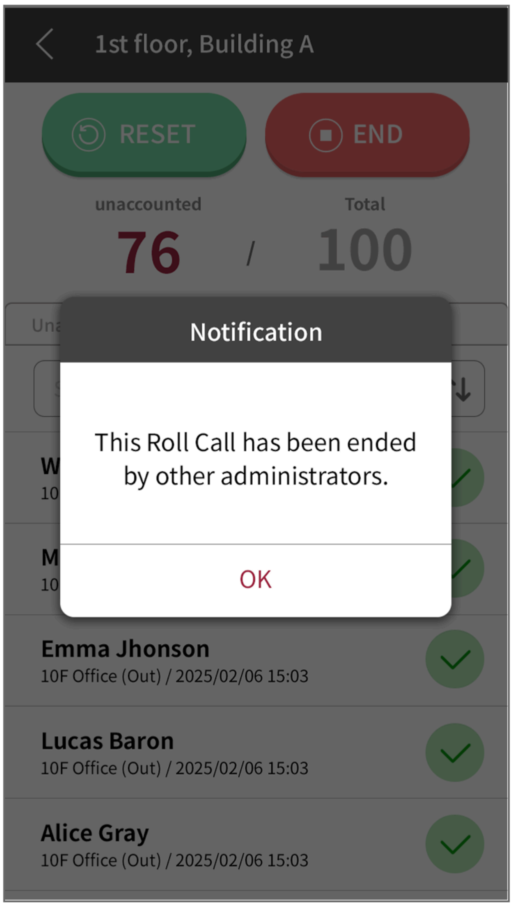
- Users entering will be marked with the ✓ icon. When all users have entered, a message indicating that roll call has ended will appear. To end the roll call, tap the **Yes** button.
- The administrator can manually change the user's entry or status. Long press the round button on the far right of the user whose status you wish to change from the user list.



William Smith
10F Office (Out) / 2025/02/06 15:03

William Smith
Manually(Administator) / 2025/02/05 15:05

- To reset an entering user, tap the **Reset** button. Change the **Accounted** user to **Unaccounted** status.
- If roll call is ended by another administrator, a notification message will appear.



Notification

This Roll Call has been ended by other administrators.

W
10

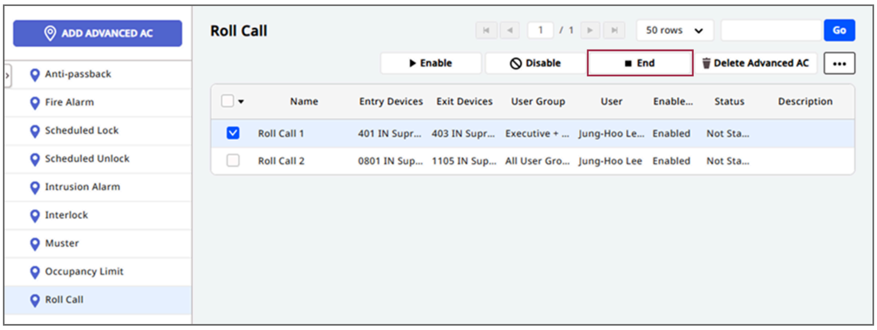
M
10

Emma Jhonson
10F Office (Out) / 2025/02/06 15:03

Lucas Baron
10F Office (Out) / 2025/02/06 15:03

Alice Gray
10F Office (Out) / 2025/02/06 15:03

- To end an ongoing roll call, tap the ■ button in the roll call list screen, or tap the **END** button in the roll call status screen.
- You can also end the ongoing roll call in **BioStar X**. Go to **Settings** → **Advanced AC** → **Events** → **Roll Call** menu, select the ongoing roll call item, and click the **Ended** button at the top right of the screen.



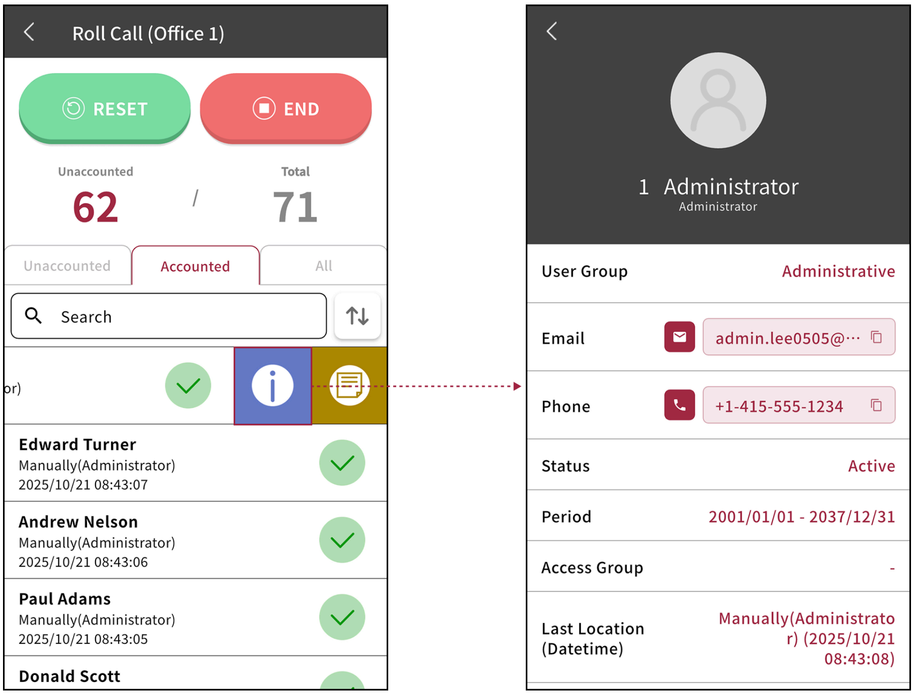
□	Name	Entry Devices	Exit Devices	User Group	User	Enable...	Status	Description
☑	Roll Call 1	401 IN Supr...	403 IN Supr...	Executive + ...	Jung-Hoo Le...	Enabled	Not Sta...	
□	Roll Call 2	0801 IN Sup...	1105 IN Sup...	All User Gro...	Jung-Hoo Lee	Enabled	Not Sta...	

- After completing the roll call, you can check related reports from **Data** → **Generate Report** → **Roll Call**. For more information, refer to the following.

User information during roll call

During roll call in the mobile app, you can check each user's information. It is useful to contact users in an emergency or to locate a user's current position.

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



Edward Turner
Manually(Administrator)
2025/10/21 08:43:07

Andrew Nelson
Manually(Administrator)
2025/10/21 08:43:06

Paul Adams
Manually(Administrator)
2025/10/21 08:43:05

Donald Scott

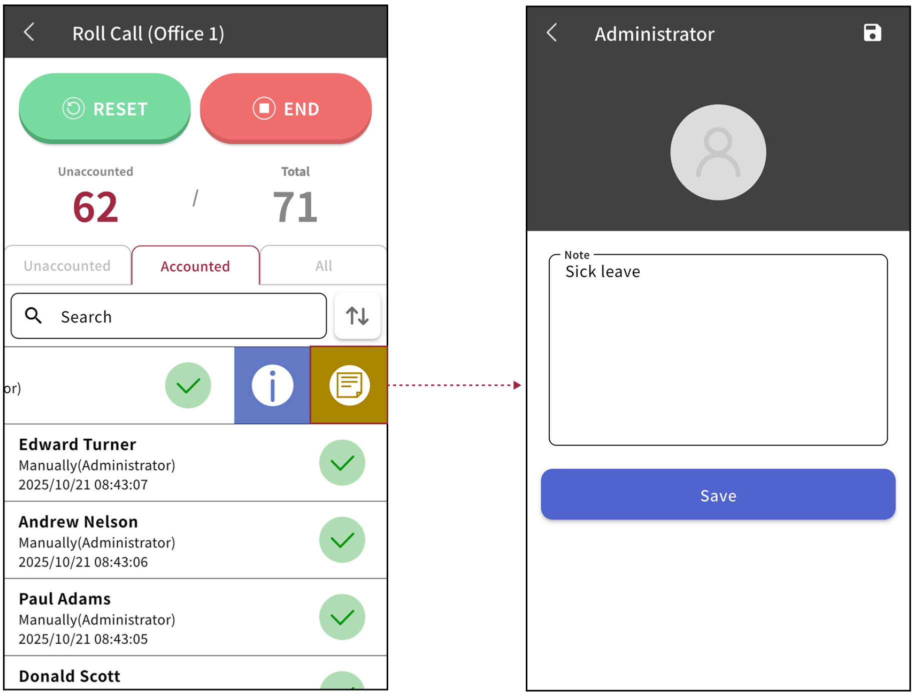
1 Administrator
Administrator

User Group	Administrative
Email	admin.lee0505@···
Phone	+1-415-555-1234
Status	Active
Period	2001/01/01 - 2037/12/31
Access Group	-
Last Location (Datetime)	Manually(Administrator) (2025/10/21 08:43:08)

Leave a note for users during roll call

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

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



Edward Turner
Manually(Administrator)
2025/10/21 08:43:07

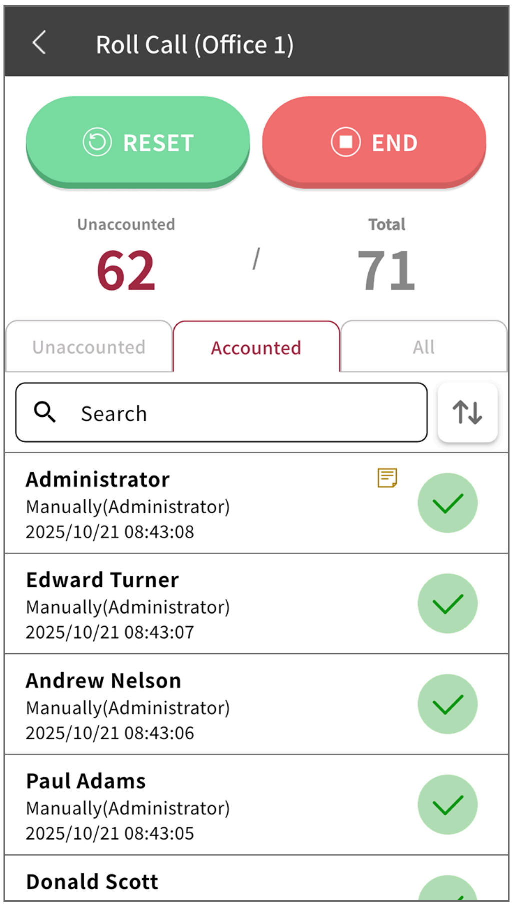
Andrew Nelson
Manually(Administrator)
2025/10/21 08:43:06

Paul Adams
Manually(Administrator)
2025/10/21 08:43:05

Donald Scott

Note
Sick leave

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



Administrator
Manually(Administrator)
2025/10/21 08:43:08

Edward Turner
Manually(Administrator)
2025/10/21 08:43:07

Andrew Nelson
Manually(Administrator)
2025/10/21 08:43:06

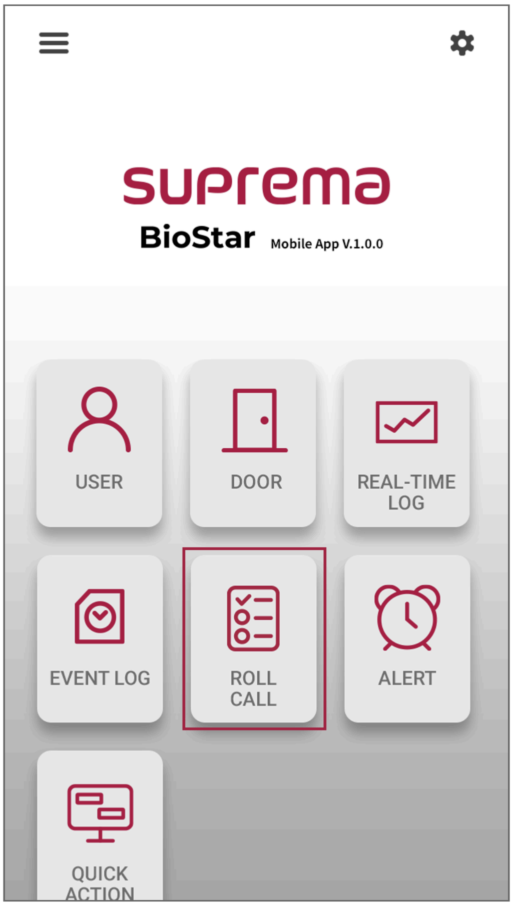
Paul Adams
Manually(Administrator)
2025/10/21 08:43:05

Donald Scott

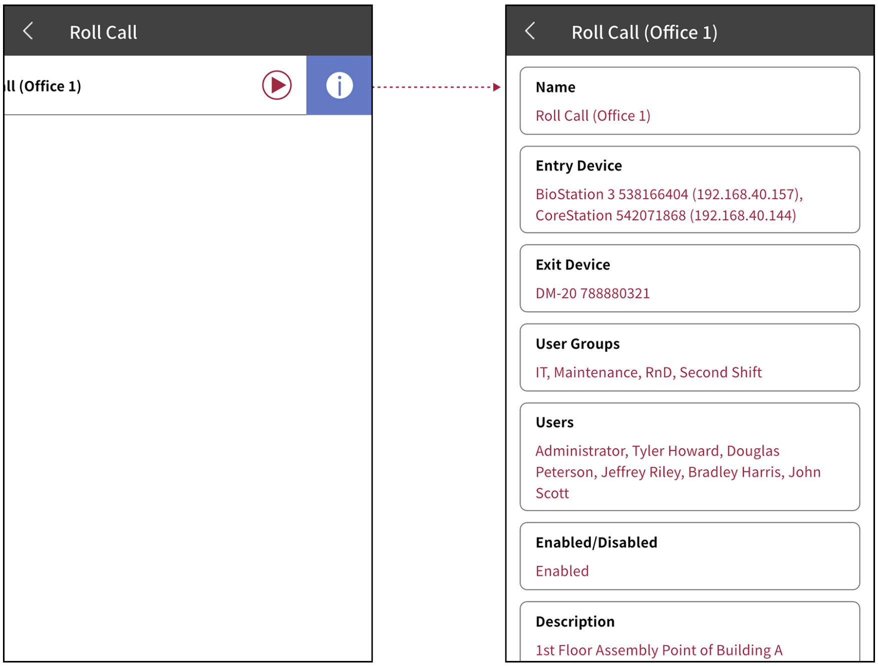
Check roll call details

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

1. Launch the **BioStar X** mobile app on your mobile device.
2. Tap the **Roll Call** button on the app's home screen.



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



Name
Roll Call (Office 1)

Entry Device
BioStation 3 538166404 (192.168.40.157), CoreStation 542071868 (192.168.40.144)

Exit Device
DM-20 788880321

User Groups
IT, Maintenance, RnD, Second Shift

Users
Administrator, Tyler Howard, Douglas Peterson, Jeffrey Riley, Bradley Harris, John Scott

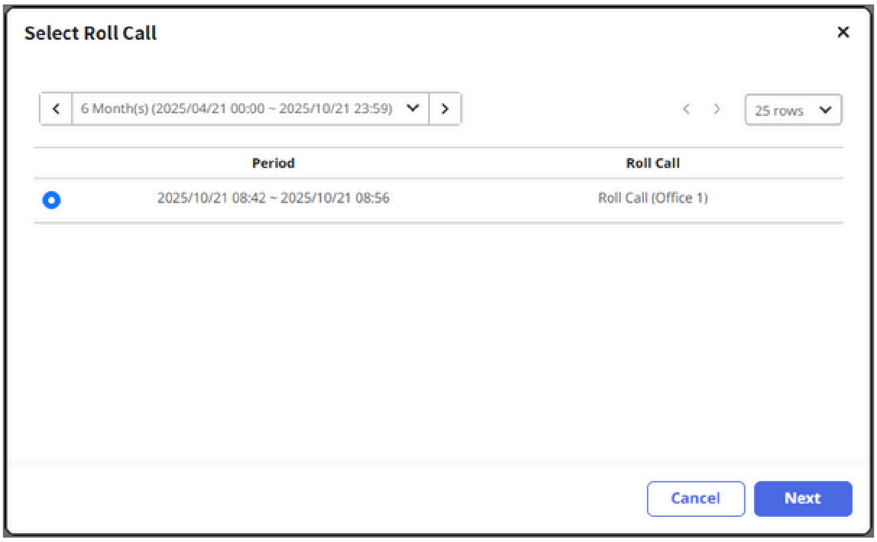
Enabled/Disabled
Enabled

Description
1st Floor Assembly Point of Building A

View roll call reports

To check the roll call report, follow these steps.

1. Click **Launcher** on the page of **Data**.
2. On the left sidebar of the screen, click **Events** → **Roll Call**.
3. When the **Select Roll Call** window appears, select the roll call item you want to check in the report, then click the **Next** button.



Select Roll Call

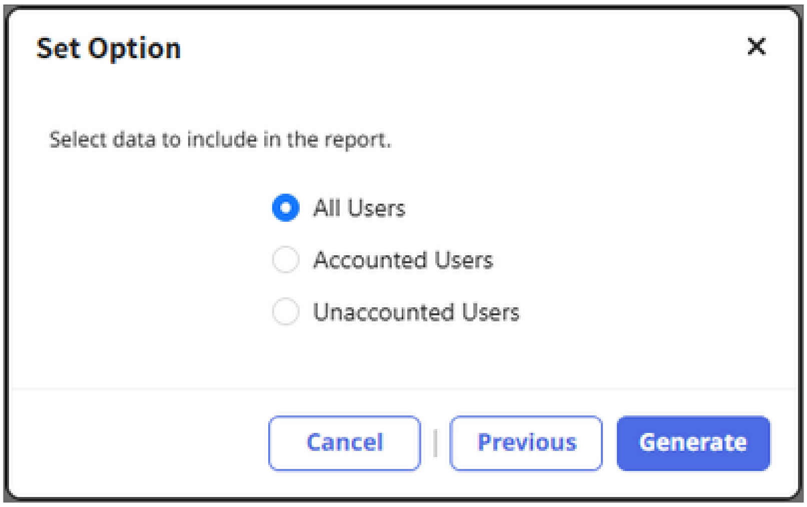
6 Month(s) (2025/04/21 00:00 ~ 2025/10/21 23:59)

25 rows

	Period	Roll Call
●	2025/10/21 08:42 ~ 2025/10/21 08:56	Roll Call (Office 1)

> ⓘ If you do not see the desired roll call item, adjust the period at the top of the screen.

4. In the option settings window, select the data to include in the report, then click the **Generate** button.

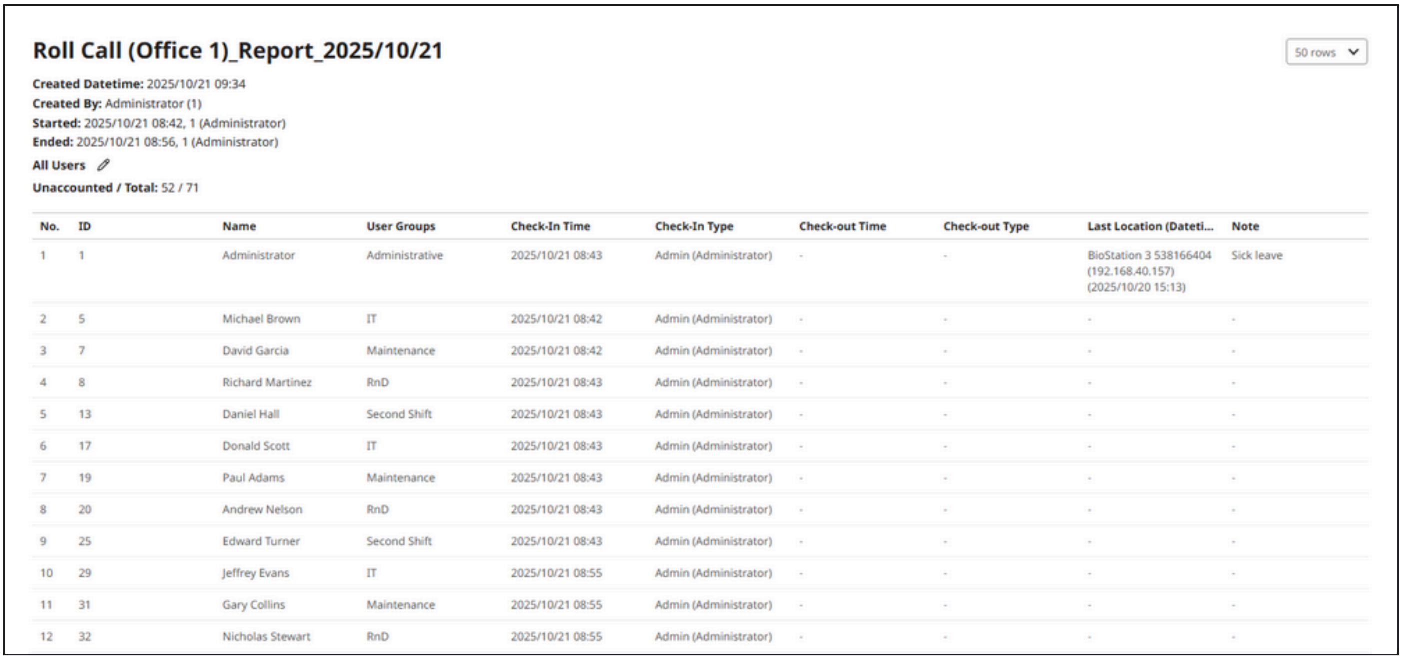


Set Option

Select data to include in the report.

● All Users
○ Accounted Users
○ Unaccounted Users

Generating the report. The report provides information on each user, including their entry time, exit time, last location, and notes.



Roll Call (Office 1)_Report_2025/10/21

Created Datetime: 2025/10/21 09:34
Created By: Administrator (1)
Started: 2025/10/21 08:42, 1 (Administrator)
Ended: 2025/10/21 08:56, 1 (Administrator)

All Users

Unaccounted / Total: 52 / 71

No.	ID	Name	User Groups	Check-In Time	Check-In Type	Check-out Time	Check-out Type	Last Location (Dateti...	Note
1	1	Administrator	Administrative	2025/10/21 08:43	Admin (Administrator)	-	-	BioStation 3 538166404 (192.168.40.157) (2025/10/20 15:13)	Sick leave
2	5	Michael Brown	IT	2025/10/21 08:42	Admin (Administrator)	-	-	-	-
3	7	David Garcia	Maintenance	2025/10/21 08:42	Admin (Administrator)	-	-	-	-
4	8	Richard Martinez	RnD	2025/10/21 08:43	Admin (Administrator)	-	-	-	-
5	13	Daniel Hall	Second Shift	2025/10/21 08:43	Admin (Administrator)	-	-	-	-
6	17	Donald Scott	IT	2025/10/21 08:43	Admin (Administrator)	-	-	-	-
7	19	Paul Adams	Maintenance	2025/10/21 08:43	Admin (Administrator)	-	-	-	-
8	20	Andrew Nelson	RnD	2025/10/21 08:43	Admin (Administrator)	-	-	-	-
9	25	Edward Turner	Second Shift	2025/10/21 08:43	Admin (Administrator)	-	-	-	-
10	29	Jeffrey Evans	IT	2025/10/21 08:55	Admin (Administrator)	-	-	-	-
11	31	Gary Collins	Maintenance	2025/10/21 08:55	Admin (Administrator)	-	-	-	-
12	32	Nicholas Stewart	RnD	2025/10/21 08:55	Admin (Administrator)	-	-	-	-

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

Video Settings

With the video settings feature of **BioStar X**, you can manage access control and video security in an integrated manner. Utilize powerful security management features such as real-time video monitoring, event-linked recording, and automatic bookmark generation by integrating with **Video Management System** (VMS).

> ⓘ **INFO**
>
> The video settings feature is available through additional options with an **Advanced** license or higher. For more information on licensing policy, refer to the following.

Video settings overview

The video settings consist of the following three steps.

1 Integrate VMS server

Set up the connection between the VMS server and **BioStar X** and configure the certificates. An essential step in building an integrated video security management system. For more information on this, refer to the following.

2 Set up the camera

Select the necessary cameras among the cameras connected to the VMS and create groups for efficient management. For more information on this, refer to the following.

3 Set up rules

Create rules that link access events with video to utilize advanced features such as automatic bookmarks and event logging. For more information on this, refer to the following.

Key features

- **Integrated monitoring**: Manage access control and video security from a single interface.
- **Automatic event logging**: Automatically record associated video and generate tags when access events occur.
- **Efficient search**: Quickly search videos and collect evidence through bookmarks and event tags.
- **Real-time response**: Instantly check relevant camera footage when security situations arise.

Integrate VMS

The **Video Management System** (VMS) is a video management system that integrates and manages video from multiple cameras, allowing for recording and playback. Integrating BioStar X with VMS allows you to manage access control and video security on a single platform.

You can gain the following benefits through VMS integration.

- **Real-time monitoring**: You can view real-time video from cameras connected to doors.
- **Integrated event management**: You can understand security situations by linking access events with video.
- **Efficient evidence collection**: You can quickly search and replay recorded video from specific points in time.
- **Bookmark function**: You can add video tags to important event moments for easy retrieval and review.

Before start

To integrate with the **Video Management System** (VMS), please check the following items.

- The VMS integration feature is available through additional options for licenses above **Advanced**. For more information on licensing policy, refer to the following.
- Make sure that the VMS server is correctly installed and configured. The VMS server must be in a state that can connect online with **BioStar X**.
- Use a VMS that is compatible with **BioStar X**. You can use **BioStar X VMS** or the **Nx Witness v5.1.5** series of VMS.
- Prepare the IP address, port number, and administrator account information of the VMS server. This information is needed to connect the VMS server with **BioStar X**.

VMS server integration settings

Follow the steps below to integrate the VMS server with **BioStar X**.

1 Install the certificate on the VMS server

To play back recorded video from the VMS server, you must use HTTPS protocol. Generate an IP address-based certificate on the VMS server.

> ⓘ
> - Before installing the certificate, ensure that Open JDK 21 or higher is installed on the PC where VMS is installed.
> - When installing the VMS server and **BioStar X** on the same server, you will need to install a certificate.

1. Navigate to the *C:\Program Files\BioStar X\third* path and run the command prompt.
2. Execute the following command.

```
java -jar scaleUtil-1.0-all.jar vmsCertCreate "C:\Windows\System32\config\systemprofile\AppData\
Local\<%VENDOR.NAME%>\<%VENDOR.NAME%> Media Server\ssl" {VMS_IP_ADDRESS}
```

```
java -jar scaleUtil-1.0-all.jar vmsCertCreate "/opt/<%VENDOR.NAME%>/mediaserver/var/ssl" {VMS_IP_ADDRESS}
```

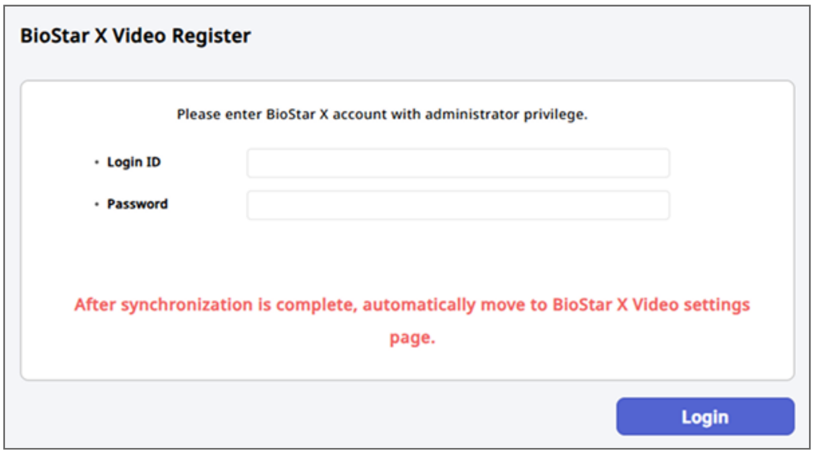
   - Enter the path where VMS is installed in the `<%VENDOR.NAME%>` section.
   - Enter the IP address of the VMS server in the `{VMS_IP_ADDRESS}` section.
   - The *ssl* path may vary depending on the installed VMS product.

3. Check whether the certificate file (*.pem*) was created in the path where VMS is installed.
4. Reboot the VMS server.

> **INFO**
>
> If VMS is installed on a different server than **BioStar X**, copy the *scaleUtil-1.0-all.jar* file to the VMS server and follow the previous steps.

2 Activate VMS integration

1. Click **Settings** on the **Launcher** page.
2. On the left sidebar, click **Video** → **VMS Integration**.
3. If this is your first time accessing, log in with the **BioStar X** administrator account.



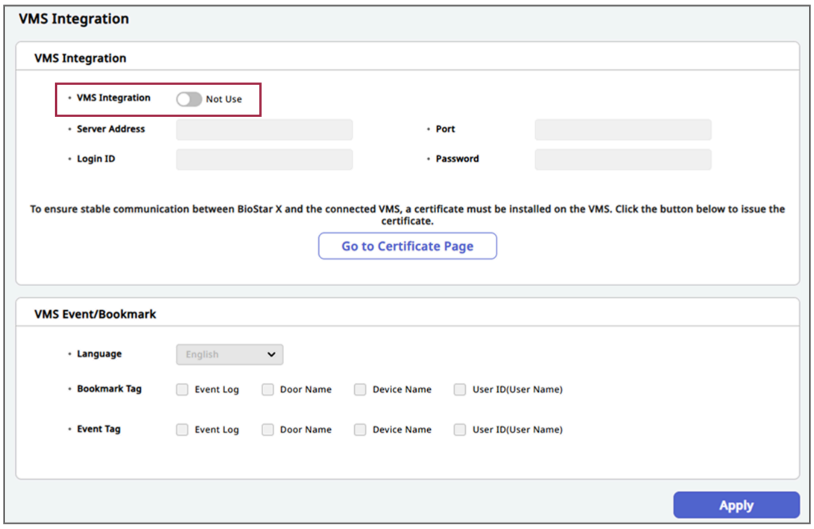
BioStar X Video Register

Please enter BioStar X account with administrator privilege.

- Login ID
- Password

After synchronization is complete, automatically move to BioStar X Video settings page.

4. Set the **VMS Integration** option to **Use**.



VMS Integration

VMS Integration

- VMS Integration ○ Not Use
- Server Address
- Port
- Login ID
- Password

To ensure stable communication between BioStar X and the connected VMS, a certificate must be installed on the VMS. Click the button below to issue the certificate.

VMS Event/Bookmark

- Language: English
- Bookmark Tag: □ Event Log □ Door Name □ Device Name □ User ID(User Name)
- Event Tag: □ Event Log □ Door Name □ Device Name □ User ID(User Name)

5. Enter the VMS server information.
   - **Server Address**: Enter the IP address of the VMS server.
   - **Port**: Enter the port number of the VMS server.
   - **Login ID**: Enter the administrator account ID of the VMS server.
   - **Password**: Enter the administrator account password of the VMS server.
6. Once you have entered all the VMS server information, click the **Apply** button at the bottom right of the screen.

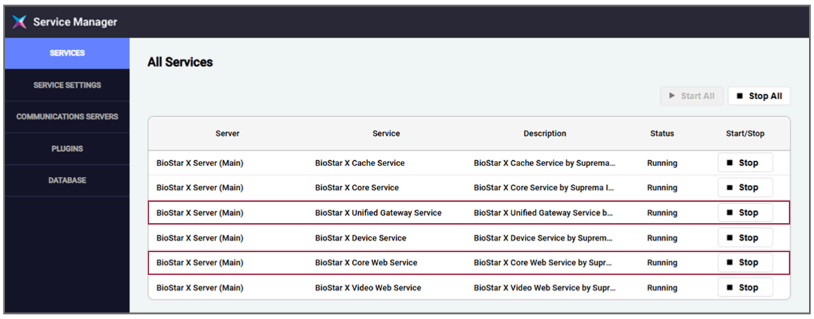
> **INFO**
>
> - If the integration with the VMS server fails and an error message appears, check the server address and administrator account information again. It is also necessary to check whether the VMS server is online and if network connections are blocked due to firewall settings.
> - For more information on the settings in the **VMS Event/Bookmark** section, refer to the following.

3 Restart service

The first time you integrate with the VMS server, **BioStar X** will automatically restart the service. If it does not automatically restart, follow the instructions below to manually restart the service.

1. Click **Start** ⊞ → **BioStar X** → **BioStar X Service Manager** on Windows.

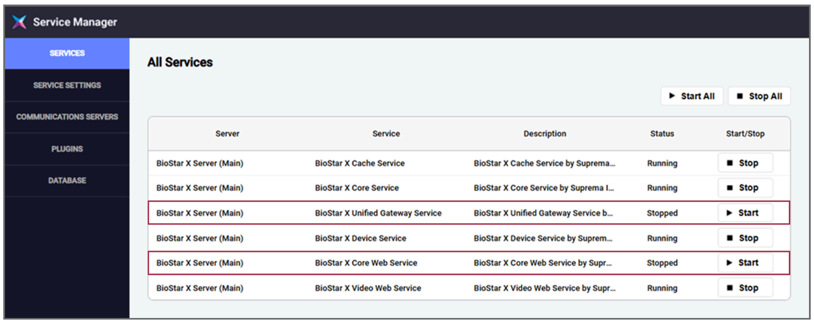
2. In the **All Services** list, click the **Stop** button for the services below to stop them.



Server	Service	Description	Status	Start/Stop
BioStar X Server (Main)	BioStar X Cache Service	BioStar X Cache Service by Suprema...	Running	■ Stop
BioStar X Server (Main)	BioStar X Core Service	BioStar X Core Service by Suprema I...	Running	■ Stop
BioStar X Server (Main)	BioStar X Unified Gateway Service	BioStar X Unified Gateway Service b...	Running	■ Stop
BioStar X Server (Main)	BioStar X Device Service	BioStar X Device Service by Suprem...	Running	■ Stop
BioStar X Server (Main)	BioStar X Core Web Service	BioStar X Core Web Service by Supr...	Running	■ Stop
BioStar X Server (Main)	BioStar X Video Web Service	BioStar X Video Web Service by Supr...	Running	■ Stop

- **BioStar X Unified Gateway Service**
- **BioStar X Core Web Service**

3. When the status of the requested service changes from **Pending** to **Stopped**, click the **Start** button to restart the service.



Server	Service	Description	Status	Start/Stop
BioStar X Server (Main)	BioStar X Cache Service	BioStar X Cache Service by Suprema...	Running	■ Stop
BioStar X Server (Main)	BioStar X Core Service	BioStar X Core Service by Suprema I...	Running	■ Stop
BioStar X Server (Main)	BioStar X Unified Gateway Service	BioStar X Unified Gateway Service b...	Stopped	▶ Start
BioStar X Server (Main)	BioStar X Device Service	BioStar X Device Service by Suprem...	Running	■ Stop
BioStar X Server (Main)	BioStar X Core Web Service	BioStar X Core Web Service by Supr...	Stopped	▶ Start
BioStar X Server (Main)	BioStar X Video Web Service	BioStar X Video Web Service by Supr...	Running	■ Stop

4 Check and configure cameras

If the VMS server is integrated normally, you can check the connected cameras in the **Video** → **Video** menu. For more information, refer to the the following.

Troubleshooting

If the following situations occur, you can install the certificate from the VMS server onto the client PC to resolve the issue.

- When accessing **Video Management System** (VMS) through the browser, and a 'Not secure' warning appears
- When real-time video plays on the **Monitoring** page but recorded video does not play

Certificate installation on client PC

1. Download the HTTPS certificate installer (*cert-register.zip*) from the login screen or **Settings** → **Server** → **HTTPS** on the client PC where **BioStar X** is installed.
2. Unzip the downloaded file and run **cert-register.exe** file. **Enrollment Certification** window will appears.

3. Select **VMS** for **Target System** and enter the following information.

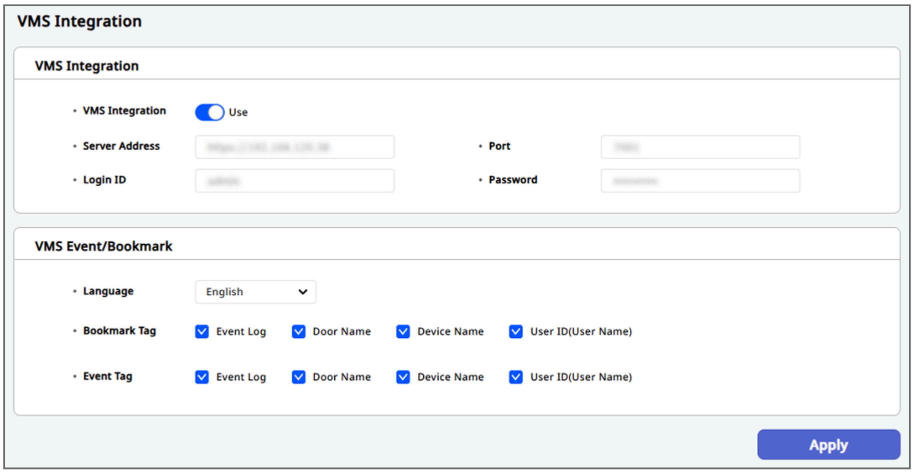
   - **Server Address**: IP address of the VMS server
   - **Port**: Port number of the VMS server

4. Click the **Enrollment** button.
5. Check the security warning message and click **Yes**.

Restart the web browser and check if the recorded video from the VMS server plays normally on the **Monitoring** page.

VMS event and bookmark settings

You can transmit bookmark tags and event tag information to the integrated VMS server. At this point, you can choose to transmit event logs, door names, device names, and user IDs together. Select the desired options and click the **Apply** button at the bottom right of the screen.



VMS Integration

VMS Integration

- VMS Integration: Use
- Server Address:
- Port:
- Login ID:
- Password:

VMS Event/Bookmark

- Language: English
- Bookmark Tag: ☑ Event Log ☑ Door Name ☑ Device Name ☑ User ID(User Name)
- Event Tag: ☑ Event Log ☑ Door Name ☑ Device Name ☑ User ID(User Name)

- **Language**: Choose the language for the event and bookmark tags transmitted to the VMS server. You can select either Korean or English.
- **Bookmark Tag**: Bookmark tags allow you to easily locate and review videos stored on the VMS server with designations and names for quick identification. Select the information to send with the bookmark tag.
- **Event Tag**: You can transmit events that occurred at specific moments to the VMS server for logging. Select the information to send with the event tag.

> **INFO**
>
> - For more information on the bookmark function in VMS, refer to the following link.
> - For more information on the event function in VMS, refer to the following link.

Disconnect VMS server integration

To disconnect the integrated VMS server, follow the steps below. Disconnecting VMS integration will delete all video settings, registered cameras, and rules.

1. Click **Settings** on the **Launcher** page.
2. On the left sidebar, click **Video** → **VMS Integration**.
3. Set the **VMS Integration** option to **Not Use**.
4. Click the **Apply** button at the bottom right of the screen.
5. Check the contents of the message window and click the **Yes** button.

Set up the camera

After completing the VMS integration, select and set up the cameras to be used in BioStar X. Appropriate camera configurations enable the use of the following security management features.

- **Optional Monitoring**: You can add only the necessary cameras from all the cameras of VMS to **BioStar X**.
- **Efficient Management**: Cameras can be systematically managed by grouping them according to location or purpose.

> ⓘ **INFO**
>
> Refer to the following for information on how to integrate with the VMS server.

Camera settings and management

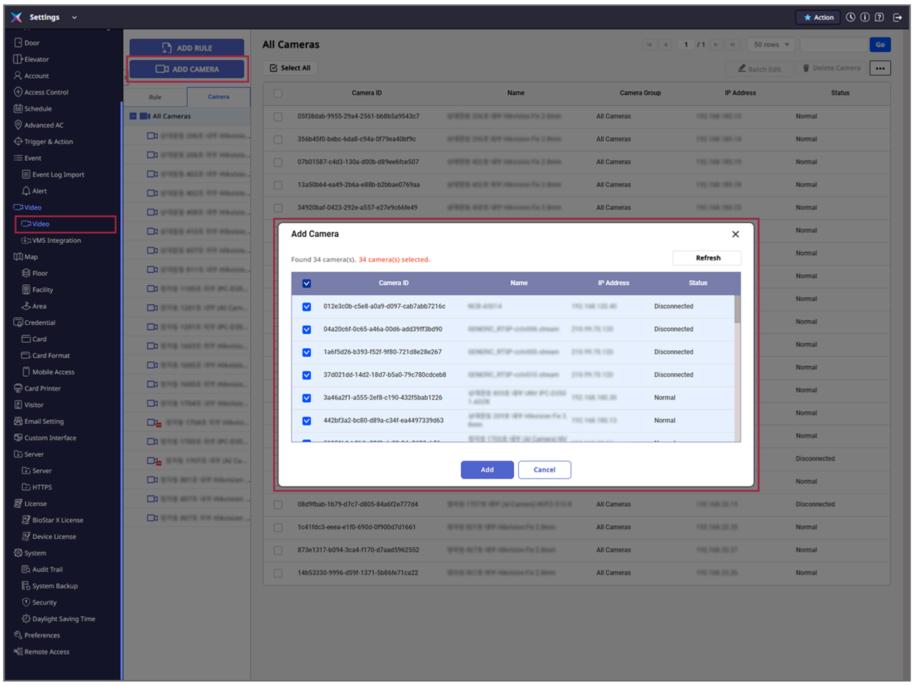
After VMS integration, you can set up and manage cameras in the menu **Settings** → **Video** → **Video**.

Add camera

If integrated with VMS, you can add cameras connected to the VMS server to **BioStar X** and play live video and recorded footage on the **Monitoring** page.

1. Click **Settings** on the **Launcher** page.
2. Click **Video** → **Video** in the left sidebar.
3. Click **ADD CAMERA**.
4. When the **Add Camera** window appears, select the cameras to exclude from the list.
   If your desired camera is not displayed, click the **Refresh** button to refresh the camera list.
5. Once you have selected the cameras, click the **Add** button in the bottom right corner of the screen.

You can check the added cameras in the camera list.



Add Camera

Found 34 camera(s). 34 camera(s) selected.

Refresh

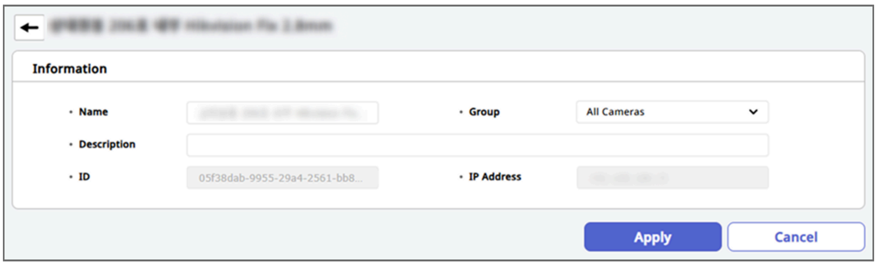
☑	Camera ID	Name	IP Address	Status
☑	012e3c0b-c5e8-a0a9-d097-cab7abb7216c	[illegible]	[illegible]	Disconnected
☑	04a20c6f-0c65-a46a-00d6-add39ff3bd90	[illegible]	[illegible]	Disconnected
☑	1a6f5d26-b393-f52f-9f80-721d8e28e267	[illegible]	[illegible]	Disconnected
☑	37d021dd-14d2-18d7-b5a0-79c780cdceb8	[illegible]	[illegible]	Disconnected
☑	3a46a2f1-a555-2ef8-c190-432f5bab1226	[illegible]	[illegible]	Normal
☑	442bf3a2-bc80-d89a-c34f-ea4497339d63	[illegible]	[illegible]	Normal

Add Cancel

Edit camera information

You can edit the information of the added cameras. You can change the camera name, group, description, etc.

1. Click **Settings** on the **Launcher** page.
2. Click **Video** → **Video** in the left sidebar.
3. Click the **Camera** tab in the upper left corner of the screen.
4. Click the camera you want to edit in the camera list.
5. When the screen showing the camera information appears, edit your desired items.



Information

- Name: [illegible]
- Group: All Cameras
- Description:
- ID: 05f38dab-9955-29a4-2561-bb8...
- IP Address: [illegible]

Apply Cancel

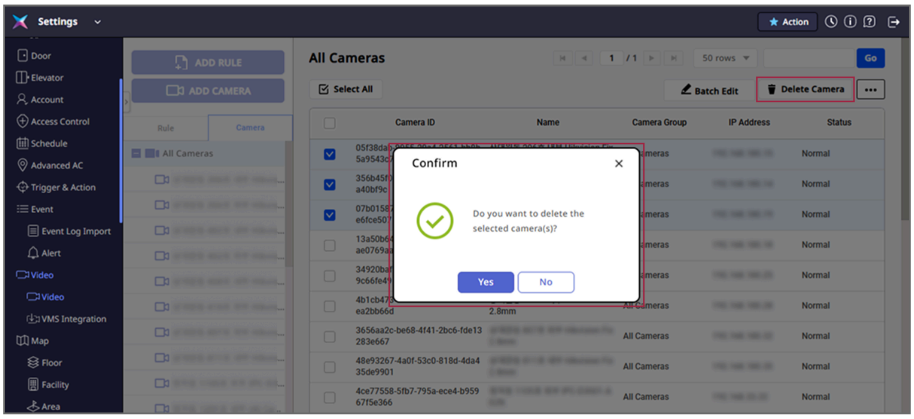
6. After editing all the camera information, click the **Apply** button in the bottom right corner of the screen.

> **INFO**
>
> The camera ID and IP address cannot be modified.

Delete camera

You can delete the added cameras.

1. Click **Settings** on the **Launcher** page.
2. Click **Video** → **Video** in the left sidebar.
3. Click the checkbox on the far left of the camera you want to delete from the camera list. You can select more than one camera.
4. Click the 🗑 **Delete Camera** button in the upper right corner of the screen.
5. Check the message and click the **Yes** button.



Confirm

Do you want to delete the selected camera(s)?

INFO

If the camera you want to delete is included in a rule, you cannot delete the camera. Remove the camera from the rule and try again. For more information on rule creation and management, refer to the following.

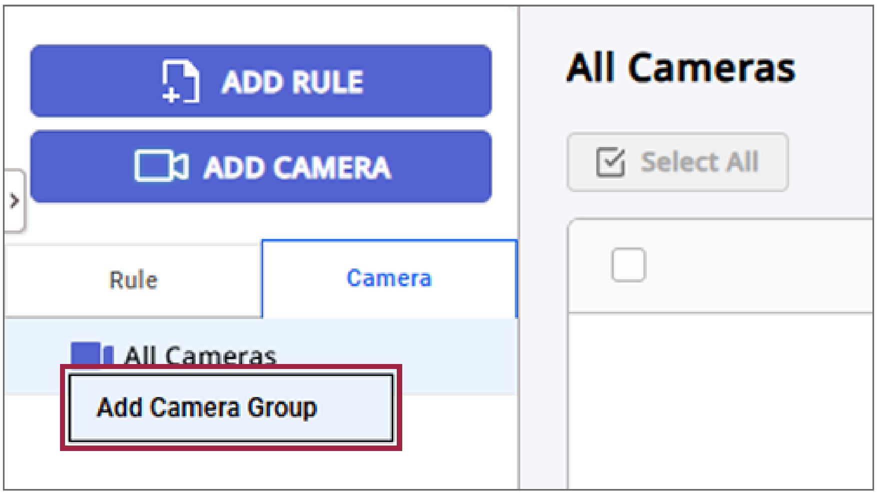
Camera group settings and management

Add camera group

You can group multiple cameras for management by adding a camera group.

1. Click **Settings** on the **Launcher** page.
2. Click **Video** → **Video** in the left sidebar.
3. Click the **Camera** tab in the upper left corner of the screen.

4. Select **All Cameras** and right-click.



5. Click **Add Camera Group** from the popup menu.

6. Enter the desired group name and press the Enter key.

> **INFO**
>
> - You can create camera groups with up to 8 subgroups.
> - Camera group names can be entered up to 48 characters long.
> - When you select a camera group from the camera list, only the cameras belonging to that group will be displayed in the list.

Add multiple cameras to the group

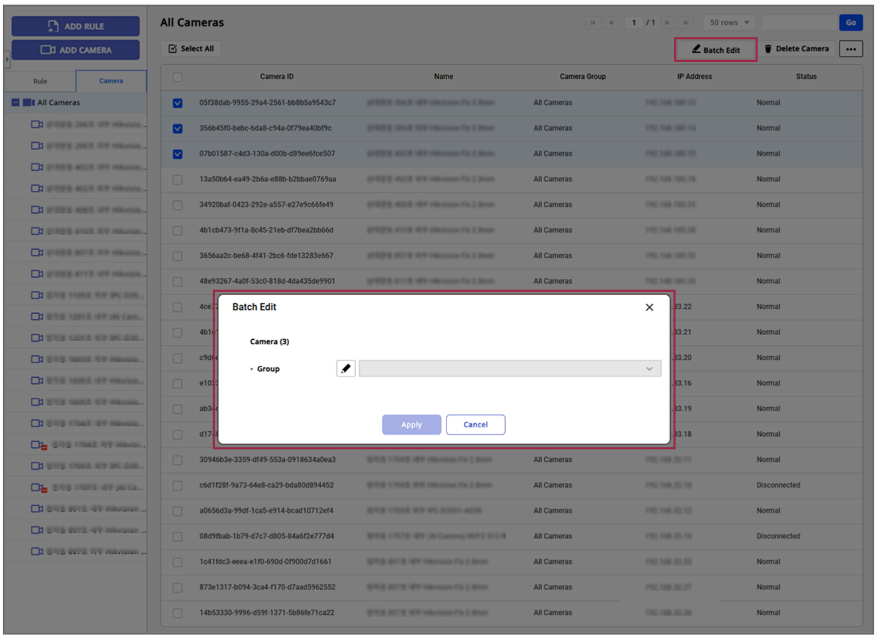
You can add more than one camera to the added group.

1. Click **Settings** on the **Launcher** page.

2. Click **Video** → **Video** in the left sidebar.

3. Click the checkbox on the far left of the cameras to be added to the group in the camera list. You can select more than one camera.

4. If you select more than one camera, the ✎ **Batch Edit** button will be activated in the upper right corner of the screen. Click the **Batch Edit** button.



☐	Camera ID	Name	Camera Group	IP Address	Status
☑	05f38dab-9955-29a4-2561-bb8b5a9543c7	[illegible]	All Cameras	[illegible]	Normal
☑	356b45f0-bebc-6da8-c94a-0f79ea40bf9c	[illegible]	All Cameras	[illegible]	Normal
☑	07b01587-c4d3-130a-d00b-d89ee6fce507	[illegible]	All Cameras	[illegible]	Normal
☐	13a50b64-ea49-2b6a-e88b-b2bbae0769aa	[illegible]	All Cameras	[illegible]	Normal
☐	34920baf-0423-292e-a557-e27e9c66fe49	[illegible]	All Cameras	[illegible]	Normal
☐	4b1cb473-9f1a-8c45-21eb-df7bea2bb66d	[illegible]	All Cameras	[illegible]	Normal
☐	3656aa2c-be68-4f41-2bc6-fde13283e667	[illegible]	All Cameras	[illegible]	Normal
☐	48e93267-4a0f-53c0-818d-4da435de9901	[illegible]	All Cameras	[illegible]	Normal
☐	4ce7			33.22	Normal
☐	4b1			33.21	Normal
☐	c9d			33.20	Normal
☐	e10			33.16	Normal
☐	ab3			33.19	Normal
☐	d17			33.18	Normal
☐	30946b3e-3359-df49-553a-0918634a0ea3	[illegible]	All Cameras	[illegible]	Normal
☐	c6d1f28f-9a73-64e8-ca29-bda80d894452	[illegible]	All Cameras	[illegible]	Disconnected
☐	a0656d3a-99df-1ca5-e914-bcad10712ef4	[illegible]	All Cameras	[illegible]	Normal
☐	08d9fbab-1b79-d7c7-d805-84a6f2e777d4	[illegible]	All Cameras	[illegible]	Disconnected
☐	1c41fdc3-eeea-e1f0-690d-0f900d7d1661	[illegible]	All Cameras	[illegible]	Normal
☐	873e1317-b094-3ca4-f170-d7aad5962552	[illegible]	All Cameras	[illegible]	Normal
☐	14b53330-9996-d59f-1371-5b86fe71ca22	[illegible]	All Cameras	[illegible]	Normal

Batch Edit ✕

Camera (3)

- Group ✎

Apply Cancel

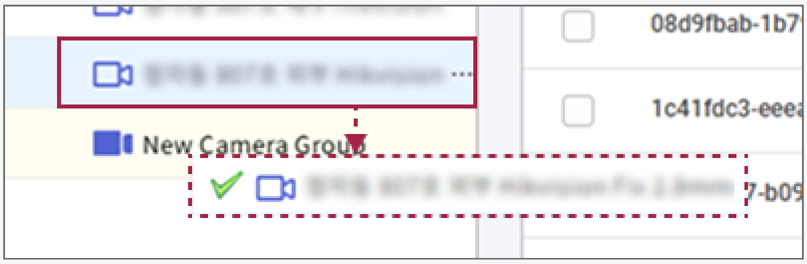
5. When the **Batch Edit** window appears, click the **Group** button of the ✎ item.

6. Select the desired group from the group list.

7. Click the **Apply** button.

ⓘ **INFO**

From the camera list in the **Camera** tab, you can also add cameras to the group by drag and drop.



Edit camera group name

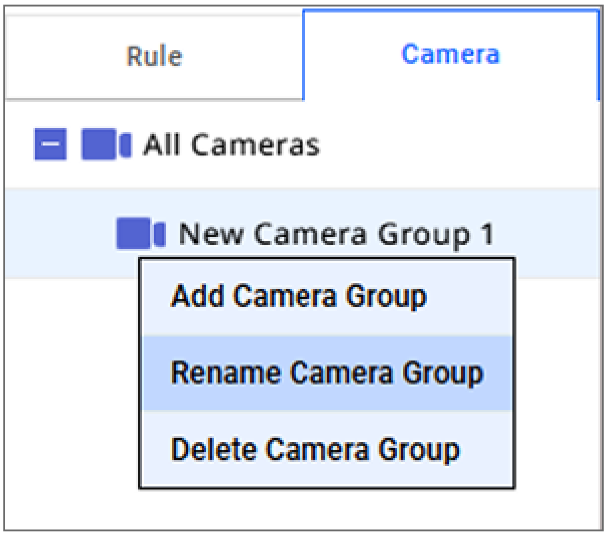
1. Click **Settings** on the **Launcher** page.

2. Click **Video** → **Video** in the left sidebar.

3. Click the **Camera** tab.

4. Select the group you want to rename and right-click.

5. Click **Rename Camera Group** from the popup menu.



6. Enter the desired group name and press the Enter key.

Delete camera group

1. Click **Settings** on the **Launcher** page.
2. Click **Video** → **Video** in the left sidebar.
3. Click the **Camera** tab.
4. Select the group you want to rename and right-click.
5. Click **Delete Camera Group** from the popup menu.
6. Check the warning message and click the **Yes** button.

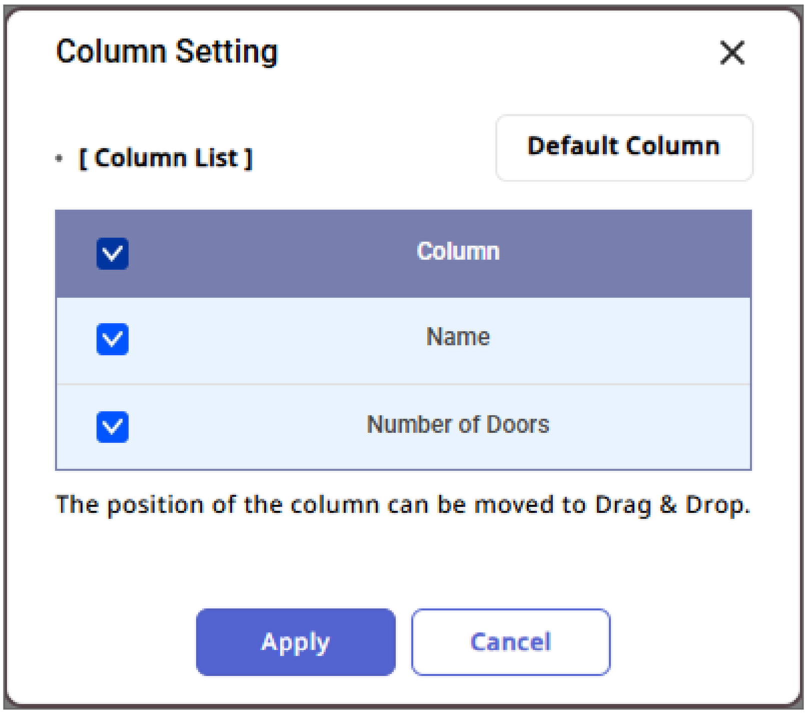
> ⓘ **INFO**
>
> If the camera group contains cameras, you cannot delete the group. Move the cameras belonging to the group to another group or remove them from the group and try again.

Column settings

You can add or change the order of columns to display in the list, or set them to be hidden.

1. Click **Settings** on the **Launcher** page.
2. Click **Video** → **Video** in the left sidebar.
3. In the upper right corner of the **All Cameras** list, click ··· → **Column Setting**.

4. When the **Column Setting** window appears, you can click the checkboxes of the columns you want to display to add or set them to be hidden. You can also change the order of columns via drag and drop.



- [Column List]

☑	Column
☑	Name
☑	Number of Doors

The position of the column can be moved to Drag & Drop.

5. Once you have changed all column settings, click the **Ok** button.

> **INFO**
>
> To initialize the column settings, click the **Default Column** button.

Set Video Rules

Rules are settings to send events and bookmarks to the VMS server by combining events that occur at the camera and door. Proper video rule settings enable the utilization of various security management features.

- **Automatic bookmark creation**: Automatically create bookmarks when specific access events occur to easily find important videos.
- **Efficient monitoring**: Monitor live footage from cameras connected to doors and check events instantly when they occur.
- **Integrated event management**: Link access events and footage to comprehensively understand security situations.

> **INFO**
>
> The video rule feature is available with an **Advanced** license or higher through additional options. For more information on licensing policy, refer to the following.

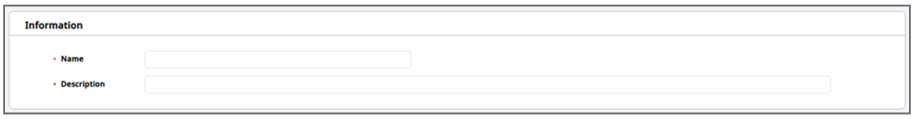
Add rule

1. Click **Settings** on the **Launcher** page.
2. Click **Video** → **Video** in the left sidebar.
3. Click the **ADD RULE** button in the upper left of the screen.

When the **Add New Rule** screen appears, set the rules according to the following instructions. After completing all settings, click the **Apply** button at the bottom of the screen to save.

Enter rule information

In the **Information** section, enter the name and description of the new rule.



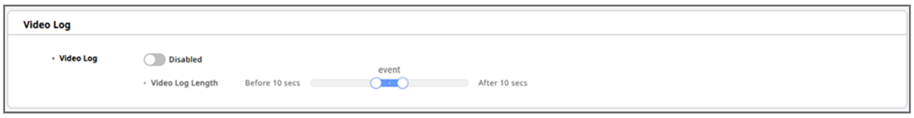
Information

- Name
- Description

> **INFO**
>
> **Description** is optional. Use it to enter a simple description to easily understand the purpose or features of the rule.

Video log settings

Video Log is a feature that automatically records video before and after a specific event occurs. It preserves footage for a designated period to understand the context before and after events.



Video Log

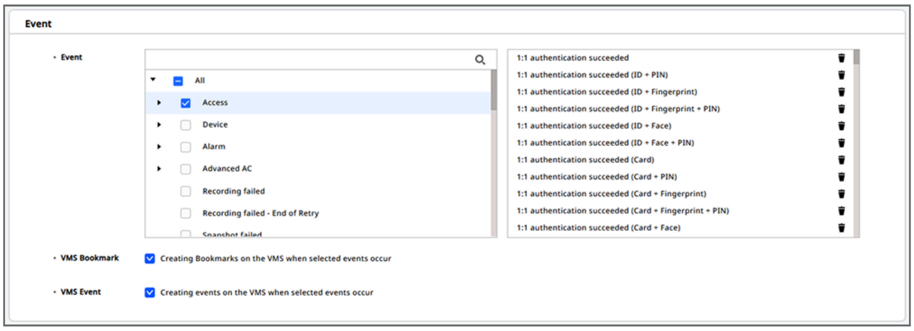
- Video Log: Disabled
- Video Log Length: Before 10 secs — event — After 10 secs

- **Video Log**: Set the usage of Video Log in the current rule.
  - **Enabled**: Automatically records video from the time before and after events occur.
  - **Disabled**: Disables the Video Log feature.
- **Video Log Length**: Set the range of footage to be recorded around ten seconds before and after the event. It can be set up to a maximum of 60 seconds.

> **INFO**
>
> The longer the set range of **Video Log Length**, the more storage space it may require. Consider system performance and storage capacity when setting an appropriate length.

Event settings to be recorded in VMS

In the **Event** section, you can select the events to record on the VMS server and set whether to send bookmarks or events.



Event

- Event
  - All
    - ☑ Access
    - □ Device
    - □ Alarm
    - □ Advanced AC
    - □ Recording failed
    - □ Recording failed - End of Retry
    - □ Snapshot failed

  1:1 authentication succeeded
  1:1 authentication succeeded (ID + PIN)
  1:1 authentication succeeded (ID + Fingerprint)
  1:1 authentication succeeded (ID + Fingerprint + PIN)
  1:1 authentication succeeded (ID + Face)
  1:1 authentication succeeded (ID + Face + PIN)
  1:1 authentication succeeded (Card)
  1:1 authentication succeeded (Card + PIN)
  1:1 authentication succeeded (Card + Fingerprint)
  1:1 authentication succeeded (Card + Fingerprint + PIN)
  1:1 authentication succeeded (Card + Face)
- VMS Bookmark: ☑ Creating Bookmarks on the VMS when selected events occur
- VMS Event: ☑ Creating events on the VMS when selected events occur

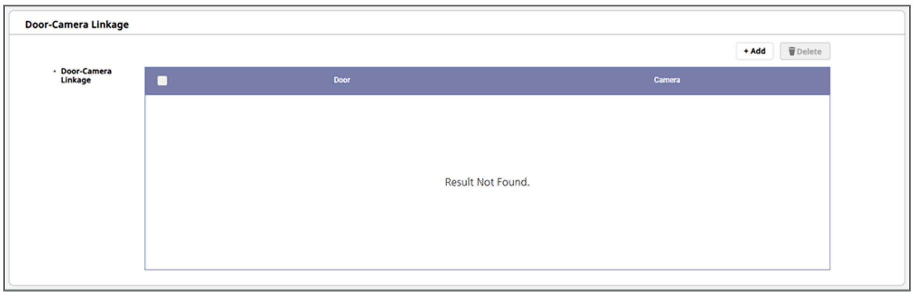
- **Event**: Select the type of event to be sent to the VMS server. When you select the desired event from the left event list, it will be added to the right list.
- **VMS Bookmark**: You can set whether to create a bookmark on the VMS server when the selected event in the event list occurs.
- **VMS Event**: You can set whether to create event records on the VMS server when the selected event in the event list occurs.

INFO

- Selecting events is not mandatory.
- You can quickly find the desired event using the search field at the top of the left event list.
- To remove an event from the right list, click the 🗑 button.
- You can set the language of the message when sending bookmarks and events to the VMS server. For more information, refer to the following.

Linking door and camera

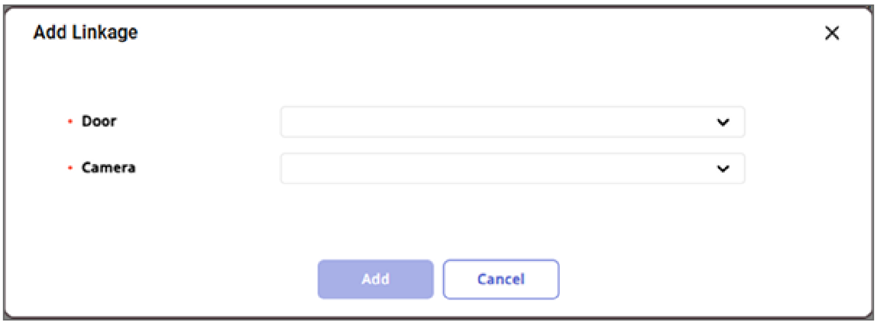
In the **Door-Camera Linkage** section, you can link doors with cameras to send footage from the connected cameras along with events that occur at the doors to the VMS server. This allows you to easily view footage related to access events.


Door-Camera Linkage

■	Door	Camera

Result Not Found.

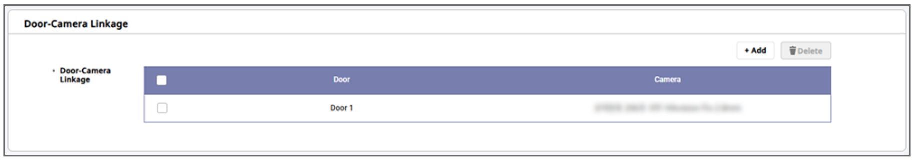
1. Click the **+ Add** button in the upper right.
2. When the **Add Linkage** window appears, select the door and then the associated camera.


Add Linkage

- Door
- Camera

3. Once you have selected both the door and the camera, click the **Add** button.

You can check the cameras linked to the door in the list.


Door-Camera Linkage

■	Door	Camera
□	Door 1	[redacted]

INFO

- A single door can have up to four cameras added.
- Doors included in a rule cannot be used in other rules.
- To delete the linkage rule of doors and cameras, click the checkbox of the items you wish to delete in the list and click the 🗑 **Delete** button in the upper right.
- Cameras linked to doors can be viewed as a substructure of the doors in the **Monitoring** page's door list. For more information, refer to the following.
- After completing all settings, click the **Apply** button at the bottom of the screen to save.

Edit rule

1. Click **Settings** on the **Launcher** page.
2. Click **Video** → **Video** in the left sidebar.
3. Click the rule you want to edit in the **All Rules** list.
4. When the rule editing screen appears, modify the desired items.
5. To save the modified rule, click the **Apply** button in the lower right of the screen.

INFO

For detailed information on each section of the rule editing screen, refer to the following.

Delete rule

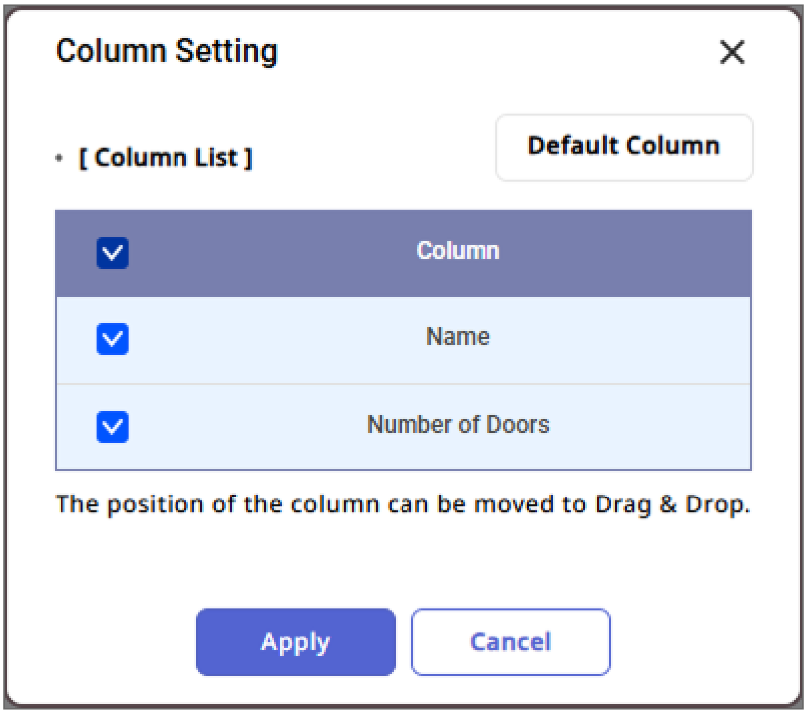
1. Click **Settings** on the **Launcher** page.
2. Click **Video** → **Video** in the left sidebar.
3. Click the checkbox of the rule you want to delete in the **All Rules** list. You can select one or more rules.
4. Click the 🗑 **Delete Rule** button in the upper right of the screen.
5. Check the message and click the **Yes** button.

Column settings

You can add or change the order of columns to display in the list, or set them to be hidden.

1. Click **Settings** on the **Launcher** page.
2. Click **Video** → **Video** in the left sidebar.

3. In the top right of the **All Rules** list, click ••• → **Column Setting**.
4. When the **Column Setting** window appears, you can click the checkboxes of the columns you want to display to add or set them to be hidden. You can also change the order of columns via drag and drop.



☑	Column
☑	Name
☑	Number of Doors

The position of the column can be moved to Drag & Drop.

5. Once you have changed all column settings, click the **Ok** button.

INFO

To initialize the column settings, click the **Default Column** button.

Manage Map

Map settings allow you to set and manage floors, facilities, and zones in conjunction with the map. Use this feature to view a map segmented by zones, facilities, and floors on the **Monitoring** page.

Configure Floors

Configure floors before configuring zones and facilities. Place doors and cameras on the floor image to visually confirm.

Configure Facility

Configure facilities and arrange floors. Arrange floors sequentially to represent the actual layout of the facility.

Configure Area

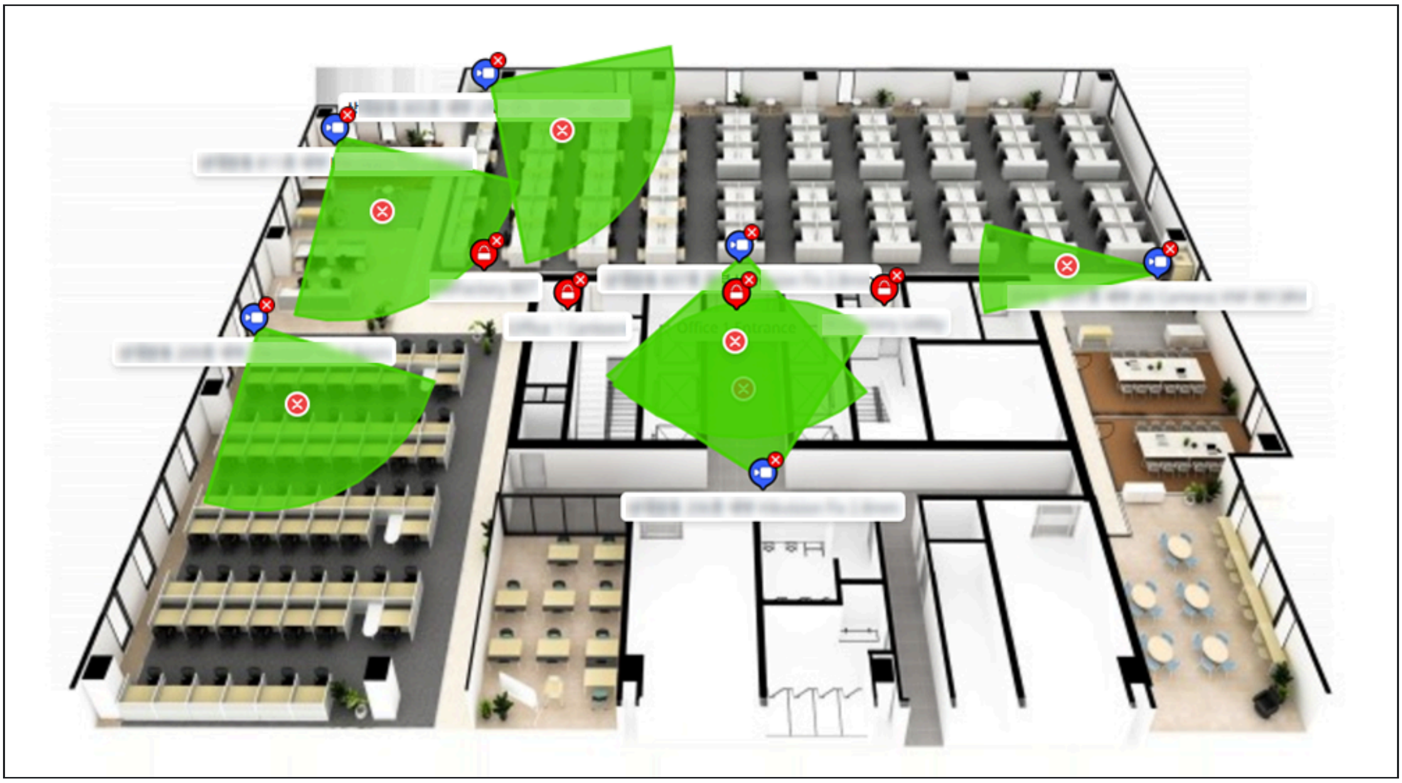
Complete the floor and facility configuration to set up the area. Verify secured areas through the map.

INFO

- For more information about map monitoring, refer to the following.
- The map settings and map monitoring features is only available with an **Advanced** or higher license.

Configure Floors

Configure floors before configuring zones and facilities. Upload the floor layout as an image and place doors and cameras for visual management. After configuring a floor, check the doors and cameras for that floor on the **Monitoring** page.



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

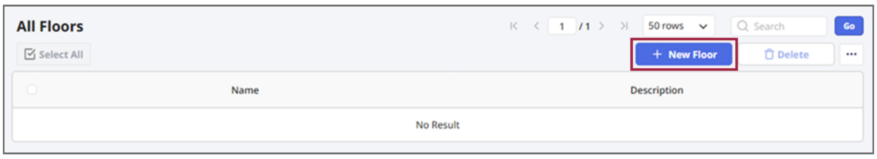
> **INFO**
>
> - Register doors before configuring floors. For more information about door enrollment, refer to the following.
> - For more information about map monitoring, refer to the following.
> - Map settings and map monitoring feature can be used via additional options with an **advanced** license or higher. For more information on licensing policy, refer to the following.

Add floor

Upload a floor layout or a 3D bird’s eye view image to add a floor and place doors and cameras.

1. Click **Settings** on the **Launcher** page.
2. In the left sidebar, click **Map** → **Floor**.

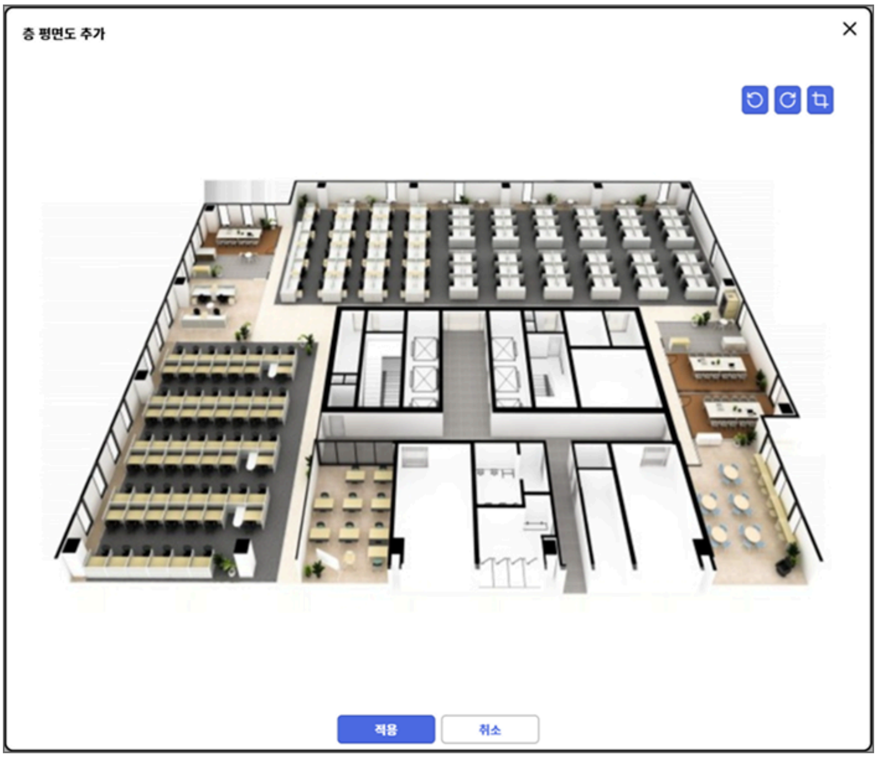
3. Click **New Floor** in the upper right corner of the floor list screen.



4. Enter the name and description of the floor you want to add in the **Add New Floor** screen's **Information** section.

5. Click **Floor Plan** in the **Floor Configuration** section or drag and drop the image to upload.

6. Confirm the uploaded image in the **Add Floor Plan** window and proceed with the settings.

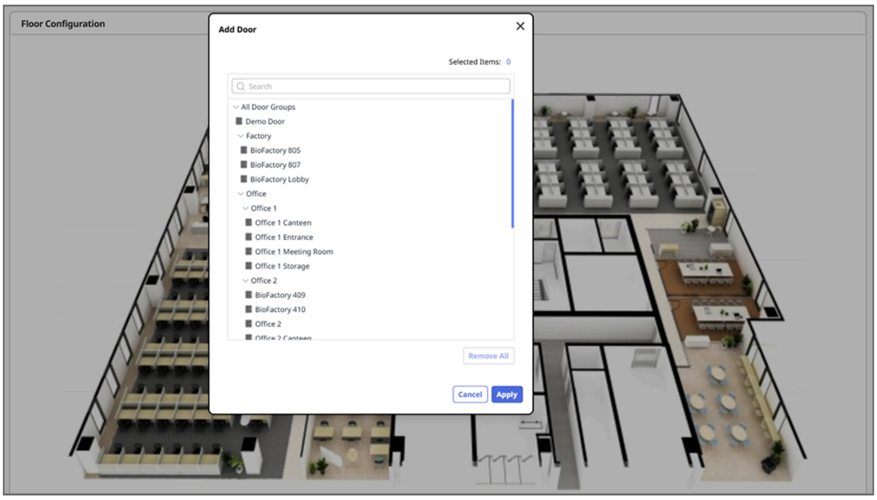


- To rotate the image, click ↺ or ↻.
- To crop the image, click ⌐.

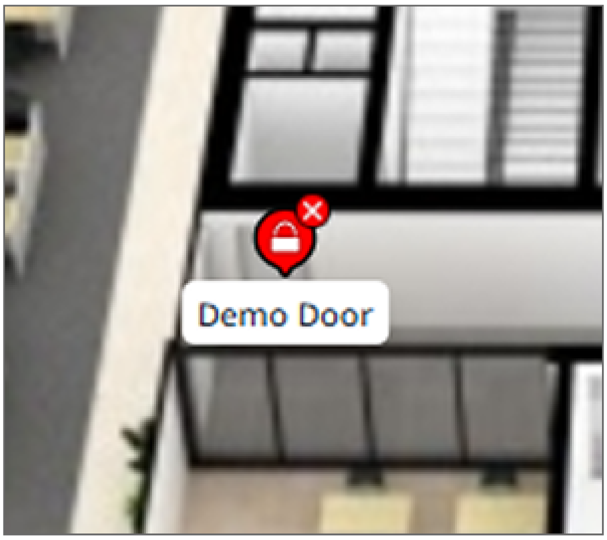
7. After completing the image settings, click **Apply**.

8. To add a door to the uploaded image in the **Floor Configuration** section, right-click on the desired location in the image and select **Add Door**.

9. When the **Add Door** window appears, select one of the registered doors.

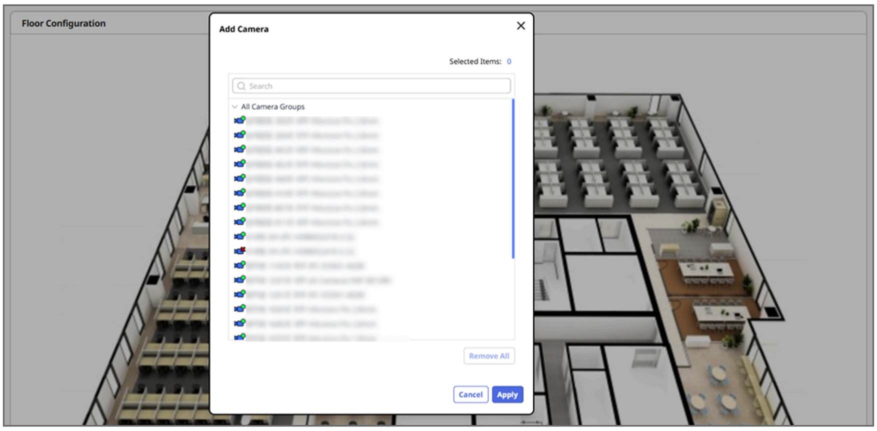


10. To place the door in the image, click **Apply**.

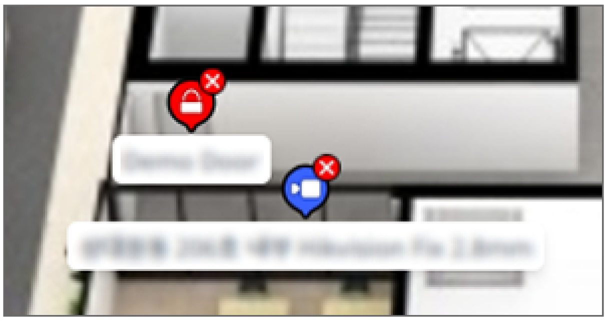


11. To add a camera to the uploaded image, right-click on the desired location in the image and select **Add Camera**.

12. When the **Add Camera** window appears, select one of the registered cameras.



13. To place the camera in the image, click **Apply**.



14. Additionally place doors and cameras as needed in the actual floor.

15. To save the configured floor settings, click **Apply** after completing all settings.

> **INFO**
>
> - To change the position of doors and cameras placed on the floor, click and drag the respective door or camera to the desired location.
> - For more information on the icons and status of the doors and cameras placed on the floor, refer to the following.

Modify floor configuration

You can modify the layout of the floor with added doors and cameras. Modifying the floor layout allows you to change or delete the positions of doors and cameras.

1. Click **Settings** on the **Launcher** page.
2. In the left sidebar, click **Map** → **Floor**.
3. Click the floor you want to modify from the list.

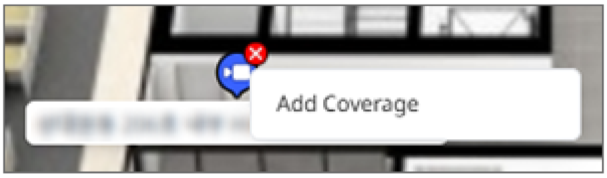
After completing all settings and saving the configured floor, click **Apply**.

Delete door/camera

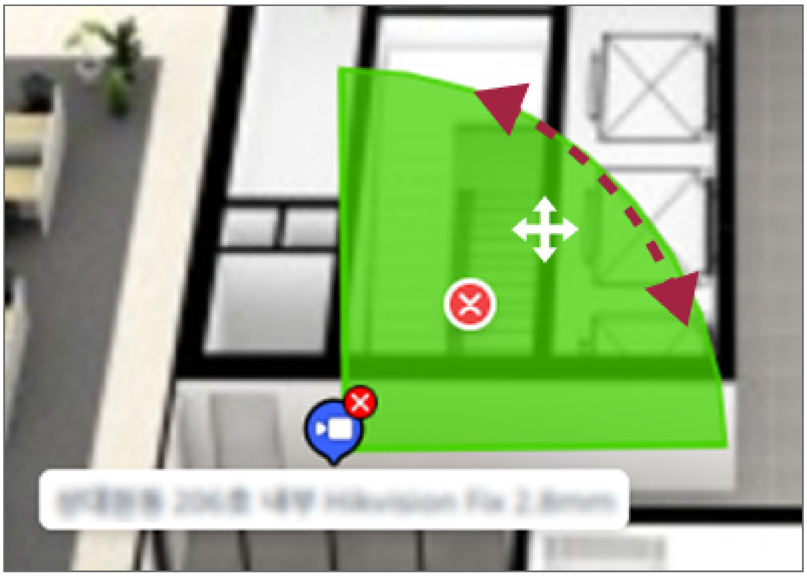
Click the ⊗ icon for the door or camera you want to delete from the floor image. You can delete the respective door or camera.

Set camera shooting range

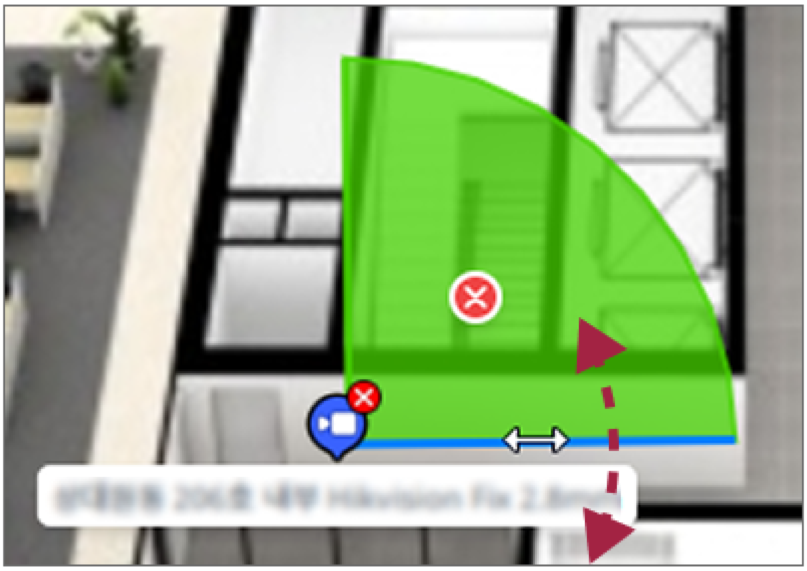
Right-click on the camera you want to set the shooting range for in the floor image. Click **Add Coverage** in the popup menu.



- To change the shooting range, move the mouse pointer into the green area. When the mouse pointer changes to a cross shape, click and drag to the desired location while holding the mouse button down.



- To adjust the coverage area, hold the edge of the range and drag to resize.



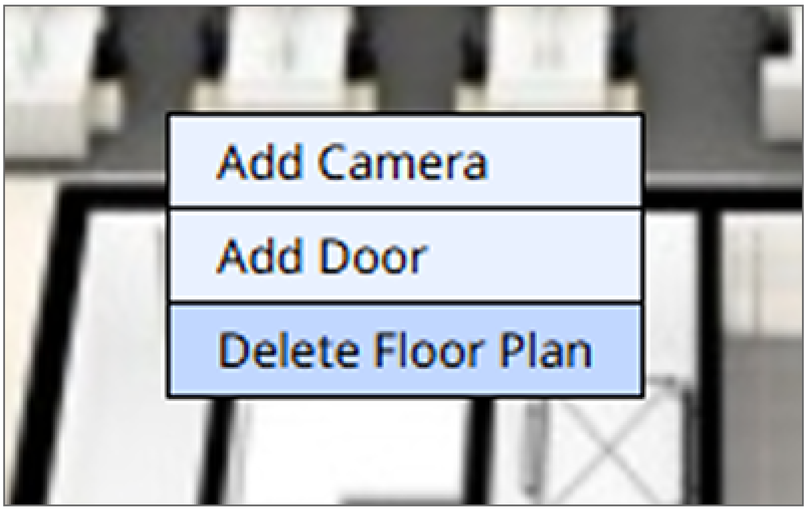
- To delete the coverage area, click the ⊗ icon.

⚠ **CAUTION**

Settings made by the user are only features provided for the convenience of security management and do not reflect the actual shooting range of the camera.

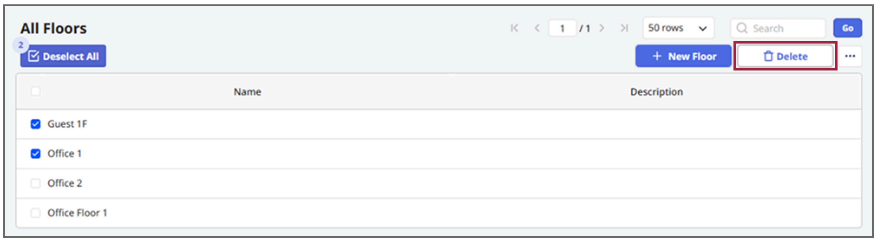
Delete floor image

To delete the floor image, right-click on the floor image and select **Delete Floor Plan** from the popup menu.



Delete floor

1. Click **Settings** on the **Launcher** page.
2. In the left sidebar, click **Map** → **Floor**.
3. Click the checkbox of the floor you want to delete from the list. You can select more than one floor.



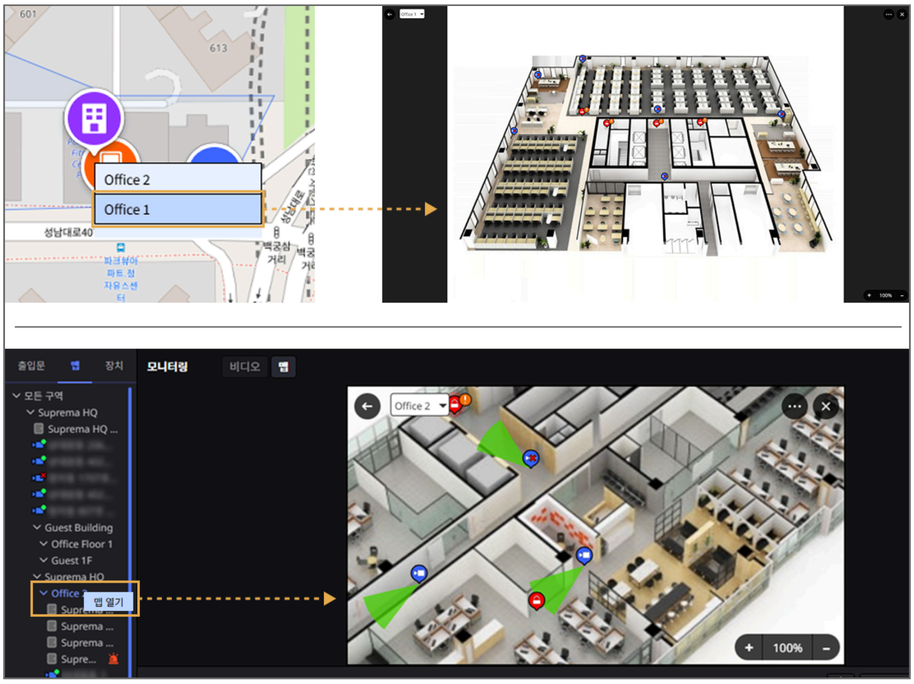
□	Name	Description
☑	Guest 1F	
☑	Office 1	
□	Office 2	
□	Office Floor 1	

4. Click **Delete** at the top right of the screen.

The selected floors will be deleted from the list. The deleted floors cannot be recovered.

Configure Facility

Configure facility and arrange floors. Arrange floors sequentially to represent the actual layout of the facility. Configuring facilities provides the feature to select facilities placed on the map in the **Monitoring** page and enter each floor for monitoring.



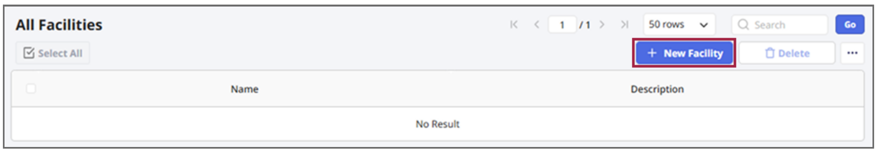
INFO

- Register floors before configuring facilities. For more information about floor registration, refer to the following.
- For more information about map monitoring, refer to the following.
- Map settings and map monitoring feature can be used via additional options with an **advanced** license or higher. For more information on licensing policy, refer to the following.

Add facility

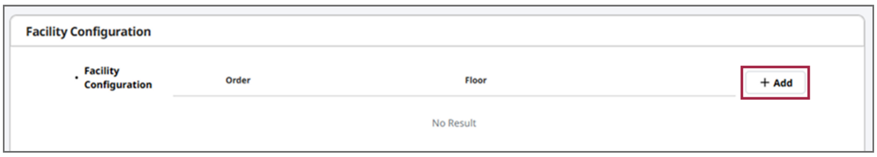
Follow these steps to design the structure by adding floors to the facility.

1. Click **Settings** on the **Launcher** page.
2. Click **Map** → **Facility** in the left sidebar.
3. Click **New Facility** in the upper right of the facility list screen.

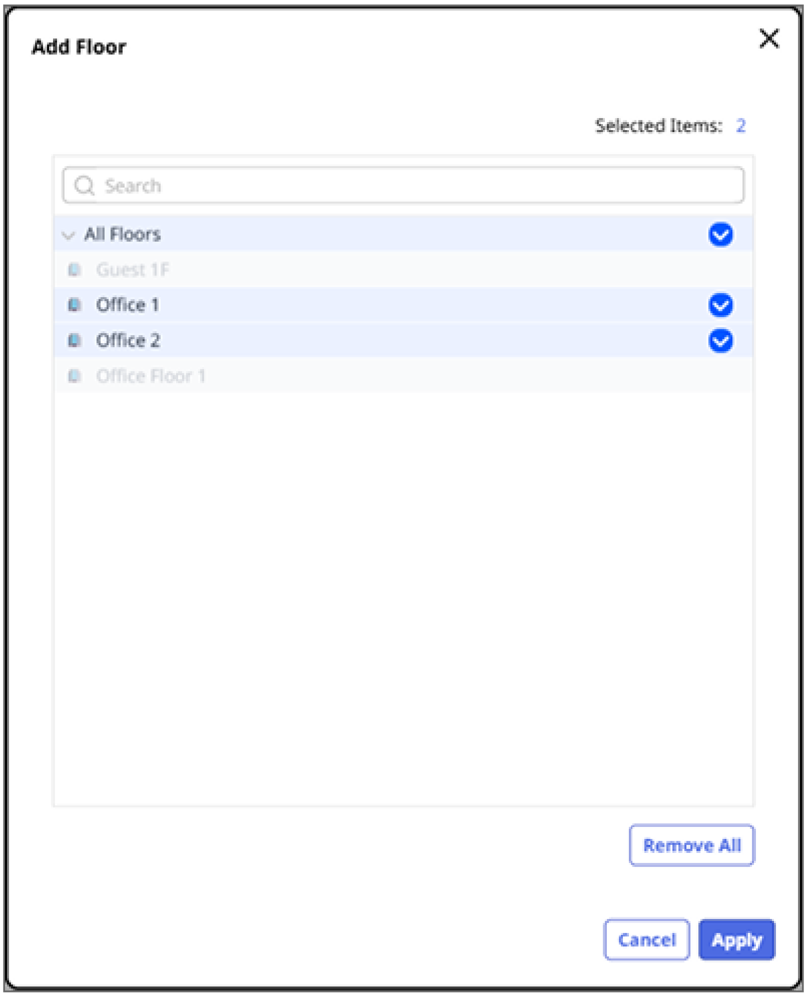


4. Enter the name and description of the facility you want to add in the **Information** section of the **Add New Facility** screen.

5. Click **Add** in the **Facility Configuration**.



6. When the **Add Floor** window appears, select the floor you want to add from the list of floors.



- You can also get floors by entering keywords in the input field.
- To select all floors, choose **All Floors**.

7. If you have selected all floors, click **Apply**.

8. To check the floors added to the access door list and change the order, drag the ⠿ icon in the **Order** column to change the order.

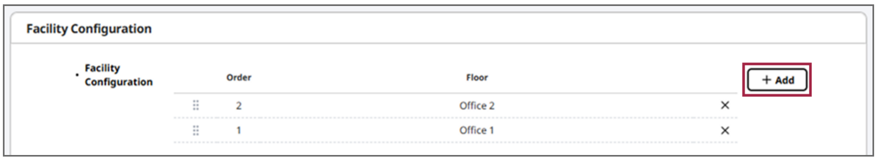
9. To complete the facility configuration and save, click the **Apply** button at the bottom right of the screen.

Modify facility

Add floors to existing facilities

You can add floors to an already created facility.

1. Click **Settings** on the **Launcher** page.
2. Click **Map** → **Facility** in the left sidebar.
3. Select the facility to which you want to add floors from the facility list.
4. Click **Add** in the **Facility Configuration**.



Facility Configuration

- Facility Configuration

	Order	Floor	+ Add
⠿	2	Office 2	×
⠿	1	Office 1	×

5. When the **Add Floor** window appears, click the checkbox of the floor to select.
6. If you have selected all floors, click **Apply**.
7. To check the floors added to the access door list and change the order, drag the ⠿ icon in the **Order** column to change the order.
8. To complete the facility configuration and save, click the **Apply** button at the bottom right of the screen.

Delete floors from the facility

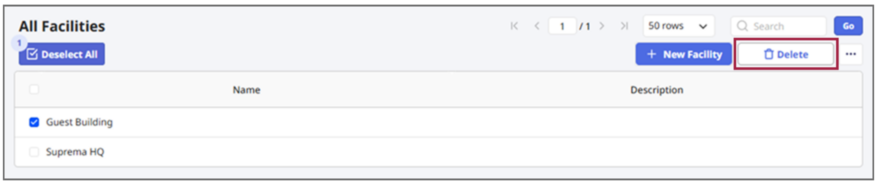
You can delete floors from an already created facility.

1. Click **Settings** on the **Launcher** page.
2. Click **Map** → **Facility** in the left sidebar.
3. Select the facility from which you want to delete floors in the facility list.
4. Click the × button of the floor you want to delete in **Facility Configuration**.
5. To complete the floor deletion and save, click the **Apply** button at the bottom right of the screen.

Delete facility

1. Click **Settings** on the **Launcher** page.
2. Click **Map** → **Facility** in the left sidebar.

3. Click the checkbox of the facility you want to delete in the facility list.



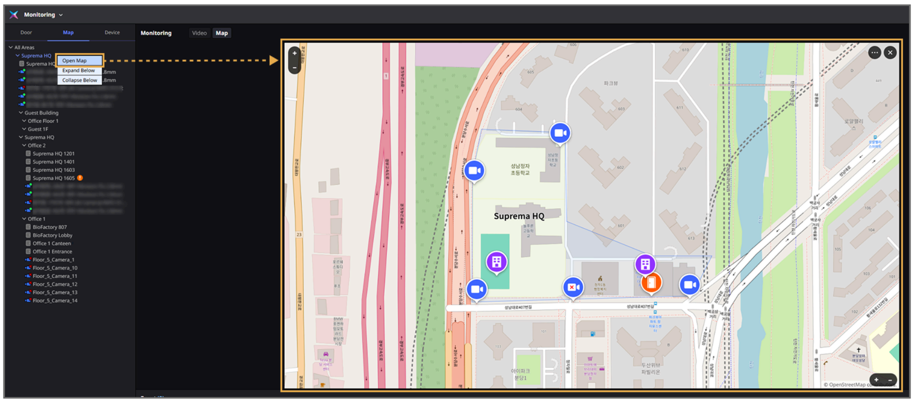
□	Name	Description
☑	Guest Building	
□	Suprema HQ	

4. Click **Delete** at the top right of the screen.

5. When the confirmation message window appears, click **Yes**.

Configure Area

Complete the floor and facility configuration to set up the area. Verify secured areas through the map. Configuring zones provides functionality to access and monitor the facilities and floors in the respective zone on the **Monitoring** page.

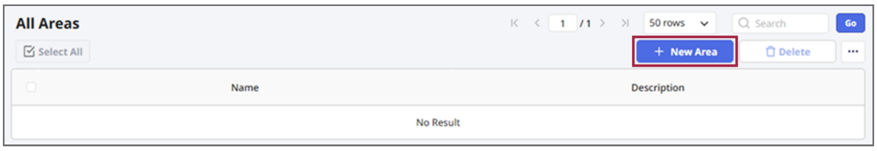


> **INFO**
>
> - Register floors and facilities before configuring zones. For more information about registering floors and facilities, refer to the following:
>   - Configure Floors
>   - Configure Facility
> - For more information about map monitoring, refer to the following.
> - Map settings and map monitoring feature can be used via additional options with an **advanced** license or higher. For more information on licensing policy, refer to the following.

Add zone

Configure and manage zones of the security areas you are currently managing via the map.

1. Click **Settings** on the **Launcher** page.
2. Click **Map** → **Area** on the left sidebar.
3. Click the **New Area** button in the upper right of the area list screen.



All Areas

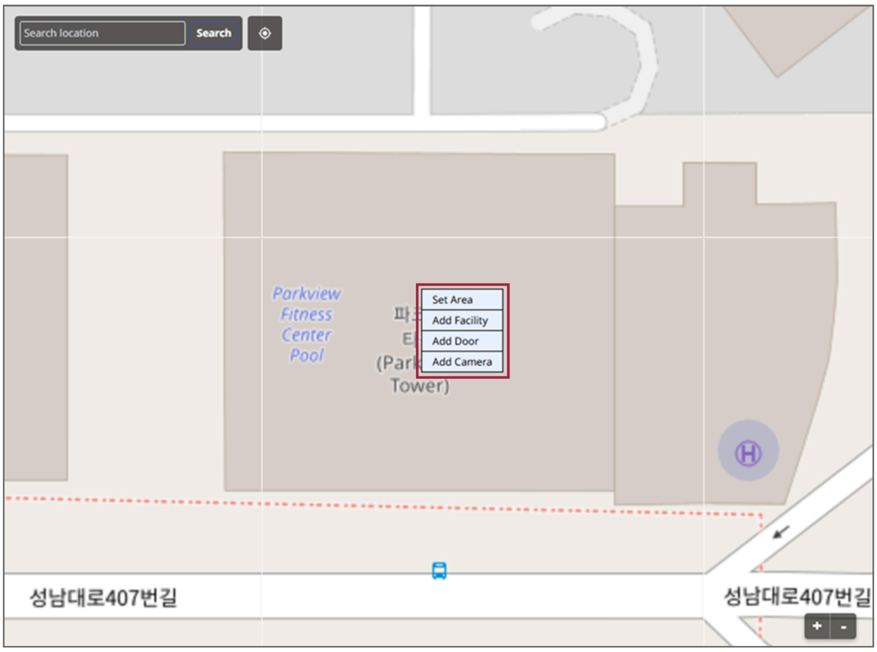
1 /1 50 rows Search Go

☐ Select All + New Area Delete ···

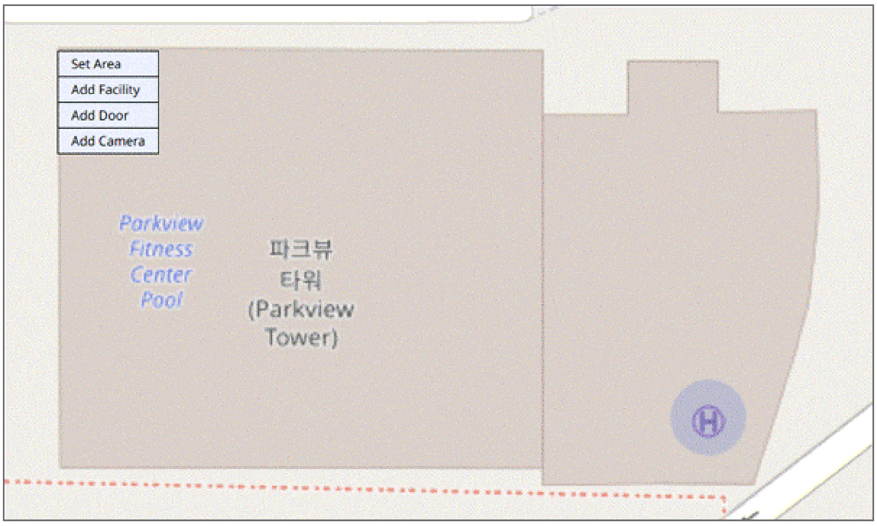
☐	Name	Description
No Result		

4. Enter the name and description of the area you want to add in the **Information** section of the **Add New Area** screen.
5. Set the location of the zone to add on the map in the **Area Configuration** section.

6. Right-click on the map and select **Set Area**.

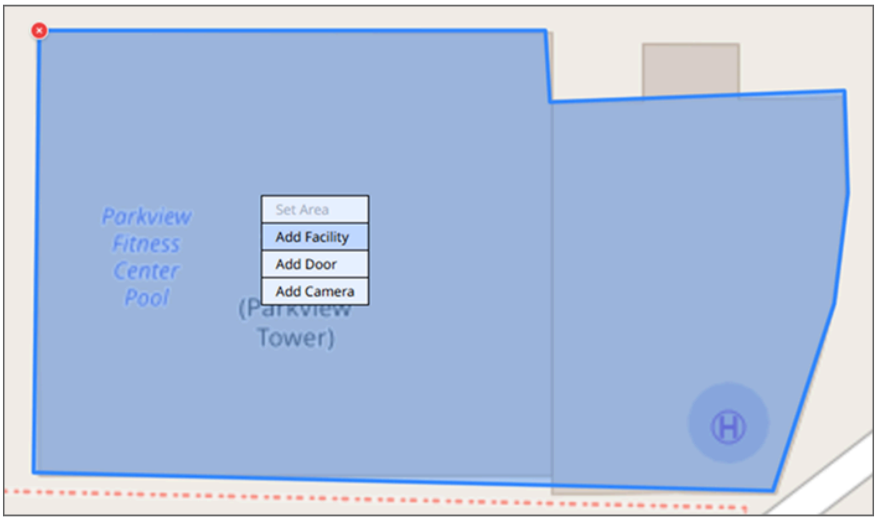


7. Set the zone in your desired shape. Click the mouse to start drawing and drag to set the zone.



> ⓘ To reset the area, you must delete the configured area. To delete the area, click the ⊗ button.

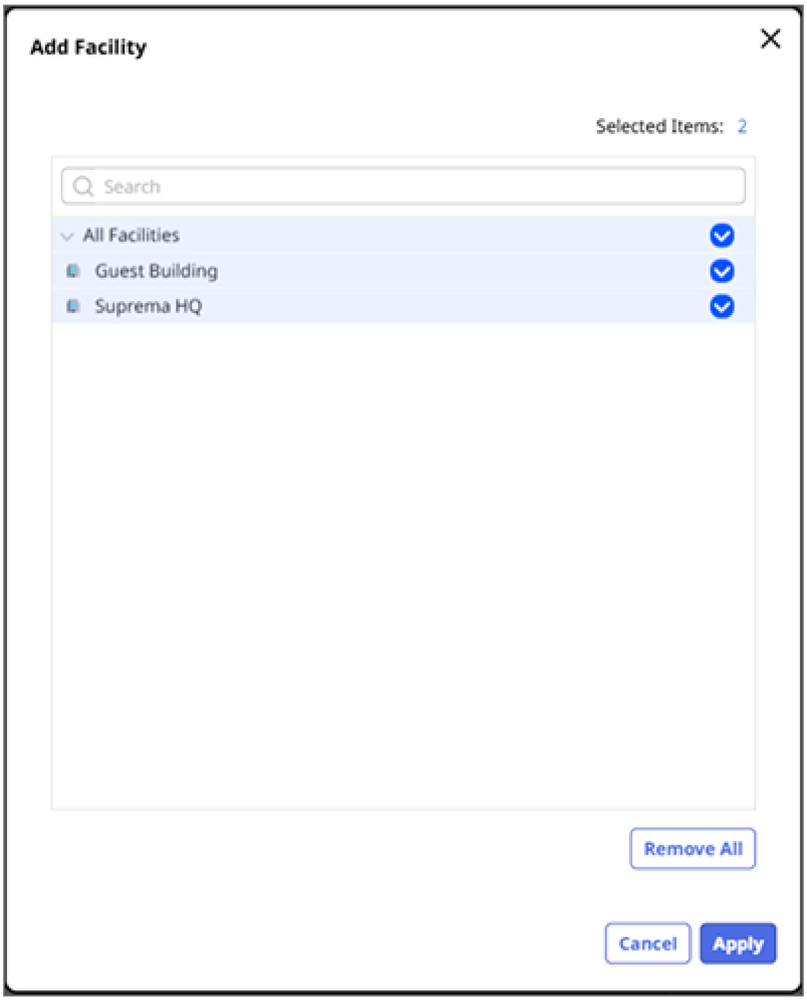
8. To add facilities to the configured area, right-click and select **Add Facility**.



ⓘ When adding a zone, at least one facility, entrance, or camera must be configured.

- To add an entrance, right-click and select **Add Door**.
- To add a camera, right-click and select **Add Camera**.

9. When the **Add Facility** window appears, select the facility to add and click **Apply**.

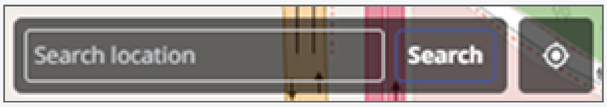


Add Facility

Selected Items: 2

> ⓘ When adding an entrance or camera, the **Add Door** or **Add Camera** window will also appear. Select the item to add and click **Apply**.

10. Once the area settings are complete, click the **Apply** button in the lower right of the screen.

> **INFO**
>
> - You can search for your desired location using the input field at the top left of the map. Click ⌖ to return to the current location.
>
> 
>
>
>
> - When adding a zone on the map, it can only be set as a single polygon. When setting a zone, ensure that the start and end points are the same. Once configured, the shape of the zone cannot be changed. To modify the zone, you must delete it and re-add it.
> - The positions of the added facilities, entrances, and cameras can be changed via drag-and-drop on the map.

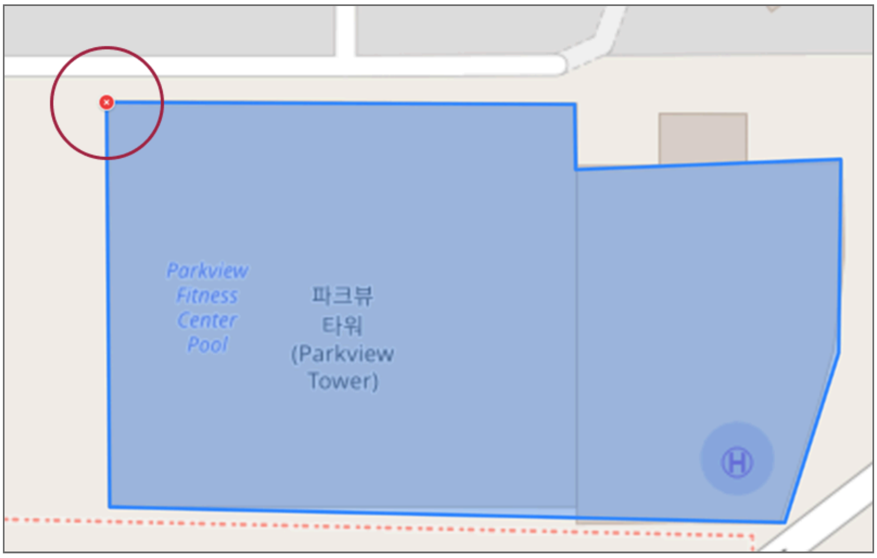
Edit zone

You can delete and reconfigure existing zones or add or remove facilities, entrances, and cameras.

Reset zone

To reset a zone on the map, you must delete the existing zone and re-add it.

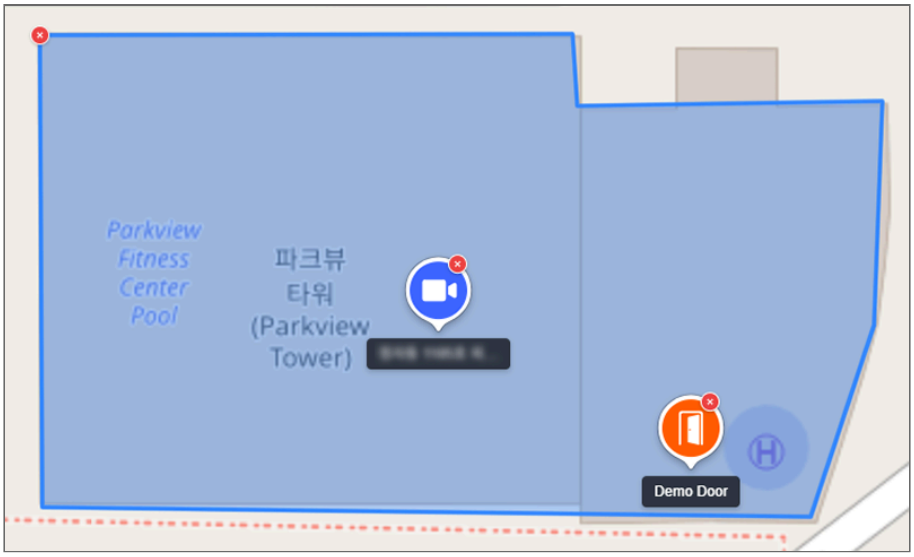
1. Click **Settings** on the **Launcher** page.
2. Click **Map** → **Area** on the left sidebar.
3. Select the zone you want to reset from the zone list.
4. In the map under the **Area Configuration** section, click the ⊗ button at the top left of the already created area.



5. Right-click on the map and select **Set Area** from the popup menu.
6. To set the area as desired and save, click the **Apply** button in the lower right of the screen.

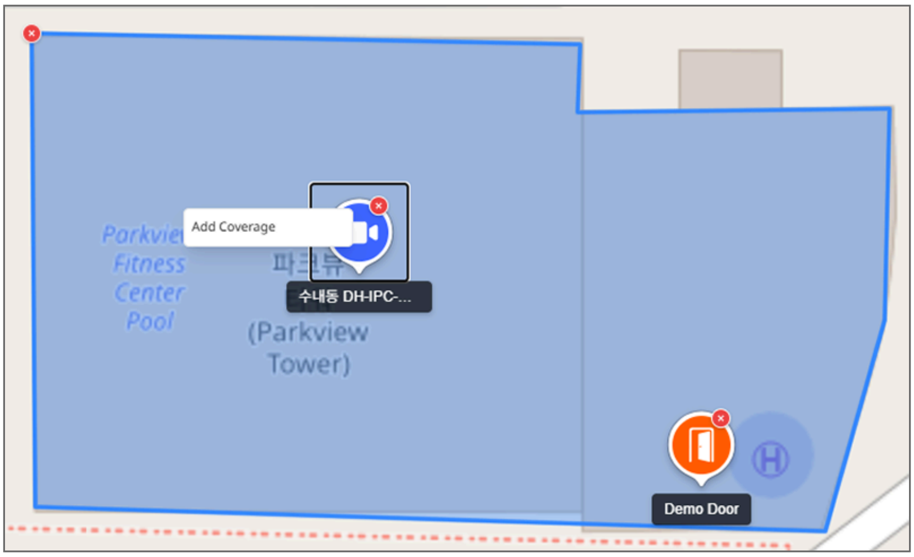
Delete facility/entrance/camera

Click the facility, entrance, or camera you want to delete on the map. The ⊗ icon will appear. Click the icon to delete the selected facility.

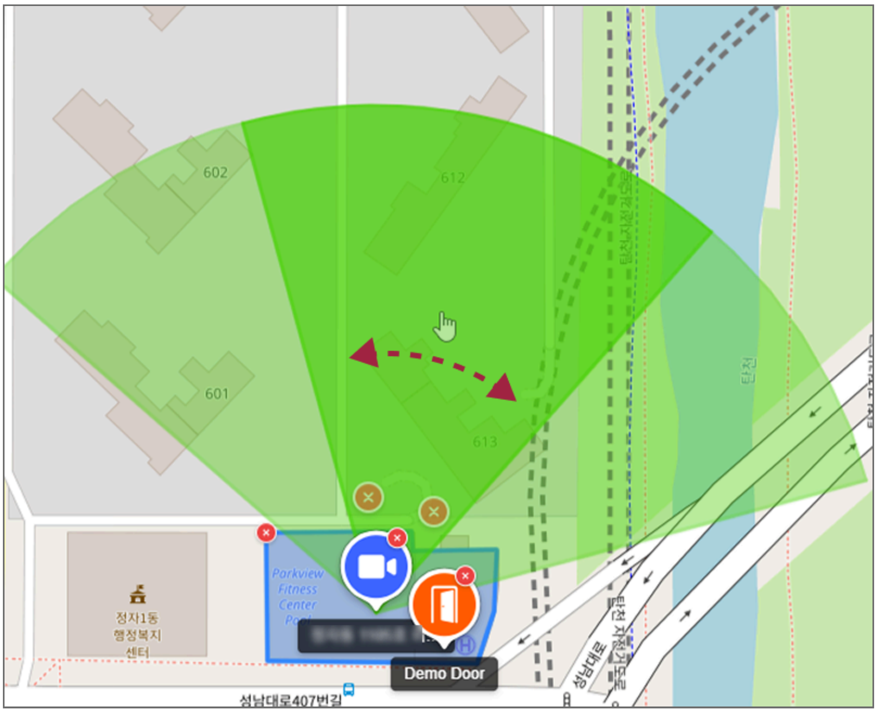


Set camera coverage

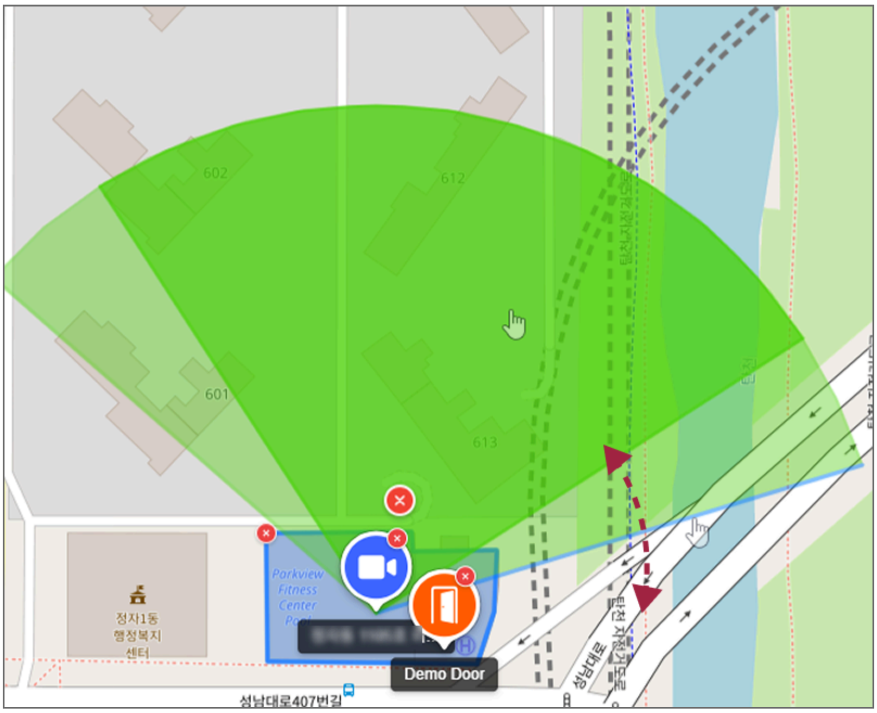
You can set the camera coverage area on the map. Right-click the icon where the camera is placed and select **Add Coverage**.



- To change the shooting range, click and drag the green area's shooting range in the desired direction.



- To adjust the coverage area, hold the edge of the range and drag to resize.



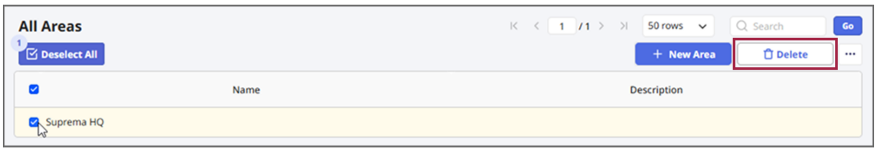
- To delete the coverage area, click the ⊗ icon.

⚠ CAUTION

Settings made by the user are only features provided for the convenience of security management and do not reflect the actual shooting range of the camera.

Delete zone

1. Click **Settings** on the **Launcher** page.
2. Click **Map** → **Area** on the left sidebar.
3. Check the checkbox of the zone you want to delete from the zone list.



4. Click **Delete** at the top right of the screen.
5. When the confirmation message window appears, click **Yes**.

Set Visitor

You can configure visiting sites and PCs. You can also set the terms and conditions for visitors. And You can create the information fields that you want to know from the visitors by using the Custom Visitor Field.

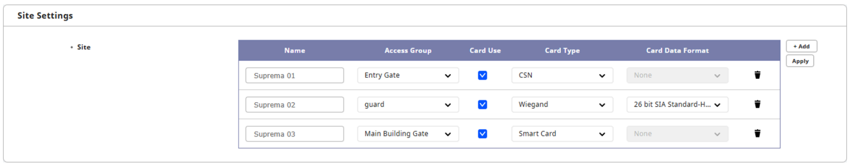
> **INFO**
>
> - The **Visitor** setting is available through additional options with an **Advanced** license or higher. For more information on licensing policy, refer to the following.
> - Activate the **Automatic User Synchronization** or **Use Server Matching** option to use the **Visitor**. For more information, refer to the following.

Visitor settings

1. Click **Settings** on the **Launcher** page.
2. In the left sidebar, click the **Visitor**.
3. Follow the instructions below to configure visitor settings.

1 Visitor site settings

You can set the access group to use in the visiting PC and managing PC of each site. You can also set whether or not to use cards. If you are using a card, you can also set Card Type and Card Data Format.



Site Settings

- Site

Name	Access Group	Card Use	Card Type	Card Data Format	
Suprema 01	Entry Gate	☑	CSN	None	🗑
Suprema 02	guard	☑	Wiegand	26 bit SIA Standard-H...	🗑
Suprema 03	Main Building Gate	☑	Smart Card	None	🗑

- **Name**: You can set the name of site.

> **INFO**
>
> – Up to 48 characters may be entered for a site name.

- **Access Group**: You can select the access group to assign to the visitor.

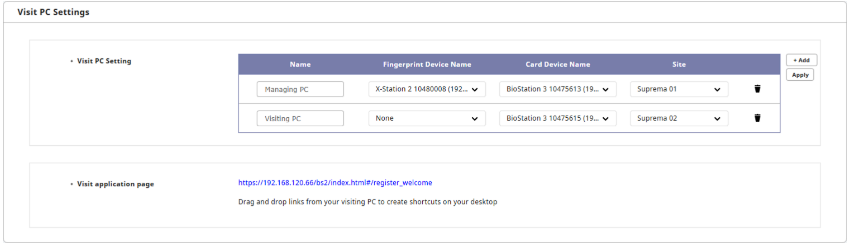
> **INFO**
>
> Pre-setting access groups for visitors makes management easier. For more information on access group settings, refer to the following.

- **Card Use**: You can set whether or not to use a card.
- **Card Type**: You can select the type of card to use in the site. The card type is activated only when you select **Card Use**.
- **Card Data Format**: You can configure the format for reading card data. The **Card Data Format** is activated only when you set the **Card Type** to **Wiegand**.

Click **Apply** to save visitor site settings.

2 Visitor PC settings

You can set the visiting PC and managing PC.



Visit PC Settings

- Visit PC Setting

Name	Fingerprint Device Name	Card Device Name	Site
Managing PC	X-Station 2 10480008 (192...	BioStation 3 10475613 (19...	Suprema 01
Visiting PC	None	BioStation 3 10475615 (19...	Suprema 02

- Visit application page

https://192.168.120.66/bs2/index.html#/register_welcome

Drag and drop links from your visiting PC to create shortcuts on your desktop

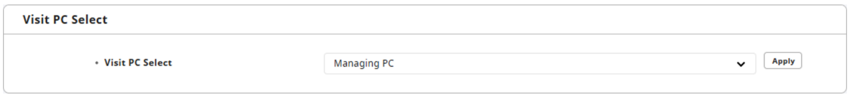
- **Name**: You can set the name of the visiting PC and managing PC.
- **Fingerprint Device Name**: Select a device to enroll visitors' fingerprints when visitors access the site using the fingerprint authentication.
- **Card Device Name**: Select a device to issue the card to visitors when visitors access the site using the card authentication. The card device name is only activated if you have set a visit where you have selected to use the card.
- **Site**: Select a site to manage the visit on the visiting PC.

Click **Apply** to save the setting of the Visit PC Setting.

> **INFO**
>
> - Up to 48 characters may be entered for a name of the visiting PC.
> - You can use the fingerprint and card device at the same time. You can select only one for each.
> - You can only select one site per PC.

3 Select visitor PC

You can select the PC set in **Visit PC Setting** and assign it to the current PC.



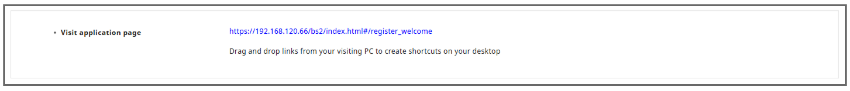
Visit PC Select

- Visit PC Select: Managing PC

Click **Apply** to save the settings.

4 Shortcut to visitor application page

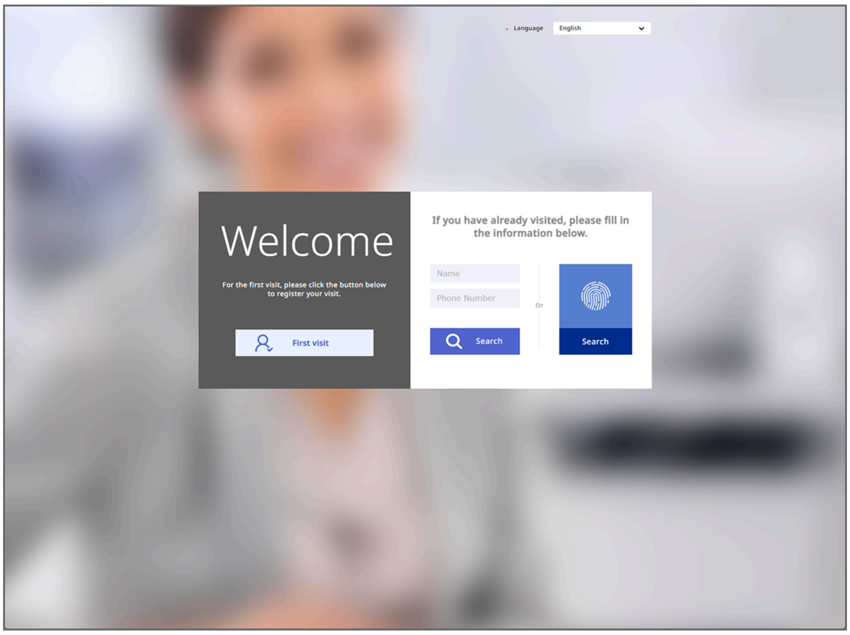
You can create a shortcut icon for the visitor application page on the desktop of the application PC. Drag the URL of **Visit application page** item to the desktop.



- Visit application page: https://192.168.120.66/bs2/index.html#/register_welcome

Drag and drop links from your visiting PC to create shortcuts on your desktop

You can access the visitor application page by connecting to the URL in a web browser.

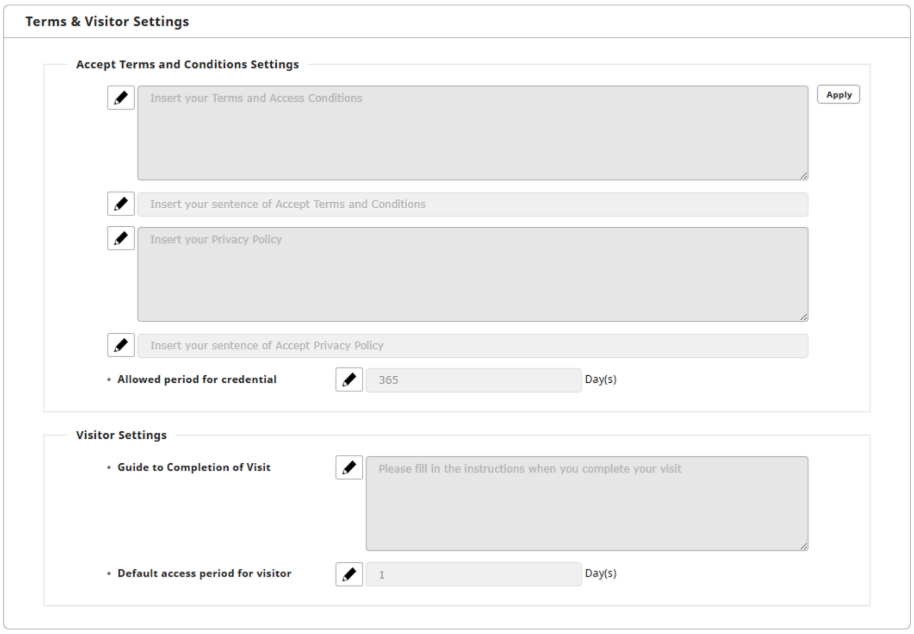


- Language: English

Welcome
For the first visit, please click the button below to register your visit.
First visit
If you have already visited, please fill in the information below.
Name
Phone Number
Or
Search
Search

Terms & set visitor

You can manage key visitor settings such as terms of entry, privacy policy, and guidance messages.



Terms & Visitor Settings

Accept Terms and Conditions Settings

✎ Insert your Terms and Access Conditions — Apply

✎ Insert your sentence of Accept Terms and Conditions

✎ Insert your Privacy Policy

✎ Insert your sentence of Accept Privacy Policy

- Allowed period for credential ✎ 365 Day(s)

Visitor Settings

- Guide to Completion of Visit ✎ Please fill in the instructions when you complete your visit
- Default access period for visitor ✎ 1 Day(s)

- **Terms and Conditions**: You can set the terms and conditions for visitors. Click ✎ to activate the input field and enter the contents of terms and conditions.

> **INFO**
>
> – Up to 65,535 characters may be entered for the sentence of terms and conditions.
>
> – Up to 64 characters may be entered for the sentence of accept terms and conditions.

- **Privacy Policy**: You can set the privacy policy for visitors. Click ✎ to activate the input field and enter the privacy policy.

> **INFO**
>
> – Up to 65,535 characters may be entered for the sentence of privacy policy.
>
> – Up to 64 characters may be entered for the sentence of accept privacy policy.

- Allowed period for credential: You can set the period for keeping personal data that visitors provide when they visit. Click ✎ to activate the input field and enter the number of days to keep personal data.

> **INFO**
>
> – You can delete the visitors that have the personal data expired in Visitor menu.

- Guide to Completion of Visit: You can set the guide to appear on the screen as a pop-up when a visitor completes an application for a visit. Click ✎ to activate the input field and enter the guide for visitors.

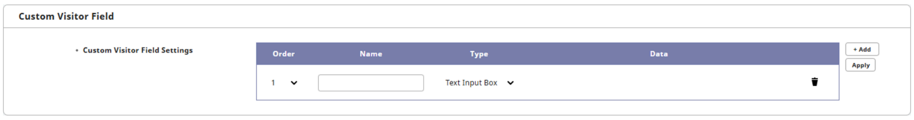
ⓘ **INFO**

- Up to 65,535 characters may be entered for the sentence of guide.
- If you do not enter the sentence of a guide, nothing will be displayed on the screen when visitors complete their visit application.

- **Default access period for visitor**: You can set the access period for visitors. Click ✎ to activate the input field and enter the default access period for visitors.

Set custom visitor fields

You can add custom visitor fields for extra visitor information and these fields appear on the visit application page.



Custom Visitor Field

- Custom Visitor Field Settings

Order	Name	Type	Data
1 ⌄		Text Input Box ⌄	

- **Order**: You can set the order of the Custom Visitor Field.
- **Name**: You can set the name of the Custom Visitor Field.
- **Type**: You can choose the Text Input Box, Number Input Box or Combo Box.
- **Data**: Enter the options to appear in the combo boxes. Each item is separated by a semicolon (;). Data is only activated when **Type** is set to **Combo Box**.

Click **Apply** to save the settings.

ⓘ **INFO**

- For a **Text Input Box**, characters and numbers are allowed.
- For a **Number Input Box**, numbers are allowed and characters are not allowed.
- For a **Combo Box**, the items that have been set to the field are displayed as item. If you want to configure a combo box field as shown in the screenshot below, you need to enter **Option 1**; **Option 2**; **Option 3**; **Option 4** in the data field.

Directory Integration Settings

This document provides guidance on how to synchronize and manage users by integrating **Microsoft Entra ID** (hereafter **Entra ID**) or **Active Directory** with **BioStar X**.

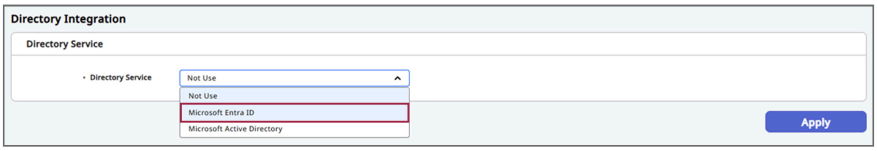
Integrating with **Entra ID** or **Active Directory** provides the following convenient features, enhancing both security and usability. This enhances both security and convenience.

- You can log in to BioStar 2 using your **Entra ID** account via Single Sign-On (SSO) provided by **Entra ID**.
- You can log in to **BioStar X** using Lightweight Directory Access Protocol (LDAP) authentication provided by **Active Directory**.
- Users and groups configured in **Entra ID** or **Active Directory** can be synchronized with **BioStar X**.
- You can map user information such as job title, department, and group used in **Entra ID** or **Active Directory** to the custom fields of **BioStar X**.

> **INFO**
>
> The **Entra ID** or **Active Directory** settings feature is available through additional options on the **Advance** license and above. For more information on licensing policy, refer to the following.

Integrate with Entra ID

1. Log in to **BioStar X** with an administrator account.
2. Click Settings on the Launcher page.
3. Click Directory Integration in the left sidebar of the screen.
4. Select Microsoft Entra ID in Directory Service.



Directory Integration

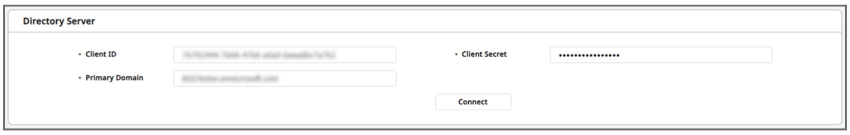
Directory Service

- Directory Service: Not Use

5. Set each item as instructed below.

1 Directory Server

Enter the server information for **Entra ID** and click Connect in Directory Server.

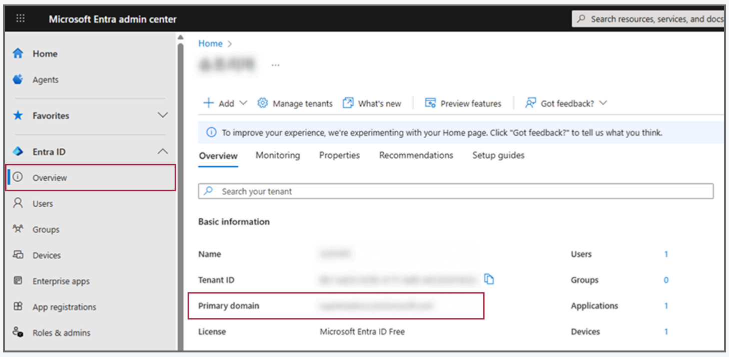


Directory Server

- Client ID: [redacted]
- Client Secret: ••••••••••••••••
- Primary Domain: [redacted]

- **Client ID**: Enter the **Client ID** of the application registered in **Entra ID**.
- **Client Secret**: Enter the **Client secret** added in **Certificates & secrets** of the application registered in **Entra ID**.
- **Primary Domain**: Enter the primary domain name that you input when creating your organization in **Entra ID**.

> ⓘ **INFO**
>
> - For more information about registering an application in **Entra ID**, refer to the following link.
> - For more information about configuring **Certificates & secrets** in **Entra ID**, refer to the following link.
> - **Tenant ID** can be found in the **Overview** of the registered application in **Entra ID**.
> - You can check the information for **Primary Domain** in the **Overview** of **Entra ID**.



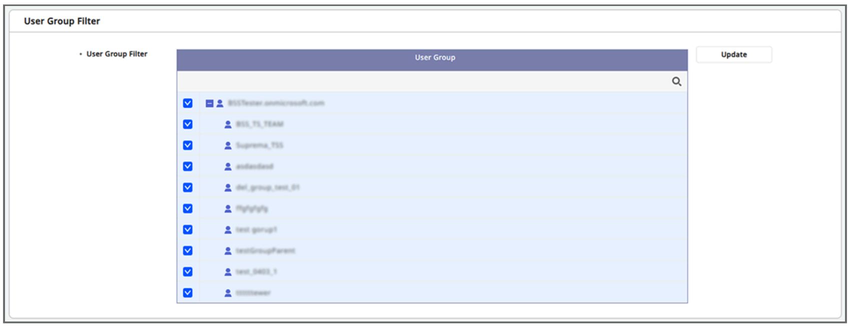
To improve your experience, we're experimenting with your Home page. Click "Got feedback?" to tell us what you think.

Basic information

Name	[redacted]	Users	1
Tenant ID	[redacted]	Groups	0
Primary domain	[redacted]	Applications	1
License	Microsoft Entra ID Free	Devices	1

2 User Group Filter

After completing the settings in **Directory Server** and clicking **Connect**, user group information from **Entra ID** will be retrieved in **User Group Filter**. Deselect the user groups that will not sync with **BioStar X**.

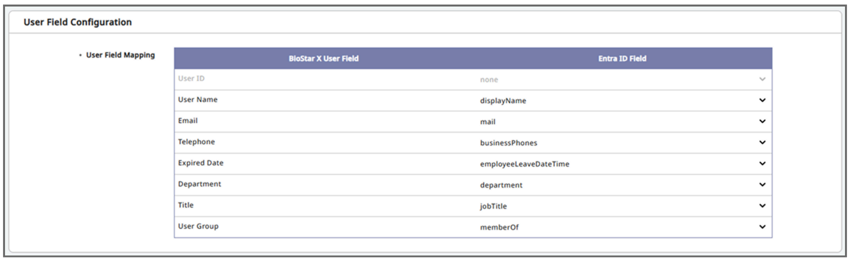


☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]

- **Update**: Click to refresh the user group information.
- Click the 🔍 icon to search for the desired user group.

3 User Field Configuration

You can set the field for **Entra ID** to map to the user fields of **BioStar X**. Select the field for **Entra ID** to use as the user field for **BioStar X** in the **User Field Configuration** section.



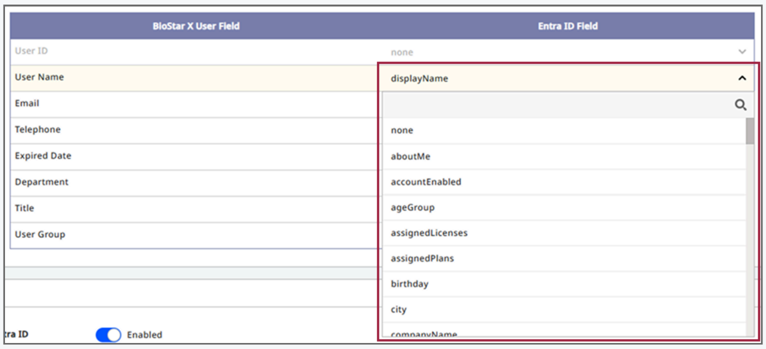
User Field Configuration

- User Field Mapping

BioStar X User Field	Entra ID Field
User ID	none
User Name	displayName
Email	mail
Telephone	businessPhones
Expired Date	employeeLeaveDateTime
Department	department
Title	jobTitle
User Group	memberOf

INFO

Each user field of **BioStar X** is set by default to map to items that match the user information of **Entra ID**. To select a field value other than the default, click the field in **Entra ID Field** and select the desired field value.



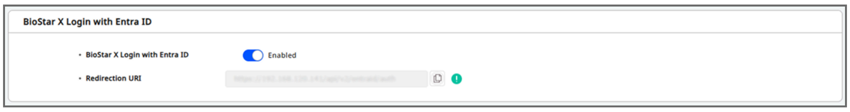
BioStar X User Field	Entra ID Field
User ID	none
User Name	displayName
Email	
Telephone	
Expired Date	
Department	
Title	
User Group	

CAUTION

The **User ID** field cannot be mapped when integrating with **Entra ID**. It is automatically generated and applied by **BioStar X**.

4 BioStar X Login with Entra ID

Change the **BioStar X Login with Entra ID** to **Enabled** to enable login to **BioStar X** using **Entra ID SSO**.



BioStar X Login with Entra ID

- BioStar X Login with Entra ID: Enabled
- Redirection URI: [redacted]

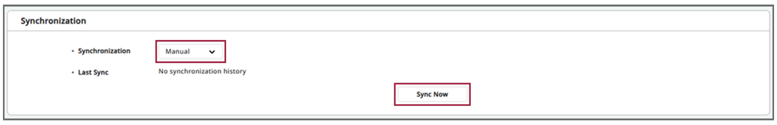
Copy the redirection URI from the **Redirection URI** field(🗐) and paste it into the SSO redirection settings in the **Entra ID** portal. When a user successfully logs in with **Entra ID**, they will be redirected to this address.

> **INFO**
>
> - For more information about registering an application in **Entra ID** and adding a redirection URI, refer to the following links.
>   - Register an application in Microsoft Entra ID
>   - How to add a redirect URI to your application
> - The redirection address can be found in the **Overview** of the registered application in **Entra ID**.

5 Synchronization

This feature allows you to synchronize user information changed in **Entra ID**.

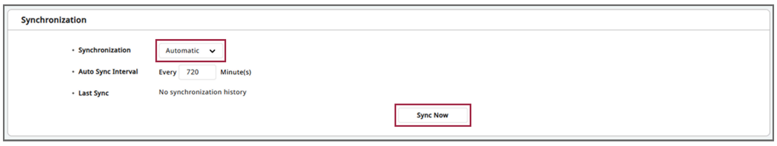
- Synchronization: You can select the desired synchronization method and set the synchronization interval.
  - Manual: Each time you click Sync Now, user information is retrieved and synchronized from **Entra ID**.

    Synchronization

    - Synchronization: Manual
    - Last Sync: No synchronization history

  - Automatic: User information is retrieved and synchronized from **Entra ID** at the interval set in the Auto Sync Interval item. The synchronization interval can be set in minutes. The minimum value is **30** minutes, and the maximum value is **10,080** minutes (7 days).

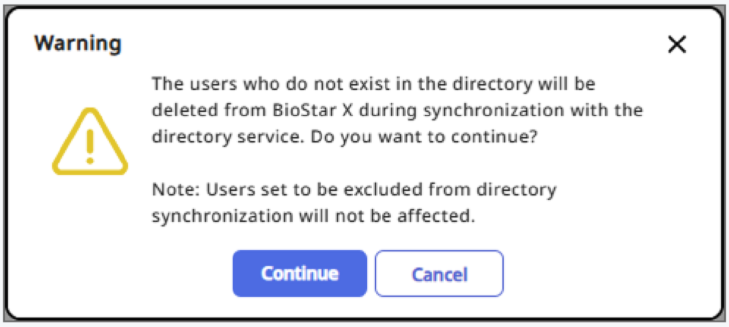
    Synchronization

    - Synchronization: Automatic
    - Auto Sync Interval: Every 720 Minute(s)
    - Last Sync: No synchronization history

- Last Sync: You can check the date and time of the most recent synchronization.

INFO

- When you click **Sync Now**, a warning message will appear. To continue, click **Continue**. To cancel, click **Cancel**.

  Warning

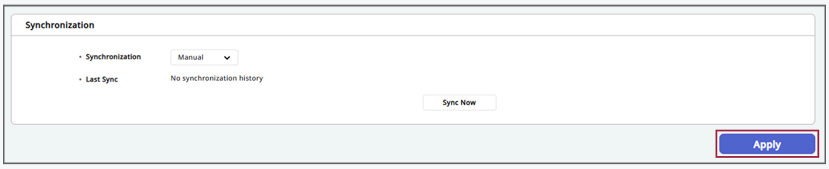
  The users who do not exist in the directory will be deleted from BioStar X during synchronization with the directory service. Do you want to continue?

  Note: Users set to be excluded from directory synchronization will not be affected.

  To exclude specific users from synchronization when using the integration feature, refer to the following.

- When the synchronization method is set to **Automatic**, you can synchronize immediately by clicking **Sync Now**.

After completing all settings for **Directory Integration**, click **Apply** at the bottom of the screen to save. Refer to the following to check the results.

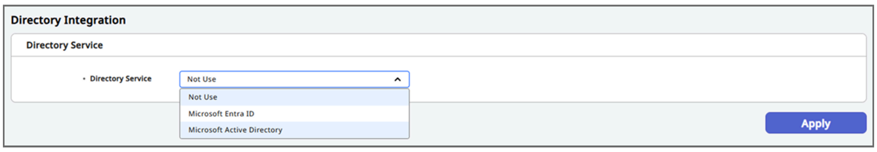


Synchronization

- Synchronization: Manual
- Last Sync: No synchronization history

Integrate with Active Directory

1. Log in to **BioStar X** with an administrator account.
2. Click **Settings** on the **Launcher** page.
3. Click **Directory Integration** in the left sidebar of the screen.
4. Select **Microsoft Active Directory** in **Directory Service**.



Directory Integration

Directory Service

- Directory Service: Not Use

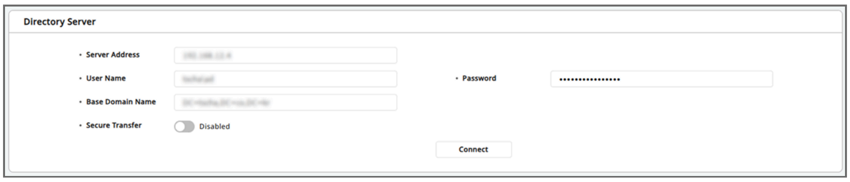
5. Set each item as instructed below.

ⓘ **INFO**

- The Active Directory is available for a system environment with Windows Server 2008 R2 or later.
- To use the Active Directory server, set the **User ID Type** to **Alphanumeric** in the **Settings** → **Server**.

1 Directory Server

Enter the server information for **Active Directory** and click **Connect** in **Directory Server**.



Directory Server

- Server Address
- User Name
- Password: ••••••••••••••••
- Base Domain Name
- Secure Transfer: Disabled

- **Server Address**: Enter the server address for Windows Active Directory.
- **User Name**: Enter the user name used by Windows Active Directory.
- **Password**: Enter the password used by Windows Active Directory.
- **Base Domain Name**: Enter the base domain name for Windows Active Directory. You can find the base domain name in the following steps:

   i. Run the **Active Directory Administrative Center**.

   ii. Right-click on the node where user data is stored, and then click **Property**.

   iii. In the **property** window, select **Expand** and then click **Attribute Editor**.

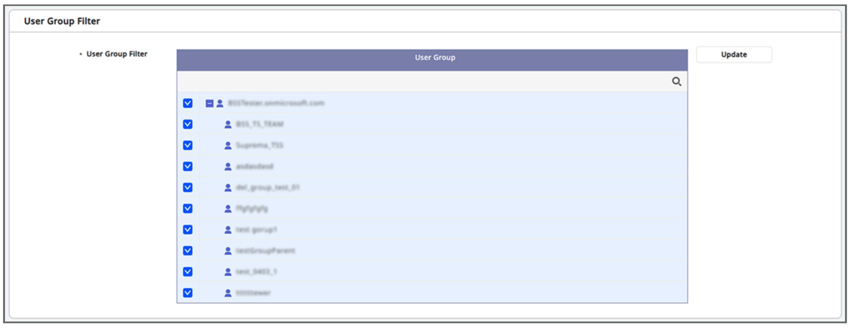
   iv. View the value of **distinguishedName**.

- **Secure Transfer**: You can use encryption when communicating with the Windows Active Directory server. To install the Active Directory Certificate Services and configure the **Keystore Password**, refer to the following.

   – **Keystore Password**: Enter the password for the encryption key store of the Windows Active Directory server. You can enter the password when the **Secure Transfer** is set to **Enabled**.

2 User Group Filter

After completing the settings in **Directory Server** and clicking **Connect**, user group information from **Active Directory** will be retrieved in **User Group Filter**. Deselect the user groups that will not sync with **BioStar X**.



User Group Filter

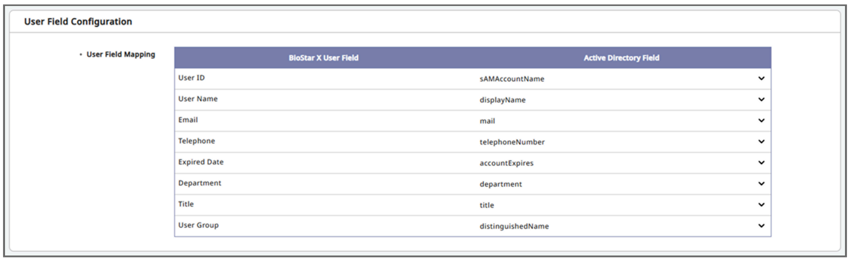
- User Group Filter

User Group
☑ ⊟ BSSTester.onmicrosoft.com
☑ BSS_TS_TEAM
☑ Suprema_TSS
☑ asdasdasd
☑ del_group_test_01
☑ ffgfgfgfg
☑ test gorup1
☑ testGroupParent
☑ test_0403_1
☑ tttttewer

- **Update**: Click to refresh the user group information.
- Click the 🔍 icon to search for the desired user group.

3 User Field Configuration

You can set the field for **Active Directory** to map to the user fields of **BioStar X**. Select the field for **Active Directory** to use as the user field for **BioStar X** in the **User Field Configuration** section.



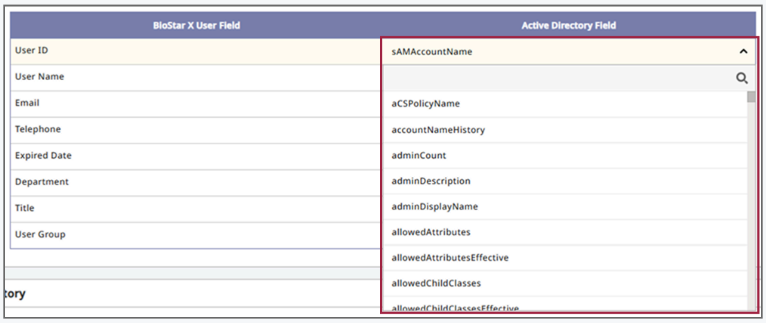
User Field Configuration

- User Field Mapping

BioStar X User Field	Active Directory Field
User ID	sAMAccountName
User Name	displayName
Email	mail
Telephone	telephoneNumber
Expired Date	accountExpires
Department	department
Title	title
User Group	distinguishedName

INFO

Each user field of **BioStar X** is set by default to map to items that match the user information of **Active Directory**. To select a field value other than the default, click the field in **Active Directory Field** and select the desired field value.

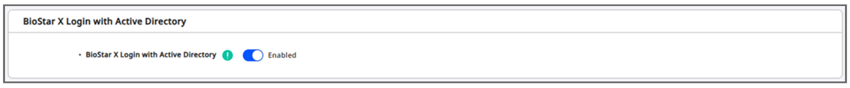


BioStar X User Field	Active Directory Field
User ID	sAMAccountName
User Name	
Email	aCSPolicyName
Telephone	accountNameHistory
Expired Date	adminCount
Department	adminDescription
Title	adminDisplayName
User Group	allowedAttributes
	allowedAttributesEffective
	allowedChildClasses
	allowedChildClassesEffective

4 BioStar X Login with Active Directory

To configure login to **BioStar X** using the user ID of the Active Directory server, change the **BioStar X Login with Active Directory** to **Enabled**. The value of the `sAMAccountName` field from the Active Directory server will be mapped to the **BioStar X** login ID.

> **CAUTION**
>
> The sAMAccountName field cannot contain special characters. You may fail to log in if it does not comply with the login ID policy of **BioStar X**.



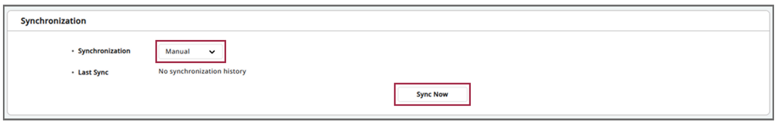
BioStar X Login with Active Directory

- BioStar X Login with Active Directory: Enabled

5 Synchronization

This feature allows you to synchronize user information changed in **Active Directory**.

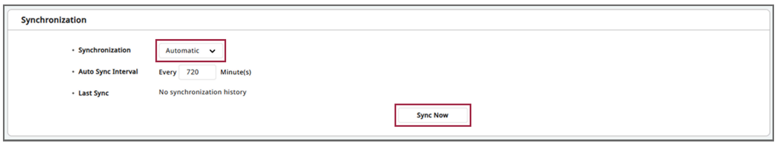
- **Synchronization**: You can select the desired synchronization method and set the synchronization interval.
  - **Manual**: Each time you click **Sync Now**, user information is retrieved and synchronized from **Active Directory**.



Synchronization

- Synchronization: Manual
- Last Sync: No synchronization history

  - **Automatic**: User information is retrieved and synchronized from **Active Directory** at the interval set in the **Auto Sync Interval** item. The synchronization interval can be set in minutes. The minimum value is **30** minutes, and the maximum value is **10,080** minutes (7 days).



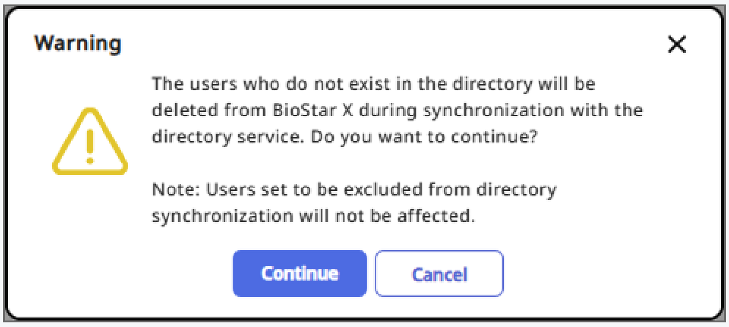
Synchronization

- Synchronization: Automatic
- Auto Sync Interval: Every 720 Minute(s)
- Last Sync: No synchronization history

- **Last Sync**: You can check the date and time of the most recent synchronization.

INFO

- When you click **Sync Now**, a warning message will appear. To continue, click **Continue**. To cancel, click **Cancel**.



Warning

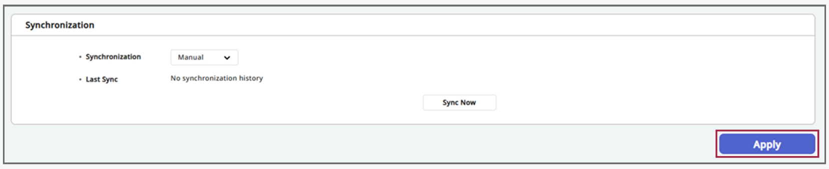
The users who do not exist in the directory will be deleted from BioStar X during synchronization with the directory service. Do you want to continue?

Note: Users set to be excluded from directory synchronization will not be affected.

To exclude specific users from synchronization when using the integration feature, refer to the following.

- When the synchronization method is set to **Automatic**, you can synchronize immediately by clicking **Sync Now**.

After completing all settings for **Directory Integration**, click **Apply** at the bottom of the screen to save. Refer to the following to check the results.



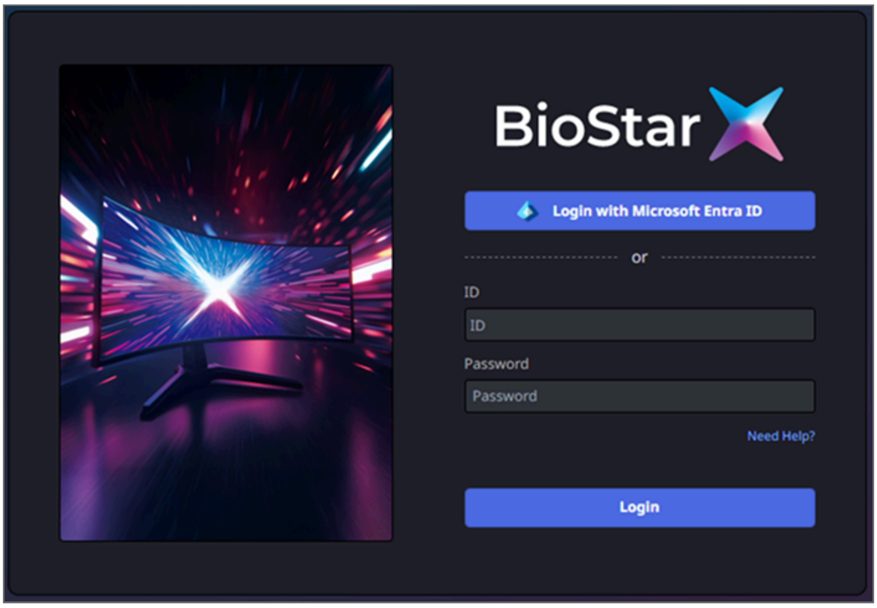
Synchronization

- Synchronization: Manual
- Last Sync: No synchronization history

Check the settings results

After completing the integration settings with **Entra ID** or **Active Directory**, click **Apply** at the bottom of the screen. Refer to the following to check the synchronized settings.

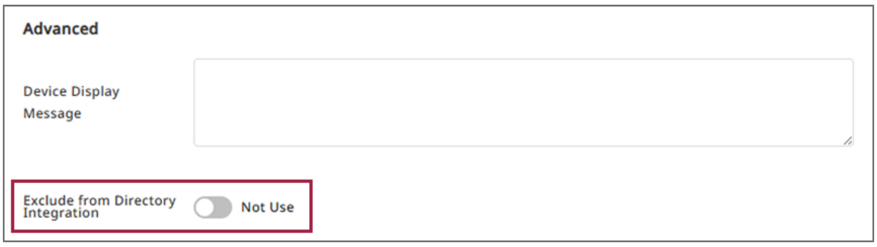
- You can check the synchronized user list in the **User** menu.
- After completing the login settings with **Entra ID** or **Active Directory**, you can see **Login with Microsoft Entra ID** when logging in to **BioStar X**.



Exclude the directory integration

When integrating with **Entra ID** or **Active Directory** via the Directory Integration feature, users who do not exist in the directory service may be deleted from **BioStar X**. If there are users that you do not want to be deleted, you can exclude them from the integration using the following method.

1. Log in to **BioStar X** with an administrator account.
2. Go to the User menu.
3. Click on the user you want to exclude from the integration in the All Users list.
4. When the detail information screen of the selected user appears, click the checkbox of **Exclude from Directory Integration** in **Advanced**.



5. Click the **Apply** button.

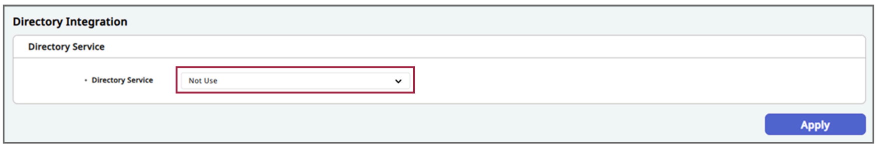
The selected users will be excluded from integration when using the Directory Integration feature.

Disable the directory integration

To disable the Directory Service feature, follow the steps:

1. Log in to **BioStar X** with an administrator account.
2. Click **Settings** → **Directory Integration**.

3. Select **Not Use** in **Directory Service**.

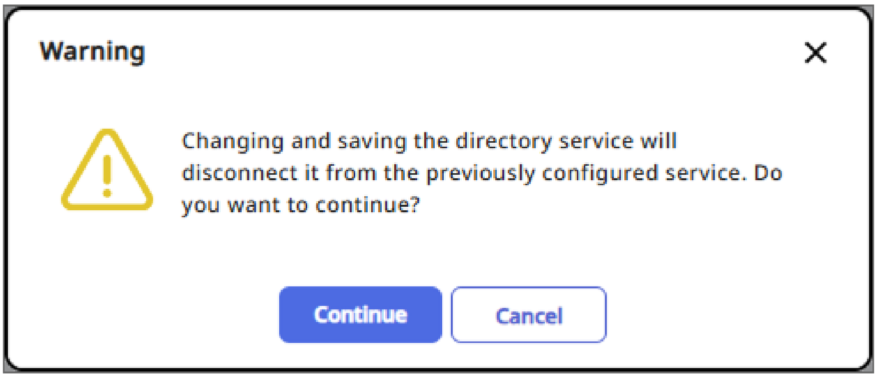


Directory Integration

Directory Service

• Directory Service: Not Use

4. When the **Warning** message appears, click **Continue**.



Warning

Changing and saving the directory service will disconnect it from the previously configured service. Do you want to continue?

5. Click **Apply** at the bottom of the screen.

> ⚠ **CAUTION**
>
> When the **Directory Service** is set to **Not Use**, all integration settings with **Entra ID** or **Active Directory** in **BioStar X** will be removed. The integrated user and group information will not be deleted, but will no longer be synchronized. Please make sure to check before disabling the integration.

Set up Remote Access

Remote access via ngrok allows secure access to internal networks from external networks. This feature enables access to the **BioStar X** server remotely without firewall settings or port forwarding.

ⓘ **INFO**

- The remote access feature is available as an additional option for **Advanced** licenses and above. For more information on licensing policy, refer to the following.
- When purchasing the remote access license, Suprema generates a bot account, endpoint, and license document for remote access use on the ngrok Suprema site.

⚠ **CAUTION**

- Remote Access is provided through ngrok’s third-party tunneling service. Remote Access is provided through ngrok’s third-party tunneling service. Before using this feature, please review Remote Access Feature Agreement.
- BioStar X simply supports the connection by calling the ngrok API, but the security, safety, and continuity of internet connectivity entirely depend on the ngrok service. Therefore, Suprema assumes no responsibility for any security incidents, data loss, or system breaches that may occur during the use of this feature.

When to use this?

Use the remote access feature in the following situations.

- When you need to connect to the **BioStar X** server from an external network
- When it's challenging to connect directly due to firewalls or NAT environments
- When you want to quickly set up remote access without complex network setups
- When you need to temporarily provide outside access rights

Remote access setup

1 Activate remote access license

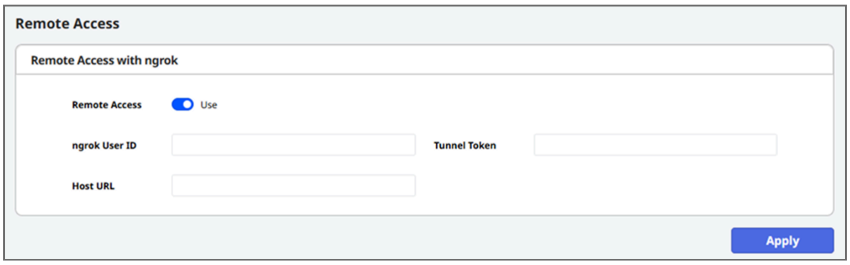
1. Log in with your **BioStar X** admin ID.
2. Click **Settings** on the **Launcher** page.

3. Click **License** → **BioStar X License** in the left sidebar.
4. Enter the remote access license key and admin name provided by Suprema, then click **Activate**.

> ⓘ **INFO**
>
> For more information on license registration, refer to the following.

2 Activate remote access

1. Log in with your **BioStar X** admin ID.
2. Click **Settings** on the **Launcher** page.
3. Click **Remote Access** in the left sidebar.
4. In the **Remote Access with ngrok** section, change the **Remote Access** option to **Use**.



Remote Access ● Use

3 Enter ngrok setup information

Enter the ngrok setup information provided by Suprema.

- **ngrok User ID**: Enter your ngrok account.
- **Authtoken**: Enter your **Authtoken**.
- **URL**: Enter the endpoint URL. The URL is in the format `your-name.bsx.ngrok.app`.

After entering all the information, click the **Apply** button. If a warning message window appears, check the content and click the **Agree** button.

Access endpoint URL

After completing the setup, verify whether you can access the **BioStar X** server from an external network using the endpoint URL you entered in **URL**.

> ⓘ **INFO**
>
> If you cannot access via endpoint URL from an external network, contact the sales point or distributor that issued your license.

Integrate Virtual Device Event Log

By using the virtual device feature, you can log events such as clock-in and clock-out directly to **BioStar X** from mobile apps or third-party services when integrating the attendance management feature. You can systematically manage event logs without a physical device, which is useful for integration with external systems.

When to use this?

Use the virtual device event log integration feature in the following situations.

- When managing events from the external T&A management system in **BioStar X**
- When you need to save access logs (Punch Log) from the mobile app or external system directly to **BioStar X** (recording check-in/check-out events without database linkage)
- When you need to send events directly via the **BioStar X** API from third-party applications or services

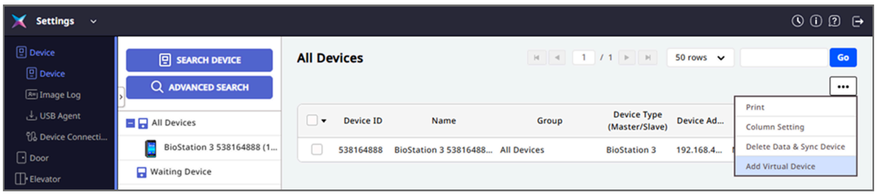
Before start

The **Event Log API** license must be activated. For more information on licensing policy, refer to the following.

> **INFO**
>
> For more information on license application, refer to the following.

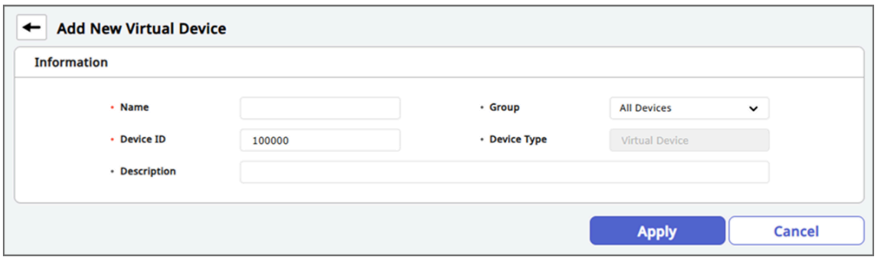
Register virtual device

1. Click **Settings** on the **Launcher** page.
2. Click **Device** in the left sidebar.
3. Click ••• at the top right of the device list and select **Add Virtual Device**.



□	Device ID	Name	Group	Device Type (Master/Slave)	Device Ad...
□	538164888	BioStation 3 53816488...	All Devices	BioStation 3	192.168.4...

4. Enter the setting information when the **Add Virtual Device** screen appears.



Add New Virtual Device

Information

- Name:
- Device ID: 100000
- Description:
- Group: All Devices
- Device Type: Virtual Device

   - **Name**: Enter the virtual device's name.
   - **Group**: Select the group to assign the virtual device.
   - **Device ID**: Enter the unique ID of the virtual device. It must be specified within a range that does not duplicate with the existing device ID.
   - **Description**: Enter the description for virtual device.

5. Click **Apply** at the bottom right of the screen to register the virtual device.

> **INFO**
>
> - **Device ID** can be specified within the range of 100000 - 999999. It must be specified within a range that does not duplicate with the existing Suprema device ID.
> - The value of **Device ID** that has already been created cannot be modified.

Manage device groups

Virtual devices can use the device group feature just like regular devices.

- You can place it in the same group as existing devices.
- If the user has group permissions, they can grant permissions to virtual devices within that group.

> **INFO**
>
> For more information on device groups, refer to the following.

Virtual device limitations

- Virtual devices appear only in the following menu.
  - **Settings** → **Device**
  - View all event logs and preview event logs in **Monitoring**
  - Retrieve event log from **Data**
- The virtual device cannot use access control features at the door and **Advanced AC**.

- Cannot be specified as a device for **T&A** setting.
- Virtual devices do not appear in the device list in the sidebar of the **Monitoring** menu.
- Cannot use device control feature.
- Not included in the number of devices for the **Multi Communication Server** license.

Log events via API

Supported event type

Only the following event types can be recorded.

- **Access granted** (`4088`)
- **Access Denied** (`6400`)

API parameters

You must provide the following parameters when logging events.

Parameter	Description	Required
`dev_id`	Only registered virtual device IDs are allowed	Yes
`evt`	Access Granted or Access Denied	Yes
`datetime`	Event occurrence time	Yes
`user_id`	User ID	Yes
`tna_key`	Only available for input with the specified value	Option

Request example

```
{
   "packet_device_id" : 100003, // required
   "is_virtual_device" : "true", // required
   "events":[ //4088 access granted, 6400 access denied
      {
         "dev_id": 100003, // required
         "evt": 6400, // required
         "datetime": "2025-08-21T14:12:00Z", // required
         "user_id": "2", // required
         "tna_key": "1"
```

Response example

```
{
  "Response": {
    "code": "0",
    "link": "https://support.supremainc.com/en/support/home",
    "message": "Success"
  }
}
```

INFO

- You can log multiple event logs for a single virtual device at once with a single API call.
- For more information on using API, refer to the following.

Retrieve event log

You can retrieve the event logs recorded through the virtual device in the menu.

- **Monitoring**: Retrieve and filter all events, event preview
- **Data**: Retrieve and filter all events

INFO

- For more information about event retrieval on **Monitoring**, refer to the following.
- For more information about **Data**, refer to the following.

Audit trail

Audit trail is recorded as shown in the example below when logs are recorded for events.

```
Access granted, 2025/08/05 03:37:49, outside access door on 12th floor, Administrator(1)
```

INFO

- Even if events are logged in batch, an individual audit trail entry is created for each event.
- For more information on **Audit Trail**, refer to the following.

Troubleshooting

If the Add Virtual Device button is not visible

Check if the **Event Log API** license is activated.

When the API call fails

- Check if the **Event Log API** license is activated.
- Check the device ID is a registered virtual device.
- Check if the API parameter format is correct.

When events are not getting retrieved

- Verify that the recorded device is the correct virtual device ID.
- Check the virtual device is selected in the event filter.
- Check audit trails to ensure no errors occurred when logging events.

Plugin

What are plugins?

BioStar X plugins are extensions of the **BioStar X** platform that provide additional features to meet customer requirements or to integrate with existing systems.

> ⓘ **INFO**
>
> - A plugin license is required to use plugin features. For more information on the licensing policy, refer to the following.
> - For more information on plugin development, refer to the following.

BioStar X plugins

List of plugins available through additional options for licenses above **Advanced**.

🗃 How to Use Time & Attendance

9 items

🗃 Manage Visitors

6 items

> ⓘ **INFO**
>
> For more information on licensing policy, refer to the following.

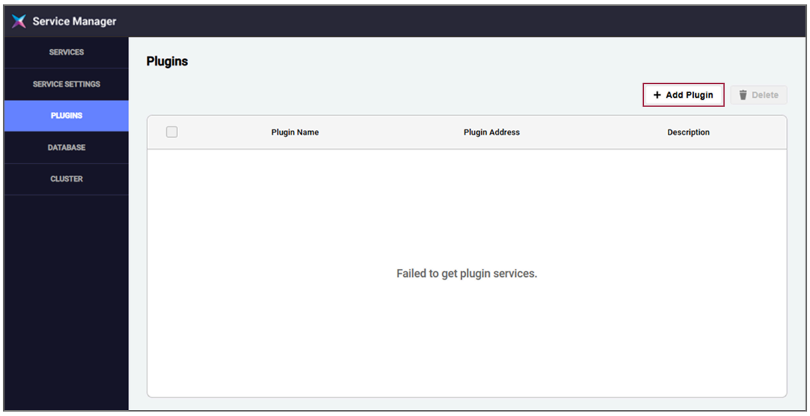
Key use cases

You can integrate various external systems through the **BioStar X** plugins system. The representative use cases are as follows.

- **Attendance Management System**: Integration with external T&A (Time & Attendance) solutions
- **Visitor Management System**: Integration with separate visitor registration and management systems
- **Reporting Solution**: Integration with customizable reporting and analysis tools
- **Third-Party System Integration**: Data integration with existing business systems such as ERP and HRM

Register plugin

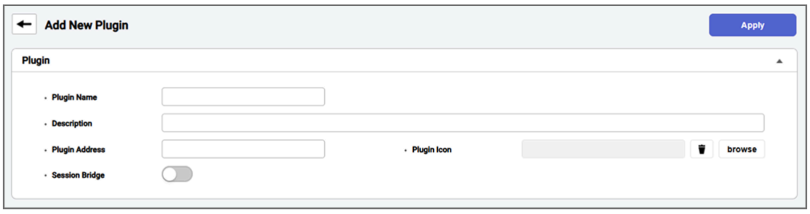
1. Click **Start** ⊞ → **BioStar X** → **BioStar X Service Manager** on Windows.
2. Click **PLUGINS** in the left side menu.
3. Click the **Add Plugin** button in the upper right.



☐	Plugin Name	Plugin Address	Description

Failed to get plugin services.

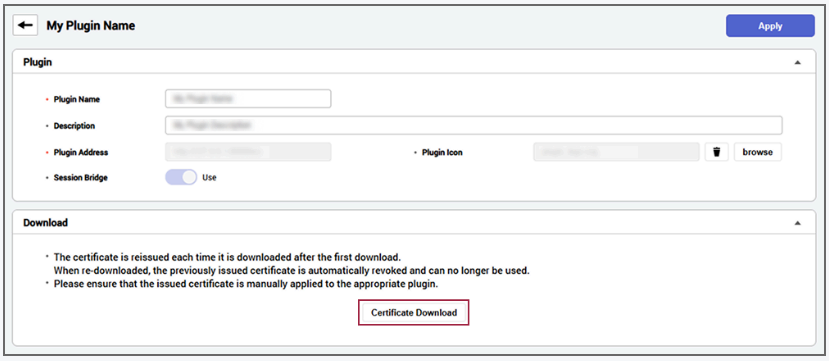
4. Enter plugin information on the **Add New Plugin** screen.



5. Enter plugin information and click **Apply** to complete registration.

INFO

If you have activated **Session Bridge**, you can download the certificate at the bottom of the screen. The certificate is required for secure communication between **BioStar X** and the plugin. If you lose the certificate, you can download it again. At this time, the existing certificate will be invalidated.



- The certificate is reissued each time it is downloaded after the first download.
  When re-downloaded, the previously issued certificate is automatically revoked and can no longer be used.
- Please ensure that the issued certificate is manually applied to the appropriate plugin.

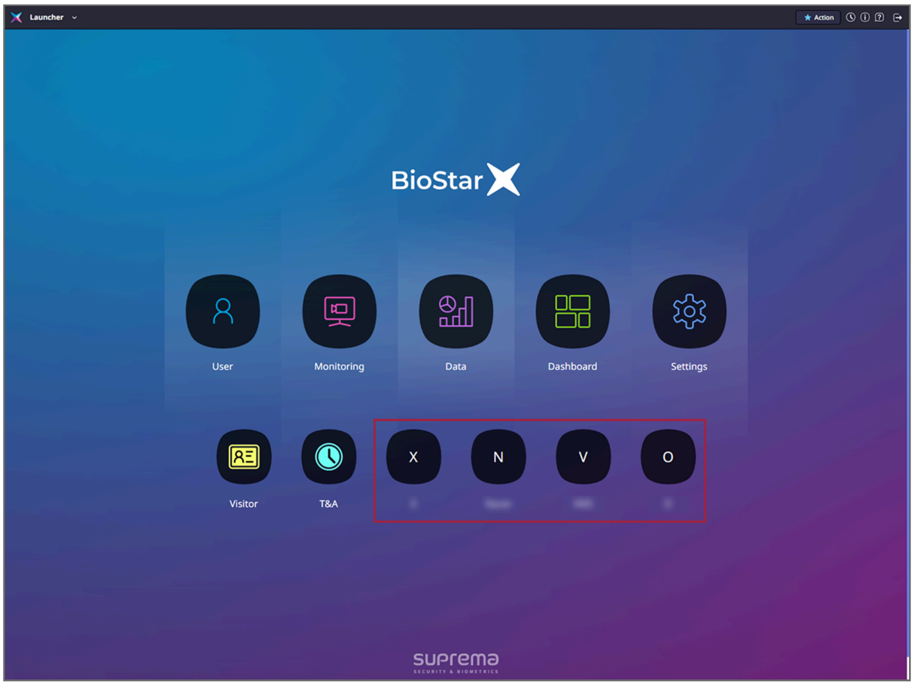
Enter plugin information

- **Plugin Name**: Enter the name of the plugin. You can enter up to 48 characters. You cannot use the same name as an existing registered plugin.
- **Description**: Enter a description of the plugin. You can enter up to 500 characters.
- **Plugin Address**: Enter the address of the plugin. It must be a valid URL starting with `http://` or `https://`, and you cannot use the same address as an existing registered plugin.
- **Plugin Icon**: Upload the plugin's icon.
  - Supported formats are JPEG, PNG, SVG, GIF.
  - The maximum file size is 1MB, and 0KB empty files cannot be uploaded.
  - Uploaded images will be automatically resized to 104×104 pixels.
- **Session Bridge**: Activate to use the session bridge. Using this feature automatically inherits permissions for BioStar X users, so no separate login is required when accessing the plugin.

> **INFO**
>
> - If you do not upload an icon, an icon will be generated automatically from the first letter of the plugin name. The uploaded icon can be deleted by clicking the 🗑 button, and it will be replaced with the automatically generated icon upon deletion.
> - Once **Session Bridge** is activated, it cannot be deactivated, and the plugin address cannot be changed for security reasons.

Check on the launcher screen

You can see the added plugins on the **Launcher** screen of **BioStar X**.



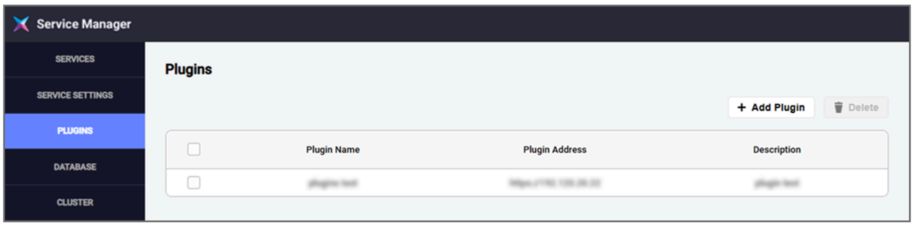
Plugin management

You can manage the plugins installed through **BioStar X Service Manager**.

Click **Start** ⊞ → **BioStar X** → **BioStar X Service Manager** on Windows. Click **PLUGINS** in the site menu of the **BioStar X Service Manager** screen.

Check plugin list

You can see all the plugins registered by the user.

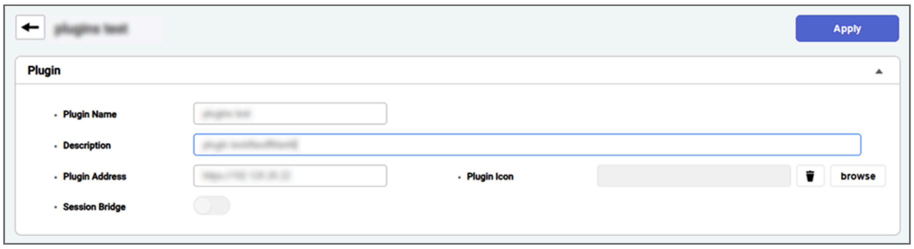


Plugins

□	Plugin Name	Plugin Address	Description
□	[illegible]	[illegible]	[illegible]

Edit plugin

Click the plugin you want to edit from the plugin list. The plugin information edit screen appears. You can edit the plugin name (**Plugin Name**), description (**Description**), and icon (**Plugin Icon**).



ⓘ **INFO**

Plugin Address cannot be edited when **Session Bridge** is enabled.

Delete plugin

1. Select the plugin to delete by clicking the checkbox on the far left of the plugin list.
2. Click the 🗑 **Delete** button in the upper right corner of the screen.
3. When the confirmation message appears, click **OK**.

ⓘ **INFO**

- Plugins added with attendance management licenses cannot be deleted.
- The attendance management plugin can be used through additional options in the **Advanced** license or higher. For more information on licensing policies, refer to the following.

How to Use Time & Attendance

Set the attendance management rules and check the recorded work history through the device or output it as a report. The T&A feature is provided as a plugin and requires a separate license.

> ⓘ **INFO**
>
> The T&A feature can be used with additional options on **advanced** (Advanced) licenses or higher. For more information on licensing policy, refer to the following.

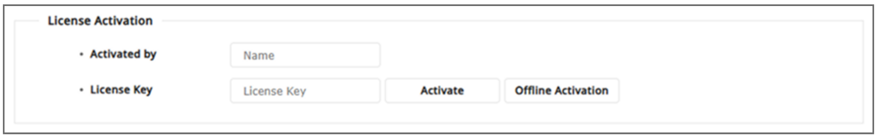
Before start

To use the T&A feature, apply the license and download the separate installation file for installation.

Apply license

Instructions for applying the T&A license. After purchasing the T&A license from a **BioStar X** vendor, follow the instructions to apply the license.

1. Log in with the **BioStar X** administrator account.
2. Click **Settings** on the **Launcher** page.
3. Click **License** → **BioStar X License** in the left sidebar.
4. Enter **License Activation** in sequence with **Activated by** and **License Key**.



5. Click Activate.

You can check the licensed registered in **Activated License**.

> ⓘ **INFO**
>
> To activate your license in a closed network environment or an offline state with limited internet access, refer to the following.

Install plugin

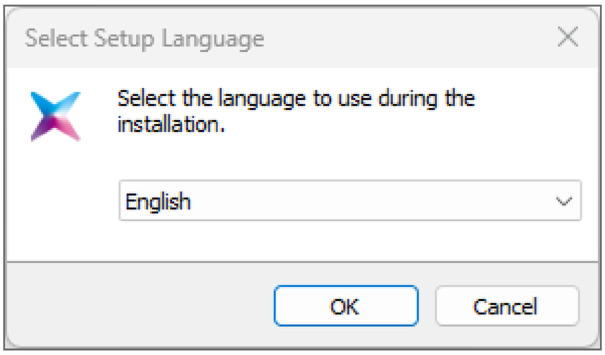
To use the T&A feature, a separate installation file must be downloaded and installed. Follow the instructions to install the plugin.

1. Access the Suprema Download Center and download the T&A plugin installation file (*BioStar X TA.X.Y.Z.BB.exe*).

2. Run the installation file and complete the installation according to the instructions.

3. Run the downloaded installation file.

4. Select the language to use and select the **OK** button.

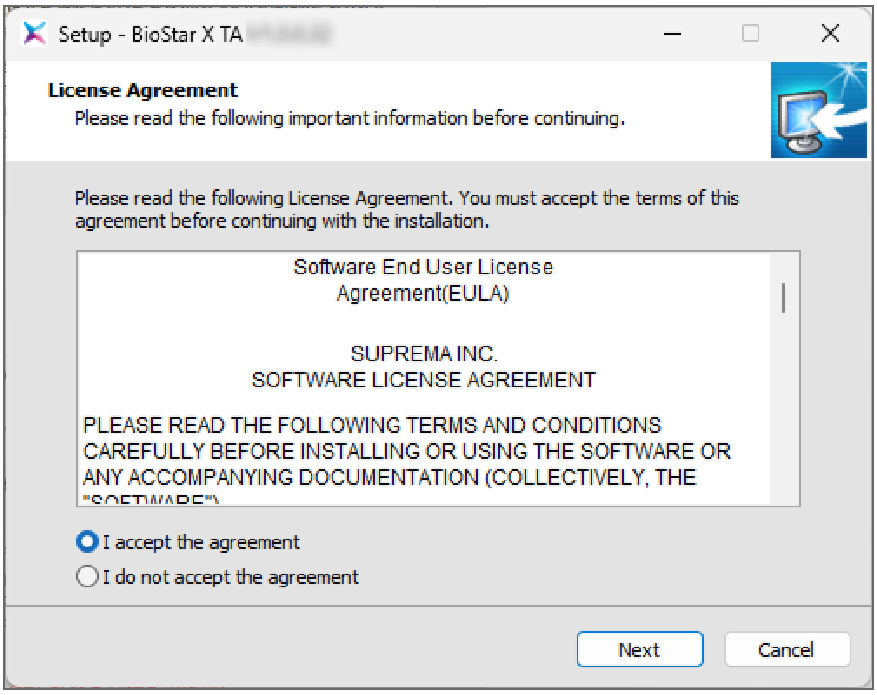


Select Setup Language

Select the language to use during the installation.

English

5. To continue the installation, select **I accept the agreement** and click the **Next** button.



Setup - BioStar X TA

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

Software End User License Agreement(EULA)

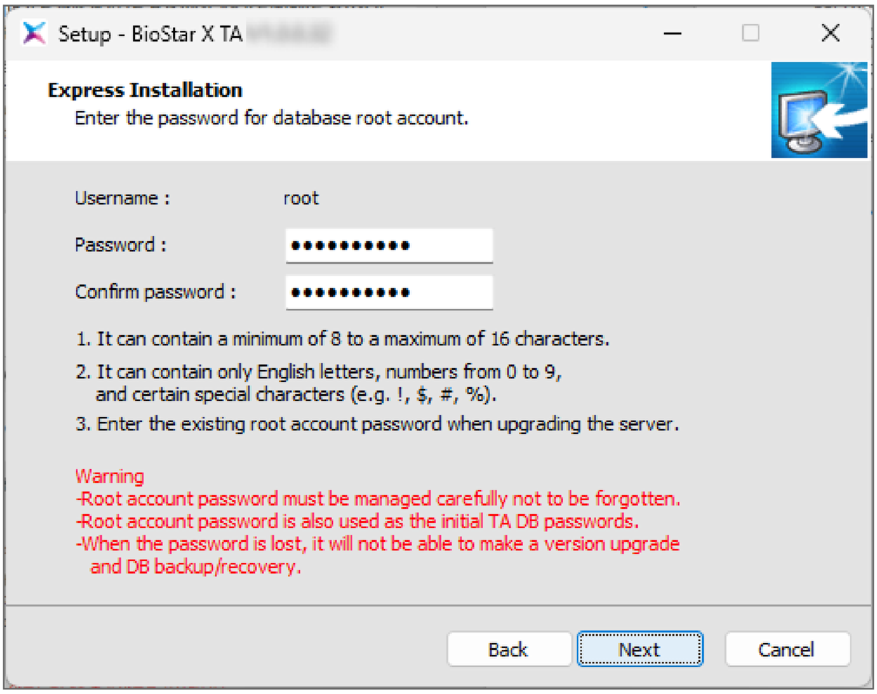
SUPREMA INC.
SOFTWARE LICENSE AGREEMENT

PLEASE READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE INSTALLING OR USING THE SOFTWARE OR ANY ACCOMPANYING DOCUMENTATION (COLLECTIVELY, THE "SOFTWARE")

● I accept the agreement

○ I do not accept the agreement

6. Enter the root account password for the database and click the **Next** button.



Express Installation

Enter the password for database root account.

Username : root

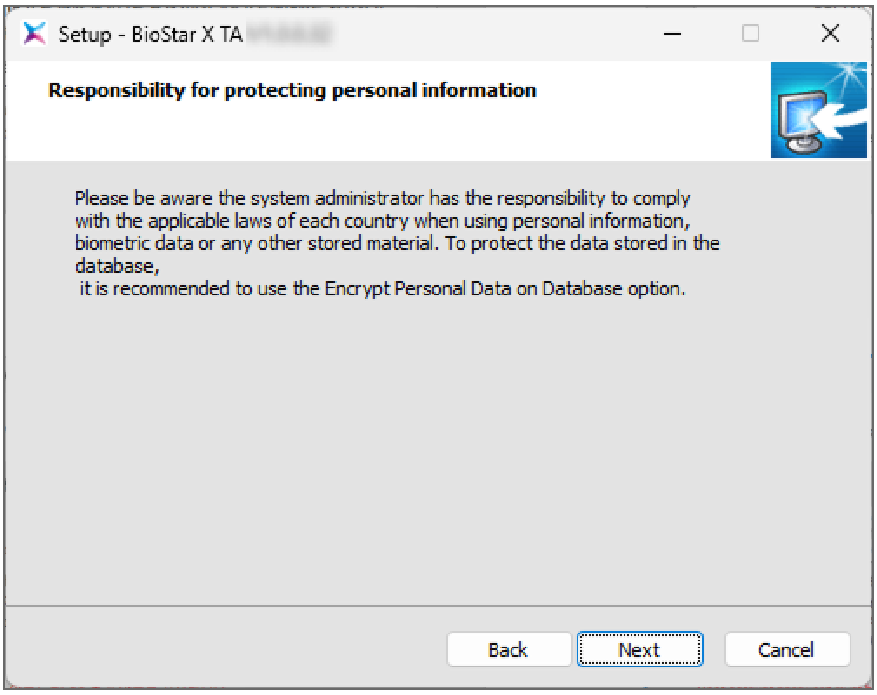
Password : ●●●●●●●●●●

Confirm password : ●●●●●●●●●●

1. It can contain a minimum of 8 to a maximum of 16 characters.
2. It can contain only English letters, numbers from 0 to 9, and certain special characters (e.g. !, $, #, %).
3. Enter the existing root account password when upgrading the server.

Warning
-Root account password must be managed carefully not to be forgotten.
-Root account password is also used as the initial TA DB passwords.
-When the password is lost, it will not be able to make a version upgrade and DB backup/recovery.

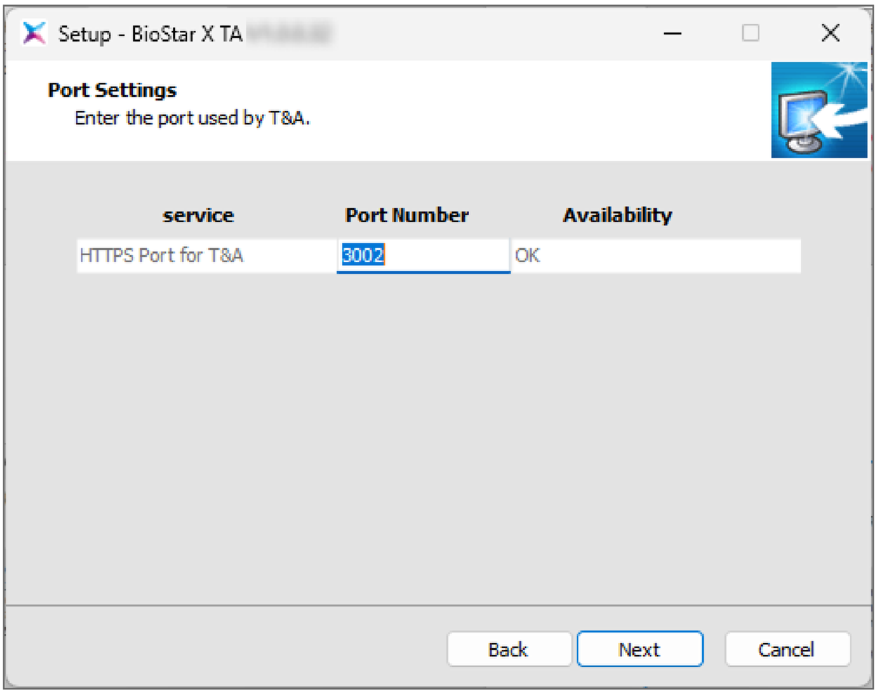
7. Read the information about the management and responsibility of personal information stored in the database, and click the **Next** button to continue the installation.



Responsibility for protecting personal information

Please be aware the system administrator has the responsibility to comply with the applicable laws of each country when using personal information, biometric data or any other stored material. To protect the data stored in the database,
it is recommended to use the Encrypt Personal Data on Database option.

8. Set the port for communication with **BioStar X** and click **Next**.



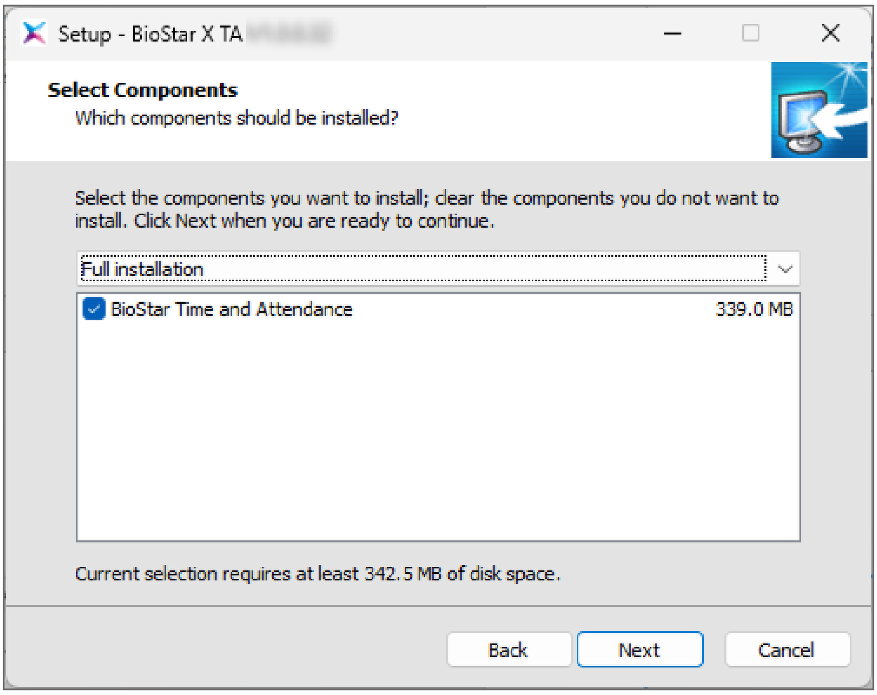
Port Settings

Enter the port used by T&A.

service	Port Number	Availability
HTTPS Port for T&A	3002	OK

> ⓘ You can use the default port number (3002) or change to a different port number. If you change the port number, ensure that the corresponding port is open in the firewall.

9. Select the installation components and click **Next**.



Select Components

Which components should be installed?

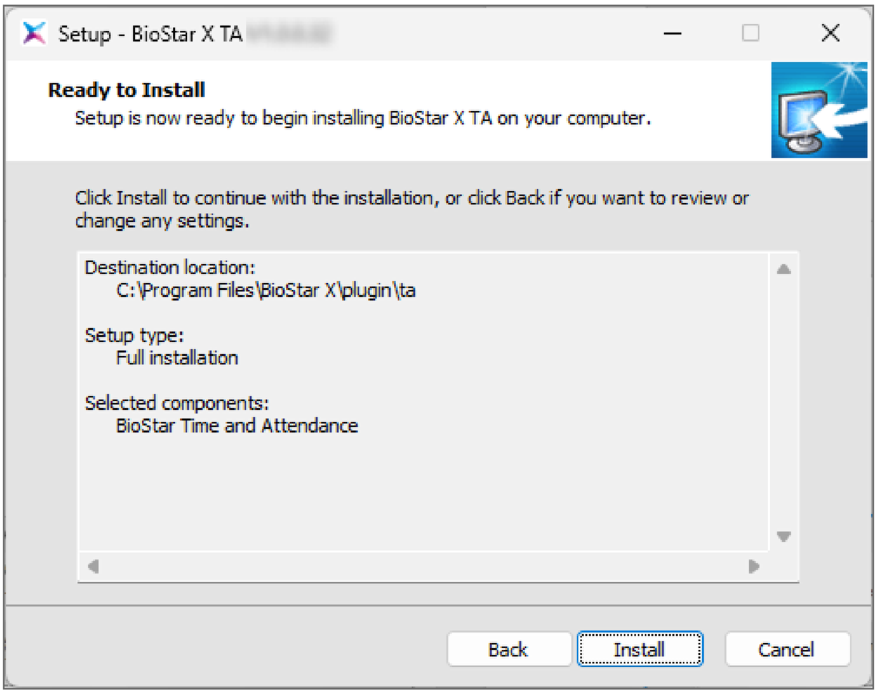
Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

Full installation

☑ BioStar Time and Attendance 339.0 MB

Current selection requires at least 342.5 MB of disk space.

10. When all preparations for installation are complete, click the **Install** button.



Ready to Install

Setup is now ready to begin installing BioStar X TA on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

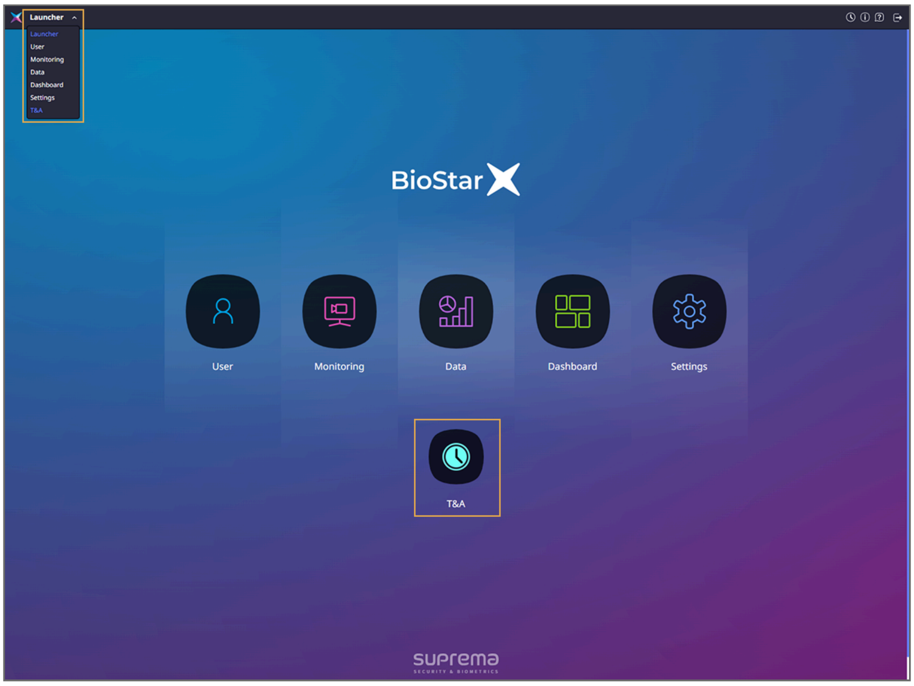
```
Destination location:
      C:\Program Files\BioStar X\plugin\ta

Setup type:
      Full installation

Selected components:
      BioStar Time and Attendance
```

ⓘ **INFO**

- In the downloaded file name, X.Y.Z is the version information and BB is the build number.
- Use the password for the root account of the database that was used when installing **BioStar X**.

T&A menu

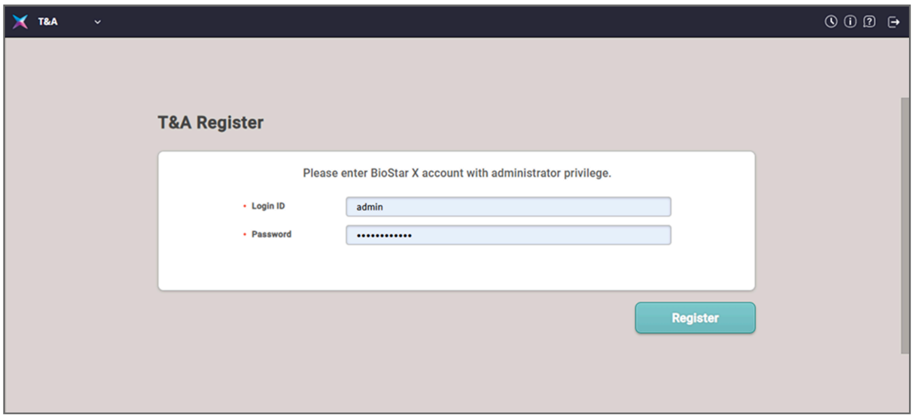
Once the T&A license and plugin installation are complete, the **Launcher** page will have the **T&A** menu added.



Click the T&A icon on the Launcher page or select T&A from the shortcut list at the top left of the screen.

T&A login

A separate login screen will appear the first time you enter the T&A feature. Log in with the **BioStar X** administrator account. When you log in to the T&A feature with the administrator account, you can use the T&A feature thereafter without a separate login process.



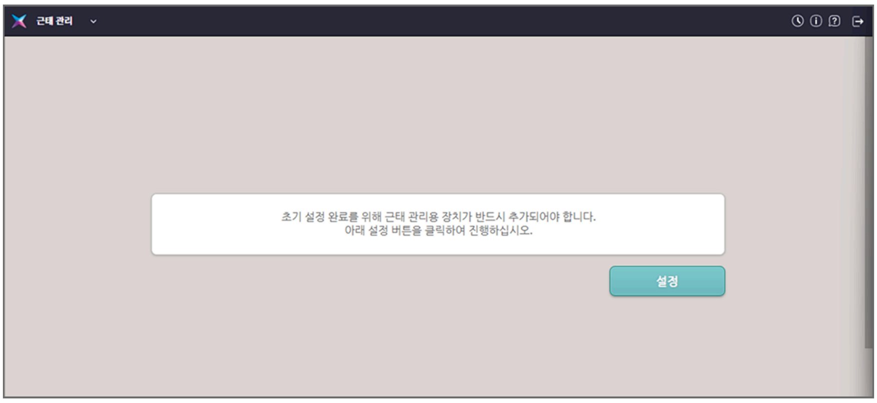
T&A Register

Please enter BioStar X account with administrator privilege.

- Login ID: admin
- Password: ••••••••••••

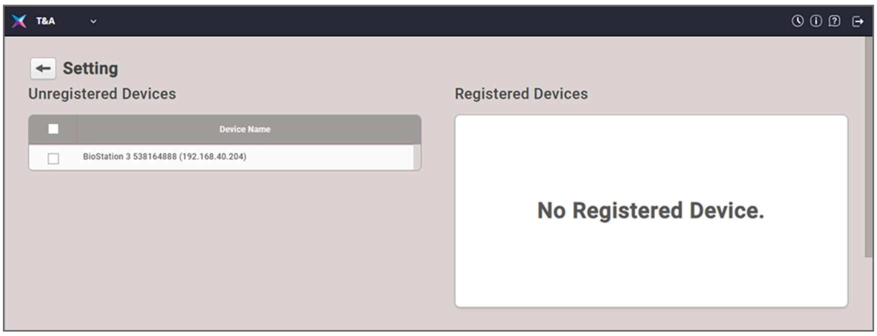
Initial setup

1. The first time you log into the T&A feature, you need to add a device for attendance management for initial setup. Click the **Settings** button on the screen.



초기 설정 완료를 위해 근태 관리용 장치가 반드시 추가되어야 합니다.
아래 설정 버튼을 클릭하여 진행하십시오.

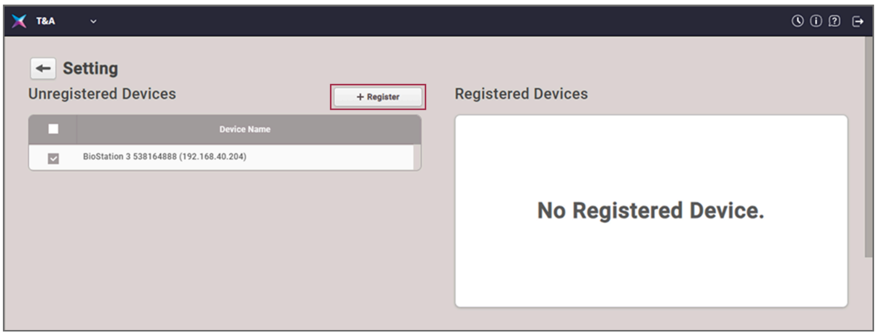
2. Select a device for attendance management from the device list.



□	Device Name
□	BioStation 3 538164888 (192.168.40.204)

No Registered Device.

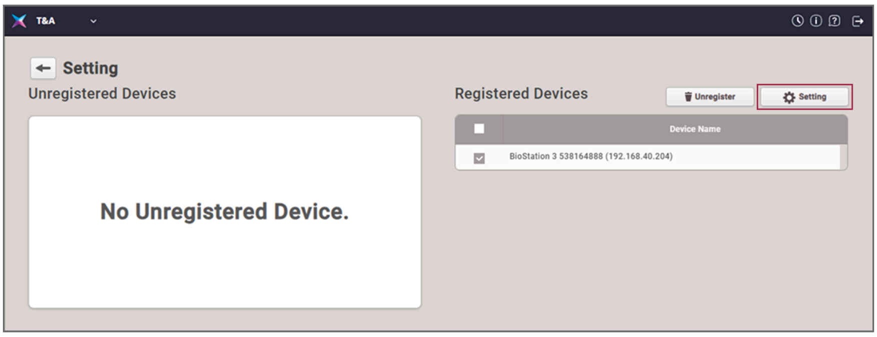
3. Click the activated + **Register** button.



□	Device Name
☑	BioStation 3 538164888 (192.168.40.204)

No Registered Device.

4. If the selected device appears in the **Registered Devices** list, click the **Setting** button.



Setting

Unregistered Devices

No Unregistered Device.

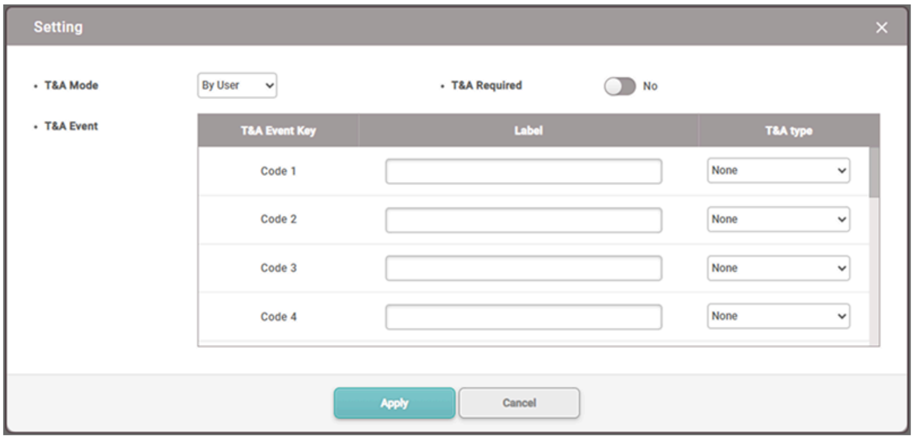
Registered Devices

□	Device Name
☑	BioStation 3 538164888 (192.168.40.204)

5. When the **Setting** window appears, complete the basic settings for attendance management.

Configure attendance mode

Proceed with the attendance mode and attendance event settings.



- T&A Mode: By User
- T&A Required: No
- T&A Event

T&A Event Key	Label	T&A type
Code 1		None
Code 2		None
Code 3		None
Code 4		None

- **T&A Mode**: Choose how to register attendance events.
  - **By User**: Users can select attendance events during authentication.
  - **By Schedule**: Attendance events automatically change according to a set schedule. You can select a schedule to apply to attendance events.
  - **Last Choice**: The last used attendance event can continue to be used.
  - **Fixed**: Only the selected attendance event can be used.
  - **Not Use**: Does not log attendance events.
- **T&A Required**: You can set it to require registration of attendance events during authentication. Can be used when **T&A Mode** is set to **By User**.
- **T&A Event**: You can modify the name of attendance events or add schedules used when setting **T&A Mode** to **By Schedule**.
  - **T&A Event Key**: This is a list of keys that can be used to register attendance.
  - **Label**: You can change the name of attendance events according to the attendance key.
  - **Schedule**: If you set **T&A Mode** to **By Schedule**, you can automatically set the schedule to change. For

more information about schedule settings, refer to the following.

ⓘ **INFO**

- Devices that do not support LCD screens can set **T&A Mode** to **By Schedule** and **Fixed**. You can register fixed attendance events or change attendance events based on pre-scheduled settings.
- Device models that support **By Schedule** and **Fixed** modes include BioEntry P2, BioEntry W2, BioEntry Plus, BioEntry W, XPass, XPass S2, XPass D2, XPass 2.
- For more information on the **Setting** menu, refer to the following.

Set Shift

This guide explains how to configure the attendance management rules by setting the work schedule in hourly, daily, and weekly units.

If this is your first time registering working rules, follow the steps below to configure it.

1

Time Code

You can set time rules for attendance record management, overtime, and absences. You can set hourly weights and can color code them for easy identification.

For more information on Time Code settings, refer to the following.

2

Shift

You can set daily working rules based on a 24-hour period. Working rules include time rule settings based on time, daily start time settings, and time rounding rules.

For more information on Shift settings, refer to the following.

3

Schedule Template

You can set weekly work rules based on the daily work rules configured. You can set weekly work rules on a weekly or daily basis.

For more information on Schedule Template settings, refer to the following.

4

Rule

This can be useful when you have not added overtime rules to the daily working rules. The overtime set in daily working rules has start and end times, but **Rule** calculates the total time exceeding the regular working hours. **Rule** can be conveniently used when managing the total overtime hours daily/weekly/monthly, and if you set **Rule**, it will apply instead of the overtime rule added to the working rules.

For more information on Rule settings, refer to the following.

5

Work schedule

You can set the period to apply the working schedule configured in the previous step, along with users, other working rules, and leave schedules.

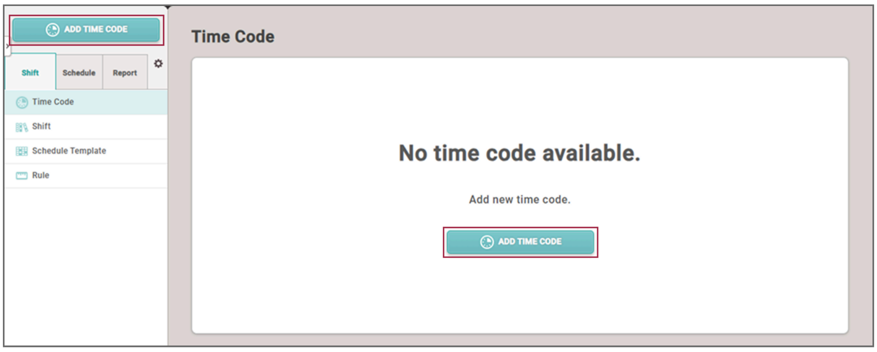
For more information on Schedule settings, refer to the following.

Set Time Code

This guides the configuration of Time Code settings used for working hour calculations. You can set standard time codes, overtime time codes, and leave time codes. Each Time Code can be used with different hourly weights.

ADD TIME CODE

1. Click **T&A** on the **Launcher** page.
2. Click **Shift** → **Time Code** on the left sidebar.
3. Click the **ADD TIME CODE** button.



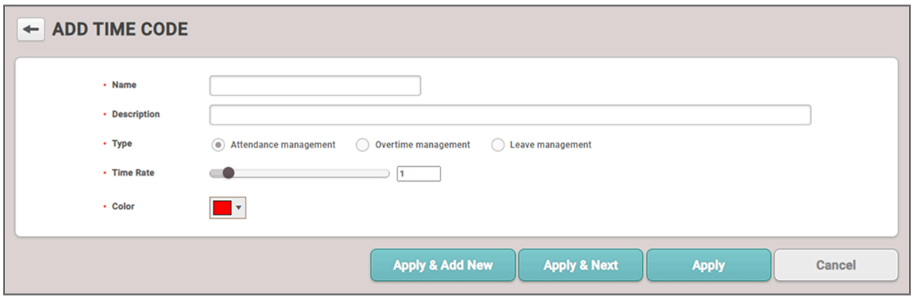
No time code available.

Add new time code.

4. When the **ADD TIME CODE** screen appears, configure each item.

> **INFO**
>
> - Click **Apply** at the bottom of the screen to save the settings.
> - To add Shift, click the **Apply & Next** button.
> - After saving the settings, click the **Apply & Add New** button to add another **Time Code**.

Setting options guide



- Name
- Description
- Type: ● Attendance management ○ Overtime management ○ Leave management
- Time Rate: 1
- Color: 🟥

- **Name**: Enter the name of the Time Code.
- **Description**: Enter a description for the Time Code.

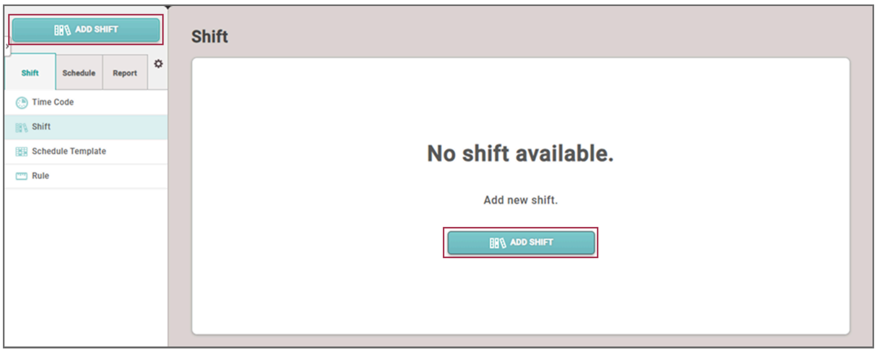
- **Type**: Select the type of Time Code.
  - **Attendance management**: Set as the Time Code to be used for normal attendance.
  - **Overtime management**: Set as the Time Code to be used for overtime.
  - **Leave management**: Set as the Time Code to be used for leaves, business trips, etc.
- Set the hourly weight according to **Time Code**. **1** is the base weight, and if set to **2**, the configured Time Code will calculate working hours as double per hour.
- **Color**: Set the color to distinguish the Time Code.

Set Daily Shift

Create work rules by applying different time rules based on time for a 24-hour period. Choose from fixed, flexible, or floating work options, and set the start time of the day, rounding rules, etc.

ADD SHIFT

1. Click **T&A** on the **Launcher** page.
2. Click **Shift** on the left sidebar.
3. Click **ADD SHIFT**.



No shift available.

Add new shift.

4. When the **ADD SHIFT** screen appears, set each item.

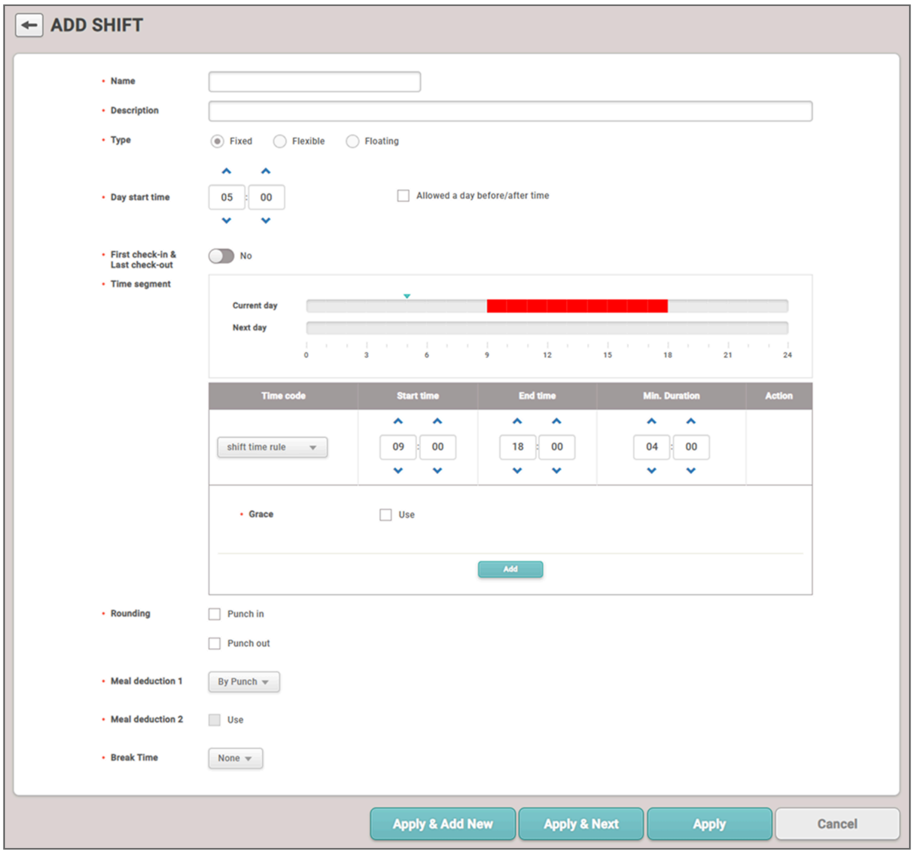
> **INFO**
>
> - Click **Apply** at the bottom of the screen to save the settings.
> - To continue adding weekly work rules, click **Apply & Next**.
> - After saving the settings, click **Apply & Add New** to add another **Shift**.

Setting options guide

Depending on the type of work rule, you can select either **Fixed**, **Flexible**, or **Floating**. Setting options may vary depending on the selected type of work rule.

Fixed

This is a work rule for arriving and departing at set times. Enter the name and description of Shift and select **Type** as **Fixed**.



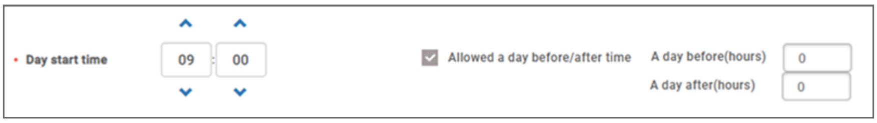
ADD SHIFT

- Name
- Description
- Type ● Fixed ○ Flexible ○ Floating
- Day start time 05 : 00 □ Allowed a day before/after time
- First check-in & Last check-out No
- Time segment

Time code	Start time	End time	Min. Duration	Action
shift time rule	09 : 00	18 : 00	04 : 00	

- Grace □ Use
- Rounding □ Punch in □ Punch out
- Meal deduction 1 By Punch
- Meal deduction 2 □ Use
- Break Time None

- **Day start time**: Set the start time for the workday.
  Allowed a day before/after time allows you to set work rules for hours worked in excess of 24 hours based on the set day start time. It can be set for a maximum of 6 hours.

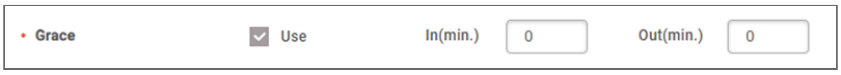


- Day start time 09 : 00 ☑ Allowed a day before/after time A day before(hours) 0 A day after(hours) 0

- **First check-in & Last check-out**: When this option is activated, the first authenticated time is recorded as the start time, and the last authenticated time is recorded as the end time.

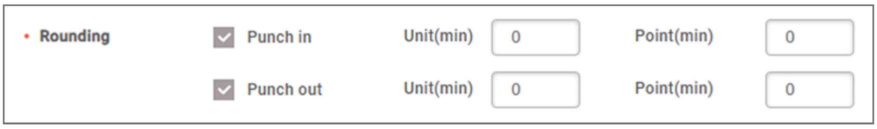
> **INFO**
>
> When this option is activated, you must set **Break by Punch** to record user break times.

- **Time segment**: After selecting the items set in the **Time code** column for attendance records, set **Start time**, **End time**, **Min. Duration**.
  - **Grace**: Set grace time to allow for normal work when arriving late or leaving early compared to the set time.



- Grace ☑ Use In(min.) 0 Out(min.) 0

- **Rounding**: Automatically round the start and end times. Set units and standards for both start and end times.



• Rounding	☑ Punch in	Unit(min)	0	Point(min)	0
	☑ Punch out	Unit(min)	0	Point(min)	0

- **Unit(min)**: Set rules to round registered time when clock-in events are recorded earlier or later than the set start time.

- **Point(min)**: Set rules to round registered time when clock-out events are recorded earlier or later than the set end time.

> **TIP**
>
> For example, if the clock-in time is set to 09:00, and **Unit(min)** is set to 15 minutes and **Point(min)** is set to 8 minutes, it will round as follows.
>
> - 09:07 clock-in → rounded down to 09:00 (less than 8 minutes)
> - 09:08 clock-in → rounded up to 09:15 (8 minutes or more)

> **INFO**
>
> The **Rounding** rules take precedence over **Grace**.

- **Meal deduction 1** / **Meal deduction 2**: Set deductions for meal times from daily working hours.
  - **By Punch**: Set to deduct based on time records registered on the attendance device without setting fixed meal deduction times.
  - **Auto**: Set to automatically deduct meal times by defining **Deduction time** and **Minimal hours before deduction**.
  - **Fixed**: Set to deduct fixed times by defining **Start time** and **End time**.

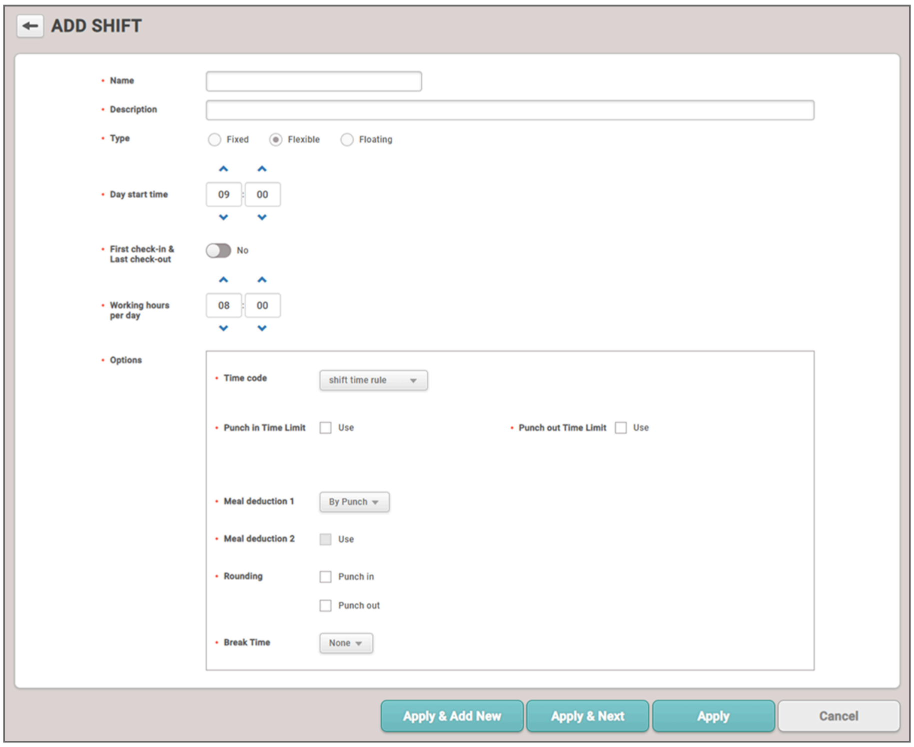
> **INFO**
>
> - Using **Meal deduction 2** allows for deductions of two meal times from daily working hours.
> - If the meal deduction types are **Auto** or **Fixed**, then **Meal deduction 1** and **Meal deduction 2** can only be set to the same type.

- **Break Time**: Set break times.
  - **By Punch**: Set to follow the time records registered on the attendance device without setting fixed break times. When this option is activated, you can set **Max. allowed break time(min.)**.
  - **Fixed**: Set **Start time** and **End time** as fixed times for user break time.

> **INFO**
>
> - You can only add one time rule set as **Attendance management** to Shift.
> - You can set **Start time**, **End time**, **Min. Duration**, and **Rounding** for a time rule set as **Overtime management**.

Flexible work

This is a work rule that sets the daily working hours and flexibly adjusts the arrival and departure times based on the start time of the day. Enter the name and description of Shift and select **Type** as **Flexible**.



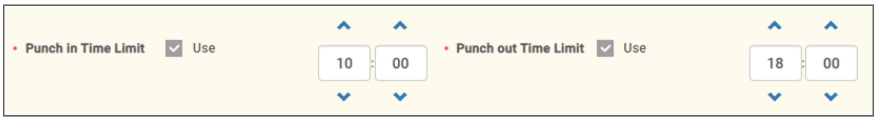
ADD SHIFT

- Name
- Description
- Type ○ Fixed ● Flexible ○ Floating
- Day start time 09 : 00
- First check-in & Last check-out No
- Working hours per day 08 : 00
- Options
  - Time code shift time rule
  - Punch in Time Limit □ Use
  - Punch out Time Limit □ Use
  - Meal deduction 1 By Punch
  - Meal deduction 2 □ Use
  - Rounding □ Punch in □ Punch out
  - Break Time None

- **Day start time**: Set the start time for the workday.
- **First check-in & Last check-out**: When this option is activated, the first authenticated time is recorded as the start time, and the last authenticated time is recorded as the end time.

> **INFO**
>
> When this option is activated, you must set **Break by Punch** to record user break times.

- **Working hours<br />per day**: Set the total working hours for the day.
- **Time code**: Select the items for attendance records.
- **Punch in Time Limit** / **Punch out Time Limit**: Set the time range in which users can authenticate their clock-in and clock-out times.



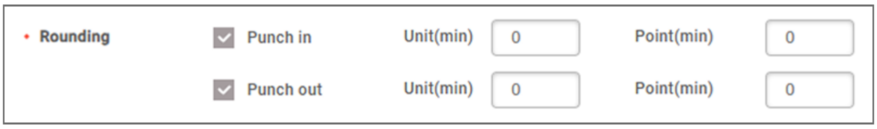
• Punch in Time Limit ☑ Use 10 : 00

• Punch out Time Limit ☑ Use 18 : 00

- **Meal deduction 1** / **Meal deduction 2**: Set deductions for meal times from daily working hours.
  - **By Punch**: Set to deduct based on time records registered on the attendance device without setting fixed meal deduction times.
  - **Auto**: Set to automatically deduct meal times by defining **Deduction time** and **Minimal hours before deduction**.
  - **Fixed**: Set to deduct fixed times by defining **Start time** and **End time**.

> **INFO**
>
> - Using **Meal deduction 2** allows for deductions of two meal times from daily working hours.
> - If the meal deduction types are **Auto** or **Fixed**, then **Meal deduction 1** and **Meal deduction 2** can only be set to the same type.

- **Rounding**: Automatically round the start and end times. Set units and standards for both start and end times.



• Rounding	☑ Punch in	Unit(min)	0	Point(min)	0
	☑ Punch out	Unit(min)	0	Point(min)	0

  - **Unit(min)**: Set rules to round registered time when clock-in events are recorded earlier or later than the set start time.
  - **Point(min)**: Set rules to round registered time when clock-out events are recorded earlier or later than the set end time.

> **TIP**
>
> For example, if the clock-in time is set to 09:00, and **Unit(min)** is set to 15 minutes and **Point(min)** is set to 8 minutes, it will round as follows.
>
> - 09:07 clock-in → rounded down to 09:00 (less than 8 minutes)
> - 09:08 clock-in → rounded up to 09:15 (8 minutes or more)

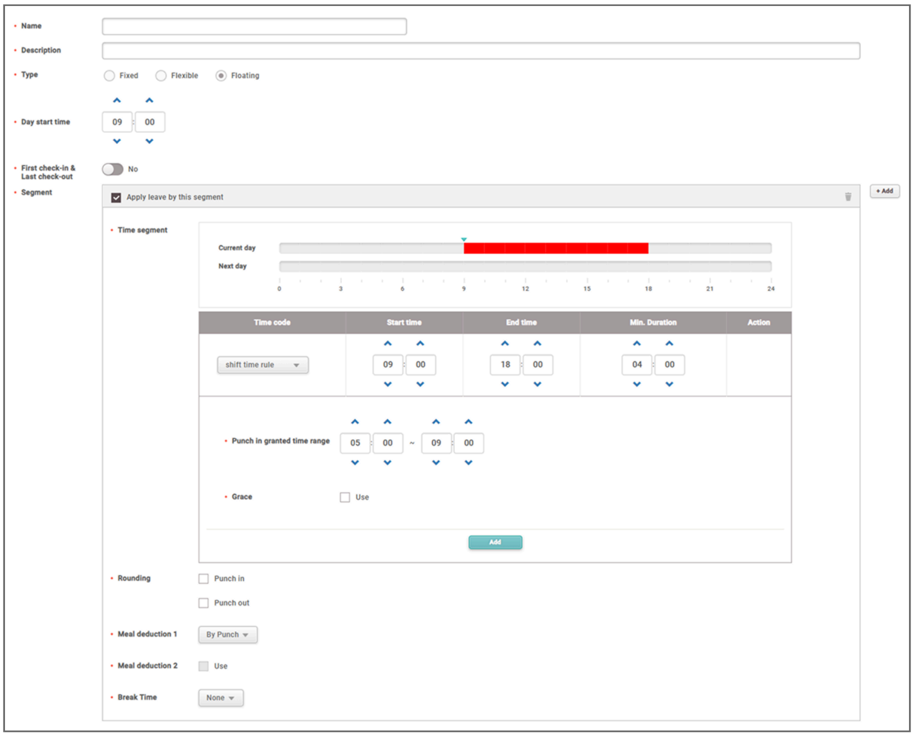
> **INFO**
>
> The **Rounding** rules take precedence over **Grace**.

- **Break Time**: Set break times.
  - **By Punch**: Set to follow the time records registered on the attendance device without setting fixed break times. When this option is activated, you can set **Max. allowed break time(min.)**.
  - **Fixed**: Set **Start time** and **End time** as fixed times for user break time.

> **INFO**
>
> A time rule set as **Overtime management** cannot be added.

Floating Shift

This is a work rule that allows flexible setting of arrival and departure times. Enter the name and description of Shift and select **Type** as **Floating**.



- Name
- Description
- Type ○ Fixed ○ Flexible ● Floating
- Day start time 09 : 00
- First check-in & Last check-out No
- Segment ☑ Apply leave by this segment

+ Add

- Time segment

Time code	Start time	End time	Min. Duration	Action
shift time rule	09 : 00	18 : 00	04 : 00	

- Punch in granted time range 05 : 00 ~ 09 : 00
- Grace □ Use

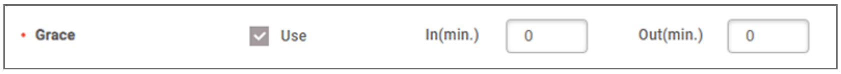
Add

- Rounding □ Punch in
□ Punch out
- Meal deduction 1 By Punch
- Meal deduction 2 □ Use
- Break Time None

- **Day start time**: Set the start time for the workday.
- **First check-in & Last check-out**: When this option is activated, the first authenticated time is recorded as the start time, and the last authenticated time is recorded as the end time.

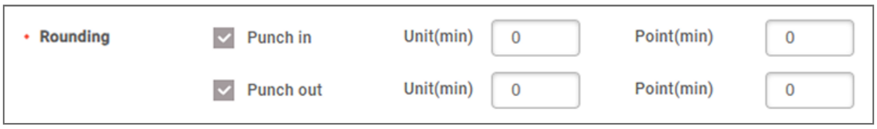
  > **INFO**
  >
  > When this option is activated, you must set **Break by Punch** to record user break times.

- **Time segment**: After selecting the items set in the **Time code** column for attendance records, set **Start time**, **End time**, **Min. Duration**.
  - **Punch in granted time range**: Set the time range that will be considered normal work when arriving early or leaving late compared to the set start or end time.
  - **Grace**: Set grace time to allow for normal work when arriving late or leaving early compared to the set time.



- Grace ☑ Use In(min.) 0 Out(min.) 0

- **Rounding**: Automatically round the start and end times. Set units and standards for both start and end times.



• Rounding	☑ Punch in	Unit(min)	0	Point(min)	0
	☑ Punch out	Unit(min)	0	Point(min)	0

  - **Unit(min)**: Set rules to round registered time when clock-in events are recorded earlier or later than the set start time.
  - **Point(min)**: Set rules to round registered time when clock-out events are recorded earlier or later than the set end time.

TIP

For example, if the clock-in time is set to 09:00, and **Unit(min)** is set to 15 minutes and **Point(min)** is set to 8 minutes, it will round as follows.

- 09:07 clock-in → rounded down to 09:00 (less than 8 minutes)
- 09:08 clock-in → rounded up to 09:15 (8 minutes or more)

INFO

The **Rounding** rules take precedence over **Grace**.

- **Meal deduction 1** / **Meal deduction 2**: Set deductions for meal times from daily working hours.
  - **By Punch**: Set to deduct based on time records registered on the attendance device without setting fixed meal deduction times.
  - **Auto**: Set to automatically deduct meal times by defining **Deduction time** and **Minimal hours before deduction**.
  - **Fixed**: Set to deduct fixed times by defining **Start time** and **End time**.

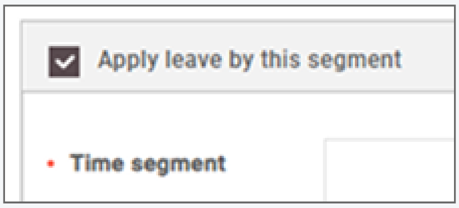
INFO

- Using **Meal deduction 2** allows for deductions of two meal times from daily working hours.
- If the meal deduction types are **Auto** or **Fixed**, then **Meal deduction 1** and **Meal deduction 2** can only be set to the same type.

- **Break Time**: Set break times.
  - **By Punch**: Set to follow the time records registered on the attendance device without setting fixed break times. When this option is activated, you can set **Max. allowed break time(min.)**.
  - **Fixed**: Set **Start time** and **End time** as fixed times for user break time.

INFO

- Work shifts can consist of up to five time slots. Click **+ Add** to add a time slot.
- When setting absences, the **Apply leave by this segment** option must be selected. **Apply leave by this segment** can be selected from the time slots configured into work shifts.



☑ Apply leave by this segment

• Time segment

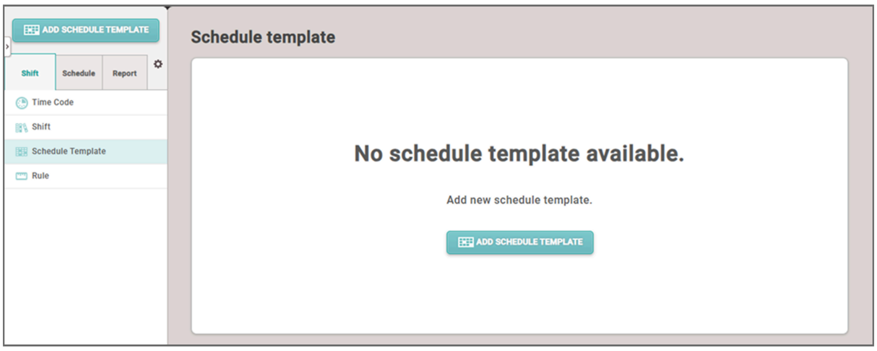
- You can set **Start time**, **End time**, **Min. Duration**, and **Rounding** for a time rule set as **Overtime management**.

Set Weekly Shifts

This guides how to create weekly shift rules based on the configured Shift.

ADD SCHEDULE TEMPLATE

1. Click **T&A** on the **Launcher** page.
2. Click **Shift** → **Schedule Template** in the left sidebar.
3. Click **ADD SCHEDULE TEMPLATE**.



Schedule template

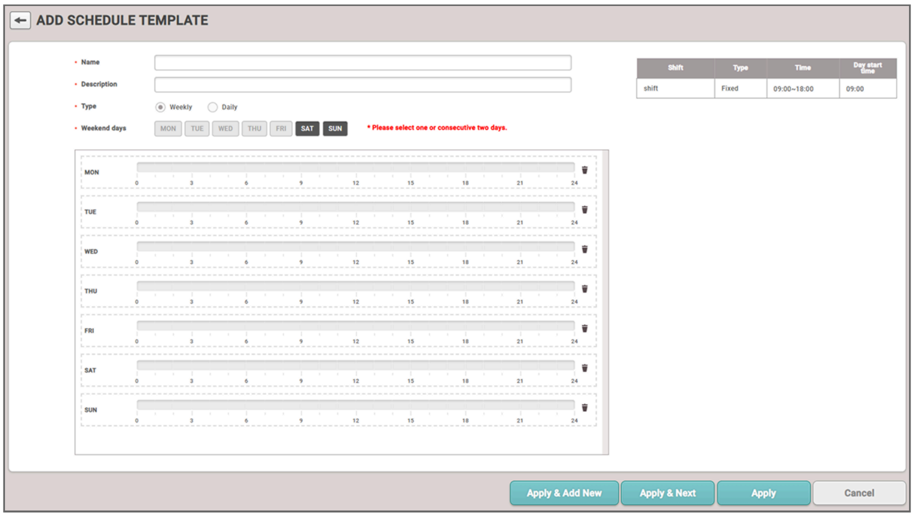
No schedule template available.

Add new schedule template.

4. When the **ADD SCHEDULE TEMPLATE** screen appears, set each item.

> **INFO**
>
> - Click **Apply** at the bottom of the screen to save the settings.
> - To continue adding the work schedule, click the **Apply & Next** button.
> - After saving the settings, click **Apply & Add New** to add another **Schedule Template**.

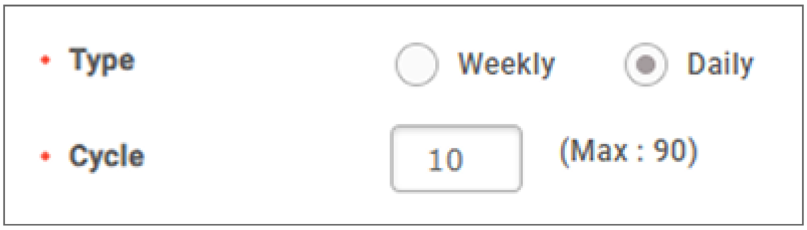
Setting options guide


ADD SCHEDULE TEMPLATE

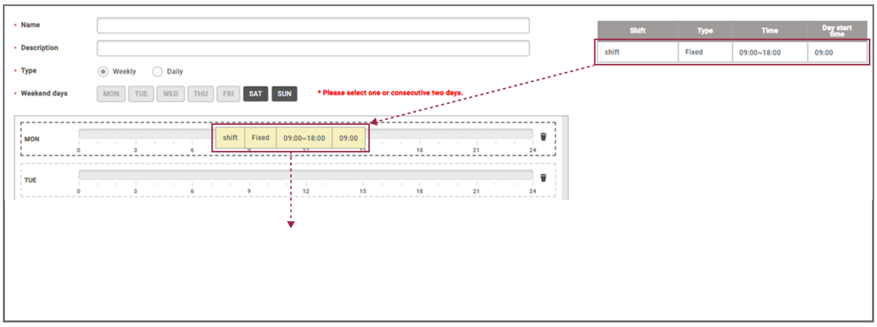
- Name
- Description
- Type ● Weekly ○ Daily
- Weekend days MON TUE WED THU FRI SAT SUN * Please select one or consecutive two days.

Shift	Type	Time	Day start time
shift	Fixed	09:00~18:00	09:00

- **Name**: Enter the name of Schedule Template.
- **Description**: Enter a description for Schedule Template.
- **Type**: Set Schedule Template to **Weekly** or **Daily** daily.
  Selecting **Daily** allows you to set the repeating usage period (**Cycle**).


- Type ○ Weekly ● Daily
- Cycle 10 (Max : 90)

- **Weekend days**: Set the days to designate as weekends.
- **Shift**: View the list of configured Shift rules.
- Weekly/daily schedule: Drag and drop the configured Shift.


- Name
- Description
- Type ● Weekly ○ Daily
- Weekend days MON TUE WED THU FRI SAT SUN * Please select one or consecutive two days.

Shift	Type	Time	Day start time
shift	Fixed	09:00~18:00	09:00

INFO

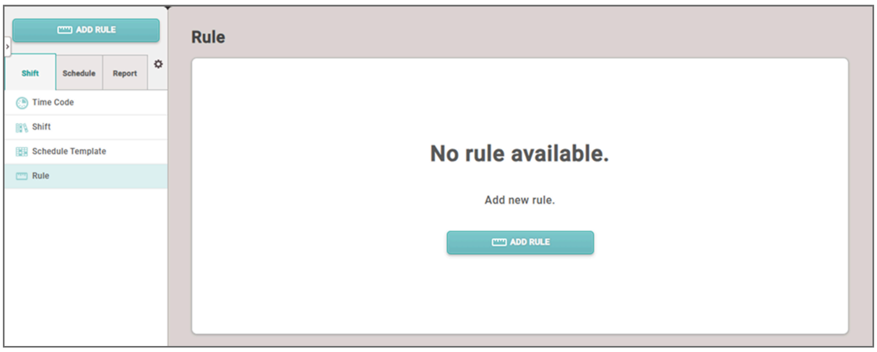
- To apply to all from Monday to Sunday, click **Copy All**.
- To remove the applied Shift, click the 🗑 button.
- Applying the set Shift with **Allowed a day before/after time** cannot be set to have an excess time positioned more than 24 hours before the start time of the daily shift rules.

Set Other Work Rules

This is useful when overtime rules are not added to Shift. The overtime settings in Shift have start and end times, while Rule calculates the total hours beyond the regular working hours. Rule is convenient for managing total overtime hours on a daily, weekly, or monthly basis. When Rule is set, it replaces the overtime rules added to Shift.

ADD RULE

1. Click **T&A** on the **Launcher** page.
2. Click **Shift** → **Rule** in the left sidebar.
3. Click the **ADD RULE** button.



No rule available.

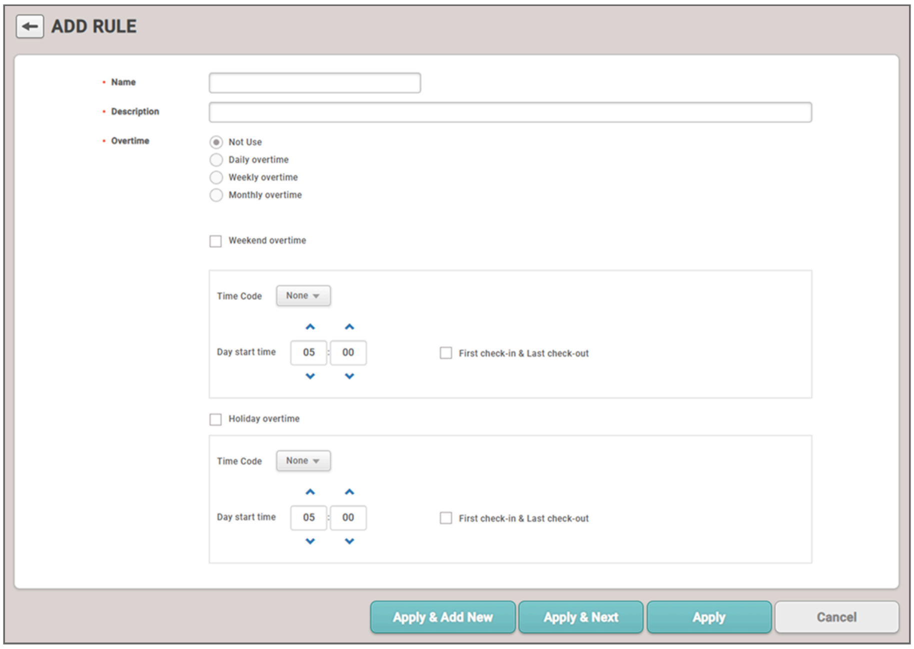
Add new rule.

4. When the **ADD RULE** screen appears, set each item.

> **INFO**
>
> - Click **Apply** at the bottom of the screen to save the settings.
> - To continue adding the work schedule, click the **Apply & Next** button.
> - After saving the settings, click the **Apply & Add New** button to add another **Rule**.

Setting options guide

Set Rule. You can set overtime rules to apply on a daily, weekly, or monthly basis.



- Name
- Description
- Overtime
  - ● Not Use
  - ○ Daily overtime
  - ○ Weekly overtime
  - ○ Monthly overtime

□ Weekend overtime

Time Code: None

Day start time: 05 : 00 □ First check-in & Last check-out

□ Holiday overtime

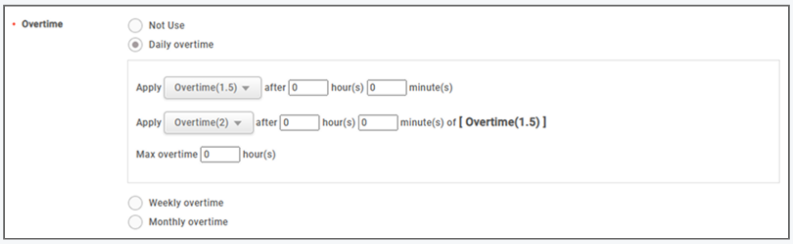
Time Code: None

Day start time: 05 : 00 □ First check-in & Last check-out

- **Name**: Enter the name of Rule.
- **Description**: Enter a description for Rule.
- **Overtime**: Select the overtime rules to apply after the regular working hours on a daily, weekly, or monthly basis. You can apply other overtime rules after a certain period of time. You can also set a maximum overtime limit to restrict the amount of overtime hours an employee can work.

TIP

If set as follows, the **Overtime(1.5)** time rule will apply from 5:00 PM to 11:00 PM when the regular work hours are from 8:00 AM to 5:00 PM, and the **Overtime(2)** time rule will apply from 11:00 PM to 2:00 AM. In addition, daily overtime is restricted to a maximum of 9 hours, and records only until 2:00 AM will be used to calculate daily wages.



- Overtime
  - ○ Not Use
  - ● Daily overtime

Apply Overtime(1.5) after 0 hour(s) 0 minute(s)

Apply Overtime(2) after 0 hour(s) 0 minute(s) of [Overtime(1.5)]

Max overtime 0 hour(s)

- ○ Weekly overtime
- ○ Monthly overtime

INFO

Total working hours do not include breaks or meal times.

- **Weekend overtime** / **Holiday overtime**: Set the work rules to apply on weekends or holidays.
  - **Time Code**: Select the Time Code to apply.
  - **Day start time**: Set the start time of work.
  -

First check-in & Last check-out: Record the time the first user authenticated as the start time and the time the last user authenticated as the end time.

Set the Schedule

You can create work schedules by specifying the set Shift, Rule, duration, and holidays.

You can also add temporary schedules or personal leave to the created work schedule.

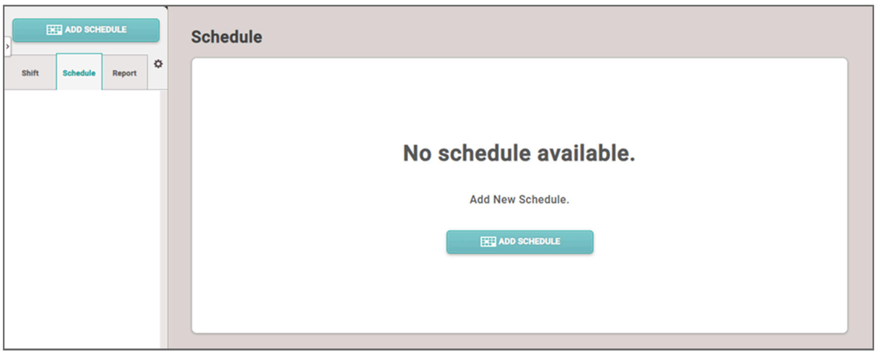
> **INFO**
>
> Before creating the schedule, ensure that you have correctly created the Time Code, Shift, Shift, and holidays.
>
> - For more information about work rule settings, refer to the following:
>   - Set Time Code
>   - Set Daily Shift
>   - Set Weekly Shifts
>   - Set Other Work Rules
> - For more information on holiday settings, refer to the following link.

Set the schedule

Add a schedule

Add the work schedule for the registered users as instructed below.

1. Click **T&A** on the **Launcher** page.
2. Click **Schedule** tab on the left sidebar of the screen.
3. Click **ADD SCHEDULE** button.



No schedule available.

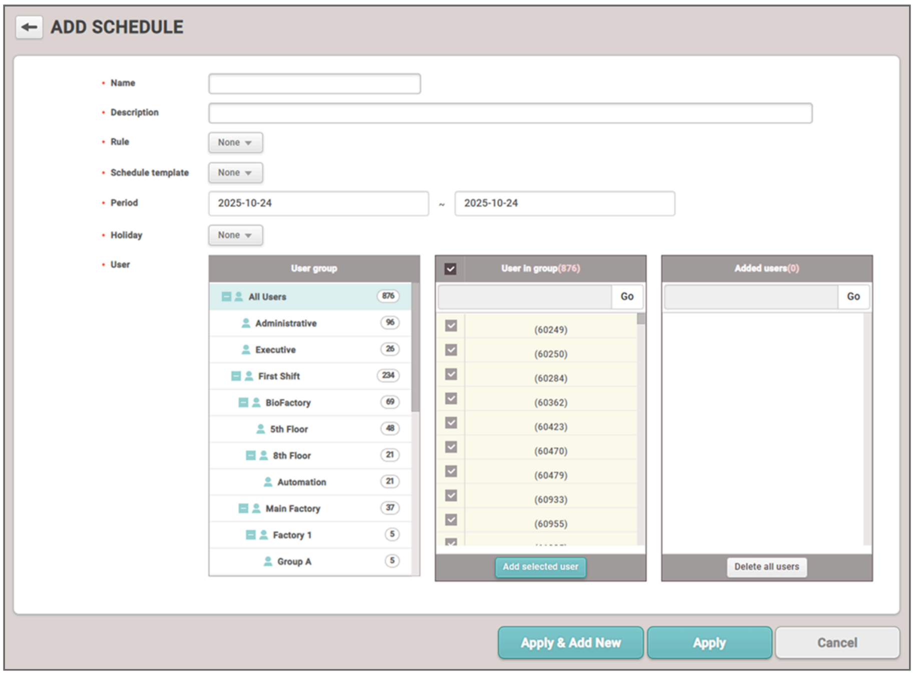
Add New Schedule.

4. When the **ADD SCHEDULE** screen appears, set each item.

> **INFO**
>
> - Click **Apply** at the bottom of the screen to save the settings.
> - After saving the settings, click **Apply & Add New** button to add another **Schedule**.

Setting options guide

Guide for work schedule configuration options.



ADD SCHEDULE

- Name
- Description
- Rule: None
- Schedule template: None
- Period: 2025-10-24 ~ 2025-10-24
- Holiday: None
- User

User group	
All Users	876
Administrative	96
Executive	26
First Shift	234
BioFactory	69
5th Floor	48
8th Floor	21
Automation	21
Main Factory	37
Factory 1	5
Group A	5

☑ User in group(876)

☑ (60249)
☑ (60250)
☑ (60284)
☑ (60362)
☑ (60423)
☑ (60470)
☑ (60479)
☑ (60933)
☑ (60955)

Added users(0)

- **Name**: Enter the name of the work schedule.
- **Description**: Enter a description for the work schedule.
- **Rule**: Select the configured Rule. Setting Rule disregards the overtime rules set on Shift. Select **None** if not in use.

  > **INFO**
  >
  > If the desired Rule is not available, you can add it. For more information, refer to the following.

- **Schedule template**: Select the configured Schedule template. Once set, Schedule template cannot be modified.

  > **INFO**
  >
  > If the desired Schedule template is not available, you can add it. For more information, refer to the following.

- **Period**: Set the period for collecting attendance events.

> **INFO**
>
> The start date cannot be changed once set. The end date can be changed later, and if it is changed to a date earlier than the set date, attendance events for the changed period will be deleted.

- **Holiday**: Select the configured holiday schedule. Select **None** if not in use.

> **INFO**
>
> If the desired holiday schedule is not available, you can add it. For more information, refer to the following.

- **User**: Add users to apply the rules.

> **INFO**
>
> The number of users included in the overall work schedule cannot exceed the maximum supported by your registered attendance management license. The maximum number of users per license is detailed in License Policy.

Edit a schedule

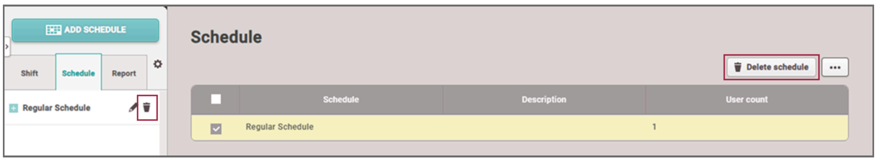
Guide for modifying registered work schedules.

1. Click **T&A** on the **Launcher** page.
2. Click **Schedule** tab on the left sidebar of the screen.
3. Click the item to modify from the **Schedule** list. Alternatively, click the ✎ button for the item to modify on the left sidebar of the screen.
4. Modify the desired item and click the **Apply** button.

Delete a schedule

Guide for deleting registered work schedules.

1. Click **T&A** on the **Launcher** page.
2. Click **Schedule** tab on the left sidebar of the screen.
3. Click the checkbox for the item you want to delete from the **Schedule** list.



Schedule

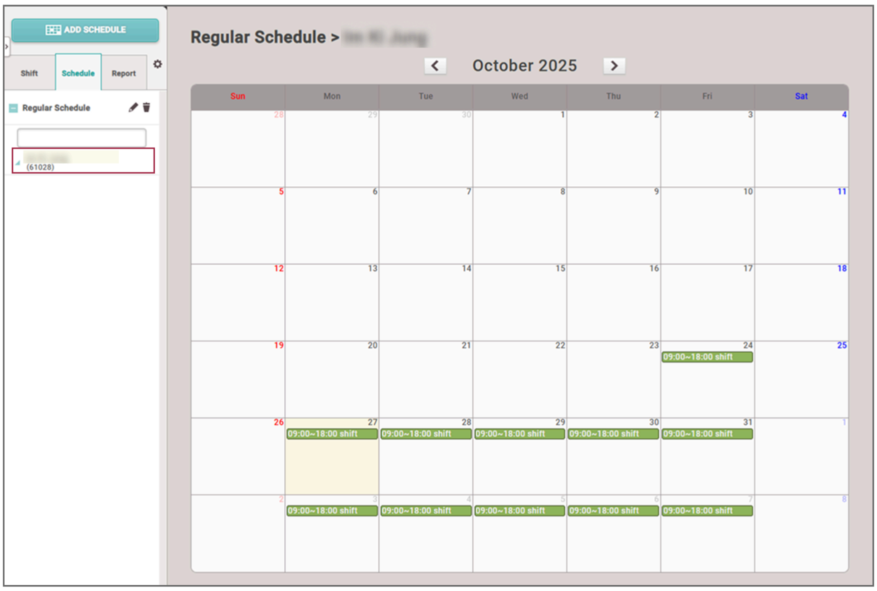
□	Schedule	Description	User count
☑	Regular Schedule		1

4. Click the **Delete schedule** button at the top right of the screen. Alternatively, click the 🗑 button for the item to delete on the left sidebar of the screen.
5. When the confirmation message appears, click **Yes**.

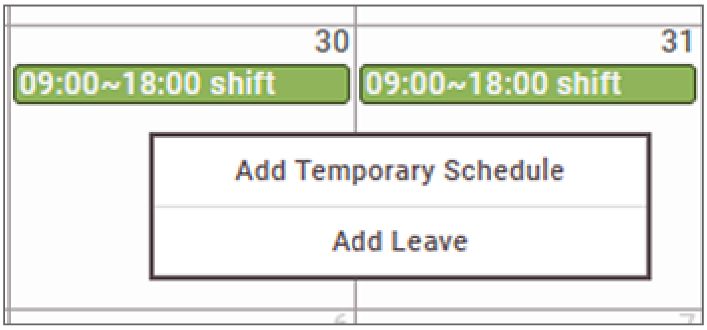
Add a temporary schedule

If a schedule is already registered, a temporary different work rule can be applied to the user.

1. Click **T&A** on the **Launcher** page.
2. Click **Schedule** tab on the left sidebar of the screen.
3. Click the + button for the desired schedule from the list on the left side of the screen.
4. A list of users assigned to the schedule will appear, and selecting a user to apply a temporary schedule will show the calendar.

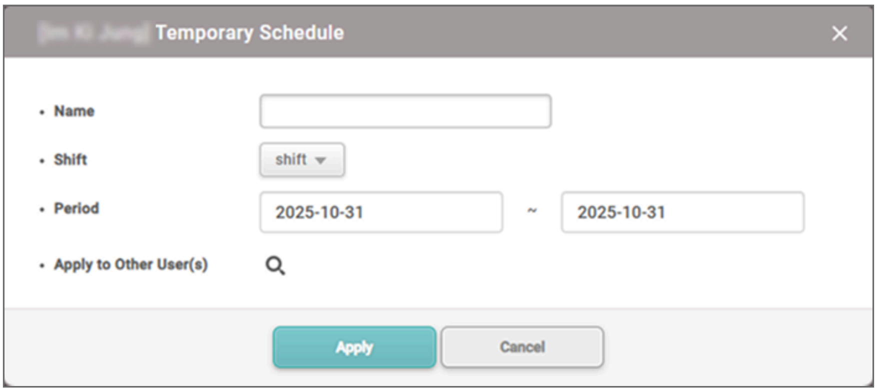


5. Click the date to which you want to add a temporary schedule on the calendar.



6. Click **Add Temporary Schedule** in the popup menu.

7. When the **Add Temporary Schedule** settings window appears, set each item.



[redacted] Temporary Schedule ✕

- Name
- Shift: shift ▾
- Period: 2025-10-31 ~ 2025-10-31
- Apply to Other User(s)

To apply the same work schedule to other users, click the 🔍 button and select the users.

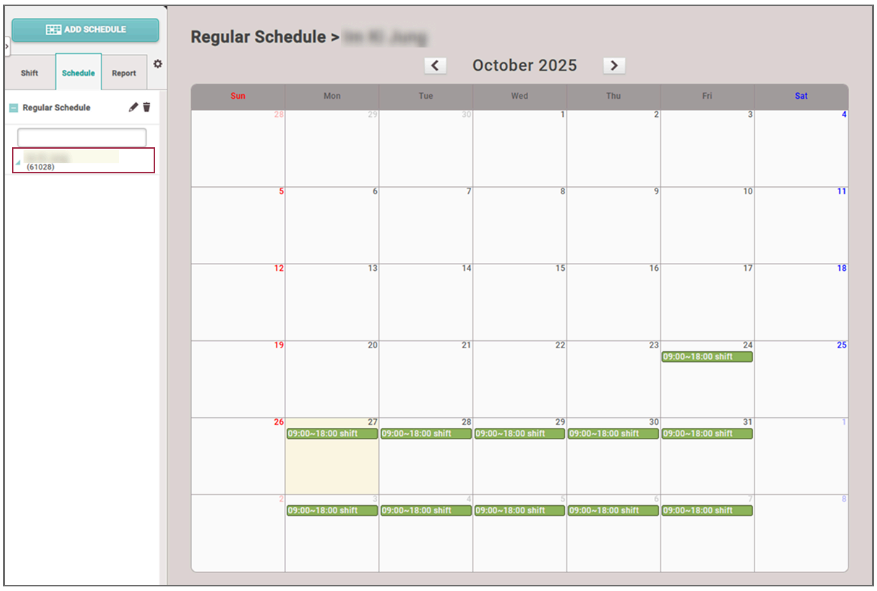
8. Click the **Apply** button to apply the set work rules.

> ⓘ **INFO**
>
> To delete the temporary schedule applied to the user, click the set temporary schedule on the calendar. Click the **Yes** button when the confirmation message window appears.

Add and remove a leave

You can add a user's personal leave schedule.

1. Click **T&A** on the **Launcher** page.
2. Click **Schedule** tab on the left sidebar of the screen.
3. Click the + button for the desired schedule from the list on the left side of the screen.
4. A list of users assigned to the schedule will appear, and selecting a user to apply the absence schedule will show the calendar.

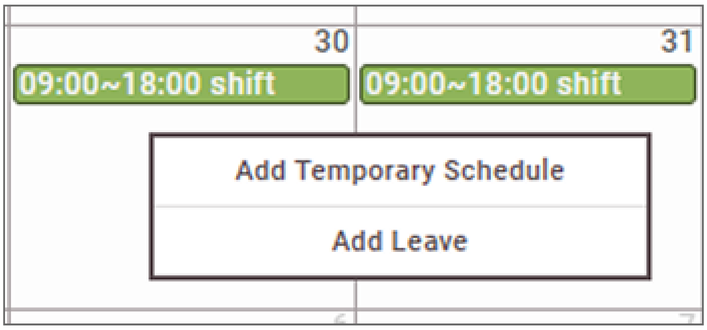


Regular Schedule > [redacted]

October 2025

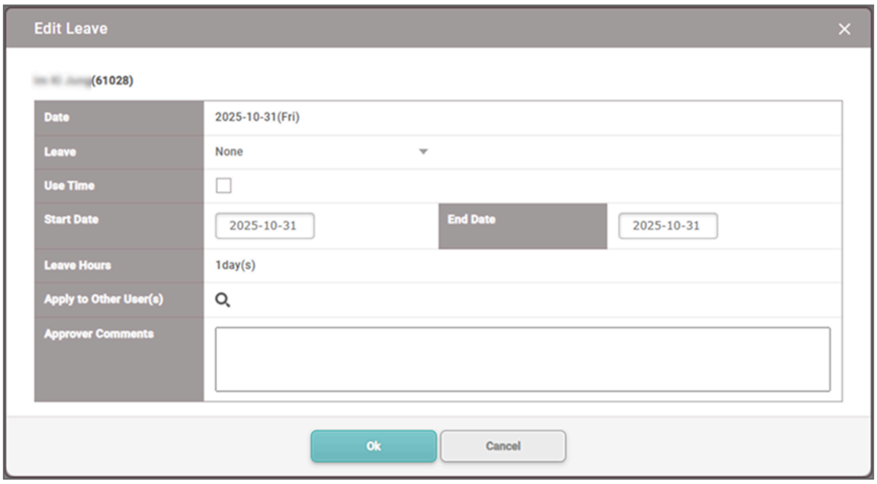
Sun	Mon	Tue	Wed	Thu	Fri	Sat
28	29	30	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24 09:00~18:00 shift	25
26	27 09:00~18:00 shift	28 09:00~18:00 shift	29 09:00~18:00 shift	30 09:00~18:00 shift	31 09:00~18:00 shift	1
2	3 09:00~18:00 shift	4 09:00~18:00 shift	5 09:00~18:00 shift	6 09:00~18:00 shift	7 09:00~18:00 shift	8

5. Click the date on the calendar to add the user's absence schedule.



6. Click **Add Leave** in the popup menu.

7. When the **Edit Leave** settings window appears, set each item.



Edit Leave

[redacted](61028)

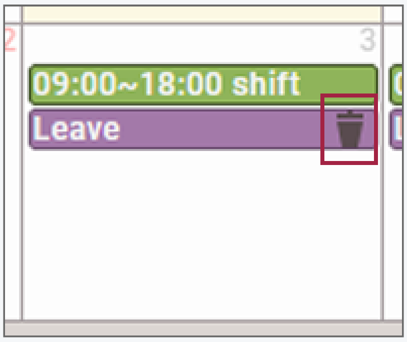
Date	2025-10-31(Fri)		
Leave	None		
Use Time	□		
Start Date	2025-10-31	End Date	2025-10-31
Leave Hours	1day(s)		
Apply to Other User(s)			
Approver Comments			

To apply the same absence schedule to other users, click the 🔍 button and select the users.

8. Click the **Apply** button to apply the set absence schedule.

INFO

- If the desired absence management time rules are not available, you can add them. For more information on adding time rules, refer to the following.
- To delete the absence schedule applied to the user, click the 🗑 button for the set absence schedule on the calendar. Click the **Yes** button when the confirmation message window appears.



View the Report

You can generate T&A reports from user attendance events collected through the system, and edit time records or export them as CSV or PDF files.

Easily use the pre-set 7 report filters, and administrators can set filters themselves.

Before start

Before using the multilingual report

BioStar X supports both Korean and English by default. To use multilingual reports, set your desired language according to the following instructions.

1. Navigate to the following path. *C:\Program Files\BioStar X\plugin\ta\dist\setup\report_fonts*
2. Create a folder with the name of the language you want to use. Refer to the ISO 639-1 standards for language names. For example, to use Spanish, create a folder named "es."
3. Copy and paste the fonts into the created folder. Only one TrueType font is supported.

Before updating the report,

BioStar X uses MariaDB as the default database. If you are using MS SQL Server database, please check the following items first.

When using **BioStar X** with MS SQL Server, if there are many registered users, the memory usage on the PC may accumulate each time the report is updated. Reset the maximum server memory of the MS SQL Server database.

1. Run **Microsoft SQL Server Management Studio**.
2. Right-click on the **BioStar X** database in the object explorer.
3. Click on **Properties** in the popup menu.
4. Click **Memory** and reduce the value of **Maximum server memory** item.

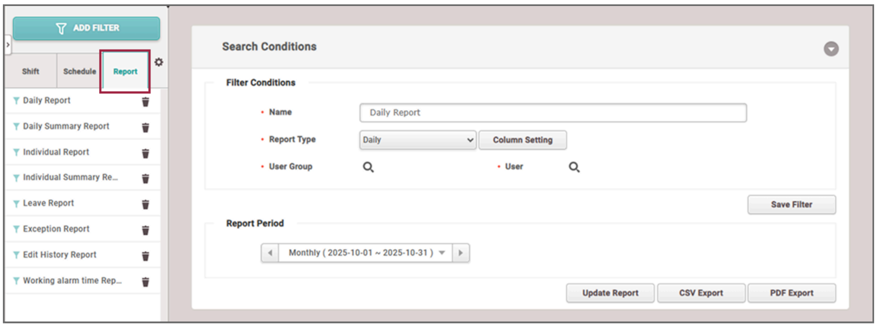
> **INFO**
>
> For more information on MariaDB and MS SQL Server settings during **BioStar X** installation, refer to the following.

Check the report

Generate the report

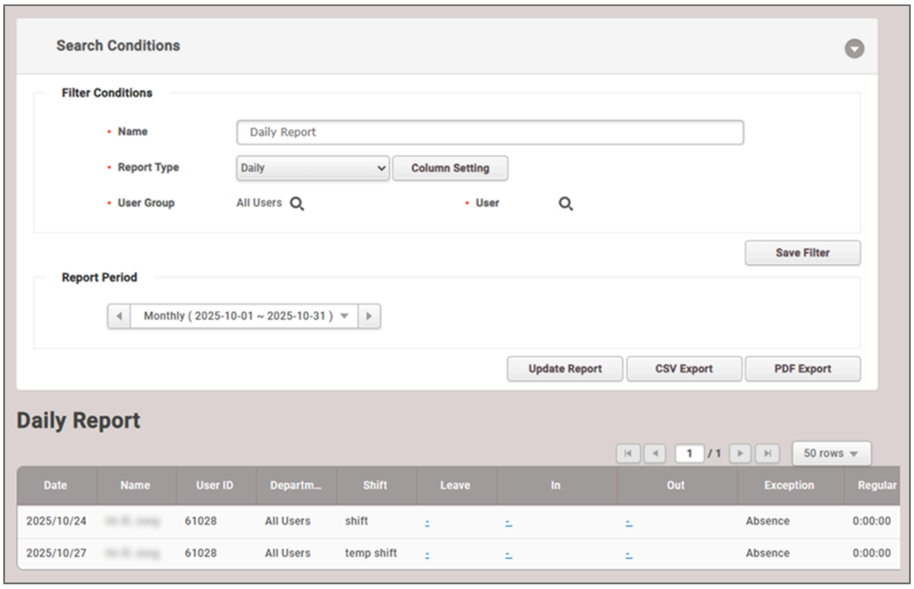
This provides instructions on generating attendance records reports for registered users.

1. Click **T&A** on the **Launcher** page.
2. Click the **Report** tab on the left sidebar of the screen.



- Name: Daily Report
- Report Type: Daily
- User Group
- User
- Monthly (2025-10-01 ~ 2025-10-31)

3. Click the desired report filter item from the left sidebar of the screen.
4. In **User Group** or **User**, click the 🔍 button, then specify the group or user.
5. To generate the report, click the **Update Report** button.
6. When the list of reports appears at the bottom of the screen, you can click the desired item to view details.



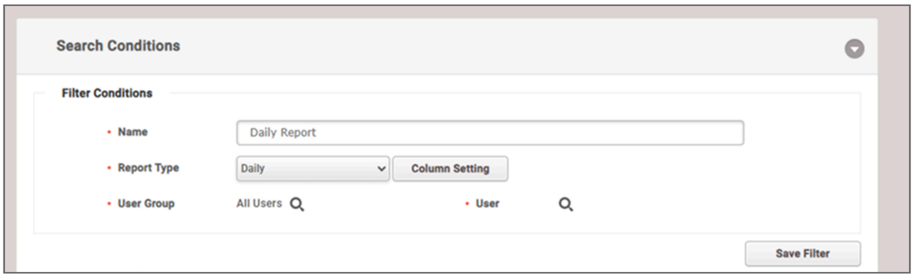
- Name: Daily Report
- Report Type: Daily
- User Group: All Users
- User
- Monthly (2025-10-01 ~ 2025-10-31)

Daily Report

Date	Name	User ID	Departm...	Shift	Leave	In	Out	Exception	Regular
2025/10/24	[redacted]	61028	All Users	shift	-	-	-	Absence	0:00:00
2025/10/27	[redacted]	61028	All Users	temp shift	-	-	-	Absence	0:00:00

Set the filter conditions

You can set filter conditions to generate a new T&A record report.

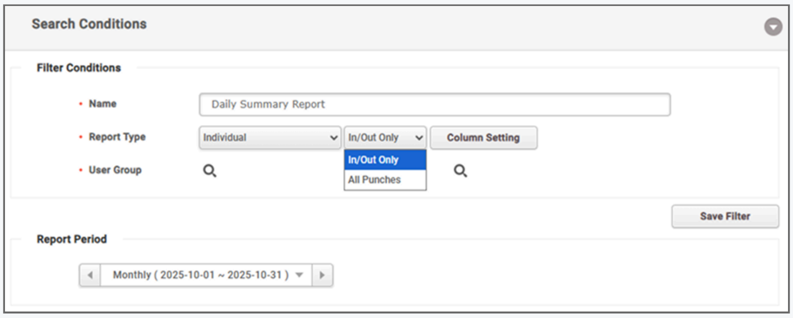


Search Conditions

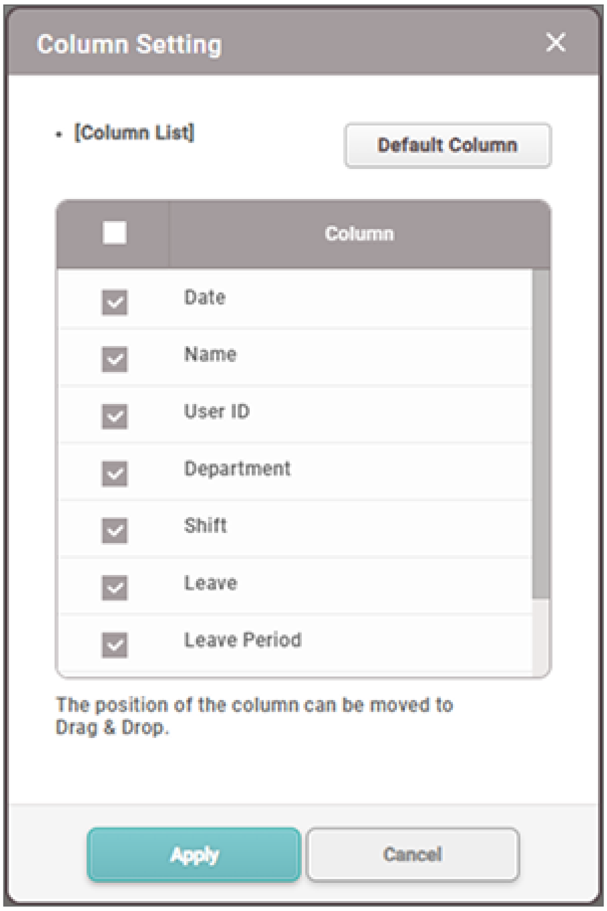
Filter Conditions

- Name: Daily Report
- Report Type: Daily
- User Group: All Users
- User

- **Name**: Enter the report name.
- **Report Type**: Select the desired report type. The available report types are as follows.
  - **Daily**, **Daily Summary**, **Individual**, **Individual Summary**, **Leave**, **Exception**, **Modified Punch Log History**, **Working alarm time**

> **INFO**
>
> By selecting **Report Type** as **Individual**, you can set whether to output user entry records.
>
> 
>
> Search Conditions
>
> Filter Conditions
>
> - Name: Daily Summary Report
> - Report Type: Individual, In/Out Only
> - User Group
>
> Report Period: Monthly (2025-10-01 ~ 2025-10-31)
>
>
>
> - **In/Out Only**: This outputs only the user's check-in and check-out records in the report.
> - **All Punches**: This outputs all user entry records in the report.

- **Column Setting**: You can change the order of the report table columns or hide them.



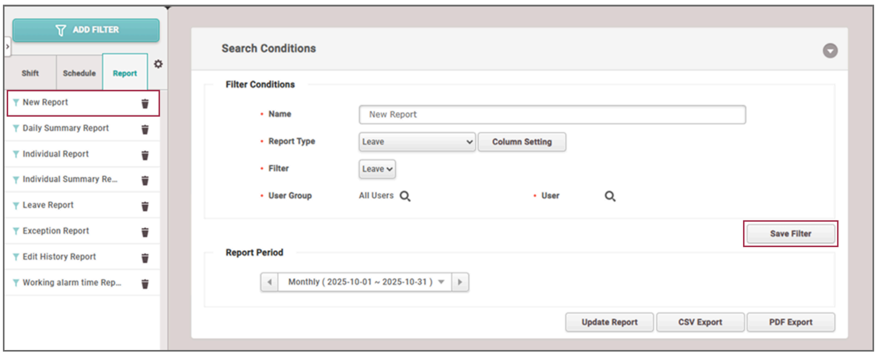
- [Column List]

☐	Column
☑	Date
☑	Name
☑	User ID
☑	Department
☑	Shift
☑	Leave
☑	Leave Period

The position of the column can be moved to Drag & Drop.

> **INFO**
>
> After changing the column order, click the **Default Column** button to restore to defaults.

- **Filter**: This will only activate when **Report Type** is set to **Leave** or **Exception**, and you can choose specific conditions for absence or exception records.
- **User Group** / **User**: Select the user group or user for report generation.
- **Save Filter**: You can save the configured attendance report as a filter.



Filter Conditions

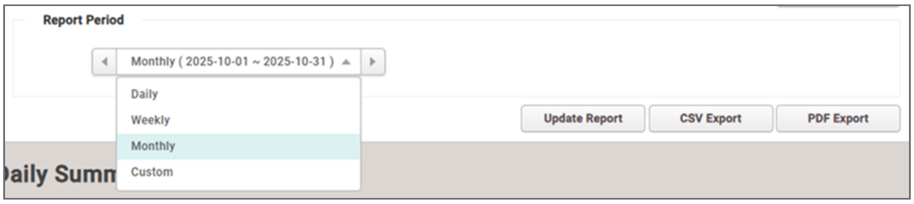
- Name: New Report
- Report Type: Leave | Column Setting
- Filter: Leave
- User Group: All Users
- User:

Report Period

Monthly (2025-10-01 ~ 2025-10-31)

Set report period

This provides instructions on setting the report period.



Report Period

Monthly (2025-10-01 ~ 2025-10-31)

You can set the report period to **Daily**, **Weekly**, or **Monthly**. To generate a report for a specific period, select **Custom**.

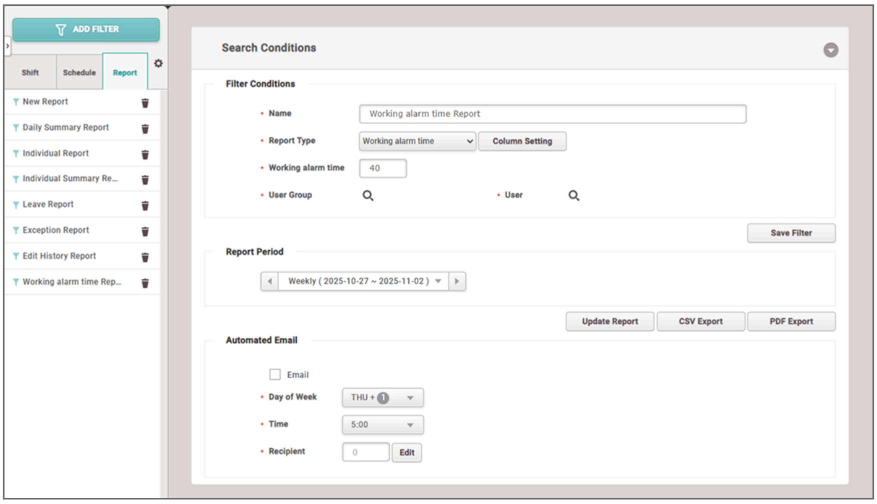
Export report

- **CSV Export**: You can save the generated report as a CSV file.
- **PDF Export**: You can save the generated report as a PDF file.

Generate working alarm time report

You can generate T&A reports for users who have reached the designated working hours or notify the administrator via email. The alert working hours report is generated weekly.

1. Click **T&A** on the **Launcher** page.
2. Click the **Report** tab on the left sidebar of the screen.
3. Click **Working Alarm Time Report** in the filter list on the left sidebar.



Search Conditions

Filter Conditions

- Name: Working alarm time Report
- Report Type: Working alarm time
- Working alarm time: 40
- User Group
- User

Report Period

Weekly (2025-10-27 ~ 2025-11-02)

Automated Email

□ Email

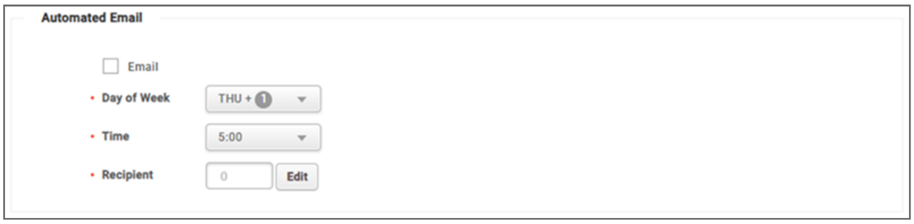
- Day of Week: THU + 1
- Time: 5:00
- Recipient: 0

4. Set each item in **Filter Conditions** and **Report Period**.
5. To generate the report, click the **Update Report** button.

> **INFO**
>
> To send notifications to the administrator via email for users who have reached the designated working hours, set **Automated Email**. For more information, refer to the following.

Automated email setting

You can automatically send alarm emails to the administrator for users who have reached the designated working hours.

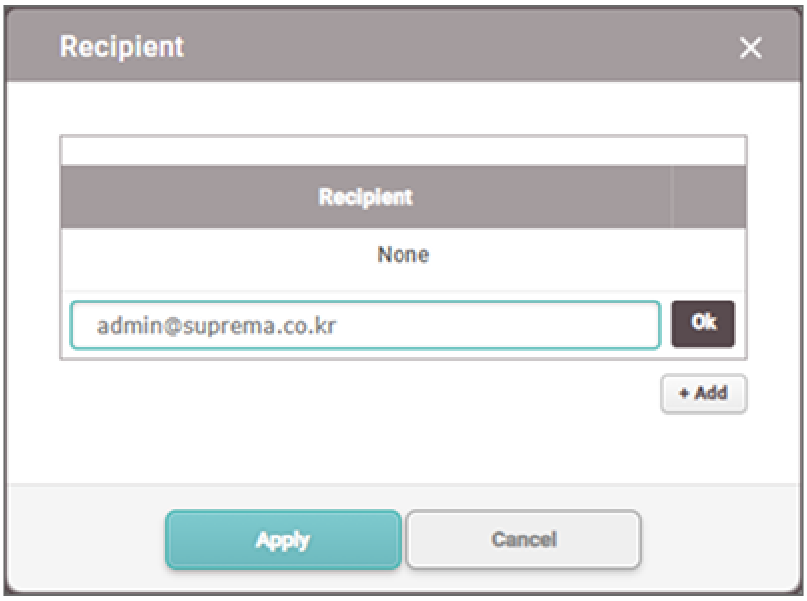


Automated Email

□ Email

- Day of Week: THU + 1
- Time: 5:00
- Recipient: 0 Edit

- **Email**: Click the checkbox to automatically send emails to the administrator.
- **Day of Week**: Select the day of the week to send emails to the administrator.
- **Time**: Set the time to send emails to the administrator.
- **Recipient**: You can specify the administrator who will receive the email. Click the **Edit** button to open the **Recipient** popup window. Enter the email address. You can specify more than one administrator.



Recipient

Recipient
None

admin@suprema.co.kr

INFO

- To set the **Automated Email** feature, you must set filter conditions and then save the filter.
- The sender information of automatically sent emails can be set in **Setting**(⚙) → **Sender Information** in the left sidebar of the screen. For more information, refer to the following.

Edit T&A Report

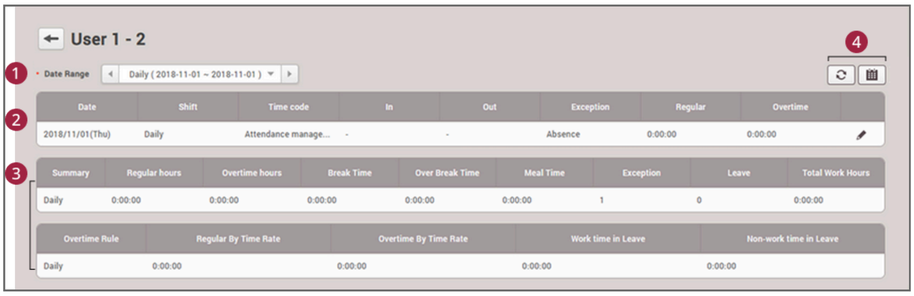
Click the generated report table to modify attendance records.

INFO

- You must first generate a report to modify the attendance records. For more information on report generation, refer to the following.
- Records of users without an attendance schedule cannot be modified.

1. Click the item in the list of generated reports to modify the record.
2. Modify the attendance records or add absences as desired.

Edit in the list



Date	Shift	Time code	In	Out	Exception	Regular	Overtime	
2018/11/01(Thu)	Daily	Attendance manage...	-	-	Absence	0:00:00	0:00:00	✎

Summary	Regular hours	Overtime hours	Break Time	Over Break Time	Meal Time	Exception	Leave	Total Work Hours
Daily	0:00:00	0:00:00	0:00:00	0:00:00	0:00:00	1	0	0:00:00

Overtime Rule	Regular By Time Rate	Overtime By Time Rate	Work time in Leave	Non-work time in Leave
Daily	0:00:00	0:00:00	0:00:00	0:00:00

1 **Date Range**: Set the period for attendance records to display in the list.

2 **Daily attendance record**: Shows the daily attendance record.

- Click in/out times to add/modify/delete attendance records. After clicking the in/out times, click the ✎ button to modify the registered attendance record, and click the **Apply** button to save changes.
- Click the ✎ button to add an absence. You need a time code set as absence to add vacation. Click 🗑 for the added user absence to delete it.

3 **Attendance record summary**: You can check attendance records for the specified period.

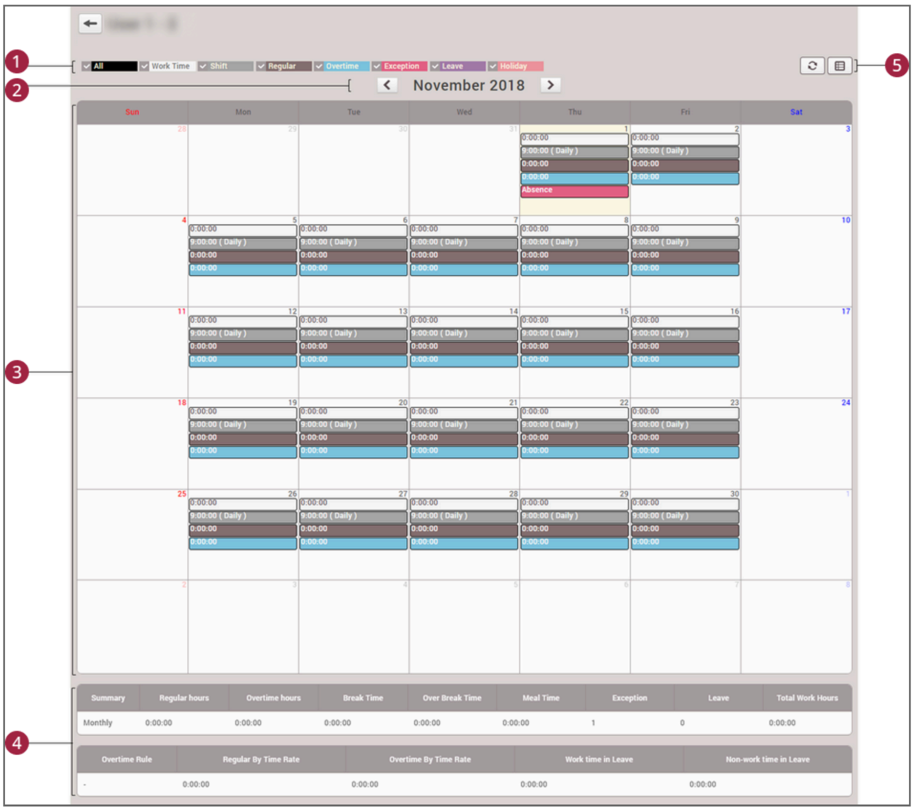
4 **Refresh / View in calendar**

- ⟳ : Refresh the attendance record list.
- 📅 : View attendance records in a calendar format.

ⓘ **INFO**

For more information on creating time codes, refer to the following.

Edit in the calendar



Summary	Regular hours	Overtime hours	Break Time	Over Break Time	Meal Time	Exception	Leave	Total Work Hours
Monthly	0:00:00	0:00:00	0:00:00	0:00:00	0:00:00	1	0	0:00:00

Overtime Rule	Regular By Time Rate	Overtime By Time Rate	Work time in Leave	Non-work time in Leave
-	0:00:00	0:00:00	0:00:00	0:00:00

1 **Event type**: You can select or hide event types to appear on the calendar.

2 **Month**: Click ‹ or › to move to the previous or next month.

3 **Daily attendance record**: Shows the daily attendance record.

- Click working hours (in white) to add/modify/delete attendance records. Click the ✎ button to modify the registered attendance record, and click the **Apply** button to save changes.
- Click working rules (in gray) to add user absence management. You need a time code set as absence to add user absence. Click 🗑 for the added user absence to delete it.

4 **Attendance record summary**: Shows the monthly attendance record.

5 **Refresh / View in list**

- ⟳ : Refresh the attendance record list.
- ▤ : View attendance records in a list format.

INFO

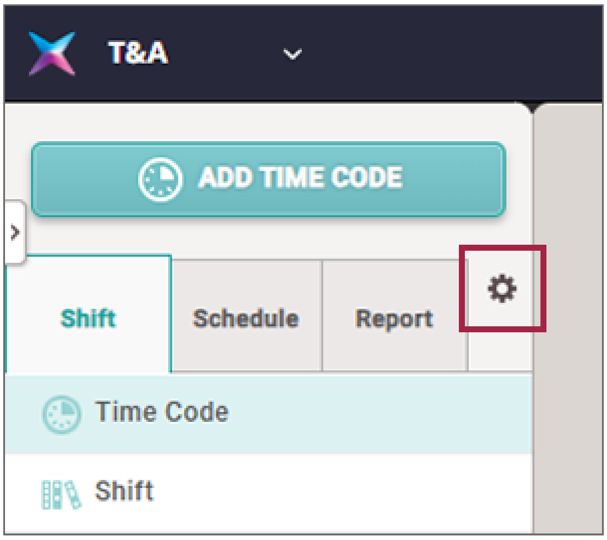
For more information on creating time codes, refer to the following.

Set Time & Attendance

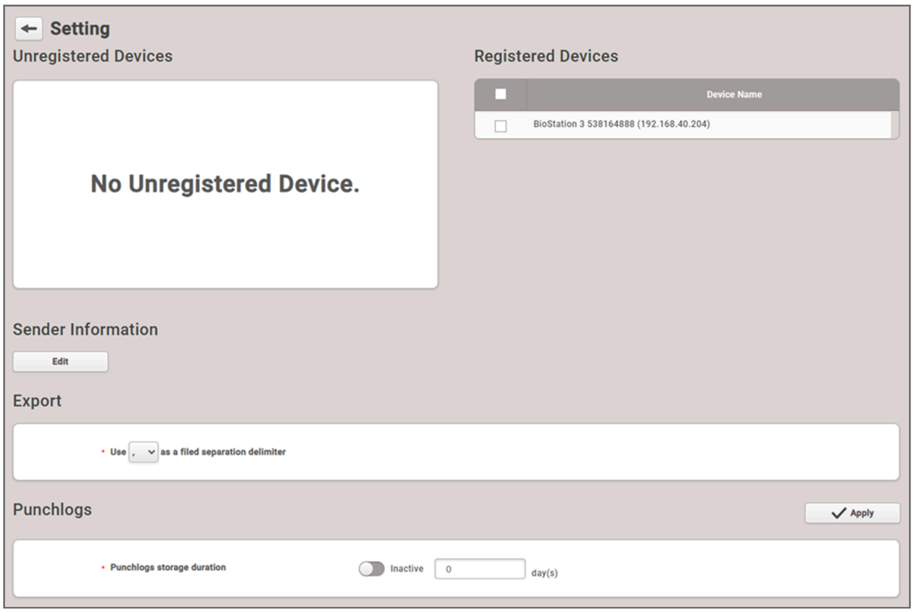
You can register devices to use for attendance management or set the sender information to be used when sending notification emails. You can also set the document delimiter for exporting attendance reports via CSV.

Access attendance management settings

1. Click **T&A** on the **Launcher** page.
2. Click ⚙ on the left sidebar.



3. Edit the necessary fields.



Setting

Unregistered Devices

No Unregistered Device.

Registered Devices

■	Device Name
□	BioStation 3 538164888 (192.168.40.204)

Sender Information

Edit

Export

- Use , as a filed separation delimiter

Punchlogs

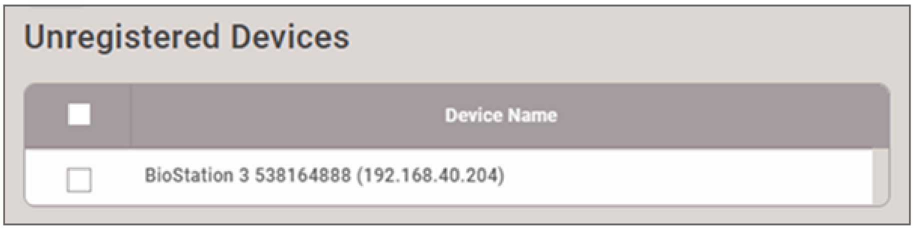
✓ Apply

- Punchlogs storage duration Inactive 0 day(s)

Attendance management settings

Unregistered Devices

List of devices that can be used for attendance management. To register as an attendance management device, select the desired device and click **Register**.



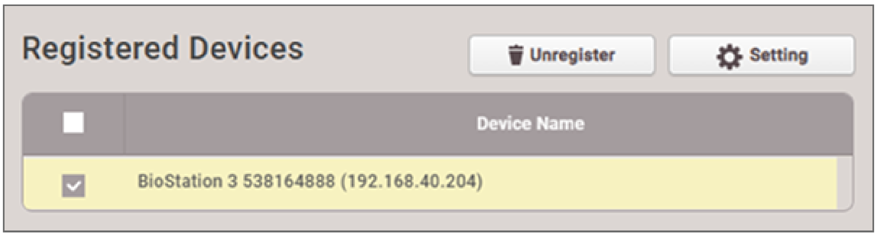
Unregistered Devices

□	Device Name
□	BioStation 3 538164888 (192.168.40.204)

Registered Devices

List of devices currently used for attendance management.

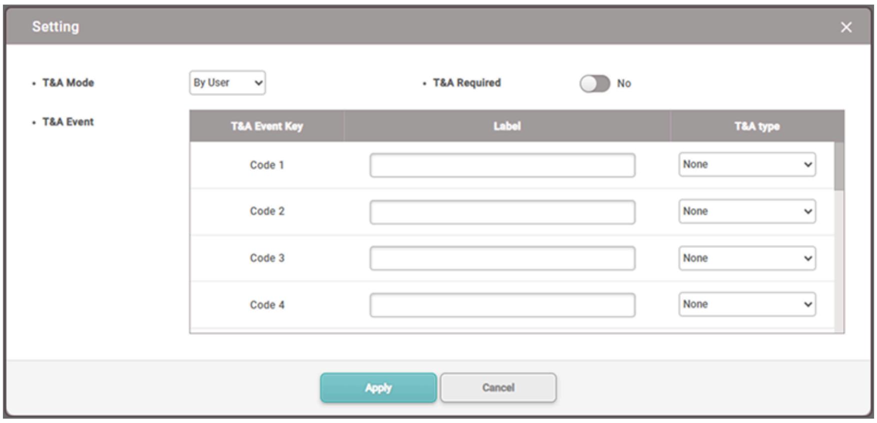
- To unregister, select the desired device and click **Unregister**.



Registered Devices

□	Device Name
☑	BioStation 3 538164888 (192.168.40.204)

- To edit the attendance settings of a registered device, click **Setting**. For more information on attendance settings, refer to the following link.



Setting

- T&A Mode: By User
- T&A Required: No
- T&A Event

T&A Event Key	Label	T&A type
Code 1		None
Code 2		None
Code 3		None
Code 4		None

T&A type is a setting to map **T&A Event Key** with attendance event types. Attendance event types are as follows:

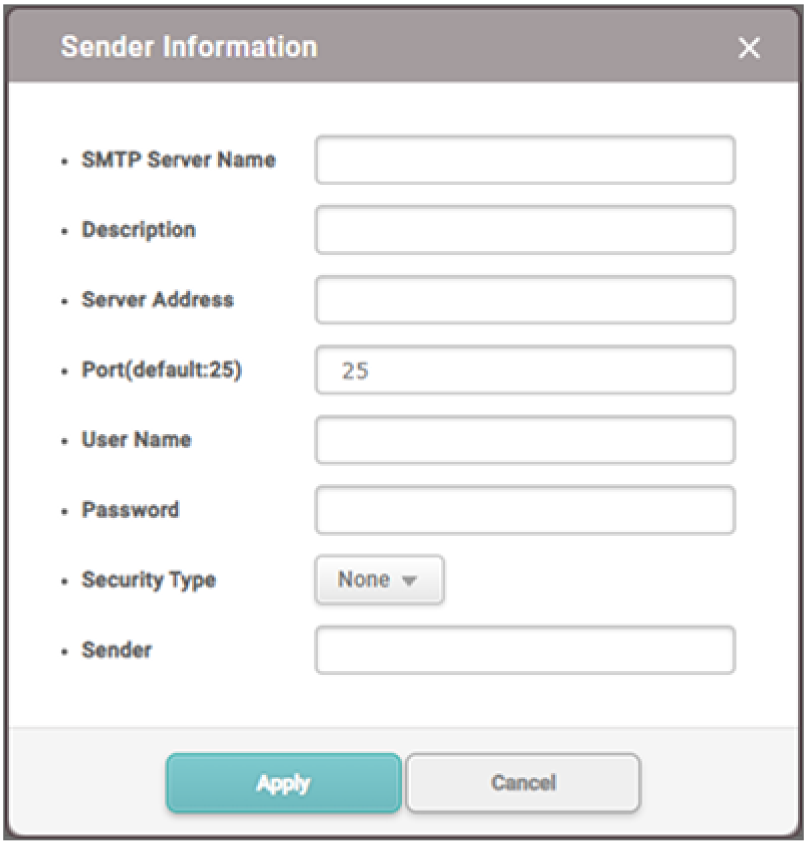
- – **Check In**
- – **Check Out**

- **Break Start**
- **Break End**
- **Meal Time Start**
- **Meal Time End**

> **INFO**
>
> - You can only edit the attendance settings of a device when connected to the device.
> - If you delete a registered device from the **Settings** → **Device** menu, the registered attendance management device will also be automatically deleted.

Sender Information

You can set the sender information to be used when sending notification emails. Click **Edit**.



Sender Information

- SMTP Server Name
- Description
- Server Address
- Port(default:25): 25
- User Name
- Password
- Security Type: None
- Sender

- **SMTP Server Name**: Enter the SMTP server name.
- **Description**: Enter the description.
- **Port(default:25)**: Enter the port number of the SMTP server. The SMTP server address is in the format `smtp.{email-service-provider}.com`, and you can confirm it on the settings screen of the email used as the SMTP server.
- **Server Address**: Enter the SMTP server address. Email Service Provider.com', and you can check it on the

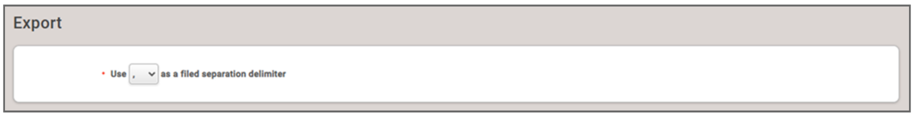
settings screen of email to use as an SMTP.

- **User Name**: Enter the account of the SMTP service.
- **Password**: Enter the password of the SMTP service.
- **Security Type**: Select security type.
- **Sender**: Enter the email address of the sender.

> **INFO**
>
> - For more information about SMTP information, contact your system administrator.
> - When using the SMTP server as an email account with two-factor authentication and change the password of the account, note the following: Once you set up two-factor authentication, the SMTP password is the same as the app password generated using two-factor authentication, not the password of the email account.
>   - When you set up two-step authentication, the SMTP password uses the app password generated by two-step authentication, not the password for the email account.
>   - At this time, if the password of the email account is changed, the app password is automatically deleted, and the SMTP password is no longer available.
>   - When changing the password for the email account, regenerate the app password and then set the SMTP password again.

Export

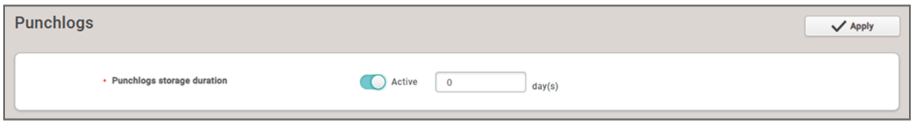
With the **CSV Export** feature, you can choose the document delimiter when exporting attendance reports.



• Use , as a filed separation delimiter

Punchlogs

You can set the period to store attendance records. Set the **Punchlogs storage duration** option to **Active** and enter the period. To save the settings, click **Apply**.



• Punchlogs storage duration ● Active 0 day(s)

Manage Visitors

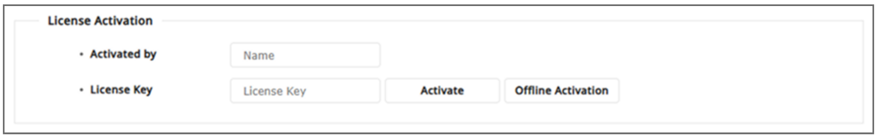
Use the **Visitor** feature to create a visitor application page on the application PC, and manage visitor access on the management PC.

> **INFO**
>
> - The **Visitor** feature is available with additional options on **Advanced** or higher license. For more information on licensing policy, refer to the following.
> - After activating the visitor feature through licensing, refer to the following for detailed setup instructions.

Applying visitor license

This guide explains how to apply the visitor license. After purchasing the Visitor license from the **BioStar X** retailer, follow the instructions below to apply the license.

1. Log in with the **BioStar X** administrator account.
2. Click **Settings** on the **Launcher** page.
3. Click **License** → **BioStar X License** in the left sidebar.
4. Enter **License Activation** in sequence with **Activated by** and **License Key**.



License Activation

- Activated by: Name
- License Key: License Key

5. Click Activate.

You can check the licensed registered in **Activated License**.

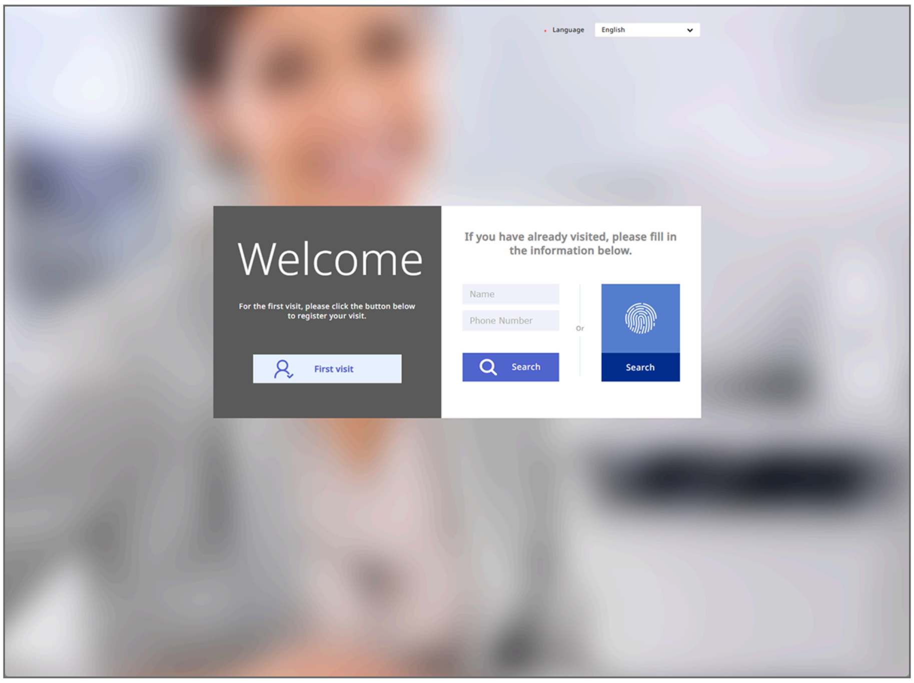
> **INFO**
>
> To activate your license in a closed network environment or an offline state with limited internet access, refer to the following.

> **TIP**
>
> Applying the visitor license activates the **Settings** → **Visitor** menu, and adds a link to the management page of **Visitor** in the shortcuts list on the top left of the screen.

Visitor application page settings

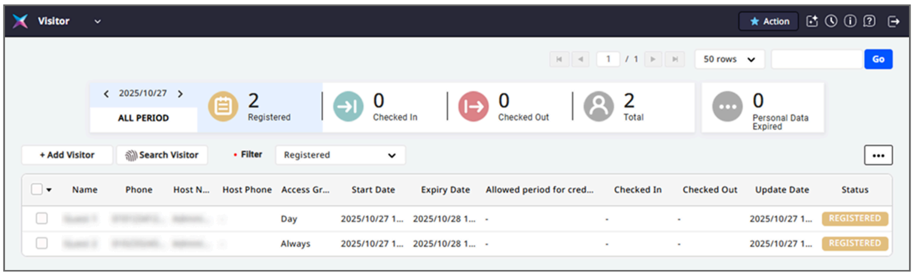
The visitor application page can be used after prioritizing visitor settings. Refer to the following for detailed instructions on setting up the visitor application page.

The visitor application page can be accessed from a dedicated application PC, allowing visitors to submit access requests. For more information on visitor applications, refer to the following.


Language
English
Welcome
For the first visit, please click the button below to register your visit.
First visit
If you have already visited, please fill in the information below.
Name
Phone Number
Or
Search
Search

Visitor access management

Check the visitor application history and manage visitor access. For more information on managing visitor access, refer to the following.



□	Name	Phone	Host N...	Host Phone	Access Gr...	Start Date	Expiry Date	Allowed period for cred...	Checked In	Checked Out	Update Date	Status
□	[redacted]	[redacted]	[redacted]	[redacted]	Day	2025/10/27 1...	2025/10/28 1...	-	-	-	2025/10/27 1...	REGISTERED
□	[redacted]	[redacted]	[redacted]	[redacted]	Always	2025/10/27 1...	2025/10/28 1...	-	-	-	2025/10/27 1...	REGISTERED

Apply to Visit

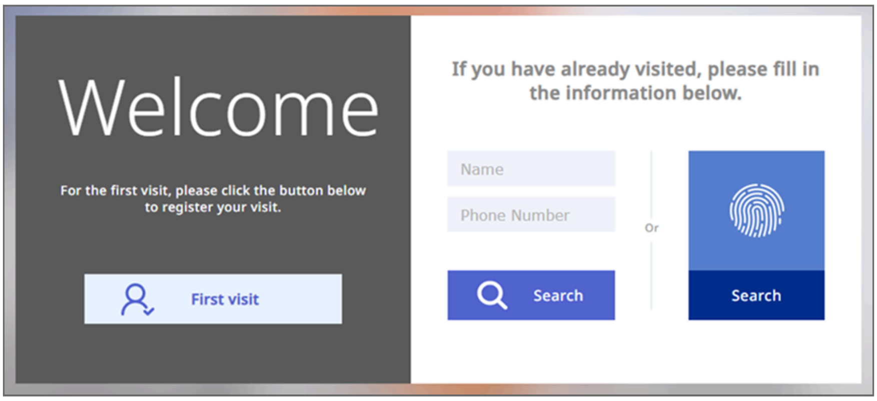
This guides how external visitors who are not internal users apply for entry using the visitor application PC.

> **INFO**
>
> - The visitor application PC must be configured separately, and visitor settings must precede it. For more information on how to set up visitor settings, refer to the following.
> - If there is no shortcut icon for the visitor application page on the visitor application PC, refer to the following to create a shortcut icon.

New visitor application

This guides how first-time visitors apply for entry using the visitor application PC.

1. Run the visitor application page on the visitor application PC. The URL address for the visitor application page is in the format `https://{biostar_x_server_ip}/#/register-welcome`.



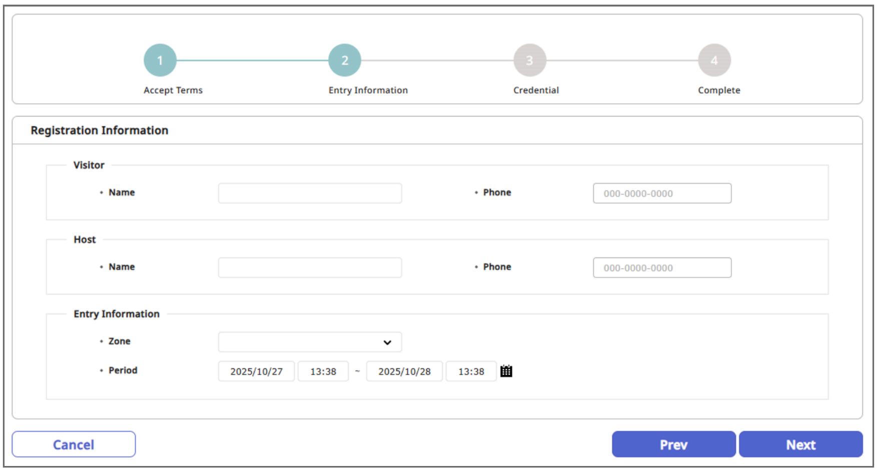
Welcome

For the first visit, please click the button below to register your visit.

If you have already visited, please fill in the information below.

2. Click **First visit** in the center of the screen.
3. After agreeing to the terms and privacy policy regarding access to the visiting department, click the **Next** button in the lower right corner of the screen.

4. Enter the information required for the visit application.



Registration Information

Visitor

- Name
- Phone 000-0000-0000

Host

- Name
- Phone 000-0000-0000

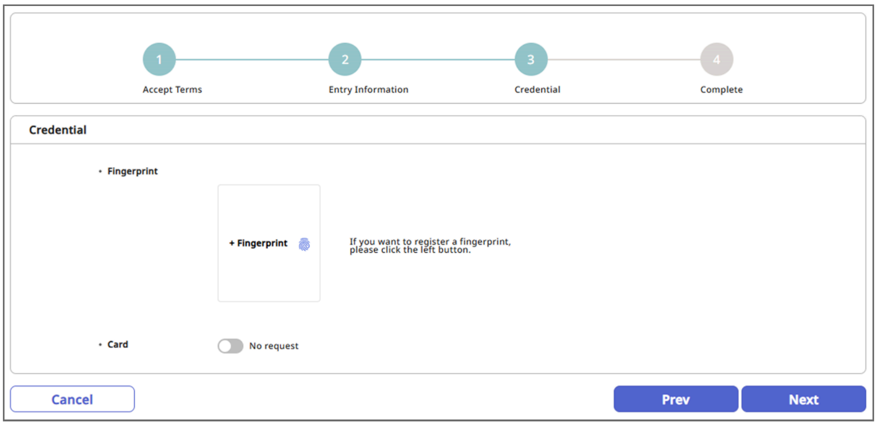
Entry Information

- Zone
- Period 2025/10/27 13:38 ~ 2025/10/28 13:38

- **Visitor**: Enter the visitor's name and phone number.
- **Host**: Enter the name and phone number of the person responsible for the visit destination.
- **Entry Information**: Set the access area and visit duration.

5. After entering the information, click the **Next** button in the lower right corner of the screen.

6. Set the means of entry.



Credential

- Fingerprint

If you want to register a fingerprint, please click the left button.

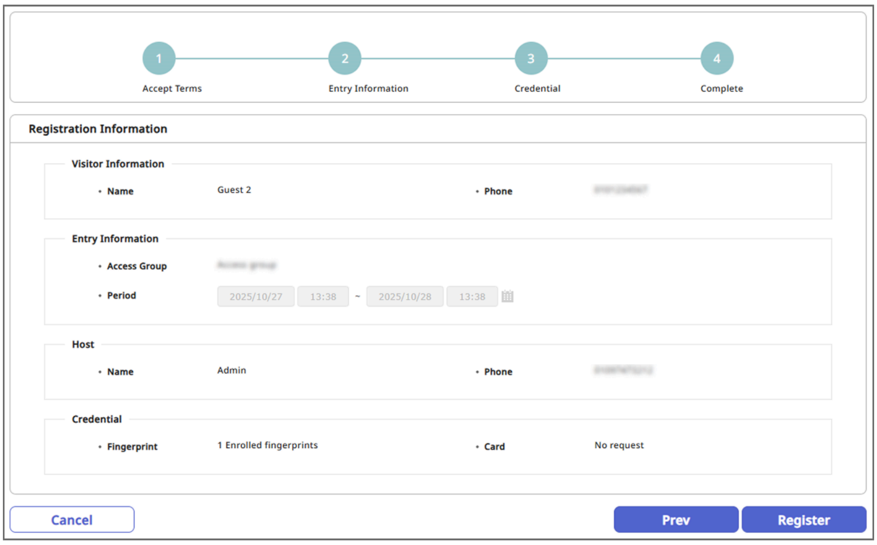
- Card

No request

- **Fingerprint**: To use fingerprint authentication, click the **+ Fingerprint** button and then enroll your fingerprint.
- **Card**: To use card authentication, set it up with **Request** and receive a card from the administrator.

7. After completing the settings, click the **Next** button in the lower right corner of the screen.

8. After confirming all the information provided, click the **Register** button in the lower right corner of the screen.



Registration Information

Visitor Information

- Name: Guest 2
- Phone: [redacted]

Entry Information

- Access Group: [redacted]
- Period: 2025/10/27 13:38 ~ 2025/10/28 13:38

Host

- Name: Admin
- Phone: [redacted]

Credential

- Fingerprint: 1 Enrolled fingerprints
- Card: No request

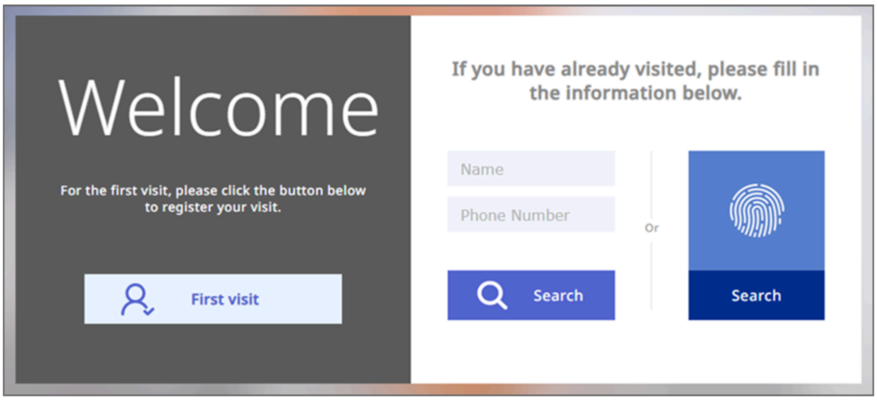
INFO

- For more information on writing terms and privacy policies regarding access to the visiting department, refer to the following.
- The name can be entered up to 48 characters long.
- To add custom fields to visitor information input, refer to the following.
- You can only select access groups assigned to the visiting department for the visit PC. For more information, refer to the following.
- For more information on access groups, refer to the following.
- To return to the previous step and modify the visit information, click the **Prev** button.
- To scan fingerprints, a fingerprint registration device must be connected to the visitor application PC.

Apply using existing information

If a fingerprint is enrolled at the visiting location, you can search for the fingerprint and apply for a visit using the existing visit information.

1. Run the visitor application page on the visitor application PC. The URL address for the visitor application page is in the format `https://{biostar_x_server_ip}/#/register-welcome`.



Welcome

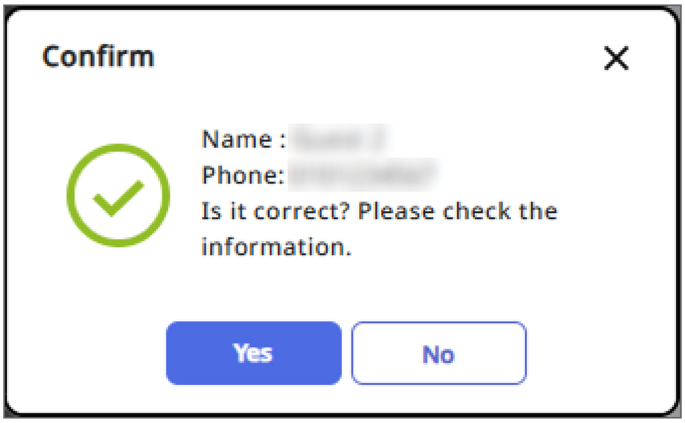
For the first visit, please click the button below to register your visit.

If you have already visited, please fill in the information below.

2. Click **Search** below the fingerprint icon in the center of the screen.

3. Scan your fingerprint on the fingerprint scanning device. Use the scanned fingerprint to search for registered users.

4. If a fingerprint matches a previously enrolled visitor, a confirmation message will appear.



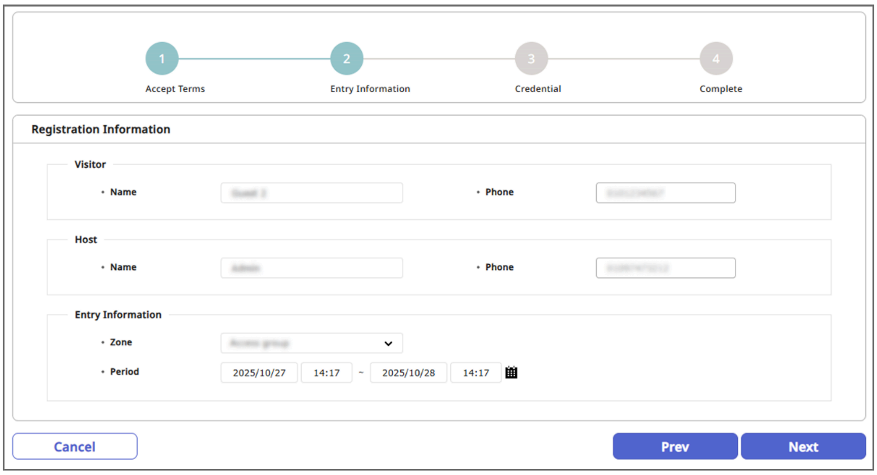
Confirm

Name : [redacted]
Phone: [redacted]
Is it correct? Please check the information.

5. If the searched visitor is correct, click the **Yes** button.

6. After agreeing to the terms and privacy policy regarding access to the visiting department, click the **Next** button in the lower right corner of the screen.

7. Confirm the visit information set during the previous visit. To modify existing information, edit each item and then click the **Next** button in the lower right corner of the screen.



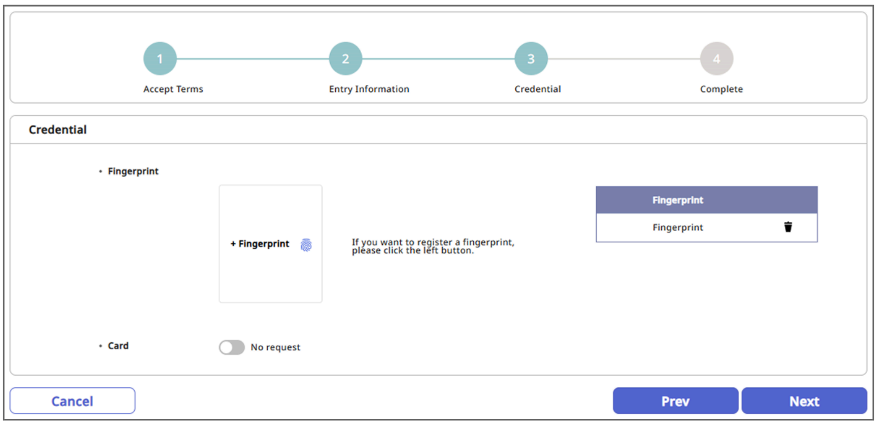
Registration Information

Visitor
- Name [redacted]
- Phone [redacted]

Host
- Name [redacted]
- Phone [redacted]

Entry Information
- Zone [redacted]
- Period 2025/10/27 14:17 ~ 2025/10/28 14:17

8. Confirm the means of entry set during the previous visit. To change the existing means of entry, edit the item to be changed and then click the **Next** button in the lower right corner of the screen.



Credential

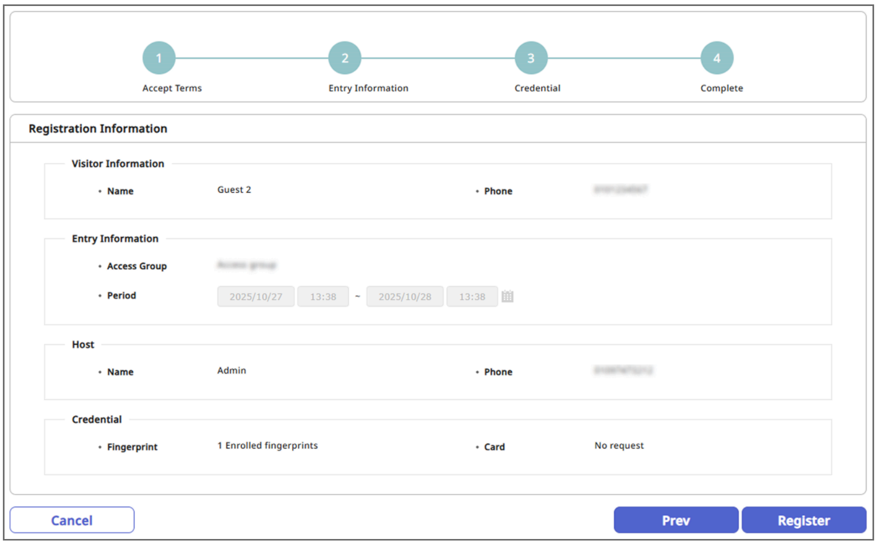
- Fingerprint

If you want to register a fingerprint, please click the left button.

Fingerprint
Fingerprint

- Card No request

9. After confirming all the information provided, click the **Register** button in the lower right corner of the screen.



Registration Information

Visitor Information
- Name Guest 2
- Phone [redacted]

Entry Information
- Access Group [redacted]
- Period 2025/10/27 13:38 ~ 2025/10/28 13:38

Host
- Name Admin
- Phone [redacted]

Credential
- Fingerprint 1 Enrolled fingerprints
- Card No request

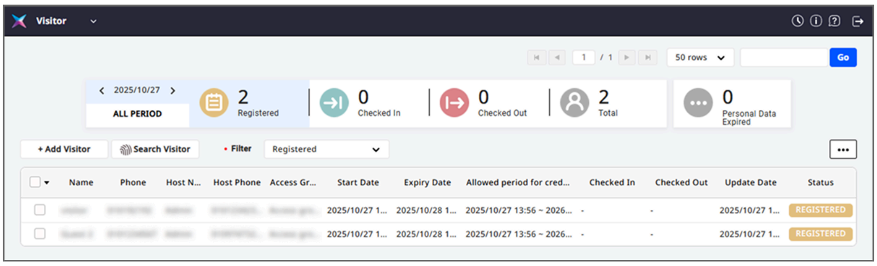
Manage Visitors

You can approve or modify visitor requests. Administrators can also add or delete visitors directly.

Visitor approval

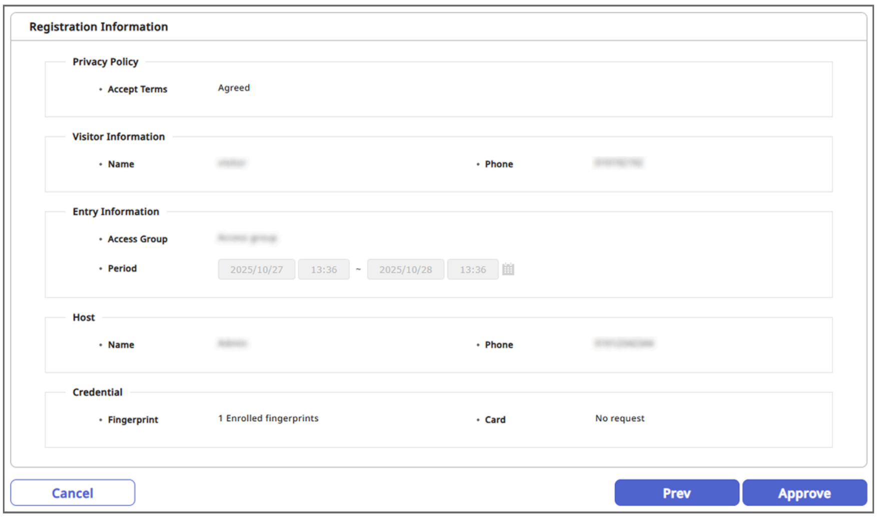
This guide shows how to check visitor requests and approve their access.

1. Click **Visitor** on the **Launcher** page.
2. Click the visitor you want to approve in the visitor list.



□	Name	Phone	Host N...	Host Phone	Access Gr...	Start Date	Expiry Date	Allowed period for cred...	Checked In	Checked Out	Update Date	Status
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/27 1...	2025/10/28 1...	2025/10/27 13:56 ~ 2026...	-	-	2025/10/27 1...	REGISTERED
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/27 1...	2025/10/28 1...	2025/10/27 13:56 ~ 2026...	-	-	2025/10/27 1...	REGISTERED

3. After checking the visitor's information, correct any required items and click **Edit**.
4. Click the **Check in** button at the bottom right of the screen.
5. Check the contents of **Registration Information** and to approve the visit, click the **Approve** button at the bottom right of the screen.



Registration Information

Privacy Policy
- Accept Terms: Agreed

Visitor Information
- Name: [redacted]
- Phone: [redacted]

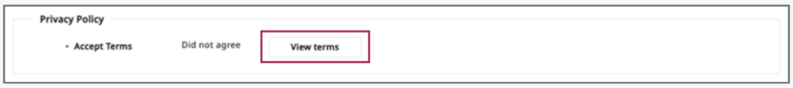
Entry Information
- Access Group: [redacted]
- Period: 2025/10/27 13:36 ~ 2025/10/28 13:36

Host
- Name: [redacted]
- Phone: [redacted]

Credential
- Fingerprint: 1 Enrolled fingerprints
- Card: No request

INFO

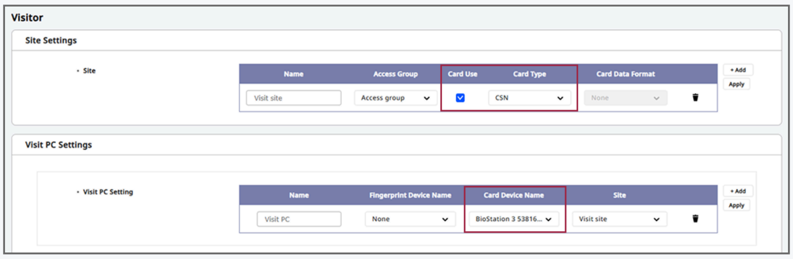
- If the applicant has not agreed to the visitor access terms, the **Approve** button will be disabled. Click the **View terms** button to provide the access terms to the visitor and obtain agreement. If the visitor does not agree to the access terms, the visit will be restricted.



Privacy Policy

- Accept Terms Did not agree

- If a card registration device is set up on the visitor PC, the **Approve and register card** button will be activated. Click the **Approve and register card** button to approve the visitor and issue an access card. For more information, refer to the following.
- To set up card usage on the visitor PC, go to **Settings** → **Visitor** menu and the following minimum settings are required. For more information, refer to the following.



Visitor

Site Settings

- Site

Name	Access Group	Card Use	Card Type	Card Data Format
Visit site	Access group	☑	CSN	None

Visit PC Settings

- Visit PC Setting

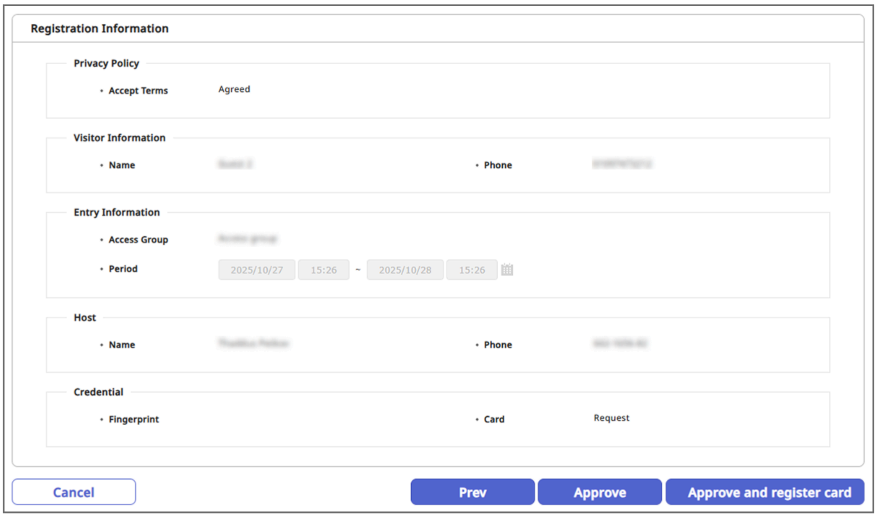
Name	Fingerprint Device Name	Card Device Name	Site
Visit PC	None	BioStation 3 53816...	Visit site

  - **Site Settings** → **Card Use** / **Card Type**
  - **Visit PC Visit PC Setting** → **Card Device Name**

Approve and enroll card

This guide shows how to approve visitor requests and issue access cards.

1. In the **Registration Information** screen, click the **Approve and register card** button at the bottom right of the screen.



Registration Information

Privacy Policy

- Accept Terms Agreed

Visitor Information

- Name [redacted]
- Phone [redacted]

Entry Information

- Access Group [redacted]
- Period 2025/10/27 15:26 ~ 2025/10/28 15:26

Host

- Name [redacted]
- Phone [redacted]

Credential

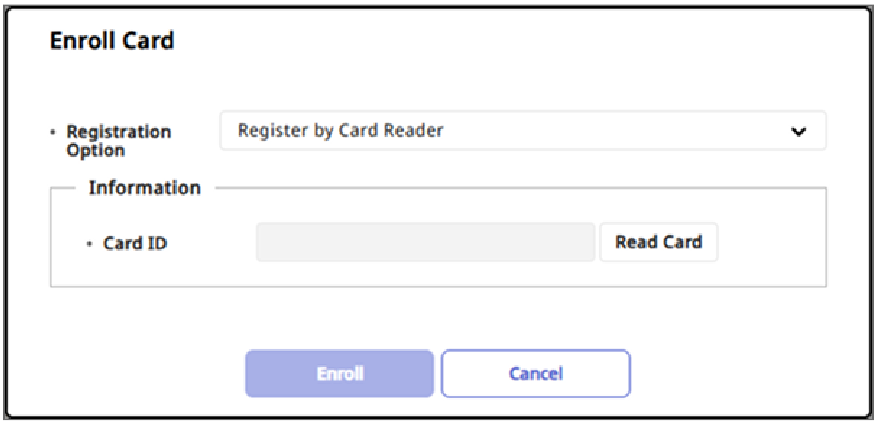
- Fingerprint
- Card Request

2. When the card registration window appears, select your desired registration method.
   - Register by Card Reader
   - Enter Manually

Register by Card Reader

You can scan card information with a device connected to the visitor PC.

1. Select **Register by Card Reader** for **Registration Option**.



Enroll Card

- Registration Option: Register by Card Reader

Information

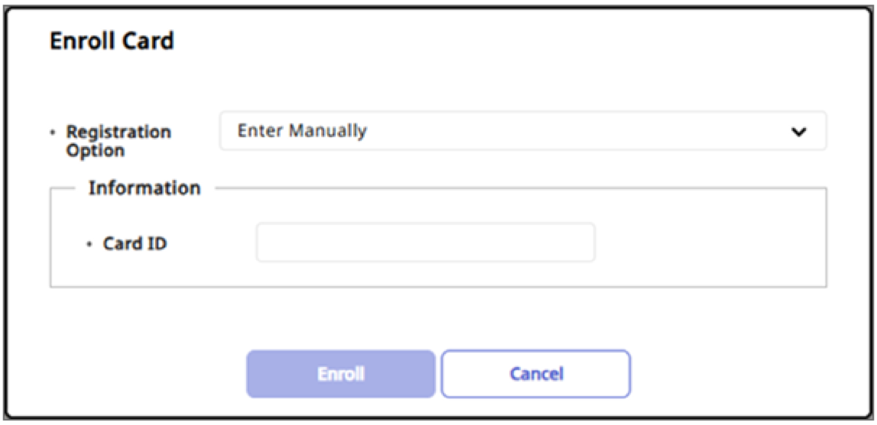
- Card ID

2. To scan the card to enroll, click the **Read Card** button.
3. To enroll the card, click the **Enroll** button.

Enter Manually

You can enroll by directly entering the card number.

1. Select **Enter Manually** for **Registration Option**.



Enroll Card

- Registration Option: Enter Manually

Information

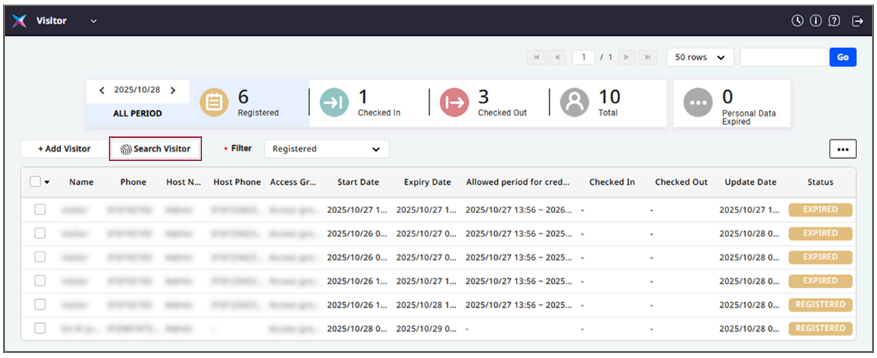
- Card ID

2. Directly enter **Card ID**.
3. To enroll the card, click the **Enroll** button.

Fingerprint search for visitor approval

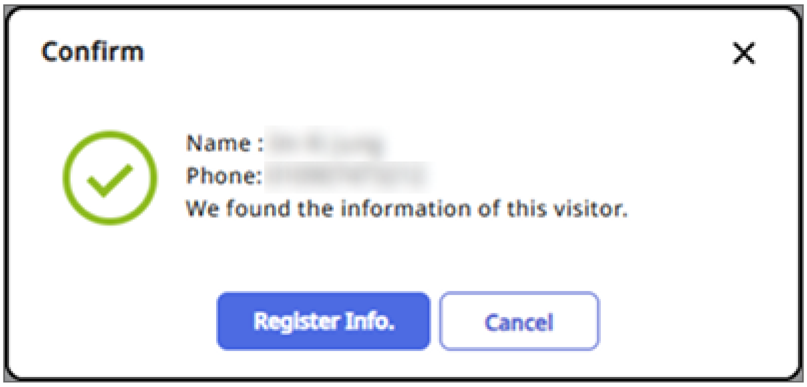
You can search for visitors with enrolled fingerprints and process their approval.

1. Click **Visitor** on the **Launcher** page.
2. Click the **Search Visitor** button in the upper left of the visitor request list.



□	Name	Phone	Host N...	Host Phone	Access Gr...	Start Date	Expiry Date	Allowed period for cred...	Checked In	Checked Out	Update Date	Status
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/27 1...	2025/10/27 1...	2025/10/27 13:56 ~ 2026...	-	-	2025/10/27 1...	EXPIRED
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/26 0...	2025/10/27 0...	2025/10/27 13:56 ~ 2025...	-	-	2025/10/28 0...	EXPIRED
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/26 0...	2025/10/27 0...	2025/10/27 13:56 ~ 2025...	-	-	2025/10/28 0...	EXPIRED
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/26 1...	2025/10/27 1...	2025/10/27 13:56 ~ 2025...	-	-	2025/10/28 0...	EXPIRED
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/26 1...	2025/10/28 1...	2025/10/27 13:56 ~ 2025...	-	-	2025/10/28 0...	REGISTERED
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/28 0...	2025/10/29 0...	-	-	-	2025/10/28 0...	REGISTERED

3. Scan the visitor's fingerprint on the fingerprint scanning device.
4. If a visitor matching the fingerprint is found, a confirmation message will appear. Click the **Register Info.** button.



Name : [redacted]
Phone: [redacted]
We found the information of this visitor.

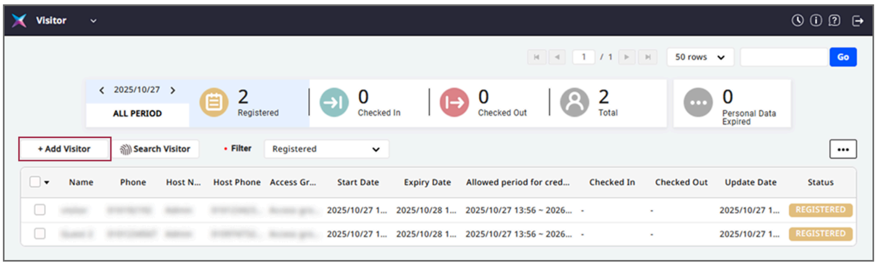
5. After checking the visitor's information, correct any required items and click **Edit**.
6. Click the **Check in** button at the bottom right of the screen.
7. Check the contents of **Registration Information** and to approve the visit, click the **Approve** button at the bottom right of the screen.

Add visitor

This guide shows how an administrator can add visitors directly.

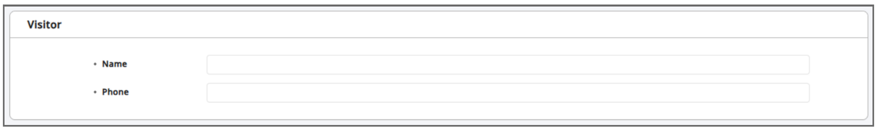
1. Click **Visitor** on the **Launcher** page.

2. Click the + **Add Visitor** button in the upper left of the visitor list.



	Name	Phone	Host N...	Host Phone	Access Gr...	Start Date	Expiry Date	Allowed period for cred...	Checked In	Checked Out	Update Date	Status
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/27 1...	2025/10/28 1...	2025/10/27 13:56 ~ 2026...	-	-	2025/10/27 1...	REGISTERED
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/27 1...	2025/10/28 1...	2025/10/27 13:56 ~ 2026...	-	-	2025/10/27 1...	REGISTERED

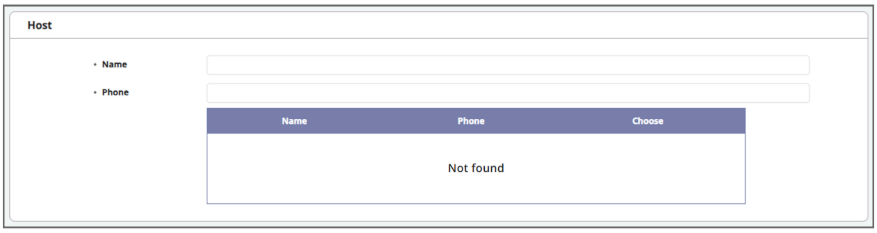
3. Enter the visitor's name and phone number in the **Visitor** section.



Visitor

- Name
- Phone

4. Enter the name and phone number of the responsible person for the visit in the **Host** section.



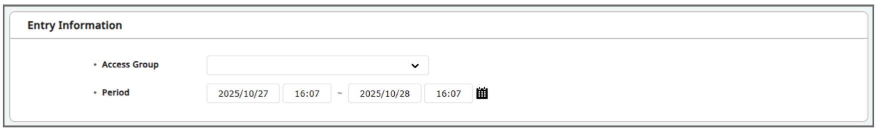
Host

- Name
- Phone

Name	Phone	Choose
Not found		

> When you enter a name or phone number, a list of users matching the entered information will be displayed. To designate the desired user, click the **Choose** button.

5. Set the access group and visit duration in the **Entry Information** section.

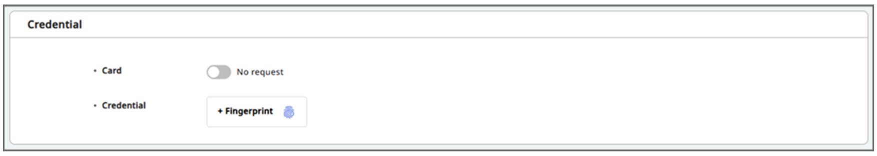


Entry Information

- Access Group
- Period 2025/10/27 16:07 ~ 2025/10/28 16:07

> You can only select access groups assigned to the visiting department for the visit PC. For more information, refer to the following.

6. Set the means of access in the **Credential** section.



Credential

- Card No request
- Credential + Fingerprint

- **Card**: To use card authentication, set it to **Request**.
- **Fingerprint**: To use fingerprint authentication, click the **+ Fingerprint** button and then enroll the visitor's fingerprint.

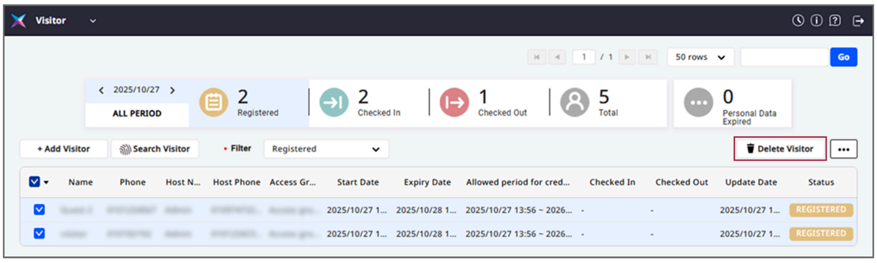
7. To complete adding the visitor, click the **Register** button at the bottom right of the screen.

INFO

- The name can be entered up to 48 characters long.
- To add custom fields to visitor information input, refer to the following.

Delete visitor

1. Click **Visitor** on the **Launcher** page.
2. Click the checkbox of the visitor you want to delete from the visitor request list.



☑	Name	Phone	Host N...	Host Phone	Access Gr...	Start Date	Expiry Date	Allowed period for cred...	Checked In	Checked Out	Update Date	Status
☑	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/27 1...	2025/10/28 1...	2025/10/27 13:56 ~ 2026...	-	-	2025/10/27 1...	REGISTERED
☑	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/27 1...	2025/10/28 1...	2025/10/27 13:56 ~ 2026...	-	-	2025/10/27 1...	REGISTERED

3. Click the **Delete Visitor** button at the top right of the screen.
4. When the confirmation message appears, click **Yes**.

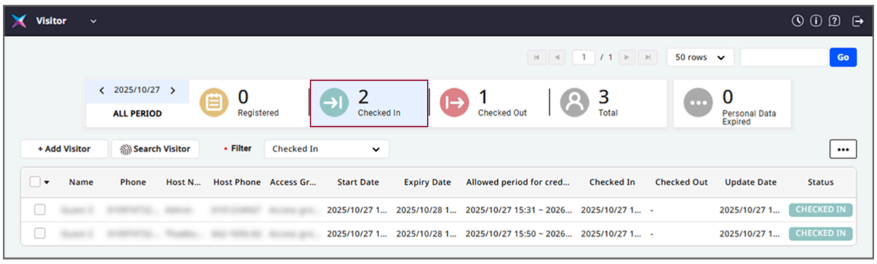
INFO

- The **Delete Visitor** button will be activated when a visitor's checkbox is clicked.
- Visitors can only be deleted from the visitor request list.

Manage Check-In Visitors

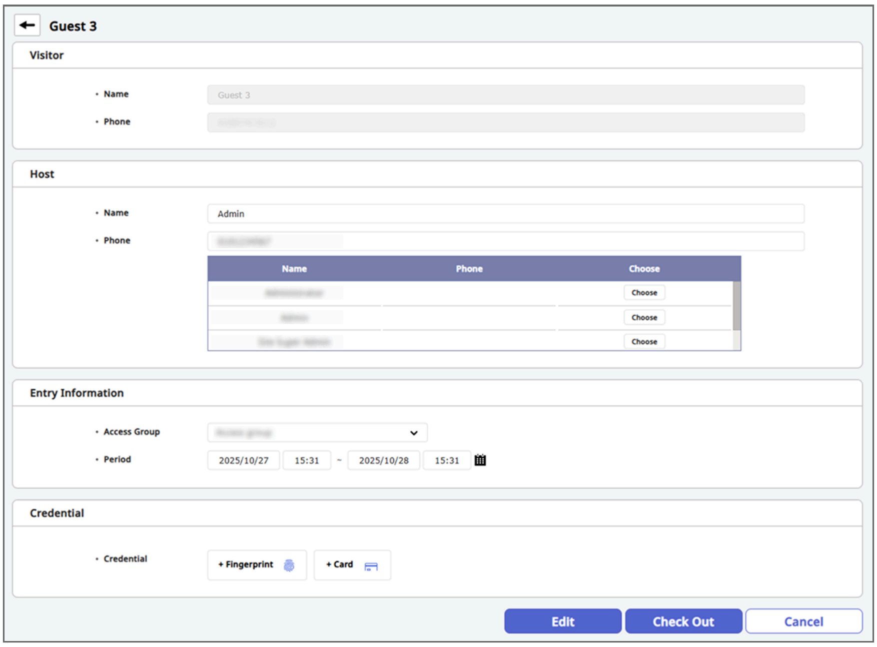
Check the visitors in check-in status and modify visit information or process check-out.

1. Click **Visitor** on the **Launcher** page.
2. Click the **Check in** tab at the top of the screen.



☐	Name	Phone	Host N...	Host Phone	Access Gr...	Start Date	Expiry Date	Allowed period for cred...	Checked In	Checked Out	Update Date	Status
☐	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/27 1...	2025/10/28 1...	2025/10/27 15:31 ~ 2026...	2025/10/27 1...	-	2025/10/27 1...	CHECKED IN
☐	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/27 1...	2025/10/28 1...	2025/10/27 15:50 ~ 2026...	2025/10/27 1...	-	2025/10/27 1...	CHECKED IN

3. Click the visitor in the list to modify or check out.
4. Check the visitor's visit request information.


Guest 3

Visitor

- Name: Guest 3
- Phone: [redacted]

Host

- Name: Admin
- Phone: [redacted]

Name	Phone	Choose
[redacted]		Choose
[redacted]		Choose
[redacted]		Choose

Entry Information

- Access Group: [redacted]
- Period: 2025/10/27 15:31 ~ 2025/10/28 15:31

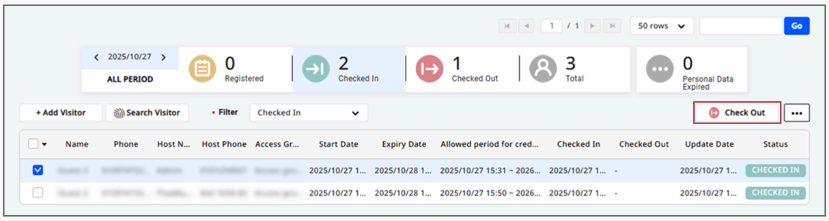
Credential

- Credential: + Fingerprint + Card

- To modify and save individual items, click the **Edit** button at the bottom right of the screen.
- To process check-out, click the **Check Out** button at the bottom right of the screen.

INFO

You can also select visitors to check out from the **Check in** list. Click the checkbox for the visitor to check out in the list and then click the **Check Out** button at the top right of the screen.

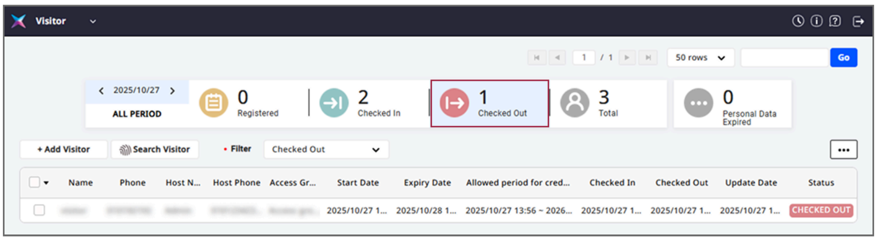


□	Name	Phone	Host N...	Host Phone	Access Gr...	Start Date	Expiry Date	Allowed period for cred...	Checked In	Checked Out	Update Date	Status
☑	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/27 1...	2025/10/28 1...	2025/10/27 15:31 ~ 2026...	2025/10/27 1...	-	2025/10/27 1...	CHECKED IN
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/27 1...	2025/10/28 1...	2025/10/27 15:50 ~ 2026...	2025/10/27 1...	-	2025/10/27 1...	CHECKED IN

Manage Visitor Checkouts

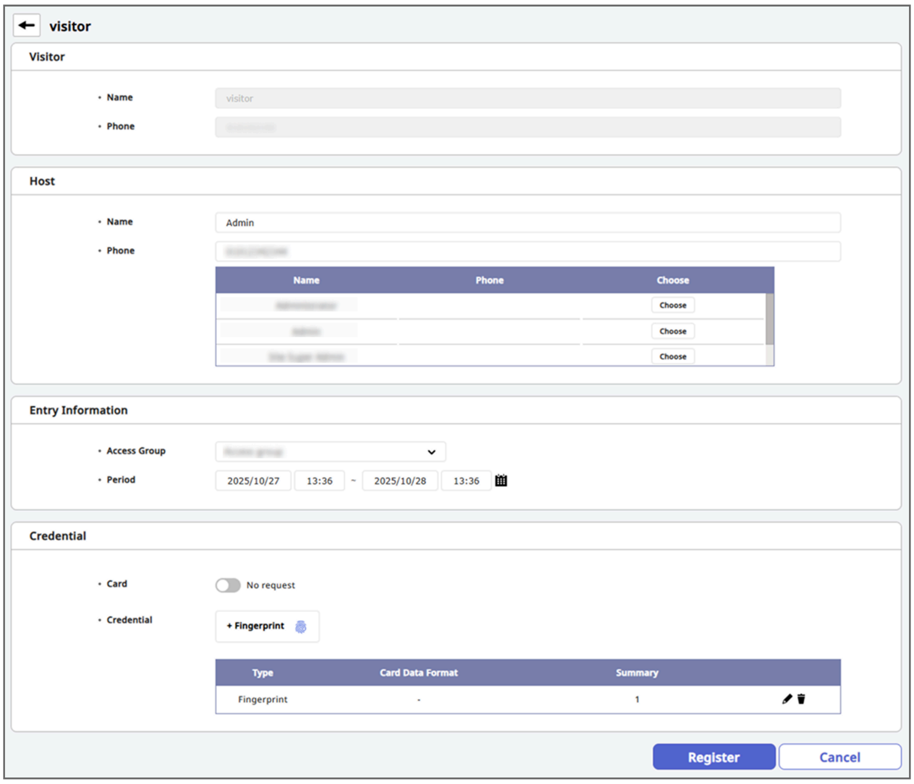
Check the visitors in checkout status and use their visit application information to register a repeat visit.

1. Click **Visitor** on the **Launcher** page.
2. Click the **Check out** tab at the top of the screen.



□	Name	Phone	Host N...	Host Phone	Access Gr...	Start Date	Expiry Date	Allowed period for cred...	Checked In	Checked Out	Update Date	Status
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/27 1...	2025/10/28 1...	2025/10/27 13:56 ~ 2026...	2025/10/27 1...	2025/10/27 1...	2025/10/27 1...	CHECKED OUT

3. Click the visitor you want to register again from the visitor list.
4. Click the **Edit** button at the bottom right of the screen.
5. If there are items that need correction, modify the individual items and then click the **Enroll** button.



- Name: visitor
- Phone: [redacted]
- Name: Admin
- Phone: [redacted]

Name	Phone	Choose
[redacted]		Choose
[redacted]		Choose
[redacted]		Choose

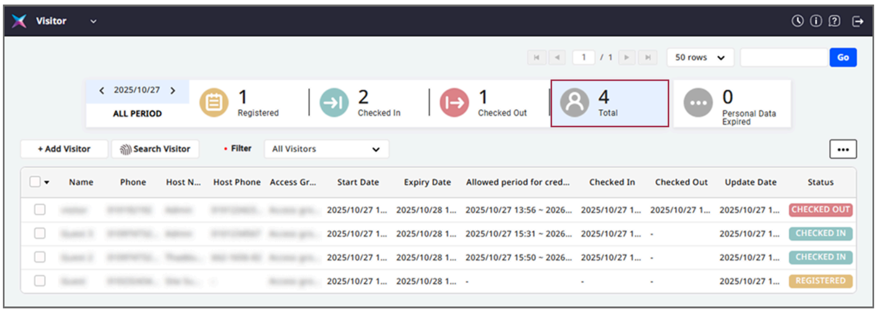
- Access Group: [redacted]
- Period: 2025/10/27 13:36 ~ 2025/10/28 13:36
- Card: No request
- Credential

Type	Card Data Format	Summary
Fingerprint	-	1

The re-registered visitor will be added to the visit application list. Click the **Register** tab at the top of the screen to check.

Manage All Visitors

1. Click **Visitor** on the **Launcher** page.
2. Click the **Total** tab at the top of the screen.



□	Name	Phone	Host N...	Host Phone	Access Gr...	Start Date	Expiry Date	Allowed period for cred...	Checked In	Checked Out	Update Date	Status
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/27 1...	2025/10/28 1...	2025/10/27 13:56 ~ 2026...	2025/10/27 1...	2025/10/27 1...	2025/10/27 1...	CHECKED OUT
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/27 1...	2025/10/28 1...	2025/10/27 15:31 ~ 2026...	2025/10/27 1...	-	2025/10/27 1...	CHECKED IN
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/27 1...	2025/10/28 1...	2025/10/27 15:50 ~ 2026...	2025/10/27 1...	-	2025/10/27 1...	CHECKED IN
□	[redacted]	[redacted]	[redacted]	-	[redacted]	2025/10/27 1...	2025/10/28 1...	-	-	-	2025/10/27 1...	REGISTERED

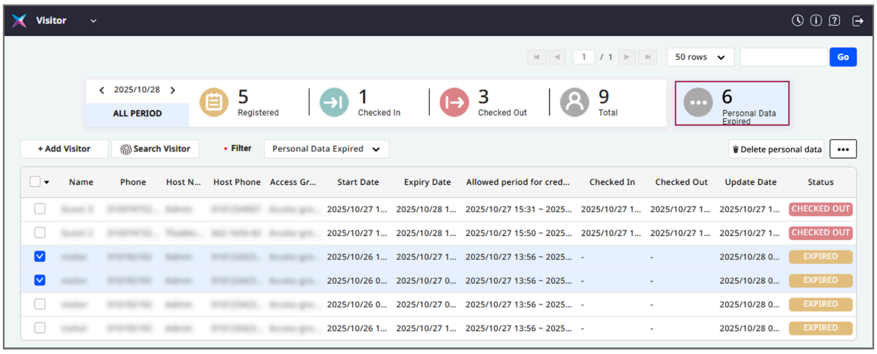
INFO

- You can approve visitor requests or add visitors from the overall visitor list. For more information, refer to the following.
- You can manage visitors with check-in or check-out status from the overall visitor list. For more information, refer to the followings.
  - Manage Check-In Visitors
  - Manage Visitor Checkouts

Delete Expired Personal Data

You can delete visitor information that has exceeded the personal data retention period.

1. Click **Visitor** on the **Launcher** page.
2. Click the **Personal Data Expired** tab at the top of the screen.
3. When the list of visitors whose personal data retention period has expired is displayed, click the checkbox for the visitor you want to delete. You can select more than one.



□	Name	Phone	Host N...	Host Phone	Access Gr...	Start Date	Expiry Date	Allowed period for cred...	Checked In	Checked Out	Update Date	Status
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/27 1...	2025/10/28 1...	2025/10/27 15:31 ~ 2025...	2025/10/27 1...	2025/10/27 1...	2025/10/27 1...	CHECKED OUT
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/27 1...	2025/10/28 1...	2025/10/27 15:50 ~ 2025...	2025/10/27 1...	2025/10/27 1...	2025/10/27 1...	CHECKED OUT
☑	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/26 1...	2025/10/27 1...	2025/10/27 13:56 ~ 2025...	-	-	2025/10/28 0...	EXPIRED
☑	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/26 0...	2025/10/27 0...	2025/10/27 13:56 ~ 2025...	-	-	2025/10/28 0...	EXPIRED
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/26 0...	2025/10/27 0...	2025/10/27 13:56 ~ 2025...	-	-	2025/10/28 0...	EXPIRED
□	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	2025/10/26 1...	2025/10/27 1...	2025/10/27 13:56 ~ 2025...	-	-	2025/10/28 0...	EXPIRED

4. Click the **Delete personal data** button in the top right of the visitor list.
5. When the confirmation message appears, click **Yes**.

> **INFO**
>
> - Only users with **Administrator** permissions can view the list of expired personal data visitors. For more information on user permissions, refer to the following.
> - For more information on setting the personal data retention period, refer to the following.

Explore UI

Explore the UI of each page of BioStar X and guide on how to use it. Explore the UI of each page of BioStar X and learn how to use it. BioStar X offers various features, each easily accessible through the user interface (UI). By examining the user interface of each page, you can understand and utilize the features of BioStar X more easily.

Learn Common UI

This guide describes the common user interface of BioStar X.

User

This guide describes the user interface of the user page.

Monitoring

This guide describes the user interface of the monitoring page.

Dashboard

Here is an overview of the User Interface of the dashboard page.

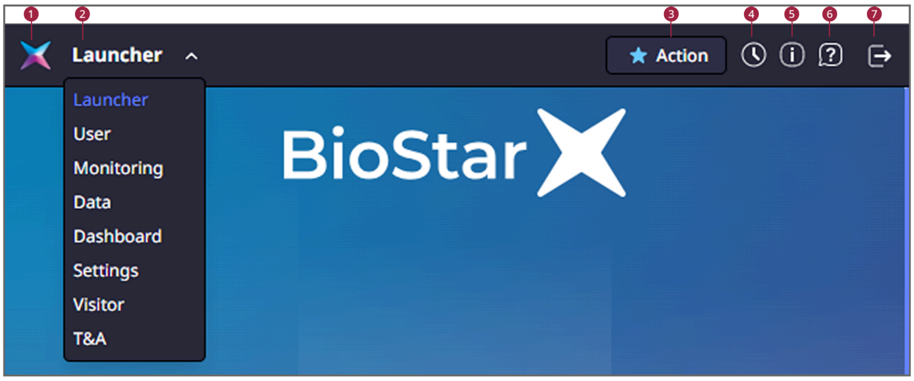
Settings

This guide describes the user interface of the setting page.

Learn Common UI

The user interface (UI) of **BioStar X** is designed to allow users to easily navigate and use the system. This document guides the common UI components of **BioStar X**. You can understand the UI of **BioStar X** and use the system more efficiently.

The header area of the screen is used across all pages and provides link buttons to access various features of **BioStar X**.



1 **BioStar X logo**: Link button that allows users to return to the **Launcher** page of **BioStar X**.

2 **Shortcuts**: Provides links to main pages offered by **BioStar X**.

3 **Action**: Execute the **action** feature set by the server user. Clicking the button displays the action list. For more information, refer to the following.

4 🕓 **Server time**: Check the current server time of the running **BioStar X** server. Hovering the mouse over the button displays the current server time.

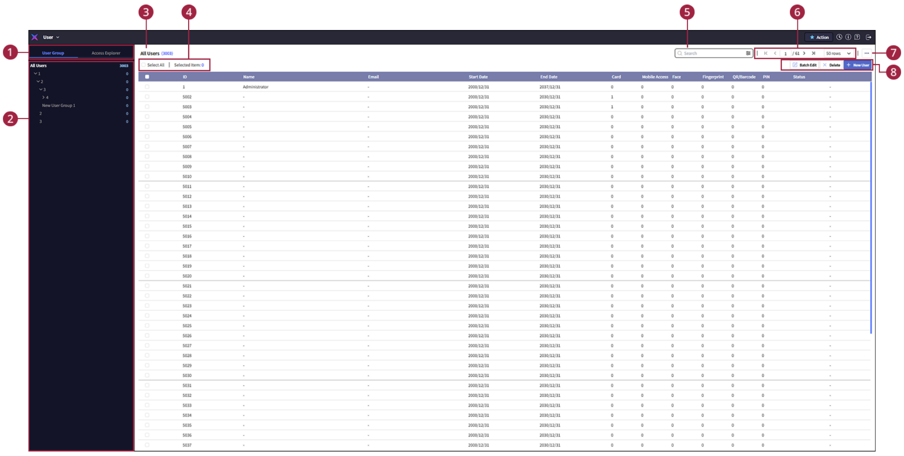
5 ⓘ **Information**: Check the version information of the installed **BioStar X**.

6 ? **Help**: Link button that leads to the help page of **BioStar X**.

7 ↦ **Logout**: End the session of the currently logged-in user and log out.

User

The **User** page's **User** menu allows efficient user management through various features such as managing user groups, managing users, and checking users by access rights, enhancing security through permissions. The UI components of the **User** page are as follows:



■	ID	Name	Email	Start Date	End Date	Card	Mobile Access	Face	Fingerprint	QR/Barcode	PIN	Status
□	1	Administrator	-	2000/12/31	2037/12/31	0	0	0	0	0	0	-
□	5002	-	-	2000/12/31	2030/12/31	1	0	0	0	0	0	-
□	5003	-	-	2000/12/31	2030/12/31	1	0	0	0	0	0	-
□	5004	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5005	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5006	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5007	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5008	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5009	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5010	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5011	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5012	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5013	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5014	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5015	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5016	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5017	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5018	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5019	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5020	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5021	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5022	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5023	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5024	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5025	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5026	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5027	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5028	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5029	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5030	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5031	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5032	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5033	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5034	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5035	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5036	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-
□	5037	-	-	2000/12/31	2030/12/31	0	0	0	0	0	0	-

1 Check user groups or access groups.

- For more information about user groups, refer to the following.
- For more information about access groups, refer to the following.

2 View user groups or access groups in tree structure format. You can expand or collapse the tree structure, and click each group to check the users belonging to that group.

3 Check the number of users in the selected user group from the side menu.

4 Click the **Select All** button to select all displayed users in the user list. The number of selected users appears in **Selected Items**.

5 Enter keywords to search for users. For more information about user search, refer to the following.

6 Click the page navigation button provided at the top right of the screen to check the next or previous user lists. You can also specify a desired page to move to. For more information, refer to the following.

7. Click the ••• button to access various features related to users.

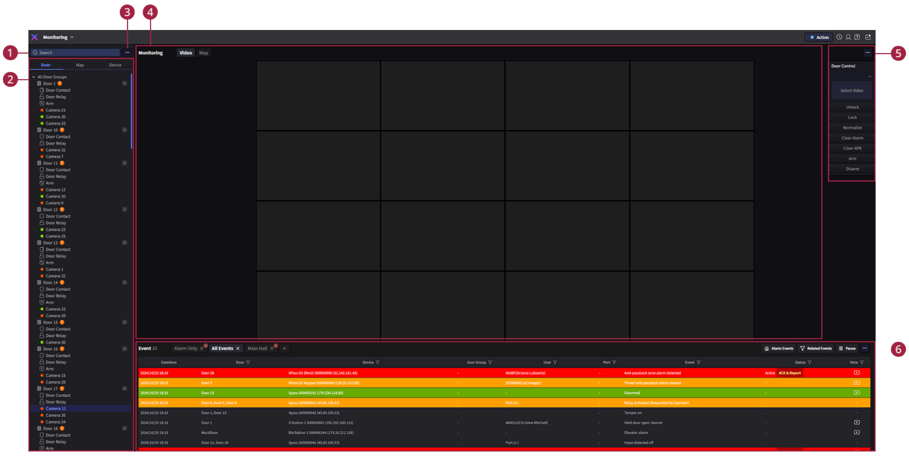
    - **Export**: Save the user list in CSV file or Data file format. For more information, refer to the following.
    - **Import**: Import user lists in CSV file or Data file format or import facial authentication information. For more information, refer to the following.
    - **Transfer to Device**: Function to send registered user information to the device. For more information, refer to the following.
    - **Face Migration**: You can enhance authentication performance by upgrading faces enrolled in older versions of **BioStar X** with the latest algorithm. For more information, refer to the following.
    - **Column Layout**: Change header items of columns in the user list. For more information on this, refer to the following.
    - **Print**: Print the user list.

8. Use the functions for user registration and batch modification or deletion.

    - **Batch Edit**: Modify information or access rights for multiple users at once. For more information, refer to the following.
    - **Delete**: Delete selected users. For more information, refer to the following.
    - **New User**: Register new users. For more information, refer to the following.

Monitoring

This guide describes you through the user interface (UI) of the **Monitoring** page. You can monitor the security status in real time based on doors, maps, and devices on the **Monitoring** page. You can also check real-time events and take necessary actions. The UI components of the **Monitoring** page are as follows.



1. Enter keywords in the search input field to get devices, doors, cameras, and other desired items.

2. Monitor the tree structure of groups by checking **Door**, **Map**, and **Device**.
   - For more information about monitoring **Door**, refer to the following.
   - For more information about monitoring **Map**, refer to the following.
   - For more information about monitoring **Device**, refer to the following.

3. Click the ••• button to expand or collapse the tree structure of the list.
   - **Expand All**: Expands all lists within the group in the side menu to display them.
   - **Collapse All**: Collapses all lists within the group in the side menu to hide them.

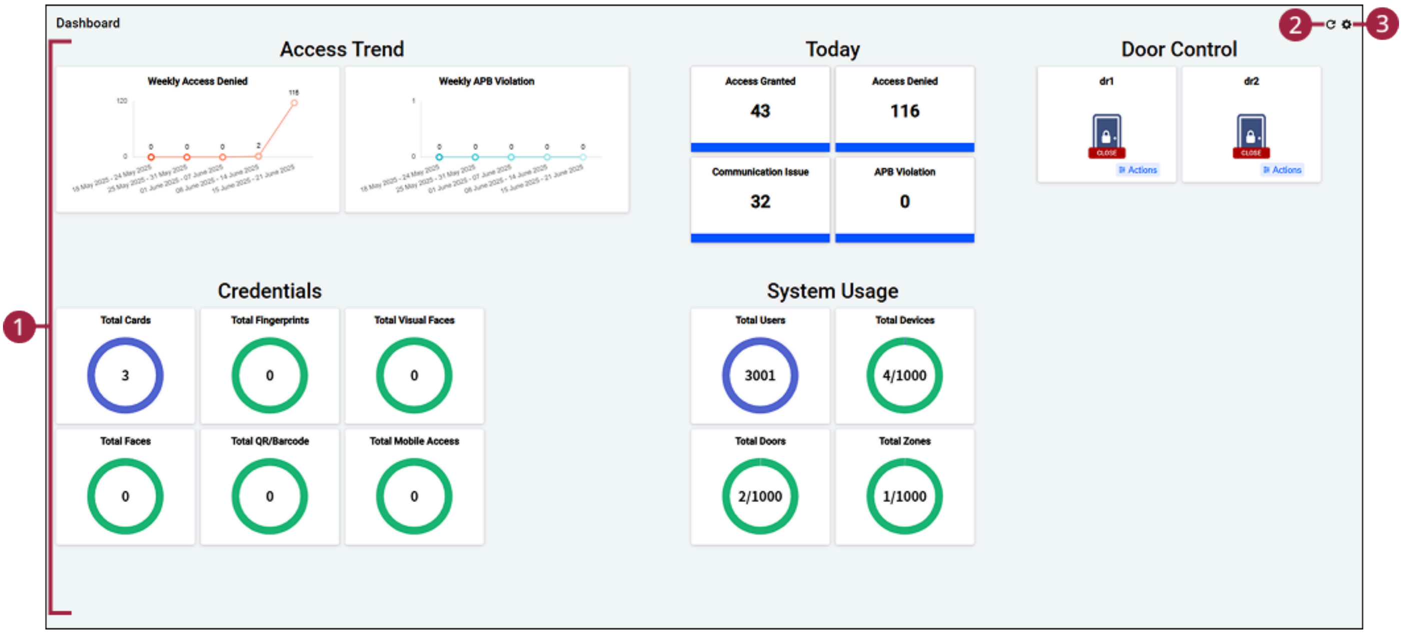
4. The **video tile** allows you to check real-time video or maps of doors, cameras, and areas. You can monitor multiple camera feeds simultaneously.
   - For more information about monitoring camera feeds, refer to the following.
   - For more information about map monitoring, refer to the following.

5. The **control panel** allows you to control the features of the selected door or device. For more information, refer to the following.

6. The **event list** allows you to check real-time events in chronological order. You can view detailed information, status, related users, and device information for each event and take immediate action if necessary. For more information, refer to the following.

Dashboard

Guides the user interface (UI) of the **Dashboard** page.



Dashboard

Access Trend

Weekly Access Denied

Weekly APB Violation

Today

Access Granted 43

Access Denied 116

Communication Issue 32

APB Violation 0

Door Control

dr1

dr2

Credentials

Total Cards 3

Total Fingerprints 0

Total Visual Faces 0

Total Faces 0

Total QR/Barcode 0

Total Mobile Access 0

System Usage

Total Users 3001

Total Devices 4/1000

Total Doors 2/1000

Total Zones 1/1000

1
2
3
120
118
0
0
0
0
2
1
0
0
0
0
0
0
18 May 2025 - 24 May 2025
25 May 2025 - 31 May 2025
01 June 2025 - 07 June 2025
08 June 2025 - 14 June 2025
15 June 2025 - 21 June 2025
CLOSE
Actions
CLOSE
Actions

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

1 **Widget Area**: The area where user-added widgets are displayed.

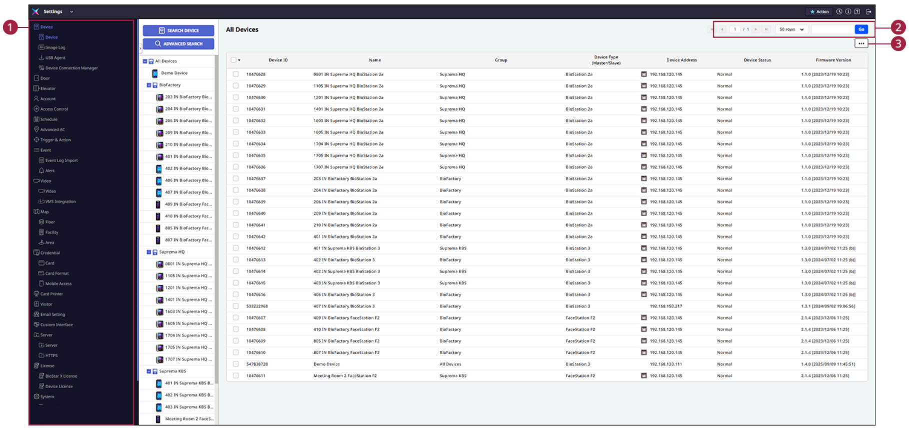
- The size of each widget can be freely adjusted within the size limits for each widget.
- Widgets can only be placed in empty areas, and they cannot overlap each other.

2 **Refresh**: Refresh the dashboard page to update the data in the modified widget.
Set the refresh cycle in **Auto Refresh Interval** in **Dashboard Settings**.

3 **Dashboard Settings**: Add new widgets or set the data and appearance of the added widgets.

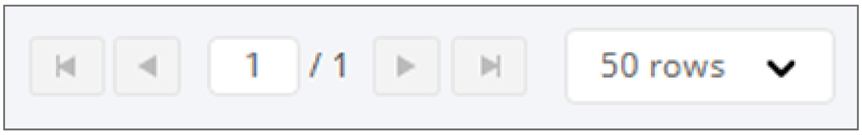
Settings

On the **Settings** page, manage various settings of **BioStar X**. The UI components of this page are as follows:



1. Check various settings menus provided in the **Settings** menu. For more information, refer to the following.

2. A tool to navigate the page list. Move between pages or go to the desired page.



   - ⏮ : Move to the first page.
   - ◀ : Move to the previous page.
   - ▶ : Move to the next page.
   - ⏭ : Move to the last page.

- Enter the page number in the input field to move to the desired page.
- Click the row selection box to set the number of items displayed on each page.

> **INFO**
>
> Support may vary depending on the settings menu.

3. Click the ⋯ button to access additional options.

> **INFO**
>
> Supported features may vary depending on the settings menu.

License Policy

BioStar X is the next generation access control software developed as a successor to **BioStar 2**. Supports various deployment environments of today and the future through an enhanced system architecture, expanded features, and a more flexible licensing model.

BioStar X offers a total of five scalable license levels ranging from **Starter** to **Elite**, allowing you to choose according to various environments from small businesses to large corporate settings. Designed in a modular structure, it can add a variety of optional features such as video integration, mobile access, and multi-server support.

Base License

The basic license is an essential component for activating and operating the system. This license serves as a foundation for applying additional features or upgrades.

	Device Manager	Starter	Essential	Advanced	Enterprise	Elite
Maximum Number of Doors	0	5	32	128	500	2000
Maximum Users	200	100	1,000	50,000	100,000	500,000
Maximum Operators	1	1	10	20	40	100
Maps	✗	✗	✗	✓	✓	✓
Video	✗	✗	✗	Add on	Add on	Add on
Advanced Access Control *(Global APB, Global Fire Alarm, Intrusion Alarm, Mustering, Occupancy Limit, Elevator, Interlock)*	✗	✗	✗	Add on	✓	✓
Upgradable *(Door/User/Admin)*	User, admin only	✗	✗	Add on	Add on	Add on

> ⓘ The **Device Manager** license is required for customers using third-party software or third-party systems who wish to efficiently manage Suprema devices through **BioStar X**.

Capacity Upgrade

License upgrades are available for holders of **Advanced**, **Enterprise**, and **Elite** licenses. License holders of the **Device Manager** can only purchase User Upgrades.

	Number
Door	32
User	5,000
Administrator	10

Feature add-ons

The following items can be purchased individually and can be additionally applied to **Advance**, **Enterprise**, and **Elite** license tiers.

Feature	License Type	Remarks
Multi Communication Server Init	Basic License	Basic license – Includes 1 server. An annual maintenance contract is required for support.
Multi Communication Server Add-on	Additional Server	Applied when an additional server is added.
GIS Map	System	You can use the GIS map to set up areas, facilities, and floors.
Video	Camera	Applies when using a Video Management System (VMS) not provided by Suprema.
Server Matching	ID, Card, Fingerprint, IR-Face Server Matching	Server Matching method compares the entered ID, card, fingerprint, and IR face from the device to the credentials stored inside the server database. An annual maintenance contract is required for advanced support.
Visitor	System	Administrators and operators can track or control visitor access.
Attendance Management (T&A)	Standard	Supports up to 500 users.
	Enterprise	There is no limit on the number of users.
Directory Integration	System	An annual maintenance contract is required for advanced support.
Roll Call	System	-

> ⓘ Not all cameras connected to the VMS need to be integrated with BioStar X. For example, even if the VMS supports 32 cameras, users only need to purchase a license for the specific camera that they want to integrate with **BioStar X**, and there is no need to purchase a license for all cameras.

The following items can be purchased individually and can be added regardless of the basic license.

Feature	License Type	Remarks
Mobile App	System	-
Event log API	System	The system can receive and log event logs via external API. This allows third-party applications or services to insert event data directly into the access control system for centralized logging and reporting.
Remote Access	System	Provides a secure tunnel feature that allows access to the **BioStar X** server from an external network. **BioStar X** also serves as a gateway for external network access to mobile and API. Required for using **Send Face Mobile Enroll Link** feature.
BioStar X Plugin	System	Supports external plugin integration. A maximum of 10 custom plugins can be used per system. For more information, refer to the following.

Package

The following items can be purchased individually from **Advance**, **Enterprise**, and **Elite** license tiers.

- **Advanced Access Control**: A package of advanced access control features - Global APB, Global Fire Alarm, Intrusion Alarm, Mustering, Occupancy Limit, Elevator Control, and Interlock.

Device License

Device licenses can be purchased individually and can be added regardless of the basic license. Device licenses are issued based on the serial number (S/N). This feature can only be activated on devices that require a license.

Feature	License Type	Supported models	Remarks
Face Server Matching	Device	-	An annual maintenance contract is required for advanced support.
Camera QR	Device	X-Station 2 (no QR reading sensor), BioStation 3	-
Wireless Lock	Device	CoreStation 40	-

Appendices

Includes legal notices contained in the product.

Disclaimers

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

Copyright Notice

Open Source License

This product contains open-source software. To request the source code covered under GPL, LGPL, MPL, and other open-source licenses which require distribution of the source code, please visit https://support.supremainc.com.

You may obtain the source code for three years after our last shipment of this product on our website.

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

Open-source licenses and the corresponding license terms for open-source software contained in this product are as follows: link

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