BioStar X

ADMINISTRATOR GUIDE

Version 1.0.3

English

EN 102.00.BSX

suprema

SECURITY & BIOMETRICS

CONTENTS

Overview 6

Enhanced operational efficiency and security 6

Provides strong scalability and stability 6

Before You Start 7

Supported Devices 11

System Minimum Requirements 13

Getting Started 16

Check Network Priority 16

Express Installation 23

Custom Installation 30

Upgrade 38

Install Multi Communications Server 45

How to Log in 52

Register License Key 54

Initial Setup Guide 57

Server Management 59

Start and Stop Server 59

Service Settings 60

Change the Main Server IP Address 63

Change the Port 66

Change the Database 67

Add Auxiliary Database 69

Uninstall BioStar X Server and Restore Security Certificates 77

Launcher 84

User 85

Manage User Groups 85

Register Users 89

Enter Basic User Information 91

Enroll User's Credential 93

Setting User Permissions 117

Configure User Advanced Settings 120

Register and Edit Users by Scanning an ID 121

Explore Users 125

Manage Users 130

Manage Access Groups 140

Login in with Multi-Factor Authentication 142

Batch Enroll Faces 144

Face Migration 149

Set Emergency Open Permissions 151

Monitoring 154

Monitor Doors 154

Monitor Map 182

Monitor Device 190

Monitor Video 199

Monitor Event 205

Data 214

Generate Report 214

Automatic Report Schedule 228

Settings 230

Dashboard 231

Add Widgets 231

Edit Widget 237

Delete Widget 238

Settings 239

Manage Devices 239

Device Settings 262

Image Log Settings 300

USB Agent Settings 304

Device Connection Management Settings 305

Manage Doors 308

Manage Operation Permissions 321

Manage Long-Term Inactive Users 327

Set Up ID Scan 331

Access Control Settings 332

Schedule Settings 342

Trigger and Action Settings 345

How to Use the Quick Action 347

Import Event Logs 351

Alert Settings 352

Manage Credentials 354

Activate License 376

Manage Audit Trail 382

System Settings 391

Advanced Settings 423

Manage Elevators 423

Advanced Access Control Settings 430

Video Settings 460

Manage Map 482

Visitor Settings 497

Directory Integration Settings 501

Remote Access Settings 513

Integrate Virtual Device Event Log 516

Plugin 521

What are plugins? 521

BioStar X plugins 521

Key use cases 521

Register plugin 521

Plugin management 523

How to Use Time & Attendance 524

Manage Visitors 570

Explore UI 585

Learn Common UI 585

User 585

Monitoring 587

Dashboard 587

Settings 588

License Policy 590

Base License 590

Capacity Upgrade 591

Feature add-ons 591

Advanced Access Control 160

Device License 380

Appendices 595

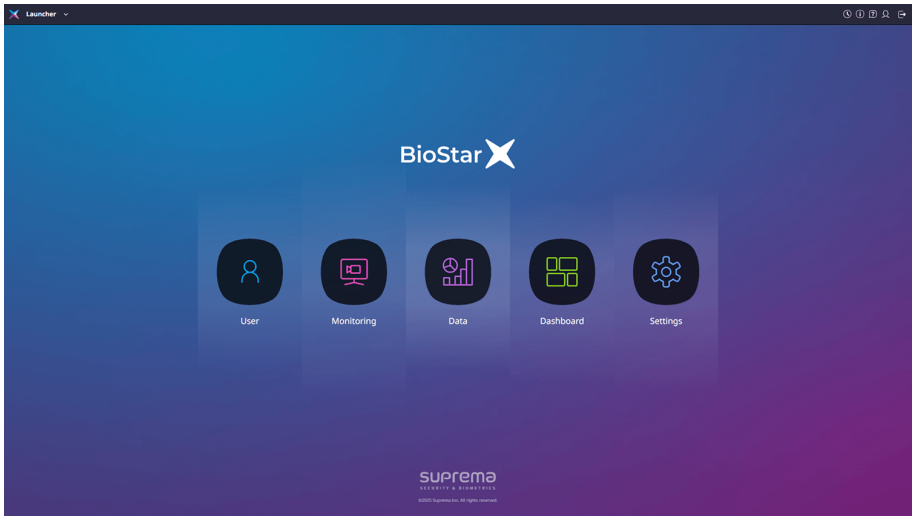
Disclaimers 595

Copyright Notice 596

Open Source License 596

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 You 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.
- For the default port used by **BioStar X**, see Service Settings. 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 `-` `_`.

Port settings

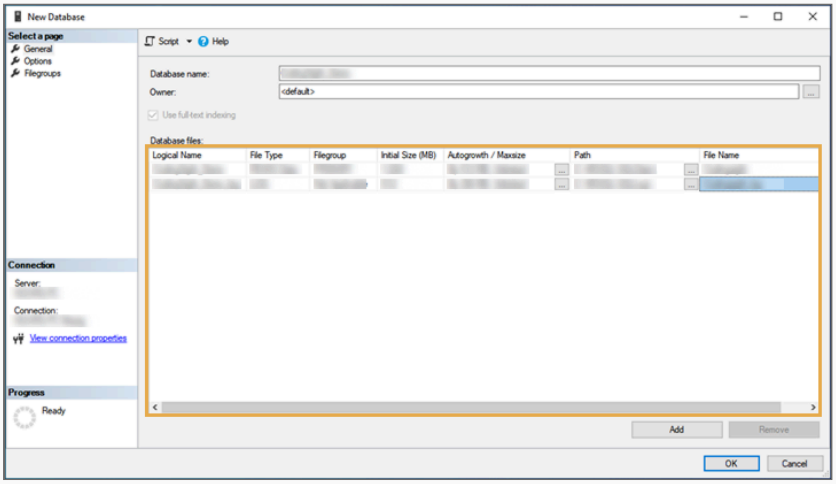
- Run **SQL Server Configuration Manager** and set **TCP/IP Protocol** for **Protocols for SQLEXPRESS** to the desired port number.
- Restart the **SQL Server Services** to apply the settings.

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

Set the following recommended values in the **Database Files** section. Configure **Autogrowth** using fixed sizes (MB/GB) rather than percentages, and avoid very small increments that would cause frequent growth events.



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

Small (under 10 GB)

- Data: **Initial Size** 1 - 5 GB, **Autogrowth** 100 - 512 MB
- Log: **Initial Size** 512 MB - 2 GB, **Autogrowth** 100 - 512 MB
- TempDB: **Initial Size** 512 MB - 1 GB

> *e.g. Data 2 GB (**Autogrowth** 256 MB) / Log 1 GB (**Autogrowth** 128 MB) / TempDB 512 MB*

Medium (10 - 500 GB)

- Data: **Initial Size** 10 - 50 GB, **Autogrowth** 512 MB - 1 GB
- Log: **Initial Size** 5 - 10 GB, **Autogrowth** 512 MB - 1 GB
- TempDB: **Initial Size** 2 - 8 GB

> *e.g. Data 20 GB (**Autogrowth** 1 GB) / Log 5 GB (**Autogrowth** 512 MB) / TempDB 4 GB*

Enterprise (500 GB or higher)

- Data: **Initial Size** 100 GB or higher, **Autogrowth** 1 - 4 GB
- Log: **Initial Size** 20 ~ 100 GB, **Autogrowth** 1 ~ 4 GB
- TempDB: **Initial Size** 8 - 32 GB

> *e.g. Data 100 GB (**Autogrowth** 2 GB) / Log 50 GB (**Autogrowth** 2 GB) / TempDB 16 GB*

Caution

- Do not set **Autogrowth** to very small increments or leave the **Maxsize** to **Unlimited**. Instead, set appropriate limits based on expected growth and monitor usage.
- 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 Preliminary settings

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 Set up MS SQL Windows Authentication with an Active Directory account

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.

Next step

Learn the minimum system requirements to install **BioStar X**.
This guide provides a simple installation method for first-time users.
This guides the user on how to set up a custom installation to integrate with a database that the user has already installed.

Supported Devices

The following devices are supported by the BioStar X platform.



BioStation 3 Max



XPass Q2



BioEntry W3



BioStation 2a



BioStation 3



X-Station 2



FaceStation F2



XPass 2



FaceLite



BioLite N2



XPass D2



BioEntry R2



BioEntry P2



FaceStation 2



BioEntry W2



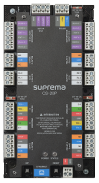
BioStation L2



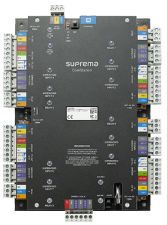
BioStation A2



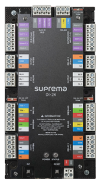
BioStation 2



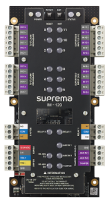
CoreStation 20



CoreStation



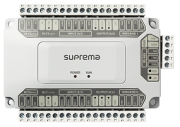
Door Interface



Input Module



Output Module



Door Module



Secure I/O 2

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 Multi Communications Server.

The main server manages the system's core management features. The Multi Communications Server handles device communication, distributes the load, and optimizes 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 the Suprema Global Technical Support Team.

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	Medium	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, Windows Server 2025		
	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

Item		Small	Medium	Enterprise
	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.
- Up to 1,000 devices can connect via Ethernet (TCP/IP). Add a Multi Communications Server to connect more devices.

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
Small	1 to 50	4 - 6
Medium	50 - 300 devices	8 - 12
Enterprise	300 - 1,000 devices	16 - 24

Using the BioStar X API

Organization	Total Devices	Number of cores
Small	1 to 50	4 - 6
Medium	50 - 300 devices	8 - 12

Organization	Total Devices	Number of cores
Enterprise	300 - 1,000 devices	16 - 24

Multi Communications Server

The Multi Communications Server handles communication with access control devices. It helps to manage many devices reliably by installing separately from the main server. A single Multi Communications Server can connect up to 1,000 devices. Add multiple Multi Communications Servers as needed.

Item		Specification
System Requirement	Operating System	Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows Server 2025
	CPU	Minimum 2.3 GHz, recommended 4.0 GHz 16-core
	RAM	Minimum 64 GB, recommended 128 GB
	SSD	1 TB

Info

Up to 1,000 devices can connect via Ethernet (TCP/IP).

Client

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

Item		Small	Medium	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**.

When is it needed?

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

- When two or more network adapters (LAN cards) 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**, see Express Installation.

> **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

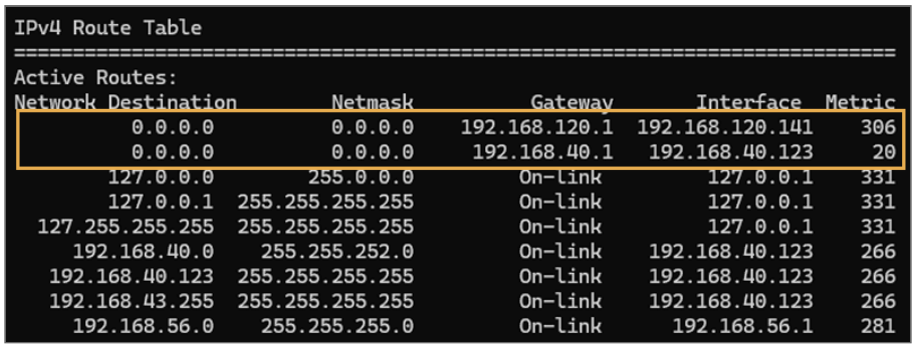
Check in command prompt

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.

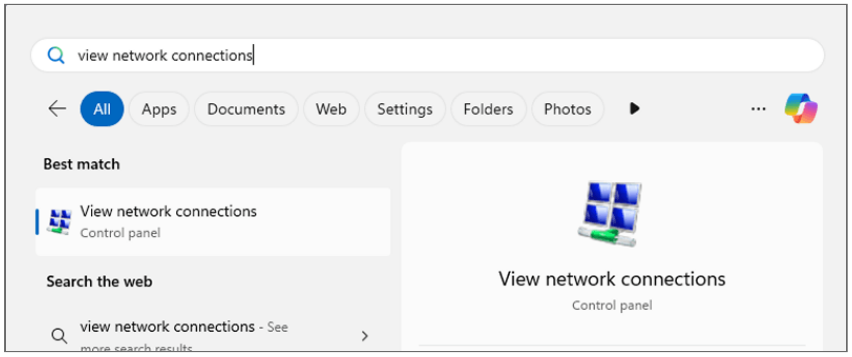
Change network priority

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.

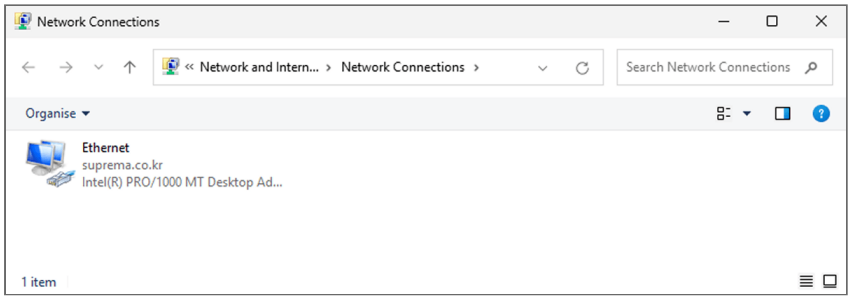
1 Open network settings

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



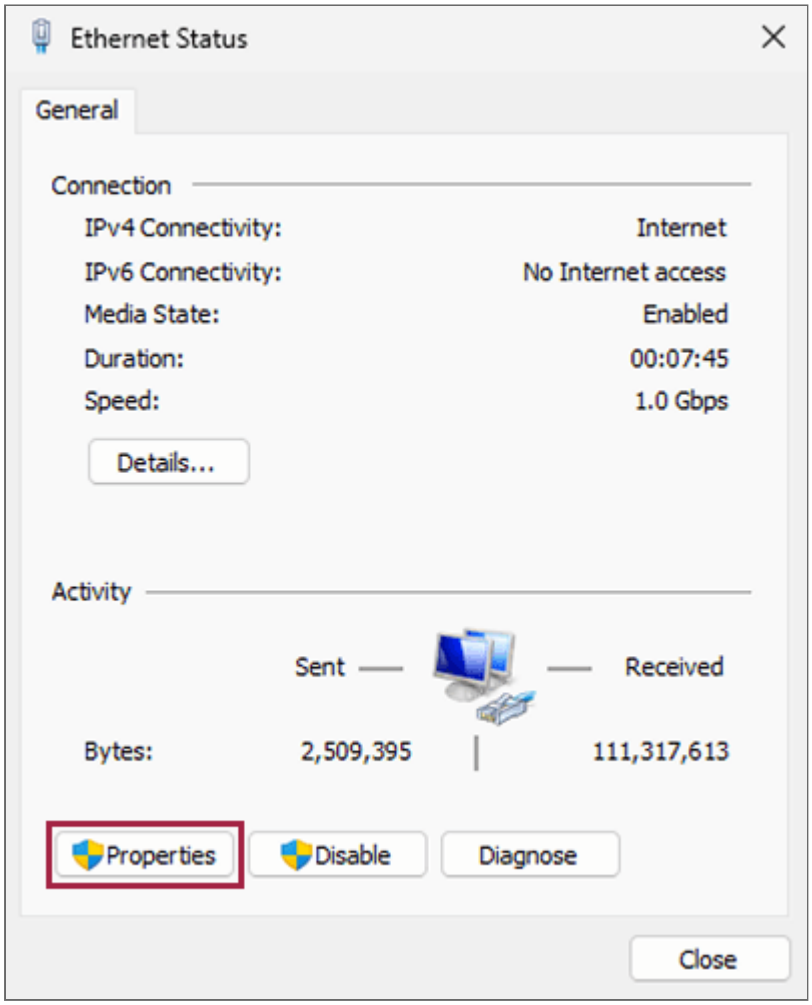
2. Click **View Network Connections** from the search results.

3. Double-click on the adapter connected to the internet from the list.

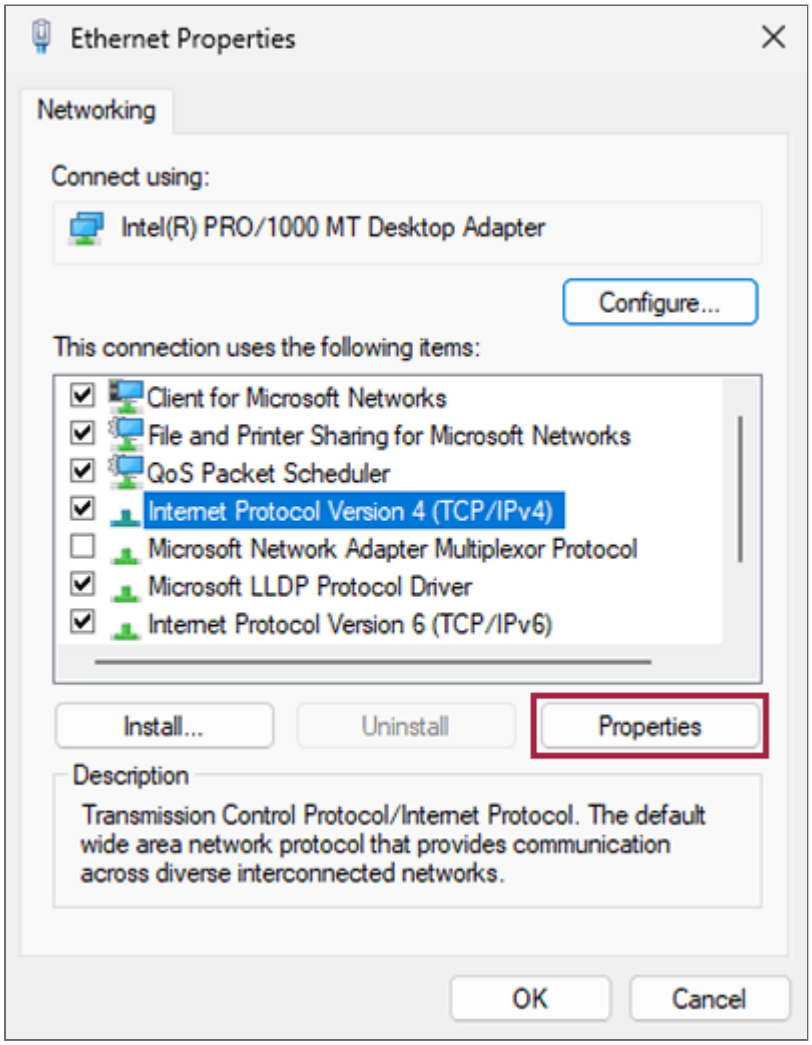


2 Open adapter options

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

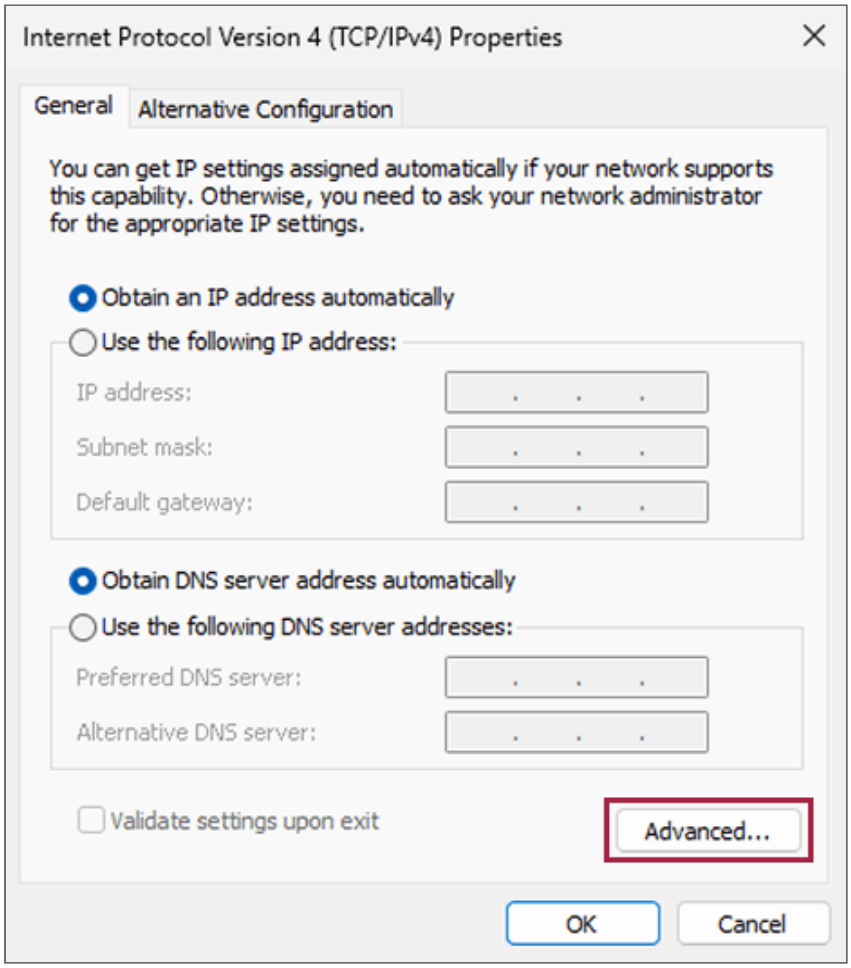


2. When the Ethernet Properties window appears, select **Internet Protocol Version 4 (TCP/IPv4)** from the list.



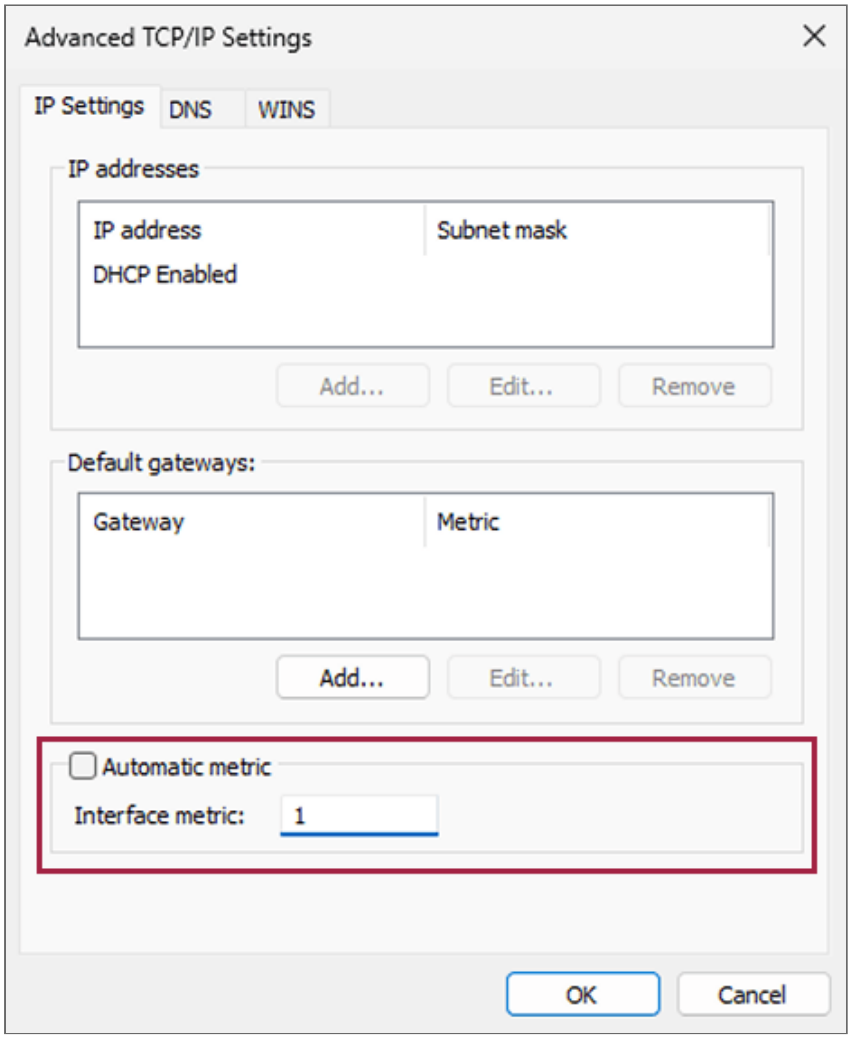
3. Click the **Properties** button.

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



3 Metric settings

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



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.

Next step

This guide provides a simple installation method for first-time users.
This guides the user on how to set up a custom installation to integrate with a database that the user has already installed.

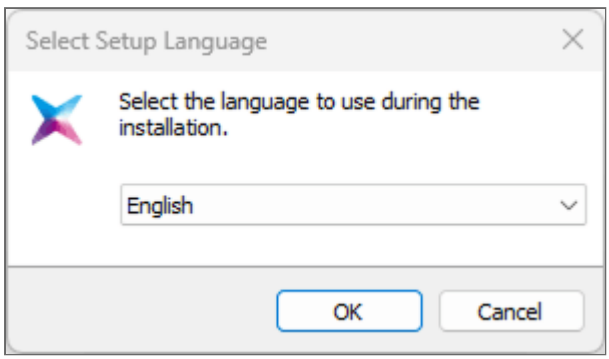
Express Installation

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.

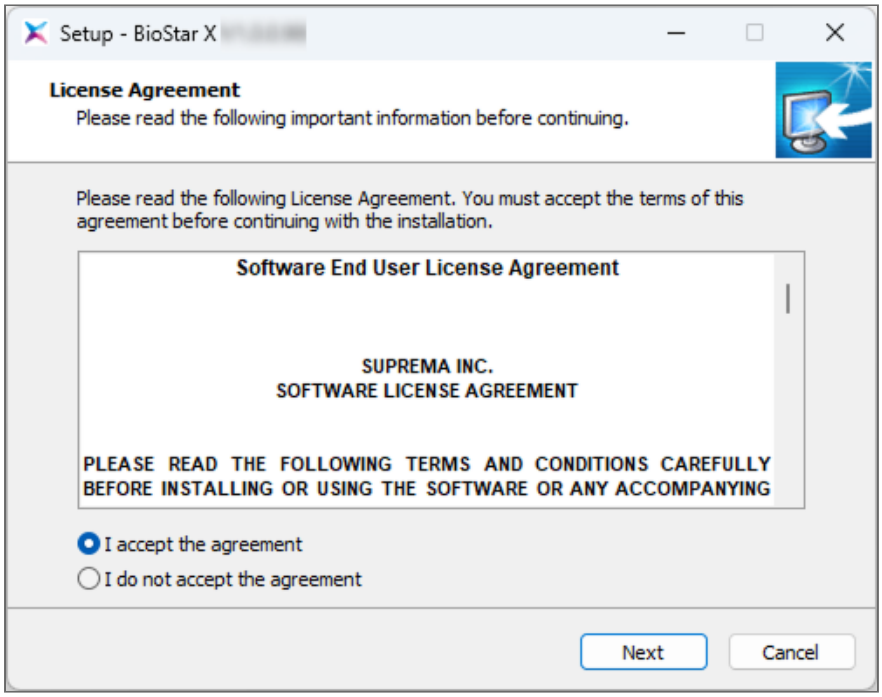
> **Info**
> To connect to an already installed database using **Custom installation**, refer to Custom Installation.

Installation guide

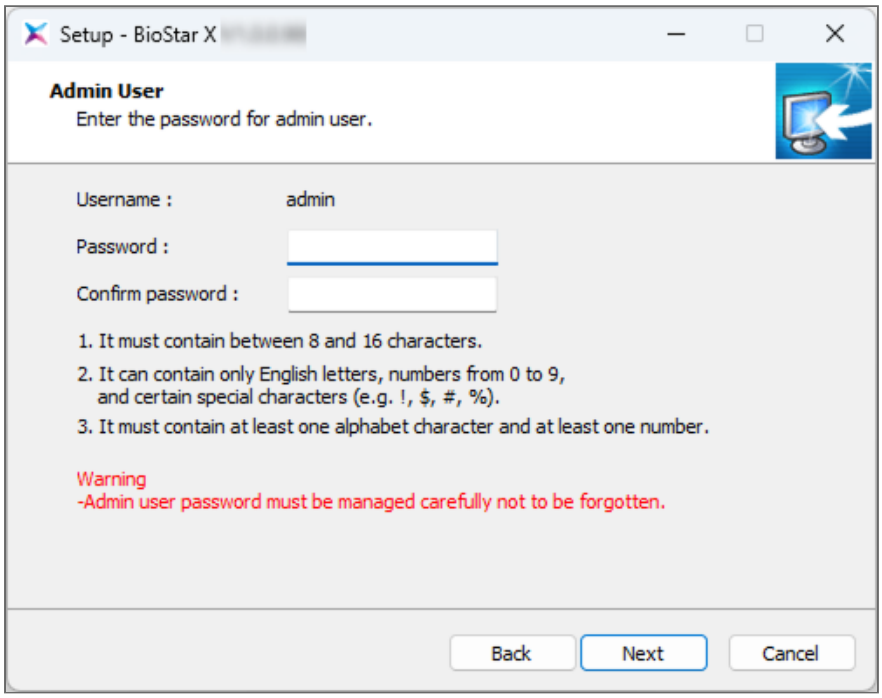
1. Go to the Suprema Download Center, log in, and download the installation package (*BioStar X Setup.X.Y.Z.BB.exe*).
2. Run the downloaded installation file.
3. Select the language to use and select the **OK** button.



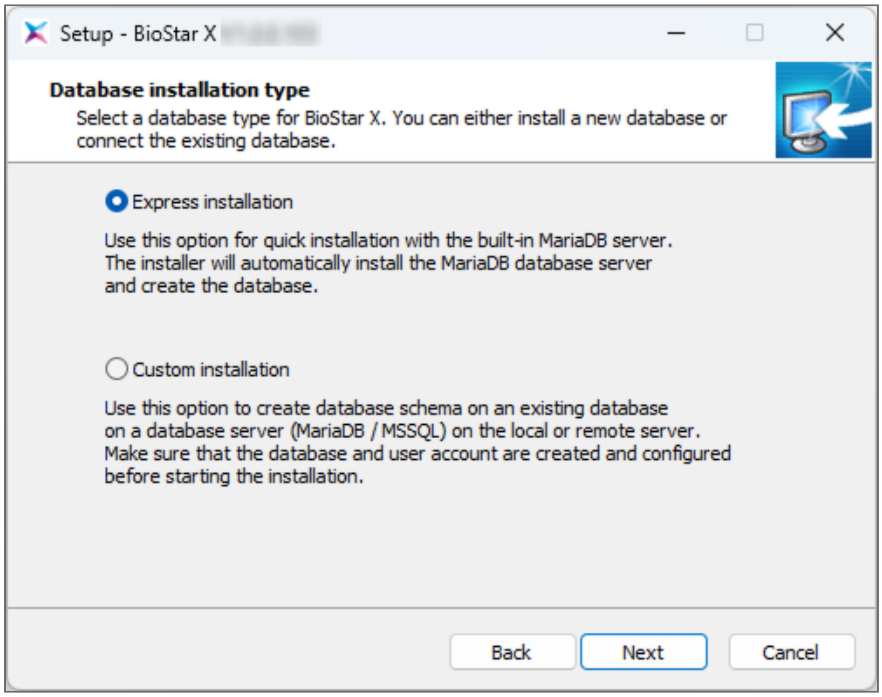
4. To continue the installation, select **I accept the agreement** and click the **Next** button.



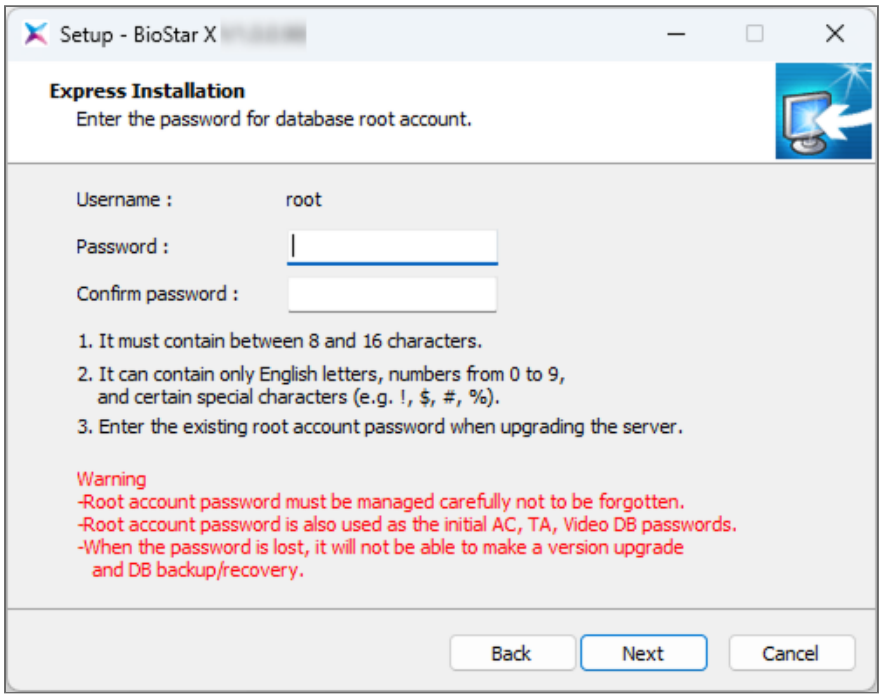
5. Enter the administrator account password and click the **Next** button.



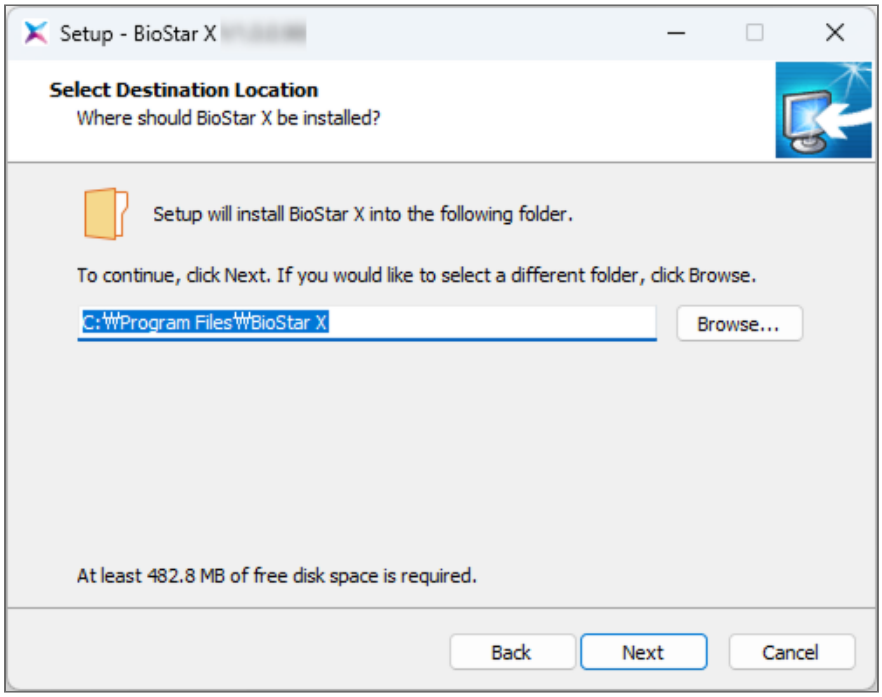
6. Select **Express installation** and click the **Next** button.



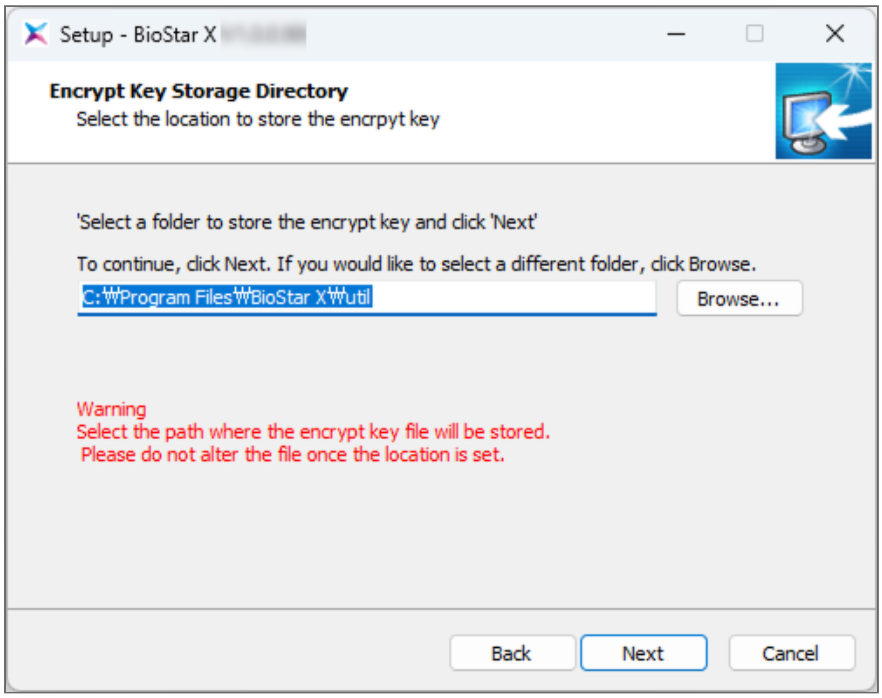
7. Enter the root account password for the database and click the **Next** button.



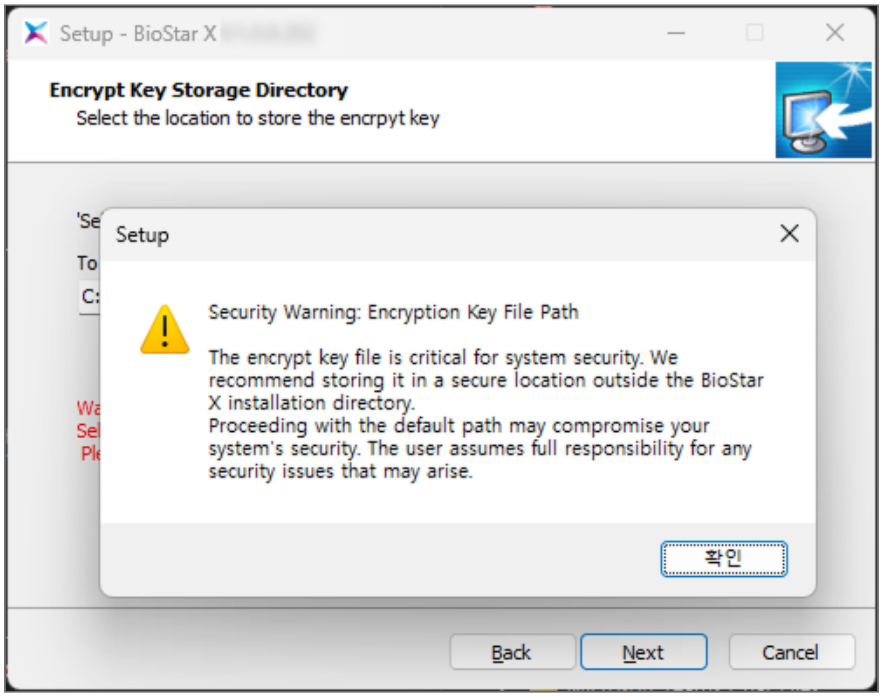
8. Set the installation path for **BioStar X** and click the **Next** button.



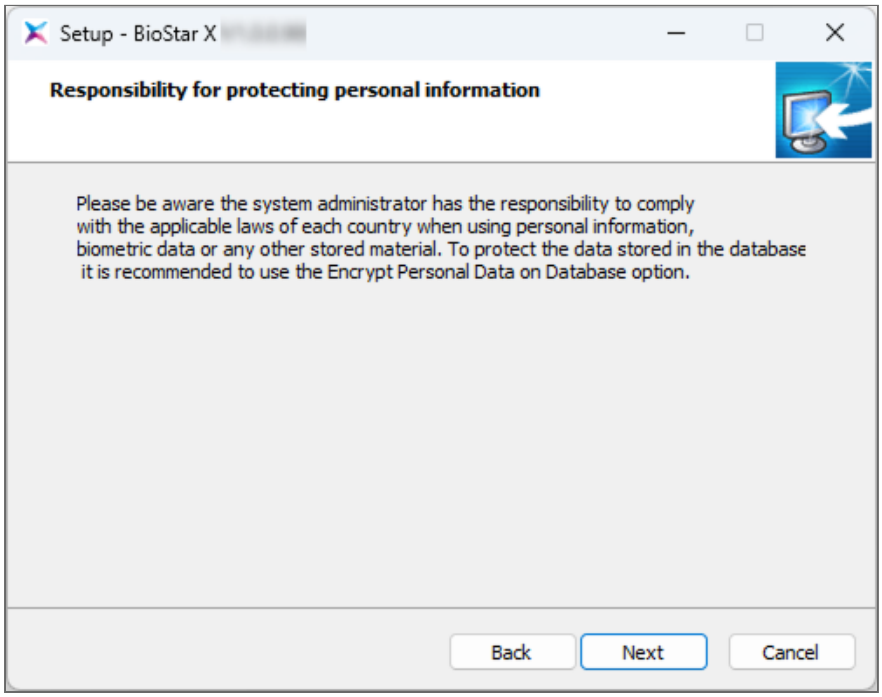
9. Set the path to store the encryption key and click the **Next** button.



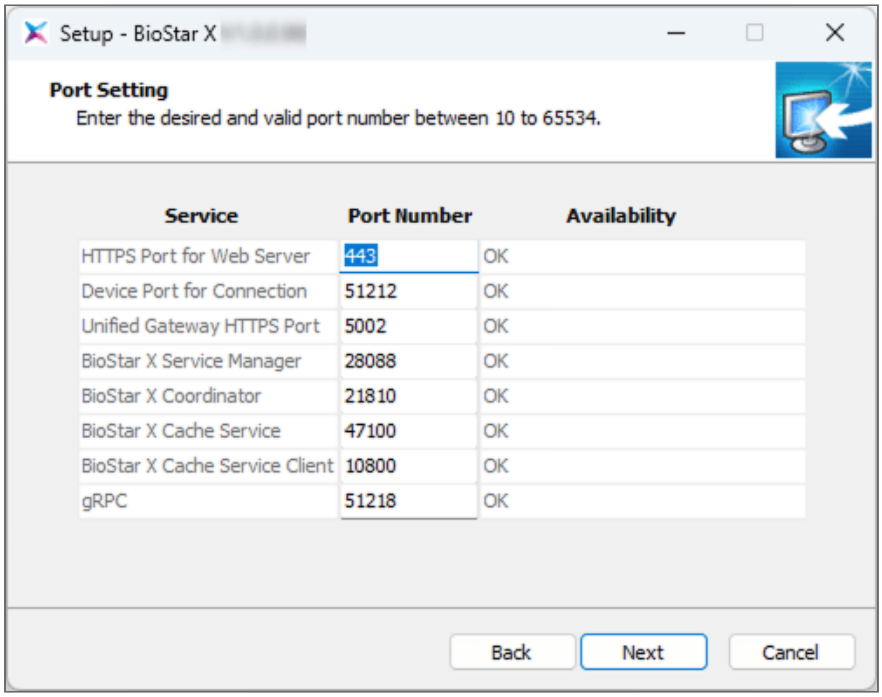
10. Check the contents of the security warning message and click **OK**.



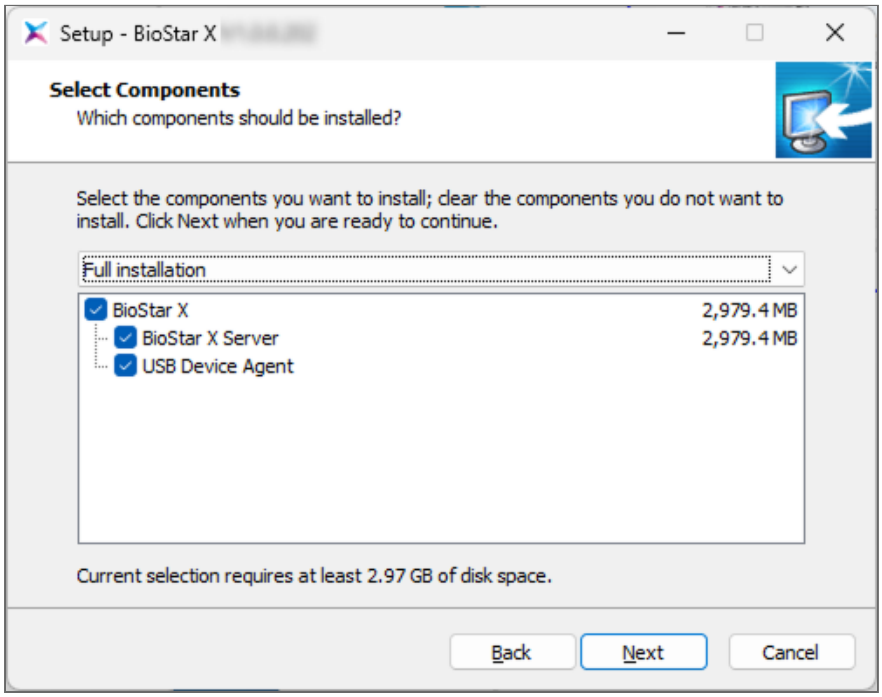
11. Read the information about the management and responsibility of personal information stored in the database, and click the **Next** button to continue the installation.



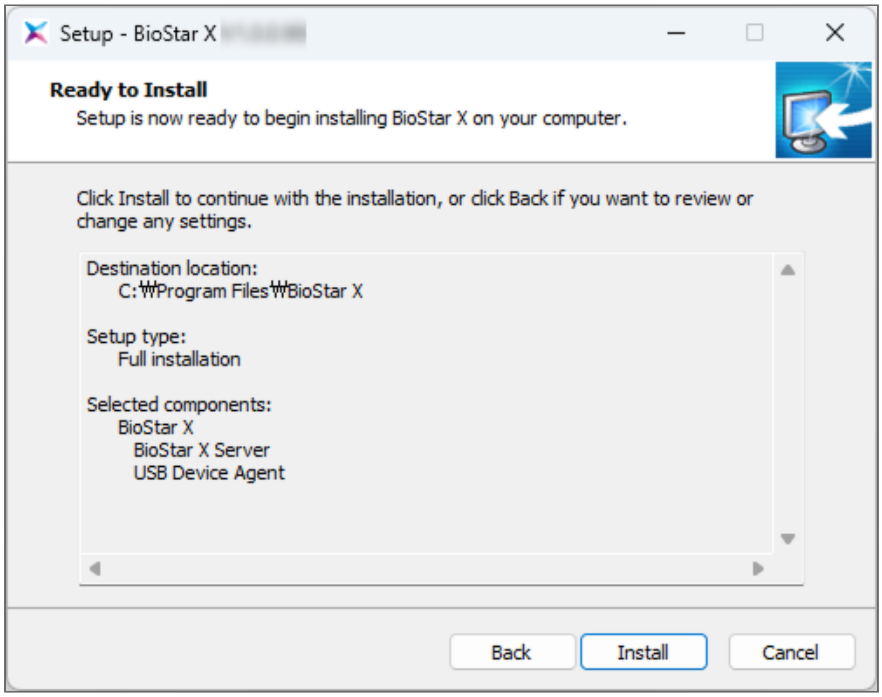
12. Set the port for **BioStar X** communication and click the **Next** button.



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.



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



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



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 more information on changing the port number, see Change the Port.
- For more information on changing database settings, see Change the Database.

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.

Next step

Check how to log in to **BioStar X** through your web browser.
Check the server status of **BioStar X** and check how to shut it down or restart it.

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 you start

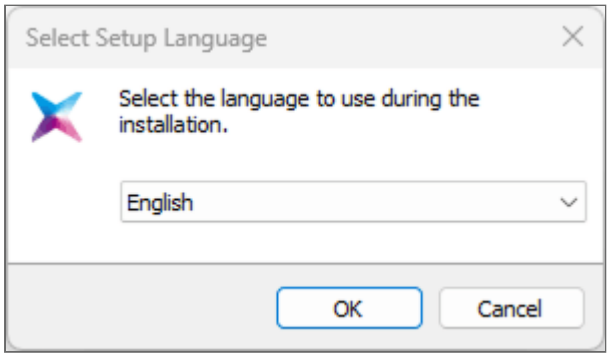
- The databases that can be used in integration with **BioStar X** are as follows.
  - MariaDB 11.4.4
  - MS SQL Server 2012 SP3
  - MS SQL Server 2014 SP2
  - MS SQL Server 2016 SP1
  - MS SQL Server 2017

  - MS SQL Server 2019
  - MS SQL Server 2022

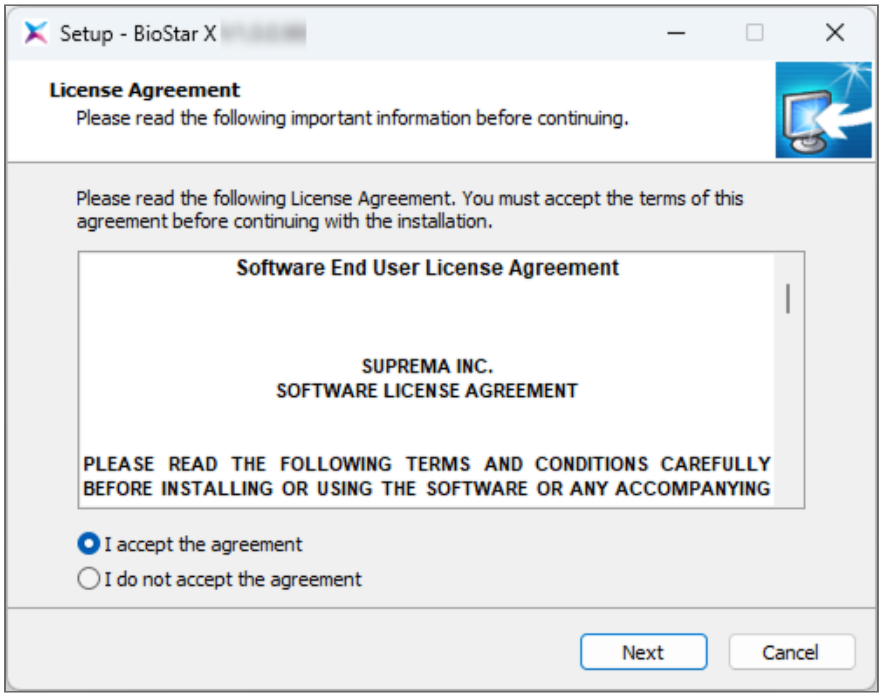
- MS SQL Server communication security supports TLS 1.2.
- If the database table creation fails when MS SQL Server is set as the Database Type, you can create the table by executing the script in *C:\Program Files\BioStar X\dbscript\mssql* folder.
- When installing with **Custom installation**, **AC 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

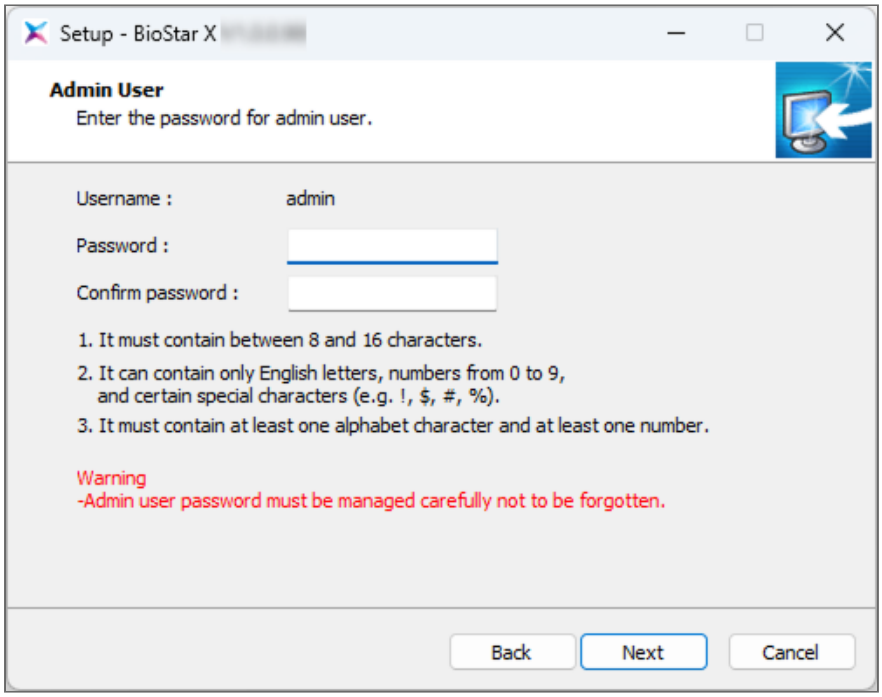
1. Go to the Suprema Download Center, log in, and download the installation package (*BioStar X Setup.X.Y.Z.BB.exe*).
2. Run the downloaded installation file.
3. Select the language to use and select the **OK** button.



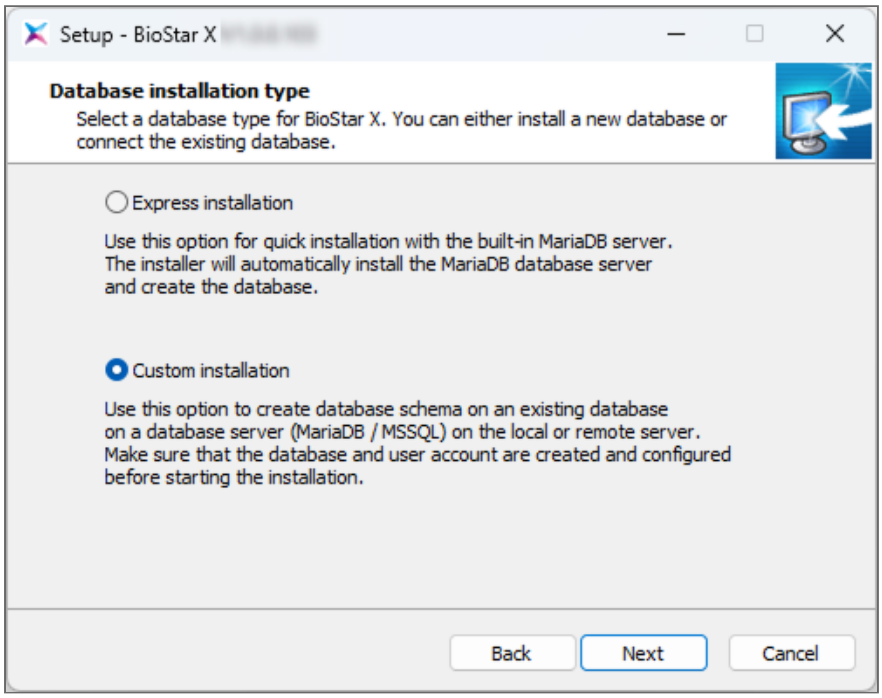
4. To continue the installation, select **I accept the agreement** and click the **Next** button.



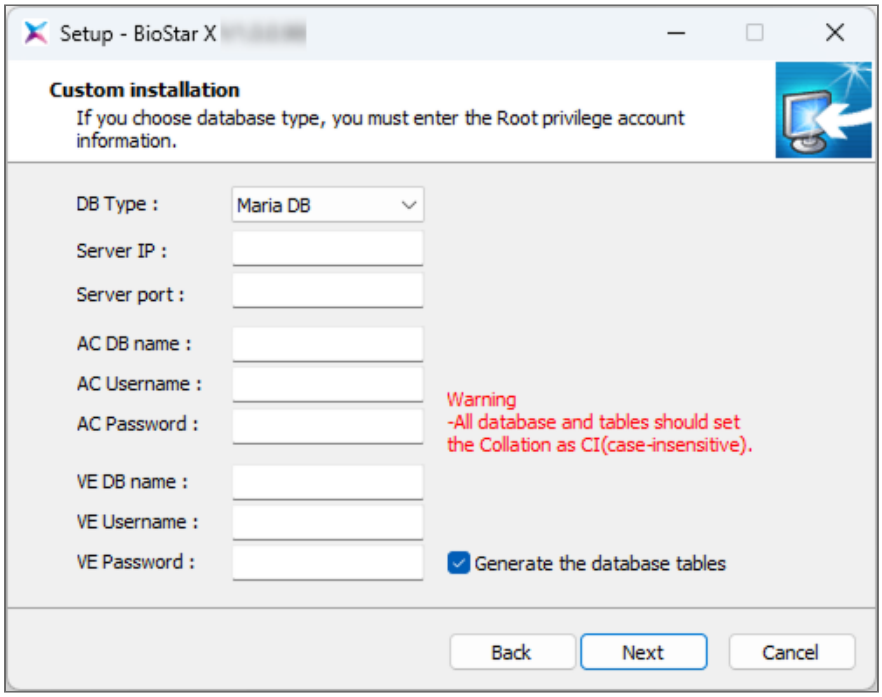
5. Enter the administrator account password and click the **Next** button.



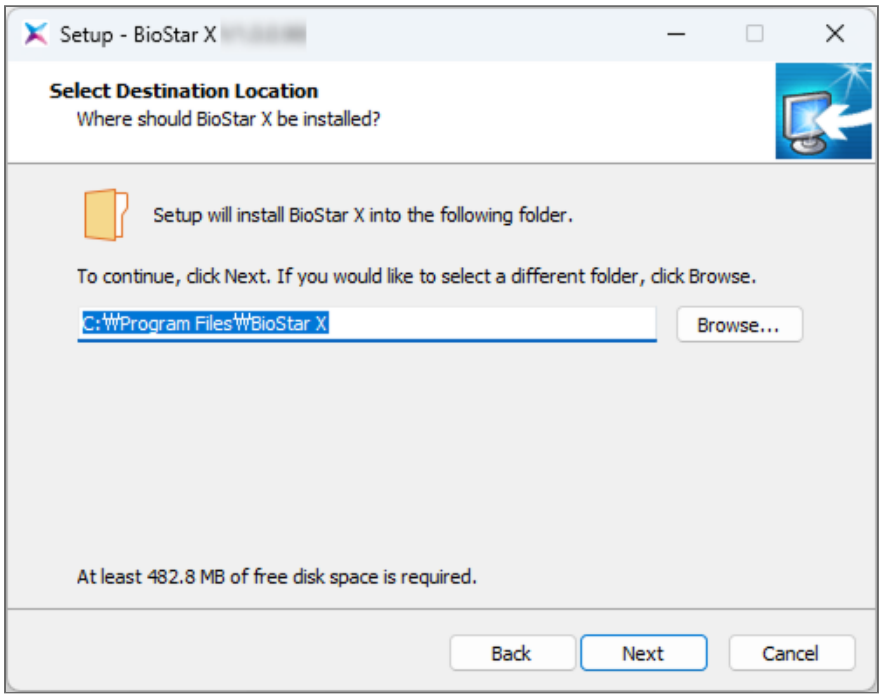
6. Select **Custom installation** and click the **Next** button.



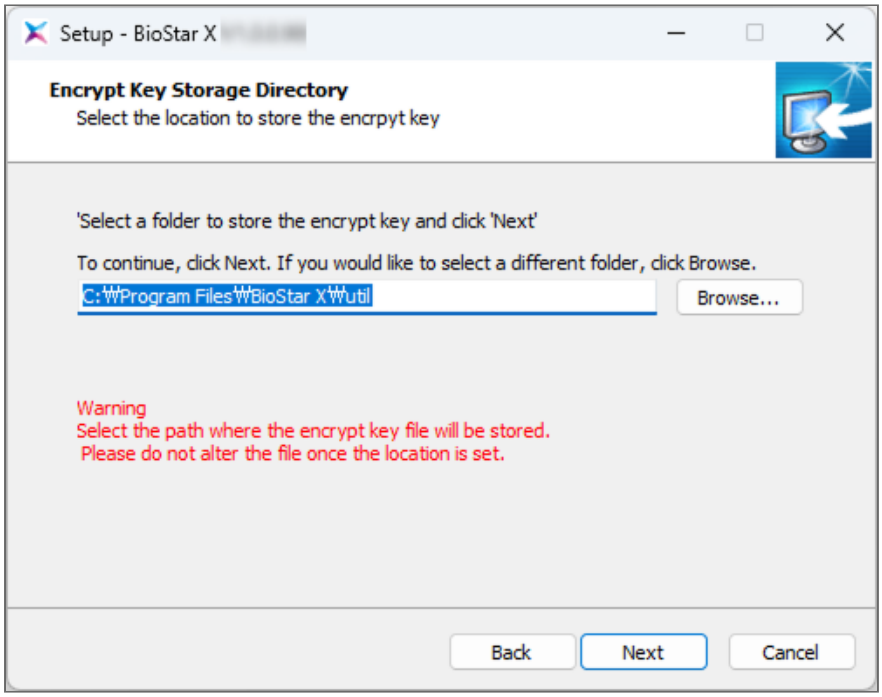
7. Enter the details of the pre-configured database and click the **Next** button.



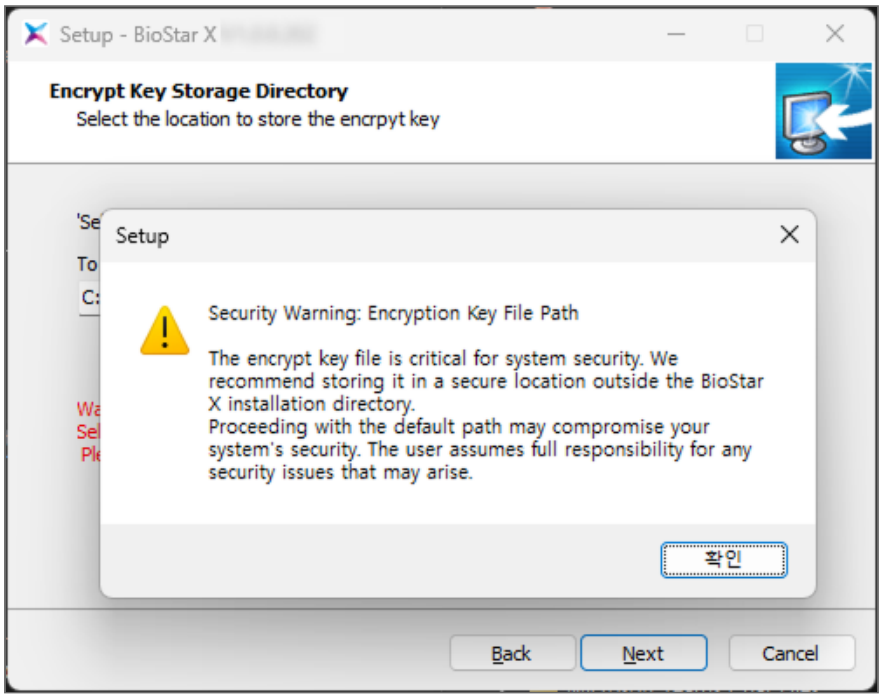
8. Set the installation path for **BioStar X** and click the **Next** button.



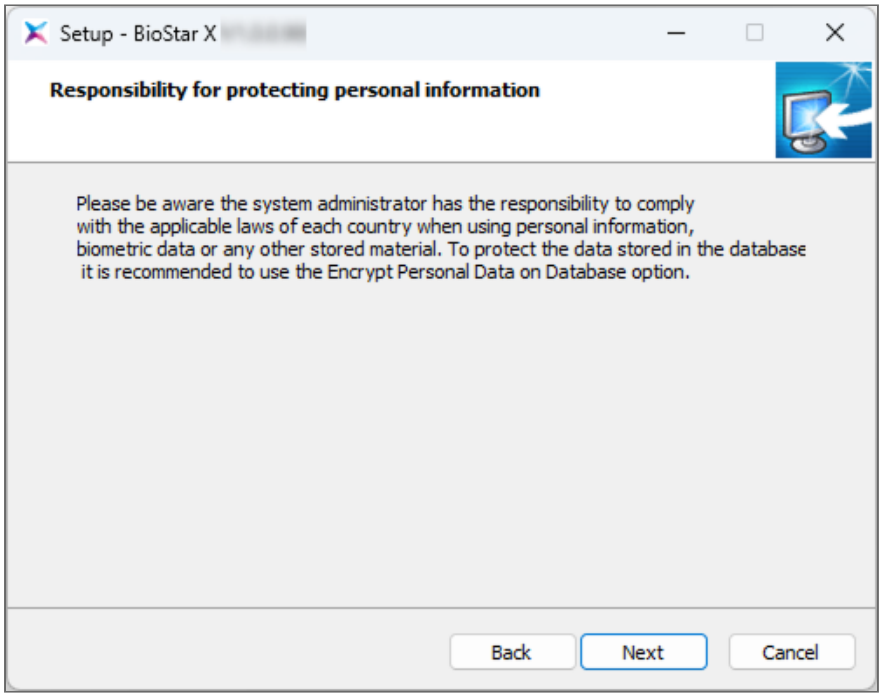
9. Set the path to store the encryption key and click the **Next** button.



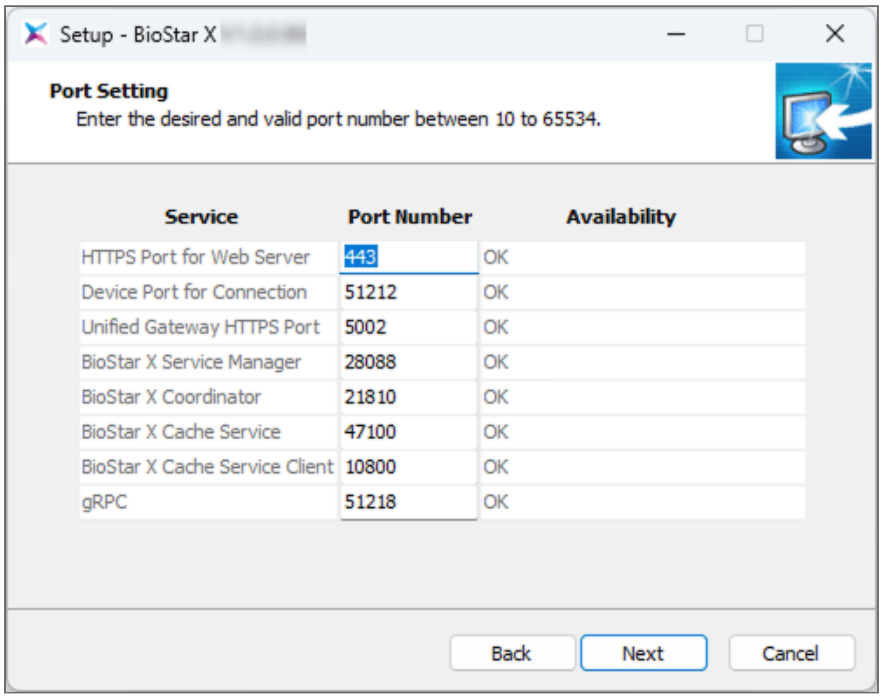
10. Check the contents of the security warning message and click **OK**.



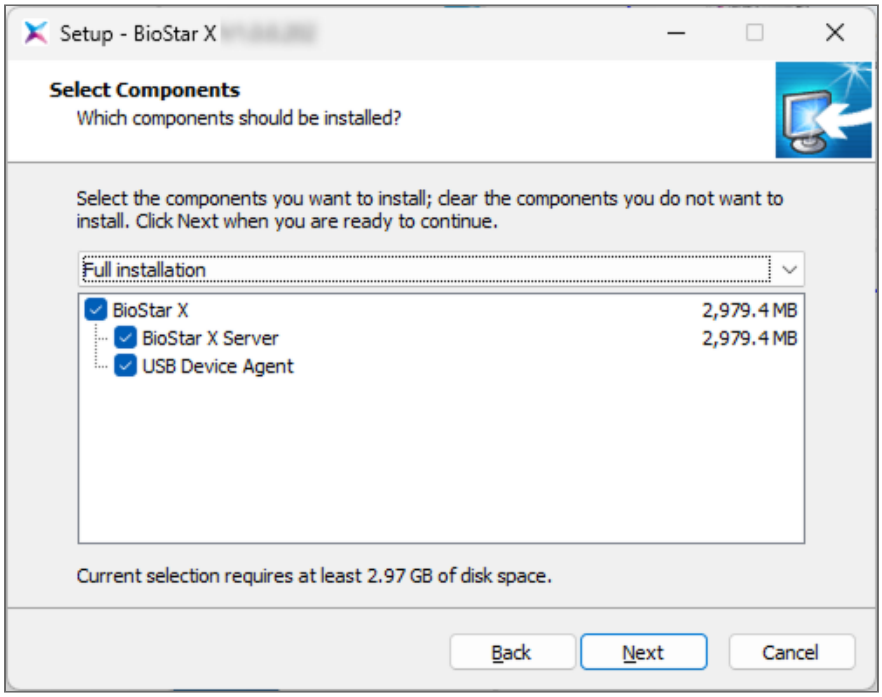
11. Read the information about the management and responsibility of personal information stored in the database, and click the **Next** button to continue the installation.



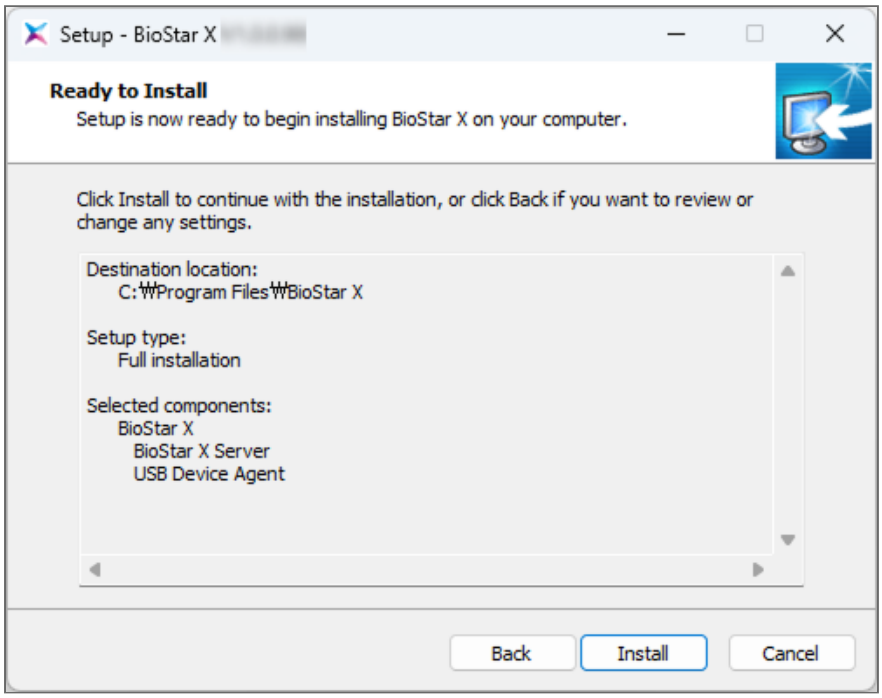
12. Set the port for **BioStar X** communication and click the **Next** button.



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.



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



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



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 more information on changing the port number, see Change the Port.
- For more information on changing database settings, see Change the Database.

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.

Next step

Check how to log in to **BioStar X** through your web browser.
Check the server status of **BioStar X** and check how to shut it down or restart it.

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 you start

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

Info

Important

Minimum requirements

- Before proceeding with the upgrade, refer to System Minimum Requirements to confirm that the server specifications meet the 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.

Warning

Verify certificate

When you upgrade from BioStar 2 to BioStar X, the `biostar_cert.crt` file in `nginx\conf` and the one in `nginx\cert` may differ. Upgrading in this state causes the following problems.

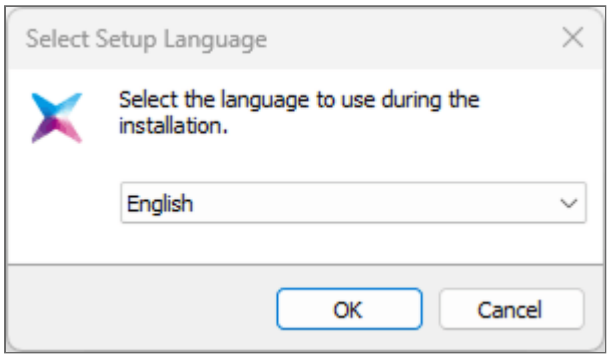
- Certain audit logs are not recorded.
- Creating user groups, adding Wiegand, and refreshing the tree fail.

Follow these steps to match the certificate files before upgrading to BioStar X.

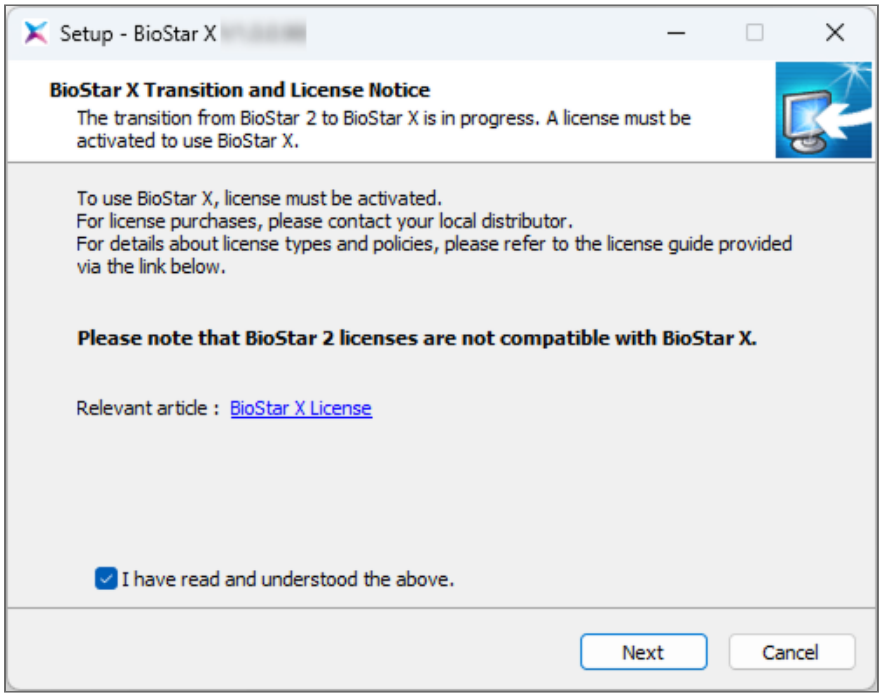
1. Stop the BioStar 2 service.
2. Overwrite the `biostar_cert.crt` and `biostar_cert.key` files in `nginx\cert` with the files from `nginx\conf`.
3. Restart the BioStar 2 service.

Upgrade installation guide

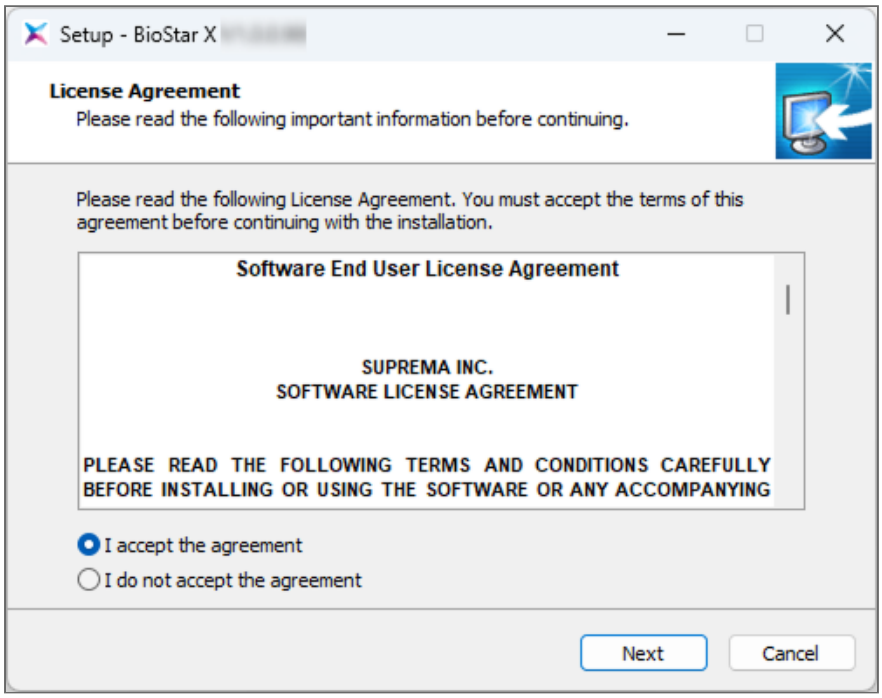
1. Go to the Suprema Download Center, log in, and download the installation package (*BioStar X Setup.X.Y.Z.BB.exe*).
2. Run the downloaded installation file.
3. Select the language to use and select the **OK** button.



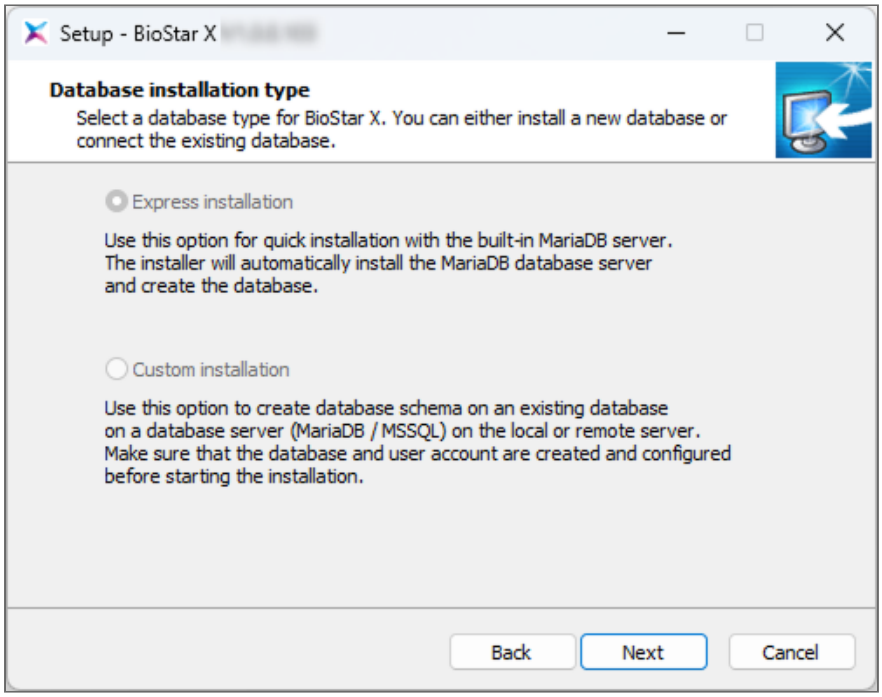
4. Agree to the licensing policy of transitioning from BioStar 2 to **BioStar X**. Click the checkbox and select the **Next** button.



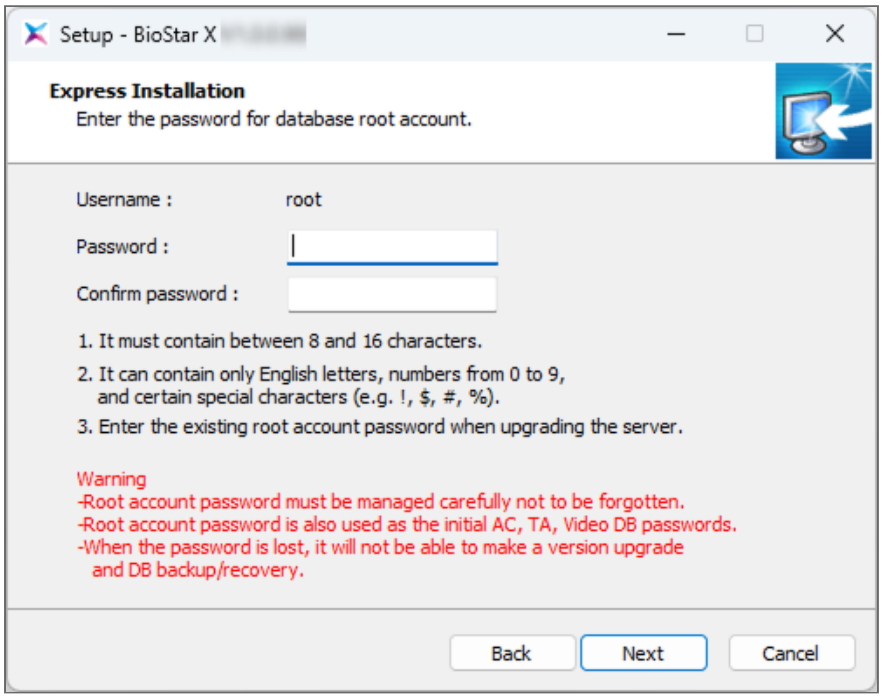
5. To continue the installation, select **I accept the agreement** and click the **Next** button.



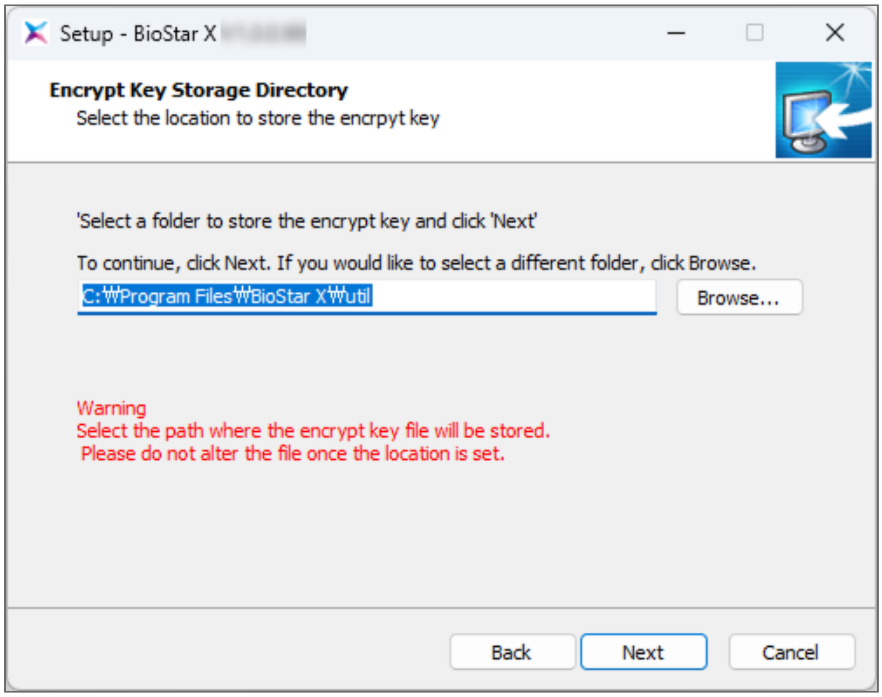
6. When upgrading from BioStar 2, the existing database will be connected to proceed with the installation. Click the **Next** button.



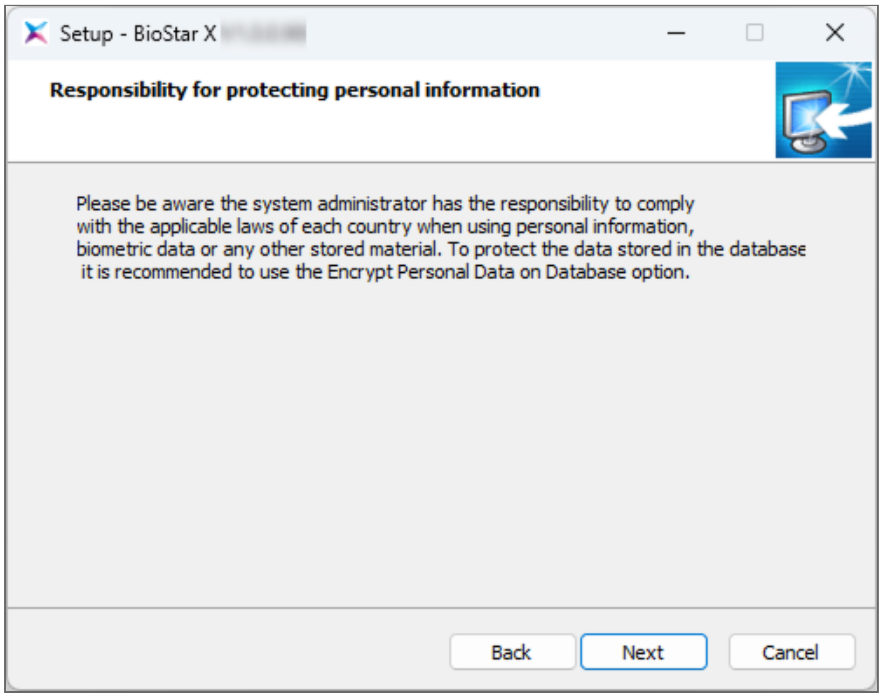
7. Enter the root account password of the existing database and click the **Next** button.



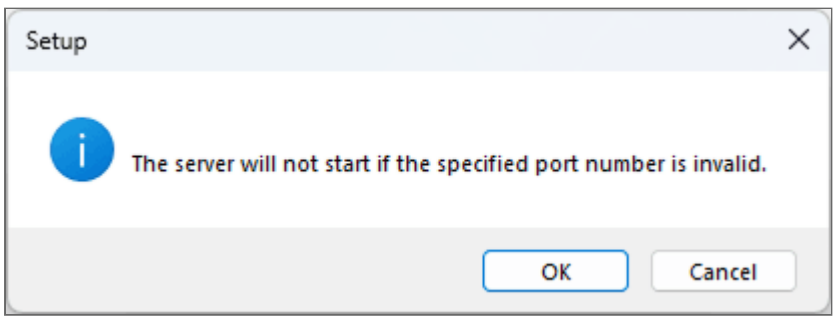
8. Set the path to store the encryption key and click the **Next** button.



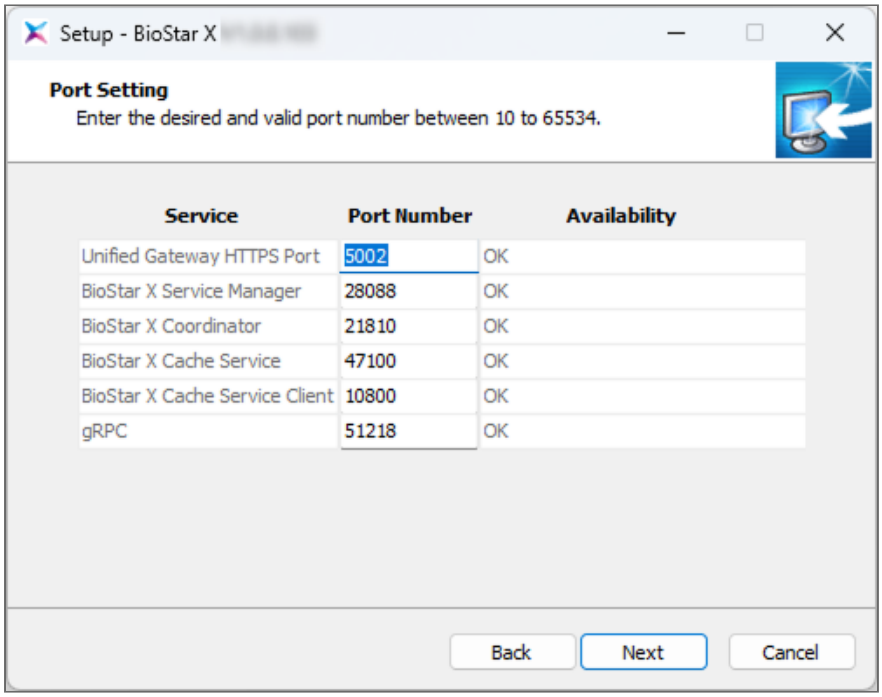
9. Read the information about the management and responsibility of personal information stored in the database, and click the **Next** button to continue the installation.



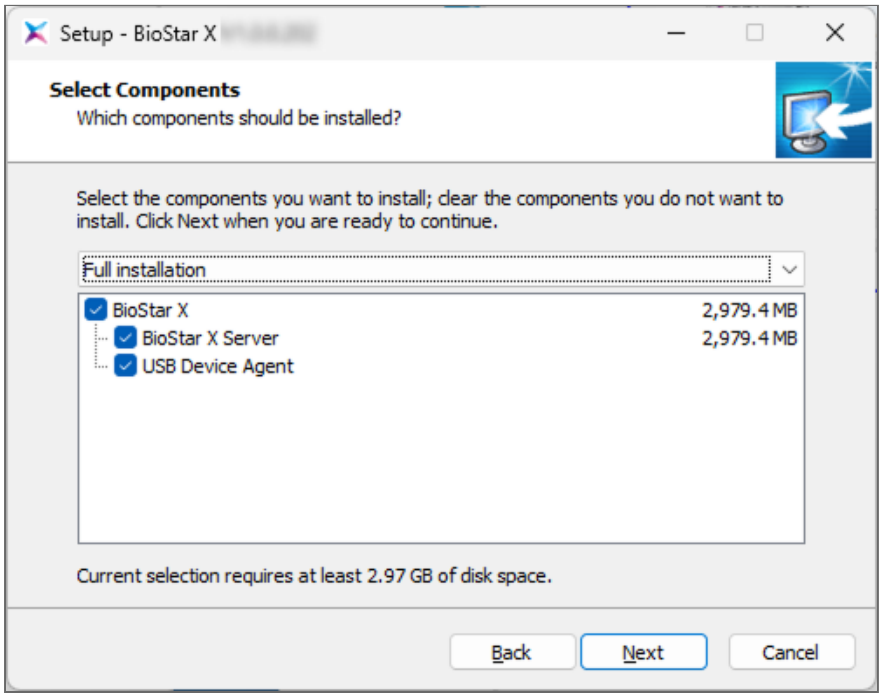
10. If a port number related message appears, click **OK**.



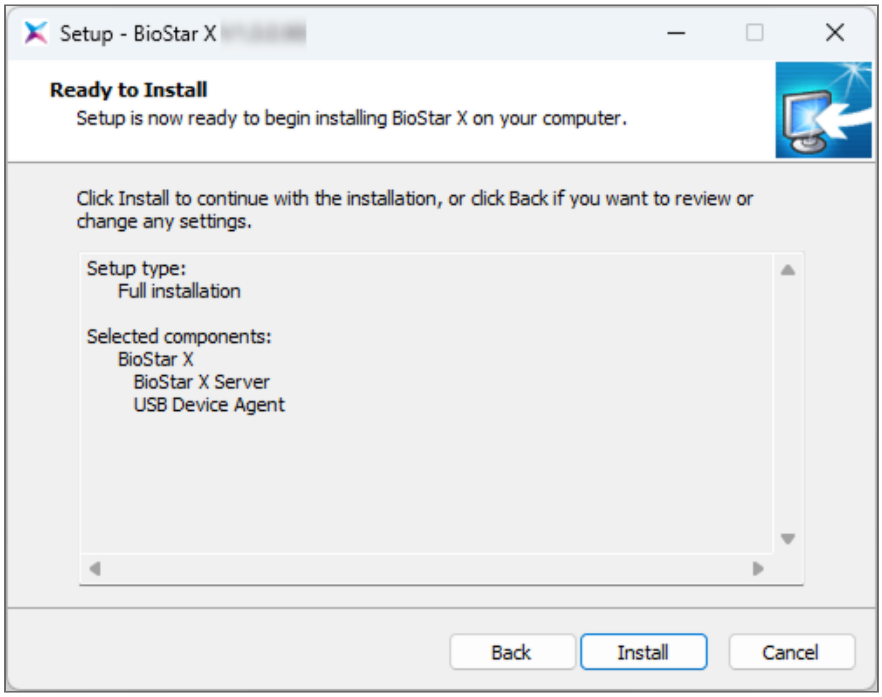
11. Set the port for **BioStar X** communication and click the **Next** button.



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.



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



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



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 more information on changing the port number, see Change the Port.
- For more information on changing database settings, see Change the Database.

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.

Next step

Check how to log in to **BioStar X** through your web browser.
Check the server status of **BioStar X** and check how to shut it down or restart it.

Install Multi Communications Server

This document explains how to install the **BioStar X Multi Communications Server**.

The Multi Communications Server handles communication with access control devices. It helps to manage many devices reliably by installing separately from the main server. A single Multi Communications Server can connect up to 1,000 devices. Add multiple Multi Communications Servers as needed.

Info

Up to 1,000 devices can connect via Ethernet (TCP/IP).

Before you start

Before installing the Multi Communications Server, check the following.

- The Multi Communications Server cannot be installed on the same server as the **BioStar X** server.

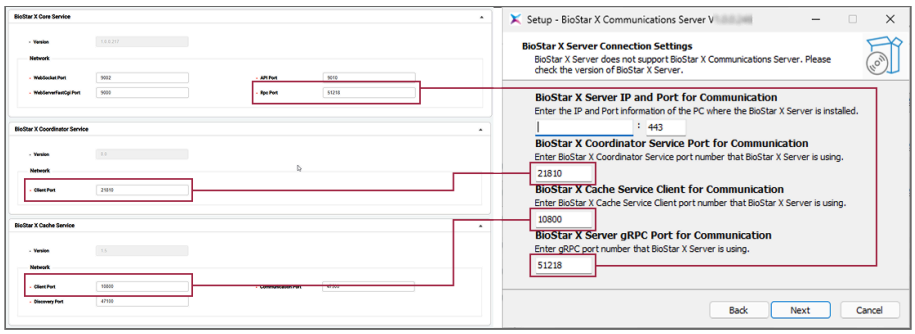
- The Multi Communications Server can only be installed on a 64-bit operating system. For more information on minimum system requirements, see System Minimum Requirements.
- A Multi Communications Server license is required to install and connect the server. For more information on licensing policies, see License Policy.

Pre-installation checks

Before installing the Multi Communications Server, run **BioStar X Service Manager** to check the information required 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 to install the Multi Communications Server. Review and prepare each item.



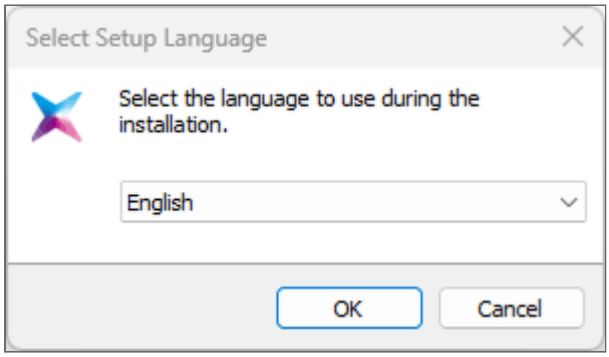
BioStar X Service Manager	Information required for Multi Communications Server installation
BioStar X Core Service → **RPC Port**	BioStar X Server gRPC Port for Communication
BioStar X Coordinator Service → **Client Port**	BioStar X Coordinator Service Port for Communication
BioStar X Cache Service → **Client Port**	BioStar X Cache Service Client for Communication

> **Info**
> For more information on **SERVICE SETTINGS**, see Service Settings.

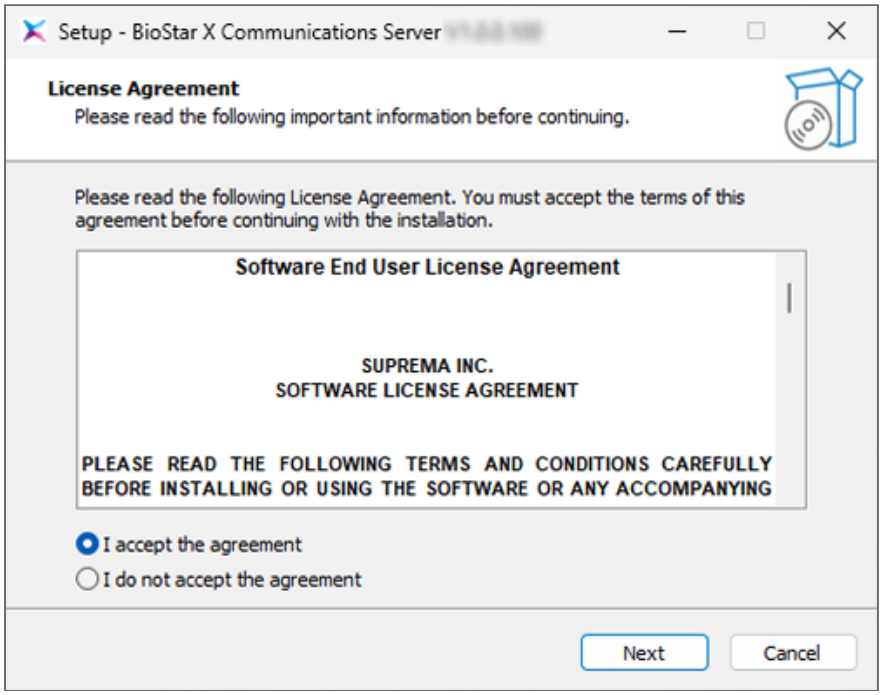
Installation guide

Follow the steps below to install the Multi Communications Server.

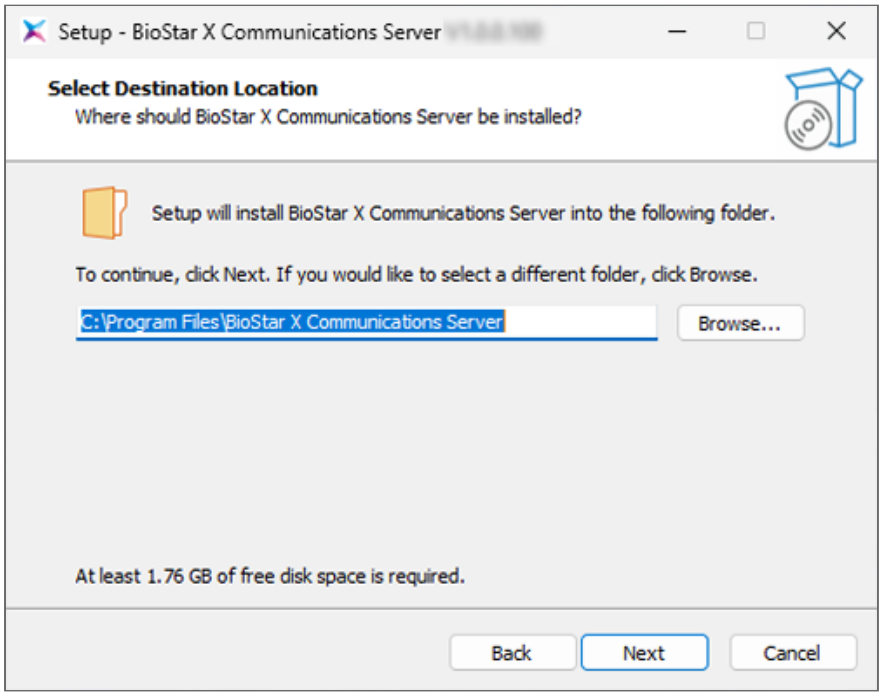
1. Access the Suprema Download Center, log in, and download the installation package (*BioStar X Communications Server.X.Y.X.BB.exe*).
2. Run the downloaded installation file.
3. Select the language to use and select the **OK** button.



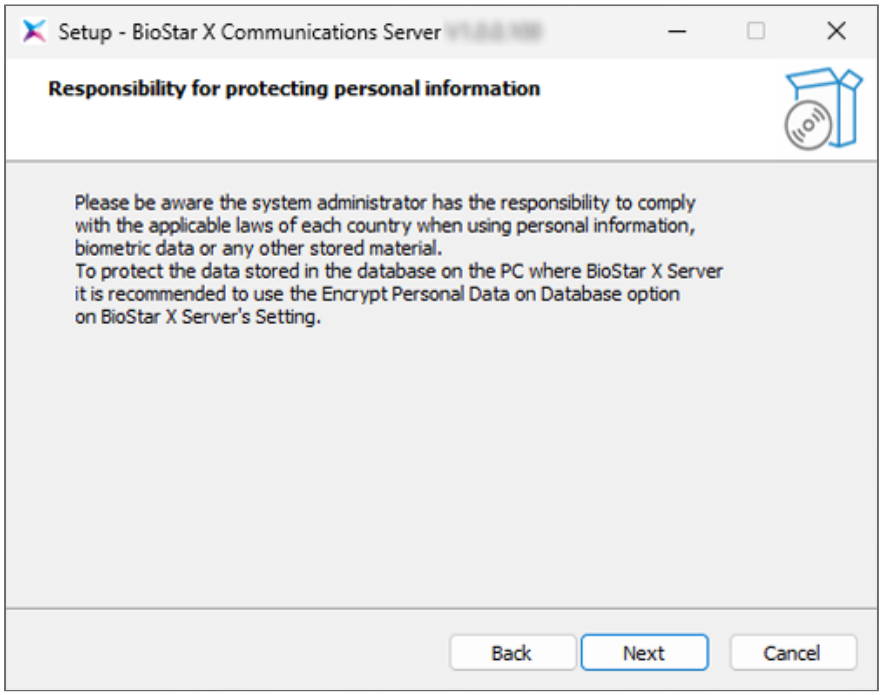
4. To continue the installation, select **I accept the agreement** and click the **Next** button.



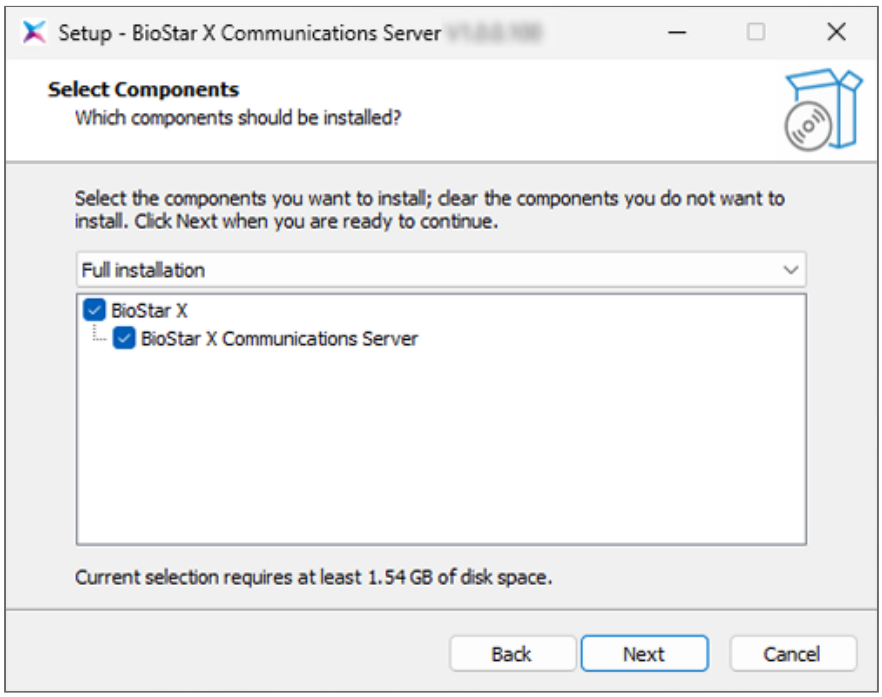
5. Set the installation path for the Multi Communications Server and click **Next**.



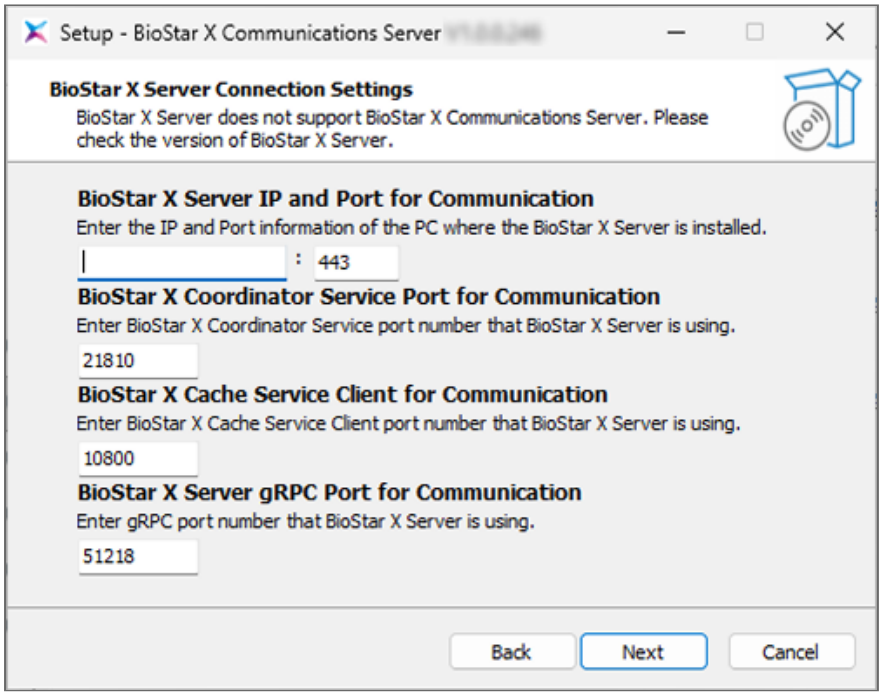
6. Review the permissions and responsibilities regarding personal information and click **Next** to continue the installation.



7. Select the components of the Multi Communications Server and click **Next**.

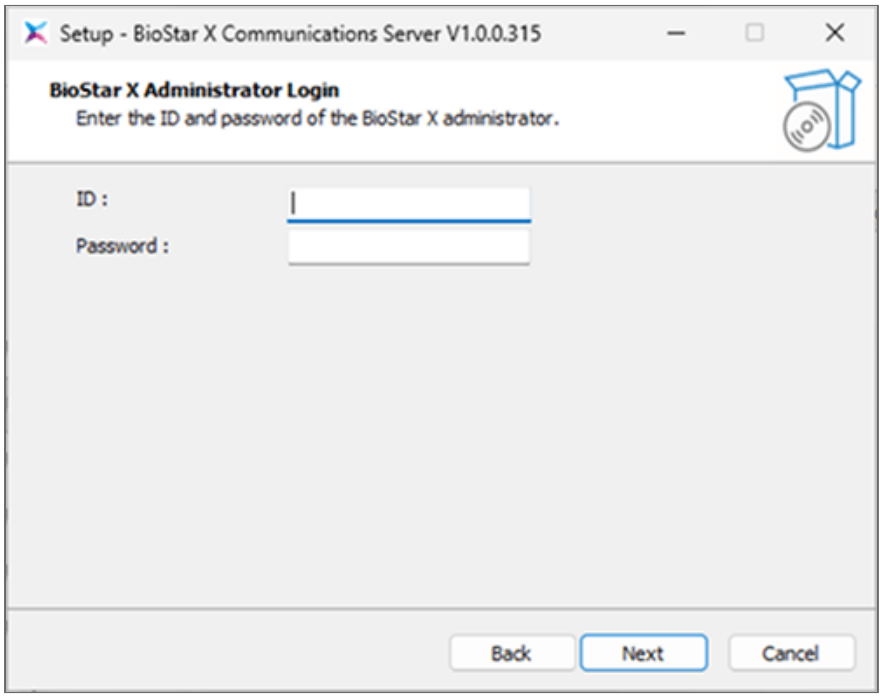


8. Enter the IP address and port number of the **BioStar X** server, and input details for connection to the **BioStar X** server. Complete your settings and click **Next**.

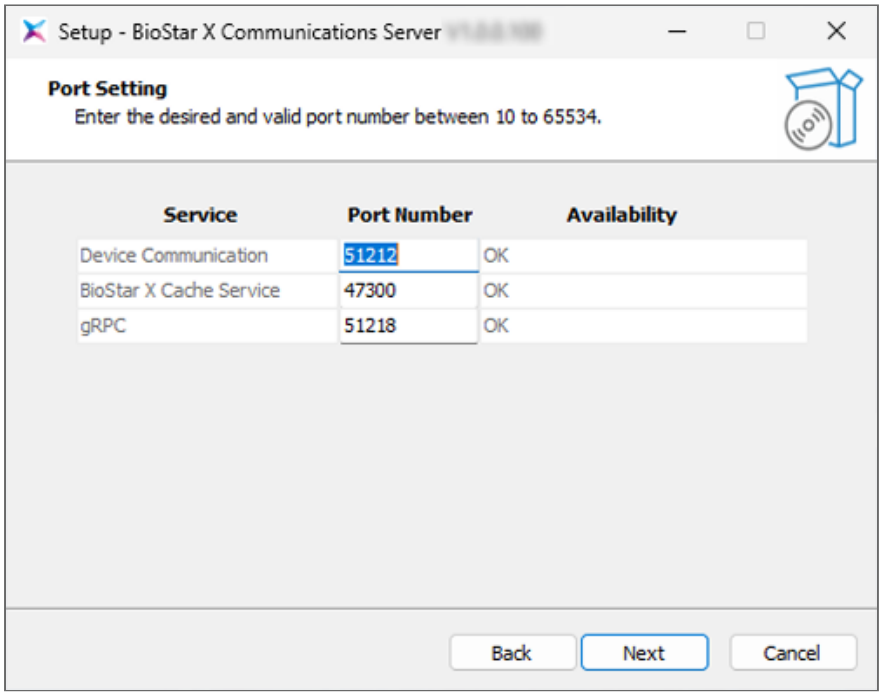


> For more information on each input field, see Pre-installation checks.

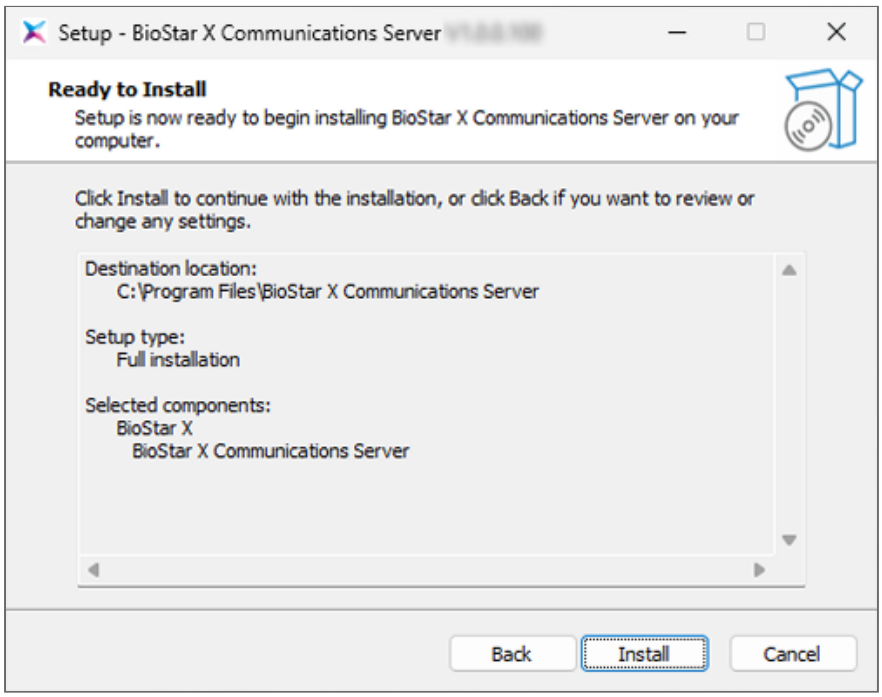
9. Enter the **BioStar X** administrator ID and password, then click **Next**.



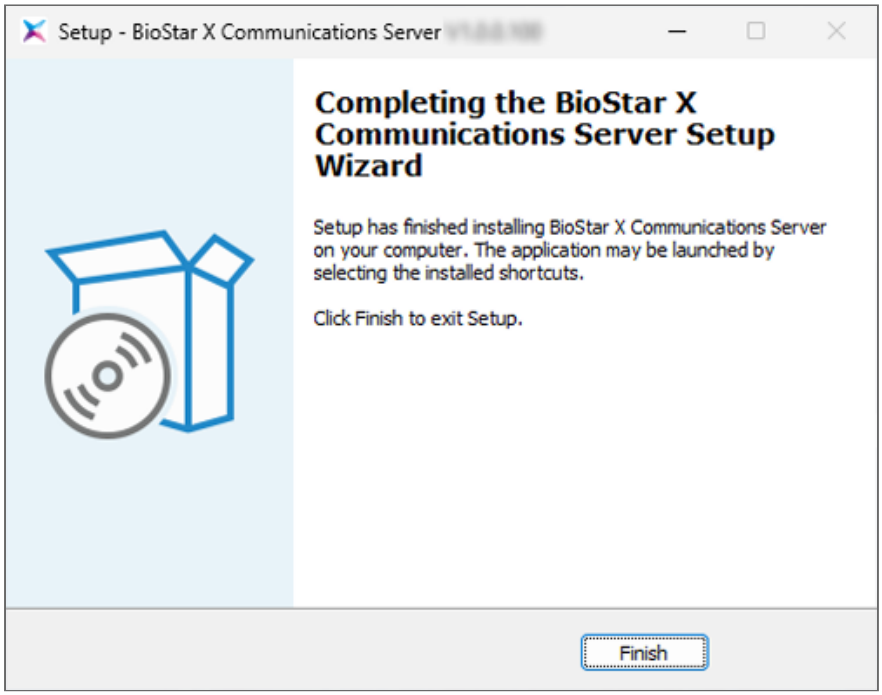
10. Set the port for communication and click **Next**.



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



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

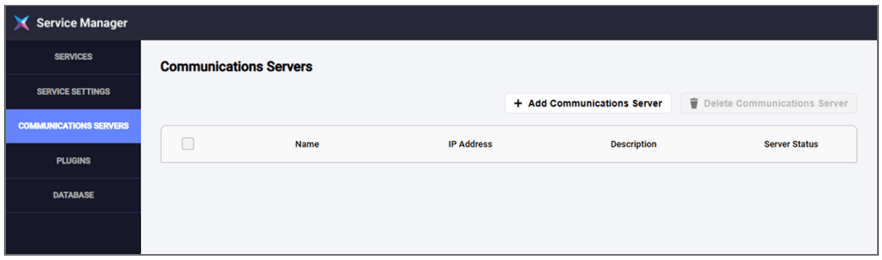


Complete the installation of the Multi Communications Server. Once the installation is complete, verify the connection between the Multi Communications Server and the **BioStar X** main server.

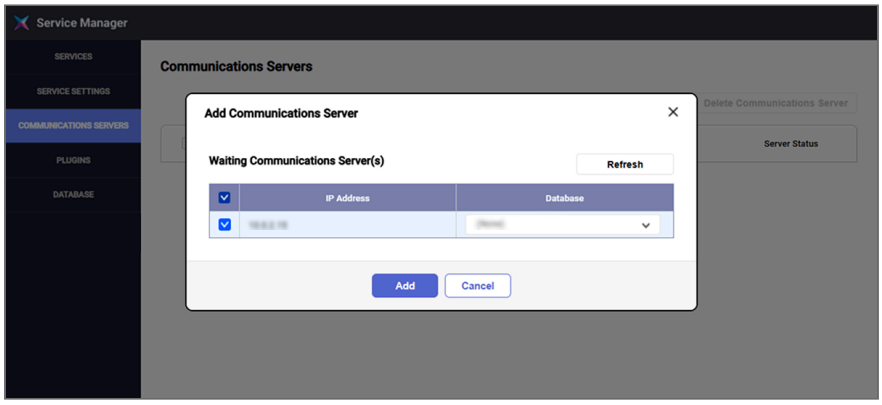
Post-installation checks

After installing the Multi Communications Server, connect it to the main server in **BioStar X Service Manager**.

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

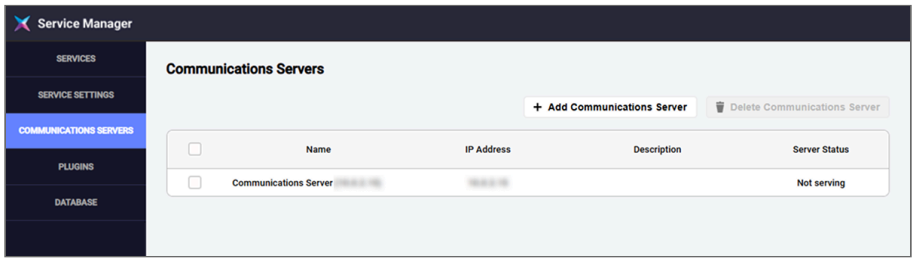


4. Click **Add Communication Server** in the upper right corner of the screen.
5. When the **Add Communication Server** window appears, select the checkbox that matches the installed Multi Communications Server IP address. In the **Database** column, select the database to use.



6. Click the **Add** button.

In the Multi Communications Server list, check that **Server Status** shows **Connected**.



Info

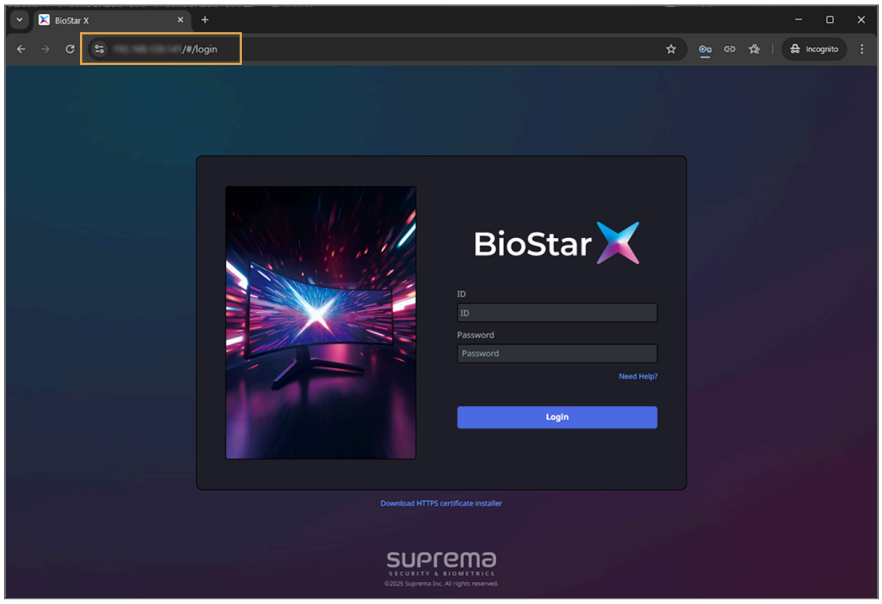
- The **COMMUNICATIONS** menu can be used when the multi-communication server license is activated. For more information on licensing policies, see License Policy.
- To delete the Multi Communications Server, check the box of the server to be deleted in the list and click **Delete Communication Server** in the upper right corner of the screen.
- When adding a Multi Communications Server, add a secondary database to reduce the load on the main server. For more information on adding a secondary database, see Add Auxiliary Database.

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.

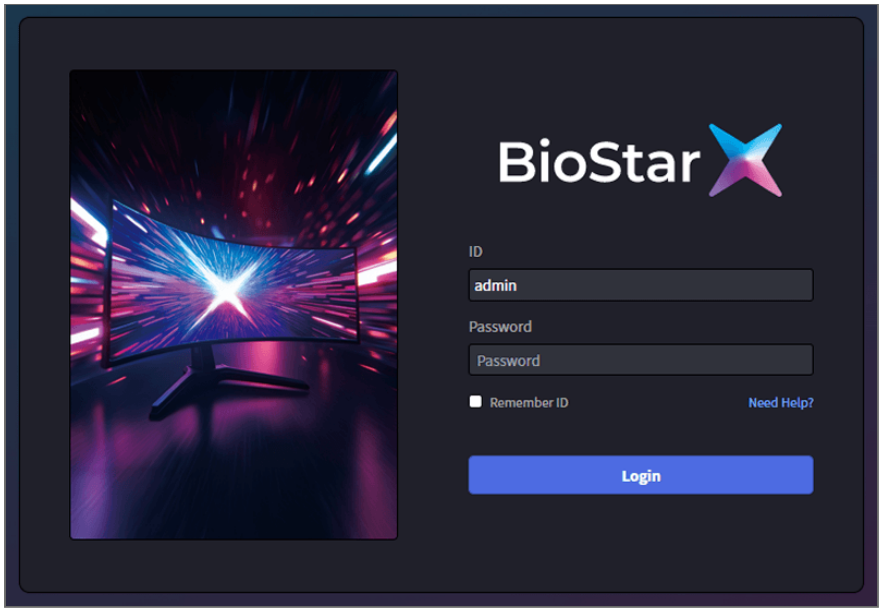
Log in from a web browser

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



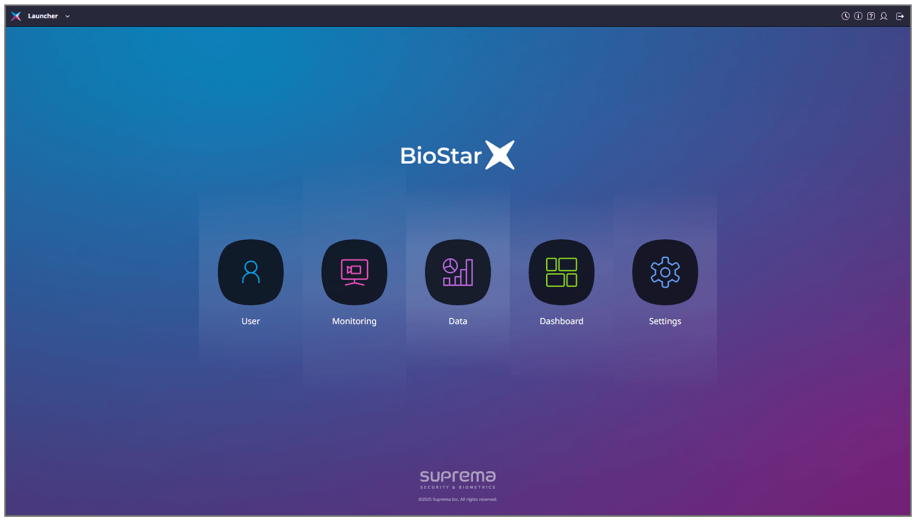
- Check the access address of **BioStar X** in the web browser's address bar.
- If you installed **BioStar X** on another PC, enter the IP address of that PC. e.g. https://192.168.0.1
- Do not use 'localhost' as the **BioStar X** access address.
- **BioStar X** processes all requests through the Unified 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 a certificate, see Install HTTPS Certificate.

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, see Change the Port.

Register License Key

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

Navigate to **Settings** → **License** → **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.

Info

- Certain features such as adding users, doors, and ports are restricted when the license is not registered.
- For more information the **License** menu, see Activate License.
- For more information on the licensing policy, see License Policy.
- For more information about license error codes, refer to the following link.

Register online

Info

The license key accepts only numbers and hyphens (`-`). Enter up to 16 digits in the `1111-1111-1111-1111` format.

Register a single license

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



Register multiple licenses

Add up to 30 licenses at a time. Click the + **Add More License** button. After entering all licenses, click **Activate**.



- When the number of fields reaches 30, the + **Add More License** button becomes disabled. You cannot add more licenses.
- Paste multiple license keys into the fields at once. The system detects only keys in the `1111-1111-1111-1111` format and splits them into each field.
- If the pasted keys exceed 30, only the first 30 are entered automatically. Extra keys are ignored.

Activation progress

Click **Activate** to open the progress pop-up. Do not close the page or popup until activation completes.

Register 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.

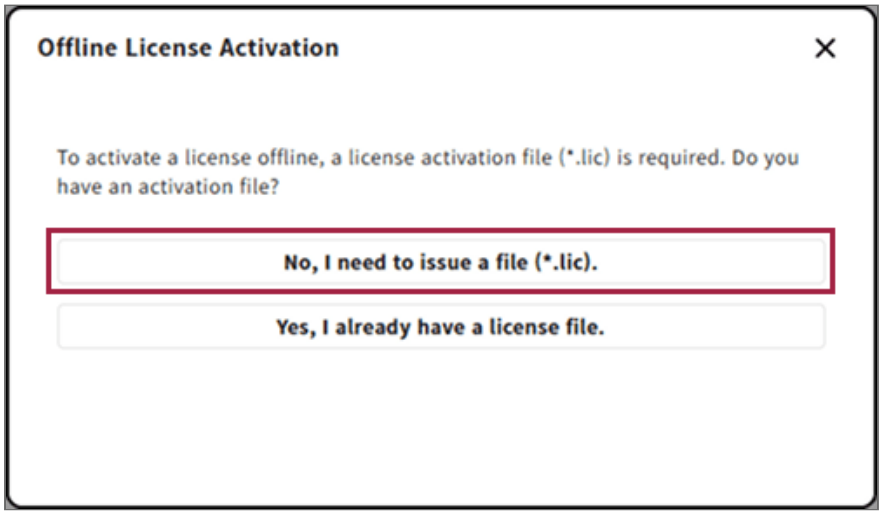
1. Enter any registration manager name for registration and the license key in the **License Activation** section.

   - The license key accepts only numbers and hyphens (`-`). Enter up to 16 digits in the `1111-1111-1111-1111` format.
   - Save or write down the administrator name and license key.
   - If you need multiple licenses, click the + **Add More License** button to add them.

2. Click **Offline Activation**.

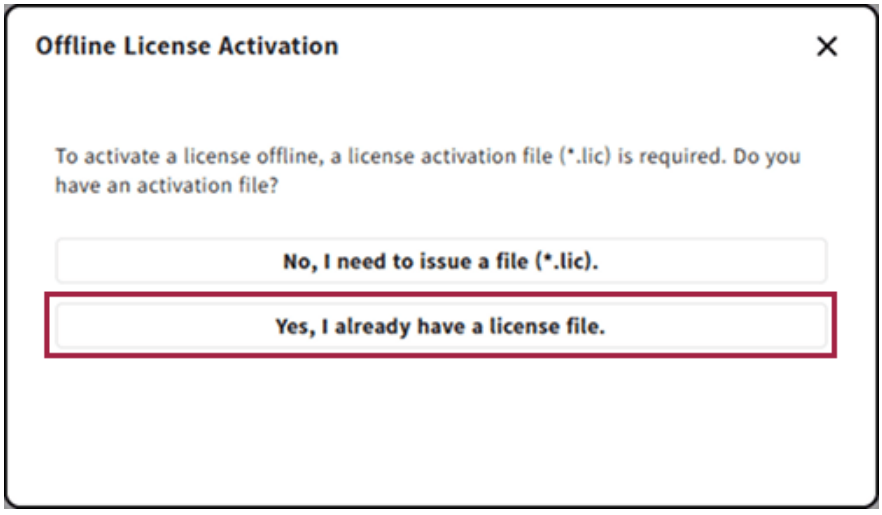


3. When the **Activate License Offline** window appears, click **No, I need to issue a file (*.lic).**.



> If an issued license file is available, click **Yes, I already have a license file.** on this screen, then go to step 9.

4. When the license request file (*.req) is created, download it to the local disk.
5. Send the downloaded request file to the reseller and request an offline activation file (*.lic).
6. After receiving the offline activation file, enter the administrator name and license key from step 1 in the **License Activation** section.
7. Click **Offline Activation**.
8. When the **Activate License Offline** window appears, click **Yes, I already have a license file.**.



9. When the Open File window appears, select the offline activation file (*.lic) or the compressed file (*.zip) stored locally.

> If you request multiple licenses, you may receive a compressed file.

10. A progress status pop-up appears. Do not close the page or popup until activation completes.

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

> **Info**
> Obtain a **Device Manager** or higher license to register devices. For more information on the licensing policy, see License Policy.

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 **Essential** or higher license. For more information on the licensing policy, see License Policy.

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

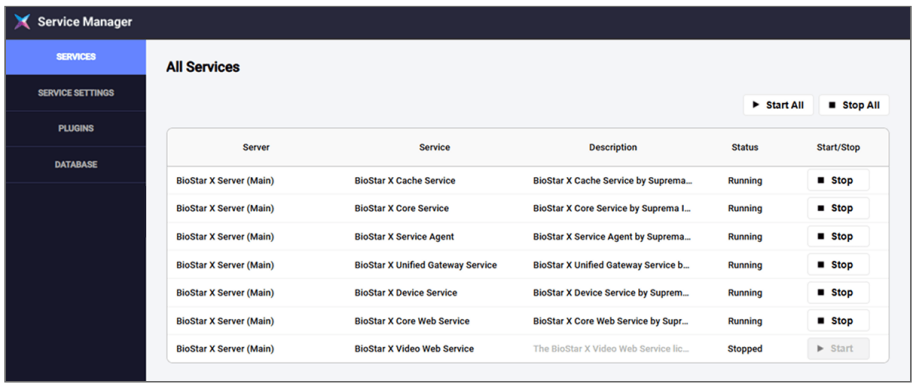
After installing BioStar X, users can efficiently operate the system through various server management features. This document guides you on the server management features of BioStar X.

Start and Stop Server

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

BioStar X Service Manager

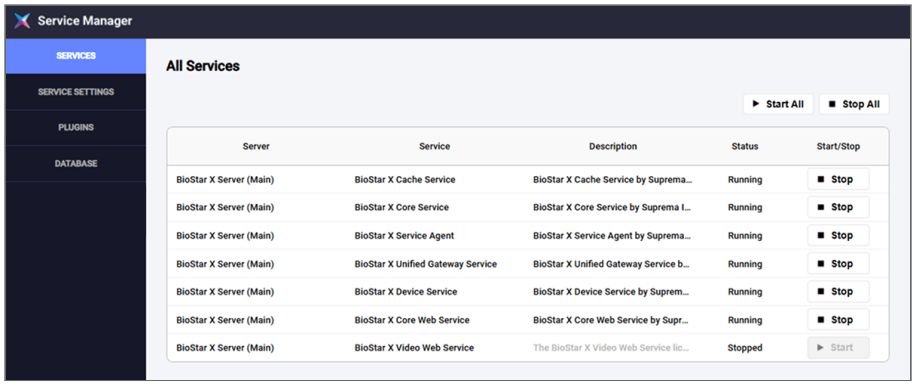
Provides a tool to manage the status of the **BioStar X** server. Click Start → **BioStar X** → **BioStar X Service Manager** on Windows. The **BioStar X Service Manager** window appears.



> **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**.

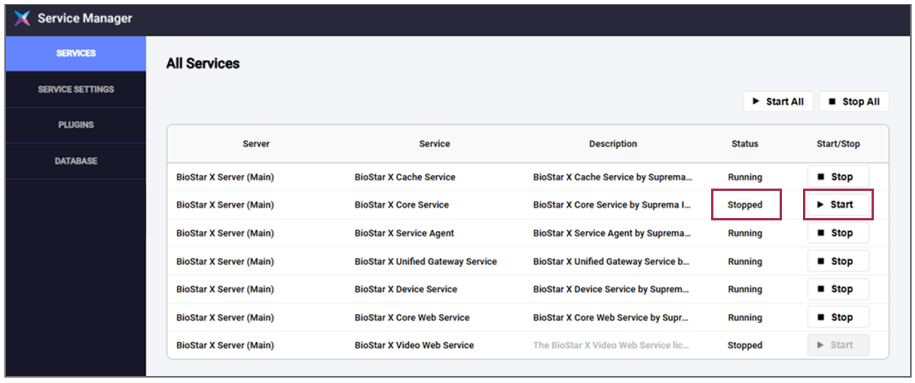
End service

To shut down **BioStar X**, click the **Stop** button for individual services in the **SERVICES** menu. To stop all services, click the **Stop All** button in the top right corner of the screen.



Start the server

To restart **BioStar X**, click **Start** for the service in the **SERVICES** menu with a **Stopped** status in the **Status** column. To restart all services, click the **Start All** button in the top right corner of the screen.



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 that require changing settings

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 **Apply** in the upper right corner of the screen.

- Restart the related service to apply the changes after changing the service setting.
- Support for changing the port may vary depending on certain services.

Caution
When changing port numbers, make sure there are no conflicts with other services or applications.

Service composition

BioStar X Core Web Service

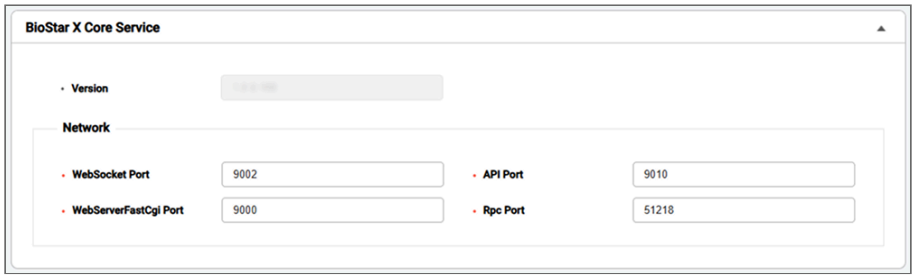
This service is responsible for the web-based user interface.



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

BioStar X Core Service

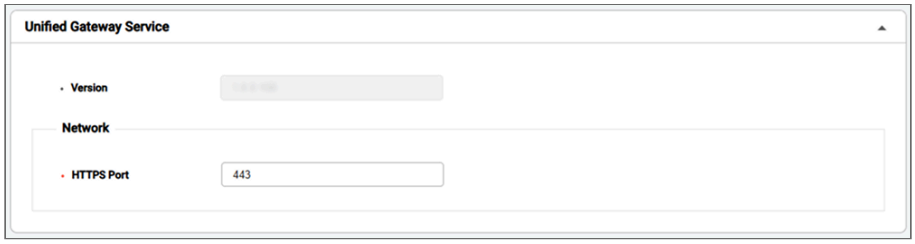
This is the main service that handles core functionalities of the system and external API communications.



- **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

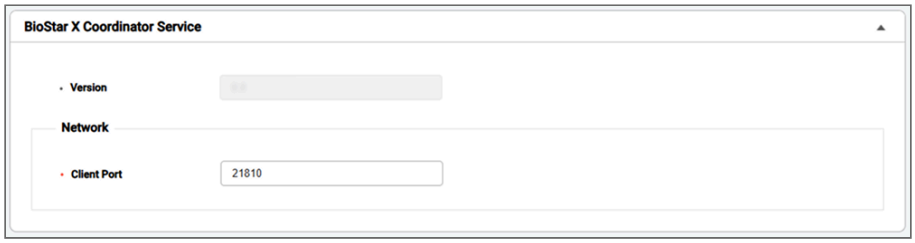
Efficiently process requests to the **BioStar X** server through reverse proxy, improve the security vulnerabilities of iframes, and minimize SSL certificate errors.



- **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.

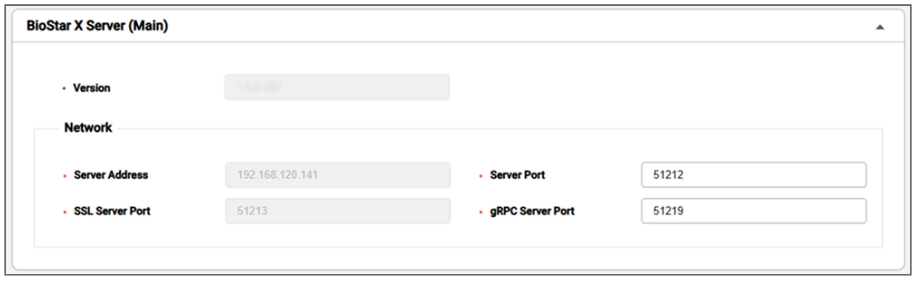


- **Client Port**: Communication port for client connections (default: 21810)

> **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.

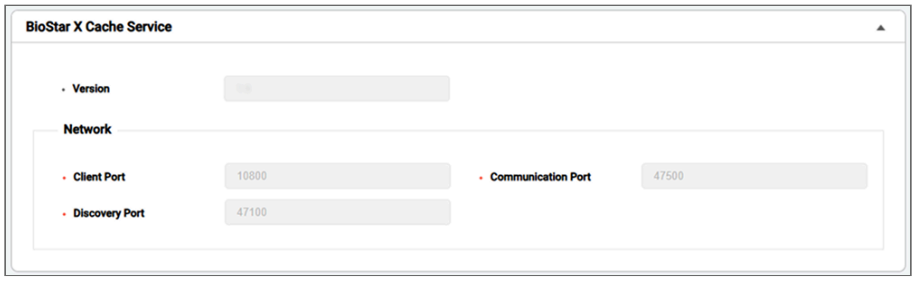


- **Server Address**: IP address of the main server
- **Server Port**: General server communication port (default: 51212)

- **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.



- **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)

Next step

Learn step-by-step how to change the default port (443) of **BioStar X**.

Change the Main Server IP Address

Refer to this document when the server's network environment changes or when you need to change the IP address after initial setup. This guide explains how to safely change the BioStar X main server IP address and reconfigure the connected Multi Communications Server.

> **Info**
> The main server IP address change feature is supported in **BioStar X v1.0.2** and later.

IP address change

First, change the IP address on the server where **BioStar X** is installed. Change the IP address of the network adapter connected to the external network.

> **Info**
> For more information on changing the IP address on Windows, please refer to Microsoft Customer Support.

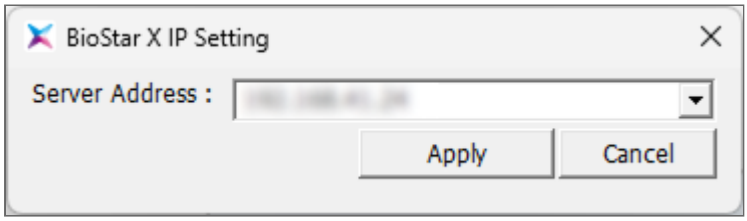
Apply the new IP address

Follow the steps below to change the IP address on the server where **BioStar X** is installed.

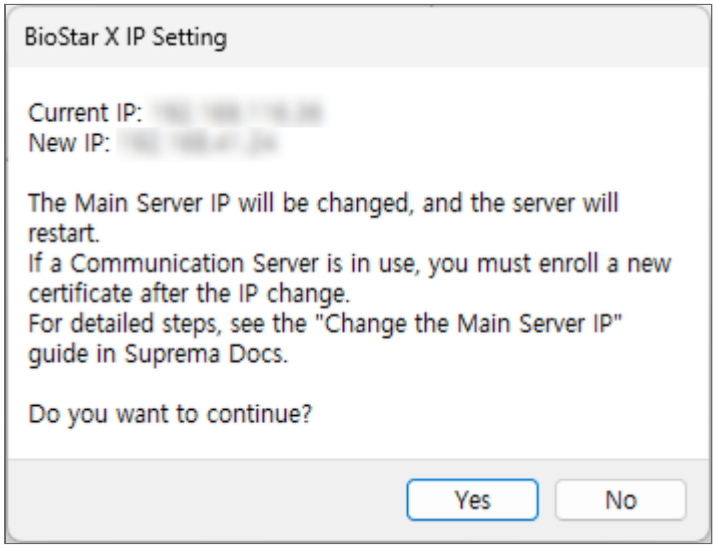
BioStar X IP Setting

Use the **BioStar X IP Setting** tool to change the IP address.

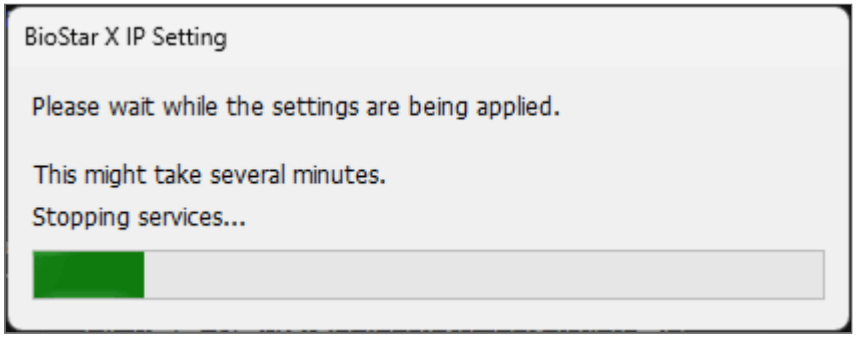
1. In Windows, click Start → **BioStar X** → **BioStar X IP Setting**.
2. When the **BioStar X IP Setting** window appears, select the IP address you want to use from **Server Address**.



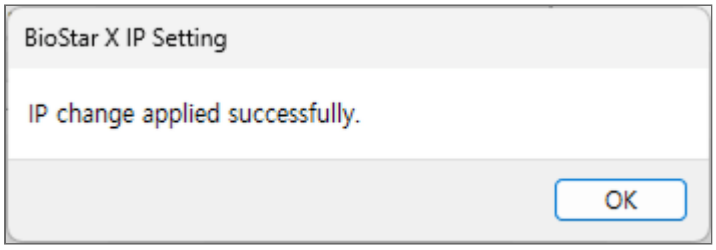
3. Click the **Apply** button.
4. If a message about the IP address change appears, review it and click the **Yes** button.



5. Wait until the IP address change process completes. When the process completes, a success message appears.



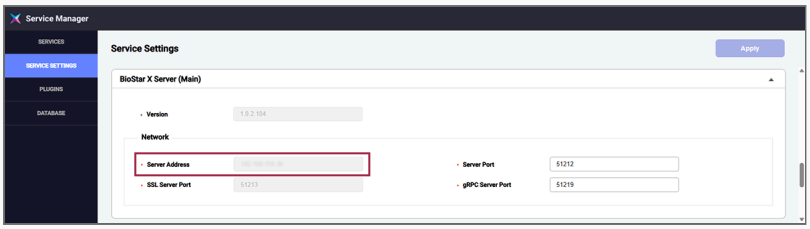
6. If the **IP change applied successfully** message appears, click the **OK** button.



After the IP address change completes, restart all services.

Info

- The IP address cannot be entered manually; select one from the IP addresses listed in **Server Address**.
- You can view the new IP address in **BioStar X Service Manager** → **SERVICE SETTINGS** → **BioStar X Server (Main)** under **Server Address**.



- If a device is registered to BioStar X with the **Device ▸ Server Connection** option, the administrator must manually update that device's server IP to the new IP address.

Modify database server settings

If the database is hosted on the same server as **BioStar X**, stop all services, then edit **BioStar X**'s *system.conf* file. Skip this step if you are using an external database server.

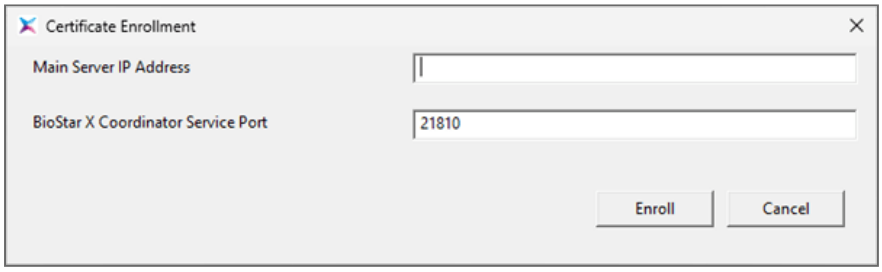
1. Stop all services related to **BioStar X** in Windows Services (service.msc).
2. Navigate to *C:\Program Files\BioStar X Server*.
3. Open the *system.conf* file with a text editor such as Notepad.
4. In the `database` section, change the `server_ip` value to the new IP address.
5. Save and close the *system.conf* file.
6. Restart all services related to **BioStar X** in Windows Services (service.msc).

Open a web browser and verify that you can access the server using the new IP address.

Update Multi Communications Server

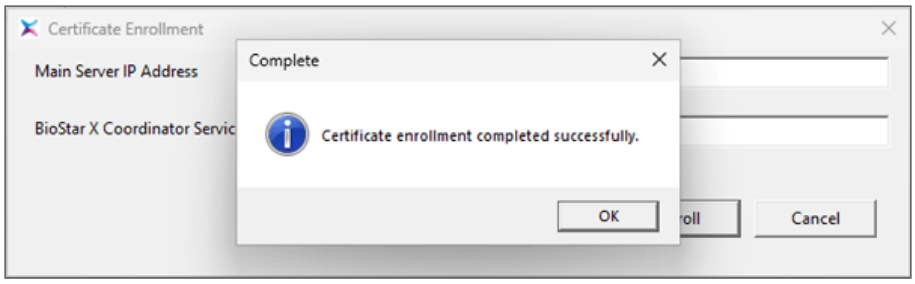
If you installed an additional Multi Communications Server, update its settings to use the main server's new IP address. Run this on the server where you installed the Multi Communications Server.

1. Navigate to *C:\Program Files\BioStar X Communications Server*.
2. Run *biostar-device-cert-enroll.exe*.
3. When the **Certificate Enrollment** window appears, enter the new IP address of the main server in the **Main Server IP Address** field.



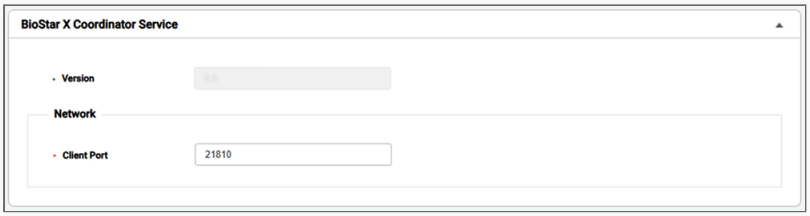
4. If the main server's port number differs from the default (21810), enter the new port number in the **BioStar X Coordinator Service Port** field.
5. Click the **Enroll** button.

After updating the main server's IP address, a success message appears.



Info

- If you didn't install a Multi Communications Server, skip this step.
- If you changed the port number on the main server where BioStar X is installed, run **BioStar X Service Manager** on the main server and check the **Client Port** value under **SERVICE SETTINGS** → **BioStar X Coordinator Service**.

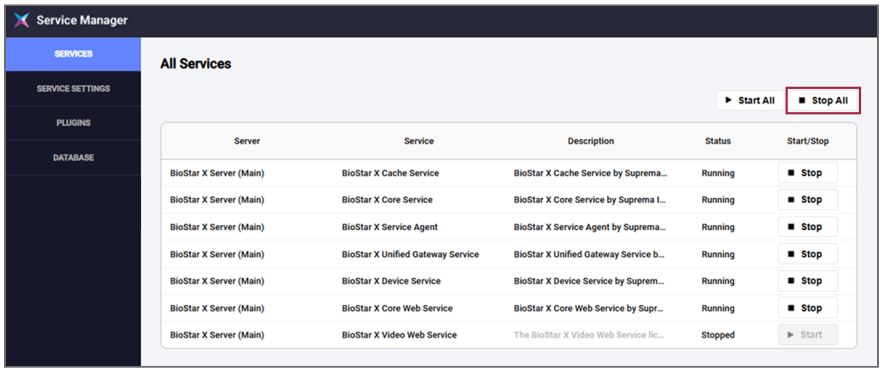


- For more information on installing the Multi Communications Server, see Install Multi Communications Server.

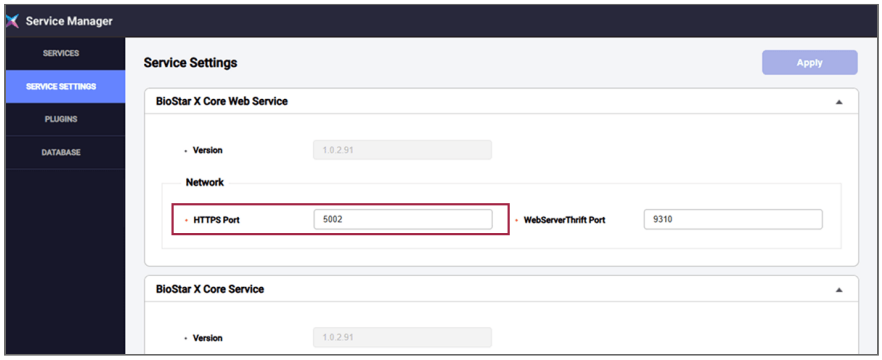
Change the Port

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. To stop all services, click the **Stop All** button in the top right corner of the screen.



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



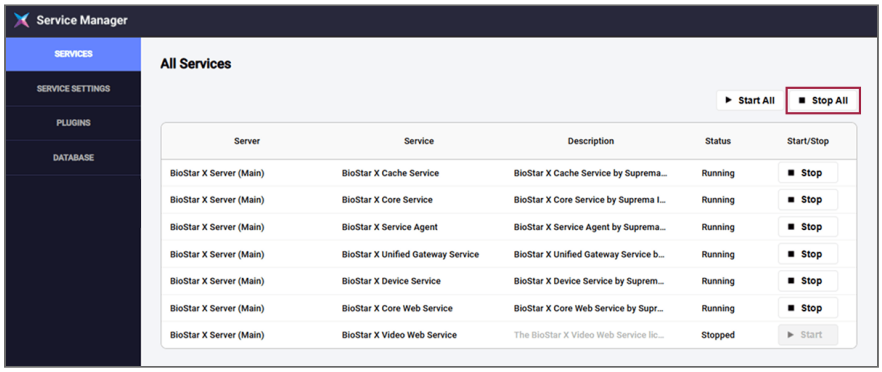
6. Click **Apply** in the upper right corner of the screen.
7. When the confirmation message appears, click **OK**.
8. Navigate to **SERVICES** and click the **Start** button for all services.
9. Access **BioStar X** through your web browser.

> **Info**
>
> - If you changed the port number to 450, enter `https://{ip_address}:450` in the address bar.
> - Support for changing the port may vary depending on certain services.

Change the Database

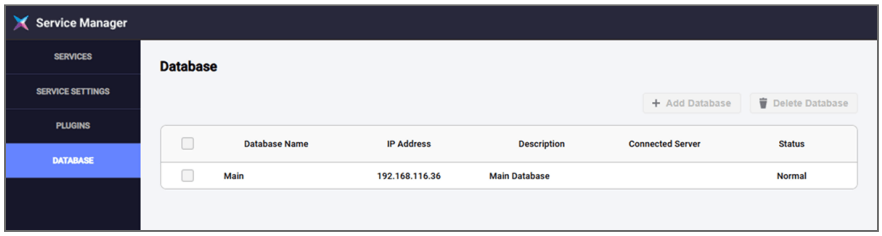
You can change the database settings.

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 the **Stop** button for all services.

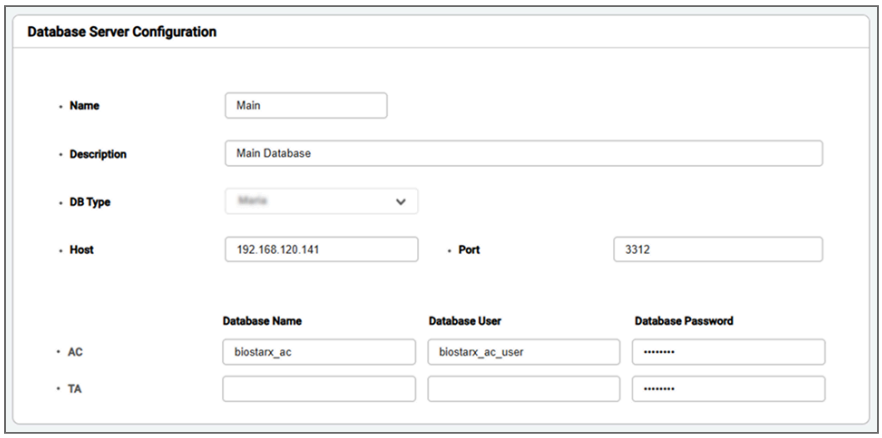


> Click **Stop All** to stop all services at once.

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



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:



- **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 the **Test Connection** button in the upper-right corner to check if the database is connected properly.
8. Click **Save** at the top right of the screen to save settings.

Add Auxiliary Database

When adding a Multi Communications 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 policies, see License Policy.
> - For more information on installing the Multi Communications Server, see Install Multi Communications Server.

Before you 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.

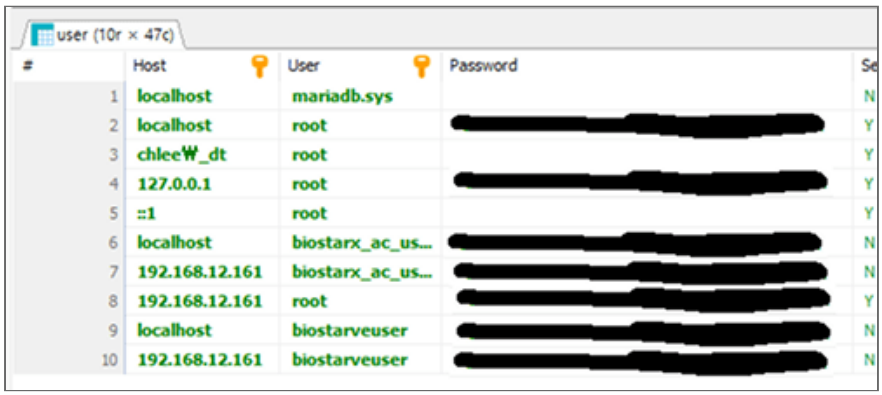
- If you do not use an IP address, `Create user` or `Grant` enrollment may not be possible.
- If you are communicating using a domain or hostname, ensure that user and permissions are registered for localhost.
- If you installed BioStar X using the convenient installation method, the root account is 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;
```



   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.

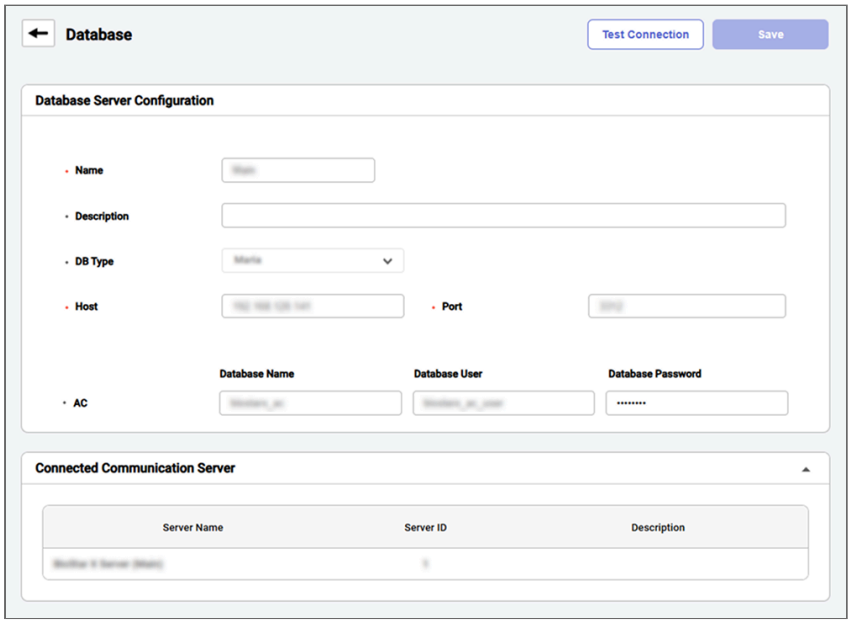
```
select
  concat(
     'CREATE TABLE IF NOT EXISTS <SubDB_AC_Database_Schema>.', table_name,
     ' ENGINE=FEDERATED ',
     'CONNECTION="default/', table_name, '";'
  ) as create_table_sql
from information_schema.TABLES
where TABLE_SCHEMA = '<MainDB_AC_Database_Schema>'
   AND TABLE_TYPE = 'BASE 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 on the left sidebar.
3. Click **+ Add Database** 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 the **Test Connection** button in the upper-right corner to check if the database is connected properly.
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.

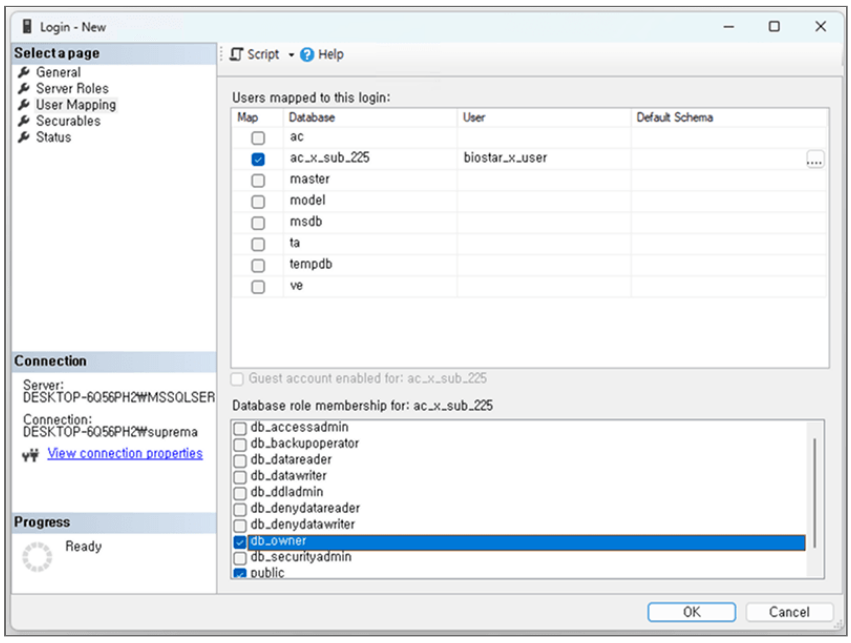
```
GRANT ALTER ANY LINKED SERVER TO [<MAIN DATABASE AC USER>];
GRANT ALTER ANY LOGIN TO [<MAIN DATABASE AC USER>];
```

Example

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



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>];
```

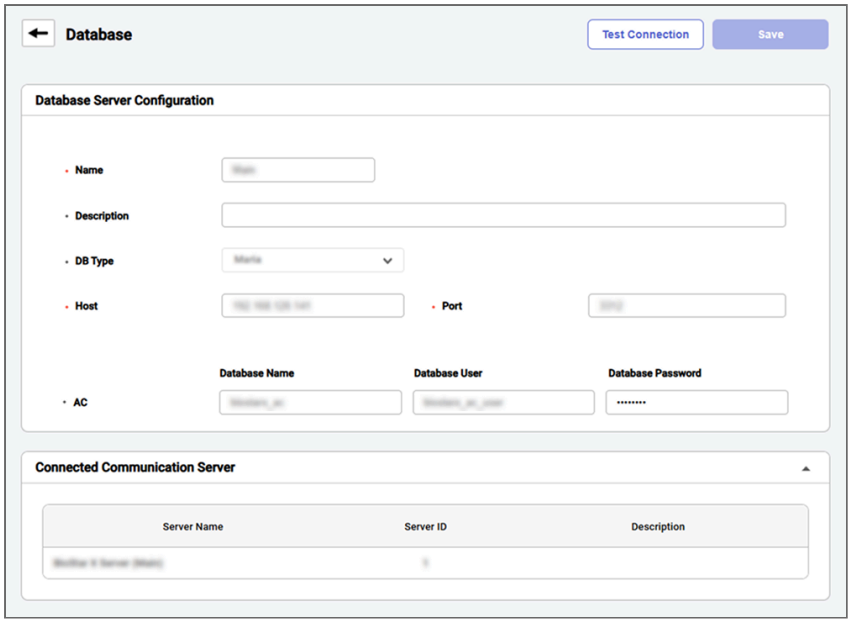
Example

```
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 on the left sidebar.
3. Click **+ Add Database** 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 the **Test Connection** button in the upper-right corner to check if the database is connected properly.
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]'
  AND t.name NOT LIKE 't_lgalmtrstrc[0-9][0-9][0-9][0-9][0-9][0-9]'
ORDER BY t.name;
```

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];
...
```

Uninstall BioStar X Server and Restore Security Certificates

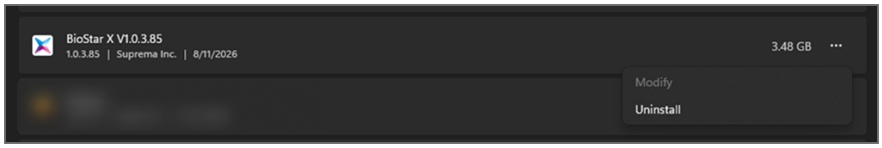
This section explains how to uninstall the **BioStar X** server from a computer. If **Secure communication with device** is not in use, uninstall **BioStar X** without backing up or restoring certificates.

If **Secure communication with device** is in use, back up the server security certificate set (root CA/server certificate/key) before uninstalling **BioStar X**. This backup provides the only way to reconnect existing devices after reinstalling the same server. To reuse only the secure communication certificates and keep the database and settings, see Restore backed-up security certificates. This differs from the system restore feature.

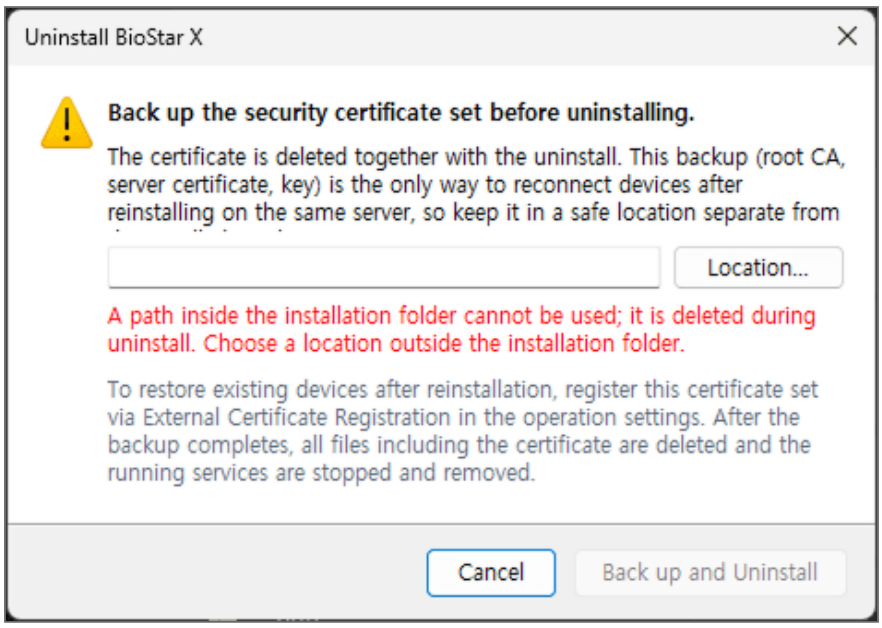
Uninstall the BioStar X server

> **Caution**
> Uninstalling **BioStar X** deletes all installation files, including certificates, and may also delete content (user information). To preserve the database, settings, and keys, back up the system before uninstalling. See System Backup.

1. In Windows, go to **Settings** → **Apps** → **Installed apps**.
2. Find **BioStar X** in the list, click ···, and select **Uninstall**.

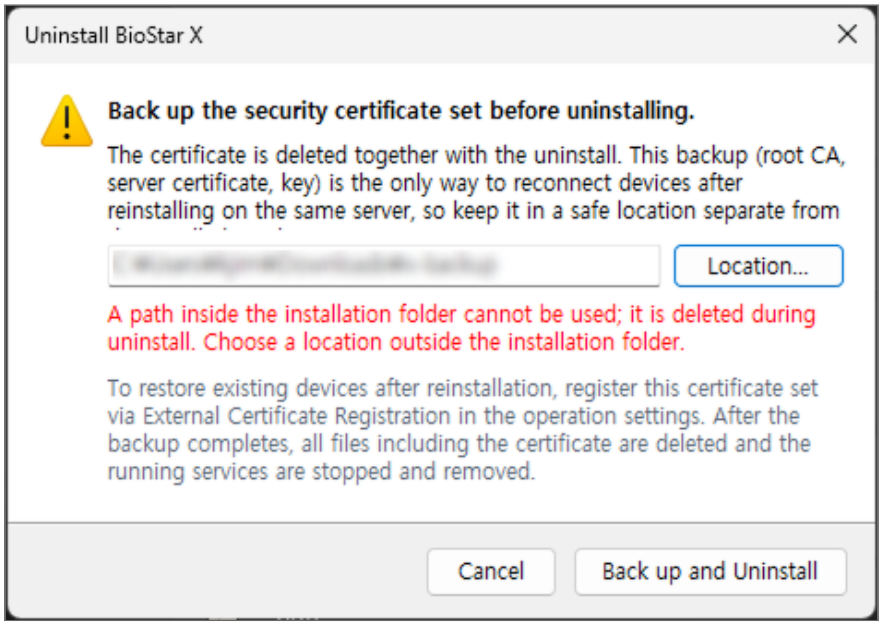


3. If **Secure communication with device** is in use, the certificate backup dialog appears. Click **Location...** and set the backup path. If this option is not in use, continue to step 7 without the certificate backup procedure.

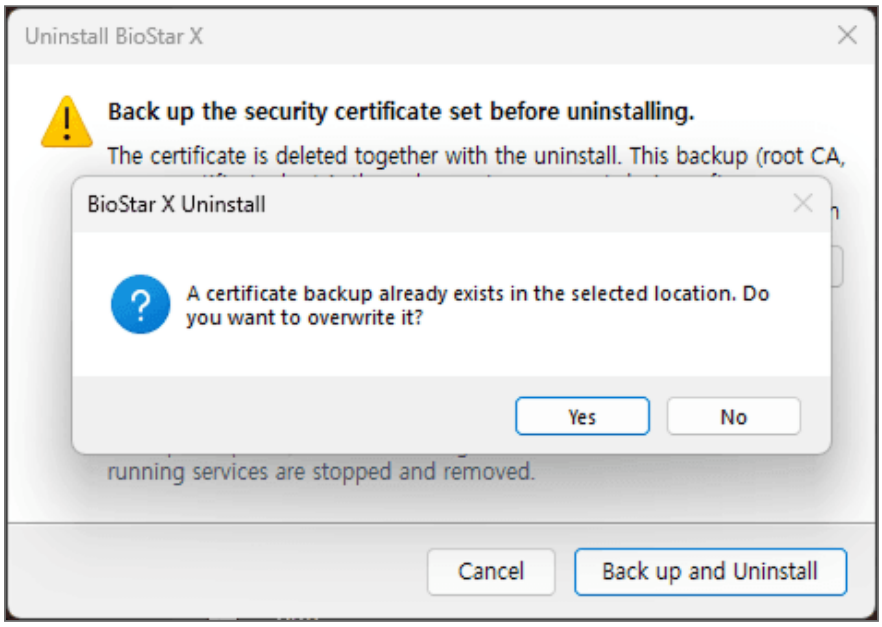


> **Caution**
> Do not use the **BioStar X** installation path as the backup location. Uninstalling **BioStar X** deletes it along with the **BioStar X** installation folder. Select a path other than the **BioStar X** installation path.

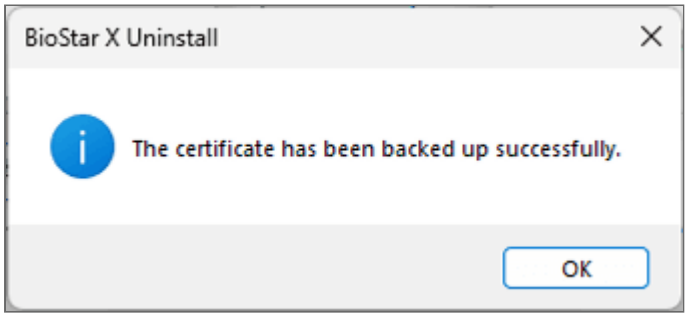
4. After selecting a path and **Back up and uninstall** becomes active, click it.



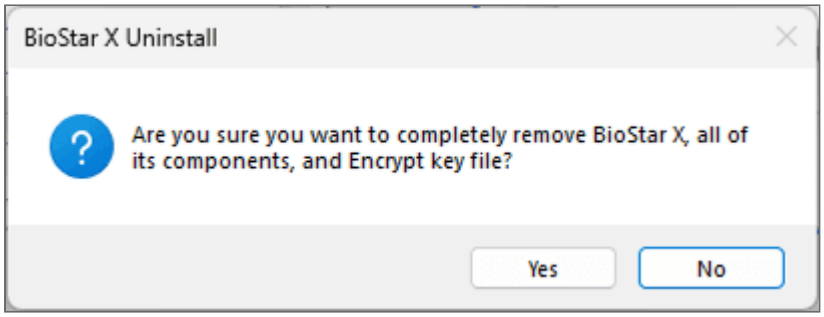
5. If a certificate backup file already exists in the selected location, a dialog asks whether to overwrite it. To overwrite the existing backup, click **Yes**. To select a different path, click **No**.



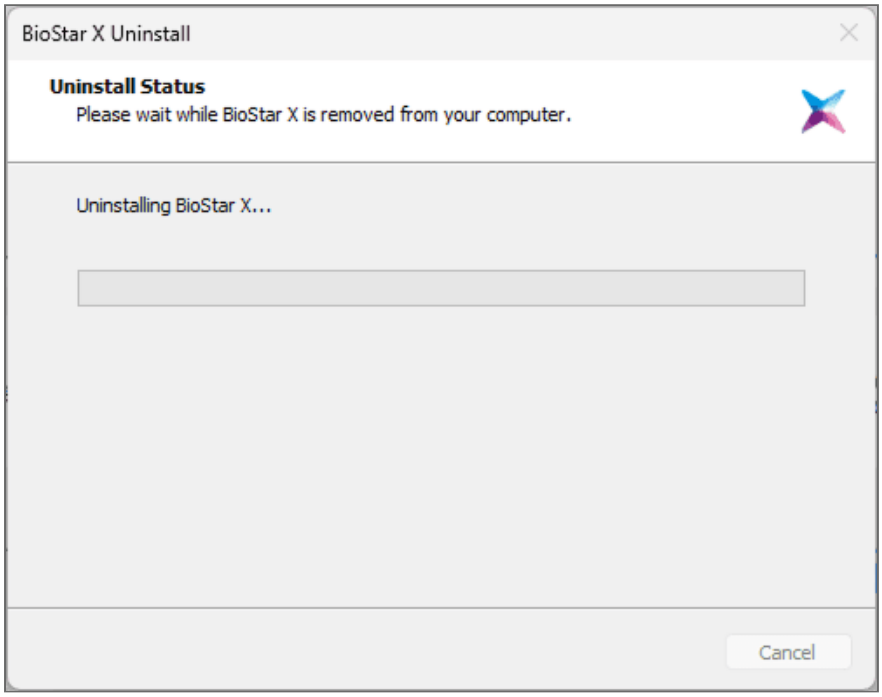
6. When the certificate backup completes, an information dialog appears. Click **OK** to save the settings.



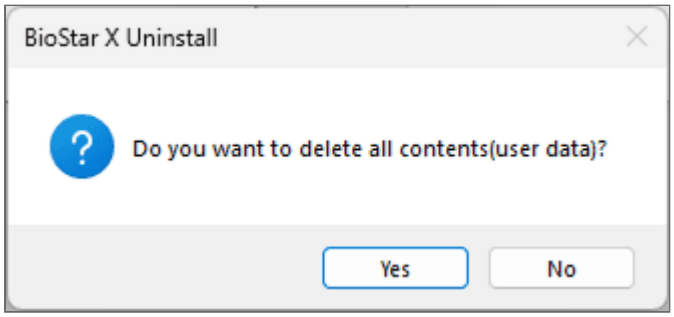
7. When prompted to confirm uninstalling **BioStar X** and all related components, click **Yes**.



8. Wait while uninstallation completes.

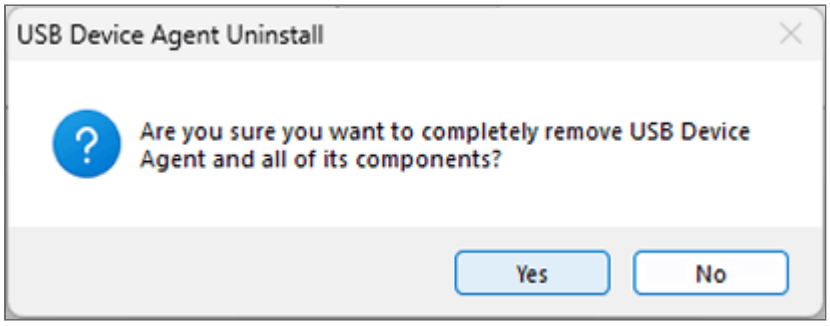


9. A dialog asks whether to delete all content (user information). To delete all data, including user information stored in the database, click **Yes**. To keep the data, click **No**.



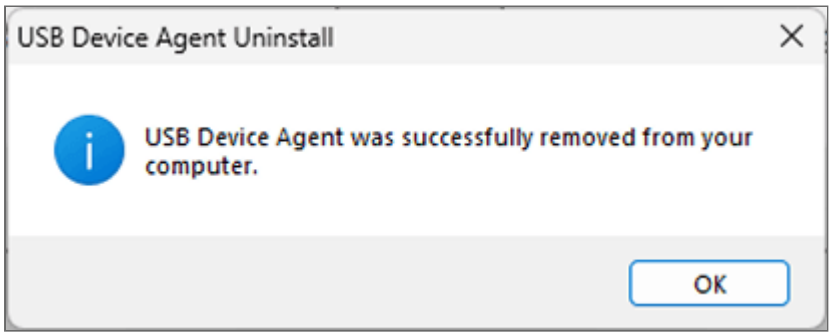
> **Caution**
> Click **Yes** to delete all data, including user information stored in the database. You cannot recover the data. To keep the data, click **No**. Before removing **BioStar X**, back up the system. See System Backup.

10. If **USB Device Agent** is installed, a dialog appears asking whether to remove it as well. Click **Yes**.

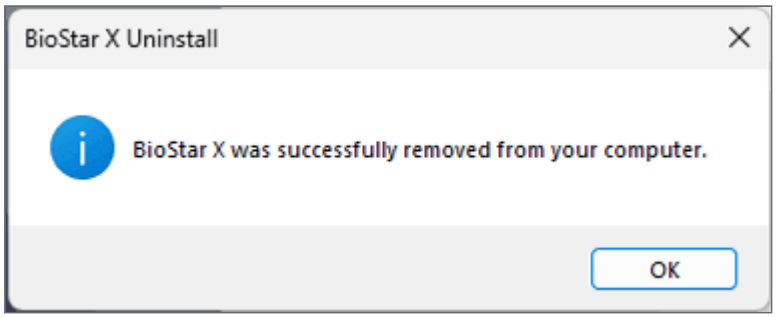


Depending on the components in use, additional uninstall dialogs for related drivers may appear. Follow the instructions on the screen to complete the uninstallation.

11. When component removal completes, a dialog appears. Click **OK** to save the settings.



12. After the system removes **BioStar X**, a dialog appears. Click **OK** to save the settings.



Restore backed-up security certificates

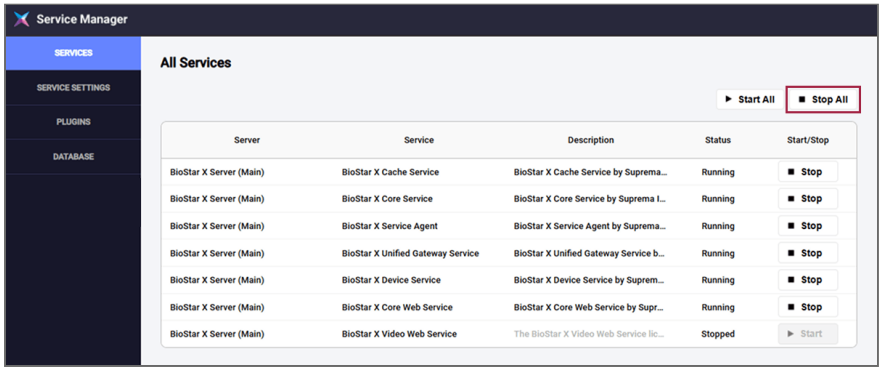
After reinstalling the server that used the **Secure communication with device** option, restore the secure communication certificate. This enables reconnection of existing devices. The System restore tool returns the entire system, including the database and settings, to a previous state. Use this method to reuse only the secure communication certificate without a system restore. Without a dedicated tool, restore the backed-up certificate files directly to the installation path.

Info

In an environment with a main server and a Multi Communication Server, each server uses its own secure communication certificate. After restoring the certificate, install and add the Multi Communication Server. The system copies its certificate automatically, so no separate restore is required.

1. Install **BioStar X** again. For installation instructions, see Express Installation or Custom Installation.
2. After installing **BioStar X**, click Start → **BioStar X** → **BioStar X Service Manager** on Windows.

3. When the **BioStar X Service Manager** window appears in the web browser, click the **SERVICES** menu.
4. To stop all services, click **Stop All** in the top right corner of the screen.



5. Copy all backed-up certificate files (root CA, server certificate, and key) to the *cert* folder under the **BioStar X** installation path.

   > *Example: C:\Program Files\BioStar X\cert*

   > The file names match the certificates created during the new installation. When a prompt asks to overwrite files, click **Yes** to replace the existing files.

6. In **SERVICES**, click **Start All** to restart all services.
7. If you use the Multi Communication Server, install it in a separate environment. For installation instructions, see Install Multi Communications Server.
8. In **BioStar X Service Manager** on the main server, add the Multi Communication Server. For instructions on adding the Multi Communications Server, see Install Multi Communications Server.

When you add the Multi Communications Server, the system copies the security certificate files from the main server *cert* folder. It copies them to the Multi Communications Server automatically.

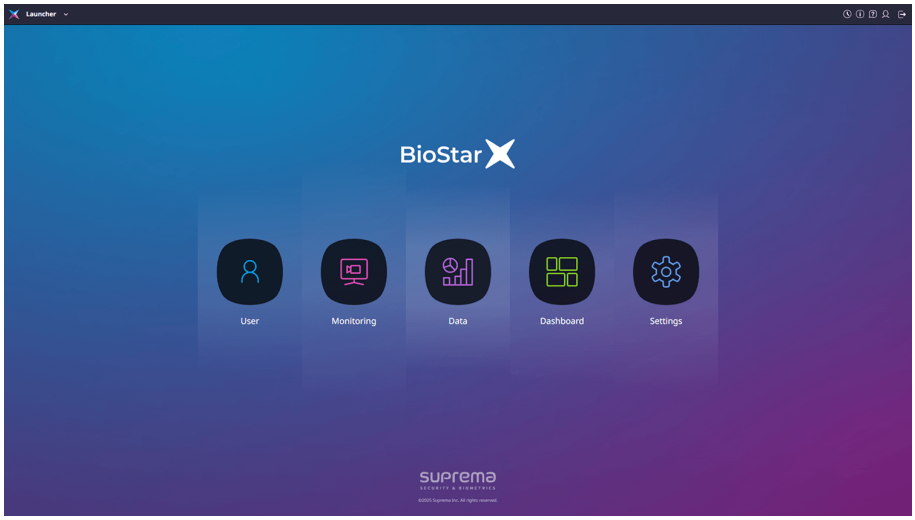
> **Caution**
>
> If you added the Multi Communications Server before restoring the certificate (steps 4~6), it already has the old certificate. In this case, replace the Multi Communications Server certificate separately. Follow the procedure below.
>
> 1. On the server where the Multi Communications Server is installed, run **BioStar X Service Manager** and stop all services.
> 2. Copy the backed-up certificate files to the *cert* folder under the Multi Communications Server installation path.
>
>   > *Example: C:\Program Files\BioStar X Communications Server\cert*
>
> 3. On both the main server and the Multi Communications Server, restart all services in **BioStar X Service Manager**.

Info

- For more information on using **BioStar X Service Manager**, see Start and Stop Server.
- For more information about the **Secure communication with device** option, see Enhance System Security.
- A Multi Communications Server license is required to install and connect the server. For more information on licensing policies, see License Policy.

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, see User.
- **Monitoring**: Monitor doors, devices, video, and events in various ways. Control related features and monitor through real-time video. For more information, see Monitoring.
- **Data**: Query user information or events based on desired criteria, and generate reports on a set schedule. For more information, see Data.
- **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, see Dashboard.
- **Settings**: Configure **BioStar X** optimized for user environments through various settings for devices, access control, user permissions, language, and time. For more information, see Settings.

Info

- For more information on the header area at the top of the screen, see Learn Common UI.
- 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, see Plugin.
  - For more information on the licensing policy, see License Policy.

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

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.

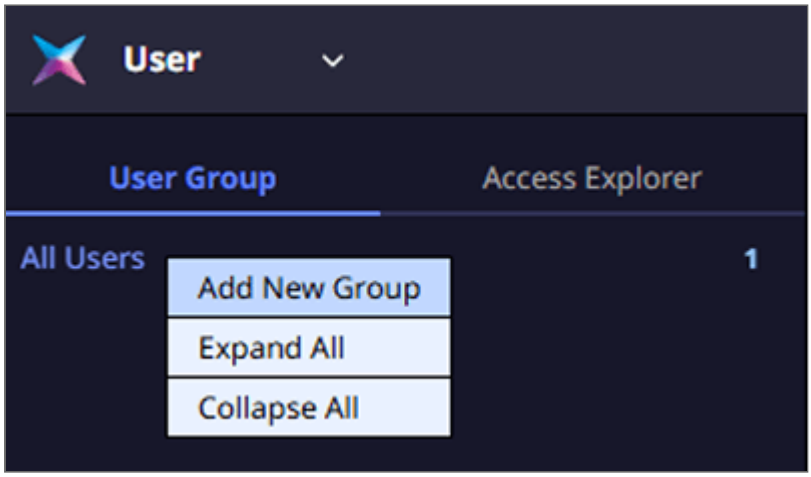
Add group

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

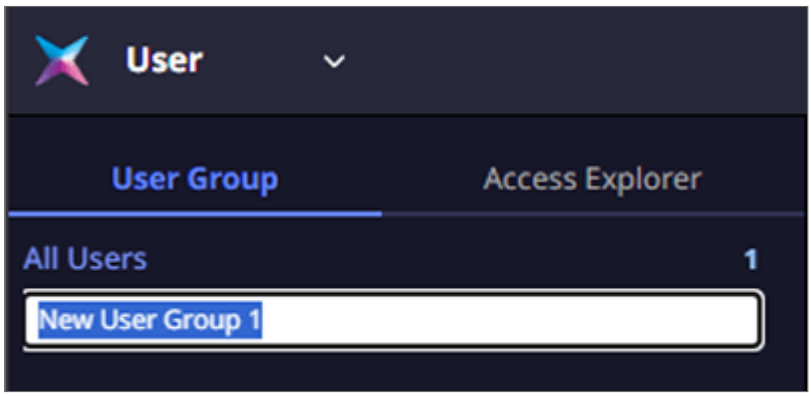
> **Info**
>
> - Registering the group name as the name of the organization or department that the user belongs to makes management easier.
> - You can create sub-groups of the group sequentially up to 8 levels.
> - The user group name can be up to 48 characters long.
> - If you select a group from the 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. On the left sidebar of the screen, select **All Users** from the **User Group** tab and right-click.

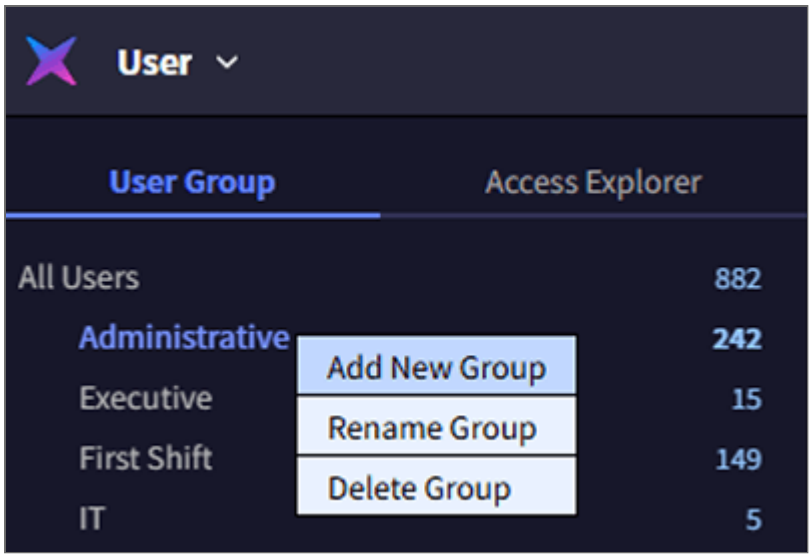


3. Click **Add New Group** in the popup menu.
4. When the group is created, enter your desired group name.



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.

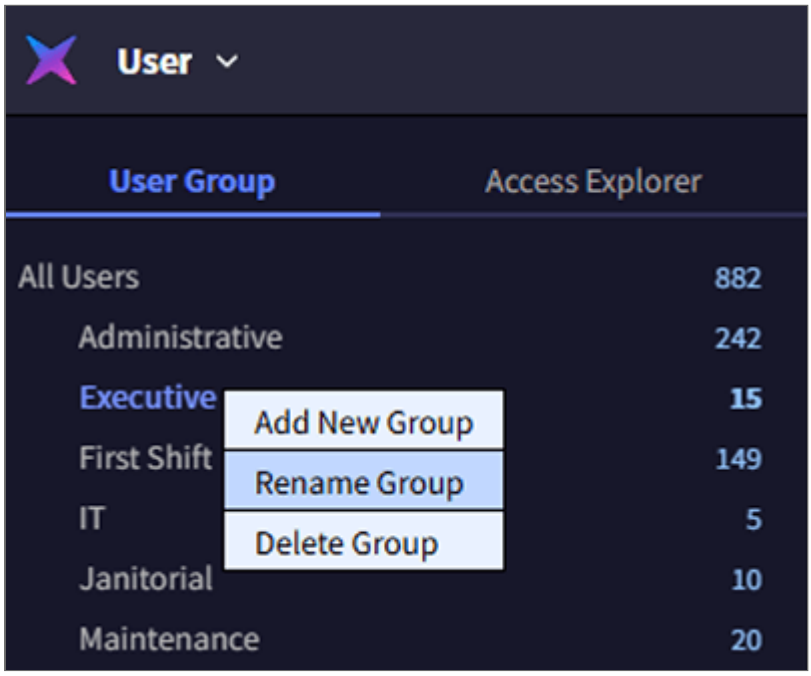
Info

- 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

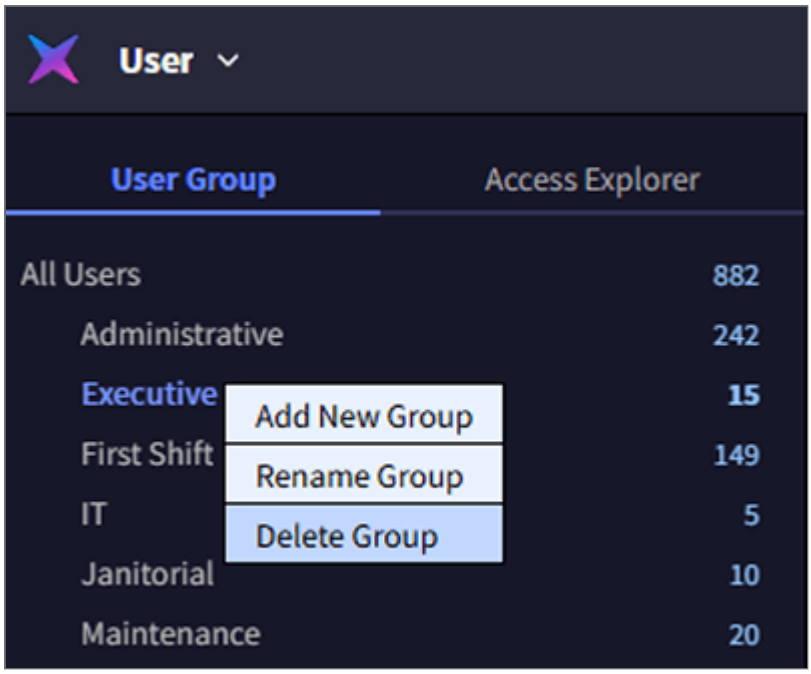
The user group name can be up to 48 characters long.

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.

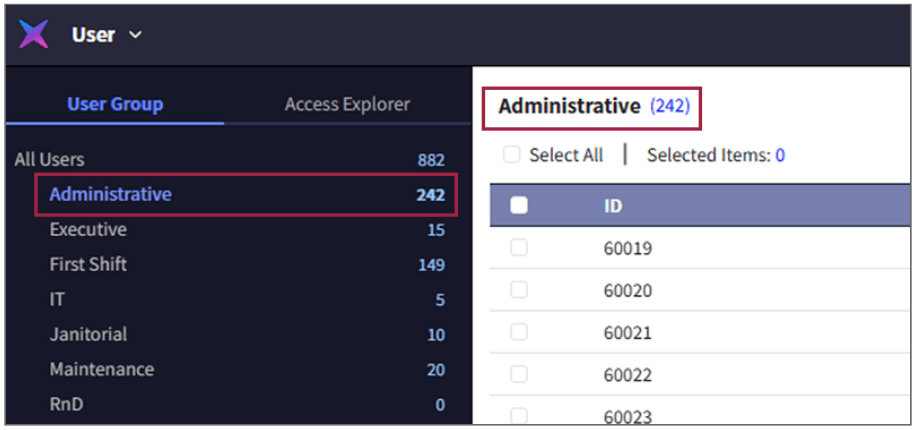


4. When the confirm message appears, click the **Yes** button.

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

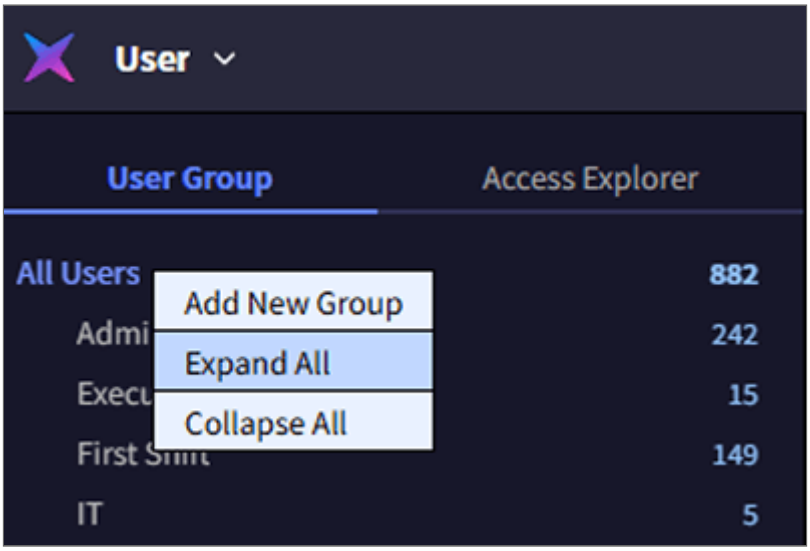
View users by group

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.

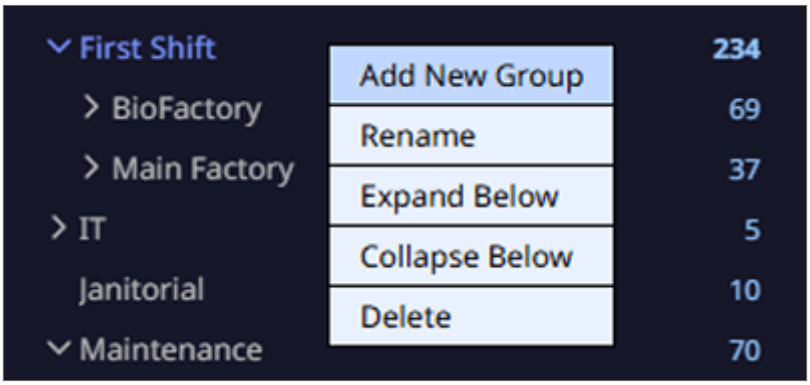


Expand/collapse group list

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



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



Register Users

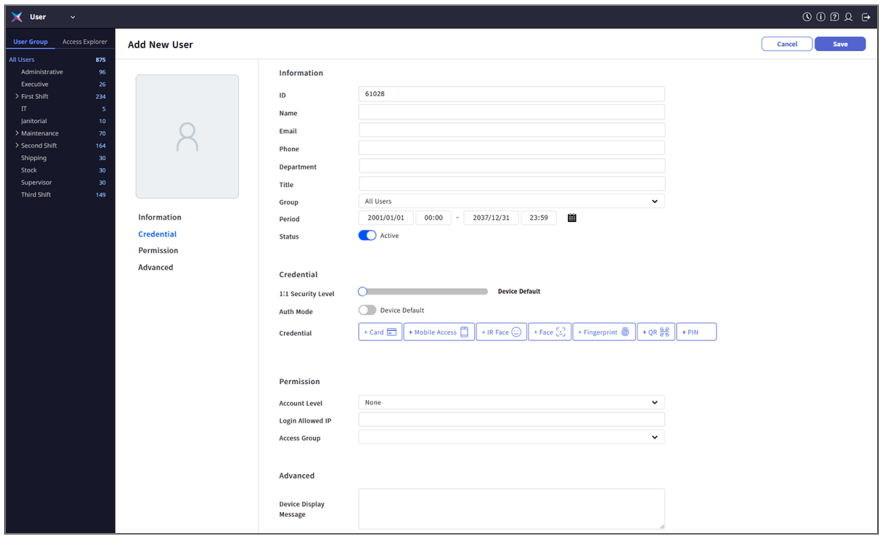
Guidelines for registering new users. You can enter information such as the user's photo, name, email, and phone number, and set the user's access permissions and biometric information.

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.



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



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.

Enter the user's basic information in the **Information** section. You can check the detailed information for each field.
Enroll the user credentials and set access authentication method in the **Credential** section.
Check how to set the user's access permissions in the **Permission** section.
In the **Advanced** section, you can set the message to display on the device when the user accesses it or exclude that user from synchronization when linking with Directory Service.
Register or edit a user by scanning a passport.

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, see Card Printer.
- Click **Cancel** at the top right of the screen to cancel user registration.

Enter Basic User Information

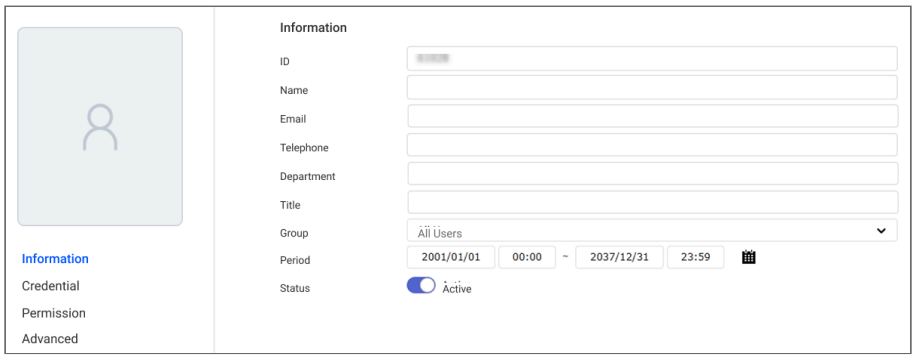
This section describes how to enter basic user information. The entered user information is used for search and management. Managing user information clearly helps comply with the organization's security and privacy policies.

- 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.

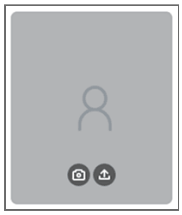
Go to the **Launcher** → **User** page. You can enter user information in the two ways below.

- **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.



- **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, see Enroll Face.

- **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 on adding and managing user groups, see Manage User Groups.

- **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.

User ID and name entry rules

- Spaces cannot be included with the value of **ID**.
- **ID** can include a period (`.`), but it cannot consist of only one period (`.`) or two periods (`..`).
- The username can be up to 48 characters, including special characters.

  > *Special characters:* `~` `!` `@` `#` `$` `%` `^` `&` `(` `)` `-` `_` `=` `+` `[` `]` `{` `}` `;` `.` `'`
- User IDs and names cannot include the following characters. `₩` `/` `:` `*` `?` `"` `<` `>` `|` `` ` ``
- User IDs also cannot include an apostrophe (`'`).
- A user name cannot start with `&@~` consecutively at the beginning. However, a user name may start with `&` , `@` , or `~` alone.

Info

- The available values for **ID** vary by the **User ID Type** option in the **Settings** → **System** → **Server** menu. For more information, see Server Detailed Settings.
  - **Number**: Enter a number from 1 to 4294967294.
  - **Alphanumeric**: Enter a combination of letters and numbers.
- 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 adding **Custom User Field**, see Server Detailed Settings.

Next step

Enroll the user credentials and set access authentication method in the **Credential** section.
Check how to set the user's access permissions in the **Permission** section.
In the **Advanced** section, you can set the message to display on the device when the user accesses it or exclude that user from synchronization when linking with Directory Service.
Check how to edit user information.

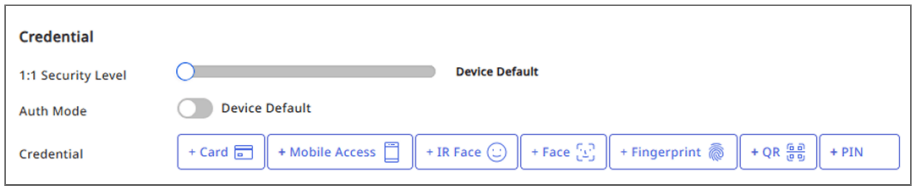
Enroll User's Credential

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.



Enroll credentials and set the appropriate security level in the **1:1 Security Level** field. 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 Airfob portal to be used. For more information on integrating with the Airfob portal and using mobile access cards, see Manage Mobile Access Cards.

Enroll credentials

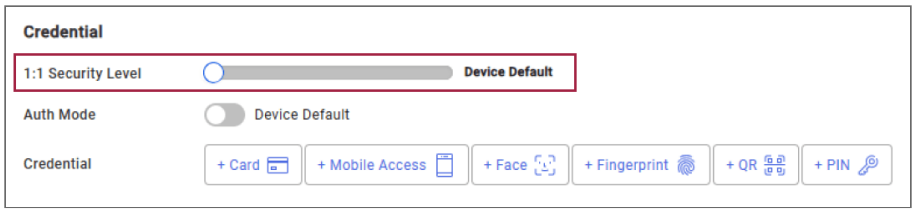
The method to enroll user credentials is as follows. Credentials can be enrolled in various forms such as fingerprints, faces, cards, and passwords.

Next step

Check how to set the user's access permissions in the **Permission** section.
In the **Advanced** section, you can set the message to display on the device when the user accesses it or exclude that user from synchronization when linking with Directory Service.
Check how to edit user information.

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.



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.

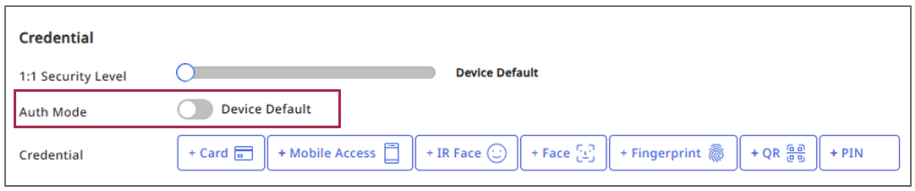
> **Info**
>
> - If you set **Private Auth Mode** in the **Credential** section to **Biometrics**, you cannot apply the 1:1 security level as the input user cannot be identified, and you can only apply the 1:1 security level when a card or ID that allows user identification is set in the authentication mode. For more information on **Private Auth Mode**, see Authentication Mode Settings.
> - 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.

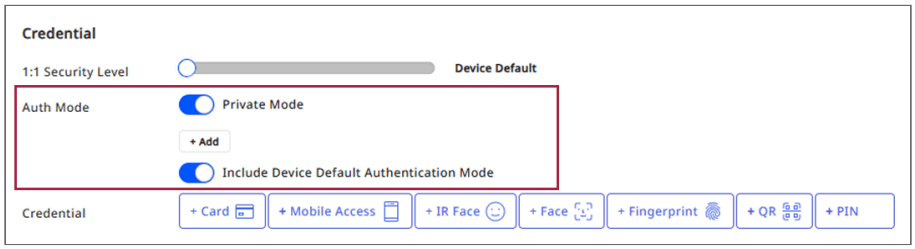
Device defaults

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



Private authentication mode

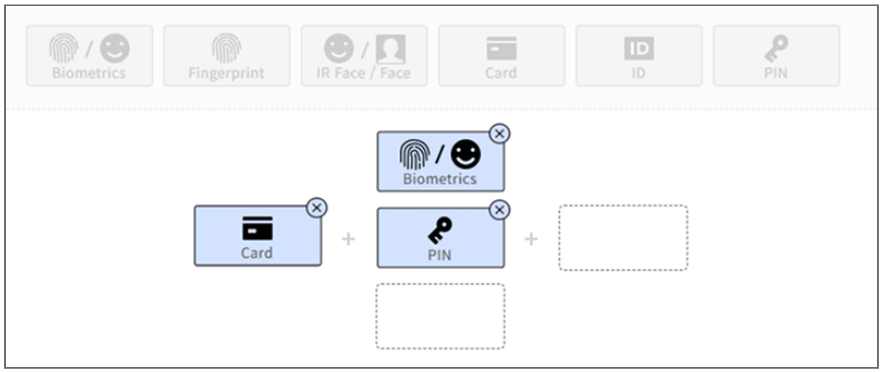
Setting the **Auth Mode** option to **Private Mode** enables different authentication methods for each user.



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



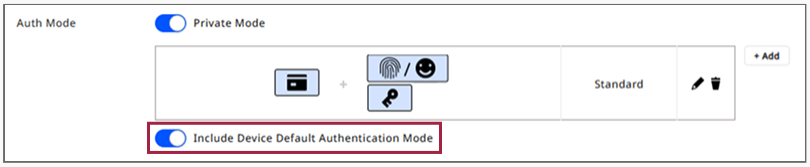
- **Extended Auth Mode**: Set whether to use the extended authentication mode. The extended authentication mode allows for a combination of facial and fingerprint authentication methods.
- **Auth Mode**: Set the authentication methods using drag and drop.



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

Info

- The **Extended Auth Mode** option is supported on the BioStation 3 Max, BioEntry W3, BioStation 3, and FaceStation F2 models.
- 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**.



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

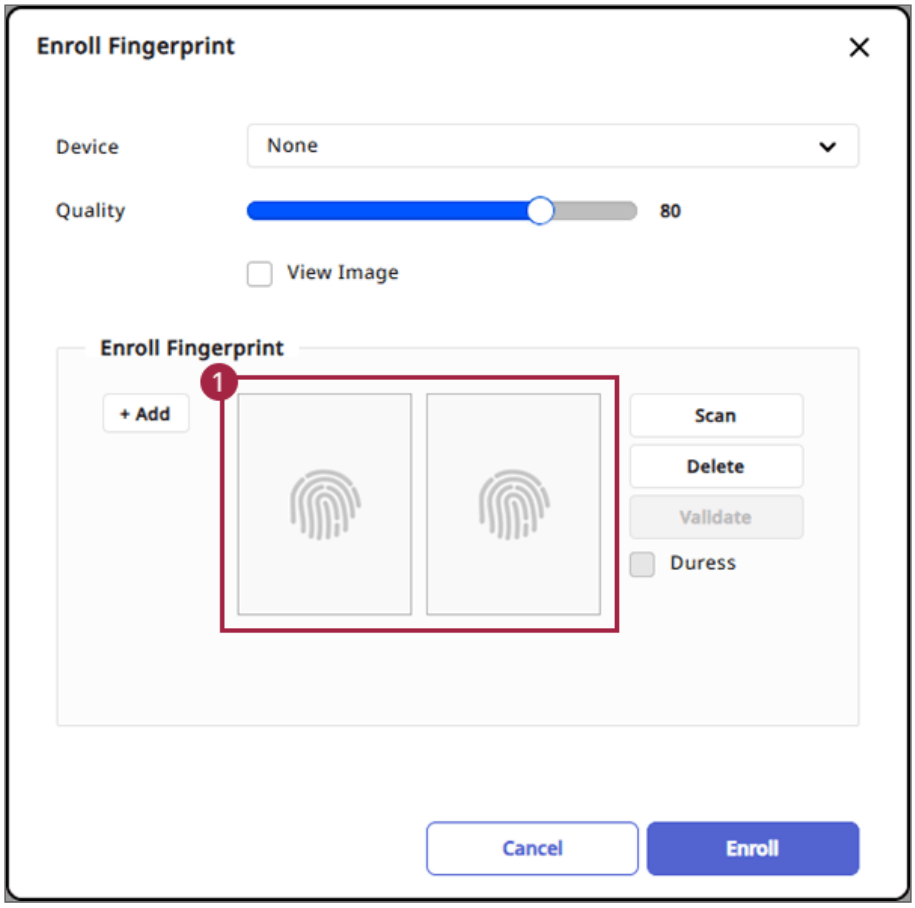
Enroll Fingerprint

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.



- **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 IR Face

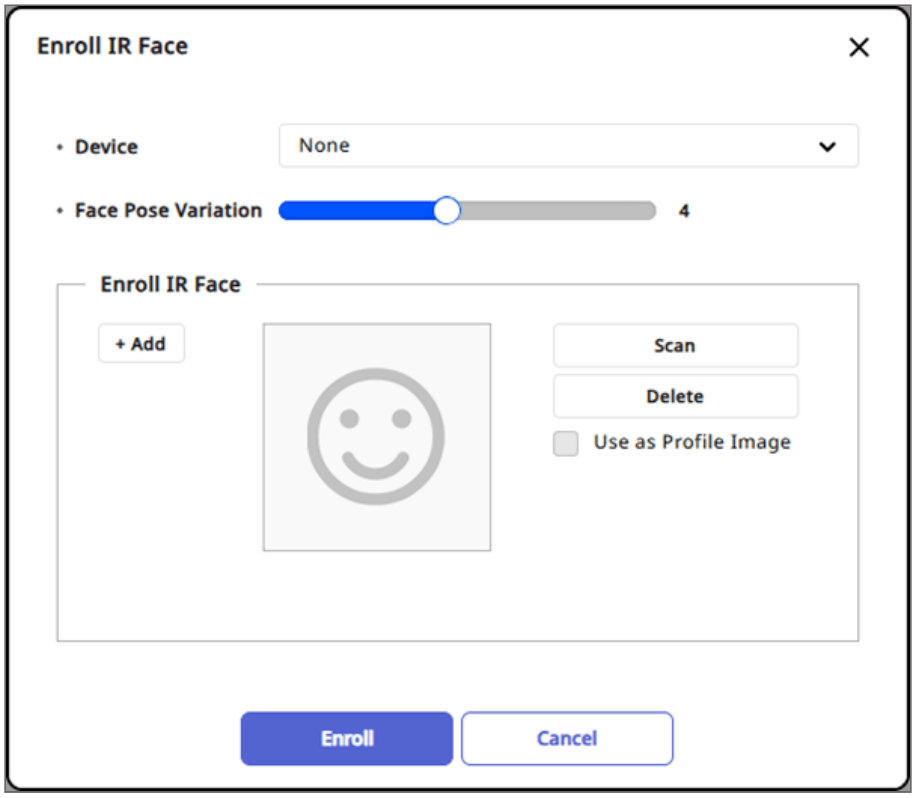
You can enroll the user's face as a means of authentication for access control. IR face enrollment is an authentication method that captures the user's face using an infrared camera.

Precautions when enrolling IR face

- Keep the distance between the device and your face at 60-100 cm 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.

Enroll by device

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



- **Device**: Select the device for enrolling the IR face.
- **Face Pose Variation**: Set sensitivity to the face's position, angle, and distance when enrolling the IR face. Set it high to obtain a precise IR face template.
- **+ Add**: Click to enroll the IR face. Add up to five IR faces.
- **Scan**: Click the added **Nth** button to scan the IR face. Follow the on-screen instructions to scan the face.



- **Use as Profile Image**: Check this option to use the enrolled IR face image as the profile image.
- **Delete**: Delete the IR face credential. Select the number to delete and click the button.

Info

- Devices that can enroll IR face are as follows:
  - FaceStation 2
  - FaceLite
- If the face authentication rate is low, delete face information and enroll a new face.

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

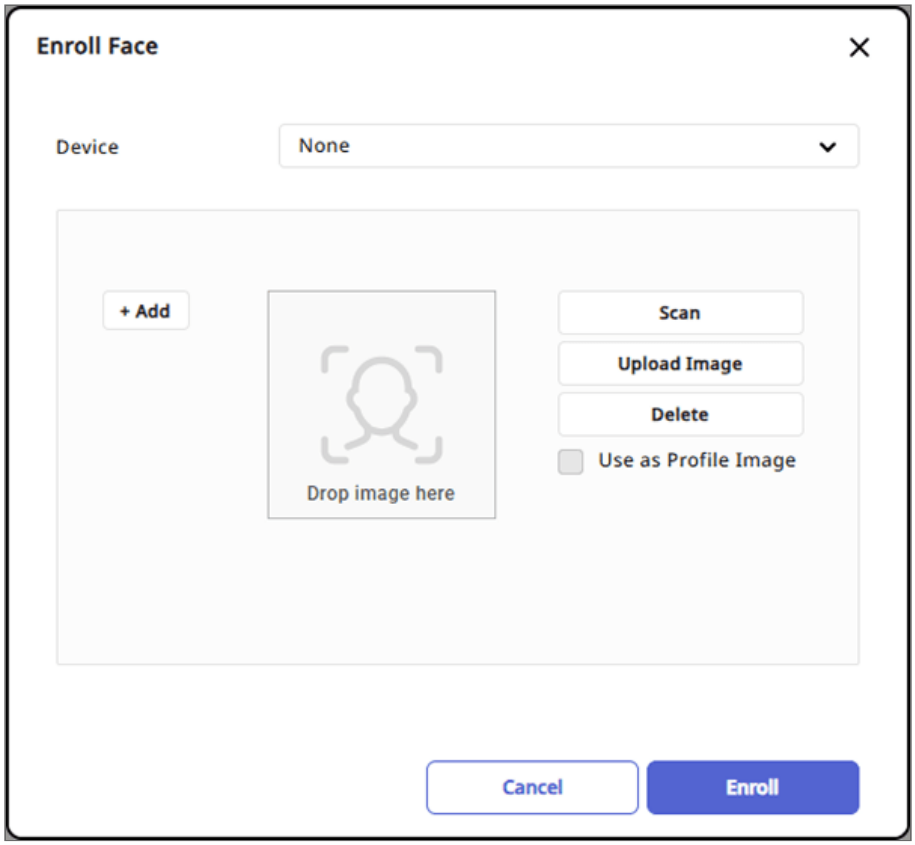
- Keep the distance between the device and your face at 60-100 cm when enrolling your face.
- Do not change your face expression.
- Do not wear masks, hats, or eye patches.
- Do not enroll a face wearing a mask. It may increase the False Acceptance Rate (FAR) if both faces with and without a mask are 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

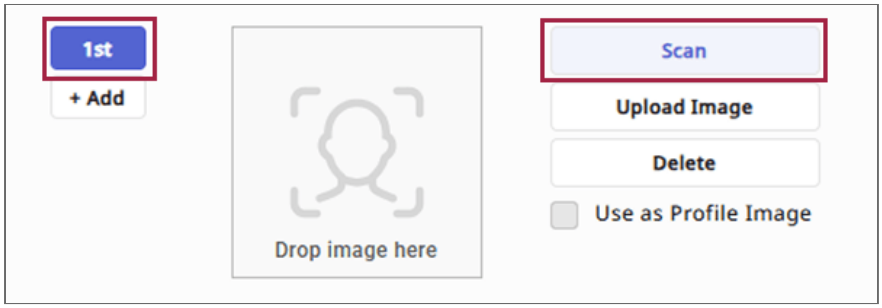
You can use the import from CSV feature or enroll multiple users' faces at once, or send an email link to multiple users for them to enroll their faces directly on a mobile device. For more information, see Batch Enroll Faces.

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**: Select this option to use the enrolled face image as the profile image.
- **Delete**: You can delete the face credential. Select the number to delete and click the button.

Info

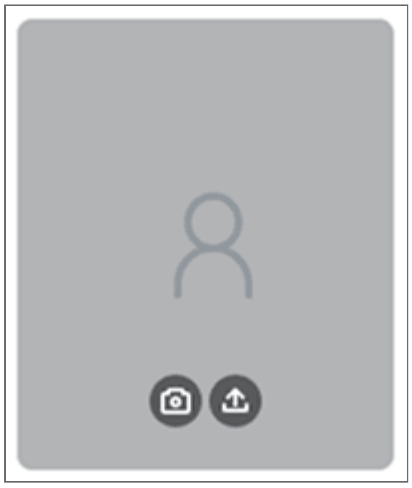
- Devices that can enroll faces are as follows:
  - BioStation 3 Max
  - BioEntry W3
  - BioStation 3
  - FaceStation F2
- If the face authentication rate is low, delete face information and enroll a new face.

Enroll with a webcam or photo

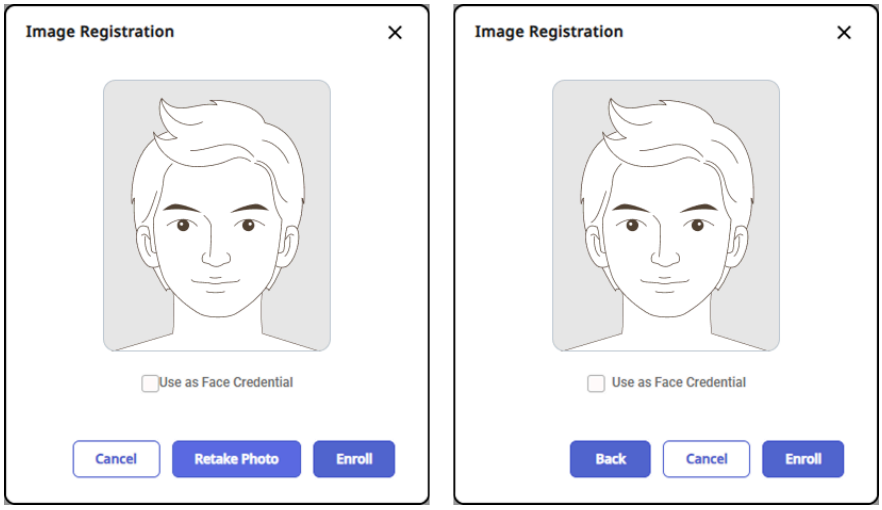
You can take a photo with a webcam connected to your PC, set the captured photo as a user profile picture, and enroll the face as a credential. Or you can enroll the uploaded photo as a face credential.

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

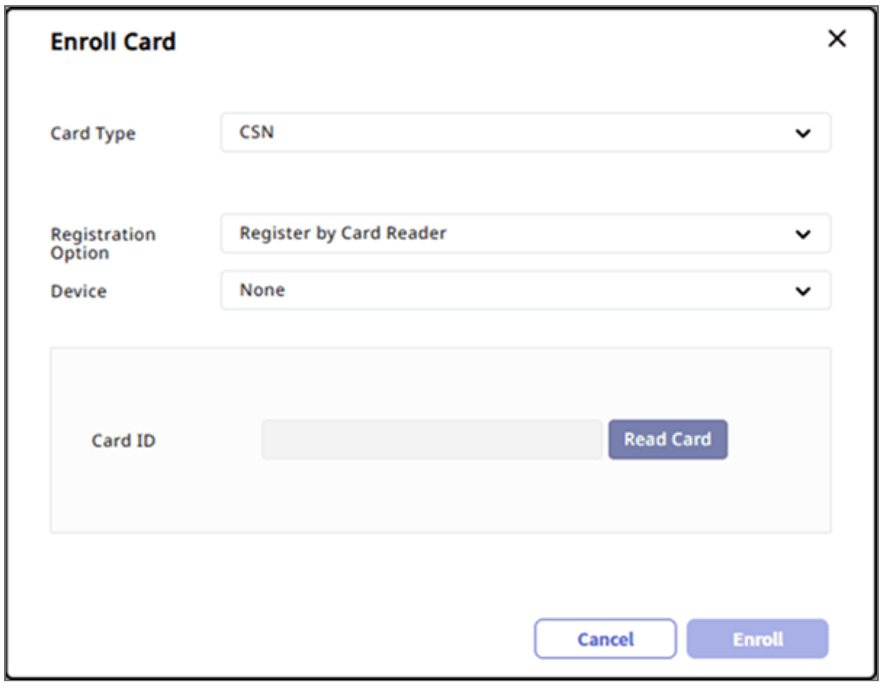
Guide users on how to enroll access cards. Explain the enrollment methods for CSN cards, Wiegand cards, and smart cards, as well as the card reading/formatting features. Refer to the manual of the device for the types of cards supported by the device.

Card enrollment using a USB agent

Card Type	CSN	Wiegand	Smart Card
EM	✕	✕	✕
MIFARE	✓	✕	✓
DESFire	✓	✕	✓
FeliCa	✓	✕	✕
HID Prox	✕	✕	✕
HID iCLASS	✕	✕	✕

CSN card

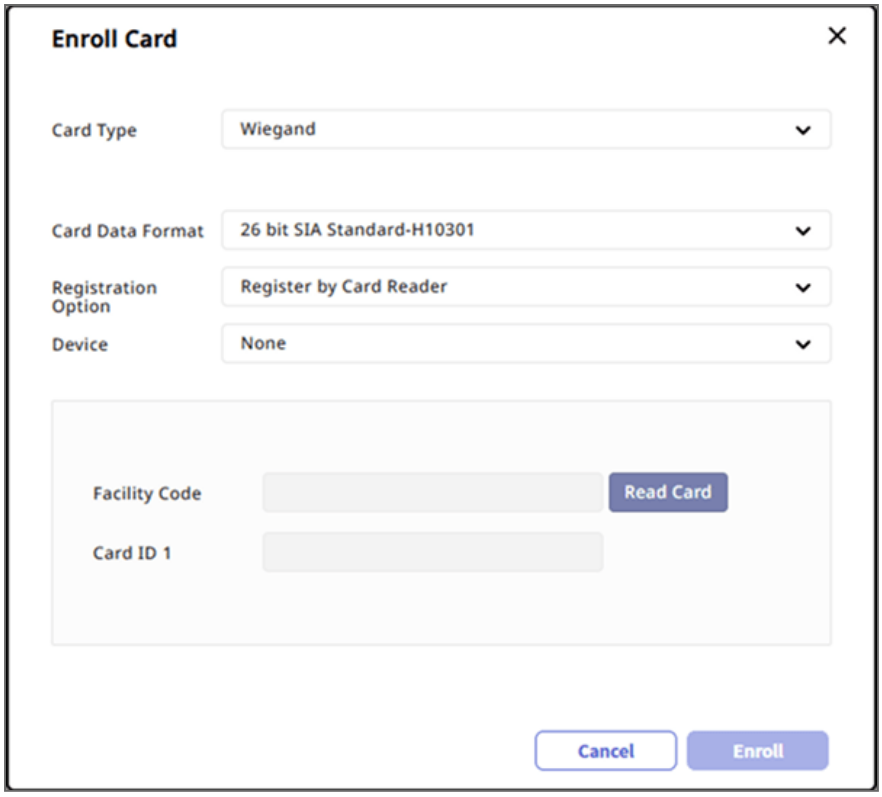
1. In the **Credential** section, click the **+ Card** button.
2. When the **Enroll Card** window appears, select **CSN** from the **Card Type** options.



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.



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 isn't available in the **Card Data Format** options, see Set Wiegand Card Format.

Smart card

Enroll an access-on card, secure credential card, or custom smart card.

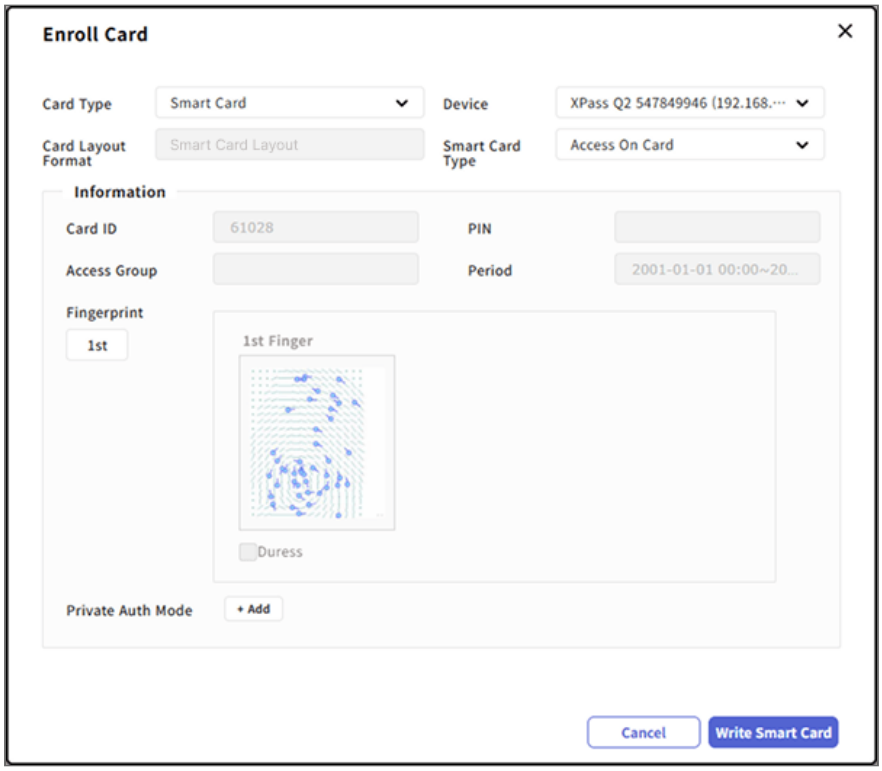
Info

- To issue a smart card, the correct card type must be set. For more information on card formats, see Set Smart Card Format.
- The user information stored on the smart card uses information stored in **BioStar X**. Failure to store updated user information may result in incorrect information being stored on the smart card. Additionally, if the updated user information is not synchronized with the device, the device may fail to perform authentication.
- To 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 on card layout, see Set Smart Card Format.
- See Authentication Settings to set up the smart card layout on the device.
- See Read/format card to format the smart card and rewrite its data.

Access On Card

Select **Access On Card** to store user information on the card. This includes card ID, PIN, access group, period, fingerprint template, face template, and personal authentication mode.

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



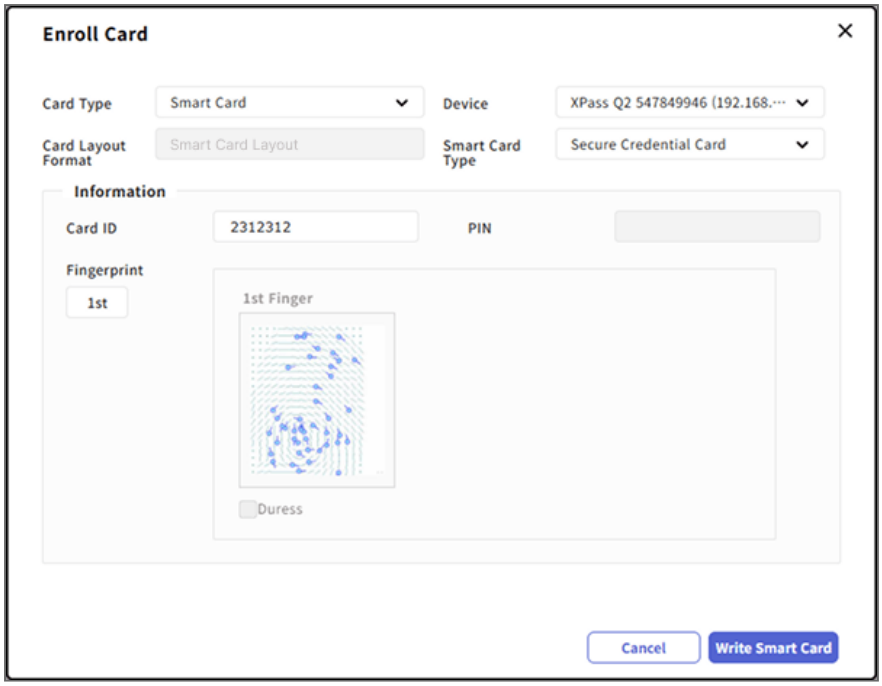
6. Select a fingerprint template if available. If no template is available, skip this step.
7. Click the **Write Smart Card** button.

> **Info**
> Access On Card cannot set the card ID manually.

Secure Credential Card

Select **Secure Credential Card** to store user information on the card. This includes card ID, PIN, fingerprint template, and face template.

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



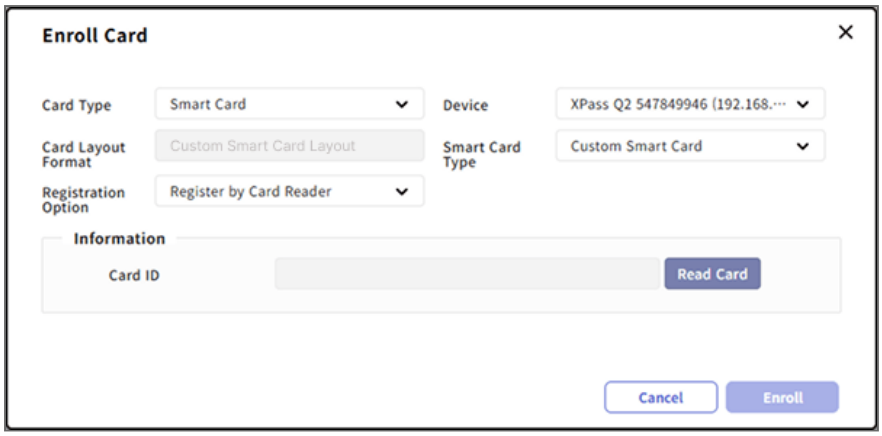
6. Directly enter **Card ID**.
7. Select a fingerprint or face template if available. If no template is available, skip this step.
8. Click the **Write Smart Card** button.

Custom Smart Card

Select **Custom Smart Card** to enroll a third-party 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.
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 **Custom Smart Card** from the **Smart Card Type** options.



6. 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 in base-10 (decimal) format.
7. Click the **Enroll** button.

Info

For devices and firmware versions supporting Custom Smart Card, refer to the list below.

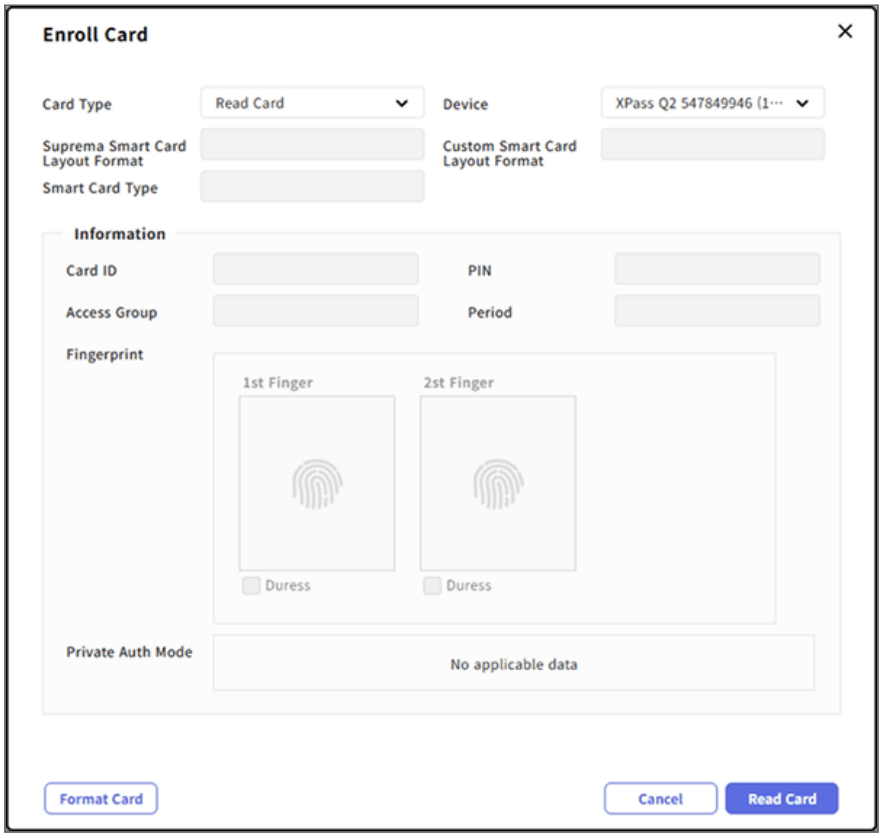
▼ View devices and firmware versions that support custom smart cards

- BioStation 3 Max firmware 1.0.0 or later
- XPass Q2 firmware 1.0.0 or later
- BioEntry W3 firmware version 1.0.0 or higher
- BioStation 2a firmware version 1.1.0 or higher
- BioStation 3 firmware version 1.3.0 or higher
- X-Station 2 firmware version 1.3.0 or higher
- BioLite N2 firmware version 1.6.2 or higher
- 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

Read/format card

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.

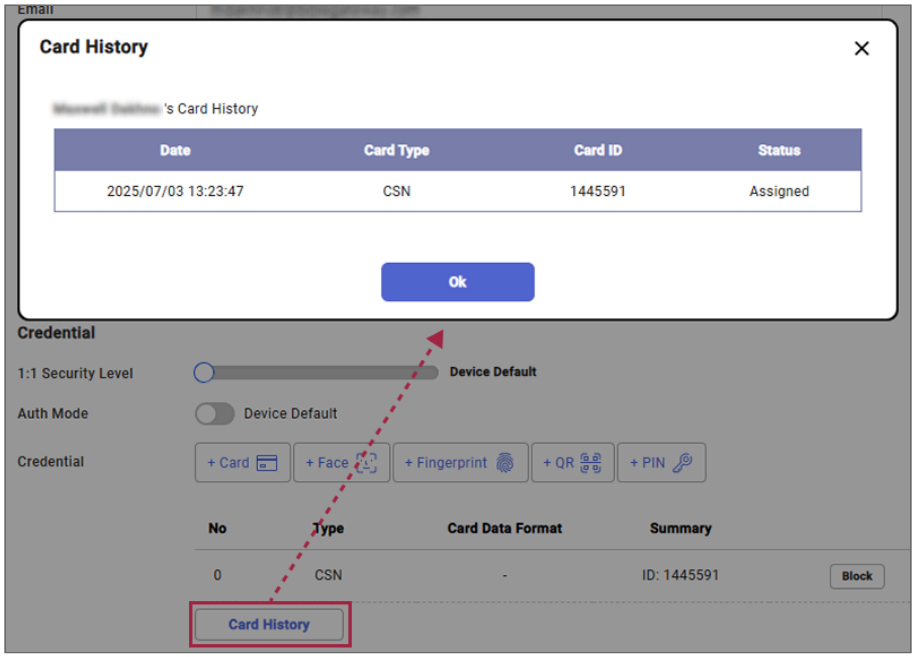


3. Select the device capable of reading smart cards from the **Device** field.
4. Select the **Smart Card Type**.
5. Click the **Read Card** button.
6. Verify the card information and click the **Format Card** button.

> **Info**
>
> - The device list in the **Device** field is shown only when the smart card layout has been configured. For more information on this setting, see Authentication Settings.
> - 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.



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 Airfob portal.

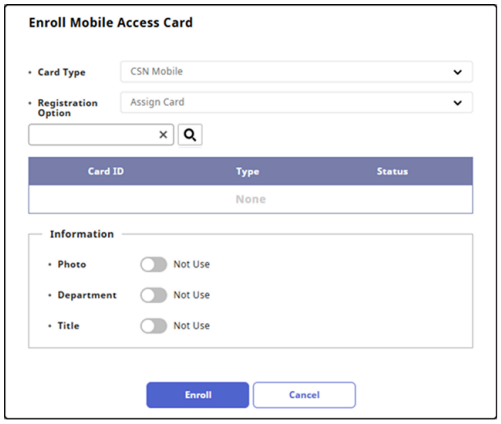
> **Info**
>
> - Only one of the **CSN Mobile Card** or the **Template on Mobile** can be used.
> - This feature can only be used when linked with the Airfob portal. For more information on integrating with the Airfob portal and using mobile access cards, see Manage Mobile Access Cards.

CSN mobile

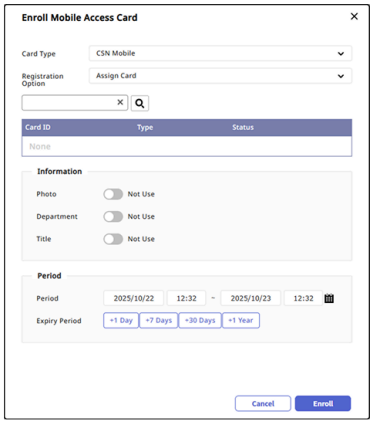
You can issue CSN mobile access cards to users.

Card assignment

1. Click **Mobile Access** 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**.



Airfob portal site: Regular



Airfob portal site: Dynamic

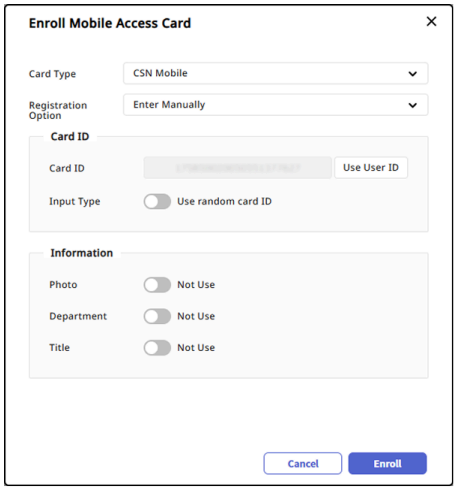
> The **Period** item is activated when setting a **Dynamic** site upon site creation in the Airfob portal. You can set the expiration duration and usage period for the mobile access cards. For more information about the Airfob Portal, refer to the following link.

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.

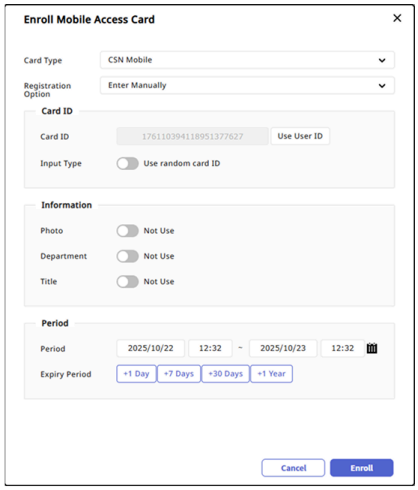
> **Info**
>
> - If you have enabled the **Photo**, **Department**, and **Title** options in the **Info** section, that information can be displayed on the user's mobile access card. The items displayed at this time are based on the information entered by the user. For more information on entering basic user information, see Enter Basic User Information.
> - The system restricts issuance if the user name contains special characters incompatible with the Mobile Access Card. Only `@` `-` `_` `+` `[` `]` `,` `.` are allowed.
> - If the user name includes a single quote(`'`), a notice appears. The system sends the value without the quote when saving the user. When this notice appears, the system already created the card record. Canceling the notice stops only the transfer to the Airpop portal, and the card remains unusable. In this case, the system saves the remaining user information without linking the unusable card to the user.

Enter manually

1. Click **Mobile Access** 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.



Airfob portal site: Regular



Airfob portal site: Dynamic

> The **Period** item is activated when setting a **Dynamic** site upon site creation in the Airfob 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. Use this only when the user ID is numeric.
   - **Enter manually**: Allows manual entry of the card ID.
5. Set the **Info** and **Period**.
6. Click the **Enroll** button.

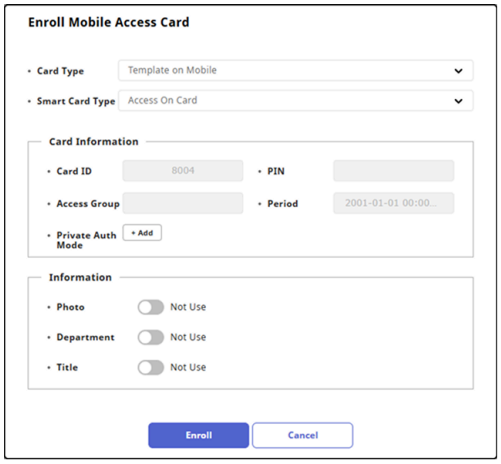
> **Info**
>
> - If you have enabled the **Photo**, **Department**, and **Title** options in the **Info** section, that information can be displayed on the user's mobile access card. The items displayed at this time are based on the information entered by the user. For more information on entering basic user information, see Enter Basic User Information.
> - The system restricts issuance if the user name contains special characters incompatible with the Mobile Access Card. Only `@` `-` `_` `+` `[` `]` `,` `.` are allowed.
> - If the user name includes a single quote(`'`), a notice appears. The system sends the value without the quote when saving the user. When this notice appears, the system already created the card record. Canceling the notice stops only the transfer to the Airpop portal, and the card remains unusable. In this case, the system saves the remaining user information without linking the unusable card to the user.
> - 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

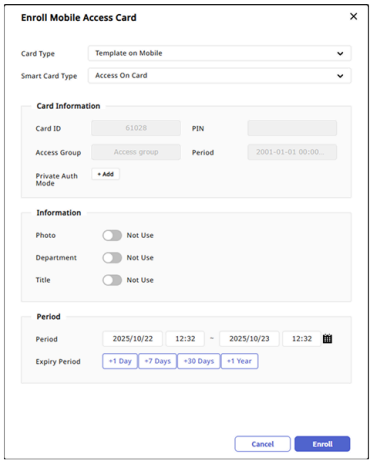
Template on Mobile is a mobile access card that stores the user's biometric template on a mobile device. It can authenticate biometrically without storing user data on the **BioStar X** server or the Airfob portal and device.

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



Airfob portal site: Regular



Airfob portal site: Dynamic

> The **Period** item is activated when setting a **Dynamic** site upon site creation in the Airfob 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 basic user information, see Enter Basic User Information.
- The system restricts issuance if the user name contains special characters incompatible with the Mobile Access Card. Only `@` `-` `_` `+` `[` `]` `,` `.` are allowed.
- If the user name includes a single quote(`'`), a notice appears. The system sends the value without the quote when saving the user. When this notice appears, the system already created the card record. Canceling the notice stops only the transfer to the Airpop portal, and the card remains unusable. In this case, the system saves the remaining user information without linking the unusable card to the user.
- For devices and firmware versions that support **Template on Mobile**, refer to the list below.
  - BioStation 3 Max firmware 1.0.0 or later
  - BioEntry W3 firmware version 1.0.0 or higher
  - BioStation 3 firmware version 1.2.0 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

- The devices that can use QR/Barcode authentication through scanner are as follows.
  - X-Station 2 (XS2-QDPB, XS2-QAPB)
- The devices that can use QR/Barcode authentication through camera are as follows.
  - BioStation 3 Max firmware 1.0.0 or later
  - XPass Q2 firmware 1.0.0 or later
  - BioStation 3 firmware version 1.1.0 or later
  - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) firmware version 1.2.0 or higher
  - X-Station 2 (XS2-QDPB, XS2-QAPB) firmware version 1.4.1 or higher
- A separate device license is required to use QR/Barcode authentication with a camera. For more information, see Device License.

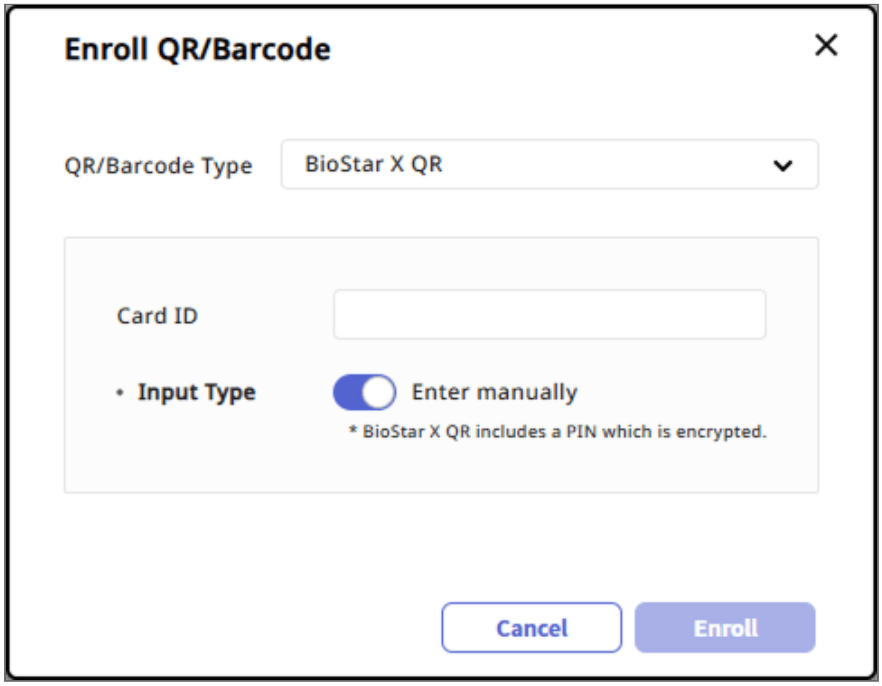
BioStar X QR

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, see Email Setting.
- To issue **BioStar QR**, you must register an email address in the user information. For more information, see Enter Basic User Information.

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.

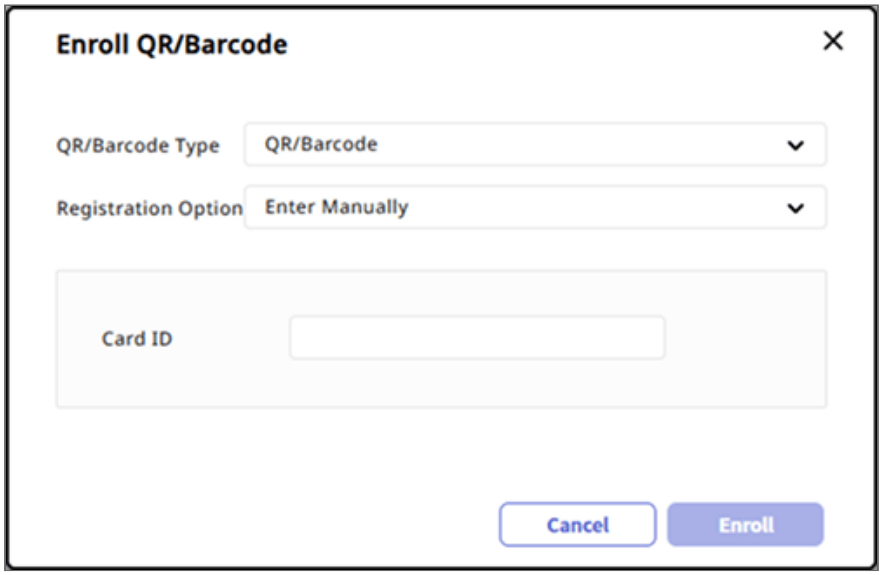
Info

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.



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.



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 4~16 digits long and contain only 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 on the CSV import feature, see Export/Import User Information.

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 **Launcher** → **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.



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.

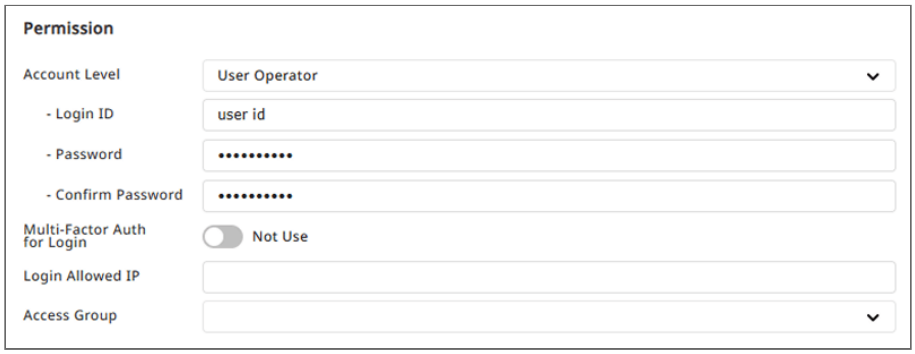
- **Administrator**: This is an administrator level that can use all menus.
- **User Operator**: The **User** menu has **read** and **edit** permissions. No permissions exist for other setting groups besides the **User** menu.
- **Monitoring Operator**: The **Monitoring** and **Data** menus have **read** and **edit** permissions, and the **Dashboard** menu has **read** permission.
- **T&A Operator**: The **TIME ATTENDANCE** menu has **read** and **edit** permissions, and the **User** menu has **read** permission.
- **Visitor Operator**: The **VISITOR** menu has **read** and **edit** 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**.
- **Edit** permission for the **Monitoring** menu allows adding tabs or controlling status tree entries.
- **Edit** permission for the **Data** menu allows saving reports, adding automated report schedules, and accessing settings.
- For information on adding custom user permissions, see Add Custom Permissions.
- 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 policies, see License Policy.

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**.



Info

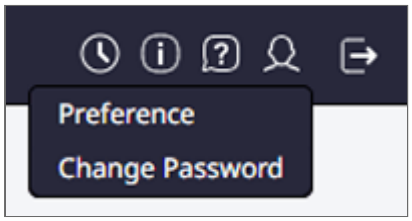
Precautions when setting ID and password

- Set the ID to a combination of letters, numbers, and a period (.) within 8~32 characters. Do not use single quotes (').
- For more information on configuring password policies, see Enhance System Security.
- Avoid using passwords that are vulnerable to security.
  - Consecutive characters or numbers (e.g., abcd, 1234)
  - Common words or patterns (e.g., qwerty, password)

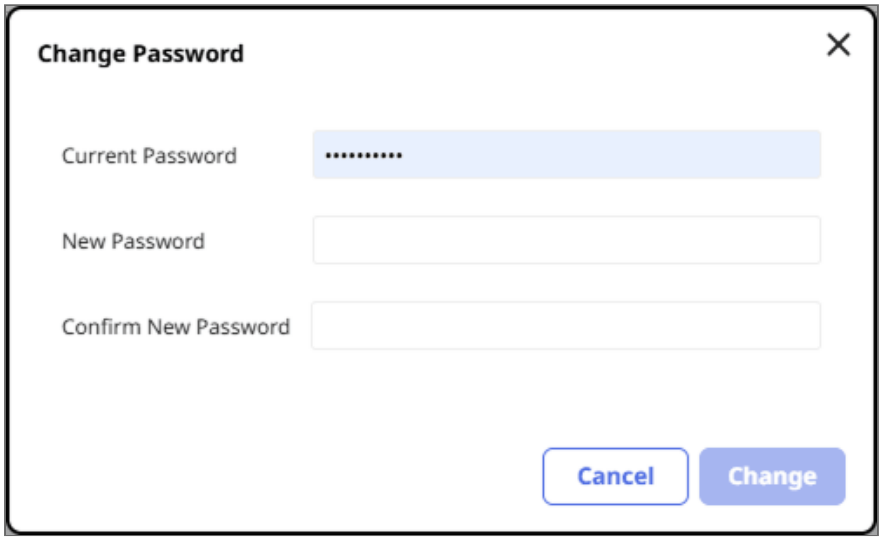
Change the login user's password

Change your password after logging in to **BioStar X**.

1. Log in to **BioStar X**.
2. Click at the top right of the screen.



3. Click **Change Password** in the dropdown menu.
4. When the **Change Password** window appears, enter the current password and a new password.



5. After entering all items, click **Change**.

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 on configuring **multi-factor authentication**, see Login in with Multi-Factor Authentication.

Login setting by 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 on adding and configuring access groups, see Manage Access Groups.

Next step

In the **Advanced** section, you can set the message to display on the device when the user accesses it or exclude that user from synchronization when linking with Directory Service.
Check how to edit user information.

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 **Launcher** → **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.



- **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 as an add-on for **Essential** licenses or higher. For more information on licensing policies, see License Policy.
> - For more information on directory integration settings, see Directory Integration Settings.

Next step

Check how to edit user information.

Register and Edit Users by Scanning an ID

Instead of entering user details one by one, you can scan an ID to get the user's name and ID photo, then register or edit the user.

Before you start

- Connect the DESKO ID Scanner to the client PC to use scan ID.
- Before registering a user with a ID scan, select the data to get from the ID. For more information on Scan ID settings, see Set Up ID Scan.

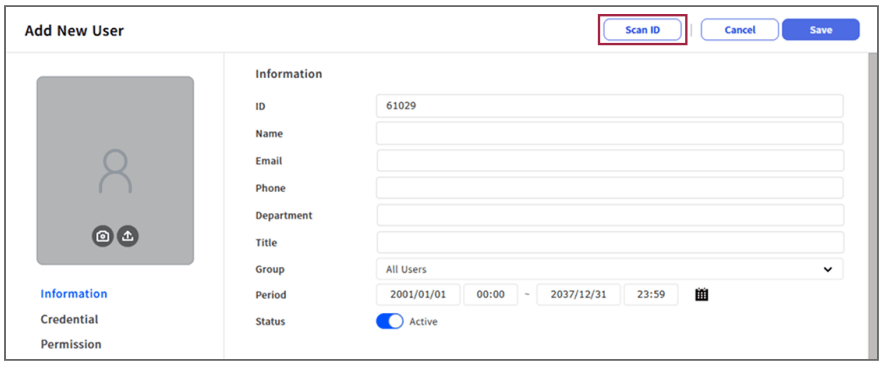
> **Info**
>
> The **Scan ID** feature currently supports only passport scans.

Register a user by ID scan

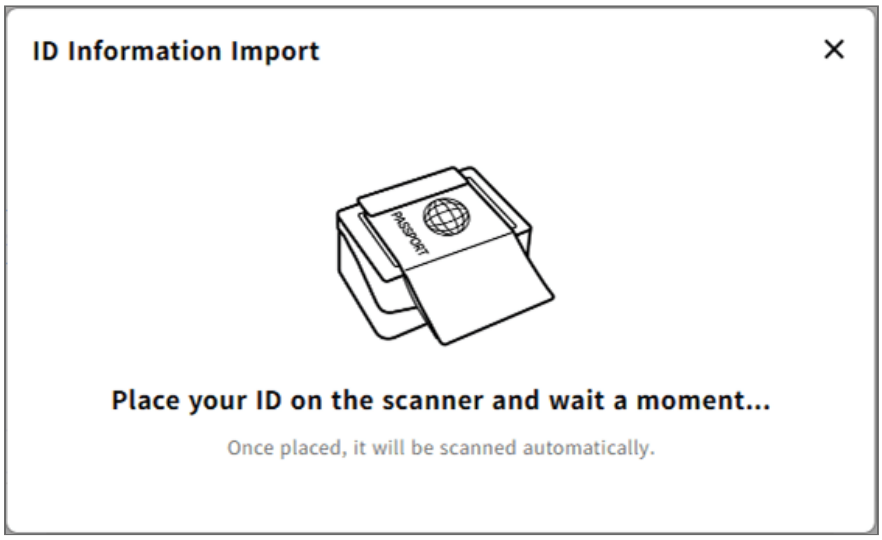
1. Click **User** on the **Launcher** page.
2. Click **New User** in the upper right corner of the **User** page.



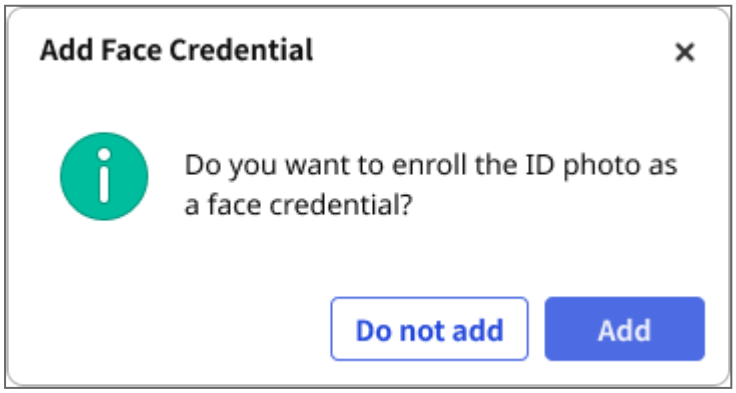
3. Click **Scan ID** in the upper right of the **Add New User** screen.



4. When the **ID Information Import** window appears, place the ID on the scanner.



5. After the ID scan success message appears, select whether to enroll the ID photo as a facial credential.



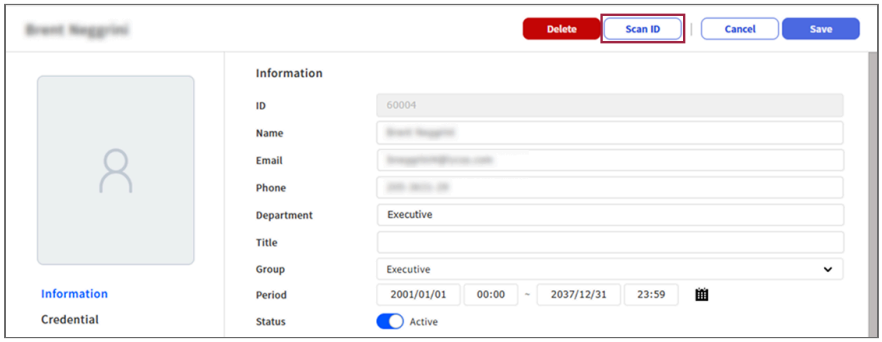
> This message appears when **Face Credential** is set to **Require Confirmation** under **Settings** → **Account** → **ID Scanning**. If you set the **Do Not Ask** option, this message will not appear and it will be enrolled immediately as a facial credential.

6. Review the information from the ID scan and edit it if needed.

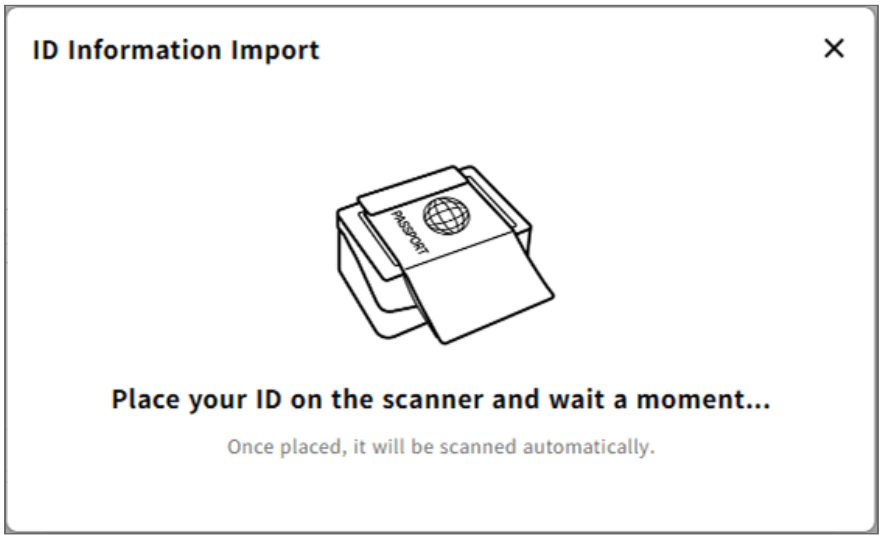
7. Click **Save** in the upper right corner of the screen to save the user.

Edit a user by ID scan

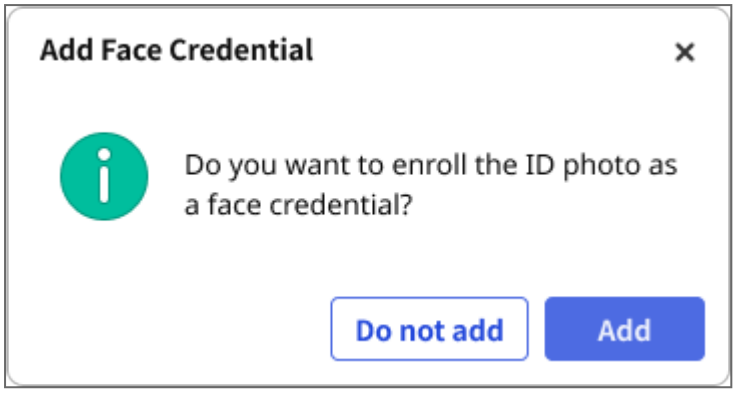
1. Click **User** on the **Launcher** page.
2. In the user list, double-click the user to edit with a ID scan.
3. Click **Scan ID** in the upper right of the edit user screen.



4. When the **ID Information Import** window appears, place the ID on the scanner.



5. After the ID scan success message appears, select whether to enroll the ID photo as a facial credential.



> This message appears when **Face Credential** is set to **Require Confirmation** under **Settings** → **Account** → **ID Scanning**. If you set the **Do Not Ask** option, this message will not appear and it will be enrolled immediately as a facial credential.

6. Review the information from the ID scan and edit it if needed.
7. Click **Save** in the upper right corner of the screen to save the updates from the scan.

> **Info**
> If the user has 2 or more facial credentials enrolled, editing via ID scan overwrites the first enrolled facial credential.

Error messages

If a problem occurs while scanning a ID, a message appears with the cause and solution. Use the information below to resolve the error.

Scan failed

If a problem occurs while the system automatically reads the ID on the scanner, one of the following messages appears.

Cause	Error message
ID security feature (UV pattern, etc.) verification failed	**Invalid ID. Check the ID and try again.**
The ID was not recognized within the specified time	**The ID was not scanned in time. Please try again.**
Other scan errors, such as the ID moving during scanning or page detection failure	**Unable to scan the ID. Check the ID and scanner, then try again.**

If this message appears, click **Retry** and scan again. Check that the ID is placed correctly on the scanner, then try again.

> **Info**
> Click **Retry** to restart automatic recognition from the **Place your ID on the scanner and wait a moment...** instructions.

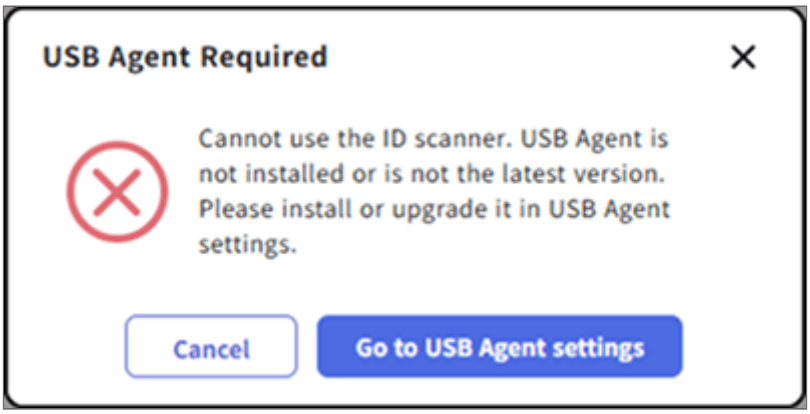
Scanner connection error

If the scanner connection fails, the following message appears. This error does not provide a retry button. Follow the instructions, then click **Scan ID** again to start scanning from the beginning.

Scenario	Error message	Solution
The scanner is not connected to the client PC	**The scanner is not connected. Please check the device connection and try again.**	Check the connection between the ID Scanner and the client PC.

USB Agent Required

Install the latest version of USB Agent before using the ID Scanner. If USB Agent is missing or outdated, an error dialog appears after clicking the **Scan ID** button.



- **Cancel**: Close the error window and do not scan.
- **Go to USB Agent settings**: Go to **Settings** → **Device** → **USB Agent**. On that screen, upgrade USB Agent to the latest version, then try scanning again.

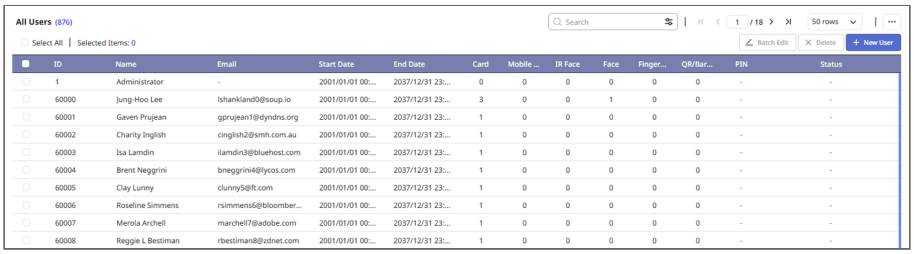
Explore Users

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

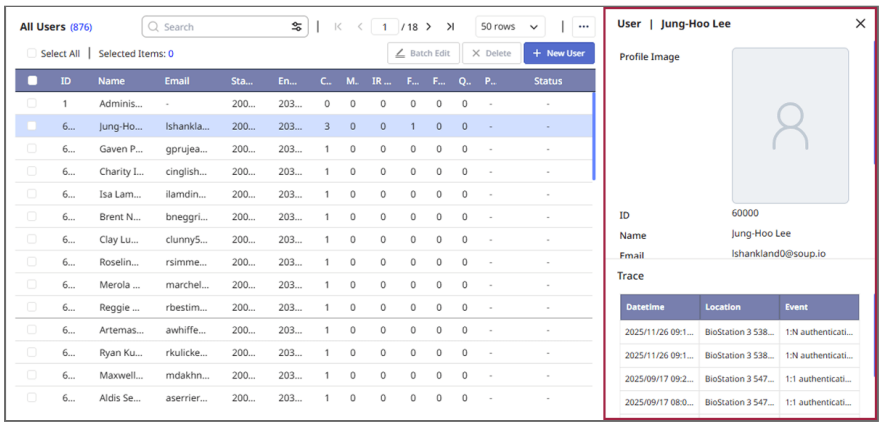
On the user list page, you can check the basic information and status of users, and view or edit the detailed information of each user.



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.



- 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 on editing user information, see Edit User Information.
> - You can change the column layout in the user list. For more information on changing the column layout, see Explore Users.

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`.

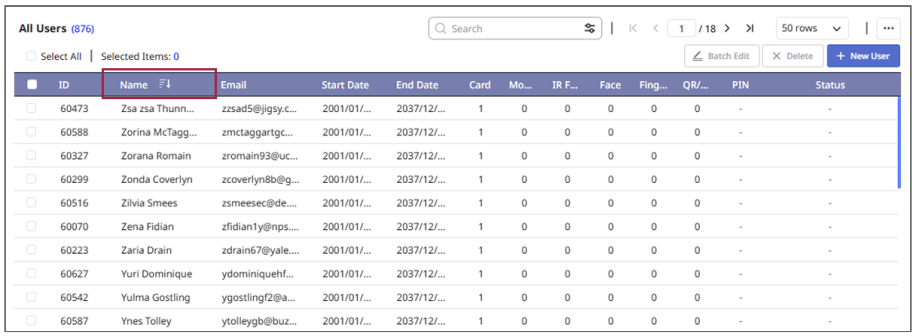
Change the number of users shown in the list

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 **Name** will sort the users' names in ascending or descending order. The clicked item will show either an ascending (↑) or descending (↓) icon.



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

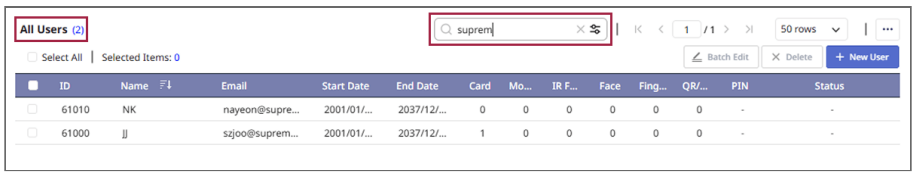
Search user

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 on entering basic user information, see Enter Basic User Information.

General search

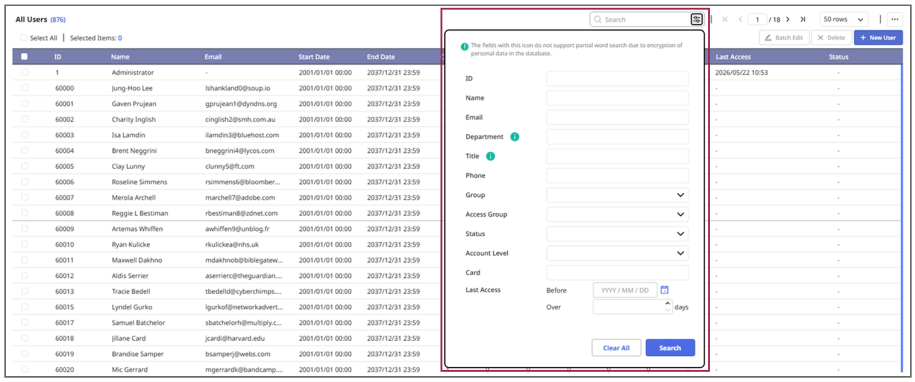
You can search based on the user's ID, name, or email. Enter the desired keywords in the search input field at the top of the screen and press the `Enter`. Users matching the specified keyword will be displayed in the list. You can check the number of search results at the very top of the list.



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**.



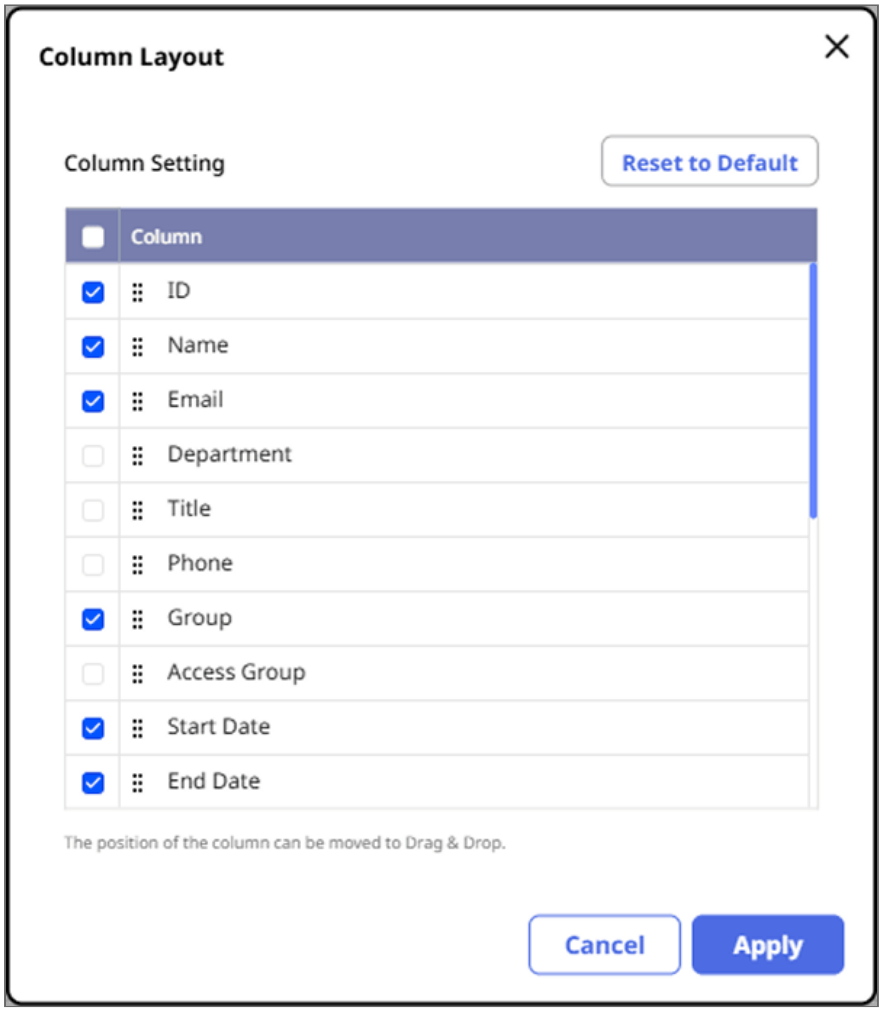
Info

- 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**, see Server Detailed Settings.

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.



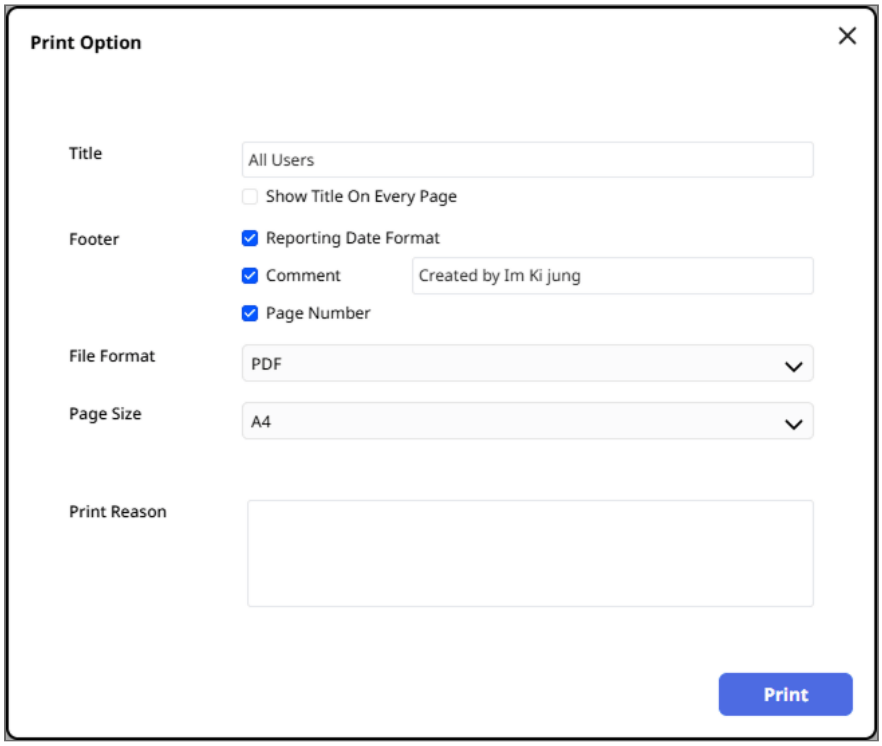
4. To change the order of the columns, click and drag the desired column to change its position.
5. Click **Apply** to save the settings.

> **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.



4. Enter **Print Reason** (optional) and click **Print**.

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

> **Info**
> **Print Reason** is optional. Check **Print Reason** records in **Settings** → **Audit Trail** → **AC Audit Log**.

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 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.

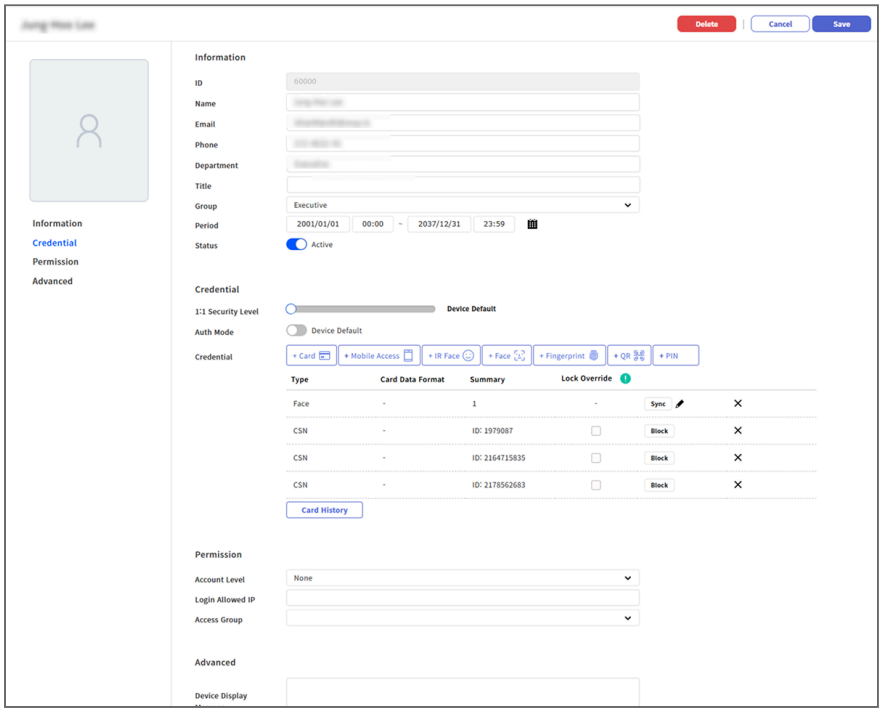
> **Info**
> A user with the original ID of `1` cannot be modified by other administrators. Only the user logged in to this account can modify their own information.

Edit user information

1. Click **User** on the **Launcher** page.
2. Select the user to edit from the user list.

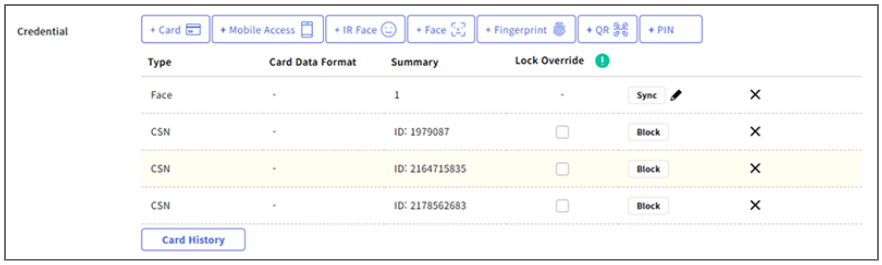
3. Double-click the user or click the **See More** button when the user's profile information appears on the right side of the screen.

4. A window for editing user information appears.



5. Modify the desired items.

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



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

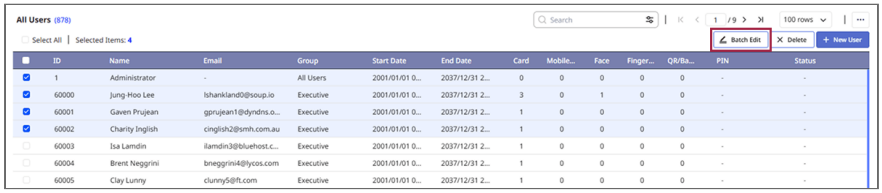
> **Info**
>
> - For more information on each field in the **Information** section, see Enter Basic User Information.
> - For more information on each field in the **Credential** section, see Enroll User's Credential.
> - For more information on each field in the **Permission** section, see Setting User Permissions.
> - You can enter the user's personal message in the **Advanced** section.

Batch edit user information

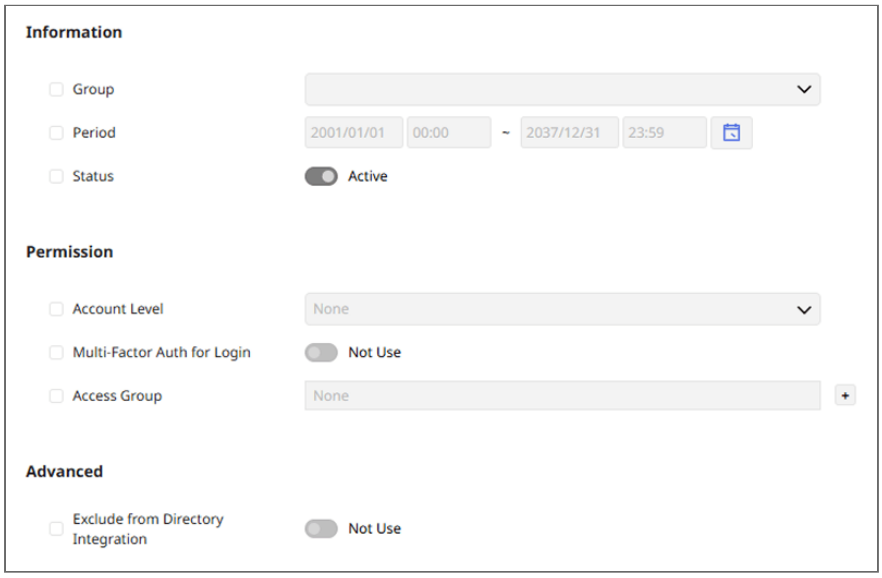
You can edit the information or access permissions of multiple users at once. This feature is useful when setting the same access permissions or groups for multiple users.

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.



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



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.

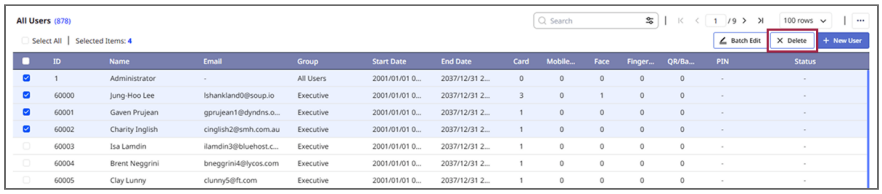
Next step

Enroll the user credentials and set the access authentication method.
Check how to set the user's access permissions.
If you have changed the user information, you must send it to the device. Check how to send user information to the device.

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.



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

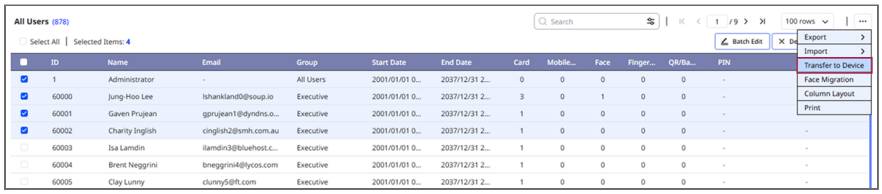
Confirm that the selected user has been deleted from the user list.

> **Info**
>
> - User with ID `1` cannot be deleted.
> - For more information on deleting user information from the device, see Manage Users Registered on Device.

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**.



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

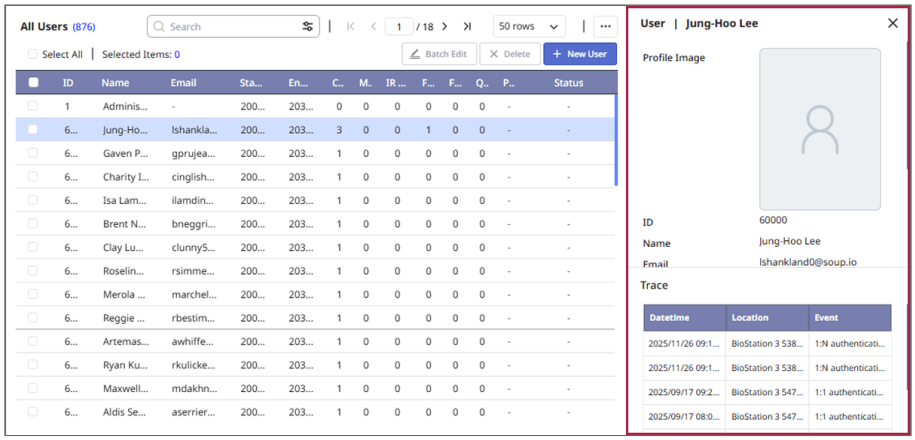
> **Info**
>
> - You can also search for devices by entering keywords in the search input field.
> - To transfer user information, the device must be connected to the **BioStar X** server.
> - If you change information for a user who is already registered on the device, you must resend the user information to reflect the changes on the device. For information on using the **Automatic User Synchronization** option to synchronize user information with the device, see Server Detailed Settings.
> - 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.



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, see Monitor Event.
> - Past access events can be viewed on the **Data** page. For more information, see Data.

Export/Import User Information

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

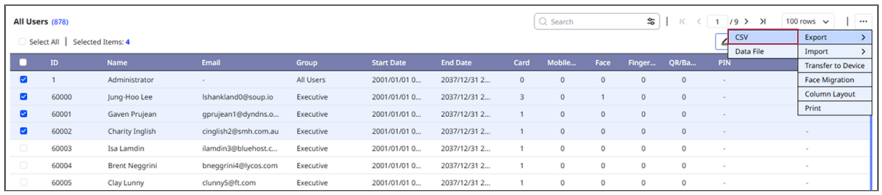
Export or import CSV

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, see Server Detailed Settings.
> - If user information is entered in a language other than English or Korean, save the CSV file in UTF-8 format.

Export CSV

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**.



4. When the **CSV Export** window appears, enter **Export Reason** (optional), and click **Download**.



5. Save the CSV file to your desired location on your local path.

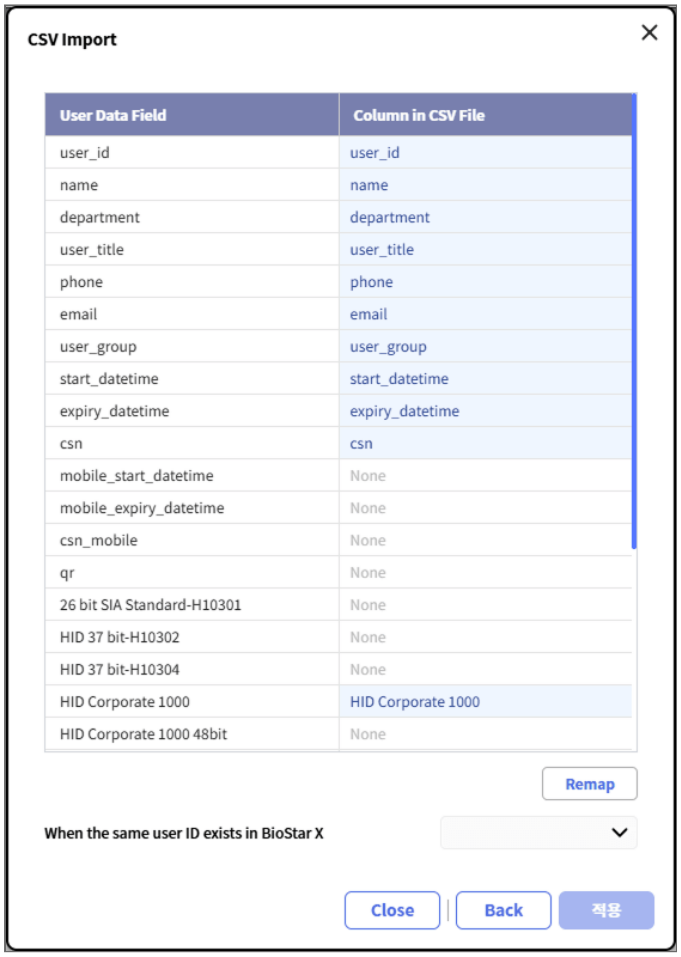
> **Info**
> **Export Reason** is optional. Check records for export reasons in **Settings** → **Audit Trail** → **AC Audit Log**.

Import CSV

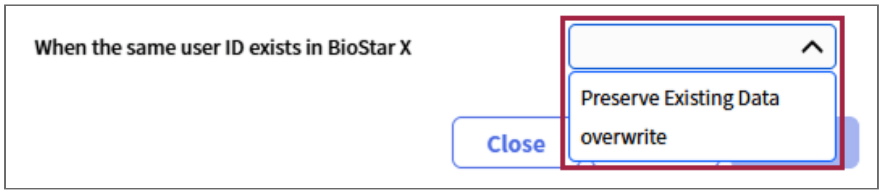
1. Click **User** on the **Launcher** page.
2. Click ••• at the top right of the screen and select **Import** → **CSV**.
3. Select the CSV file saved locally.
4. Set **Start import at row** in the **CSV Import** window and click the **Next** button.



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.



6. Select 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**.



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

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, see Batch Enroll Faces.
- User PINs can be enrolled through CSV import. For more information, see Enroll PIN.
- If you add columns that do not match the saved CSV file, you cannot import the file into **BioStar X**.
- If a username starts with `&@~`, importing that CSV entry fails.
- Set the validity period (expiration date and time) up to 2037-12-31 23:59:59. Import fails for entries with values after this date.
- Avoid opening the exported CSV file directly in spreadsheet programs such as Excel. If a username starts with the `=` character, the program may treat it as a formula and show a different value.

Export or import data files

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

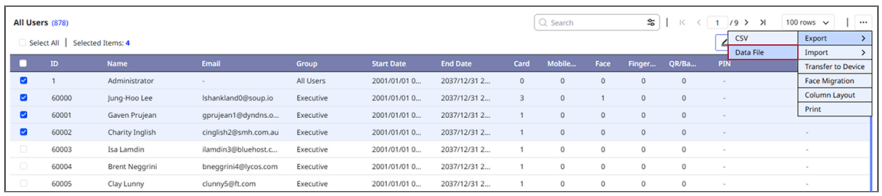
- Data exported from devices using outdated firmware cannot be imported into **BioStar X**. Always use the latest version of the firmware.
- Data cannot be imported if different fingerprint template formats are used. For example, data exported from devices using the Suprema fingerprint template format 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

Export data

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**.



4. In the **Data File Export** window, select the device to apply the data file.



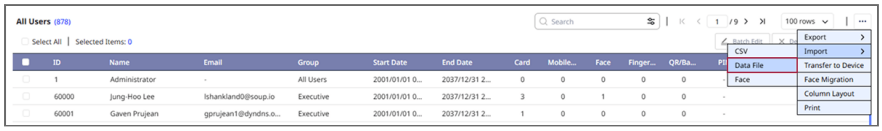
5. Enter **Export Reason** (optional) and click **Apply**.
6. Save the data file in your desired local path.

> **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.
> - **Export Reason** is optional. Check records for export reasons in **Settings** → **Audit Trail** → **AC Audit Log**.

> **Caution**
>
> To import file exported from **BioStar X** into devices, you must rename the file as follows so that the device can recognize it. The file name format will be adjusted to be automatically recognized through future device firmware updates.
>
> ***BioStarX**_YYYYMMDD_HHMMSS.tgz* → ***BioStar2**_YYYYMMDD_HHMMSS.tgz*

Import data

1. Click **User** on the **Launcher** page.
2. Click ••• in the top right corner of the screen, then select **Import** → **Data File**.



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

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

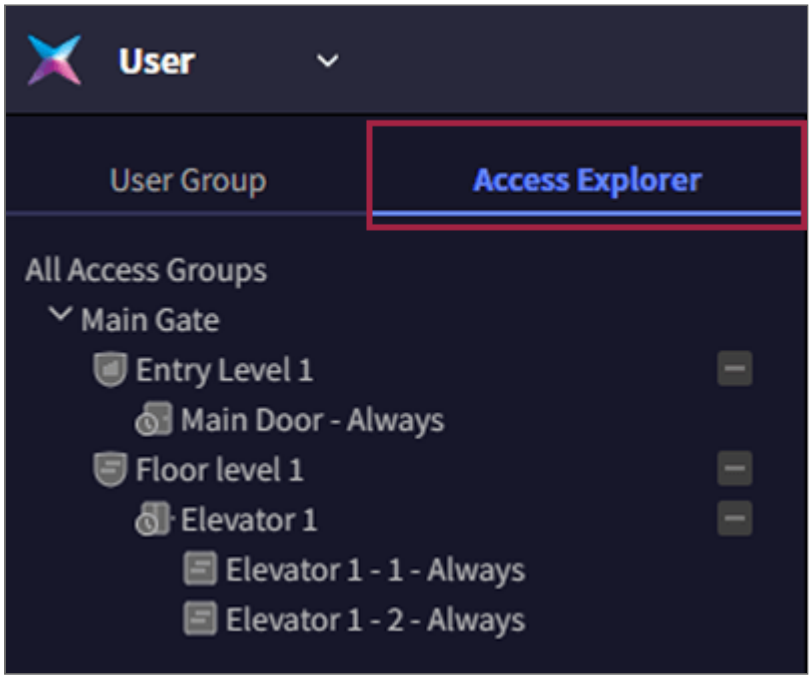
Manage Access Groups

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, see Access Control Settings.

Check users by access group

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



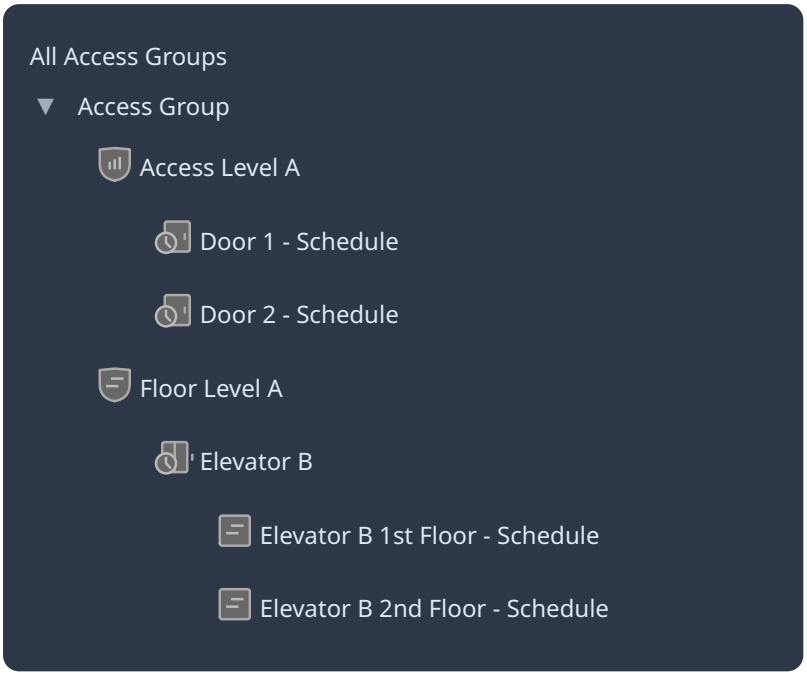
3. Click the desired access permission group in **All Access Groups**.

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.



- **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**. See Manage Access Groups For more information on creating access groups.

- **Access level** sets the times when users can enter and grants permission to access doors during this time. See Manage Access Levels For more information on creating access levels.
- You can manage the floors users can access via elevators through the **floor level**. See Manage Floor Levels For more information on creating floor levels.
- **Schedule** is a feature that efficiently operates access control and attendance management by setting access and holiday schedules. See Schedule Settings For more information on registering schedules.
- You can register elevators and manage the floors accessible via the elevators. For more information on registering an elevator, see Register Elevator.

Info

The elevator registration feature is available as an additional option with an **Essential** license or higher. For more information on licensing policies, see License Policy.

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

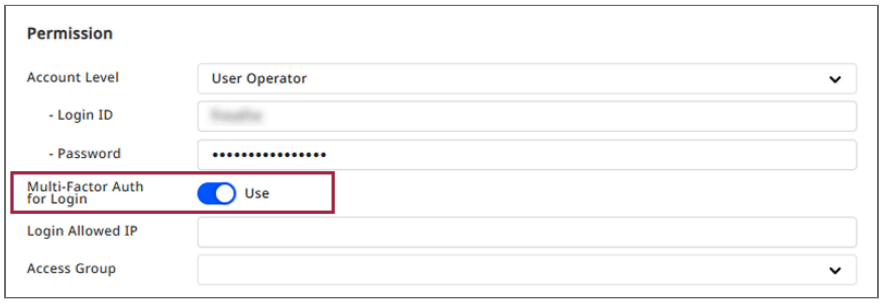
- After setting up the multi-factor authentication feature for the main admin account (ID 1), be aware that you will not be able to log in with that account if the fingerprint authentication becomes unavailable.
- If login becomes impossible due to fingerprint issues, contact Suprema Global Technical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

Multi-factor authentication settings

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.



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

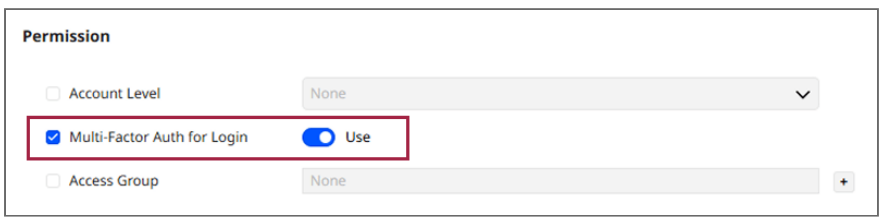
Completing multi-factor authentication setup.

Multi-factor authentication batch settings

> **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. For more information, see Setting User Permissions.

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**.



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

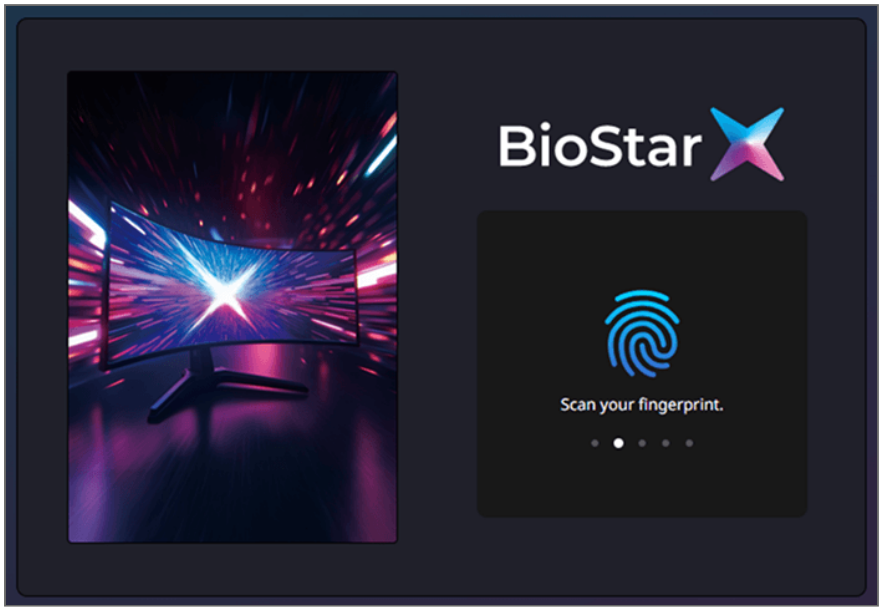
Completing the multi-factor authentication setup for multiple selected users.

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 you 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.

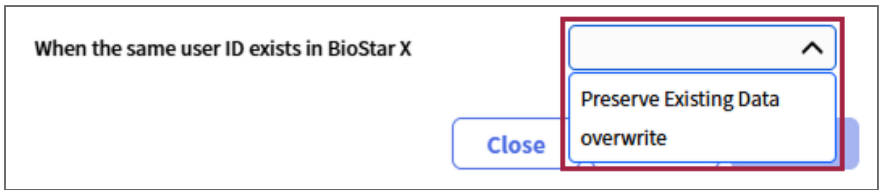
Enroll with CSV file import

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

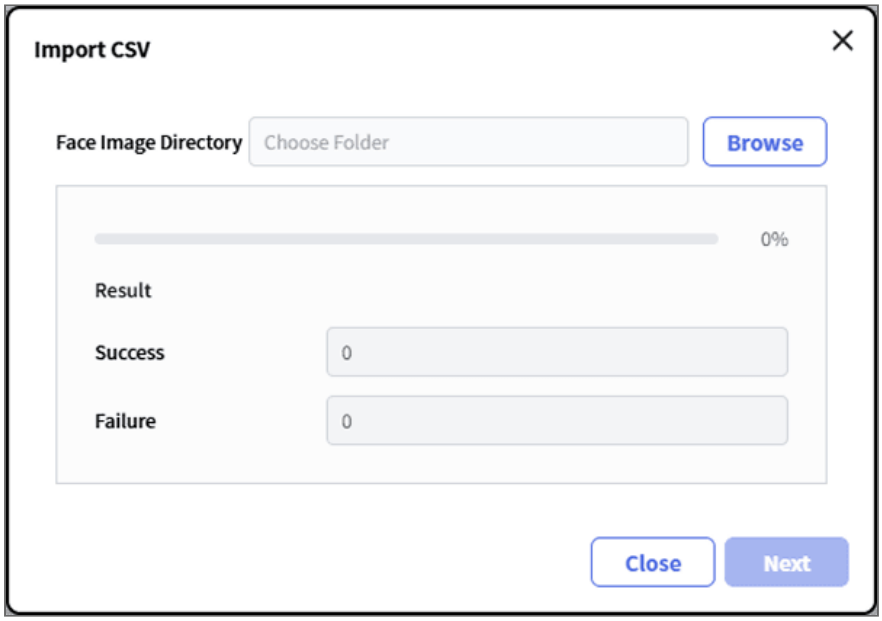
1. Click **User** on the **Launcher** page.
2. In the user list, check the checkbox of the user whose face you want to enroll. You can select more than one user.
3. Click the ••• button in the upper right corner of the screen and select **Export** → **CSV**.
4. When the CSV export window appears, click **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**.



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



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



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

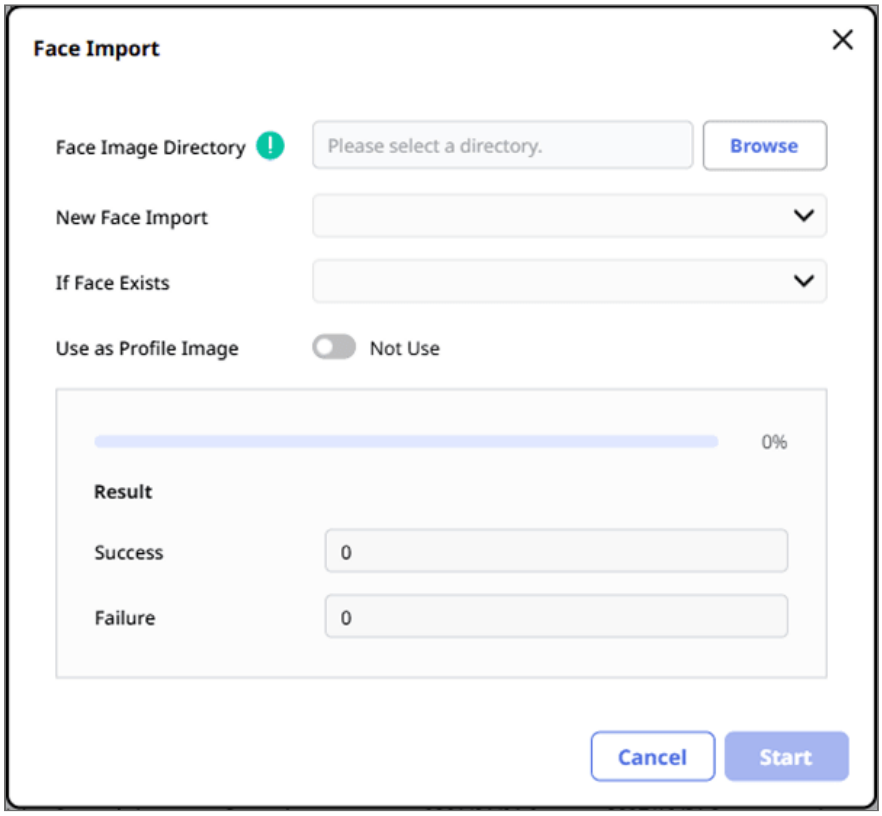
If an error occurs while importing the CSV file, you can recheck and upload only the CSV data that caused the error.

> **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 ••• in the top right corner of the screen, then select **Import** → **Face**.
3. When the **Face Import** window appears, click **Browse**.



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.

Enroll faces using a mobile device

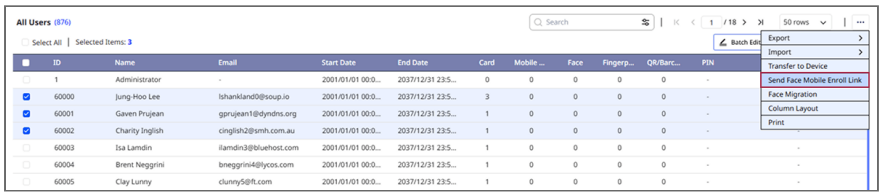
You can send face enrollment links to users via email. Users can access the link on their mobile devices to enroll faces directly.

Before you start

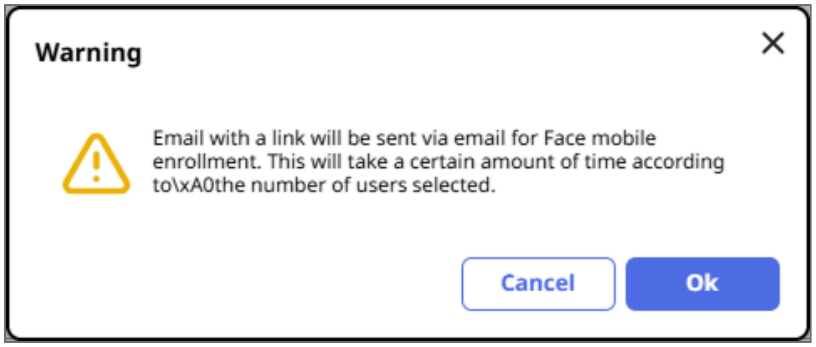
- Complete the email information settings, including SMTP settings, before using the mobile face enrollment feature. For more information, see Email Setting.
- You must enable the **Remote Access** feature to use the mobile face enrollment feature. For more information on **Remote Access**, see Remote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

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**.



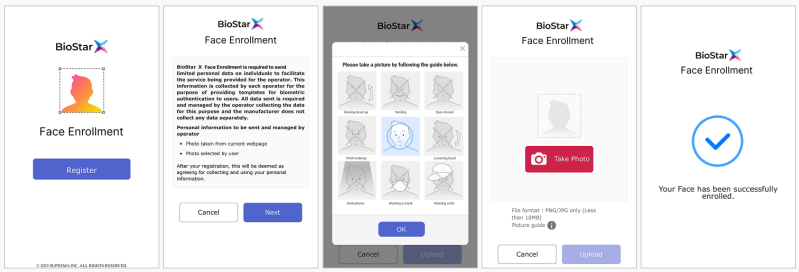
4. When the message window appears, click **Ok**.



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 on the system audit trail, see Manage Audit Trail.
- 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 face enrollment mobile link that was sent, the face enrollment service will be executed as shown below. Follow the instructions on the screen.



- 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 you 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.

- BioStation 3 Max firmware v1.0.0 or later
- BioEntry W3 firmware v1.0.0 or later

- BioStation 3 firmware v1.3.1 or later
- FaceStation F2 firmware v2.2.0 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 BioStation 3 Max, BioEntry W3, BioStation 3, and FaceStation F2.

- **NPU Type**: BioStation 3 Max, BioEntry W3, BioStation 3
- **GPU Type**: FaceStation F2

- **Synchronization Time Between Devices with Different Face Template Types**

  Before you run **Face Migration**, note that if you add BioStation 3 Max, BioEntry W3, or BioStation 3 to an environment that previously used only FaceStation F2 and then synchronize, the template type will change and NPU-type templates will be extracted from the images. This may take a considerable amount of time depending on the number of faces registered 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:

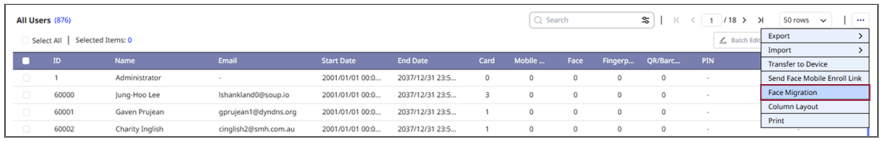
- FaceStation F2 firmware v2.2.0 or later
- BioStation 3 firmware v1.3.1 or later

Caution

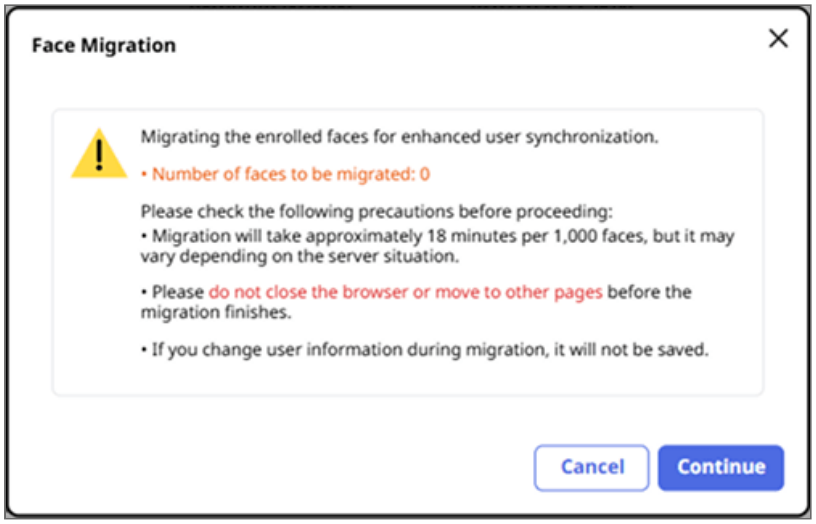
When using FaceStation F2 or BioStation 3, it is recommended to upgrade to the latest firmware version. The latest firmware can be downloaded from the Suprema Download Center.

How to face migration

1. Click **User** on the **Launcher** page.
2. Select ••• at the top right of the screen and click the **Face Migration** button.



3. Check the contents of the warning popup and click **Continue**.



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 on how to transfer user information to the device, see Transfer User Information to the Device.
- 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 on how to store only the template, without saving the user's facial image to the server, see Server Detailed Settings.

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 you start

You must first add the card credentials before setting the emergency open permissions. For more information on adding card credentials, see Enroll Access Card.

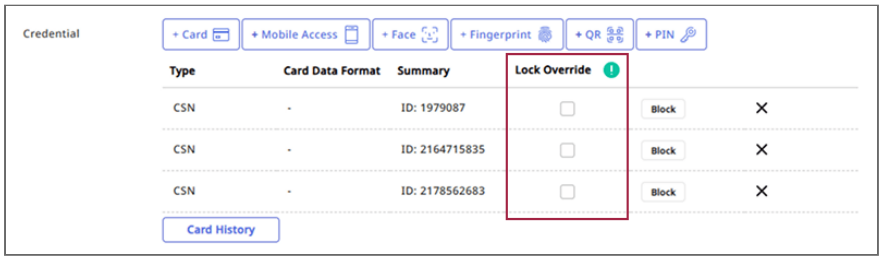
Info

- 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 Max firmware v1.0.0 or later
  - XPass Q2 firmware v1.0.0 or later
  - BioStation 3 firmware v1.4.0 or higher

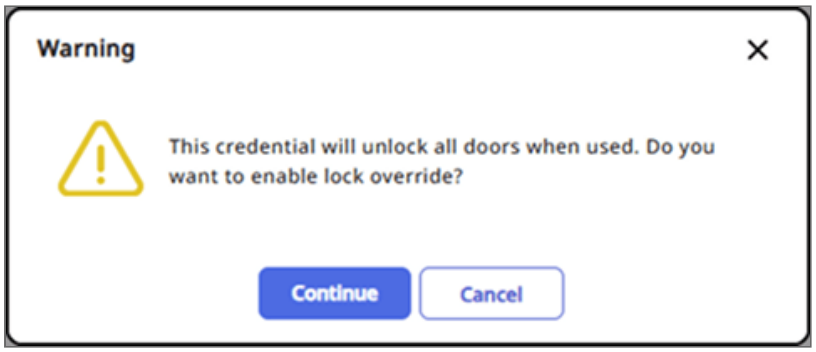
Set emergency open permissions

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.



5. When a warning message appears, check the content and click **Continue**.



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.

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 status

Monitor door, elevator, and advanced access control status in real time to operate the security system reliably. Use the status icons in **Monitoring** to check alarms and abnormal status at a glance. Review only entries that need action and respond immediately.

Click **Monitoring** on the **Launcher** page or select **Monitoring** from the shortcut list at the top left of the screen. Check the status of each entry in the **Door** tab on the left sidebar of the screen.

Before you start

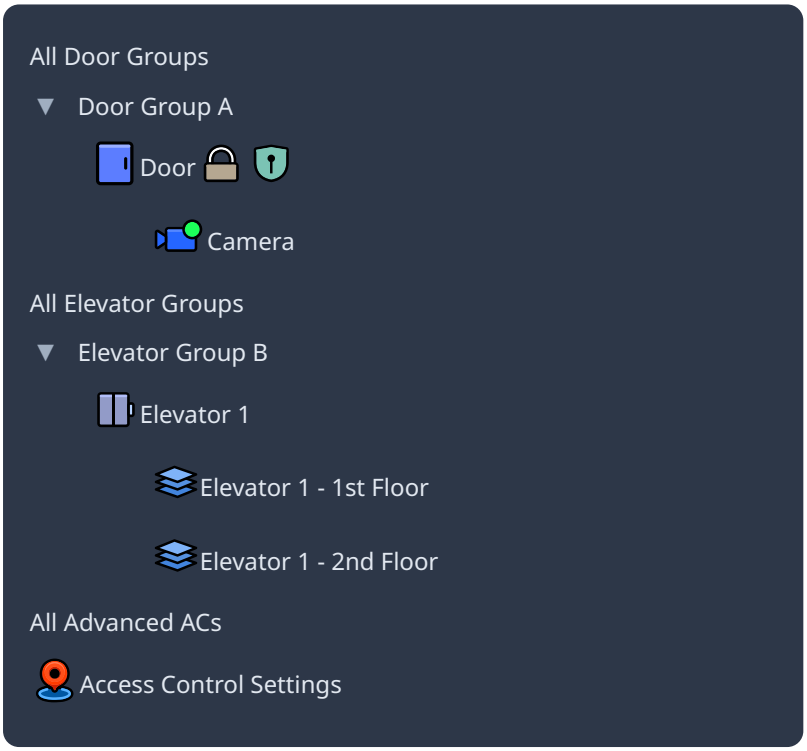
Ensure that the devices connected to the door are correctly configured. It is important to check if the device is connected to the network and updated with the latest firmware. In case of an issue, it is advisable to first check the power status and network connection of the device.

Info

- For more information on adding and configuring devices, see Manage Devices.
- For more information on adding and configuring doors, see Manage Doors.
- The **Log Upload** feature must be enabled to monitor or control the status of the access door. Enable this feature under **Settings** → **System** → **Server** in the **General** section.
- The feature to connect cameras to doors through the VMS server is available as an additional option with an **Essential** license or higher. For more information on licensing policies, see License Policy.

Learn about the tree structure

The tree structure in the **Door** tab of the left sidebar is organized as follows.



Info

- For more information on adding and configuring devices, see Manage Devices.
- For more information on adding and configuring doors, see Manage Doors.
- For more information on adding and configuring elevators, see Manage Elevators.
- For more information on advanced access control settings, see Advanced Access Control Settings.
- For more information on linking doors and cameras, see Set Video Rules.

Check status

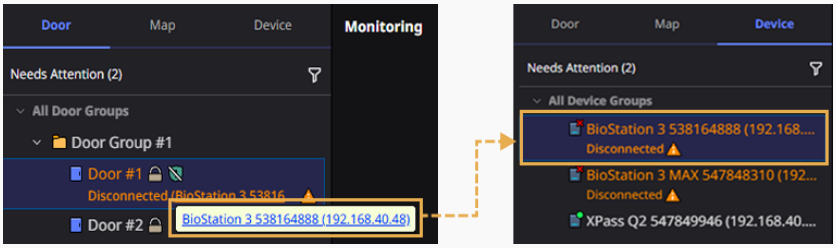
Check connection errors and alarms

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.

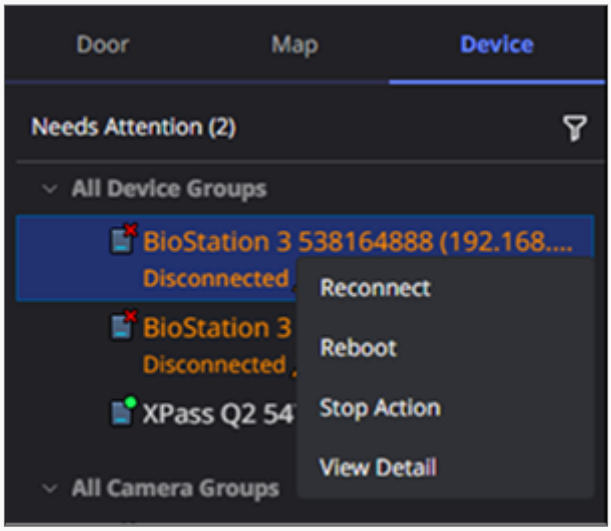
Status Icon	Description
⚠	Displays device abnormal statuses such as disconnection, Multi Communications Server errors, and synchronization errors.
🚨	Displays the status of entry doors, elevators, advanced access control, and AI video analysis alarms.

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.



Right-click on the device and select the **Reconnect** or **Reboot** option.

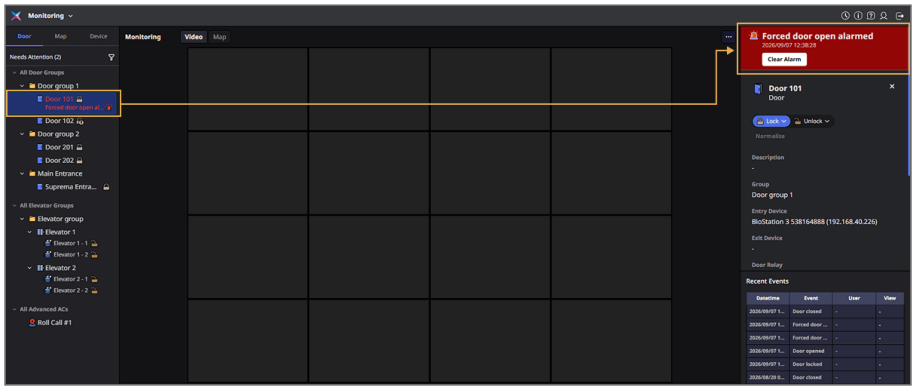


Info

- 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 configuring video rules, see Set Video Rules.
- 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, see Monitor Event.

Check alarms in the preview panel

In the **Door** tab, select a door, elevator, or advanced access control area with an alarm( ) icon. Review alarm details at the top of the preview panel on the right. For doors and elevators, the top of the panel also shows abnormal status ( ).



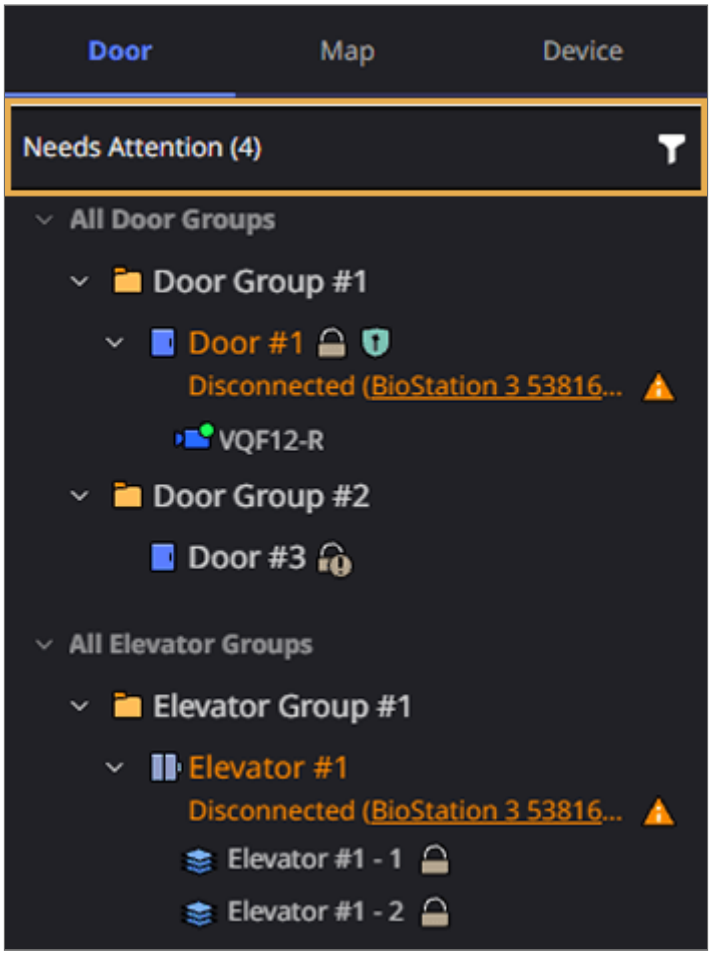
A banner at the top of the panel shows current status details, such as the alarm name and time. It also provides buttons to execute the appropriate action.

Info

- Even if multiple alarms occur at the same time, the banner displays only 1 alarm—the most recent one.
- For doors or elevators, alarms triggered while the device is disconnected show only the alarm type, without a timestamp.
- The buttons on the banner vary by alarm type. Click a button to take the action for the alarm.
- Door controls, such as locking and unlocking, remain available while an alarm appears. For more information on door control, see Door Control.

View entries that need attention

Administrators can view only doors and elevators that need action at a glance. In the left sidebar, click the **Needs Attention**. Check door and elevator status and take immediate action when problems occur.



> **Info**
> See Attention criteria for the conditions that mark doors and elevators as requiring attention.

Attention criteria

Door

A door requires attention if any condition below applies.

Door mode change

This includes doors locked or unlocked by an administrator, a schedule, or an emergency.

Reason	Status indicator
Manual operation by an administrator	**Locked by Operator** / **Unlocked by Operator**
Schedule	**Locked by Schedule** / **Unlocked by Schedule**
Emergency	**Locked by Emergency** / **Unlocked by Emergency**

Alarm

If any alarm remains uncleared, the system marks it as needing attention. Forced open, door held open, and anti-passback alarms are classified as alarms, not abnormal statuses.

Alarm types	Description
Door forced open	Door opened by force without unlocking
Door held open too long	Door remains open longer than the set time
Anti-passback (APB) alarm	Anti-passback rule violated
Timed anti-passback alarm	Time-based anti-passback rule violated
Lock override alarm	Unlocked by lock override card authentication in a locked state (locked by an administrator or by schedule)
AI video analytics alarm	Video analytics-based alarms, such as tailgating, loitering, intrusion, falls, and abandoned objects

Abnormal status

The system determines it based on the connection status of devices connected to the door.

Abnormal status type	Description
Disconnected	The device is disconnected from the network
Synchronization error	Connected, but data is out of sync
Multi Communications Server error	An error has occurred on the device's Multi Communications Server

Info

- The **Needs Attention** filter includes device lock and lockout due to consecutive authentication failures (Auth Fail Lockout), in addition to the abnormal statuses above.
- If an alarm and an abnormal status occur together, both icons appear in one row without overlap.
- Abnormal statuses from child devices roll up to the parent door node. Follow the hierarchy to find the problem while the filter is on.

Elevator

Evaluate elevators under the same conditions as doors. However, abnormal status and alarm conditions differ as follows.

- **Mode change**: Same as doors. The system marks the elevator as needing attention when an admin, schedule, or

emergency locks or unlocks it.

- **Abnormal status**: Use door criteria. However, elevators do not have forced open or long-held open status, so exclude them from evaluation.
- **Alarm**: Elevators have dedicated alarms that differ from door alarms. Please refer to the below.

Alarm types	Description
Elevator alarm triggered	Elevator alarm activated
Elevator input alarm	Alarm triggered by an external input signal
Elevator all-floor unlock alarm	All floors forcibly opened

Info

- Floors appear as independent nodes under the elevator node, and each floor has only locked ( ) or unlocked ( ) status.
- Alarms and abnormal statuses appear on the parent elevator node, not on floors. When the elevator expands, only floors that require action appear, and the system hides normal floors.

Advanced access control

Entries in the advanced access control group (anti-passback, fire alarm, intrusion, muster, occupancy limit, and interlock) are also included when determining whether action is required. However, unlike doors or elevators, mode changes and abnormal status conditions do not apply. If any alarm remains uncleared, it appears as requiring action.

Alarm types	Description
Anti-passback (APB) alarm	Anti-passback rule violated
Fire Alarm	Alarm triggered by detecting a fire
Scheduled lock alarm	Alarm triggered while scheduled lock is set
Intrusion alarm	Alarm triggered by detecting an intrusion
Interlock alarm	Interlock rule violation
Muster alarm	Alarm triggered during a muster event

Info

- Armed status and disabled items are not shown as requiring action. Armed means the zone operates normally, and Disabled means it is intentionally off.
- Each entry appears directly under the advanced access control group, and doors do not expand under it. Only entries that require action remain in the tree. If no entries require action, the advanced access control group is removed from the tree.

Checking door status

Check whether the door is closed, open, or in an abnormal state. Refer to the following for door status.

Status Icon	Description
	The door is closed.
	The door is open.
	The door sensor is not set up.

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 system locks the door using the **Timed** or **Permanent** option.
	The entrance door is open.
	The system unlocks the door using the **Timed** or **Permanent** option.

Info

For more information about door control options, see Door Control.

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.

Info

- If the camera linked to the access door isn't visible, check the camera group's permissions. If the administrator for a custom permission hasn't configured the camera group permissions, the camera may not be visible. For more information on configuring camera group permissions, see Set Up the Camera.
- To link a door to a camera, add a video rule. For more information, see Set Video Rules.

Checking arming status

You can check the security status of the entrance door or advanced access control settings.

Status Icon	Description
	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 intrusion alarm settings, see Intrusion Alarm.

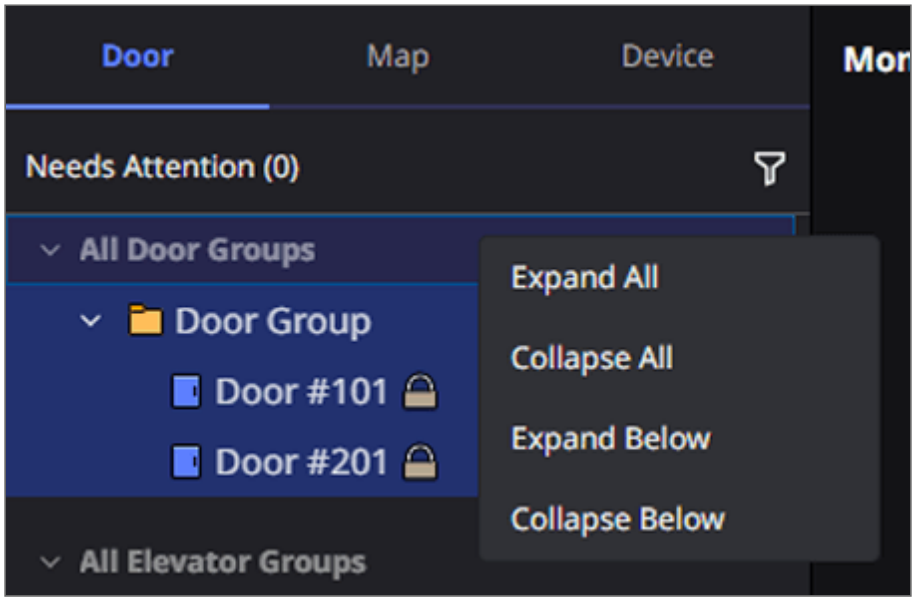
Check elevator status

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.

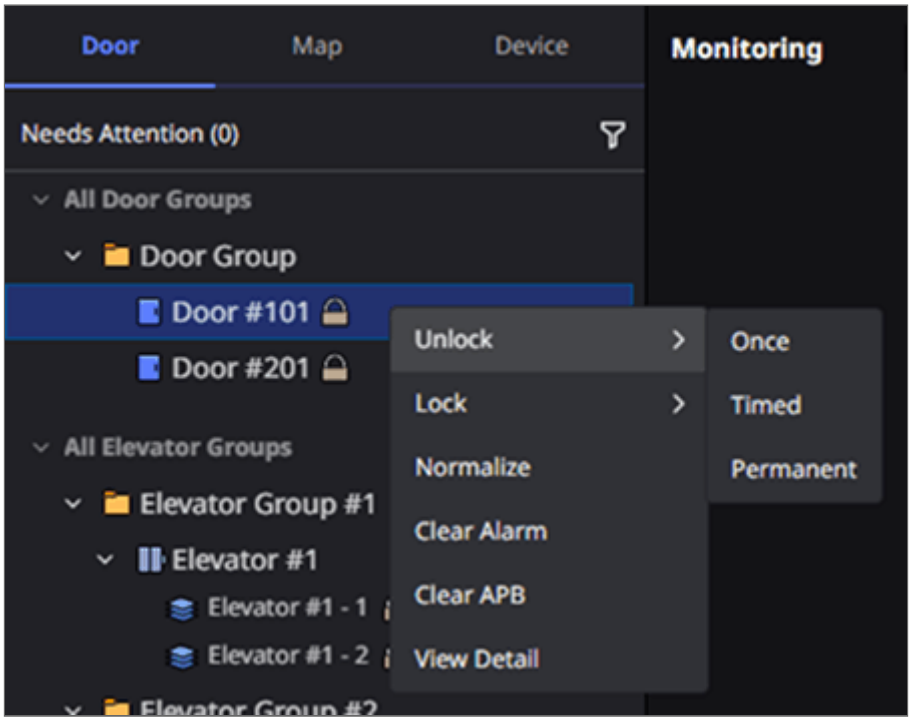
You can expand or collapse the list of the selected sub-group.

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.

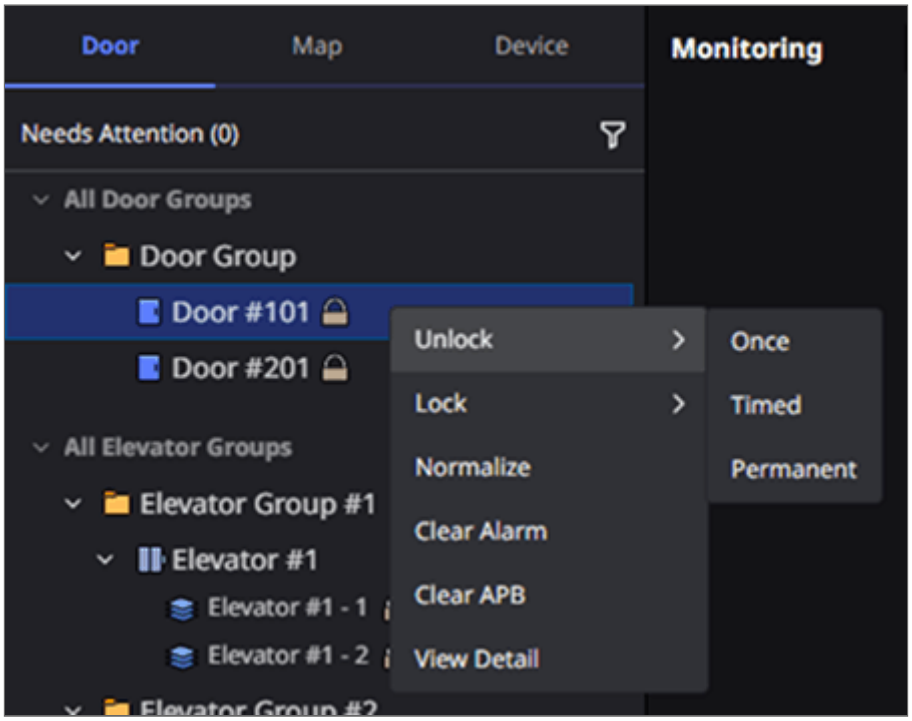


Info

- The **Log Upload** feature must be enabled to monitor or control the status of the access door. Enable this feature under **Settings** → **System** → **Server** in 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 is available through the purchase of add-on options with an **Essential** license or higher. For more information on the licensing policy, see License Policy.
- To control multiple doors at once, see Bulk Control.

Door open

The opened door can be accessed by anyone. Click **Unlock** in the popup menu and select the desired option.



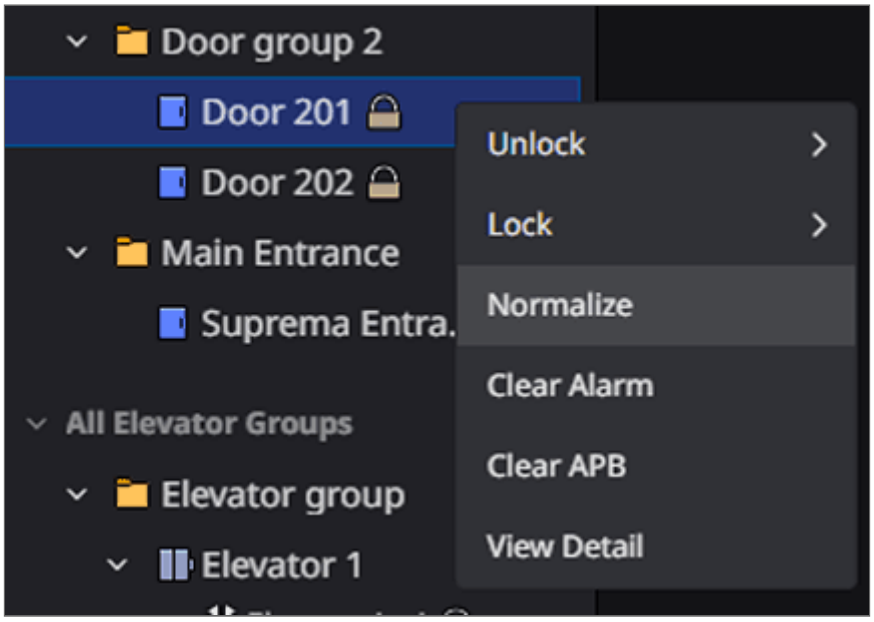
- **Once**: Unlocks the door once.
- **Timed**: Opens the door for a certain time. Enter the desired time in seconds.
- **Permanent**: Unlocks the door regardless of time.

Temporarily opening the door changes the door relay icon from to . Opening the door with the **Timed** or **Permanent** option changes the icon 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.

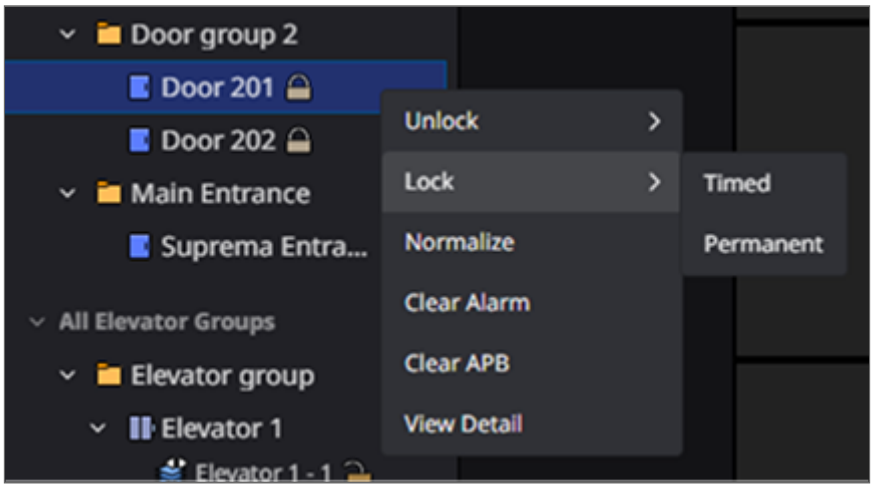
Door normalize

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.

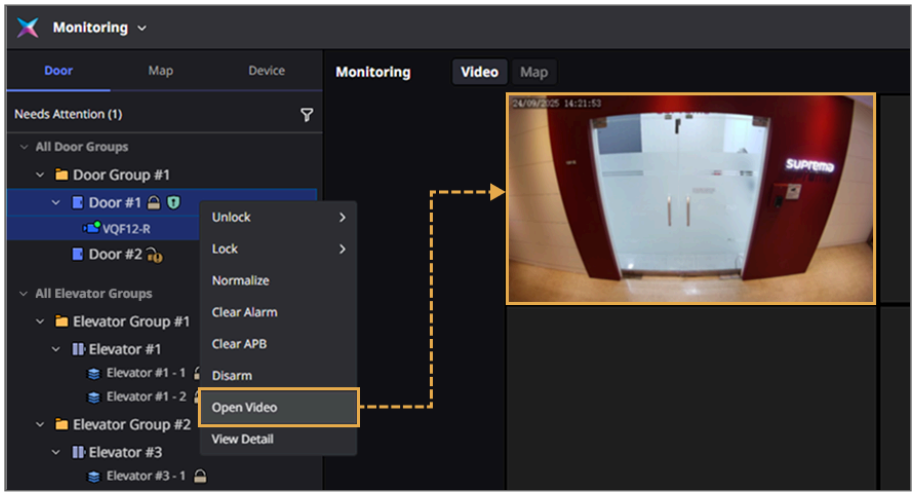


- **Timed**: Changes the door to a locked state for a certain period of time. Enter the desired time in seconds.
- **Permanent**: Changes the door to a locked state regardless of time.

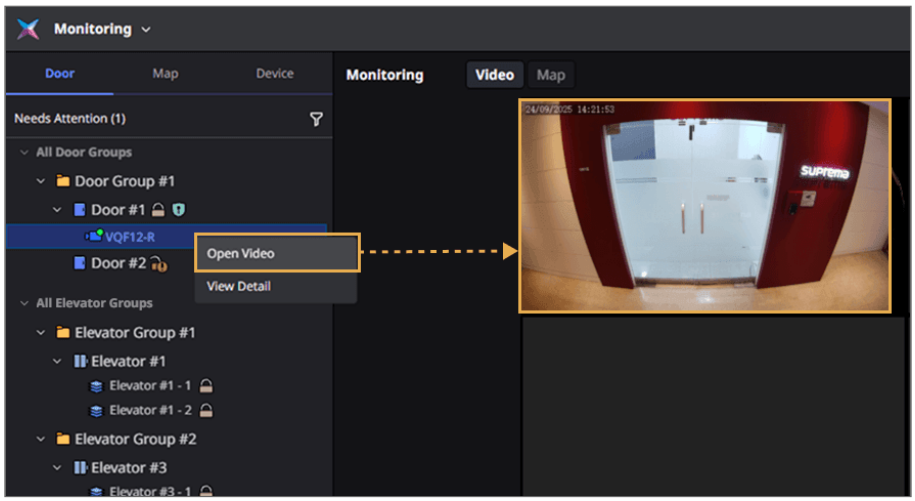
Locking the door changes the door relay icon to .

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.

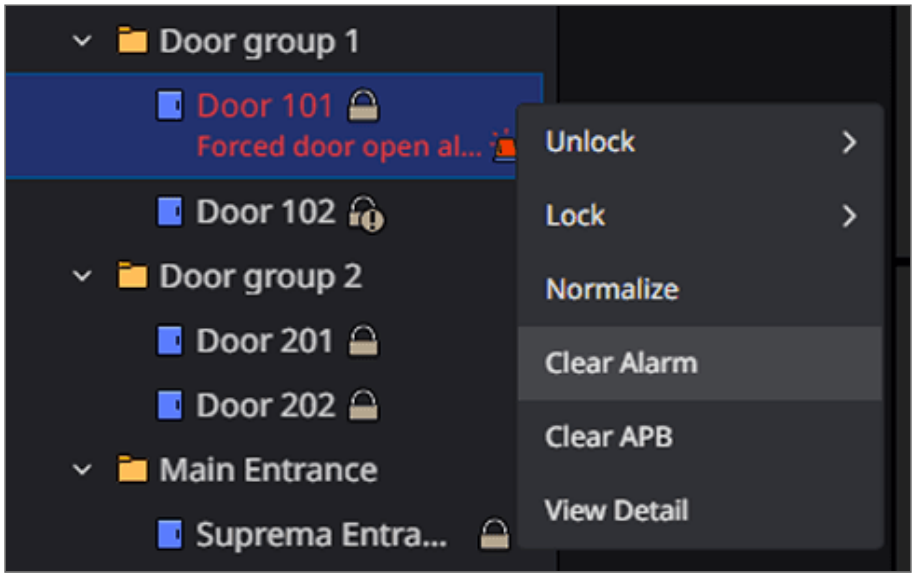


Info

- 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 on video monitoring, see Monitor Video.
- If the camera linked to the access door isn't visible, check the camera group's permissions. If the administrator for a custom permission hasn't configured the camera group permissions, the camera may not be visible. For more information on configuring camera group permissions, see Set Up the Camera.
- This feature is available by purchasing add-on options with an **Essential** license or higher. For more information on licensing policies, see License Policy.

Clear alarm

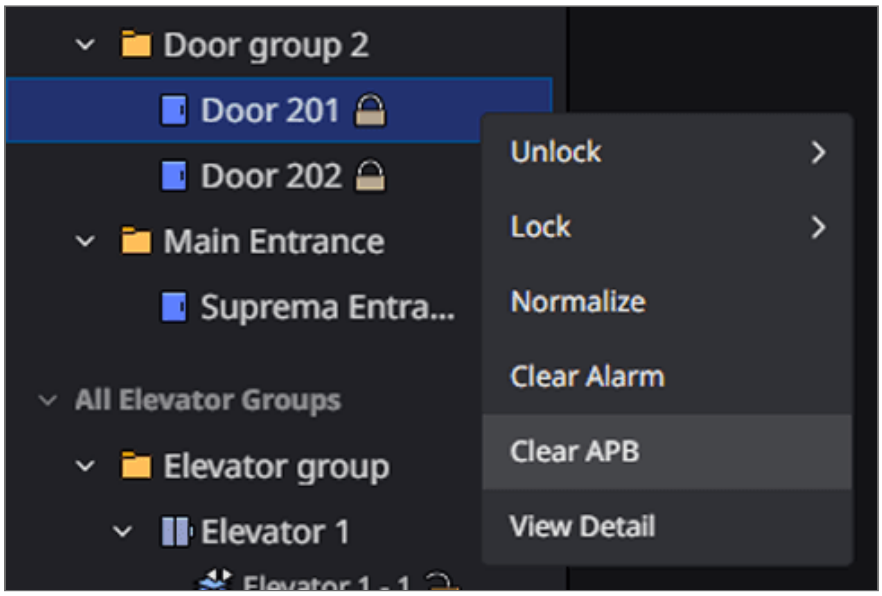
You can deactivate the alarm that occurred at the door. Click **Clear Alarm** in the popup menu. An alarm message appears in the upper right corner of the screen.



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 all users.



3. Select the user who have violated anti-passback and click **Apply**.

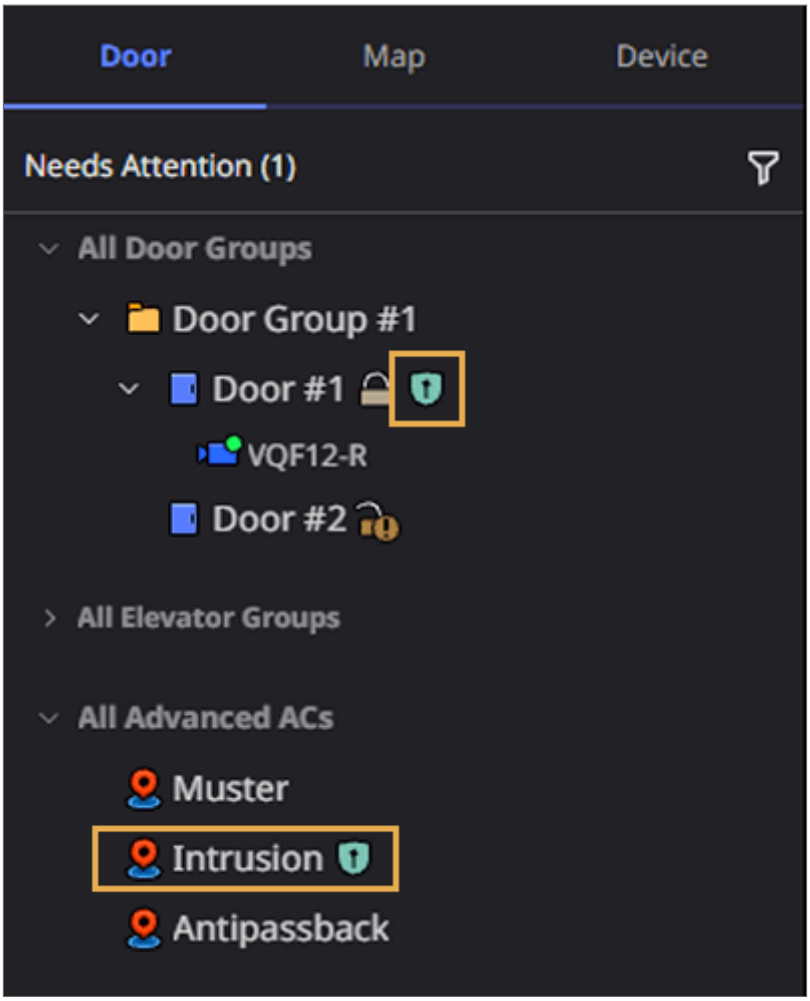
A completion message appears in the upper right corner of the screen.

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 setting up **anti-passback** for a door, see Register Door.

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.

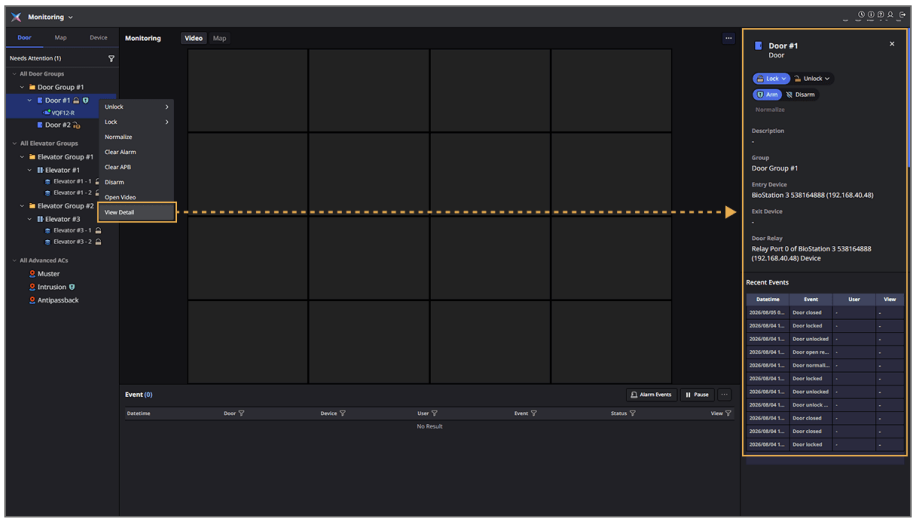


An armed door changes the armed status icon from to . The icon also applies to the corresponding access control setting.

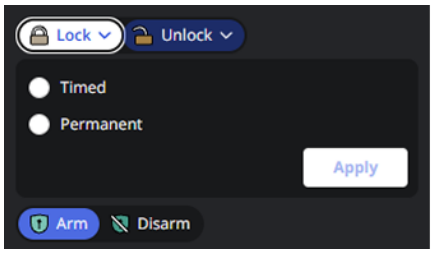
> **Info**
>
> This feature is available by purchasing add-on options with an **Essential** license, or with an **Enterprise** license or higher. For more information on the licensing policy, see License Policy.

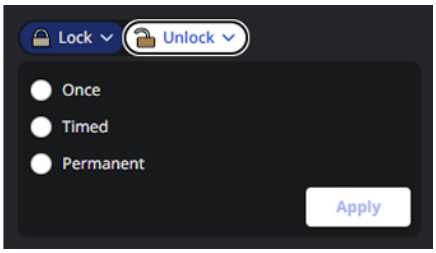
View details

You can check detailed information about the door and the event history. Click **View Detail** in the popup menu. A panel appears on the right side of the screen, showing door control, door details, and event history.



- **Door control**: Change the door status to locked, open, armed, or disarmed.





- **Normalize**: Use this option if an administrator manually opens or locks the door.
- **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 on each item in the door details section, see Register Door.

Control Elevators

This guide describes how to control the elevator. You can control the elevator or check detailed information through the provided features.

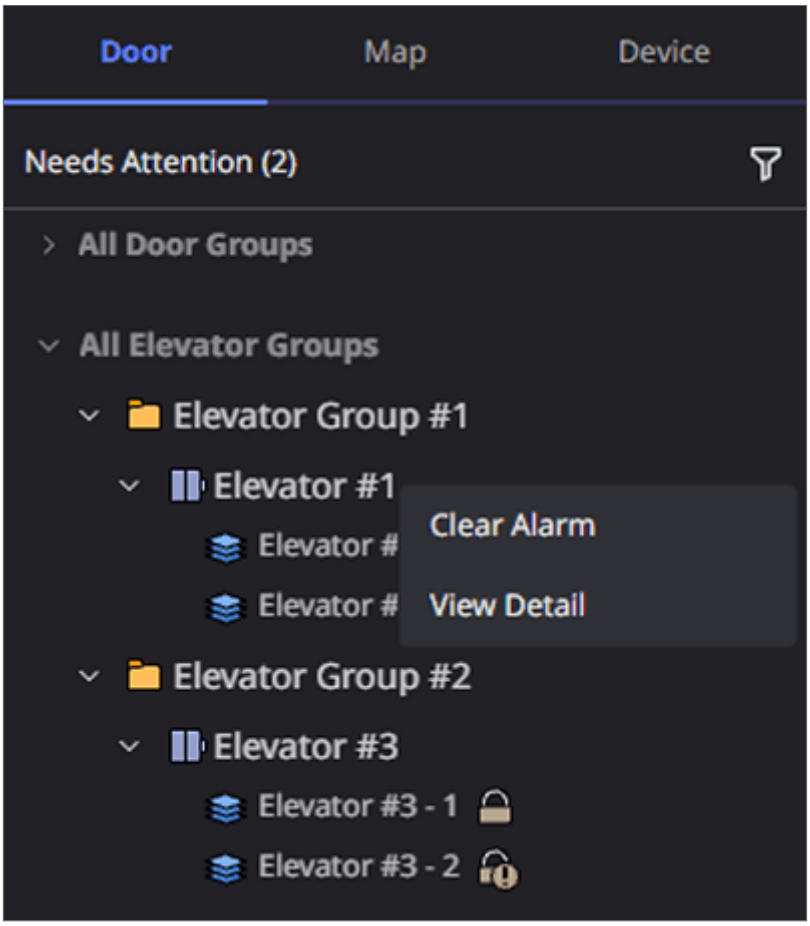
1. Click **Monitoring** on the **Launcher** page or select **Monitoring** from the shortcut list at the top left of the screen.

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 on setting up elevators and configuring groups, see Manage Elevators.
> - To control multiple elevators and floors at once, see Bulk Control.

Control Elevators

You can acknowledge or check details of alarms triggered by the elevator.

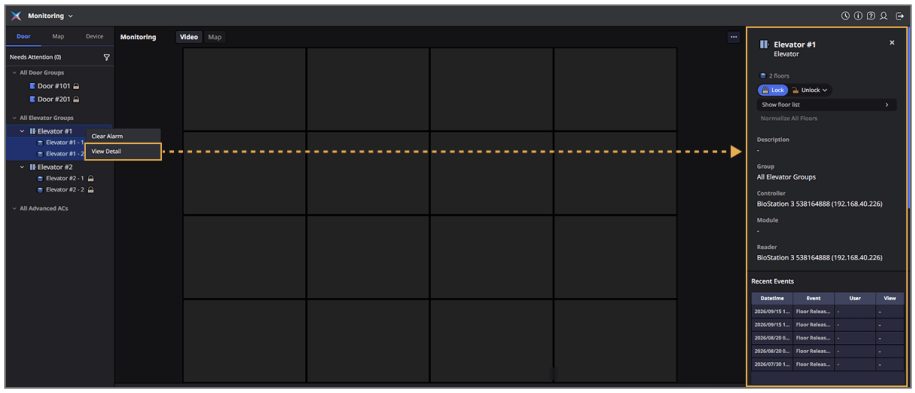


Clear alarm

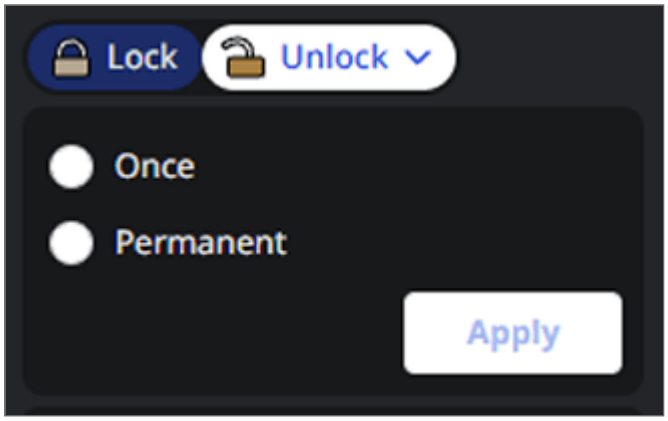
You can deactivate the alarm that occurred at this elevator. Click **Clear Alarm** in the popup menu. A completion message appears in the upper right corner of the screen.

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 control**: Set the elevator to locked or open.



- **Show floor list**: Shows the list of floors set for the elevator.

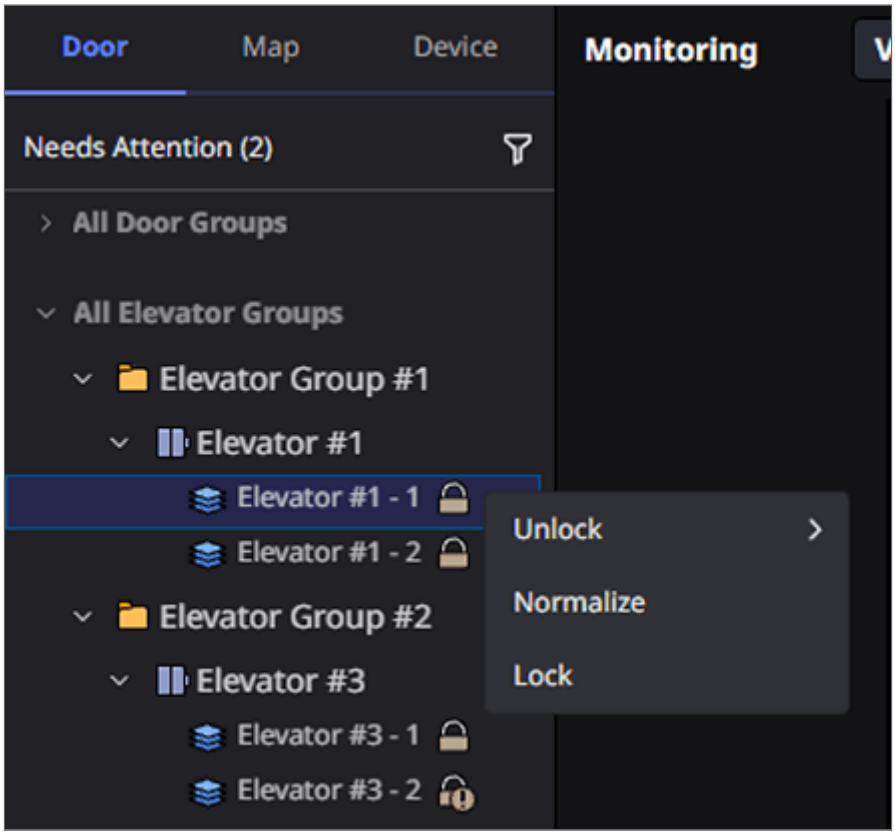


- **Normalize All Floors**: Use this when an administrator manually opens or locks all floors.
- **View Details**: You can check the name, location, status information, and more for the elevator.
- **Recent Events**: You can check the recent event list that occurred at the selected elevator.

> **Info**
> For more information about each item in the elevator details section, see Register Elevator.

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

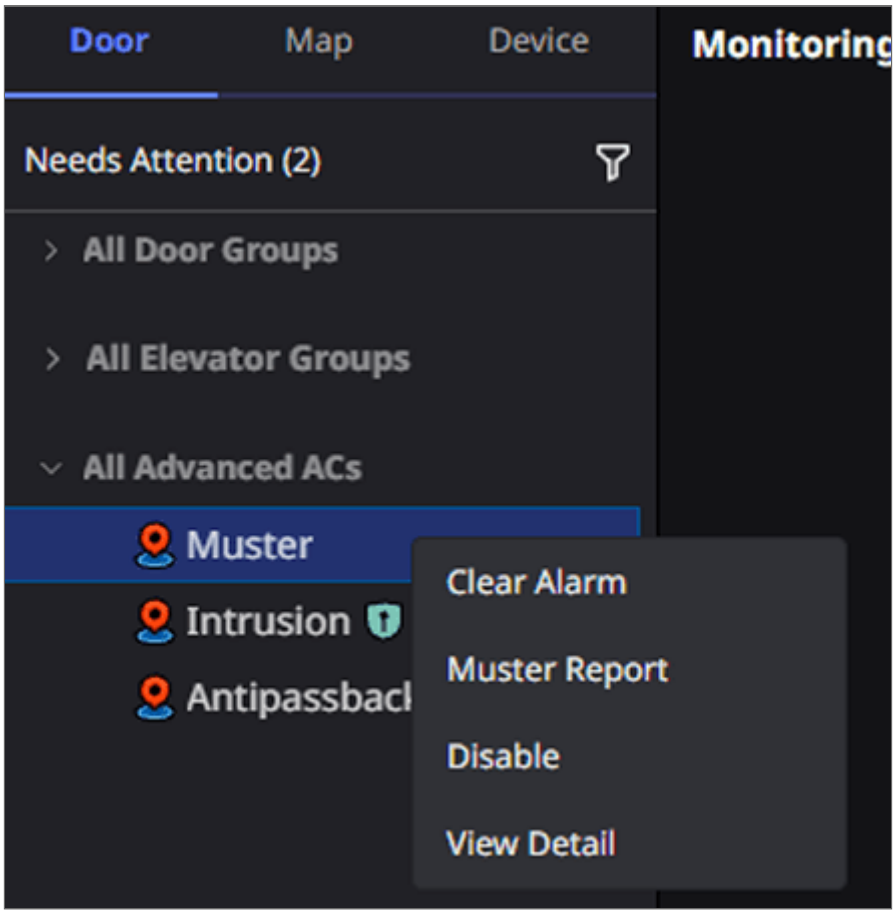
Changing the floor to **Lock** status will prevent anyone from access. Click **Lock** in the popup menu.

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
  - Roll Call
- For more information on each advanced access control feature, see Advanced Access Control Settings.
- To select and control multiple advanced access control settings at once, see Bulk Control.

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 on **Anti-Passback** settings, see Anti-passback.
- For more information on **Anti-Passback**, see Glossary.

Clear alarm

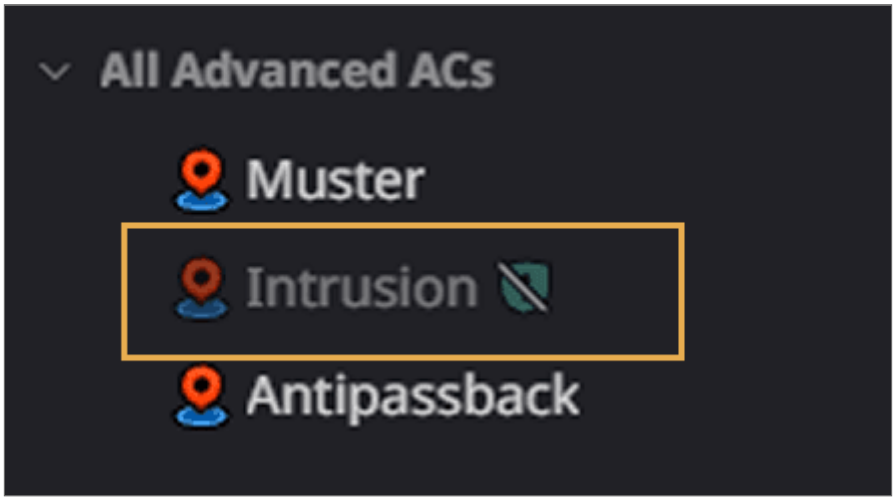
You can clear the alarm that occurred at the door or device. Click **Clear Alarm** in the popup menu. A completion message appears at the top of the screen.

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 appears dimmed. 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 intrusion alarm settings, see Intrusion Alarm.

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 on the muster feature, see Muster.

Monitoring occupancy limit

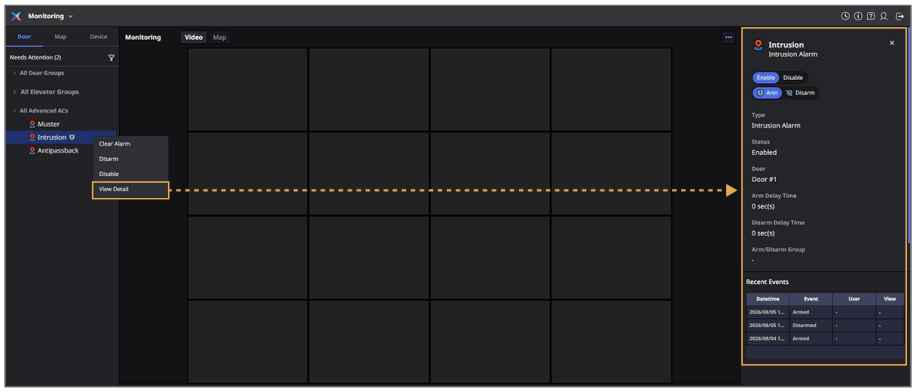
You can check the status of devices set with the occupancy limit feature. Click **Occupancy Monitoring** in the popup menu. In the new window, go to the **Settings** → **Access Management** → **Advanced AC** menu. You can check the status in the **Occupancy Limit** list.

Info

- The **Occupancy Monitoring** feature is only available for items set with the occupancy limit feature.
- For more information on occupancy limit settings, see Occupancy Limit.

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.



- **Advanced access control**: Control the selected advanced access control.
- **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

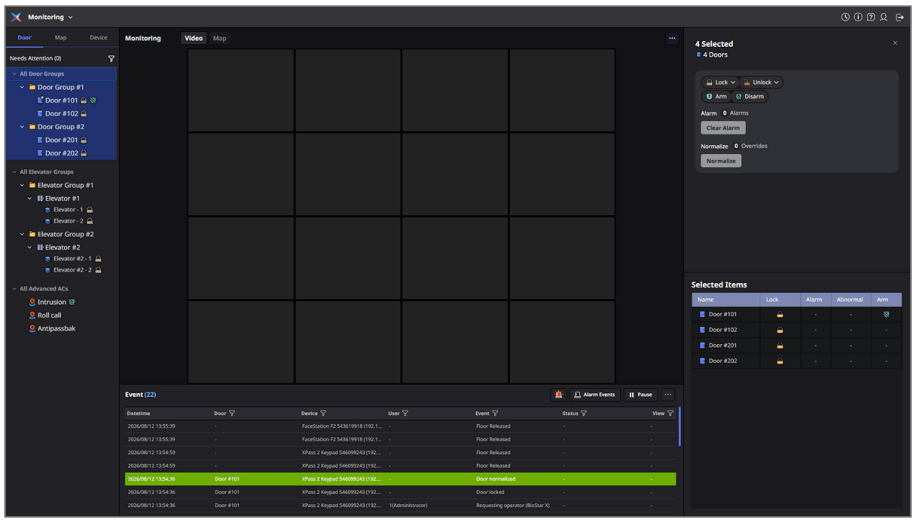
For more information on each item in the advanced access control details section, see Advanced Access Control Settings.

Bulk Control

This guide explains selecting multiple doors, elevators, or advanced access control settings and running Unlock, Lock, or Clear Alarm at once.

- If you select two or more entries in the status tree, the bulk control panel appears on the right side of the screen. Execute commands at once without controlling each entry individually.
- Respond quickly during emergencies or when controlling multiple entrances at the same time.
- Select doors, elevators (floors), or advanced access control settings in bulk and control them. The system does not allow bulk control for mixed types.

Click **Monitoring** on the **Launcher** page or select **Monitoring** from the shortcut list at the top left of the screen. If you select two or more entries in the status tree on the left sidebar, the bulk control panel appears on the right side of the screen.



Info

- Bulk control does not include cameras. If you select cameras with other entries, the system removes them from the selection list.
- This document covers how to control multiple entries at once. To control a single door, elevator, or advanced access control setting, see the following document.
  - Door Control
  - Control Elevators
  - Control Advanced Access Control

Select multiple entries

To select doors, elevators, floors, or advanced access control in the status tree on the left sidebar, do the following. This works the same way as selecting multiple files in Windows File Explorer.

- **Click**: Select one entry. This clears the previous selection.
- `Ctrl` + **Click**: Add the clicked entry to the selection list or remove it. This keeps the remaining selection.
- `Shift` + **Click**: Select the visible range from the last clicked entry to the current entry. Replace the current selection with this range.
- `Ctrl` + `Shift` + **Click**: Add a range without clearing the current selection. Use this to select multiple nonadjacent entries.
- **Click a group**: Click a group ( ) name to select all doors, elevators, floors, and advanced access control settings under it. To expand or collapse a group, click the arrow (›) before the group name.

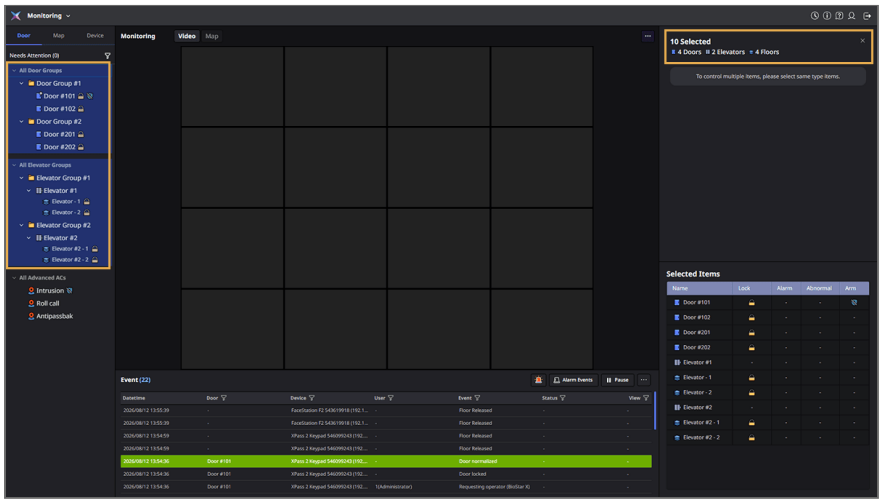
> **Info**
>
> The bulk control panel does not open when none or only one entry is selected. When only one entry remains selected, its view detail appears. When all selections are cleared, the right panel disappears.

Bulk control panel layout

Select multiple entries in the status tree on the left sidebar. The bulk control panel appears on the right as follows.

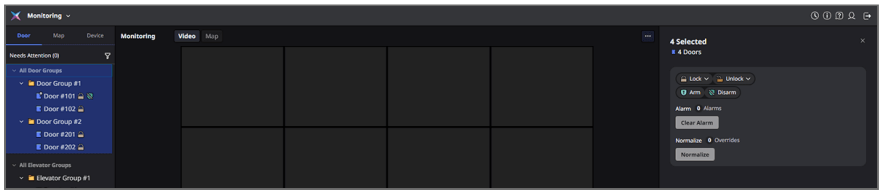
- **Selection count and types**: For example, if you select 4 doors, 2 elevators, and 4 floors, it is displayed as follows.

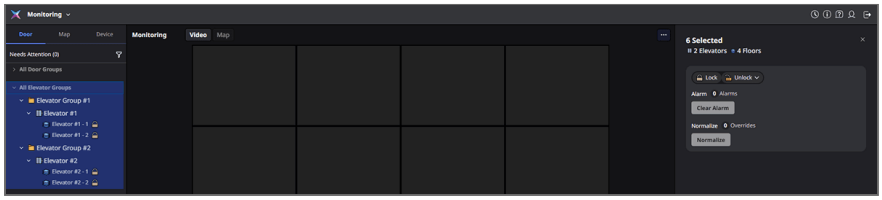
  > ***10 Selected** / **4 Doors 2 Elevators 4 Floors***



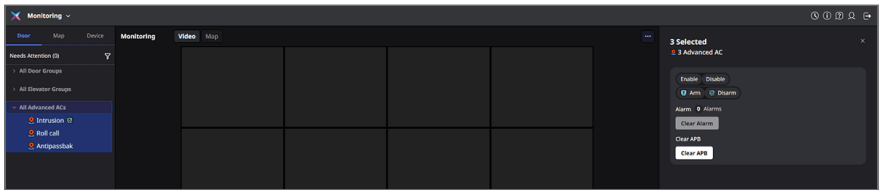
  > Control features are unavailable when you select different types together.

- **Door/Elevator control**: Shows control features available for doors and elevators.

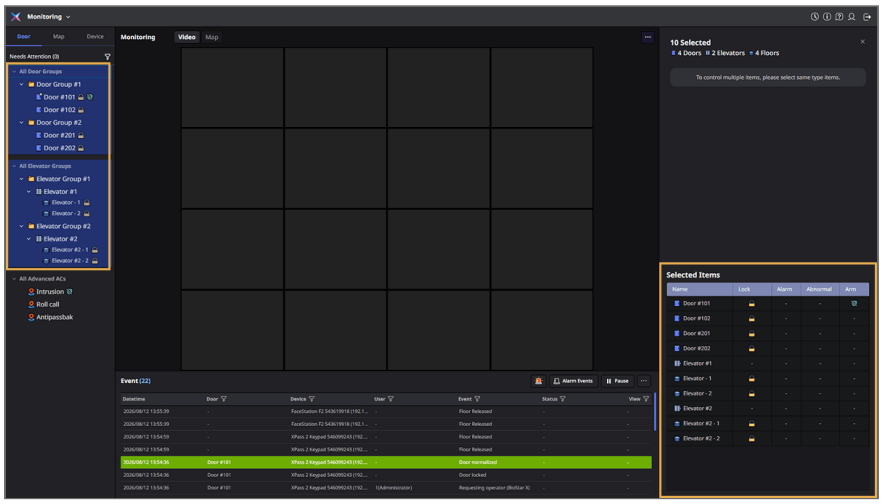




- **Advanced access control**: Shows control features available in advanced access control.

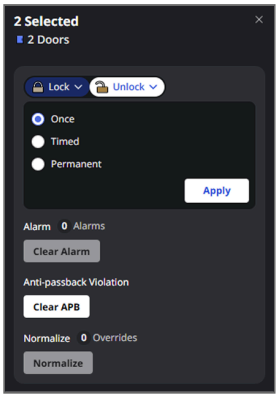


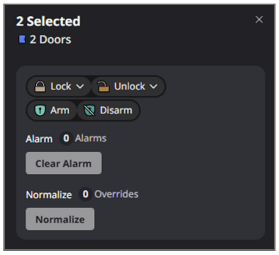
- **Summary table of selected entries**: The bottom of the right panel shows the name and status of each selected entry. Drag the divider between the control area and the summary table up or down to adjust their heights. If many entries are selected, drag the divider to expand the summary table area.



Bulk door control

When at least two doors are selected, use the same basic and advanced controls as single-door control.





Basic control

- **Once**: Applies the unlock state once.
- **Timed**: Keeps the locked or unlock state for the specified time.
- **Permanent**: Sets the locked or unlock state regardless of time.

Select a command to apply, and click **Apply**.

Advanced control

Use the following buttons when at least one selected entry meets the conditions below.

- **Clear Alarm**: Available when at least one selected door has an active alarm.
- **Clear APB**: Available when at least one selected door has anti-passback enabled. For more information, refer to Door Control.
- **Normalize**: Available when an administrator manually unlocks or locks a door. This excludes statuses changed by schedules or emergencies.
- **Arm** / **Disarm**: Appears only when a door is set to intrusion alarm, an advanced access control setting.

Info

- Click **Clear Alarm** or **Normalize**. A pop-up appears. In the pop-up, click **Normalize** or **Normalize** to clear it. In contrast, **Arm**/**Disarm** changes the status without a confirmation dialog.
- Advanced access control settings are available by purchasing an add-on with an **Essential** license, or with an **Enterprise** license or higher. For more information on the licensing policy, see License Policy.

Bulk control of elevators and floors

Select an elevator to control all configured floors together. To control only certain floors, select the floors directly.

The differences from doors are as follows.

Control feature	Door	Elevator, floor
Unlock	**Once**, **Timed**, **Permanent**	**Once**, **Permanent**
Lock	**Timed**, **Permanent**	**Permanent**
Normalize	Supported	Supported
Clear Alarm	Supported	Appears when the selection includes an elevator; does not appear when only floors are selected
Clear APB	Supported	Not supported

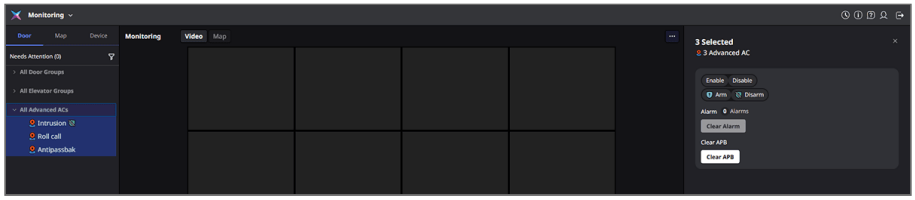
Info

If you select an elevator and its floors, the system sends one unlock/lock command per elevator.

Bulk control of advanced access control

Select multiple advanced access control settings to control them at once. When selecting two or more, the right panel switches to the bulk control panel. Selection, range, and filter actions match doors and elevators.

Advanced access control settings lack lock relays and operator unlock/lock, so control options differ from doors and elevators. The following control buttons appear depending on the selected setting type.



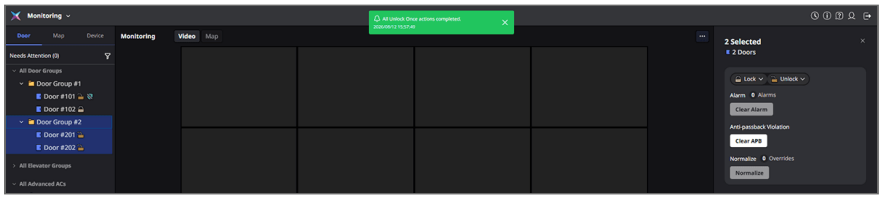
- **Enable**/**Disable**: Appears for all advanced access control settings.
- **Arm**/**Disarm**: Appears only when the selection is set to intrusion alarm.

- **Clear Alarm**: Appears only when the selection includes alarm-triggering settings (anti-passback, fire alarm, schedule lock, intrusion alarm, interlock, or muster). It does not appear when you select only non-alarm settings, such as Occupancy limit or Headcount check.
- **Clear APB**: Appears only when the selection includes the anti-passback setting. Click this button. In the user selection window, select a user who violated anti-passback, and clear the APB alarm. For more information, see Control Advanced Access Control.

> **Info**
>
> - Bulk control does not include **Lock**, **Unlock**, or **Normalize**. The bulk control panel also excludes features that open other screens, such as muster report and occupancy limit monitoring. Use these features on the details screen when one setting is selected.
> - For more information on advanced access control, see Control Advanced Access Control.

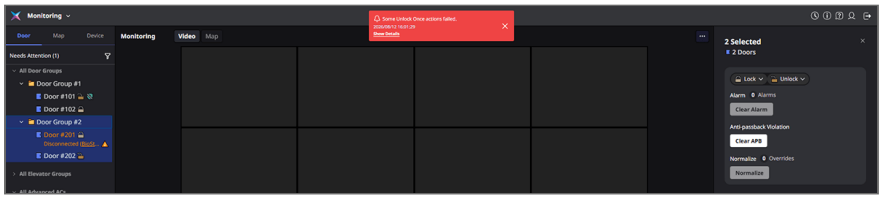
Check execution results

- If all selected entries succeed, a success message appears at the top of the screen.



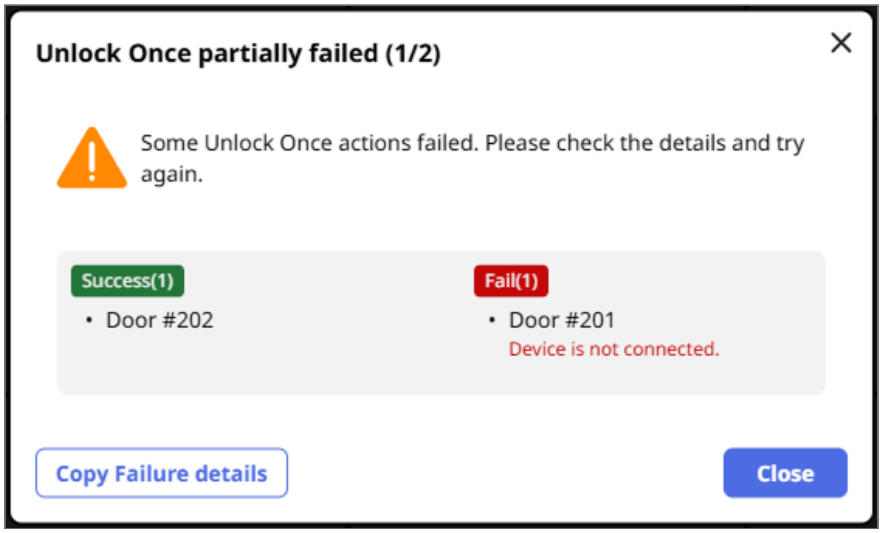
The image above is an example screen and may differ from the actual screen.

- If any entry fails, a failure message appears with the **Show Details** button.



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

Click **Show Details** to view results grouped into **Success**, **Failure**, and **Skipped**. Click **Copy Failure details** to copy the names and reasons for failed entries to the clipboard.



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

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.



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.

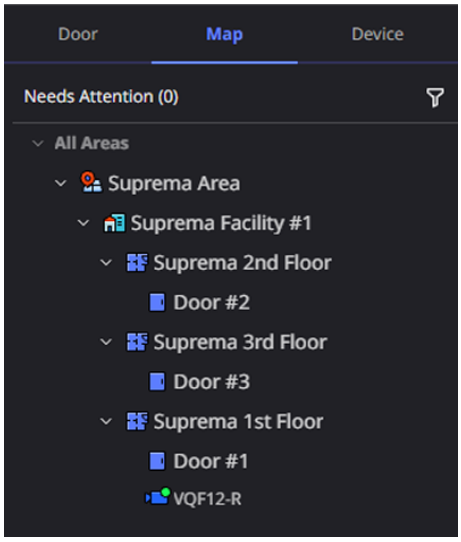
Info

- For more information on configuring the map, see Manage Map.
- The **Monitoring** area remains disabled if the system has no registered device cameras or no registered map components (areas, facilities, or floors).
- The GIS-integrated map monitoring feature is available as an add-on with an **Essential** license or higher. For more information on licensing policies, see License Policy.

Components and options

Map tree components

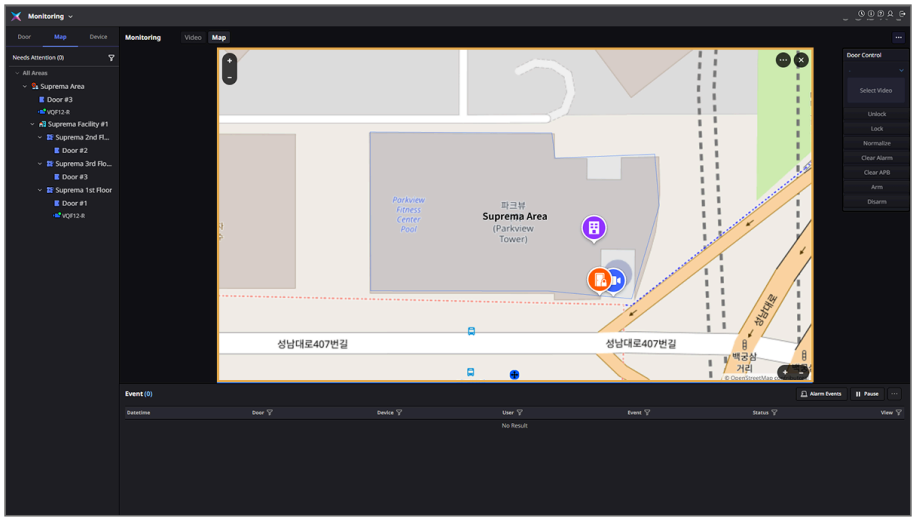
The left sidebar shows the map tree components. Each component icon in the map tree identifies whether it is a zone, facility, floor, door, or camera.



Icon	Name
	Area
	Facility
	Floor
	Door
	Camera

Map area components

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 on the available features, see Door Control.
	**Camera**: Click on the camera to play the video of the corresponding facility or floor.

Component	Description
	**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.
	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.

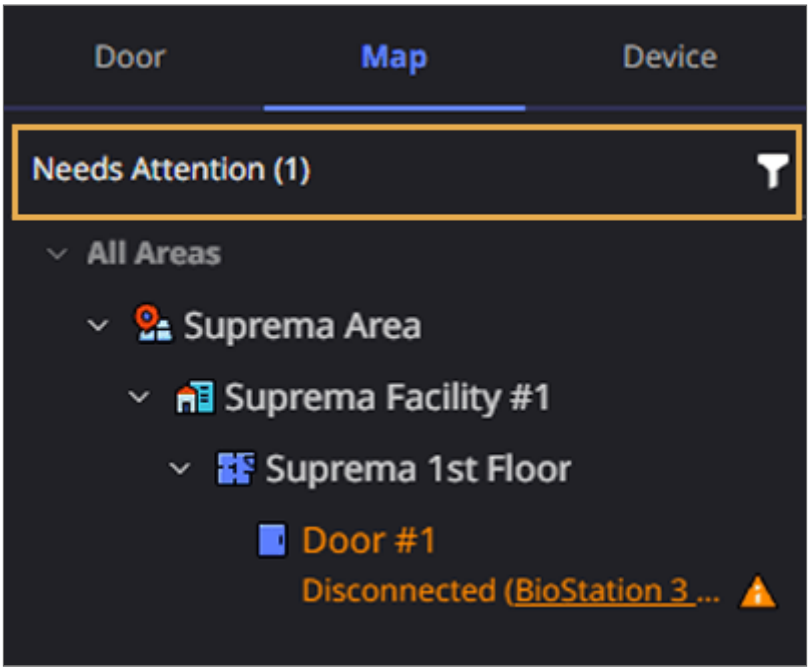
Check status

On 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
	Multi Communications Server error or connection 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.

View entries that need attention

Administrators can filter the list to show only entries that require action. In the left sidebar, click the **Needs Attention**. Check door status by area, facility, and floor, and take action on problem doors.



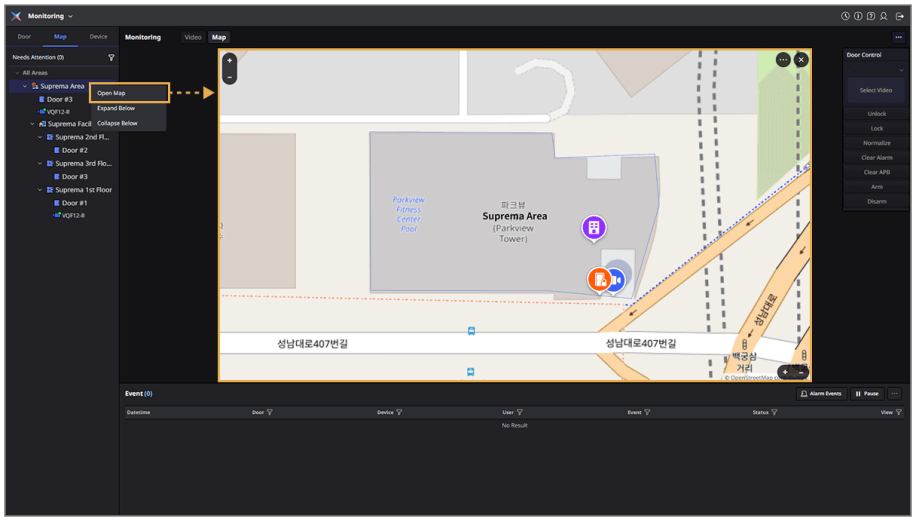
> **Info**
> For the criteria used to determine door actions, see Check status.

Open map

If the area is linked to the GIS map, you can display the map in the **Monitoring** section.

1. On 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.

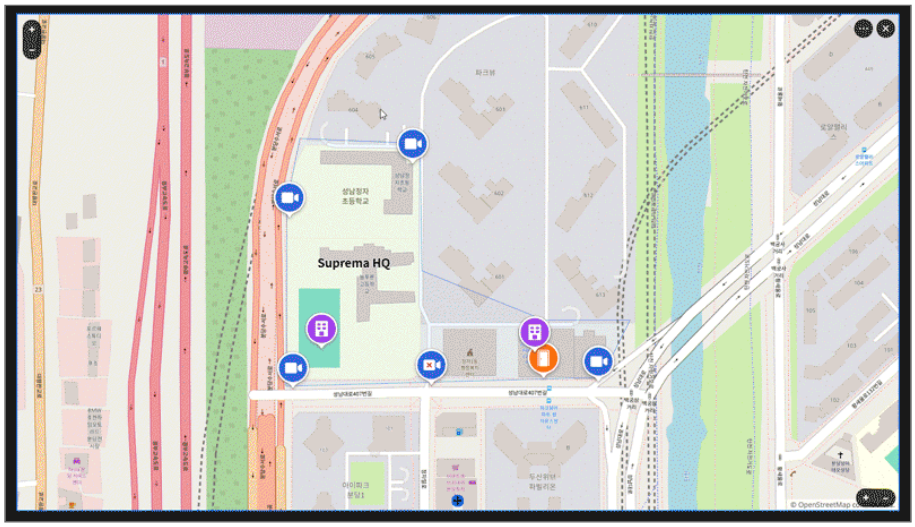


Info

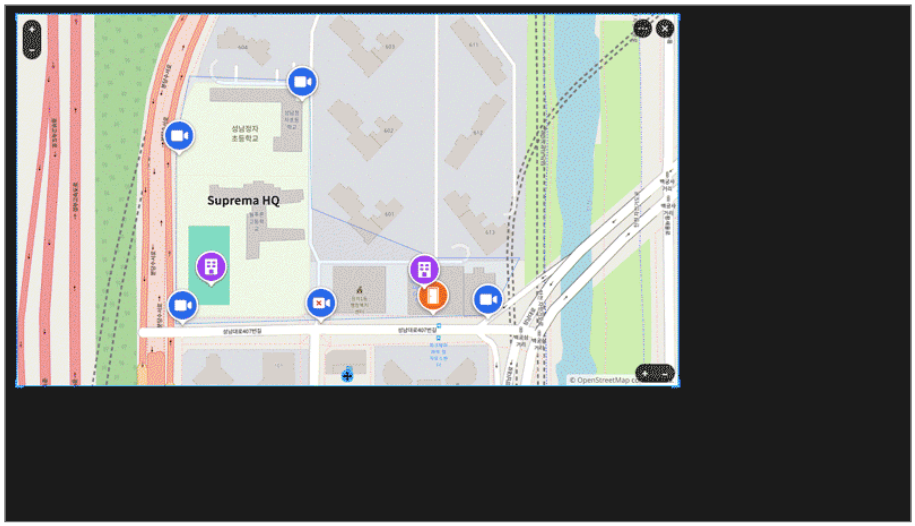
- Double-click the facility on the left sidebar to open the map where the facility is located.
- The image is an example screen. The actual screen may differ.
- For more information on configuring areas linked to the GIS map, see Configure Area.

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.



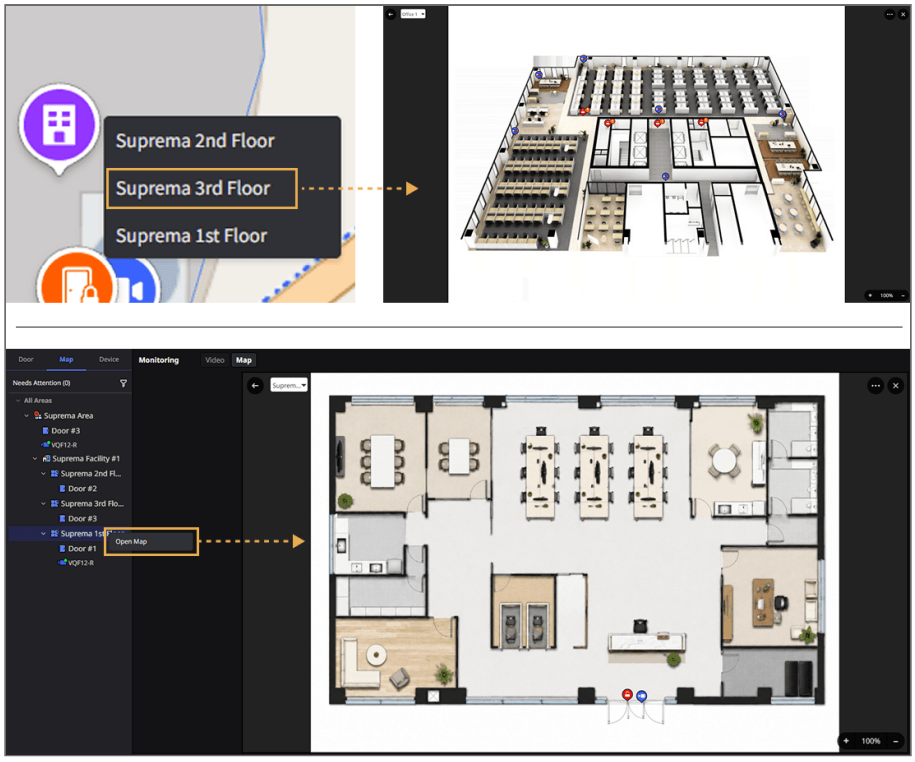
To move the map to another location while resizing, click on the icon over the map and drag it to the desired position.



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.

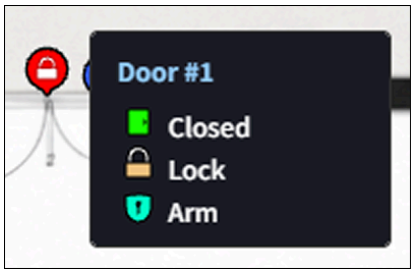
Or, double-click the floor on the left sidebar or right-click it and select **Open Map** from the popup menu.

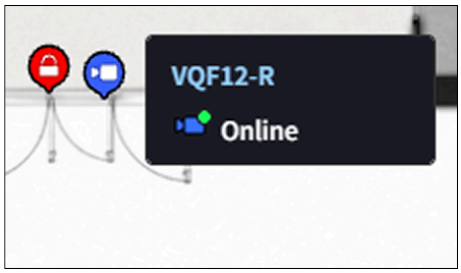


Component	Description
	**Open Door**: The door placed on the floor is in an open state.
	**Locked Door**: The door placed on the floor is in a locked state.

Component	Description
	**Camera**: Click on the camera to play the video of the corresponding facility or floor.

- Hover over a door or camera to check its current status.

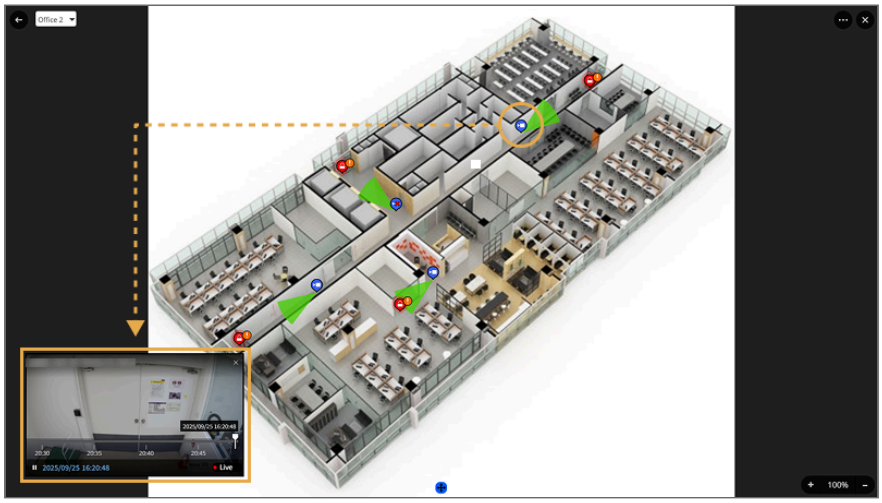




- Clicking the door will display a popup menu that allows you to control that door. For more information on the available features, see Door Control.



- Double-clicking the camera allows you to play the live feed.



Info

- To navigate to the map displaying the facility, click ← at the top left.
- For more information on setting up doors and cameras on a floor (Floor), see Configure Floors.
- For more information on video controls and the tools displayed in the video, see Monitor Video.
- 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.

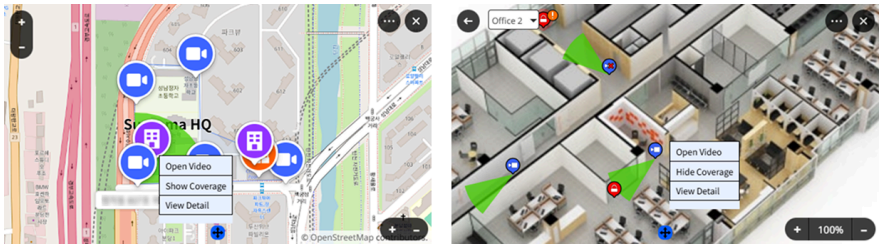


Info

- To navigate to the map displaying the facility, click ← 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 configuring floors within a facility, see Configure Facility.

Controlling camera

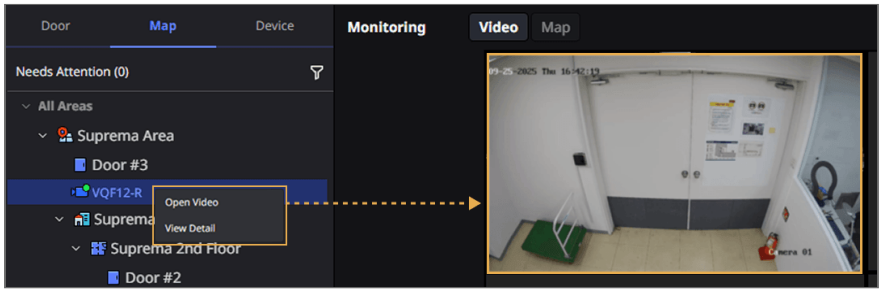
- To control the camera on the map or floor, click the camera icon. Select the desired feature from the pop-up menu.



  - **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 on video controls and the tools displayed in the video, see Monitor Video.
> - If a camera isn't visible on the map, check the camera group's permissions. If the administrator for a custom permission hasn't configured the camera group permissions, the camera may not be visible. For more information on configuring camera group permissions, see Set Up the Camera.

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

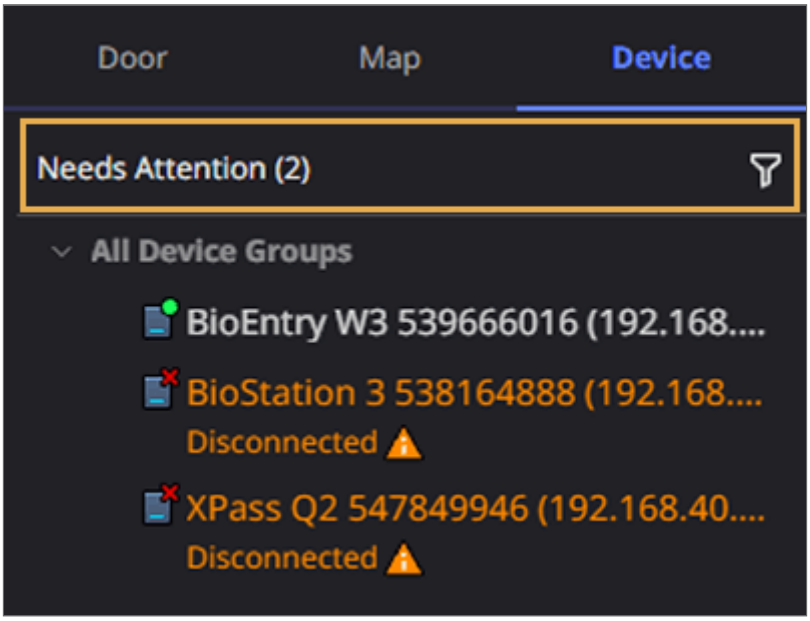
Click the **Device** tab on the left sidebar. You can check the status of all devices and cameras. Refer to the following for the status of devices and cameras.

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

Status Icon	Description
	The camera is off or disconnected.

View devices that need attention

Administrators can view only devices that require action in one list. In the left sidebar, click the **Needs Attention**. Check device status and take action on devices with issues.



Criteria for action-required devices

In the device tree, the system marks abnormal devices as action-required.

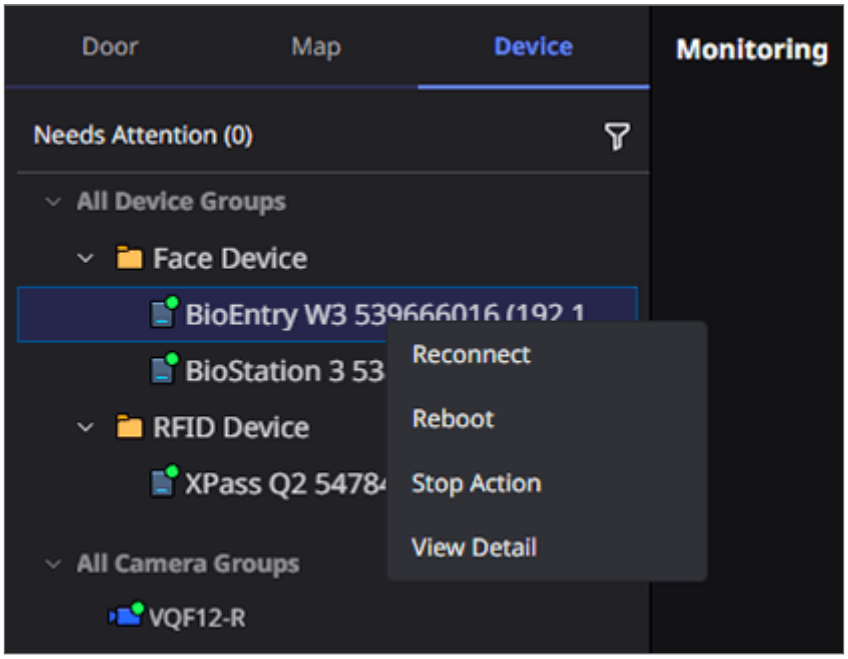
Abnormal status type	Status indicator	Description
Disconnected	**Disconnected**	The device is disconnected from the network
Synchronization error	**Sync Error**	Connected, but data is out of sync
Multi Communications Server error	**Communications Server Error**	An error has occurred on the device's Multi Communications Server
Lock device	**Device Locked**	The device is locked due to job conditions and actions
Authentication failure lockout	**Auth Failure Lockout**	The device is locked after authentication fails more than the specified number of times

Info

- The **Device Locked** condition depends on the job conditions and actions set in Trigger and Action Settings. For information on checking and releasing this status, see Unlock the device.
- Configure the **Auth Failure Lockout** condition in device settings. For details, see Authentication Settings. For information on checking and releasing this status, see Clear authentication failure lockout.

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.



The control features shown may vary depending on the device type.

Device type	Control feature
Master device, a primary device that connects directly to the server without slaves	**Stop Action**, **Reboot**, **Unlock Device**, **Release Auth Failure Lockout**, **Reconnect**(only when the server connects to the device)
Slave device	**Stop Action**, **Reboot**, **Unlock Device**, **Release Auth Failure Lockout**
OSDP communication device	**Unlock Device**, **Reconnect** (depends on the connection method)
Wiegand device	**Unlock Device**
Expansion modules (Secure I/O 2, DM-20, OM-120, IM-120)	**Stop Action**
Devices using device-to-server connections	**Stop Action**, **Reboot**, **Unlock Device**, **Release Auth Failure Lockout**

Device type	Control feature
Wireless antenna module	None

Reconnect device

Regardless of the device connection status, click **Reconnect** in the popup menu. Use this to reconnect disconnected devices, or resend settings and clear abnormal states on connected devices. When the device reconnects, the status icon changes to normal status ( ).

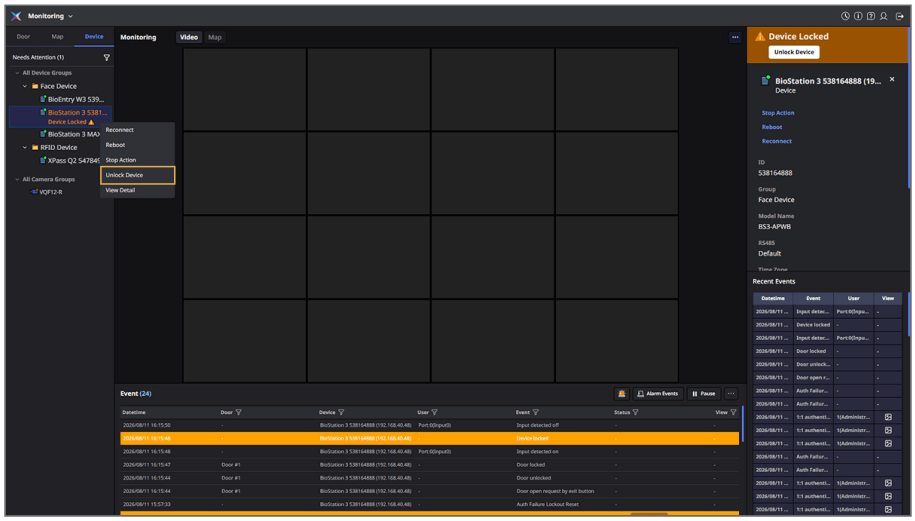
> **Info**
>
> The **Reconnect** feature does not support devices set to the **Device ▸ Server Connection** option. For more information on registering devices, see Register Device.

Restart device

To restart the device, click **Reboot** in the popup menu. When the warning message window appears, click **Ok**.

Unlock the device

When the device locks based on admin-defined conditions, **Device Locked** appears under the device name in the left sidebar. Selecting the device shows the same banner at the top of the right preview panel.



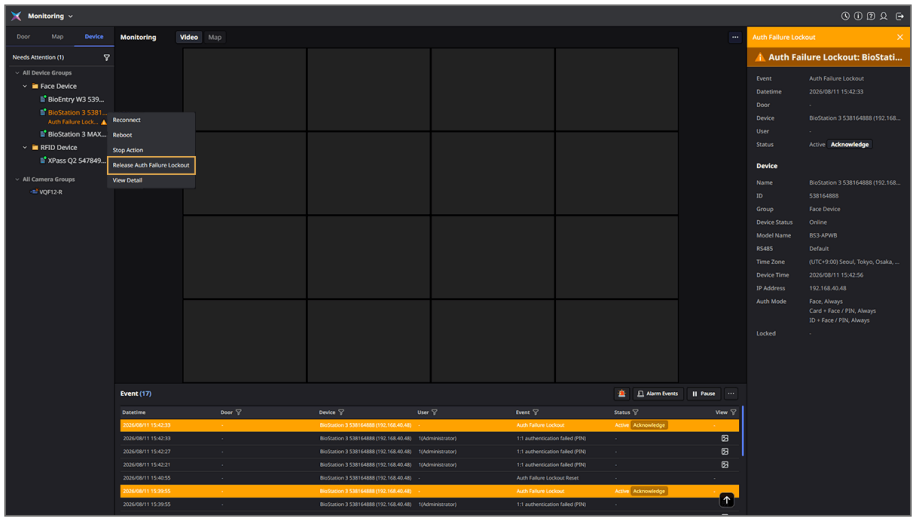
- The popup menu shows **Unlock Device** only when the device is locked. Select the locked device, then click **Unlock Device** in the popup menu.
- Select the locked device. In the banner at the top of the right preview panel, click **Unlock Device**.

> **Info**
>
> Only users with **Administrator** or **Monitoring Operator** privileges see **Unlock Device**.

Clear authentication failure lockout

If authentication fails the number of times set in **Auth Failure Lockout**, the device switches to the locked state. When the device is in authentication failure lockout, **Auth Failure Lockout** appears under the device name in the left sidebar. Selecting the device shows the same banner at the top of the right preview panel. The banner shows the event time and device information.

The popup menu shows **Release Auth Failure Lockout** only when the device is in authentication failure lockout. Select the locked device, then click **Release Auth Failure Lockout** in the popup menu.



Info

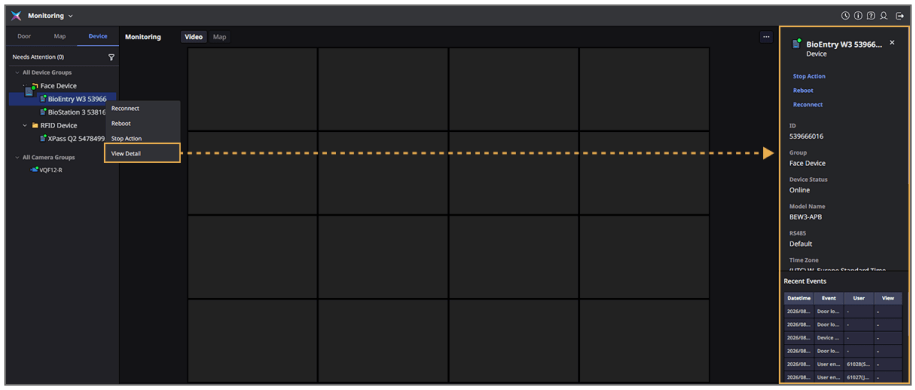
- Only users with **Administrator** or **Monitoring Operator** privileges see the **Release Auth Failure Lockout** menu.
- After the set lockout time (**1st Lockout Duration**/**2nd Lockout Duration**) elapses, the device unlocks automatically. The lockout clears without additional action. For more information on lockout conditions and lockout time settings, see Authentication Settings.

Stop action

To stop all alarm-based and trigger-based actions running on the device, click **Stop Action** in the context menu. A success message for stopping the action will appear at the top of the screen.

Device detailed view

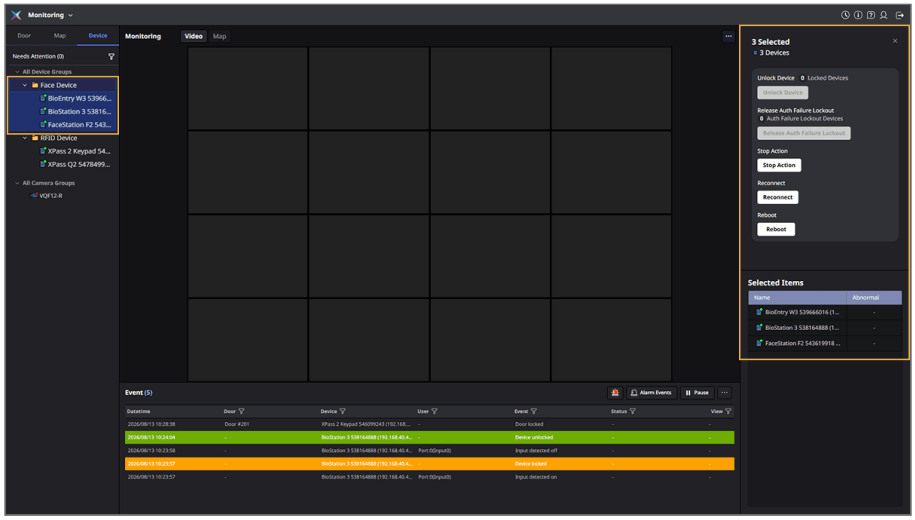
To view detailed information about the device, click **View Detail** in the popup menu. Or double-click the device. The detailed information of the device will appear on the right side of the screen.



- **Device control**: Use controls to stop tasks, restart, or reconnect.
- **Device details**: Check the device ID, group, model name, uptime, and IP address.
- **Recent Events**: View the list of recent events on the selected device.

Control multiple devices at once

This section describes how to select multiple devices and run commands such as reconnect, restart, or unlock. Select two or more devices in the **Device** tab on the left sidebar. The batch control panel appears on the right.



> **Info**
> Bulk control does not include cameras. For camera control, see Controlling camera.

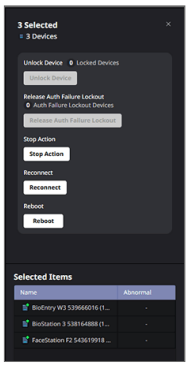
Select multiple devices

Use the following methods to select devices in the **Device** tab on the left sidebar.

- `Ctrl` + **click**: Add or remove the clicked device from the selection list. This keeps the remaining selection.
- `Shift` + **click**: Select a range from the last clicked device to the clicked device. Device groups are excluded from range selection.
- **Click a group (** **)**: Click a group name to add all devices under it to the selection list. Keep currently selected devices selected.

Info

- If only an empty group with no devices is selected, the right panel closes.
- Selecting one device opens the device details panel. Selecting two or more devices switches to the batch control panel.



Batch control panel layout

- **Unlock Device**, **Release Auth Failure Lockout**: These buttons activate when selected devices are locked or in authentication-failure lockout. The target count appears next to each button.
- **Stop Action**, **Reconnect**, **Reboot**: These buttons activate if selected devices support the control. They do not show the target device count.
- **Device control**: Use these buttons: **Unlock Device**, **Release Auth Failure Lockout**, **Stop Action**, **Reconnect**, and **Reboot**.
- **Divider**: Drag the divider between device control and **Selected Items** up or down to adjust each area's height.
- **Selected Items**: Check the connection status, name, and abnormal status of the selected devices. See Criteria for action-required devices for abnormal status types.

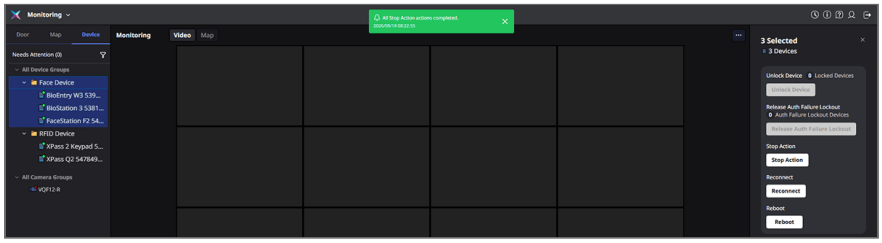
Click each button to open the confirmation dialog. In the confirmation dialog, click **Cancel** to close without executing the selected feature. Click the button for the selected feature to execute it on all selected devices.

Info

If the selection includes different device types, the system shows the combined supported controls. Buttons do not appear for controls that none of the selected devices support. If no controls are supported, only the guidance text and the selected device list table appear.

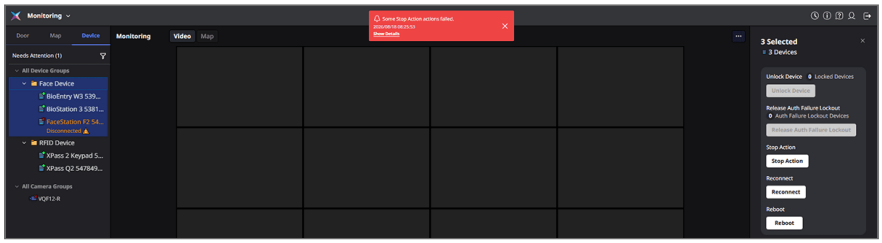
Check execution results

- If all selected devices succeed, only a success message appears.



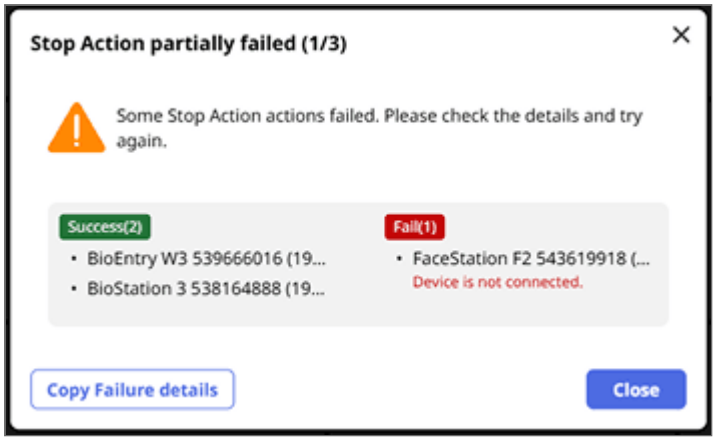
The image above is an example screen and may differ from the actual screen.

- If any device fails, a failure message appears, along with the **Show Details** button.



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

Click **Show Details** to view results grouped into **Success**, **Failure**, and **Skipped**. Click **Copy Failure details** to copy the names and reasons for failed entries to the clipboard.



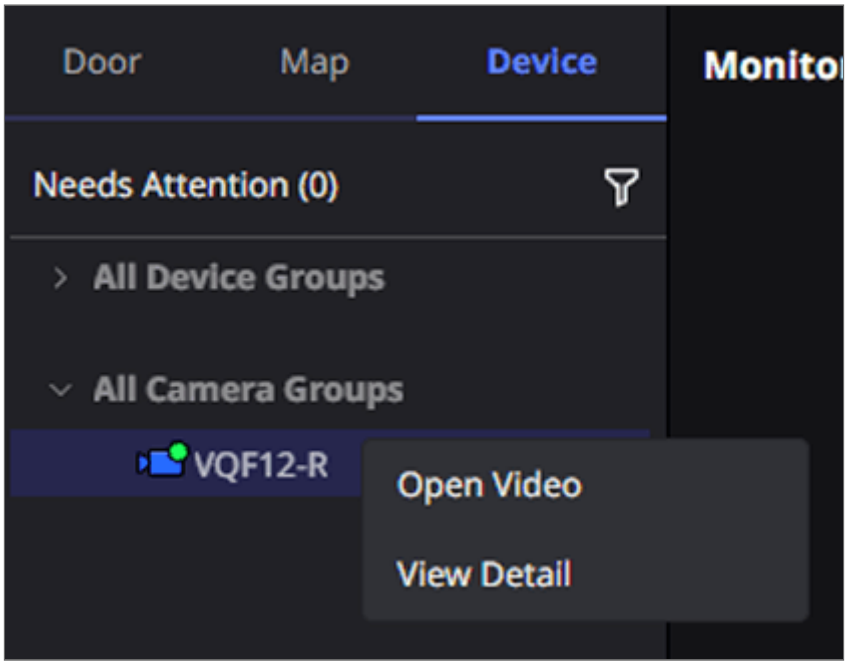
The image above is an example screen and may differ from the actual screen.

Info

- The **Reconnect** button is an exception. After the system accepts the request, only a success message appears. It does not provide failure status or a detailed results window. Check the status tree to confirm whether the connection succeeded.
- **Unlock Device** and **Release Auth Failure Lockout** execute separately, and separate result windows appear.

Controlling camera

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:

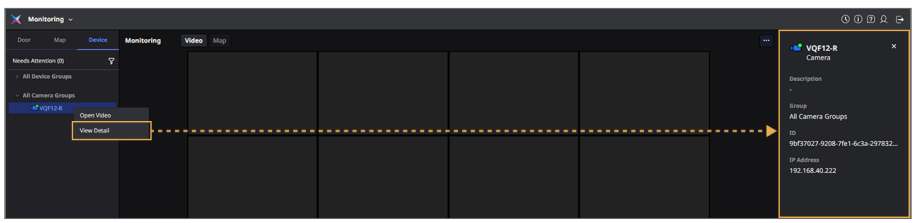
- Double-click the camera to play the video from the camera on the left sidebar.
- You can also add video by dragging and dropping the camera into the video tile area.

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 more information on video controls and the tools displayed on the video, see Monitor Video.
- If a camera does not appear in the **All Camera Groups** list, check the camera group permissions. If the administrator for a custom permission hasn't configured the camera group permissions, the camera may not be visible. For more information on configuring camera group permissions, see Set Up the Camera.

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.

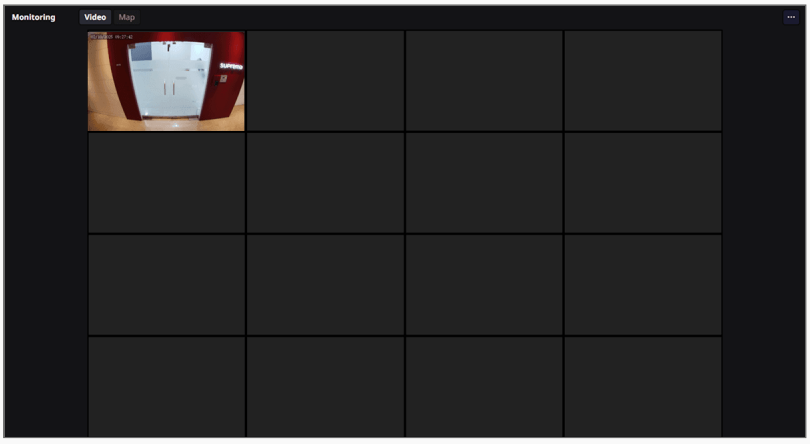


Monitor Video

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.



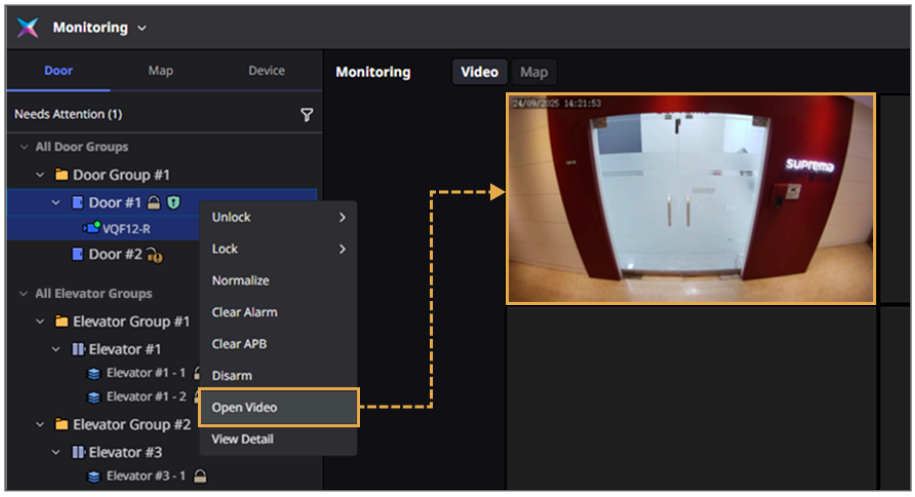
- The **Monitoring** area remains disabled if the system has no registered device cameras or no registered map components (areas, facilities, or floors).
- For more information on integrating with VMS and adding and managing cameras, see Video Settings.
- If a load error occurs when playing back recordings 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
- If cameras associated with this area aren't visible, check the camera group's permissions. If the administrator for a custom permission hasn't configured the camera group permissions, the camera may not be visible. For more information on configuring camera group permissions, see Set Up the Camera.
- Video monitoring is available as an additional option with the **Essential** (Essential) license or higher. For more information on licensing policies, see License Policy.

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.

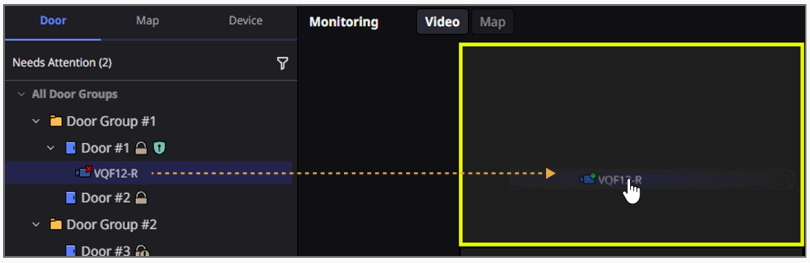
1. Select the camera device you wish to view from the **Door** or **Map**, **Device** tabs on the left sidebar.
2. Right-click.
3. Click **Open Video** in the popup menu.

The selected camera video can be placed in the video tile in the center of the screen.



Info

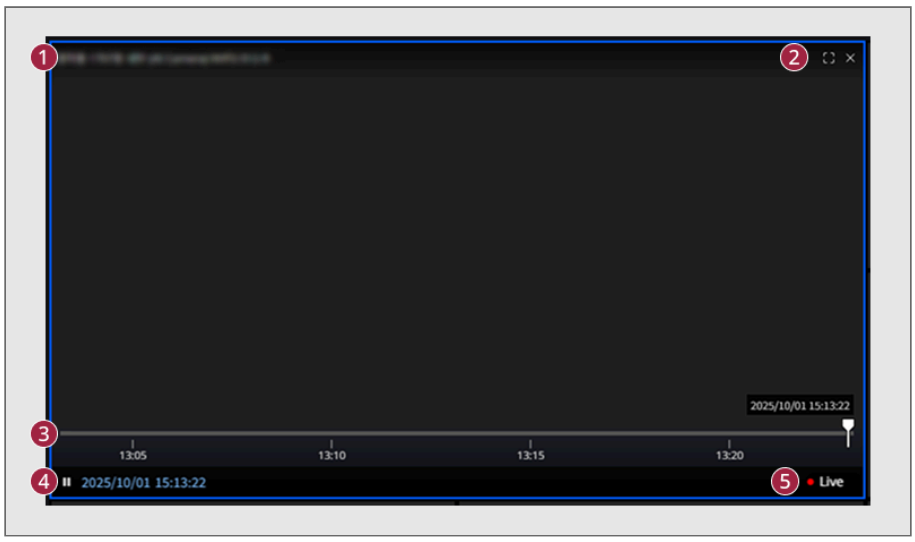
- You can also select cameras from the list in the sidebar and drag and drop them into the video tile area.



- 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.

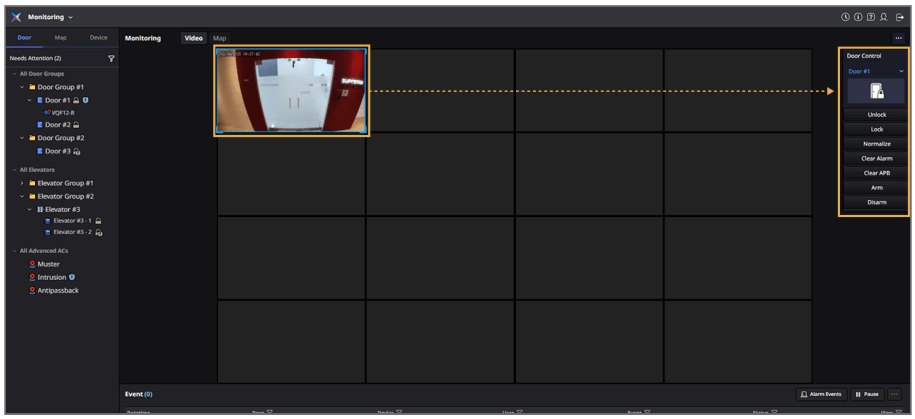
Recorded video playback retention and failure notice

Leave the **Video** tab (for example, go to another page, switch to the **Map** tab, or refresh). When you return to the **Video** tab, it keeps the playback state of the recorded video. Each video tile reloads the video in the order it appears.

> **Info**
>
> Playback failure may appear at different times on each tile because response times vary by video. However, tiles that fail to play tend to appear toward the end of the tile order.

Door control tool

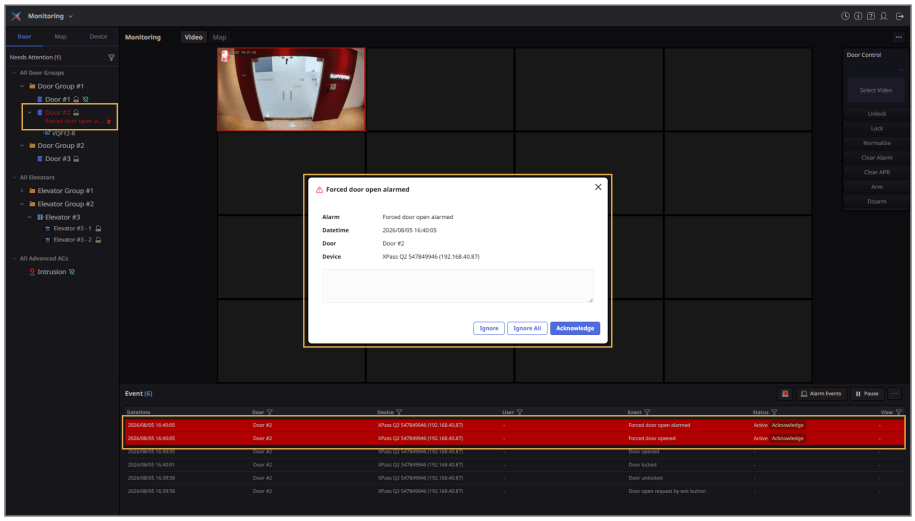
After adding a video, use the **Door Control** tool for additional actions. Selecting the camera linked to the door from the video tile activates the **Door Control** tool that can control the door. You can use functions such as open or lock the door, unlock, and disable the alarm.



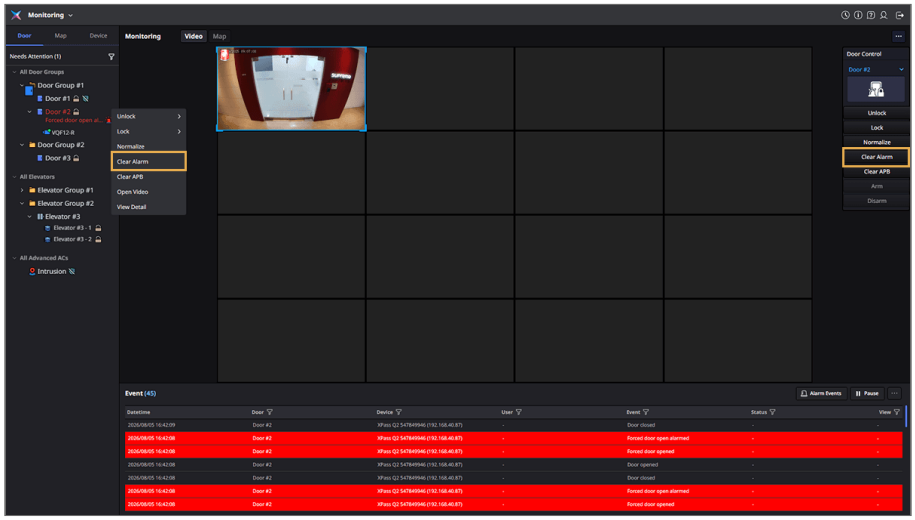
> **Info**
>
> - The **Door Control** tool can be used when there is nothing open in the right panel. If the detailed information is open in the right panel, use it while it is closed.
> - This feature requires a camera to be linked to the door. For more information on linking cameras and doors, see Set Video Rules.
> - For more information on the features available in the **Door Control** tool, see Door Control.

Check video alarm

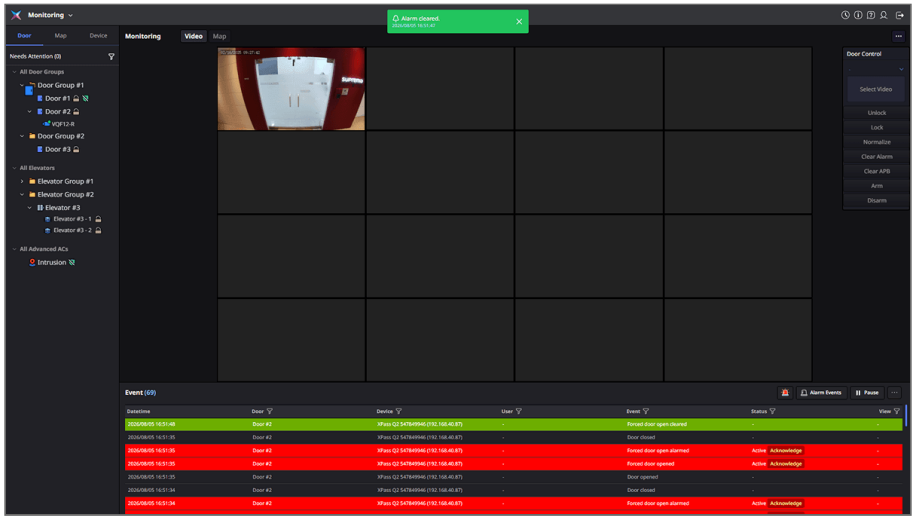
When an alarm state is triggered for one of the doors linked to the camera, an alarm icon appears on the video. All alarms linked to the door must be cleared for the alarm icon to disappear.



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**.



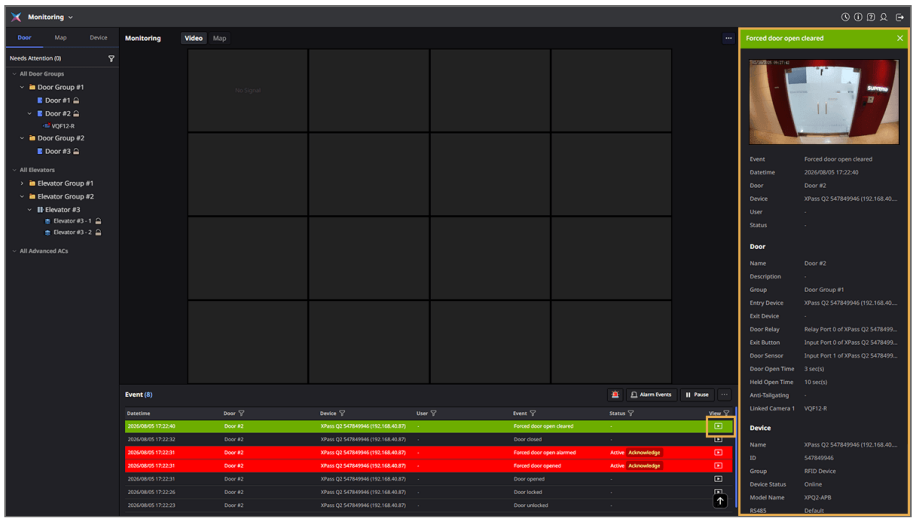
A success or failure message will appear at the top of the screen.



> **Info**
>
> For more information on the **Event** section at the bottom of the screen, see Monitor Event.

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.



Info

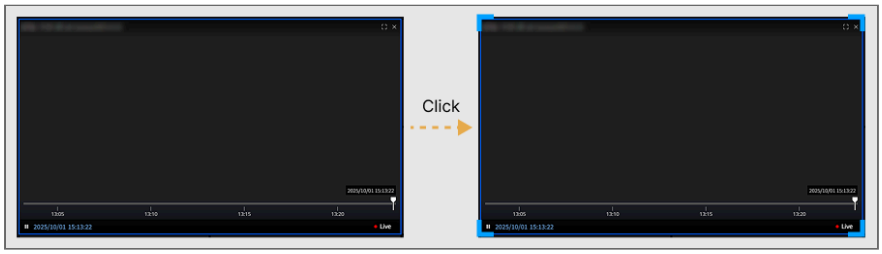
- The video log icon is displayed only when a camera is linked to the door. For more information on linking cameras and doors, see Set Video Rules.
- The first connected camera is prioritized for playback based on event setting rules. To view the video on a larger screen, double-click on it.
- You can 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 on the **Event** section at the bottom of the screen, see Monitor Event.

Set video tile layout

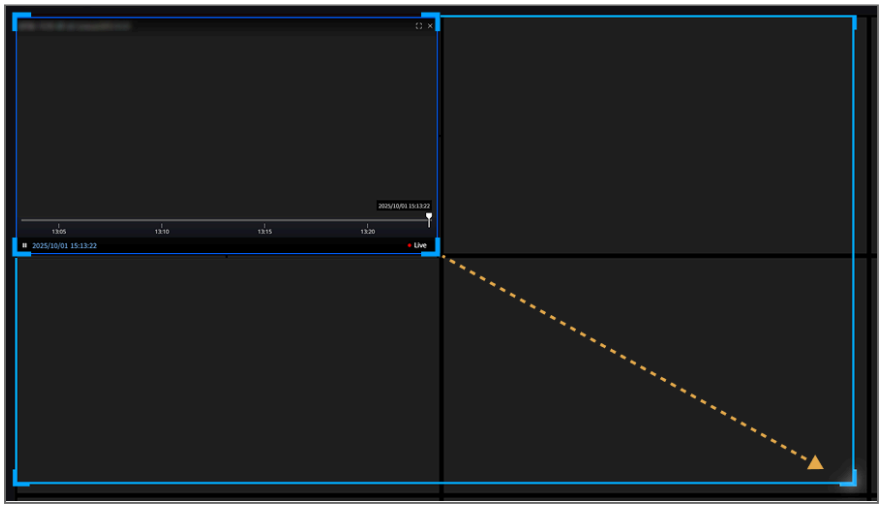
You can resize the video placed in the video tile or reposition it as desired. Adjust the size and position of the video based on its importance for monitoring.

Change video size

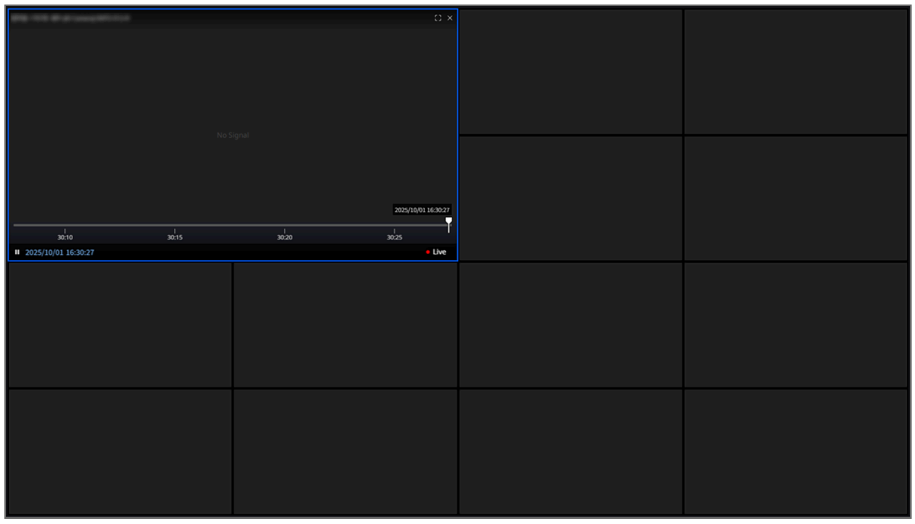
1. Click on the video whose size you want to change to activate the frame of the selected video.



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.

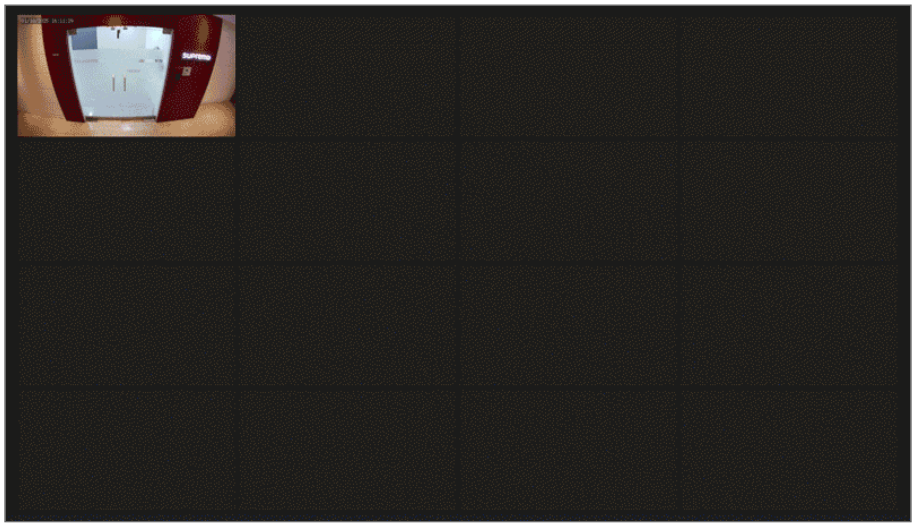


You can resize the video proportionally to the size of the placed tile. Conversely, you can also reduce the size of the video.



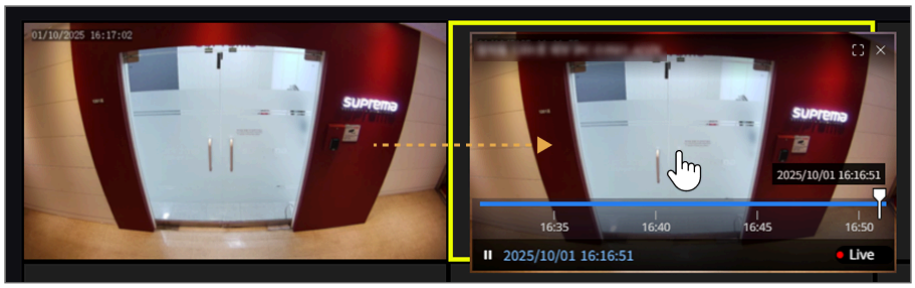
Enlarge video size

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.

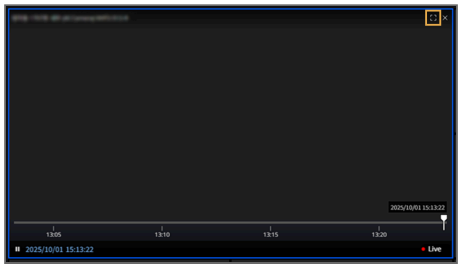


Change video location

Click on the video to move and drag it to the desired location. You can change the position of the selected video.



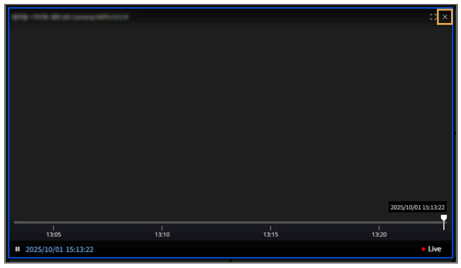
Full-screen view



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 key on the keyboard.

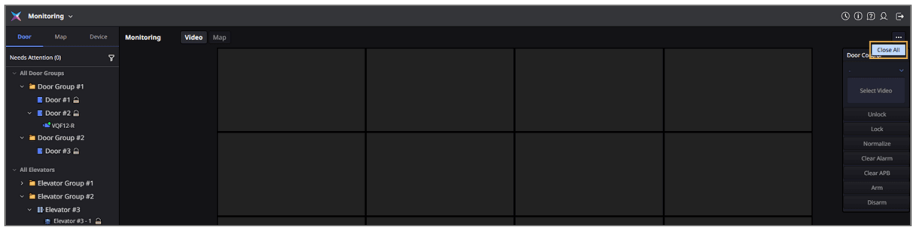
Close video



To close the video placed in the video tile, click ✕ at the upper right of the video.

Close all videos

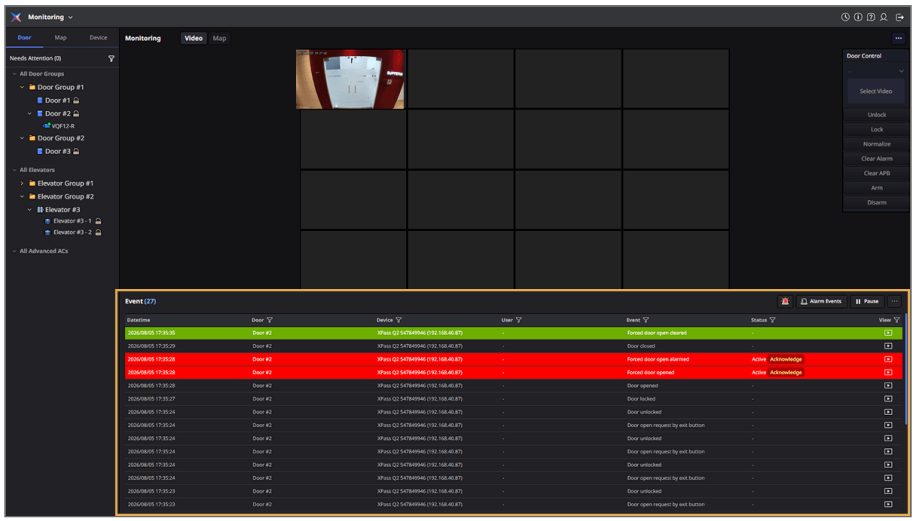
To close all videos placed in the video tile, click ••• at the upper right corner of the screen. Click **Close All** in the popup menu.



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.



Checking the event list

In the **Event** section, you can view events as they occur in real time. Each event includes the following information:



- **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.

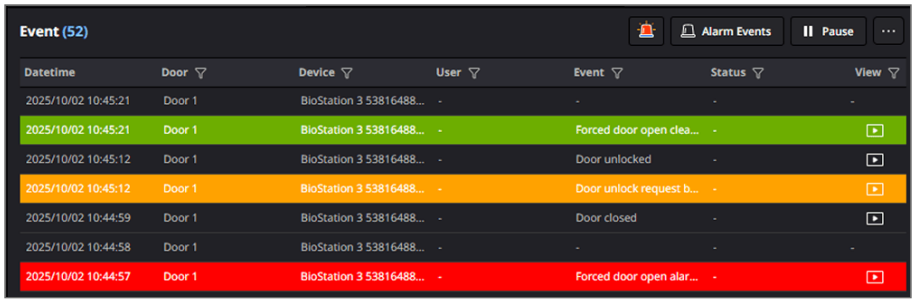


- **View**: If the event includes video information from the camera connected to the door, a video icon (▶) is displayed. Clicking this icon lets you view the video.

> **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

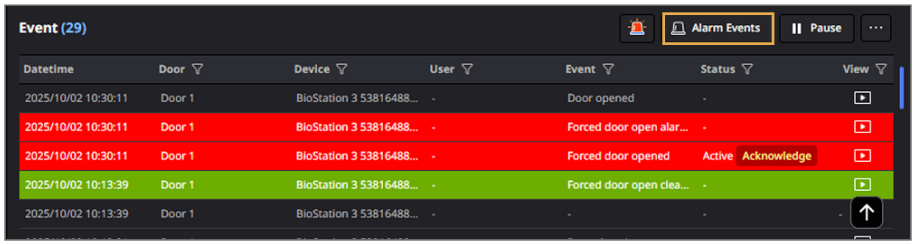
Events in the event list can be distinguished by color:



- **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

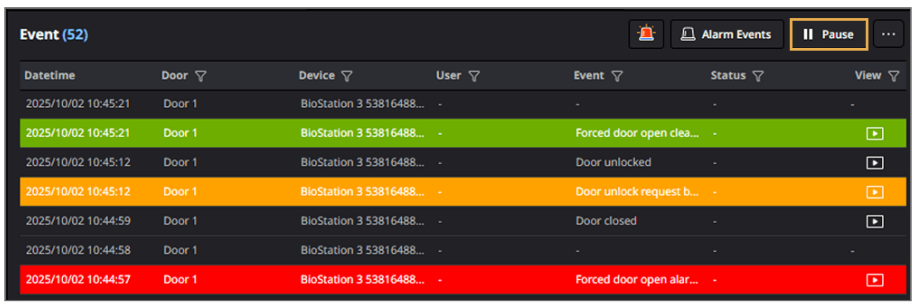
Only alarm events can be viewed in the **Event** section. Click **Alarm Events** in the upper right corner of the **Event** section. The event list will display only alarm events, which are indicated in red. Alarm events are displayed in red.



> **Info**
>
> To view all events, click **All Events** 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.

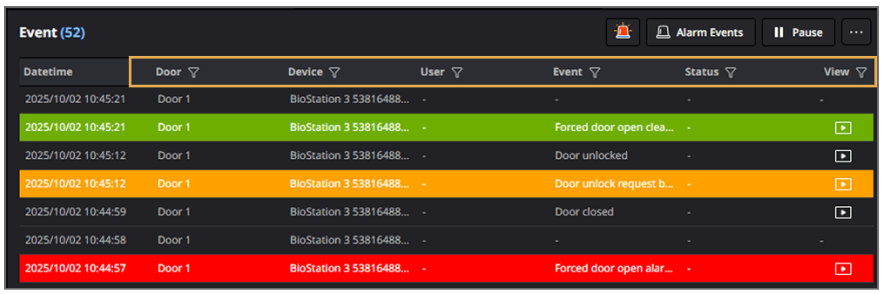


Filtering events

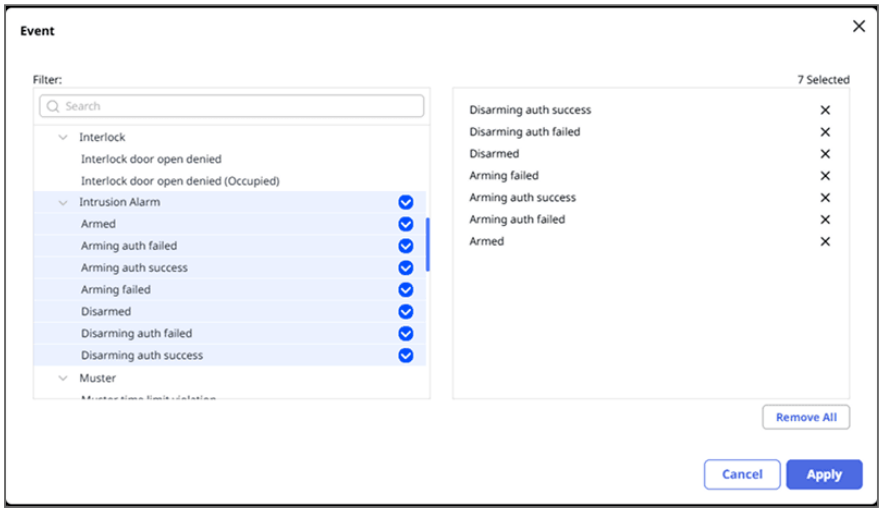
Applying filters

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.



2. When the filter window appears, select the desired item from the left list.



   - Select a parent option to select all child options.
   - Click ✕ to deselect the selected option. To clear all items, click **Remove All**.

3. Once all settings are complete, click **Apply**.

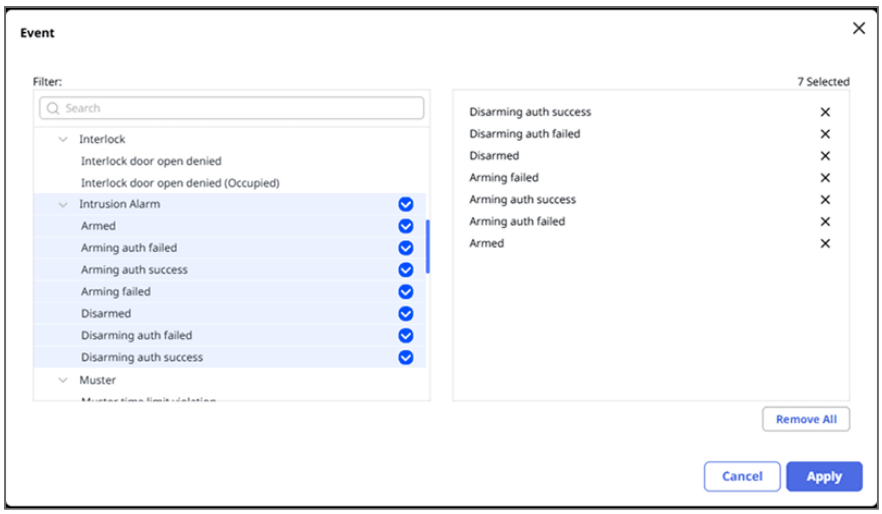
Only events that meet the set conditions will be displayed in the event list.

> **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 you set filter conditions, the ▼ icon in the header column changes color.

Remove filters

You can clear the applied filter conditions.

1. In the **Event** section list, click the ▼ icon on the header column where filters have been applied.
2. When the filter window appears, click ✕ to the right of the option to deselect in the right list. To clear all filters, click **Remove All**.

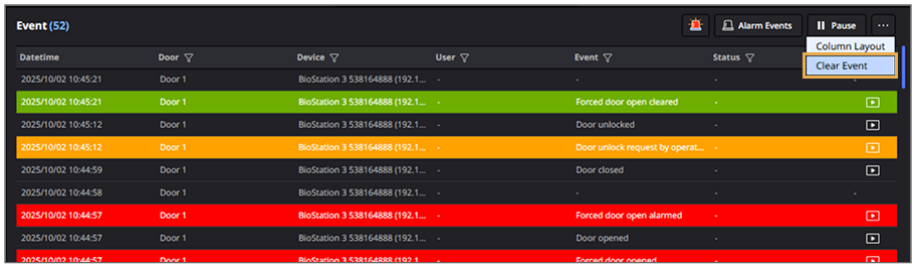


3. Once all conditions to be cleared are set, click **Apply**.

> **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.

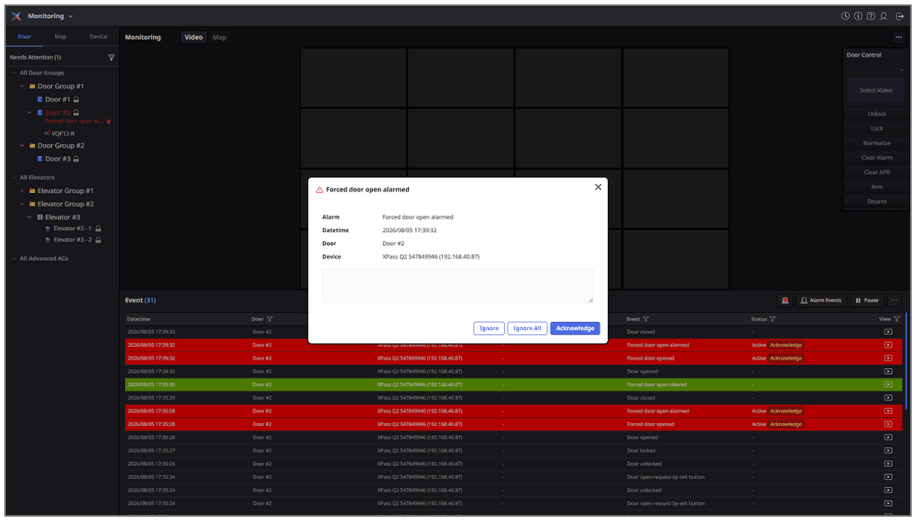
Clear the event list

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.



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.

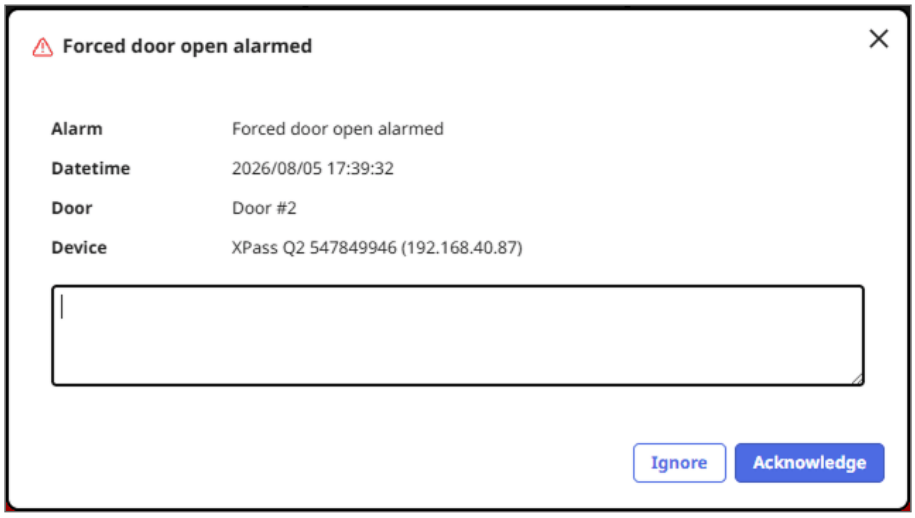


Info

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.



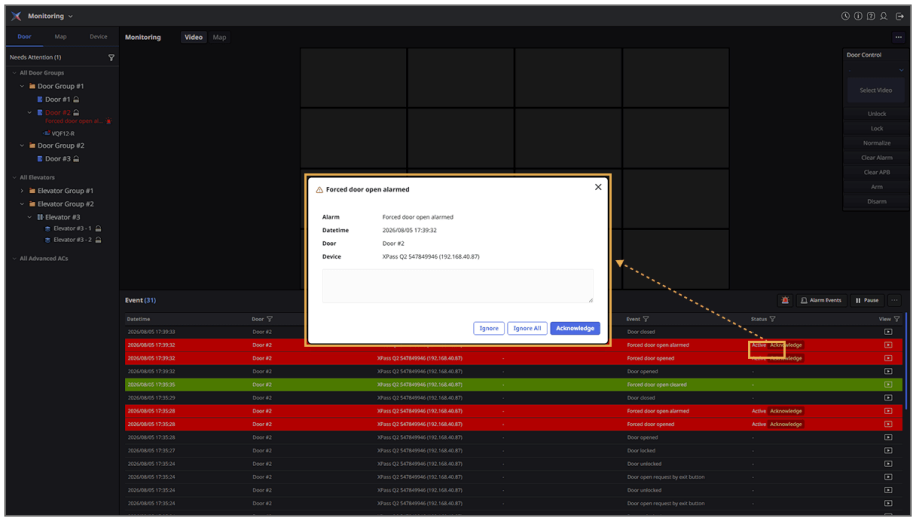
Defer acknowledgment of an alarm event

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.



Checking alarm events in the event list

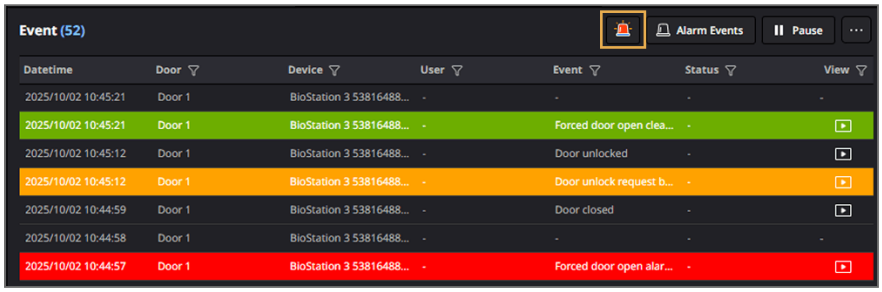
Clicking the **Acknowledge** button displayed in the **Status** column of the event list allows recording of the acknowledgement and actions regarding the triggered alarm events. Complete your entry and click the **Acknowledge** button.



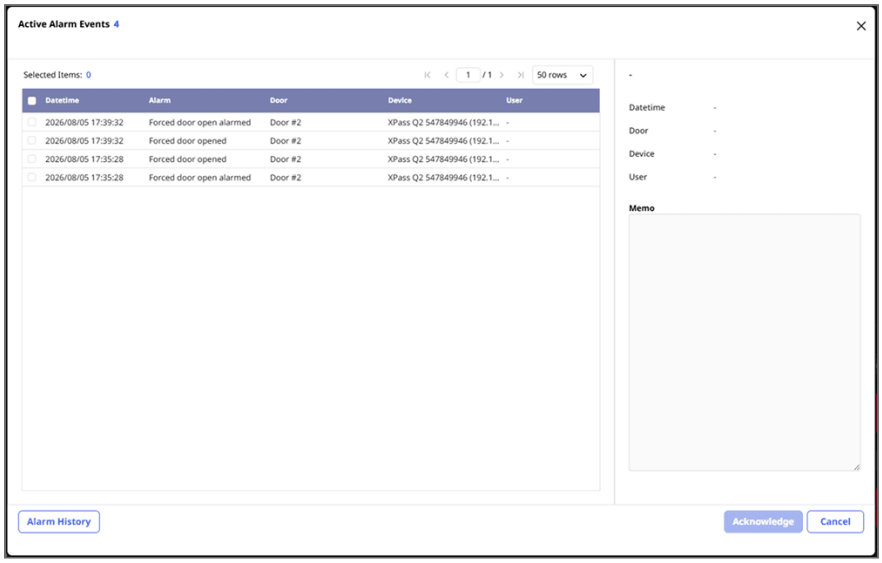
Viewing unacknowledged alarm events

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  in the upper right corner of the **Event** section.



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.



3. Enter actions regarding the alarm event in the **Memo** input field.

4. Click **Acknowledge**.

Records the actions taken for the selected event. A popup window will appear where you can enter your acknowledgement

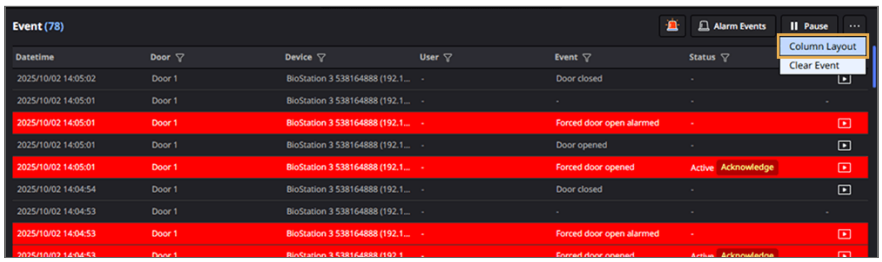
of the alarm event and any actions taken.

> **Info**
> You must select more than one event from the alarm event list for the **Acknowledge** button to be activated.

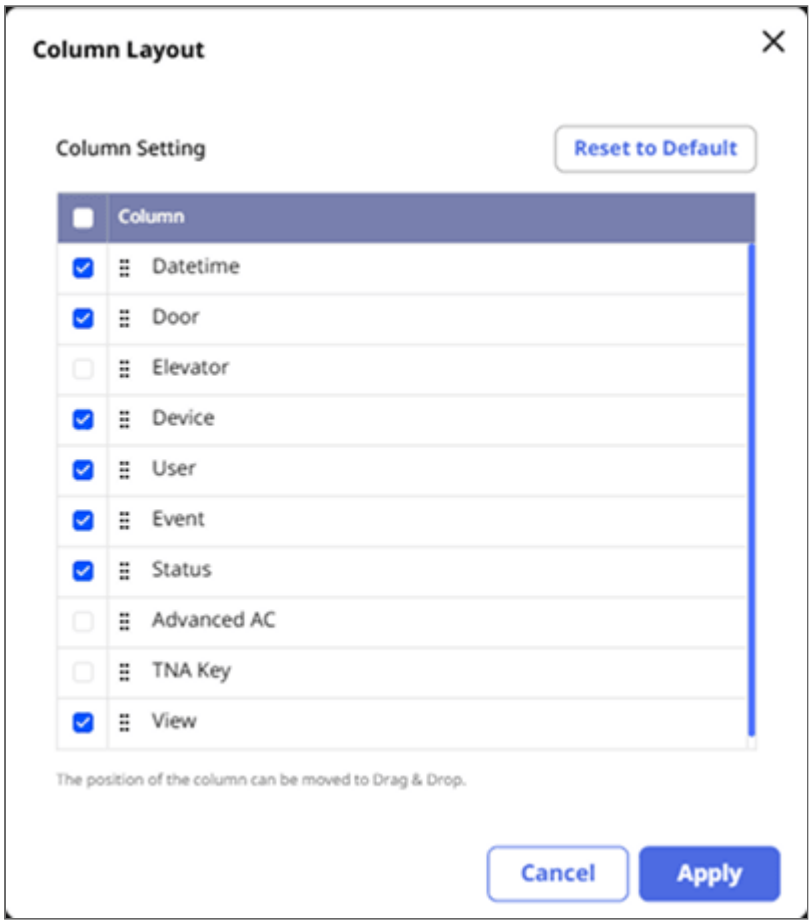
Event list column settings

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.



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.



3. After making all changes to column settings, click the **Apply** button.

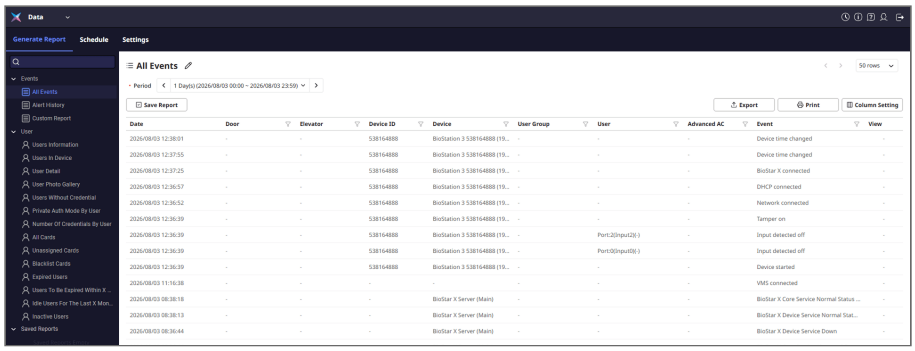
Info

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.



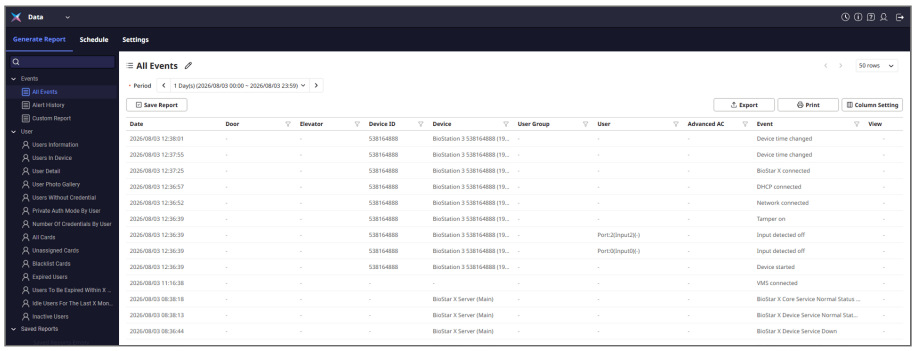
Generate Report

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.

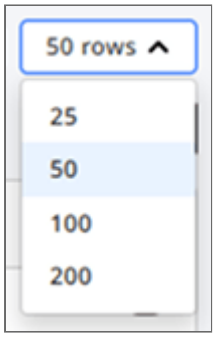
Click **Data** or select **Data** from the shortcut list at the top left of the screen on the **Launcher** page.

View all events

You can view all events that occurred in **BioStar X**. Click **Events** → **All Events** on the left sidebar of the screen.

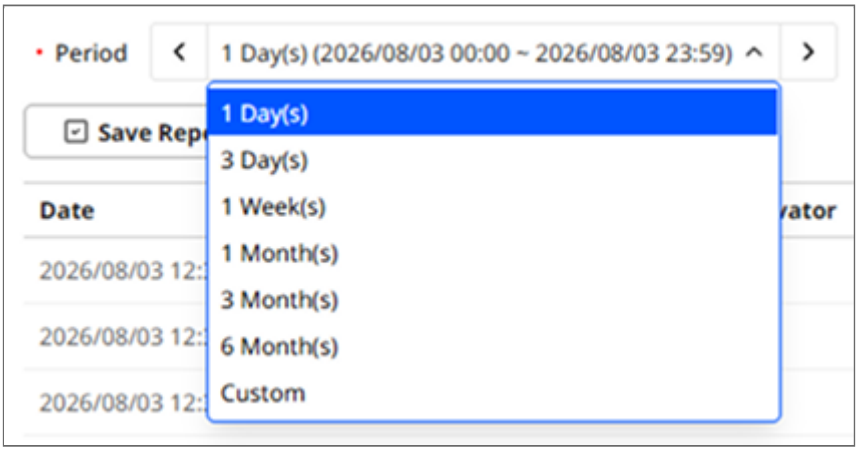


- To check the previous or next page from the listed results, click ‹ or › at the top right of the screen.
- To change the number of rows displayed in the list, click the dropdown menu at the top right of the screen and select your desired value. You can select from a minimum of 25 rows to a maximum of 200 rows.

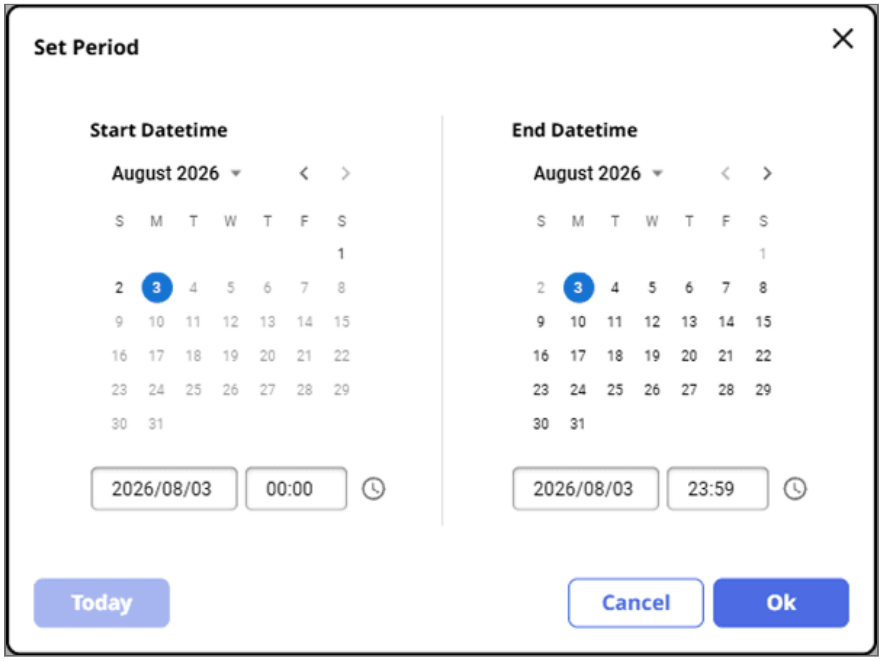


Set period

You can set the desired period in the **Period** option at the top left of the screen. Click the date area.



- 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 **Custom**, 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.

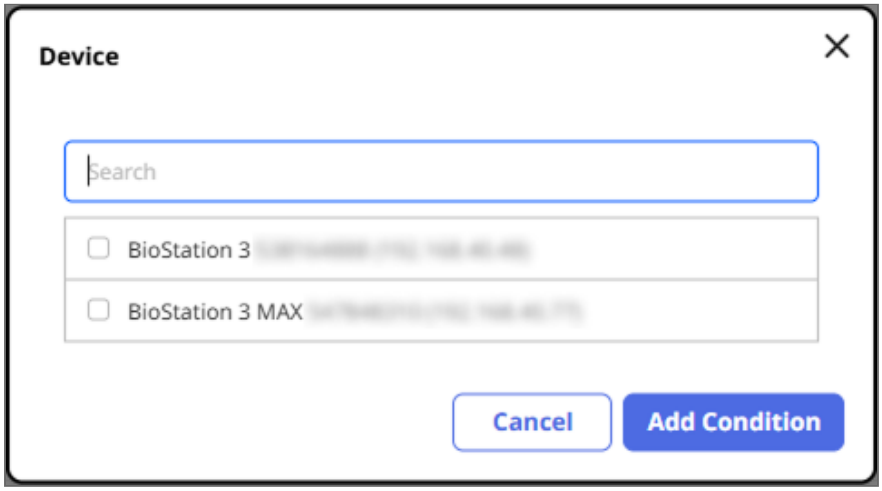


> **Info**
> To select today's date, click **Today**.

Set query conditions

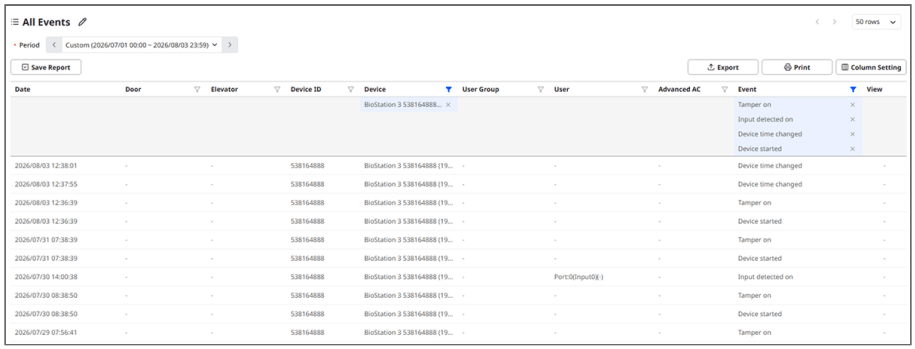
You can filter the list by setting your desired conditions in the header section of the query list. You can set conditions for all items except for dates.

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.



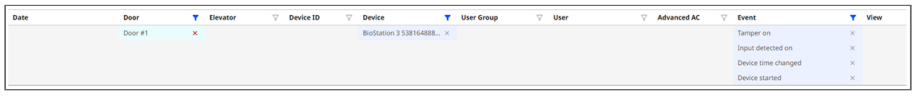
3. Once your selections are complete, click the **Add Condition** button.

Only events matching the selected conditions will be displayed in the list.



Clear query conditions

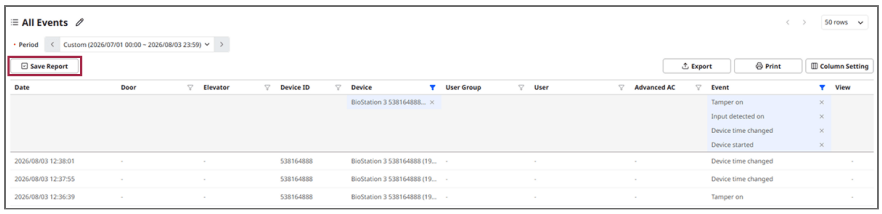
To clear the set query conditions, click the ✕ button in the conditions set below the header section. The set conditions will be cleared, and all events will be displayed in the list again.



Report Save

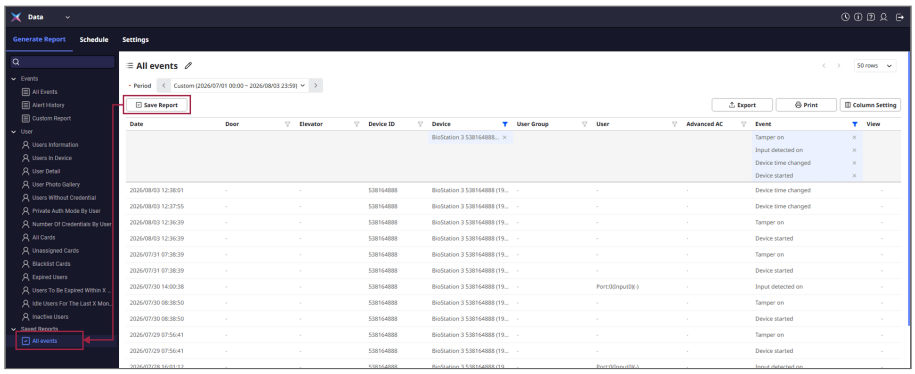
Save events as a report using the query period and conditions you set.

1. Click **Save Report** at the top left of the event list.



2. When a message confirms the report template saved successfully, click **Ok**.

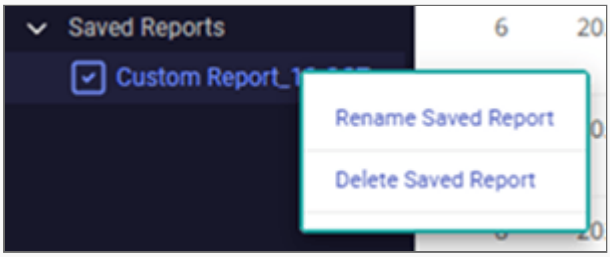
3. Saved reports appear under **Saved Reports** in the left sidebar.



The system stores saved reports as templates for reuse when generating reports under the same conditions.

Info

- Click the ✎ button at the top of the report to edit the title of the saved report, event items, period, and filter conditions.
- The report title can also be changed under **Saved Reports** on 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 on managing reports, see Report management.

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.



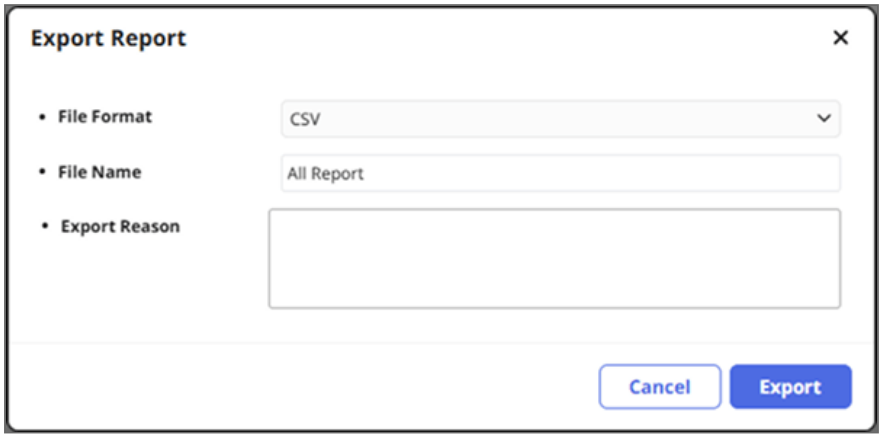
Info

- 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 on setting up camera rules, see Set Video Rules.
- For more information on linking cameras and doors, see Set Video Rules.
- This feature is available by purchasing add-on options with an **Essential** license or higher. For more information on licensing policies, see License Policy.

Export to CSV

You can export the queried event list as a CSV file.

1. Click **Export** at the top right of the screen.
2. When the **Export Report** window appears, select **CSN** from **File Format**.

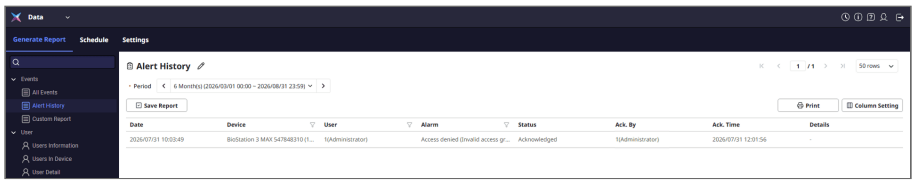


3. You can edit the file name to be saved in **File Name**.
4. Enter **Export Reason** (optional) and click **Export**.
5. Save the CSV file to your desired location on your local path.

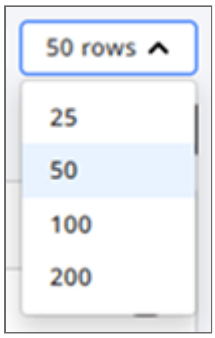
> **Info**
>
> **Export Reason** is optional. Check records for export reasons in **Settings** → **Audit Trail** → **AC Audit Log**.

View alarm history

You can only view alarm (alert) history. Click **Events** → **Alert History** on the left sidebar of the screen.



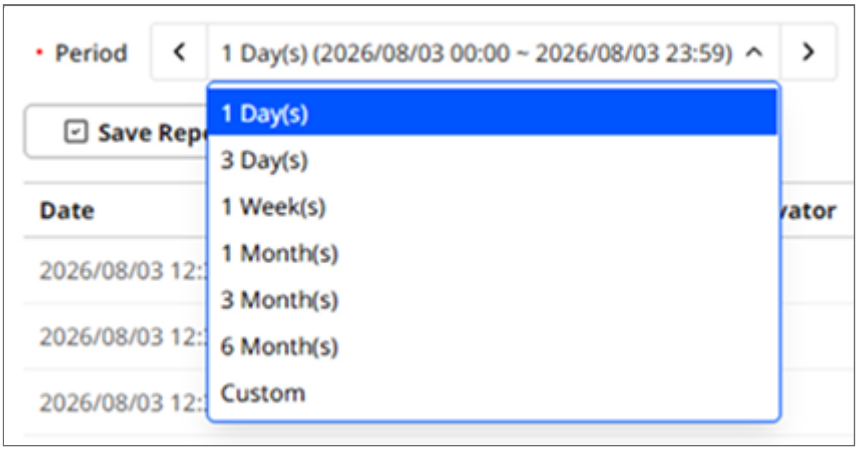
- To check the previous or next page from the listed results, click ‹ or › at the top right of the screen.
- To go to the first or last page of the queried list, click |‹ or ›| at the top right of the screen.
- To change the number of rows displayed in the list, click the dropdown menu at the top right of the screen and select your desired value. You can select from a minimum of 25 rows to a maximum of 200 rows.



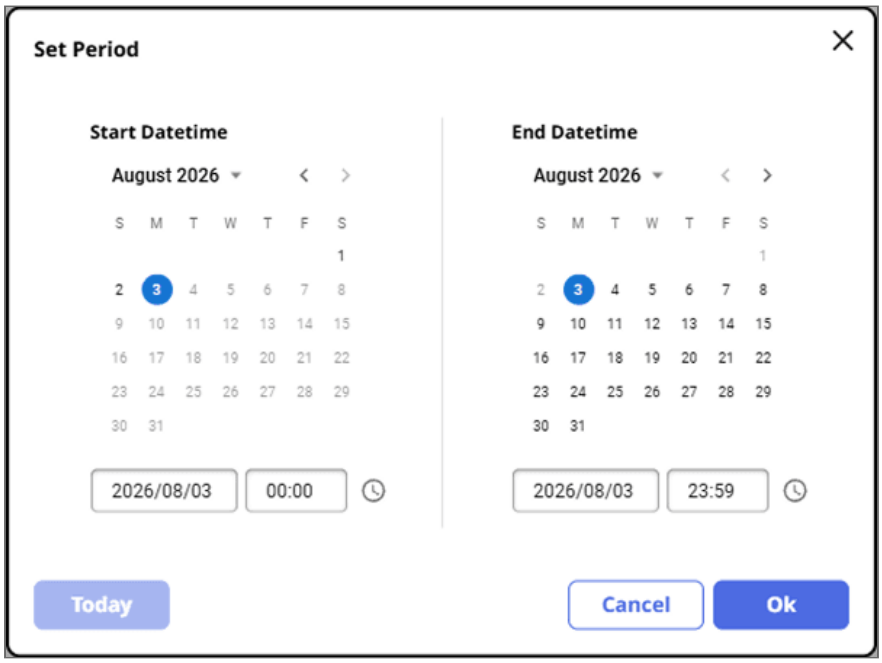
> **Info**
>
> For more information on viewing alarm (alert) events in event monitoring, see Monitor Event.

Set period

You can set the desired period in the **Period** option at the top left of the screen. Click the date area.



- 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 **Custom**, 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.

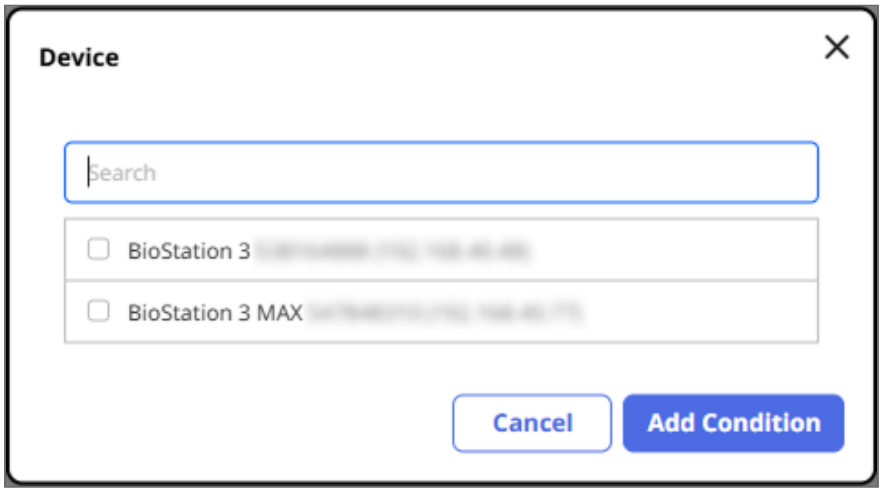


> **Info**
> To select today's date, click **Today**.

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.



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.



Report Save

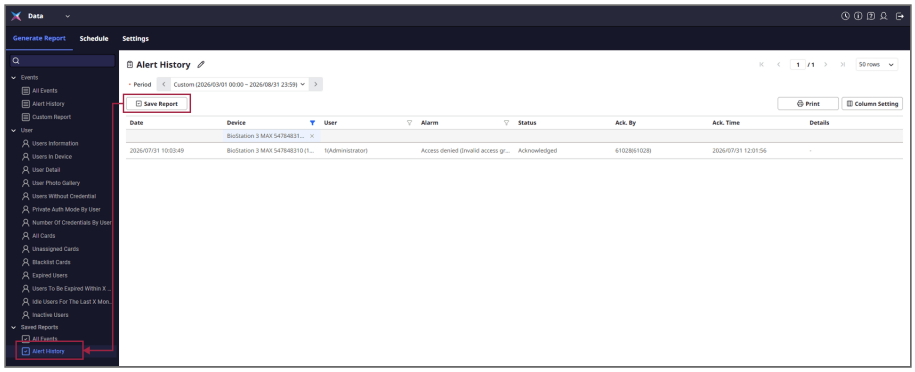
Save alarm history as a report using the query period and conditions you set.

1. Click **Save Report** at the top left of the alarm history list.



2. When a message confirms the report template saved successfully, click **Ok**.

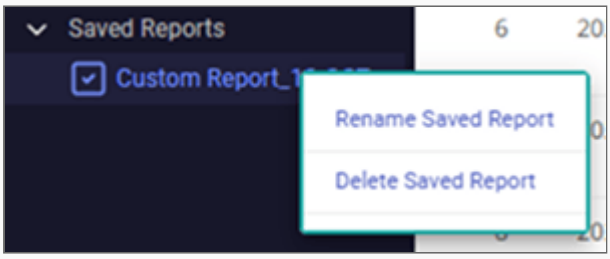
3. Saved reports appear under **Saved Reports** in the left sidebar.



The system stores saved reports as templates for reuse when generating reports under the same conditions.

Info

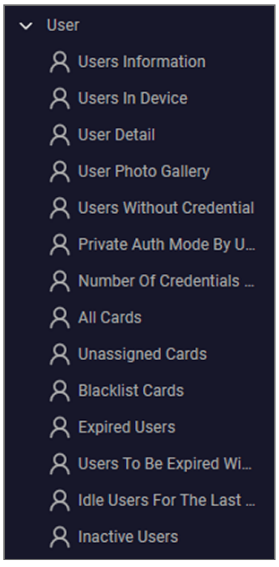
- Click the button at the top of the report to edit the title of the saved report, event items, period, and filter conditions.
- The report title can also be changed under **Saved Reports** on the left sidebar of the screen. Select the custom report for which you want to change the title and right-click. Select **Rename Saved Report** from the pop-up menu.



- For more information on managing reports, see Report management.

View user reports

You can select user-related templates to generate reports. On 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 on managing reports, see Report management.

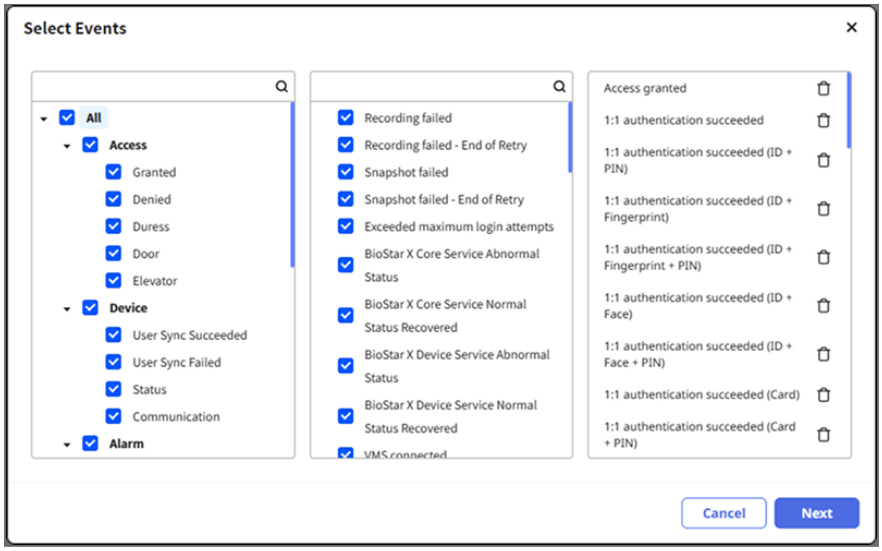
Generate a custom report

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.

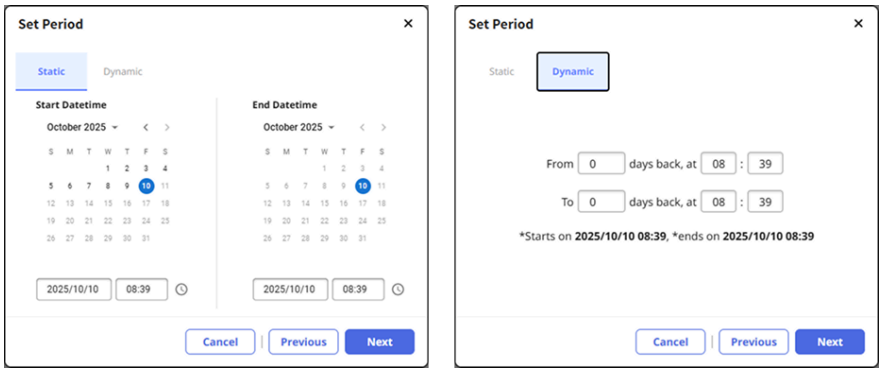


3. Once you have completed your desired event selection, click the **Next** button.



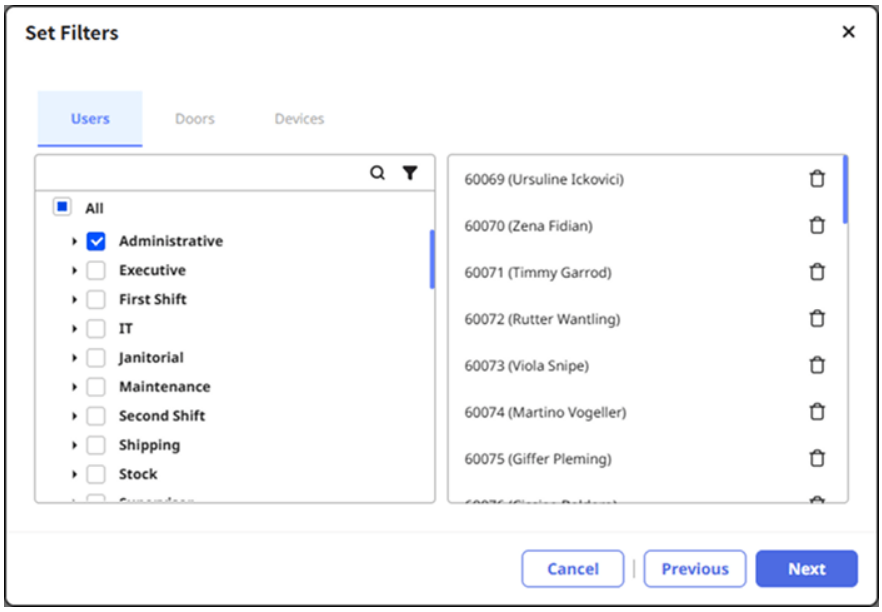
- In the search (🔍) input field, you can search for desired items.
- By clicking the 🗑 button in the rightmost list, you can exclude the selected items.

4. Set the query period and click the **Next** button.



- **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.

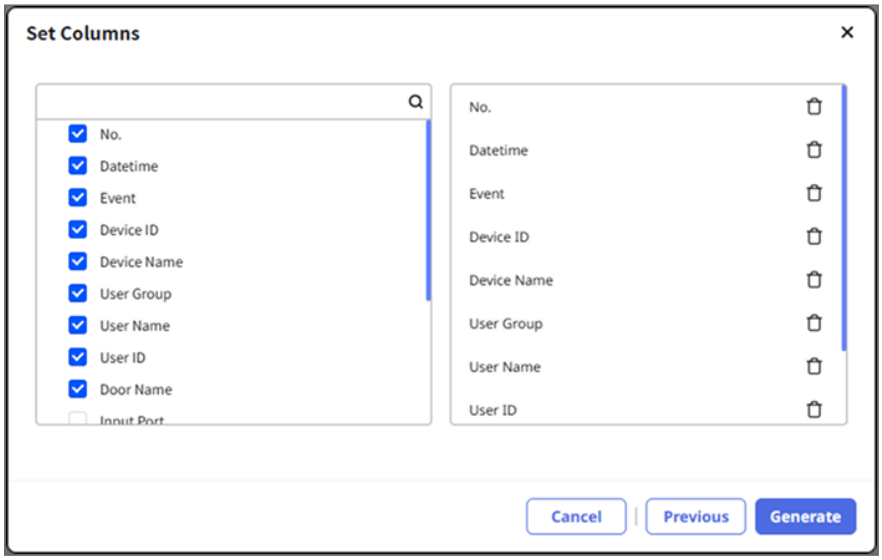
5. You can set conditions based on users, doors, and devices, either grouped or individually.



- By clicking the button in the right list, you can exclude the selected items.

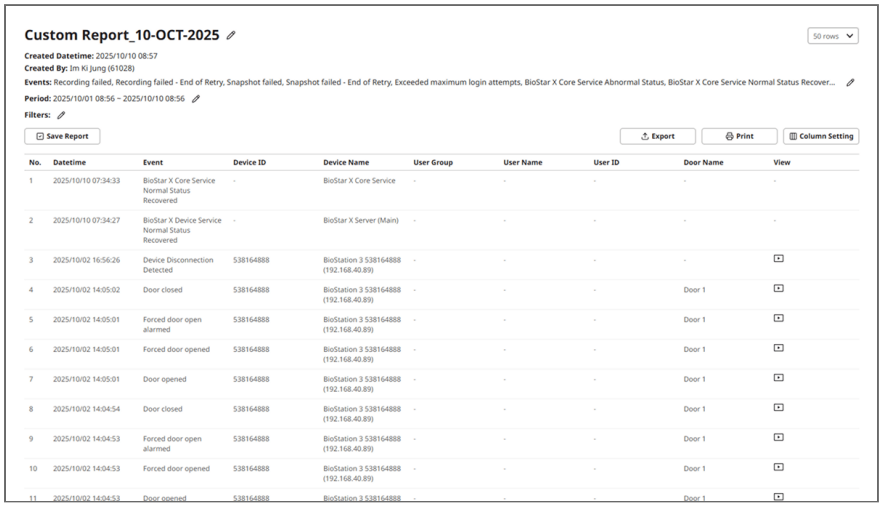
6. Select your desired conditions and click the **Next** button.

7. In the column settings window, select the columns to be displayed in the report.

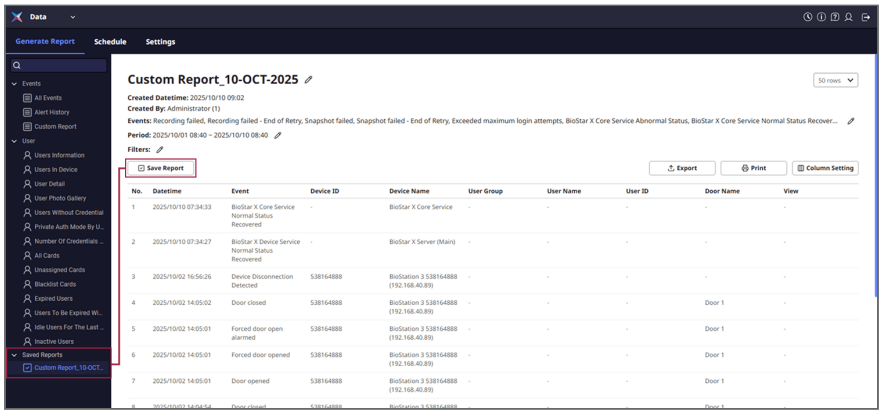


8. Once you have finished selecting your desired columns, click the **Generate** button.

9. Generate a report based on the conditions you set.



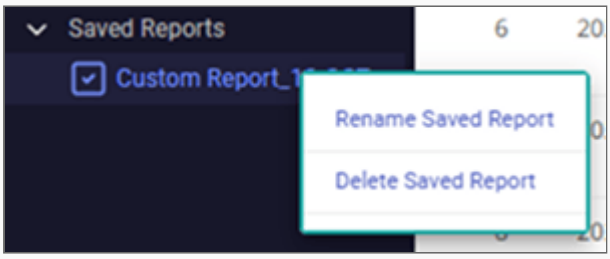
10. To save the generated report as a template, click **Save Report** at the top left of the list. Saved reports can be viewed under **Saved Reports** on the left sidebar of the screen.



The system stores saved reports as templates for reuse when generating reports under the same conditions.

Info

- Click the ✎ button at the top of the report to edit the title of the saved report, event items, period, and filter conditions.
- The report title can also be changed under **Saved Reports** on 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.

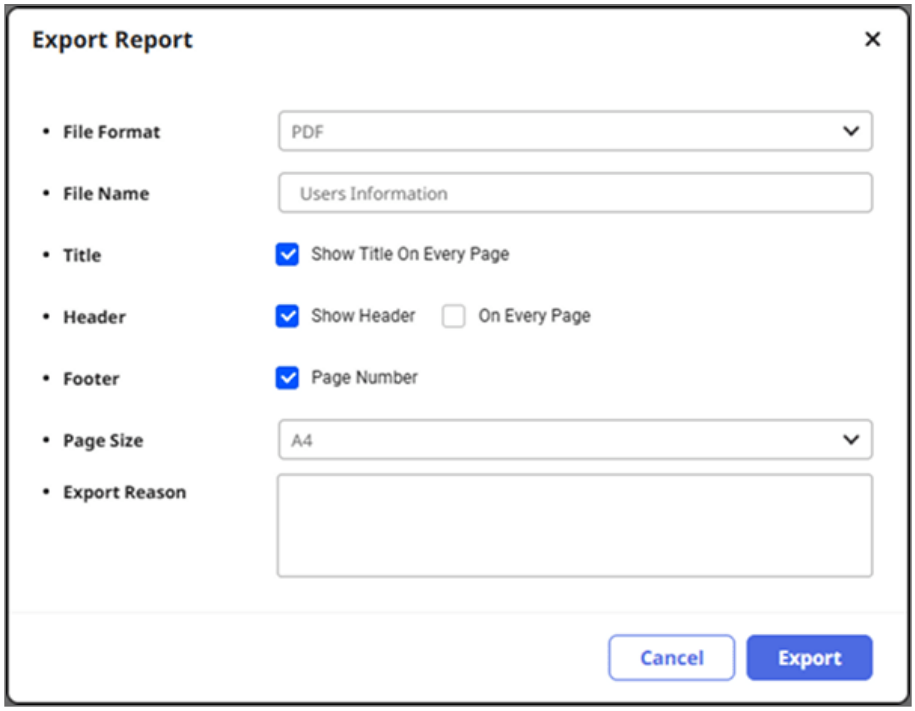


- For more information on managing reports, see Report management.

Report management

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 **Export**.

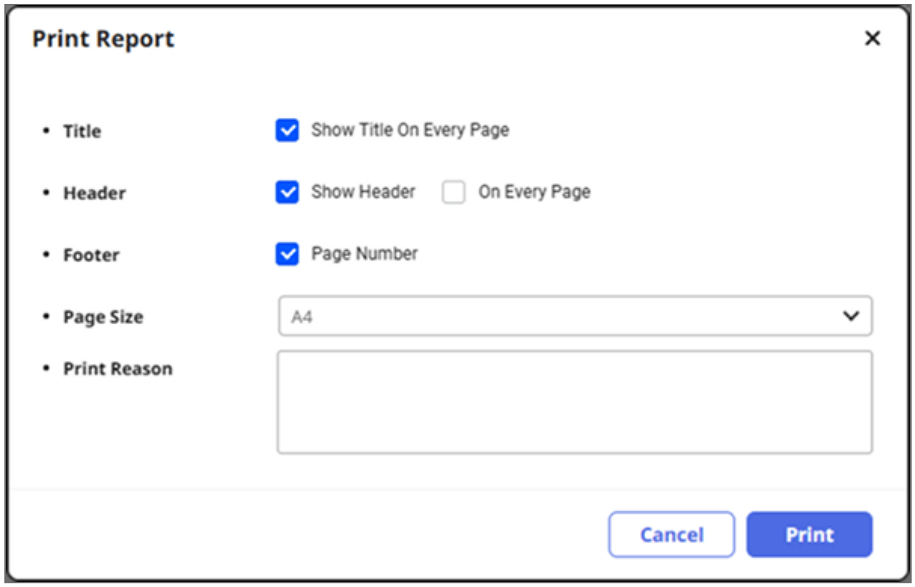


Info

Export Reason is optional. Check records for export reasons in **Settings** → **Audit Trail** → **AC Audit Log**.

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 **Print**.

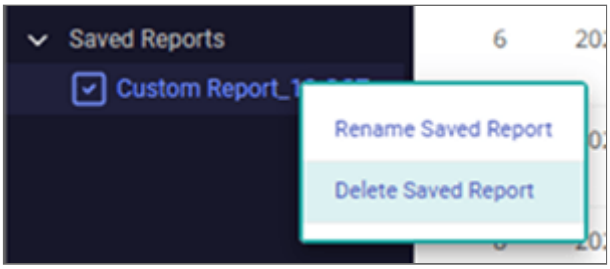


The print preview screen will appear in a new tab of your web browser. Click the print button at the top right of the screen to start printing.

> **Info**
> **Print Reason** is optional. Check records for print reasons in **Settings** → **Audit Trail** → **AC Audit Log**.

Delete report

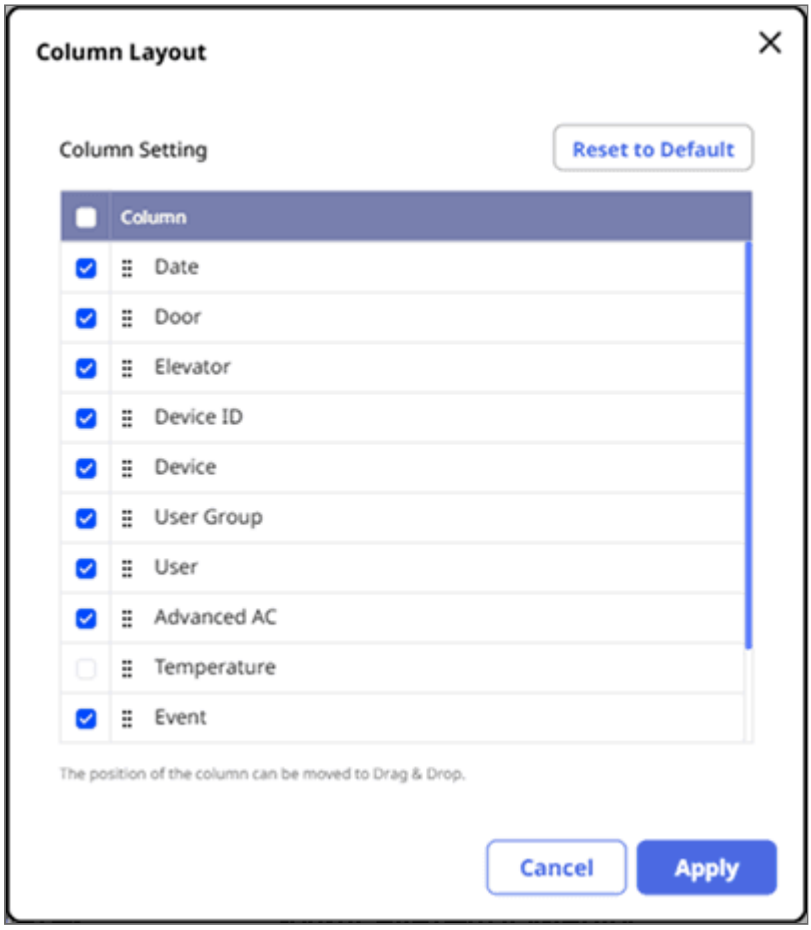
To delete a saved report, select the report to be deleted under **Saved Reports** on the left sidebar and right-click. Select **Delete Saved Report** from the pop-up menu.



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.



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

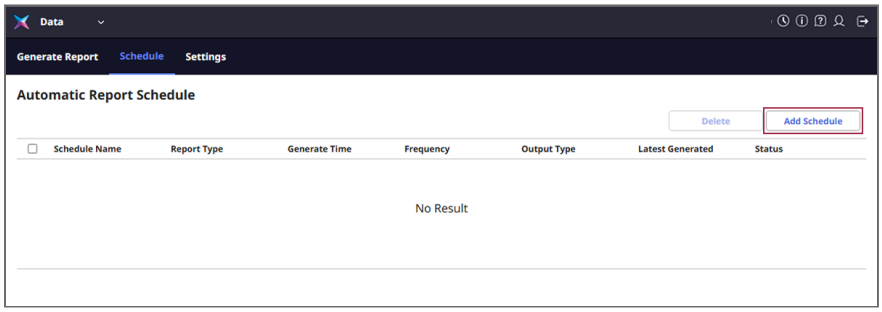
> **Info**
>
> - To reset the column layout settings, click the **Default Column** button.
> - Depending on the generated report, the columns that can be selected or deselected may vary.

Automatic Report Schedule

Set a schedule to automatically generate **Custom Report** created by setting the DYNAMIC period.

Add auto-generated schedule

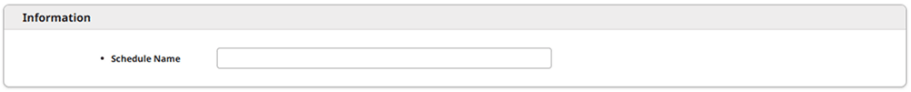
1. Click **Data** or select **Data** from the shortcut list at the top left of the screen on the **Launcher** page.
2. Click the **Schedule** tab.
3. Click **Add Schedule** at the top right of the screen.



4. When the **Add Automatic Report Schedule** screen appears, set each item.

Information setting

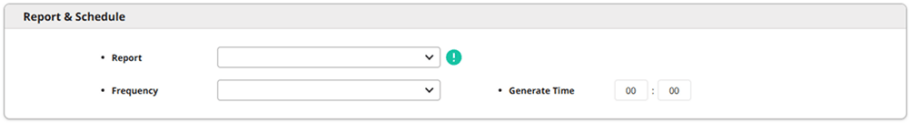
Set basic information of Automatic Report Schedule.



- **Schedule Name**: Enter the schedule name.

Report and schedule settings

Set the schedule to be automatically generated for each report.

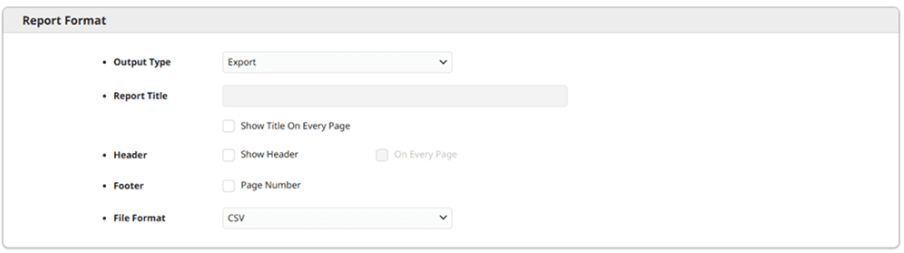


- **Report**: Select a custom report to automatically generate. Only custom reports set to DYNAMIC period will appear.
- **Frequency**: Set the frequency to automatically generate reports.
- **Generate Time**: Set the time to automatically generate reports.

> **Info**
> For more information on creating custom reports, see Generate Report.

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.

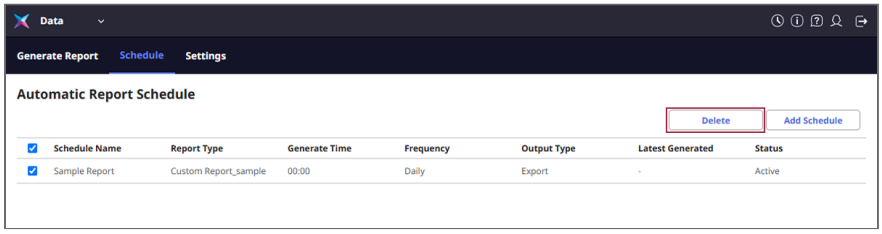
- **Footer**: Set whether to display page numbers.
- **File Format**: Set the file format for exporting reports.

3. Click **Apply** to save the settings.

> **Info**
> If all settings are complete, set the path to save the report. For more information, see Settings.

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 the **Schedule** tab.
3. Click the checkbox of the schedule to delete from the auto schedule list.

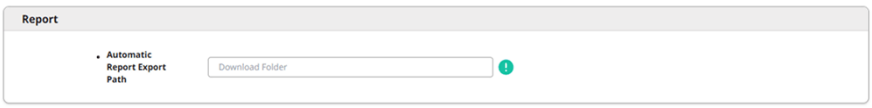


4. Click **Delete** at the top right of the screen.

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.



- **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 **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

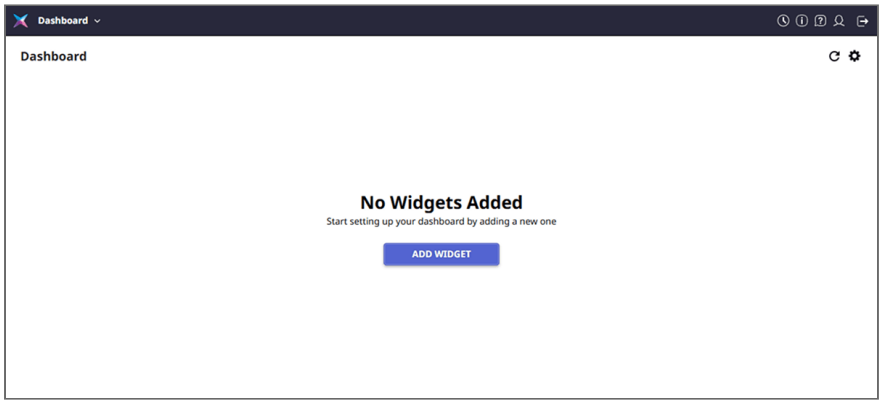
You can gain the following advantages from the widgets placed on the dashboard.

- **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

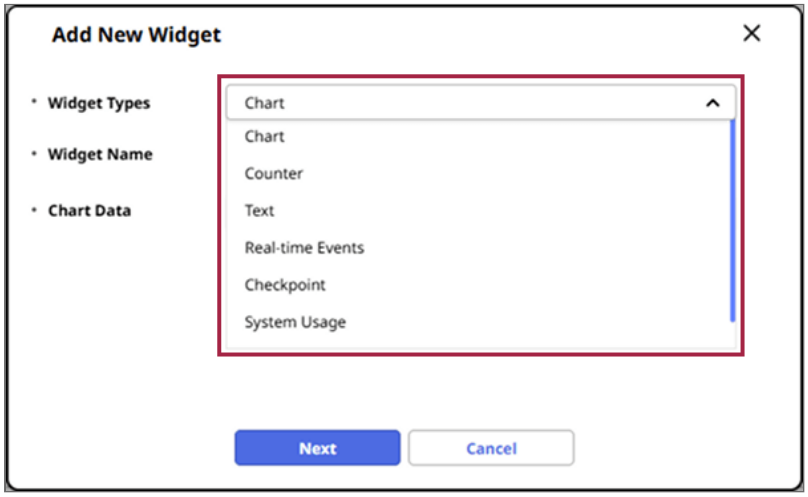
Add widgets

You can add widgets to **Dashboard** to check the information you want.

1. Click **Dashboard** on the **Launcher** page.
2. Click **Add Widget**.



3. When the **Add New Widget** window appears, select the desired item in **Widget Type** and enter or set the required fields.

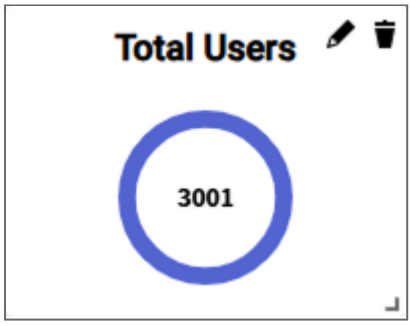


4. Complete the widget settings and click the **Apply** button.
5. When the widget is created in the widget display area, adjust its size or place it in the desired location.
6. Once you have completed all settings, click **Apply** in the upper right corner of the screen.

> **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

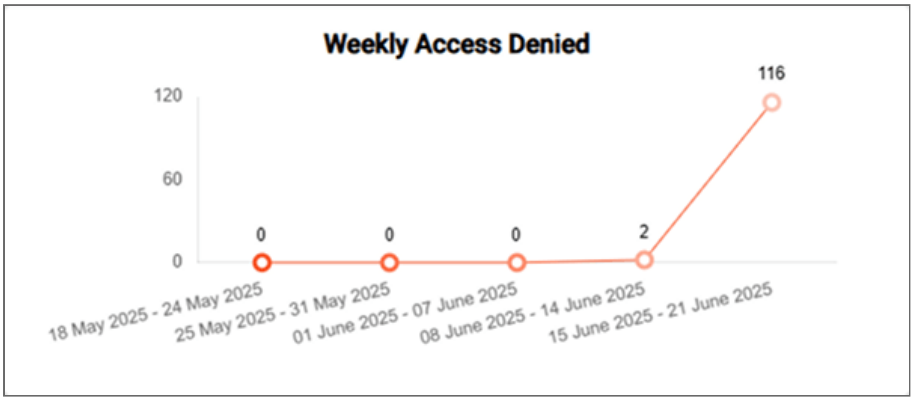
- The default widget size is set differently for each widget and is optimized to look best at the default.
- All widgets can be resized by dragging the lower-right corner.



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.



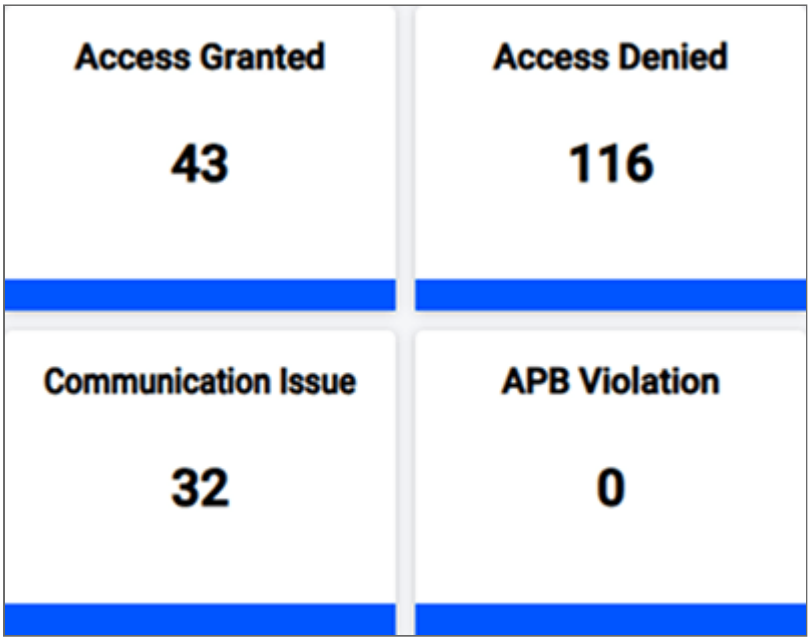
The image above is an example screen and may differ from the actual screen.

- **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.

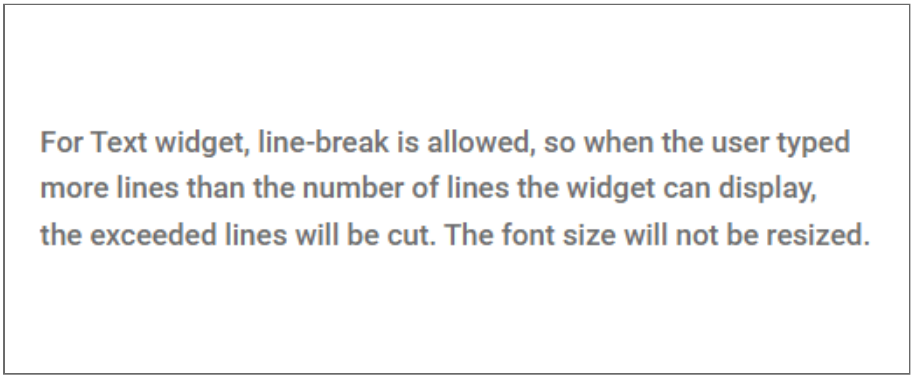


The image above is an example screen and may differ from the actual screen.

- **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.

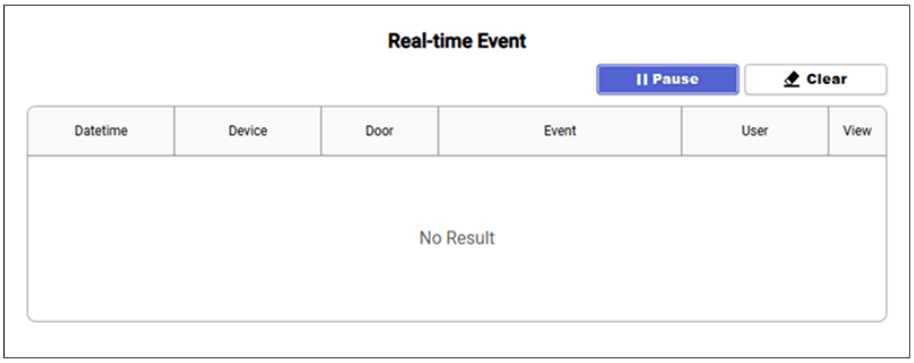


The image above is an example screen and may differ from the actual screen.

> **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.



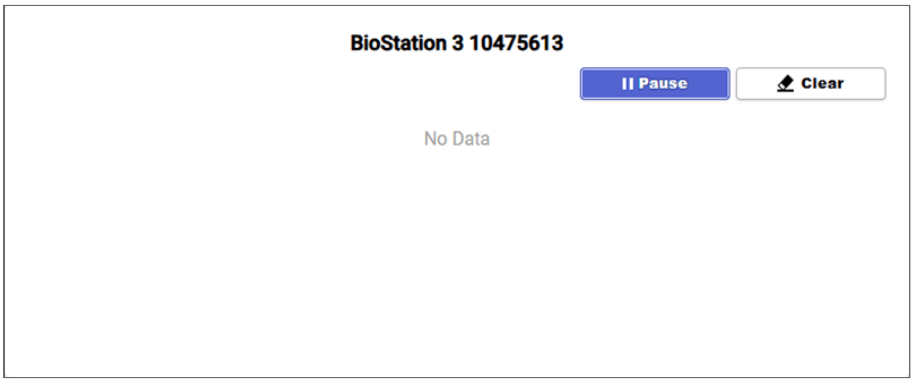
The image above is an example screen and may differ from the actual screen.

- **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.



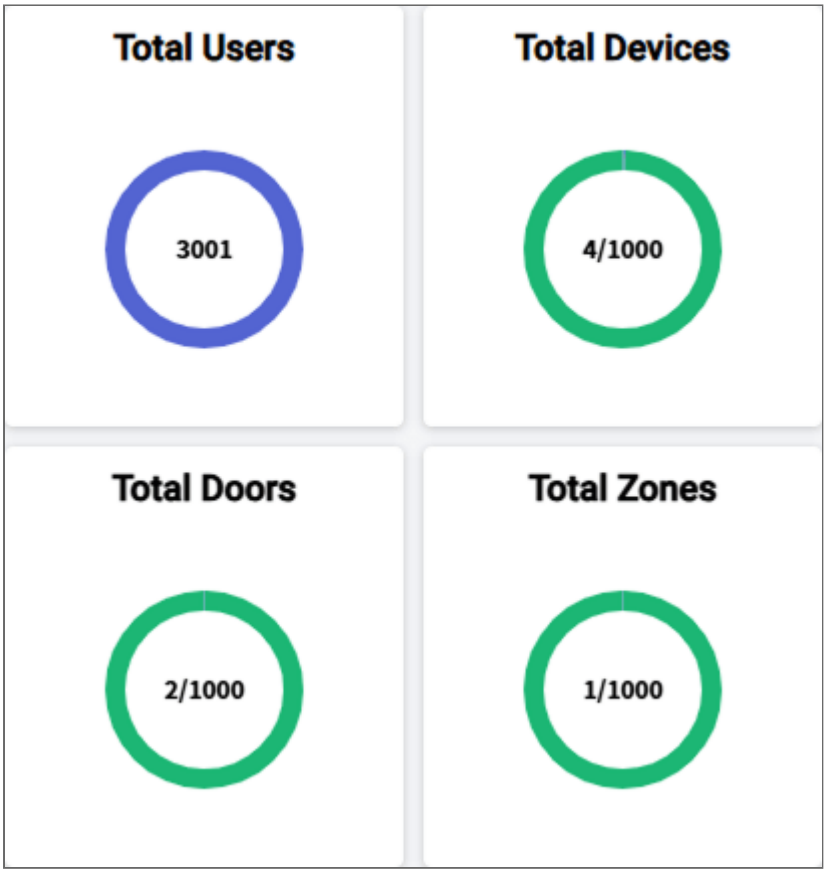
The image above is an example screen and may differ from the actual screen.

- **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 Advanced ACs**, **Total Access Groups**, **Total User Groups**, **Total Device Groups**, **IR Face**

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

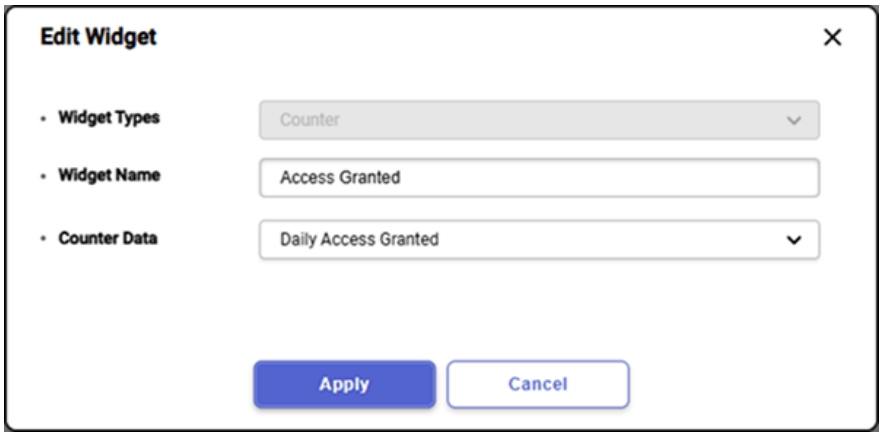
You can set the data refresh interval of widgets added to the dashboard.

1. Click **Dashboard** on 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** on the **Launcher** page.
2. Click the ⚙ icon in the upper right corner of the screen.
3. After entering **Dashboard Settings** mode, click ✎ at the top right of the **widget** you want to edit.
4. When the **Edit Widget** window appears, modify your desired items.



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** on 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.



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 on the menus accessible at each user permission level, see Setting User Permissions.

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.

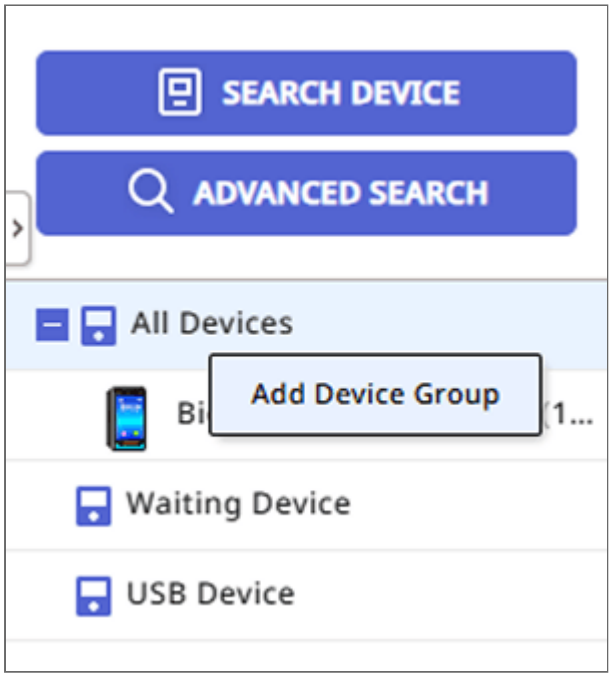
Manage Device Groups

This guide describes to the device group feature for efficiently managing multiple devices. 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** → **Device** on the left sidebar.
3. Right-click **All Devices** in the device list.

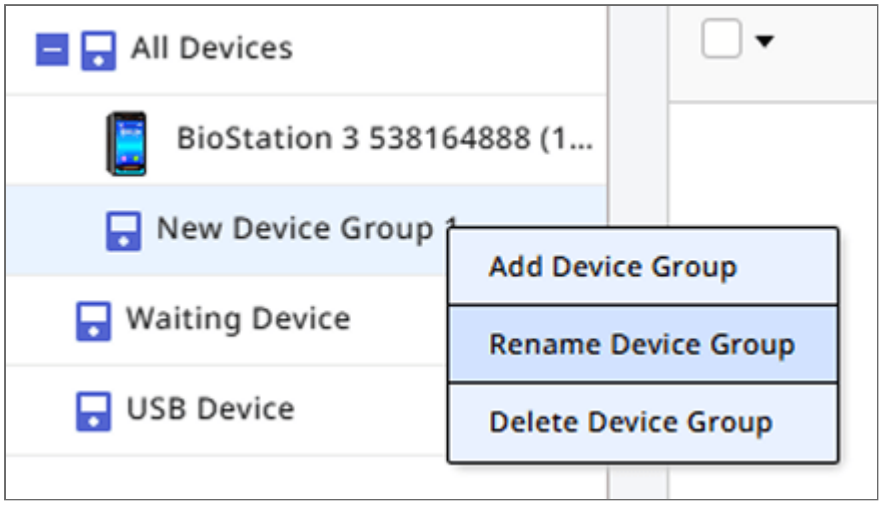


4. Click **Add Device Group** in the popup menu.
5. Enter your desired group name.

> **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** → **Device** on the left sidebar.
3. From the sublist of **All Devices**, select the device group whose name you want to change and right-click.



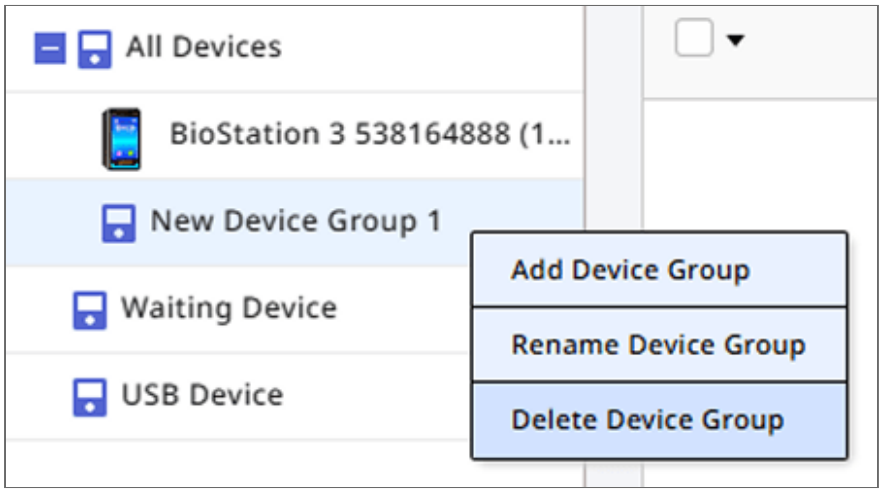
4. Click **Rename Device Group** in the popup menu.

5. Enter the new name for the group.

> **Info**
> Device group names can be up to 48 characters long.

Delete a device group

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Device** on 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, see Server Detailed Settings.
- To register a device and configure its details, see Device Settings.
- Up to 1,000 devices can connect via Ethernet (TCP/IP).
- Obtain a **Device Manager** or higher license to register devices. For more information on the licensing policy, see License Policy.

Before you start

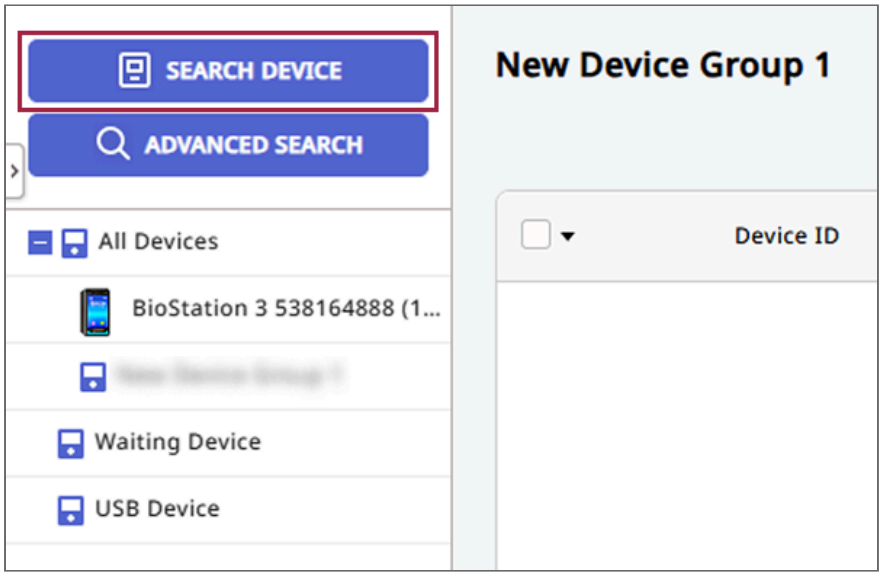
Check the following before registering the device.

- Set access levels, access groups, and floor levels for access control. For more information, see Access Control Settings.
- Create a group to manage devices efficiently. For more information, see Manage Device Groups.

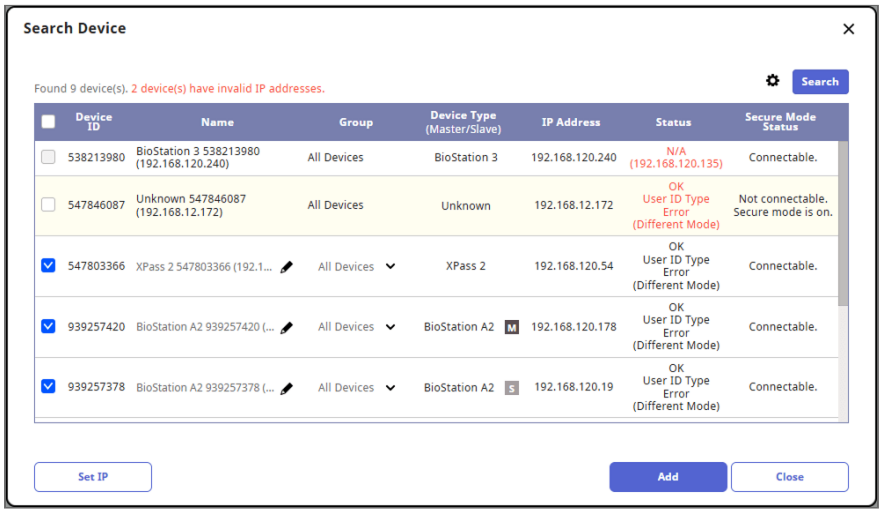
Quick registration

Devices on the same network as **BioStar X** can be automatically searched and registered.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Device** on the left sidebar.
3. Click **Search Device** in the device list.

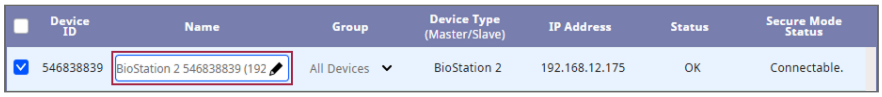


4. When the **Search Device** window appears, a list of all devices that can be registered will be displayed. If the desired device is not in the list, click **Search** in the top right corner.

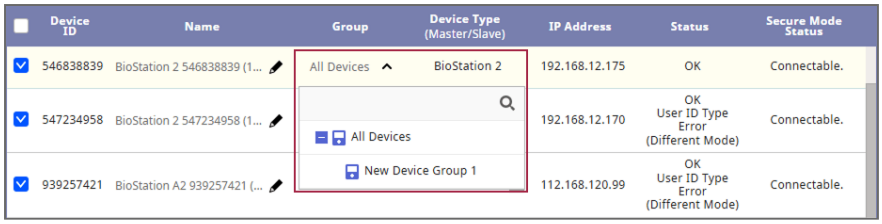


5. Select the devices to register from the device list or deselect devices to not register.

6. To change the name of the device to be registered, click ✎ in the **Name** column and make the change.

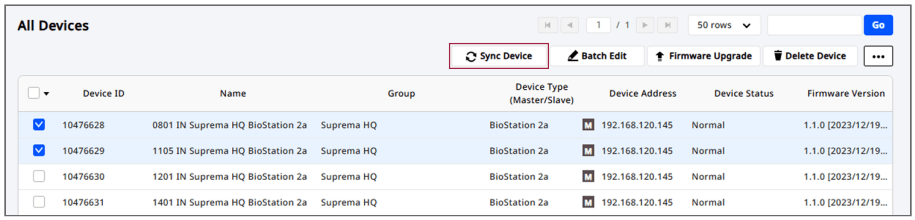


7. To specify the group for the device to be registered, select it in the **Group** column.



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**.

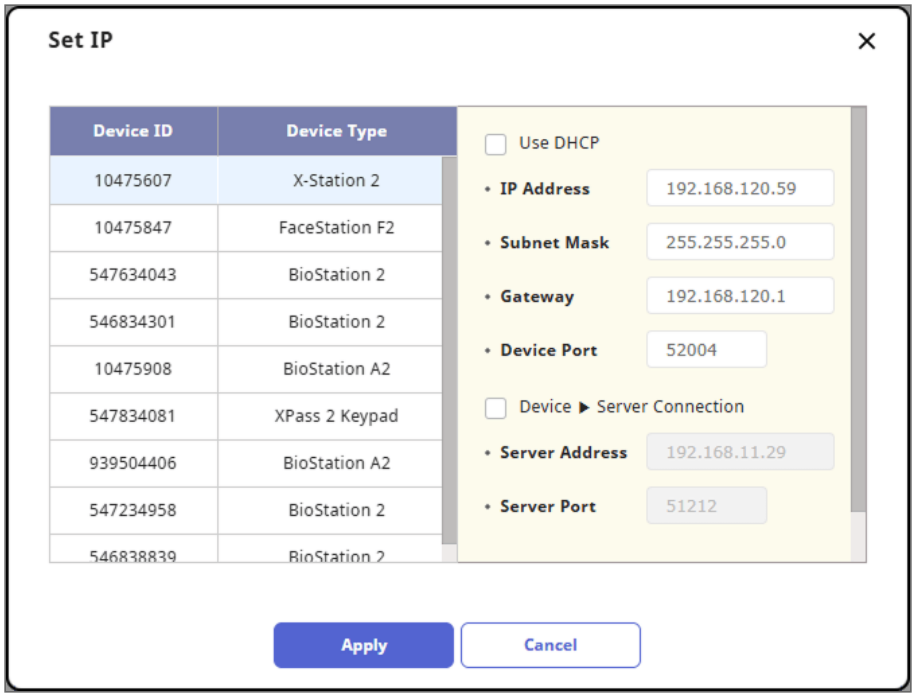


Info

Devices for which the IP address is unavailable or needs to be changed can be modified by clicking **Set IP**. For more information, see IP address setting.

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.



- **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.

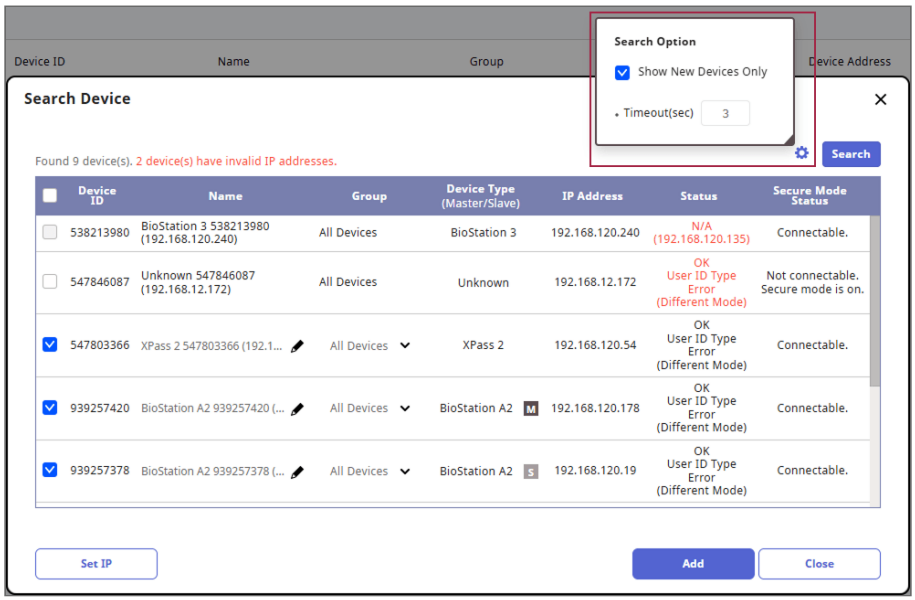
- **Device ▸ Server Connection**: Select this option to configure the device to connect to the **BioStar X** server. You will need to enter the IP address and port number of the server where **BioStar X** is installed.

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.

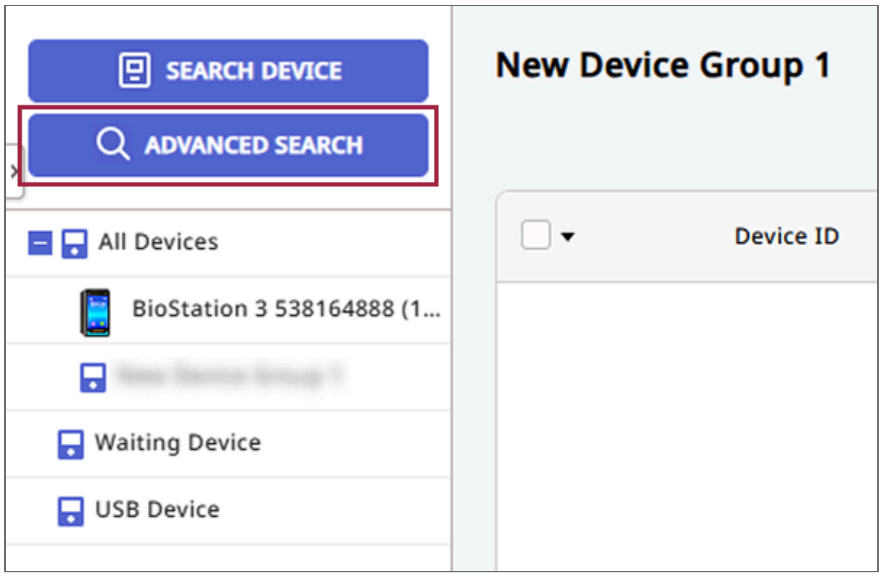


- **Show New Devices Only**: Select this option to display only newly discovered devices in the search list.
- **Timeout(sec)**: Set the desired time to exclude devices that do not respond for a certain period from the search list. This can be set in seconds, with a default of 3 seconds.

Advanced search

You can specify the IP address and port number of a specific device to register it.

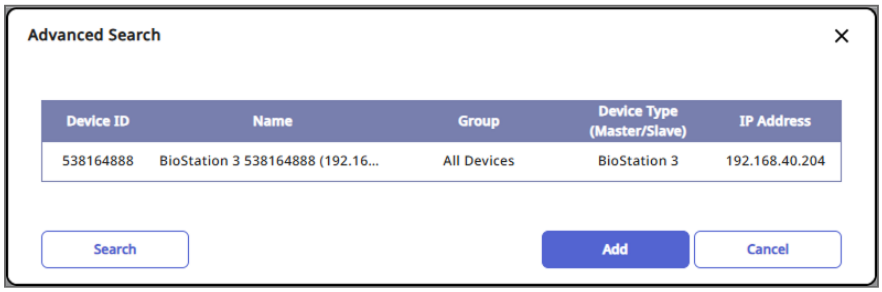
1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Device** on the left sidebar.
3. Click **ADVANCED SEARCH** in the device list.



4. When the **ADVANCED SEARCH** window appears, enter the IP address and port number of the device to be registered.



5. Click **Search** to display devices matching the entered criteria.



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 waiting devices

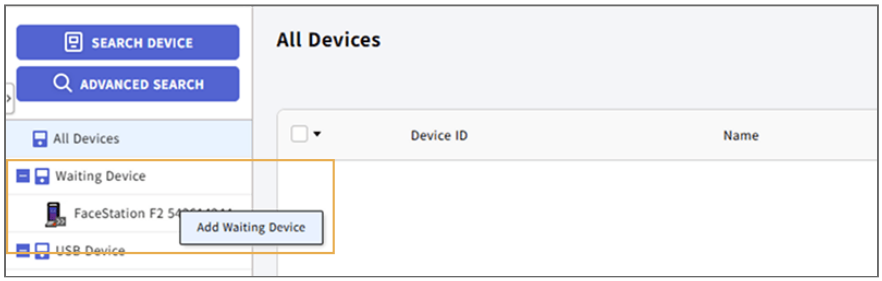
Devices with the **Device → Server** option set try to connect to the **BioStar X** server using the server IP address and port number. Devices connected this way do not automatically register in the active device list. These devices appear in the **Waiting Device** group, and an authorized administrator must register them manually.

1. In the device's **Device → Server** option, set the IP address and port number of **BioStar X**.
2. Click **Settings** on the **Launcher** page.
3. Click **Device → Device** on the left sidebar.
4. Check the devices shown in the **Waiting Device** group.



5. To register an individual device, right-click the device name in the **Waiting Device** group.

   To register all devices in the **Waiting Device** group, right-click the **Waiting Device** group.



6. In the popup menu, click **Add Waiting Device**(individual device) or **Add All Waiting Devices**(all devices).

After an administrator registers a device in the **Waiting Device** group, it moves to the **All Devices** list.

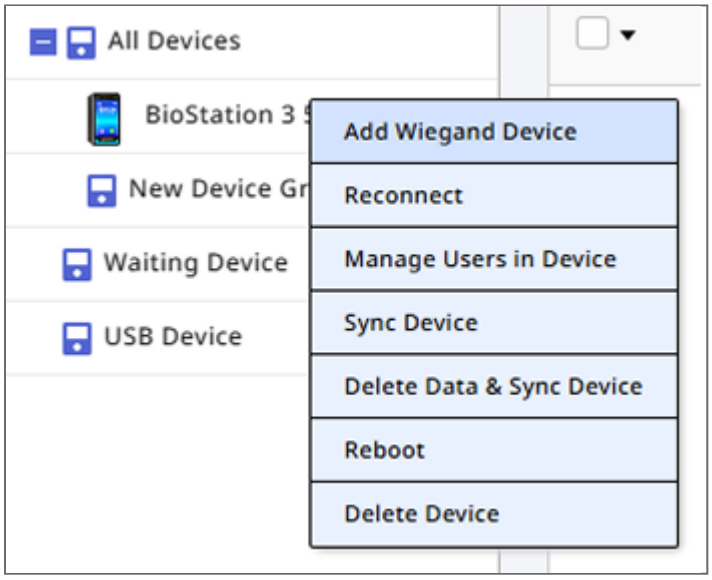
> **Info**
>
> - Set the device **Device** → **Server** option at **SETTINGS** → **NETWORK** → **Server**. Menu paths may vary by device.
> - You can also configure this setting in **BioStar X** via **Set IP** → **Device** ▸ **Server Connection** (IP address setting).
> - Devices that remain in the **Waiting Device** group are not synchronized. User data, access levels, access groups, and device settings are not transferred to a device until it has been registered and sync device has been performed.

Register Wiegand Credentials

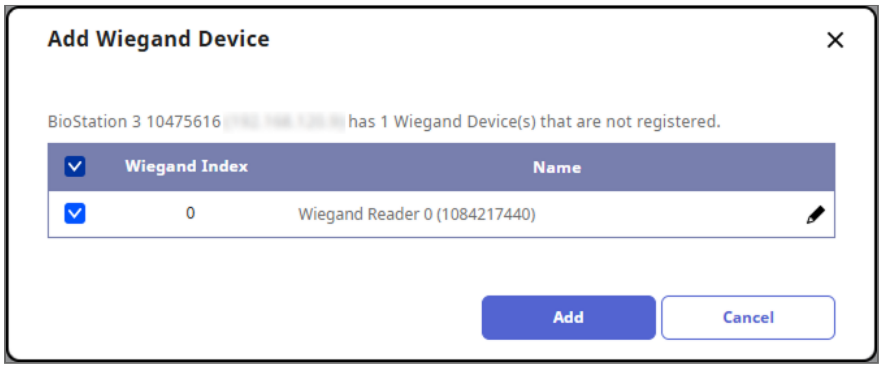
This guide outlines how to add a Wiegand device to the registered master or slave device.

> **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** → **Device** on 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.



6. Click **Add**.
7. When the device registration confirmation message appears, click **Apply**.

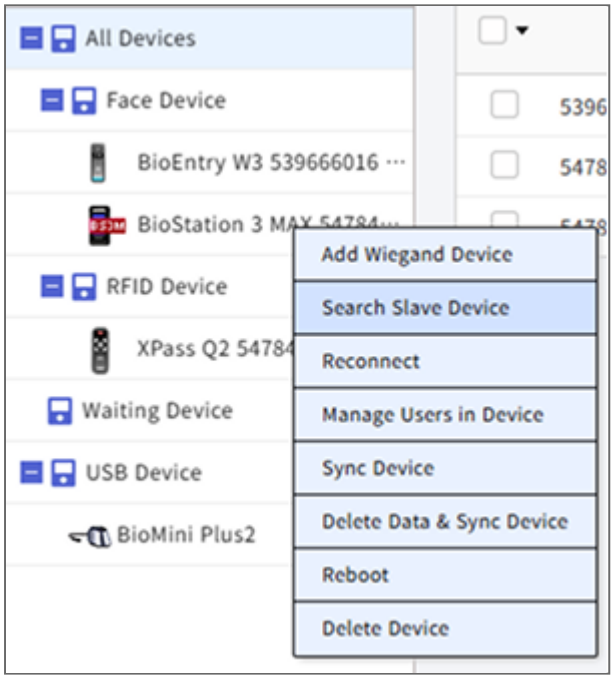
The registered Wiegand device will appear under the selected device.



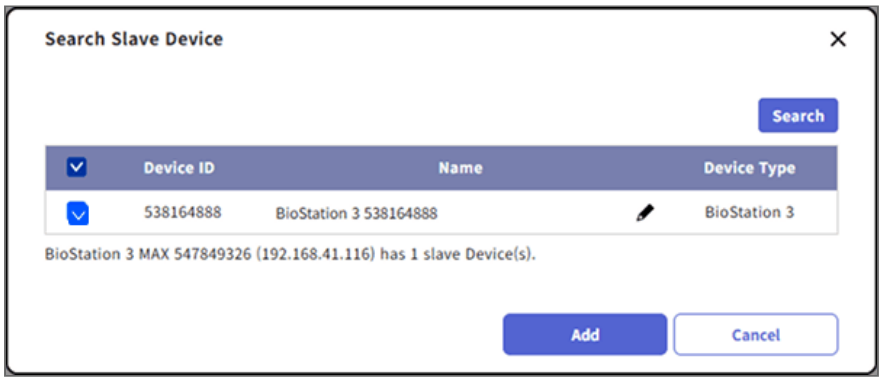
Register Slave

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** → **Device** on the left sidebar.
3. Right-click on the master or slave device in the **All Devices** list.

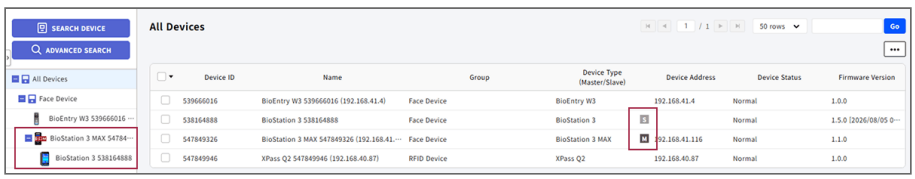


4. Click **Search Slave Device** in the popup menu.
5. When the list of slave devices connected to the master device appears, select the device to register. If the desired device is not listed, click **Search** in the upper right corner.



6. Click **Add**.
7. When the device registration confirmation message appears, click **Ok**.

The registered slave device will appear under the selected device. In the device list, the master shows the icon, and the slave shows the icon.



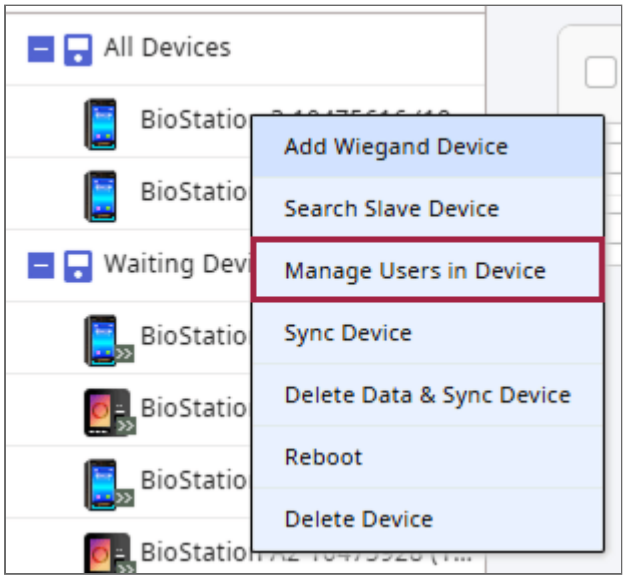
Info

- 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.

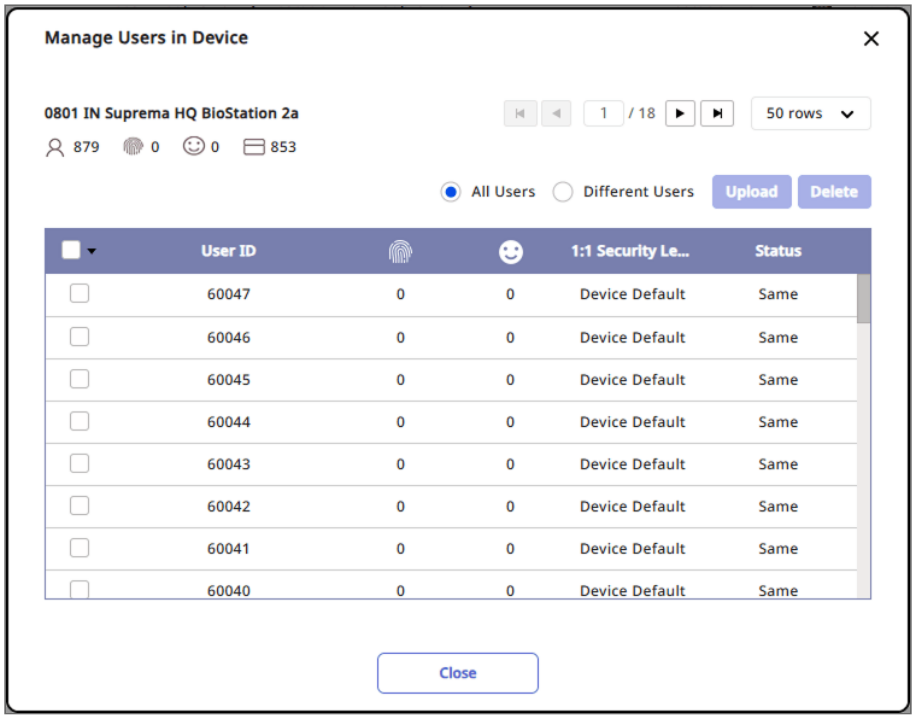
Manage Users Registered on Device

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** → **Device** on 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**.



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 **Delete**. To send user information to the **BioStar X** server, click **Upload**.

Info

- The **Manage Users in Device** feature can only be used with one device selected.
- When clicking **Upload**, 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 on device settings, see Device Settings.

Upgrade Firmware

Devices connected to **BioStar X** can easily upgrade firmware without additional connections or operations. Keeping the device firmware up to date resolves security vulnerabilities and allows access to new features.

Before you start

Before upgrading the device firmware, prepare the new version of the firmware file. Save the downloaded firmware file to the path below and extract it. 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.

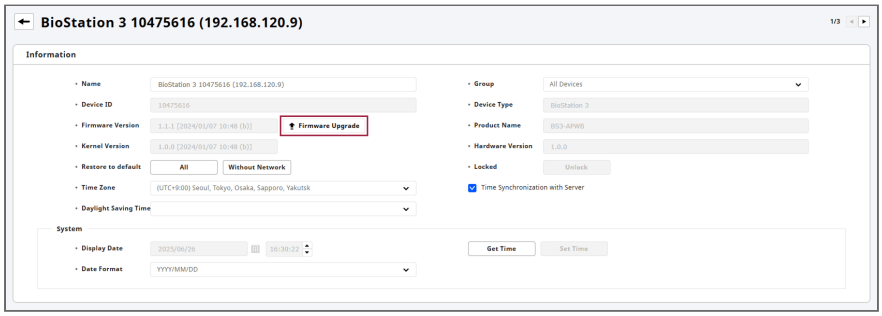
Firmware upgrade

Caution

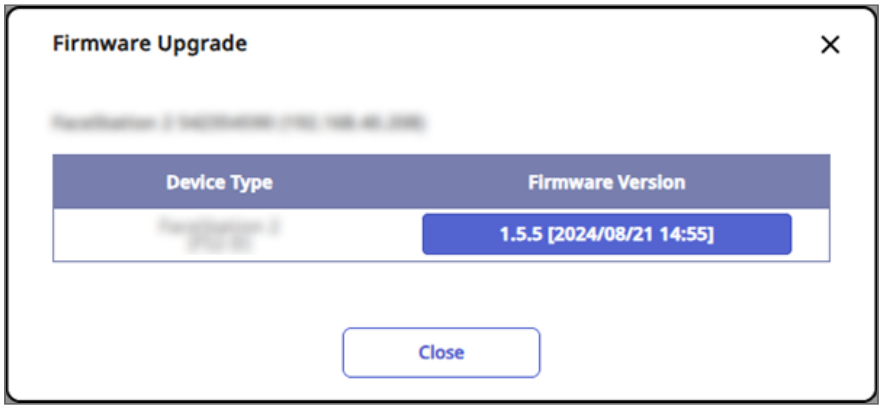
- Before upgrading firmware, make sure the device has power and network connectivity. In particular, make sure power is not interrupted during the upgrade.
- Depending on the device type and mode, it may take up to 1 hour or longer. Also, the device cannot be used during the upgrade.
- Do not turn off the device during the firmware upgrade. When the upgrade is complete, the device restarts automatically.

Upgrade firmware for a single device

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Device** on the left sidebar.
3. Click the device in the device list that you want to upgrade.
4. Click **Firmware Upgrade** in the **Information** section of the device details screen.



5. When the **Firmware Upgrade** window appears, click the firmware version.

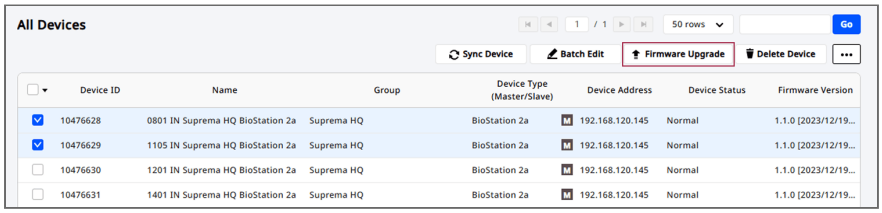


6. When the warning message window appears, click **Continue**.

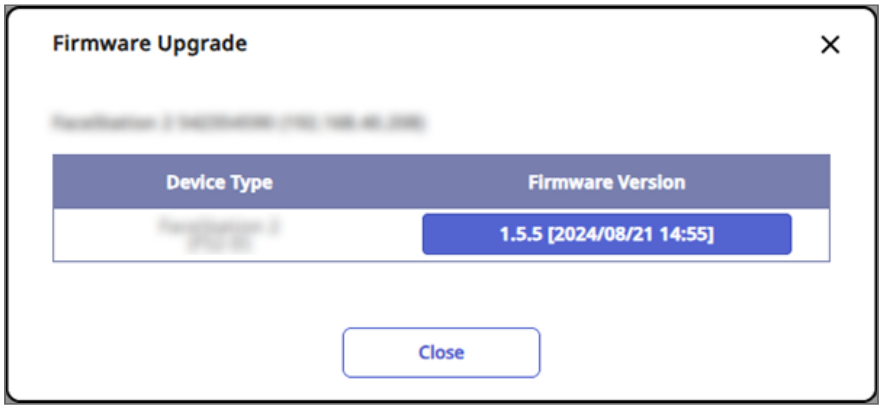
This initiates the firmware upgrade for the device.

Upgrade firmware for multiple devices

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Device** on 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 **Firmware Upgrade** at the top right of the device list.



5. When the **Firmware Upgrade** window appears, click the firmware version.



6. When the warning message window appears, click **Continue**.

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.

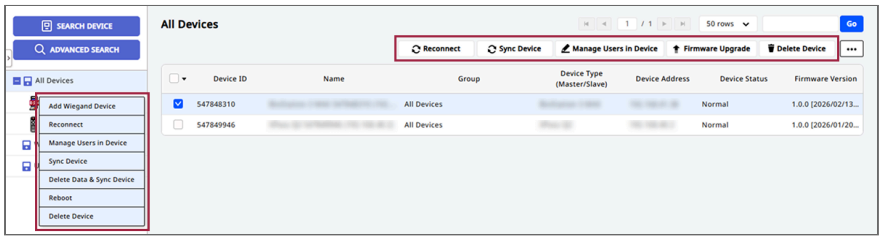
Use Device Management Feature

This guide explains how to use additional features of **BioStar X**. This section explains how to reconnect devices, synchronize, batch edit device information, delete devices, and export/import settings. It also explains how to delete secure communication certificates when deleting devices.

Manage a Single Device

Use the following steps to manage a single device.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Device** on the left sidebar.
3. Select the device from the **All Devices** list and right-click. Or, click the checkbox for the device you want in the device list.



4. Select the desired action from the pop-up menu or from the top of the device list.

Refer to the features below. The features provided may vary depending on the device.

- **Reconnect**: Reconnect the selected device. This option is available when one device is selected. In general, the device automatically returns online without user intervention after the network connection is restored. Use this feature when the device does not reconnect automatically after the network is restored.

  > **Info**
  >
  > This feature is not supported by devices connected with the **Device** ▸ **Server Connection** option. For more information on registering devices, see Register Device.

- **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, see Manage Users Registered on Device.
- **Firmware Upgrade**: Easily upgrade the device firmware. For more information, see Upgrade Firmware.
- **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. For more information, see Delete devices.

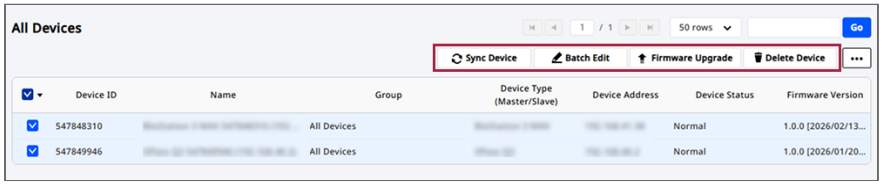
> **Info**
>
> - For more information on the **Add Wiegand Device** feature, see Register Wiegand Credentials.
> - For more information on the **Search Slave Device** feature, see Register Slave.

Manage multiple devices

Use the following steps to manage one or more devices.

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

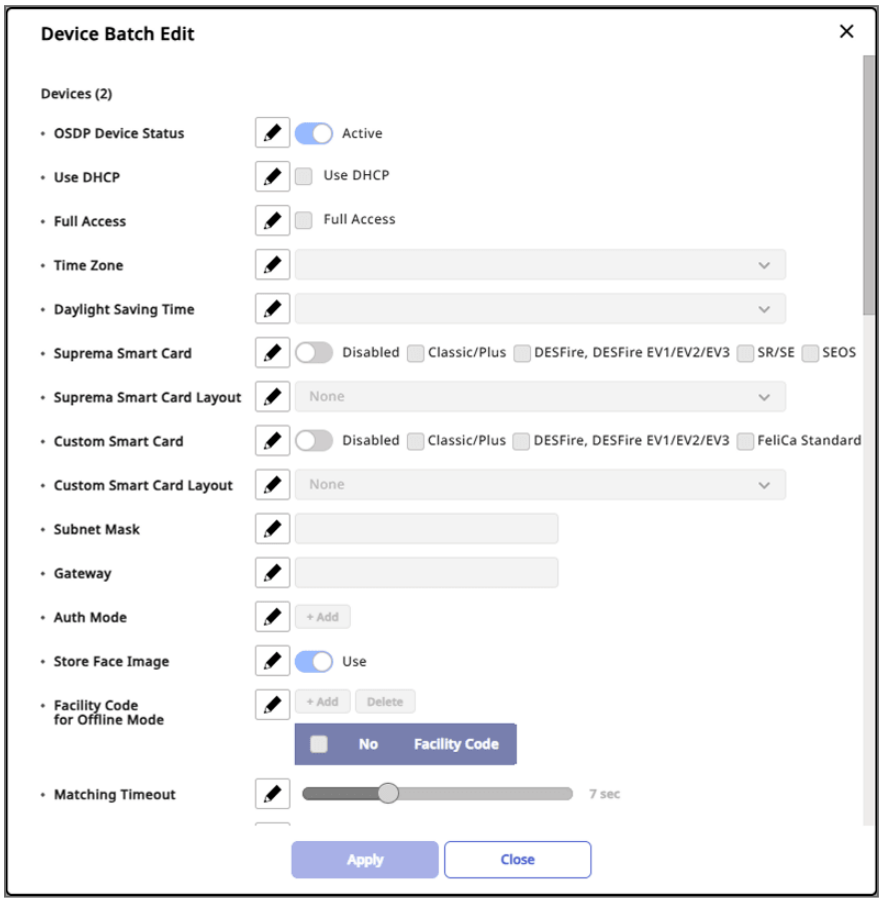
2. Click **Device** → **Device** on the left sidebar.
3. Click the checkbox for the device you want in the device list. You can select 1 or more devices.



4. Select the desired feature at the top of the device list.

Refer to the features below. The features provided may vary depending on the device.

- **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.
- **Batch Edit**: Batch edit information for the selected devices. Click the button to open the **Device Batch Edit** window.



> **Info**
>
> – 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.

- **Firmware Upgrade**: Easily upgrade the device firmware. For more information, see Upgrade Firmware.

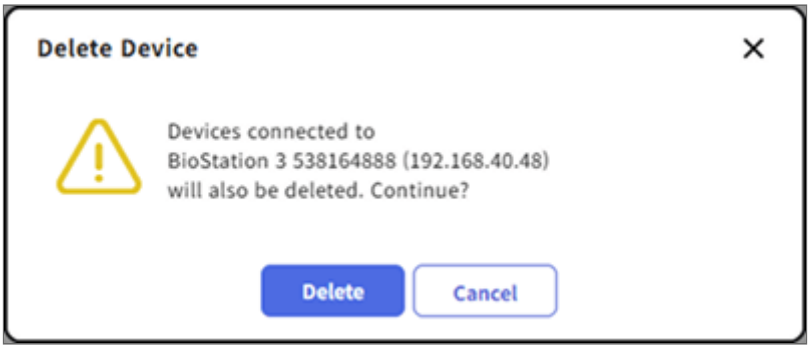
- **Delete Device**: Delete the selected device from the list. Devices set as doors or zones cannot be deleted. For more information, see Delete devices.

Delete devices

Use **Delete Device** to delete devices from the list. The options that appear during deletion depend on whether **Secure communication with device** is enabled.

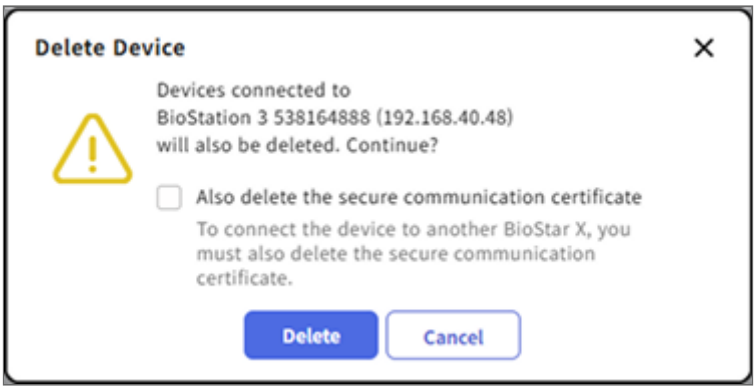
When secure communication is disabled

When **Secure communication with device** is set to **Not Use**, delete the selected device without additional options.



When secure communication is enabled

When **Secure communication with device** is set to **Use**, the **Delete Device** dialog shows the **Also delete the secure communication certificate** option.



- If **Also delete the secure communication certificate** is cleared (default), delete only the device and keep the certificate.
- If **Also delete the secure communication certificate** is selected, also delete the secure communication certificate stored on the device. Use this option to connect the device to another **BioStar X** server after deleting it.

> **Caution**
> If a device disconnects from **BioStar X**, it cannot delete its certificate. If **Also delete the secure communication certificate** is selected, device deletion fails. To delete the device, clear the option or reconnect the device, then try again.

Info

- If **Secure communication with device** is enabled, deleting the device without selecting **Also delete the secure communication certificate** leaves the certificate on the device. Then change the **Secure communication with device** option to **Not Use**, and enroll the device in **BioStar X** again. The device fails to connect because the certificate remains. If you use the default certificate, change the **Secure communication with device** option back to **Use**.
- If all selected devices are slave devices or do not support secure communication, delete devices without the **Also delete the secure communication certificate** option.
- The **Also delete the secure communication certificate** option appears only when **Secure communication with device** is enabled. For more information, see Enhance System Security.

Export/import device configuration

Export configurations from one device to a file, then import and apply them to another device of the same model. Instead of entering the same configurations on multiple devices, create a configuration file from a configured device and apply it to the others.

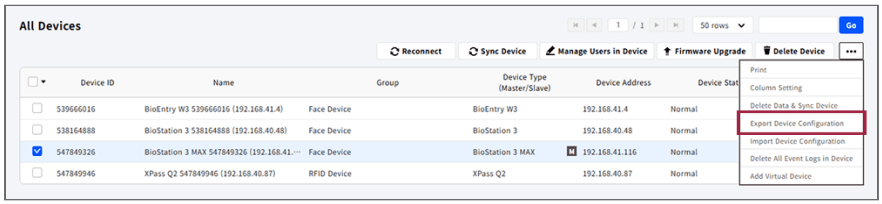
Info

- Same model means the detailed model name and part number match (for example, XXX in XPD2-XXX).
- The export/import device configuration feature is available to administrators with full permissions for device settings. For more information about administrator permission settings, see Manage Operation Permissions.

Export device configuration

To download the configurations for a single device as a file, follow these steps.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Device** on the left sidebar.
3. In the device list, click the checkbox for the device whose configurations to export. You can select only one device.
4. Click ••• → **Export Device Configuration** at the top of the device list.



5. When the download window appears, save the configurations file locally.

Caution

Configurations export is unavailable for the following devices.

- Devices disconnected from **BioStar X** or with a response timeout
- Virtual device
- Devices without RS-485 communication mode (for example, Wiegand devices, I/O modules, Door Interface, Door modules, Secure modules, and OSDP Antenna/Reader)

Info

- You cannot run this feature unless you select exactly one device.
- The file name is set automatically in this order: model name, device ID, RS-485 communication mode (Master/Default/Slave), and export date. The date follows the date format set in **Settings** → **System** → **Preferences**.

  For example, if the model name is BS3-DB, the device ID is 538001234, the serial communication mode is **Master**, and the export date is 6/23/2026, the file is saved as `BS3-DB_538001234_Master_20260623.json`.

Configurations excluded from export

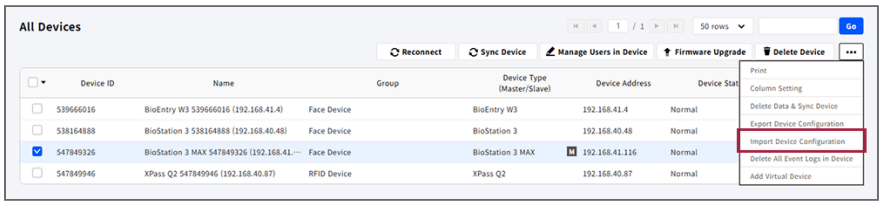
The following configurations are not included in the export file because they must be unique per device, are stored only on the device, or contain sensitive information such as credentials.

- Device-specific configurations: Name, Group, wired and wireless network, server connection, OSDP identifier, and Trigger & Action
- These configurations are stored only on the device. You cannot move them to another device: language resources, Home screen, and sound options in Display/Sound, the SCB key for serial communication, and video options added to BioStation 3 Max
- Credentials and sensitive information: usernames and passwords for IP intercom and RTSP, Master Admin, and the Two-step Authentication option

Import device configuration

To apply the exported configurations file to one or more devices of the same model, follow these steps.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Device** on the left sidebar.
3. In the device list, click the checkbox for the device that will receive the configurations. You can select one or more devices.
4. Click ••• → **Import Device Configuration** at the top of the device list.



5. When the Open window appears in the web browser, select the configurations file saved locally.

6. When the Import device configurations result message appears, review it and click **Ok**.

> **Caution**
> The system accepts configuration files created on other sites or servers as valid files without verifying the source or showing a warning. Verify that a trusted source created the file to import.

> **Info**
> Select at least one device to run this feature.

When you run Import, the system checks the following in order before applying the configurations. If any check fails, the system does not apply the configurations and shows the reason.

- Whether all selected devices have the same model name (including the part number)
- Whether the RS-485 communication mode matches between the selected devices and the file
- Whether the model name saved in the file (including the part number) matches the model names of the selected devices (including the part number)
- Whether any of the selected devices is a virtual device (Virtual Device)

If the checks pass, the system applies all configurations except Configurations excluded from export to all selected devices.

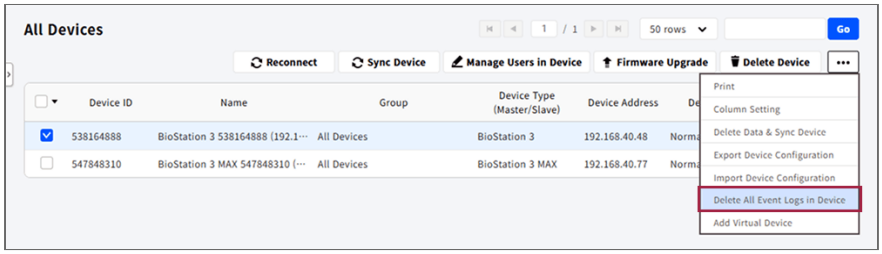
> **Info**
>
> - Importing a file from an unsupported device sets the feature Off and turns off enabled options. Importing a file from a supported device into an unsupported device skips the feature and applies the remaining configurations. In both cases, the system does not mark the import as failed or add it to the failure list.
> - Configurations that require a device license do not apply to devices without that license. Importing a file from an unlicensed device sets the configuration Off and turns off enabled options. In both cases, the system does not mark the import as failed or add it to the failure list.
> - The system shows a success message after it applies the configurations to all devices. If configurations fail to apply, a message shows failed device count and a link to download the CSV failure list. The file lists each failed device ID, name, and reason (disconnected, or access groups block full access permissions).
>
> > *For example, if an import run at 15:45:30 on 6/23/2026 fails, the file name is `Device_Template_Import_Error_20260623T154530.csv`.*
>
> - CoreStation devices are also included.
> - View the export and import history for device configurations at **Settings** → **Audit Trail** → **AC Audit Log**.

Delete event logs from a device

You can delete event logs stored on the device.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Device** on the left sidebar.
3. Click the checkbox for the device you want in the device list. You can select 1 or more devices.

4. Click ••• → **Delete All Event Logs in Device** at the top of the device list.



5. If a warning dialog appears, review the message and click **Continue**.

When the device event log deletion is complete, a pop-up message appears. View the number of target devices, successful devices, and failed devices.

> **Caution**
>
> Event logs deleted from a device cannot be recovered and cannot be resent from the server to the device. Before proceeding with deletion, confirm the device event logs are stored on the server. Also, if the selected devices include slave, virtual, or Wiegand devices, those devices do not store logs and are excluded from log deletion.

> **Info**
>
> - Only users with the **Administrator Role** permission can use this feature.
> - View the device event log deletion history at **Settings** → **Audit Trail** → **AC Audit Log**.

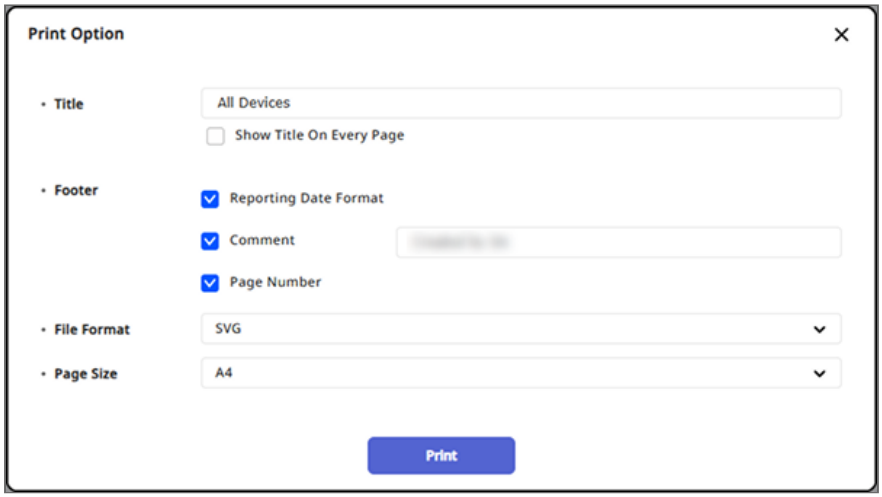
Additional features

Use additional features such as printing the device list or changing column settings.

Print device list

Save the device list as a PDF or SVG file for printing.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Device** on the left sidebar.
3. Click ••• at the top of the device list.
4. Click **Print** in the popup menu.
5. When the **Print Option** window appears, select your desired format in the **File Format** options and set the other options.



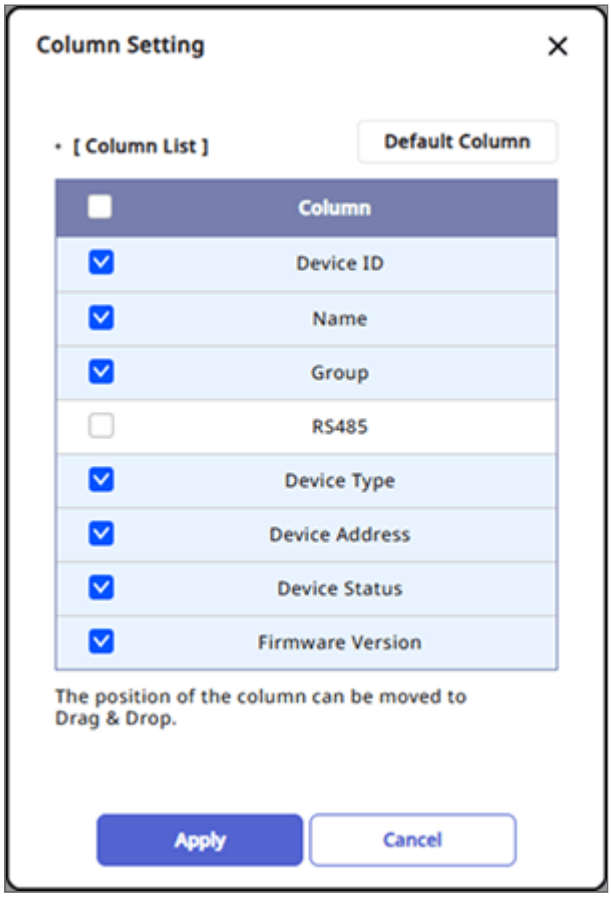
6. Click **Print**.

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

Device List Column (Column) Settings

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

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Device** on the left sidebar.
3. Click ••• at the top of the device list.
4. Click **Column Setting** in the popup menu.
5. When the **Column Setting** window appears, select or deselect the desired columns.



6. To change the order of the columns, click and drag the desired column to change its position.
7. Click **Apply** to save the settings.

> **Info**
> To initialize the column settings, click **Default Column**.

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.

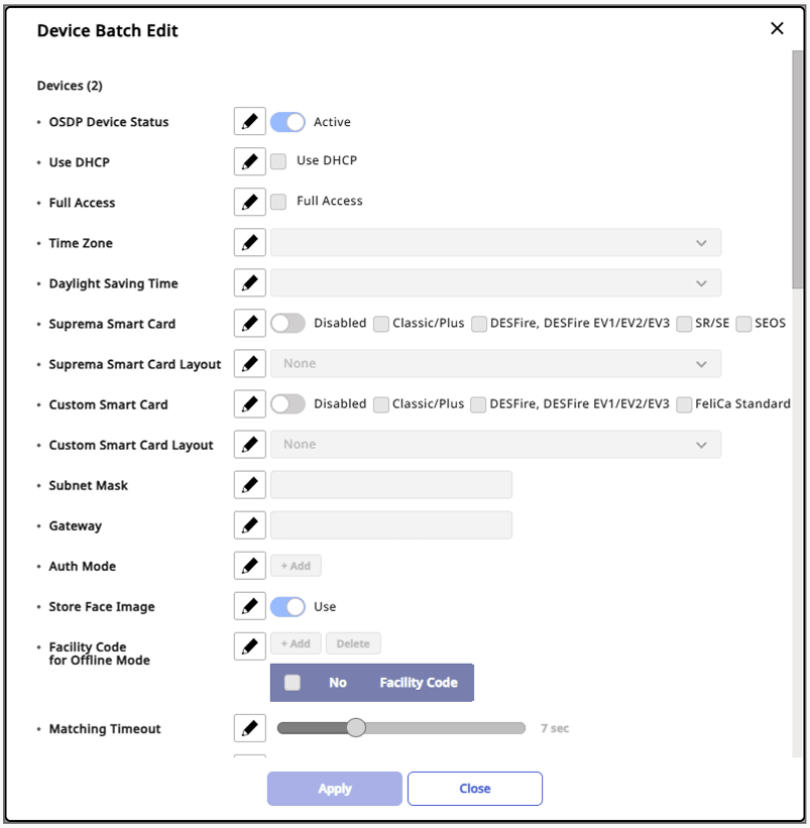
1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Device** on the left sidebar.
3. Select the device you want to configure from the device list.
4. Reference the details in each section to configure the device information.
   - **Information**: Verify and modify the device's name and group, time zone, hardware, and firmware versions. For more information, see Basic Information Setting.
   - **Network**: Configure the network settings of the device for TCP/IP, RS-485, and server communication. For more information, see Network Settings.

- **Authentication**: Configure options related to user authentication for the device. For more information, see Authentication Settings.
- **Advanced**: You can configure Master Administrator, Device Management, Display/Sound, Operating Conditions, and Actions. For more information, see Advanced Settings.
- **Thermal & Mask** / **Mask**: Configure details related to thermal camera and mask usage. For more information, see Thermal and Mask Settings.
- **Intercom**: Configure details for using the IP intercom. For more information, see Intercom Settings.
- **RTSP**: Set details for **Real Time Streaming Protocol** (RTSP) streaming. For more information, see RTSP Settings.

5. Once all configurations are complete, click **Apply** at the bottom of the screen.

Info

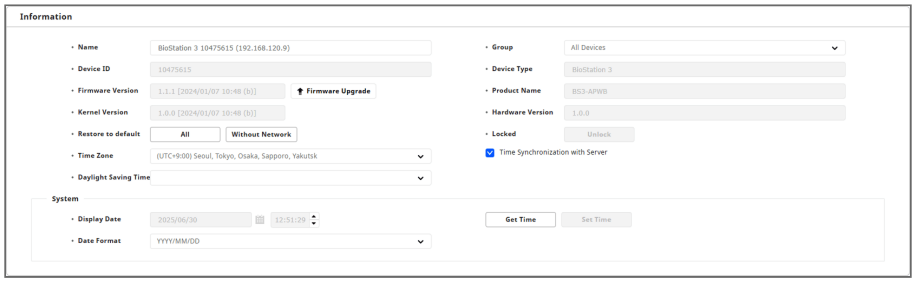
- You can also modify the information of multiple devices at once. Select two or more devices, then click **Batch Edit** in the upper right corner of the screen.



- 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.



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 on creating, renaming, or deleting device groups, see Manage Device Groups.

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 on upgrading device firmware, see Upgrade Firmware.

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. To add a new daylight saving time, see 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 trigger conditions and action settings, see Trigger and Action Settings.

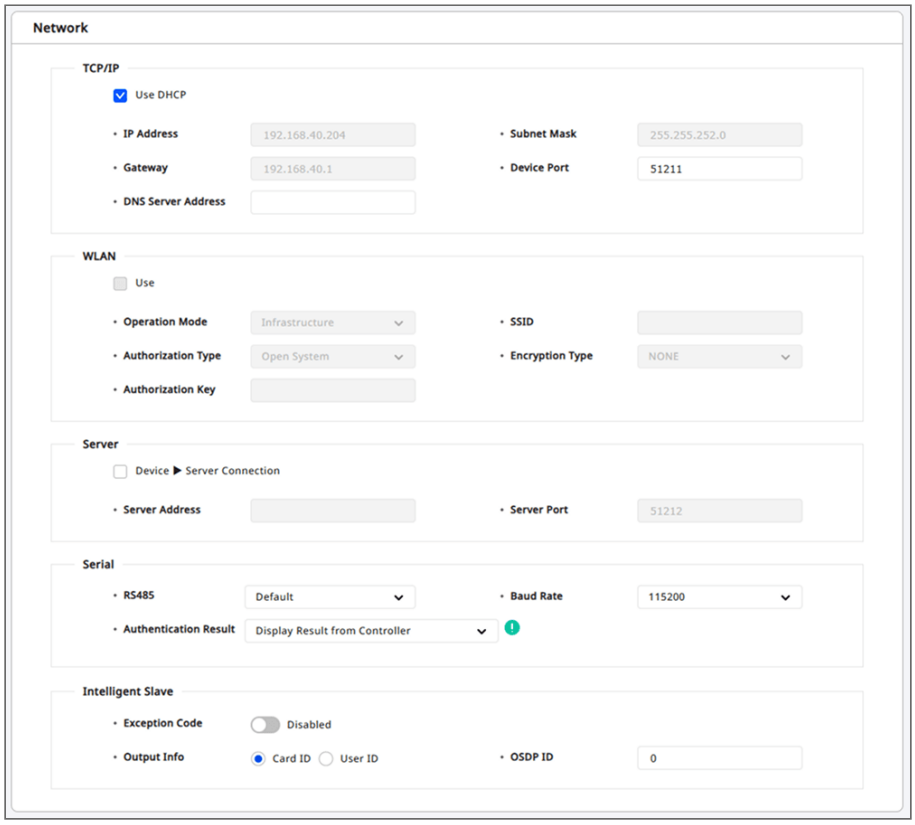
Initialize the device

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.



> **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 on IP address settings when registering a device, see Register Device.

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 3 Max firmware 1.0.0 or later
- XPass Q2 firmware 1.0.0 or later
- BioEntry W3 firmware version 1.0.0 or higher
- BioStation 3 firmware 1.0.0 or higher
- X-Station 2 firmware 1.0.0 or higher
- FaceStation F2 firmware 1.0.0 or higher
- XPass 2 firmware 1.0.0 or higher
- FaceLite firmware 1.0.0 or higher
- BioLite N2 firmware 1.0.0 or higher
- FaceStation 2 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

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 3 Max firmware 1.0.0 or later
- XPass Q2 firmware 1.0.0 or later
- BioEntry W3 firmware version 1.0.0 or higher
- BioStation 3 firmware 1.0.0 or higher
- X-Station 2 firmware 1.0.0 or higher
- FaceStation F2 firmware 1.0.0 or higher
- XPass 2 firmware 1.0.0 or higher
- FaceLite firmware 1.0.0 or higher
- BioLite N2 firmware 1.0.0 or higher
- BioEntry P2 firmware 1.0.0 or higher
- FaceStation 2 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

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.

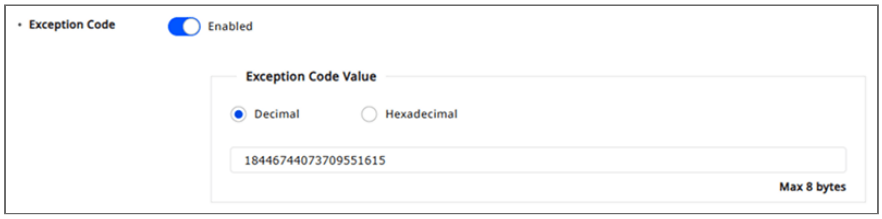
Info

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.



- **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

- BioStation 3 Max firmware 1.0.0 or later
- XPass Q2 firmware 1.0.0 or later
- BioEntry W3 firmware version 1.0.0 or higher
- BioStation 3 firmware 1.0.0 or higher
- X-Station 2 firmware 1.1.0 or higher
- FaceStation F2 firmware 1.1.2 or higher
- XPass 2 firmware 1.2.3 or higher
- BioLite N2 firmware 1.4.1 or higher
- BioEntry P2 firmware 1.4.1 or higher
- BioEntry W2 firmware 1.6.3 or higher
- BioStation L2 firmware 1.6.1 or higher

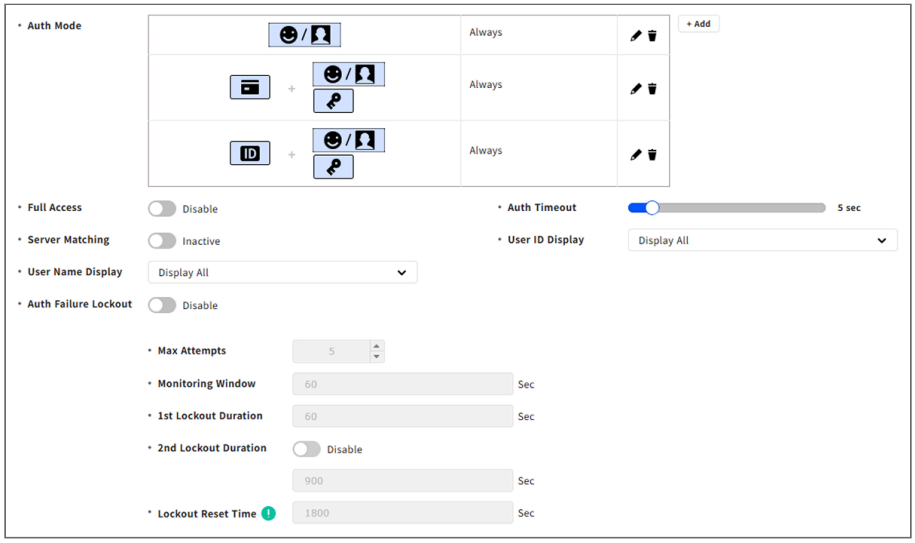
Authentication Settings

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 **Apply**. 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**: Set the authentication mode of the device by combining one or more credentials. For more information, see Add authentication mode.
  - 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**
> – BioStation 3 Max firmware 1.0.0 or later

  - XPass Q2 firmware 1.0.0 or later
  - BioEntry W3 firmware version 1.0.0 or higher
  - BioStation 3 firmware 1.0.0 or higher
  - X-Station 2 firmware 1.0.0 or higher
  - FaceStation F2 firmware 1.0.0 or higher
  - XPass 2 firmware 1.0.0 or higher
  - BioLite N2 firmware 1.0.0 or higher
  - XPass D2 firmware version 1.0.0 or higher
  - BioEntry P2 firmware 1.0.0 or higher
  - FaceStation 2 firmware version 1.4.0 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
  - CoreStation firmware version 1.0.0 or higher
  - FaceLite does not support server matching feature.
  - The BioStation 3, BioEntry W3, and FaceStation F2 devices cannot use server-based 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**
- **Auth Failure Lockout**: If authentication fails repeatedly within a short time, the device locks for a certain period. This blocks brute-force attacks. Set this option to **Enable** to configure the settings below. The default is **Disable**.
  - **Max Attempts**: Set the number of authentication failures allowed before lockout to 3~15 attempts. The default is 5 attempts.
  - **Monitoring Window**: Set the time window for counting authentication failures to 30~300 seconds. The default is 60 seconds.

- **1st Lockout Duration**: Set the lockout time applied when failures reach **Max Attempts** to 30~900 seconds. The default is 60 seconds, and a value is required.
- **2nd Lockout Duration**: 2nd lockout time, applied when authentication failures continue even after the 1st lockout is cleared. Set this option to **Use** to enter a value between 900~3,600 seconds. The default is 900 seconds.

> Set this option to **Disable** to repeatedly apply only the 1st lockout, without a 2nd lockout.

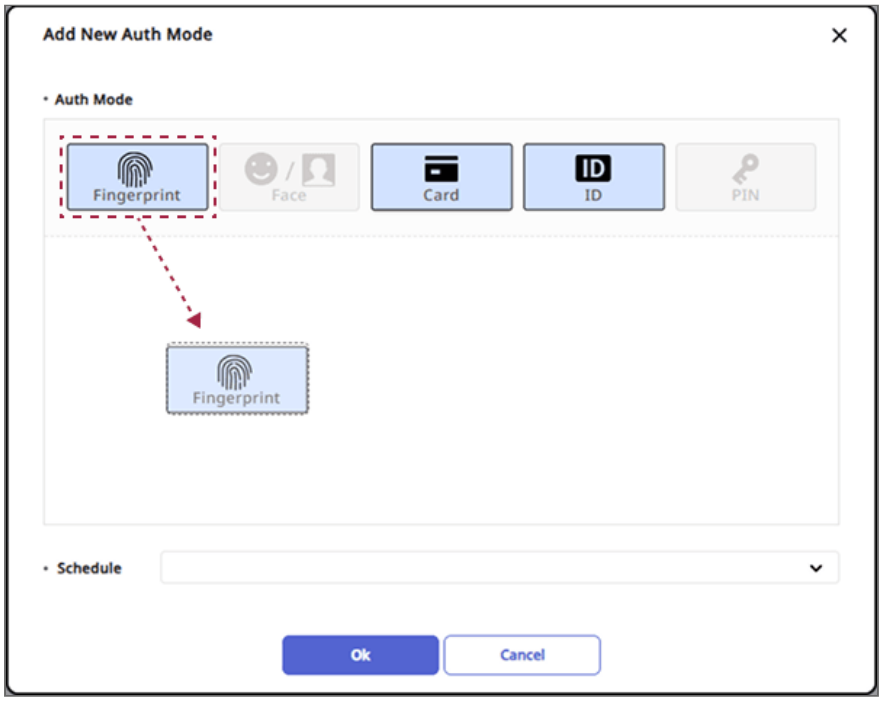
- **Lockout Reset Time**: If no additional failures occur within this time after the last failure, the device initializes the cumulative failure count. Set it to 600~3,600 seconds. The default is 1,800 seconds.

> **Info**
>
> - When the device is locked, change **Auth Failure Lockout** to **Disable** and save. The device unlocks immediately. However, changing **2nd Lockout Duration** to **Disable** and saving does not unlock the device.
> - Support for the **Auth Failure Lockout** option is included in BioStation 3 firmware 1.5.0 or later.

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.



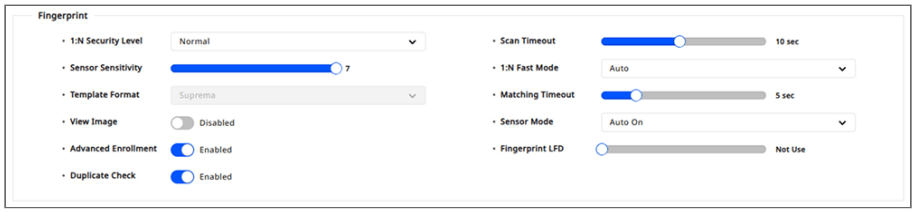
You can add up to five desired authentication modes.

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 on schedule settings, see Schedule Settings.

Fingerprint authentication settings

In the **Fingerprint** group, you can configure details related to the device's fingerprint authentication.



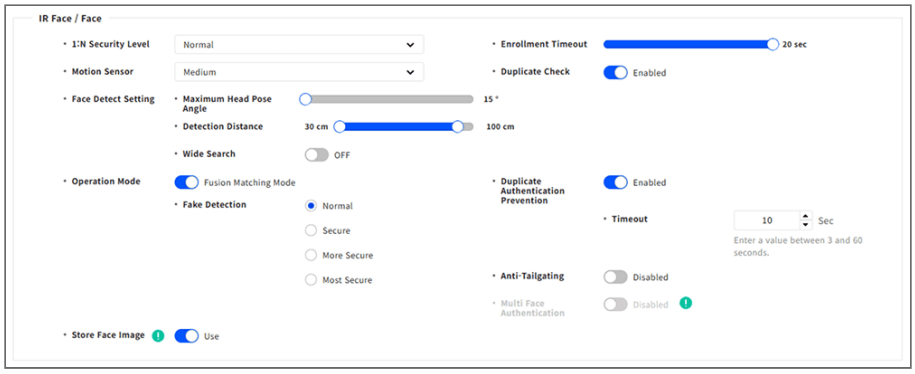
- **1:N Security Level**: Set the security level used for authenticating fingerprints. Higher security levels increase the False Rejection Rate (FRR) but decrease the False Acceptance Rate (FAR).
- **Scan Timeout**: Set the timeout for fingerprint scanning. Failure to scan within the time set will result 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.
- **View Image** option is supported on BioStation 3 Max (BS3M-ODB, BS3M-OAPB), X-Station 2 (XS2-ODPB, XS2-OAPB), FaceStation F2 (FSF2-ODB), BioLite N2, BioStation L2, BioStation A2, and BioStation 2.
- **Fingerprint LFD** option is supported on BioStation 3 Max (BS3M-ODB, BS3M-OAPB), X-Station 2 (XS2-ODPB, XS2-OAPB), FaceStation F2 (FSF2-ODB), BioLite N2, BioStation L2, BioStation A2, and BioEntry W2.

Facial authentication settings

In the **IR Face / Face** or **Face** group, you can configure the device's facial authentication settings.



- **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 Timeout**: 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.

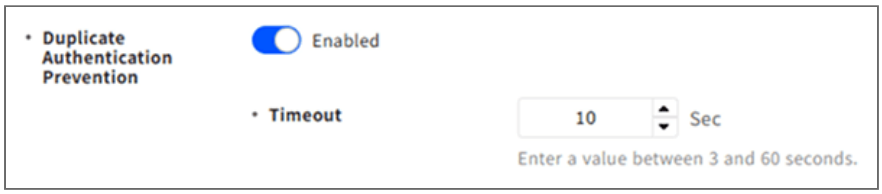
  - **Fusion Matching Mode**: Perform both visual and infrared matching to enhance the accuracy of facial authentication.

  - **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**.

- **Store Face Image**: Stores both the actual facial image and a template containing only the extracted feature data. Disable this setting if you do not want to store the actual image.

- **Duplicate Authentication Prevention**: Set this to prevent duplicate authentication when the same user's face is detected again within a short time. Set this option to **Enable** and set **Timeout** to 3~60 seconds.



> This setting applies to both **Anti-Tailgating** and **Multi Face Authentication**, regardless of which option is enabled.

- **Anti-Tailgating**: If the camera detects 2 or more faces at the same time within the device camera's capture range, it considers this tailgating and stops authentication.

- **Multi Face Authentication**: Authenticates multiple users in sequence within the camera view.

> – This option requires a separate device license. Devices without a license cannot enable this option. For more information, see Device License.
> – Set this option to **Use** to use Facial Authentication only, regardless of the **Auth Mode** setting.
> – Devices that use this option cannot use **T&A** or **Server Private Message**.

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.
- **Face Detect Setting**, **Operation Mode** options are supported on BioStation 3 Max, BioStation 3, and FaceStation F2 models.
- Do not set **Anti-Tailgating** and **Multi Face Authentication** to **Use** at the same time. Set one option to **Use**; the other automatically switches to **Not Use**.
- Set **Duplicate Authentication Prevention** and **Multi Face Authentication** only on the master device. Set the **Anti-Tailgating** option separately on the master and slave devices.
- Support for **Duplicate Authentication Prevention**, **Anti-Tailgating**, and **Multi Face Authentication** may vary by device model and firmware version.
  - BioStation 3 firmware version 1.5.0 or later

QR/Barcode settings

In the **QR/Barcode** group, you can configure details for QR/barcode authentication on the device.



- **Use QR/Barcode through Camera** / **Use QR/Barcode**: Set whether to use QR/barcode authentication through the device's camera.
- **Camera Timeout** / **Scan 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.
- **LED Light**: Set whether to use the device's LED illumination when authenticating QR codes.

Info

- The **Use QR/Barcode through Camera** option requires a separate device license. For more information, see Device License.
- The devices supporting **Use QR/Barcode through Camera**, **Camera Timeout**, **Use QR as Card**, and **Motion Sensor** options are as follows.
  - BioStation 3 Max firmware version 1.0.0 or later
  - BioStation 3 firmware version 1.1.0 or later
  - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) firmware version 1.2.0 or higher
  - X-Station 2 (XS2-QDPB, XS2-QAPB) firmware version 1.4.1 or higher
- The devices supporting **Use QR/Barcode through Scanner** and **Scanner Timeout** options are as follows.
  - X-Station 2 (XS2-QDPB, XS2-QAPB)
- **Use QR/Barcode**, **Scan Timeout**, **LED Light** options are supported on the following devices.
  - XPass Q2 firmware 1.0.0 or later

Card authentication settings

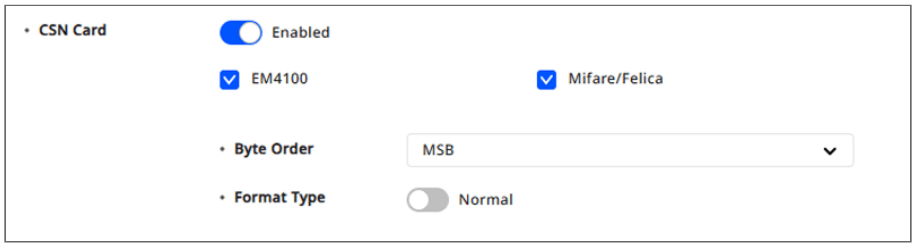
In the **Card Type** group, you can set the types of cards to be used on the device.

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.

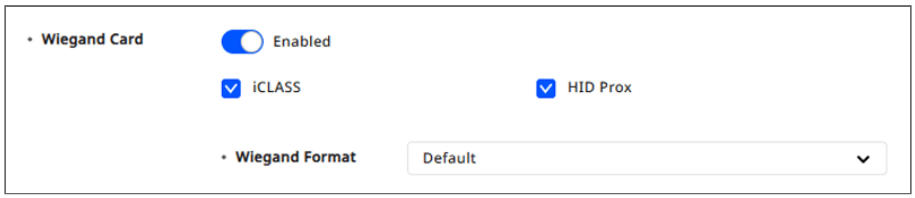


- **Byte Order**
  - **MSB**: Processes card data in order from large byte units to small byte units, sequentially storing the card serial number (CSN) from left to right.
  - **LSB**: Processes card data in order from small byte units to large byte units, storing the card serial number (CSN).
- **Format Type**
  - **Normal**: 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. See Set Wiegand Card Format to set a new Wiegand format.

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.

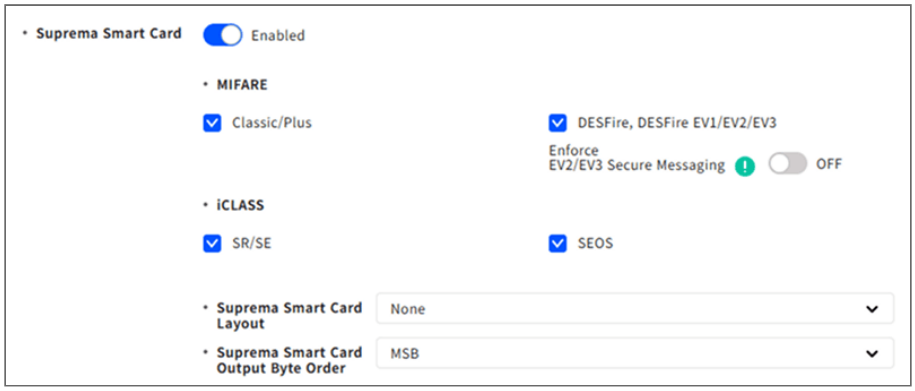


Info

See Set Wiegand Card Format to set a new Wiegand format.

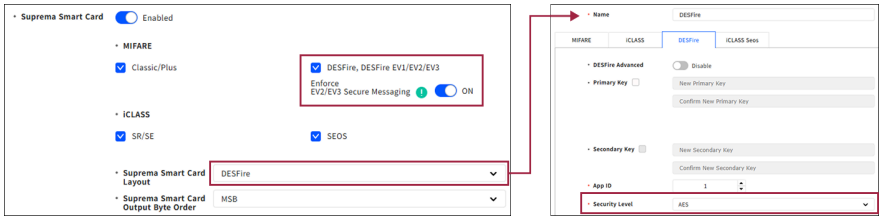
Suprema Smart Card

Select the types of Suprema smart cards and set the card layout and byte order.



- **Enforce EV2/EV3 Secure Messaging**: Set this option to **ON** to authenticate only with cards that support EV2 secure messaging (DESFire EV2/EV3). The device rejects DESFire EV1 cards that do not support EV2 secure messaging.

  This option becomes available when you select **DESFire, DESFire EV1/EV2/EV3** and **Security Level** of the selected **Suprema Smart Card** is **AES**. If **Suprema Smart Card** is not in use, this option appears as **OFF**.

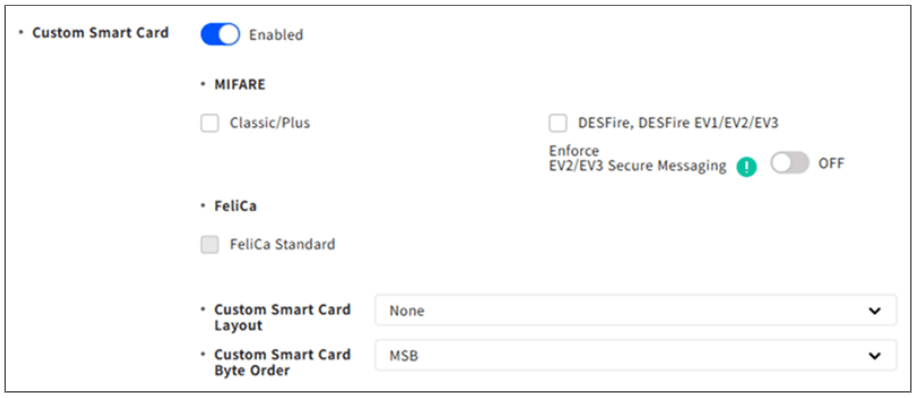


- **Suprema Smart Card** and **Custom Smart Card** share the same settings. If either one is in use, a confirmation message appears when changing either value. Click **Ok** in the dialog to change both options together. If either option does not use a smart card, change the value without a confirmation dialog.
- Secure messaging is available only on DESFire EV2 and EV3 cards. Enable DESFire, and set the card layout encryption type to AES.
- If the device does not support EV2 secure messaging, the **Enforce EV2/EV3 Secure Messaging** option does not appear.
- To set this option for multiple devices, use **Device Batch Edit**. Batch editing automatically excludes devices that do not support EV2 secure messaging.

- **Suprema Smart Card Layout**: Choose the Suprema smart card layout. See Set Smart Card Format to set a new smart card layout.
- **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.

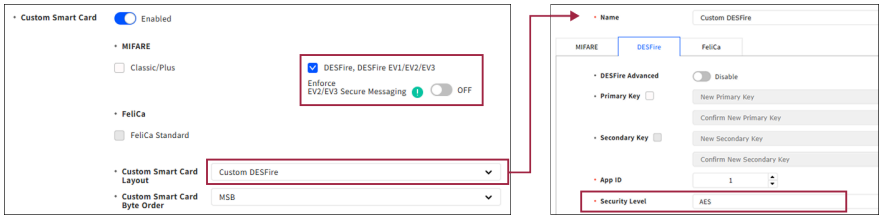
Custom Smart Card

Select types of custom smart cards issued by third parties and set the card layout and byte order.



- **Enforce EV2/EV3 Secure Messaging**: Set this option to **ON** to authenticate only with cards that support EV2 secure messaging (DESFire EV2/EV3). The device rejects DESFire EV1 cards that do not support EV2 secure messaging.

  This option becomes available when you select **DESFire, DESFire EV1/EV2/EV3** and **Security Level** of the selected **Custom Smart Card** is **AES**. If **Custom Smart Card** is not in use, this option appears as **OFF**.



> – **Suprema Smart Card** and **Custom Smart Card** share the same settings. If either one is in use, a confirmation message appears when changing either value. Click **Ok** in the dialog to change both options together. If either option does not use a smart card, change the value without a confirmation dialog.
> – Secure messaging is available only on DESFire EV2 and EV3 cards. Enable DESFire, and set the card layout encryption type to AES.
> – If the device does not support EV2 secure messaging, the **Enforce EV2/EV3 Secure Messaging** option does not appear.
> – To set this option for multiple devices, use **Device Batch Edit**. Batch editing automatically excludes devices that do not support EV2 secure messaging.

- **Custom Smart Card Layout**: Choose the custom smart card layout. See Set Smart Card Format to set a new smart card layout.
- **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**

- BioStation 3 Max firmware version 1.3.0 or higher
- XPass Q2 firmware 1.0.0 or later
- BioEntry W3 firmware version 1.0.0 or higher
- BioStation 2a firmware version 1.1.0 or higher
- BioStation 3 firmware version 1.3.0 or higher
- X-Station 2 firmware version 1.3.0 or higher
- BioLite N2 firmware version 1.6.2 or higher
- 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

CSN Mobile

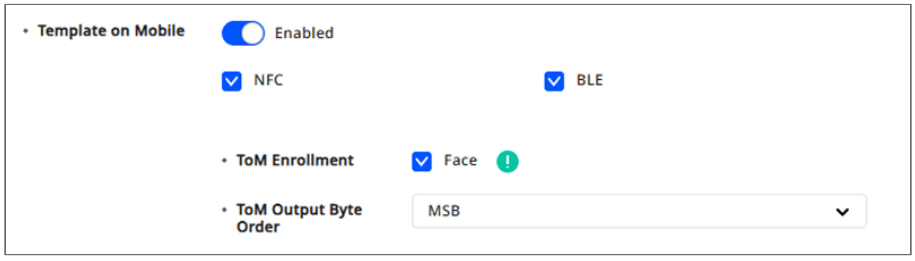
You can set the method for recognizing mobile cards.



- **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.



- **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 Max firmware 1.0.0 or later
- BioEntry W3 firmware version 1.0.0 or higher
- BioStation 3 firmware version 1.2.0 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.



> **Info**
> The **Scramble Keypad** option is only available on Suprema products that support user interfaces through the LCD screen.

Advanced Settings

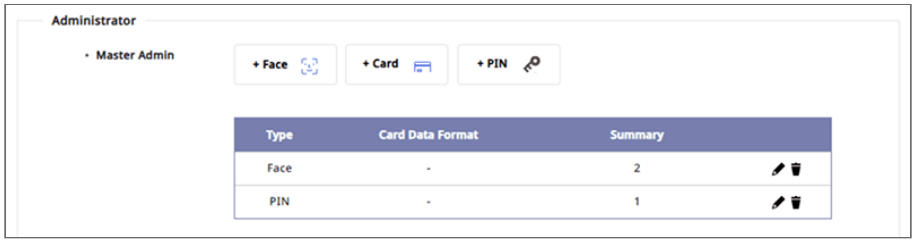
This section provides guidance on configuring items in the **Advanced** settings. You can check how to configure various advanced features such as Master Administrator, administrator permission management, attendance events, screen and sound, operating conditions and actions, image logs, Wiegand, security 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 **Apply**. Changes will not be applied to the device if not saved.

Add master administrator CE products

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.



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.

Credential Type	Number of Enrollments	Conditions
Fingerprint	Up to 2	-
PIN	1	Must enter at least 8 digits.

- To change the enrolled credential, click ✎ to the right of that credential.
- To delete the enrolled credential, click 🗑 to the right of that credential.

Caution

This feature is available only on **CE products** that support an LCD user interface. For more information on supported devices and firmware versions, see Master Admin Setup Guide.

Enrollment conditions

- You must enroll at least two types of credentials.
- The same conditions apply to all firmware-upgraded devices that support master administrators.
- 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 had their firmware upgraded do not show the **Master Admin** menu in BioStar X's device settings.
- Certain devices do not include the **Master Admin** setting (for example, devices updated by a firmware upgrade). Use the **Two-step Authentication** option to enhance administrator permissions. Depending on the device, the **Two-step Authentication** option may not appear.
- Master administrator credentials are stored separately on the device and managed independently of user PINs. Changing or deleting a user PIN does not affect master administrator credentials.

Two-step authentication setting

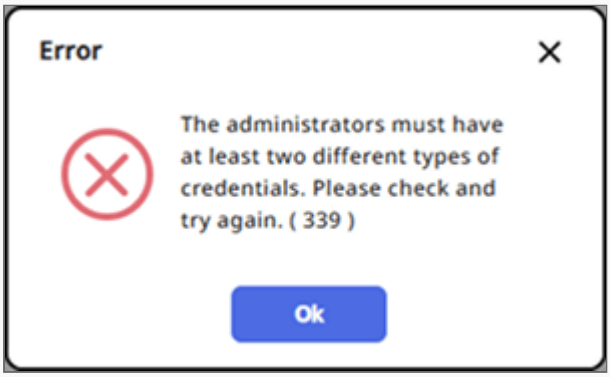
After upgrading firmware on a global device that does not support **Master Admin**, enable the **Two-step Authentication** option. This enhances full administrator permissions and improves security.



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

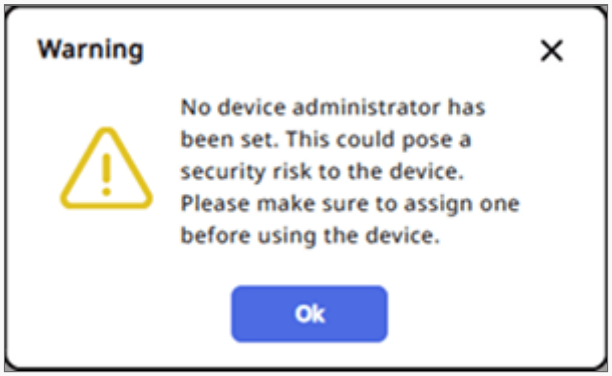
- If fewer than 2 types of credentials are enrolled for all administrators, activation fails and an error message is displayed. Enroll 2 or more types of credentials for all administrators and try again.



- Depending on the device, **Two-step Authentication** may not appear, but the previously enabled setting remains active. BioStar X does not let users disable this setting. Contact Suprema Global Technical Support Team.

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**.

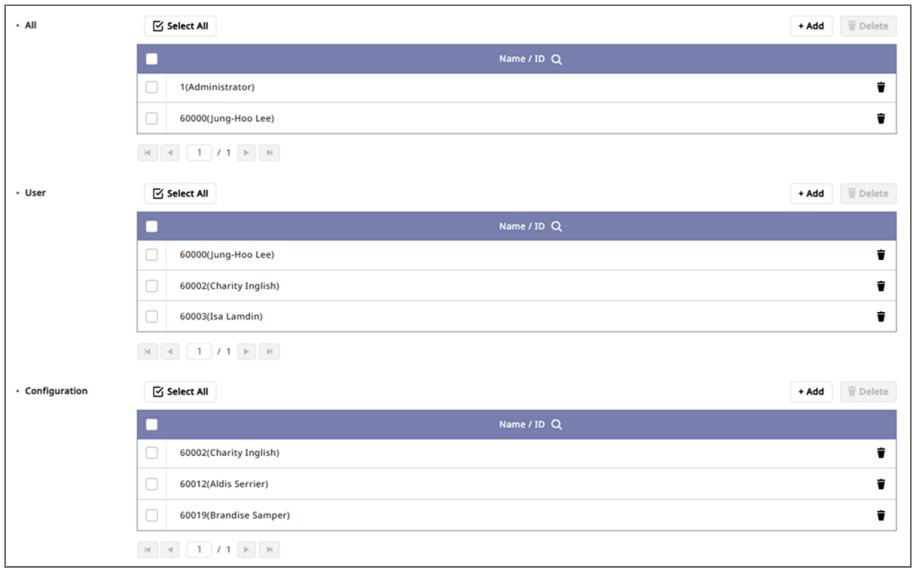


Warning

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.



To add an administrator by permission level, click **+ Add**. When the user list appears, select the desired user. You can also search for the desired user by clicking 🔍 in the user list.

Refer to the permissions for each level below.

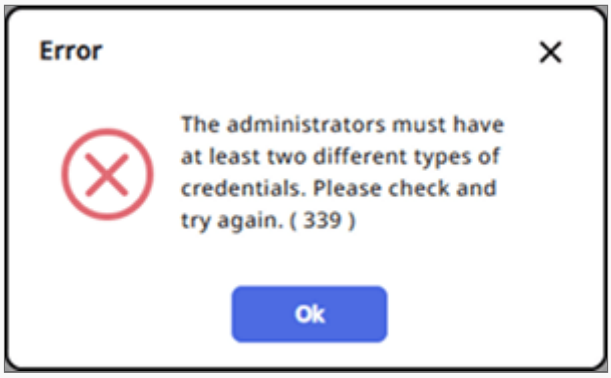
Level	User Information Management	Device Settings
All	✔	✔
User	✔	✕
Configuration	✕	✔

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 🔍 in **Name / ID**.
- **Device Settings** allows changes to settings for screen and sound, network, RS-485, etc.
- To delete an administrator, click 🗑 to the right of the administrator.
- Administrators set for each device do not affect **BioStar X** permissions.
- If a device administrator registered on a device that supports master administrators (**CE products**) has a PIN shorter than 8 digits, enroll the PIN again with at least 8 digits. For more information on enrolling PINs, see Enroll PIN.
- First, remove the user from administrator roles on all devices. Then change the PIN to 4 digits for the user with **Configuration** permissions.

Caution

If the user being set as a device administrator has fewer than 2 types of credentials enrolled, an error message appears. Enroll 2 or more types of credentials for all device administrators and try again.



Handle administrator registration for deleted users

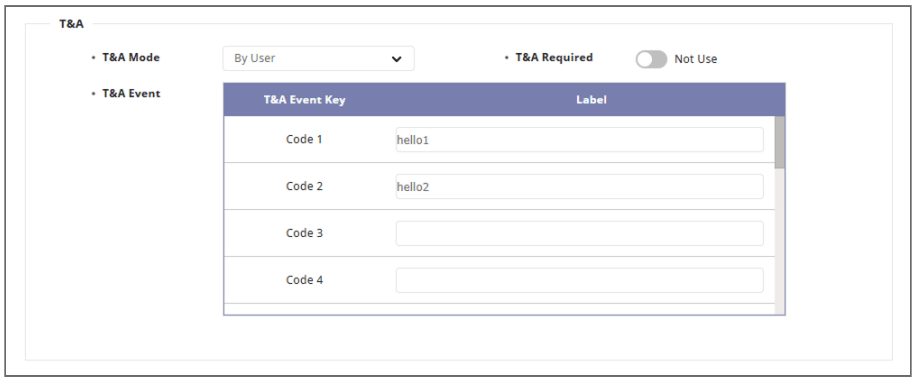
If the device administrator list includes a user deleted from **BioStar X**, a pop-up appears when you save the settings. Click **Apply** at the bottom of the screen.



- **Yes**: Remove the deleted user from the administrator list and save the settings.
- **No**: Cancel saving.

Attendance management

The **T&A** group allows you to change attendance event names or set attendance modes.



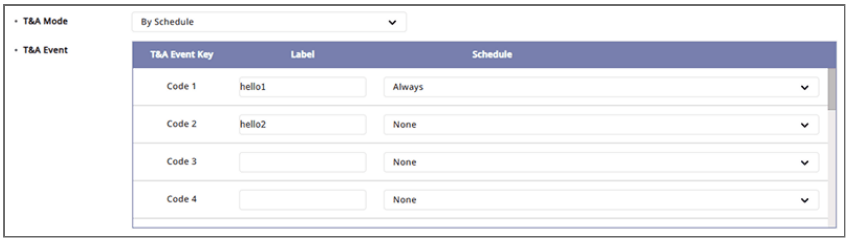
- **T&A Mode**: Set how attendance events are registered.

  - **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**.



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. Supported devices are XPass Q2, XPass 2, XPass D2, BioEntry P2 and BioEntry W2.
- For more information on setting up a new schedule, see Schedule Settings.
- Setting **Multi Face Authentication** to **Use** on the device disables time and attendance management. For more information on **Multi Face Authentication**, see Authentication Settings.

Screen and sound settings

You can change settings related to the device's screen and sound. Available options may vary depending on the device.

▼ **XPass 2, XPass D2, BioEntry P2, BioEntry W2**

- **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.

▼ **FaceLite, BioLite N2, BioStation L2, BioStation 2**

- **Language**: Set the language to be displayed on the device's screen. Click **Update Resource** 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 **Add** 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 **Add** to register an image.

  > – To reflect changes in real time on the device, click **Update**.
  > – If you change the type of background wallpaper, clicking **Update** will not apply it to the device. At the bottom of the screen, click **Apply**.
  > – 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 **Browse**.

  > To reflect changes in real time on the device, click **Update**.

▼ **BioStation 3 Max, BioStation 3, X-Station 2, FaceStation F2, FaceStation 2, BioStation A2**

- **Language**: Set the language to be displayed on the device's screen. Click **Update Resource** 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.

> Setting **Multi Face Authentication** to **Use** on the device disables this option. For more information on **Multi Face Authentication**, see Authentication Settings.

- **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 **Add** to register an image.
  - **Notice**: Administrators can display their input on the home screen.

> - To reflect changes in real time on the device, click **Update**.
> - If you change the type of background wallpaper, clicking **Update** will not apply it to the device. At the bottom of the screen, click **Apply**.
> - Setting the home screen as **Logo** and **Slide Show** allows displaying up to 10 images as a slideshow on the home screen. Click **Add** 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 **Browse**.

> To reflect changes in real time on the device, click **Update**.

- **Default Idle Screen**: Select the idle screen that appears when the device is not in use.
  - **Screen Saver**: Shows the screen saver as the idle screen.
  - **Home Screen**: Shows the option selected under **Home Screen**.

> - This option is supported on BioStation 3 Max, BioStation 3, X-Station 2, FaceStation F2, and FaceStation 2.
> - For more information on the **Play Video** option, see Play a video on the idle screen.

▼ XPass Q2

LED/Buzzer: Select and set the event items that will activate the LED or buzzer.

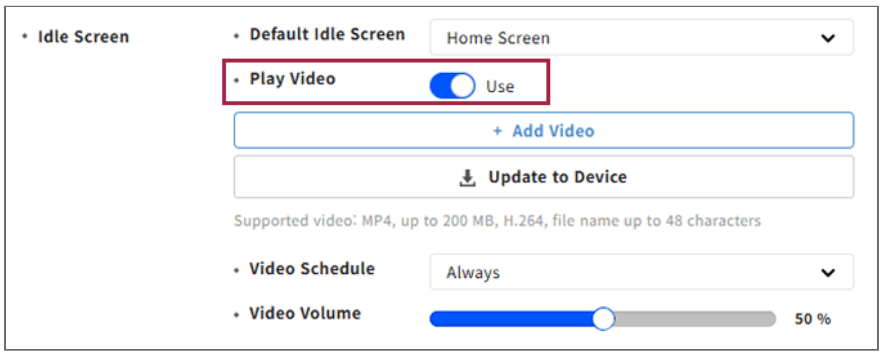
Play a video on the idle screen

> The feature to play videos on the idle screen is supported on **BioStation 3 Max** firmware version 1.1.0 or later. Prepare the video before sending it to the device.

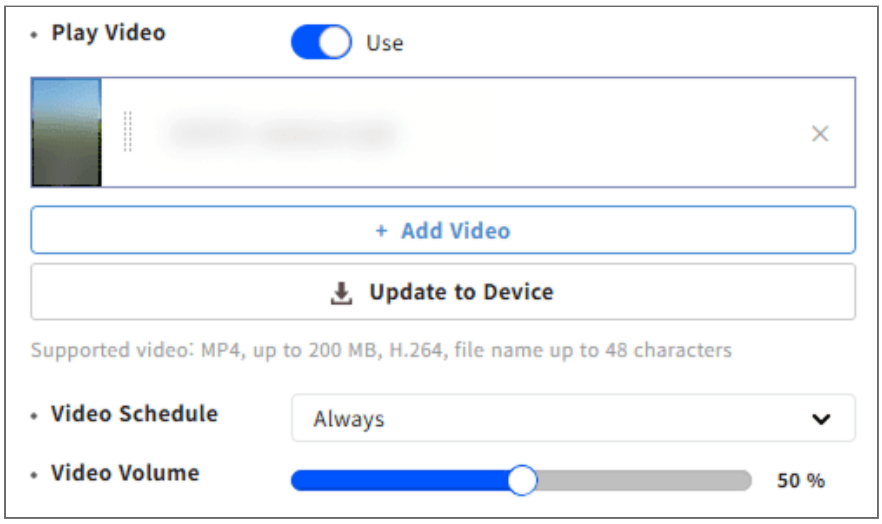
Add a video and transfer it to the device

Set the device to play specific content on the idle screen.

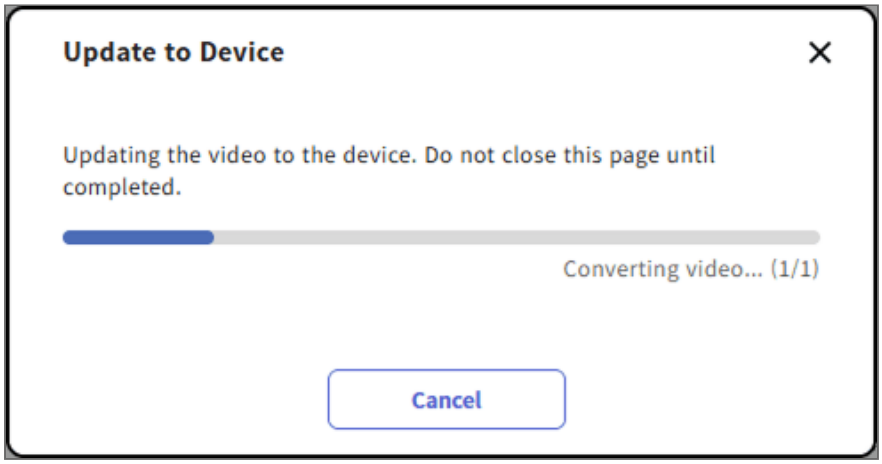
1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Device** on the left sidebar.
3. In the device list, click **BioStation 3 Max**.
4. Go to the **Advanced** → **Display/Sound** section.
5. **Idle Screen** → **Play Video** option: Set it to **Use**.



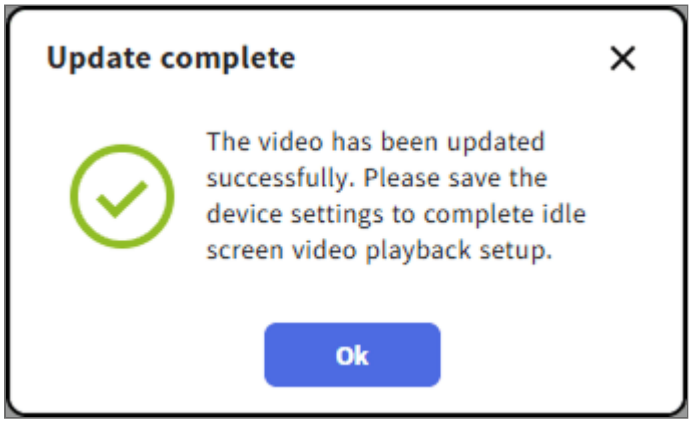
6. Click **Add Video**.
7. Select the video saved locally.
8. After the video uploads, set **Video Schedule** and **Video Volume**.



9. Click **Update to Device** to transfer the uploaded video to the device.
10. The update progress pop-up appears. Do not close the page until the upload completes.



11. When the upload complete message appears, click **Ok**.



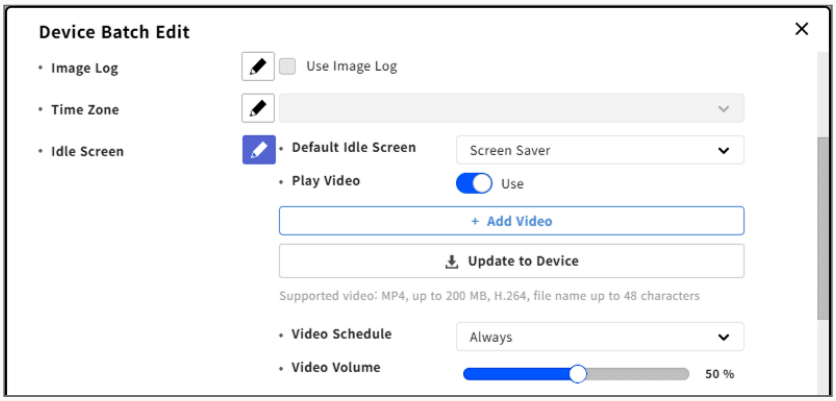
12. Click **Apply** at the bottom of the screen to save the changes.

Info

- Videos play only when **Play Video** is set to **Use**, at least 1 video is registered, and the schedule is configured in **Video Schedule**. For schedules that do not meet these conditions, the screen selected in **Default Idle Screen** appears.
- The maximum supported video file size is 200 MB, and the file format is MP4 (H.264).
- Video file names can be up to 48 characters long. The file name cannot include characters such as a period(`.`), apostrophe(`'`), or backtick(`` ` ``).
- Add up to 3 videos. When 3 videos are added, the **Add Video** button is disabled.
- If the device is connected as a slave (via RS-485), you cannot add, delete, or transfer videos.
  - If the master device supports video playback, the slave screen shows the master's video list as read-only. The list is read-only. Add, delete, transfer, and reorder videos on the master device only.
  - If the master device does not support video playback, the slave screen shows only **Default Idle Screen**.

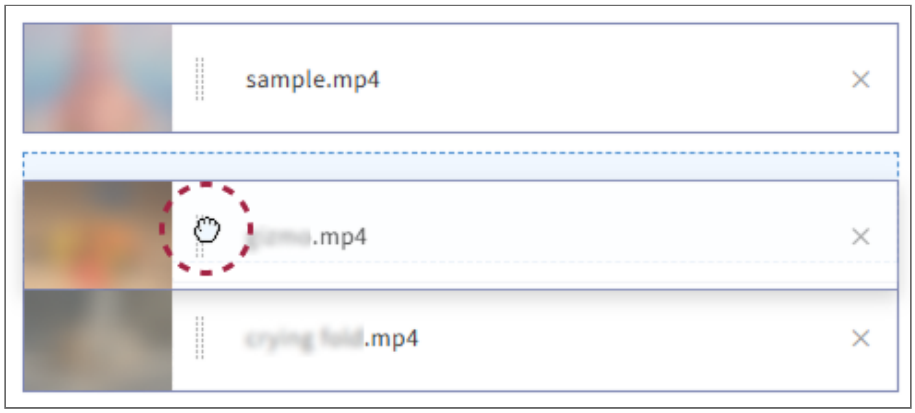
Tip

Use **Batch Edit** to add and transfer videos to multiple devices at once. For more information on the **Batch Edit** feature, see Use Device Management Feature.



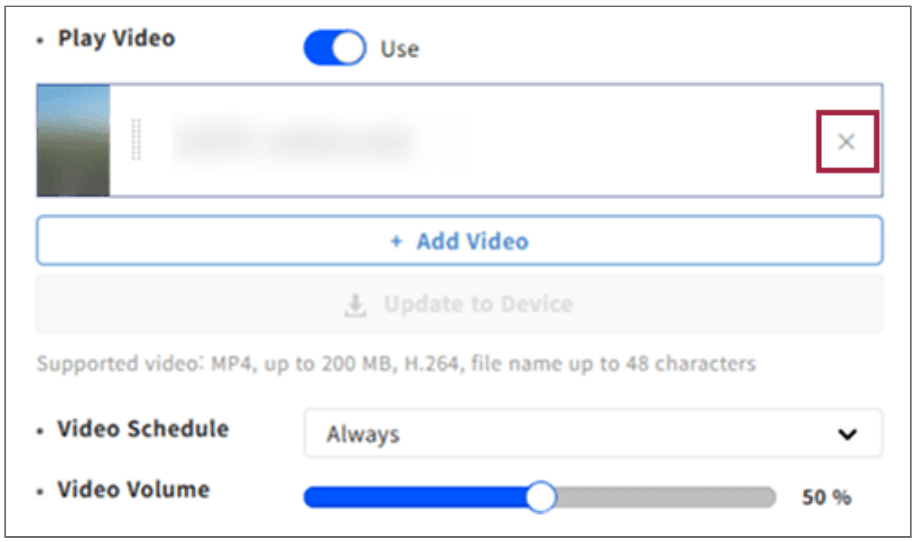
Change video playback order

Drag the area to the right of a video thumbnail to change the playback order. To save changes, click **Apply** at the bottom of the screen.



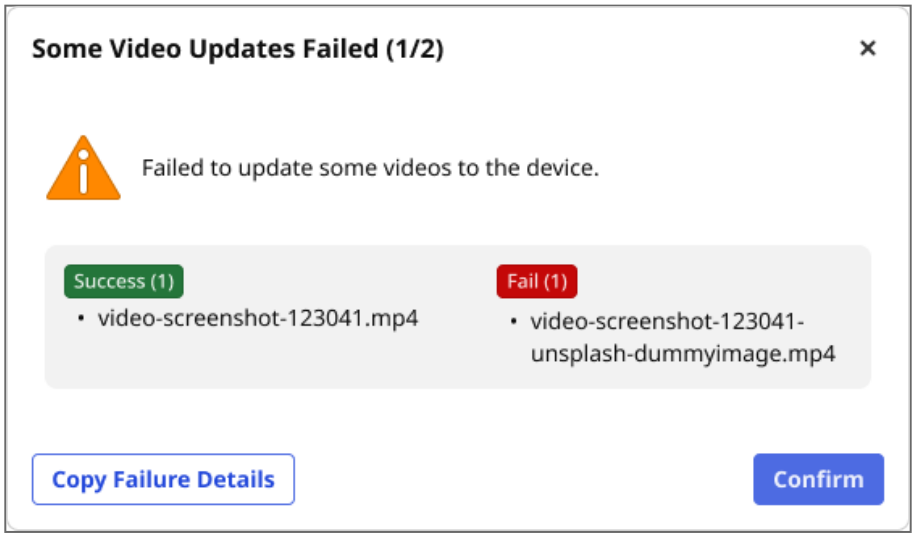
Delete videos

In **Idle Screen** → **Play Video**, click ✕ for the video to delete. Then click **Update to Device**. Click **Apply** at the bottom of the screen to save the changes.



Video transfer failure

If the video transfer to the device fails, a pop-up shows the name of the video that failed to transfer.



The main reasons for transfer failure are as follows.

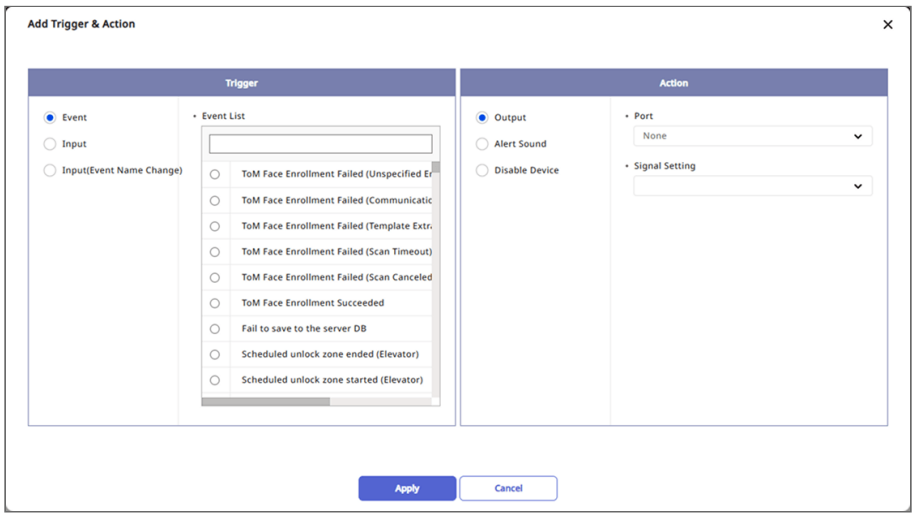
- When an error occurs while processing the device response
- When an error occurs for reasons other than those above

> **Tip**
> If video batch transfer to multiple devices using the **Batch Edit** feature fails on only certain devices, click **Copy Failure Details** in the results pop-up to copy the list of failed devices and reasons to the clipboard.

Trigger conditions and action 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 + **Add** on the right.



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 on schedule settings, see Schedule Settings.
> - 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

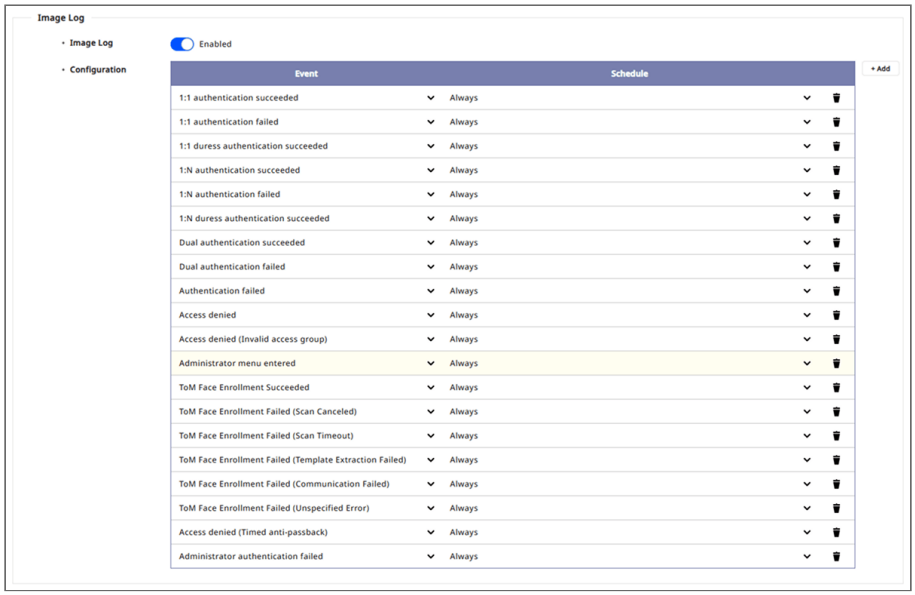
You can select predefined actions or add custom actions.

> **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.



Info

- This feature is supported on BioStation 3 Max, BioStation 3, X-Station 2, FaceStation F2, FaceStation 2, and BioStation A2.
- For more information on default image log settings, see Image Log Settings.

Wiegand settings

In the **Wiegand** group, you can configure input and output details related to Wiegand devices.



- **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 on Wiegand format settings, see Set Wiegand Card Format.

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**.



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 is supported on the FaceStation F2, BioStation 3, BioEntry W3, and BioStation 3 Max models.
> - 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.

> **Info**
> For more information on the **Mask Check Mode** option, see Thermal and mask verification methods.

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

In the **Thermal & Mask Check Mode** or **Mask Check Mode** group, set the **Mask Detection** or **Thermal Camera Use** option to **Use** to configure the verification method based on the device's intended 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

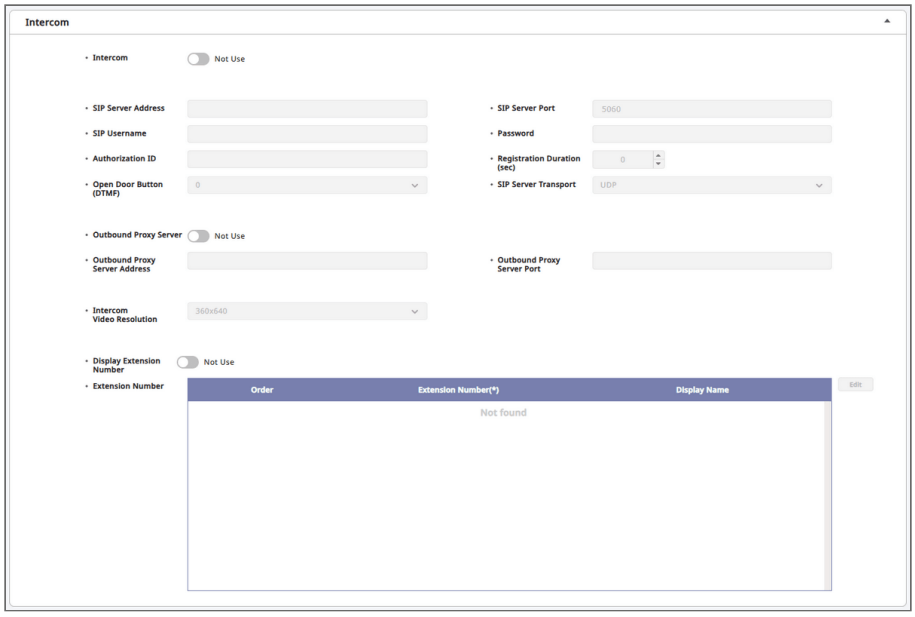
In the **Intercom** section, you can set detailed options for using the intercom.

Info

- This feature is supported on the BioStation 3 Max, BioStation 3, FaceStation 2, and BioStation A2 models.
- 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**: 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**.

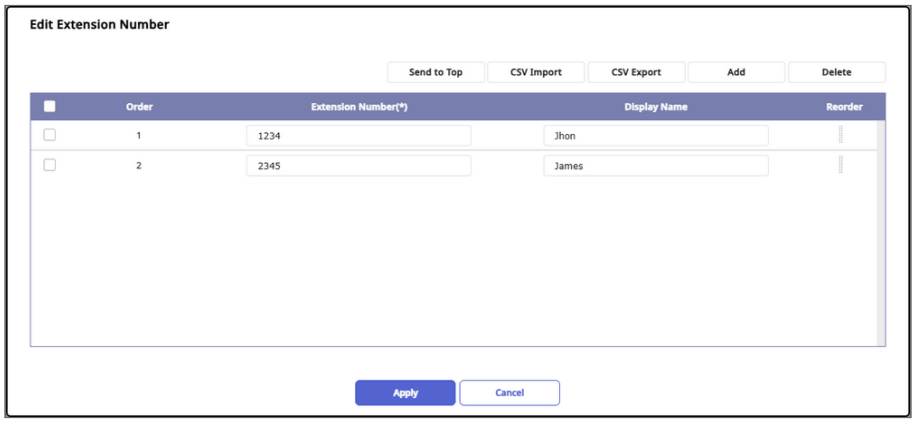
- **Display Extension Number**: Set to **Disable** to prevent the device from displaying the extension number. Without displaying the extension number, you cannot distinguish the recipient on the calling screen.
- **Extension Number**: You can register up to 128 extension numbers. To add or edit extension numbers, click the **Edit** button. For more information, see Edit extension numbers.

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.



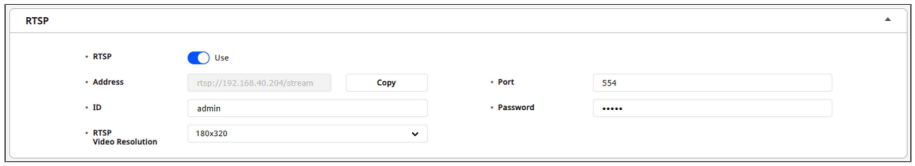
- **Send to Top**: Move the selected extension number to the top of the list.
- **CSV Import**: Import a CSV file that contains the extension numbers.
- **CSV Export**: Export the saved extension numbers to a CSV file.
- **Add**: Add an extension number.
- **Delete**: Delete an extension number.
- **Reorder**: 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.

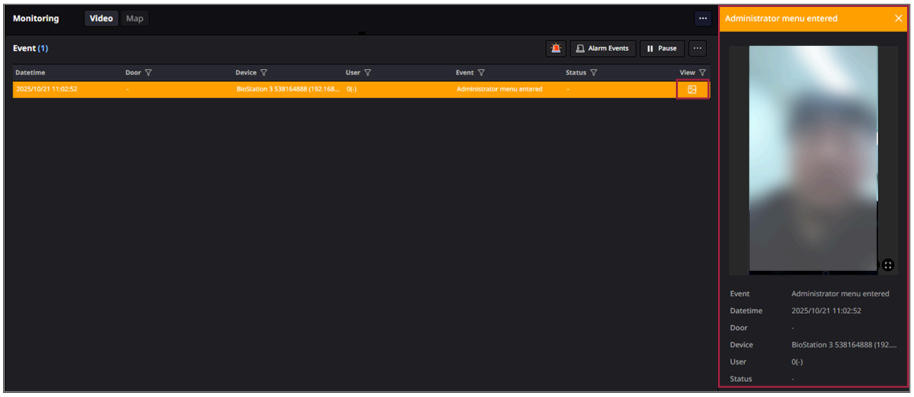


- **RTSP**: Enable RTSP streaming by setting **Enabled**.
- **Address**: The RTSP server address is fixed. Click the **Copy** button to copy the RTSP address.
- **Port**: Set the RTSP port.
- **ID**: Enter the RTSP server ID.
- **Password**: Enter the RTSP server password.
- **RTSP Video Resolution**: Select the resolution of the video output when using RTSP. The default is **180 x 320**.

> **Info**
>
> - This feature is supported on the BioStation 3 Max, BioStation 3, and BioEntry W3.
> - 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.



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 on BioStation 3 Max, BioStation 3, X-Station 2, FaceStation F2, FaceStation 2, and BioStation A2.
- For more information on viewing event logs on the **Monitoring** page, see Monitor Event.

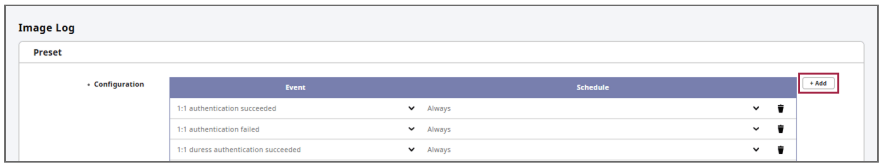
Caution

Settings in the **Settings** → **Device** → **Image Log** menu do not apply to the device. Enable the **Image Log** option on each device. For more information, refer to Advanced Settings.

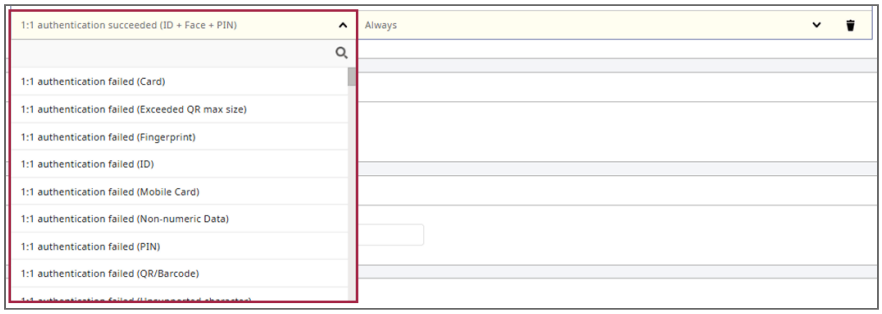
Add basic settings

Configure the basic settings that take effect when **Image Log** is enabled on a device. Configure events and schedules for image log creation. 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** on the left sidebar.
3. Click **+ Add** to the right of the **Preset** section.



4. When an event is added at the bottom of the list, click ⌄ for the desired event and select your options.



5. Click ⌄ 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.

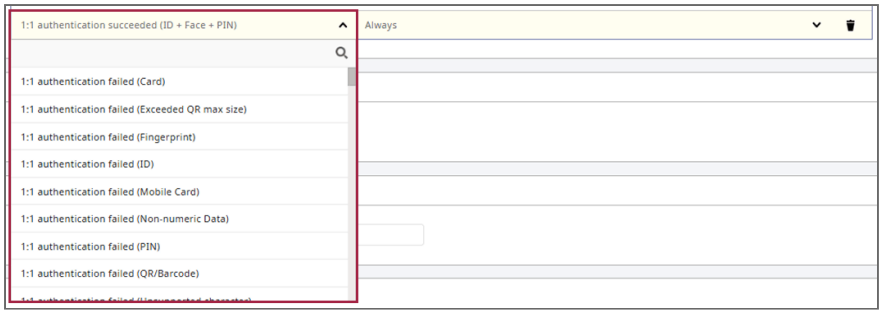
Info

If the desired schedule is not available, click **+ Add Schedule** to add one. For more information on schedule settings, see Schedule Settings.

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** on the left sidebar.
3. In the list of the **Preset** section, click ⌄ for the event you want to modify and select your options.



4. Click ⌄ in the schedule for the selected event and choose the preferred option.



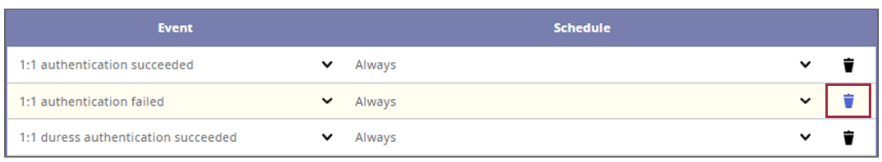
5. Click **Apply** at the bottom of the screen to save the settings.

> **Info**
>
> - If the desired schedule is not available, click **+ Add Schedule** to add one. For more information on schedule settings, see Schedule Settings.
> - The modified basic settings apply only to newly added devices. The changes do not apply to devices where **Image Log** is already enabled. Add the changes in each device's settings.

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** on the left sidebar.
3. In the list of the **Preset** section, click 🗑 for the event you want to delete.



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** on the left sidebar.
3. Set the conditions for deleting image logs in the **Delete Option** section.



   - **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** on 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.



4. Click **Apply** at the bottom of the screen to save the settings.

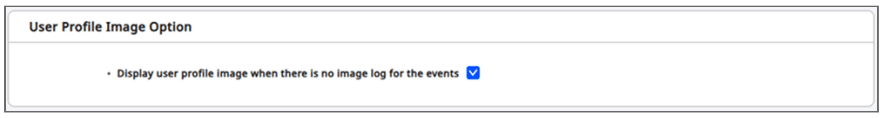
> **Info**
>
> - The storage path is not created automatically, so it must be created in advance for storing image logs.
> - For example, entering `.\imagelog\` will store image logs under the path where BioStar X is installed.
>
>   *C:\Program Files\BioStar X\imagelog*

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** on 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.



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 more information on viewing event logs on the **Monitoring** page, see Monitor Event.

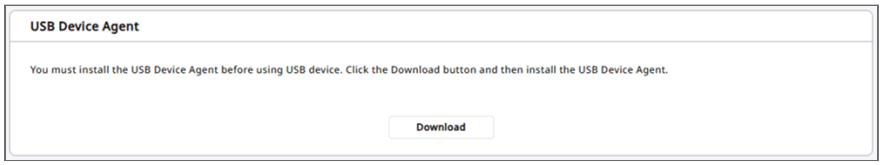
USB Agent Settings

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** on the left sidebar.
3. Click **Download** in the **USB Device Agent** section.



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 byte order for the USB card device

You can set the byte order for the USB card device.

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **USB Agent** on the left sidebar.

3. Setting the **Byte Order of USB Card Device** option in the **Byte Order** section.



   - **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).

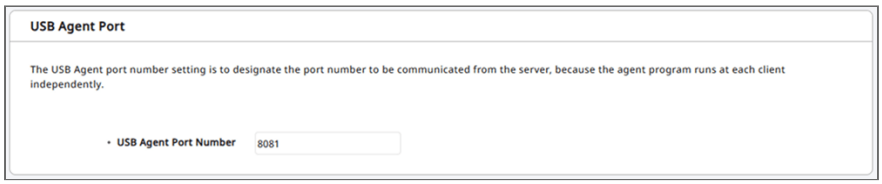
4. Once all configurations are complete, click **Apply** at the bottom of the screen.

> **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** on the left sidebar.
3. Enter the port number in the **USB Agent Port Number** input field in the **USB Agent Port** section.



4. Once all configurations are complete, click **Apply** 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 on the licensing policy, see License Policy.
- For more information on the Multi Communications Server specifications and installation, refer to the followings:
  - System Minimum Requirements
  - Install Multi Communications Server

Key features

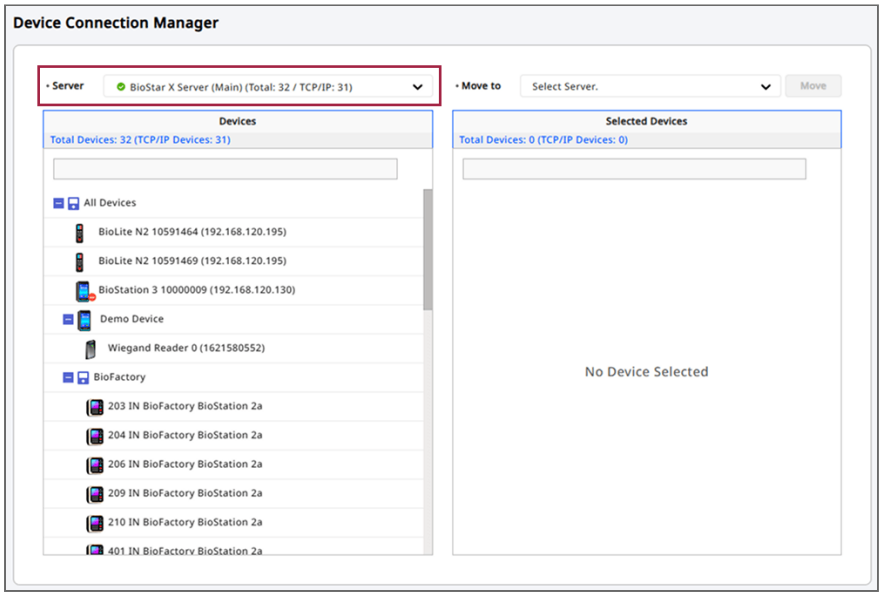
- **Server Expansion**: Install communication servers on additional computers besides the main computer to connect more devices.
- **Multiple Server Operation**: Use up to three servers together to support a total of 3,000 devices.
- **Convenient Device Management**: When adding new devices, choose which 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 Multi Communications Server is a dedicated service that separates the device connection feature from the BioStar X integrated server. It focuses solely on reliable communication with devices, enhancing the performance of the overall system.

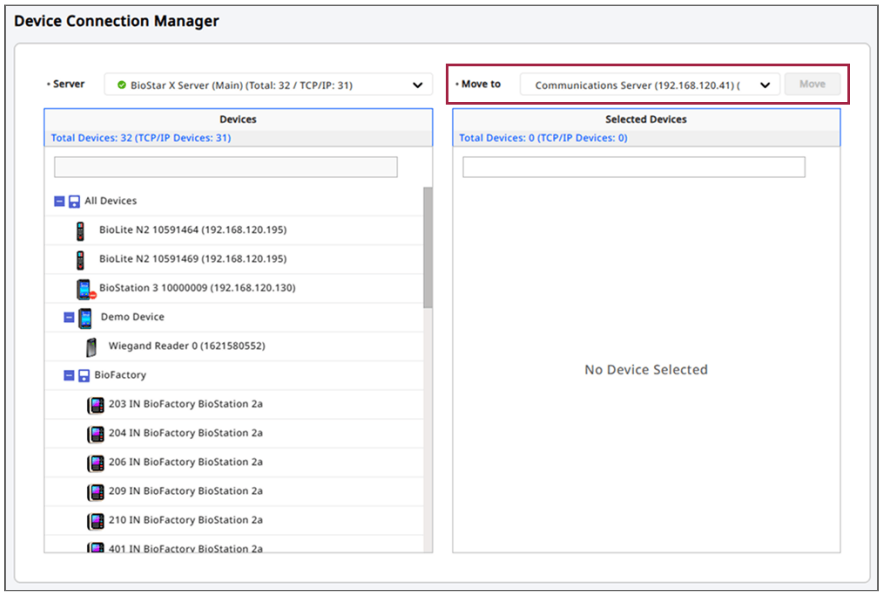
Move devices to another server

This feature lets you move devices from the main server or another Multi Communications Server to another Multi Communications Server. This feature helps maintain the connection status of the devices while moving them between servers.

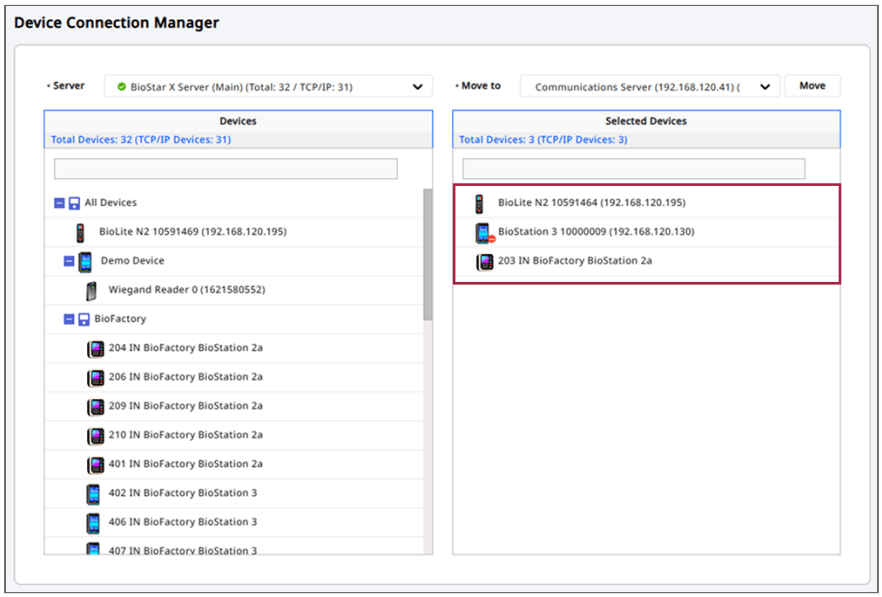
1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Device Connection Manager** on the left sidebar.
3. From the **Server** section on the left, select the server where the device you want to move is registered.



4. In the **Move to** section on the right, select the target server to which you want to move the devices.

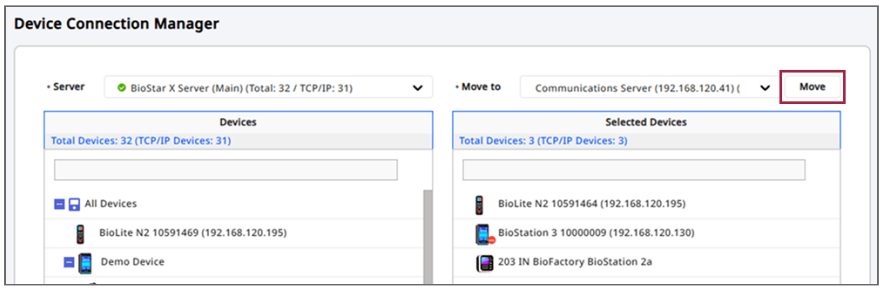


5. Select the device(s) you want to move from the device list. You can select multiple devices.



> 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.



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.

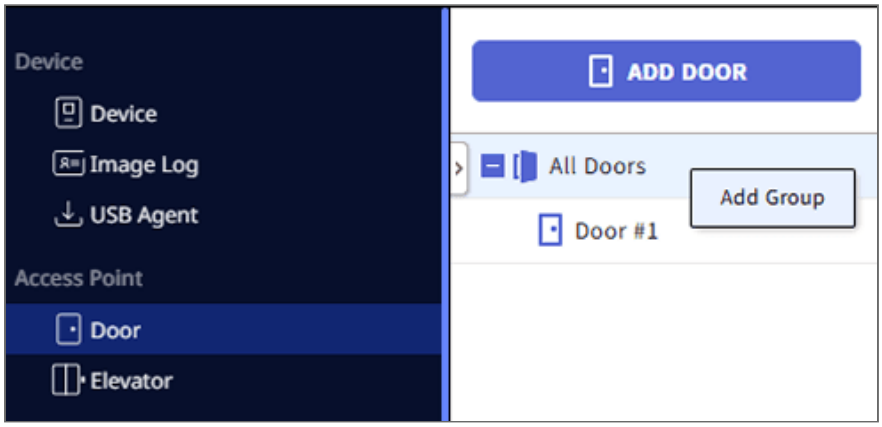
Manage Door Group

This guide describes how to set up groups to easily manage multiple doors. A door group is a feature that allows you to manage several doors as one group. If you set up a group, you can configure multiple doors at once.

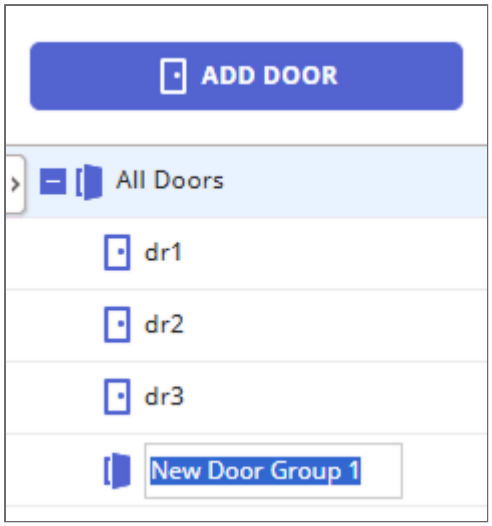
> **Tip**
> Register group names using door locations or office names for easier management.

Add door group

1. Click **Settings** on the **Launcher** page.
2. Click **Access Point** → **Door** on the left sidebar.
3. Right-click on **All Doors** from the door list.



4. Click **Add Group** in the popup menu.



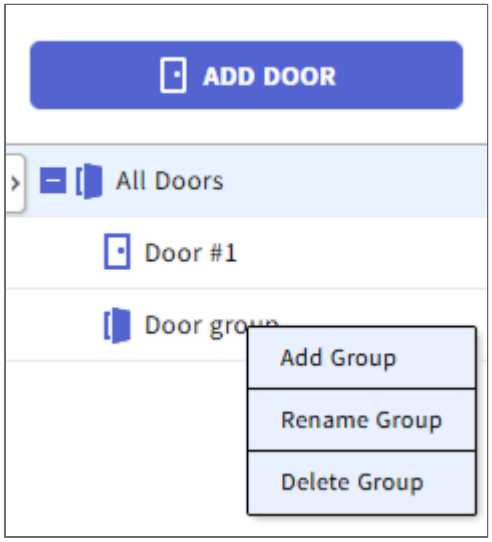
5. Enter your desired group name.

> **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 **Access Point** → **Door** on the left sidebar.
3. Right-click on the group you want to rename from the door list.

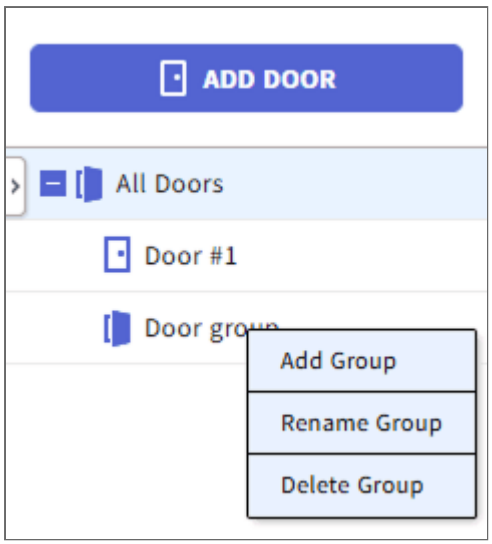


4. Click **Rename Group** in the popup menu.
5. Enter the new group name.

> **Info**
> The door group name can be up to 48 characters long.

Delete door group

1. Click **Settings** on the **Launcher** page.
2. Click **Access Point** → **Door** on the left sidebar.
3. Right-click on the group you want to delete from the door list.



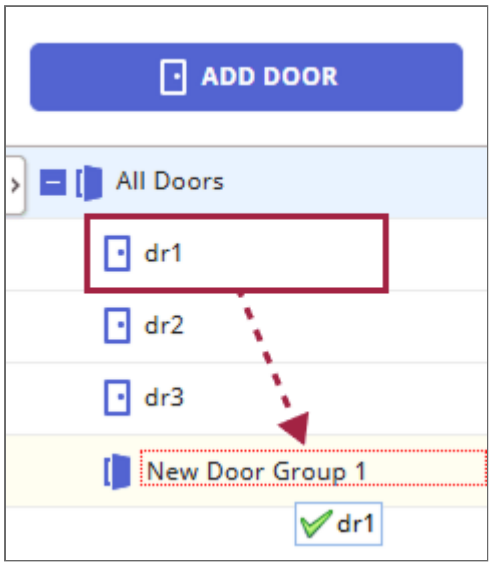
4. Click **Delete Group** in the popup menu.

> **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.

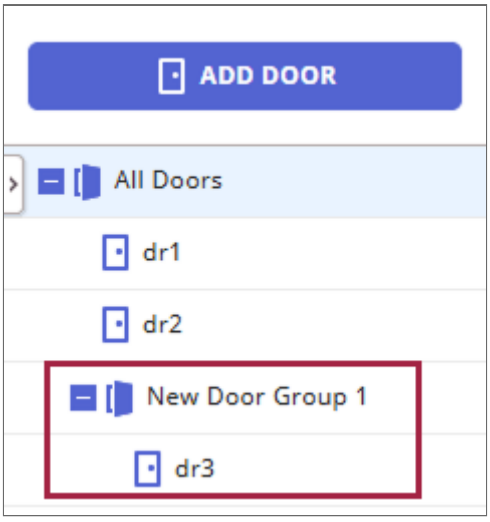
Add door to group

Add from door list

1. Click **Settings** on the **Launcher** page.
2. Click **Access Point** → **Door** on 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.



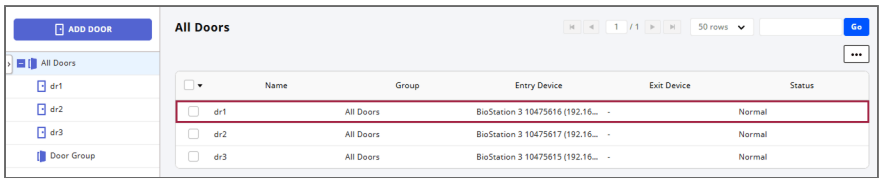
The selected door moves to the group.



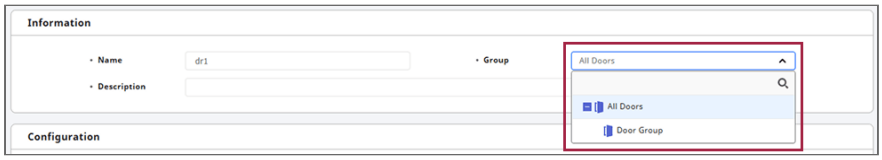
Add from door information

1. Click **Settings** on the **Launcher** page.
2. Click **Access Point** → **Door** on the left sidebar.

3. Click the door you want to add to a group from the list on the right side of the screen.



4. When the door information edit 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 Door

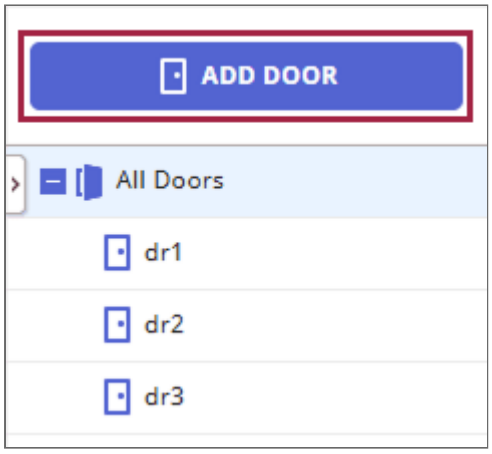
This guide describes how to register and set up doors. Connect entry and exit devices for each door, and configure security features such as anti-passback and dual authentication to establish a systematic access management environment. Additionally, configure alarms based on the door status to prevent security incidents in advance.

Before you start

- Set access levels, access groups, and floor levels for access control before registering doors. For more information, see Access Control Settings.
- 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 **Access Point** → **Door** on 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, see Set basic information.
   - **Configuration**: Set devices connected to the door, and entry and exit buttons along with door sensors. For more information, see Set door settings.
   - **Option**: Set additional options. For more information, see Set additional options.
   - **Anti PassBack**: Set the anti-passback feature to manage access history and enhance security. For more information, see Set anti-passback.
   - **Timed Anti PassBack**: Set the initialization time for the anti-passback feature. For more information, see Set timed anti-passback.
   - **Alarm**: You can set the alarm to trigger or block device usage when an anti-passback violation occurs. For more information, see Set alarms.
5. Once all configurations are complete, click **Apply** 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.

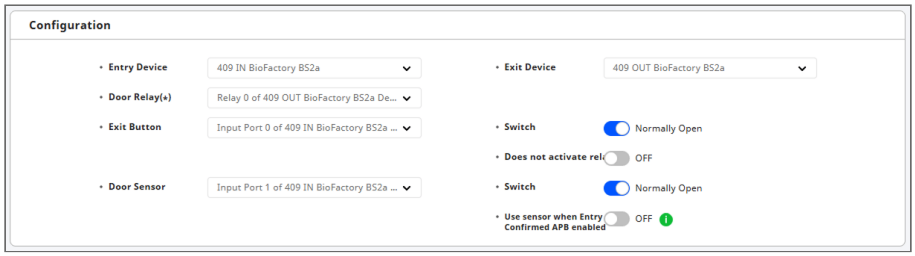


- **Name**: Enter the door name. Enter a name that can be specified for convenient management.
- **Group**: Select the door group.
- **Description**: Enter a brief description of the door.

> **Info**
>
> - The door name can be up to 48 characters long.
> - For more information on registering door groups, see Manage Door Group.

Set door settings

In the **Configuration** section, you can set the devices connected to the door, exit buttons, and door sensors.



- **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.

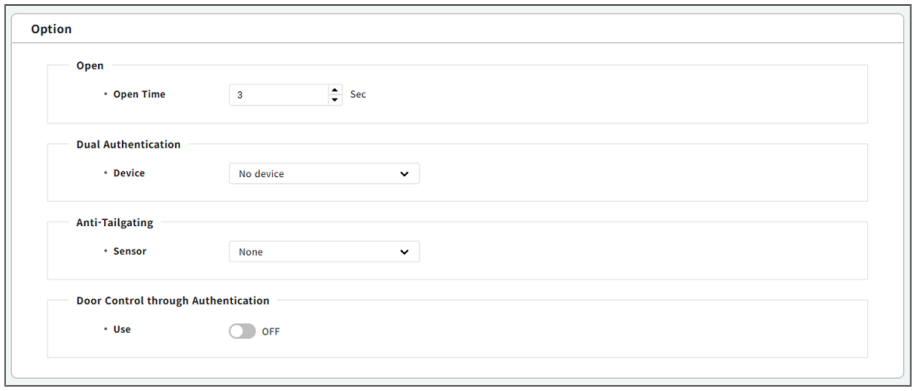
> If **Timed Anti PassBack** is enabled, the **Use sensor when Entry Confirmed APB enabled** option cannot be used.

- **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.



- **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 **On**, the **Lock when door is closed** option cannot be used.

> 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. To disable 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 door will not open.

> - Modify settings in the following menu to change the dual authentication of the device configured for occupancy limit settings. **Settings** → **Access Management** → **Advanced AC** → **Occupancy Limit**
>
> For more information on the **Occupancy Limit** settings, see Advanced Access Control Settings.
> - For more information on schedule settings, see Schedule Settings.

- **Anti-Tailgating**: Set to detect tailgating where an unauthorized person follows an authorized person to enter.
  - **Sensor**: Select a sensor to detect tailgating.
- **Door Control through Authentication**: Enable the door to remain unlocked when an authorized user performs a Double Badge (Double Badge). For more information, refer to Configure Door Control through Authentication.

> This setting is unavailable on the Add Door screen because the door is not in an access group. Save the door, add it to an access group, then set this on the Edit Door Information screen.

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 more information on setting up the exit device, see Set door settings.
> - 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

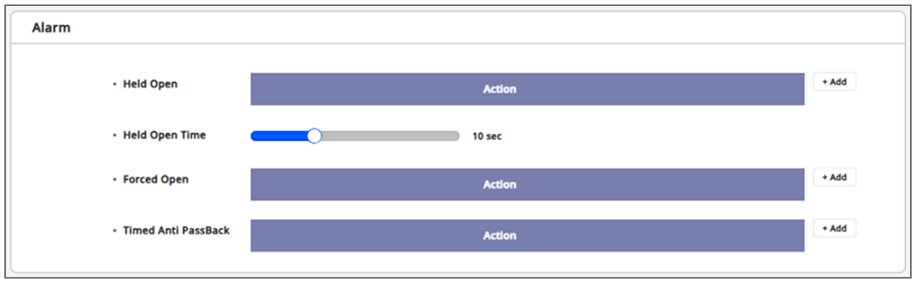
When a user attempts to re-authenticate on the same device after entry authentication, the anti-passback feature will prevent immediate re-authentication. The **Timed Anti PassBack** section sets the initialization time for the anti-passback feature to effectively limit frequent entries by users.



- **Timed 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 **+ Add** for the item to add an alarm.



- **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 **Access Point** → **Door** on 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 **Apply** at the bottom of the screen.

> **Info**
> - For more information on each section of the edit door information screen, see Register Door.
> - After adding a door to an access group, configure the **Door Control through Authentication** feature. For more information, refer to Configure Door Control through Authentication.

Batch edit multiple doors

1. Click **Settings** on the **Launcher** page.
2. Click **Access Point** → **Door** on 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.



   - **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.

Configure Door Control through Authentication

Door control through authentication switches a door to always open when a designated user authenticates twice in a row (Double Badge) with the same card on a supported device. In Always Open mode, double-badge again. The door returns to its original mode when the allowed schedule ends.

Before you start

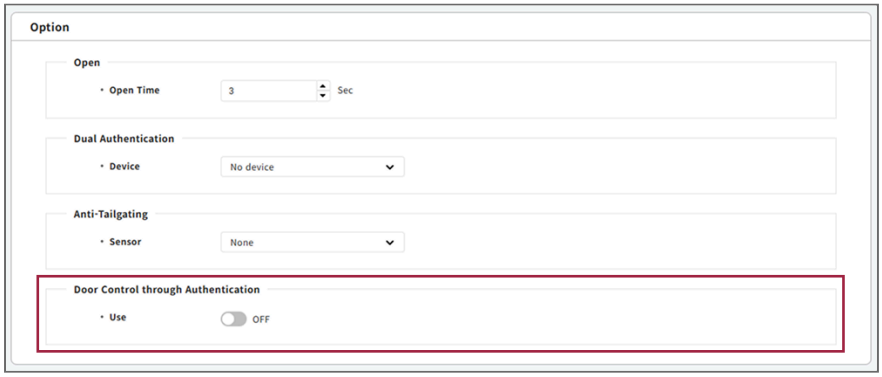
- The door must belong to an access group. On the Add Door screen, this feature is unavailable because the door is not in an access group yet. Save the door, add it to an access group, and set this feature on the Edit Door Info screen. For more information on access group settings, see Access Control Settings.
- For more information about adding doors and editing door information, see the following documents.
  - Register Door
  - Modify Door Information

Info

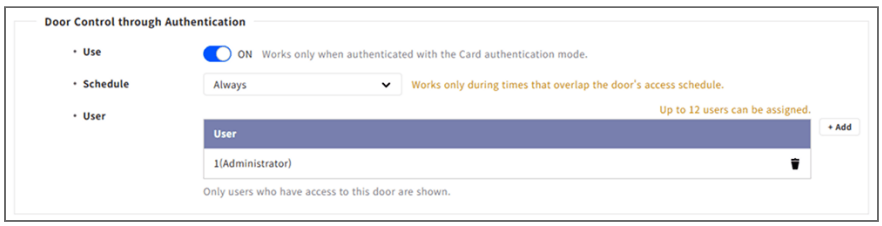
- Support for door control through authentication starts with the following devices and firmware versions. Use this feature only on doors that use supported devices.
  - XPass 2 firmware version 1.5.3 or higher
  - FaceStation F2 firmware 2.3.0 or higher
- This feature works only with card-type credentials (CSN, Wiegand, smart cards, and mobile card CSN/ToM). This feature does not apply to template credentials or biometric authentication such as fingerprint and Facial Authentication. The system processes them as standard access authentication.
- Door control through authentication works only when the device authentication mode is set to Card. **BioStar X** does not check the device authentication mode. Verify the device authentication mode before using this feature.
- The device recognizes a double badge only when the two authentications occur within 3 seconds. If the interval exceeds 3 seconds, the device treats each authentication as a separate access authentication.

Set door control through authentication

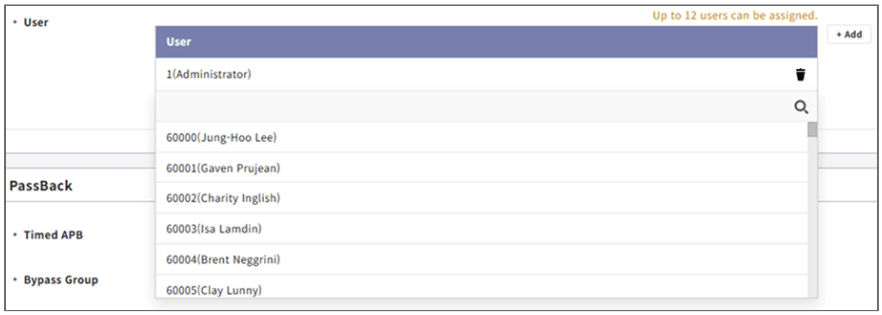
1. Click **Settings** on the **Launcher** page.
2. Click **Access Point** → **Door** on the left sidebar.
3. In the door list, click the door to configure.
4. In the **Option** section, go to **Door Control through Authentication**.



5. Set the **Use** option to **ON**.



6. In **Schedule**, select the schedule for using this feature. The default is **Always**. If the schedule is not available, add a schedule first.
7. To add users who can control the door with Double Badge, click **+ Add** and select from the **User** list.



- **User** list shows only users with door access. Check access groups and access levels in **Settings** → **Access Management** → **Access Control**.
- Specify up to 12 users.
- Click 🔍 to search for a specific user.
- Select individual users only. User group selection is unavailable.

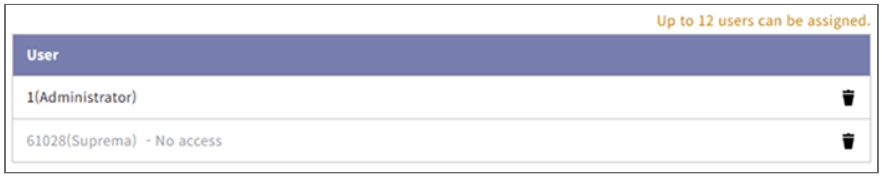
8. Once all configurations are complete, click **Apply** at the bottom of the screen.

Info

- For more information on adding schedules, see Schedule Settings.
- For more information on setting access groups and access levels, see Access Control Settings.

Notes

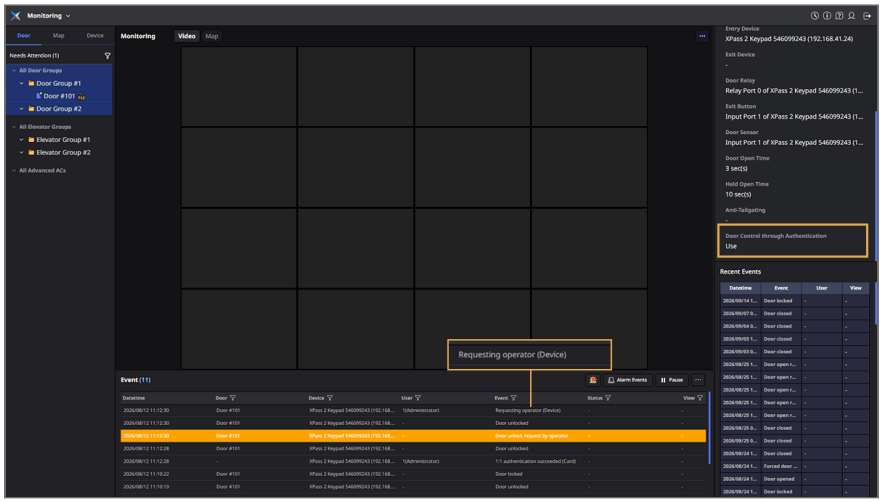
- Doors that use door control through authentication cannot change the entry or exit device to an unsupported model. Before changing the device, set **Door Control through Authentication** to **OFF**.
- If a control user loses door access, the list marks the user as **No access**. This status prevents saving. Grant access again or remove the user from the list.



- Saving requires at least one control user.
- If the selected schedule is deleted, the **Schedule** field shows **Deleted Schedule**. This status prevents saving. Select another schedule.
- In Hard mode, access is denied when an anti-passback violation occurs, so door control through authentication does not work. In Soft mode, access is allowed, so it does work.
- When other advanced access control features apply, they take priority.

Related information

- Check door control through authentication in the door preview panel on **Monitoring**. Related events appear as **Requesting operator** in **Event**. For more information on door monitoring, see Monitor Doors.

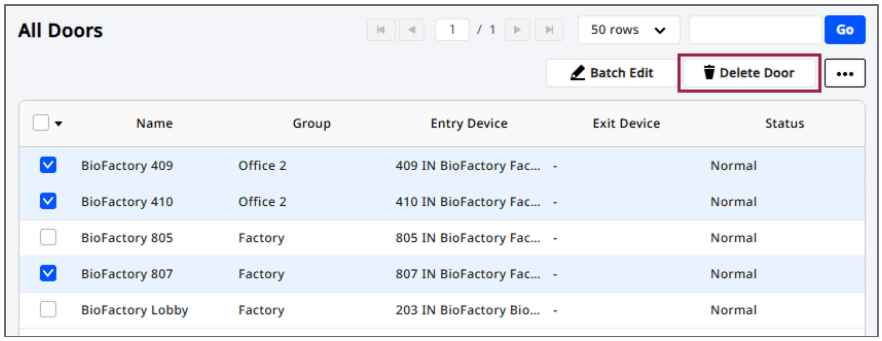


- The audit trail records setting changes. For more information, refer to View Access Control Audit Logs.

Delete Door

This guide describes how to delete registered doors.

1. Click **Settings** on the **Launcher** page.
2. Click **Access Point** → **Door** on the left sidebar.
3. Click the checkbox of the door you want to delete from the list.
4. Click **Delete Door** at the top right of the screen.



5. Click **Yes** when the confirmation message window appears.

The selected door will be deleted. Deleted doors cannot be recovered.

> **Info**
> **Delete Door** 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** → **Account** on the left sidebar. Refer to the provided accounts based on permission levels.

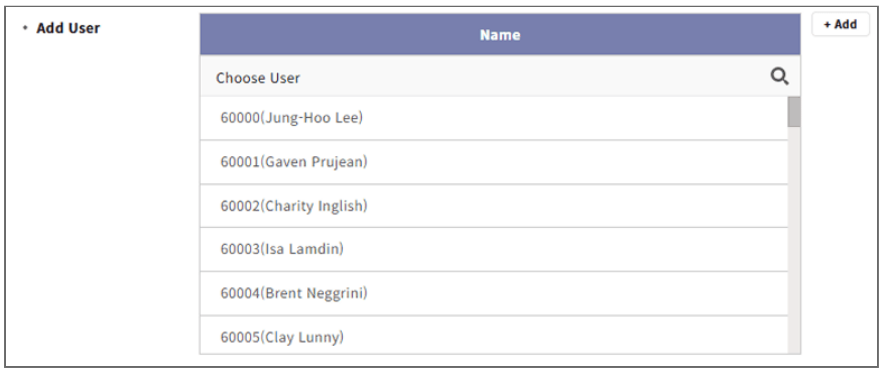
- **Administrator**: This is an administrator level that can use all menus.
- **User Operator**: The **User** menu has **read** and **edit** permissions. No permissions exist for other setting groups besides the **User** menu.
- **Monitoring Operator**: The **Monitoring** and **Data** menus have **read** and **edit** permissions, and the **Dashboard** menu has **read** permission.
- **T&A Operator**: The **TIME ATTENDANCE** menu has **read** and **edit** permissions, and the **User** menu has **read** permission.
- **Visitor Operator**: The **VISITOR** menu has **read** and **edit** permissions.

> **Info**
>
> - **Edit** permission for the **Monitoring** menu allows adding tabs or controlling status tree entries.
> - **Edit** permission for the **Data** menu allows saving reports, adding automated report schedules, and accessing settings.
> - For information on adding custom user permissions, see Add Custom Permissions.
> - 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 policies, see License Policy.

Granting operator permissions to users

Guide on granting operator permissions to general users.

1. Click **Settings** on the **Launcher** page.
2. Click **Account** → **Account** on the left sidebar.
3. Click the desired item from the account list.
4. Click **+ Add** in the **Add User** option.



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.

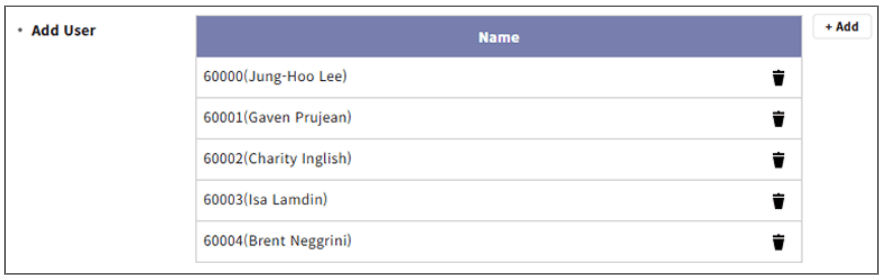
Info

- 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. For more information, see Setting User Permissions.
- 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** → **Account** on the left sidebar.
3. Click the desired account type from the account list.
4. Click 🗑 for the user to exclude from operation in the **Add User** option.

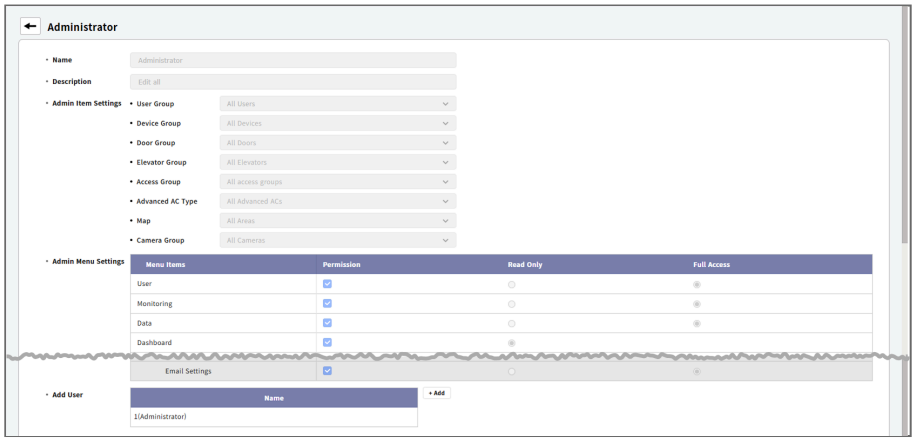


The image above is an example screen and may differ from the actual screen.

5. Click **Apply** at the bottom of the screen to save the settings.

Checking operator permission details

Click an account in the account list in the **Account** menu to view its operator permission details.



- **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.
  - **Read Only**: Grants permission to add, edit, or delete items in the menu.
  - **Full Access**: Grants permission to enter the menu and only view the settings.
- **Add User**: Can view users granted permissions.

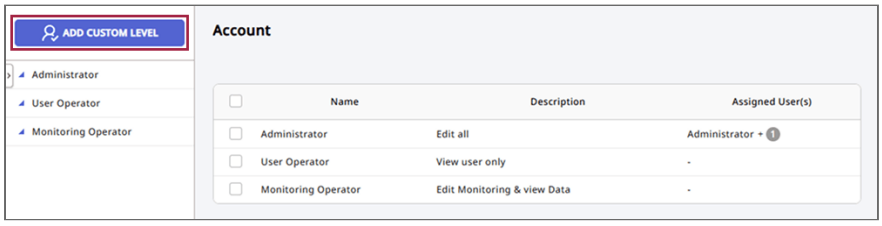
> **Info**
> For more information on how to grant permissions to a specific user, see Granting operator permissions to users.

Add Custom Permissions

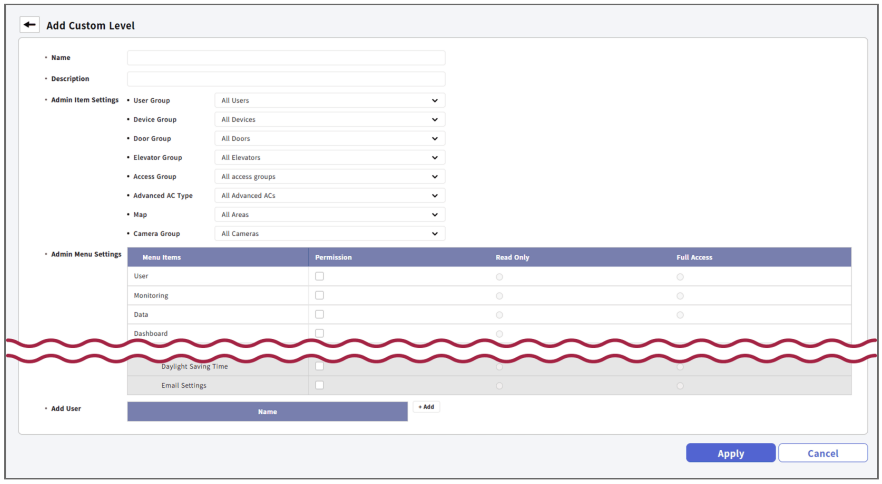
This guide describes how to add the desired permission level. Custom permissions are user-customizable features that allow for additional permissions beyond the default operational permissions.

Add custom permissions

1. Click **Settings** on the **Launcher** page.
2. Click **Account** → **Account** on the left sidebar.
3. Click **Add Custom Level**.



4. Enter a name and description for the newly created permission.



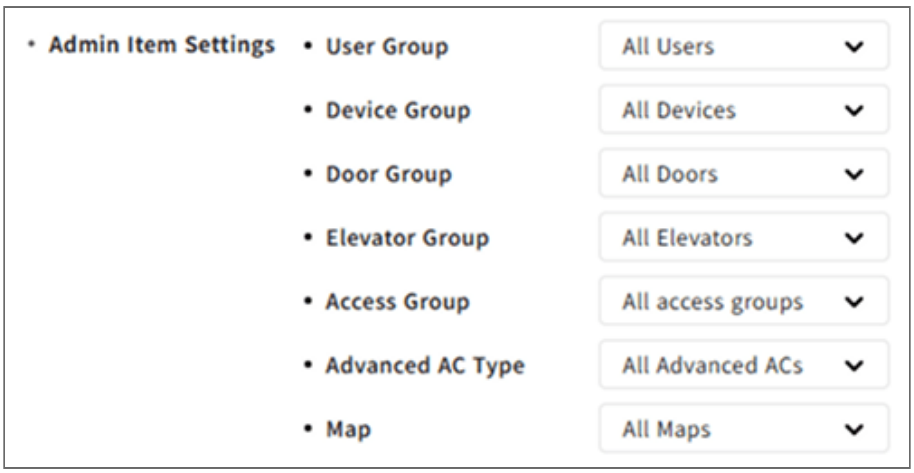
5. Fill in or select each of the remaining items.
6. Click **Apply** at the bottom of the screen to save the settings.

Info

- The types of **Admin Menu Settings** settings you can configure may vary depending on the activated license type.
- For more information on **Admin Item Settings**, see detailSetting.
- For more information on **Admin Menu Settings**, see menuSetting.
- For more information on **Add User**, see addUser.

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.

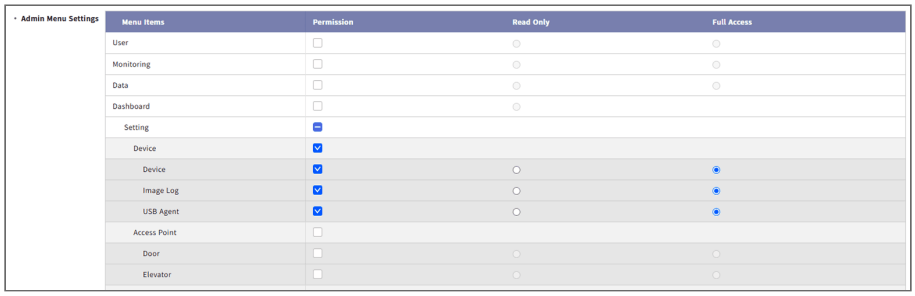


Info

- 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:
  - Manage User Groups
  - Manage Device Groups
  - Manage Door Group
  - Manage Elevator Group
  - Manage Access Groups
- The **Map** permission is available with an **Essential** license or higher. For more information on the licensing policy, see License Policy.
- The **Elevator Group**, **Advanced AC Type**, **Camera Group** permissions are available as an add-on option with an **Essential** license or higher. For more information on licensing policies, see License Policy.

Admin Menu Settings

Select **Read Only** or **Full Access** for each menu. Assign different permissions to each menu. Click the **Permission** checkbox, then select **Read Only** or **Full Access**.



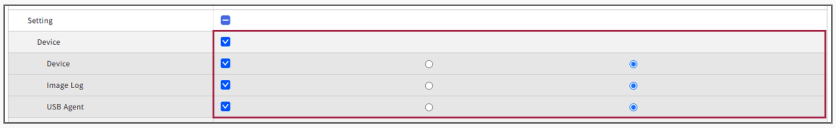
- **Read Only**: Grants permission to enter the menu and only view the settings.
- **Full Access**: Grants permission to add, edit, or delete entries in the menu.

Info

- In the **Monitoring** menu, **Full Access** allows adding tabs or controlling state tree entries.
- In the **Data** menu, **Full Access** allows saving reports, adding automatic report schedules, and accessing settings.
- In the **Dashboard** menu, **Read Only** permission allows creating new dashboards and widgets.
- Menus not listed in **Menu Items** are accessible regardless of permissions.

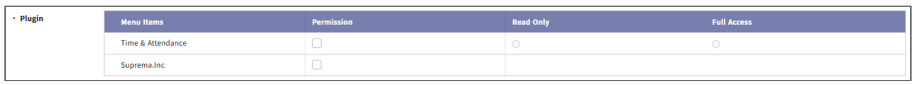
Tip

Click a parent menu permission to enable permissions for all submenus.



Plugin

After adding a plugin, configure plugin permissions. Users without plugin permissions cannot access the plugin, and the plugin does not appear on the home screen or launcher.

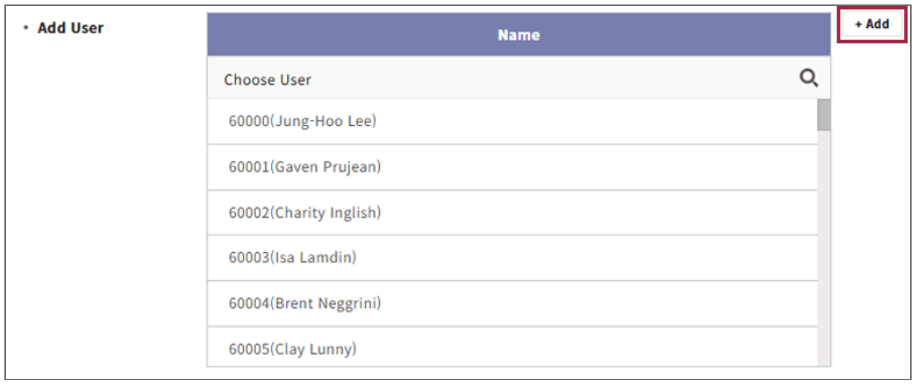


Info

- A plugin license is required to use plugin features. For more information on licensing policies, see License Policy.
- Apply **Read Only** or **Full Access** only to the **Time & Attendance** plugin.

Add User

You can add or verify user information for granting permissions. Click **+ Add** to add a user. Select the user to grant permissions from the user list.



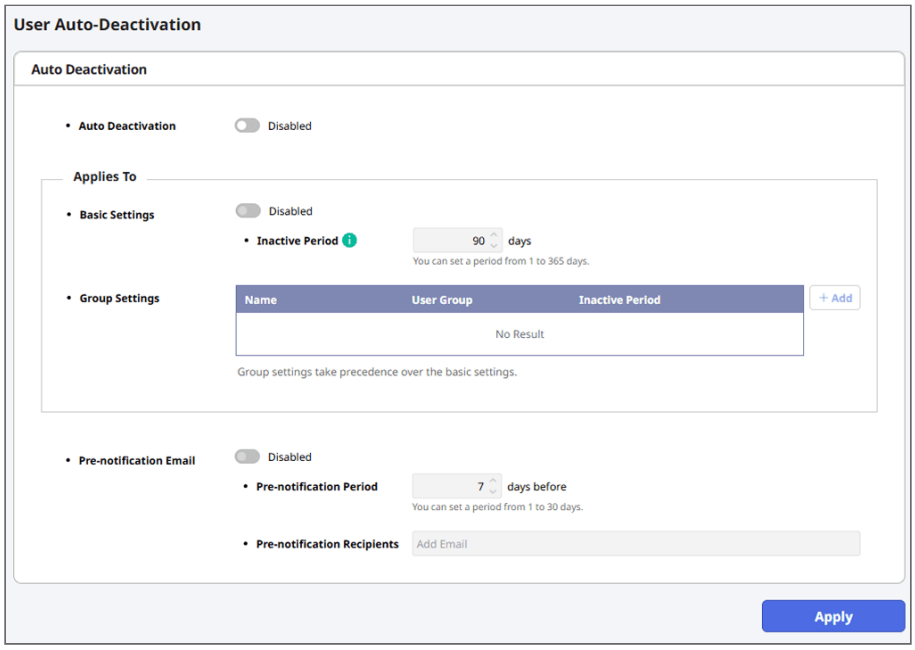
Info

Clicking 🗑 next to a user in the user list will exclude that user from permissions.

Manage Long-Term Inactive Users

Leaving credentials active for users who have not accessed for a long time, such as after resignation or leave, can lead to security threats, including credential theft and unauthorized access. The auto deactivation feature automatically deactivates users after a set period since their last access, so administrators can manage accounts securely without manual cleanup each time. Before auto deactivation, the system sends a pre-notification email to the specified recipients, giving time to review or make exceptions.

Click **Settings** on the **Launcher** page. Click **Account** → **User Auto-Deactivation** on the left sidebar.

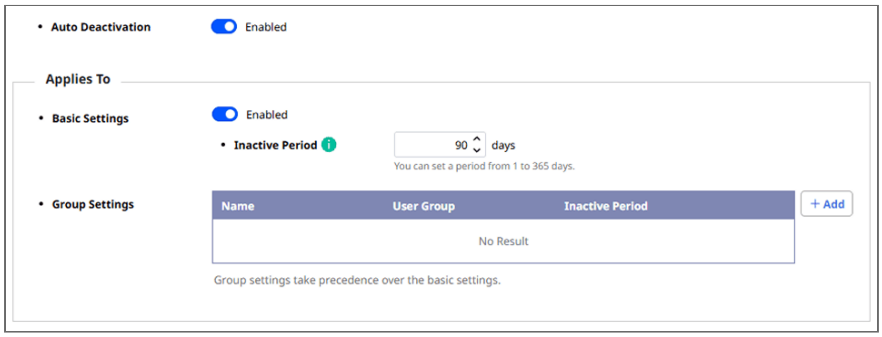


Info

Only administrators with permission for this menu can access **Account** → **User Auto-Deactivation**. To grant an administrator permission for a specific menu, see Manage Operation Permissions.

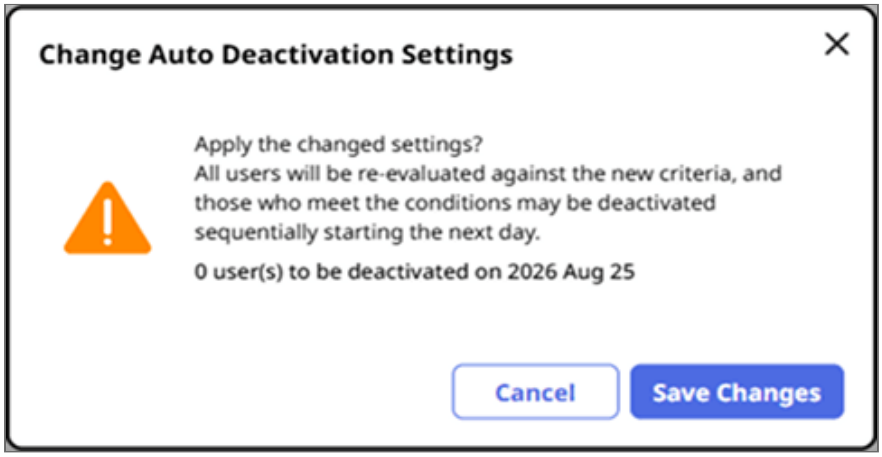
Configure auto deactivation

1. In **Auto Deactivation**, click the toggle button to enable it.
2. In the **Applies To** section, set the targets for auto deactivation.



   - To apply the same criteria to all users, enable **Basic Settings** and enter **Inactive Period**. Set a value from 1 to 365 days.
   - To apply different criteria to certain user groups, add **Group Settings**. For more information, see Apply different criteria by group.

3. Once you complete the settings, click **Apply** at the very bottom of the screen.
4. When the confirmation window appears, check the next scheduled date for automatic processing and the number of users scheduled for deactivation, then click **Save Changes**.



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

Info

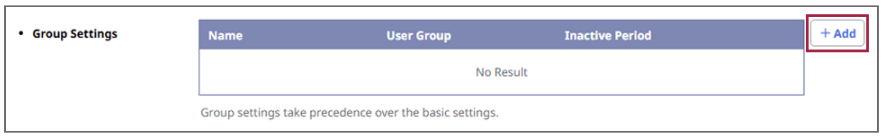
- To email the specified recipients before a user is automatically deactivated, configure **Pre-notification Email**. See Pre-notification email settings for details.
- Enabling the **Auto Deactivation** option does not automatically enable **Basic Settings**. To build the policy using only **Group Settings**, leave **Basic Settings** disabled.
- Auto deactivation uses the last access authentication time. The system excludes users with no access history or only pre-registration access history.
- If a user meets both **Basic Settings** and **Group Settings**, **Inactive Period** in **Group Settings** takes precedence. If the user belongs to 2 or more **Group Settings**, the shortest **Inactive Period** applies.
- Automatic deactivation runs 1 time a day (midnight). Setting changes apply at the next processing time and do not affect advance notice schedules already sent.
- When you set the **Auto Deactivation** option to inactive, the system saves it immediately without a confirmation dialog.

Apply different criteria by group

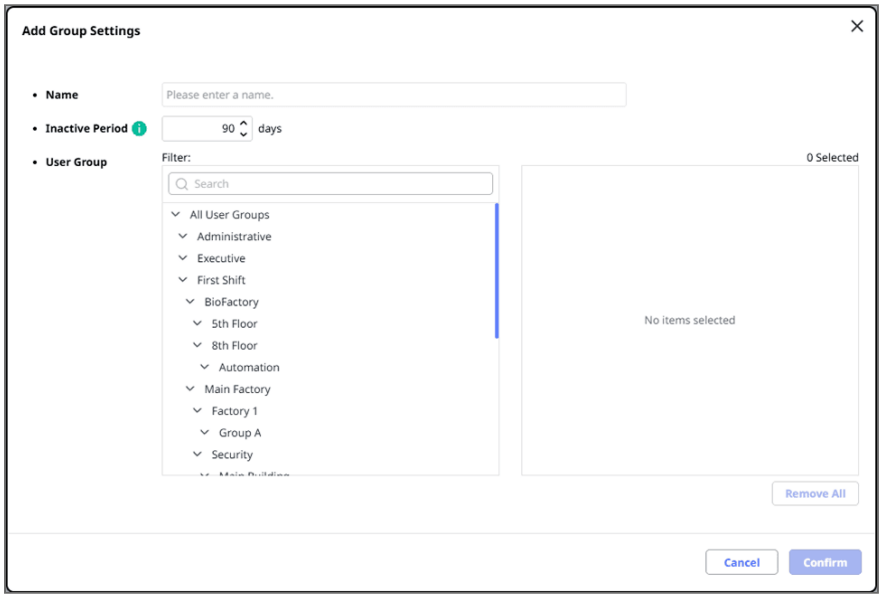
Apply a different **Inactive Period** to certain user groups than **Basic Settings**.

Add group settings

1. Click **+ Add** to the right of the **Group Settings** list.



2. When the **Add Group Settings** window appears, set each field.



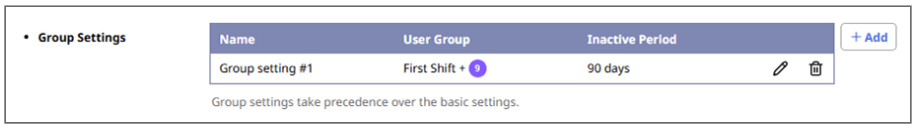
- **Name**: Enter a name that does not duplicate other group settings. Case and leading or trailing spaces do not matter.
- **Inactive Period**: Set from 1 to 365 days.

- **User Group**: Select the user groups to apply this setting to. Selecting a group also selects its subgroups.

3. After selecting user groups, click **Confirm**.
4. Click **Apply** at the bottom of the screen to save changes.
5. When the confirmation window appears, check the next scheduled date for automatic processing and the number of users scheduled for deactivation, then click **Save Changes**.

> **Info**
>
> - In **User Group**, user groups outside the administrator's permission scope appear disabled, but remain visible in the list. Expand this group. Select subgroups within the permission scope.
> - Administrators with administrator privileges set to **All users**, or full administrators, have no limits on user group selection. For more information on administrator roles, see Manage Operation Permissions.

Edit and delete group settings



- To edit, in the **Group Settings** list, click for the desired row, change the value, and then click **Confirm**.
- Click for the row to delete. When the confirmation message appears, click **Delete**.

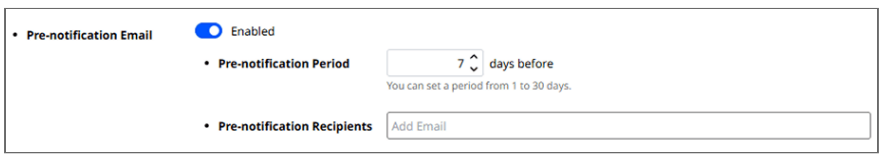
To save your edits or deletions, click **Apply** at the bottom of the screen. When the confirmation window appears, check the next scheduled date for automatic processing and the number of users scheduled for deactivation, then click **Save Changes**.

> **Info**
>
> - If **Group Settings** includes user groups outside the administrator's permission scope, the list still shows them. The system disables editing and deletion.
> - **Group Settings** takes precedence over **Basic Settings**.
> - Deleting **Group Settings** does not restore users already deactivated. After deletion, the system switches to another applicable setting (such as **Basic Settings**).

Pre-notification email settings

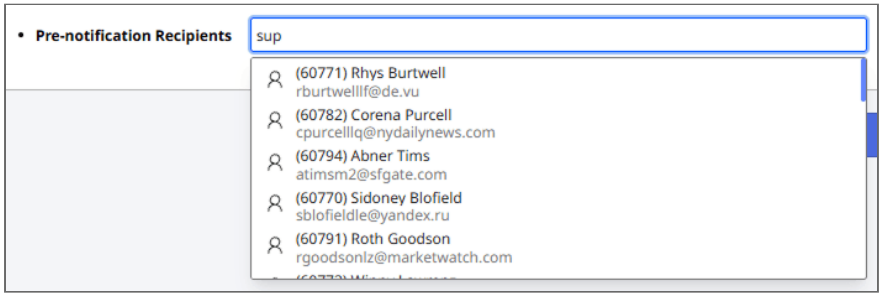
This feature sends an email notice to specified recipients before users are automatically deactivated.

1. Click the toggle in the **Pre-notification Email** option to enable it.



2. Enter a value for **Pre-notification Period**. The system sends auto-deactivation notice emails for the entered period. Set the period from 1 to 30 days.

3. In the **Pre-notification Recipients** field, search and select a user by name, ID, or email, or enter an email address, then press `Enter`.



4. Once you complete the settings, click **Apply** at the very bottom of the screen.

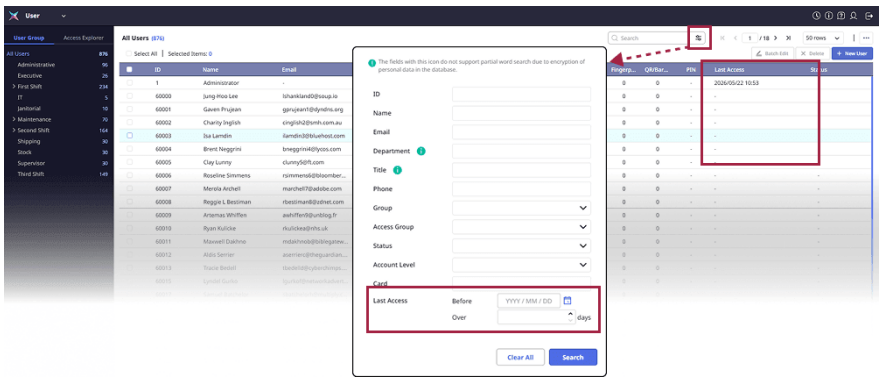
5. When the confirmation window appears, check the next scheduled date for automatic processing and the number of users scheduled for deactivation, then click **Save Changes**.

Info

- Set up SMTP settings to use pre-notification emails. For more information, see Email Setting.
- Set **Pre-notification Period** shorter than the inactive period in **Basic Settings** and every **Group Settings**.
- Add email addresses not in **BioStar X** as recipients.
- The system sends a consolidated email 1 time per day, not separate emails for each user.
- If **Basic Settings** is disabled and no **Group Settings** exists, enabling only **Pre-notification Email** leaves no targets, so the system sends no emails.

Related information

- View long-term inactive users in the **Last Access** column of the user list or use Advanced Search. For more information on selecting view options, refer to Explore Users.

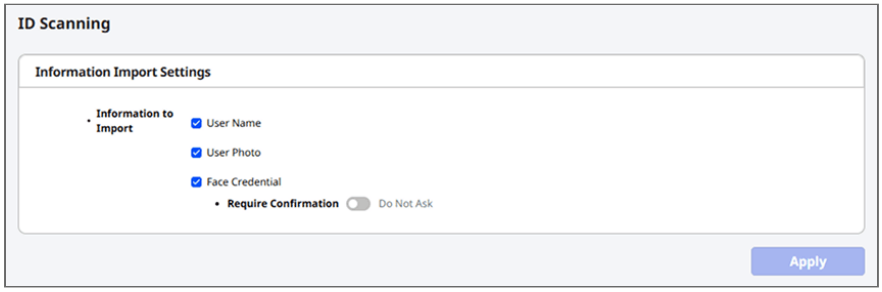


- Check the history of users deactivated automatically or manually in the **Inactive Users** report. For more information on selecting view options, refer to Generate Report.

Set Up ID Scan

Before registering users by scanning ID, choose the user name and profile image to import. Then choose the face credential enrollment method. This article explains setting up ID scanning.

1. Click **Settings** on the **Launcher** page.
2. Click **Account** → **ID Scanning** on the left sidebar.



3. Select the data to import when scanning a ID.
   - **User Name**: Imports the name printed on the ID.
   - **User Photo**: Imports the profile image printed on the ID.
   - **Face Credential**: Enrolls the face image printed on the ID as a face credential.
     - **Require Confirmation**: Always asks for confirmation when enrolling the face image printed on the ID as a face credential.
     - **Do Not Ask**: Enrolls the face image printed on the ID as a face credential without asking for confirmation.
4. Click **Apply** to save the settings.

> **Info**
>
> - Select **User Photo** to enable **Face Credential**.
> - For more information on registering or updating users by scanning ID, see Register and Edit Users by Scanning an ID.

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

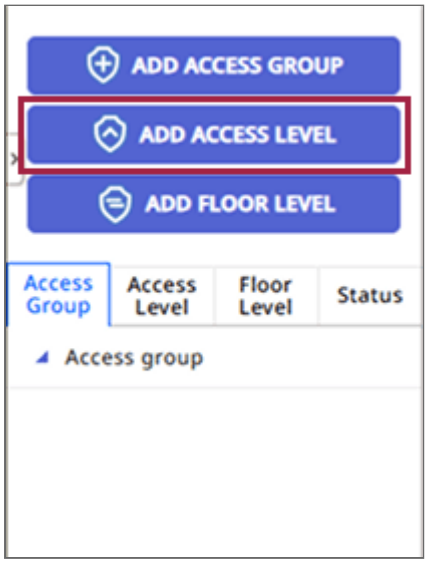
Access levels enable users to set times for entry and grant permission to access doors during those times. Access levels are a key element for configuring access groups.

Before you start

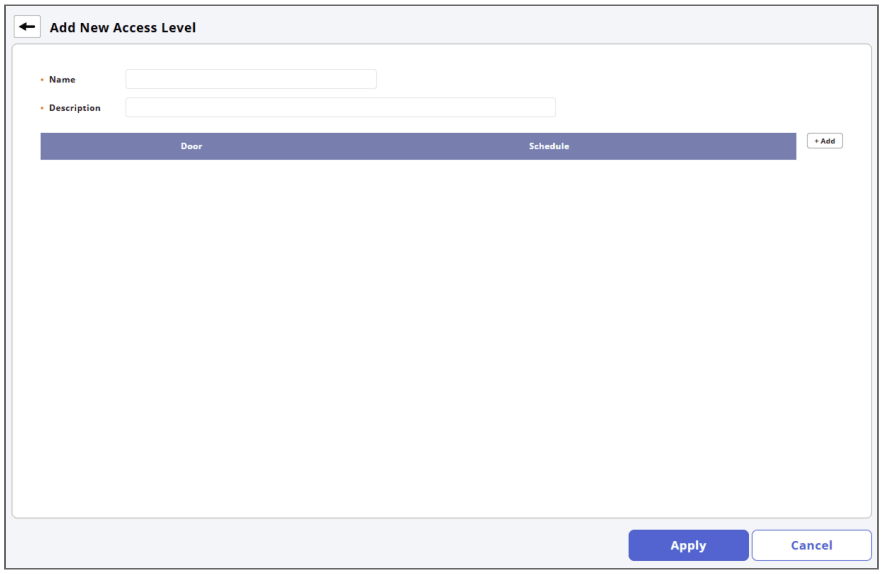
- Initialize doors before enrolling access levels. For more information on registering doors, see Register Door.
- You can predefine time to apply to access levels through schedule settings. For more information on schedule settings, see Schedule Settings.

Register access level

1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Access Control** on the left sidebar.
3. Click **ADD ACCESS LEVEL**.



4. Enter **Name** and **Description** in the **Add New Access Level** screen.



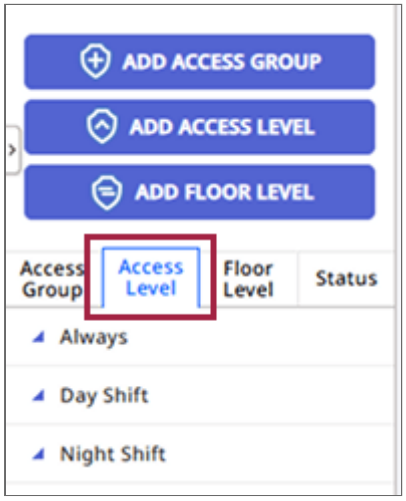
5. Select the door to apply the access level in the **Door** field.
6. Select the schedule to apply the access level in the **Schedule** field.
7. Click **Apply** at the bottom of the screen to register the access level.

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 on registering doors, see Register Door.
- If the desired schedule is not available, click **+ Add Schedule** to add one. For more information on schedule settings, see Schedule Settings.

Edit access level

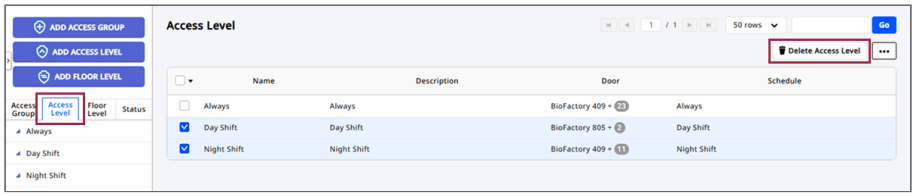
1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Access Control** on the left sidebar.
3. Click the **Access Level** tab.



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 Management** → **Access Control** on 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.



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.

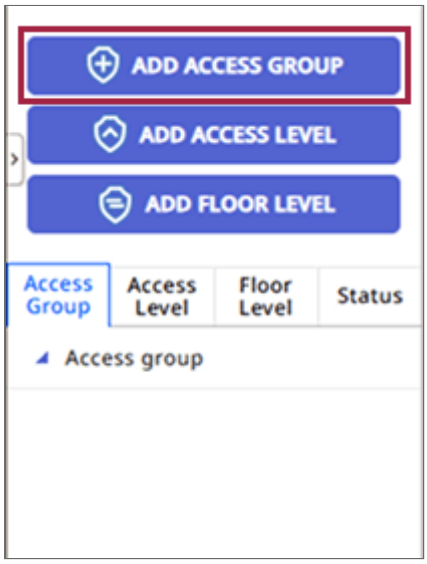
Before you start

Confirm the following before registering access groups.

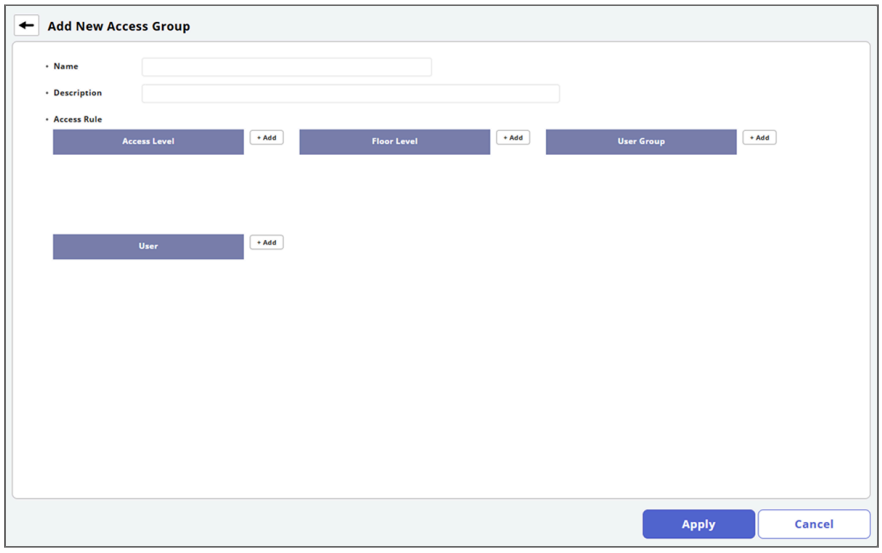
- Set up access levels. For more information on registering access levels, see Manage Access Levels.
- Set up floor levels. For more information on registering floor levels, see Manage Floor Levels.
- Set up user groups. For more information on registering user groups, see Manage User Groups.

Register access groups

1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Access Control** on the left sidebar.
3. Click **ADD ACCESS GROUP**.



4. On the **Add New Access Group** screen, enter **Name** and **Description**.



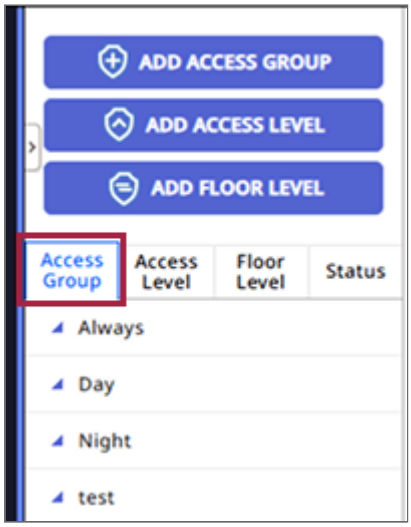
5. In the **Access Level** field, click **+ Add** to select the access levels to apply to the access group.
6. In the **Floor Level** field, click **+ Add** to select the floor levels to apply to the access group.
7. In the **User Group** field, click **+ Add** to select the user groups to apply to the 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 on registering access levels, see Manage Access Levels.
- If the desired floor level is not available, you will need to register a new floor level. For more information on registering floor levels, see Manage Floor Levels.
- To delete added items, click .
- To search for a desired item, click .

Edit access groups

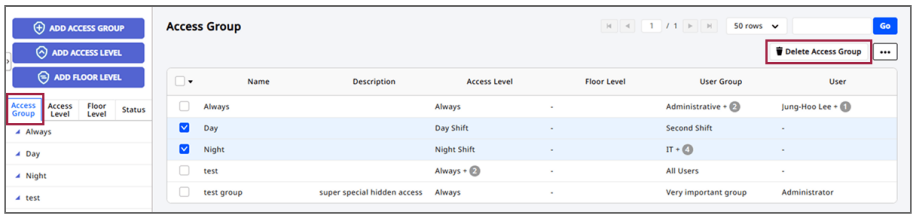
1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Access Control** on the left sidebar.
3. Click the **Access Group** tab.



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 Management** → **Access Control** on 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.



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**
>
> Floor level features are available through add-on options for **Essential** licenses and above. For more information on the licensing policy, see License Policy.

Before you start

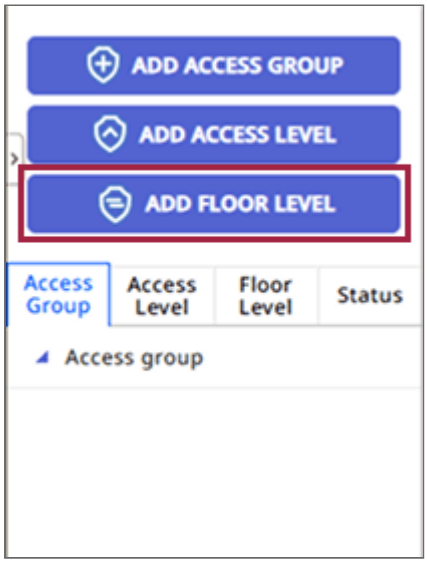
- You must set up the elevator before enrolling floor levels. For more information on registering an elevator, see Register

Elevator.

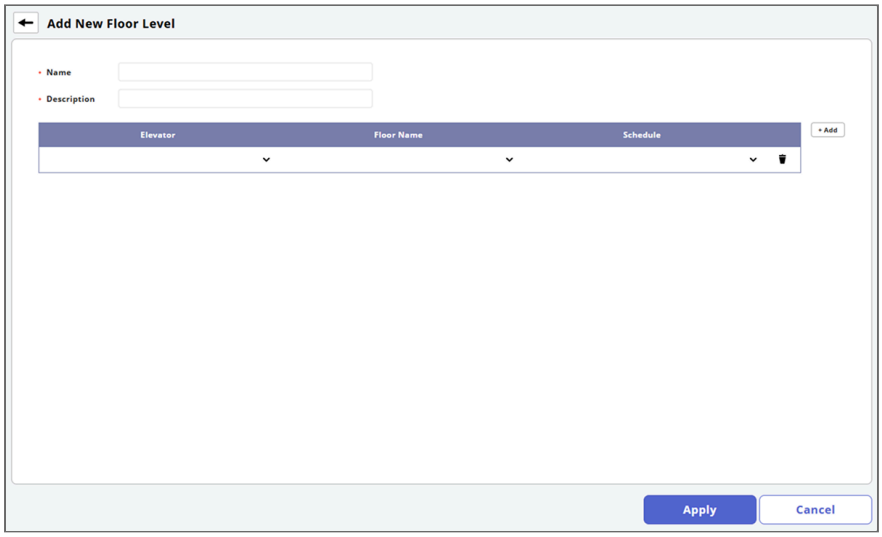
- You can define the time to apply to the floor grade in advance through schedule settings. For more information on schedule settings, see Schedule Settings.

Register floor levels

1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Access Control** on the left sidebar.
3. Click **ADD FLOOR LEVEL**.



4. In the **Add New Floor Level** screen, enter **Name** and **Description**.



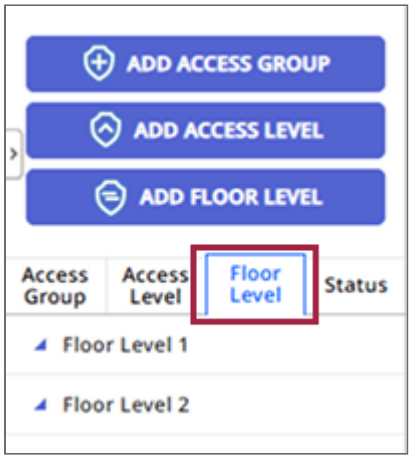
5. Select the elevator to apply to the floor grade in the **Elevator** item.
6. Select the floor to apply to the floor grade in the **Floor Name** item.
7. Select the schedule to apply to the floor grade in the **Schedule** item.
8. Click **Apply** at the bottom of the screen to register the floor level.

Info

- If the desired access level is not available, you will need to register a new access level. For more information on registering access levels, see Manage Access Levels.
- If the desired elevator is not available, you need to register a new elevator. For more information on registering an elevator, see Register Elevator.
- If the desired schedule is not available, click **+ Add Schedule** to add one. For more information on schedule settings, see Schedule Settings.
- 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 Management** → **Access Control** on 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 Management** → **Access Control** on 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.

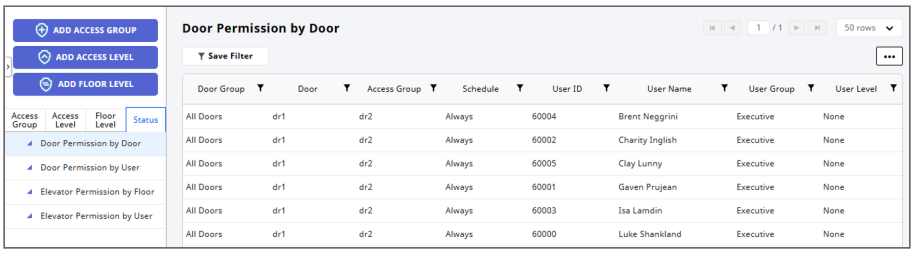


Check Access Permission Status

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.



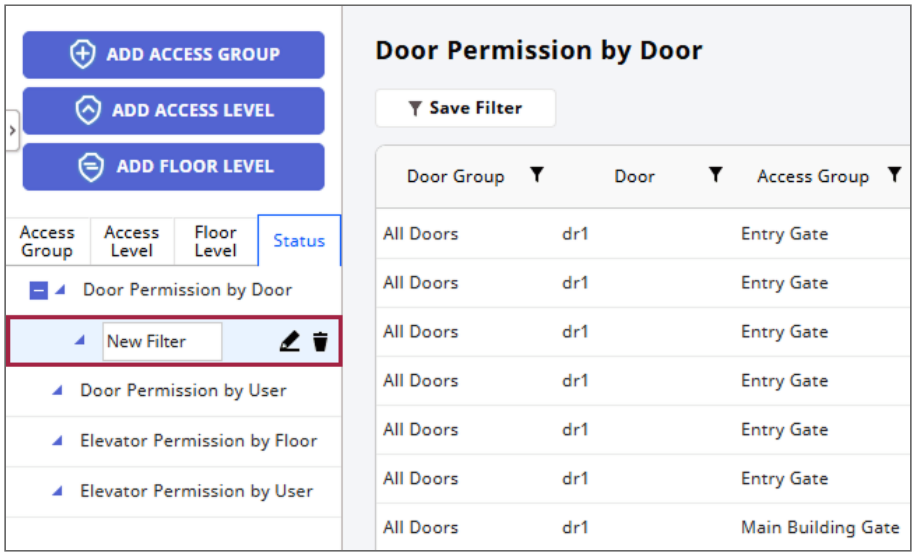
1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Access Control** on the left sidebar.
3. Click the **Status** tab.
4. Click the desired item from the list of statuses under the **Status** tab.
   - **Door Permission by Door**
   - **Door Permission by User**
   - **Elevator 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 ▼ in the header of the access permission list table. You can add filter conditions.

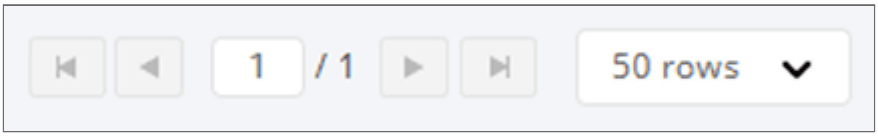
After setting the filter, you can save it. Click **Save Filter**. The saved filter can be checked in the status list under the **Status** tab.



- 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.



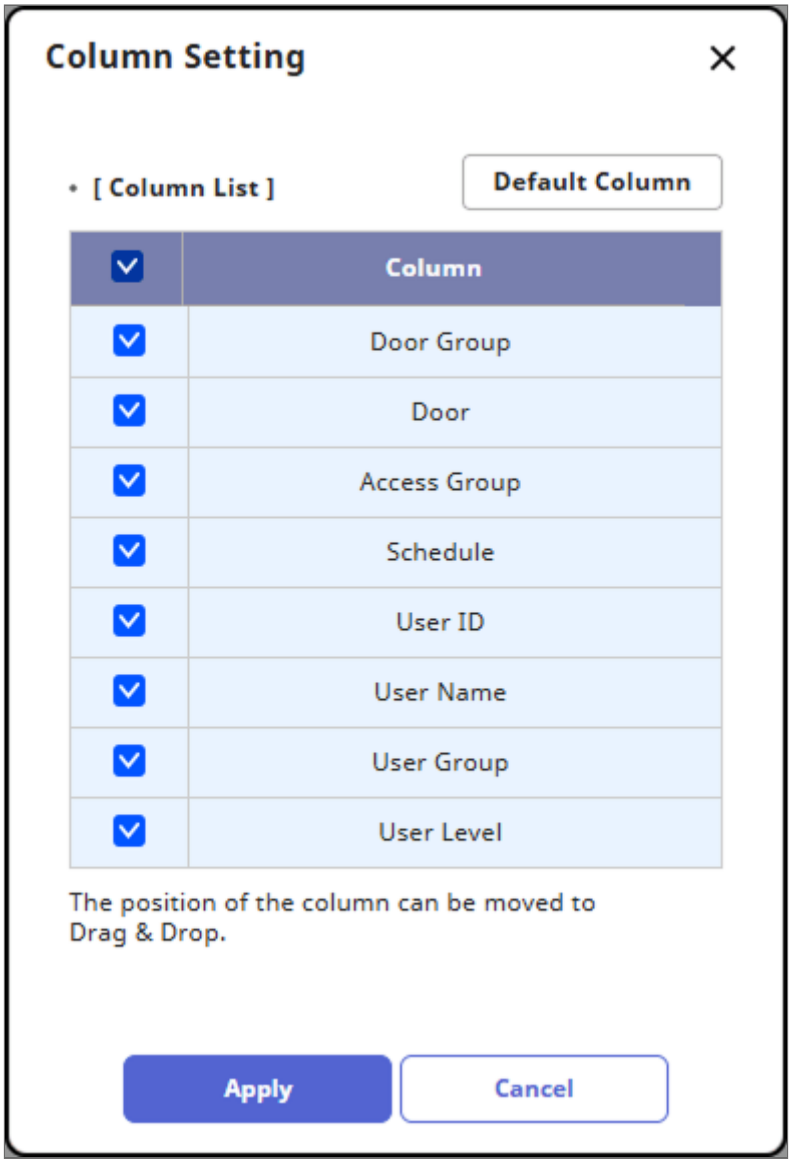
- ⏮: Move to the first page.
- ◀: Move to the previous page.
- ▶: Move to the next page.
- ⏭: Move to the last page.
- Enter the page number in the input field to move to the desired page.
- Click the row selection box to set the number of items displayed on each page.

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**.



- 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.

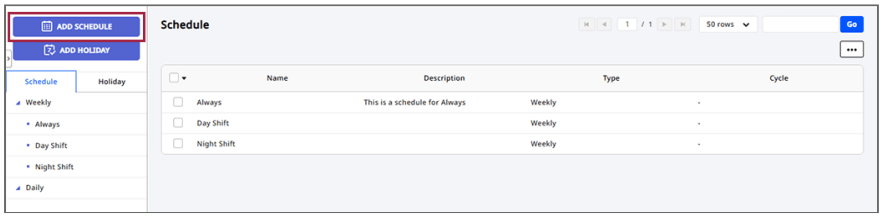
Once all settings are complete, click **Apply**.

Schedule Settings

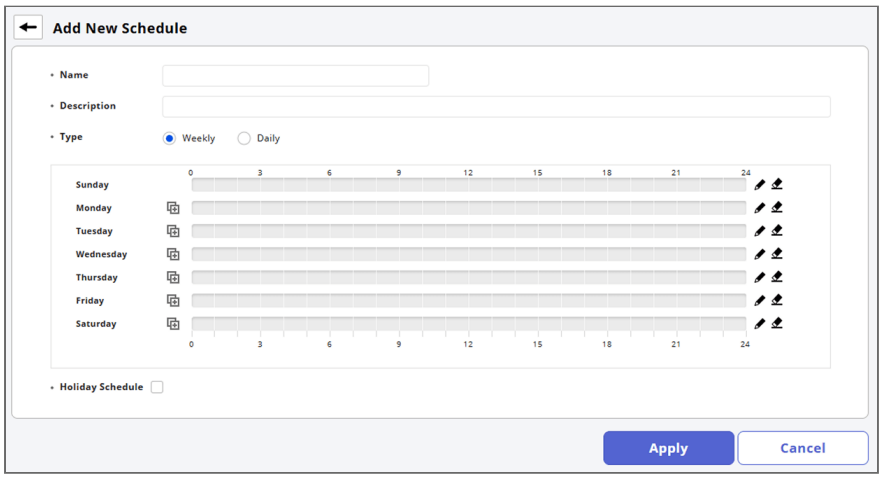
This guide describes how to efficiently operate access control and attendance management by setting up access and holiday schedules. Schedules are an important factor that can be applied to access control, allowing management of user access times and holidays.

Register schedule

1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Schedule** on the left sidebar.
3. Click **ADD SCHEDULE** at the top left of the screen.



4. Enter or set each item on the **Add New Schedule** screen.

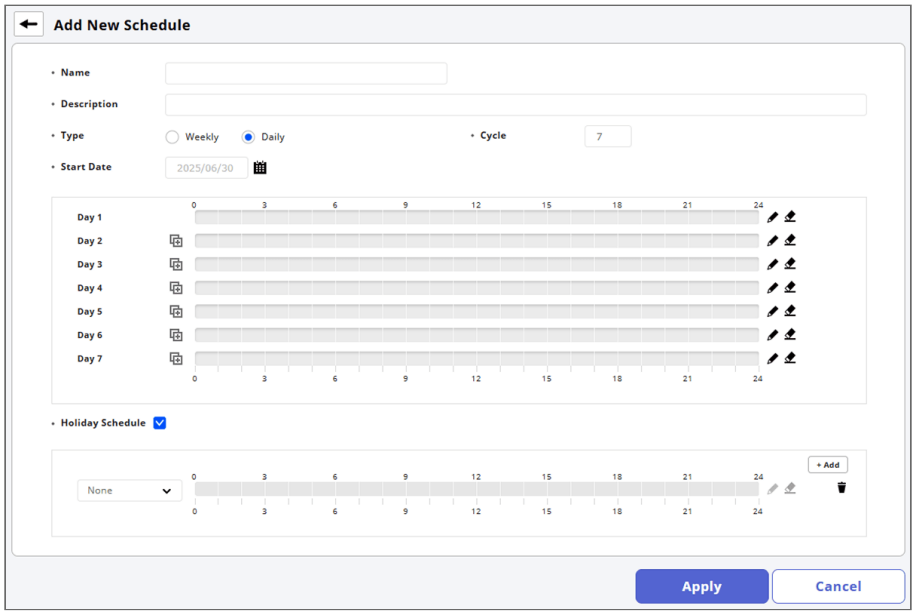


5. Once all settings are complete, click **Apply** at the bottom of the screen.

> **Info**
>
> For more information on the individual items on the **Add New Schedule** screen, see New schedule addition options.

New schedule addition options

Guide to individual items that can be set on the **Add New Schedule** screen.

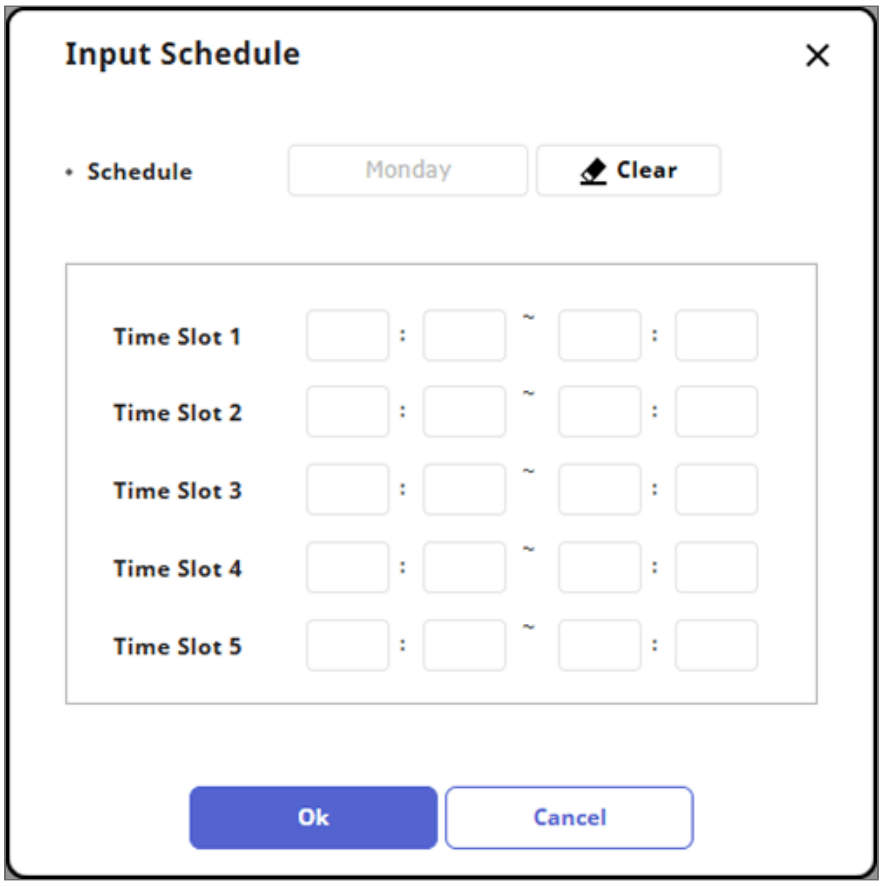


- **Name**: Enter the schedule name.
- **Description**: Enter a brief description of the schedule.

- **Type**: Choose a weekly or daily schedule. Selecting **Daily** will allow you to select **Cycle** and **Start Date**.



- Click the **Time segment** in the middle area to set the desired time. Once completed, click **Apply**.



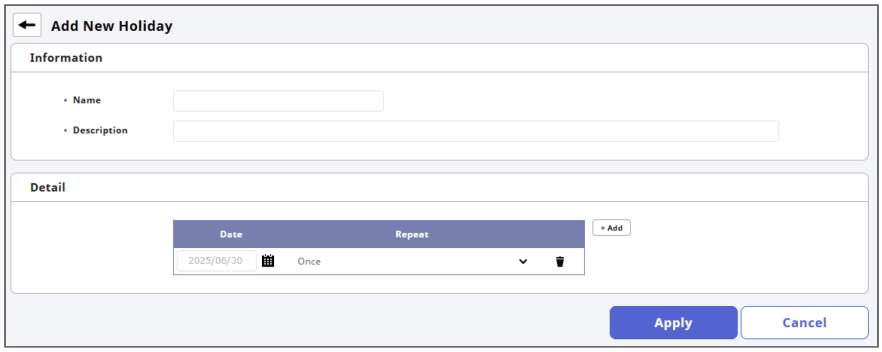
  - You can set up to 5 time slots per day or weekly.
  - To copy the time slots set above, schedule them and click .
  - Click to modify a time slot. Click to delete a set time slot.

- **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 to modify a time slot. Click to delete a set time slot.
> - To delete added holidays, click .
> - For more information on adding a holiday schedule, see Add holiday schedule.

Add holiday schedule

1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Schedule** on 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.



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 .

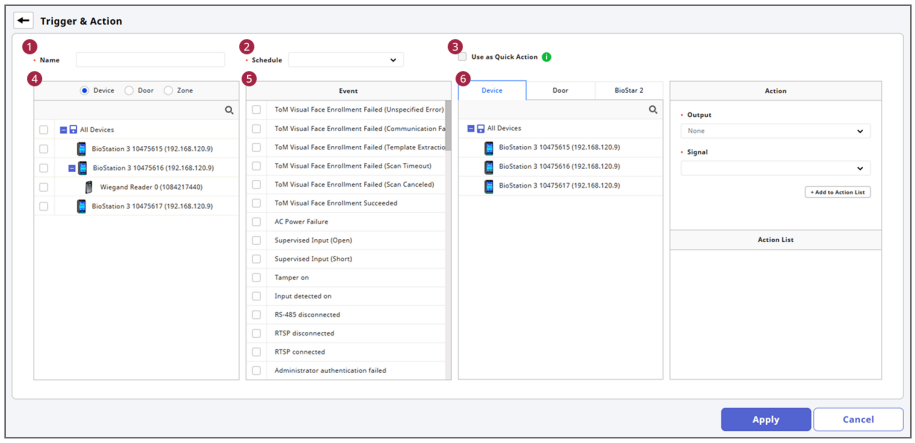
Trigger and Action Settings

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 **Access Management** → **Trigger & Action** on the left sidebar.
3. Click **Access Management** → **ADD TRIGGER & ACTION** in the upper left corner of the screen.



Follow the instructions on the screen to set the details.



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 on schedule settings, see Schedule Settings.

3 Use as Quick Action

Setting **Quick Action** allows you to control multiple doors at once using **Quick Action** 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** → **Access Management** → **Quick Action**. For more information on **Quick Action**, see How to Use the Quick Action.

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 AC** option can be enabled as an additional option with an **Essential** license or higher. For more information on the licensing policy, see License Policy.

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 ⚙ on the **BioStar X** tab. When the **SMTP Option** window appears, enter the email server information and click the **Apply** button. For more information, see Email Setting.
> - For detailed information on email server settings, contact your system administrator.

Once all settings are completed, click the **Apply** button.

How to Use the Quick Action

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

Add a quick action button in the **Quick Action** menu. Click it on the **BioStar X** main screen to control multiple doors at once.

> **Info**
> To add the **Quick Action** as a Quick Action, see Trigger and Action Settings.

Add quick action button

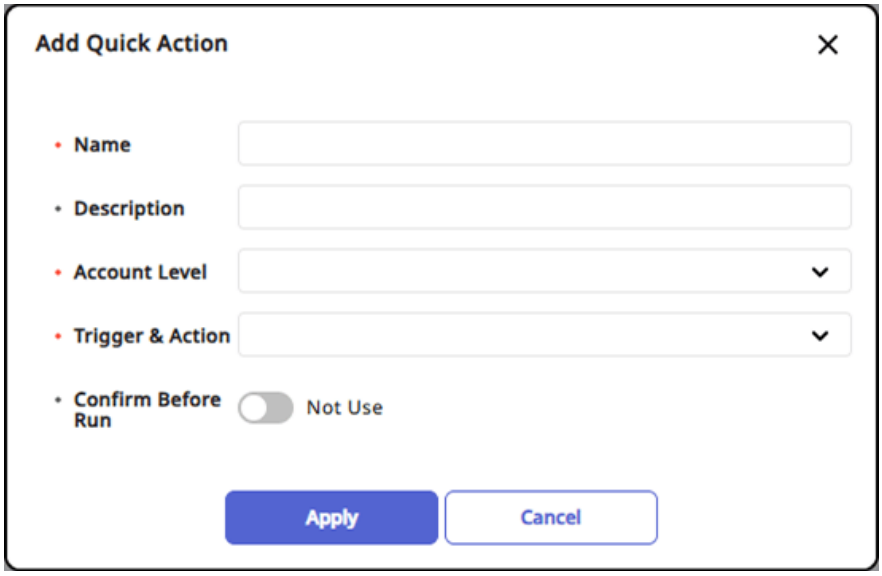
1. Click **Settings** on the **Launcher** page.

2. Click **Access Management** → **Quick Action** on the left sidebar.



3. Click **+ Add** in the **Quick Action Layout** 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** 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 **Quick Action**.

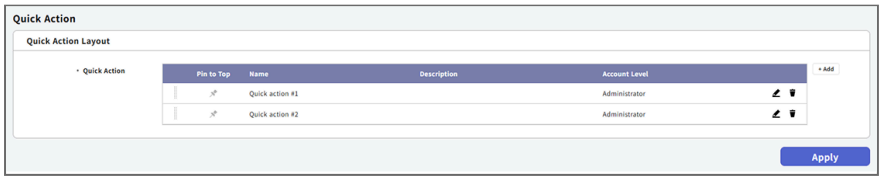


Info

- 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**.

Edit Quick Action button

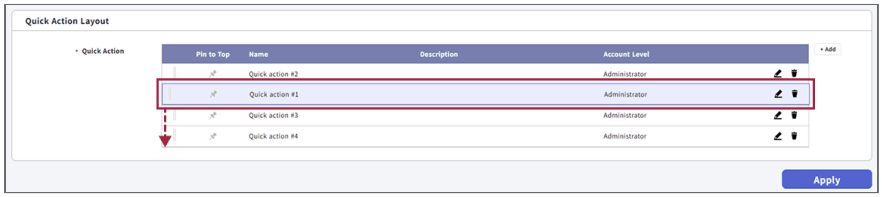
1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Quick Action** on the left sidebar.
3. Click the ✎ button on the right side of the quick action button you want to modify.



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.

Change Quick Action order

1. Click **Settings** on the **Launcher** page.
2. On the left sidebar, click **Access Management** → **Quick Action**.
3. In the quick action list, click and hold the leftmost column, then drag it to the desired position.



4. Click **Apply** in the bottom right corner of the screen to save the new order.

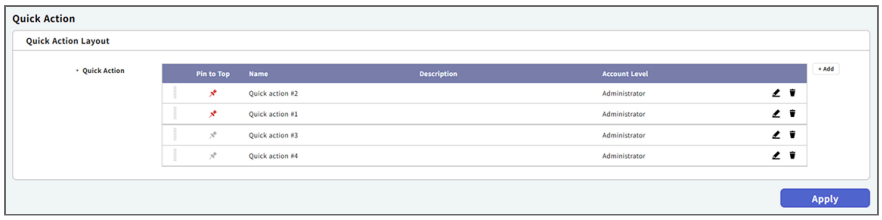
The quick action list at the top right of the screen shows the updated order.



Pin buttons to the header

Place quick actions that require quick access in the header area.

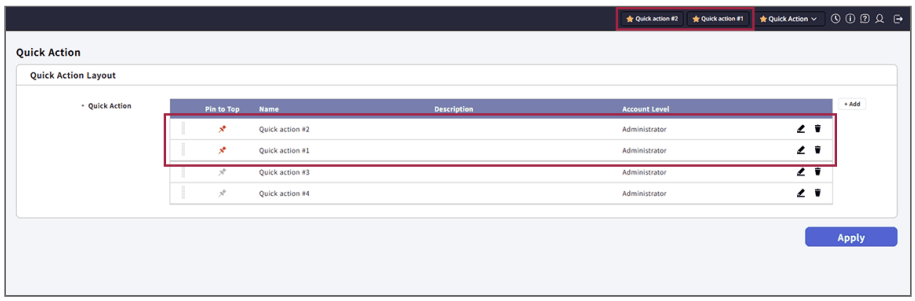
1. Click **Settings** on the **Launcher** page.
2. On the left sidebar, click **Access Management** → **Quick Action**.
3. Click **Pin to Top**( ) to pin the quick action to the header area.



> Drag the leftmost column to reorder. Click **Pin to Top** again to unpin.

4. Select all quick actions to pin to the header area. Click **Apply** in the bottom right corner.

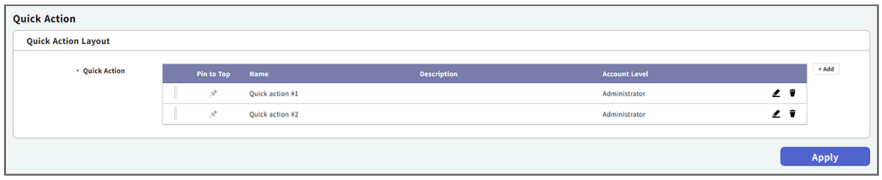
Pinned quick actions appear to the left of the **Quick Action** button at the top right of the screen.



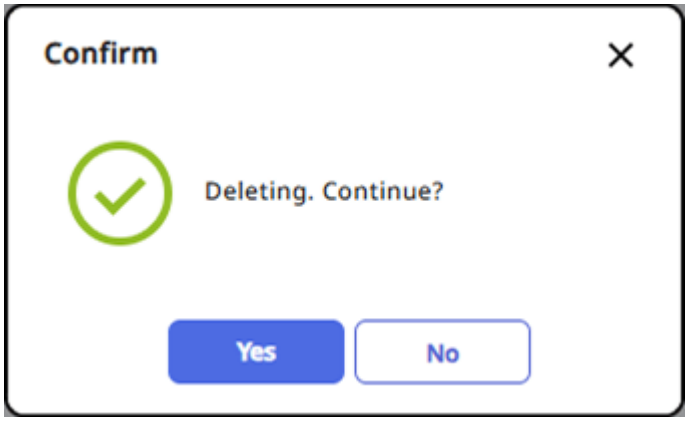
> **Info**
>
> - Pin up to 4 quick actions to the header area. When 4 quick actions are already pinned, you cannot pin more. Unpin another entry, then try again.
> - When the browser window narrows, all individual buttons in the header disappear, and you can find the pinned quick actions with the pin ( ) icon in the dropdown list of the **Quick Action** button.
> - If all added quick actions are pinned to the header area, the **Quick Action** button does not appear. Unpin certain entries to show the button again.

Delete Quick Action button

1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Quick Action** on the left sidebar.
3. Click to the right of the quick action button you want to delete.



4. Check the deletion confirmation pop-up and click **Yes**.



5. To reflect the deleted items, click **Apply** at the bottom right of the screen.

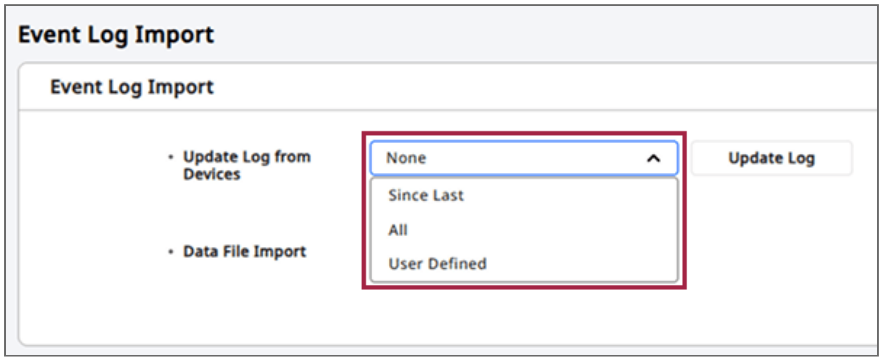
Import Event Logs

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, see Server Detailed Settings.

Import manually

1. Click **Settings** on the **Launcher** page.
2. Click **Event** → **Event Log Import** on the left sidebar.
3. Select the period for fetching logs in **Update Log from Devices**.



- **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 **Update Log** 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** on the left sidebar.
3. Click **Browse** 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.

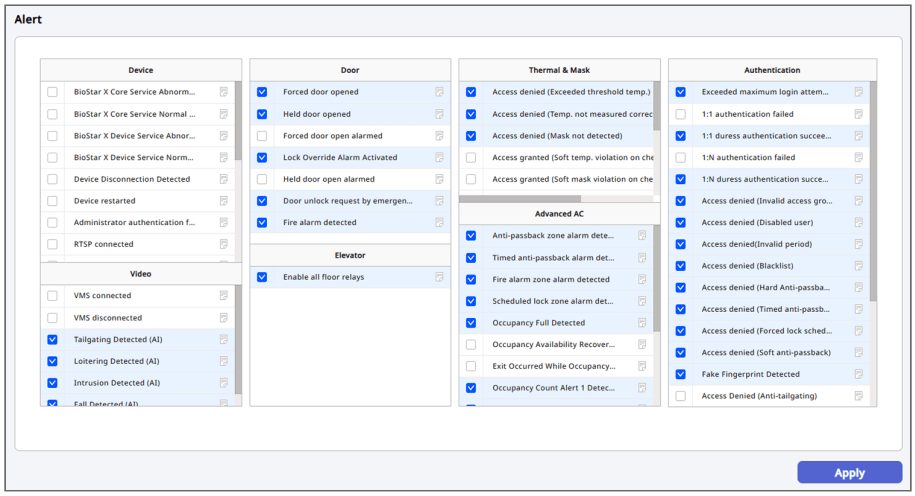
> **Info**
>
> - Data exported from devices using an outdated firmware version cannot be imported into **BioStar X**. Always use the latest version of the firmware.
> - Only data files exported from the following models can be imported: BioStation 3 Max, BioStation 3, X-Station 2, FaceStation F2, FaceLite, FaceStation 2, BioStation A2, and BioStation 2.
> - 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** on 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.



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 you don't have a sound file to play, see Configure Preferences for instructions on how to upload one.

Manage Credentials

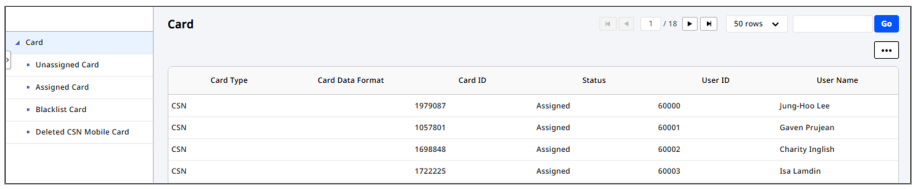
This guide describes how to manage credentials for access authentication. Check the card issuance status, cardholders, and the blacklist, and set Wiegand and smart card formats. This guide also covers card printing with cardPresso, mobile access card management with the Airfob Portal (Airfob Portal), and IR Face group matching setup.

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** on the left sidebar.
3. You can see the enrolled cards on the card list screen.



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

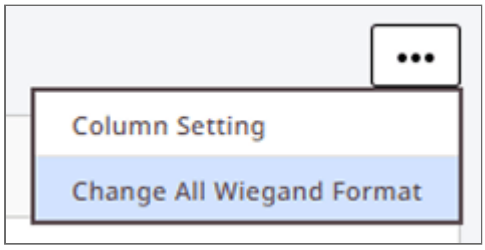
You can change the Wiegand card data format in use all at once.

> **Caution**
> Changing the data format of cards already assigned to users will also occur, so be cautious.

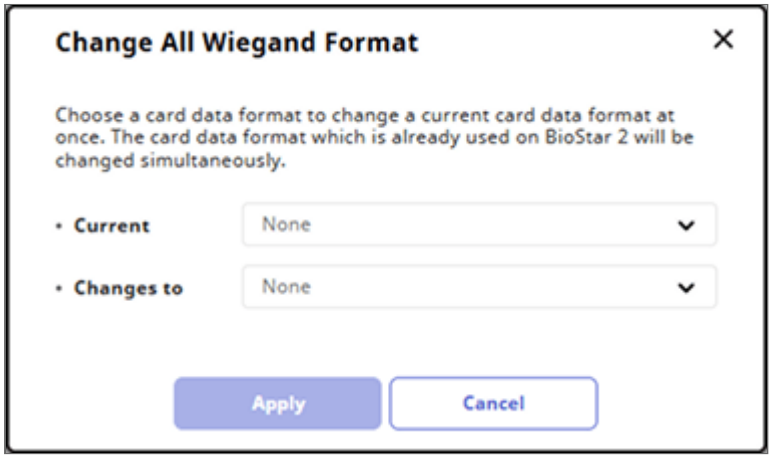
1. Click **Settings** on the **Launcher** page.

2. Click **Credential** → **Card** on 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.



5. Select the desired card data format from the **Changes to** list.

6. Click **Apply** to change the card data format.

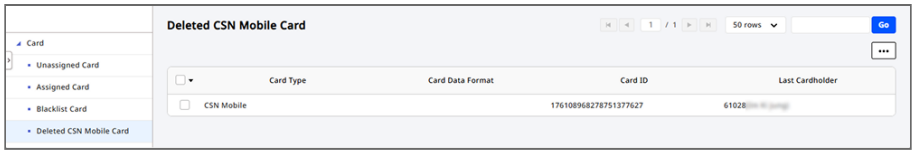
CSN Mobile Card Deletion Management Guidelines

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 **Deleted CSN Mobile Card** list from **Settings** → **Credential** → **Card**. In this list, you can view the **Card Type**, **Card Data Format**, **Card ID**, and **Last Cardholder**.

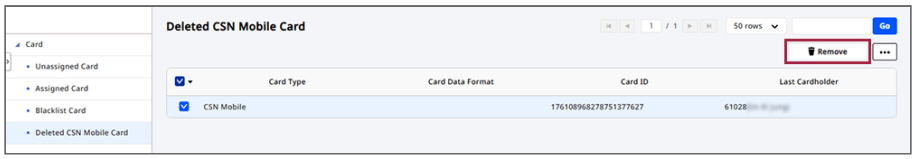


Preventing reissuance of deleted card IDs

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.



Info

CSN mobile cards included in the **Deleted CSN Mobile Card** list cannot be deleted from the **Unassigned Card** list.

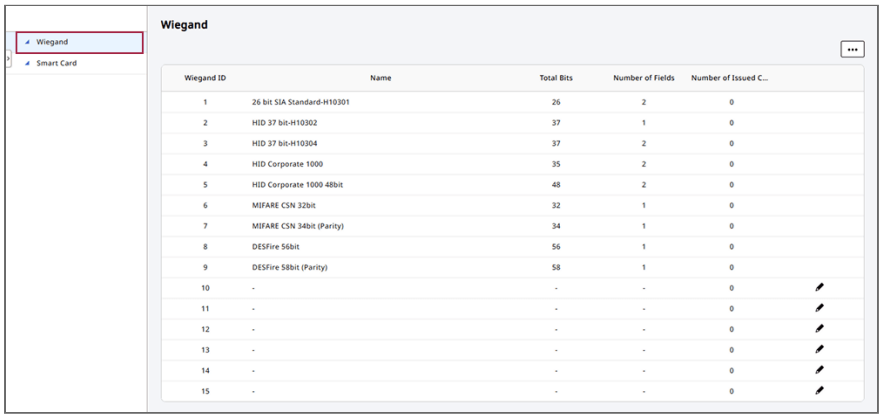
To delete a card from the **Unassigned Card** list, first remove the card from the **Deleted CSN Mobile Card** list and then proceed with the deletion.

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.



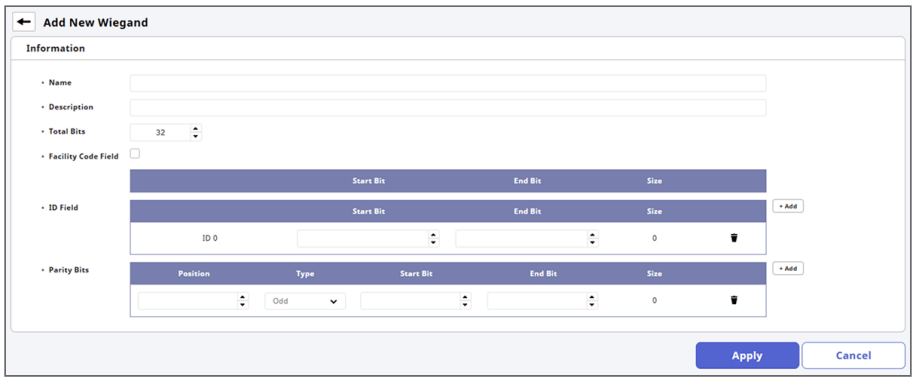
4. Click the ✎ button for the unnamed item in the Wiegand format list.
5. When the **Add New Wiegand** screen appears, set each item. For more information, see Setting options guide.
6. Click **Apply** to add the configured Wiegand format.

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**: 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

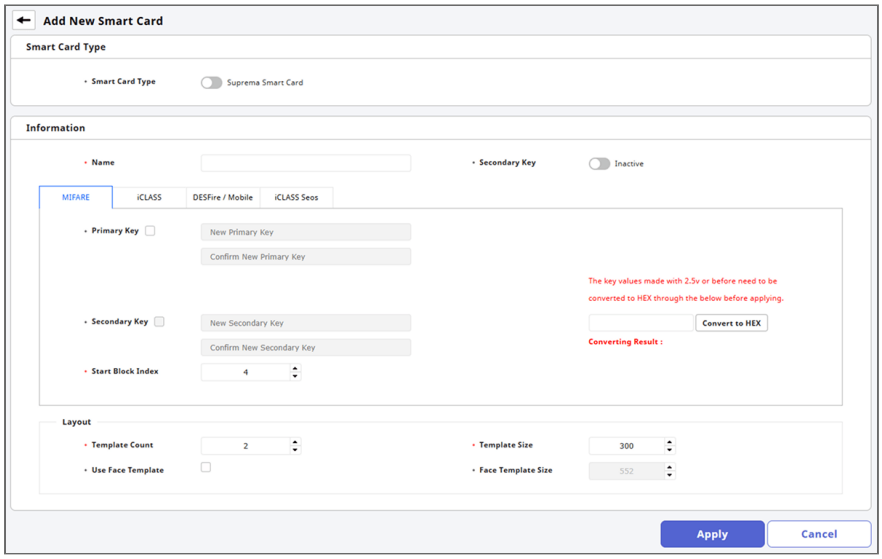
Set layout of smart cards such as MIFARE, iCLASS, DESFire, iCLASS Seos.

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, see Smart card types.

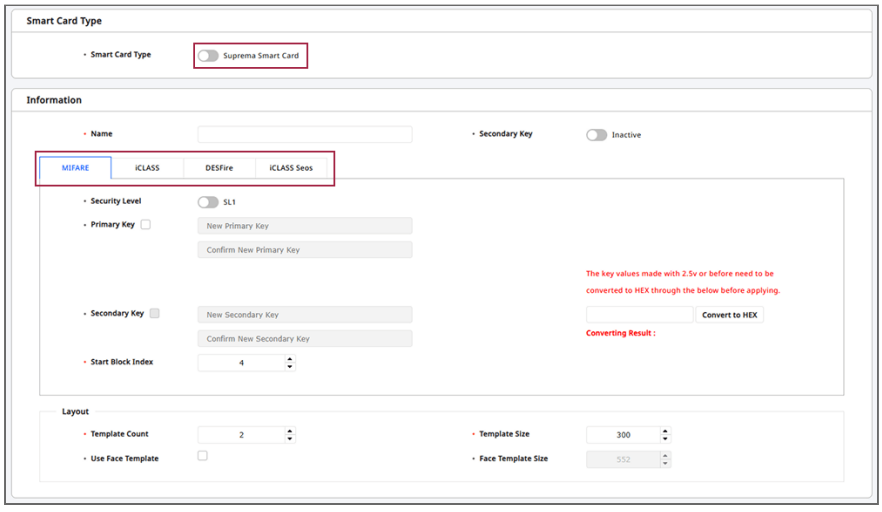


6. Once all settings are completed, click **Apply**.

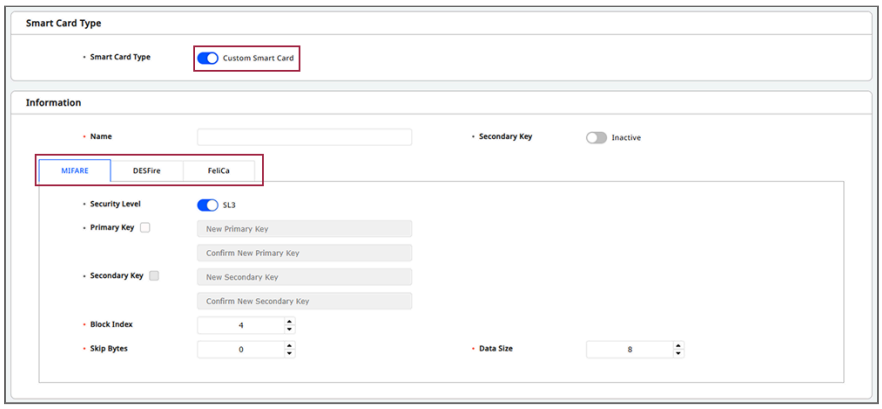
Smart card types

You can set the desired smart card type in the **Smart Card Type** option.

- **Suprema Smart Card**



- **Custom Smart Card**

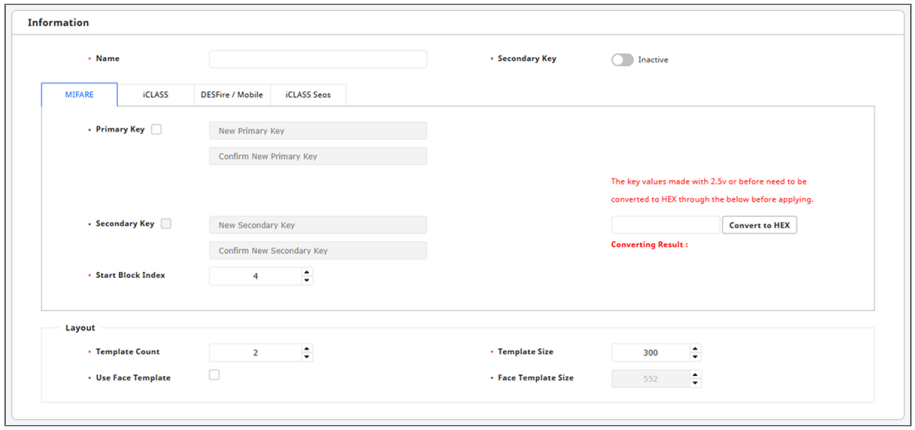


Info

- 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.

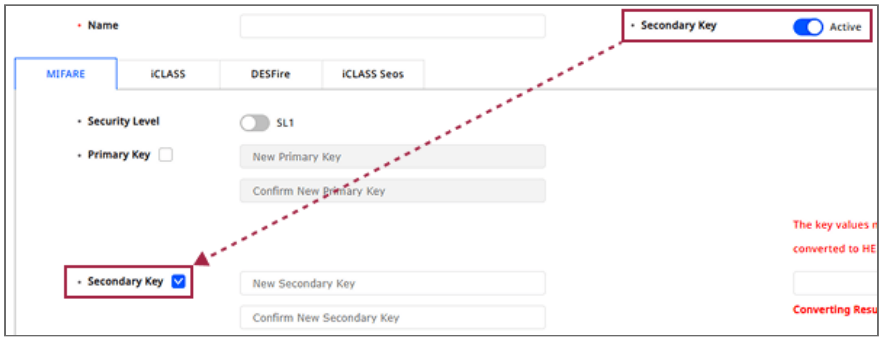


Info

- 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.



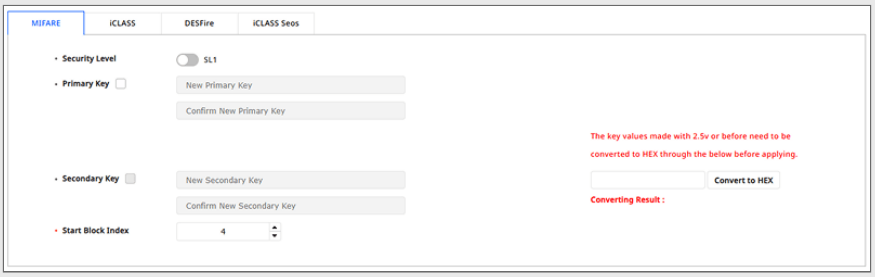
Set smart card

You can set the structure of the smart card.

Suprema smart card

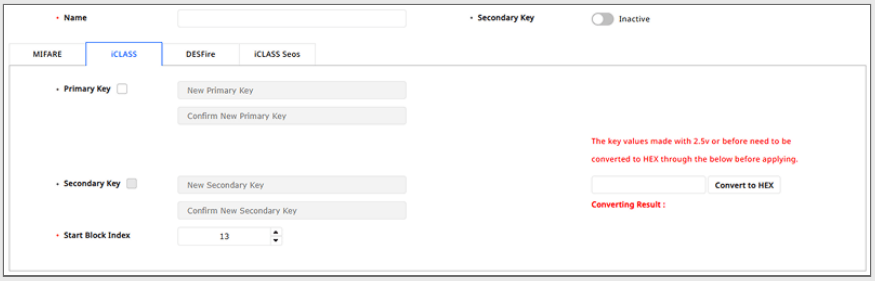
The **Primary Key** and **Secondary Key** support only hexadecimal. Enter the key value for each input field and click **Convert to HEX**. Use the converted value as the site key.

▼ MIFARE



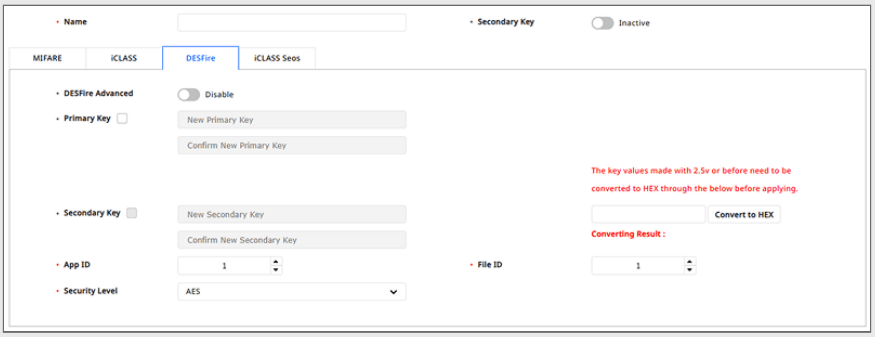
- **Security Level**: Set encryption type to **SL1** or **SL3**.
- **Primary Key**: The key that encrypts communications between the smart card and the card reader.
- **Secondary Key**: Used for authentication when the card's primary site key does not match. The secondary site key can only be entered 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



- **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



- **DESFire Advanced**: You can use DESFire cards issued by third parties. Only DESFire 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**.

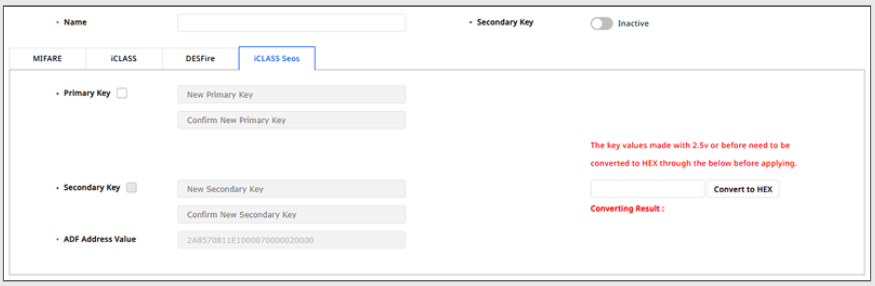
Info

When changing a card layout saved with **AES** encryption to **DES/3DES**, the following warning pop-up appears.

> ***Changing the Encryption Type to DES/3DES makes Enforce EV2/EV3 Secure Messaging unavailable on devices that use this card layout.***

Click the **Ok** button to save the changes. The **Enforce EV2/EV3 Secure Messaging** option turns off automatically for devices using this card layout. For more information about the **Enforce EV2/EV3 Secure Messaging** option, see Authentication Settings.

▼ iClass Seos



- **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

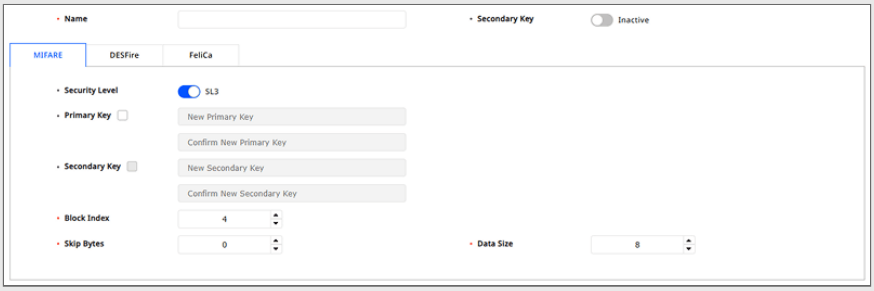
Use Face Template is available on the BioStation 3 Max, BioEntry W3, BioStation 3, and FaceStation F2 models.

Custom smart card

Custom smart cards only support MIFARE, DESFire, and FeliCa.

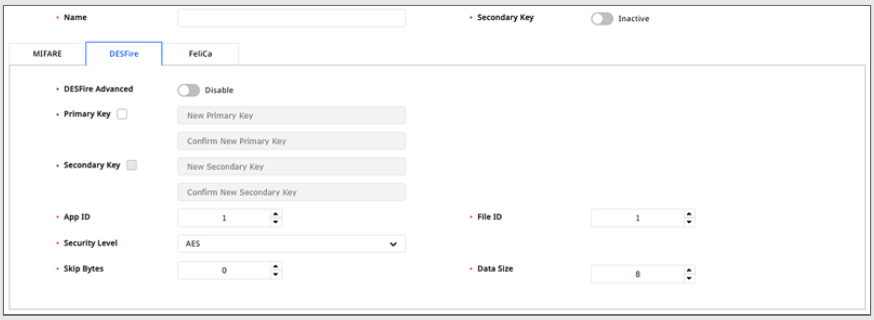
> **Info**
> FeliCa is only supported on BioStation 3 firmware version 1.3.0 or higher.

▼ MIFARE



- **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



- **DESFire Advanced**: You can use DESFire cards issued by third parties. Only DESFire 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**.

Info

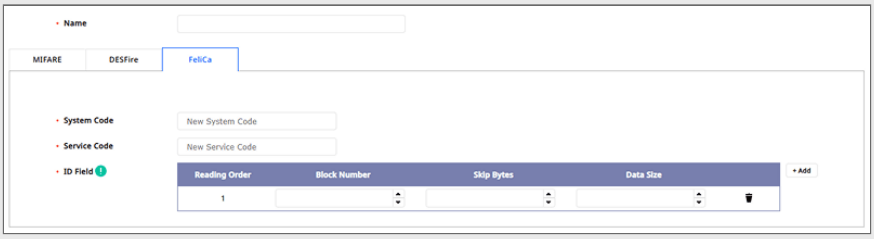
When changing a card layout saved with **AES** encryption to **DES/3DES**, the following warning pop-up appears.

> ***Changing the Encryption Type to DES/3DES makes Enforce EV2/EV3 Secure Messaging unavailable on devices that use this card layout.***

Click the **Ok** button to save the changes. The **Enforce EV2/EV3 Secure Messaging** option turns off automatically for devices using this card layout. For more information about the **Enforce EV2/EV3 Secure Messaging** option, see Authentication Settings.

- **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**



- **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.
- **ID Field**: Set to read a certain area on the card. You can set up to 8 blocks to read by clicking **+ Add**.

  Block Number: Set the block to read from the card. (0-150)

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 you 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

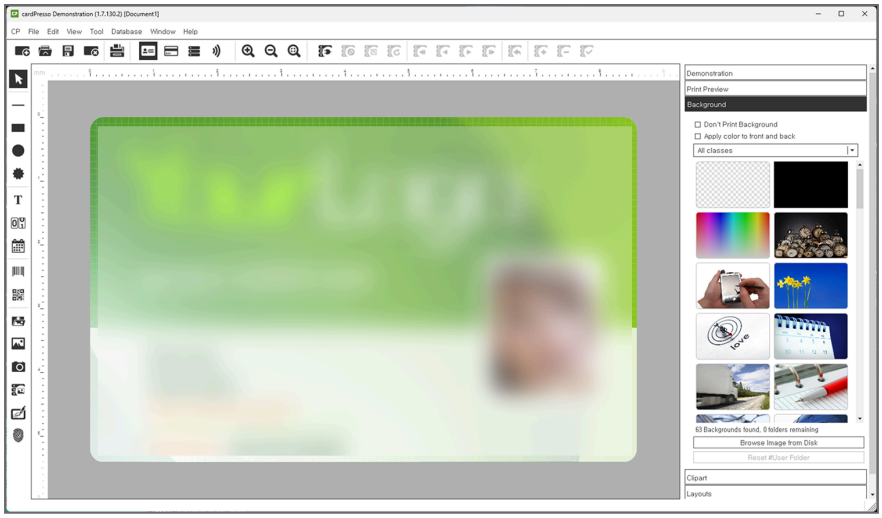
- For more information on the license types of the cardPresso program, refer to the following link.
- The web printing server function is supported only on Windows operating systems.

Install and configure 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.

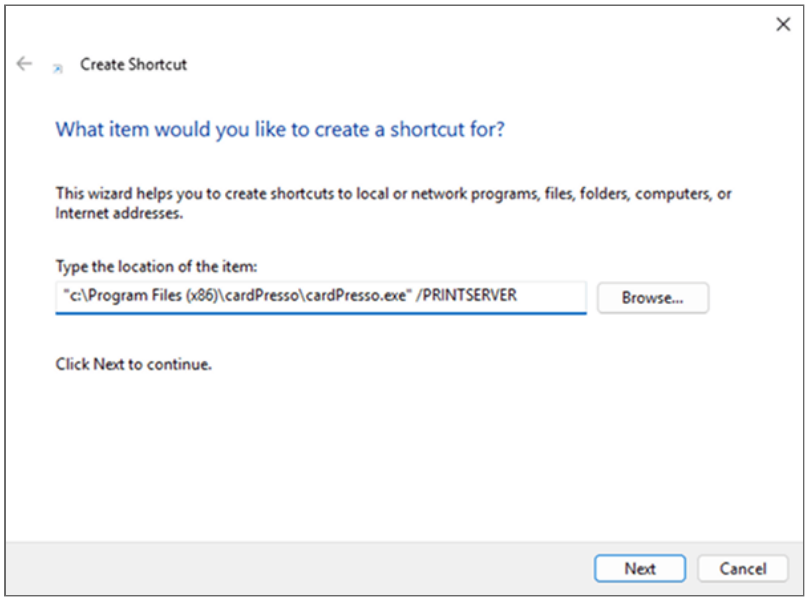
1. Download the latest version of cardPresso compatible with the operating system of the PC to be operated as a web printing server from cardPresso Download.
2. Install the program and activate the license issued by cardPresso.
3. After running cardPresso, create a card template.



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

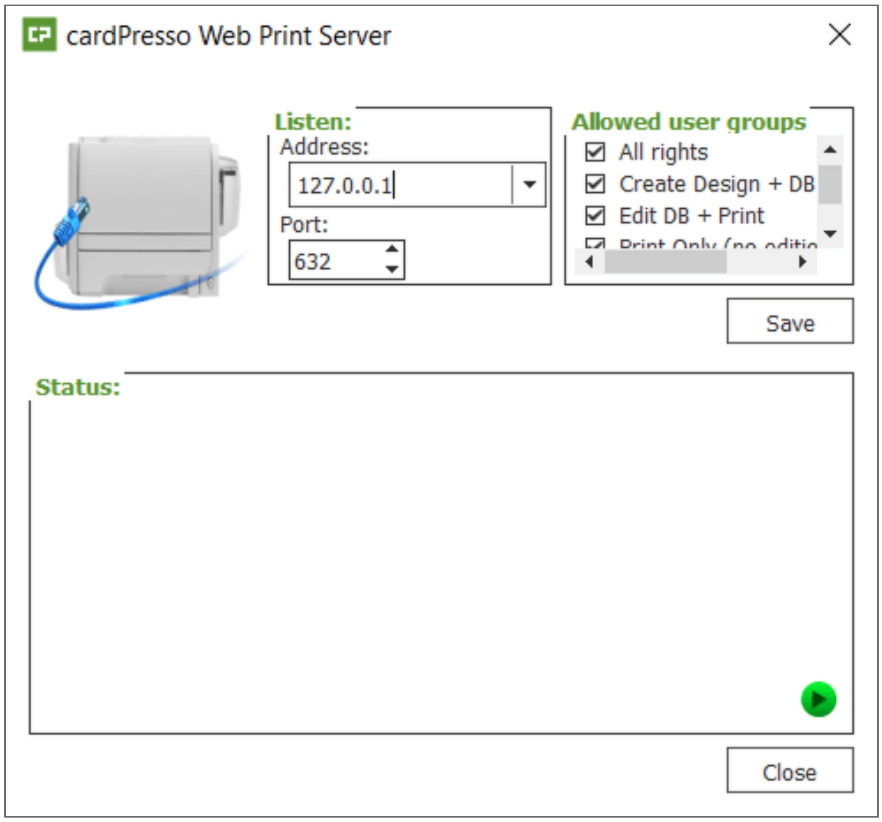
4. Save the created card template to a desired location on the server where **BioStar X** is installed. (ex. *C:\template\example.card*)
5. Right-click on the desktop of the PC where cardPresso is installed, then click **New** → **Shortcut** from the popup menu.
6. Enter the following in the **Item Location** field, then click the **Next** button.

```
"C:\Program Files (x86)\cardPresso\cardPresso.exe" /PRINTSERVER
```



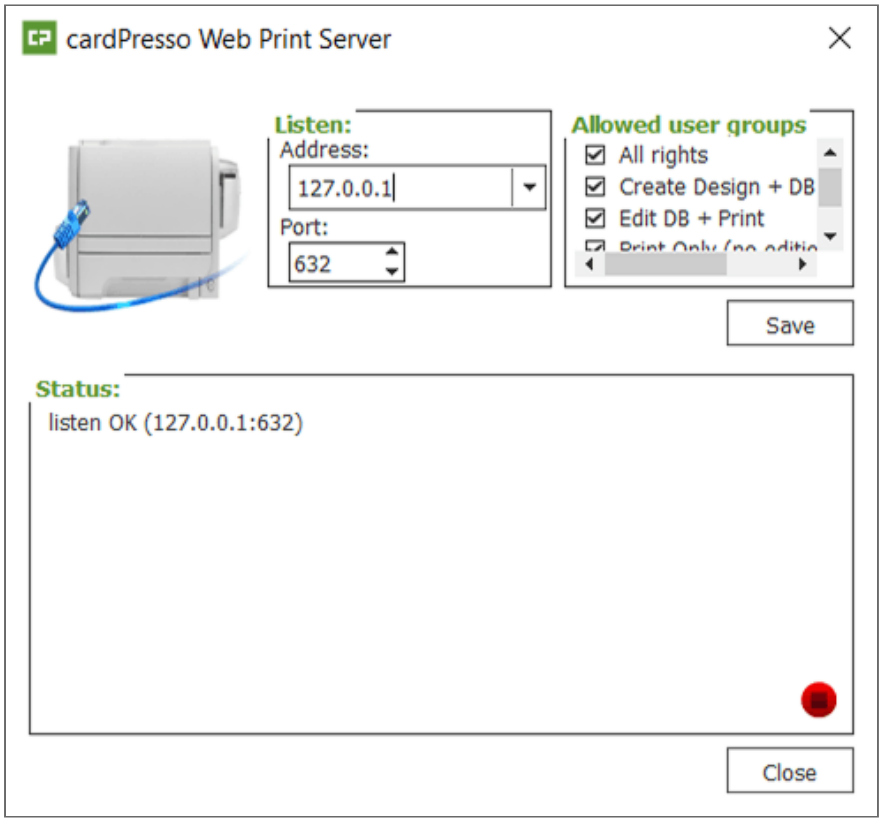
> The path where cardPresso is installed may differ based on the installation environment. After confirming the path where cardPresso is installed, modify it appropriately according to the above path.

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**: 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.

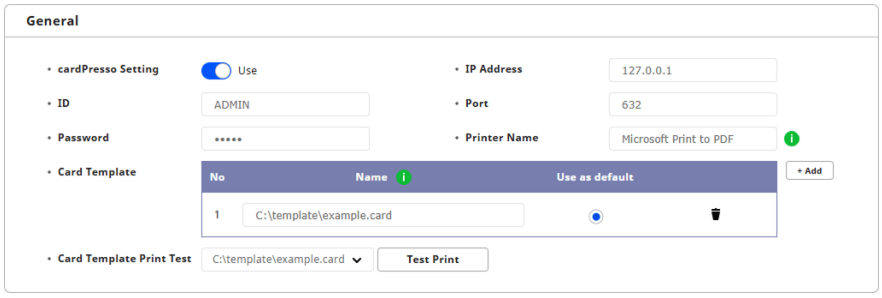


> Do not close the window until card printing is complete.

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. Click **Credential** → **Card Printer** on the left sidebar.
3. Activate the **cardPresso Setting** to **Use**, then enter each item.



- **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.

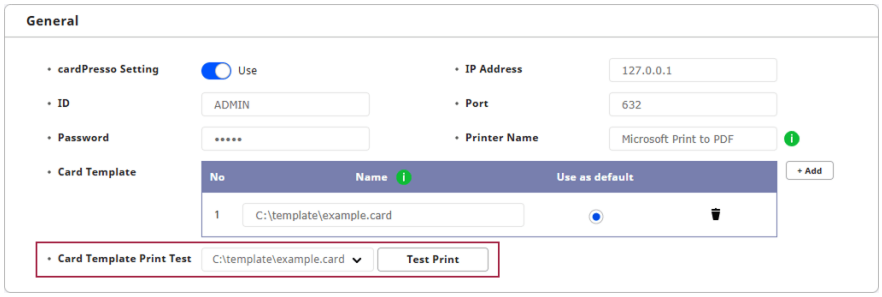
- **Card Template**: Click **+ Add** to add a **Card Template**. In the **Name** item, enter the full path including the filename and extension of the card template.
  - The file name of the card template can be entered using alphanumeric, and special characters.
  - Up to 20 card templates are supported.
  - 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. Click **Credential** → **Card Printer** on the left sidebar.
3. Select the card template you want to print, then click the **Test Print** button.

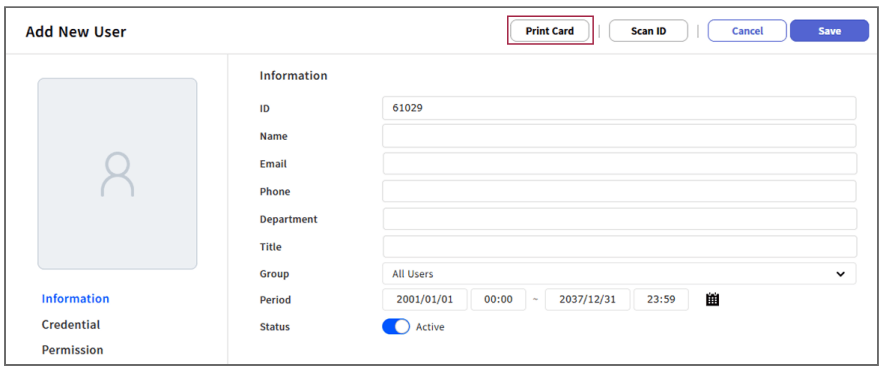


4. Card template with Administrator information is printed.

Print card templates by user

Print cards with per-user card templates.

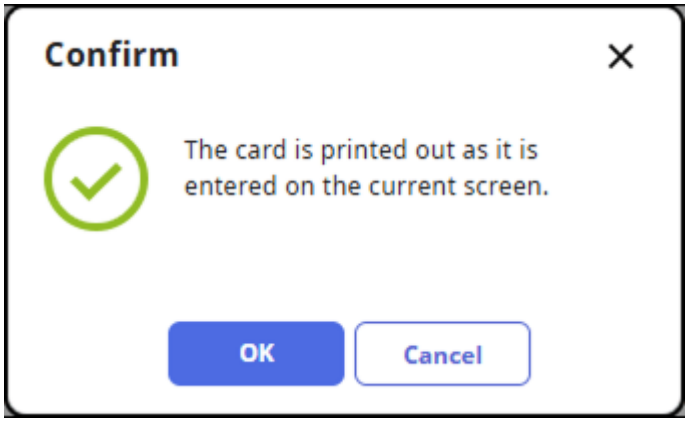
1. Click **User** on the **Launcher** page.
2. Click the **New User** button at the top right of the screen. The **New User** window appears.
3. Fill out the form and click the **Print Card** button.
   - Each item can be entered with alphanumeric and special characters.



4. Select the card template you want to print and click the **Print** button.



5. When the popup window asking whether to print the card appears, click the **OK** button.

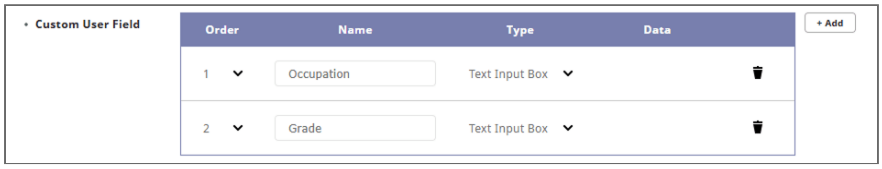


New user will be created and a card is printed as a card template with user information.

Add custom user fields

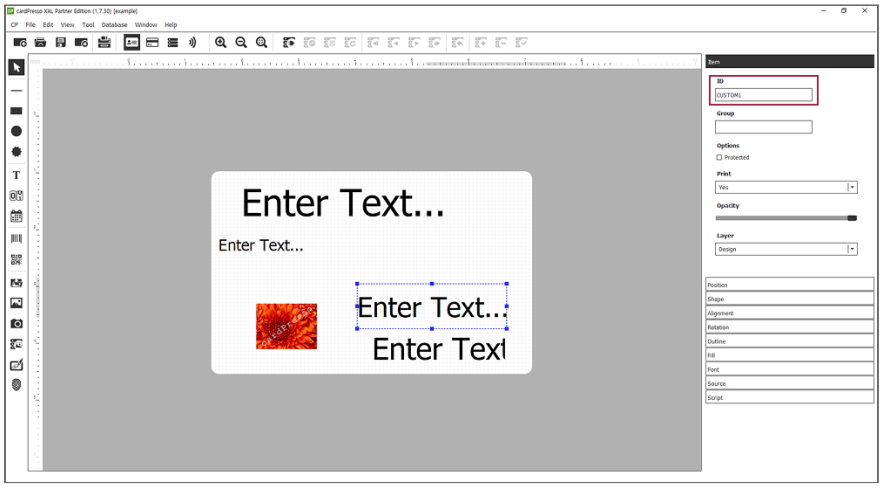
Print a card with a card template with custom user field added.

1. Click **Settings** on the **Launcher** page.
2. Click **System** → **Server** on the left sidebar.
3. In the **User/Device Management** section, click **+ Add** in **Custom User Field** to enter a **Name** and select a **Type**. The order of the **Custom User Field** adds decides the element **ID** of the card template.



   Based on the BioStar X element ID, **Order 1** is the same as **CUSTOM1**. For more information on BioStar X attribute IDs, see Card template attribute ID.

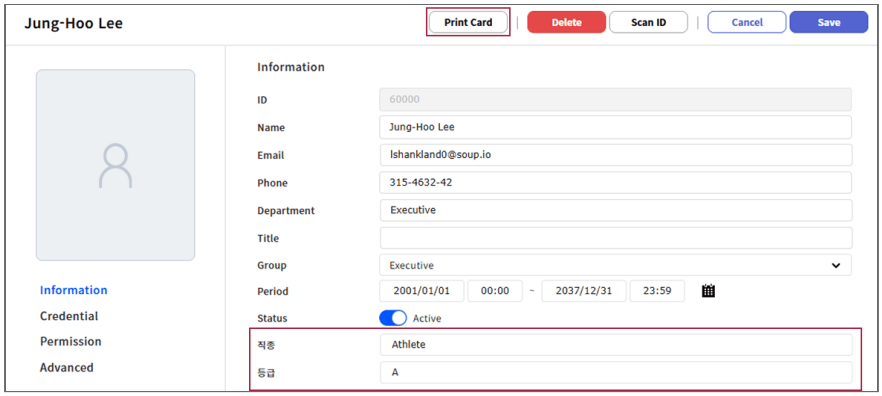
4. Once you complete the settings, click the **Apply** button at the very bottom of the screen.
5. Open the card template file by clicking **File** → **Open Template** in the cardPresso program. Add a new element and enter the **ID** as the **XML item ID name** in the BioStar X element ID order.



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.

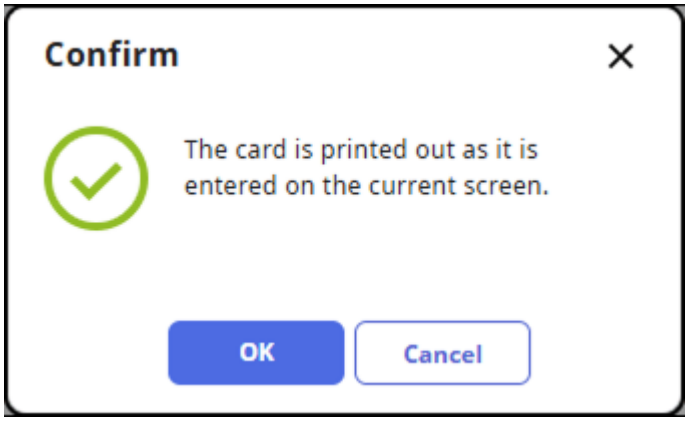
8. You can check the custom user fields you added. Fill in accordance with the form and click the **Print Card** button.



9. Select the card template you want to print and click the **Print** button.



10. When the popup window asking whether to print the card appears, click the **OK** button.



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

Index	BioStar X User Data	XML item ID name
16	Custom Field 9	CUSTOM9
17	Custom Field 10	CUSTOM10

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

  – BioStation 3 Max firmware 1.0.0 or later
  – XPass Q2 firmware 1.0.0 or later
  – BioEntry W3 firmware version 1.0.0 or higher
  – BioStation 3 firmware 1.0.0 or higher
  – X-Station 2 firmware 1.0.0 or higher
  – FaceStation F2 firmware 1.0.0 or higher
  – XPass 2 firmware version 1.1.0 or higher
  – FaceLite firmware version 1.2.0 or higher
  – BioLite N2 firmware version 1.3.0 or higher
  – XPass D2 (Rev 2) firmware version 1.4.0 or higher
  – FaceStation 2 firmware version 1.4.0 or higher
  – BioEntry W2 (Rev 2) firmware version 1.6.0 or higher
  – BioStation A2 firmware version 1.8.0 or higher (NFC supported model)
  – BioStation 2 firmware version 1.9.0 or higher (NFC supported model)

- Refer to the following for devices and firmware versions that support **Template on Mobile**.
  – BioStation 3 Max firmware 1.0.0 or later
  – BioEntry W3 firmware version 1.0.0 or higher
  – BioStation 3 firmware version 1.2.0 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.

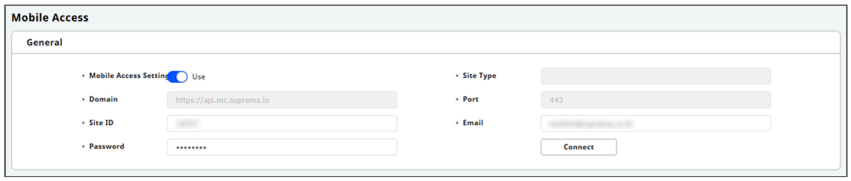
12. Click **Create**. Site creation will be completed.
13. Click the site name to access the Airfob Portal for that site.

> **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** on the left sidebar.
3. Edit the necessary fields.



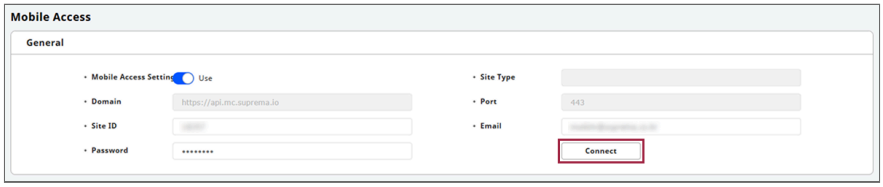
- **Mobile Access Setting**: You can set whether to use mobile access cards. Set to **Use** to issue mobile access cards to users.
- **Site ID**: Enter the site ID created in the Airfob Portal. The site ID can be found in the Airfob Portal pathway **Settings** → **Site**.
- **Email**: Enter the email 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, see Sign up for Airfob Portal and create Site.

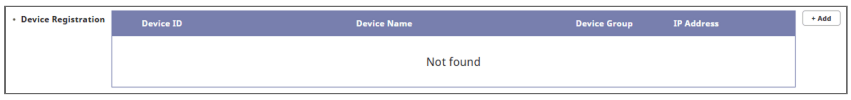
3 Register device

You can register devices that will use mobile access cards directly from the Airfob Pass application or **BioStar X**.

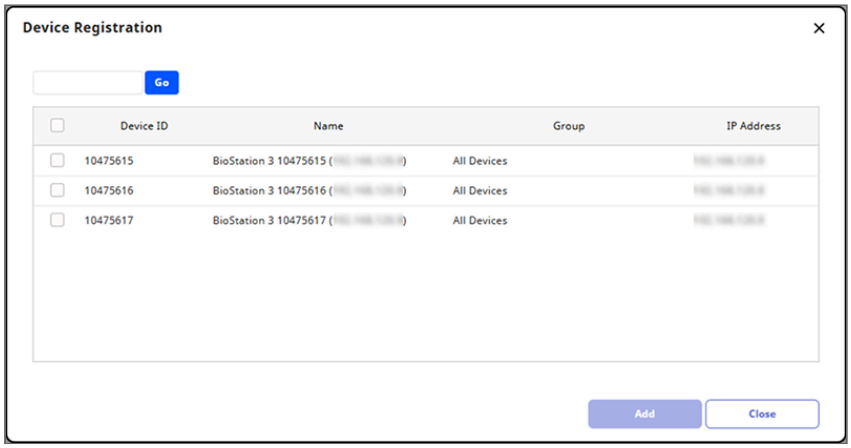


Once the settings for integration with the Airfob Portal are completed, click **Connect**. The **Device Registration** option will be available.

1. To add a device that will use mobile access cards, click **+ Add**.



2. In the device list of the **Device Registration** window, click the checkbox for the device that will use the mobile access card.



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

  – BioStation 3 Max firmware 1.0.0 or later
  – XPass Q2 firmware 1.0.0 or later
  – BioEntry W3 firmware version 1.0.0 or higher
  – BioStation 3 firmware 1.0.0 or higher
  – X-Station 2 firmware 1.0.0 or higher
  – FaceStation F2 firmware 1.0.0 or higher
  – XPass 2 firmware version 1.1.0 or higher
  – FaceLite firmware version 1.2.0 or higher
  – BioLite N2 firmware version 1.3.0 or higher
  – XPass D2 (Rev 2) firmware version 1.4.0 or higher
  – FaceStation 2 firmware version 1.4.0 or higher
  – BioEntry W2 (Rev 2) firmware version 1.6.0 or higher
  – BioStation A2 firmware version 1.8.0 or higher (NFC supported model)
  – BioStation 2 firmware version 1.9.0 or higher (NFC supported model)

- 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

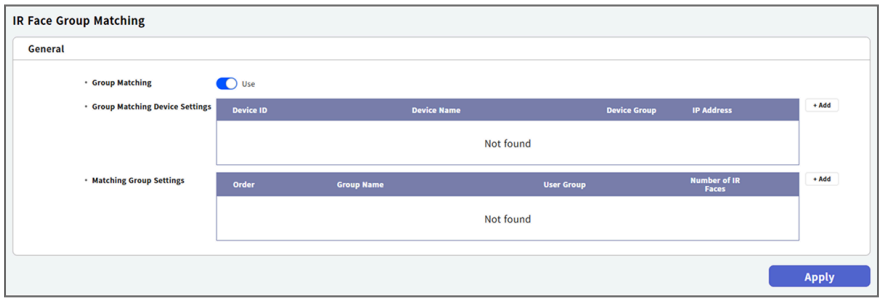
You can issue mobile access cards to users registered in **BioStar X**. To issue a mobile access card to a user, essential user information based on the method of sending the mobile access card must be entered. For more information, refer to the followings.

- Register Users
- Enroll Mobile Access Cards

Set IR Face Group Matching

IR Face Group Matching authenticates users by setting matching groups based on user groups. Use this feature to allow access via IR face authentication only to users in certain user groups.

1. Click **Settings** on the **Launcher** page.
2. Click **Credential** → **IR Face Group Matching** on the left sidebar.
3. Change the **Group Matching** option to **Use**.



4. Click **+ Add** in the **Group Matching Device Settings**.
5. When the **Group Matching Device Settings** window appears, select the device and click **Add**.

> Only the FaceStation 2 model can be selected.

6. Click **+ Add** in the **Matching Group Settings**.
7. Set the **Group Name** and **User Group** fields.
8. Click **Apply** at the bottom right of the screen to save the settings.

Info

- Up to 10 matching groups can be created.
- Each group can contain up to 3,000 IR face templates.
- Multiple user groups can be assigned to a single matching group.
- The total number of IR face templates in a matching group cannot exceed 5,000.
- If a user group contains more than 3,000 IR face templates, it cannot be set as a matching group.
- This feature is supported only by the FaceStation 2 model.
- Delete all configured devices and group settings to disable the group matching feature.

Activate License

This guide explains how to activate the **BioStar X** license and device licenses.

BioStar X License

Register the purchased **BioStar X** license.

How to register **BioStar X License** varies depending on the 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** on the left sidebar.

Info

- For more information on the licensing policy, see License Policy.
- For more information about license error codes, refer to the following link.

Register online

Info

The license key accepts only numbers and hyphens (-). Enter up to 16 digits in the `1111-1111-1111-1111` format.

Register a single license

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



Register multiple licenses

Add up to 30 licenses at a time. Click the + **Add More License** button. After entering all licenses, click **Activate**.



- When the number of fields reaches 30, the + **Add More License** button becomes disabled. You cannot add more licenses.
- Paste multiple license keys into the fields at once. The system detects only keys in the `1111-1111-1111-1111` format and splits them into each field.
- If the pasted keys exceed 30, only the first 30 are entered automatically. Extra keys are ignored.

Activation progress

Click **Activate** to open the progress pop-up. Do not close the page or popup until activation completes.

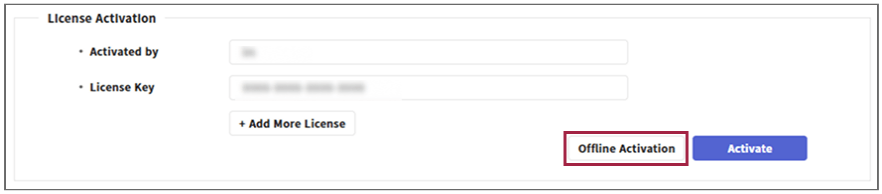
Register offline

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.

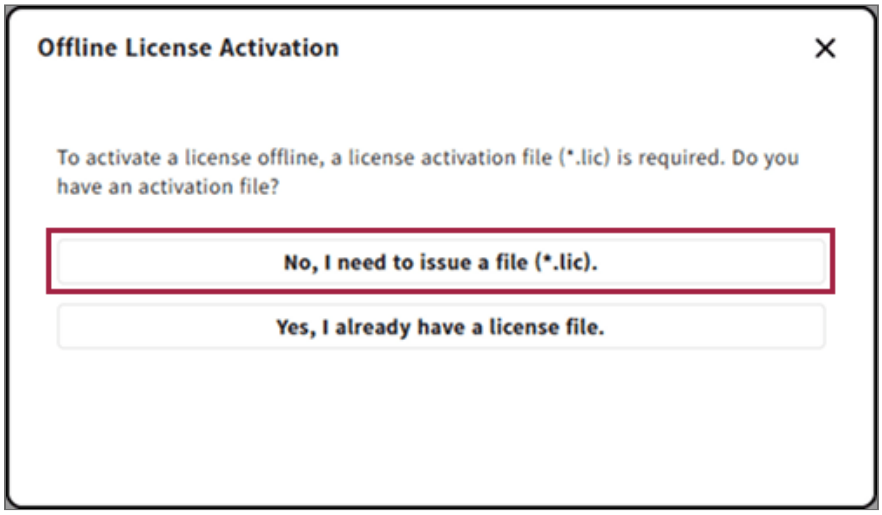
1. Enter any registration manager name for registration and the license key in the **License Activation** section.

   - The license key accepts only numbers and hyphens (`-`). Enter up to 16 digits in the `1111-1111-1111-1111` format.
   - Save or write down the administrator name and license key.
   - If you need multiple licenses, click the + **Add More License** button to add them.

2. Click **Offline Activation**.

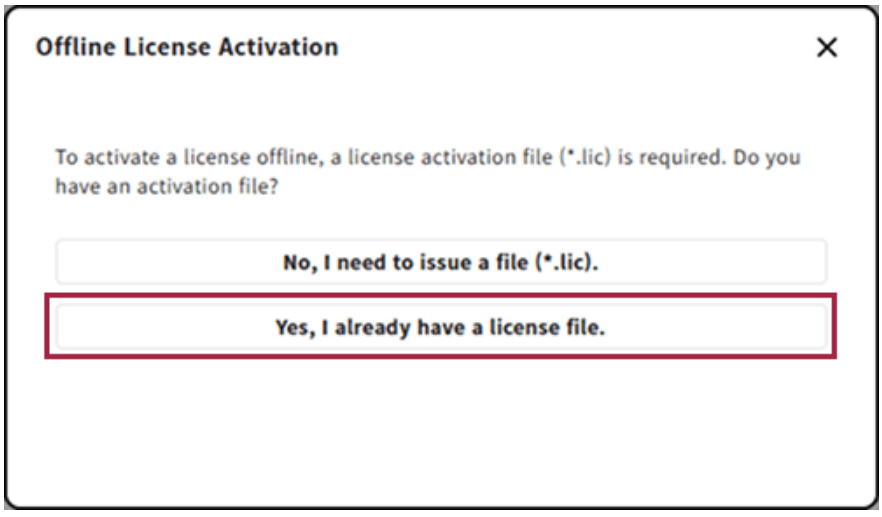


3. When the **Activate License Offline** window appears, click **No, I need to issue a file (*.lic).**.



> If an issued license file is available, click **Yes, I already have a license file.** on this screen, then go to step 9.

4. When the license request file (*.req) is created, download it to the local disk.
5. Send the downloaded request file to the reseller and request an offline activation file (*.lic).
6. After receiving the offline activation file, enter the administrator name and license key from step 1 in the **License Activation** section.
7. Click **Offline Activation**.
8. When the **Activate License Offline** window appears, click **Yes, I already have a license file.**.



9. When the Open File window appears, select the offline activation file (*.lic) or the compressed file (*.zip) stored locally.

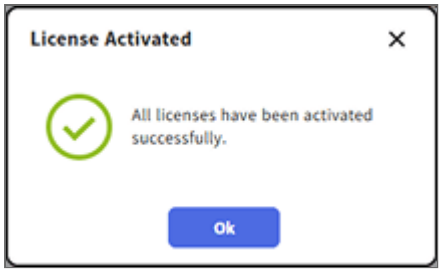
> If you request multiple licenses, you may receive a compressed file.

10. A progress status pop-up appears. Do not close the page or popup until activation completes.

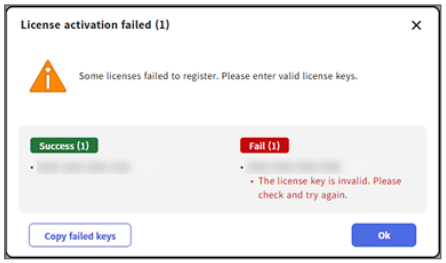
Check license activation results

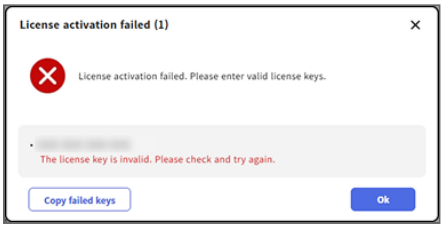
Depending on the activation results for the entered license key, the following message appears.

- If all entered license keys are valid, a success message appears.



- If the system activates only certain keys or fails to activate all keys, check each key's status and failure reason. The fields for successful keys clear, and failed keys remain for reentry.





- If all keys fail without an internet connection, a message tells you to check the connection and retry. The **Offline Activation** button appears. If the network is closed, click this button to register offline.

> **Info**
> Click **Copy failed keys** to copy the failed keys.

Verify activated license

Check the registered **BioStar X** license information in **Activated License**.



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.

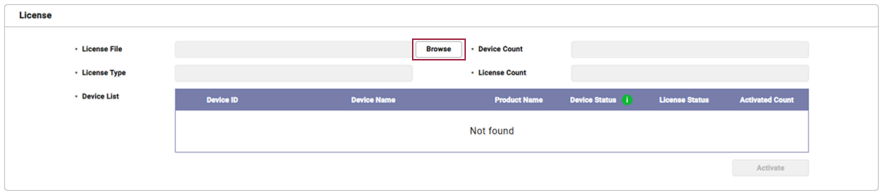
Before you start

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 on adding devices, see Register Device.

Apply device license

1. Click **Settings** on the **Launcher** page.
2. Click **License** → **Device License** on the left sidebar.
3. Click **Browse**.



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**.



6. Check **Device List**, and to activate the device license, click **Activate**.

> **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.
    - BioStation 3 Max firmware 1.0.0 or later
    - XPass Q2 firmware 1.0.0 or later
    - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) firmware version 1.2.0 or higher
    - X-Station 2 (XS2-QDPB, XS2-QAPB) firmware version 1.4.1 or higher
    - BioStation 3 firmware version 1.1.0 or later

  - **Multi Face Authentication**

    The following devices can use the **Multi Face Authentication** license.
    - BioStation 3 firmware version 1.5.0 or later

    Set the **Multi Face Authentication** option on devices with this license enabled. Refer to Authentication Settings.

  - **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**: The name of the device.
  - **Product Name**: 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**: Indicates whether the license is activated. Only **Not Activated** devices can activate licenses.
    - **Not Activated**, **Activated**, **N/A**
  - **Activated Count**: The connection status of the wireless door locks.

Info

- Values for **License Count**, **Activated Count** will only appear when the wireless door lock device license is loaded.

Manage 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.

The **Audit Trail** group on the left sidebar includes the following menus.

- **AC Audit Log**: Records access control activities, including creating, updating, deleting, viewing, exporting, importing, and administrative actions for users, devices, and doors.
- **Audit Settings**: Sets the audit log retention period and whether to record view history.

> **Info**
>
> For more information on **T&A Audit Log**, see View Time and Attendance Audit Logs. **T&A Audit Log** menu is available only with an active time and attendance (T&A) license.

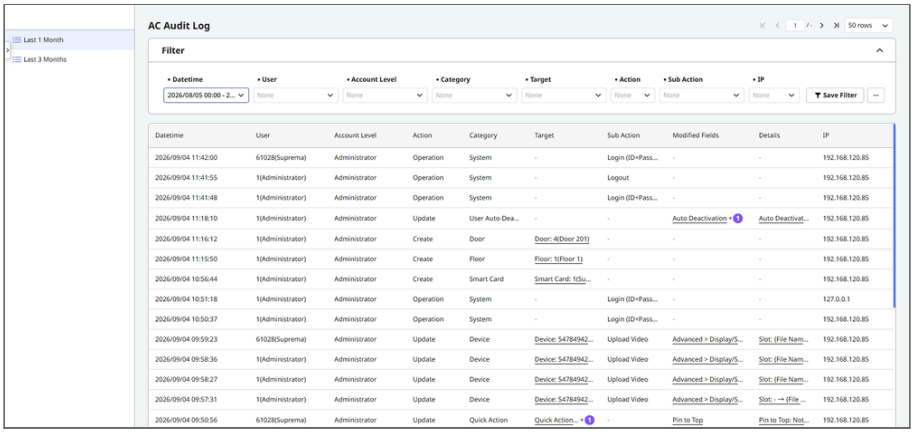
View Access Control Audit Logs

The **AC Audit Log** feature records access control activity for users, devices, and doors: create, update, delete, view, export, import, and operations. Each record shows when, who made the change, what changed, and how, to support audits and troubleshooting.

- **Security audit**: Detect unauthorized access attempts or privilege abuse.
- **Troubleshooting**: Track when system errors occur and review setting changes.
- **Compliance**: Keep access records, including personal data access history, and create audit reports.

Check access control audit logs

1. Click **Settings** on the **Launcher** page.
2. Click **Audit Trail** → **AC Audit Log** on the left sidebar.
3. The audit log list appears on the screen.



> **Info**
>
> - To change audit log policies such as the retention period, see Manage Audit Trail Retention Settings.
> - After upgrading to version 1.0.3, the system encrypts new audit logs regardless of the **Encrypt Personal Data on Database** option under **Settings** → **System** → **Security**.
> - If the system does not record certain audit logs after the upgrade from BioStar 2 to **BioStar X**, see Upgrade.

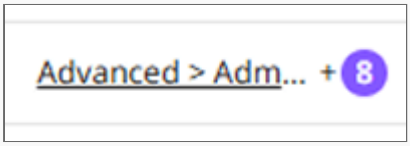
Table layout

The audit log list table has 10 columns and shows records in descending order by **Datetime**.

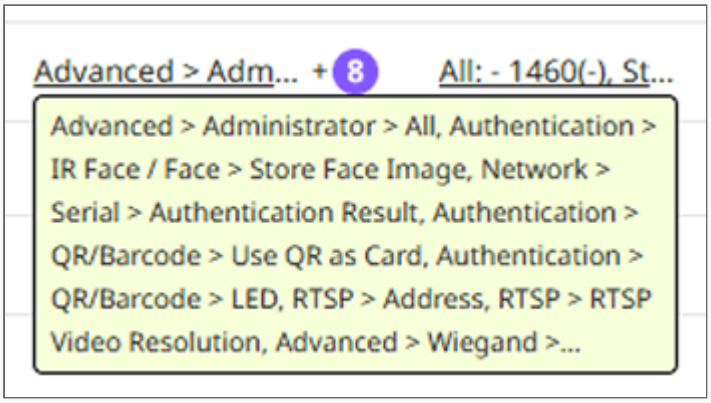
Column	Description
Datetime	The date and time the event occurred.
User	The user who performed the event. Displayed in the **id(name)** format.
Account Level	The administrator level of the user who performed the event.
Action	The type of action executed. Classified as one of **Create**, **Update**, **Delete**, **Read**, **Export**, **Import**, or **Operation**.
Category	The domain category of the event target (for example, users, devices, and doors).
Target	The target the action applies to. Displayed in the **type: id(name)** format.
Sub Action	Shows only when a detailed action name exists, such as login method or alarm disarm.
Modified Fields	The name of the field that changed or was viewed.
Details	Detailed information for each action. (e.g., changed values, reasons, and search criteria)
IP	IP address from which the user accessed. The system shows automatically issued records as **127.0.0.1**.

Info

- If the **Target** or **Modified Fields** value has 2 or more entries, only the first item is shown, and the rest are collapsed into a remaining-count badge on the right (e.g., **+208**). If the remaining count is 1,000 or more, the badge shows **+999**. Check the exact total count in the detail popup title. Click the badge to open the detail popup for that cell.

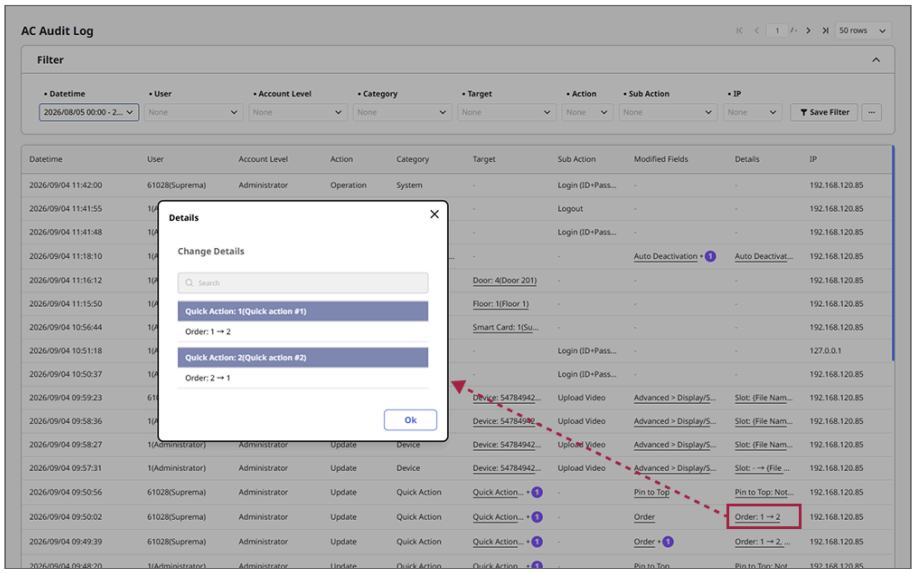


- Long cell values truncate to one line with an ellipsis. Hover over the value to see the full text in a tooltip. The tooltip truncates overflow text as `...`.



View details

The **Target**, **Modified Fields**, and **Details** columns appear underlined and are clickable when they have values. Click a value in the column to open the action-specific detail popup. To close the popup, click **OK** or ✕.

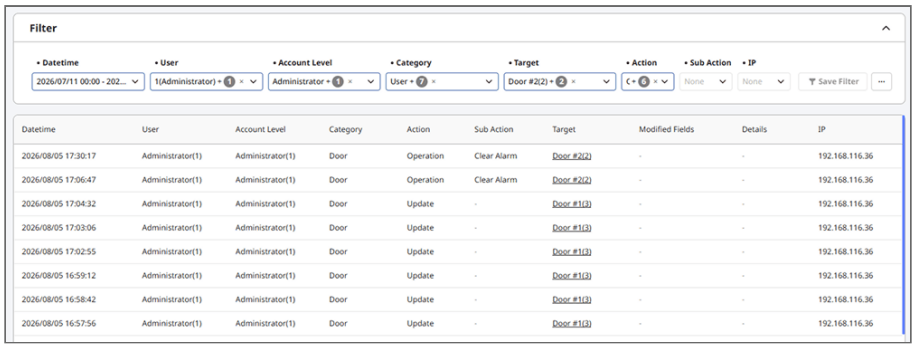


Enter a keyword in the **Search** field at the top of the popup to highlight or filter matching entries. When searching, the target popup updates groups and counts per group. The title total count stays the same.

Find records with filters

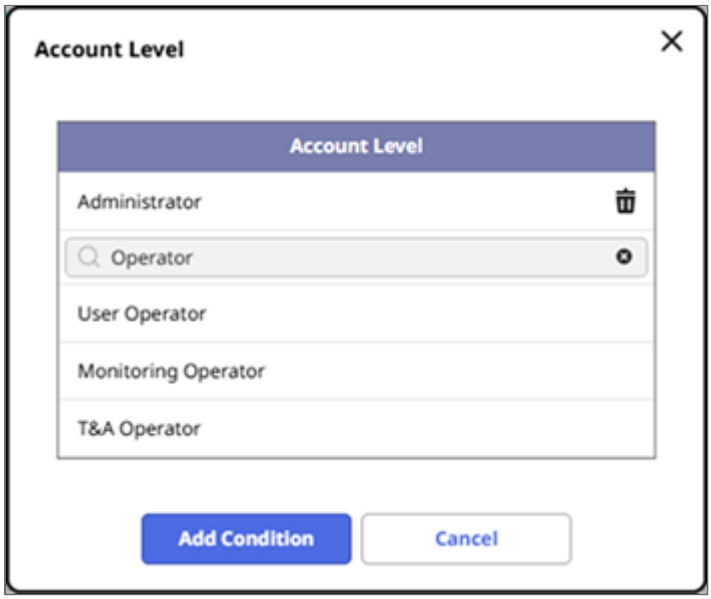
Combine the filters in the **Filter** section to narrow down and find the records you need. Select multiple values in one filter to

combine them with OR. Apply multiple filters together to combine them with AND.

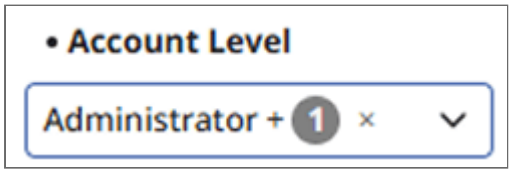


Filter	How it works
Datetime	Set the start and end dates and times. No length limit applies to the search period.
User	Enter a search term and press Enter to find matching users. The list is empty when you first open it.
Account Level	Enter a search term and press Enter to find matching administrator levels.
Category	Select one or more categories from the searchable checkbox list.
Target	Enter a search term and press Enter to find matching targets.
Action	Select one or more actions from the checkbox list.
Sub Action	Select a detailed action from the searchable list.
IP	Enter a search term, then press Enter to find matching IP addresses.

- If you apply no filters, records from the last 30 days appear by default.
- Select a value in each filter popup, then click **Add Condition** to apply it to the search immediately. Click **Cancel** to cancel the selection and close the popup.



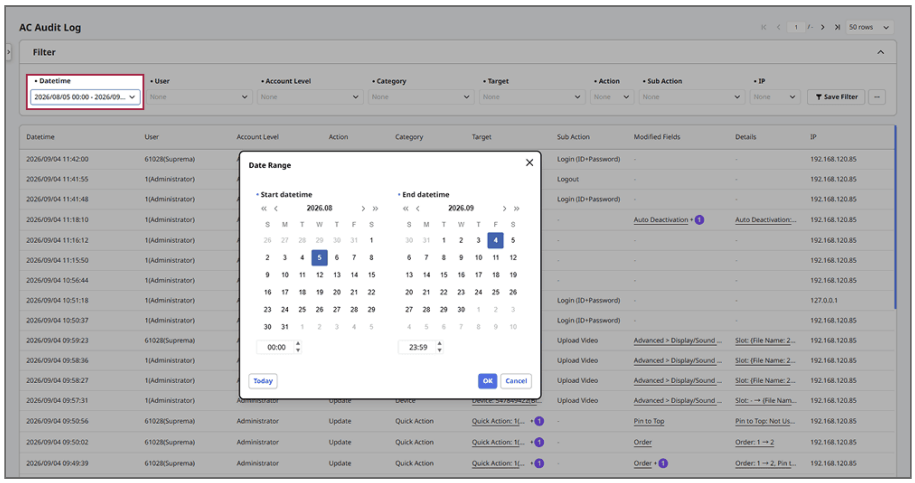
- Applied filters appear as the first filter and the number of additional filters. Click ✕ to disable only that filter. Filters with no selected value appear as **None**.



> **Info**
>
> Enter a search term to see results for the **User**, **Account Level**, **Target**, and **IP** filters. The search supports partial matches; enter part of a name or ID. The search includes deleted targets and marks them as **Deleted**.

Set the query period

Click **Datetime** to open the **Date Range** popup.

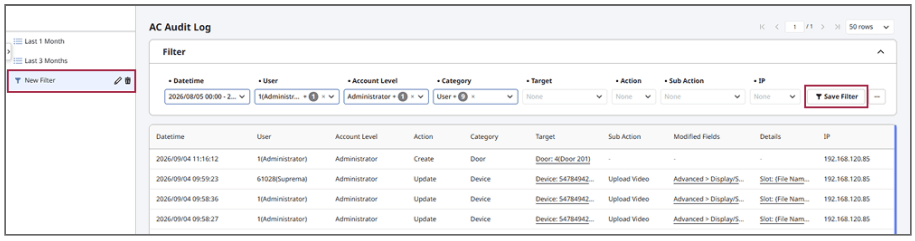


1. Set the date and time for **Start datetime** and **End datetime**. Click **Today** to jump to today.
2. Click **OK** to apply the query period.

Save filter

Save frequently used search conditions in **Saved Filters**, then load them when needed.

1. Set filters to match the required conditions.
2. Click **Save Filter** in the **Filter** section.
3. The system adds **New Filter** to the filter list on the left.



- Click ✎, enter a new name, then press Enter to rename the filter.

- Click to delete the filter.

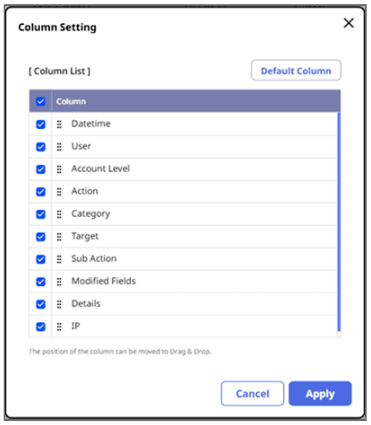
> **Info**
> You can save up to 20 filters. The browser stores saved filters, so they do not appear on other PCs or browsers.

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.
- : Go to the next page.
- : Go to the last page.
- 50 rows : Select the number of rows per page.

Set columns



Change column positions or hide columns in the audit log table. On the right side of the **Filter** section, click → **Column Setting**.

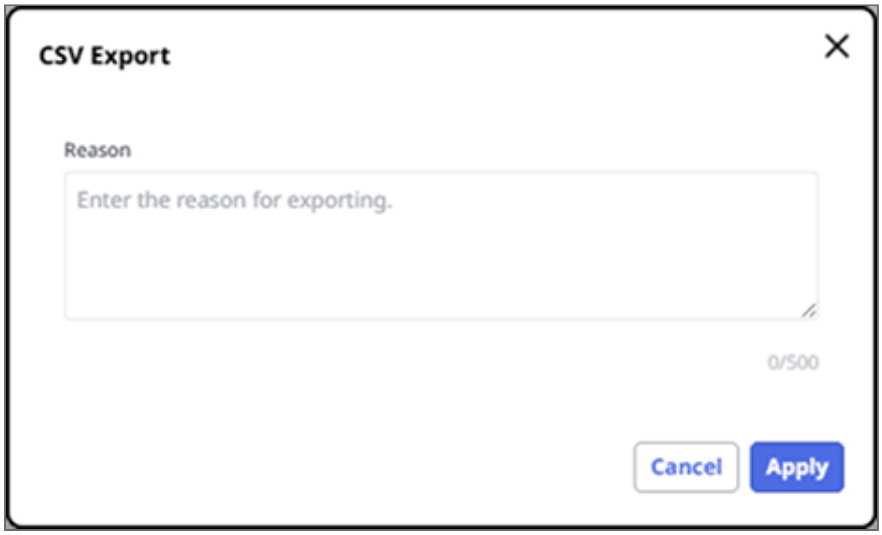
- In **[Column List]**, clear the checkbox for the column to hide.
- Drag a column to change the column order.
- Click **Default Column** to initialize column settings.

Click **Apply** to save the settings.

Export to CSV

Export audit logs 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.
3. When the **CSV Export** window appears, enter **Export Reason** (optional), and click **Apply**.



The exported CSV includes 10 columns, one row per record, and quotes all values. Values with multiple targets use a vertical bar (|) (e.g., **User: 7(Kim)|User: 8(Lee)**). The **Details** value includes all targets and fields without truncation.

> **Caution**
> The CSV file includes values as-is, including values a spreadsheet program may interpret as formulas. Do not open the downloaded CSV file directly in a spreadsheet program. If needed, open it with the text import feature.

> **Tip**
> If you set filters, the export includes only the filtered results in the CSV file.

Review BioStar 2 records

The same table also shows records from earlier versions (BioStar 2). BioStar 2 records appear as follows.

- **User** and **Target** are preserved in the original **name(id)** format (including space variations).
- **Modified Fields** always shows a hyphen (-).
- you can also search BioStar 2 records with the provided filters, and **User** and **Target** match both name and ID.

> **Info**
> Legacy records may include unsupported search criteria. When you load a saved filter, a notice appears if certain criteria are excluded.

Manage Audit Trail Retention Settings

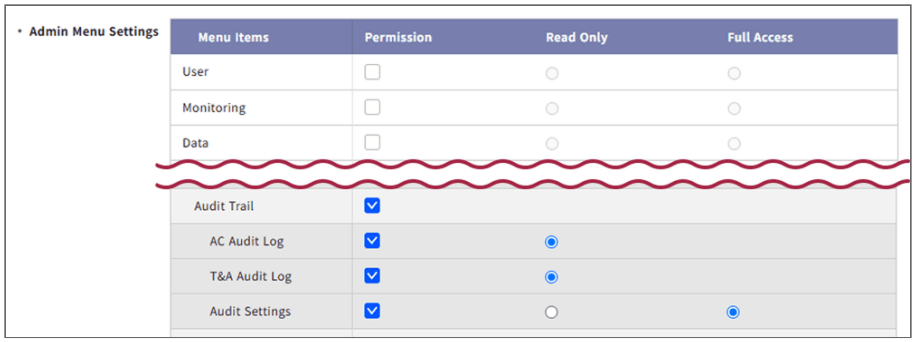
Audit logs accumulate over time, so manage the retention period to save storage space and protect privacy. In **Audit Settings**, set the retention period for **AC Audit Log** logs and whether to keep query history.

> **Info**
> A separate document covers the retention policy for Time and Attendance (T&A) audit logs.

Privilege information

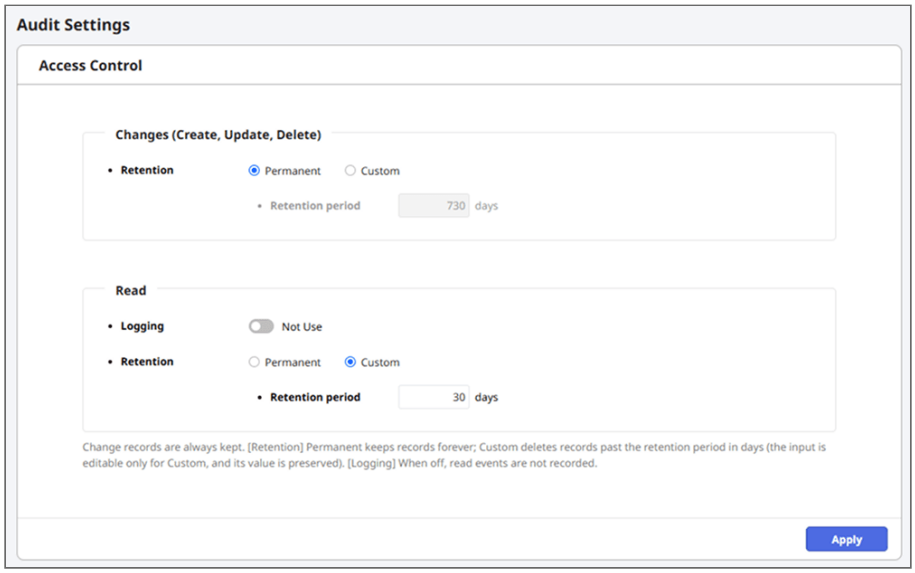
Administrator can always view and change settings in the **Audit Settings** menu. For a custom privilege administrator, in **Admin Menu Settings**, set **Audit Settings** to **Read Only** for view-only, or to **Full Access** for view and change.

> ***Settings*** → ***Account*** → ***Account*** → ***Add Custom Level***



Open audit settings

1. Click **Settings** on the **Launcher** page.
2. On the left sidebar, click **Audit Trail** → **Audit Settings**.



Retention policy settings

The **Access Control** section consists of the following two groups.

- **Changes (Create, Update, Delete)**: Creation, update, and deletion logs. Always recorded. Cannot turn logging on or off.
- **Read**: View logs. Set whether to record logs.

> **Info**
>
> - Enter **Retention period** as an integer between 1 and 2,147,483,647 days.
> - Check **AC Audit Log** for audit logs of setting changes in the **Access Control** section.

Change logs

Because the **Changes (Create, Update, Delete)** group is always recorded, select the **Retention** setting.

- **Permanent**: Keep logs permanently without automatic deletion.
- **Custom**: Select this option to limit the retention period for compliance or internal policy. When the **Retention period** field becomes active, enter the retention period in days.

View logs

In the **Read** group, set whether to keep view logs.

- **Logging**: Set to **Use** to keep view logs. If not needed, set it to **Not Use**.
- **Retention**: Select a retention method.
  - **Permanent**: Keep view logs permanently without automatic deletion.
  - **Custom**: Activates the **Retention period** field. Enter the retention period in days.

> **Info**
>
> When **Logging** is set to **Not Use**, the system does not record view events. After setting it to **Use**, the system cannot view earlier records.

Save Settings

After completing the **Changes (Create, Update, Delete)** and **Read** settings, click the **Apply** button at the bottom of the **Access Control** section. Save both group settings together.

How automatic deletion works

The server runs this job daily at 1 a.m. It deletes records past the retention period set in **Custom**, regardless of user actions. The job evaluates and deletes records at the same time. It runs only once a day.

> *For example, set **Read** records to 30 days in **Custom**. At 1 a.m., the job deletes records older than 30 days. Records just past the retention period remain until the next 1 AM job runs.*

When **Retention** is set to **Permanent**, the automatic deletion job does not run, and records are retained permanently.

System Settings

Explains settings for stable operation of the **BioStar X** system. Set up basic server information and HTTPS certificates, protect data with system backup and restore, and enhance security with password policies and encryption. Set basic settings such as daylight saving time, email notifications, language, and time zone.

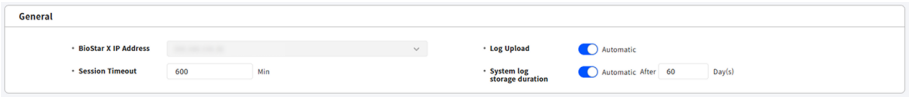
Server Detailed Settings

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 **System** → **Server** on 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.

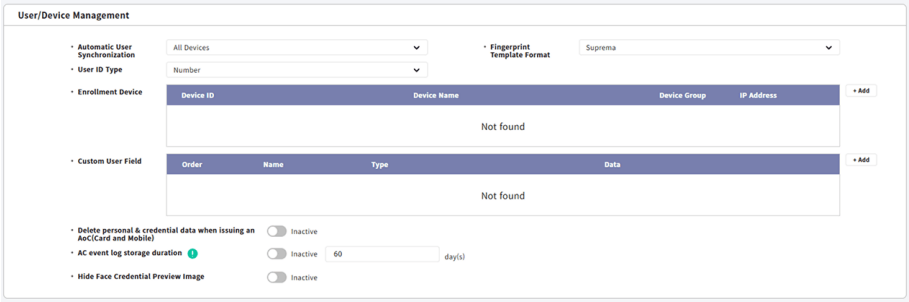


- **BioStar X IP Address**: You can check the server IP address.
- **Log Upload**: Select an event log upload method. If real-time communication with the server is difficult, set this to **Manual**.
- **System log storage duration**: The log retention period can be set from 1 to 120 days.
- **Session 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.

> **Info**
>
> If you set the **Log Upload** to **Automatic**, the event logs stored on the device upload automatically to the server when the connection between the server and device is lost and restored.

User and device management

In the **User/Device Management** section, you can set the synchronization and authentication methods between users and devices.



Automatic User Synchronization

In the **Automatic User Synchronization** option, you can choose how to synchronize user information between the server and devices. Synchronization includes access levels and access groups assigned to users. If you change access levels or access groups on the **BioStar X** server, the changes automatically apply to the related 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. Go to **Settings** → **Device** → **Device**, select each device, and click **Delete Data & Sync Device** to start synchronization. For more information on the **Delete Data & Sync Device** feature, see Use Device Management Feature.
- 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**

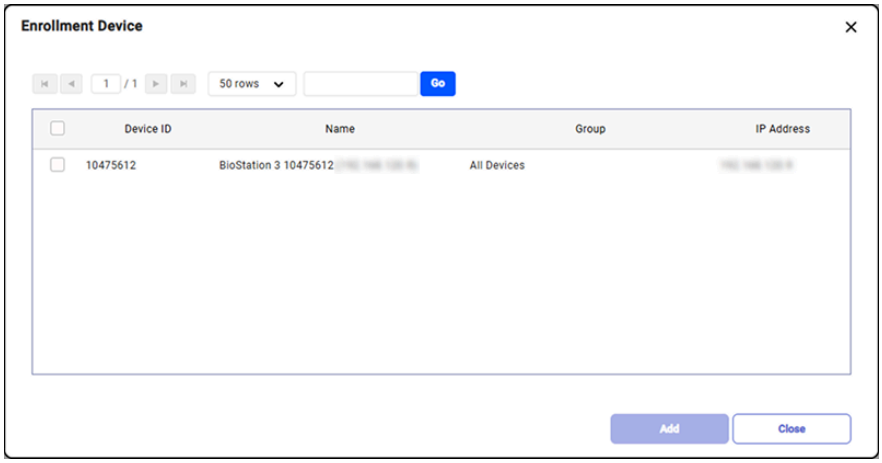
- BioStation 3 Max firmware 1.0.0 or later
- XPass Q2 firmware 1.0.0 or later
- BioStation 3 firmware 1.0.0 or higher
- X-Station 2 firmware 1.0.0 or higher
- XPass 2 firmware 1.0.0 or higher
- FaceLite firmware 1.0.0 or higher
- BioLite N2 firmware 1.0.0 or higher
- XPass D2 firmware version 1.0.0 or higher
- BioEntry R2 FW 1.0.0 or later
- BioEntry P2 firmware 1.0.0 or higher
- FaceStation 2 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
- CoreStation firmware version 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 **+ Add** to add a device.
2. When the **Enrollment Device** window appears, click the checkbox of the desired device from the list.



3. Click **Add** to add the selected device.

4. Click **Apply** at the bottom right of the screen to save the added device settings.

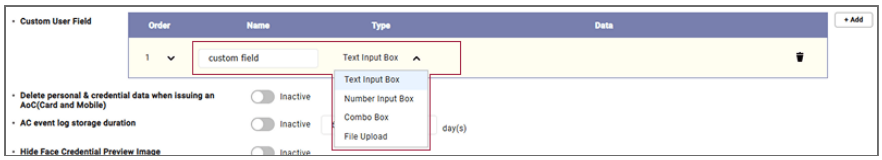
> **Info**
>
> - If you find it difficult to locate a registered device from the list due to the large number, enter keywords in the search input field to find devices. You can enter the device ID, device name, device group, and IP address.
> - For more information on enrolling fingerprints or face, card credentials, refer to the followings:
>   - Enroll Fingerprint
>   - Enroll Face
>   - Enroll Access Card
>   - Enroll Mobile Access Cards

Custom User Field

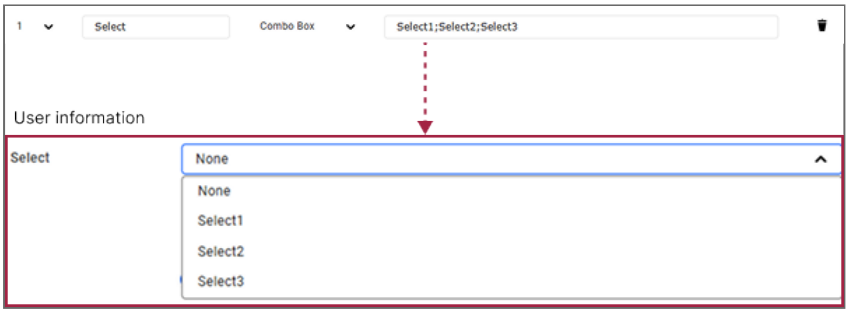
In the **Custom User Field** option, you can add fields to input additional information about the user. The added fields will be displayed on the user information screen.

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.



- **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)



- **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.
  – There are no restrictions on file extensions, and uploaded files are encrypted and stored in the database.

3. Click **Apply** 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 **Apply** at the bottom right of the screen.
- Click to delete a custom user field. Deleted fields cannot be recovered.
- For more information on registering and editing user information, see User.
- User information with added custom user fields can be printed on a card. For more information on adding custom user fields, see Card Printer.

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 that support NFC mobile cards**

- Mobile device OS: Android 7.0 or later
- BioStar X Mobile
- BioStation 3 Max
- XPass Q2
- XPass 2
- FaceLite
- BioLite N2
- XPass D2
- BioEntry R2
- BioEntry P2
- FaceStation 2
- BioEntry W2
- BioStation L2: BSL2-OM
- BioStation A2: BSA2-OMPW, BSA2-OIPW
- BioStation 2: BS2-OMPW, BS2-OIPW

▼ **View devices that support BLE mobile cards**

- Mobile device OS: Android 7.0 or later / iOS 13.0 or later
- BioStar X Mobile
- BioStation 3 Max
- XPass Q2
- XPass 2
- FaceLite: FL-DB
- BioLite N2
- XPass D2
- FaceStation 2: FS2-AWB

- **Mobile Access Card** and **Mobile Access** features cannot be used at the same time.

Other settings

- **AC event log storage duration**: Set the retention period for access control event logs.

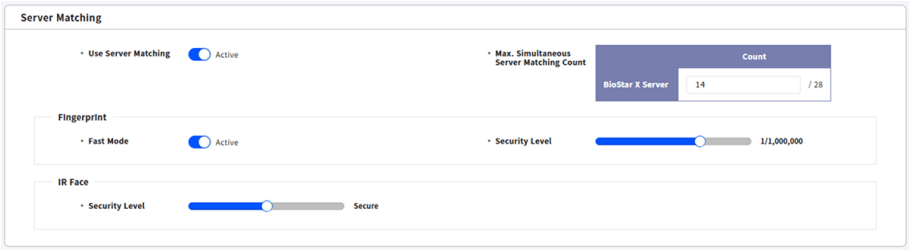
Info

The access control event log retention setting applies only to server logs. This setting does not apply to device event logs. Go to **Settings** → **Device** → **Device**, and delete device event logs individually.

- **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.



- **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.

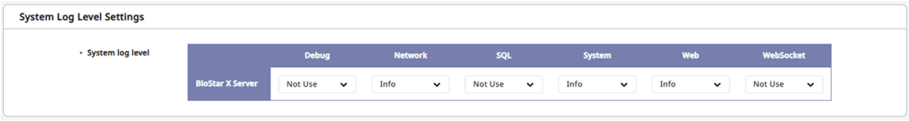
- **Fingerprint**
  - **Fast Mode**: You can configure the fingerprint matching speed.
  - **Security Level**: Configure the server matching security level for fingerprints. The higher the security level is set, the more the false rejection rate (FRR) can occur.
- **IR Face**
  - **Security Level**: Configure the server matching security level for IR faces. The higher the security level is set, the more the false rejection rate (FRR) can occur.

Info

The **Server Matching** feature is available as an additional option with an **Essential** or higher license. For more information on the licensing policy, see License Policy.

System log level settings

In the **System Log Level Settings** section, you can set the level of system logs stored in the database.



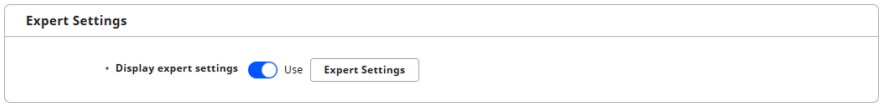
System logs are managed according to predefined categories, and the log levels are classified into **Trace**, **Debug**, **Info**, **Warning**, and **Error**. The high level contains all lower level logs. For example, if you select **Trace**, it will include and save all lower levels of **Debug**, **Info**, **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 enabling the **Display expert settings** option, save any changes in the **Server** menu first. Click **Apply** at the bottom right of the screen.

1. In the **Expert Settings** section, set the **Display expert settings** option to **Use**.



2. Click **Expert Settings**.
3. When you enter the **Expert Settings** screen, set the **Store Face Image** option.



   - **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.

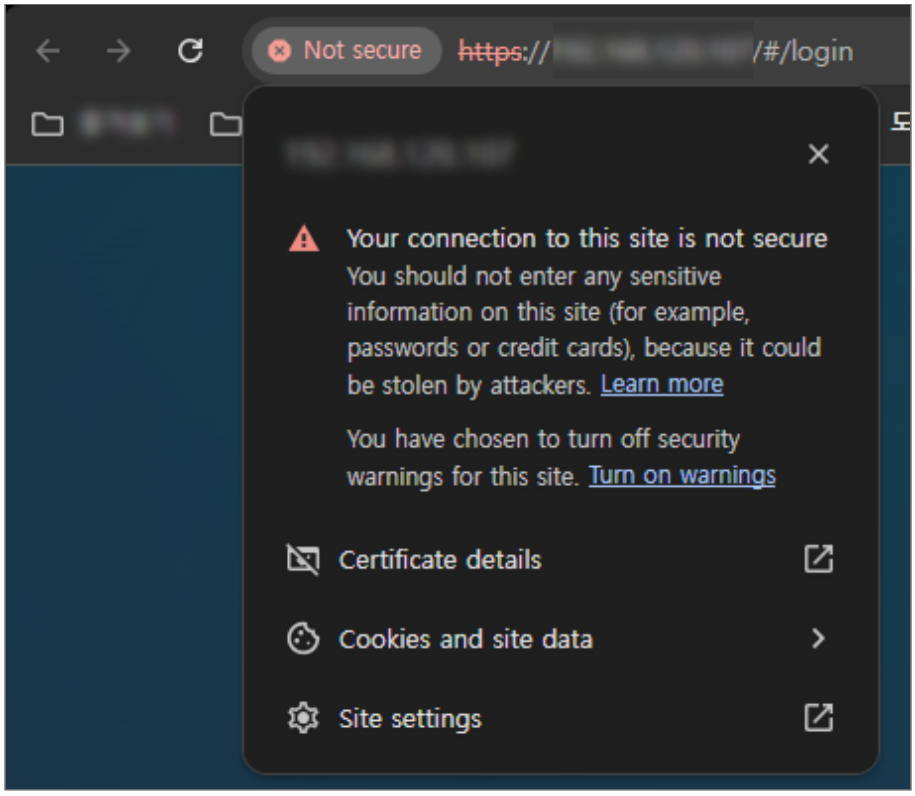
> **Caution**
>
> **Precautions when disabling the Store Face Image option**
>
> - If you disable this feature, all stored facial images will be deleted, and future enrolled facial images will only save the templates excluding the images.
> - This feature cannot be disabled if the enrolled facial images do not have both types of templates. For more information on the **Face Migration** feature, see Face Migration.
> - 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.

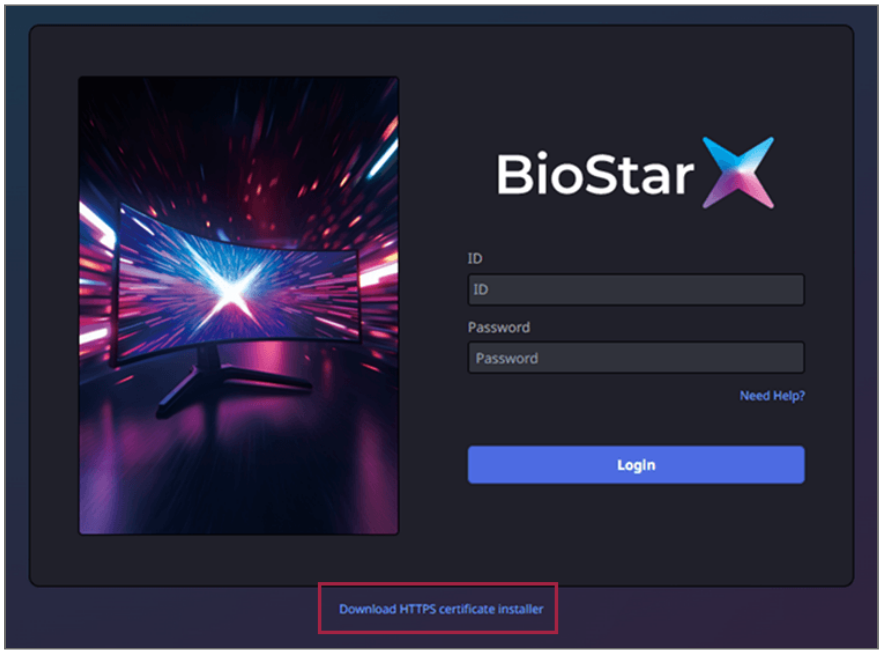


These warnings appear because the browser cannot verify the identity of the server. Installing the certificate will make the browser trust the **BioStar X** server, allowing for a secure HTTPS connection without security warnings.

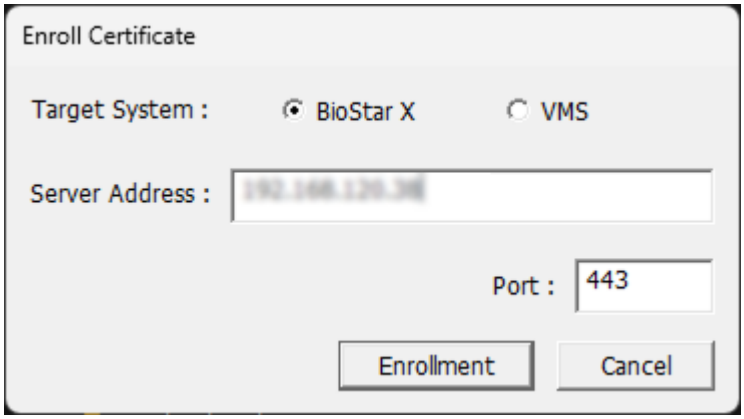
Certificate installation

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.



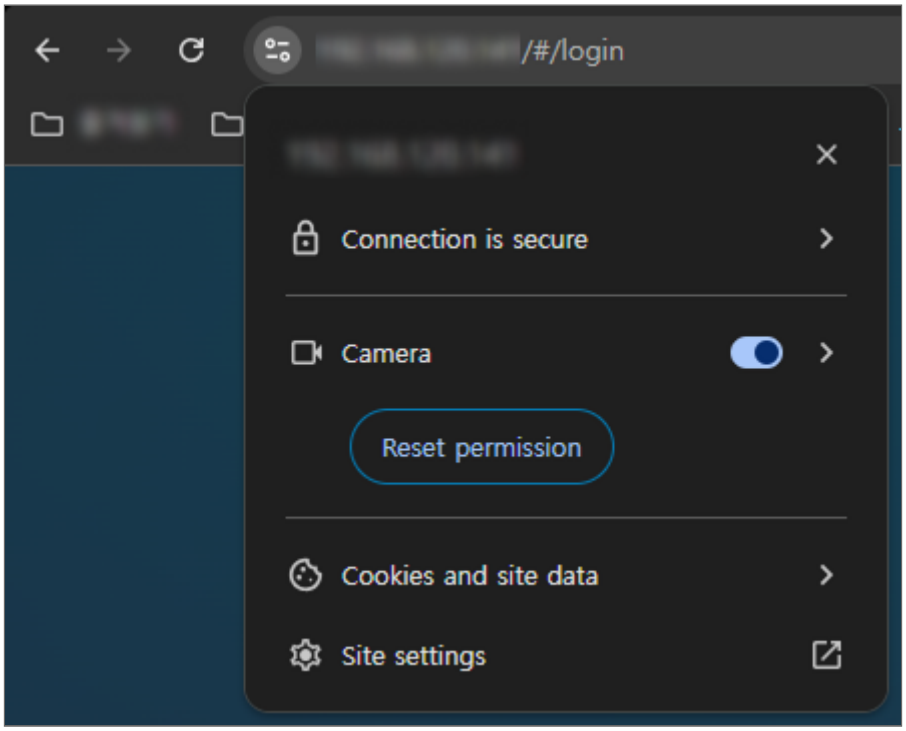
3. Save the *cert-register.zip* file locally.
4. Extract the downloaded file and run the *cert-register.exe* file. The **Enroll Certificate** program runs.
5. Select **BioStar X** for **Target System**, enter the IP address of the PC where **BioStar X** is installed in **Server Address**, and click **Enrollment**.



> 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**.

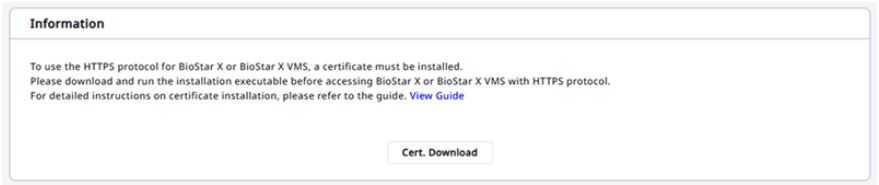
Restart the web browser and enter the registered IP address to navigate to the **BioStar X** page. When you click the icon to the left of the address bar, the message **This connection is secure** will appear.



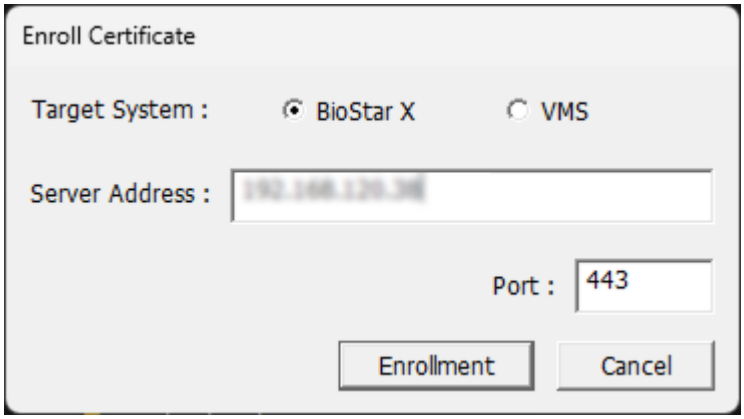
> **Info**
> The IP address entered in **Enroll Certificate** must be the same as the IP address set in **BioStar X**. You can check it in the menu path **Settings** → **System** → **Server** under **BioStar X IP Address**.

Certificate installation in server settings

1. Click **Settings** on the **Launcher** page.
2. Click **System** → **HTTPS** on the left sidebar.
3. Click **Cert. Download**.



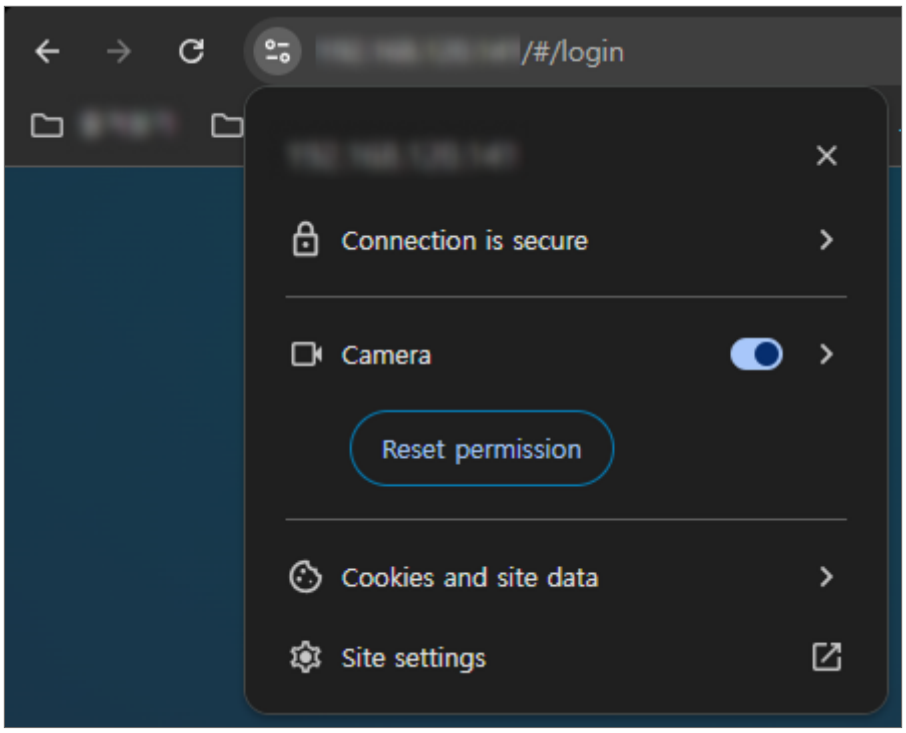
4. Save the *cert-register.zip* file locally.
5. Unzip the downloaded file and run **cert-register.exe** file. The **Enroll Certificate** program runs.
6. Select **BioStar X** for **Target System**, enter the IP address of the PC where **BioStar X** is installed in **Server Address**, and click **Enrollment**.



> 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.



Certificate installation for the VMS server

If the following situations occur, you can install the certificate from the VMS server onto the client PC to resolve the issue.

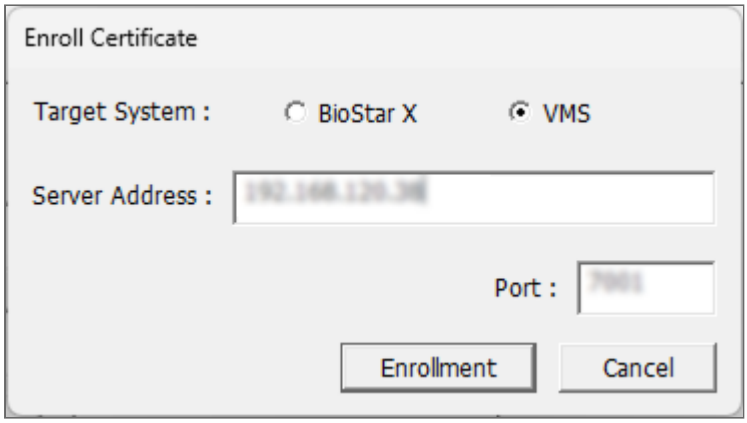
- When accessing **Video Management System** (VMS) through the browser, and a 'Not secure' warning appears
- When real-time video plays on the **Monitoring** page but recorded video does not play
- When installing the VMS server and **BioStar X** on the same server

Info

- For more information on installing the certificate on the VMS server, see Integrate VMS.
- The function to integrate with the VMS server must be purchased separately in an additional options package. For more information on the licensing policy, see License Policy.

Install the certificate on the client PC

1. On a **BioStar X** client PC, download the HTTPS certificate installer (*cert-register.zip*) from the login screen or **Settings** → **System** → **HTTPS**.
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.



   - **Server Address**: IP address of the VMS server
   - **Port**: Port number of the VMS server
4. Click **Enrollment**.
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.

System Backup

You can back up key information such as the database of **BioStar X**, various settings, and keys. Backup files also include user-defined settings, such as the encryption key (enc key) and the image log path. 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.

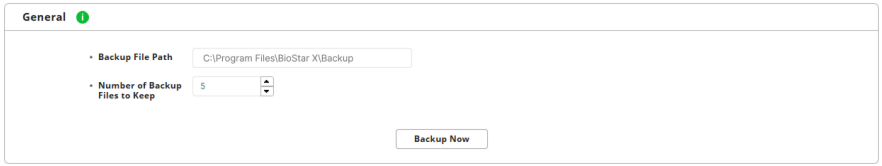
Info

- 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, see System Restore.

Manual backup

Users can create backup files manually.

1. Click **Settings** on the **Launcher** page.
2. Click **System** → **System Backup** on the left sidebar.
3. In the **General** section, set the path to save the backup file and the maximum number of backup files.



   - **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 **Backup Now**.
5. If a warning message appears, review it and click **Continue**.

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.

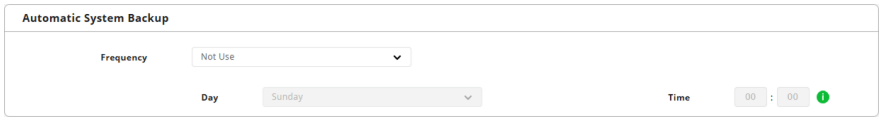
Info

- 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.
3. In the **Automatic System Backup** section, select the **Frequency** option.



- **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.

After you enable automatic backup, backups will run at regular intervals. If an automatic backup fails, the failure will be recorded in the event log and audit trail; detailed information about the cause is available in the log files.

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 time zone settings, see Configure Preferences.

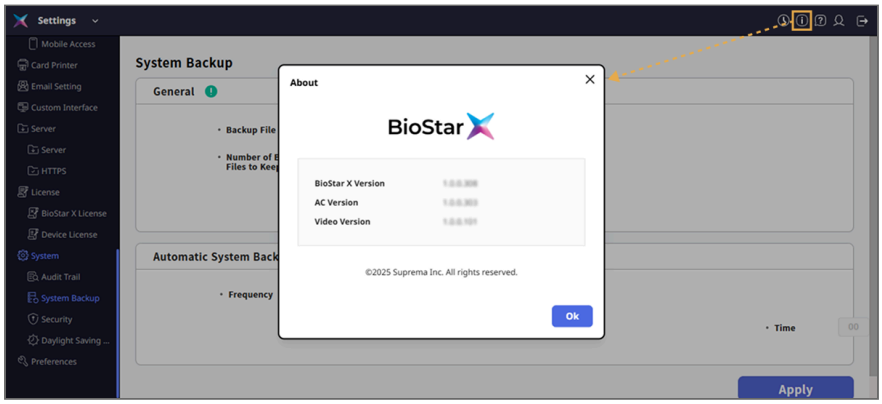
System Restore

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. Using the Restore feature, you can restore the database, settings, and license information to their state at the time of the backup.

Before you start

Before starting the system restore, check the following.

- 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 ⓘ at the top right of the screen.



- 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.

- If the SQL Server database and **BioStar X** are installed on different servers, you cannot use **BioStar X** system backup and restore.
- If the restore target server's IP address differs from the backup server's:
  - **BioStar X v1.0.2 or later**: During a restore, BioStar X detects the restore target's IP address and automatically reissues the certificate based on the new IP address. After the certificate is reissued, services that use the certificate automatically reconnect, so no additional action is required.
  - **BioStar X v1.0.1 or earlier**: The restore may fail. Verify the server IP address before proceeding with the restore.
- Even if the encryption key or image log path has changed, the restore follows the current setting paths of the target **BioStar X**. If no custom path is specified, the restore will use the default path on the target **BioStar X**.
- When you perform a restore, the current data is automatically backed up. If the restore fails, you can revert to the state prior to the restore.

> **Info**
> For more information on creating a system backup, see System Backup.

System Restore

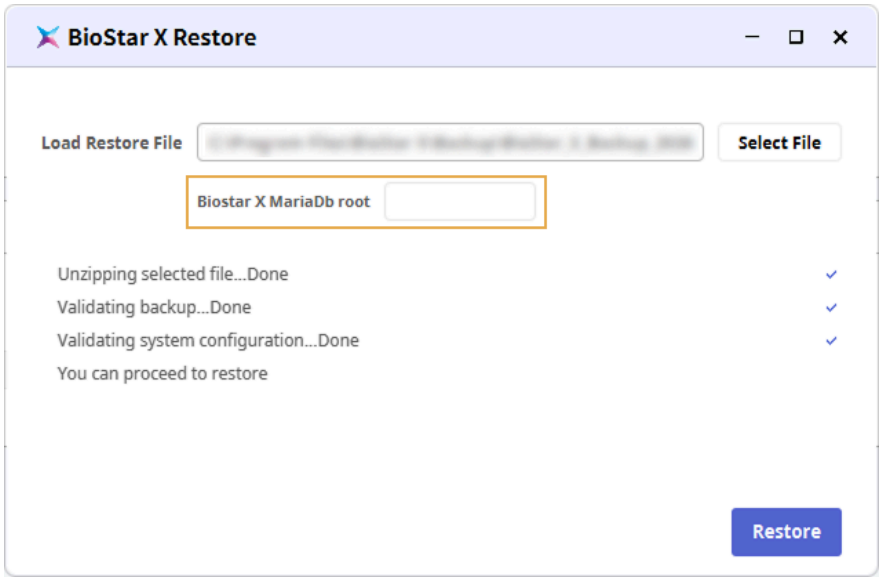
1. In Windows, run Start → **BioStar X** → **BioStar X Restore**.

   Program path: C:\Program Files\BioStar X\biostar-restore.exe

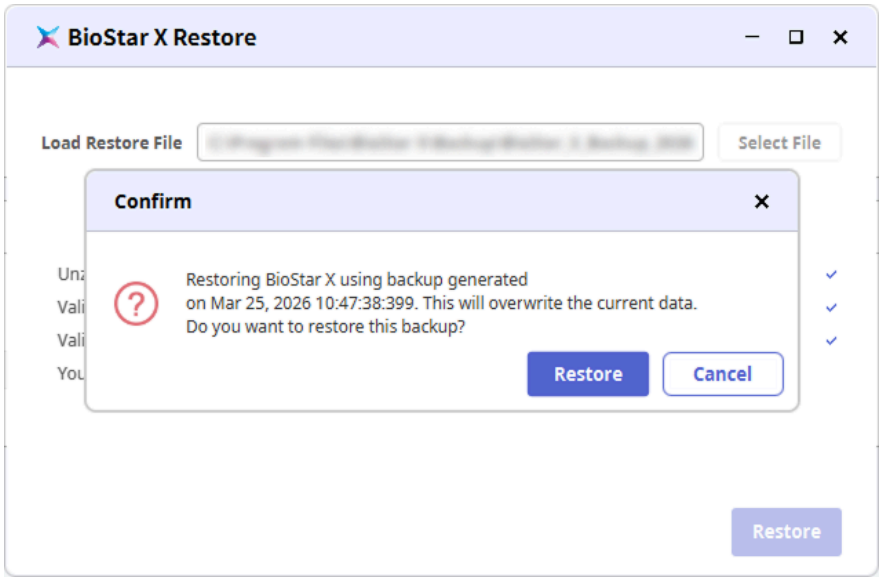
2. Click **Select File** and choose the backup file to restore.



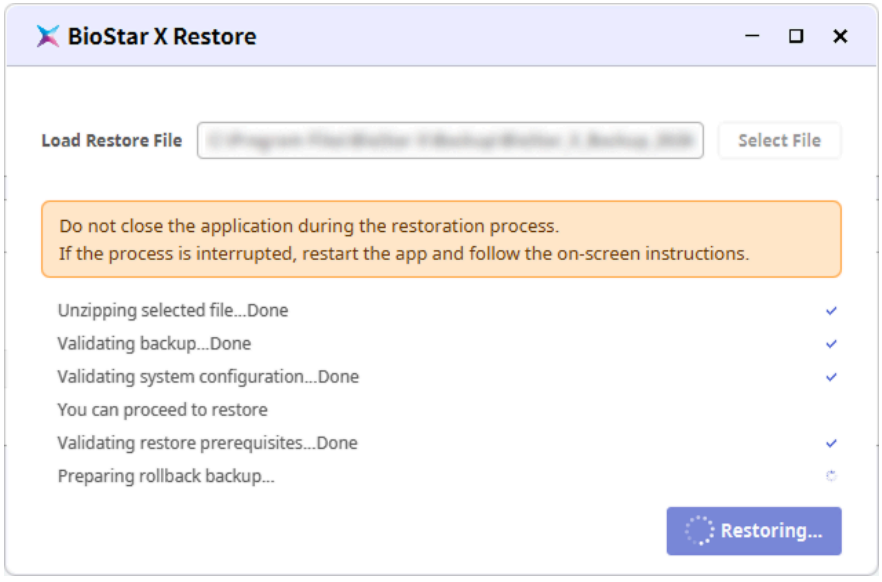
3. To start the restoration, click **Restore**.
4. Validate the backup file.
5. When the **You can proceed to restore** message appears, enter the database password and click **Restore**.



6. Click **Restore** to confirm and continue the restore.

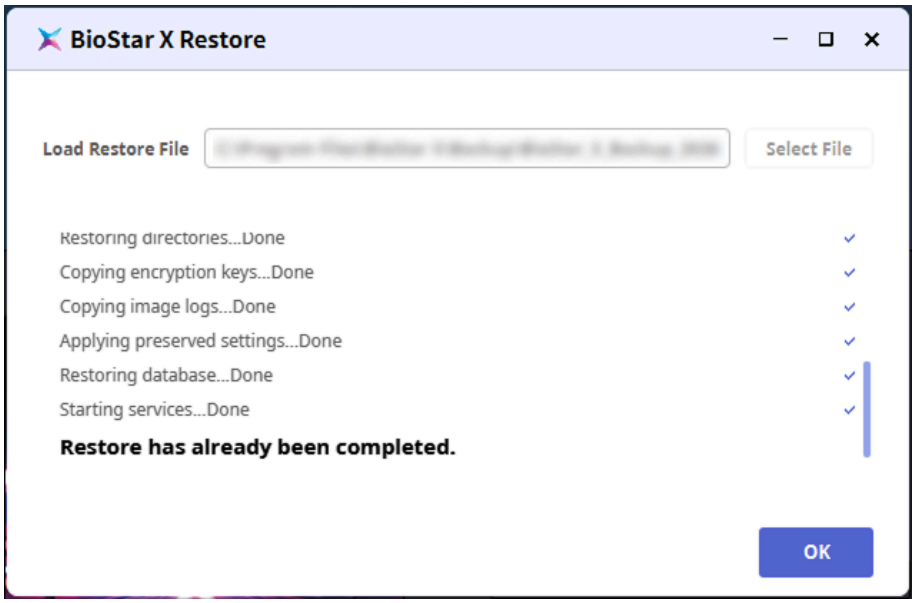


7. A message appears showing restore progress. Wait for the restore to complete.



If the **Restore has already been completed** message appears, the restore is complete. Access **BioStar X** to verify the

restored data.



Info

- If the PC shuts down unexpectedly during the restore, run **BioStar X Restore** again to retry the restore.
- If the restore server IP differs from the backup server IP while using a Multi Communications Server, reissue the certificate. For more information on how to reissue the certificate for the Multi Communications Server, see Change the Main Server IP Address.

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.

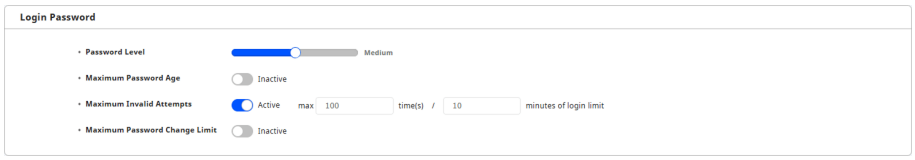
Use system security

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, see Set password policy.
   - **Advanced Security Settings**: Enhance communication security between personal information and devices. For more information, see Advanced security settings.
   - **Session Security**: Enhance session security. For more information, see Concurrent access control.
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.



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.



> **Info**
> The **Advanced Security Settings** section activates only when you log in with the initial administrator account.

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 **Change** 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.
- After upgrading to version 1.0.3, the system encrypts new audit logs regardless of the **Encrypt Personal Data on Database** option.

Set secure communication between devices

Protect communication between the **BioStar X** server and access control devices with certificates to enhance security. A newly installed **BioStar X** system sets the **Secure communication with device** option to **Use** by default, so no additional activation steps are required. When you upgrade an existing system, it keeps previous settings, reuses the security certificate, and reconnects registered devices.

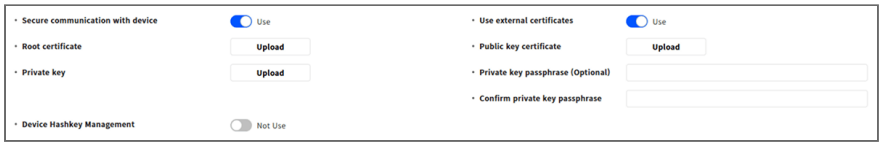
- **Secure communication with device**: Protect communication between the **BioStar X** server and access control devices with certificates. When this option is set to **Use**, the server automatically generates a certificate, sends it to devices, and encrypts all communication thereafter. Devices use this certificate to establish a secure channel when exchanging data with the **BioStar X** server.

  To use an external certificate, set the **Use external certificates** option to **Use**, and register the following.

  – Upload the **Root certificate**, **Public key certificate**, and **Private key** files separately.

  – If a passphrase is set for the private key, enter the same value in **Private key passphrase (Optional)** and **Confirm private key passphrase**. (Optional)

To restore the security certificate backed up during server removal, copy it directly to the **BioStar X** installation path. For instructions on backing up and restoring security certificates, see Uninstall BioStar X Server and Restore Security Certificates.



- **Device Hashkey Management**: Manually manage the hash key applied to devices. Set this option to **Use** to check and change the **Device Hashkey** value. Click **Change** and set a new hash key value.

Caution

Before enabling the **Device Hashkey Management** option, check the following.

- When enabled, the device is set to delete user data, logs, and encryption key values together when a tamper (Tamper) event occurs to enhance security, so use caution.
- If a user other than the Administrator Role account has a password or PIN, the system cannot apply the hash key. Delete the login password or PIN, then try again. The system encrypts passwords and PINs in a non-decryptable way to meet security requirements.
- Changing the device hash key deletes the master administrator PIN information stored on the device. Use extra caution because deleting credentials may prevent access to the Device Manager menu.
- **Encrypt Personal Data on Database** and **Device Hashkey Management** settings cannot be enabled at the same time. Disable one of the two options, then set the other.

Info

- **BioStar X** keeps the server-generated default certificate after setting **Secure communication with device** to **Not Use**. Changing the option back to **Use** reuses the existing certificate. It creates a new one only if none exists. Changing **Use** → **Not Use** → **Use** keeps the same certificate. Previously added devices reconnect without extra steps. Switching to **Not Use** while using an external certificate deletes the external certificate (root certificate, public key certificate, private key) from the server. It also deletes the private key password from the server.
- Change **Secure communication with device** and **Use external certificates** only when all added devices and the multi-communication server are connected to the server. If any device disconnects or the multi-communication server is not connected, the system rejects the change and shows an error message. Reconnect the device or the multi-communication server, then try again. If you no longer use the device, delete it from the device list, then try again.
- If a previously connected device fails to connect due to a certificate mismatch, **BioStar X** records it in the system log. If the device suddenly fails to connect, check the system log. Then initialize the device or re-enroll the exported certificate set with **Use external certificates**. If you remove and reinstall the server, see Uninstall BioStar X Server and Restore Security Certificates.
- For instructions on backing up certificates when removing a server, see Uninstall BioStar X Server and Restore Security Certificates.

▼ **View supported devices and firmware versions for Secure communication with device feature**

- BioStation 3 Max firmware 1.0.0 or later
- XPass Q2 firmware 1.0.0 or later
- BioStation 3 firmware 1.0.0 or higher
- BioStation 2a Firmware 1.0.0 or higher
- X-Station 2 firmware 1.0.0 or higher
- XPass 2 firmware 1.0.0 or higher
- FaceLite firmware 1.0.0 or higher
- BioLite N2 firmware 1.0.0 or higher
- BioEntry P2 FW 1.1.0 or later
- FaceStation 2 FW 1.1.0 or later
- BioEntry W2 FW 1.2.0 or later
- BioStation L2 FW 1.3.0 or later
- BioStation A2 FW 1.5.0 or later
- BioStation 2 FW 1.6.0 or later
- CoreStation FW 1.1.0 or later

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.



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.

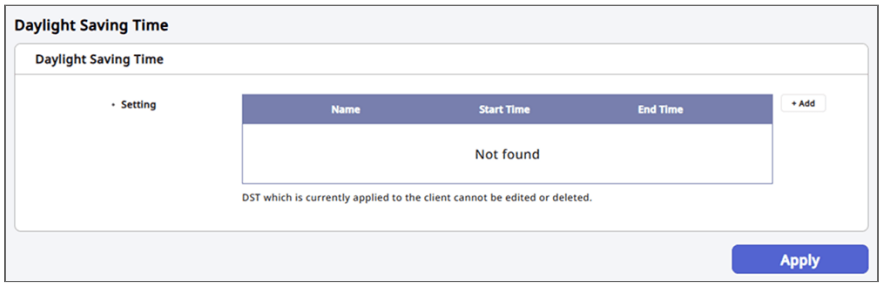
Info

Set Daylight Saving Time in the following cases.

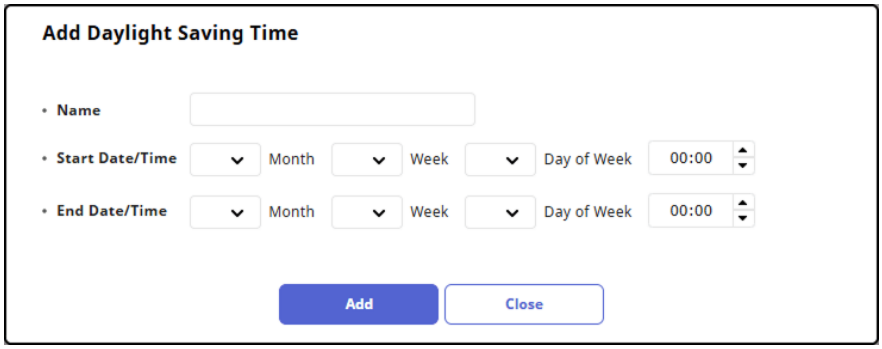
- If you operate the system in countries or regions that adopt Daylight Saving Time
- If you need to record accurate access times integrated with attendance management systems
- If you manage a consolidated security system operating across multiple time zones

Add daylight saving time

1. Click **Settings** on the **Launcher** page.
2. Click **System** → **Daylight Saving Time** on the left sidebar.
3. Click **+ Add**.



4. Set each item and click **Add**.



5. Click **Apply** at the bottom right of the screen to save the added settings.

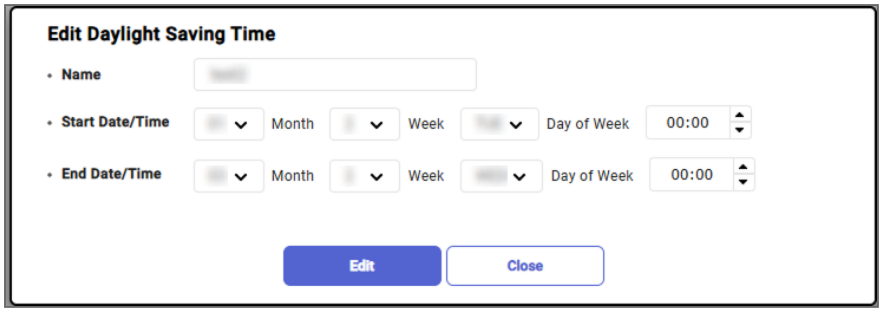
Info

- The current Daylight Saving Time settings cannot be modified or deleted. You can check the current Daylight Saving Time settings in the **Settings** → **System** → **Preferences** menu.
- For more information on applying the newly added Daylight Saving Time settings to the system, see Configure Preferences.

Edit daylight saving time

> **Info**
> The currently used settings cannot be modified. To modify, first uncheck the selection in the **Language / Time Zone** section from the **Settings** → **System** → **Preferences** menu.

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.



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, see Configure Preferences.

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.

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.

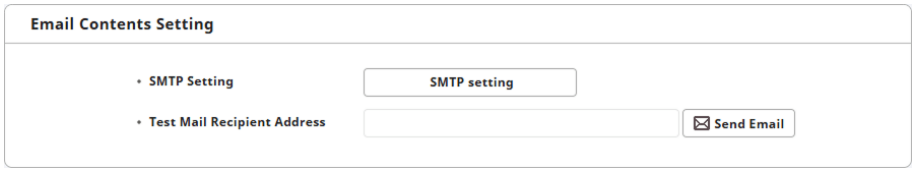
Info

- 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 on user details, see Enter Basic User Information.
- The devices that can perform **facial authentication** are as follows.
  - FaceStation F2, BioStation 3, BioEntry W3, BioStation 3 Max
- The devices that can use **QR/Barcode authentication through scanner** are as follows.
  - X-Station 2 (XS2-QDPB, XS2-QAPB)
- The devices that can use **QR/Barcode authentication through camera** are as follows.
  - BioStation 3 Max firmware 1.0.0 or later
  - BioStation 3 firmware version 1.1.0 or later
  - X-Station 2 (XS2-ODPB, XS2-OAPB, XS2-DPB, XS2-APB) firmware version 1.2.0 or higher
  - X-Station 2 (XS2-QDPB, XS2-QAPB) firmware version 1.4.1 or higher
- Using **Use QR/Barcode through Camera** requires a separate device license. For more information on device licenses, see Device License.

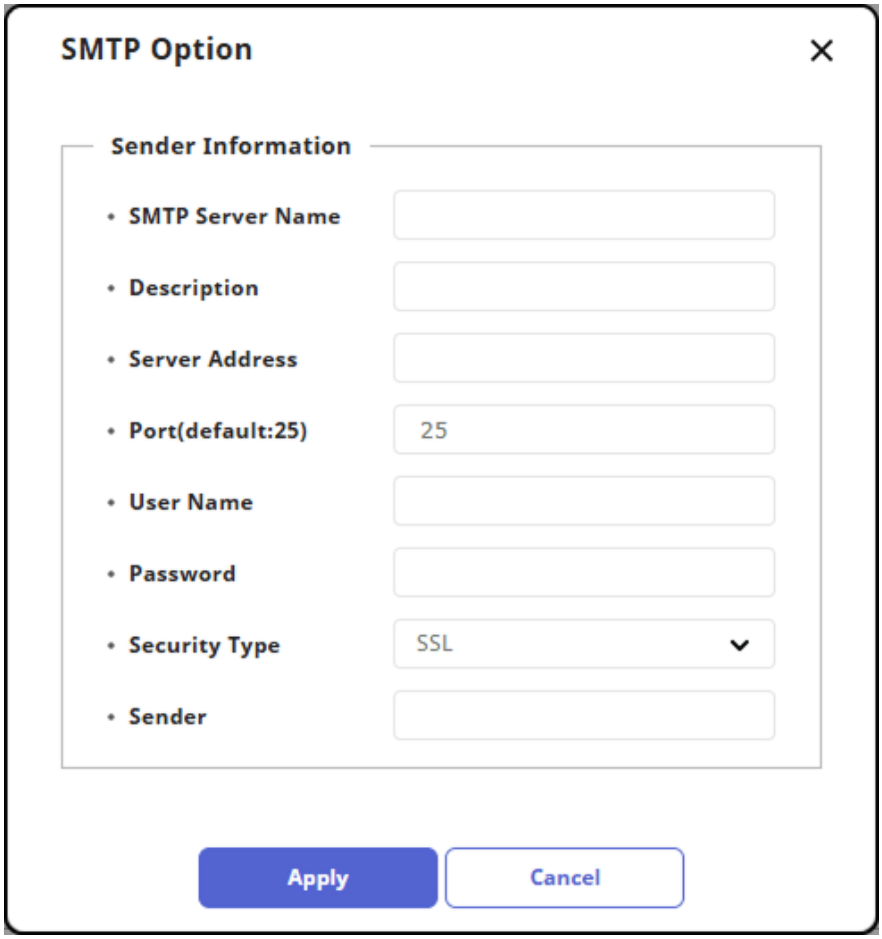
1. Click **Settings** on the **Launcher** page.
2. Click **System** → **Email Settings** on the left sidebar.
3. Edit the necessary fields.
4. Click **Apply** to save the settings.

Set up email content

Enter the SMTP server information for sending emails.



- **SMTP Setting**: Set the SMTP(Simple Mail Transfer Protocol) for sending emails. Click **SMTP setting** to open the **SMTP Setting** settings window.



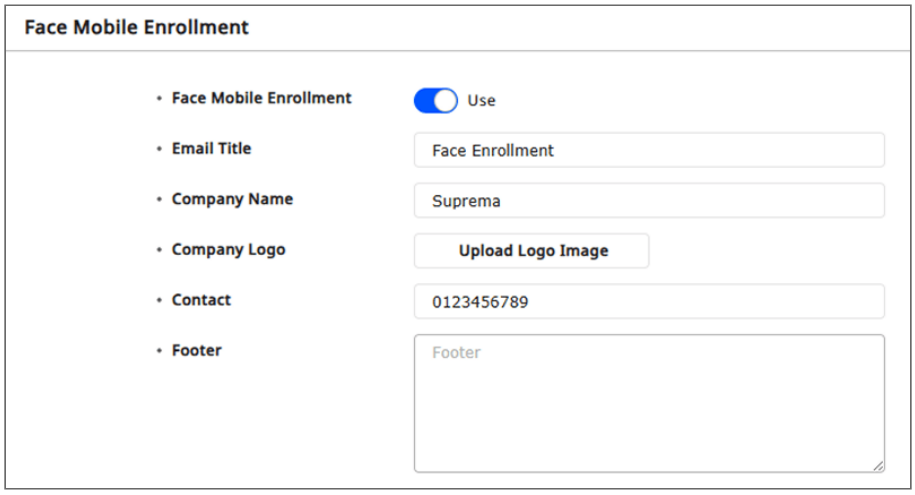
- **SMTP Server Name**: Enter the SMTP server name.
- **Description**: Enter the description.
- **Server Address**: Enter the SMTP server address. The SMTP server address is in the format `smtp.{email-service-provider}.com`, and you can confirm it on the settings screen of the email used as the SMTP server.
- **Port(default:25)**: Enter the port number of the SMTP server. You can find this on the email settings screen of your SMTP service provider.
- **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.

- **Test Mail Recipient Address**: 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.



- **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.

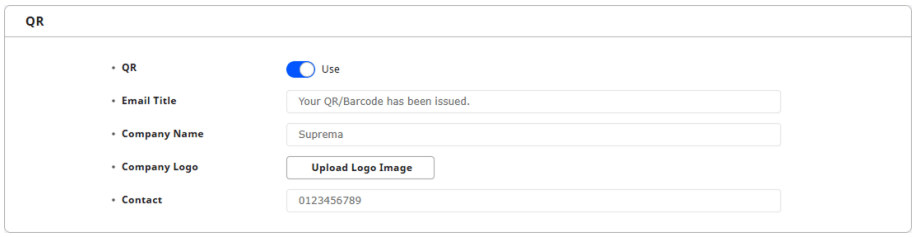
> **Info**
>
> – Supported image file formats are GIF, JPG, JPEG, JPE, JFIF, PNG.
>
> – Supported image file size is up to 5MB.

- **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**.



- **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.

Configure Preferences

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 preferences

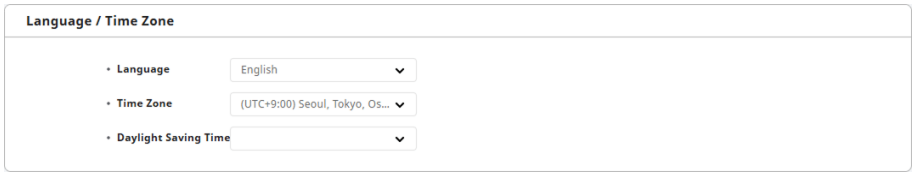
1. Click **Settings** on the **Launcher** page.
2. Click **System** → **Preferences** on the left sidebar.
3. Set desired options in each section.
   - **Language / Time Zone**: Interface language and time zone, daylight saving time
   - **Date/Time**: Date and time format

- **Sound**: Event notification sound

4. After completing all settings, click **Apply** at the bottom right of the screen.

Set language and time zone

You can set the interface language for **BioStar X**, the time zone, and daylight saving time rules.



- **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 item you want isn't available, see Daylight Saving Time for instructions on how 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 Format**: Changes the date format.
  - **mm/dd/yyyy**: 01/31/2025
  - **yyyy/mm/dd**: 2025/01/31
  - **dd/mm/yyyy**: 31/01/2025
- **Time Format**: Changes 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

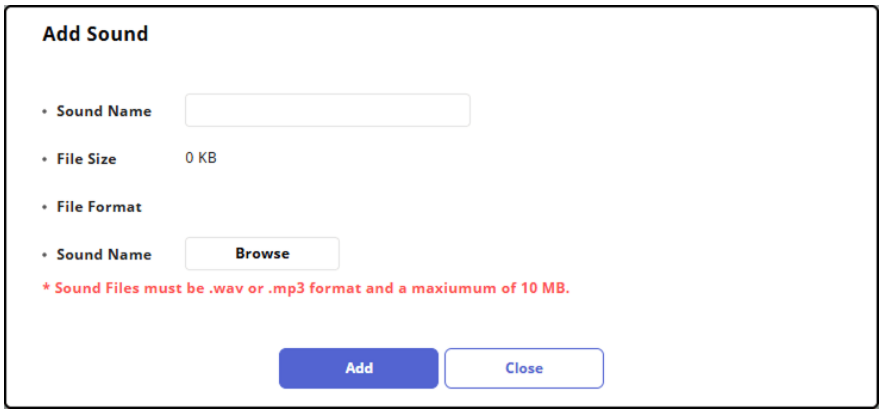
Click **Apply** at the bottom right of the screen to save the settings.

Set event notification sound

You can upload a sound file to be used when an event occurs.



1. Click **+ Add**.
2. When the **Add Sound** window appears, click **Browse**.



3. Select the *.wav* or *.mp3* file you want to upload and click **Open**.
4. Click **Add** 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.
- To learn how to apply the uploaded sound file when an event occurs, see Alert Settings.

Advanced Settings

Provides guidance on the advanced settings feature available with an **Essential** license when you purchase add-on options, or with an **Enterprise** license or higher.

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.

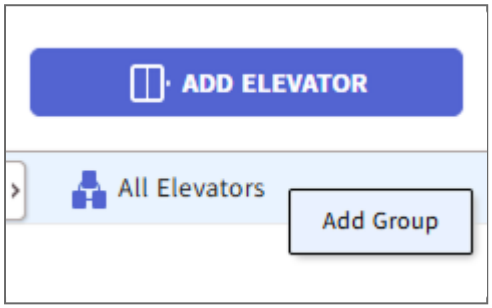
Manage Elevator Group

This guide describes how to set up groups to manage multiple elevators easily. Elevator groups allow for managing several elevators as one unit. If you set up a group, you can configure multiple elevators at once.

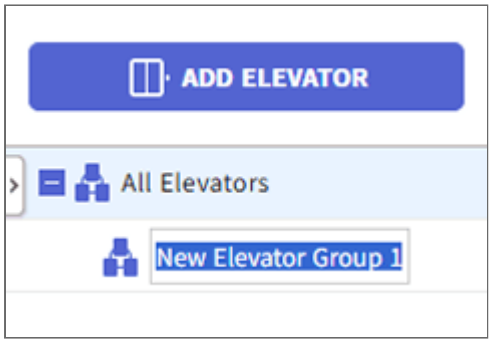
> **Tip**
> Registering the group name based on elevator location makes management convenient.

Add elevator group

1. Click **Settings** on the **Launcher** page.
2. Click **Access Point** → **Elevator** on the left sidebar.
3. Select **All Elevators** in the elevator list and right-click.



4. Click **Add Group** in the popup menu.
5. Enter your desired group name.

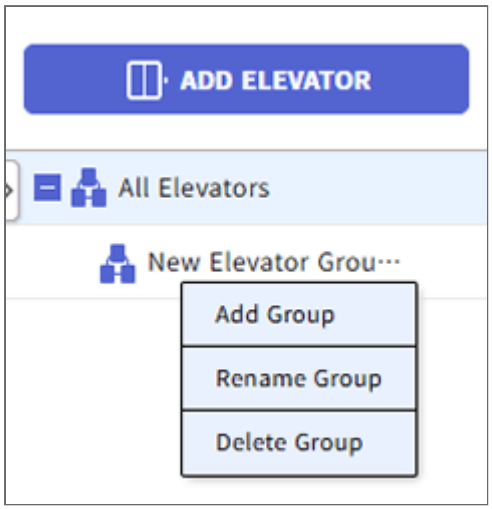


Info

- 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 **Access Point** → **Elevator** on 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.

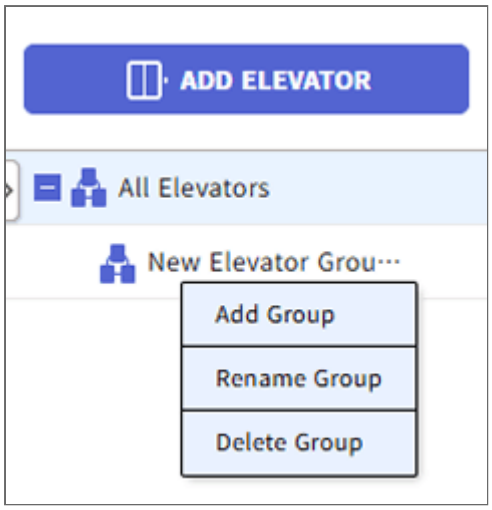
Info

The elevator group name can be up to 48 characters long.

Delete elevator group

1. Click **Settings** on the **Launcher** page.
2. Click **Access Point** → **Elevator** on the left sidebar.

3. Select the group you want to delete from the elevator list and right-click.



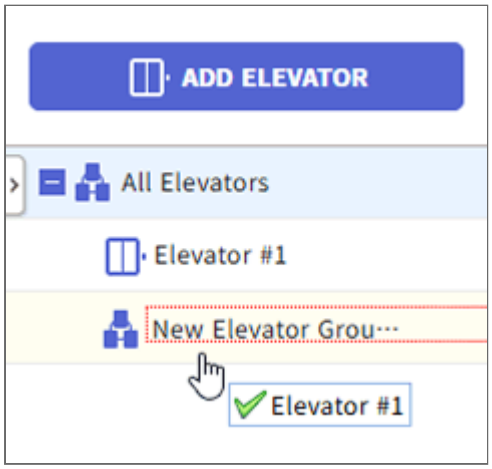
4. Click **Delete Group** in the popup menu.

> **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 **Access Point** → **Elevator** on 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 **Access Point** → **Elevator** on 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

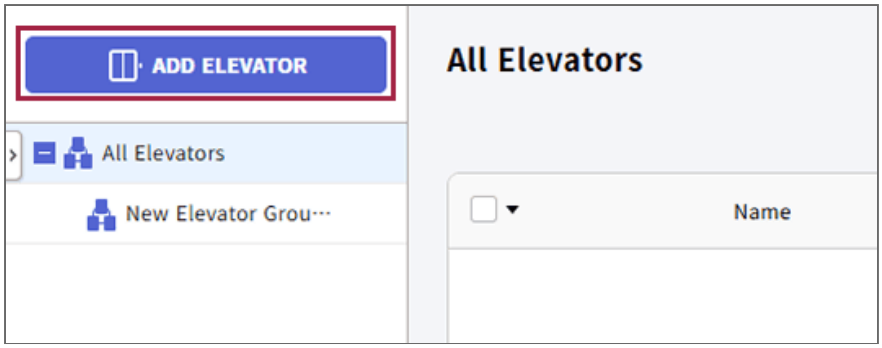
This document provides guidance on how to register and set up an elevator. The elevator is used for floor control and forms part of the access control system along with the entrance door. Registering the elevator allows control over access permissions for specific floors.

Before you start

- Set the access level, access group, and floor level for access control before registering the elevator. For more information, see Access Control Settings.
- 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 **Access Point** → **Elevator** on the left sidebar.
3. Click **ADD ELEVATOR** in the upper left of the screen.



4. Once the **Add New Elevator** screen appears, set each section item in order.
   - **Information**: Set the basic information for the elevator. For more information, see Set basic information.
   - **Detail**: Set the detailed information for the elevator. For more information, see Set detailed information.
   - **Option**: Set additional options. For more information, see Set additional options.

- **Alarm**: You can set the alarm to trigger or block device usage when an anti-passback violation occurs. For more information, see Set alarms.

5. Once all configurations are complete, click **Apply** 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.

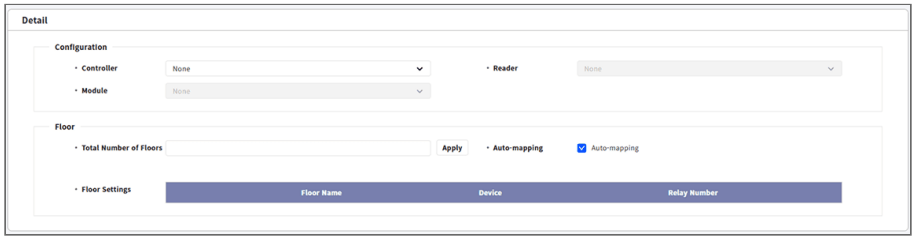


- **Name**: Enter the elevator's name. It is convenient to enter a name that specifies the elevator's location for easier management.
- **Group**: Select the elevator group.
- **Description**: Enter a brief description of the elevator.

> **Info**
>
> - The elevator name can be up to 48 characters long.
> - For more information on registering elevator groups, see Manage Elevator Group.

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** → **Access Management** → **Advanced AC** → **Occupancy Limit**

  For more information on the **Occupancy Limit** settings, see Advanced Access Control Settings.
- For more information on schedule settings, see Schedule Settings.

- **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. Click **+ Add** to add work conditions and actions.



- **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.

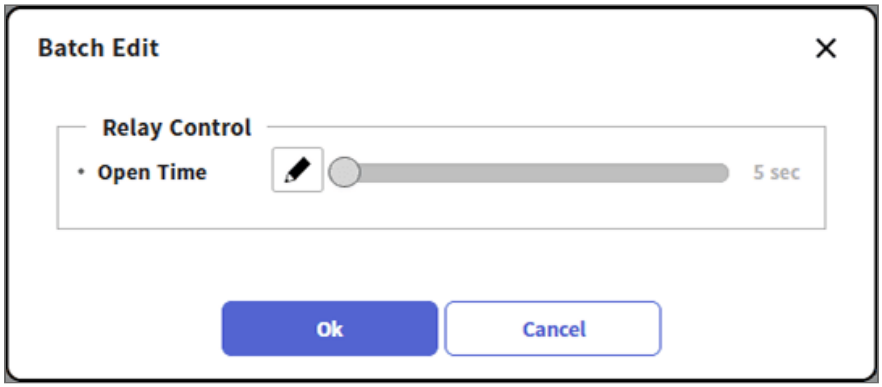
Edit information for one elevator

1. Click **Settings** on the **Launcher** page.
2. Click **Access Point** → **Elevator** on 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 **Apply** at the bottom of the screen.

> **Info**
> For more information on each section on the edit elevator information screen, see Register Elevator.

Batch edit multiple elevators

1. Click **Settings** on the **Launcher** page.
2. Click **Access Point** → **Elevator** on 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.
> - In batch editing, modify only the **Open Time** option.

Delete Elevator

This guide describes how to delete registered elevators.

1. Click **Settings** on the **Launcher** page.
2. Click **Access Point** → **Elevator** on the left sidebar.
3. Click the checkbox of the elevator you want to delete from the elevator list.
4. Click **Delete Elevator** at the top right of the screen.

The selected elevator will be deleted. Deleted elevators cannot be recovered.

> **Info**
>
> **Delete Elevator** activates only after selecting one or more elevators in 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

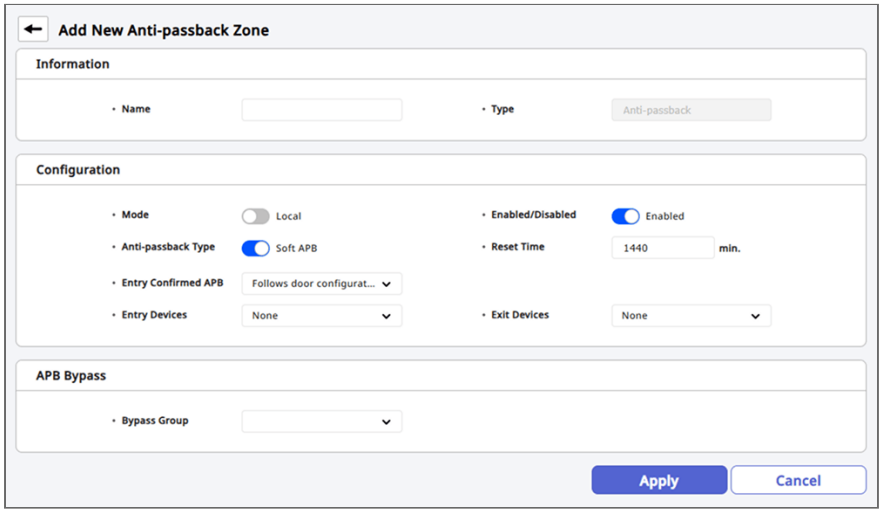
Anti-passback provides enhanced features compared to anti-passback generated based on doors or devices. Set up anti-passback to force users to use designated doors and devices upon entry and exit. This prevents unauthorized re-entry and enhances security.

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 **Access Management** → **Advanced AC** on 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.



6. Set the details of the anti-passback feature in the **Settings** section. For more information, see Setting options guide.
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.

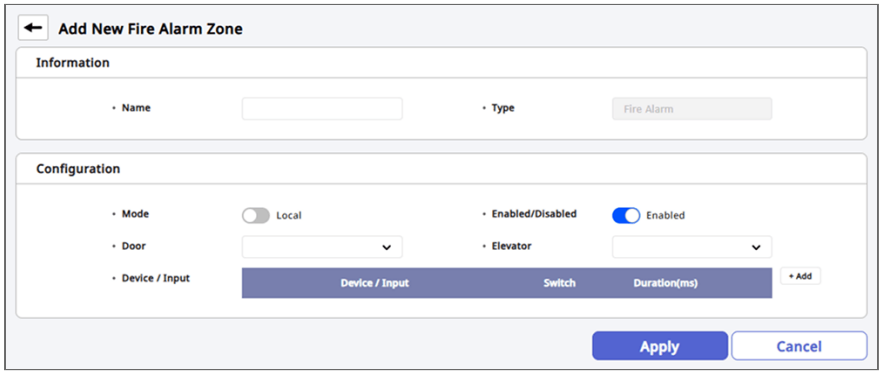
> **Info**
> For more information about device registration, refer to the following.
> - Register Device
> - Register Wiegand Credentials
> - Register Slave

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 **Access Management** → **Advanced AC** on 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.



6. Set the details of the fire alarm in the **Settings** section. For more information, see Setting options guide.
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.
- **Door**: Select the doors to designate for the fire alarm rule.
- **Elevator**: Select the elevator to designate the fire alarm rules.
- 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

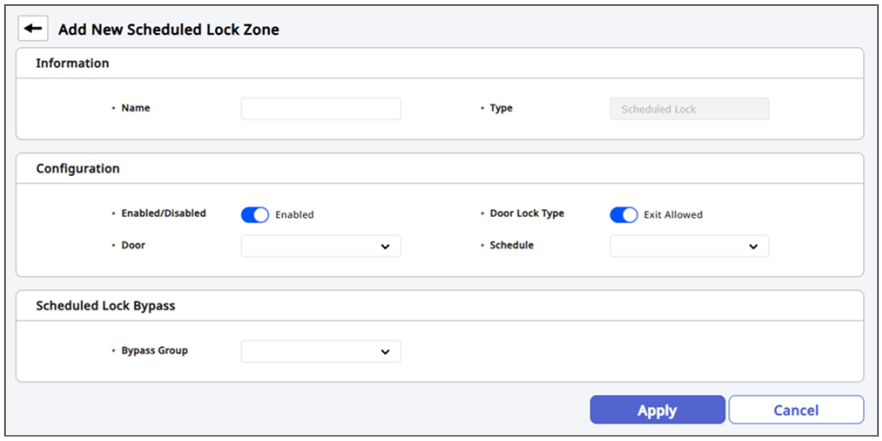
Guidance on how to set up schedule lock. Schedule lock provides the ability to lock doors at specific times. This feature enhances access control and is useful for restricting access during certain periods.

Info

Schedule lock settings only support **Local** mode.

Register scheduled lock

1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Advanced AC** on 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.



6. Set the details of the schedule lock feature in the **Settings** section. For more information, see Setting options guide.
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 on schedule settings, see Schedule Settings.

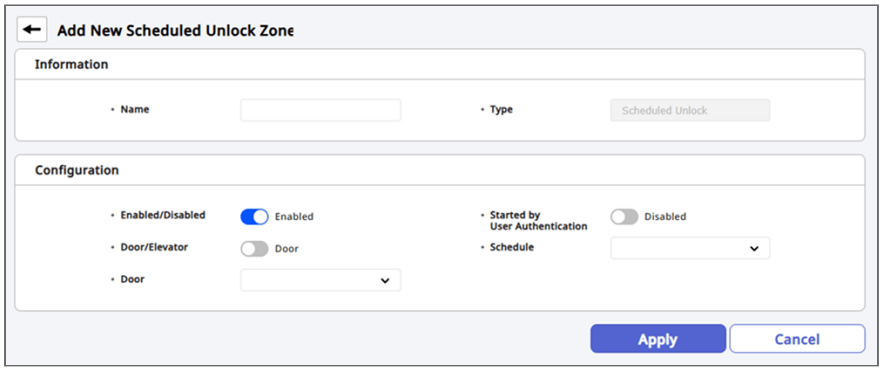
Scheduled Unlock

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 **Access Management** → **Advanced AC** on 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.



6. Set the details of the schedule unlock feature in the **Settings** section. For more information, see Setting options guide.
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 on registering an elevator, see Register Elevator.

- **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 on schedule settings, see Schedule Settings.

Intrusion Alarm

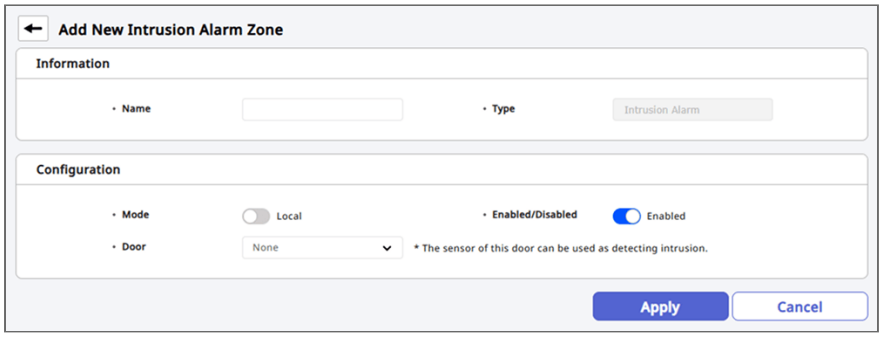
This guides you on how to set up security. The intrusion alarm settings provide capabilities to lock doors or trigger alarms

when intrusion is detected.

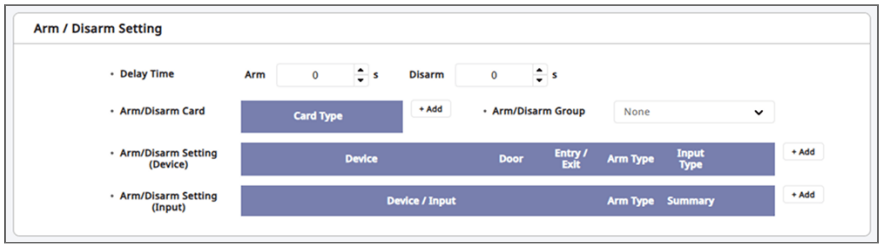
> **Info**
>
> **Intrusion Alarm Zone**: A zone set to emit a warning sound or relay signal if an unauthorized person attempts an intrusion after Arm. This zone normally begins monitoring after the day's work, and emits a preset alarm or signal when an intrusion attempt is detected.

Register intrusion alarm

1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Advanced AC** on 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.



6. Set the details of the intrusion alarm settings in the **Settings** section. For more information, see Setting options guide.
7. Add authentication settings for arming and disarming in the **Arm / Disarm Setting** section. For more information, see Arming or disarming settings.



> 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, see Intrusion detection settings.



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.

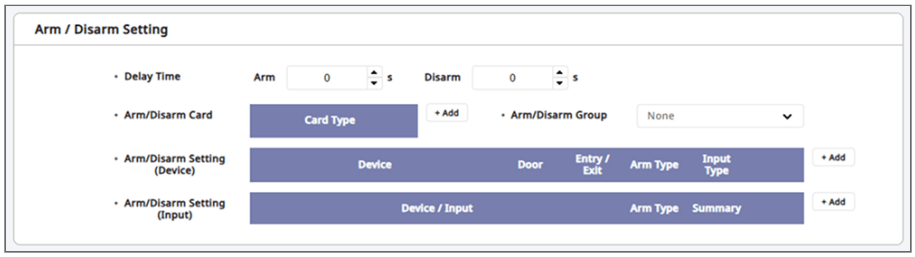
Setting options guide

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.
- **Door**: Select the door to apply the intrusion alarm feature.

Arming or disarming settings

You can add authentication settings for arming and disarming.

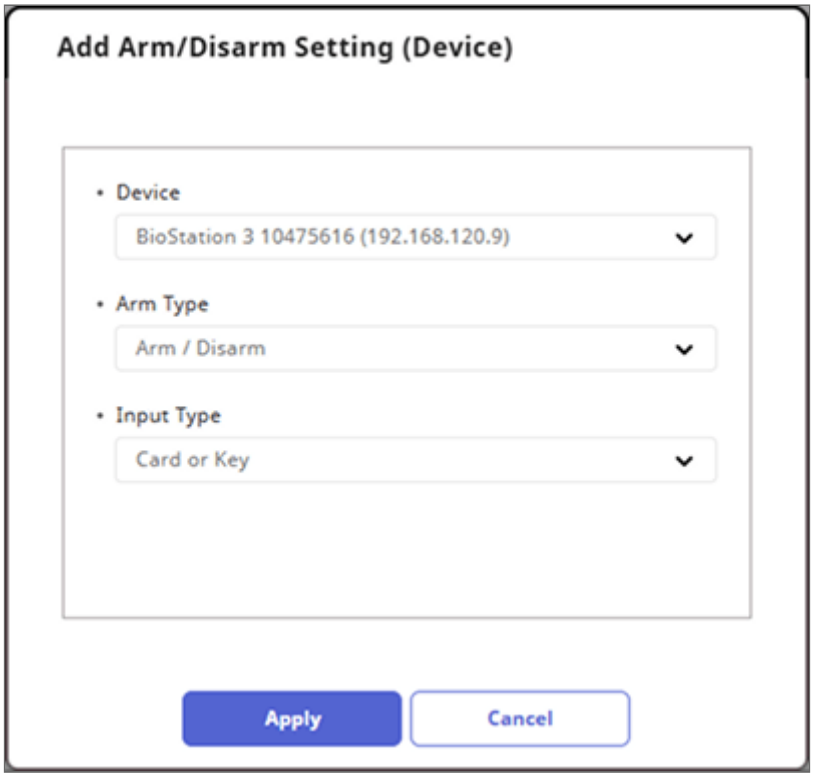


- Set the delay time until arming or disarming with **Delay Time**. This means that the arming is the delay time after authentication until the alarm starts, and the disarming is the delay time before the alarm is triggered after an intrusion is detected.
- Add cards authorized for arming or disarming 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 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.



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).



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.

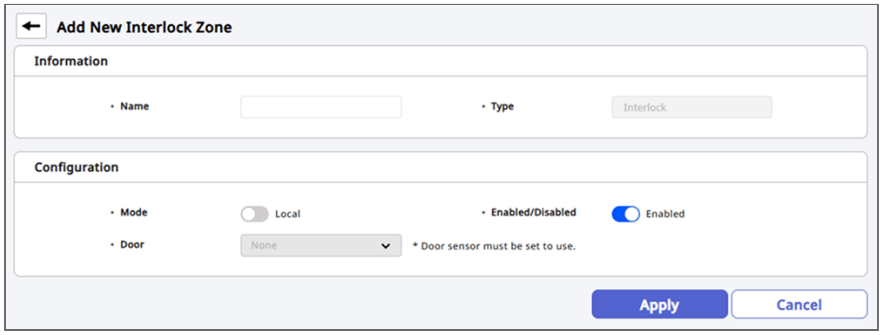
This method enhances security by preventing multiple doors from being opened simultaneously.

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.

Register interlock

1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Advanced AC** on 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.



6. Set the details of the interlock setting in the **Settings** section. For more information, see Setting options guide.
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 the **Door** option is 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:

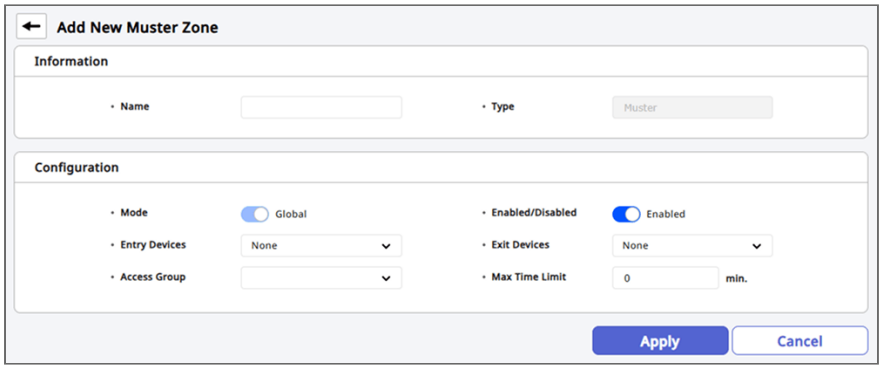
- **Emergency response**: Designate a location where users can safely gather in case of emergencies, such as fires or earthquakes.
- **Personnel monitoring**: Check the current number of people and the list of entrants in real-time in a specific location.

- **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 **Access Management** → **Advanced AC** on 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.



6. Set the details of the muster settings in the **Settings** section. For more information, see Setting options guide.
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.

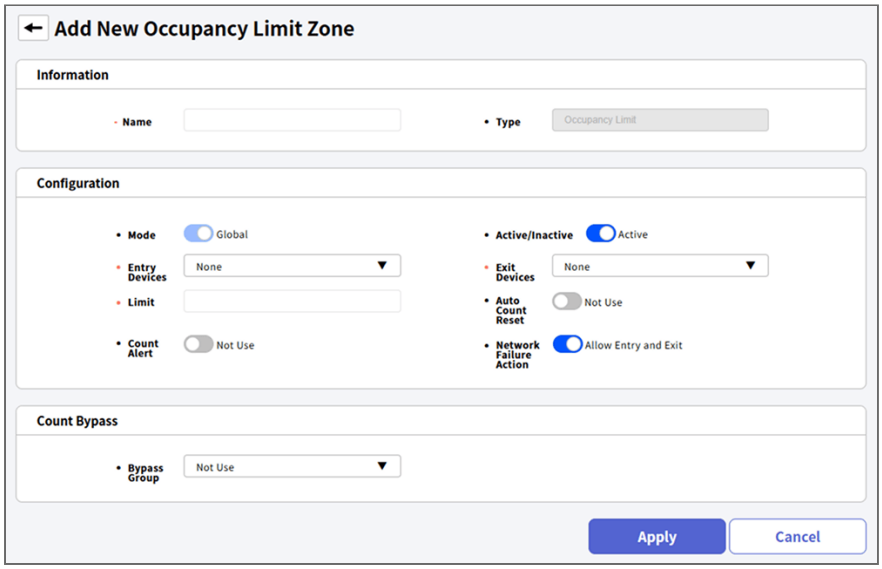
By utilizing these features, administrators can establish tailored personnel management policies suited to the characteristics of each space, ensuring safe and efficient facility operations.

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

Register occupancy limit

1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Advanced AC** on 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.



6. Configure the details of the occupancy limit setting in the **Configuration** section. For more information, see Setting options guide.

7. In the **Count Bypass** section, you can select access groups that can always bypass the occupancy limit setting. For more information, see Always-pass headcount setting.

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**.
- A device configured with **Dual Authentication** on a door cannot be assigned to **Entry Devices** or **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 headcount 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 **Access Management** → **Advanced AC** on 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 **Access Management** → **Advanced AC** on 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.

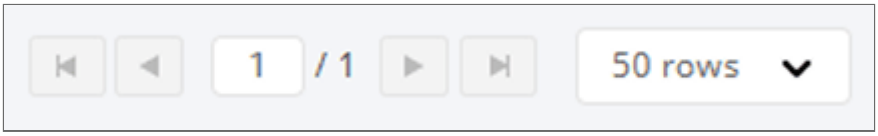
Delete

1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Advanced AC** on 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

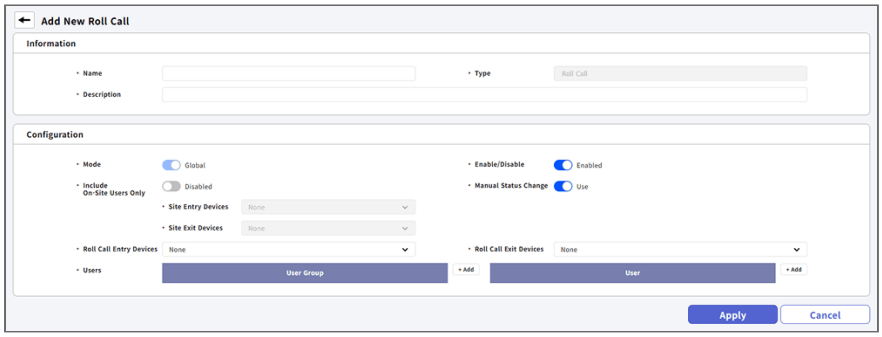
Roll Call quickly generates a personnel list based on entry records within a specific time and place. When an emergency occurs, the system can determine whether a user has arrived at the roll call location by authenticating through the entry or exit device at a predesignated location.

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

> **Info**
> Roll call settings can be used through an add-on option with an **Essential** license or higher. For more information on licensing policies, see License Policy.

Register roll call

1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Advanced AC** on 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.



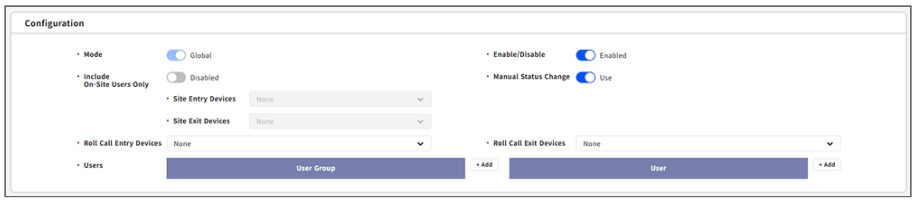
6. Set details in the **Configuration** section. For more information, see Setting options guide.

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.



- **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.
- **Include On-Site Users Only**: Set to **Use**. The system locks roll call targets to **users who last authenticated at an on-site entry device** when roll call starts. The default is **Not Use**. In this case, all configured users (user groups and individual users) become roll call targets.

  > The system determines whether each user is on site based on authentication records from on-site entry or exit devices within the last 7 days. If the most recent authentication before roll call starts occurred at an on-site entry device, the system considers the user on site. If it occurred at an on-site exit device, the system considers the user off site. The system considers users without authentication records within the last 7 days off site and excludes them from the target list.
  >
  > The target list is finalized only once when roll call starts, and it does not change if users enter or exit while roll call is in progress.

  The following options are available when **Include On-Site Users Only** is set to **Use**.

  – **Site Entry Devices**: Select the device for on-site entry authentication.

  – **Site Exit Devices**: Select the device for on-site exit authentication.

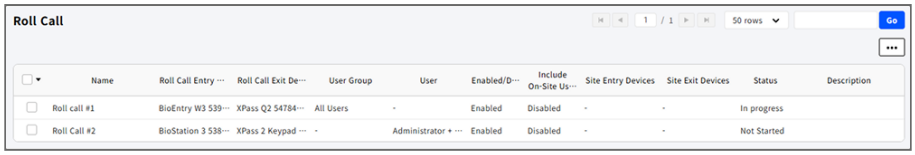
- **Manual Status Change**: You can set it to change the status manually.

- **Roll Call Entry Devices**: Select the device to be used when entering. You can choose from the list of registered devices.
- **Roll Call 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 **Roll Call Entry Devices** and **Roll Call Exit Devices** at the same time.
> - Select up to 10 devices for **Roll Call Entry Devices** and **Roll Call Exit Devices**.
> - For more information about device registration, refer to the following.
>   - Register Device
>   - Register Wiegand Credentials
>   - Register Slave

Check roll call list status

The roll call list shows details and status for each roll call setting.

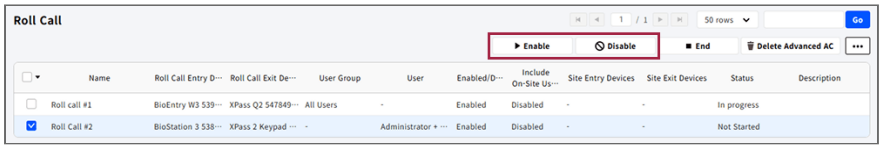


- **Name**: Shows the name.
- **Roll Call Entry Devices** / **Roll Call Exit Devices**: Shows the selected devices.
- **User Group** / **Users**: Shows the selected targets.
- **Enabled/Disabled**: Shows the activation status.
- **Include On-Site Users Only**: Shows whether it is enabled.
- **Site Entry Devices** / **Site Exit Devices**: Shows the selected on-site entry or exit devices.
- **Status**: Shows the roll call status (**Not Started**, **In progress**, etc.).
- **Description**: Shows the description.

Activate/deactivate

You can activate disabled roll call settings or deactivate activated settings.

1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Advanced AC** on 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.

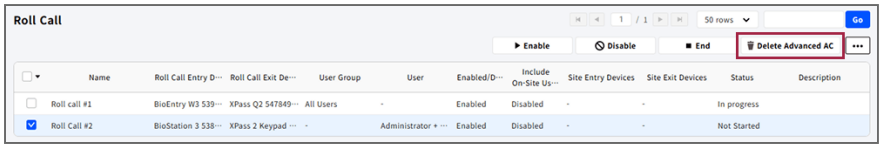


5. Click **Enable** or **Disable** in the upper right corner of the screen.

> **Info**
>
> - Select **Disable**, and a confirmation message appears. Select **Yes** or **No**.
> - Cannot deactivate an ongoing roll call. Check and try again.

Delete

1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Advanced AC** on 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.

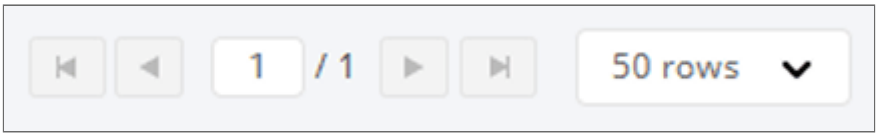


5. Click **Delete Advanced AC** at the top right of the screen.
6. When the warning message appears, click the **Continue** button.

> **Info**
>
> Cannot delete an ongoing roll call. End the roll call and try again.

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.

Use roll call in the mobile app

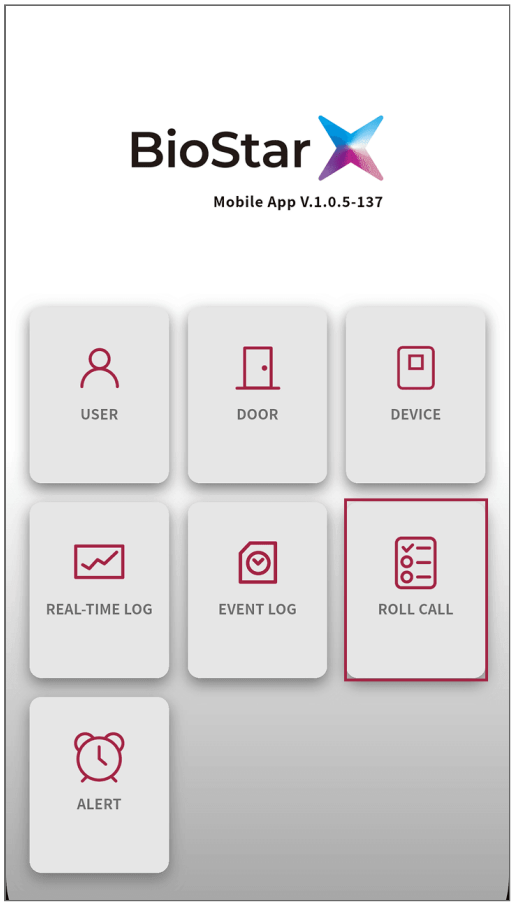
The roll call feature is available in the BioStar X mobile app.

> **Info**
> You can install the BioStar X mobile app via the following links.
> - iOS: Apple App Store
> - Android: Google Play'

Start roll call

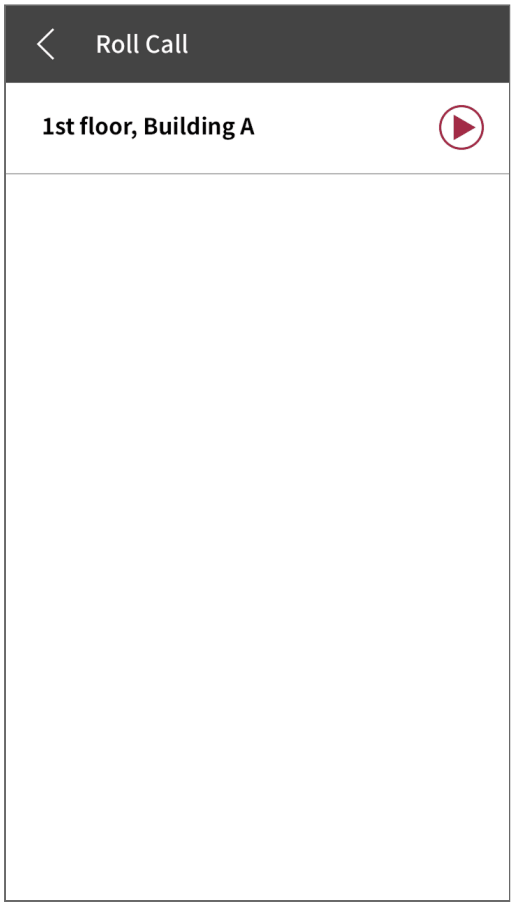
To start the roll call feature in the mobile app, follow these steps.

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



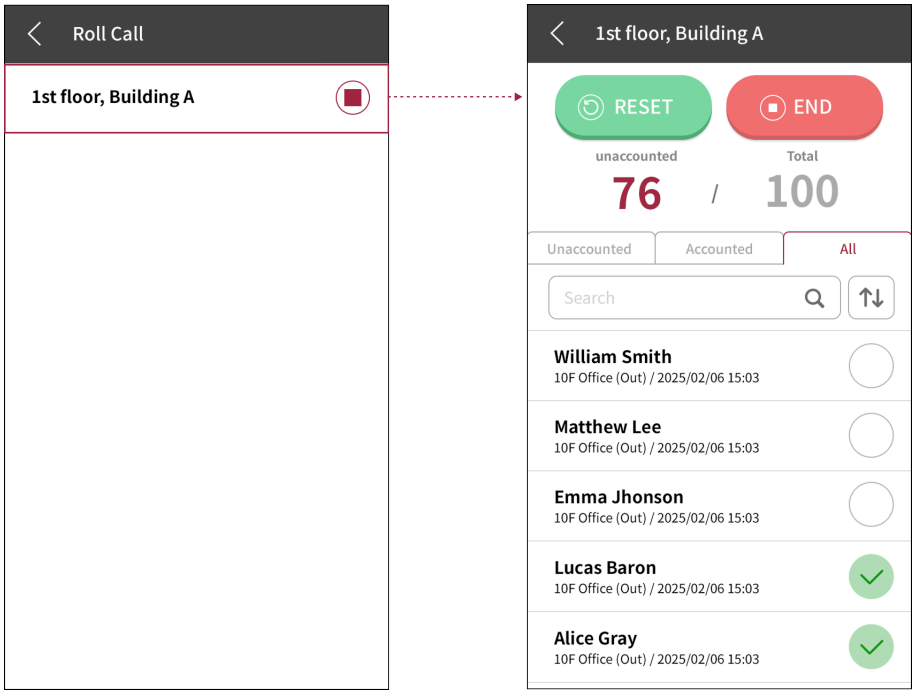
> You can also access it through the side menu. Tap ☰ → **Monitoring** → **Roll Call**.

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



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

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



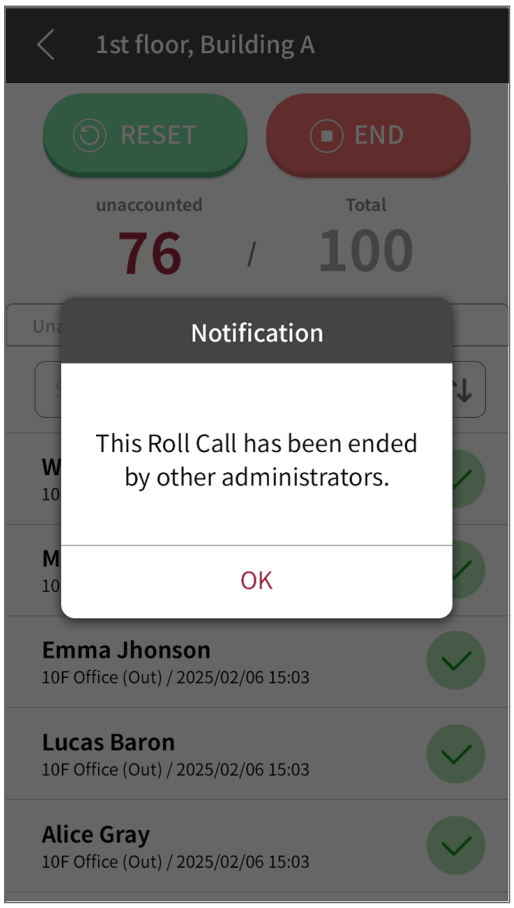
Control an in-progress roll call

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

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



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

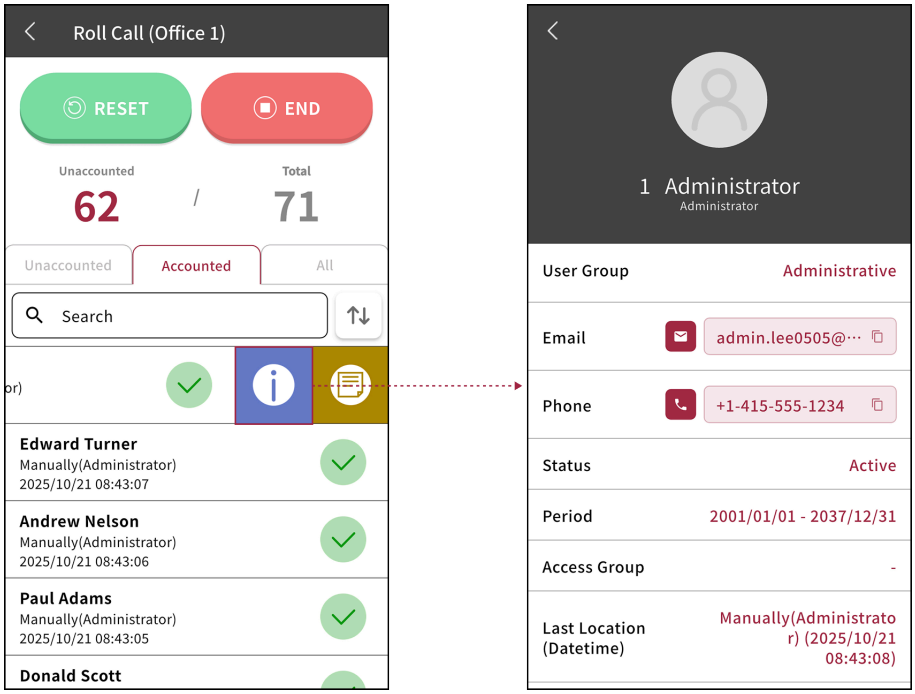


- After completing the roll call, you can check related reports from **Data** → **Generate Report** → **Roll Call**. For more information, see View roll call reports.

User information during roll call

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

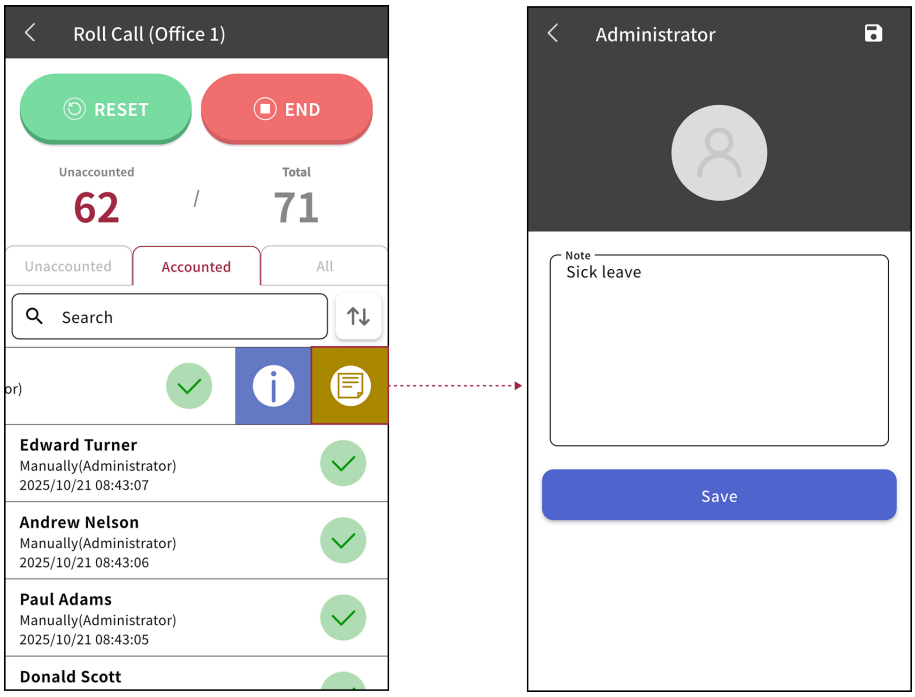
Swipe left on the user item for which you want to check details during roll call. Then tap ⓘ.



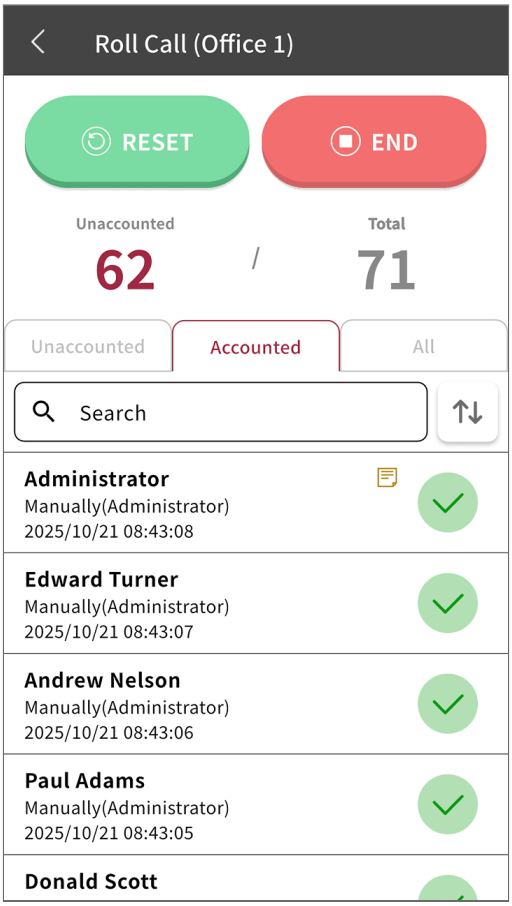
Leave a note for users during roll call

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

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



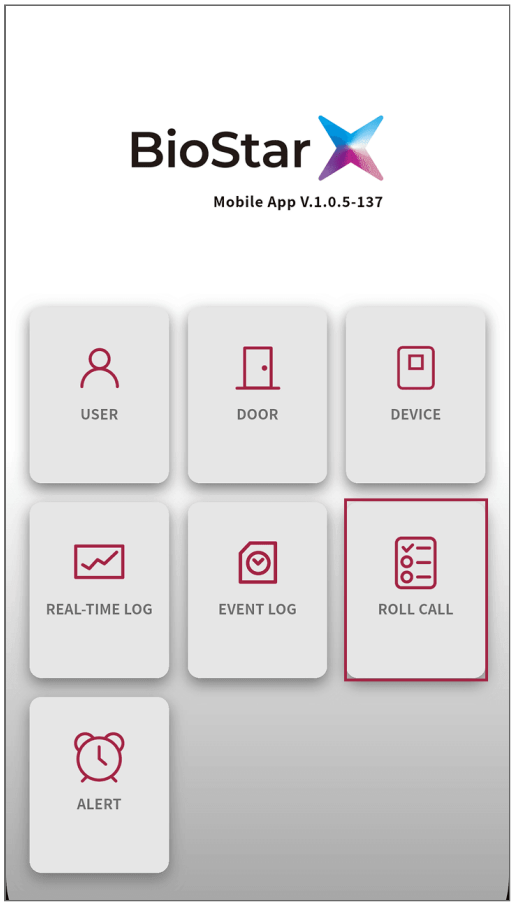
Users who have entered notes will be marked with the icon in the roll call list.



Check roll call details

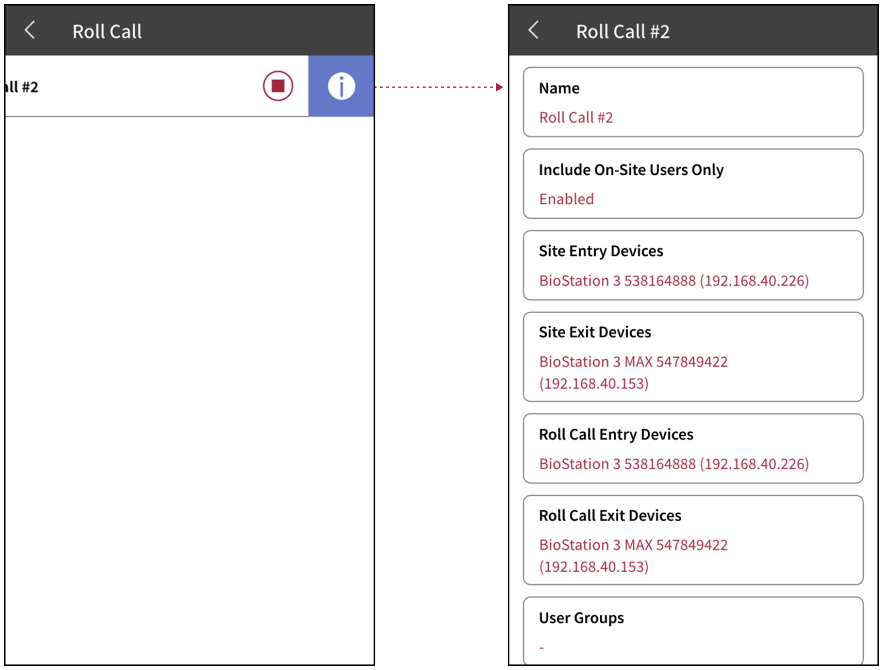
You can check the details of the roll call settings in the mobile app.

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



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

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

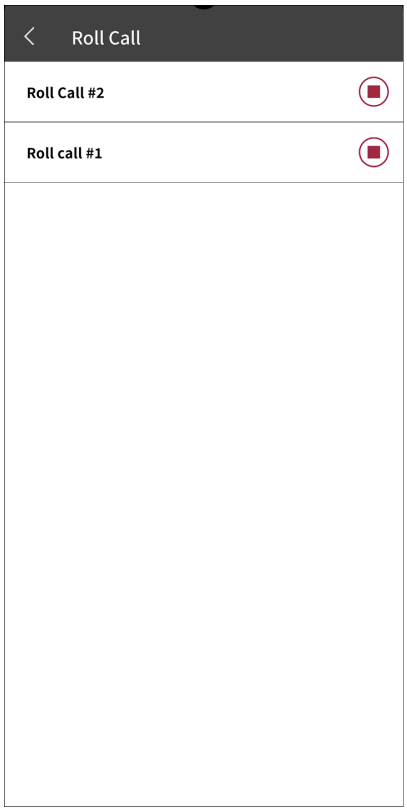


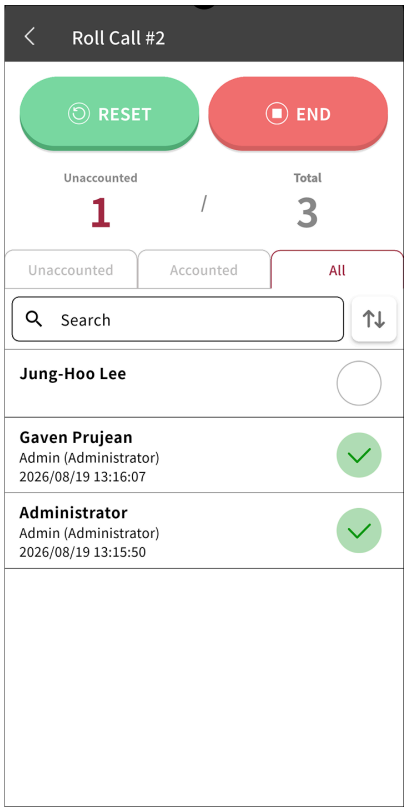
End roll call

End ongoing roll calls in both the **BioStar X** mobile app and on the web.

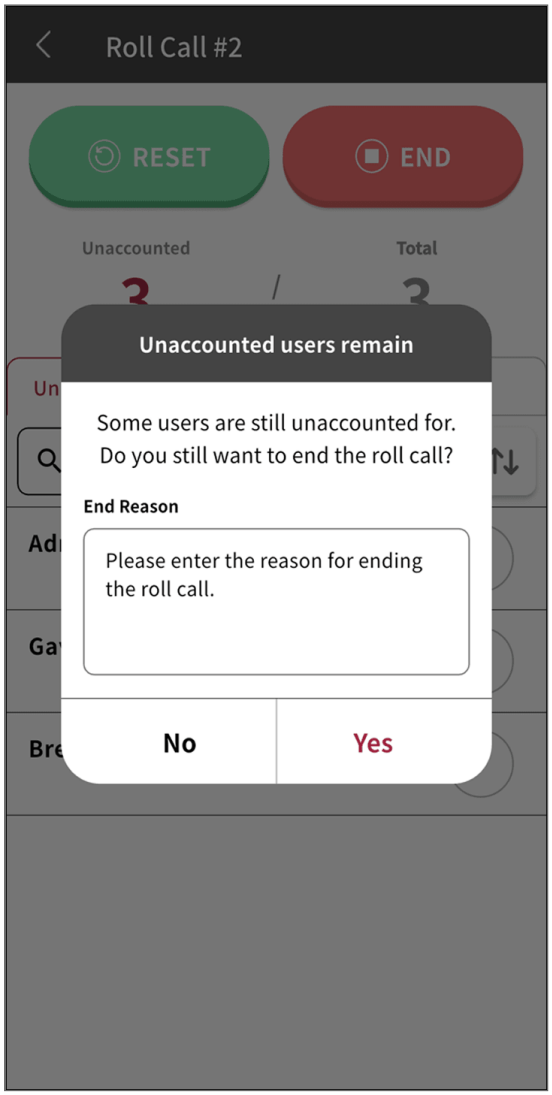
End in the mobile app

1. To end a roll call, tap the button in the roll call list screen, or tap the **END** button in the roll call status screen.



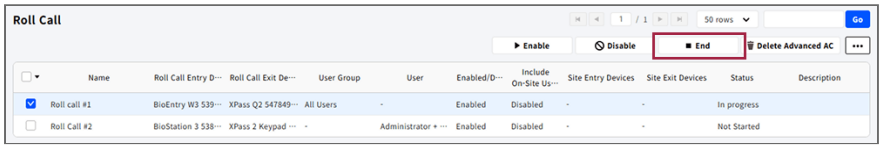


2. If unaccounted users remain, a warning pop-up appears. Enter an end reason, and tap **Yes**.



End on the web

1. Click **Settings** on the **Launcher** page.
2. Click **Access Management** → **Advanced AC** on the left sidebar.
3. Click **Roll Call** from the list.
4. In the roll call list, click the checkbox for the roll call to end.



5. Click **End** at the top right of the screen.
6. When the confirmation message appears, click **Yes**.

A roll call with no unaccounted users ends immediately. For a roll call with unaccounted users, a dialog appears with the **Unaccounted Users** list and the **End Reason** field. Enter a reason, and click **End Roll Call** to end the roll call.



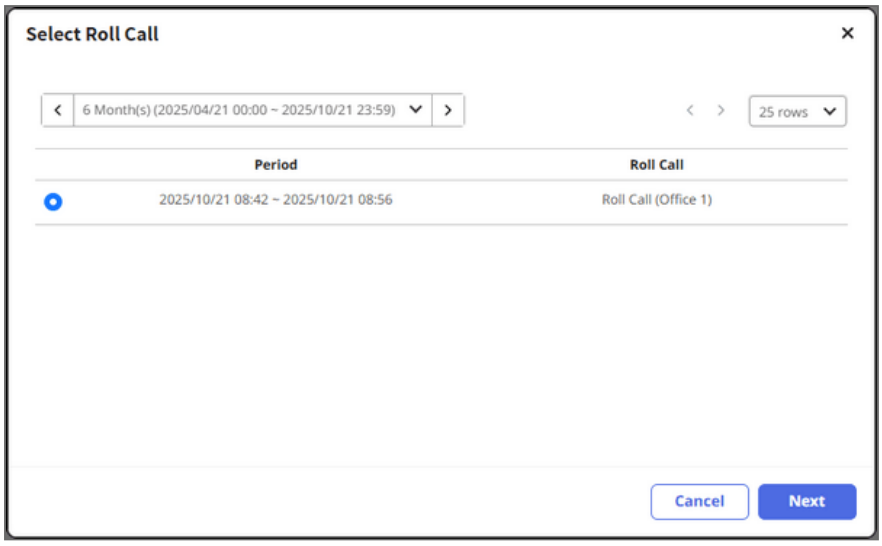
Info

- **End Reason**: Enter up to 500 characters.
- The system cannot end multiple roll calls at once if any roll call has unaccounted users. End roll calls one at a time.

View roll call reports

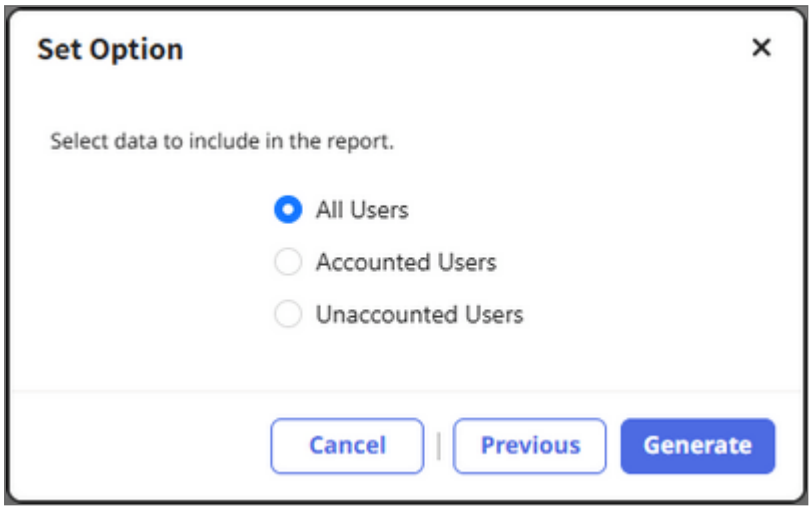
To check the roll call report, follow these steps.

1. Click **Data** on the **Launcher** page.
2. Click **Events** → **Roll Call** on the left sidebar.
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.

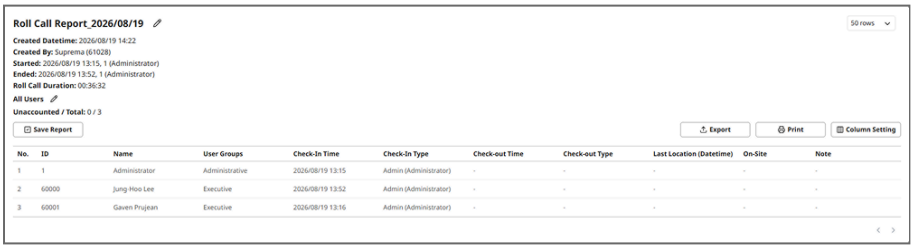


> If you do not see the desired roll call item, adjust the period at the top of the screen.

4. In the option settings window, select the data to include in the report, then click the **Generate** button.

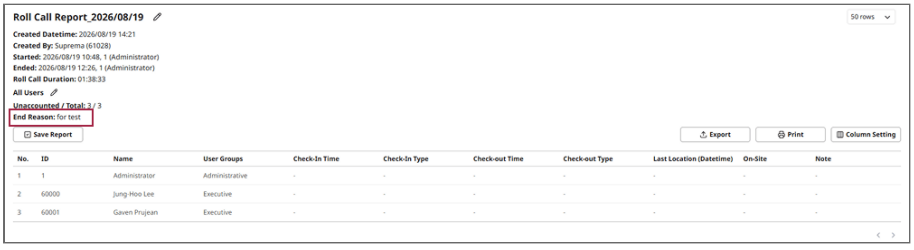


Generating the report. The report provides information on each user, including their entry time, exit time, last location, and notes.



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

Check **End Reason** in roll call reports with unconfirmed users.



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 **Essential** license or higher. For more information on licensing policies, see License Policy.

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, see Integrate VMS.

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, see Set Up the Camera.

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, see Set Video Rules.

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 use the following features 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 you start

To integrate with the **Video Management System** (VMS), please check the following items.

- The VMS integration feature is available as an add-on option for **Essential** or higher licenses. For more information on licensing policies, see License Policy.

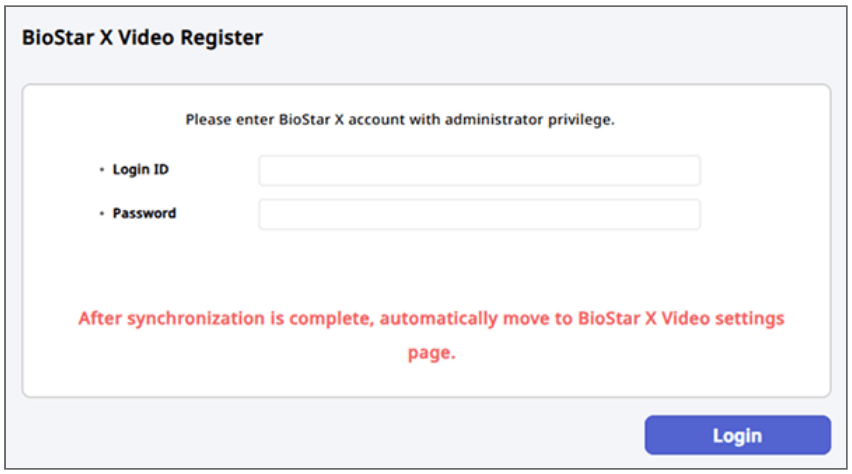
- Make sure that the VMS server is correctly installed and configured. The VMS server must be in a state that can connect online with **BioStar X**.
- Use a VMS that is compatible with **BioStar X**. You can use BioStar X VMS or the **Nx Witness v5.1.5**, **v6.x.x** series of VMS.
- Prepare the IP address, 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

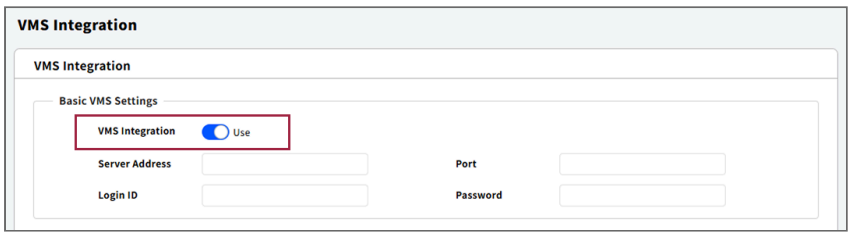
Follow the steps below to integrate the VMS server with **BioStar X**.

1 Activate VMS integration

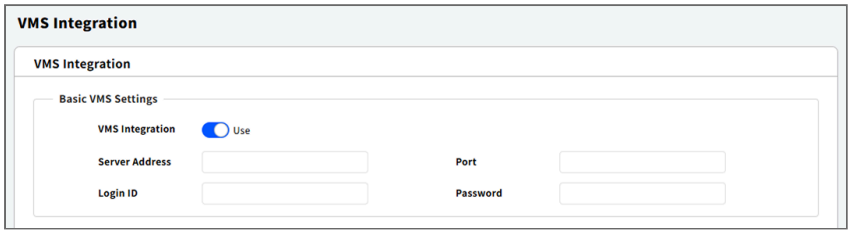
1. Click **Settings** on the **Launcher** page.
2. Click **Video** → **VMS Integration** on the left sidebar.
3. If this is your first time accessing, log in with the **BioStar X** administrator account.



4. Set the **VMS Integration** option to **Use**.



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.

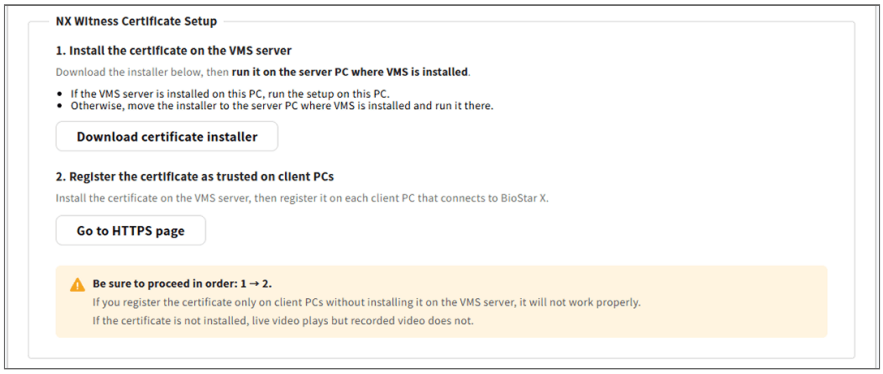
> **Info**
>
> - If the integration with the VMS server fails and an error message appears, check the server address and administrator account information again. It is also necessary to check whether the VMS server is online and if network connections are blocked due to firewall settings.
> - For more information on the settings in the **VMS Event/Bookmark** section, see VMS event and bookmark settings.

2 Install the certificate on the VMS server

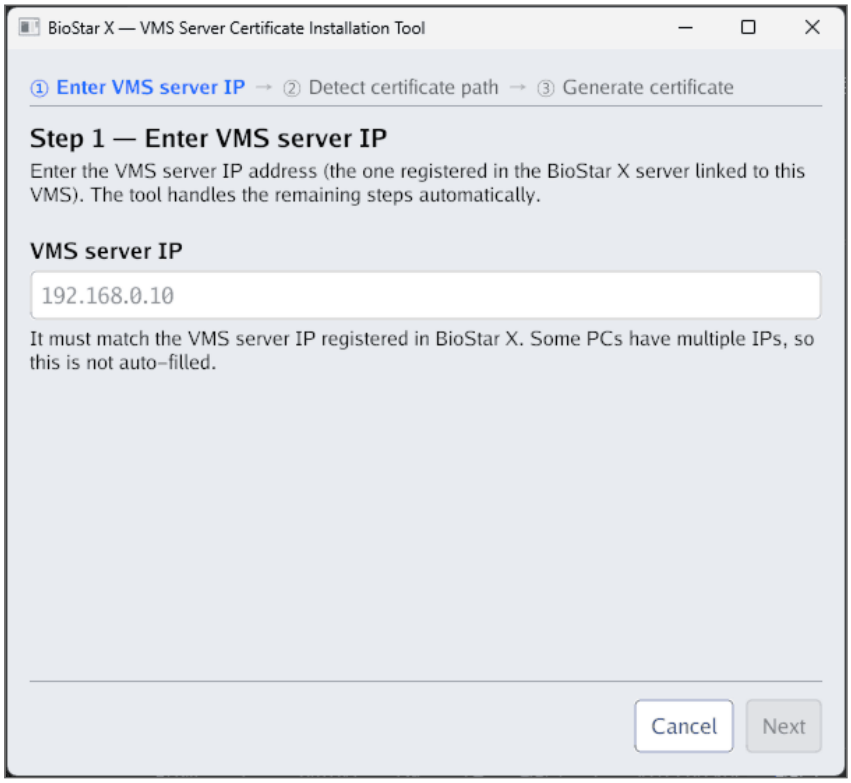
To play back recorded video from the VMS server, you must use HTTPS protocol. Standard SSL certificates are issued for domain names, so they aren't valid when accessing the VMS server by its IP address. Therefore, you need to create a separate certificate that includes the VMS server's IP address.

> **Info**
>
> You must install a certificate whether the VMS server and **BioStar X** are installed on the same server or on separate servers.

The **NX Witness Certificate Setup** section becomes available only when the **VMS Integration** option is set to **Use**.

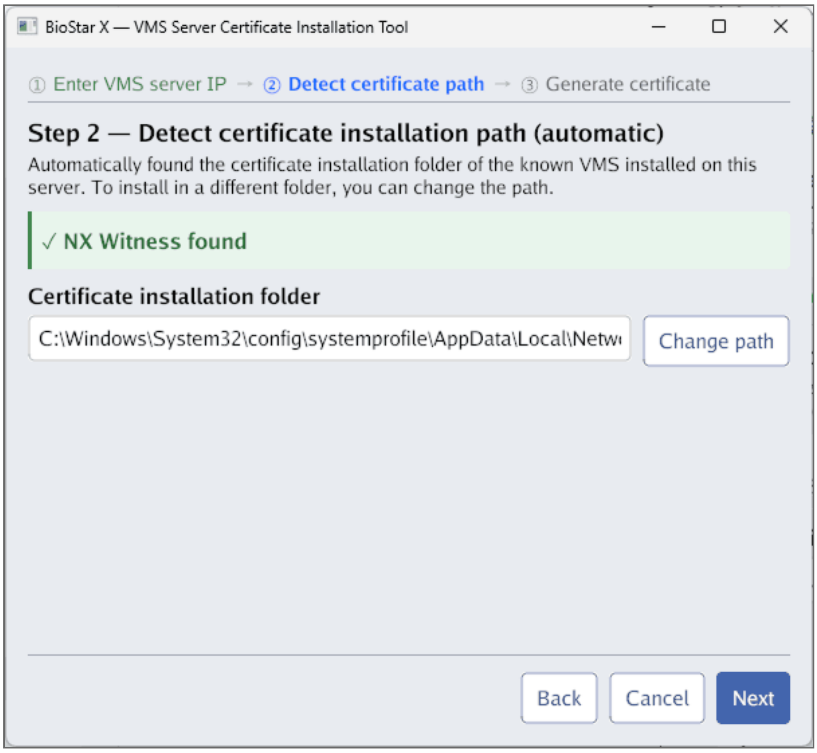


1. On the server where VMS is installed, click **Download certificate installer** to download the certificate installer.
2. Run the downloaded *vmsCertMaker.exe* file.
3. Enter the IP address in the **VMS server IP** field.

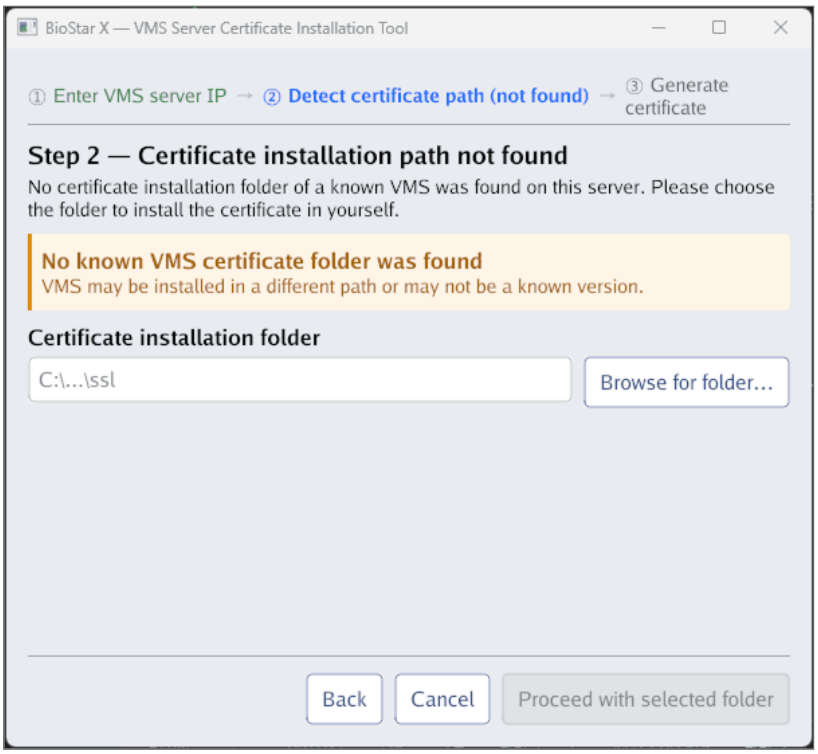


> Use the IPv4 address format. e.g., 192.168.0.10

4. Enter an IP address in the correct format to enable the **Next** button. Click **Next**.
5. Select the VMS certificate installation path.
   - For compatible VMS, the installer detects the installation path automatically.

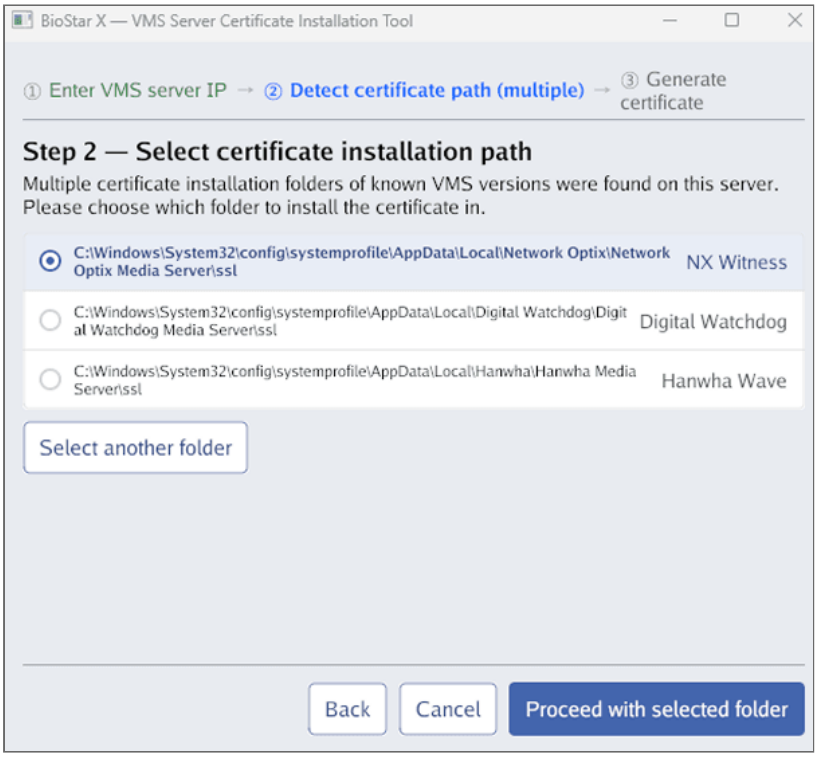


- If the installer does not detect the installation path automatically, click **Browse for folder** and select the path manually.



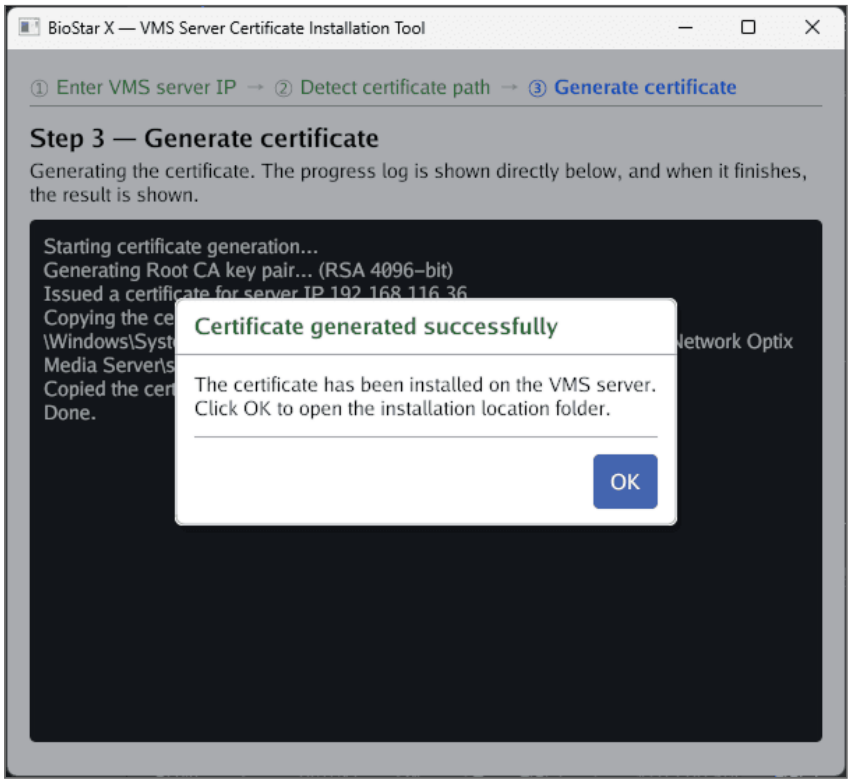
> The installation path of the certificate may vary depending on the VMS. Refer to the examples below.
>
> – **BioStar 2 VMS**: *C:\Windows\System32\config\systemprofile\AppData\Local\Suprema Inc\Suprema Inc. Media Server\ssl*
>
> – **Digital Watchdog**: *C:\Windows\System32\config\systemprofile\AppData\Local\Digital Watchdog\Digital Watchdog Media Server\ssl*
>
> – **Hanwha Wave**: *C:\Windows\System32\config\systemprofile\AppData\Local\Hanwha\Hanwha Media Server\ssl*
>
> – **NX**: *C:\Windows\System32\config\systemprofile\AppData\Local\Network Optix\Network Optix Media Server\ssl*

- If multiple VMS certificate paths exist, all paths appear. Click **Select another folder** and select the desired path.



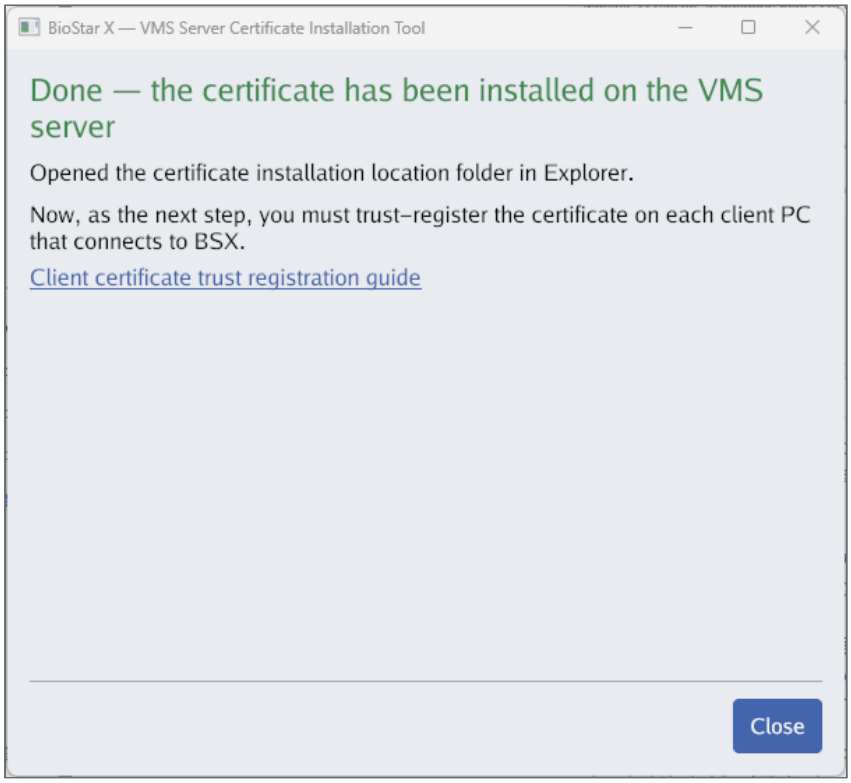
6. Click **Next** or **Proceed with selected folder**.

7. After certificate generation completes, the **Certificate generated successfully** message appears.



8. The certificate installation path appears when you click **OK**. Confirm that the certificate file (*cert.pem*) exists.

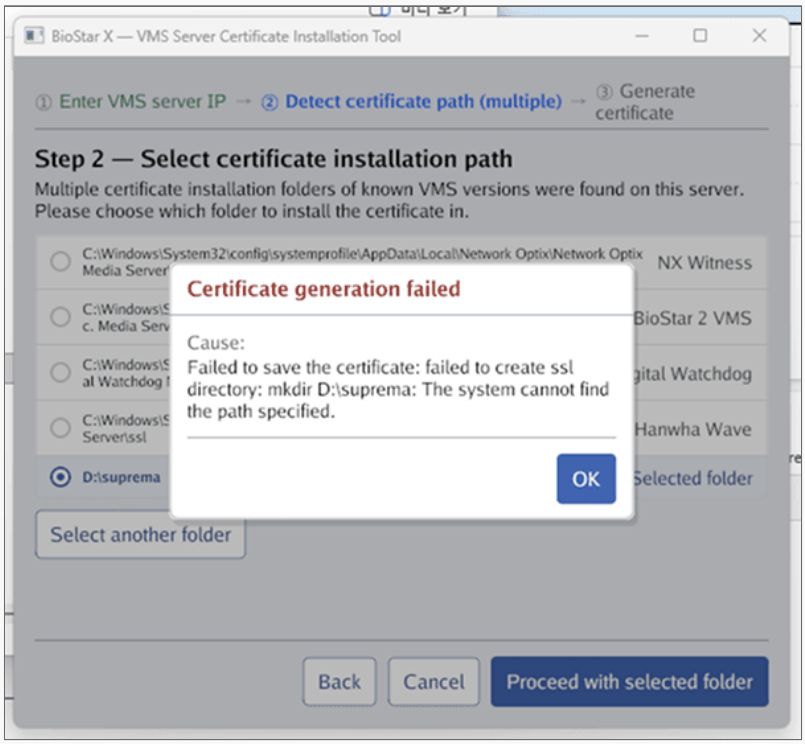
9. After certificate installation completes, click **Close**.



10. Reboot the VMS server.

Info

If certificate installation fails, the message shows the reason. Review the message, then take the required action.



3 Install the certificate on the client PC

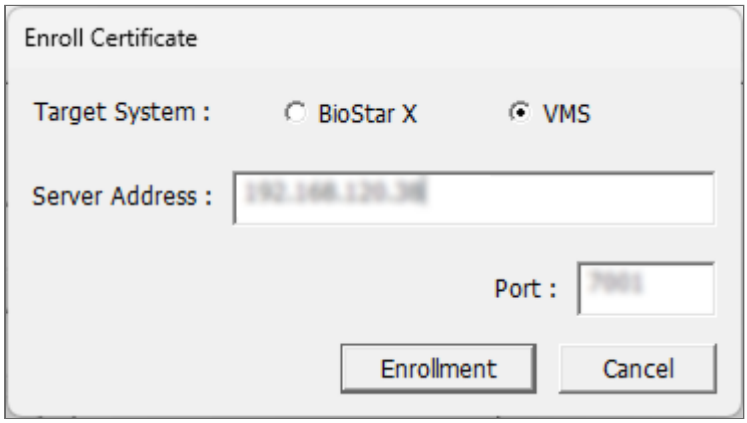
If the following situations occur, you can install the certificate from the VMS server onto the client PC to resolve the issue.

- 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

> **Caution**
> Enrolling the certificate only on the client PC, without installing it on the VMS server, prevents normal operation.

---

1. Access **BioStar X** through your web browser.
2. Download the HTTPS certificate installer (*cert-register.zip*) from the login screen or **Settings** → **System** → **HTTPS**.
3. Unzip the downloaded file and run **cert-register.exe** file. The **Enroll Certificate** window appears.
4. 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 (default: 7001)
5. Click **Enrollment**.
6. 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.

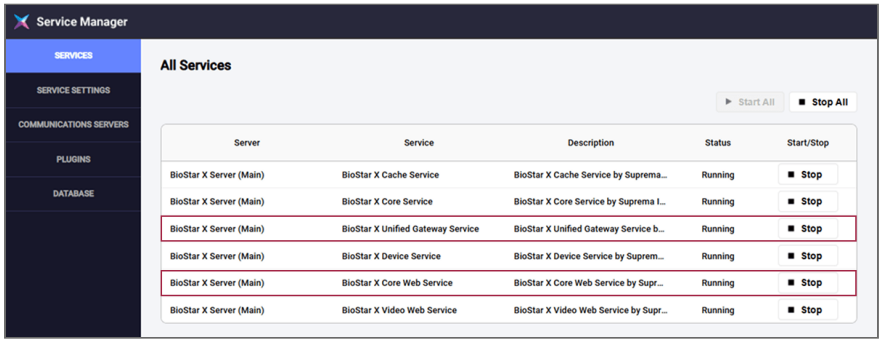
4 Check and set the camera

If the VMS server is integrated normally, you can check the connected cameras in the **Video** → **Video** menu. For more information, see Set Up the Camera.

Troubleshooting

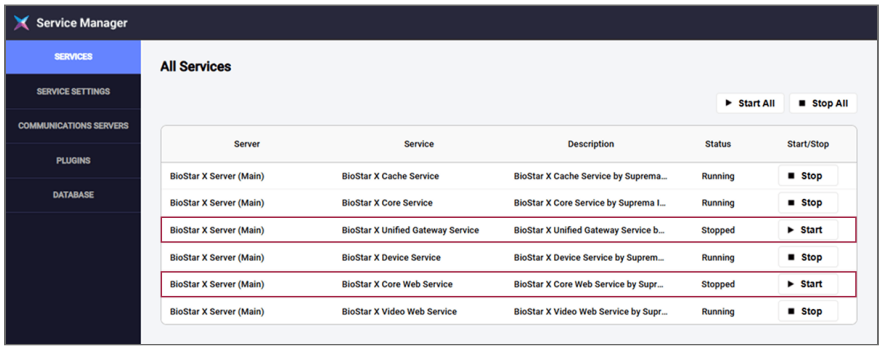
If the service does not work after first integration with the VMS server, manually restart it as follows.

1. Click Start → **BioStar X** → **BioStar X Service Manager** on Windows.
2. In the **All Services** list, click **Stop** for the services below to stop them.



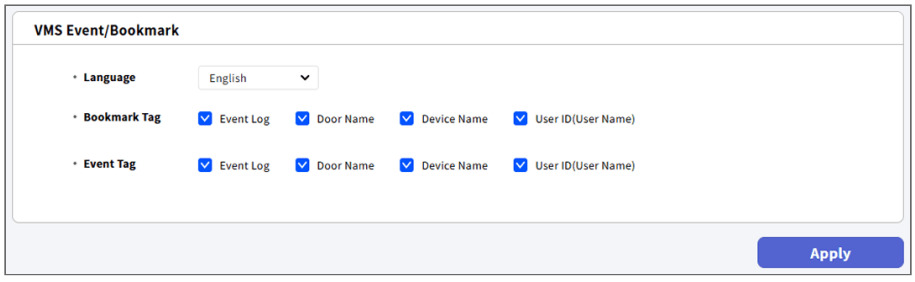
- **BioStar X Unified Gateway Service**
- **BioStar X Core Web Service**

3. When the status of the requested service changes from **Pending** to **Stopped**, click **Start** to restart the service.



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 **Apply** at the bottom right of the screen.



- **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.
- If bookmark or event tags include the following characters, the system removes them before sending them to the VMS server.
  - Event tag: `\` `'` `,` `#` `%` `=` `&` `<` `>`
  - Bookmark tag: `<` `'`

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. Click **Video** → **VMS Integration** on the left sidebar.
3. Set the **VMS Integration** option to **Not Use**.
4. Click **Apply** at the bottom right of the screen.
5. Check the contents of the message window and click **Yes**.

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

- For more information on how to integrate with the VMS server, refer to Integrate VMS.
- The camera group permission is required to add cameras or configure groups. For more information on camera group permissions, see Camera group permission setting.

Camera settings and management

After VMS integration, you can set up and manage cameras in the menu **Settings** → **Video** → **Video**.

Add camera

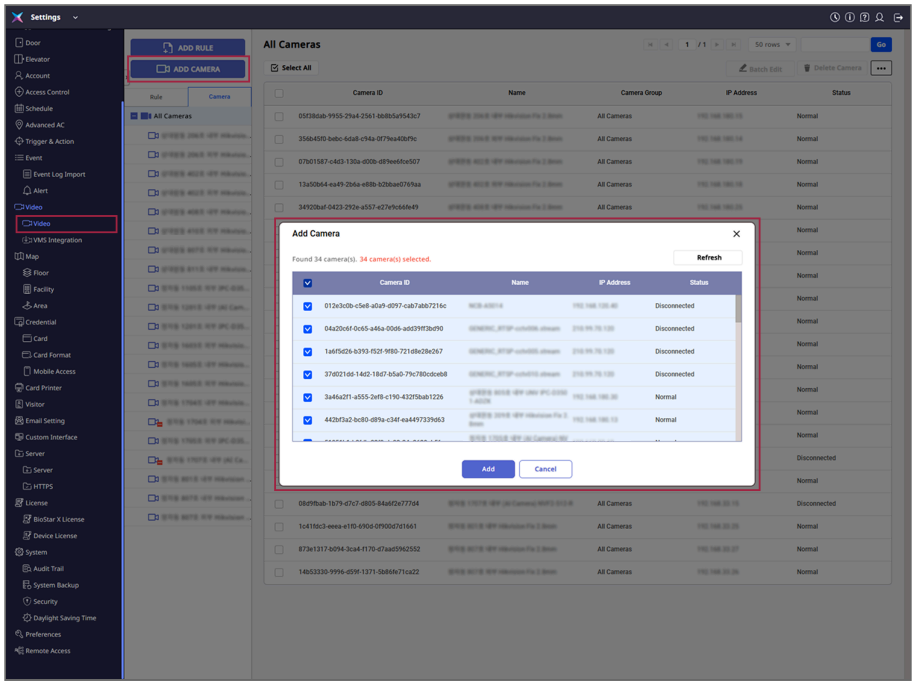
If integrated with VMS, you can add cameras connected to the VMS server to **BioStar X** and play live video and recorded footage on the **Monitoring** page.

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

2. Click **Video** → **Video** on 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 **Refresh** to refresh the camera list.
5. Once you have selected the cameras, click **Add** in the bottom right corner of the screen.

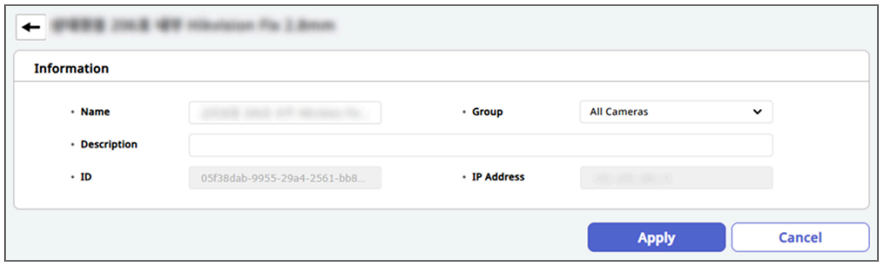
You can check the added cameras in the camera list.



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** on 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.



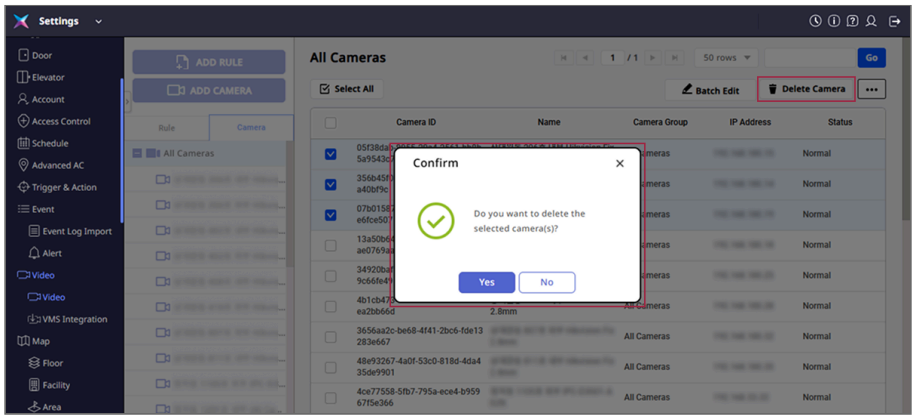
6. After editing all the camera information, click **Apply** in the bottom right corner of the screen.

> **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** on 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 **Delete Camera** in the upper right corner of the screen.
5. Check the message and click **Yes**.



> **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 creating and managing rules, see Set Video Rules.

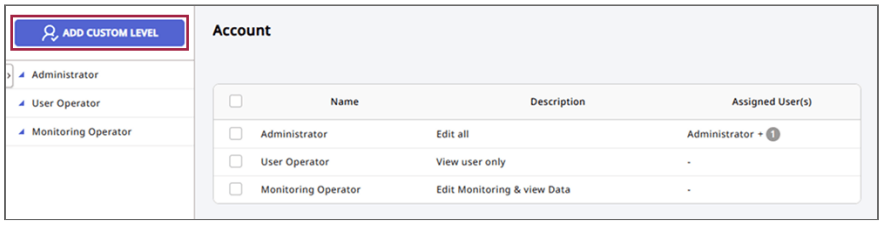
Camera group settings and management

You can group multiple cameras to manage them systematically by location or purpose. Follow the steps below to create and manage camera groups.

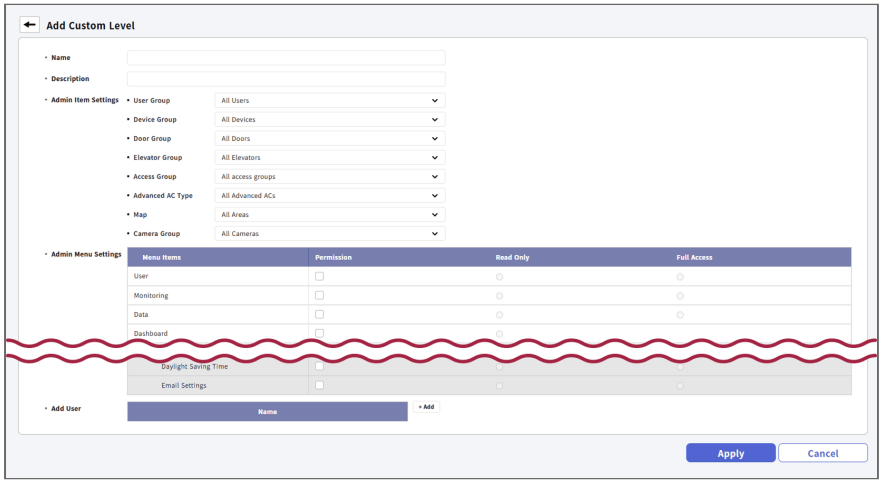
Camera group permission setting

Administrators need the camera group permission to add cameras or configure groups. System administrators, user administrators, and monitoring administrators have access to all camera groups. If you need different permission settings, add a custom permission to configure camera group access.

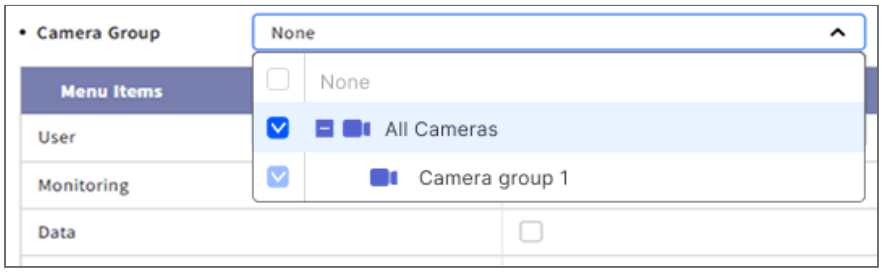
1. Click **Settings** on the **Launcher** page.
2. Click **Account** → **Account** on the left sidebar.
3. Click **Add Custom Level**.



4. Enter a name and description for the newly created permission.



5. In **Admin Item Settings**, under **Camera Group**, select the camera group to assign permissions to.



- Select **All Cameras** to grant permissions for all camera groups.
- To grant permissions for an individual camera group, select the desired group from the camera group list. You can select one or more groups.

6. In **Add User**, click **+ Add** and select the users to assign permissions to.
7. Click **Apply** at the bottom of the screen to save the settings.

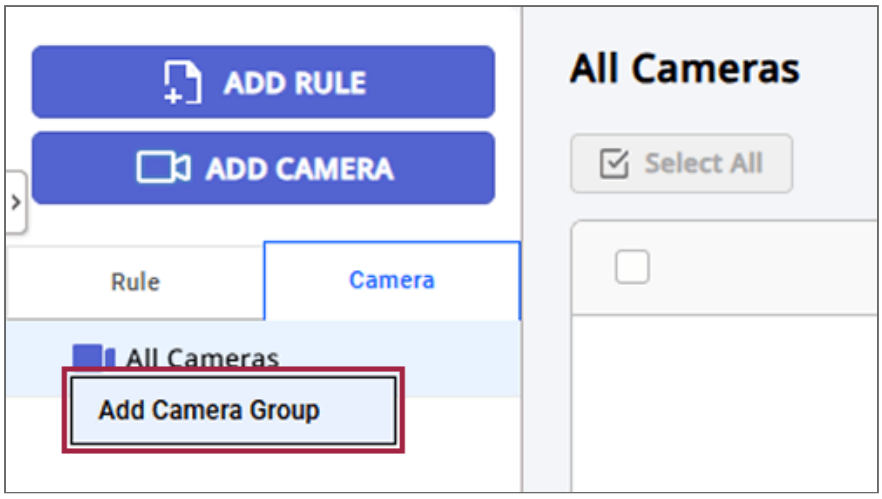
> **Info**
> If you do not have permission for a specific camera group, you cannot view the cameras in that group.

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** on 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

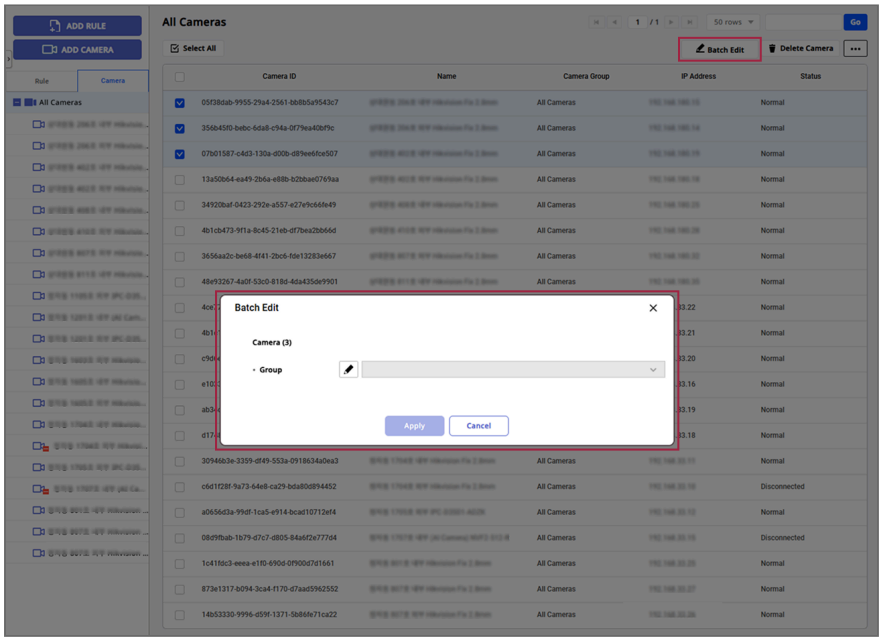
You can add more than one camera to the added group.

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

2. Click **Video** → **Video** on 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, **Batch Edit** will be activated in the upper right corner of the screen. Click **Batch Edit**.



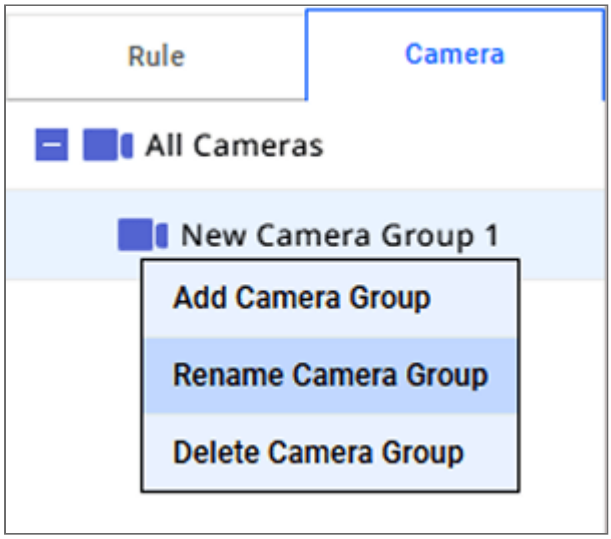
5. When the **Batch Edit** window appears, click the **Group** button of the ✎ item.
6. Select the desired group from the group list.
7. Click **Apply**.

> **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** on 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

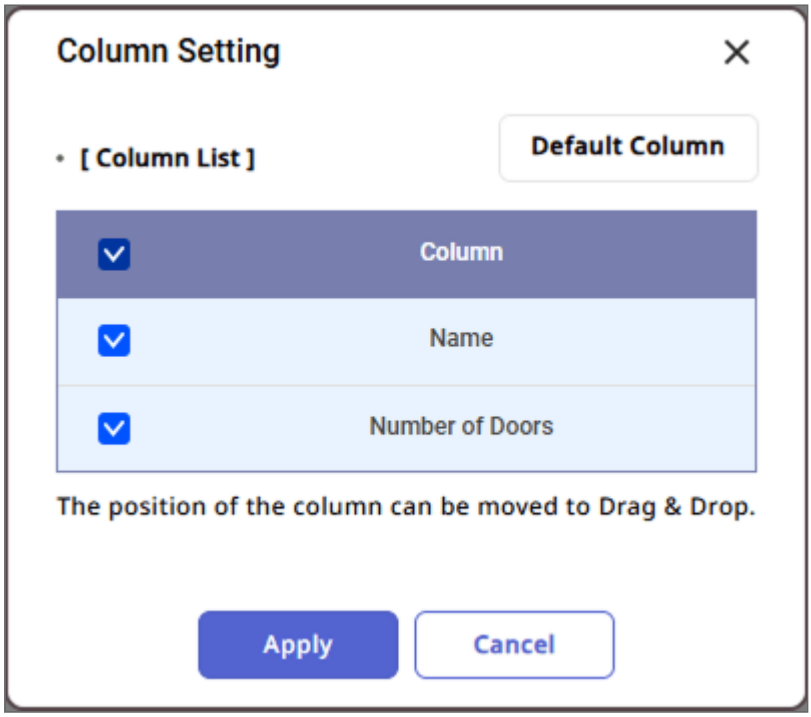
1. Click **Settings** on the **Launcher** page.
2. Click **Video** → **Video** on the left sidebar.
3. Click the **Camera** tab.
4. Select the group you want to rename and right-click.
5. Click **Delete Camera Group** from the popup menu.
6. Check the warning message and click **Yes**.

> **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** on 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.



5. Once you have changed all column settings, click **Ok**.

> **Info**
> To initialize the column settings, click **Default Column**.

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 **Essential** license or higher through additional options. For more information on licensing policies, see License Policy.
> - To link a door to a camera, you must have permission for the camera's group. For more information on configuring camera group permissions, see Set Up the Camera.

Add rule

1. Click **Settings** on the **Launcher** page.
2. Click **Video** → **Video** on the left sidebar.

3. Click **ADD RULE** at the top left of the screen.

When the **Add New Rule** screen appears, set the rules according to the following instructions. Click **Apply** at the bottom of the screen to complete and save all settings.

Enter rule information

In the **Information** section, enter the name and description of the new rule.



> **Info**
> **Description** is optional. Use it to enter a simple description to easily understand the purpose or features of the rule.

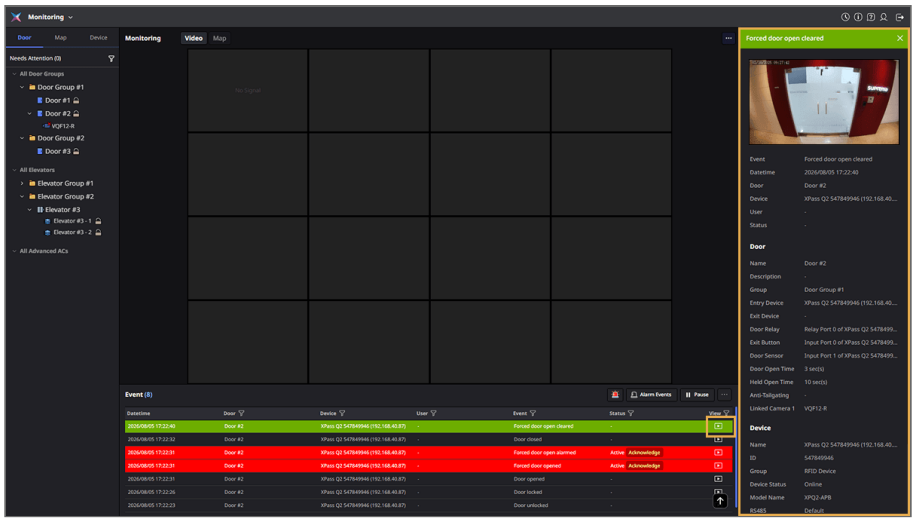
Video log settings

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**: 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.

Enable the **Video Log** option. The video log (▶) icon appears next to events in the event panel on the Monitoring screen. 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.

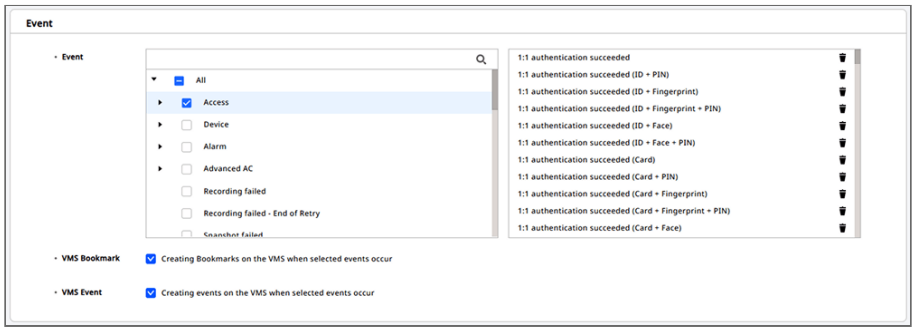


Info

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**: 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 🗑.
- You can set the language of the message when sending bookmarks and events to the VMS server. For more information, see Integrate VMS.

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.



1. Click **+ Add** in the upper right.

2. When the **Add Linkage** window appears, select the door and then the associated camera.



3. Once you have selected both the door and the camera, click **Add**.

You can check the cameras linked to the door in the list.



Info

- Administrators who lack permission for a camera group cannot view or select cameras in that group. For more information on configuring camera group permissions, see Set Up the Camera.
- A single door can have up to four cameras added.
- Doors included in a rule cannot be used in other rules.
- Cameras can be linked to multiple doors without restrictions, and you can also reuse cameras already linked to other doors.
- To delete the linkage rule of doors and cameras, click the checkbox of the items you wish to delete in the list and click **Delete** 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, see Check status.
- Click **Apply** at the bottom of the screen to complete and save all settings.

Edit rule

1. Click **Settings** on the **Launcher** page.
2. Click **Video** → **Video** on 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 **Apply** in the lower right of the screen.

Info

For more information on each section of the rule editing screen, see Add rule.

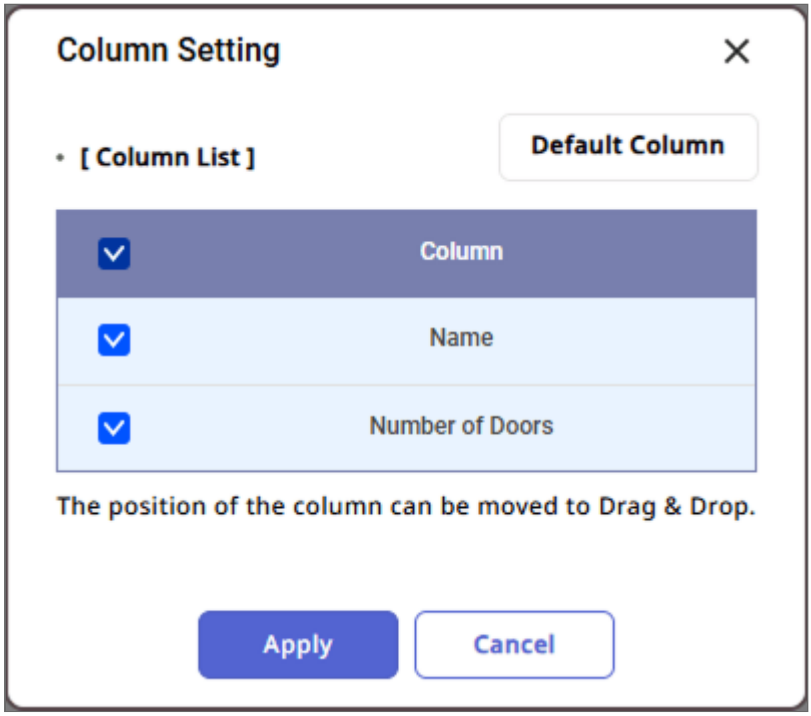
Delete rule

1. Click **Settings** on the **Launcher** page.
2. Click **Video** → **Video** on 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 **Delete Rule** in the upper right of the screen.
5. Check the message and click **Yes**.

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** on 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.



5. Once you have changed all column settings, click **Ok**.

> **Info**
> To initialize the column settings, click **Default Column**.

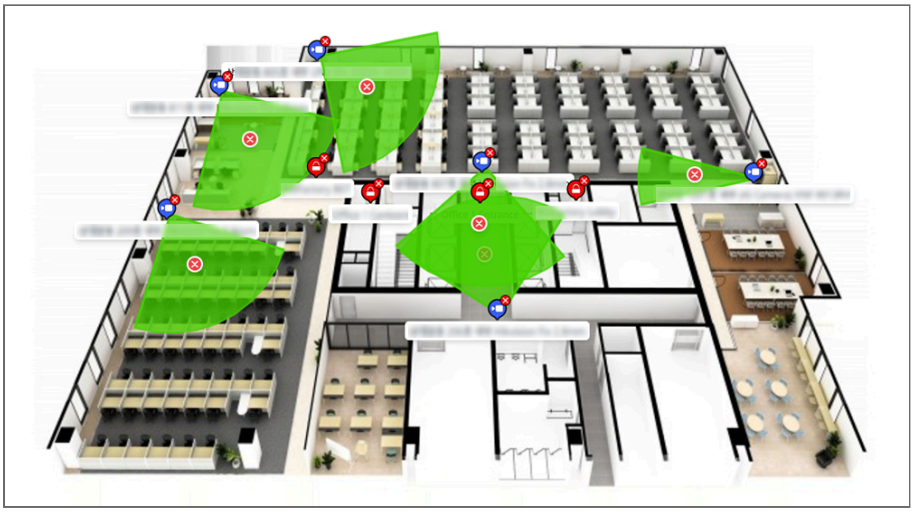
Manage Map

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.

> **Info**
>
> For more information on map monitoring, see Monitor Map.

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 on registering doors, see Register Door.
> - For more information on map monitoring, see Monitor Map.
> - The add floor and floor settings features are available with an **Essential** license or higher. For more information on licensing policies, see License Policy.

Add floor

Upload a floor layout or a 3D bird's eye view image to add a floor and place doors and cameras.

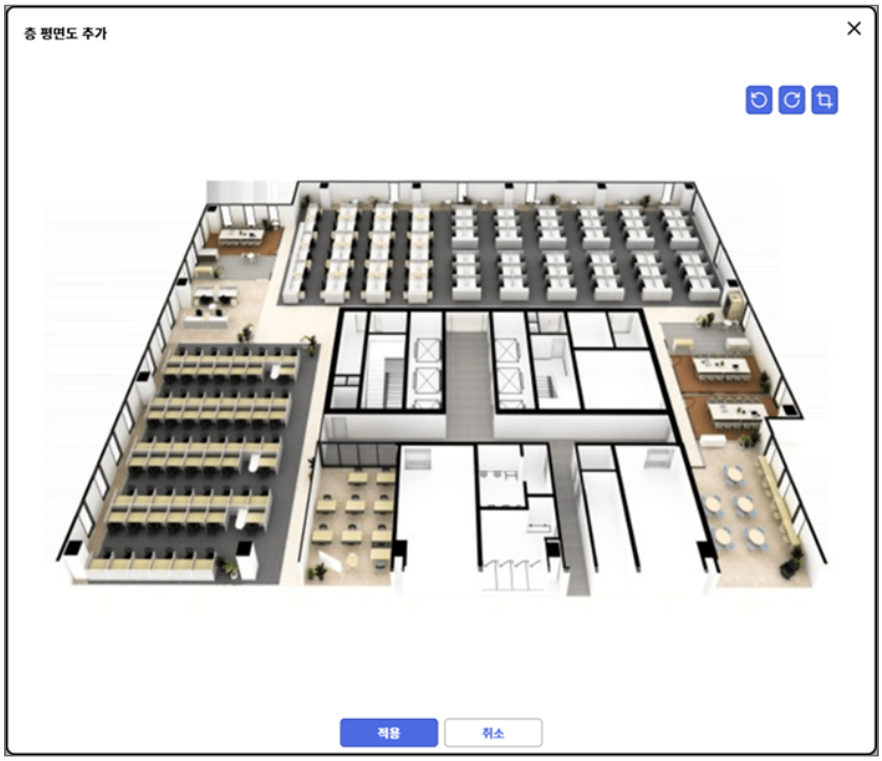
1. Click **Settings** on the **Launcher** page.
2. Click **Map** → **Floor** on the left sidebar.
3. Click **New Floor** in the upper right corner of the floor list screen.



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.

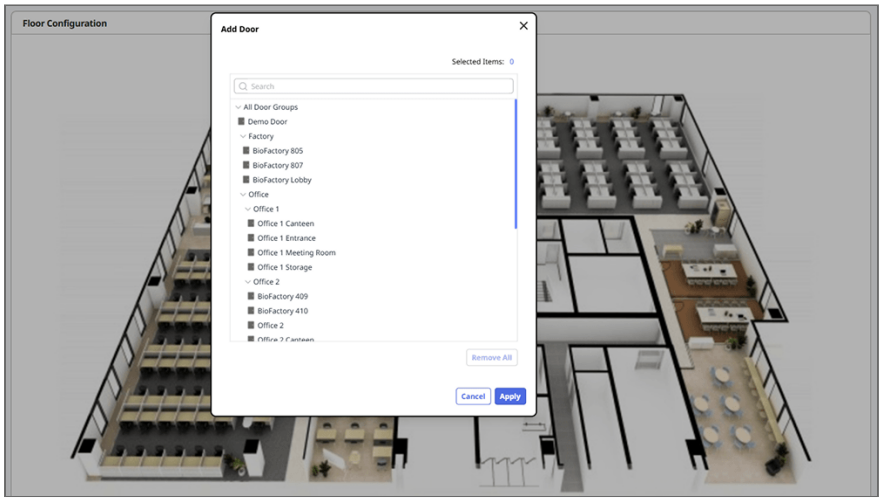
> Supported image formats are PNG, JPEG, and JPG.

6. Confirm the uploaded image in the **Add Floor Plan** window and proceed with the settings.

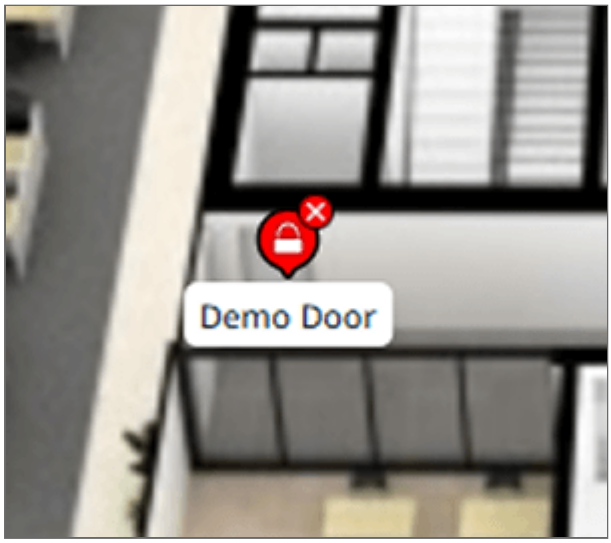


- To rotate the image, click ↺ or ↻.
- To crop the image, click ⧉.

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.

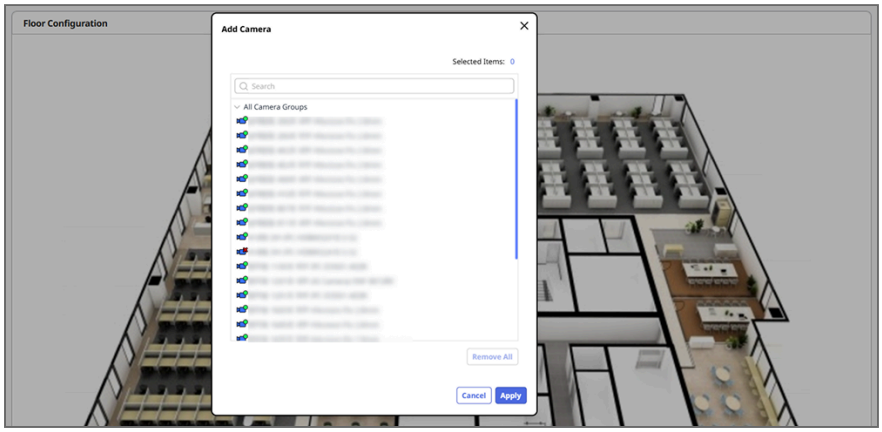


10. To place the door in the image, click **Apply**.



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. After completing all settings and saving the configured floor, click **Apply**.

> **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 on the floor, see Monitor Map.

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. On the left sidebar, click **Map** → **Floor**.
3. Click the floor you want to modify from the list.

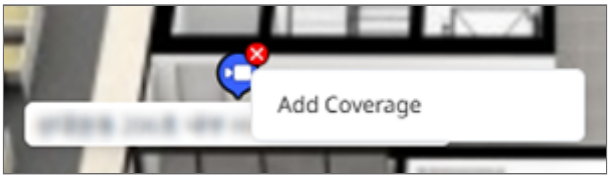
After completing all settings and saving the configured floor, click **Apply**.

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 coverage

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.

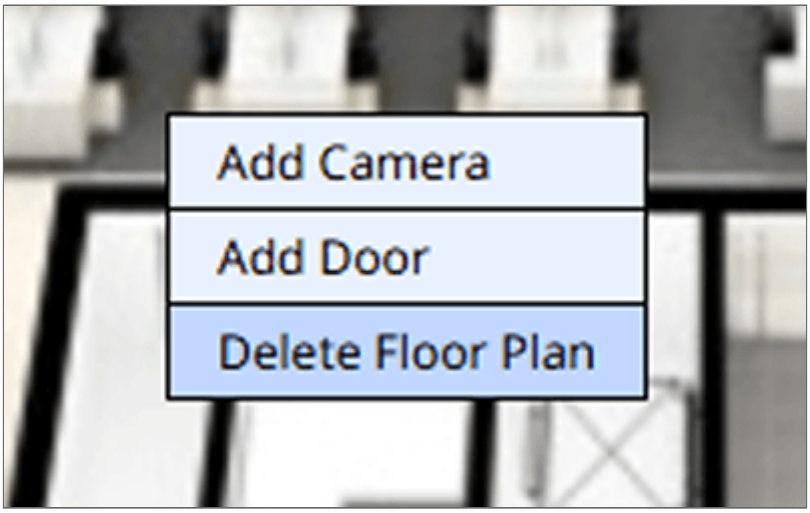


- To delete the coverage area, click the icon.

> **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.

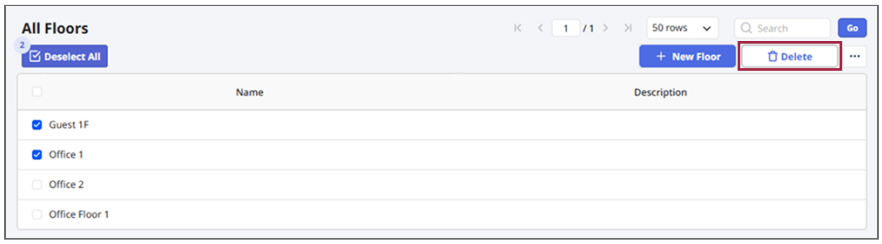
Delete floor image

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. Click **Map** → **Floor** on the left sidebar.
3. Click the checkbox of the floor you want to delete from the list. You can select more than one floor.

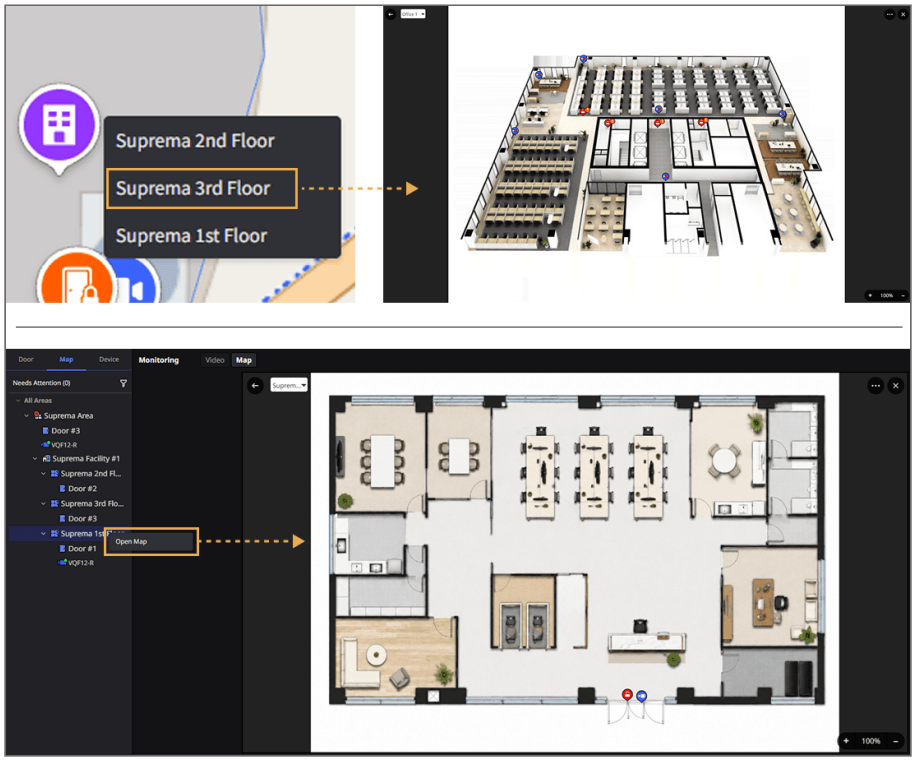


4. Click **Delete** at the top right of the screen.

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 on registering floors, see Configure Floors.
- For more information on map monitoring, see Monitor Map.
- The add and configure Facilities feature is available with an **Essential** license or higher. For more information on licensing policies, see License Policy.

Add facility

Follow these steps to design the structure by adding floors to the facility.

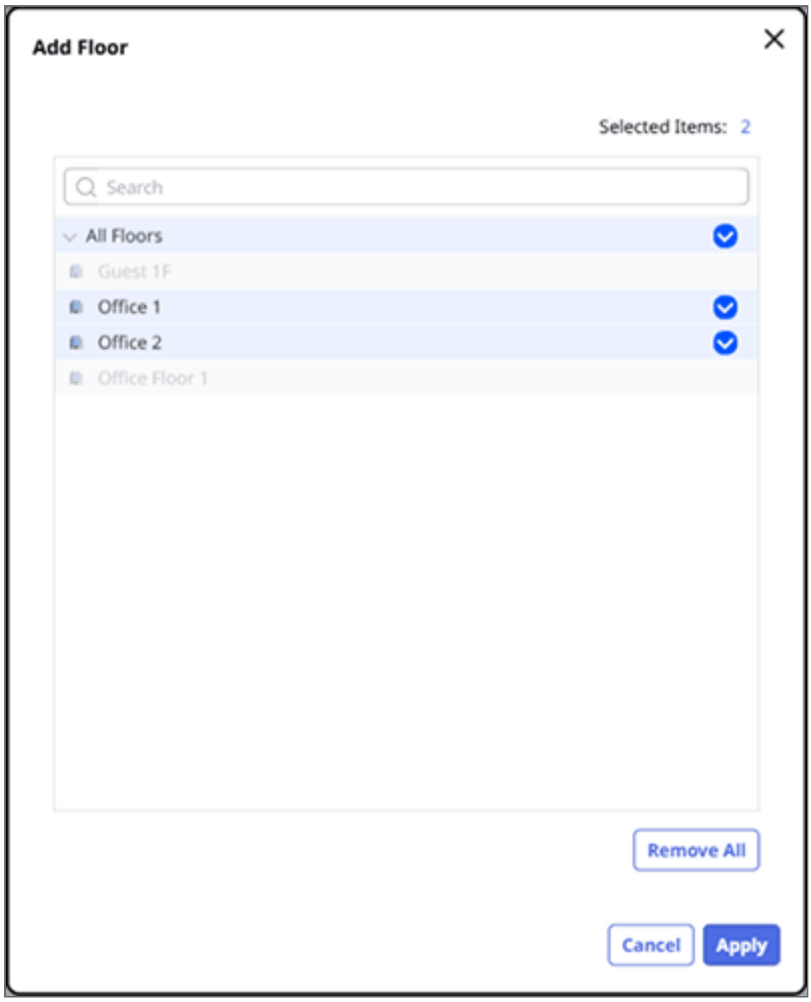
1. Click **Settings** on the **Launcher** page.
2. Click **Map** → **Facility** on the left sidebar.
3. Click **New Facility** in the upper right of the facility list screen.



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**.

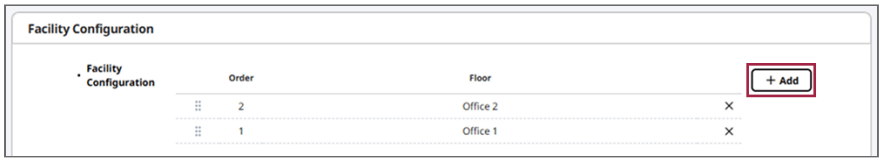
7. If you have selected all floors, click **Apply**.
8. To check the floors added to the access door list and change the order, drag ⠿ in the **Order** column to change the order.
9. To complete the facility configuration and save, click **Apply** at the bottom right of the screen.

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** on 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**.



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 ⠿ in the **Order** column to change the order.
8. To complete the facility configuration and save, click **Apply** 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** on the left sidebar.
3. Select the facility from which you want to delete floors in the facility list.
4. Click ✕ of the floor you want to delete in **Facility Configuration**.
5. To complete the floor deletion and save, click **Apply** at the bottom right of the screen.

Delete facility

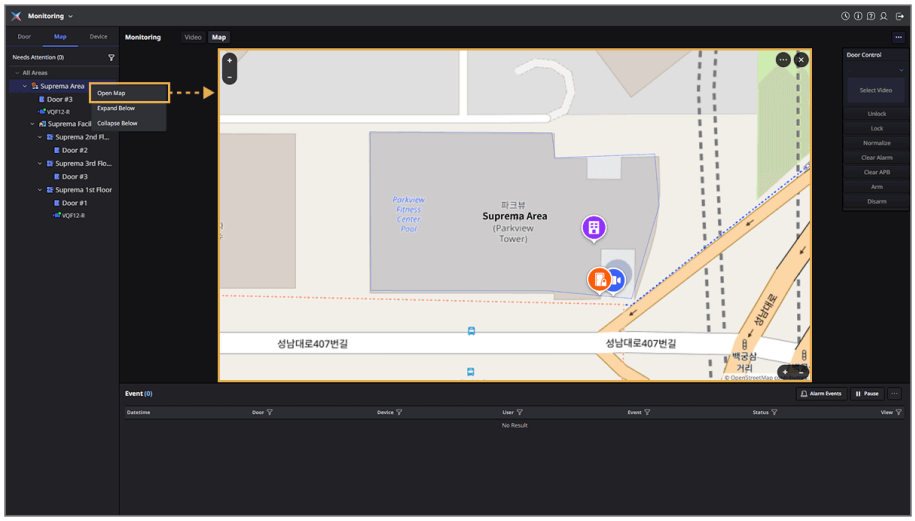
1. Click **Settings** on the **Launcher** page.
2. Click **Map** → **Facility** on the left sidebar.
3. Click the checkbox of the facility you want to delete in the facility list.



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 on map monitoring, see Monitor Map.
- The add zone and settings feature is available through additional options with an **Essential** license or higher. For more information on licensing policies, see License Policy.

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 **New Area** in the upper right of the area list screen.



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**.

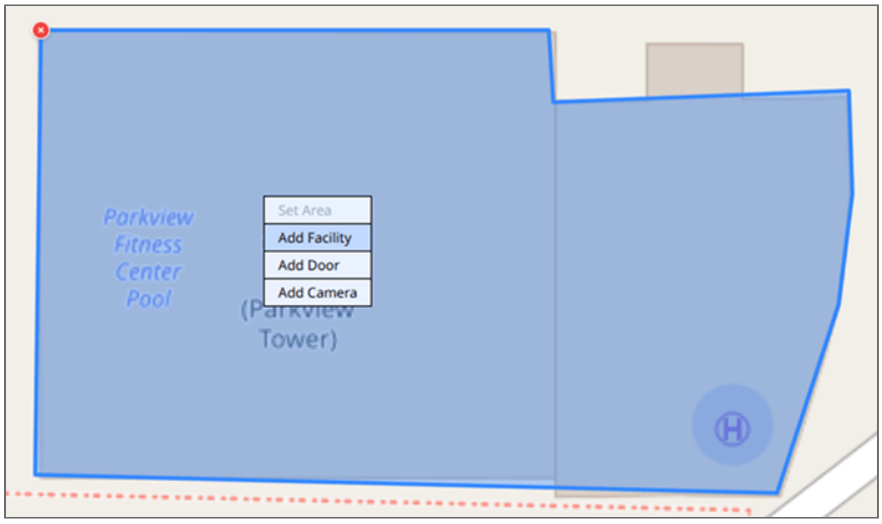


7. Set the zone in your desired shape. Click the mouse to start drawing and drag to set the zone.



> To reset the area, you must delete the configured area. To delete the area, click .

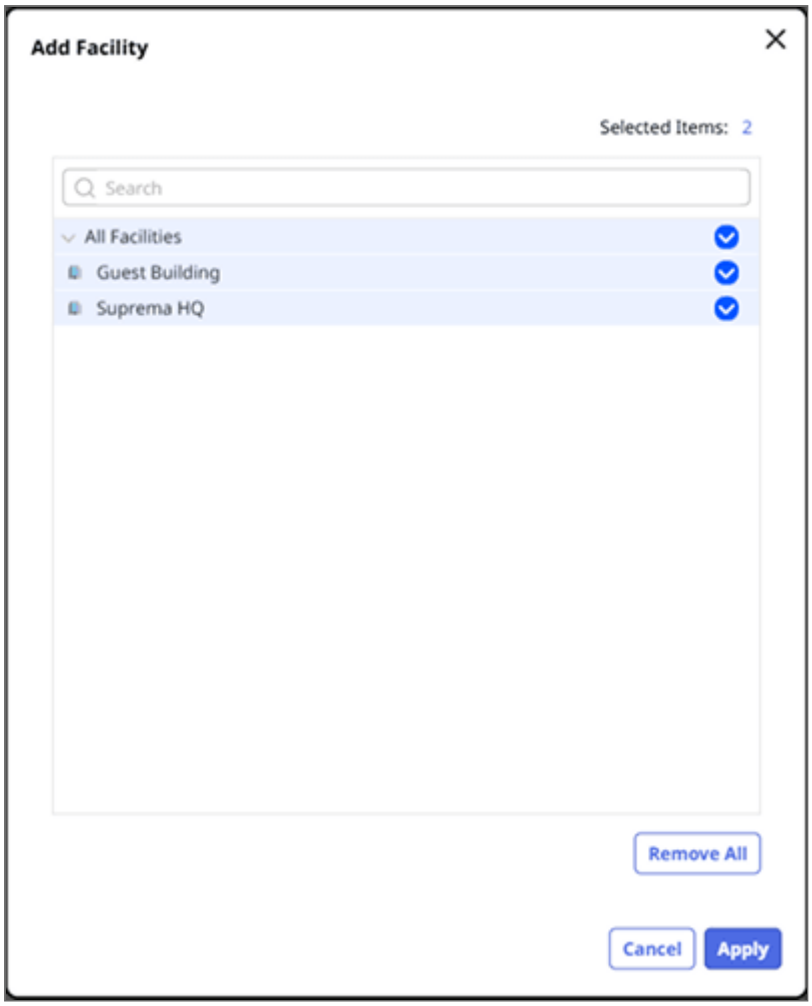
8. To add facilities to the configured area, right-click and select **Add Facility**.



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**.



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 **Apply** 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 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 **Apply** in the lower right of the screen.

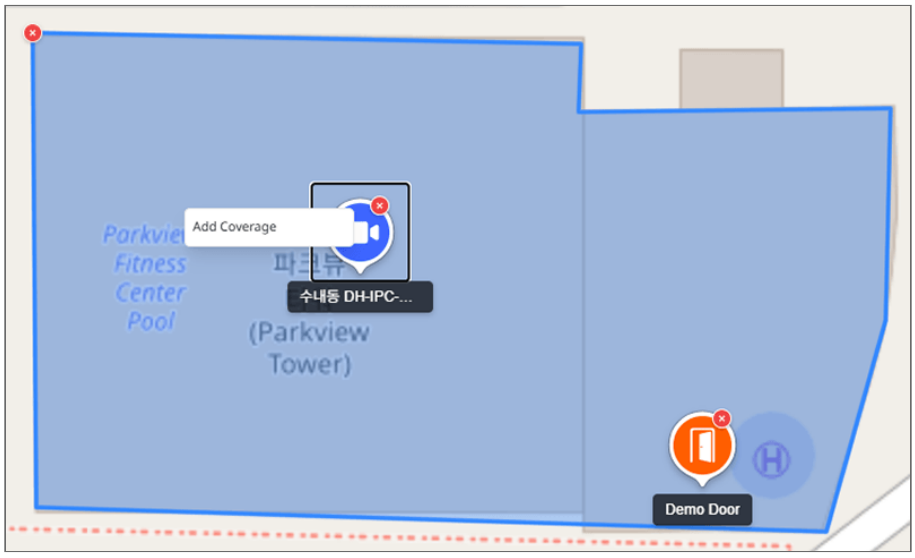
Delete facility/entrance/camera

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.

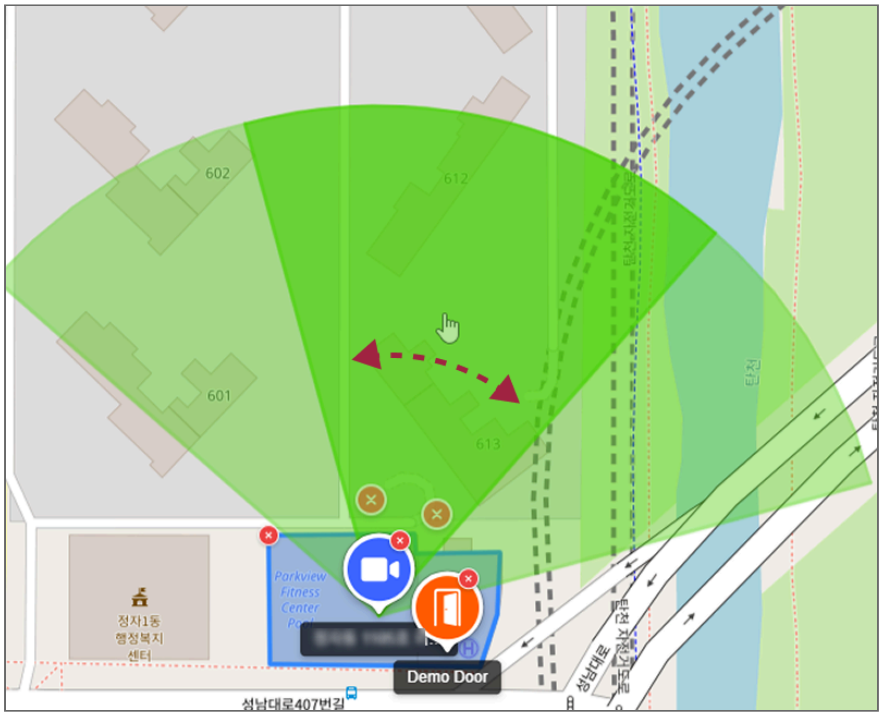


Set camera coverage

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**.

Visitor Settings

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.

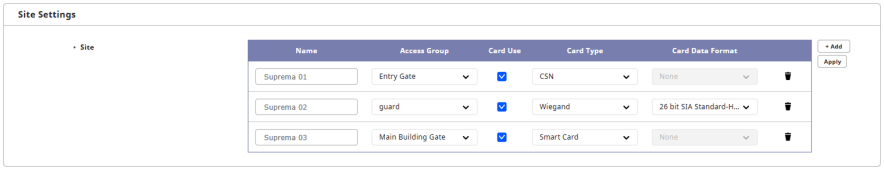
> **Info**
>
> - The **Visitor** setting is available as an additional option with an **Essential** license or higher. For more information on licensing policies, see License Policy.
> - Activate the **Automatic User Synchronization** or **Use Server Matching** option to use the **Visitor**. For more information, see Server Detailed Settings.

Visitor settings

1. Click **Settings** on the **Launcher** page.
2. Click **Visitor** → **Visitor** on the left sidebar.
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.



- **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.

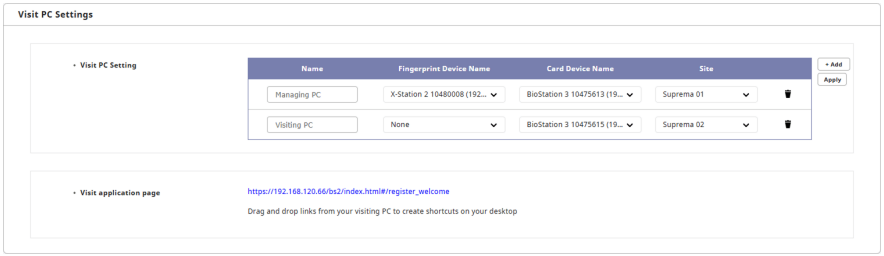
> **Info**
>
> Pre-setting access groups for visitors makes management easier. For more information on access group settings, see Manage Access Groups.

- **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.



- **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

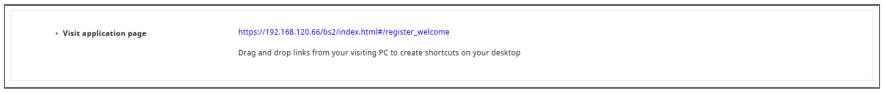
You can select the PC set in **Visit PC Setting** and assign it to the current PC.



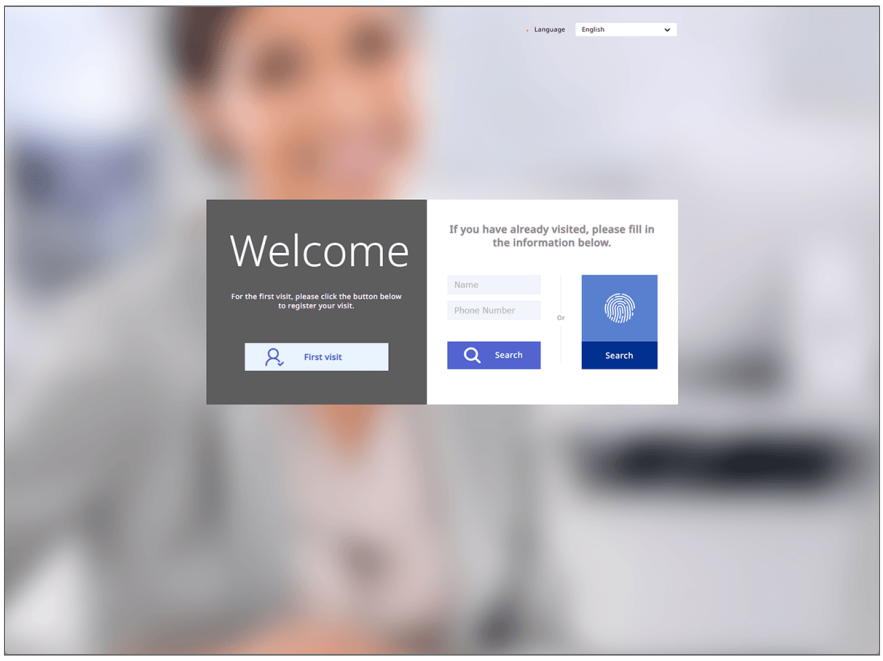
Click **Apply** to save the settings.

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.

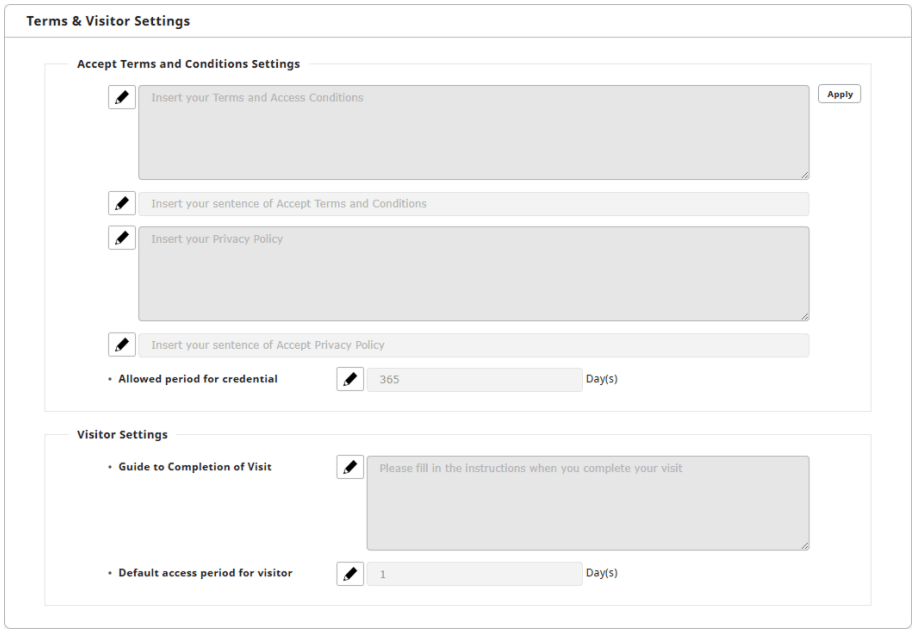


You can access the visitor application page by connecting to the URL in a web browser.



Set terms & visitor settings

You can manage key visitor settings such as terms of entry, privacy policy, and guidance messages.



- **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.

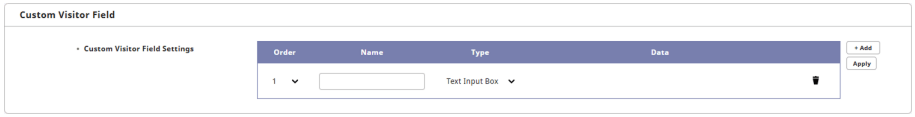
- **Guide to Completion of Visit**: You can set the guide to appear on the screen as a pop-up when a visitor completes an application for a visit. Click ✎ to activate the input field and enter the guide for visitors.

> **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.



- **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**.

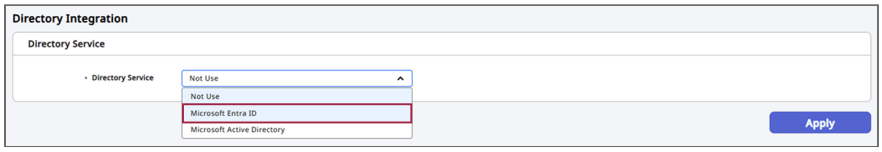
- You can map user information such as job title, department, and group used in **Entra ID** or **Active Directory** to the custom fields of **BioStar X**.

> **Info**
>
> The **Entra ID** or **Active Directory** settings feature is available as an add-on with the **Essential** license or higher. For more information on licensing policies, see License Policy.

Directory integration settings

Entra ID

1. Log in to **BioStar X** with an administrator account.
2. Click **Settings** on the **Launcher** page.
3. Click **System** → **Directory Integration** on the left sidebar.
4. Select **Microsoft Entra ID** in **Directory Service**.



5. Set each item as instructed below.

> **Info**
>
> To integrate with Entra ID, go to **System** → **Server** and set **User ID Type** to **Alphanumeric**.

1 Directory Server

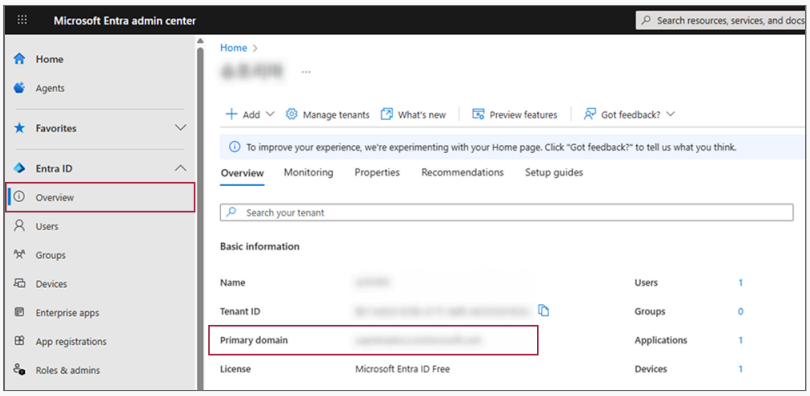
Enter the server information for **Entra ID** and click **Connect** in **Directory Server**.



- **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**.

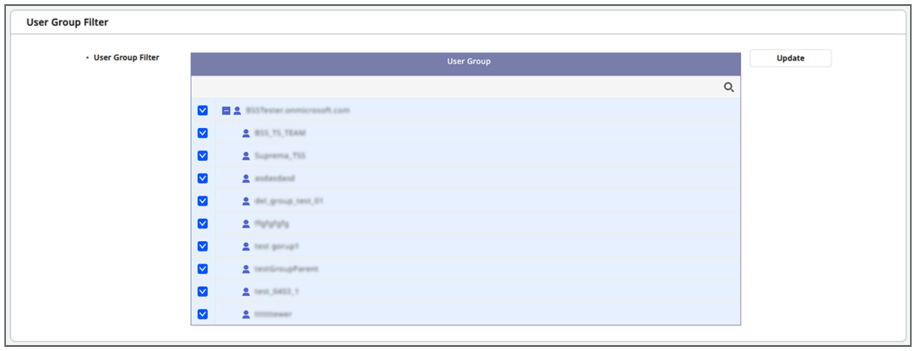
Info

- 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**.



1 User Group Filter

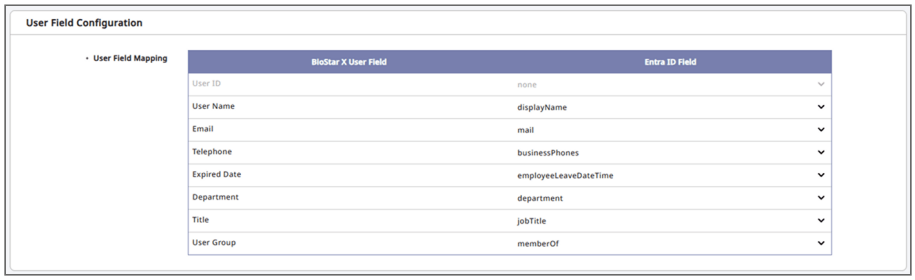
After completing the settings in **Directory Server** and clicking **Connect**, user group information from will be retrieved in **User Group Filter**. Deselect the user groups that will not sync with **BioStar X**.



- **Update**: Click to refresh the user group information.
- Click the icon to search for the desired user group.

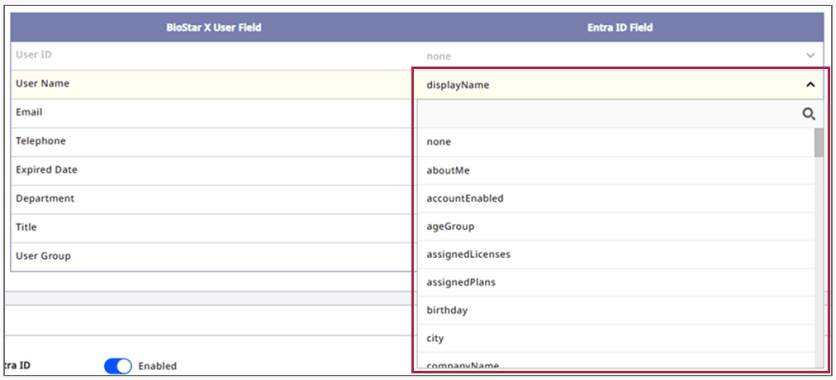
1 User Field Configuration

You can set the field for to map to the user fields of **BioStar X**. Select the field for to use as the user field for **BioStar X** in the **User Field Configuration** section.



Info

By default, **BioStar X** maps each user field to a matching user information field in . To use a field value other than the default, click an entry in the **Entra ID Field** column and select a different field value.

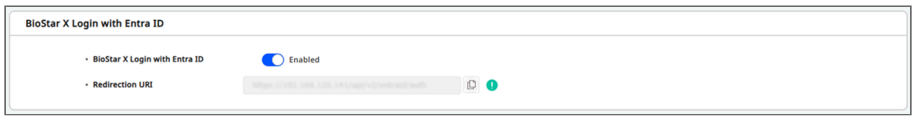


Caution

The **User ID** field cannot be mapped when integrating with **Entra ID**. **User ID** is automatically generated and applied by **BioStar X**.

1 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**.



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.

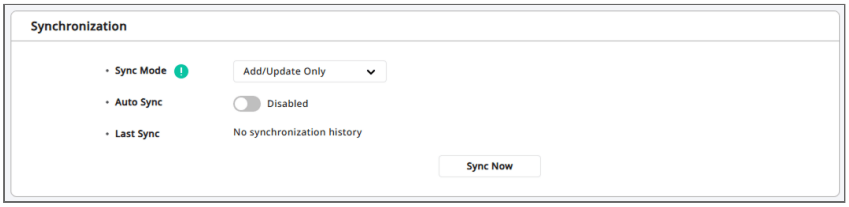
Info

- 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**.

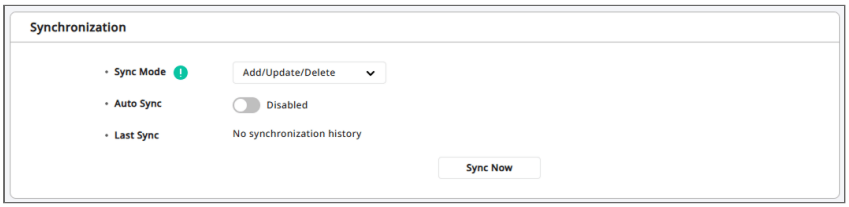
1 Synchronization

This feature allows you to synchronize user information changed in .

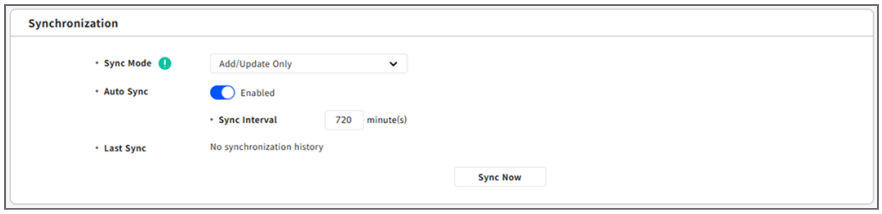
- **Sync Mode**: Select the desired synchronization mode.
  - **Add/Update Only**: When synchronizing users from the integrated directory service, add users who are not in **BioStar X** and update users whose information has changed. However, the following users will not be deleted.
    - Users registered only in **BioStar X**
    - Users deleted from



  - **Add/Update/Delete**: Synchronize **BioStar X** user information to match the integrated directory service exactly. Synchronizes users, including those registered only in **BioStar X** and those deleted from , to keep the data identical on both sides.



- **Auto Sync**: Set the automatic synchronization interval. Synchronization runs automatically at the interval set in **Sync Interval**. Enter the interval in minutes. The minimum value is **30** minutes, and the maximum value is **10,080** minutes (7 days).



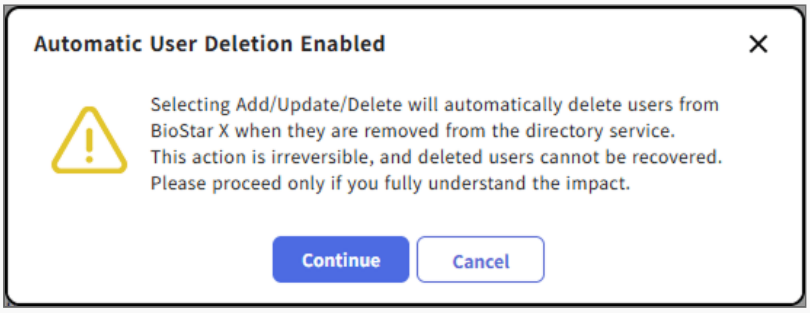
- **Last Sync**: You can check the date and time of the most recent synchronization.

Caution

- When using **Add/Update Only** mode, if a group with the same name exists, it is retained rather than deleted.
- **Add/Update/Delete** mode:
  - **If a group with the same name already exists**: the group is not created, and the existing group's information is retained. However, all users in that group are removed and then re-added to reflect the directory service's latest information. However, users in that group who share the same name are retained.
  - **Users created in BioStar X**: Users created directly in **BioStar X** are not linked to the directory service. When synchronizing, update these users so their information is linked to the directory service.
  - **Limitations**: After synchronization, if a group with the same name already exists, that group's information and members may not synchronize properly.
- If you upgrade to **BioStar X v1.0.2** with directory integration enabled, the synchronization mode defaults to **Add/Update/Delete**.

Info

- Each time you click **Sync Now**, user information is synchronized with the directory service using the selected synchronization mode.
- When you select **Add/Update/Delete** mode, a warning message will appear. To continue, click **Continue**. To cancel, click **Cancel**.



- To exclude specific users from synchronization when integrating, see Exclude from directory integration.
- If a synchronized user identifier or user name contains characters that **BioStar X** does not allow, register it with only those characters removed. However, a period (.) in a user ID and a period (.) or apostrophe (') in a username remain unchanged. For more information on disallowed characters, see User ID and name entry rules.

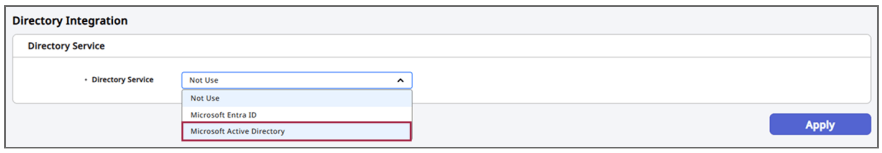
1 Save Settings

After completing all settings for **Directory Integration**, click **Apply** at the bottom of the screen to save. To view the settings results, see Check settings results.

Active Directory

1. Log in to **BioStar X** with an administrator account.
2. Click **Settings** on the **Launcher** page.
3. Click **System** → **Directory Integration** on the left sidebar.

4. Select **Microsoft Active Directory** in **Directory Service**.



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 integrate with Active Directory, go to **System** → **Server** and set **User ID Type** to **Alphanumeric**.

1 Directory Server

Enter the server information for **Active Directory** and click **Connect** in **Directory Server**.



- **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:

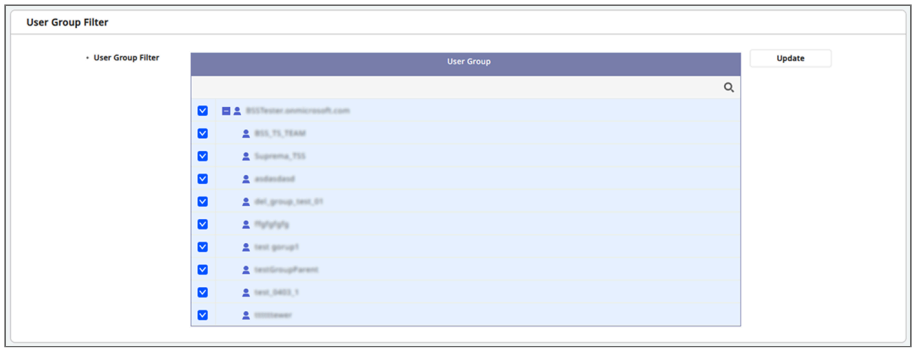
  1. Run the **Active Directory Administrative Center**.
  2. Right-click on the node where user data is stored, and then click **Property**.
  3. In the **property** window, select **Expand** and then click **Attribute Editor**.
  4. View the value of **distinguishedName**.

- **Secure Transfer**: You can use encryption when communicating with the Windows Active Directory server. To install Active Directory Certificate Services and configure the **Keystore Password**, see Active Directory Encryption.

  – **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**.

1 User Group Filter

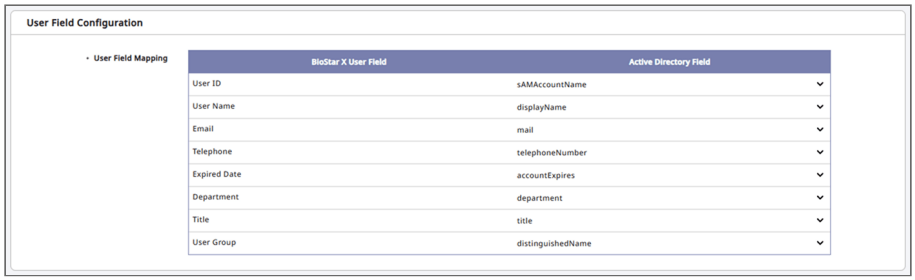
After completing the settings in **Directory Server** and clicking **Connect**, user group information from will be retrieved in **User Group Filter**. Deselect the user groups that will not sync with **BioStar X**.



- **Update**: Click to refresh the user group information.
- Click the 🔍 icon to search for the desired user group.

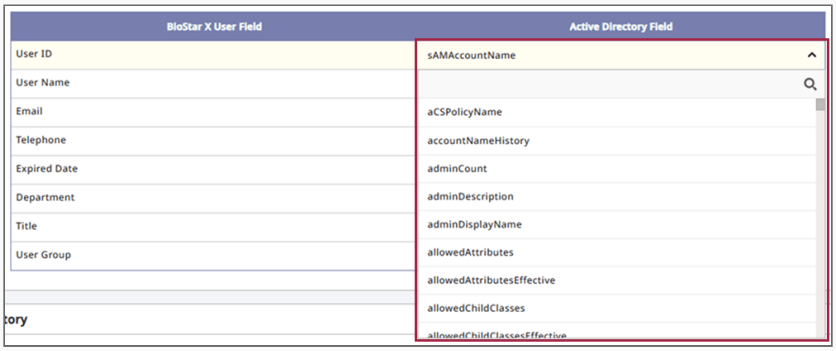
1 User Field Configuration

You can set the field for to map to the user fields of **BioStar X**. Select the field for to use as the user field for **BioStar X** in the **User Field Configuration** section.



Info

By default, **BioStar X** maps each user field to a matching user information field in . To use a field value other than the default, click an entry in the **Active Directory Field** column and select a different field value.



1 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

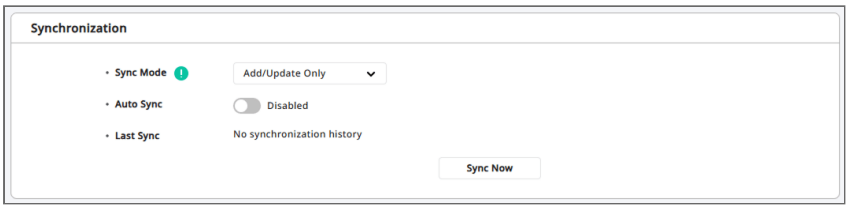
The sAMAccountName field cannot contain special characters. You may fail to log in if it does not comply with the login ID policy of **BioStar X**.



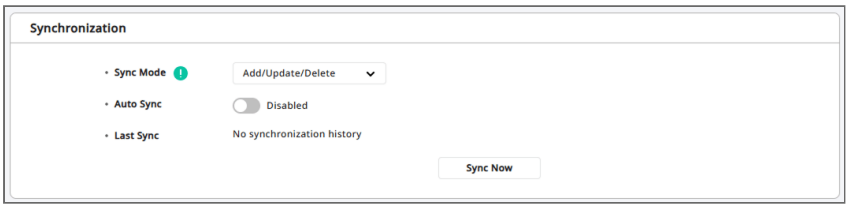
1 Synchronization

This feature allows you to synchronize user information changed in .

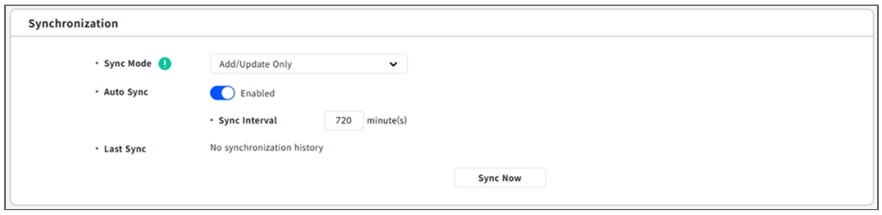
- **Sync Mode**: Select the desired synchronization mode.
  - **Add/Update Only**: When synchronizing users from the integrated directory service, add users who are not in **BioStar X** and update users whose information has changed. However, the following users will not be deleted.
    - Users registered only in **BioStar X**
    - Users deleted from



  - **Add/Update/Delete**: Synchronize **BioStar X** user information to match the integrated directory service exactly. Synchronizes users, including those registered only in **BioStar X** and those deleted from , to keep the data identical on both sides.



- **Auto Sync**: Set the automatic synchronization interval. Synchronization runs automatically at the interval set in **Sync Interval**. Enter the interval in minutes. The minimum value is **30** minutes, and the maximum value is **10,080** minutes (7 days).



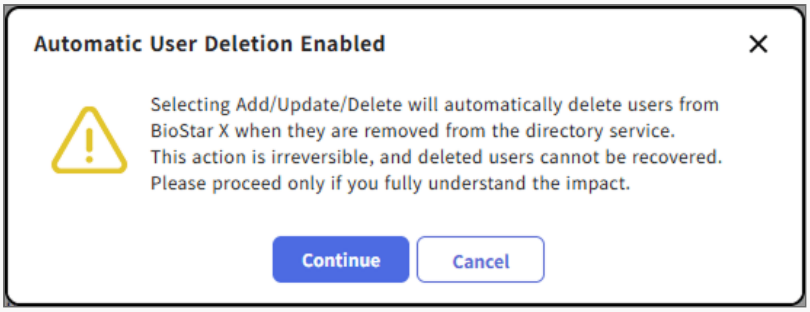
- **Last Sync**: You can check the date and time of the most recent synchronization.

Caution

- In **Add/Update Only** mode, user groups with the same name and users with the same user ID are not deleted; they are retained.
- **Add/Update/Delete** mode:
  - **If a group with the same name already exists**: the group is not created, and the existing group's information is retained. However, all users in that group are removed and then re-added to reflect the directory service's latest information. However, users in that group who share the same name are retained.
  - **Users created in BioStar X**: Users created directly in **BioStar X** are not linked to the directory service. When synchronizing, update these users so their information is linked to the directory service.
  - **Limitations**: After synchronization, if a group with the same name already exists, that group's information and members may not synchronize properly.
- If you upgrade to **BioStar X v1.0.2** with directory integration enabled, the synchronization mode defaults to **Add/Update/Delete**.

Info

- Each time you click **Sync Now**, user information is synchronized with the directory service using the selected synchronization mode.
- When you select **Add/Update/Delete** mode, a warning message will appear. To continue, click **Continue**. To cancel, click **Cancel**.



- To exclude specific users from synchronization when integrating, see Exclude from directory integration.
- If a synchronized user identifier or user name contains characters that **BioStar X** does not allow, register it with only those characters removed. However, a period (.) in a user ID and a period (.) or apostrophe (') in a username remain unchanged. For more information on disallowed characters, see User ID and name entry rules.

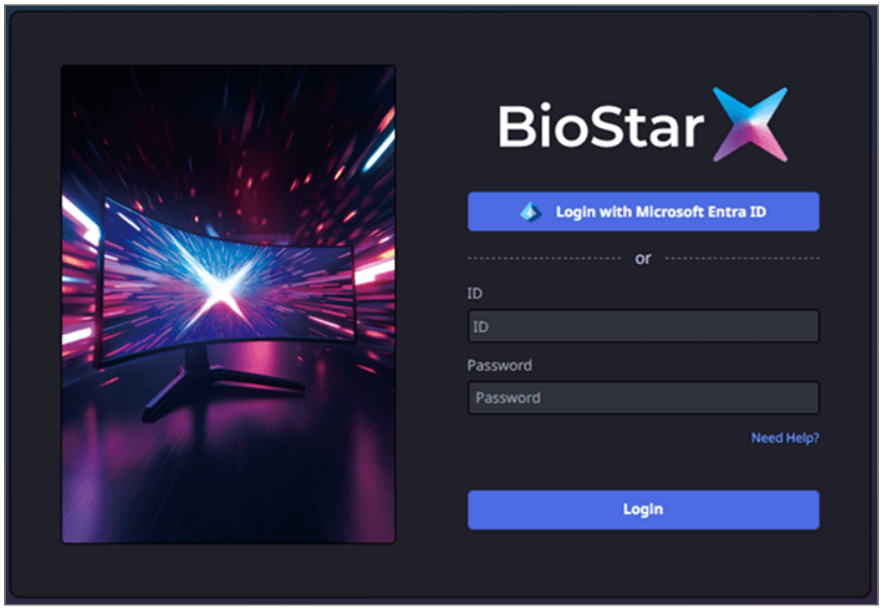
1 Save Settings

After completing all settings for **Directory Integration**, click **Apply** at the bottom of the screen to save. To view the settings results, see Check settings results.

Check 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**.



Handle unsupported characters

If a user ID or name in **Entra ID** or **Active Directory** includes unsupported characters, the system synchronizes the user after removing them.

> *For example, if a directory service user id is `john/doe` and the user name is `John<Doe>`, **BioStar X** registers them as `johndoe` and `JohnDoe`.*

Info

- The system excludes periods(`.`) and apostrophes(`'`) in user names from unsupported characters and saves the original directory service values.

  > *Example: `O'Brien`, `John.Doe` → Saved with the original directory service values*

- The system excludes periods(`.`) from unsupported characters in user IDs and saves the original directory service values, but removes apostrophes(`'`) because user IDs cannot include them.

  > *Directory service user ID examples:*
  >
  > – `O'Brien` → *Saved as* `OBrien`
  >
  > – `john.doe` → *Saved as* `john.doe`

- For more information about user ID and name input rules, see Enter Basic User Information.

Exclude from 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 selected user's details screen appears, in the **Advanced** section, enable the **Exclude from Directory Integration** option.



5. Click **Apply**.

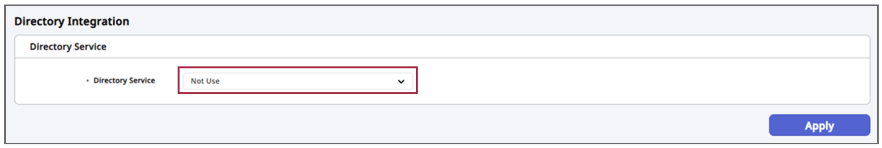
The selected users will be excluded from integration when using the **Directory Integration** feature.

> **Info**
>
> The system automatically excludes these users from integration.
>
> - When a user name starts with `&@~` consecutively at the beginning
> - User id or user name is blank
> - The user ID (up to 32 characters) or user name (up to 48 characters) exceeds the length limit
> - user id matches a system-reserved value, such as `admin`
> - The user ID is a single period (`.`) or two periods (`..`)

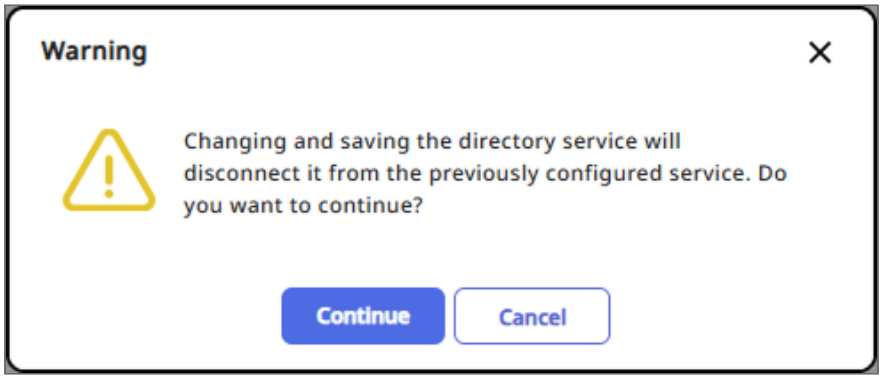
Disable directory integration

To disable the **Directory Service** feature, follow the steps:

1. Log in to **BioStar X** with an administrator account.
2. Click **System** → **Directory Integration**.
3. Select **Not Use** in **Directory Service**.



4. When the **Warning** message appears, click **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.

Remote Access Settings

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 more information on licensing policies, see License Policy. The remote access license is an annual subscription.
- 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. 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** on 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, see BioStar X License.

2 Activate remote access

1. Log in with your **BioStar X** admin ID.
2. Click **Settings** on the **Launcher** page.
3. Click **System** → **Remote Access** on the left sidebar.
4. In the **Remote Access with ngrok** section, change the **Remote Access** option to **Use**.



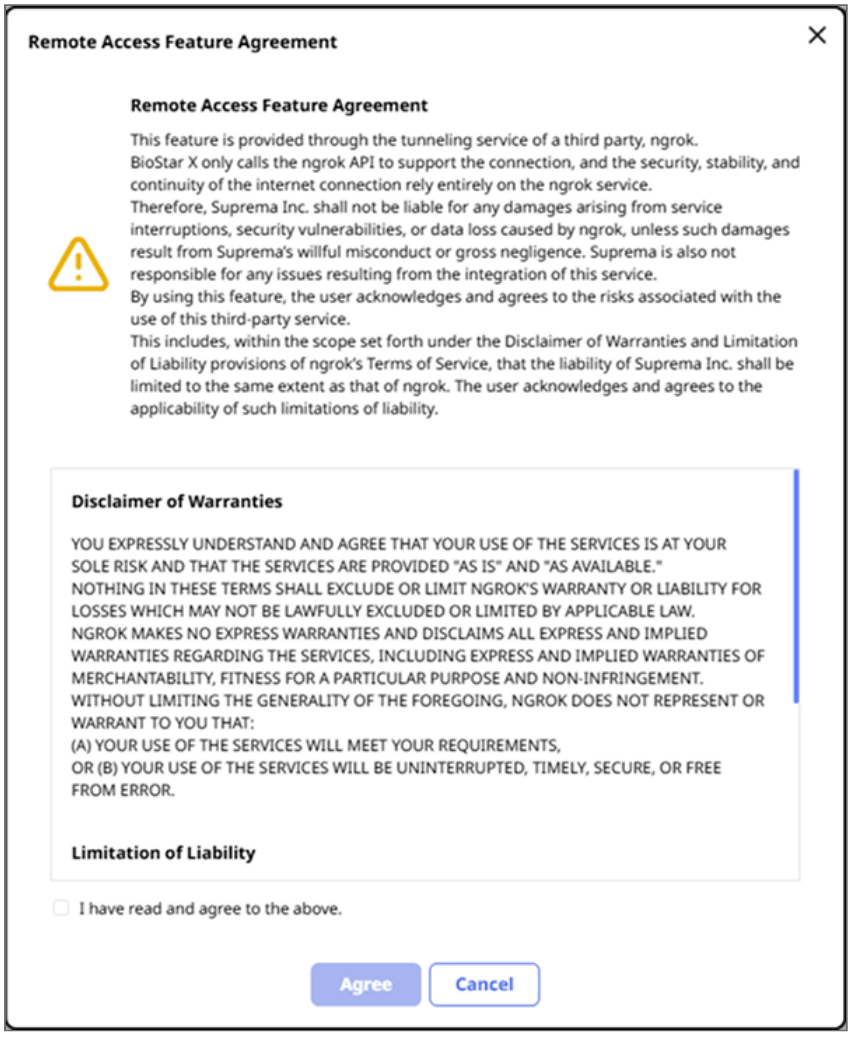
3 Enter ngrok setup information

Enter the ngrok setup information provided by Suprema.

- **Authtoken**: Enter your **Authtoken**.
- **URL**: Enter the endpoint URL. The URL is in the format `https://subdomain.bsx.ngrok.app`.

> **Info**
>
> The subdomain (`subdomain`) must follow the rules below. Subdomains that do not comply with the rules cannot be used.
>
> - Only English letters (A-Z, a-z), numbers (0-9), and hyphens (`-`) are allowed.
> - Special characters and spaces are not allowed.

1. After entering all the information, click **Apply**.
2. When the **Remote Access Feature Agreement** window appears, review the contents.



3. Select the checkbox to agree to the terms, then click **Agree**.

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

- After connecting to the endpoint URL, go to **Settings** → **Audit Trail** → **AC Audit Log** to check access logs.

  > *Example: [Remote Access] 192.168.1.100*

- 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 you start

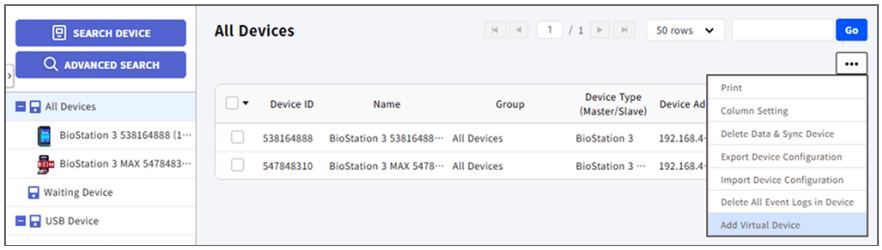
The **Event Log API** license must be activated. For more information on licensing policies, see License Policy.

Info

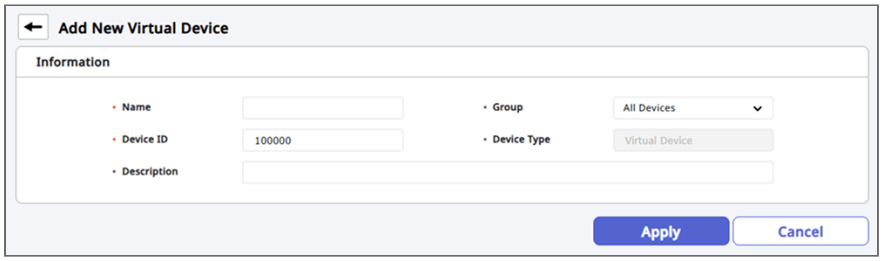
For more information on applying licenses, see BioStar X License.

Register virtual device

1. Click **Settings** on the **Launcher** page.
2. Click **Device** → **Device** on the left sidebar.
3. Click ••• at the top right of the device list and select **Add Virtual Device**.



4. Enter the setting information when the **Add Virtual Device** screen appears.



- **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, see Manage Device Groups.

Virtual device limitations

- Virtual devices appear only in the following menu.
  - **Settings** → **Device** → **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"
    },
    {
      "dev_id": 100003,
      "evt": 6400,
      "datetime": "2025-08-21T14:13:01Z",
      "user_id": "2",
      "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 the API, see the BioStar X API.

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 on viewing events in the **Monitoring** menu, see Monitor Event.
- For more information on the **Data** menu, see Generate Report.

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**, see Manage Audit Trail.

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, see License Policy.
> - For more information on developing plugins, see BioStar X Plugin Developer Guide.

BioStar X plugins

List of plugins available through the license add-on option.

- How to Use Time & Attendance
- Manage Visitors

> **Info**
>
> For more information on licensing policies, see License Policy.

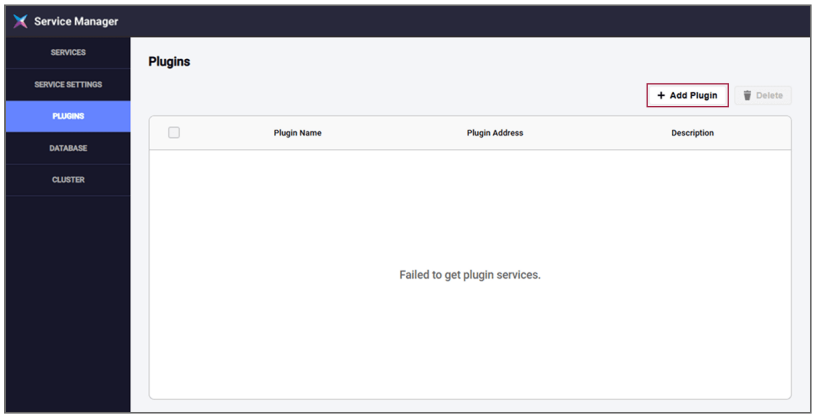
Key use cases

You can integrate various external systems through the **BioStar X** plugins system. The representative use cases are as follows.

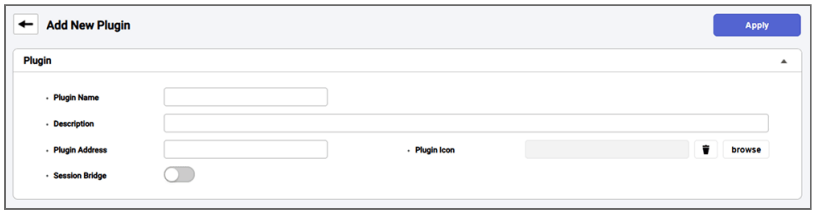
- **Attendance Management System**: Integration with external T&A (Time & Attendance) solutions
- **Visitor Management System**: Integration with separate visitor registration and management systems
- **Reporting Solution**: Integration with customizable reporting and analysis tools
- **Third-Party System 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.

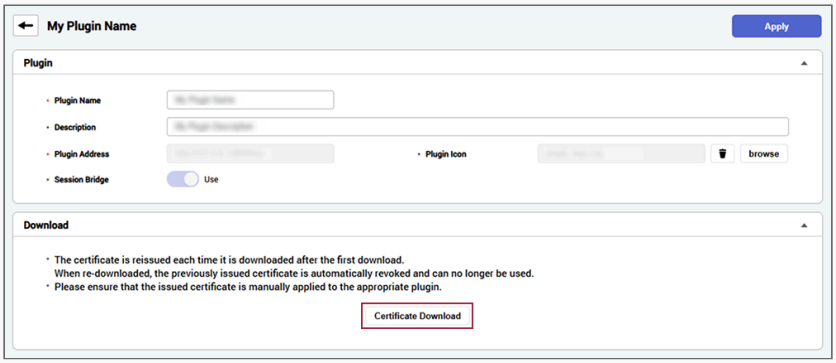


4. Enter plugin information on the **Add New Plugin** screen.



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.



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**.



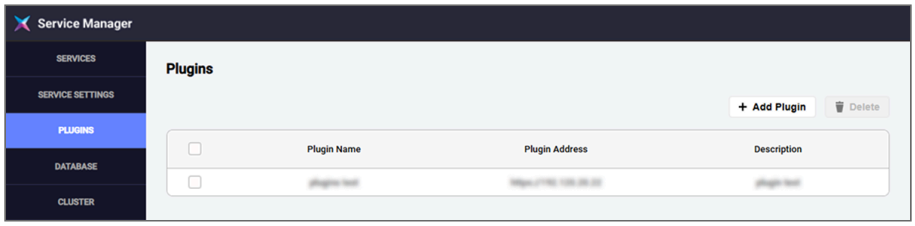
Plugin management

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.

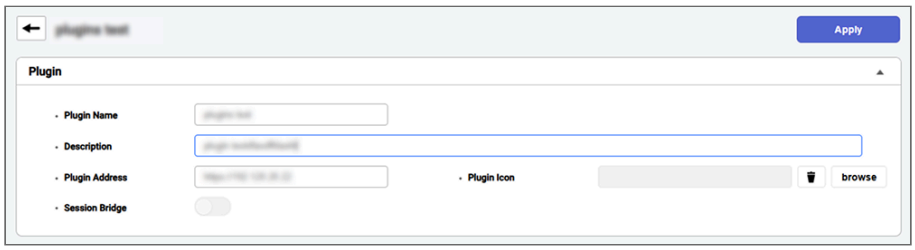
Check plugin list

You can see all the plugins registered by the user.



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 **Delete** in the upper right corner of the screen.
3. When the confirmation message appears, click **OK**.

> **Info**
>
> - The time and attendance (T&A) plugin added with the time and attendance license cannot be deleted.
> - The time and attendance management plugin is available as an additional option. For more information on licensing policies, see License Policy.

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 is available through an add-on option. For more information on licensing policies, see License Policy.

Before you 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** on the left sidebar.
4. Enter **License Activation** in sequence with **Activated by** and **License Key**.



5. Click **Activate**.

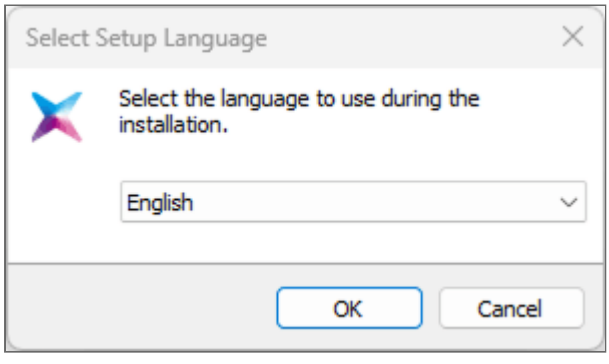
You can check the licensed registered in **Activated License**.

> **Info**
> To activate your license in a closed network environment or when internet access is restricted or unavailable, see BioStar X License.

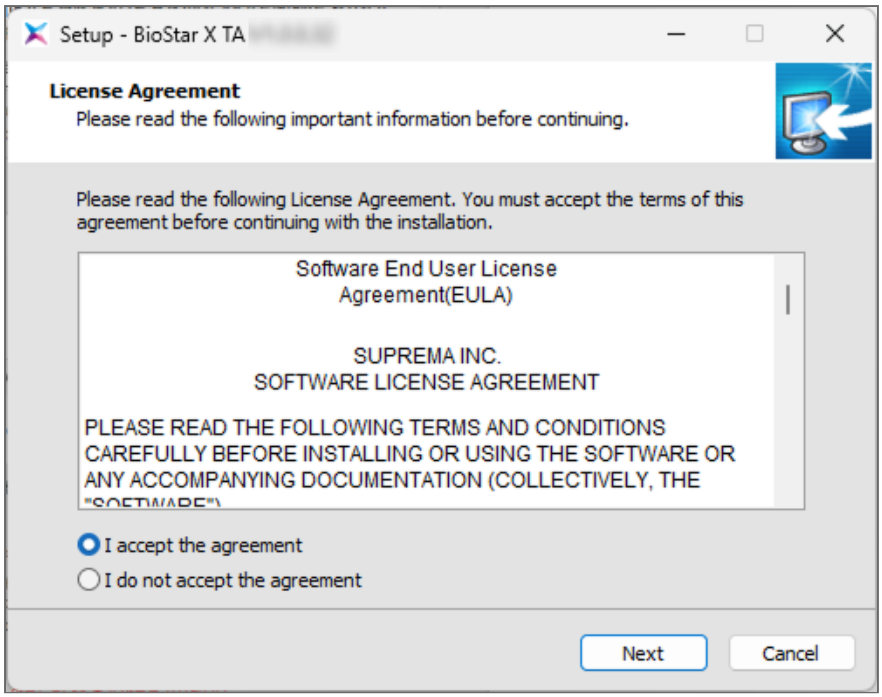
Install plugin

To use the T&A feature, a separate installation file must be downloaded and installed. Follow the instructions to install the plugin.

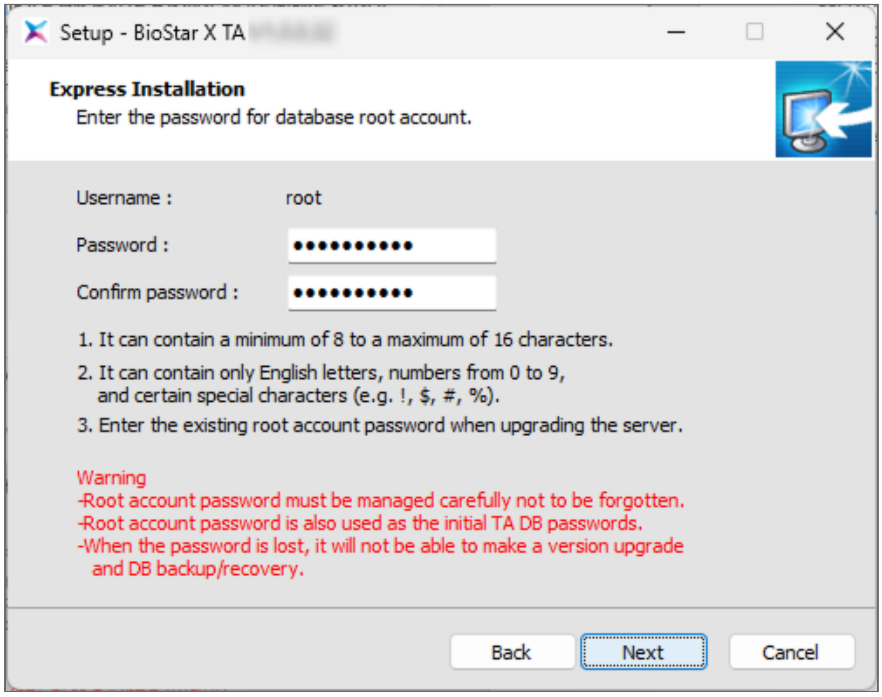
1. Access the Suprema Download Center and download the T&A plugin installation file (*BioStar X TA.X.Y.Z.BB.exe*).
2. Run the installation file and complete the installation according to the instructions.
3. Run the downloaded installation file.
4. Select the language to use and select the **OK** button.



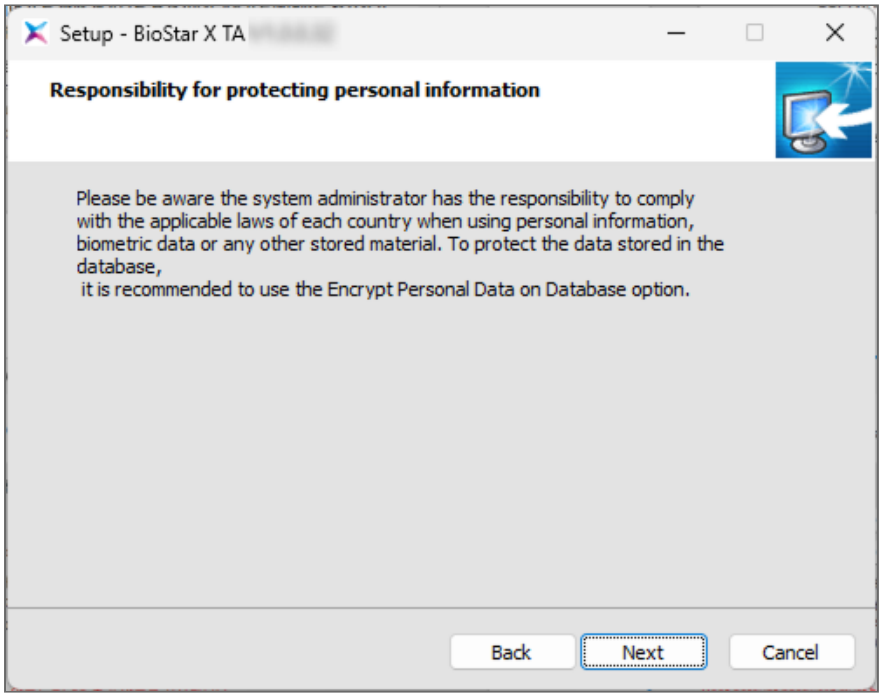
5. To continue the installation, select **I accept the agreement** and click the **Next** button.



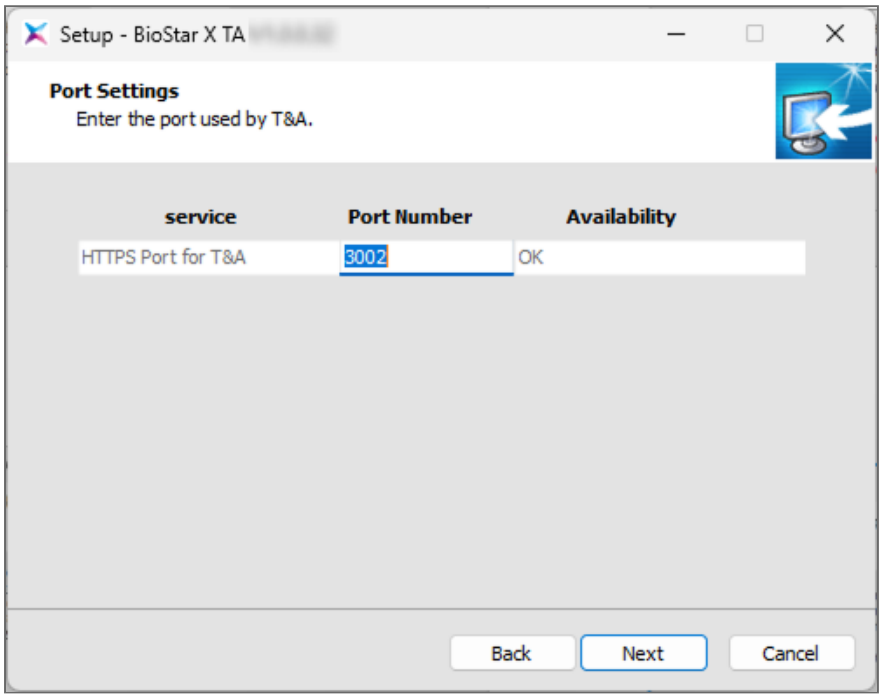
6. Enter the root account password for the database and click the **Next** button.



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.

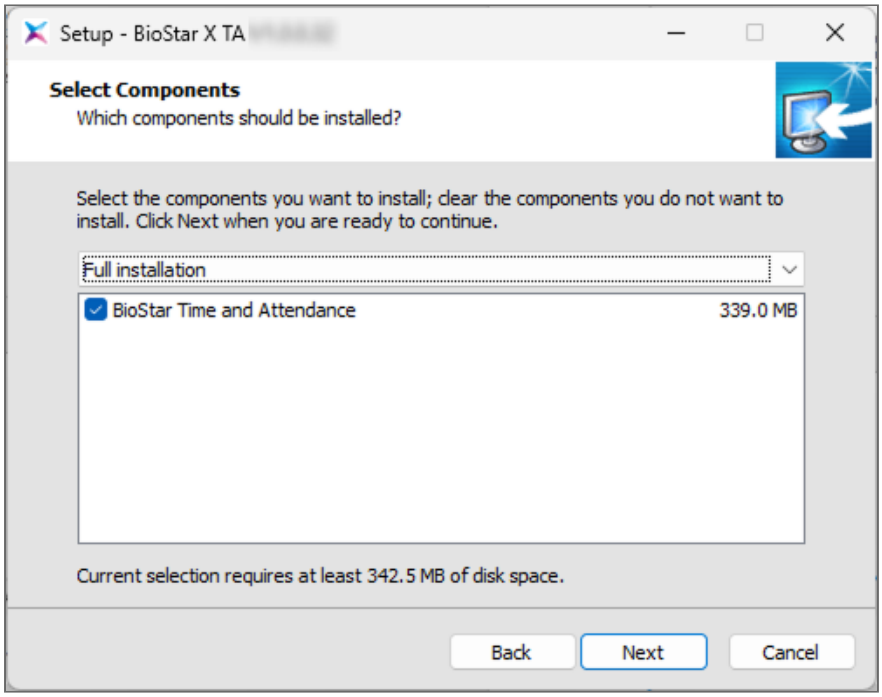


8. Set the port for communication with **BioStar X** and click **Next**.

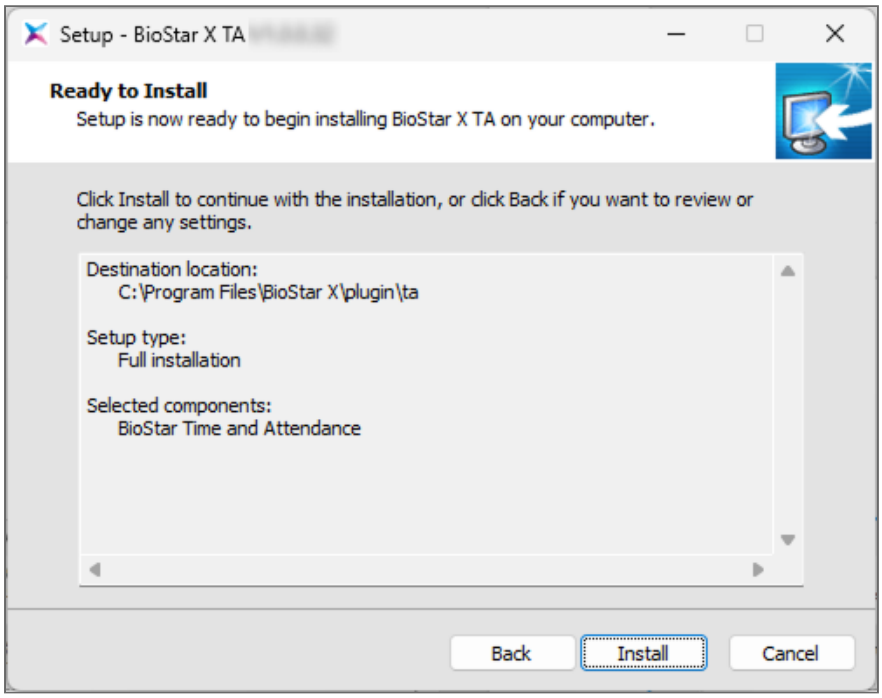


> You can use the default port number (3002) or change to a different port number. If you change the port number, ensure that the corresponding port is open in the firewall.

9. Select the installation components and click **Next**.



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

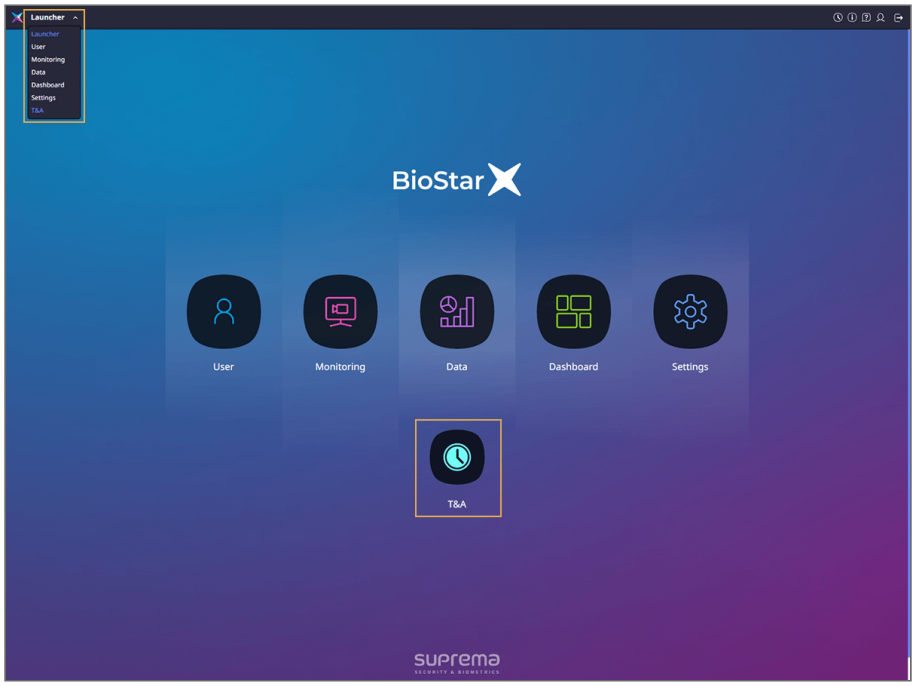


Info

- 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

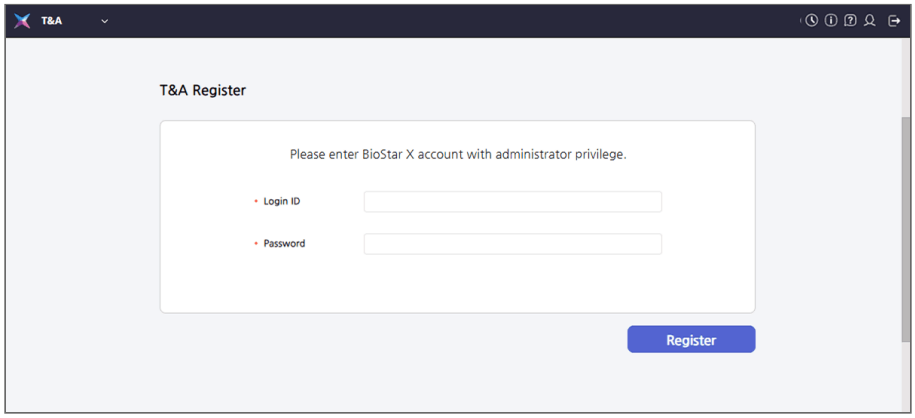
Once the T&A license and plugin installation are complete, the **Launcher** page will have the **T&A** menu added.



Click the **T&A** icon on the **Launcher** page or select **T&A** from the shortcut list at the top left of the screen.

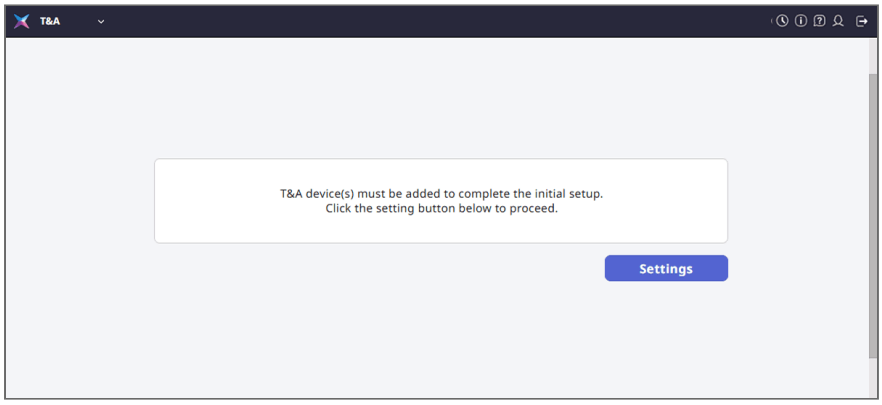
T&A login

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.

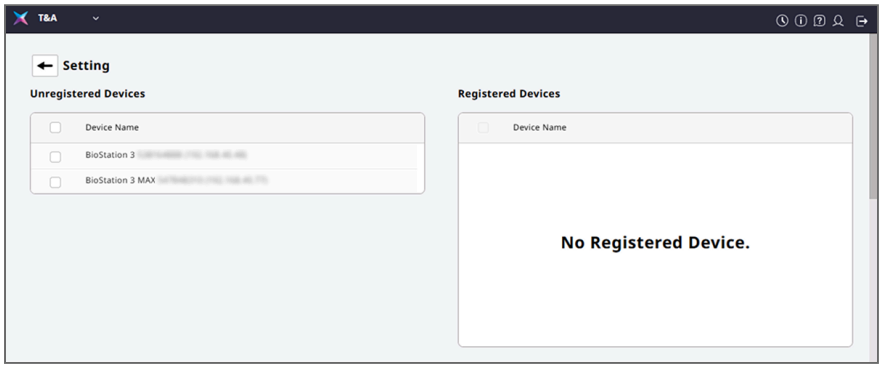


Initial setup

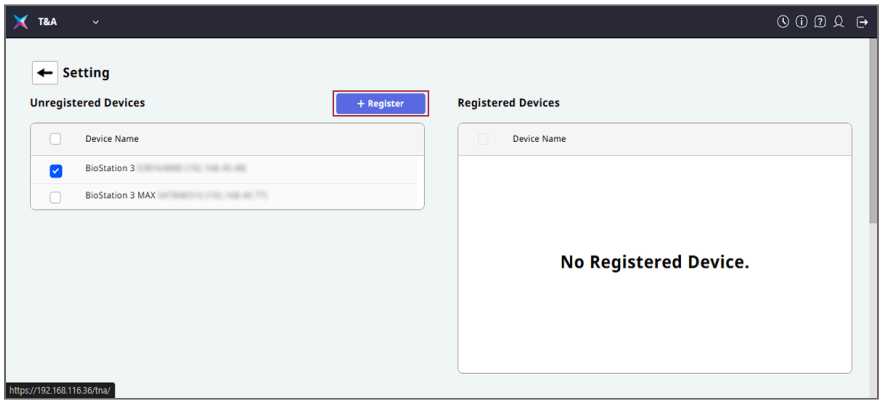
1. The first time you log into the T&A feature, you need to add a device for attendance management for initial setup. Click the **Settings** button on the screen.



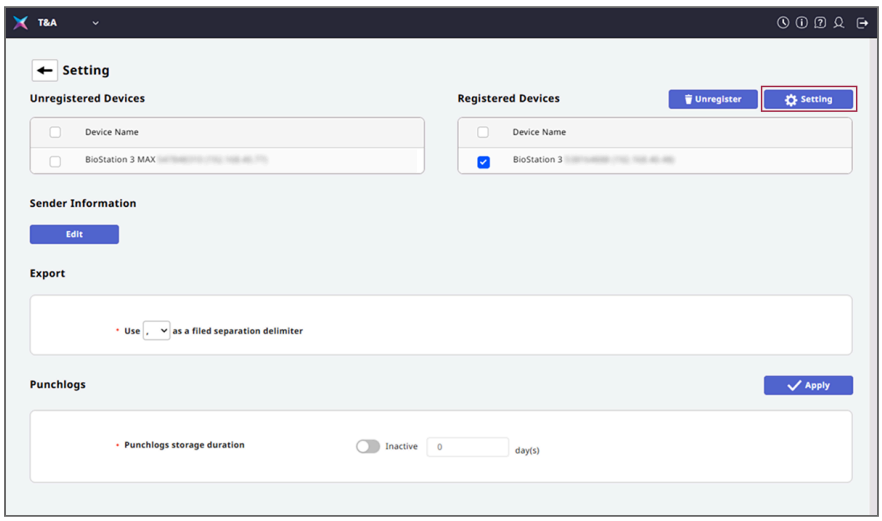
2. Select a device for attendance management from the device list.



3. Click the activated + **Register** button.



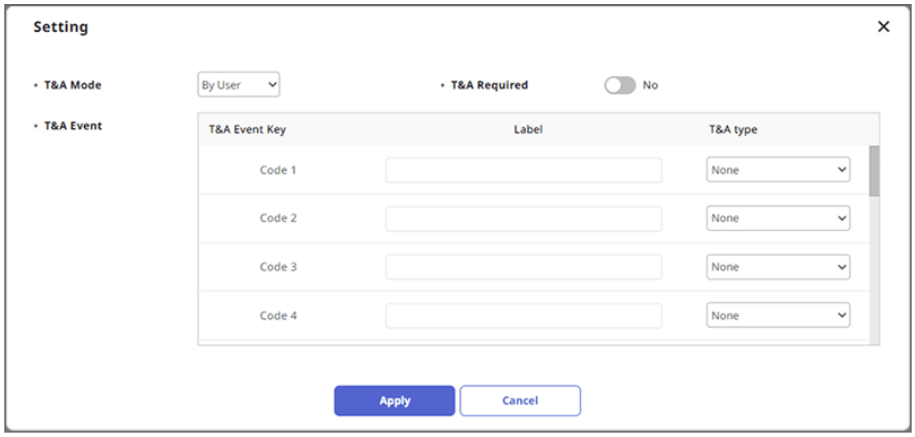
4. If the selected device appears in the **Registered Devices** list, click the **Setting** button.



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**: 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 on schedule settings, see Schedule Settings.

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.
- These models support the **By Schedule** and **Fixed** modes: XPass Q2, XPass 2, XPass D2, BioEntry W3, BioEntry P2, and BioEntry W2.
- For more information on the **Setting** menu, see Set Time & Attendance.

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 the Time Code settings, see Set Time Code.

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 the Shift settings, see Set Daily Shift.

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 the Schedule Template settings, see Set Weekly Shifts.

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 the Rule settings, see Set Other Work Rules.

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.

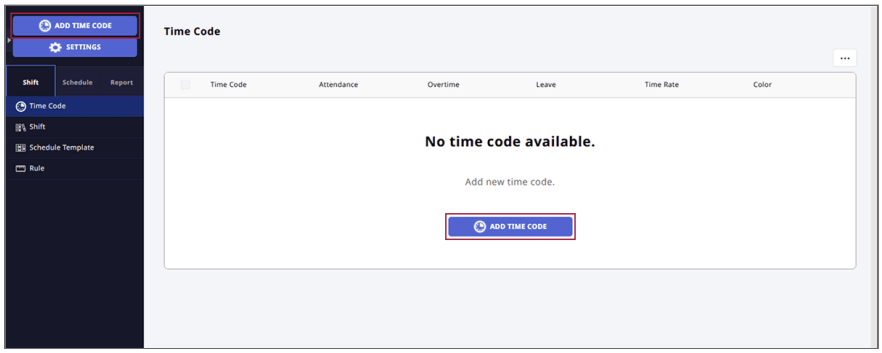
For more information on the Schedule settings, see Set the Schedule.

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

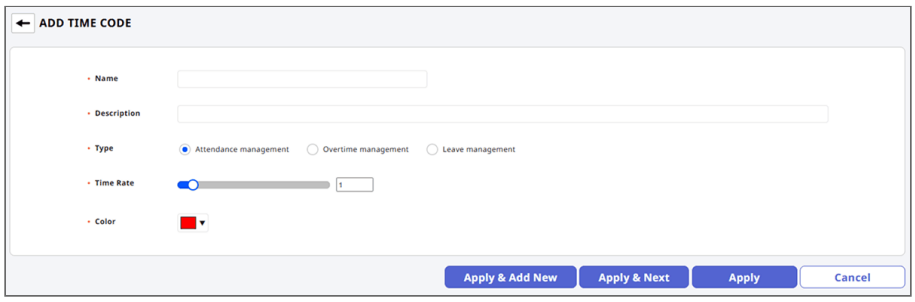
1. Click **T&A** on the **Launcher** page.
2. Click **Shift** → **Time Code** on the left sidebar.
3. Click **ADD TIME CODE**.



4. When the **ADD TIME CODE** screen appears, set each item.

> **Info**
>
> - Click **Apply** at the bottom of the screen to save the settings.
> - To add Shift, click **Apply & Next**.
> - After saving the settings, click **Apply & Add New** to add another **Time Code**.

Setting options guide



- **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.
- **Time Rate**: 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.

Next step

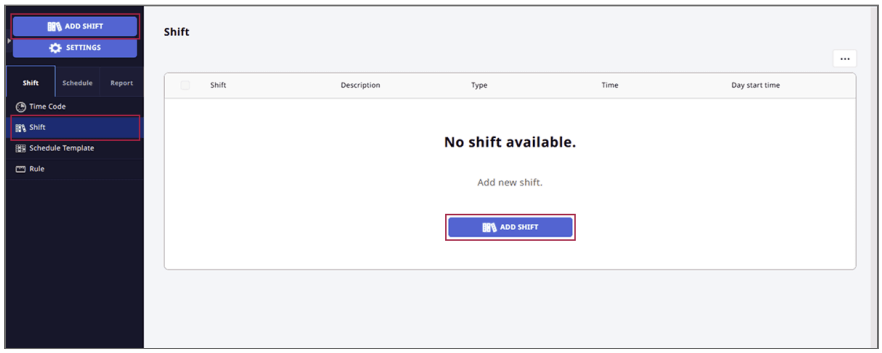
You can set daily working rules based on a 24-hour period. Working rules include time rule settings based on time, daily start time settings, and time rounding rules.

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** → **Shift** on the left sidebar.
3. Click **ADD SHIFT**.



4. When the **ADD SHIFT** screen appears, set each item.

Info

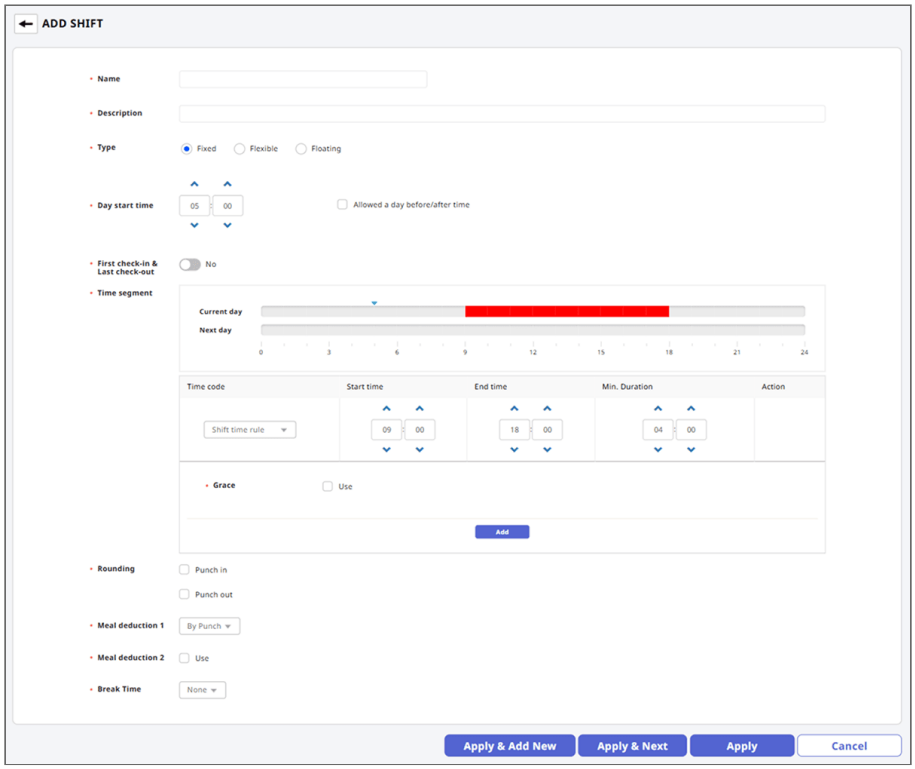
- Click **Apply** at the bottom of the screen to save the settings.
- To continue adding weekly work rules, click **Apply & Next**.
- After saving the settings, click **Apply & Add New** to add another **Shift**.

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**.



- **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.



- **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.



- **Rounding**: Automatically round the start and end times. Set units and standards for both start and end times.



  – **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** rule takes 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**.

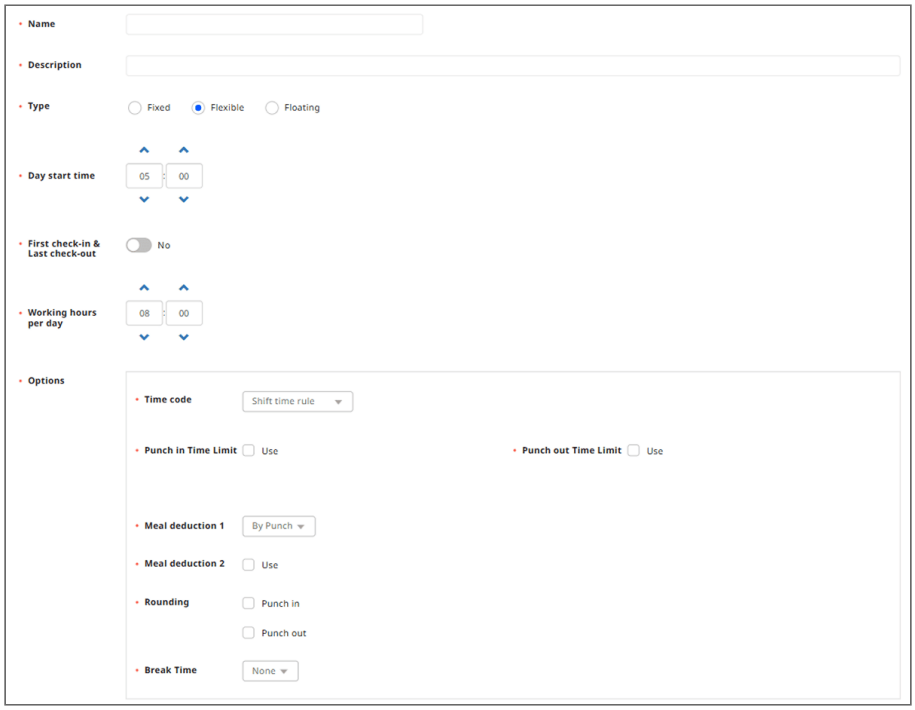
> **Info**
>
> - Using **Meal deduction 2** allows for deductions of two meal times from daily working hours.
> - If the meal deduction types are **Auto** or **Fixed**, then **Meal deduction 1** and **Meal deduction 2** can only be set to the same type.

- **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**.



- **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
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.



- **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.



  – **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** rule takes precedence over **Grace**.

- **Break Time**: Set break times.

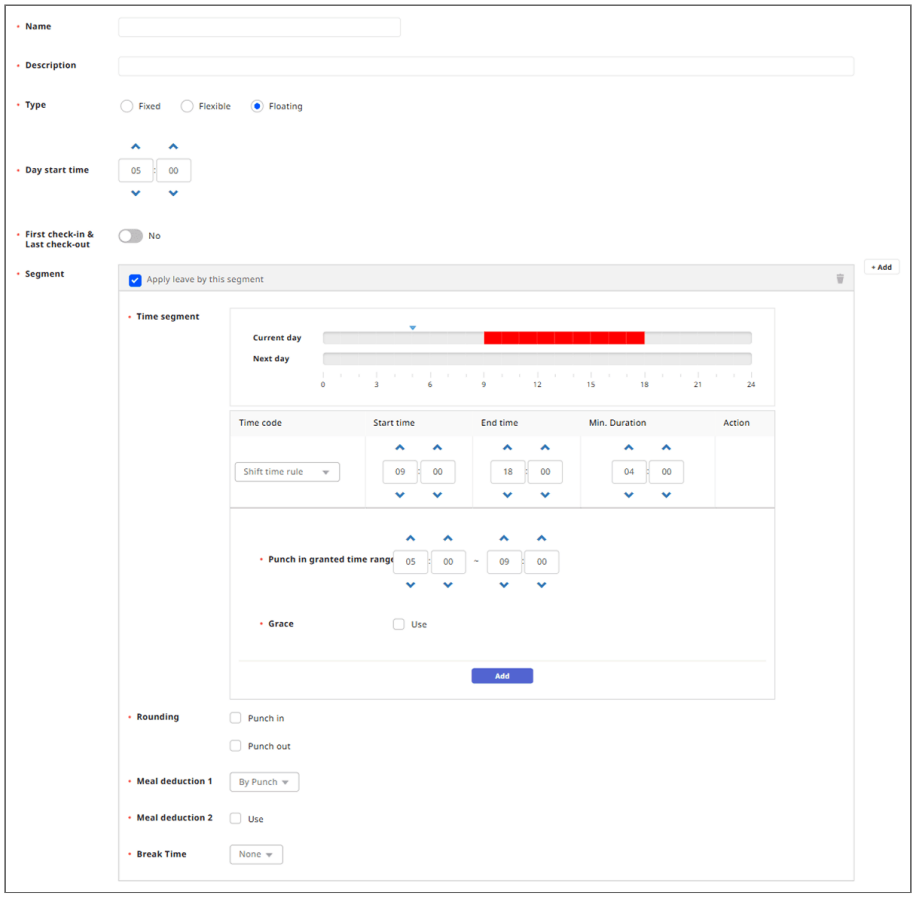
  – **By Punch**: Set to follow the time records registered on the attendance device without setting fixed break times. When this option is activated, you can set **Max. allowed break time(min.)**.

  – **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

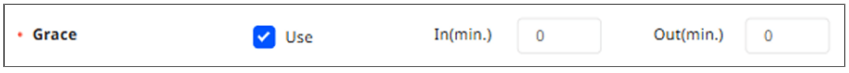
This is a work rule that allows flexible setting of arrival and departure times. Enter the name and description of Shift and select **Type** as **Floating**.



- **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.



- **Rounding**: Automatically round the start and end times. Set units and standards for both start and end times.



  - **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** rule takes precedence over **Grace**.

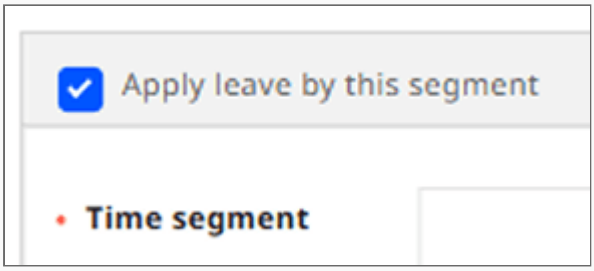
- **Meal deduction 1** / **Meal deduction 2**: Set deductions for meal times from daily working hours.
  - **By Punch**: Set to deduct based on time records registered on the attendance device without setting fixed meal deduction times.
  - **Auto**: Set to automatically deduct meal times by defining **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.



- You can set **Start time**, **End time**, **Min. Duration**, and **Rounding** for a time rule set as **Overtime management**.

Next step

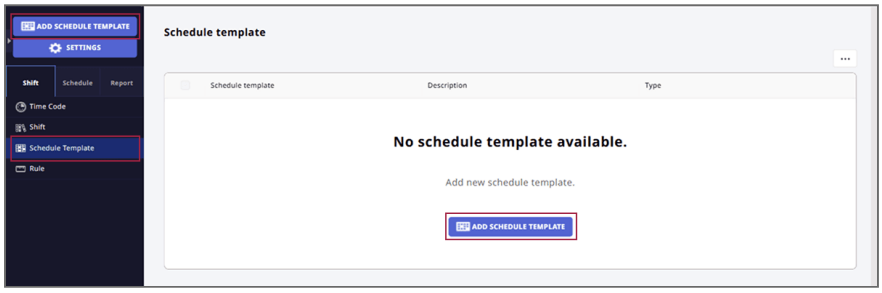
You can set weekly work rules based on the daily work rules configured. You can set weekly work rules on a weekly or daily basis.

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** on the left sidebar.
3. Click **ADD SCHEDULE TEMPLATE**.

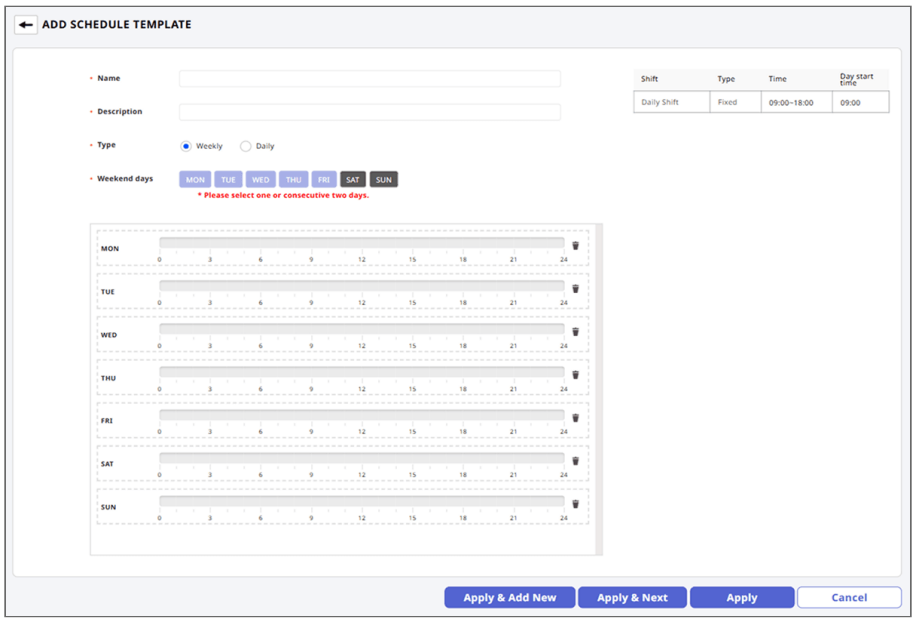


4. When the **ADD SCHEDULE TEMPLATE** screen appears, set each item.

Info

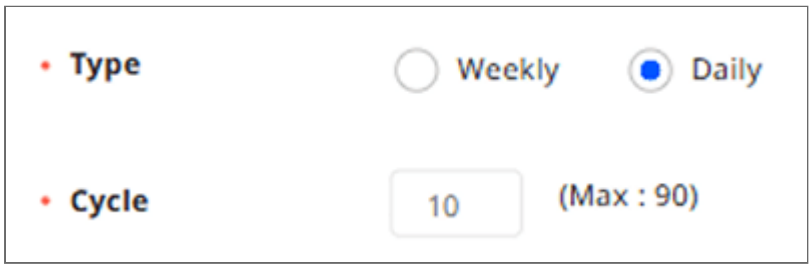
- Click **Apply** at the bottom of the screen to save the settings.
- To continue adding the work schedule, click **Apply & Next**.
- After saving the settings, click **Apply & Add New** to add another **Schedule Template**.

Setting options guide



- **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**).



- **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.



Info

- To apply to all from Monday to Sunday, click **Copy All**.
- To remove the applied Shift, click 🗑.
- 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.

Next step

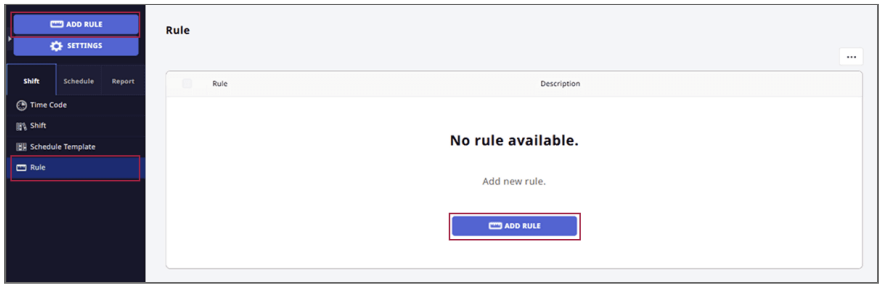
This guides how to create flexible shift rules by additionally applying overtime rules to daily shift rules.

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** on the left sidebar.
3. Click **ADD RULE**.



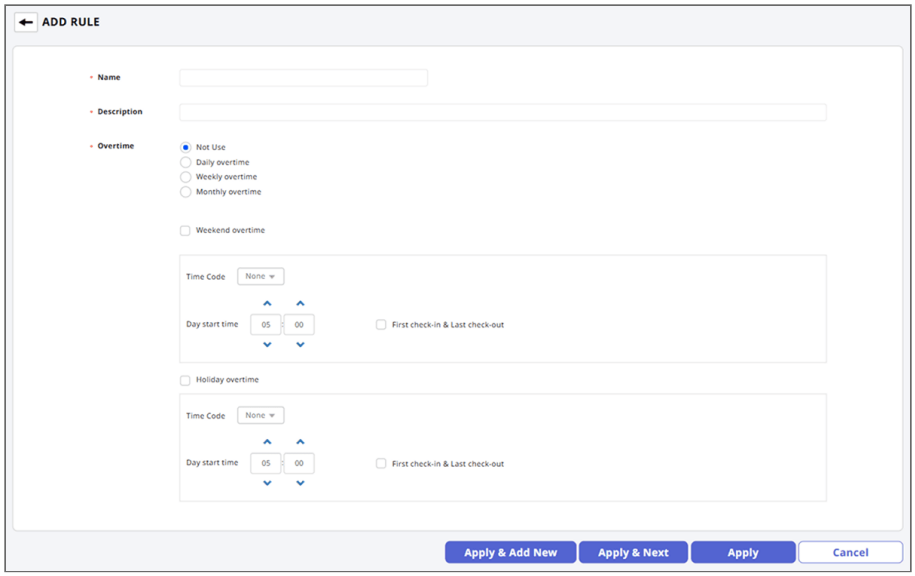
4. When the **ADD RULE** screen appears, set each item.

Info

- Click **Apply** at the bottom of the screen to save the settings.
- To continue adding the work schedule, click **Apply & Next**.
- After saving the settings, click **Apply & Add New** to add another **Rule**.

Setting options guide

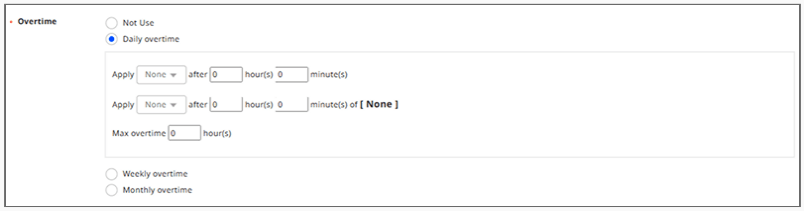
Set Rule. You can set overtime rules to apply on a daily, weekly, or monthly basis.



- **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.



> **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.

Next step

This guides you on how to set up your work schedule by configuring period, users, other work rules, and leave schedules.

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.

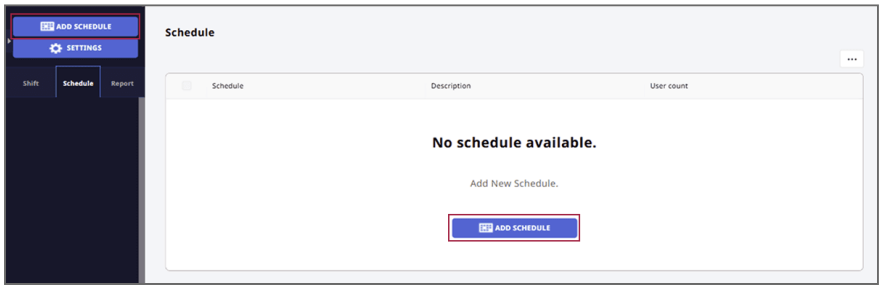
> **Info**
> Before creating the schedule, ensure that you have correctly created the Time Code, Shift, Shift, and holidays.
> - For more information about work rule settings, refer to the following:
>   - Set Time Code
>   - Set Daily Shift
>   - Set Weekly Shifts
>   - Set Other Work Rules
> - For more information on holiday settings, see Schedule Settings.

Work 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**.

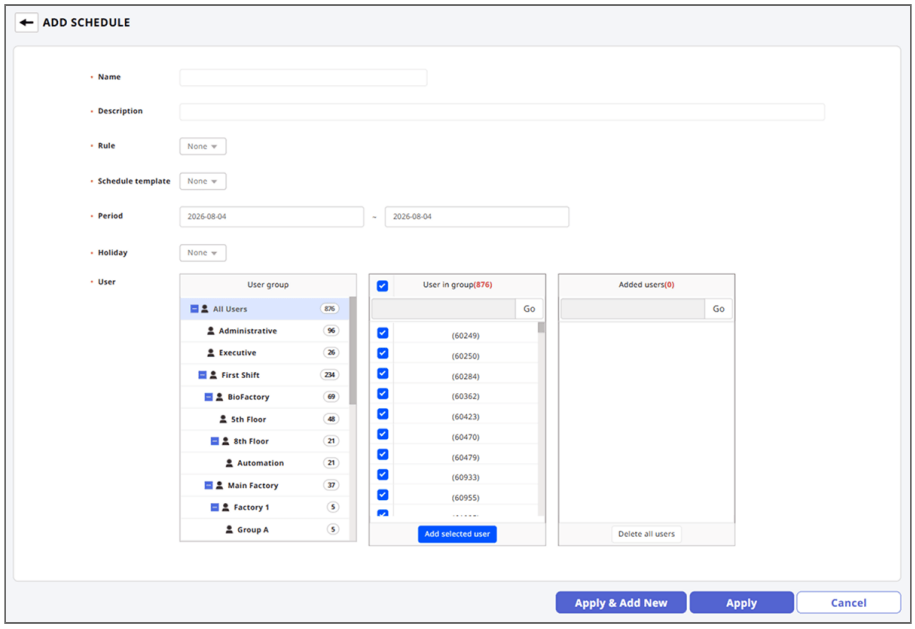


4. When the **ADD SCHEDULE** screen appears, set each item.

> **Info**
>
> - Click **Apply** at the bottom of the screen to save the settings.
> - After saving the settings, click **Apply & Add New** to add another **Schedule**.

Setting options guide

Guide for work schedule configuration options.



- **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, see Set Other Work Rules.

- **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, see Set Weekly Shifts.

- **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, see Schedule Settings.

- **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 ✎ for the item to modify on the left sidebar of the screen.
4. Modify the desired item and click **Apply**.

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.



4. Click **Delete schedule** at the top right of the screen. Alternatively, click 🗑 for the item to delete on the left sidebar of the screen.

5. When the confirmation message appears, click **Yes**.

Add a temporary schedule

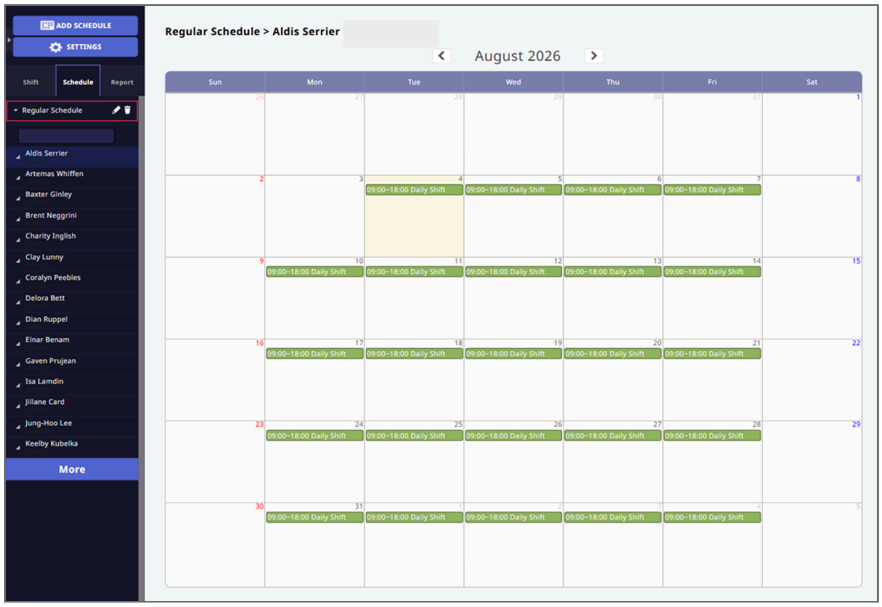
If a schedule is already registered, a temporary different work rule can be applied to the user.

1. Click **T&A** on the **Launcher** page.

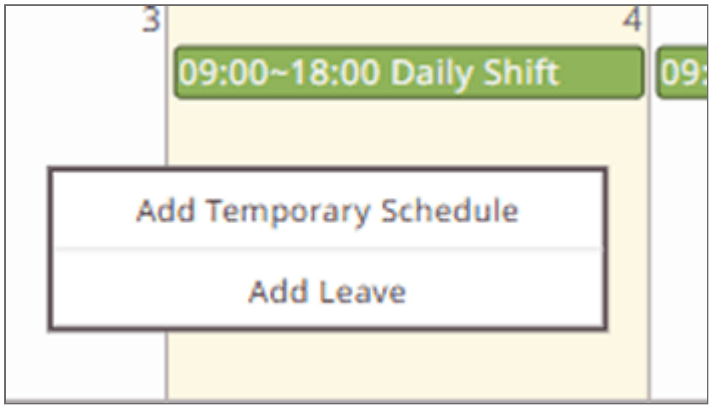
2. Click **Schedule** tab on the left sidebar of the screen.

3. Click ▶ 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.

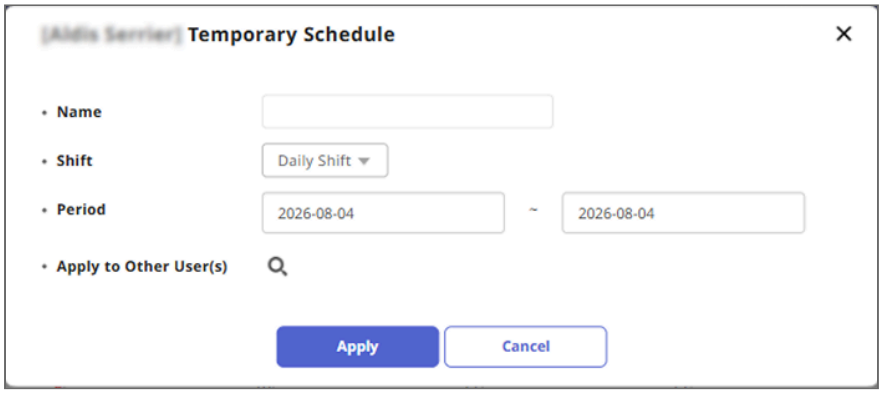


5. Click the date to which you want to add a temporary schedule on the calendar.



6. Click **Add Temporary Schedule** in the popup menu.

7. When the **Add Temporary Schedule** settings window appears, set each item.



To apply the same work schedule to other users, click 🔍 and select the users.

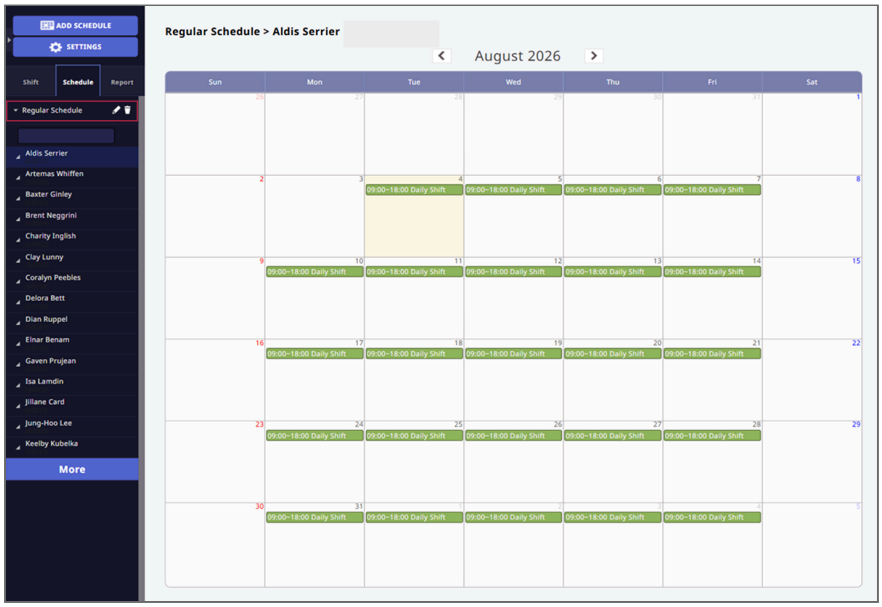
8. Click **Apply** to apply the set work rules.

> **Info**
> To delete the temporary schedule applied to the user, click the set temporary schedule on the calendar. Click **Yes** when the confirmation message window appears.

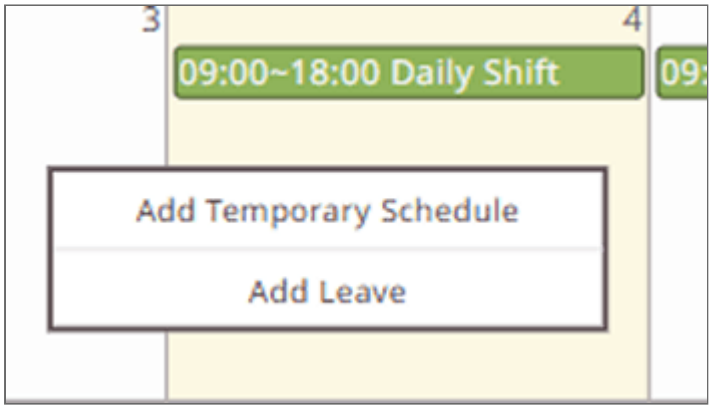
Add and remove a leave

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 ▶ 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.

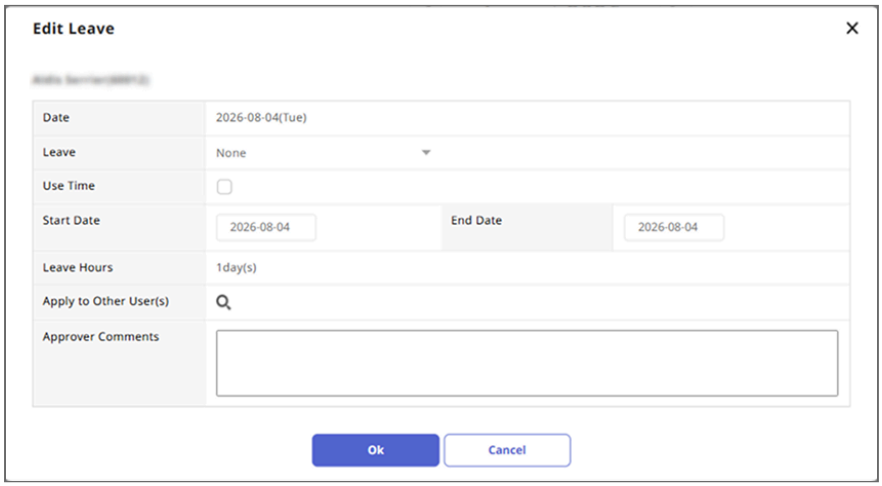


5. Click the date on the calendar to add the user's absence schedule.



6. Click **Add Leave** in the popup menu.

7. When the **Edit Leave** settings window appears, set each item.

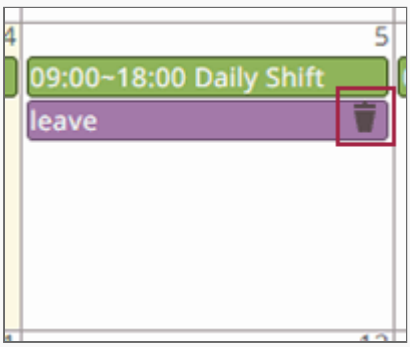


To apply the same absence schedule to other users, click 🔍 and select the users.

8. Click **Apply** 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, see Set Time Code.
- To delete the absence schedule applied to the user, click 🗑 for the set absence schedule on the calendar. Click **Yes** 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 you 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.

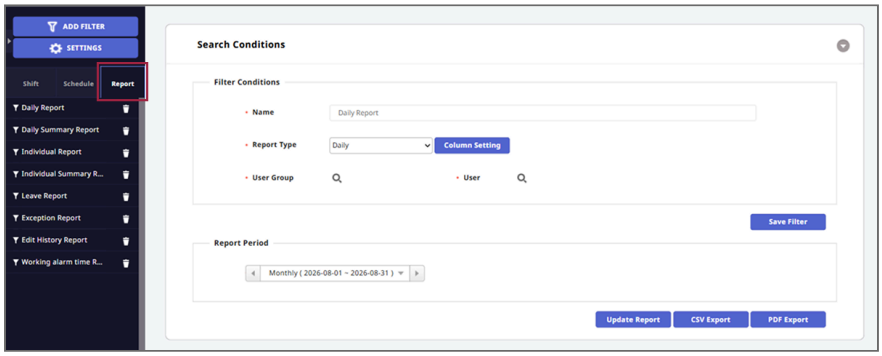
> **Info**
>
> For more information on MariaDB and MS SQL Server settings during **BioStar X** installation, refer to Custom Installation.

Check the report

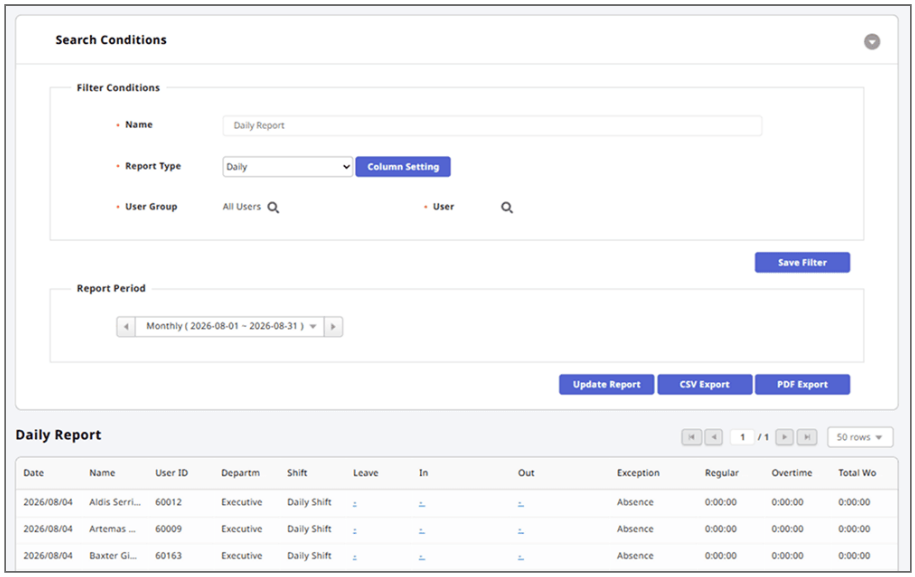
Generate the report

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.

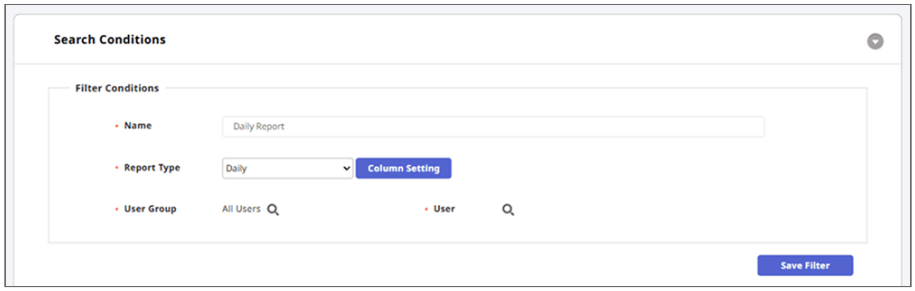


3. Click the desired report filter item from the left sidebar of the screen.
4. In **User Group** or **User**, click the 🔍 button, then specify the group or user.
5. To generate the report, click the **Update Report** button.
6. When the list of reports appears at the bottom of the screen, you can click the desired item to view details.



Set the filter conditions

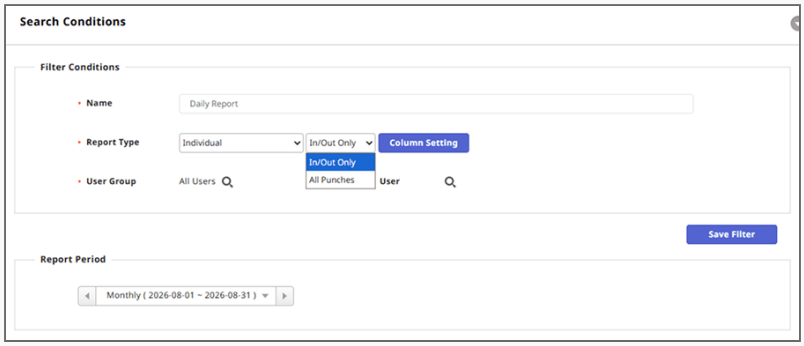
You can set filter conditions to generate a new T&A record report.



- **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**

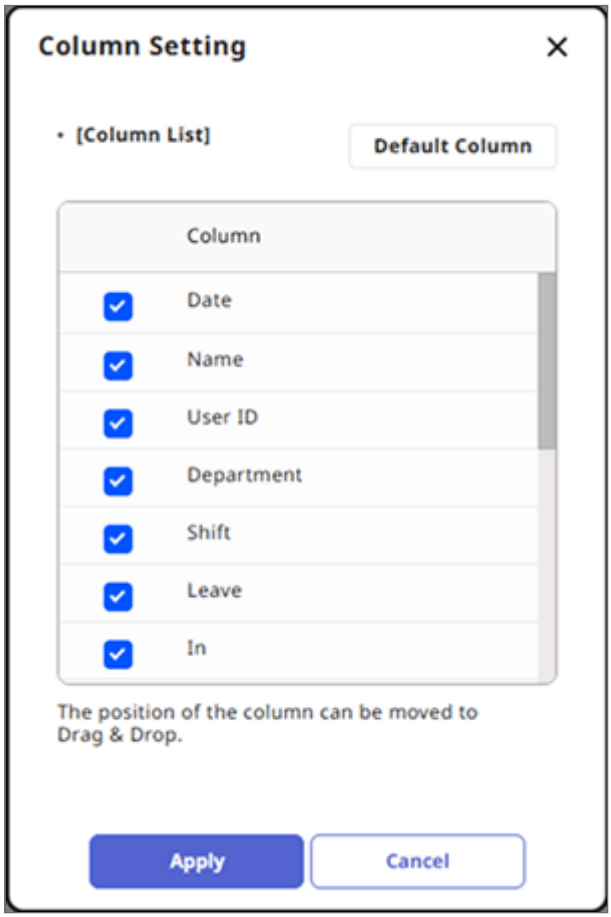
Info

By selecting **Report Type** as **Individual**, you can set whether to output user entry records.



- **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.

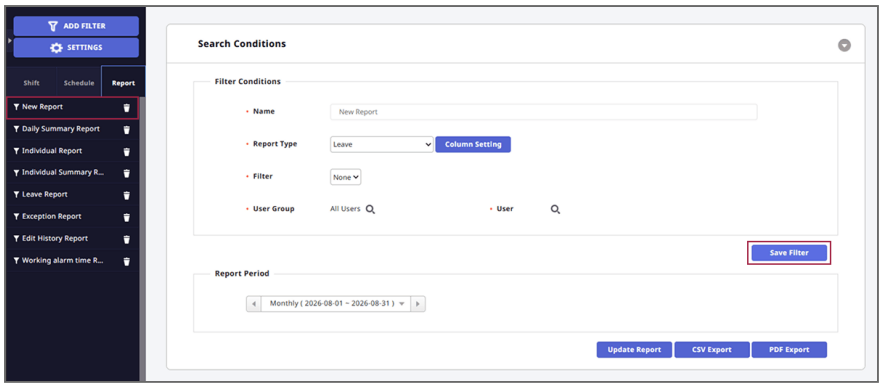


Info

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.



Set report period

This provides instructions on setting the report period.



You can set the report period to **Daily**, **Weekly**, or **Monthly**. To generate a report for a specific period, select **Custom**.

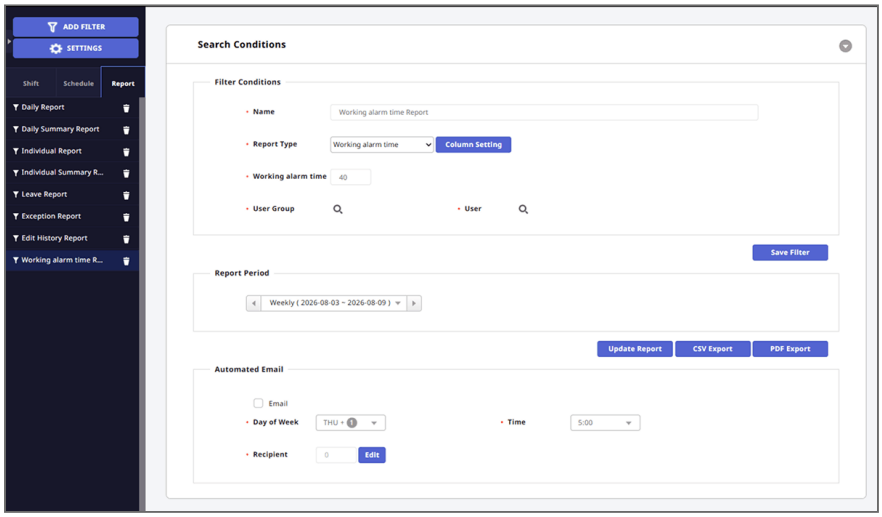
Export report

- **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.



4. Set each item in **Filter Conditions** and **Report Period**.

5. To generate the report, click the **Update Report** button.

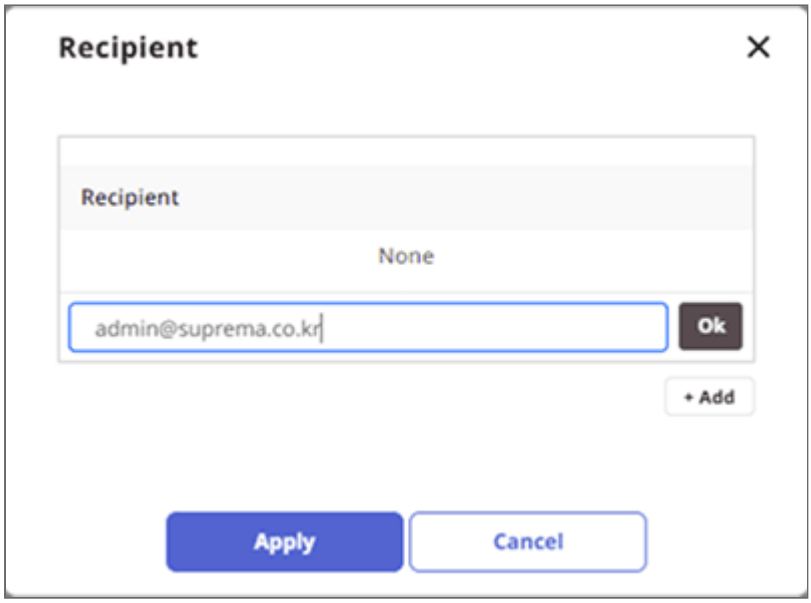
> **Info**
>
> To send notifications to the administrator via email for users who have reached the designated working hours, set **Automated Email**. For more information, see Automatic email sending setting.

Automatic email sending setting

You can automatically send alarm emails to the administrator for users who have reached the designated working hours.



- **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 **Edit** to open the **Recipient** popup window. Enter the email address. You can specify more than one administrator.



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** on the left sidebar of the screen. For more information, see Set Time & Attendance.

Edit T&A Report

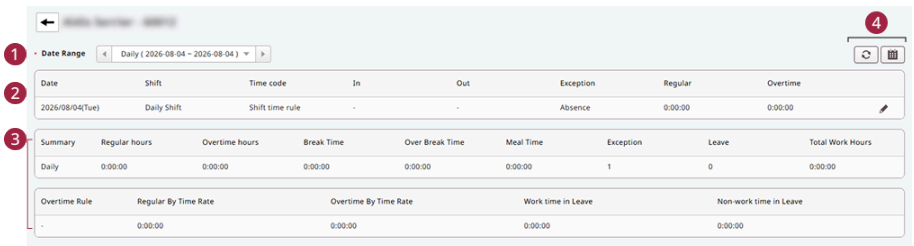
Click the generated report table to modify attendance records.

Info

- You must first generate a report to modify the attendance records. For more information on generating reports, see View the Report.
- 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



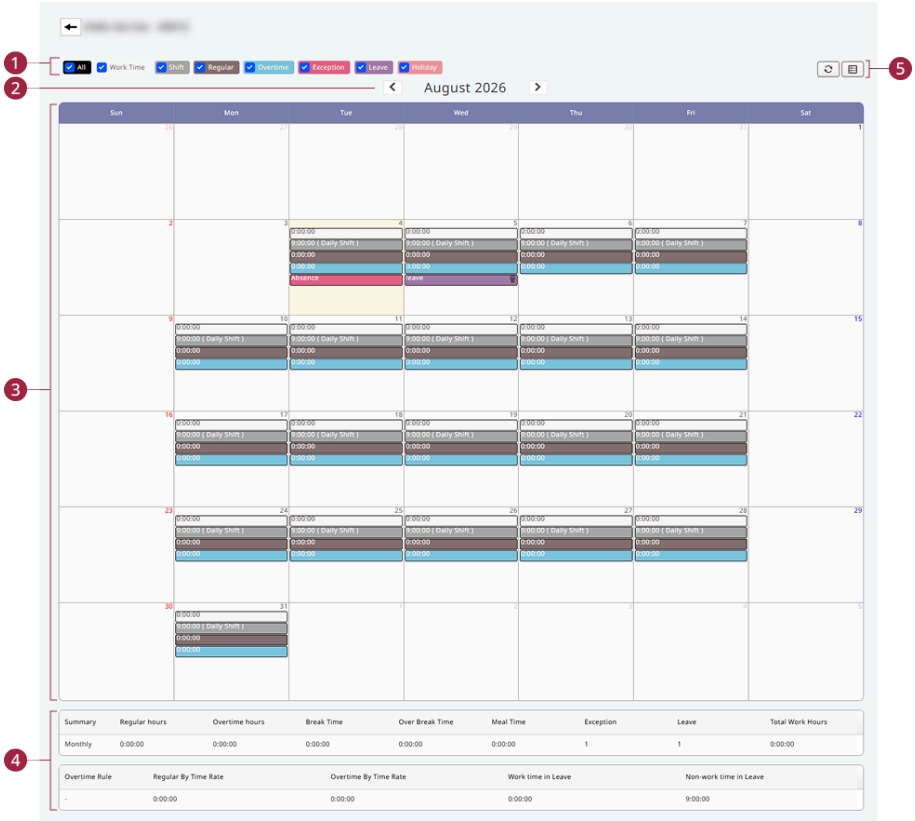
1. **Date Range**: Set the period for attendance records to display in the list.
2. **Daily attendance record**: Shows the daily attendance record.

- Click in/out times to add/modify/delete attendance records. After clicking the in/out times, click ✎ to modify the registered attendance record, and click **Apply** to save changes.
- Click ✎ 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 rules, see Set Time Code.

Edit in the calendar



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 ✎ to modify the registered attendance record, and click **Apply** 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.

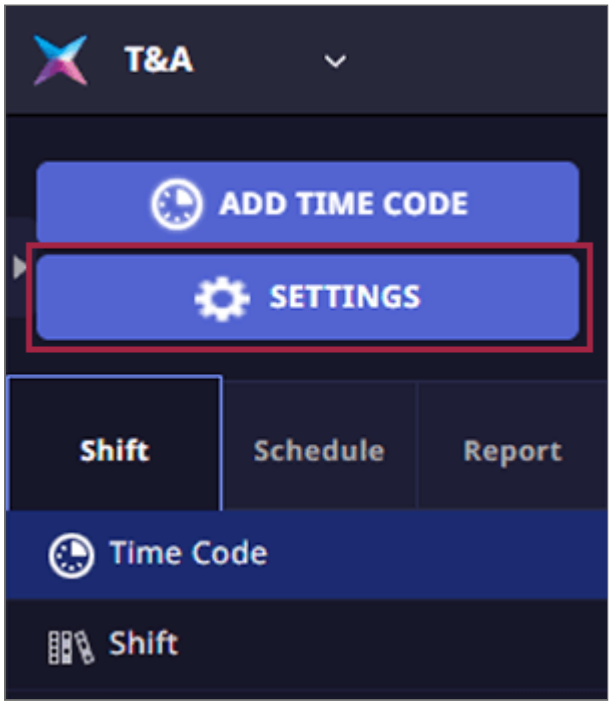
> **Info**
> For more information on creating time rules, see Set Time Code.

Set Time & Attendance

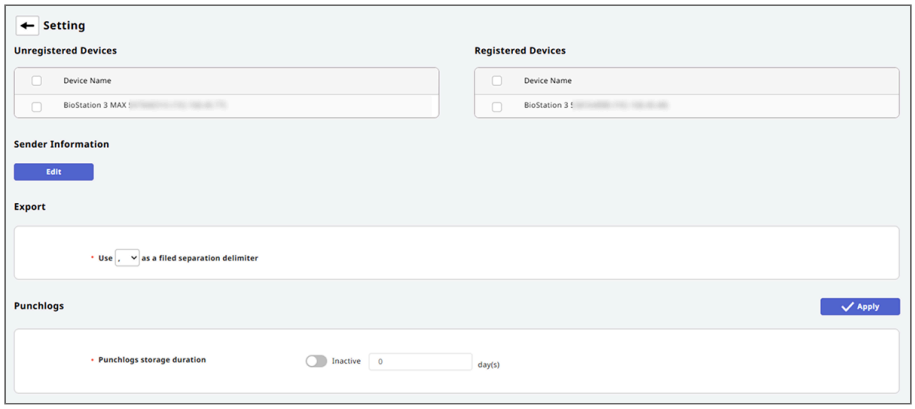
You can register devices to use for attendance management or set the sender information to be used when sending notification emails. You can also set the document delimiter for exporting attendance reports via CSV.

Access attendance management settings

1. Click **T&A** on the **Launcher** page.
2. Click **Settings** on the left sidebar.



3. Edit the necessary fields.



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**.



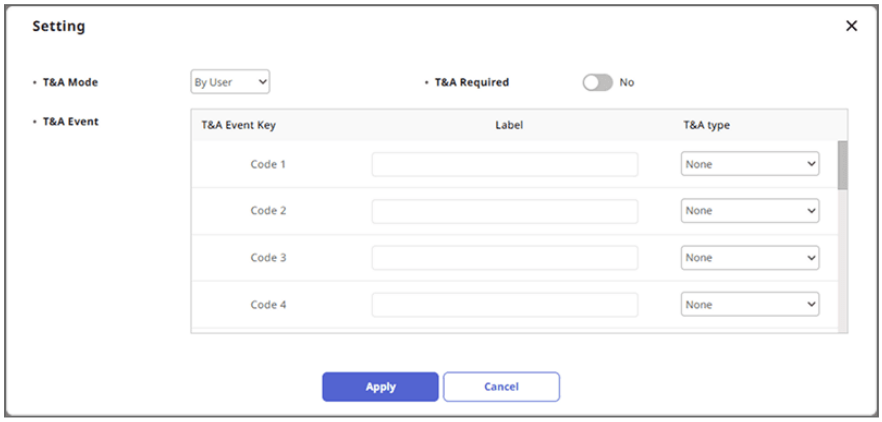
Registered Devices

List of devices currently used for attendance management.

- To unregister, select the desired device and click **Unregister**.



- To edit the attendance settings of a registered device, click **Setting**. For more information on attendance settings, see Advanced Settings.



T&A type is a setting to map **T&A Event Key** with attendance event types. Attendance event types are as follows:

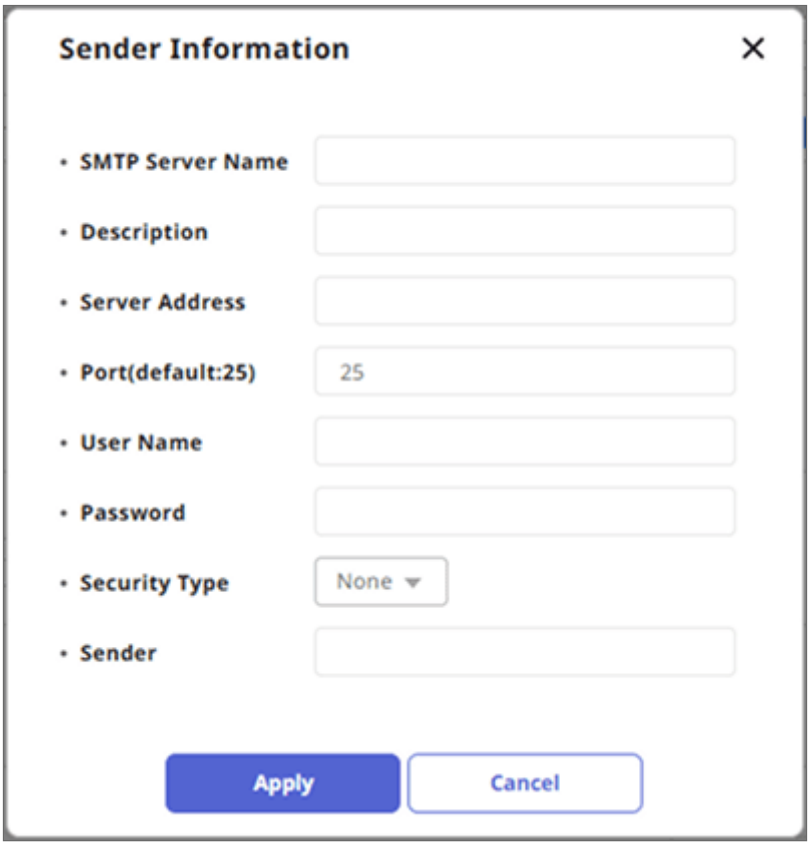
  - **Check In**

- **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** → **Device** menu, the system also automatically deletes the registered attendance management device.
> - If you set the **Multi Face Authentication** option to **Use**, the device does not support attendance management. For more information on **Multi Face Authentication**, see Authentication Settings.

Sender Information

You can set the sender information to be used when sending notification emails. Click **Edit**.



- **SMTP Server Name**: Enter the SMTP server name.
- **Description**: Enter the description.
- **Server Address**: Enter the SMTP server address. 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.
- **Port(default:25)**: Enter the port number of the SMTP server. You can find this on the email settings screen of your SMTP service provider.

- **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.

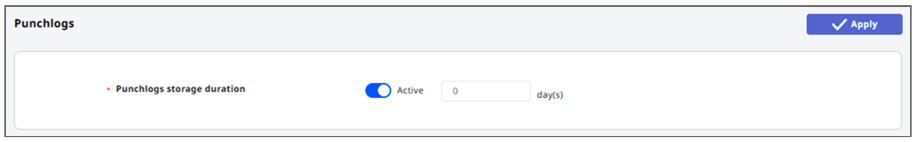
Export

With the **CSV Export** feature, you can choose the document delimiter when exporting attendance reports.



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**.



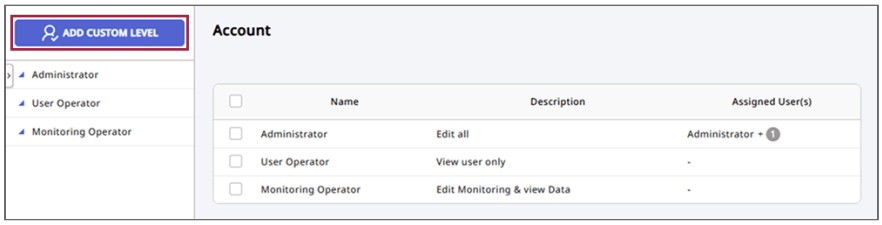
View Time and Attendance Audit Logs

The **T&A Audit Log** feature records all activities related to time and attendance management, such as work, schedules, and reports. Each record shows when, who made the change, what changed, and how, to support audits and troubleshooting.

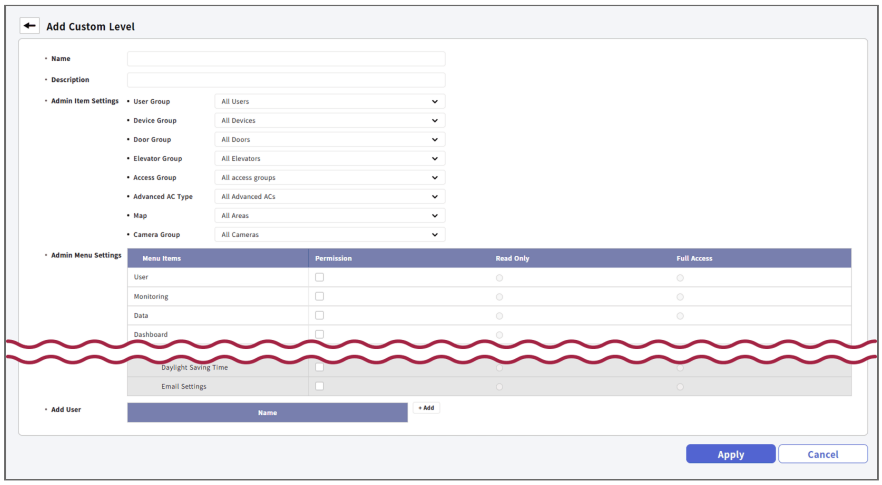
> **Info**
>
> The **T&A Audit Log** menu requires an active Time and Attendance (T&A) license and operations administrator permission. The **T&A Operator** account created by default during Time and Attendance plugin installation lacks this permission. Add and assign a custom permission.

Add Time and Attendance audit permission

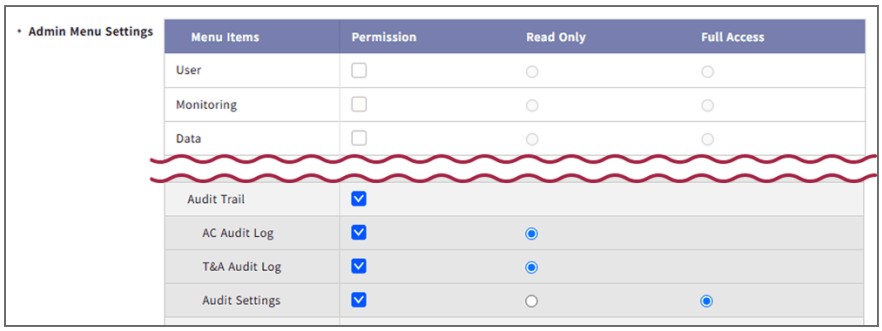
1. Click **Settings** on the **Launcher** page.
2. Click **Account** → **Account** on the left sidebar.
3. Click **Add Custom Level**.



4. Enter a permission name and description to view Time and Attendance audit logs.



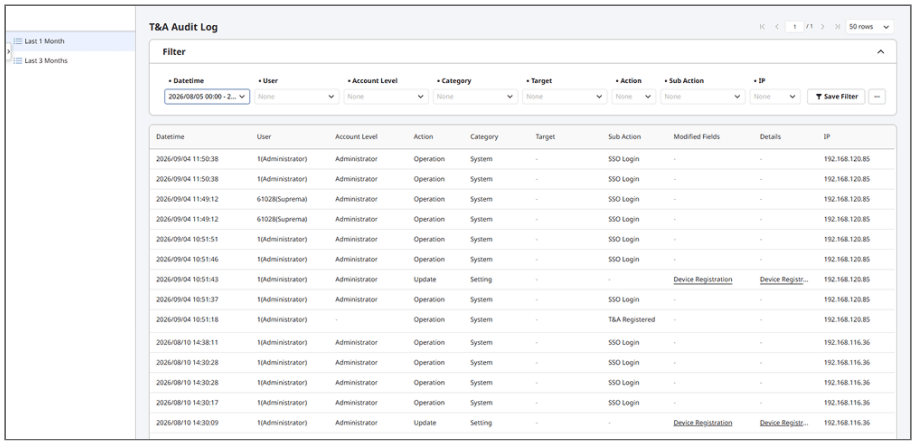
5. In **Admin Menu Settings**, set permissions for **T&A Audit Log** and **Audit Settings** under the **Audit Trail** menu.



6. In **Add User**, click **+ Add** and select a user group or users.
7. Click **Apply** at the bottom of the screen to save the custom permission.

View Time and Attendance audit logs

1. Click **Settings** on the **Launcher** page.
2. Click **Audit Trail** → **T&A Audit Log** on the left sidebar.
3. The Time and Attendance audit log list appears on the screen.



Info

- To change audit log policies such as the retention period, see Set Time & Attendance Audit.
- After upgrading to version 1.0.3, the system encrypts new audit logs regardless of the **Encrypt Personal Data on Database** option under **Settings** → **System** → **Security**.
- If the system does not record certain audit logs after the upgrade from BioStar 2 to **BioStar X**, see Upgrade.

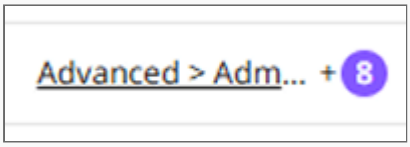
Table layout

The audit log list table has 10 columns and shows records in descending order by **Datetime**.

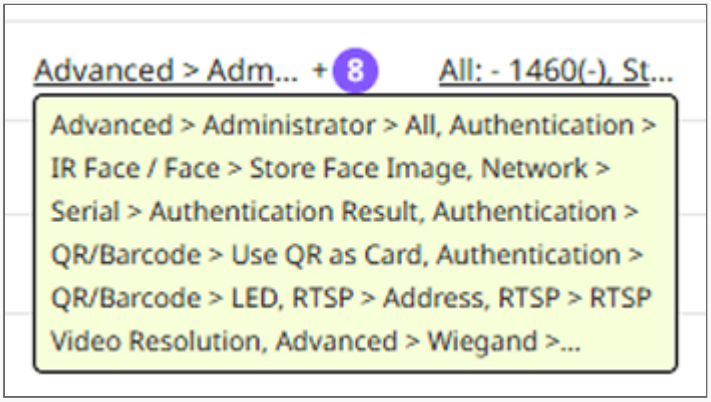
Column	Description
Datetime	The date and time the event occurred.
User	The user who performed the event. Displayed in the **id(name)** format.
Account Level	The administrator level of the user who performed the event. Leave this field blank for actions the system executes automatically.
Action	The type of action executed. This field shows **Create**, **Update**, **Delete**, **Read**, **Export**, or **Operation**.
Category	Domain category of the event target. (**Shift**, **Schedule**, **Report**, **T&A Audit Log**, **Setting**, **System**)
Target	The target the action applies to. Displayed in the **type: id(name)** format.
Sub Action	Detailed action name that appears only for **Operation**, **Read**, and **Export** actions.
Modified Fields	The name of the field that changed or was viewed. Always leave **Operation** blank.
Details	Detailed information for each action. (Changed values, query conditions, field snapshots, and more)
IP	IP address from which the user accessed. The system shows automatically issued records as **127.0.0.1**.

Info

- Records where **Action** is **Update** always refer to only 1 target. Time and Attendance does not include bulk editing that changes multiple targets at once, so targets never appear as a group.
- Names shown in **User**, **Target**, and **Change Details** keep the value from when the record occurred. If the name changes later or the target is deleted, the name shown in past records stays the same.
- If the **Target** or **Modified Fields** value has 2 or more entries, only the first item is shown, and the rest are collapsed into a remaining-count badge on the right (e.g., **+208**). If the remaining count is 1,000 or more, the badge shows **+999**. Check the exact total count in the detail popup title. Click the badge to open the detail popup for that cell.

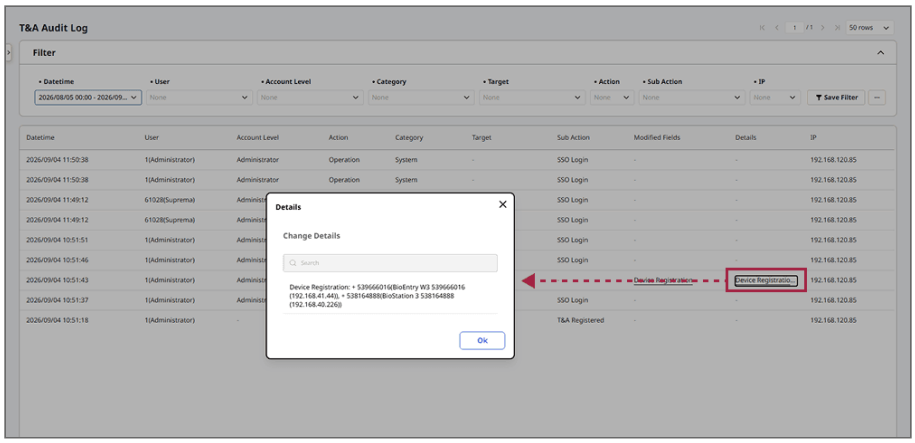


- Long cell values truncate to one line with an ellipsis. Hover over the value to see the full text in a tooltip. The tooltip truncates overflow text as ... .



View details

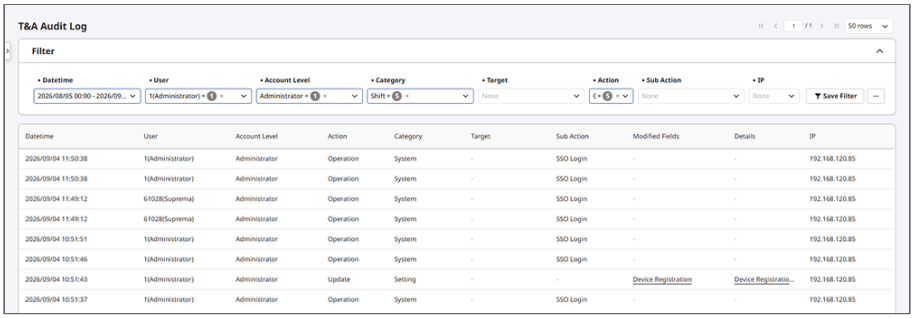
Cells with values in **Target**, **Modified Fields**, or **Details** appear underlined and are clickable. Click a cell to open a details pop-up for that row's action. Close it with **OK** or ✕.



Enter a keyword in the **Search** field at the top of the popup to highlight or filter matching entries. When searching, the target popup updates groups and counts per group. The title total count stays the same.

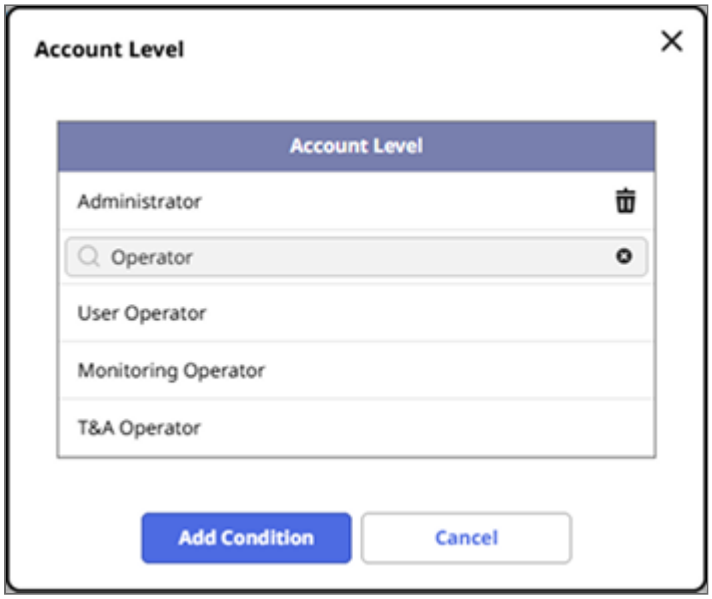
Find records with filters

Combine the filters in the **Filter** section to narrow down and find the records you need. Select multiple values in one filter to combine them with `OR`. Apply multiple filters together to combine them with `AND`.

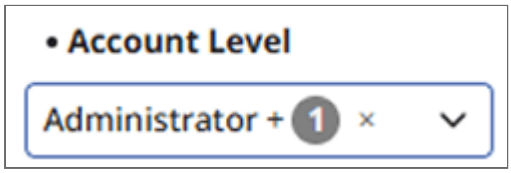


Filter	How it works
Datetime	Set the start and end dates and times. No length limit applies to the search period.
User	Enter a search term and press `Enter` to find matching users. The list is empty when you first open it.
Account Level	Enter a search term and press `Enter` to find matching administrator levels.
Category	Select one or more categories from the searchable checkbox list.
Target	Enter a search term and press `Enter` to find matching targets.
Action	Select one or more actions from the checkbox list.
Sub Action	Select a detailed action from the searchable list.
IP	Enter a search term, then press `Enter` to find matching IP addresses.

- If you apply no filters, records from the last 30 days appear by default.
- Select a value in each filter popup, then click **Add Condition** to apply it to the search immediately. Click **Cancel** to cancel the selection and close the popup.



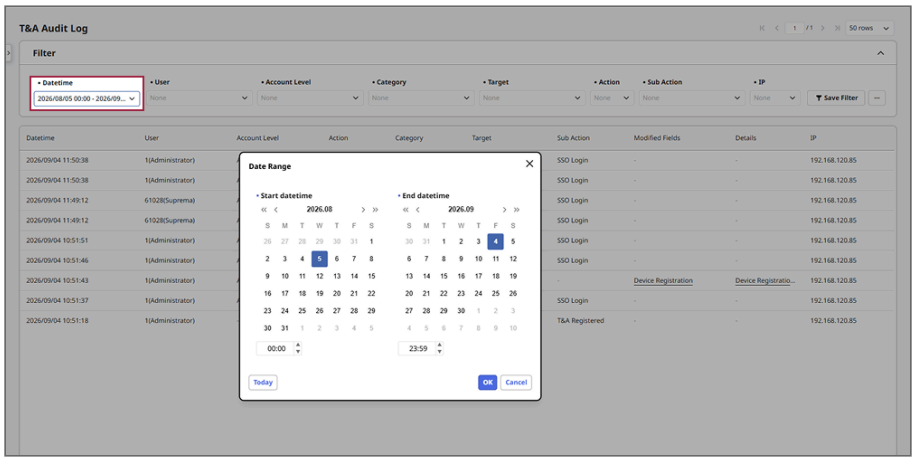
- Applied filters appear as the first filter and the number of additional filters. Click ✕ to clear only that filter. Filters with no selected value appear as **None**.



> **Info**
>
> Enter a search term to see results for the **User**, **Account Level**, **Target**, and **IP** filters. The search supports partial matches; enter part of a name or ID. The search includes deleted targets and marks them as **Deleted**.

Set the query period

Click **Datetime** to open the **Date Range** popup.

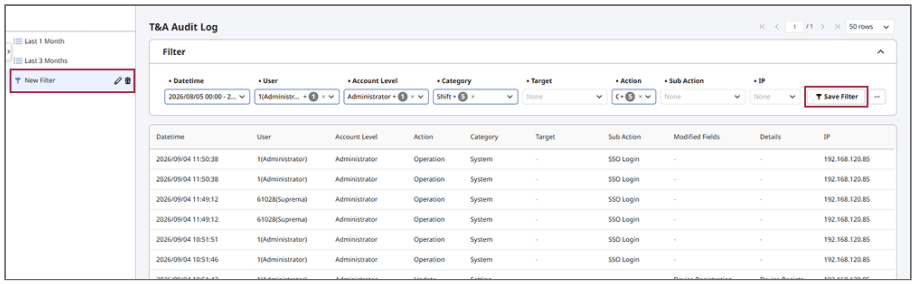


1. Set the date and time for **Start datetime** and **End datetime**. Click **Today** to jump to today.
2. Click **OK** to apply the query period.

Save filter

Save frequently used search conditions in **Saved Filters**, then load them when needed.

1. Set filters to match the required conditions.
2. Click **Save Filter** in the **Filter** section.
3. The system adds **New Filter** to the filter list on the left.



- Click ✎, enter a new name, then press Enter to rename the filter.
- Click 🗑 to delete the filter.

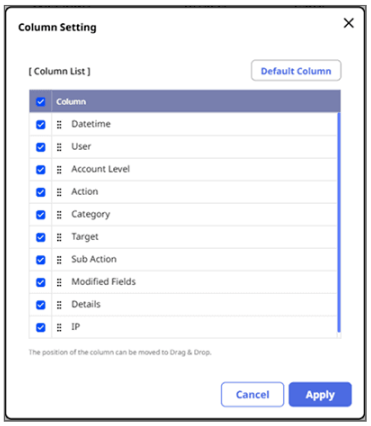
> **Info**
> You can save up to 20 filters. The browser stores saved filters, so they do not appear on other PCs or browsers.

Additional records from cascading deletion

Editing or deleting a work schedule may also delete temporary schedules and absences for users who use it. The system logs each deleted temporary schedule and absence separately from the work schedule change or deletion.

- If cascading deletion deletes nothing, the system creates no additional records.
- **Target** includes 1 work schedule that caused the deletion and only the users whose entries were actually deleted. It does not include all users in the schedule.
- **Details** shows the number of deletions. When you delete a work schedule, it also shows the affected period.

Set columns



Change column positions or hide columns in the audit log table. On the right side of the **Filter** section, click ••• → **Column Setting**.

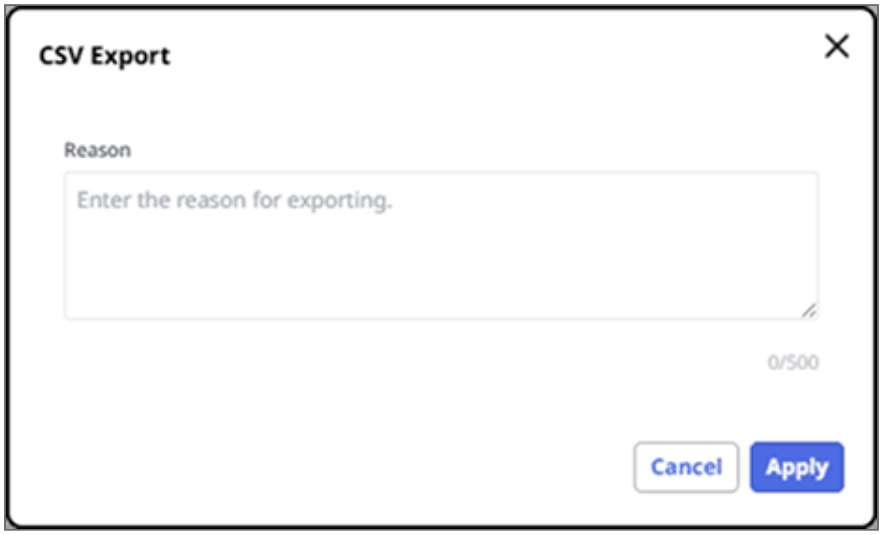
- In **[Column List]**, clear the checkbox for the column to hide.
- Drag a column to change the column order.
- Click **Default Column** to initialize column settings.

Click **Apply** to save the settings.

Export to CSV

Export audit logs 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.
3. When the **CSV Export** window appears, enter **Export Reason** (optional), and click **Apply**.



The exported CSV file includes all 10 columns, one line per record. It adds quotation marks only to cells that contain commas. Use a vertical bar (|) to separate multiple values in cells such as **Target** and **Modified Fields** (example: **Schedule: 7(Team Schedule)| User: 12(Robert)**). In records where **Action** is **Update**, **Details** includes all fields without ellipses.

> **Caution**
> The CSV file includes values as-is, including values a spreadsheet program may interpret as formulas. Do not open the downloaded CSV file directly in a spreadsheet program. If needed, open it with the text import feature.

> **Tip**
> If you set filters, the export includes only the filtered results in the CSV file.

Set Time & Attendance Audit

Audit logs accumulate over time, so manage the retention period to save storage space and protect privacy. In **Audit Settings**, set the retention period for **T&A Audit Log** records and whether to keep view history.

Privilege information

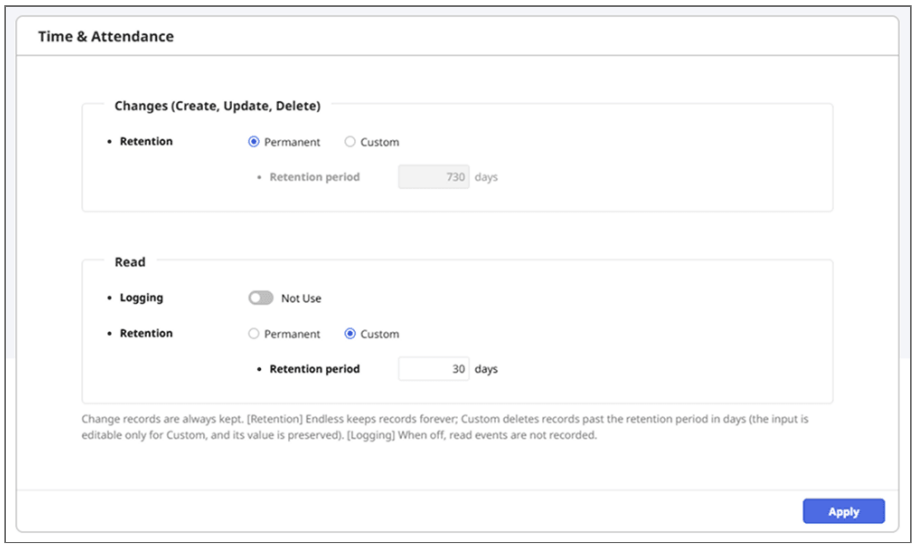
Administrator can always view and change settings in the **Audit Settings** menu. For a custom privilege administrator, in **Admin Menu Settings**, set **Audit Settings** to **Read Only** for view-only, or to **Full Access** for view and change.

Info

- The default Time & Attendance admin account lacks this permission. The system creates this account when you install the Time & Attendance plugin. Grant the permission separately if needed.
- For more information on adding Time & Attendance audit permissions, see View Time and Attendance Audit Logs.

Open audit settings

1. Click **Settings** on the **Launcher** page.
2. On the left sidebar, click **Audit Trail** → **Audit Settings**.
3. Scroll down to the **Time & Attendance** section.



Retention policy settings

The **Time & Attendance** section consists of the following two groups.

- **Changes (Create, Update, Delete)**: Creation, update, and deletion logs. Always recorded. Cannot turn logging on or off.
- **Read**: View logs. Set whether to record logs.

Info

- Enter **Retention period** as an integer between 1 and 2,147,483,647 days.
- Check **T&A Audit Log** for **Update** logs of setting changes in the **Time & Attendance** section.

Change logs

Because the **Changes (Create, Update, Delete)** group is always recorded, select the **Retention** setting.

- **Permanent**: Keep logs permanently without automatic deletion.
- **Custom**: Select this option to limit the retention period for compliance or internal policy. When the **Retention period**

field becomes active, enter the retention period in days.

View logs

In the **Read** group, set whether to keep view logs.

- **Logging**: Set to **Use** to keep view logs. If not needed, set it to **Not Use**.
- **Retention**: Select a retention method.
  - **Permanent**: Keep view logs permanently without automatic deletion.
  - **Custom**: Activates the **Retention period** field. Enter the retention period in days.

> **Info**
> When **Logging** is set to **Not Use**, the system does not record view events. After setting it to **Use**, the system cannot view earlier records.

Save Settings

After completing the **Changes (Create, Update, Delete)** and **Read** settings, click the **Apply** button at the bottom of the **Time & Attendance** section. Save both group settings together.

How automatic deletion works

The server runs this job daily at 1 a.m. It deletes records past the retention period set in **Custom**, regardless of user actions. The job evaluates and deletes records at the same time. It runs only once a day.

> *For example, set **Read** records to 30 days in **Custom**. At 1 a.m., the job deletes records older than 30 days. Records just past the retention period remain until the next 1 AM job runs.*

When **Retention** is set to **Permanent**, the automatic deletion job does not run, and records are retained permanently.

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 as an additional option with an **Essential** or higher license. For more information on licensing policies, see License Policy.
> - After activating the visitor feature through licensing, see Visitor Settings 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** on 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**.

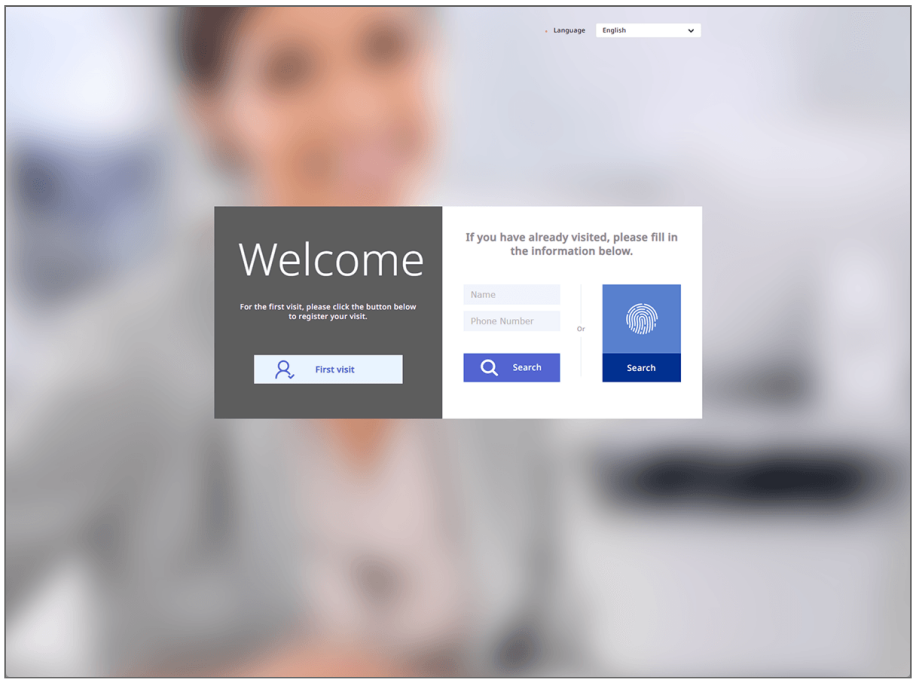
> **Info**
>
> To activate your license in a closed network environment or when internet access is restricted or unavailable, see BioStar X License.

> **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

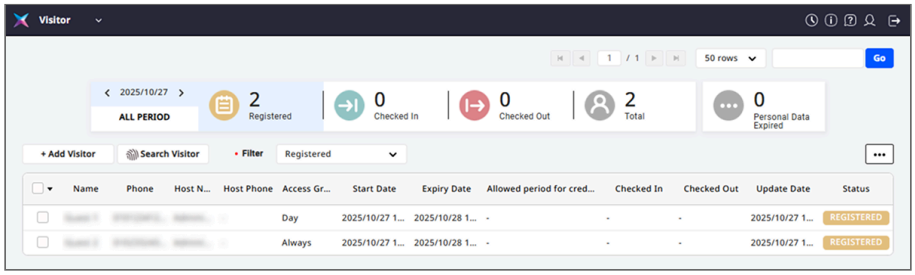
The visitor application page can be used after prioritizing visitor settings. For more information on setting up the visitor application page, see Visitor Settings.

The visitor application page can be accessed from a dedicated application PC, allowing visitors to submit access requests. For more information on visitor registration, see Apply to Visit.



Visitor access management

Check the visitor application history and manage visitor access. For more information on managing visitor access, see Manage Visitors.



Apply to Visit

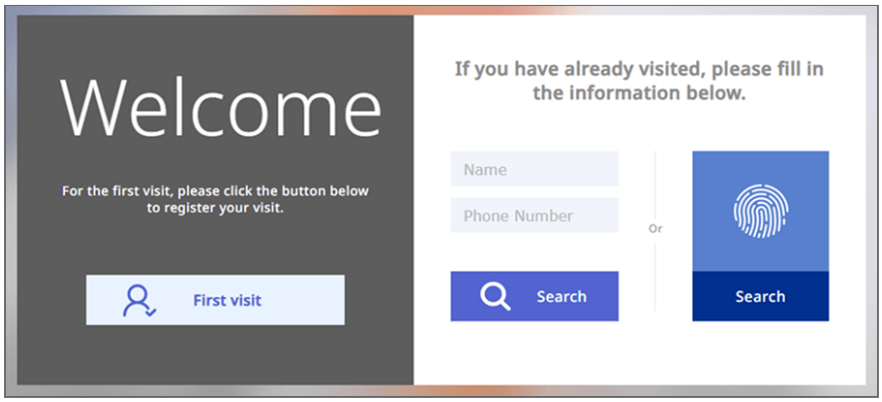
This guides how external visitors who are not internal users apply for entry using the visitor application PC.

> **Info**
>
> - The visitor application PC must be configured separately, and visitor settings must precede it. For more information on visitor settings, refer to Visitor Settings.
> - If there is no shortcut icon for the visitor application page on the visitor application PC, see Visitor Settings to create a shortcut icon.

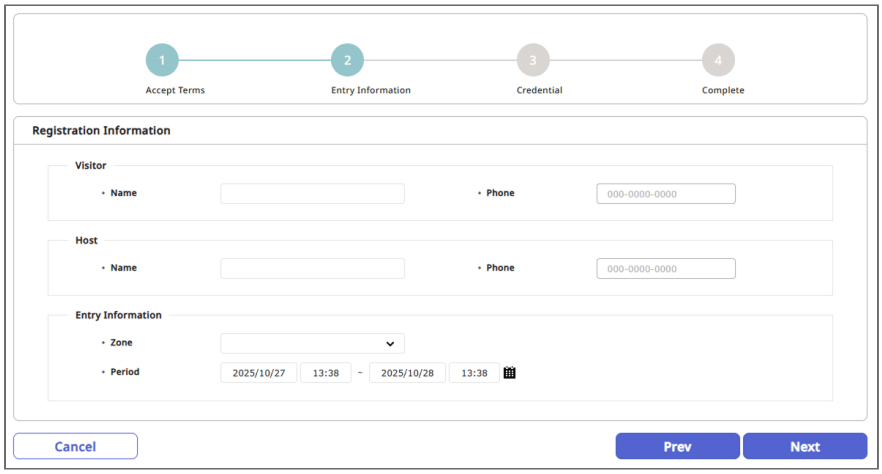
New visitor application

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`.

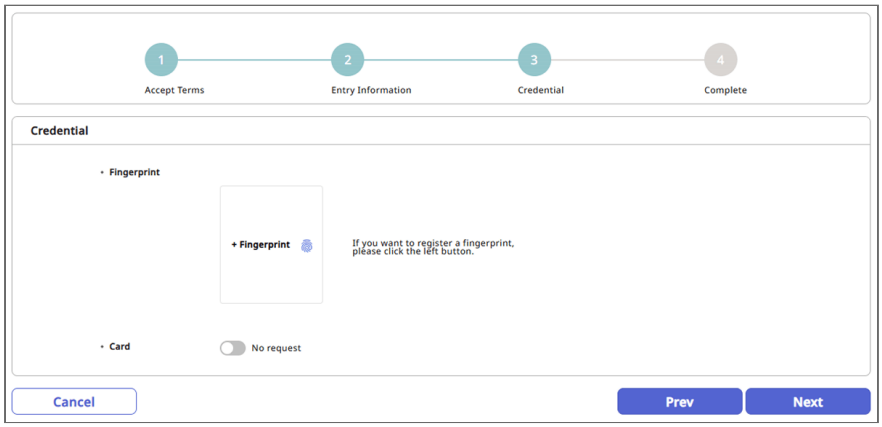


2. Click **First visit** in the center of the screen.
3. After agreeing to the terms and privacy policy regarding access to the visiting department, click the **Next** button in the lower right corner of the screen.
4. Enter the information required for the visit application.



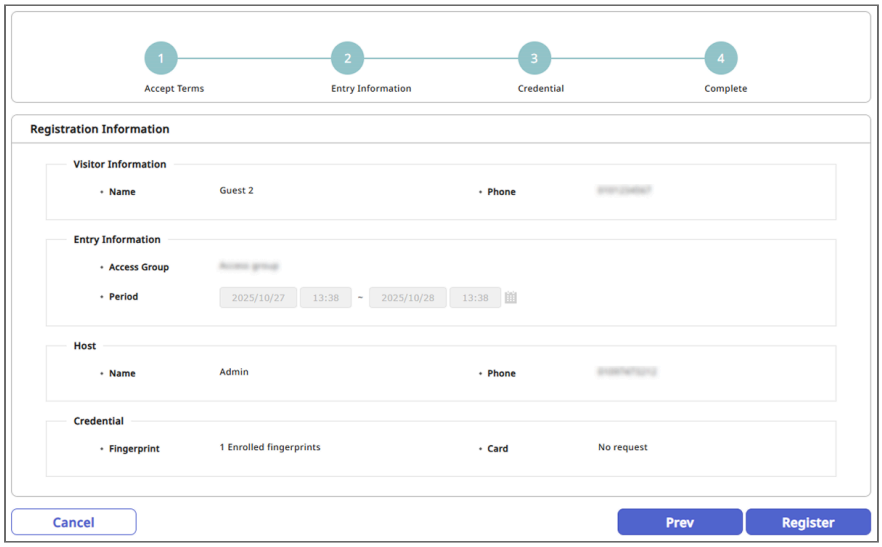
- **Visitor**: Enter the visitor's name and phone number.
- **Host**: Enter the name and phone number of the person responsible for the visit destination.
- **Entry Information**: Set the access area and visit duration.

5. After entering the information, click the **Next** button in the lower right corner of the screen.
6. Set the means of entry.



- **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.



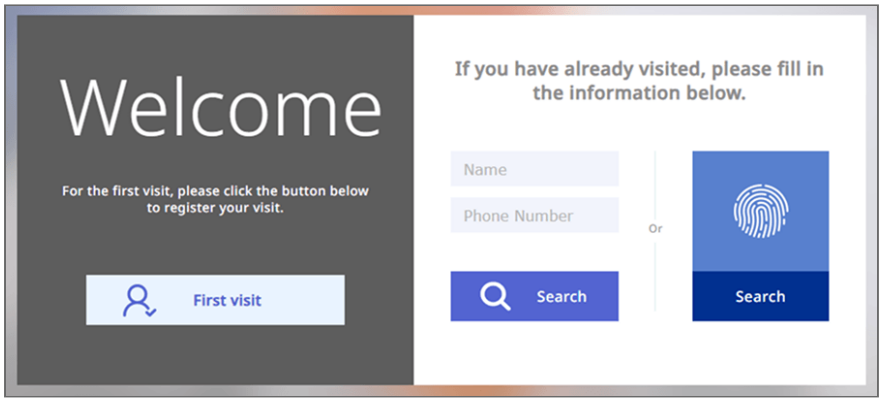
Info

- For more information on creating terms of use and a privacy policy for visitor access, see Visitor Settings.
- The name can be entered up to 48 characters long.
- For more information on adding custom fields to visitor information, see Visitor Settings.
- You can only select access groups assigned to the visiting department for the visit PC. For more information, see Visitor Settings.
- For more information on access groups, see Manage Access Groups.
- 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.

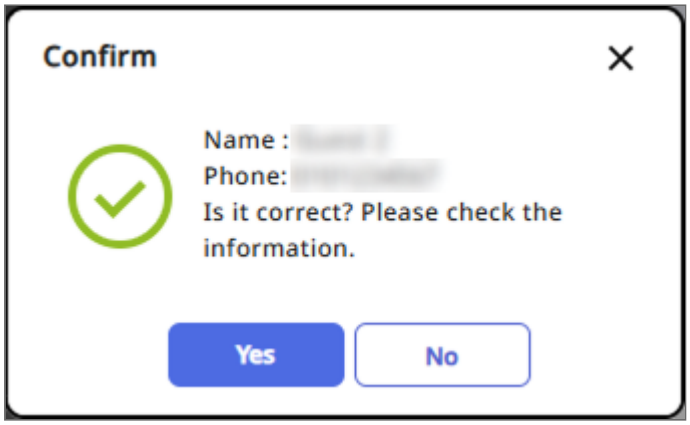
Apply using existing information

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`.



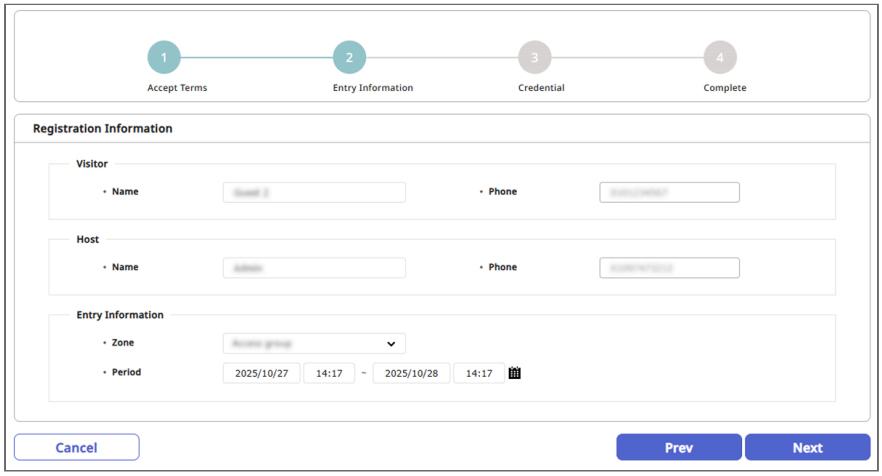
2. Click **Search** below the fingerprint icon in the center of the screen.
3. Scan your fingerprint on the fingerprint scanning device. Use the scanned fingerprint to search for registered users.
4. If a fingerprint matches a previously enrolled visitor, a confirmation message will appear.



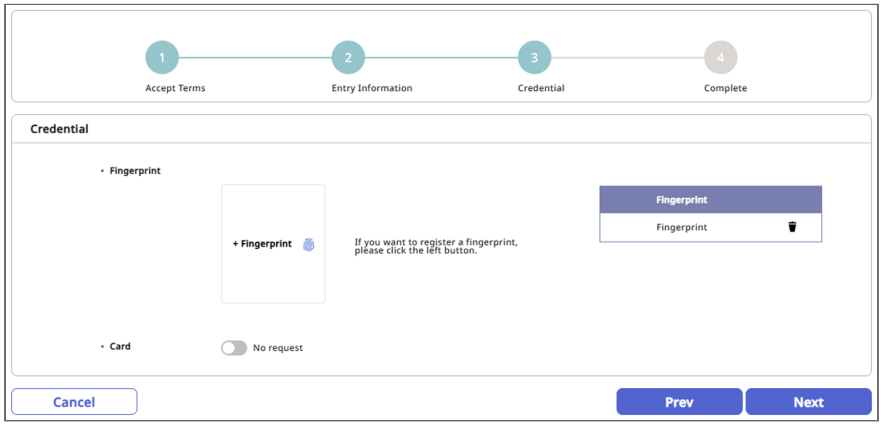
5. If the searched visitor is correct, click the **Yes** button.

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.

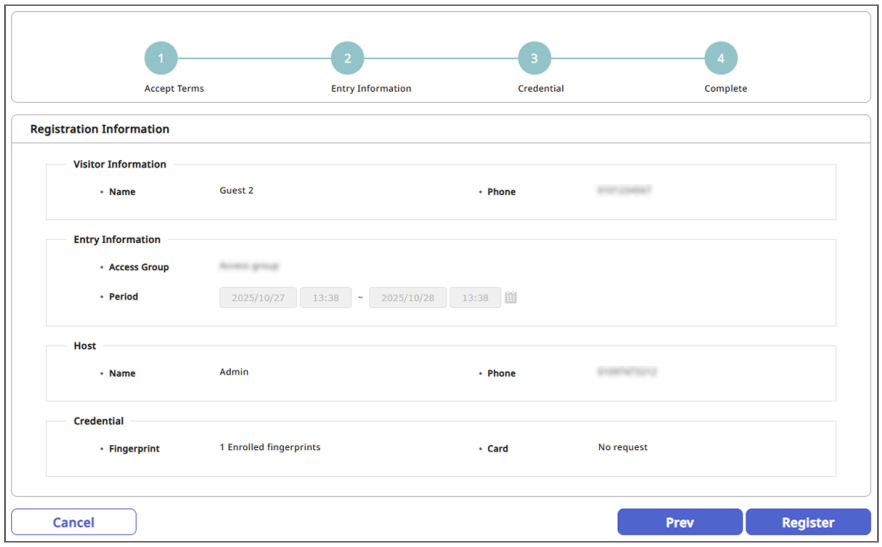
7. Confirm the visit information set during the previous visit. To modify existing information, edit each item and then click the **Next** button in the lower right corner of the screen.



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.



9. After confirming all the information provided, click the **Register** button in the lower right corner of the screen.



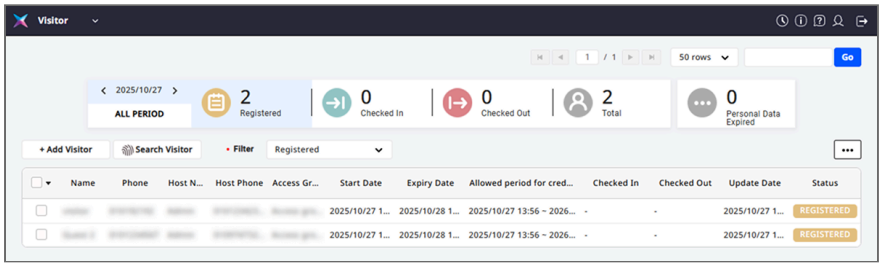
Manage Visitors

You can approve or modify visitor requests. Administrators can also add or delete visitors directly.

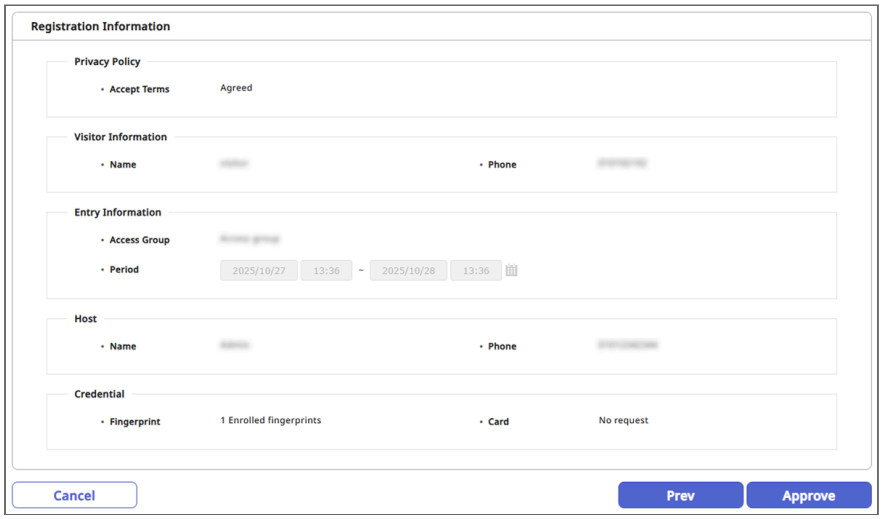
Visitor approval

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.



3. After checking the visitor's information, correct any required items and click **Edit**.
4. Click **Check in** 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.

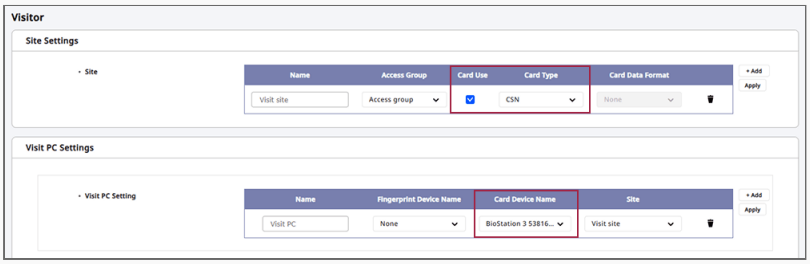


Info

- 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.



- 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, see Approve and enroll a card.
- To set up card usage on the visitor PC, go to **Settings** → **Visitor** menu and the following minimum settings are required. For more information, see Visitor Settings.

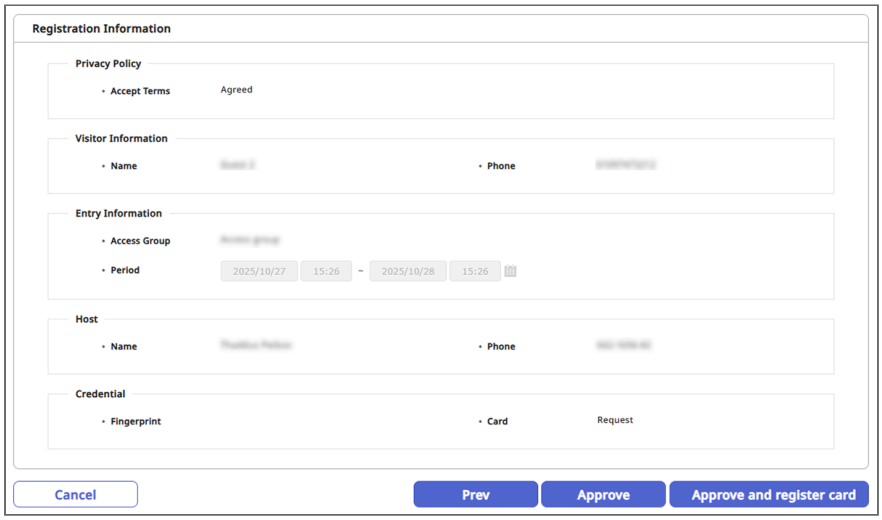


  - **Site Settings** → **Card Use** / **Card Type**
  - **Visit PC Visit PC Setting** → **Card Device Name**

Approve and enroll a 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.

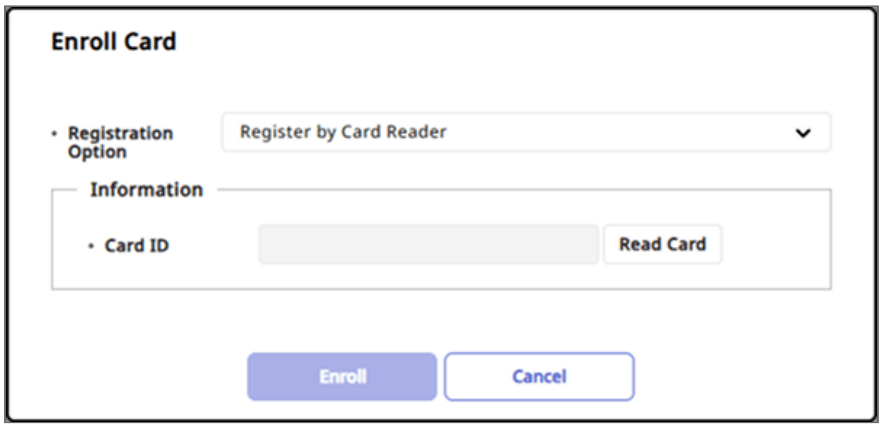


2. When the card registration window appears, select your desired registration method.
   - **Register by Card Reader**
   - **Enter Manually**

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**.

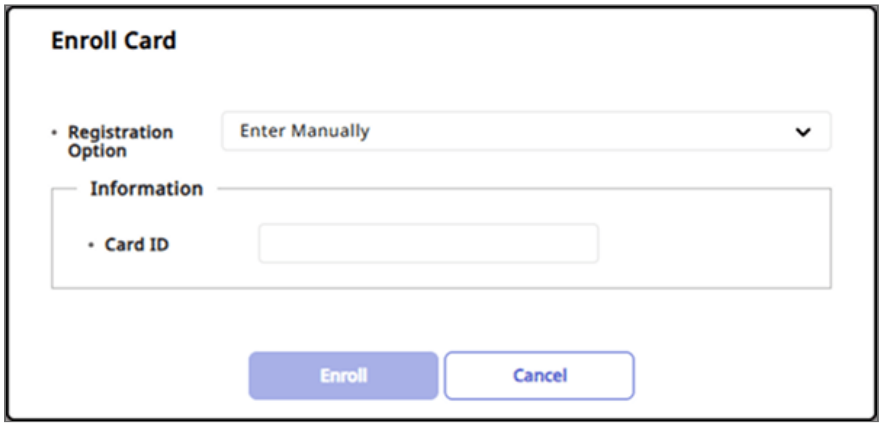


2. To scan the card to enroll, click the **Read Card** button.
3. To enroll the card, click the **Enroll** button.

Enter Manually

You can enroll by directly entering the card number.

1. Select **Enter Manually** for **Registration Option**.

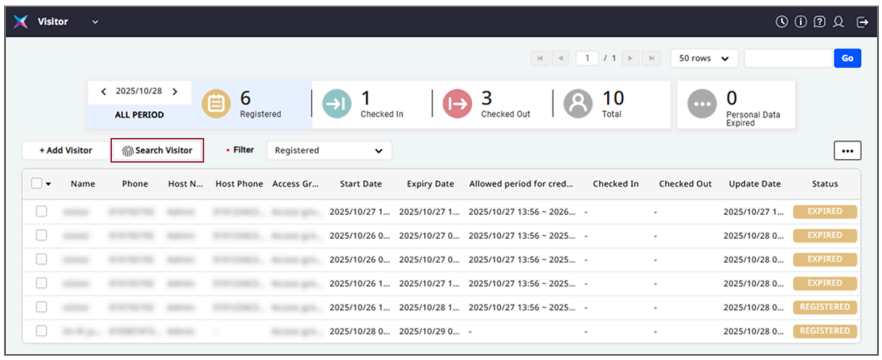


2. Directly enter **Card ID**.
3. To enroll the card, click the **Enroll** button.

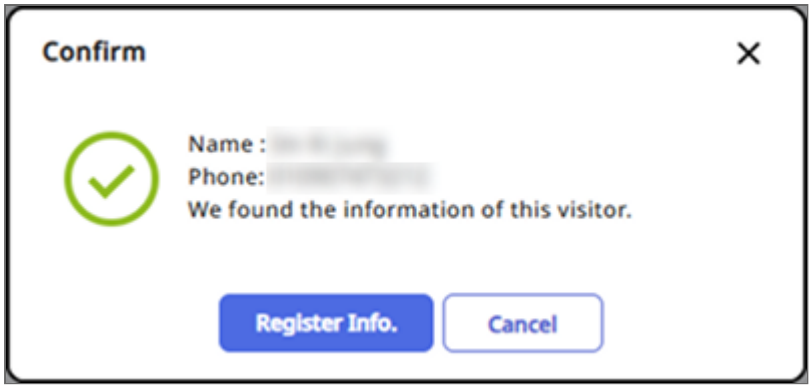
Fingerprint search for visitor approval

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.



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 **Register Info.**.

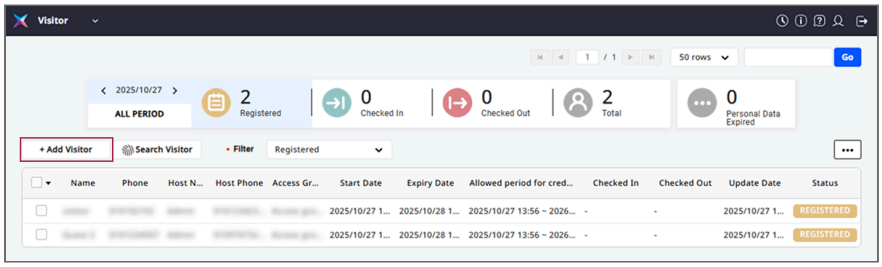


5. After checking the visitor's information, correct any required items and click **Edit**.
6. Click **Check in** at the bottom right of the screen.
7. Check the contents of **Registration Information** and to approve the visit, click the **Approve** button at the bottom right of the screen.

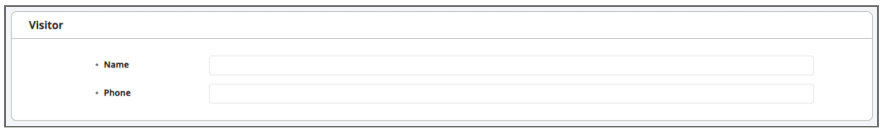
Add visitor

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.



3. Enter the visitor's name and phone number in the **Visitor** section.

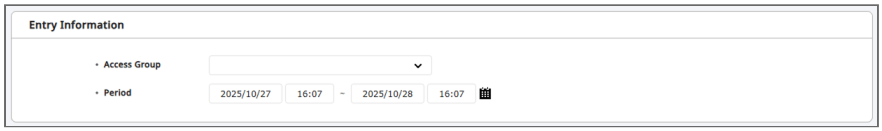


4. Enter the name and phone number of the responsible person for the visit in the **Host** section.



> 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.



> You can only select access groups assigned to the visiting department for the visit PC. For more information, see Visitor Settings.

6. Set the means of access in the **Credential** section.



- **Card**: To use card authentication, set it to **Request**.

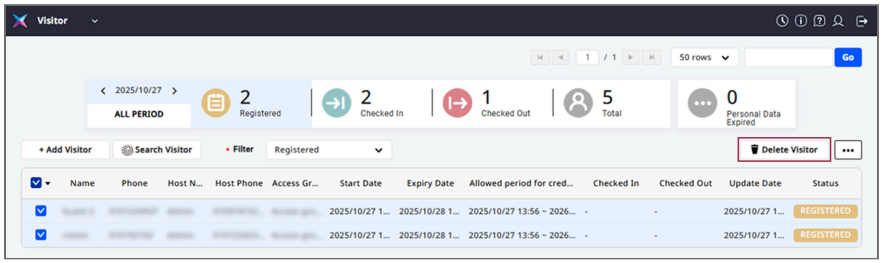
- **Fingerprint**: To use fingerprint authentication, click the **+ Fingerprint** button and then enroll the visitor's fingerprint.

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.
> - For more information on adding custom fields to visitor information, see Visitor Settings.

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.



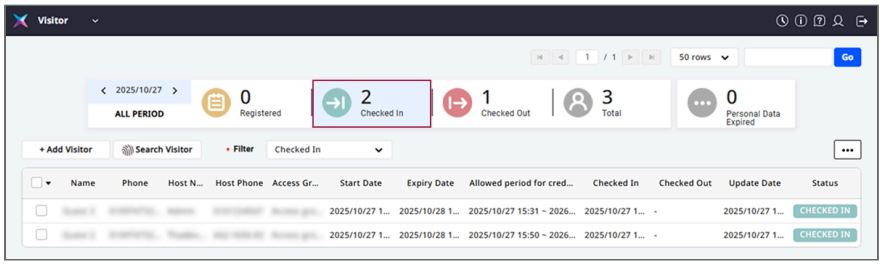
3. Click **Delete Visitor** at the top right of the screen.
4. When the confirmation message appears, click **Yes**.

> **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.

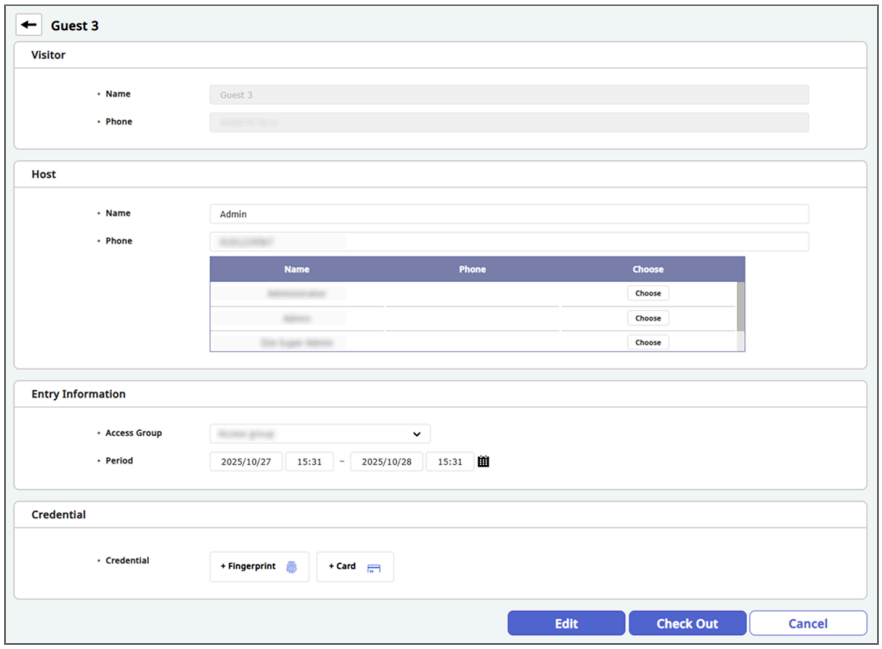
Manage Check-In Visitors

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.



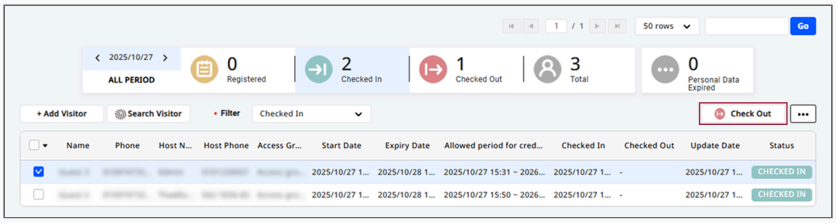
3. Click the visitor in the list to modify or check out.
4. Check the visitor's visit request information.



- 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

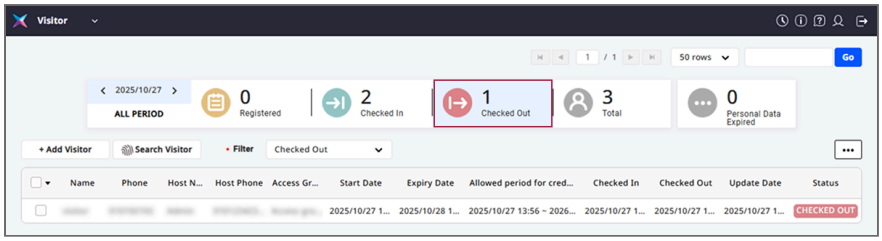
You can also select visitors to check out from the **Check in** list. Click the checkbox for the visitor to check out in the list and then click the **Check Out** button at the top right of the screen.



Manage Visitor Checkouts

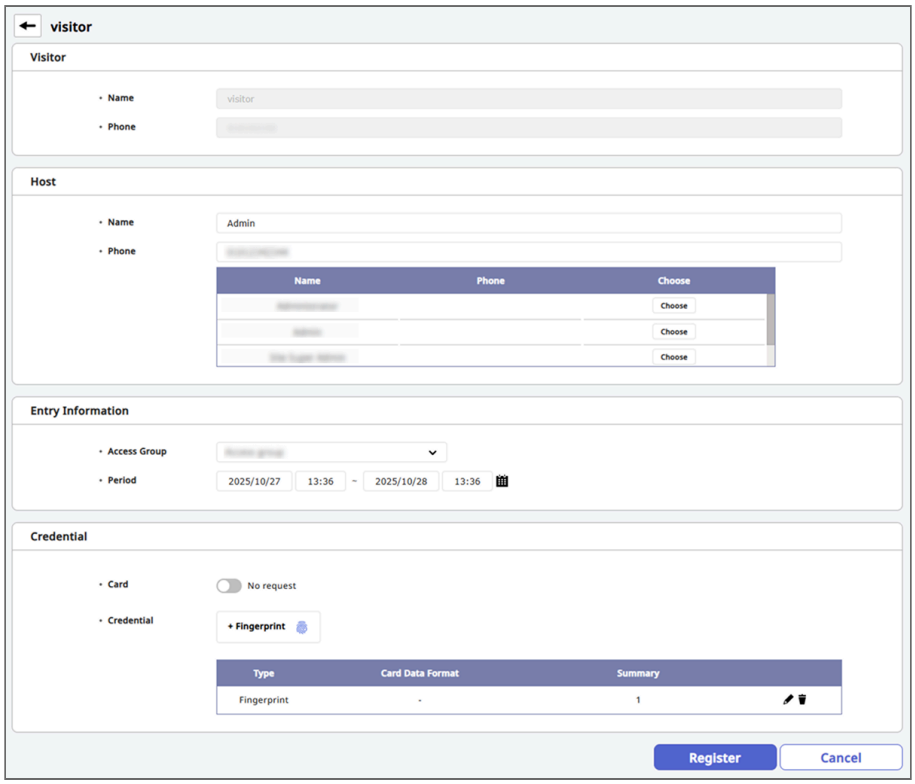
Check the visitors in checkout status and use their visit application information to register a repeat visit.

1. Click **Visitor** on the **Launcher** page.
2. Click the **Check out** tab at the top of the screen.



3. Click the visitor you want to register again from the visitor list.
4. Click **Edit** at the bottom right of the screen.

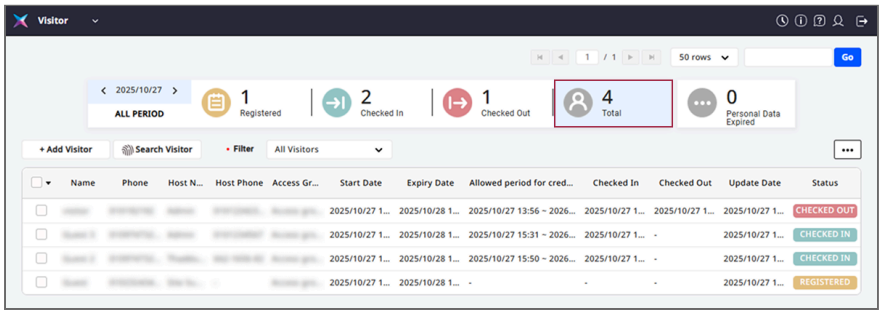
5. If there are items that need correction, modify the individual items and then click the **Enroll** button.



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.



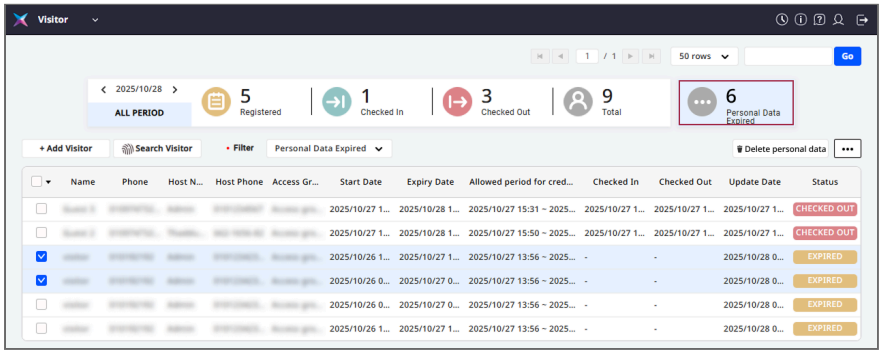
Info

- You can approve visitor requests or add visitors from the overall visitor list. For more information on visitor registration, see Apply to Visit.
- 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.



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, see Register Users.
- For more information on setting the personal data retention period, see Visitor Settings.

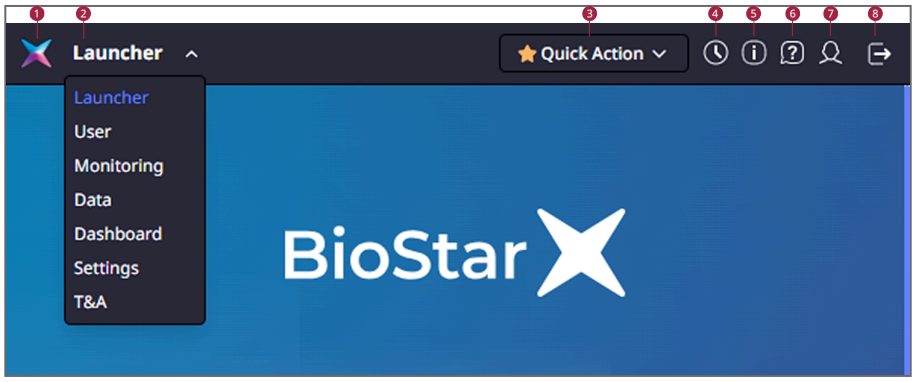
Explore UI

Explore the UI of each page of BioStar X and guide on how to use it. BioStar X offers various features, each easily accessible through the user interface (UI). By exploring the user interface on each page, you can better understand and make full use of BioStar X's features. Following is an overview of BioStar X's main pages and their user interface components.

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.

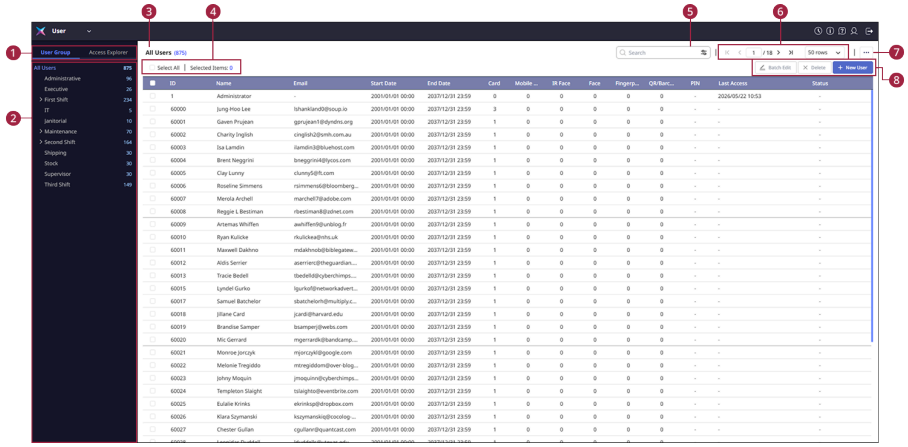
The header area of the screen is used across all pages and provides link buttons to access various features of **BioStar X**.



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. **Quick Action**: Execute the **action** feature set by the server user. Clicking the button displays the action list. For more information, see How to Use the Quick Action.
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. **Account**: Go to **Preferences** or change the password of the currently logged-in user.
   - For more information on the **Preferences** menu, see Configure Preferences.
   - For more information on changing the password of the currently logged-in user, see Setting User Permissions.
8. **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:

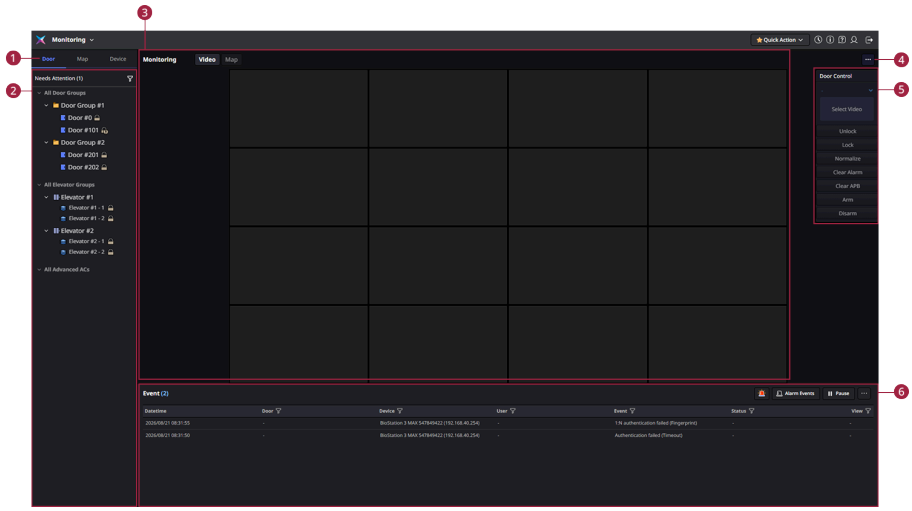


1. Check user groups or access groups.
   - For more information on **User Group**, see Manage User Groups.
   - For more information on **Access Explorer**, see Manage Access Groups.
2. View user groups or access groups in tree structure format. You can expand or collapse the tree structure, and click 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 **Select All** 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 on searching for users, see Explore Users.
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 on selecting view options, refer to Explore Users.
7. Click ⋯ to access various features related to users.
   - **Export**: Save the user list in CSV file or Data file format. For more information on exporting or importing user information, see Export/Import User Information.
   - **Import**: Import user lists in CSV file or Data file format or import facial authentication information. For more information on exporting or importing user information, see Export/Import User Information.
   - **Transfer to Device**: Function to send registered user information to the device. For more information on transferring user information to a device, see Transfer User Information to the Device.
   - **Face Migration**: You can enhance authentication performance by upgrading faces enrolled in older versions of **BioStar X** with the latest algorithm. For more information, see Face Migration.
   - **Column Layout**: Change header items of columns in the user list. For more information on user list column settings, refer to Explore Users.
   - **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 on bulk editing user information, see Edit User Information.
   - **Delete**: Delete selected users. For more information on deleting users, refer to Delete User.

- **New User**: Register new users. For more information, see Register Users.

Monitoring

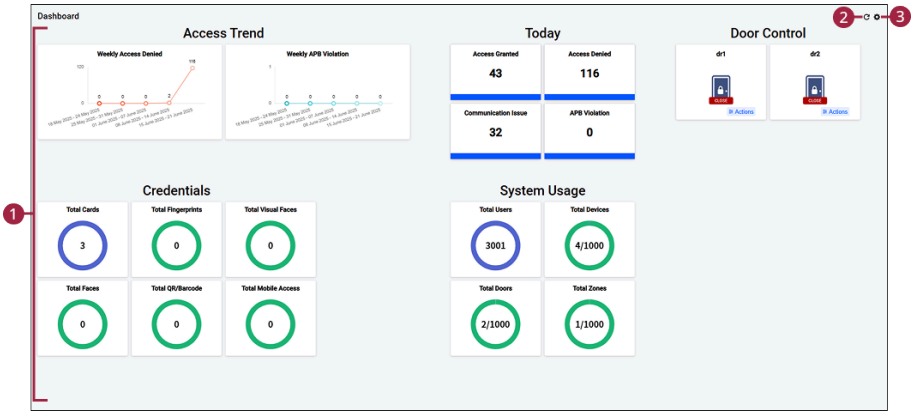
This guide describes you through the user interface (UI) of the **Monitoring** page. You can monitor the security status in real time based on doors, maps, and devices on the **Monitoring** page. You can also check real-time events and take necessary actions. The UI components of the **Monitoring** page 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 on monitoring **Door**, see Monitor Doors.
   - For more information on monitoring **Map**, see Monitor Map.
   - For more information on monitoring **Device**, see Monitor Device.
3. 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 on monitoring camera feeds, see Monitor Video.
   - For more information on map monitoring, see Monitor Map.
4. Click ••• to use the **Close All** feature to close all elements in the video tile.
5. The **control panel** allows you to control the features of the selected door or device. For more information, see Door Control.
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, see Monitor Event.

Dashboard

This guide describes you through the user interface (UI) of the **Dashboard** page.



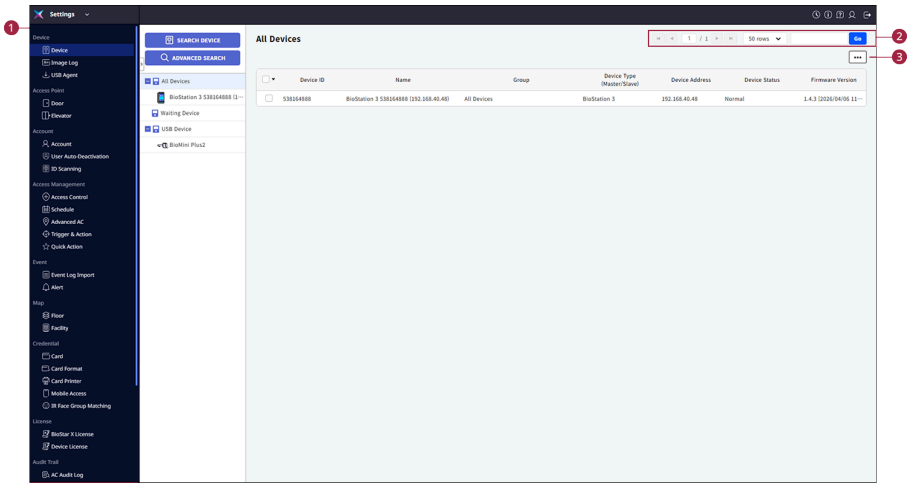
The image above is an example screen and may differ from the actual screen.

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.

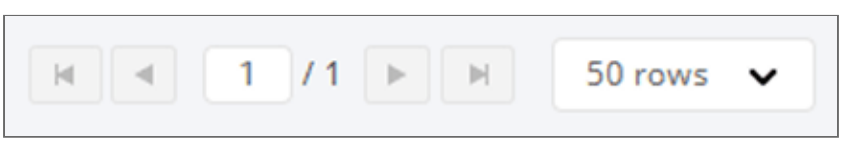
   Set the refresh cycle in **Auto Refresh Interval** in **Dashboard Settings**.
3. **Dashboard Settings**: Add new widgets or set the data and appearance of the added widgets.

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, see Settings.
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.

Use the **BioStar X License Calculator** to resolve complex licensing requirements. The tool helps determine the required license type and quantity.

Base License

The base 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
Maximum Connected IP Devices	1,000	1,000	1,000	1,000	1,000	1,000
Maps	✕	✕	✔	✔	✔	✔
Video	✕	✕	Add on	Add on	Add on	Add on

	Device Manager	Starter	Essential	Advanced	Enterprise	Elite
Advanced Access Control *(Anti-passback, Fire Alarm, Intrusion Alarm, Muster, Occupancy Limit, Elevator, Interlock)*	✕	✕	Add on	Add on	✔	✔
Capacity Upgrade *(Doors/Users/Operators)*	Users, Operators only	✕	Add on	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**.
- **Maximum Operators** refers to the number of users who are granted access permissions to the system.
- If the maximum number of connected IP devices exceeds 1,000, it is recommended to use the **Multi Communications** server.

Capacity Upgrade

License upgrades are available for holders of **Essential**, **Advanced**, **Enterprise**, and **Elite** licenses. License holders of the **Device Manager** can only purchase User and Operator Upgrades.

	Number
Doors	32
Users	5,000
Operators	10

Feature add-ons

The following options are available for individual purchase and can be added to **Essential**, **Advanced**, **Enterprise**, and **Elite** license tiers.

Feature	License Type	Remarks
Multi Communications Server Init	Base License	Includes 1 Multi Communications Server. Supports up to 1,000 IP devices.
Multi Communications Server Add-on	Additional Server	Required to add 1 additional Multi Communications Server. Extends IP device capacity by 1,000 per add-on.
GIS Map	System	You can use the GIS map to set up areas, facilities, and floors.
Video	Camera	Required when integrating third-party VMS. Supports up to 1,000 integrated cameras per system.
Server Matching	ID, Card, Fingerprint, IR face	Server matching method compares the ID, card, fingerprint, and IR face stored on the device to the credentials stored in the server database.
Visitor	System	Administrators and operators can track or control visitor access.
Directory Integration	System	Supports integration with directory services for centralized user management.
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 base 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 (billed annually)	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, see Plugin.

Feature	License Type	Remarks
Attendance Management (T&A)	Standard	Supports up to 500 users.
	Enterprise	There is no limit on the number of users.

Info

Time & attendance (T&A) users follow the base license limit and are allowed up to the maximum user count permitted by the **time & attendance** edition. (e.g., 500 users for the Standard edition)

Advanced Access Control

Advanced access control consists of the following 7 individual features, and you can select and purchase only the features you need. **Essential** and **Advanced** license tiers offer these as add-on options, while **Enterprise** and **Elite** license tiers include all 7 features by default.

Feature	License Type	Remarks
APB(Anti-passback)	System	-
Fire Alarm	System	-
Intrusion Alarm	System	-
Muster	System	-
Occupancy Limit	System	-
Elevator	System	-
Interlock	System	-

- Scheduled Lock(Scheduled Lock) and Scheduled Unlock(Scheduled Unlock) are basic access control features that do not require a license and are always available separately from the 7 features above.
- Customers who previously purchased the Advanced Access Control package can continue to use it. From new purchases onward, the 7 features can be selected and purchased individually.

Device License

Device licenses can be purchased individually and can be added regardless of the base 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
Camera QR	Device	BioStation 3 Max, XPass Q2, BioStation 3, X-Station 2	-
Multi Face Authentication	Device	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

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

Open Source License

This product contains open-source software. Source code subject to GPL, LGPL, MPL, and other open source licenses requiring source code distribution can be requested from the Suprema Global Technical Support Team.

The source code of this product can be requested from the Suprema Global Technical Support Team for 3 years from the final delivery date of the product.

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

ffmpeg

BioStar X includes ffmpeg (https://ffmpeg.org) for video file conversion and probing. It ships two ffmpeg command-line binaries, *ffmpeg.exe* and *ffprobe.exe*; both are built from the single ffmpeg source tarball below (ffprobe is part of the ffmpeg project, not a separate component).

- Component: ffmpeg (ffmpeg.exe, ffprobe.exe)
- Version: 8.1
- License: GNU Lesser General Public License v2.1

  Full text: see COPYING.LGPLv2.1
- Source code: ffmpeg-8.1.tar.xz
- Upstream URL: ffmpeg-8.1.tar.xz
- SHA-256: b072aed6871998cce9b36e7774033105ca29e33632be5b6347f3206898e0756a

Build configuration:

```
./configure \
  --arch=x86_64 \
  --target-os=mingw64 \
  --disable-gpl \
  --disable-nonfree \
  --disable-libx264 \
  --disable-libx265 \
  --disable-libxvid \
  --enable-mediafoundation \
  --enable-libmp3lame \
  --disable-doc \
  --disable-debug \
  --enable-small \
  --pkg-config-flags=--static \
  --extra-ldflags="-static"
```

Modifications: None. Binary built from vanilla upstream source tarball.

Encoders used by **BioStar X**:

- h264_mf (H.264 via Windows Media Foundation)
- libmp3lame (MP3 audio, LGPL)

libmp3lame

BioStar X uses libmp3lame for MP3 audio encoding.

- Component: libmp3lame (LAME MP3 Encoder)
- Version: 3.100
- License: GNU Lesser General Public License v2.1

  Full text: see COPYING.LGPLv2.1 (same LGPL v2.1 version as ffmpeg)
- Source code: lame-3.100.tar.gz
- Upstream URL: lame-3.100.tar.gz
- SHA-256: ddfe36cab873794038ae2c1210557ad34857a4b6bdc515785d1da9e175b1da1e

Modifications: None. Vanilla upstream source tarball, statically linked into both *ffmpeg.exe* and *ffprobe.exe* via `--enable-libmp3lame` at build time.

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA

Tel: +82 31 783 4502 | Fax: +82 31 783 4503 | Inquiry: sales_sys@supremainc.com

For more information about Suprema's global branch offices,
visit the webpage below by scanning the QR code.
https://supremainc.com/en/about/global-office.asp

© 2026 Suprema Inc. Suprema and identifying product names and numbers herein are registered trade marks of Suprema, Inc.
All non-Suprema brands and product names are trademarks or registered trademarks of their respective companies.
Product appearance, build status and/or specifications are subject to change without notice.