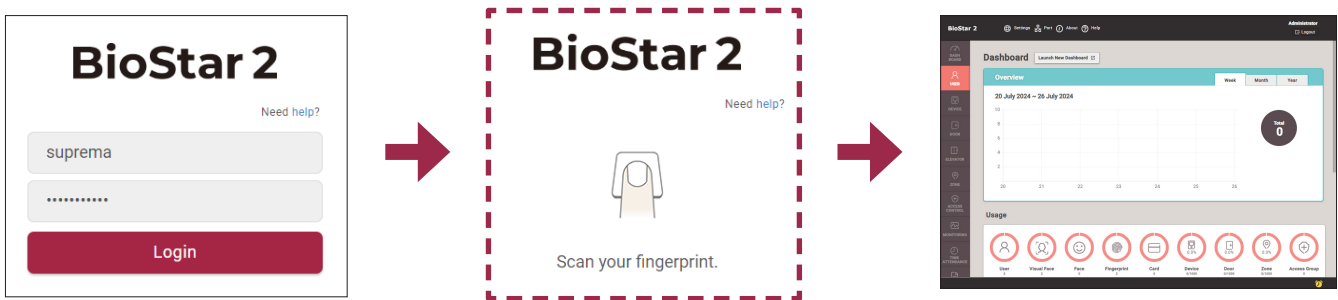


Logging in Biostar 2 with Multi-Factor Authentication

If users feel that using only an ID and password to log in to BioStar 2 is not secure enough or want to enhance their account security, they can use the **Multi-Factor Auth for Login** feature to improve their account security.

Multi-Factor Auth for Login enhances user account security by adding a fingerprint authentication step using a fingerprint scanner to the existing ID and password login method.



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



- To use the **Multi-Factor Auth for Login** feature, a fingerprint scanner that supports multi-factor authentication login must be connected to the BioStar 2 client.

The supported fingerprint scanners are as follows:

- BioMini
- BioMini Plus 2

Before Using



When using **Multi-Factor Auth for Login** with the main Administrator (ID 1) account, if fingerprint authentication becomes unavailable, the main Administrator account may be permanently unable to log in. Please be cautious.

- If login becomes impossible due to fingerprint issues, please contact Suprema Technical Support (<https://support.supremainc.com>).



- When a user with **Multi-Factor Auth for Login** enabled accesses BioStar 2 through the **BioStar 2 Cloud**, fingerprint authentication for login is not supported, so **Multi-Factor Auth for Login** cannot be used.
- **Multi-Factor Auth for Login** cannot be used if the **Use for BioStar 2 Login** option is enabled for an Active Directory server account.
- Users with **Multi-Factor Auth for Login** enabled cannot be registered for BioStar 2 services other than BioStar 2 AC.

How to Use Multi-Factor Authentication Login

- 1 Click **USER**.
- 2 Click on the user who needs to use **Multi-Factor Auth for Login**.
- 3 Set **Multi-Factor Auth for Login** to **Use**.



- Before using the **Multi-Factor Auth for Login** feature, the following conditions must be met:
 - The user who intends to use this feature must have an enrolled fingerprint for authentication.
 - **Operator Level, Login ID, and Password** must be set.

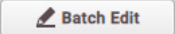

The screenshot shows a user profile page for 'David'. The 'Information' section includes fields for Name (David), Department (BTS), ID (5), Group (All Users), and Period (2001/01/01 00:00 to 2037/12/31 23:59). The 'Permission' section includes fields for Access Group, Operator Level (User), Password, User IP, Login ID (david23), and Confirm Password. The 'Multi-Factor Auth for Login' toggle is set to 'Use' and is highlighted with a red box.

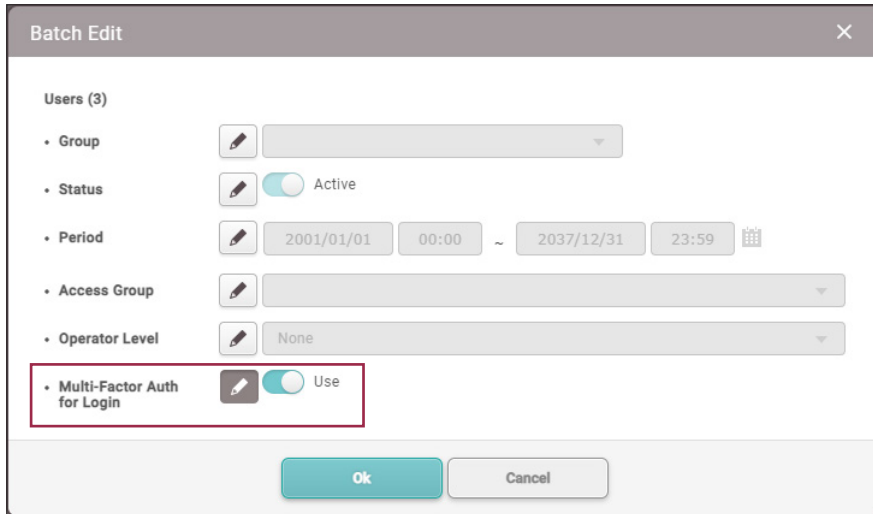
The image above is an example screen and may differ from the actual screen.

- 4 Click **Apply** to save the settings.

How to Set Up for Multiple Users at Once

In batch editing, multiple users can be selected and set up at once.

- 1 Click **USER**.
- 2 In the user list, check and select the users to configure, then click .
- 3 Click the  for **Multi-Factor Auth for Login** to change to edit mode, then set it to **Use** and click **Ok**.



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

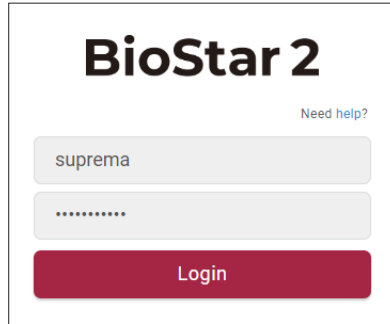
- If any of the selected users do not meet the conditions required to set **Multi-Factor Auth for Login** to **Use**, a pop-up message will display '**Not applicable user(s)**'. Please check the conditions required for the settings and try again.



- Before using the **Multi-Factor Auth for Login** feature, the following conditions must be met:
 - The user who intends to use this feature must have an enrolled fingerprint for authentication.
 - **Operator Level**, **Login ID**, and **Password** must be set.

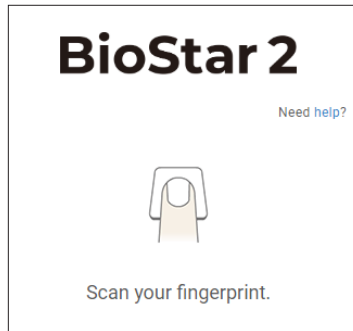
Logging in with Multi-Factor Authentication

1 Enter the user ID and password on the BioStar 2 login screen and login.



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

2 The fingerprint input screen will appear. Place the enrolled finger on the fingerprint scanner to scan your fingerprint.



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



- 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.
- In the case of authentication failure, click the **Retry** to attempt fingerprint authentication again. Up to two retry attempts are allowed.
 - If authentication fails after two retry attempts, the process will revert to the ID and Password login step.

