www.supremainc.com

NEW FEATURE GUIDE

BioStar 2.2.x

English

Version 1.00

Contents

- This document describes the new features in BioStar 2.2 and 2.2.1.
- Please refer to BioStar 2 administrator's manual for detailed instructions on how to use each feature.

AC & TA License Policy

BioStar 2.2 implemented the license policy for particular users that require additional features. Please check the AC and TA license policy shown below.

Feature		License Type		
		Free	Access Control Standard	Time and Attendance Standard
Access Control	Number of devices	1000	1000	1000
	Number of clients	100	100	100
	Number of access groups	128	128	128
	Zones	Door anti-passback	Fire alarm (local/global), Anti-passback (local/global), Scheduled lock zone, Scheduled unlock zone	Door anti-passback
	Server matching	Not supported	Supported	Not supported
	Mobile app	Supported	Supported	Supported
Time and Attendance	Number of schedules	1	1	2 or more
	Users per schedule	99	99	100 or more

BioStar 2.2.0

BioStation A2 - Biometric device boasting stellar performance

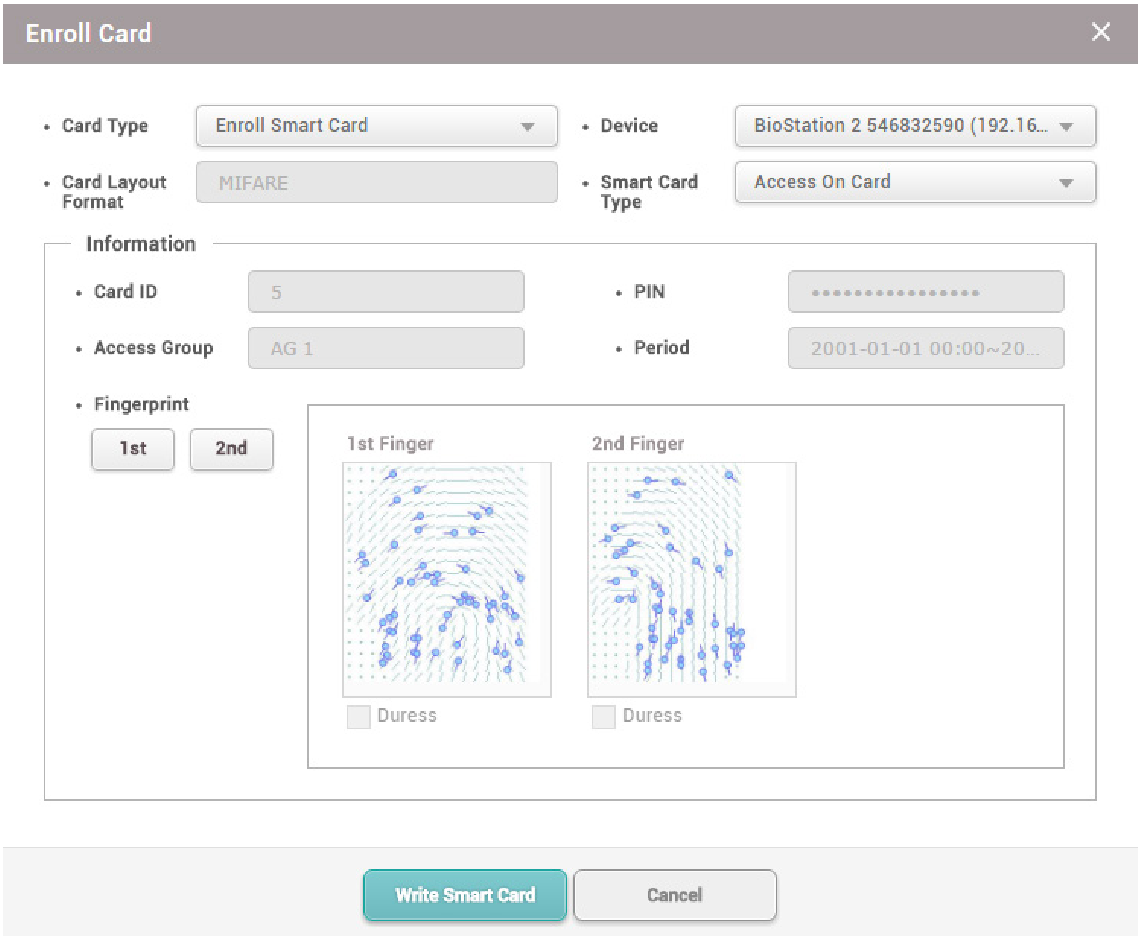
BioStation A2 is an access control and time & attendance device with most powerful performance up to date. This device not only holds a quad-core CPU and 8GB of memory but also mounts the new OP5 sensor and fingerprint recognition algorithm to demonstrate incredible performance. It can match up to 150,000 fingerprints per second and can hold up to 500,000 user information. Furthermore, it provides all the features that a user would require such as live finger detection (LFD), image log, and the time and attendance function.

Access on Card - A safer Template on Card with a Secure ID.

Access on card is similar to the template on card which is supported in BioStar 1. These two types of cards both save fingerprint template(s) on the card, but access on cards store a Secure ID instead of a CSN (Card Serial Number). The CSN is written in an unencrypted area which could be a security risk because it can be easily duplicated. To avoid this risk, access on card records the user ID in a secure area instead of using a CSN. Other people cannot duplicate the card since encrypted user ID information is utilized. Furthermore, a user can be authenticated without storing the user's information in the server or the device which provides superior security compared to other card types.

Access on card not only saves the user ID and fingerprint template, but also stores the user's access group, period, and PIN.

Fingerprint Template | Secure ID (User ID) | Period | PIN | Access Group



Enroll Card

Card Type	Enroll Smart Card	Device	BioStation 2 546832590 (192.16...
Card Layout Format	MIFARE	Smart Card Type	Access On Card

Information

Card ID	5	PIN	••••••••••••••••
Access Group	AG 1	Period	2001-01-01 00:00~20...

Fingerprint

[Access on card enrollment screen]

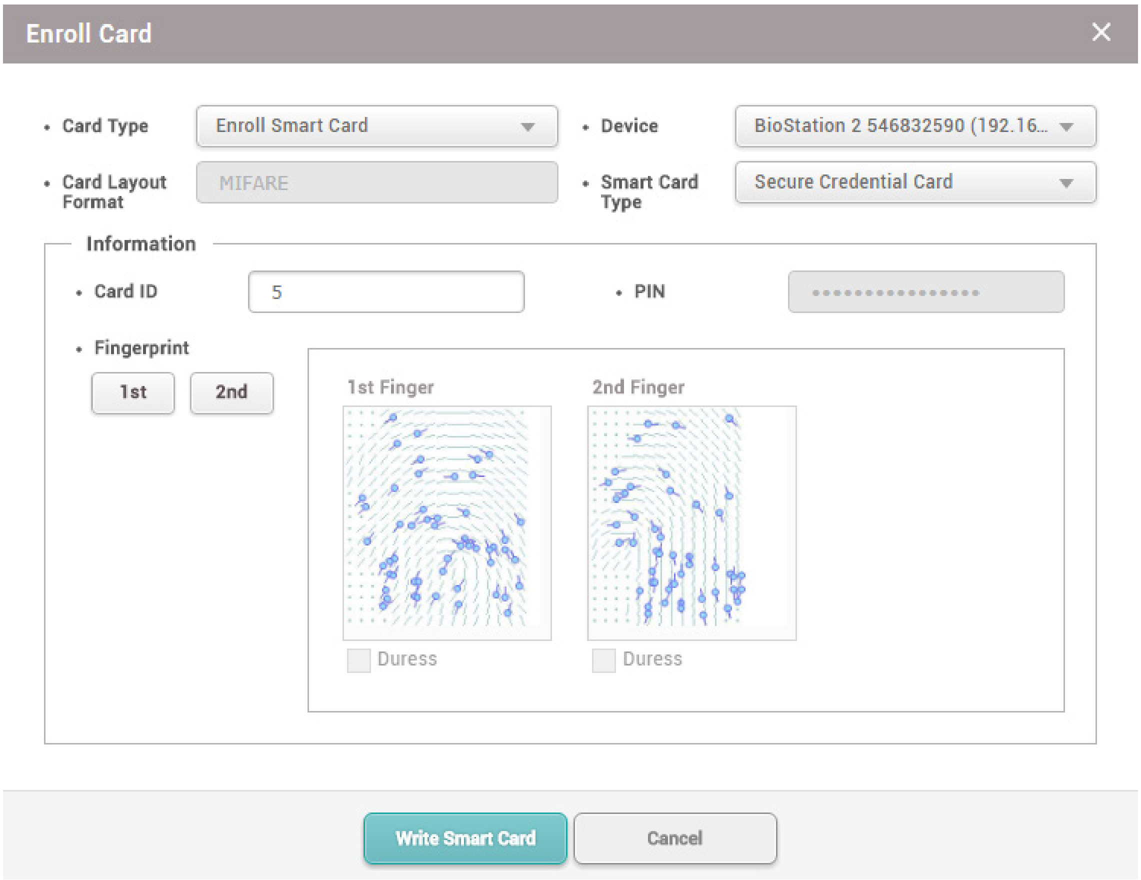
Note

- 13.56 MHz iCLASS/MIFARE/DESFire/DESFire EV1 Cards can be used as an Access on Card

Secure Credential Card - More convenient than Access on Card

Access on card has excellent security but comes with the inconvenience of update requirements which is necessary each time when the user access group is altered. The secure credential card solves this problem.
Similar to the access on card, a secure credential card utilizes a Secure ID to assign a unique ID and stores the fingerprint template, user ID, and PIN. The difference is that the user access group information is stored in the device. The security level may be lower with a secure credential card since the device stores the user's access group, but it prevents the inconvenience of rewriting the card every time a user's access group information is modified.

Fingerprint Template	Secure ID (Modifiable)	User ID	PIN



Enroll Card

- Card Type: Enroll Smart Card
- Device: BioStation 2 546832590 (192.16...
- Card Layout Format: MIFARE
- Smart Card Type: Secure Credential Card

Information

- Card ID: 5
- PIN: ••••••••••••••••
- Fingerprint

[Secure Credential Card enrollment screen]

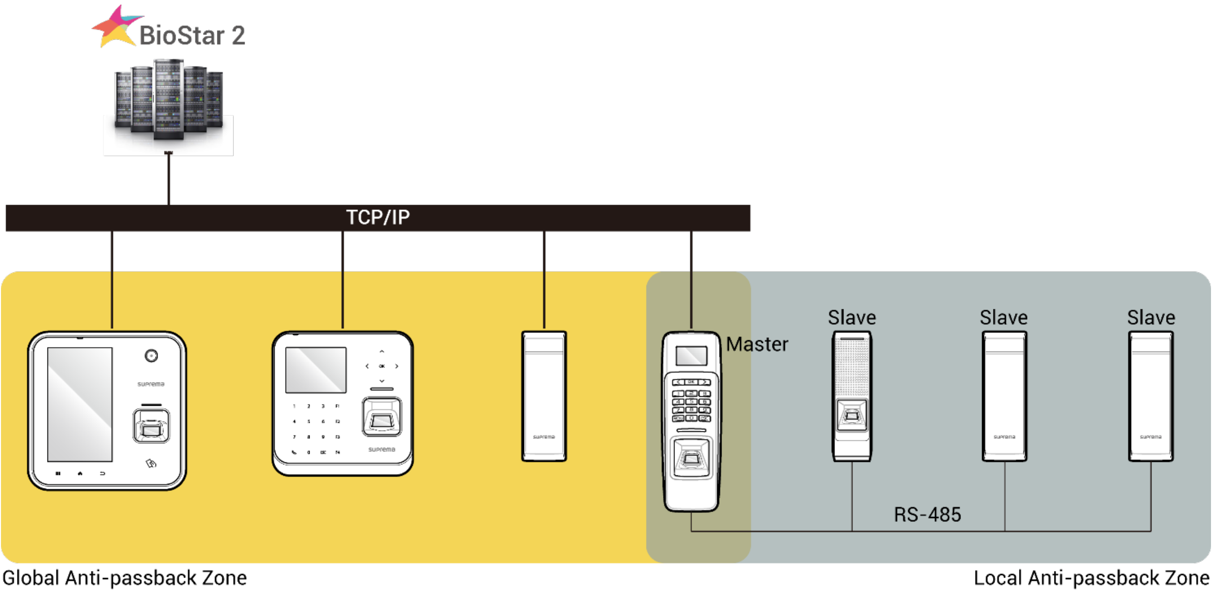
ⓘ Note

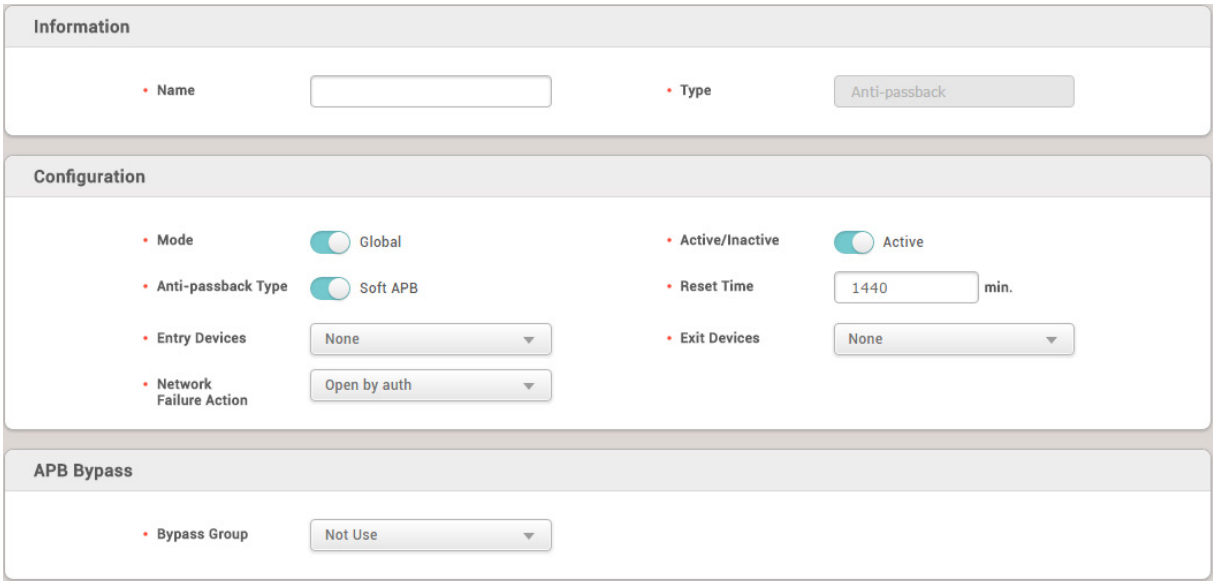
- Only 13.56 MHz MIFARE cards can be used.

Global Anti-passback – Ethernet is all you need

The local anti-passback zone supported in BioStar 2.1 still requires the master device to be connected with the slave device with RS-485 cables. RS-485 is a useful communication method but requires the cumbersome task of rewiring and has the limitation of connecting 31 slave devices to one master device.

BioStar 2.2 can configure a global anti-passback zone solely with Ethernet cable connections. In this setup, BioStar 2 takes the role of master device for the devices connected via TCP/IP and hence the troublesome task of connecting all slave devices to the master device with RS-485 cables is reduced and the benefits of TCP/IP communication speed and security can be utilized. Moreover, configuration is more flexible because there are no restrictions for the number of devices in a single zone. There are several backup options to choose in case the network is unstable as well.





Information

• Name		• Type	Anti-passback

Configuration

• Mode	Global	• Active/Inactive	Active
• Anti-passback Type	Soft APB	• Reset Time	1440 min.
• Entry Devices	None	• Exit Devices	None
• Network Failure Action	Open by auth		

APB Bypass

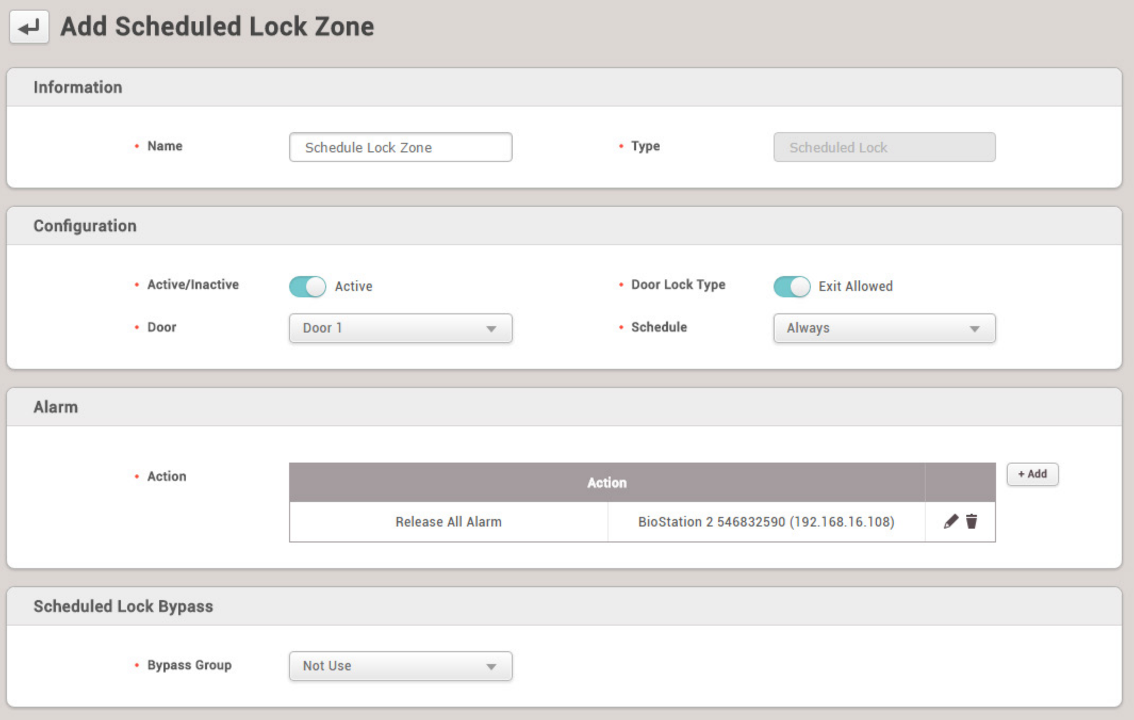
• Bypass Group	Not Use

[Anti-passback configuration screen]

Scheduled Lock and Unlock Zone – Opening and closing in desired times

Scheduled lock and unlock zones which restricts door entrance can be configured in BioStar 2.2. These two zones are different from configuring user access rights since it assigns allowable entrance times based on doors.
A scheduled lock zone can be configured to restrict entrance by users without access privileges but allow exits during the specified schedule. A scheduled unlock zone can allow the door lock to be open for the configured schedule. Therefore, you could configure this zone so that users may enter without authentication.

A scheduled lock zone can be used for areas such as server rooms to restrict access excluding specific users or user groups. Scheduled unlock zones can be applied on areas such as conference rooms or restaurant entrances which have frequent entries in a specified schedule by users that do not require special entrance privileges.



Add Scheduled Lock Zone

Information

- Name: Schedule Lock Zone
- Type: Scheduled Lock

Configuration

- Active/Inactive: Active
- Door Lock Type: Exit Allowed
- Door: Door 1
- Schedule: Always

Alarm

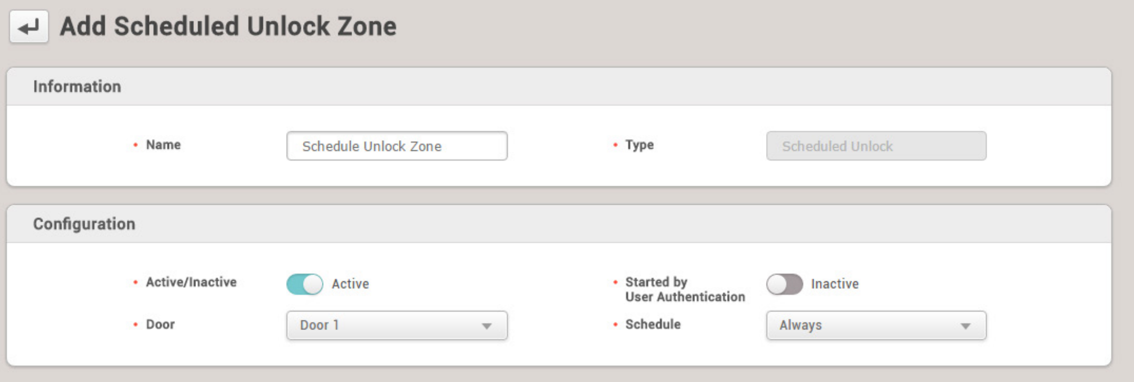
- Action

Action		
Release All Alarm	BioStation 2 546832590 (192.168.16.108)	

Scheduled Lock Bypass

- Bypass Group: Not Use

[Scheduled lock zone configuration screen]



Add Scheduled Unlock Zone

Information

- Name: Schedule Unlock Zone
- Type: Scheduled Unlock

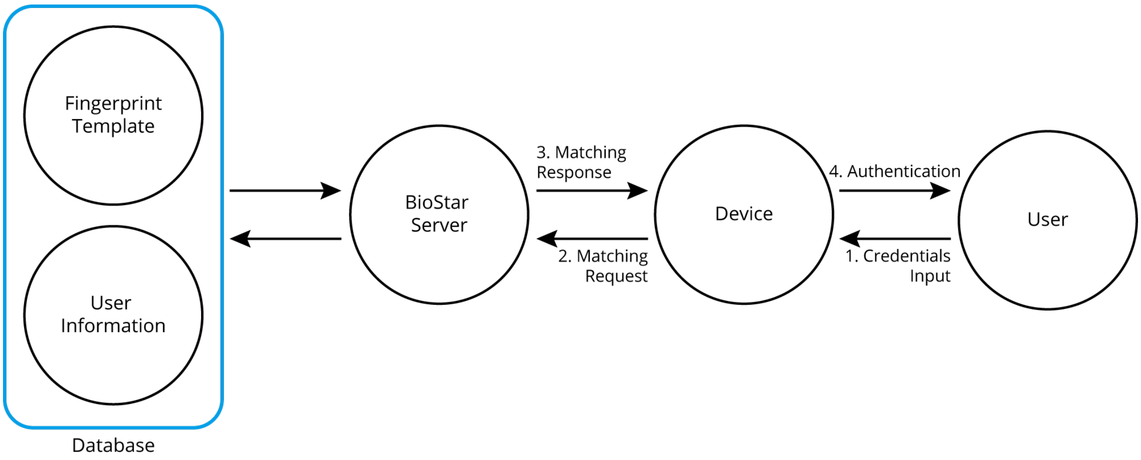
Configuration

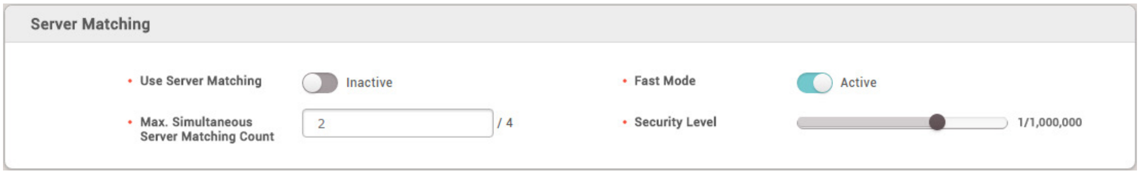
- Active/Inactive: Active
- Started by User Authentication: Inactive
- Door: Door 1
- Schedule: Always

[Scheduled unlock zone configuration screen]

Server Matching – Matching fingerprints on the server

Server matching can now be used in BioStar 2.2. When server matching is used, the users' credential information are stored in the PC where BioStar 2 is installed so there is no reason to worry about storage space or device damage. Furthermore, if the user's credential information is stored in the device, the device can take up the authentication role if the TCP/IP connection is lost.




Server Matching

- Use Server Matching: Inactive
- Max. Simultaneous Server Matching Count: 2 / 4
- Fast Mode: Active
- Security Level: 1/1,000,000

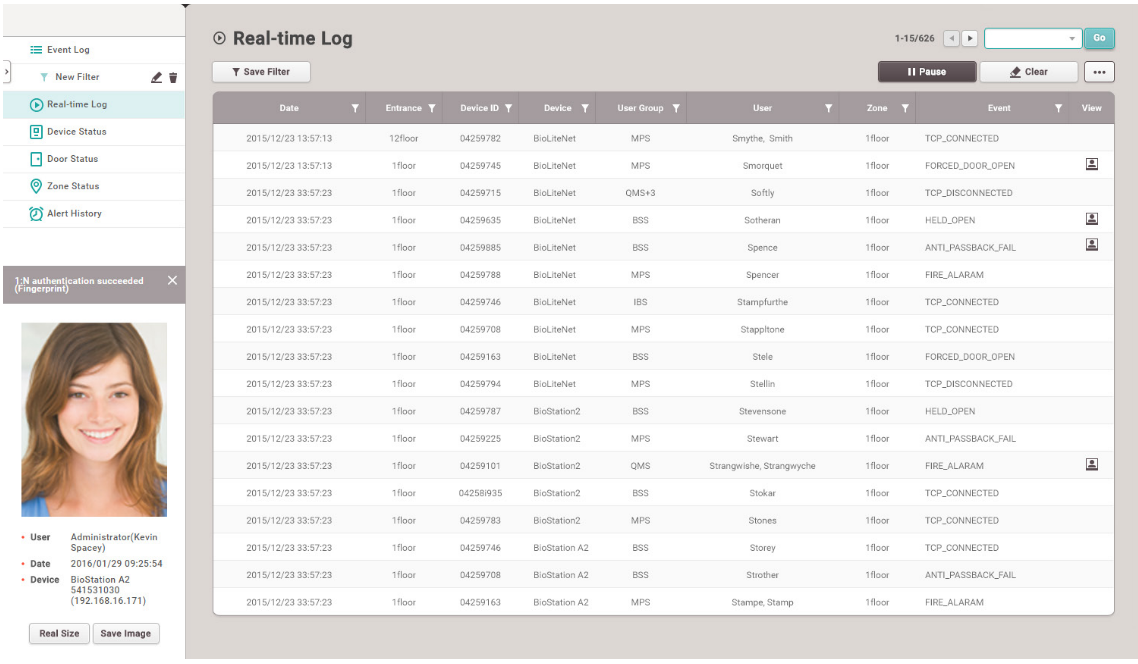
[Server matching configuration screen]

Note

- Access control standard license has to be purchased to use this feature.

Image Log – A picture is worth a thousand words

If you are using a device with a built-in camera, you can configure it to record an image log when a security event such as user authentication occurs. The schedule and event in which image logs will be recorded can be configured in BioStar 2.2 and the delete cycle can be configured as well to avoid filling up the disk space.



1:N authentication succeeded (Fingerprint)

- **User** Administrator(Kevin Spacey)
- **Date** 2016/01/29 09:25:54
- **Device** BioStation A2 541531030 (192.168.16.171)

Date	Entrance	Device ID	Device	User Group	User	Zone	Event	View
2015/12/23 13:57:13	12floor	04259782	BioLiteNet	MPS	Smythe, Smith	1floor	TCP_CONNECTED	
2015/12/23 13:57:13	1floor	04259745	BioLiteNet	MPS	Smorquet	1floor	FORCED_DOOR_OPEN	👤
2015/12/23 33:57:23	1floor	04259715	BioLiteNet	QMS+3	Softly	1floor	TCP_DISCONNECTED	
2015/12/23 33:57:23	1floor	04259635	BioLiteNet	BSS	Sotheran	1floor	HELD_OPEN	👤
2015/12/23 33:57:23	1floor	04259885	BioLiteNet	BSS	Spence	1floor	ANTI_PASSBACK_FAIL	👤
2015/12/23 33:57:23	1floor	04259788	BioLiteNet	MPS	Spencer	1floor	FIRE_ALARAM	
2015/12/23 33:57:23	1floor	04259746	BioLiteNet	IBS	Stampfurthe	1floor	TCP_CONNECTED	
2015/12/23 33:57:23	1floor	04259708	BioLiteNet	MPS	Stappltone	1floor	TCP_CONNECTED	
2015/12/23 33:57:23	1floor	04259163	BioLiteNet	BSS	Stele	1floor	FORCED_DOOR_OPEN	
2015/12/23 33:57:23	1floor	04259794	BioLiteNet	MPS	Stellin	1floor	TCP_DISCONNECTED	
2015/12/23 33:57:23	1floor	04259787	BioStation2	BSS	Stevensone	1floor	HELD_OPEN	
2015/12/23 33:57:23	1floor	04259225	BioStation2	MPS	Stewart	1floor	ANTI_PASSBACK_FAIL	
2015/12/23 33:57:23	1floor	04259101	BioStation2	QMS	Strangwishe, Strangwyche	1floor	FIRE_ALARAM	👤
2015/12/23 33:57:23	1floor	04258i935	BioStation2	BSS	Stokar	1floor	TCP_CONNECTED	
2015/12/23 33:57:23	1floor	04259783	BioStation2	MPS	Stones	1floor	TCP_CONNECTED	
2015/12/23 33:57:23	1floor	04259746	BioStation A2	BSS	Storey	1floor	TCP_CONNECTED	
2015/12/23 33:57:23	1floor	04259708	BioStation A2	BSS	Strother	1floor	ANTI_PASSBACK_FAIL	
2015/12/23 33:57:23	1floor	04259163	BioStation A2	MPS	Stampe, Stamp	1floor	FIRE_ALARAM	

BioStar 2.2.1

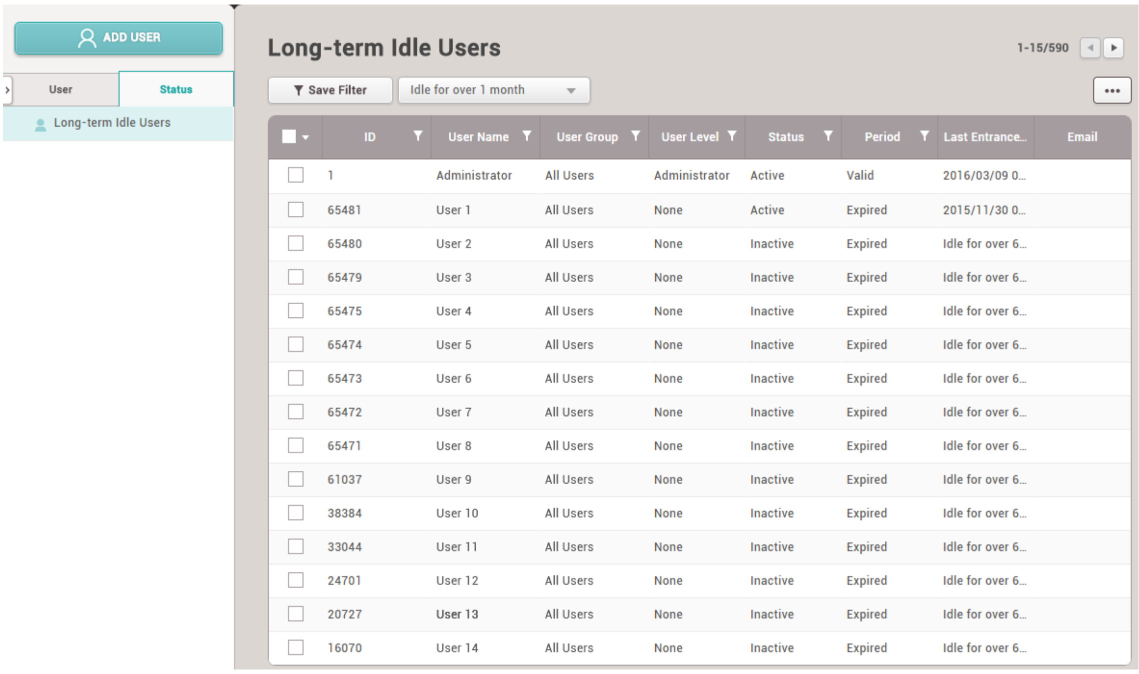
BioStation L2 – A powerful affordable biometric device

BioStation L2 is an access control and time & attendance device developed based on Suprema's latest fingerprint recognition technology and hardware. This device not only has a quad-core CPU and 2GB of memory but also mounts the OP5 sensor and the latest fingerprint recognition algorithm which are also used in BioStation A2. Live fingerprint detection and time & attendance management features are both included as well, which adds to its superb performance and allows this affordable device to be used in diverse environments.

Management of Long-term Idle Users – More convenient user management

One of the hurdles in access control system management is to find an effective way to manage information of users such as temporary or resigned employees and those who were assigned temporary entrance rights.

To make this task more manageable, the long-term idle user management feature was added to allow the administrator to see idle users for a specific period (1~6 months) in a single glance, and to modify and delete user information.



Long-term Idle Users

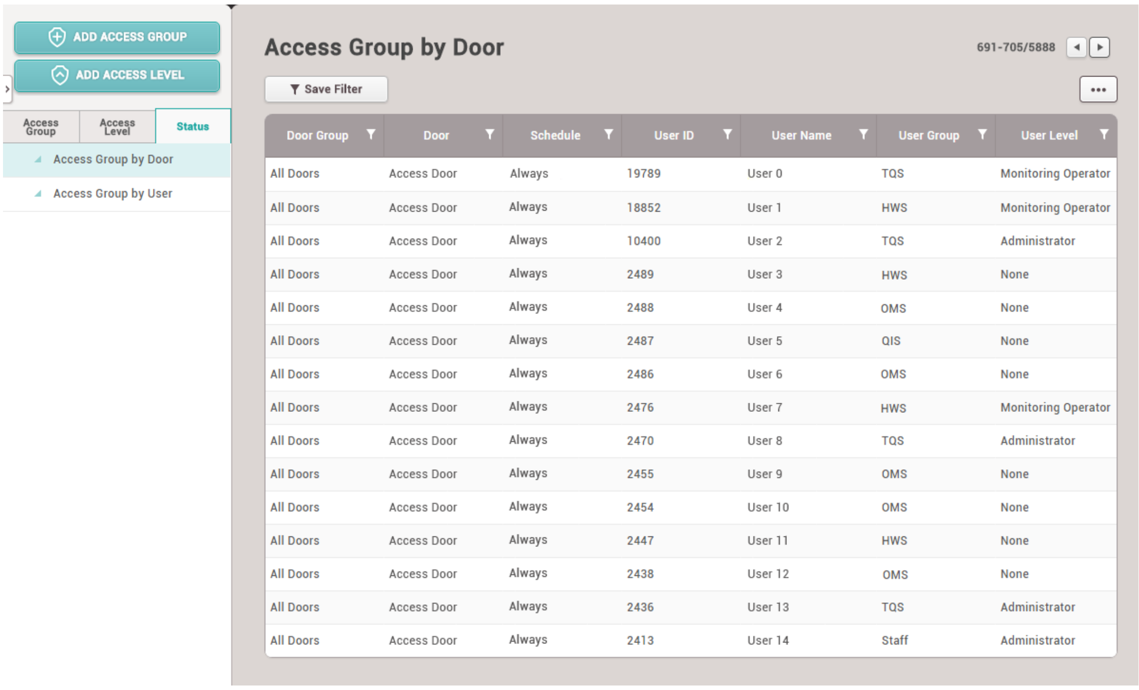
Idle for over 1 month

□	ID	User Name	User Group	User Level	Status	Period	Last Entrance…	Email
□	1	Administrator	All Users	Administrator	Active	Valid	2016/03/09 0…	
□	65481	User 1	All Users	None	Active	Expired	2015/11/30 0…	
□	65480	User 2	All Users	None	Inactive	Expired	Idle for over 6…	
□	65479	User 3	All Users	None	Inactive	Expired	Idle for over 6…	
□	65475	User 4	All Users	None	Inactive	Expired	Idle for over 6…	
□	65474	User 5	All Users	None	Inactive	Expired	Idle for over 6…	
□	65473	User 6	All Users	None	Inactive	Expired	Idle for over 6…	
□	65472	User 7	All Users	None	Inactive	Expired	Idle for over 6…	
□	65471	User 8	All Users	None	Inactive	Expired	Idle for over 6…	
□	61037	User 9	All Users	None	Inactive	Expired	Idle for over 6…	
□	38384	User 10	All Users	None	Inactive	Expired	Idle for over 6…	
□	33044	User 11	All Users	None	Inactive	Expired	Idle for over 6…	
□	24701	User 12	All Users	None	Inactive	Expired	Idle for over 6…	
□	20727	User 13	All Users	None	Inactive	Expired	Idle for over 6…	
□	16070	User 14	All Users	None	Inactive	Expired	Idle for over 6…	

[Long-term idle users management screen]

Access Group Status – Managing user access rights in a single glance

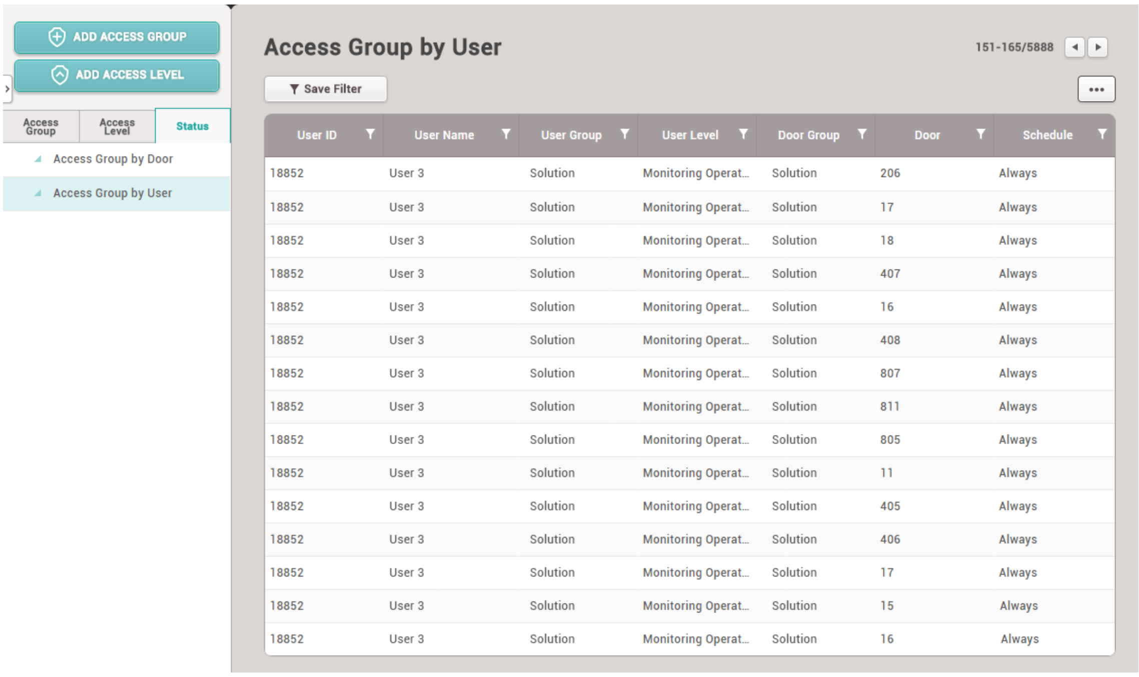
Access group status is a feature that allows effective management of users in line with long-term idle user management. Even if access control was strictly assigned based on users, it was difficult to remember or confirm each of the configurations in the previous versions of BioStar 2.
Access level status is a convenient way to check user access privileges based on either door or user. You can also confirm which users have access to which doors during specified schedules.



Access Group by Door

Door Group	Door	Schedule	User ID	User Name	User Group	User Level
All Doors	Access Door	Always	19789	User 0	TQS	Monitoring Operator
All Doors	Access Door	Always	18852	User 1	HWS	Monitoring Operator
All Doors	Access Door	Always	10400	User 2	TQS	Administrator
All Doors	Access Door	Always	2489	User 3	HWS	None
All Doors	Access Door	Always	2488	User 4	OMS	None
All Doors	Access Door	Always	2487	User 5	QIS	None
All Doors	Access Door	Always	2486	User 6	OMS	None
All Doors	Access Door	Always	2476	User 7	HWS	Monitoring Operator
All Doors	Access Door	Always	2470	User 8	TQS	Administrator
All Doors	Access Door	Always	2455	User 9	OMS	None
All Doors	Access Door	Always	2454	User 10	OMS	None
All Doors	Access Door	Always	2447	User 11	HWS	None
All Doors	Access Door	Always	2438	User 12	OMS	None
All Doors	Access Door	Always	2436	User 13	TQS	Administrator
All Doors	Access Door	Always	2413	User 14	Staff	Administrator

[Access level status – by door]



Access Group by User

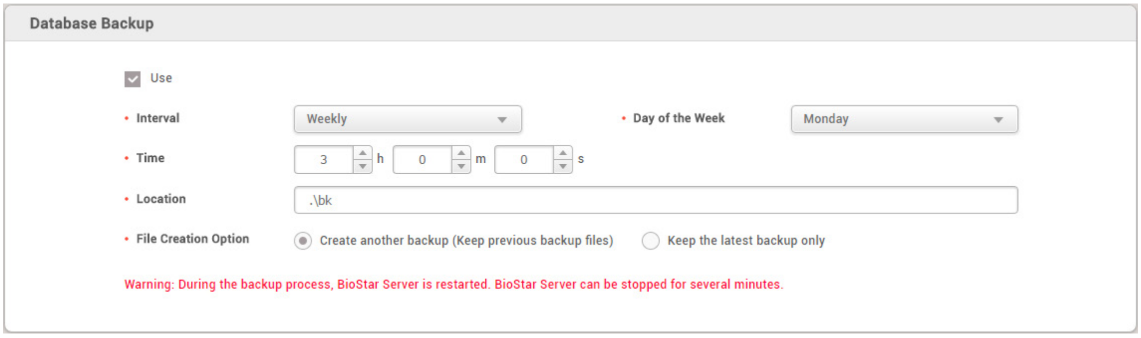
User ID	User Name	User Group	User Level	Door Group	Door	Schedule
18852	User 3	Solution	Monitoring Operat...	Solution	206	Always
18852	User 3	Solution	Monitoring Operat...	Solution	17	Always
18852	User 3	Solution	Monitoring Operat...	Solution	18	Always
18852	User 3	Solution	Monitoring Operat...	Solution	407	Always
18852	User 3	Solution	Monitoring Operat...	Solution	16	Always
18852	User 3	Solution	Monitoring Operat...	Solution	408	Always
18852	User 3	Solution	Monitoring Operat...	Solution	807	Always
18852	User 3	Solution	Monitoring Operat...	Solution	811	Always
18852	User 3	Solution	Monitoring Operat...	Solution	805	Always
18852	User 3	Solution	Monitoring Operat...	Solution	11	Always
18852	User 3	Solution	Monitoring Operat...	Solution	405	Always
18852	User 3	Solution	Monitoring Operat...	Solution	406	Always
18852	User 3	Solution	Monitoring Operat...	Solution	17	Always
18852	User 3	Solution	Monitoring Operat...	Solution	15	Always
18852	User 3	Solution	Monitoring Operat...	Solution	16	Always

[Access level status – by user]

Automatic Database Backup – Securing your vital data

BioStar 2 not only stores user information but also records and saves essential data such as user group, access group, device configuration information, and logs. To secure these important data, you can use the automatic database backup feature.

User information, log and etc. can be automatically backed up based on the schedule that the user configures to avoid database damage or loss. Back up interval, time, location, and file creation options can be configured.



Database Backup

☑ Use

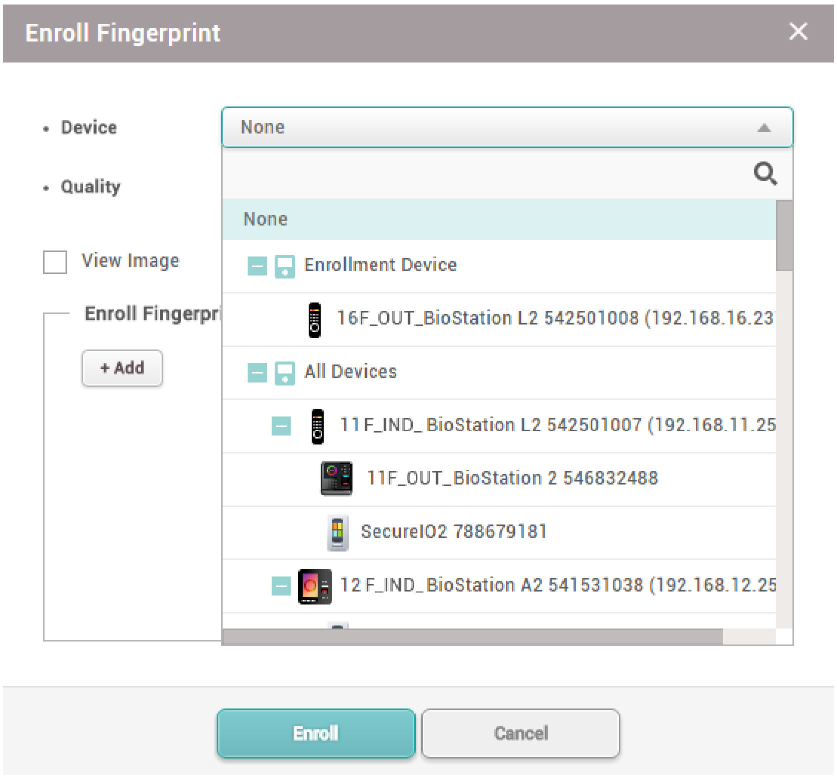
- Interval: Weekly
- Day of the Week: Monday
- Time: 3 h 0 m 0 s
- Location: .\bk
- File Creation Option: ● Create another backup (Keep previous backup files) ○ Keep the latest backup only

Warning: During the backup process, BioStar Server is restarted. BioStar Server can be stopped for several minutes.

[Database backup configuration screen]

User Enrollment Device – Find your frequently used enrollment devices effortlessly

This feature allows you to register devices that are used often when enrolling users to avoid scrolling through the entire list to select your device.



Enroll Fingerprint

- Device: None
- Quality

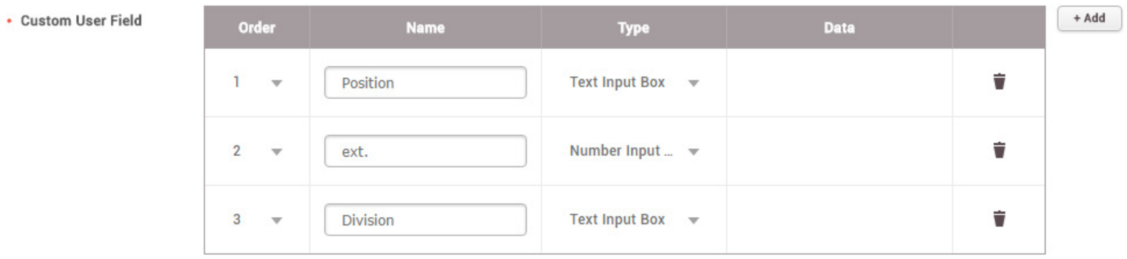
□ View Image

Enroll Fingerpri

None
Enrollment Device
16F_OUT_BioStation L2 542501008 (192.168.16.23
All Devices
11 F_IND_ BioStation L2 542501007 (192.168.11.25
11F_OUT_BioStation 2 546832488
SecureIO2 788679181
12 F_IND_ BioStation A2 541531038 (192.168.12.25

Custom User Fields - Store more types of user information

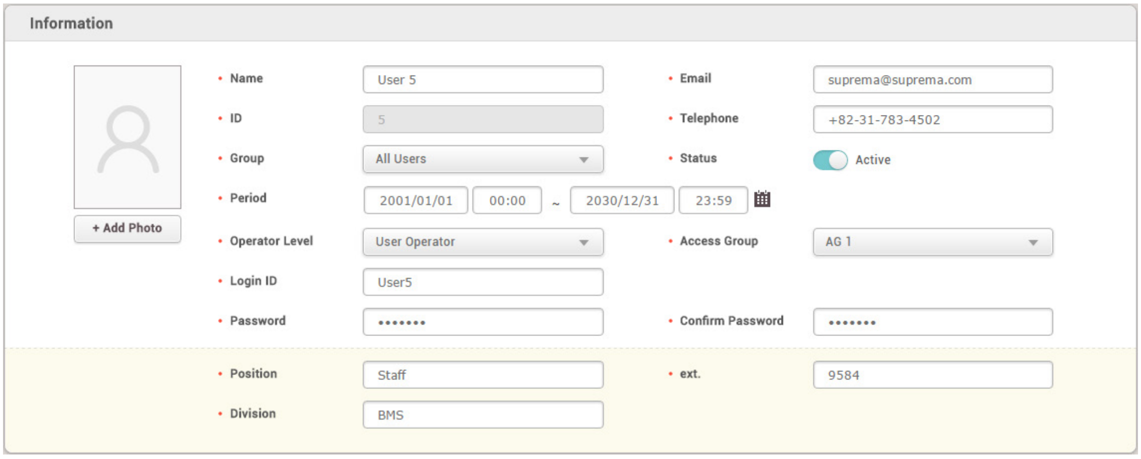
BioStar 2.2.1 provides up to 10 custom user fields to add supplementary user information.
The available options for these fields are number input box, text input box, and combo box. If the combo box is used, up to 20 items can be added and each item can be up to 32 characters long. Each item is separated with a semicolon(;) sign.
You can use these fields to add and manage supplemental information such as department information, company id number, and etc. which are not included in the basic user fields.



• Custom User Field

Order	Name	Type	Data	
1	Position	Text Input Box		
2	ext.	Number Input ...		
3	Division	Text Input Box		

[Custom user field configuration screen]



Information

• Name: User 5
• Email: suprema@suprema.com
• ID: 5
• Telephone: +82-31-783-4502
• Group: All Users
• Status: Active
• Period: 2001/01/01 00:00 ~ 2030/12/31 23:59
• Operator Level: User Operator
• Access Group: AG 1
• Login ID: User5
• Password: •••••••
• Confirm Password: •••••••
• Position: Staff
• ext.: 9584
• Division: BMS

[A sample screen where custom user fields have been applied]

BioStar 2.2.2

BioEntry W2 – Small but versatile biometric device for outdoor use

BioEntry W2 is an access control and time & attendance device in which Suprema's latest hardware and software coexists. This device mounts a quad-core CPU, 2GB of memory, OP5 sensor, and the latest fingerprint algorithm. It can match 150,000 fingerprints in a single second. It also includes live fingerprint detection (LFD) and time & attendance features to provide excellent performance. This device can be used in various environments since the device has a small width size of 50mm and IK08 rated vandal-proof, and IP67 dust & water proof structure. This device also provides added flexibility in system design feature multi-card support with dual-frequency RFID technology.

www.supremainc.com

Suprema Inc. 16F Parkview Office Tower, Jeongja-dong, Bundang-gu Seongnam, Gyeonggi, 463-863 Korea
Tel) +82-31-783-4502 Fax) +82-31-783-4503
Sales information sales@supremainc.com **Technical support** support@supremainc.com