Suprema Webinar 2020

BioStar2 AC Beginner (Crash Course)

Speaker

Hatem Kahla

Regional Technical Manager| Suprema Middle East

Date: Wednesday, May 20, 2020
Time: 12:00 PM Dubai (GMT +4)
Time: 5:00 PM Seoul (GMT +9)
Asia, Europe, Middle East, Africa

Date: Thursday, May 21, 2020
Time: 8:00 PM Dubai (GMT +4)
Time: 12:00 PM New York (GMT-4, EDT)
North America, Latin America

Contents

1. Webinar Goal
2. Understanding BioStar2 Access Control License
3. After BioStar2 installation
4. Activate BioStar2 license (online & offline)
5. Add devices (server mode, device mode, network precautions)
6. Add users (finger enrollment precautions to avoid FAR & FRR)
7. Add doors (with 1 reader (IN) for a door and 2 readers (IN & OUT) for another door)
8. Create Access group & Access level
9. Batch edit for users, devices, & doors
10. Private authentication for users
11. Custom fields for user profiles
12. Device configuration quick look
13. Understanding zones configuration

DISCLAIMER

This presentation is solely for the use of Suprema's employees. No part of this material may be circulated, quoted, or reproduced for distribution outside the customer's organization without prior written approval from Suprema Inc. This material was prepared by Suprema Inc. solely for informative purpose and was not independently verified. No representations or warranties, express or implied, are made as to, and no reliance should be placed on, the accuracy, fairness or completeness of the information presented or contained in this presentation.

LET's START

Contents

1. **Webinar Goal**
2. Understanding BioStar2 Access Control License
3. After BioStar2 installation
4. Activate BioStar2 license (online & offline)
5. Add devices (server mode, device mode, network precautions)
6. Add users (finger enrollment precautions to avoid FAR & FRR)
7. Add doors (with 1 reader (IN) for a door and 2 readers (IN & OUT) for another door)
8. Create Access group & Access level
9. Batch edit for users, devices, & doors
10. Private authentication for users
11. Custom fields for user profiles
12. Device configuration quick look
13. Understanding zones configuration

DISCLAIMER

This presentation is solely for the use of Suprema's employees. No part of this material may be circulated, quoted, or reproduced for distribution outside the customer's organization without prior written approval from Suprema Inc. This material was prepared by Suprema Inc. solely for informative purpose and was not independently verified. No representations or warranties, express or implied, are made as to, and no reliance should be placed on, the accuracy, fairness or completeness of the information presented or contained in this presentation. © 2020 Suprema Inc. All rights reserved.

1 - Webinar Goal

BioStar 2 Access Control (Crash Course)

The aim of this webinar that we are going to explore the basic configuration of BioStar2 Access Control which will highlight the typical configuration and precautions must be taken into consideration while configuration.

All the information in this webinar is useful for Sales, pre-Sales, and technical teams. However, Technical team are to focus & concentrate more in this webinar.

Contents

1. Webinar Goal
2. **Understanding BioStar2 Access Control License**
3. After BioStar2 installation
4. Activate BioStar2 license (online & offline)
5. Add devices (server mode, device mode, network precautions)
6. Add users (finger enrollment precautions to avoid FAR & FRR)
7. Add doors (with 1 reader (IN) for a door and 2 readers (IN & OUT) for another door)
8. Create Access group & Access level
9. Batch edit for users, devices, & doors
10. Private authentication for users
11. Custom fields for user profiles
12. Device configuration quick look
13. Understanding zones configuration

DISCLAIMER

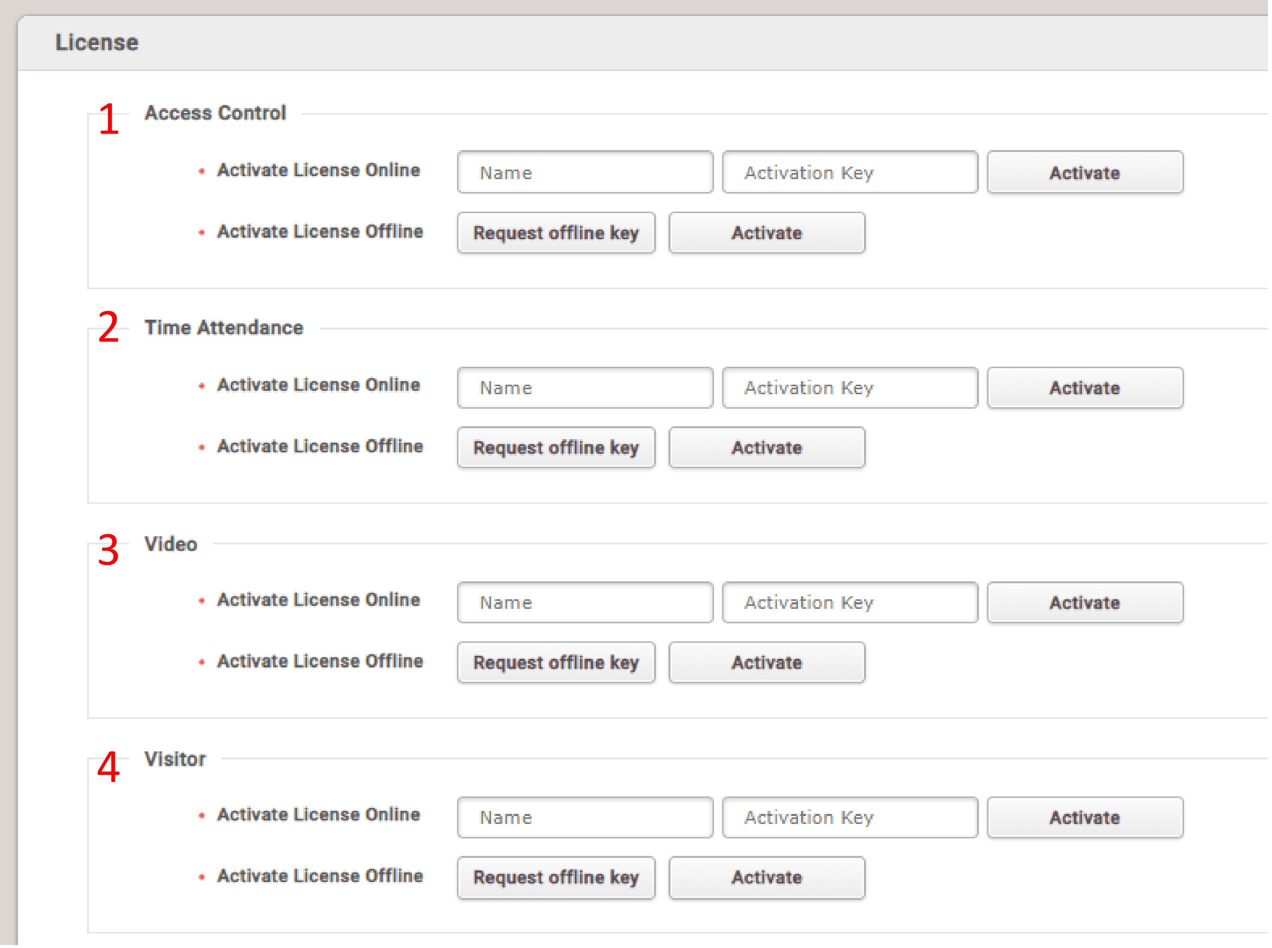
This presentation is solely for the use of Suprema's employees. No part of this material may be circulated, quoted, or reproduced for distribution outside the customer's organization without prior written approval from Suprema Inc. This material was prepared by Suprema Inc. solely for informative purpose and was not independently verified. No representations or warranties, express or implied, are made as to, and no reliance should be placed on, the accuracy, fairness or completeness of the information presented or contained in this presentation.

2 – Understanding BioStar2 Access Control License

BioStar2 Licenses:

We have 4 categories of Licenses:

1. Access Control
2. Time Attendance
3. Video
4. Visitor Management



License

1 Access Control

- Activate License Online — Name, Activation Key, Activate
- Activate License Offline — Request offline key, Activate

2 Time Attendance

- Activate License Online — Name, Activation Key, Activate
- Activate License Offline — Request offline key, Activate

3 Video

- Activate License Online — Name, Activation Key, Activate
- Activate License Offline — Request offline key, Activate

4 Visitor

- Activate License Online — Name, Activation Key, Activate
- Activate License Offline — Request offline key, Activate

2 – Understanding BioStar2 Access Control License

BioStar2 Access Control Licenses:

	Items	Starter (free of charge)	Basic	Standard	Advanced	Professional	Enterprise
Access Control	No. of Doors	5	20	50	100	300	1,000
	Maximum No. of Connected Devices	1,000	1,000	1,000	1,000	1,000	1,000
	Maximum No. of Access Levels	2048	2048	2048	2048	2048	2048
	Maximum No. of Access Groups	2048	2048	2048	2048	2048	2048
	Maximum No. of Access Groups per User	16	16	16	16	16	16
	Maximum No of Access Levels per Access Group	128	128	128	128	128	128
	Access Group Auto Sync	v	v	v	v	v	v
Users	Maximum No. of Cards per User	8	8	8	8	8	8
	Maximum No. of Fingerprints per User	10	10	10	10	10	10
	User Auto Sync	v	v	v	v	v	v
	Access-on-Card	v	v	v	v	v	v
	Security Credential Cards	v	v	v	v	v	v
	iCLASS Seos Card	v	v	v	v	v	v
	Inactivation User Reports	v	v	v	v	v	v
	Custom Field	v	v	v	v	v	v
Elevator Control	Maximum No. of Elevators	-	-	-	1,000	1,000	1,000
	Maximum No. of Floors per Elevator	-	-	-	192	192	192
	Maximum No. of Floor Levels	128	128	128	128	128	128
Zones	Anti-Passback	△(Door)	△(Door)	v	v	v	v
	Fire Alarm	-	-	v	v	v	v
	Schedule Lock/Unlock	-	-	v	v	v	v
	Intrusion Alarm Zone	-	-	v	v	v	v
	Interlock Zone	-	-	v	v	v	v
	Muster Zone	-	-	v	v	v	v
Monitoring	Graphic Map	-	-	-	v	v	v
Features	Server Matching	-	-	-	v	v	v
	Active Directory	-	-	-	v	v	v
	Cloud	-	-	v	v	v	v
	Local API Server	-	-	v	v	v	v

v = supported | - = not supported | △ = Local

2 – Understanding BioStar2 Access Control License

BioStar2 Access Control Licenses:

	Items	Starter (free of charge)	Basic	Standard	Advanced	Professional	Enterprise
Access Control	No. of Doors	5	20	50	[illegible]	300	1,000
	Maximum No. of Connected Devices	1,000	1,000	1,000	[illegible]	[illegible]	1,000
	Maximum No. of Access Levels	2048	2048	[illegible]	[illegible]	[illegible]	2048
	Maximum No. of Access Groups	2048	2048	2048	[illegible]	[illegible]	2048
	Maximum No. of Access Groups per User	16	16	16	[illegible]	[illegible]	[illegible]
	Maximum No of Access Levels per Access Group	128	128	128	[illegible]	[illegible]	[illegible]
	Access Group Auto Sync	v	v	v	[illegible]	[illegible]	v
[illegible]	Maximum No. of Cards per User	8	8	8	8	[illegible]	[illegible]
	Maximum No. of Fingerprints per User	10	10	10	10	[illegible]	[illegible]
	User Auto Sync	v	v	v	v	[illegible]	v
	Access-on-Card	v	v	v	v	v	v
	Maximum No. of Floor Levels	128	128	128	128	128	128
Zones	Anti-Passback	△(Door)	△(Door)	v	v	v	v
	Fire Alarm	-	-	v	v	v	v
	Schedule Lock/Unlock	-	-	v	v	v	v
	Intrusion Alarm Zone	-	-	v	v	v	v
	Interlock Zone	-	-	v	v	v	v
	Muster Zone	-	-	v	v	v	v
Monitoring	Graphic Map	-	-	-	v	v	v
Features	Server Matching	-	-	-	v	v	v
	Active Directory	-	-	-	v	v	v
	Cloud	-	-	v	v	v	v
	Local API Server	-	-	v	v	v	v

Precaution

Make sure to say BioStar2 ACCESS CONTROL License when you order,,,

Standard, Advanced, & Professional are also in BioStar2 TIME ATTENDANCE

v = supported | - = not supported | △ = Local

Contents

1. Webinar Goal
2. Understanding BioStar2 Access Control License
3. **After BioStar2 installation**
4. Activate BioStar2 license (online & offline)
5. Add devices (server mode, device mode, network precautions)
6. Add users (finger enrollment precautions to avoid FAR & FRR)
7. Add doors (with 1 reader (IN) for a door and 2 readers (IN & OUT) for another door)
8. Create Access group & Access level
9. Batch edit for users, devices, & doors
10. Private authentication for users
11. Custom fields for user profiles
12. Device configuration quick look
13. Understanding zones configuration

DISCLAIMER

This presentation is solely for the use of Suprema's employees. No part of this material may be circulated, quoted, or reproduced for distribution outside the customer's organization without prior written approval from Suprema Inc. This material was prepared by Suprema Inc. solely for informative purpose and was not independently verified. No representations or warranties, express or implied, are made as to, and no reliance should be placed on, the accuracy, fairness or completeness of the information presented or contained in this presentation.

3 – After BioStar2 installation

Recommended configuration After BioStar2 installation

After successful installation of BioStar2 (wither on MariaDB or MSSQL – please refer to previous webinar (LINK) for the installation)

We recommend to do the below steps:

A. Installing HTTPS Certificate

B. Change the Logs (MSSQL installation)

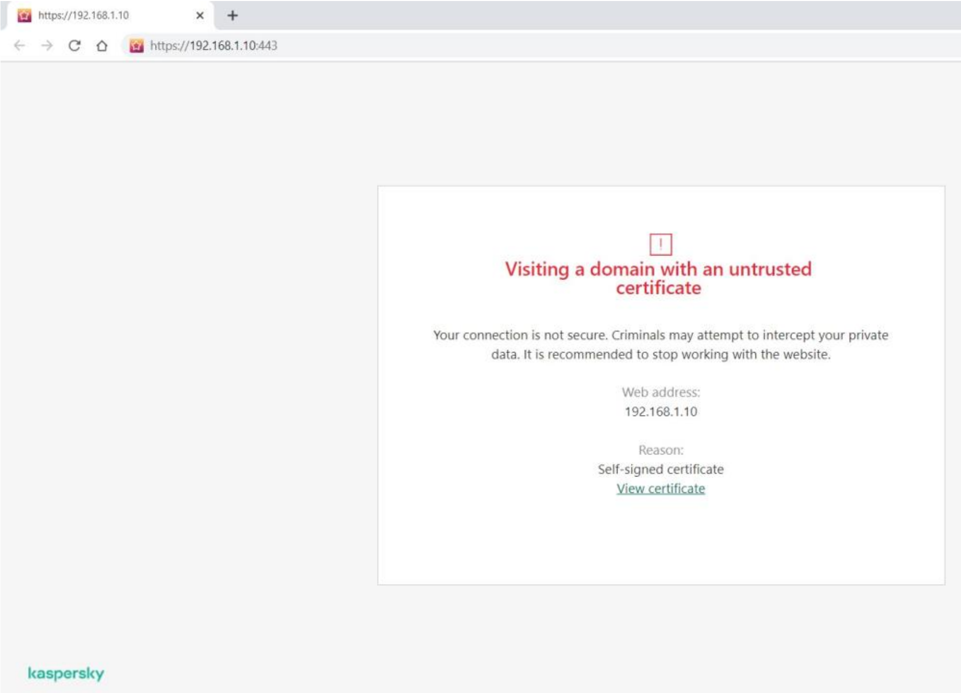
C. Add a maintenance user as admin

3 – After BioStar2 installation

A. Installing HTTPS Certificate

1. Access BioStar2 via Chrome by typing https://serverIP:443

   The first login to BioStar2, warning of connection is not private of untrusted certificate will appear



https://192.168.1.10

https://192.168.1.10:443

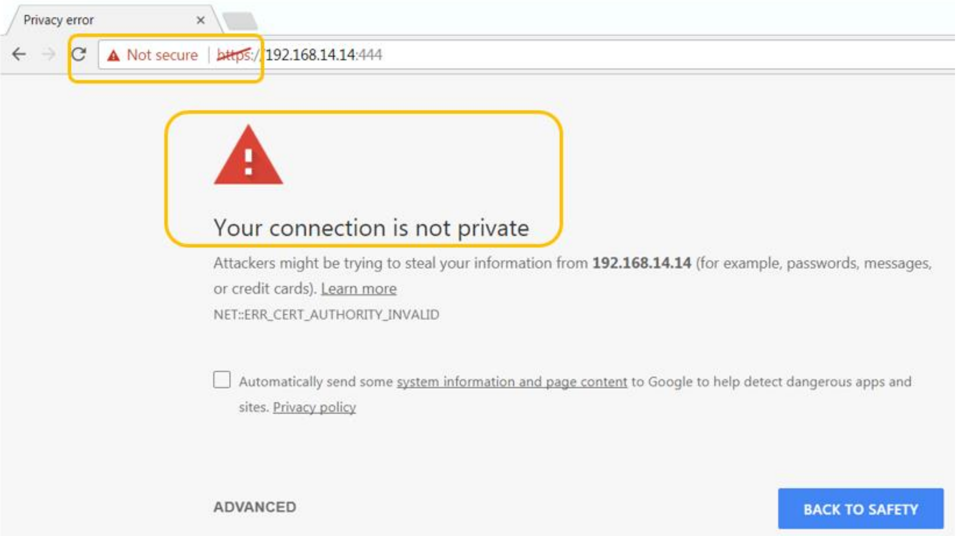
Visiting a domain with an untrusted certificate

Your connection is not secure. Criminals may attempt to intercept your private data. It is recommended to stop working with the website.

Web address:
192.168.1.10

Reason:
Self-signed certificate
View certificate

kaspersky



Privacy error

Not secure | ~~https~~://192.168.14.14:444

Your connection is not private

Attackers might be trying to steal your information from **192.168.14.14** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

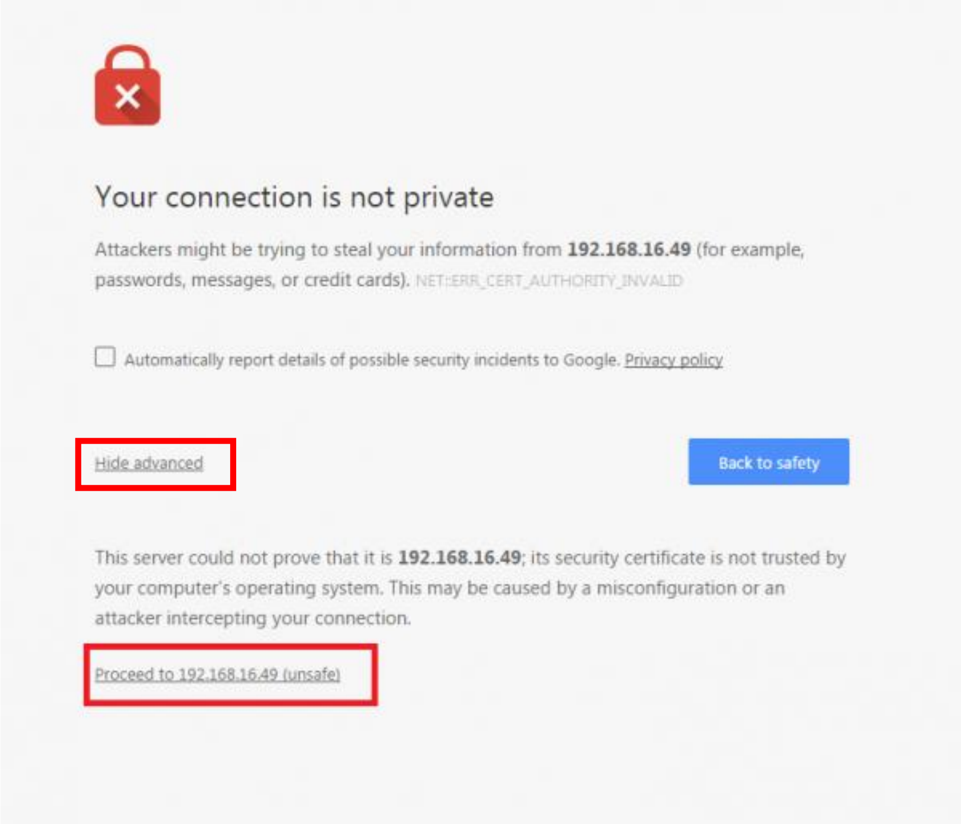
Precaution

2. Please aware of restriction of some antivirus which will not allow you to open the webpage

3 – After BioStar2 installation

A. Installing HTTPS Certificate (continued)

3. Incase of no antivirus, please check advanced and then click proceed to "serverIP"



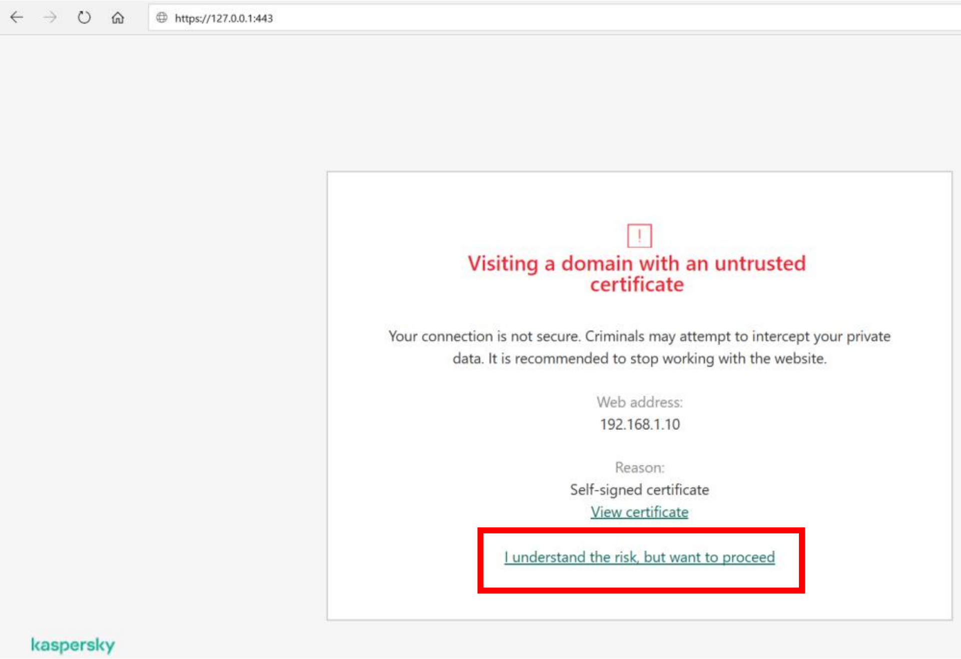
Your connection is not private

Attackers might be trying to steal your information from **192.168.16.49** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

☐ Automatically report details of possible security incidents to Google. Privacy policy

This server could not prove that it is **192.168.16.49**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

4. Incase of antivirus, you can
   a. disable the antivirus, or
   b. access via https://127.0.0.1:443 and click
   "Iunderstand the risk, but want to proceed"



Visiting a domain with an untrusted certificate

Your connection is not secure. Criminals may attempt to intercept your private data. It is recommended to stop working with the website.

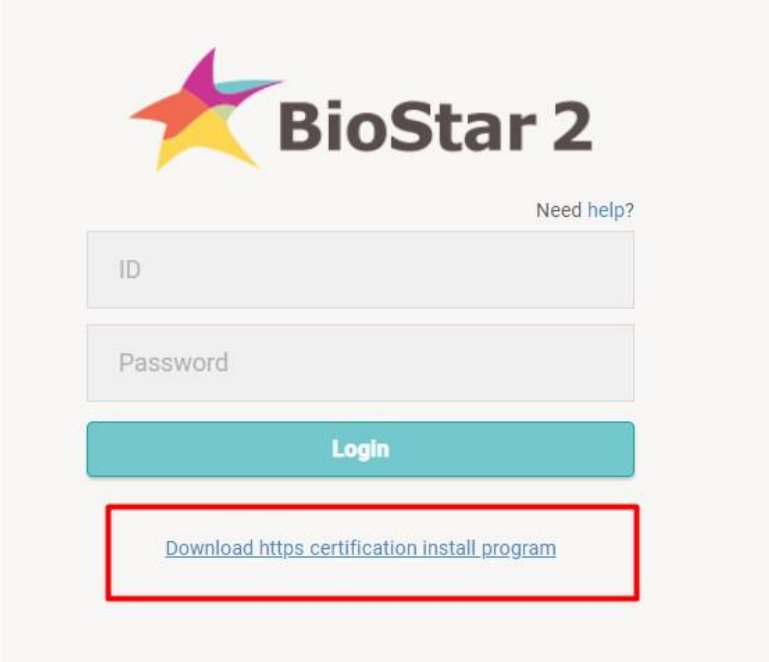
Web address:
192.168.1.10

Reason:
Self-signed certificate

3 – After BioStar2 installation

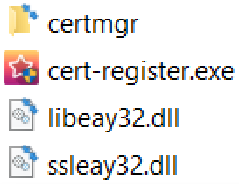
A. Installing HTTPS Certificate (continued)

5. Open the login page of BioStar2 and download https certification install program

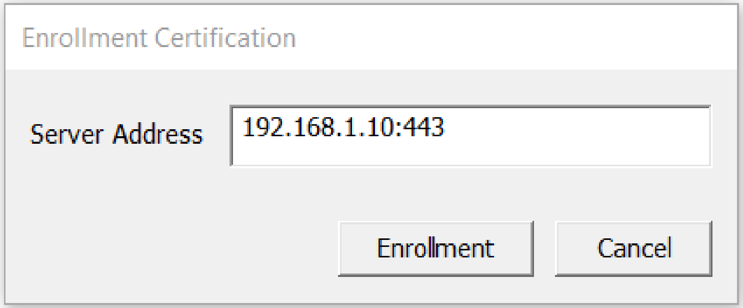


Download https certification install program

6. Unzip the file and run cert-register.exe
7. Type the serverIP:port then click Enrollment



certmgr
cert-register.exe
libeay32.dll
ssleay32.dll



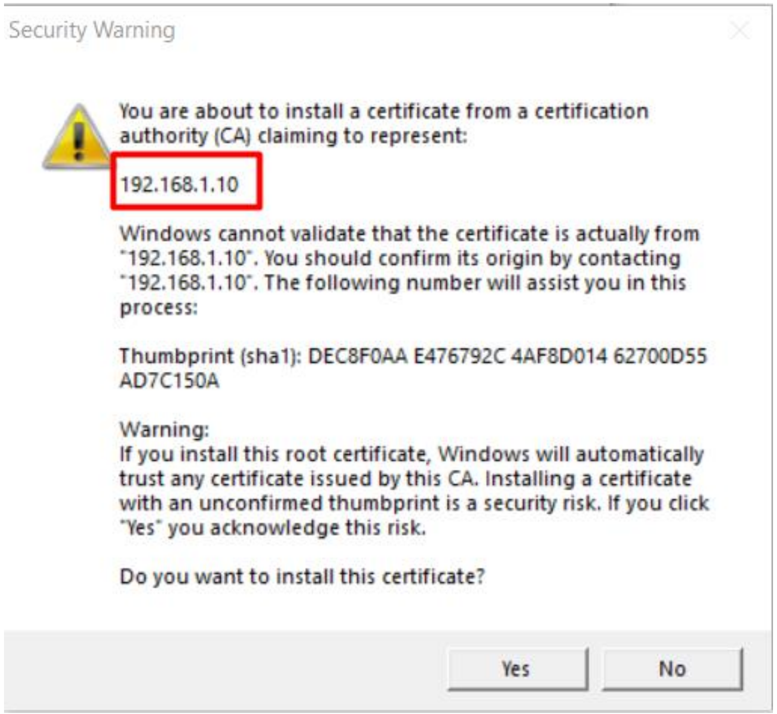
Server Address: 192.168.1.10:443

3 – After BioStar2 installation

A. Installing HTTPS Certificate (continued)

Precaution

8. Make sure that the serverIP is shown then click YES



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

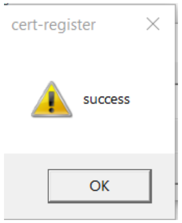
192.168.1.10

Windows cannot validate that the certificate is actually from "192.168.1.10". You should confirm its origin by contacting "192.168.1.10". The following number will assist you in this process:

Thumbprint (sha1): DEC8F0AA E476792C 4AF8D014 62700D55 AD7C150A

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

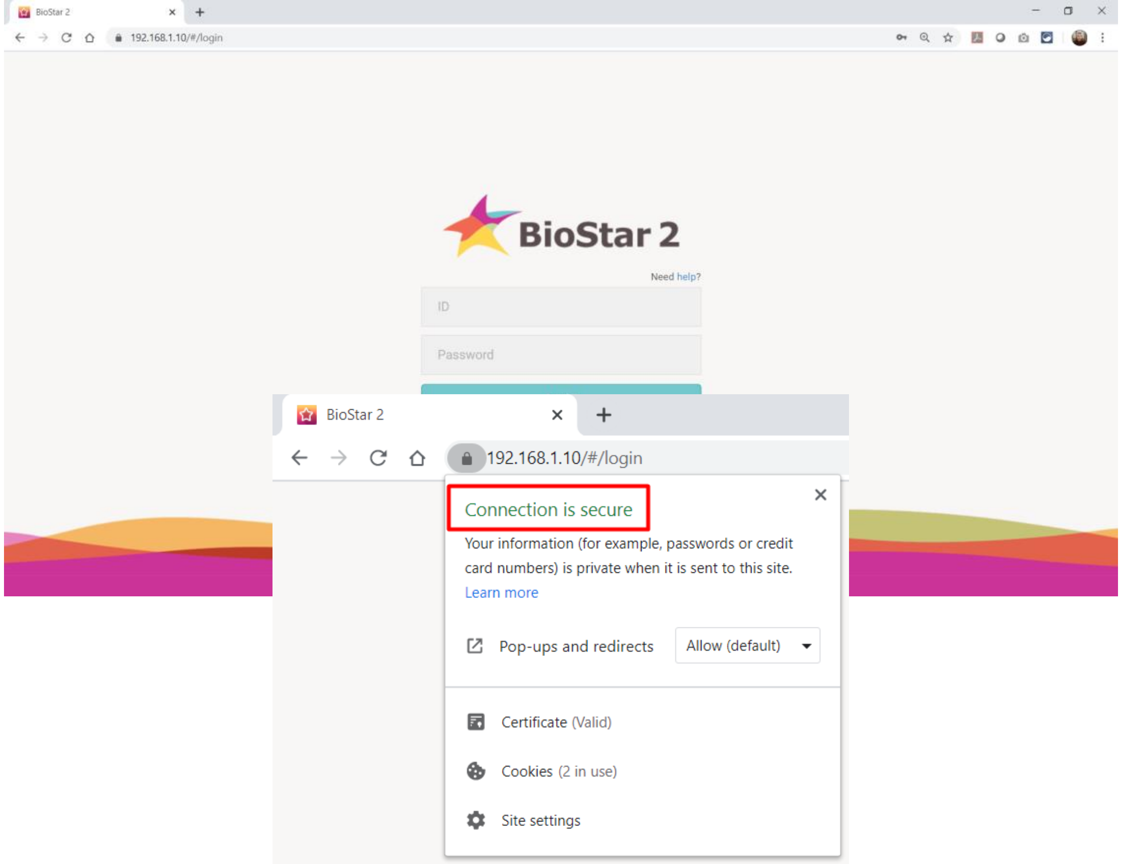
Do you want to install this certificate?



cert-register

success

9. Make sure that all Chrome pages are closed
10. Open a new Chrome page and enter BioStar2 URL:
    https://severIP:port
    Or
    Use the shortcut on the desktop



Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.
Learn more

Pop-ups and redirects: Allow (default)

Certificate (Valid)

Cookies (2 in use)

Site settings

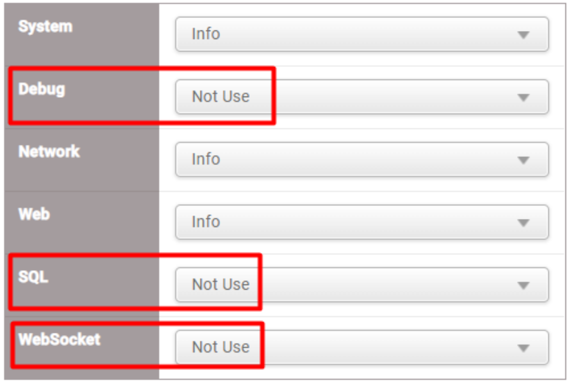
3 – After BioStar2 installation

B. Change the Logs (MSSQL installation)

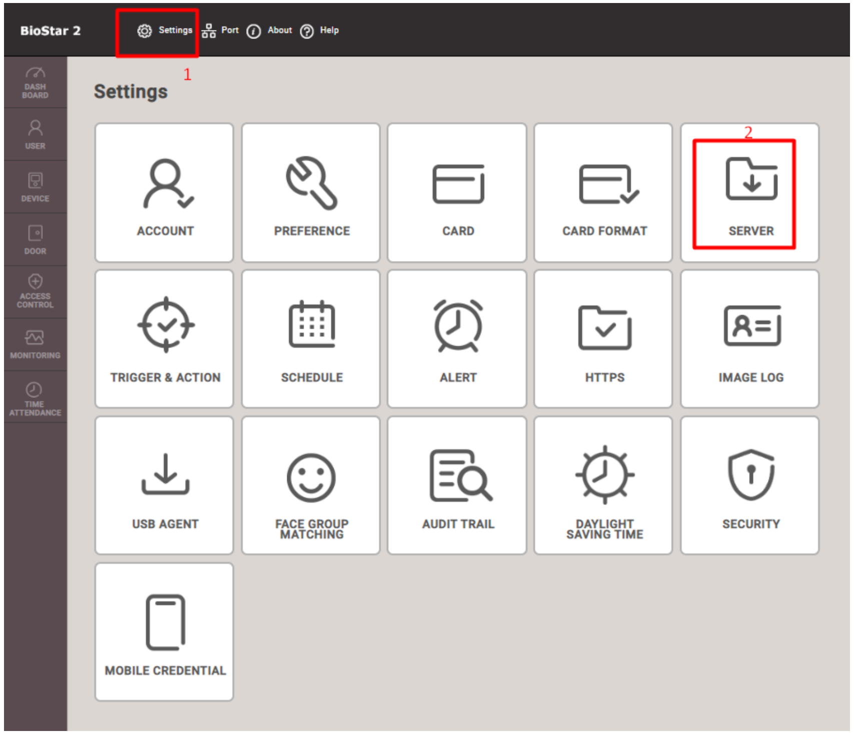
System logs is important for lots things but the most is the troubleshooting.

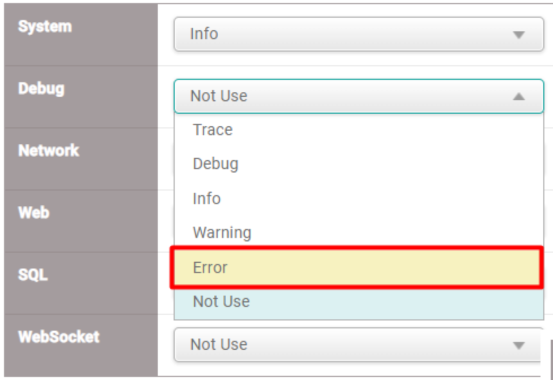
By default, some of the logs are not used and it is recommended it to change the log status from not use to at least error (those log files are stored on BioStar2 installation folder on the application server).

To change that, please go to Settings → server → System logs Level Settings:

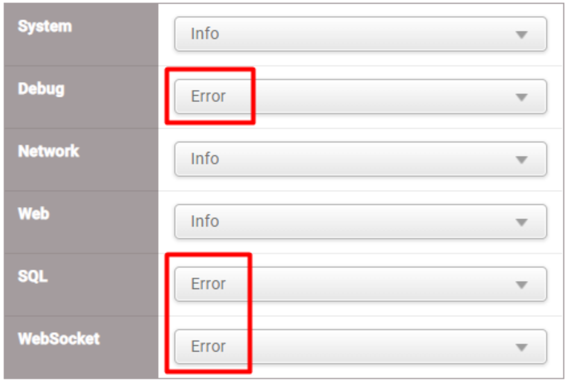


System	Info
Debug	Not Use
Network	Info
Web	Info
SQL	Not Use
WebSocket	Not Use





System	Info
Debug	Not Use
Network	
Web	
SQL	
WebSocket	Not Use



System	Info
Debug	Error
Network	Info
Web	Info
SQL	Error
WebSocket	Error

3 – After BioStar2 installation

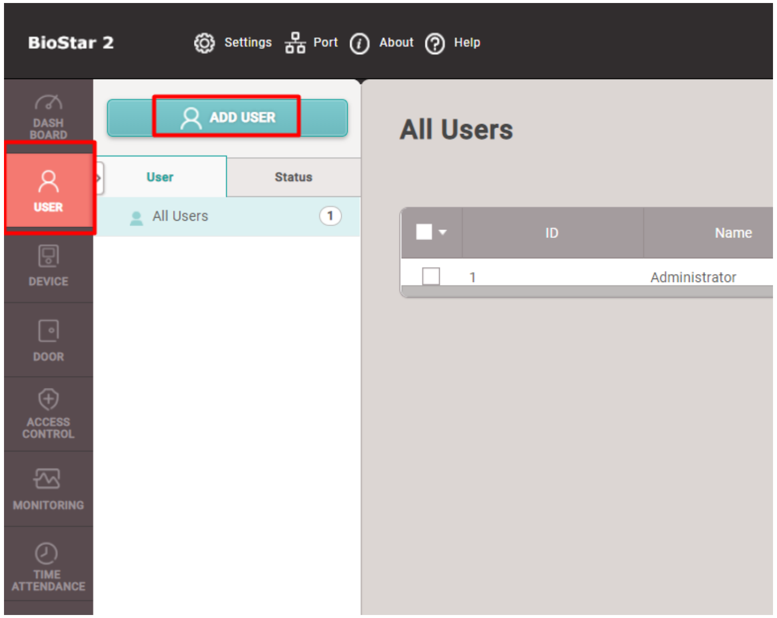
C. Add a maintenance user as admin

Adding a maintenance user is mainly recommended in case of Admin user forgot the password.

Resetting the password of BioStar2 Admin will require a remote session from one of Suprema Technical support (security reasons).

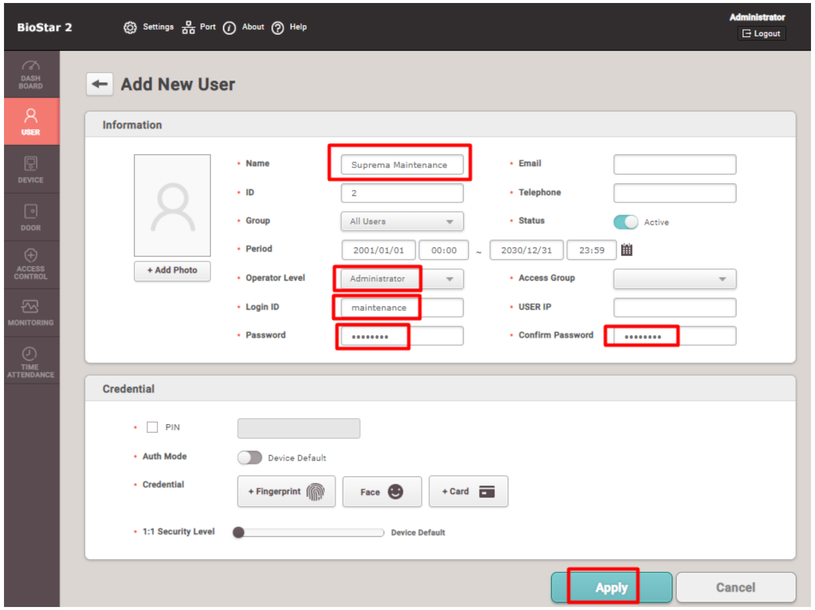
By adding at least another use which has access to BioStar2, will ease resetting BioStar2 administrator password.

To do that, please go to user menu → Add User →
Enter the details and select operator level , then login & password details then **apply**.



All Users

☐	ID	Name
☐	1	Administrator



Add New User

Information

- Name: Suprema Maintenance
- ID: 2
- Group: All Users
- Period: 2001/01/01 00:00 ~ 2030/12/31 23:59
- Operator Level: Administrator
- Login ID: maintenance
- Password: ••••••••
- Email:
- Telephone:
- Status: Active
- Access Group:
- USER IP:
- Confirm Password: ••••••••

Credential

- ☐ PIN
- Auth Mode: Device Default
- Credential
- 1:1 Security Level: Device Default

Contents

1. Webinar Goal
2. Understanding BioStar2 Access Control License
3. After BioStar2 installation
4. **Activate BioStar2 license (online & offline)**
5. Add devices (server mode, device mode, network precautions)
6. Add users (finger enrollment precautions to avoid FAR & FRR)
7. Add doors (with 1 reader (IN) for a door and 2 readers (IN & OUT) for another door)
8. Create Access group & Access level
9. Batch edit for users, devices, & doors
10. Private authentication for users
11. Custom fields for user profiles
12. Device configuration quick look
13. Understanding zones configuration

4 – Activate BioStar2 license (online & offline)

BioStar2 License:

BioStar2 online license key consists of 16 numbers in the format of 1234-5678-1234-5678

You can activate BioStar2 either

A. Online (Internet connection is available on BioStar2 application server)
B. Offline (**NO** Internet connection available on BioStar2 application server)

Precaution

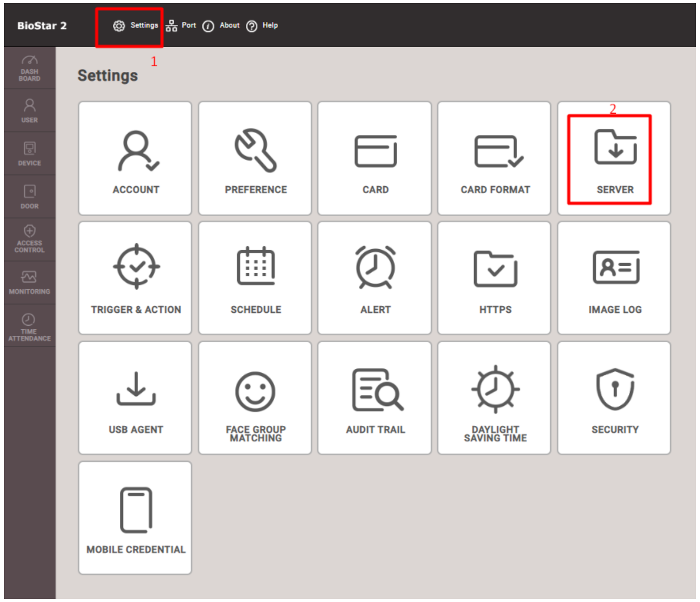
Make sure that you put the 16 numbers with (-) license and in the correct field (Access Control)

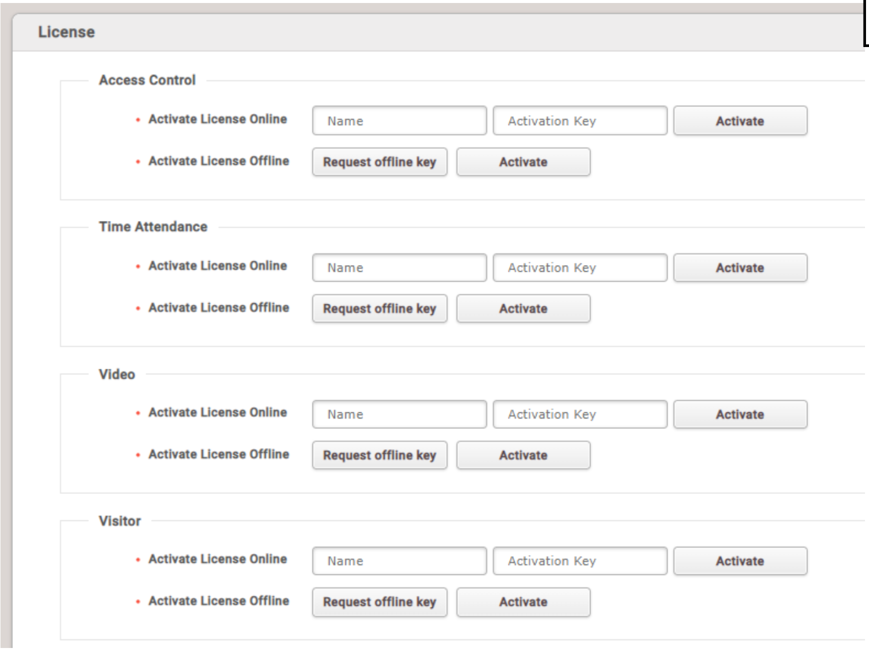
Troubleshooting Activating online license

A. Activating Online License

Please note that you must enter the same format (1234-5678-1234-5678) while activating the license.

Go to setting → Server → License → enter the name of the customer and the 16 numbers license key then click activate in the Access Control part and it will be activated

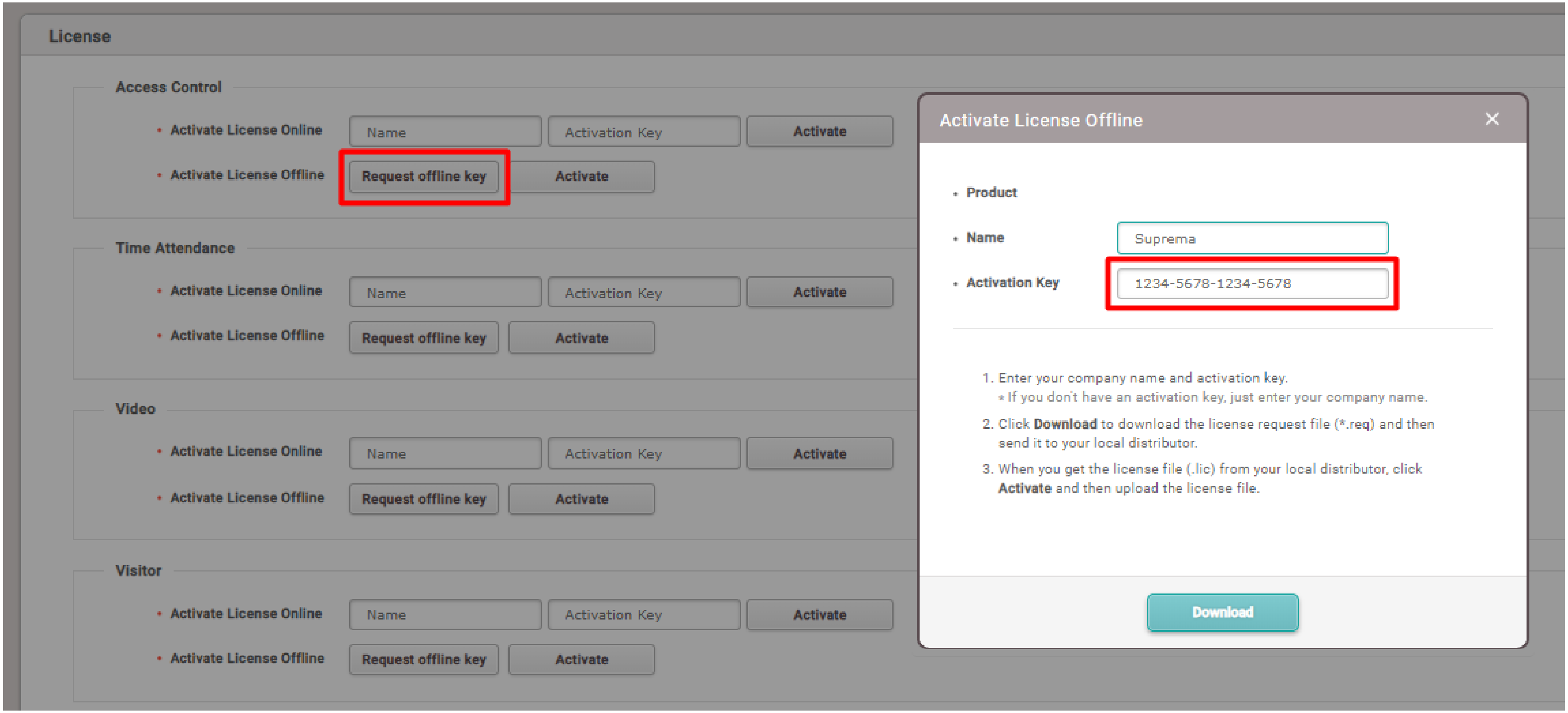




4 – Activate BioStar2 license (online & offline)

B. Activating Offline License

1. Go to setting → Server → License → Click on Request offline Key → fill the customer name and enter the 16 number which you have purchased and click Download



Activate License Offline

- Product
- Name: Suprema
- Activation Key: 1234-5678-1234-5678

1. Enter your company name and activation key.
   * If you don't have an activation key, just enter your company name.
2. Click **Download** to download the license request file (*.req) and then send it to your local distributor.
3. When you get the license file (.lic) from your local distributor, click **Activate** and then upload the license file.

Download

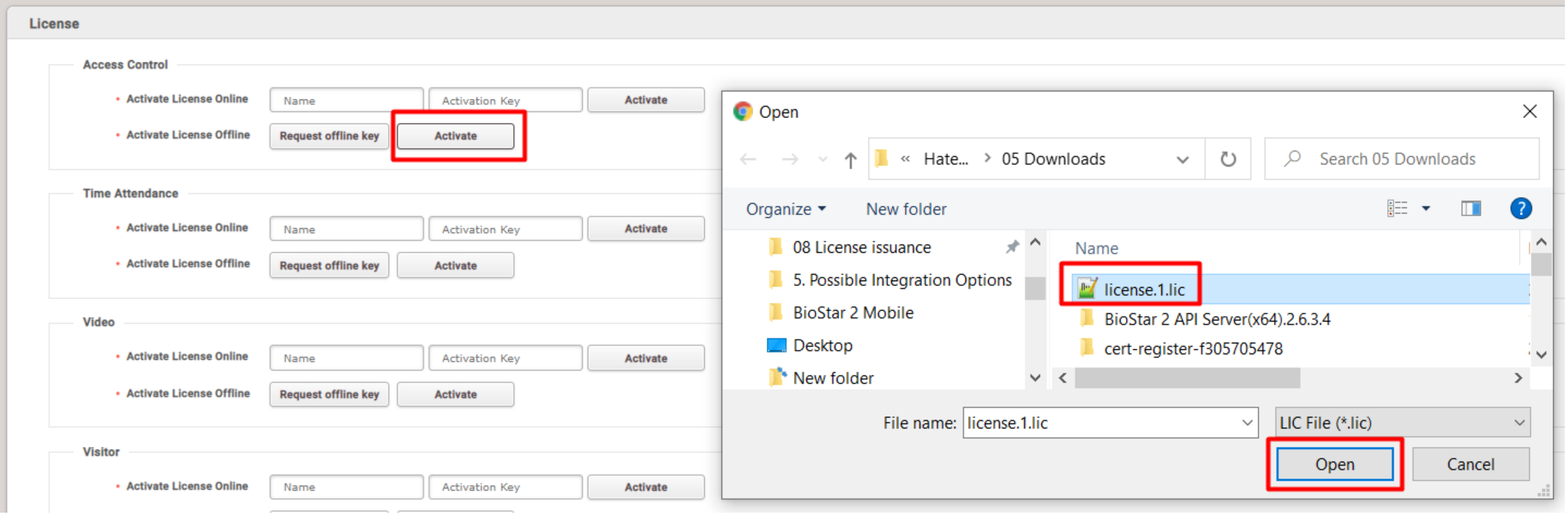
4 – Activate BioStar2 license (online & offline)

B. Activating Offline License

2. Send the downloaded request file (request_to_activate_Suprema_1.0.req) to your Suprema Sales representative and he will return to you with the file (*.lic), please save it to your hard drive (example: desktop)

3. In the same location where you downloaded the request file, please click Activate (next to Request offline key) and the browse will open to chose the *.lic file you have received and click open.

4. **License is activated**



Demonstration

Demonstration of previous Steps

And

Q&A

Contents

1. Webinar Goal
2. Understanding BioStar2 Access Control License
3. After BioStar2 installation
4. Activate BioStar2 license (online & offline)
5. **Add devices (server mode, device mode, network precautions)**
6. Add users (finger enrollment precautions to avoid FAR & FRR)
7. Add doors (with 1 reader (IN) for a door and 2 readers (IN & OUT) for another door)
8. Create Access group & Access level
9. Batch edit for users, devices, & doors
10. Private authentication for users
11. Custom fields for user profiles
12. Device configuration quick look
13. Understanding zones configuration

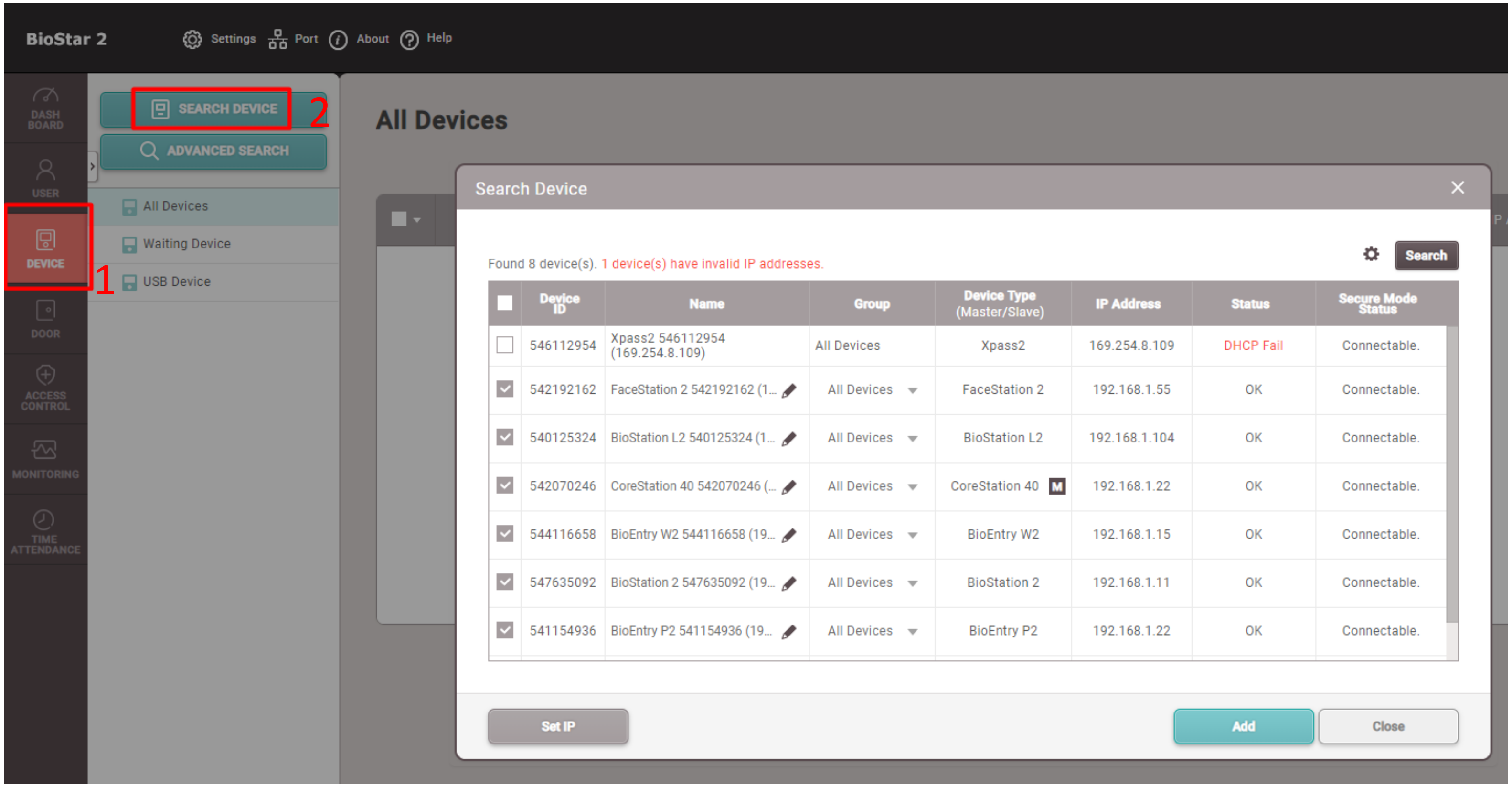
5 – Add devices (server mode, device mode, network precautions)

Adding devices to the server is very easy, in order to do that, we need to understand 3 methods of connections:

1. Server to Device (default)
2. Device to Server
3. Slave devices (Master-Slave Connection)

1. Server to Device

In this mode, the application server will search the LAN network for Suprema devices, simply, go to DEVICE menu and click on Devices then SEARCH DEVICE



Found 8 device(s). 1 device(s) have invalid IP addresses.

☐	Device ID	Name	Group	Device Type (Master/Slave)	IP Address	Status	Secure Mode Status
☐	546112954	Xpass2 546112954 (169.254.8.109)	All Devices	Xpass2	169.254.8.109	DHCP Fail	Connectable.
☑	542192162	FaceStation 2 542192162 (1...	All Devices	FaceStation 2	192.168.1.55	OK	Connectable.
☑	540125324	BioStation L2 540125324 (1...	All Devices	BioStation L2	192.168.1.104	OK	Connectable.
☑	542070246	CoreStation 40 542070246 (...	All Devices	CoreStation 40 M	192.168.1.22	OK	Connectable.
☑	544116658	BioEntry W2 544116658 (19...	All Devices	BioEntry W2	192.168.1.15	OK	Connectable.
☑	547635092	BioStation 2 547635092 (19...	All Devices	BioStation 2	192.168.1.11	OK	Connectable.
☑	541154936	BioEntry P2 541154936 (19...	All Devices	BioEntry P2	192.168.1.22	OK	Connectable.

5 – Add devices (server mode, device mode, network precautions)

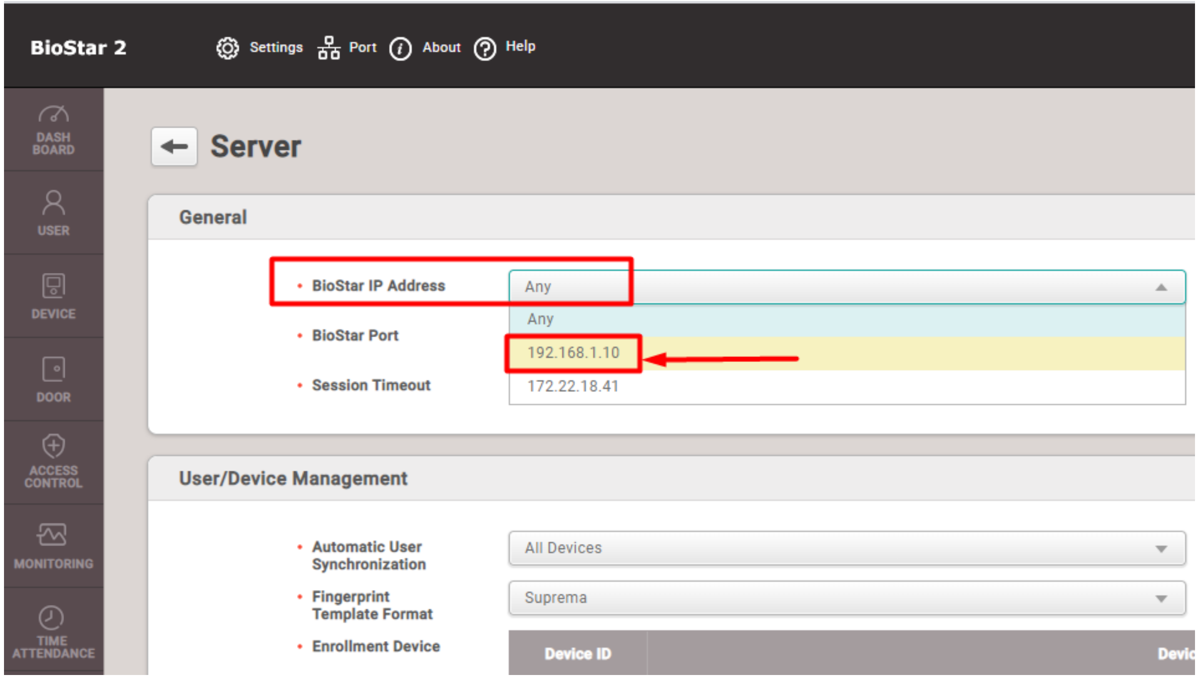
1. Server to Device (Cont'd)

In this mode, mostly it is used for searching the devices without Screens
(BEW2 & BEP2 & CoreStation)

BioStar2 server will search the LAN (No Wan)

Make sure that BioStar2 server has only 1 active network with 1 IP Address at the time of search (disable the Wi-Fi until the search is completed)

If the network card must have 2 IP Addresses, Please make sure that you define BioStar2 server IP in server setting:
Go to Settings → SERVER then change BioStar IP Address from Any to the correct server IP → apply.



Server

General

- BioStar IP Address: Any
  - Any
  - 192.168.1.10
  - 172.22.18.41
- BioStar Port
- Session Timeout

User/Device Management

- Automatic User Synchronization: All Devices
- Fingerprint Template Format: Suprema
- Enrollment Device

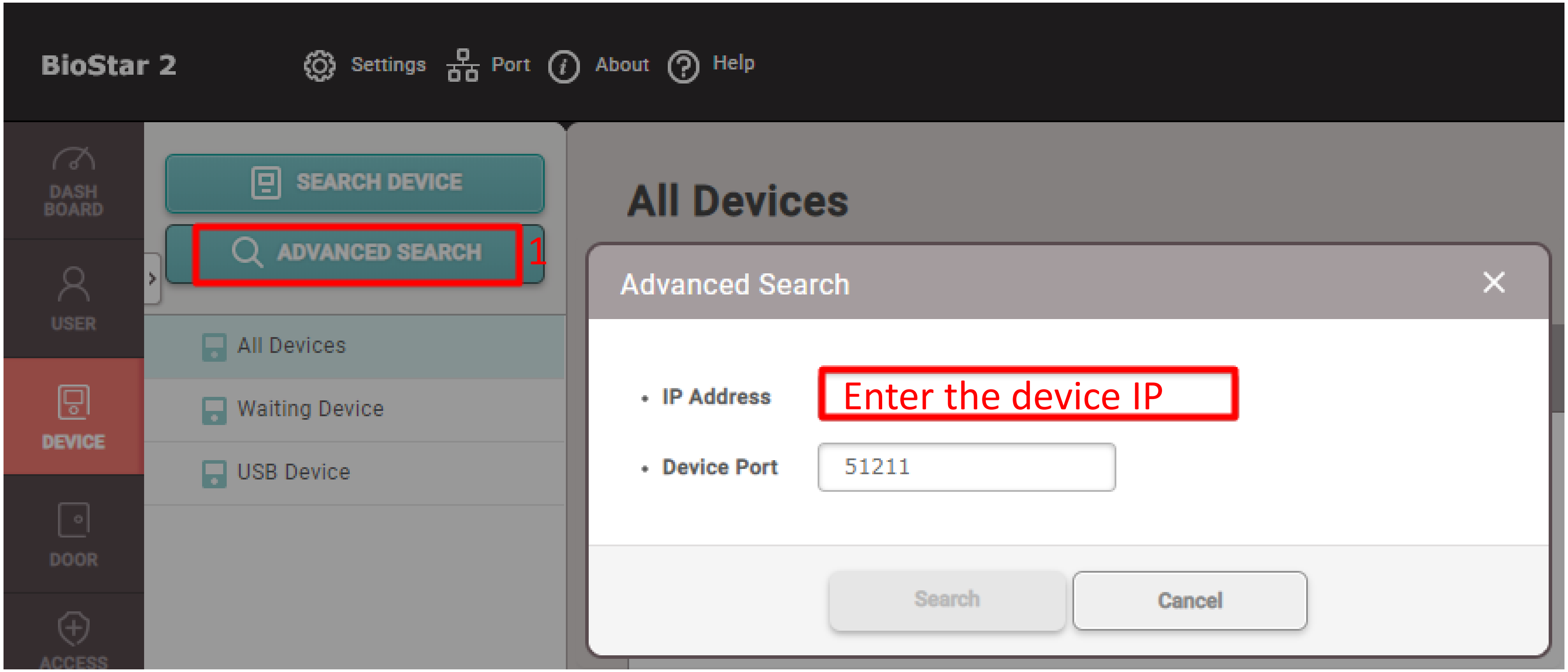
Device ID	Devic

5 – Add devices (server mode, device mode, network precautions)

1. Server to Device (Cont'd)

Precaution

Sometimes the VLANS will prevent the search and also will not find the devices with screens that you have setup the IP Manually, it will not be searched, then you can use ADVANCED SEARCH



Advanced Search

- IP Address: Enter the device IP
- Device Port: 51211

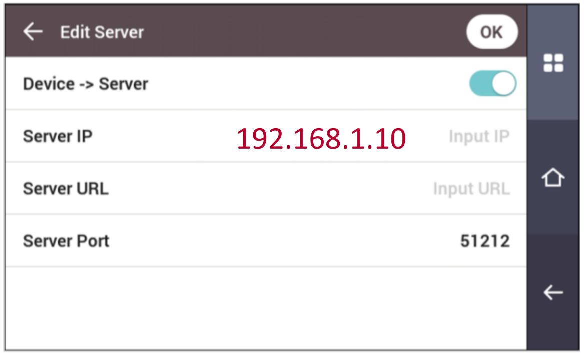
5 – Add devices (server mode, device mode, network precautions)

2. Device to Server

Let's assume that you have BioStar2 server in Dubai and one of the devices is in Seoul and another one in Cairo

So we must use **Device to Server** mode which means that the device will search and find the server and the device will be added to Waiting Devices on BioStar2

If the device has screen, you can enter the serverIP in the network setting



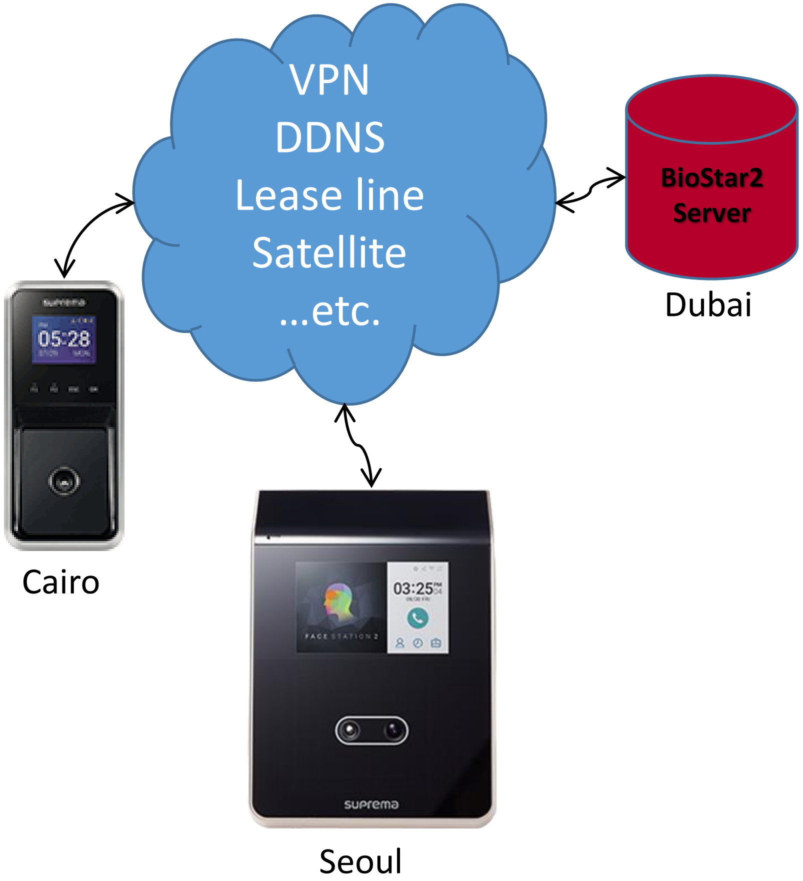
Edit Server

Device -> Server: on

Server IP: 192.168.1.10

Server URL: Input URL

Server Port: 51212



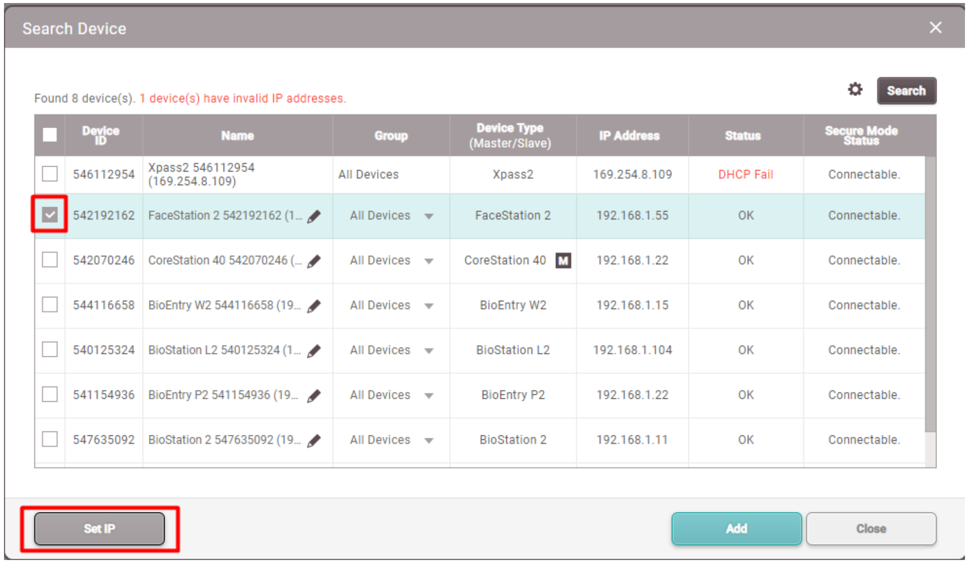
If the device doesn't have screen, then you need to add it from search device
Or after adding the device on BioStar2

LET'S See How

5 – Add devices (server mode, device mode, network precautions)

2. Device to Server (Cont'd)

When you search for devices and find them, please check the box next to the device and click Set IP

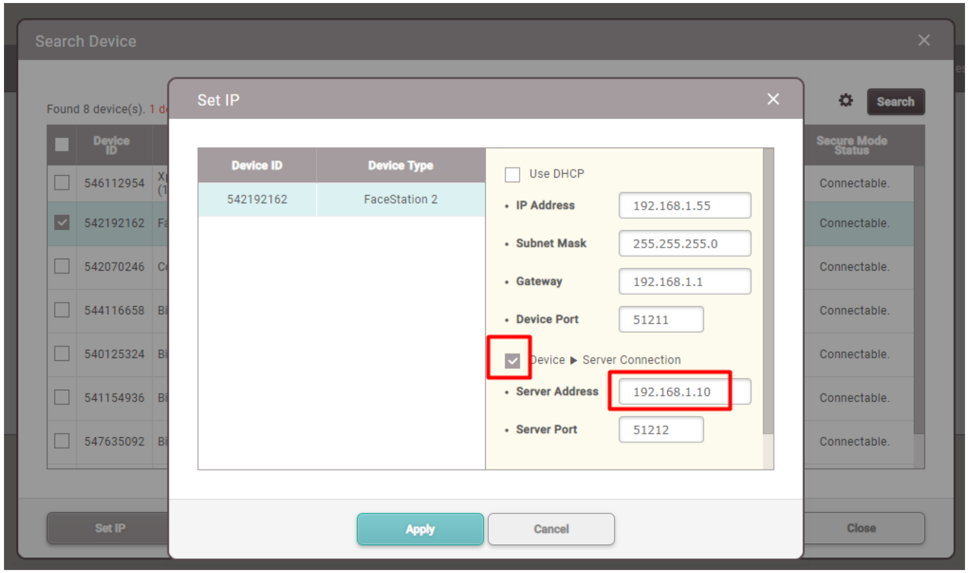


Search Device

Found 8 device(s). 1 device(s) have invalid IP addresses.

□	Device ID	Name	Group	Device Type (Master/Slave)	IP Address	Status	Secure Mode Status
□	546112954	Xpass2 546112954 (169.254.8.109)	All Devices	Xpass2	169.254.8.109	DHCP Fail	Connectable.
☑	542192162	FaceStation 2 542192162 (1...	All Devices	FaceStation 2	192.168.1.55	OK	Connectable.
□	542070246	CoreStation 40 542070246 (...	All Devices	CoreStation 40 M	192.168.1.22	OK	Connectable.
□	544116658	BioEntry W2 544116658 (19...	All Devices	BioEntry W2	192.168.1.15	OK	Connectable.
□	540125324	BioStation L2 540125324 (1...	All Devices	BioStation L2	192.168.1.104	OK	Connectable.
□	541154936	BioEntry P2 541154936 (19...	All Devices	BioEntry P2	192.168.1.22	OK	Connectable.
□	547635092	BioStation 2 547635092 (19...	All Devices	BioStation 2	192.168.1.11	OK	Connectable.

Check the box of Device → Server Connection and enter the BioStar2 application server → Apply → Yes



Set IP

Device ID	Device Type
542192162	FaceStation 2

□ Use DHCP

- IP Address: 192.168.1.55
- Subnet Mask: 255.255.255.0
- Gateway: 192.168.1.1
- Device Port: 51211

☑ Device ▶ Server Connection

- Server Address: 192.168.1.10
- Server Port: 51212

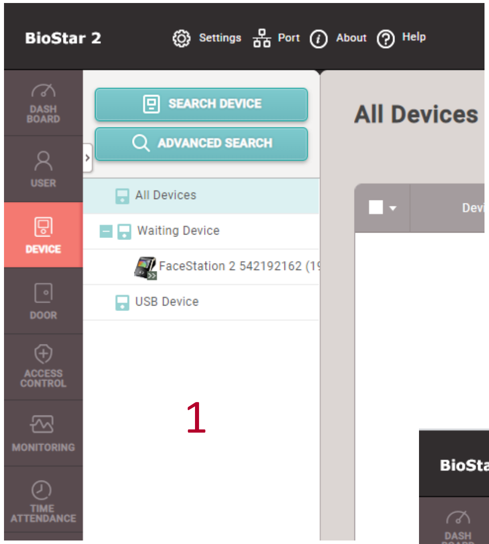
Network setup and configuration from Seoul & Cairo to reach Dubai server will be done by the customer Network Administrator or the ne
provider to the customer

Precaution

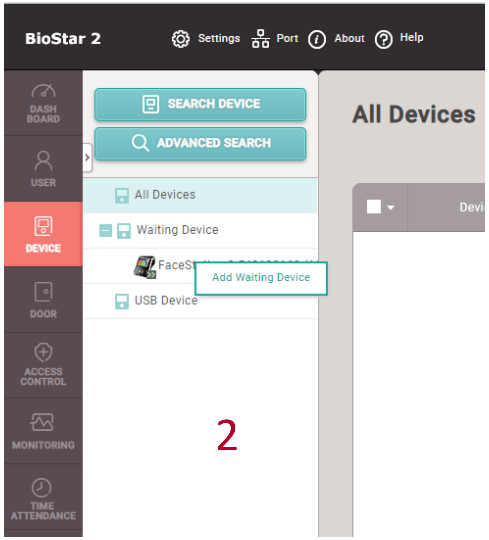
5 – Add devices (server mode, device mode, network precautions)

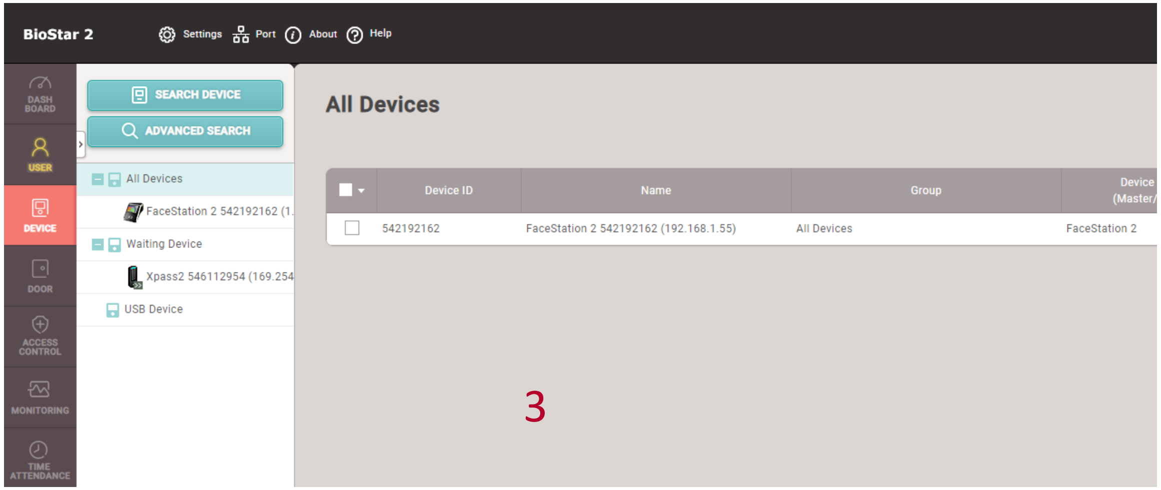
2. Device to Server (Cont'd)

After little time, the device will appear under Waiting Device list



Right click on the device and click Add Waiting Device





All Devices

□	Device ID	Name	Group	Device (Master/
□	542192162	FaceStation 2 542192162 (192.168.1.55)	All Devices	FaceStation 2

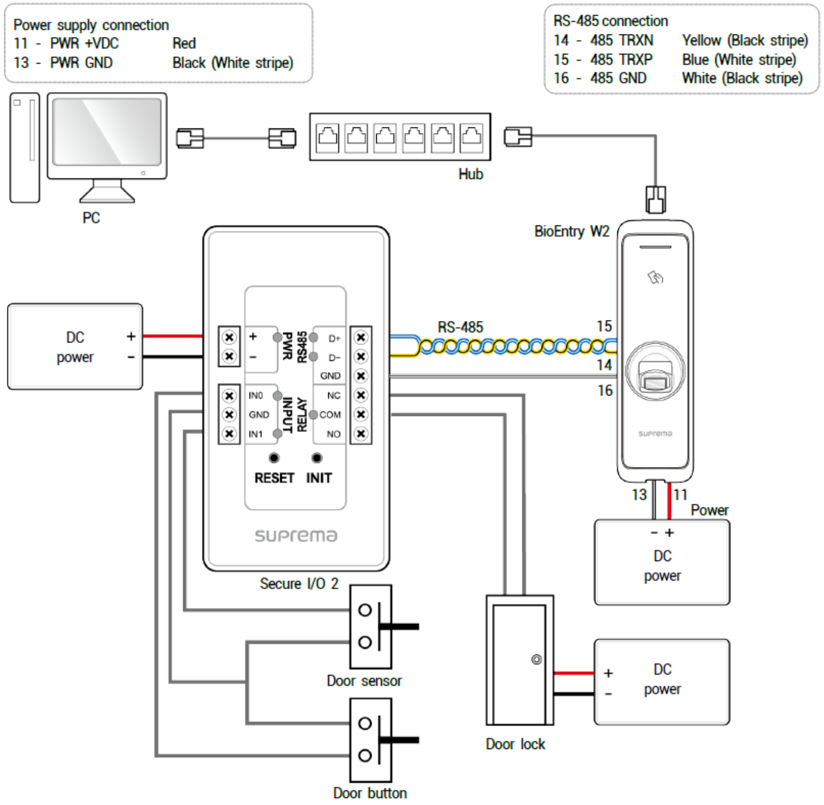
The device will be added to devices and other devices will start to appear if it is configured in Device to Server mode.

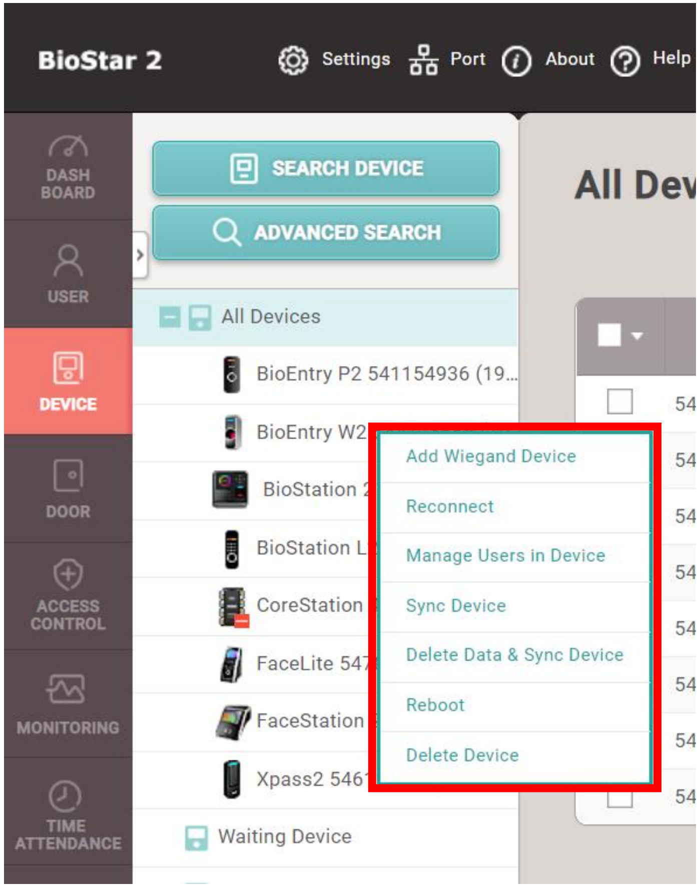
3. Slave devices

Slave devices are set to send the data (finger, card, face) to the master device

Can we add a Slave device directly to a master device? Is there any steps we must do before adding slave device?

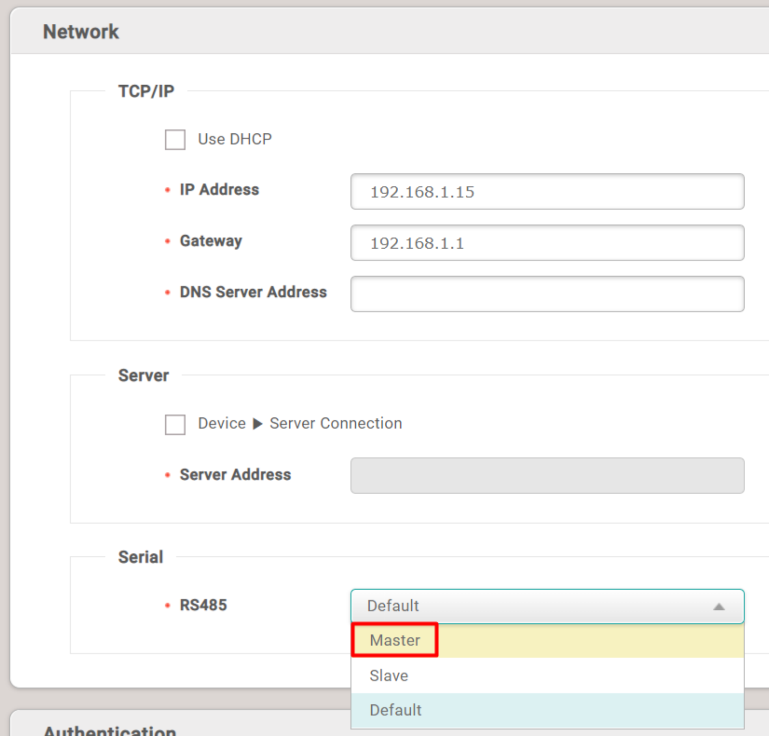
Precaution





5 – Add devices (server mode, device mode, network precautions)

3. Slave devices (Cont'd)



Network

TCP/IP

□ Use DHCP

• IP Address: 192.168.1.15

• Gateway: 192.168.1.1

• DNS Server Address:

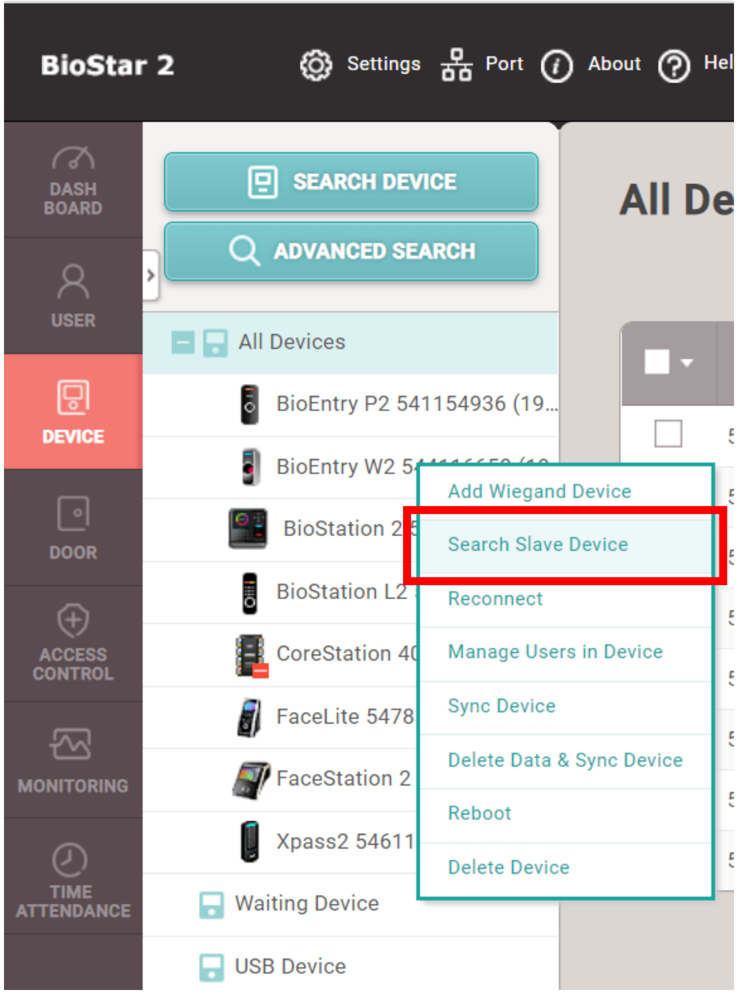
Server

□ Device ▶ Server Connection

• Server Address:

Serial

• RS485: Default



Demonstration of previous Steps
And
Q&A

Contents

1. Webinar Goal
2. Understanding BioStar2 Access Control License
3. After BioStar2 installation
4. Activate BioStar2 license (online & offline)
5. Add devices (server mode, device mode, network precautions)
6. **Add users (finger enrollment precautions to avoid FAR & FRR)**
7. Add doors (with 1 reader (IN) for a door and 2 readers (IN & OUT) for another door)
8. Create Access group & Access level
9. Batch edit for users, devices, & doors
10. Private authentication for users
11. Custom fields for user profiles
12. Device configuration quick look
13. Understanding zones configuration

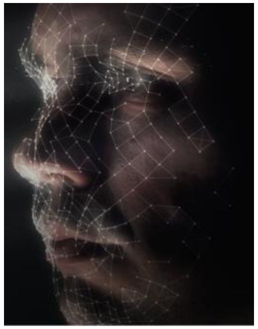
6 – Add users (finger enrollment precautions to avoid FAR & FRR)

Before we start adding users, lets understand the difference between 1:N mode & 1:1, Also FAR & FRR

1:N Mode (1 to Many):

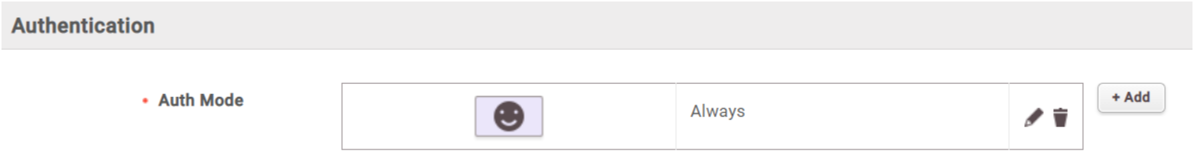
Show your face to device

Device extract your template from your face



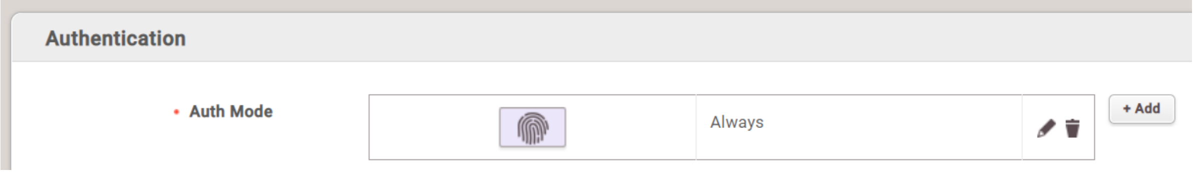
Device match your template with all stored templates on device

Result in less than 1 second



Authentication

• **Auth Mode**	☺	Always	+ Add



Authentication

• **Auth Mode**	▨	Always	+ Add

Setup 1:N mode on devices
(Face & Finger)

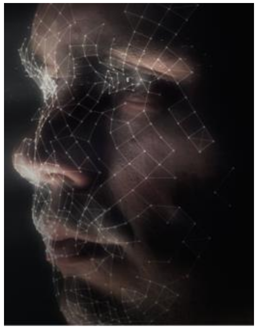
6 – Add users (finger enrollment precautions to avoid FAR & FRR)

1:1 Mode:

Put your Mobile Card or Access Card or enter your ID

ID

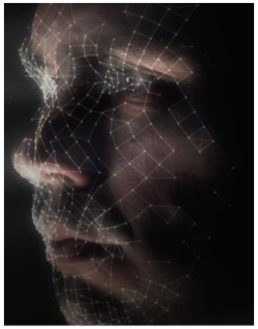
Device will ask to show your face and at the same time will get only your template from the stored templates on the device



1

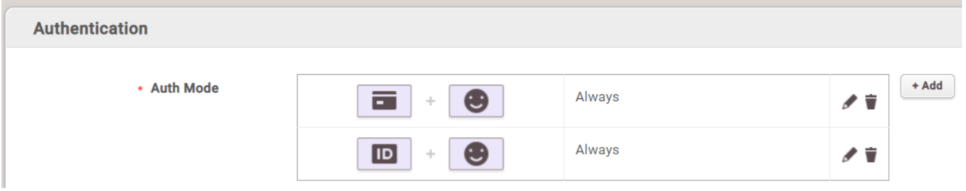
Matching between real template form the person to the template form the device

to



1

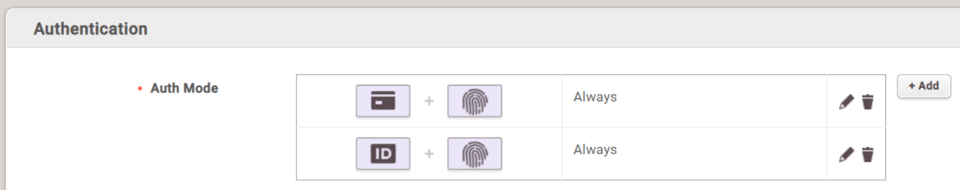
Result in less than 1 second



Authentication

Auth Mode

▭ + ☺	Always	+ Add
ID + ☺	Always	



Authentication

Auth Mode

▭ +	Always	+ Add
ID +	Always	

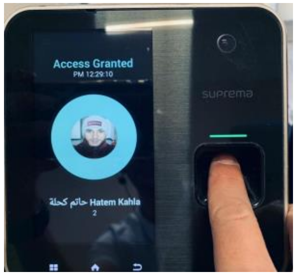
6 – Add users (finger enrollment precautions to avoid FAR & FRR)

؟؟؟ FAR ???

FAR = False Acceptance Ratio

Kate & Hatem fingers are enrolled

Kate put her finger on the device



Results of template check is **Hatem**

Reason is

???????

What do you think is the reason ?

Can you tell me?

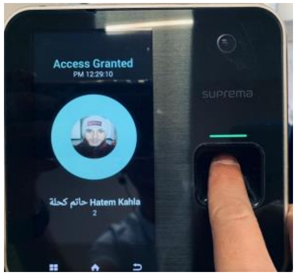
6 – Add users (finger enrollment precautions to avoid FAR & FRR)

؟؟؟ FAR ???

FAR = False Acceptance Ratio

Kate & Hatem fingers are enrolled

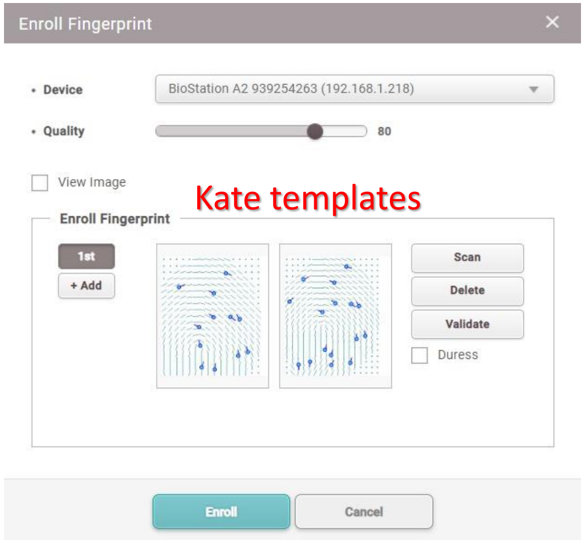
Kate put her finger on the device



Results of template check is **Hatem**

Reason is

Poor Enrollment



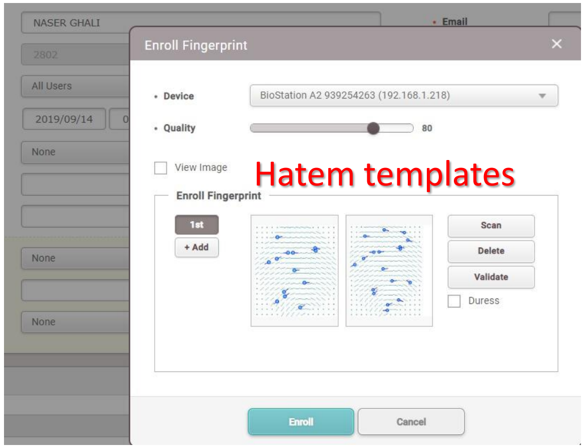
Enroll Fingerprint ✕

- Device: BioStation A2 939254263 (192.168.1.218)
- Quality: 80

□ View Image

Kate templates

Enroll Fingerprint



NASER GHALI
2802
All Users
2019/09/14
None
None
None
- Email

Enroll Fingerprint ✕

- Device: BioStation A2 939254263 (192.168.1.218)
- Quality: 80

□ View Image

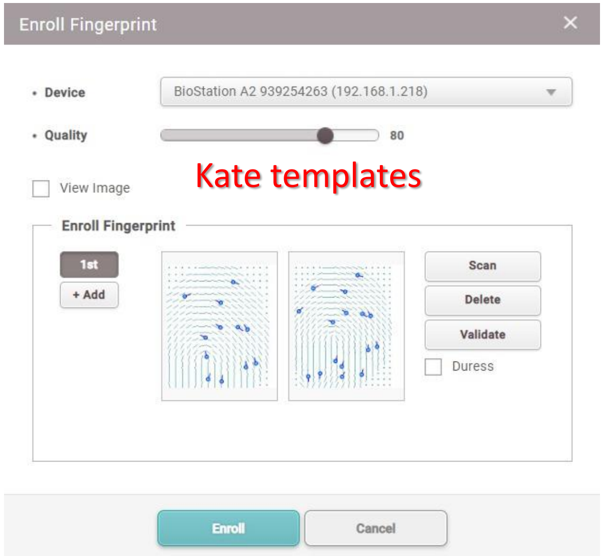
Hatem templates

Enroll Fingerprint

Similar Templates

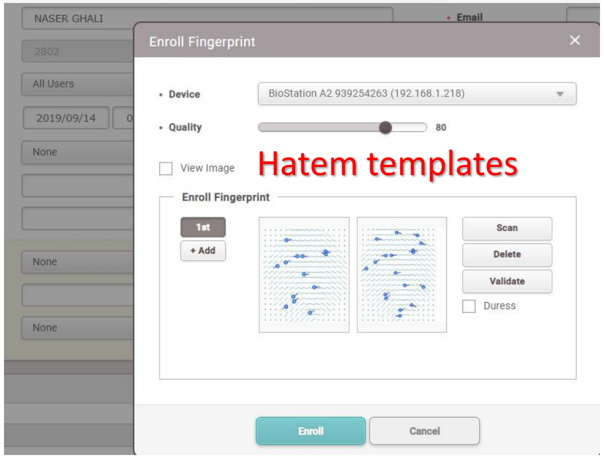
6 – Add users (finger enrollment precautions to avoid FAR & FRR)

FAR Solution:
re-enrollment for both users


Enroll Fingerprint
- Device: BioStation A2 939254263 (192.168.1.218)
- Quality: 80

☐ View Image

Kate templates

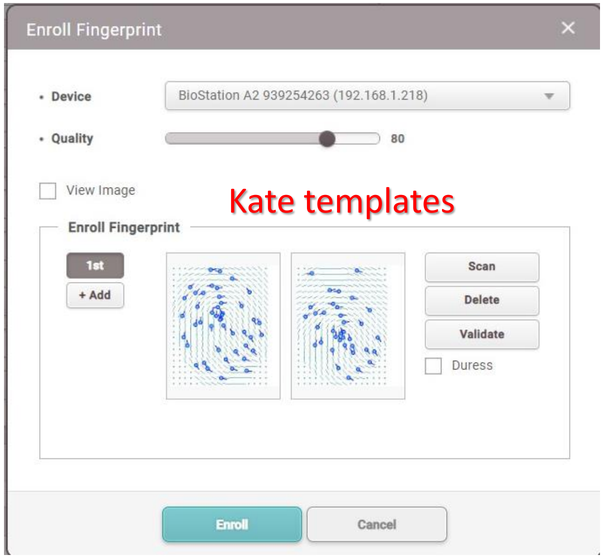

NASER GHALI
Email
2802
All Users
2019/09/14
None
None
None

Enroll Fingerprint
- Device: BioStation A2 939254263 (192.168.1.218)
- Quality: 80

☐ View Image

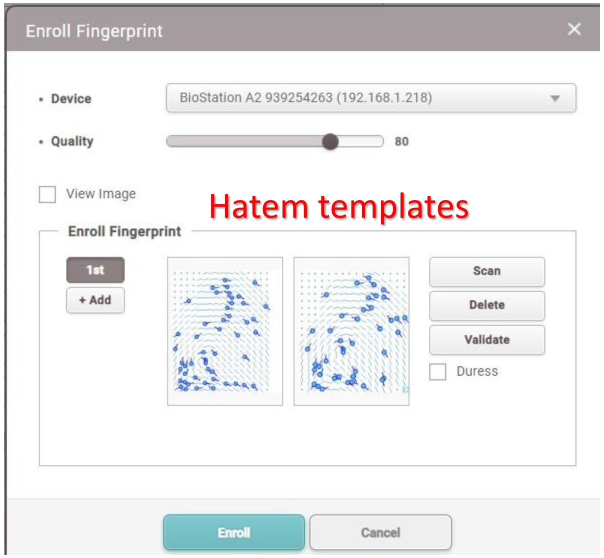
Hatem templates

After
Re-Enrollment


Enroll Fingerprint
- Device: BioStation A2 939254263 (192.168.1.218)
- Quality: 80

☐ View Image

Kate templates


Enroll Fingerprint
- Device: BioStation A2 939254263 (192.168.1.218)
- Quality: 80

☐ View Image

Hatem templates

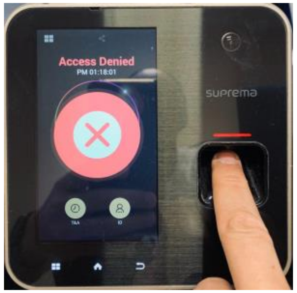
6 – Add users (finger enrollment precautions to avoid FAR & FRR)

¿¿¿ FRR ???

FRR = False Rejection Ratio

Kate finger is enrolled & stored in the device memory

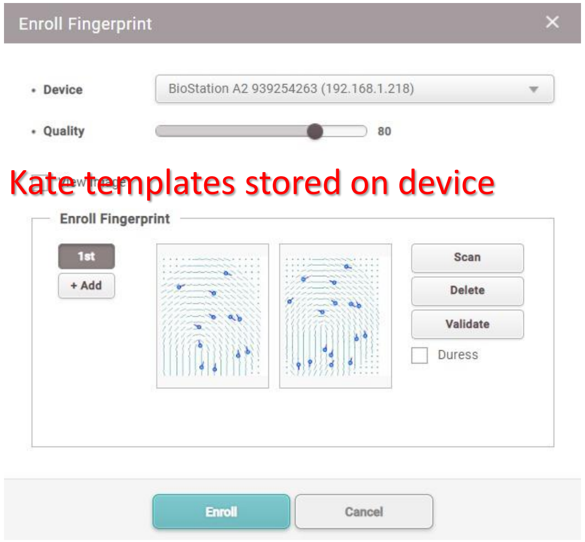
Kate put her finger on the device



Results is Access Denied !!!!!!

Reason is

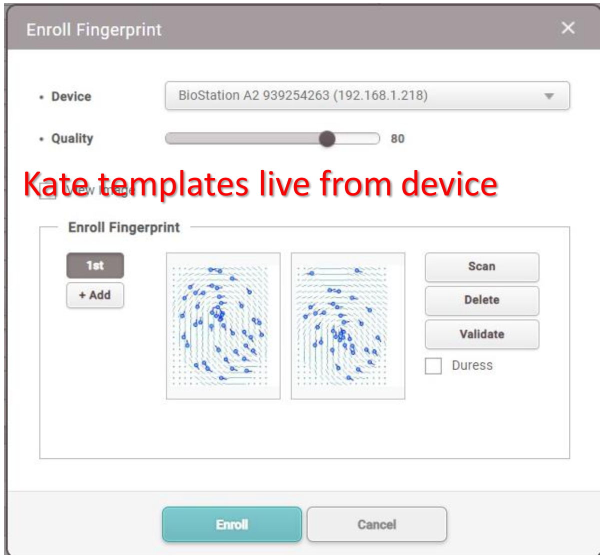
Poor Enrollment



Kate templates stored on device

Enroll Fingerprint

- Device: BioStation A2 939254263 (192.168.1.218)
- Quality: 80



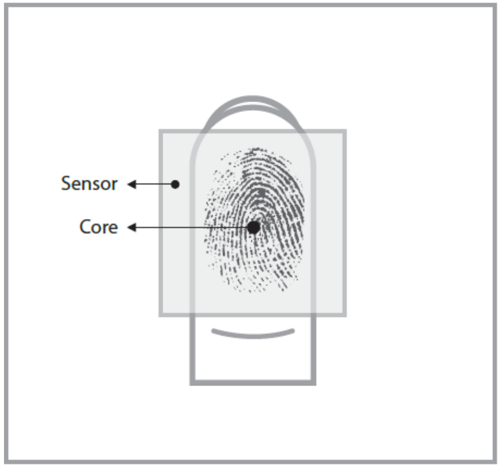
Kate templates live from device

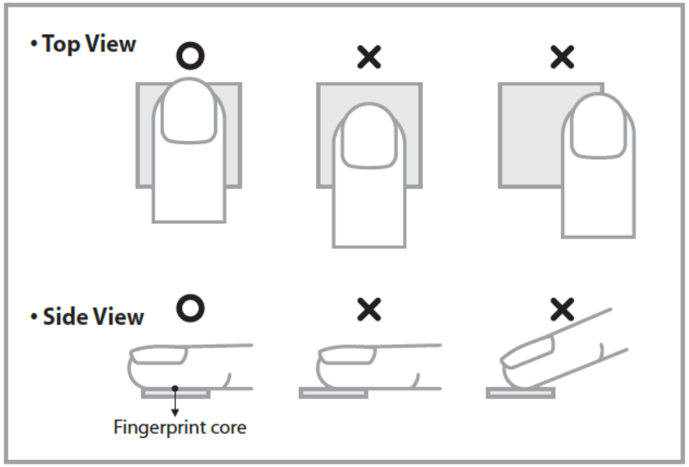
Enroll Fingerprint

- Device: BioStation A2 939254263 (192.168.1.218)
- Quality: 80

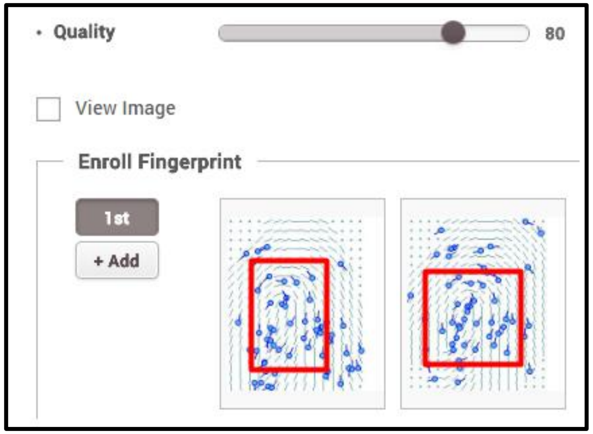
6 – Add users (finger enrollment precautions to avoid FAR & FRR)

Prober enrollment instructions or Finger





Precaution



More details in below link

[Fingerprint Enrollment Guide](#)

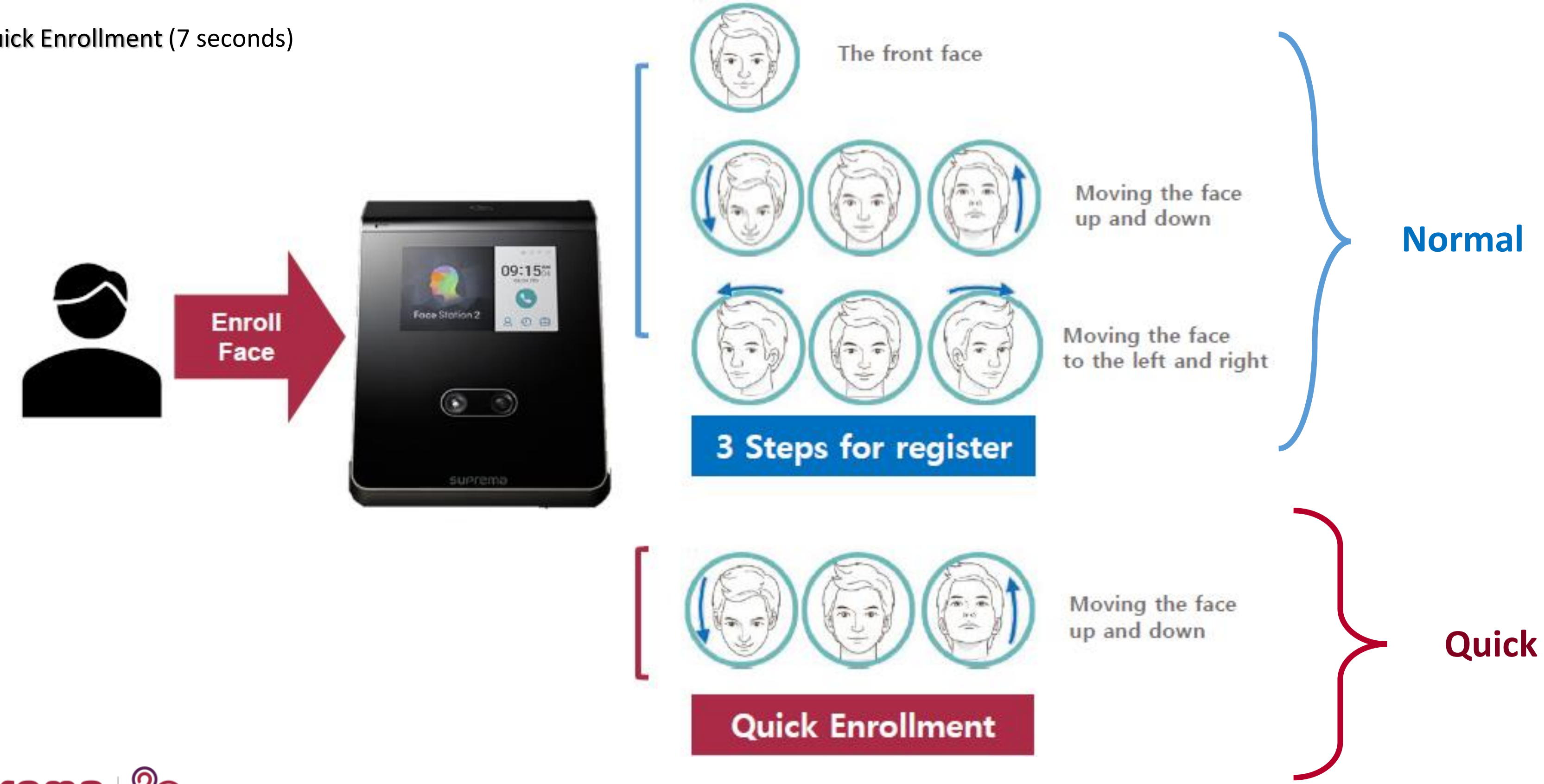
6 – Add users (finger enrollment precautions to avoid FAR & FRR)

Prober enrollment instructions or Face

We have 2 modes for enrollment:

1. Normal mode (around 21 seconds)

2. Quick Enrollment (7 seconds)



Demonstration

Demonstration of previous Steps

And

Q&A

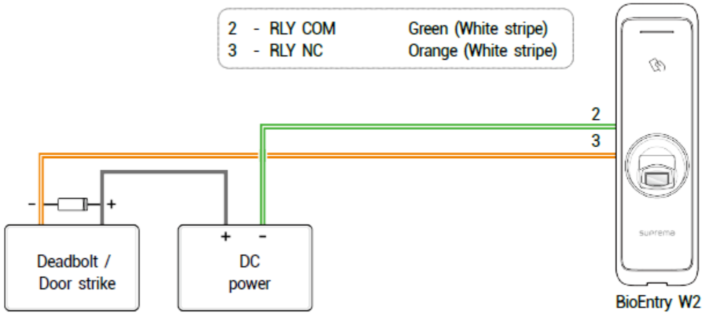
Contents

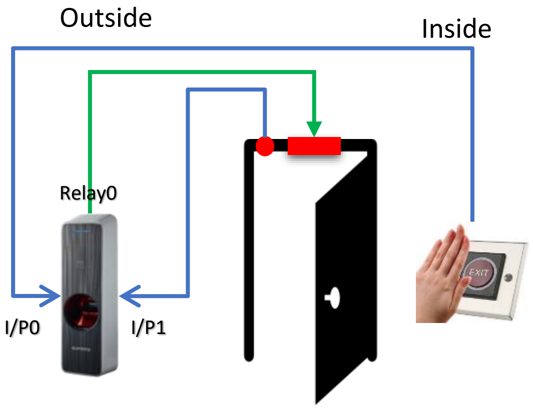
1. Webinar Goal
2. Understanding BioStar2 Access Control License
3. After BioStar2 installation
4. Activate BioStar2 license (online & offline)
5. Add devices (server mode, device mode, network precautions)
6. Add users (finger enrollment precautions to avoid FAR & FRR)
7. **Add doors (with 1 reader (IN) for a door and 2 readers (IN & OUT) for another door)**
8. Create Access group & Access level
9. Batch edit for users, devices, & doors
10. Private authentication for users
11. Custom fields for user profiles
12. Device configuration quick look
13. Understanding zones configuration

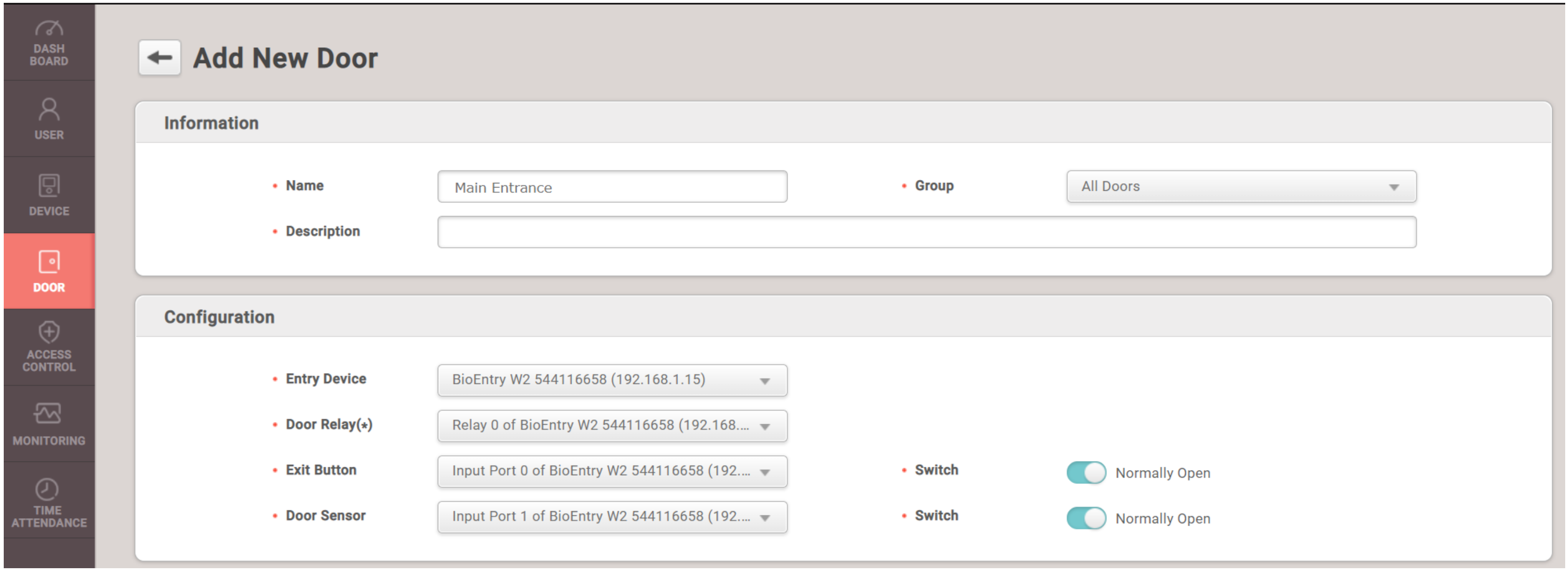
7 – Add doors (with 1 reader (IN) for a door and 2 readers (IN & OUT) for another door)

1. Adding a door with 1 reader (IN)

Usually in this setup, you will have 1 reader (IN), 1 Lock, 1 Exit Button, 1 Door Contact


2 - RLY COM Green (White stripe)
3 - RLY NC Orange (White stripe)
2
3
- +
Deadbolt / Door strike
+ -
DC power
suprema
BioEntry W2





Add New Door

Information

- Name: Main Entrance
- Group: All Doors
- Description:

Configuration

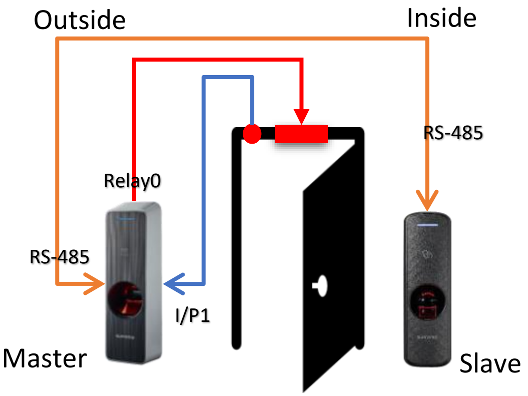
- Entry Device: BioEntry W2 544116658 (192.168.1.15)
- Door Relay(*): Relay 0 of BioEntry W2 544116658 (192.168....
- Exit Button: Input Port 0 of BioEntry W2 544116658 (192.... • Switch: Normally Open
- Door Sensor: Input Port 1 of BioEntry W2 544116658 (192.... • Switch: Normally Open

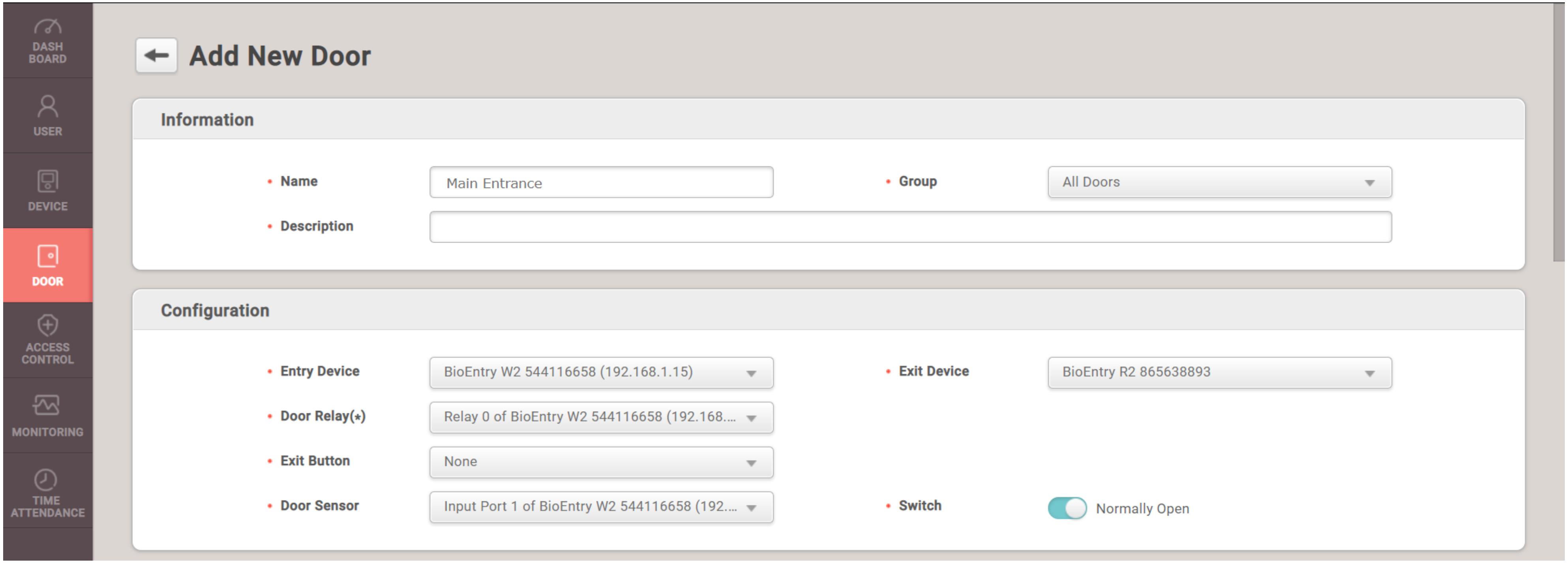
7 – Add doors (with 1 reader (IN) for a door and 2 readers (IN & OUT) for another door)

2. Adding a door with 2 readers (IN & OUT)

Usually in this setup, you will have 2 reader (IN & OUT), 1 Lock, 1 Door Contact

▬ ●





Add New Door

Information

- Name: Main Entrance
- Group: All Doors
- Description:

Configuration

- Entry Device: BioEntry W2 544116658 (192.168.1.15)
- Exit Device: BioEntry R2 865638893
- Door Relay(*): Relay 0 of BioEntry W2 544116658 (192.168....
- Exit Button: None
- Door Sensor: Input Port 1 of BioEntry W2 544116658 (192....
- Switch: Normally Open

Contents

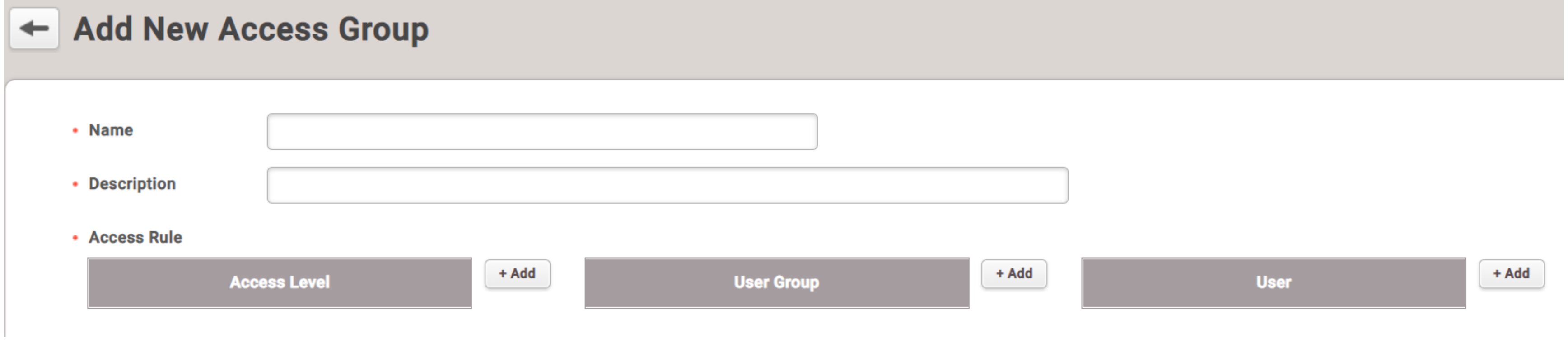
1. Webinar Goal
2. Understanding BioStar2 Access Control License
3. After BioStar2 installation
4. Activate BioStar2 license (online & offline)
5. Add devices (server mode, device mode, network precautions)
6. Add users (finger enrollment precautions to avoid FAR & FRR)
7. Add doors (with 1 reader (IN) for a door and 2 readers (IN & OUT) for another door)
8. **Create Access group & Access level**
9. Batch edit for users, devices, & doors
10. Private authentication for users
11. Custom fields for user profiles
12. Device configuration quick look
13. Understanding zones configuration

8 – Create Access group & Access level

What is Access Group?

A user/user group that has the right to access one or more Access Levels.

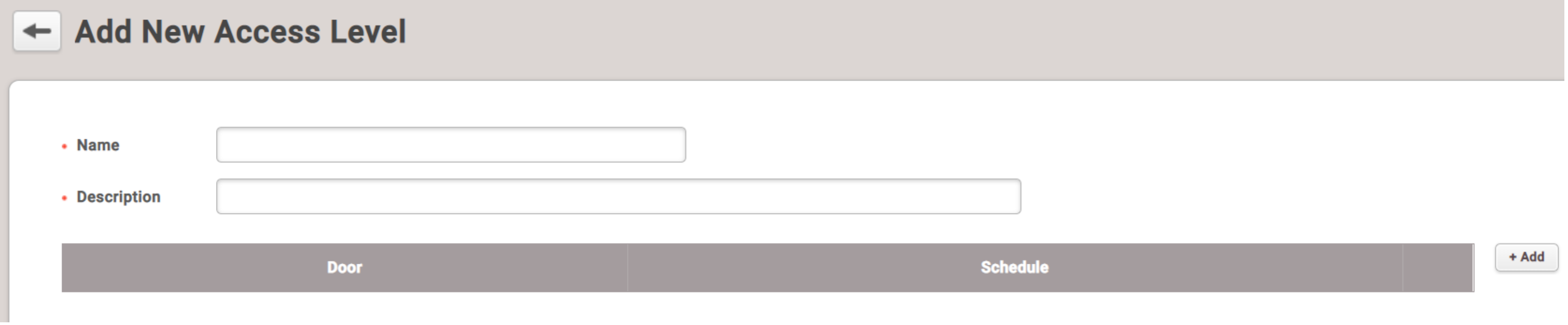
Access Group = user/user group + Access Level



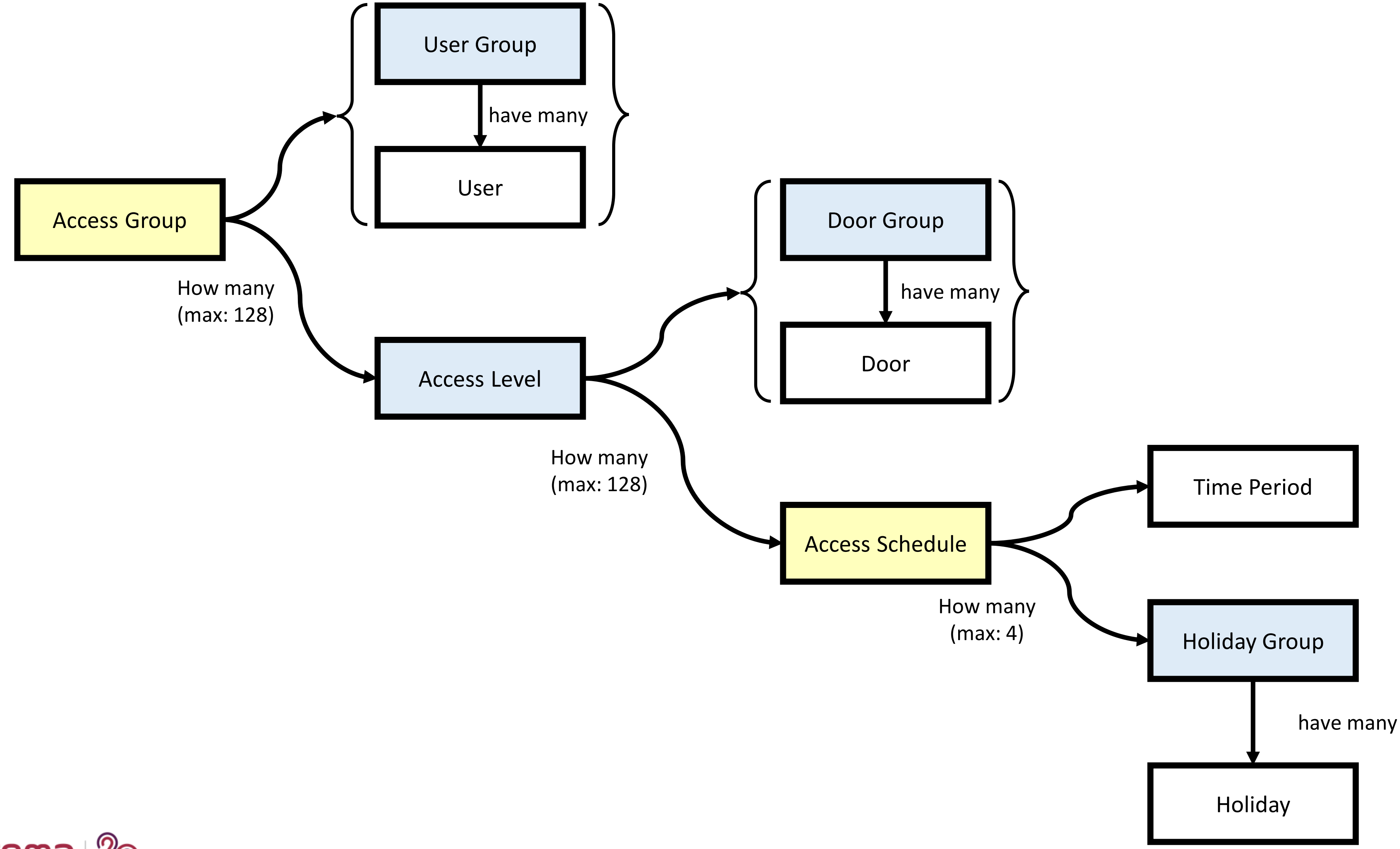
What is Access Level?

A door/door group with a scheduled period of time.

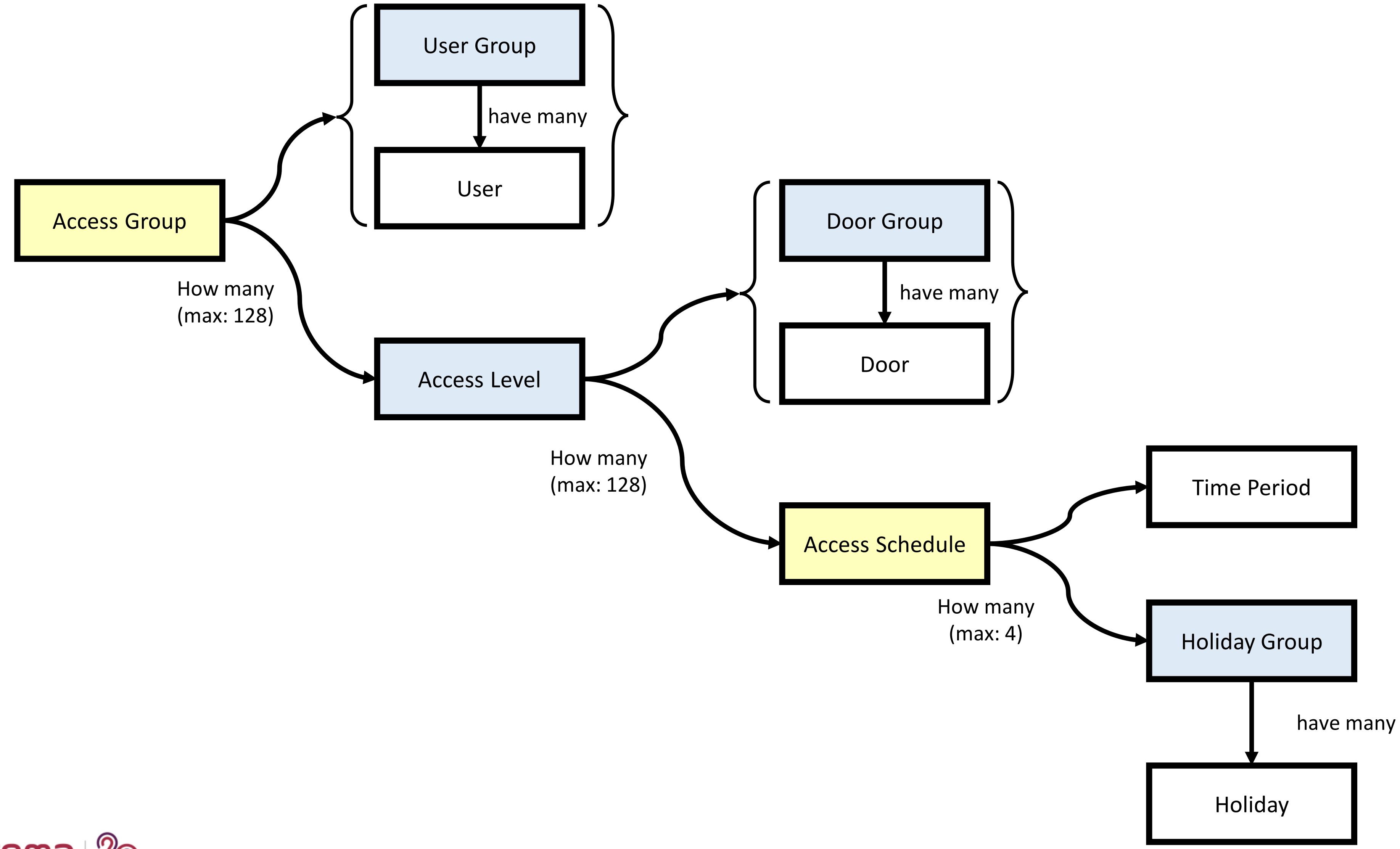
Access Level = Door/Door Group + Schedule



8 – Create Access group & Access level



8 – Create Access group & Access level



8 – Create Access group & Access level

How many Access Group & Access Levels can you Create?

There are 2 parts need to be considered:

1. Creation on BioStar2 →

Unlimited

2. Device: Synchronization with devices (device memory) →

Max Access Group	**2048**
Max Access Level	**2048**
Max Access Level per 1 Access Group	128
Max Door per 1 Access Level	128
Max Access Group per User	16

128 Access Levels assigned to one Access Group

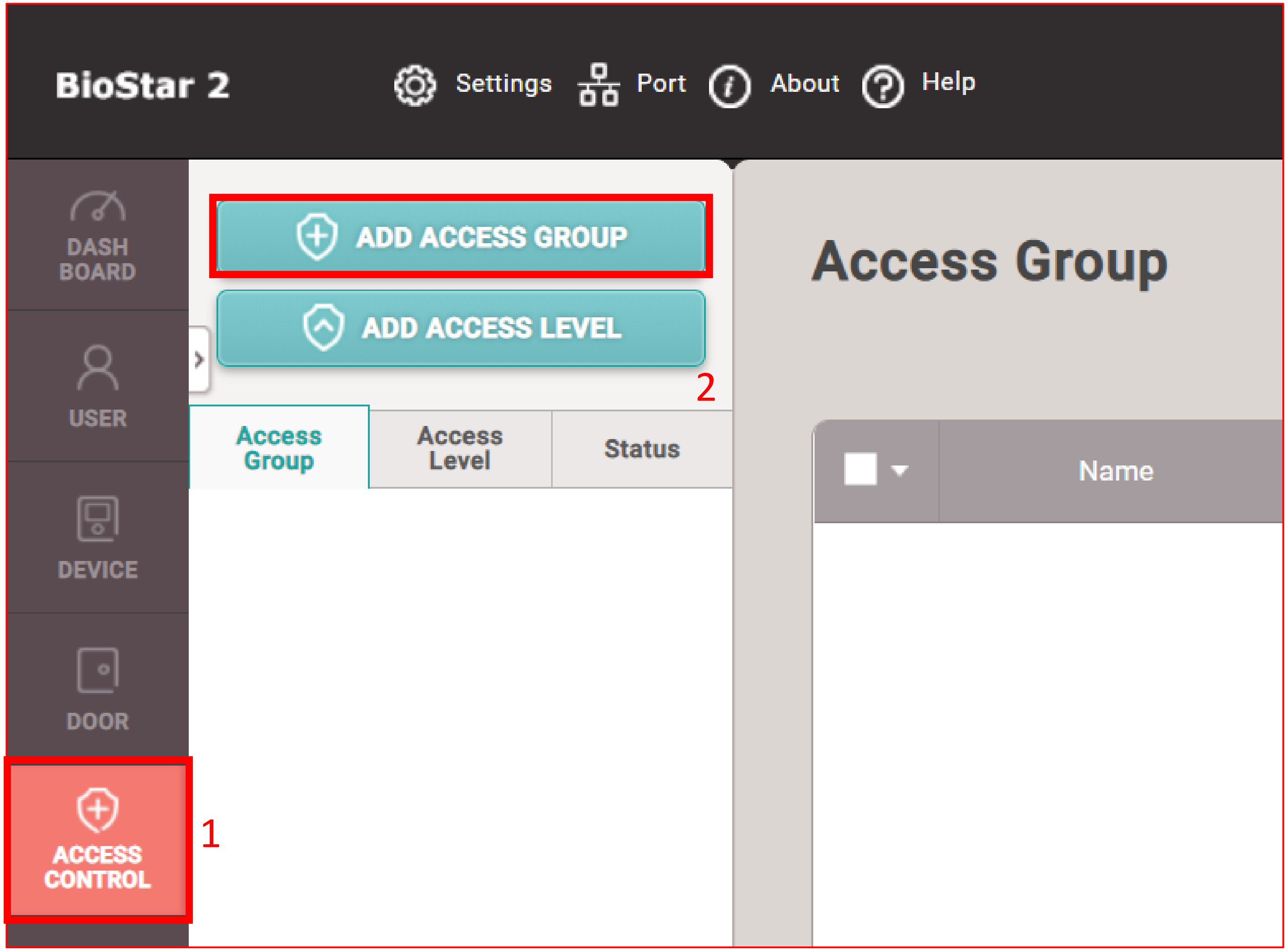
128 doors assigned to one Access Level

16 Access Group assigned to one user

Why do we need to store the AG & AL on the device? → **So the device will work offline**

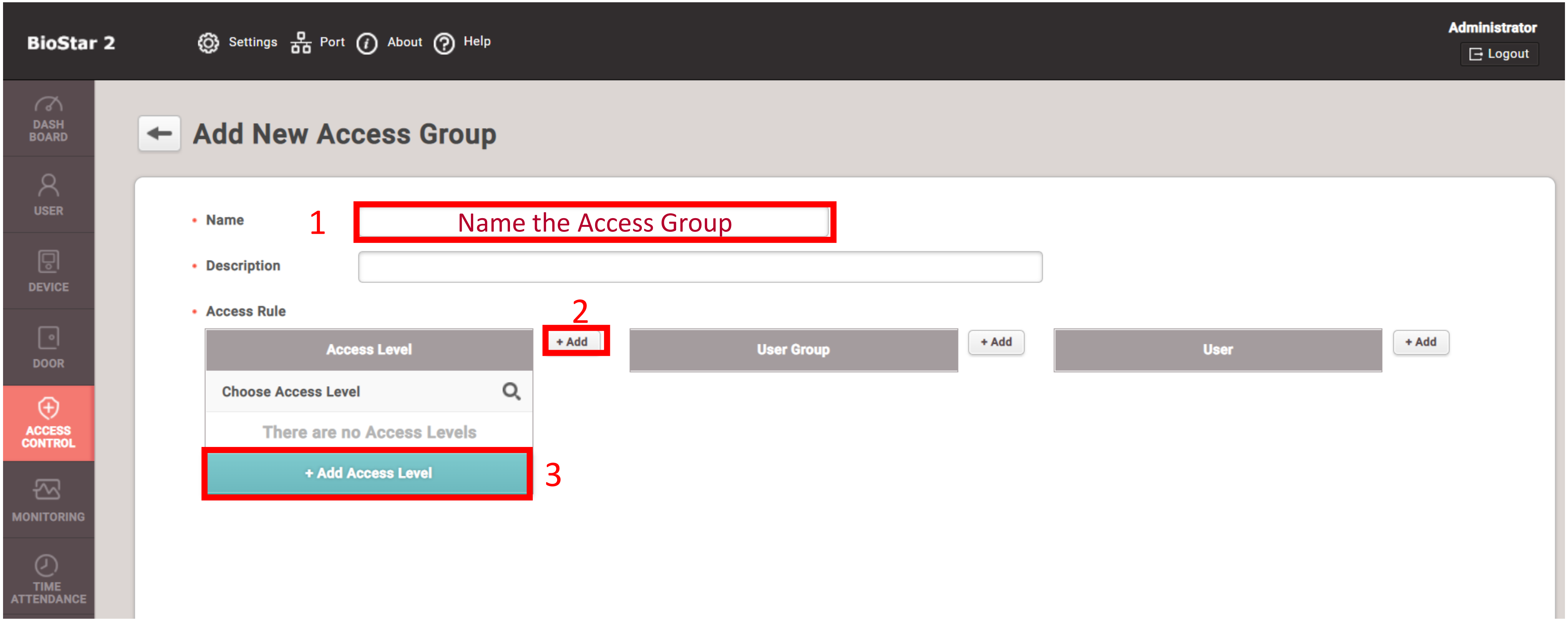
8 – Create Access group & Access level

How to create Access Group ?



8 – Create Access group & Access level

How to create Access Group ?



Add New Access Group

- Name 1 Name the Access Group
- Description
- Access Rule 2

Access Level

Choose Access Level

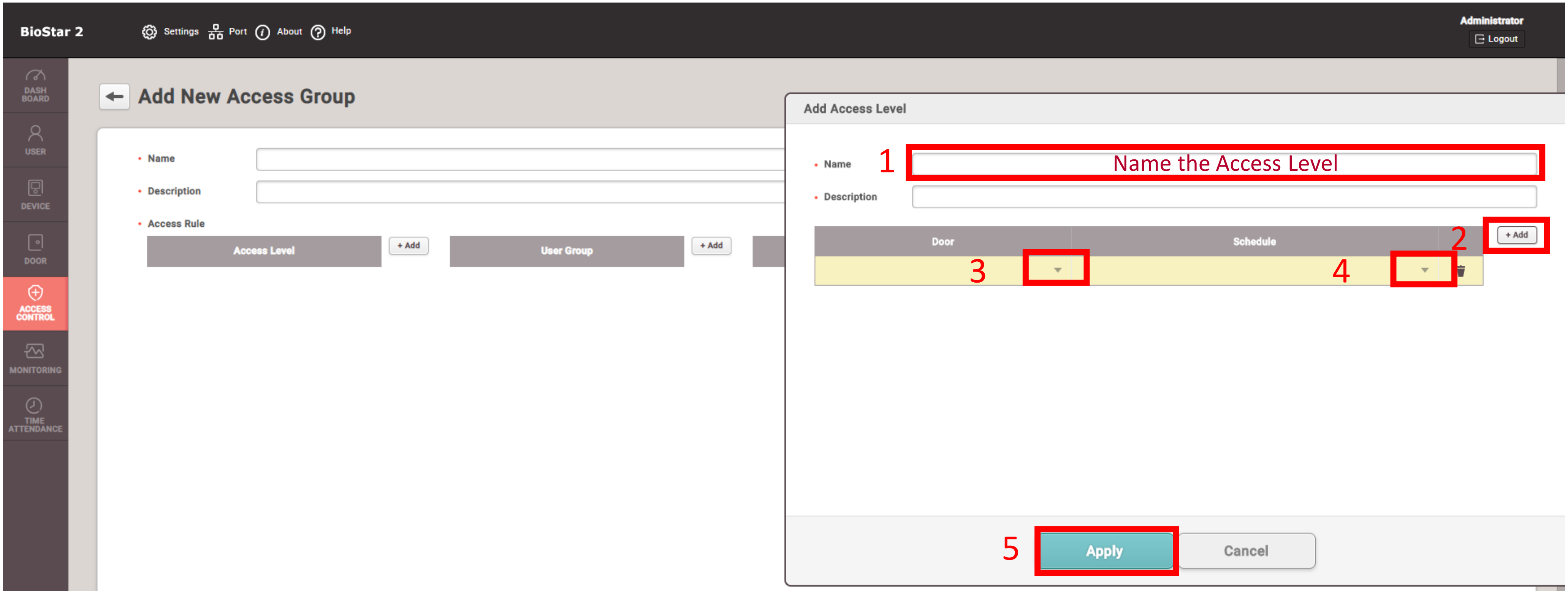
There are no Access Levels

+ Add Access Level 3

8 – Create Access group & Access level

1. Webinar Goal 2. License 3. After Installation 4. Activate license 5. Add Devices 6. Add Users 7. Add Doors 8.Access Group 9. Batch edit 10. Private Auth. 11. Custom Field 12. Device menu 13. Zones

How to create Access Group ?



1 Name the Access Level

2

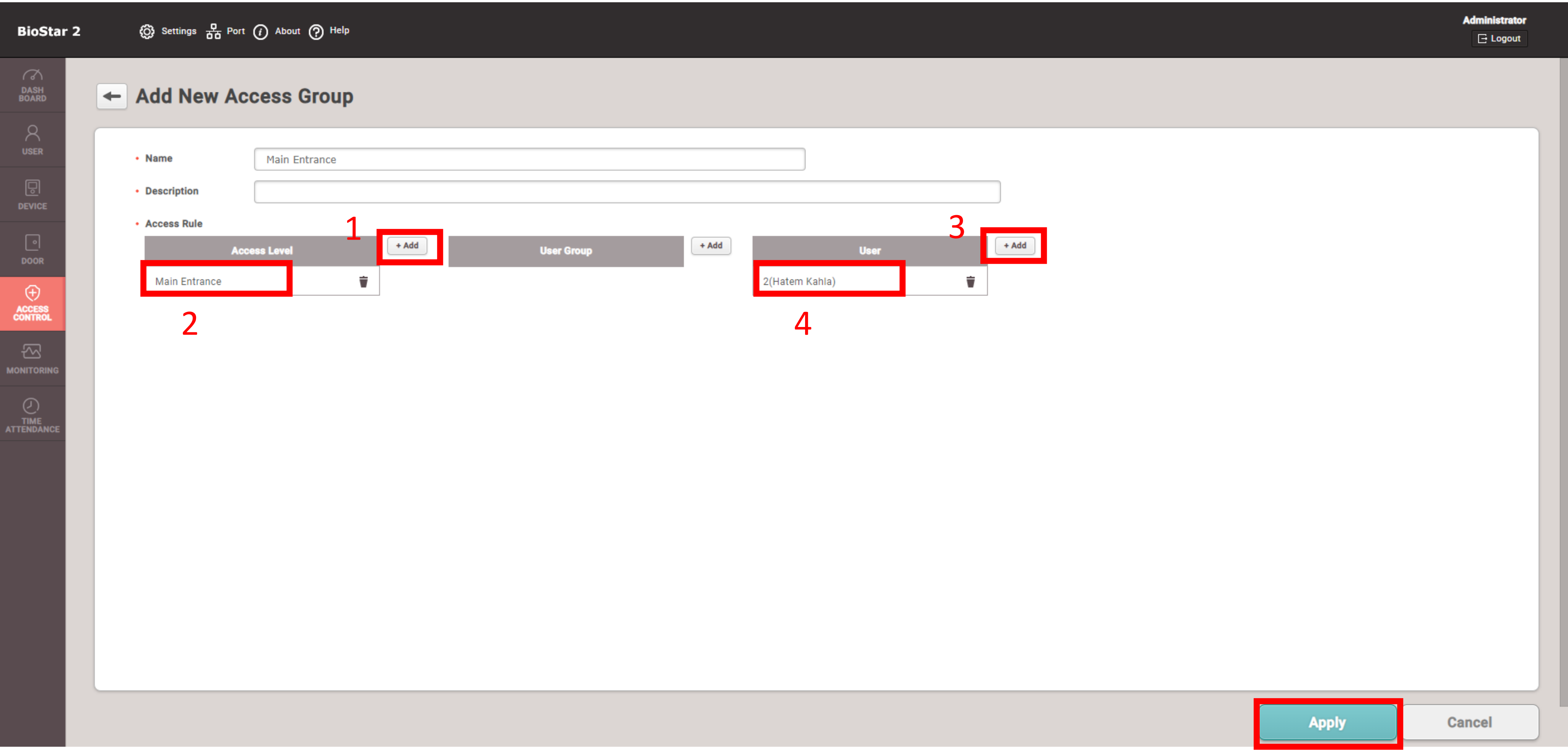
3

4

5

8 – Create Access group & Access level

How to create Access Group ?



BioStar 2

Add New Access Group

- Name: Main Entrance
- Description:
- Access Rule

Access Level	User Group	User
Main Entrance		2(Hatem Kahla)

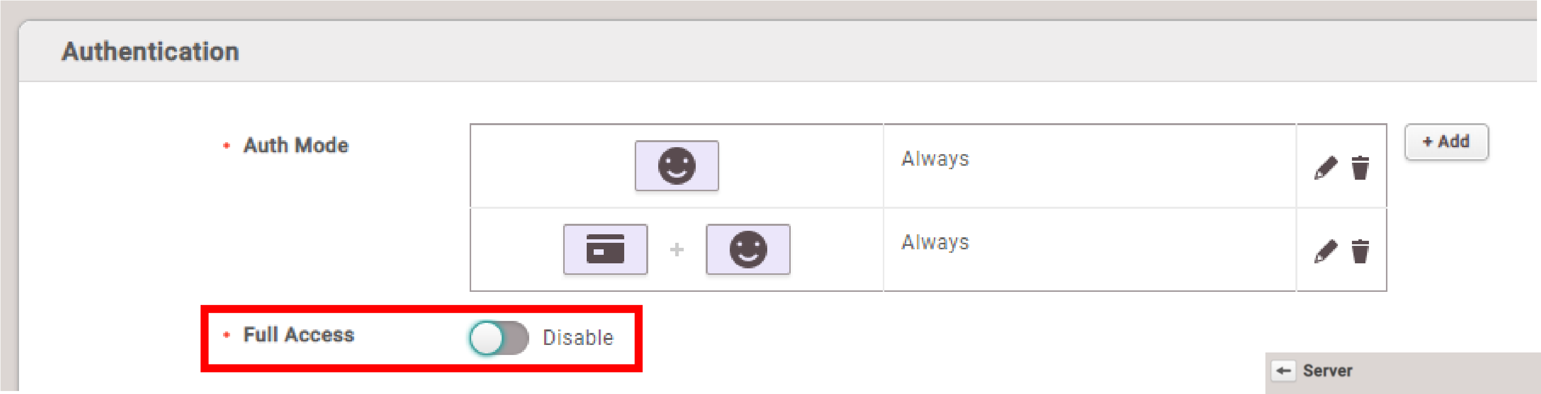
8 – Create Access group & Access level

Can we enable access to users without access group?

YES

There is an option called **Full Access** which will allow the access to all users saved on the reader

To enable that: go to device settings → Authentication → Full Access:



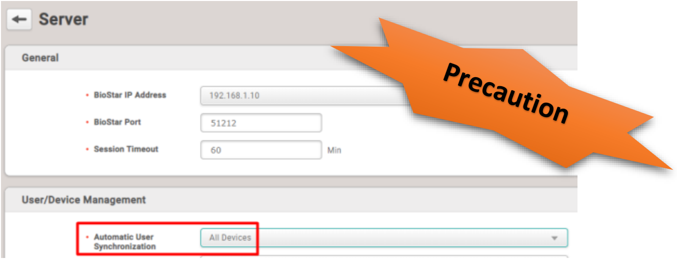
Authentication

- Auth Mode

☻	Always	✎ 🗑
▭ + ☻	Always	✎ 🗑

+ Add

- Full Access: Disable



Server

General

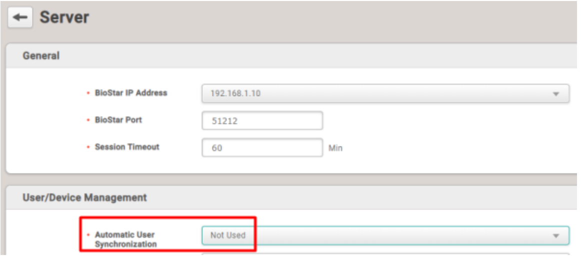
- BioStar IP Address: 192.168.1.10
- BioStar Port: 51212
- Session Timeout: 60 Min

User/Device Management

- Automatic User Synchronization: All Devices

Note: Automatic user synchronization is important:

1. If you want all enrolled users of the customer to access this door, chose All Devices



Server

General

- BioStar IP Address: 192.168.1.10
- BioStar Port: 51212
- Session Timeout: 60 Min

User/Device Management

- Automatic User Synchronization: Not Used

2. If you want specific users, chose Not used and transfer the users manually to the device

3. The door which has Full Access, Can't assign to Access Group

Demonstration of previous Steps
And
Q&A

Contents

1. Webinar Goal
2. Understanding BioStar2 Access Control License
3. After BioStar2 installation
4. Activate BioStar2 license (online & offline)
5. Add devices (server mode, device mode, network precautions)
6. Add users (finger enrollment precautions to avoid FAR & FRR)
7. Add doors (with 1 reader (IN) for a door and 2 readers (IN & OUT) for another door)
8. Create Access group & Access level
9. **Batch edit for users, devices, & doors**
10. Private authentication for users
11. Custom fields for user profiles
12. Device configuration quick look
13. Understanding zones configuration

9 – Batch edit for users, devices, & doors

What is Batch Edit?

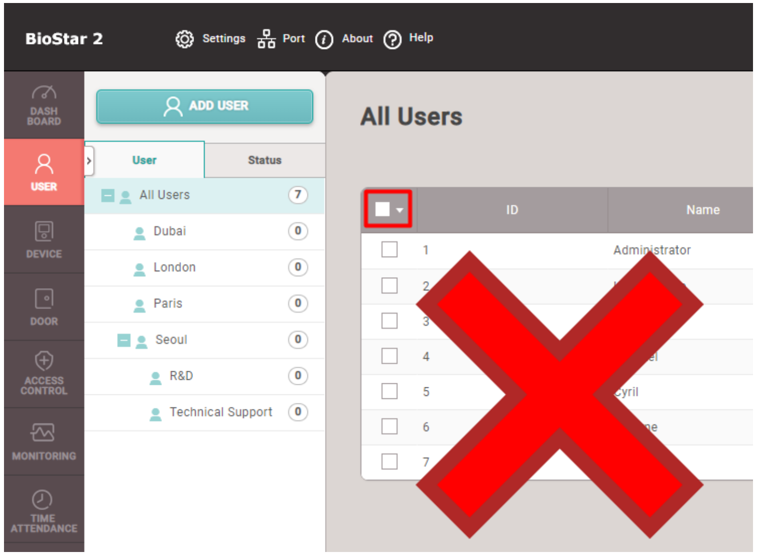
You can change the configuration of multiple selection at once in BioStar 2

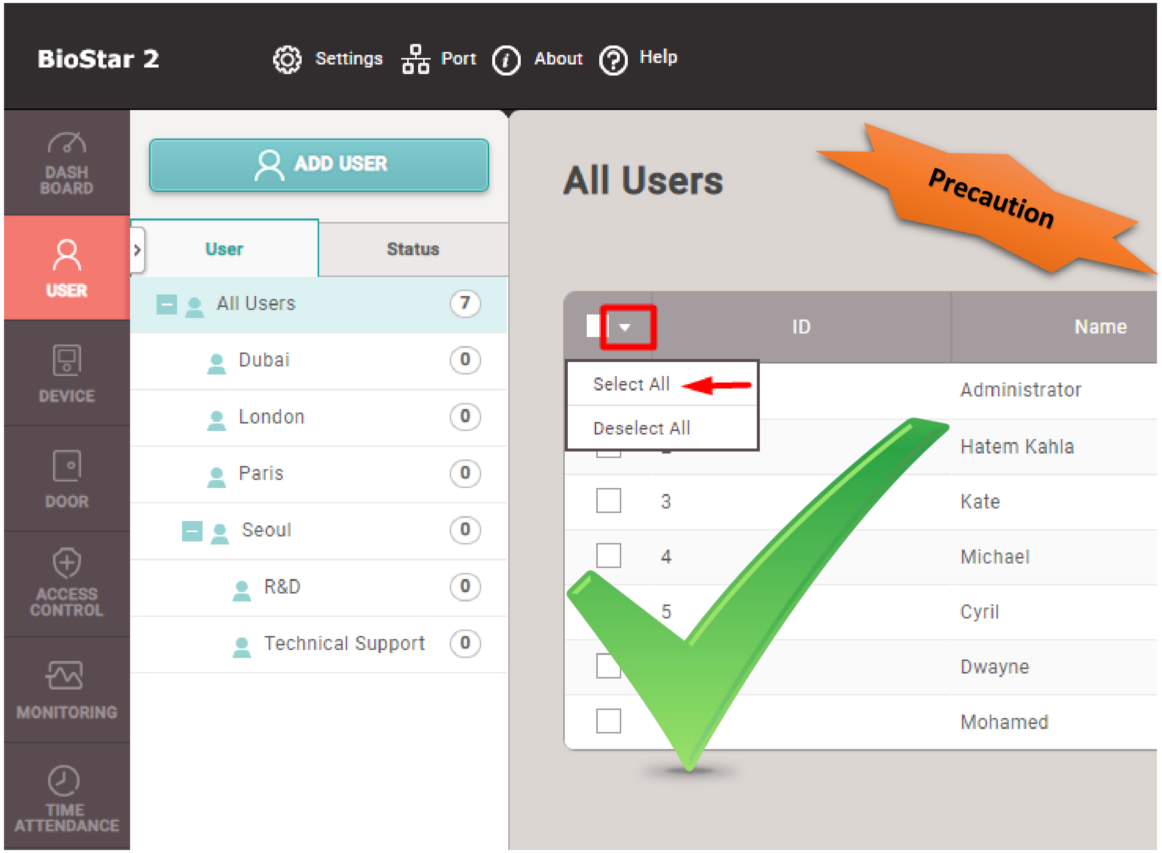
Which settings/configuration can I do Batch Edit to?

1. Users
2. Devices
3. Doors

How to chose all items in the list?

By clicking the top check box in the heading?

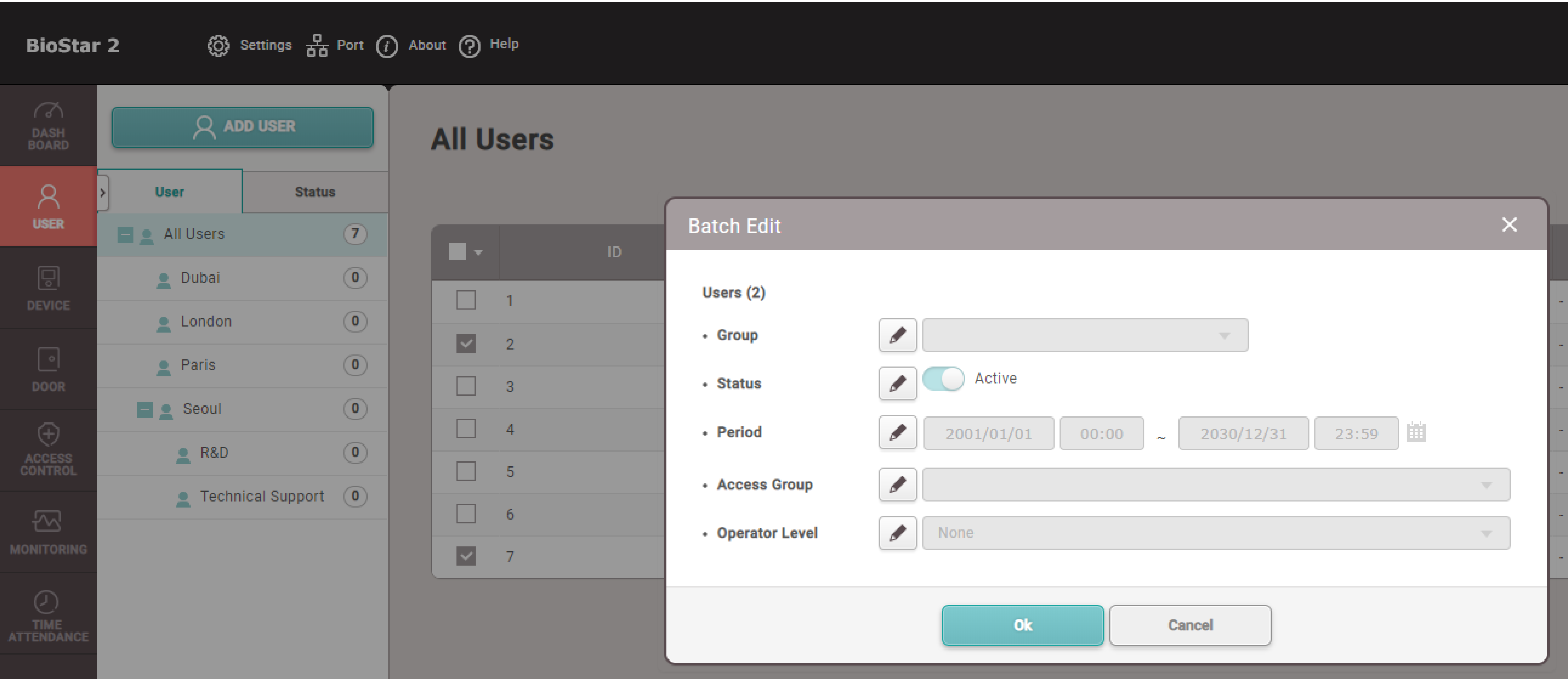




9 – Batch edit for users, devices, & doors

1. Batch Edit for Users

Select Users / All Users and click batch edit

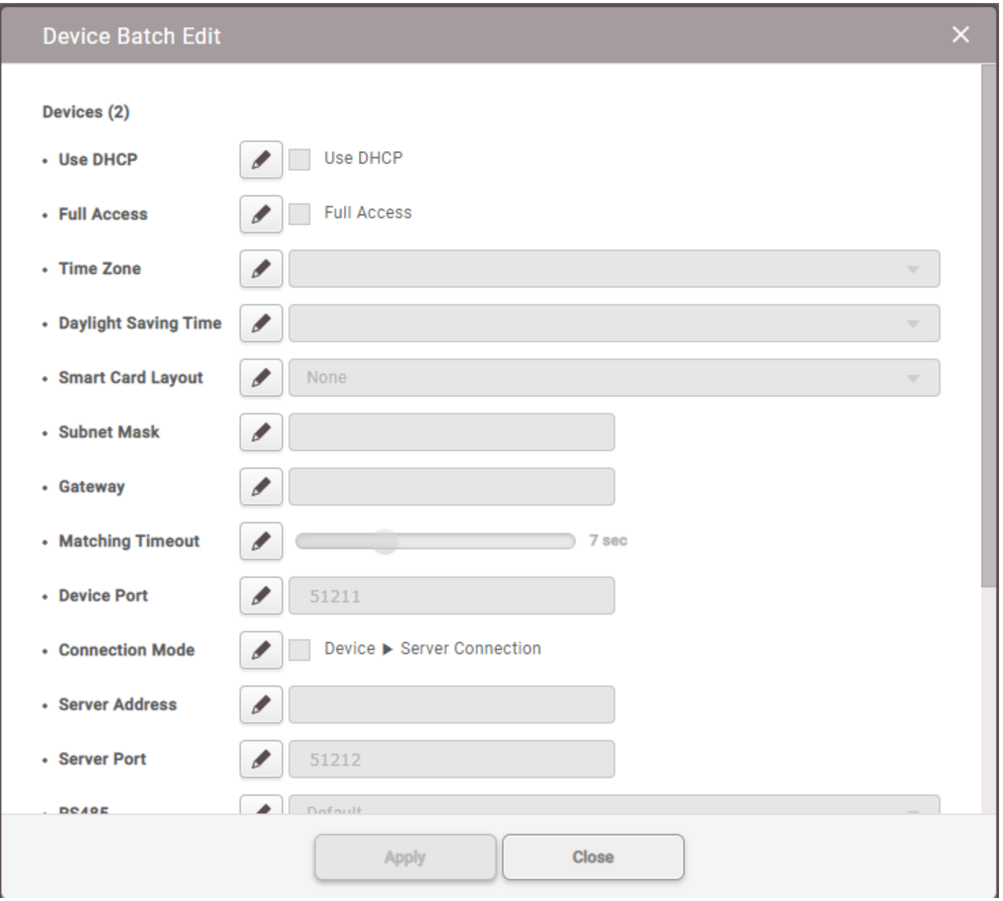


Users (2)

- Group
- Status: Active
- Period: 2001/01/01 00:00 ~ 2030/12/31 23:59
- Access Group
- Operator Level: None

2. Batch Edit for Device

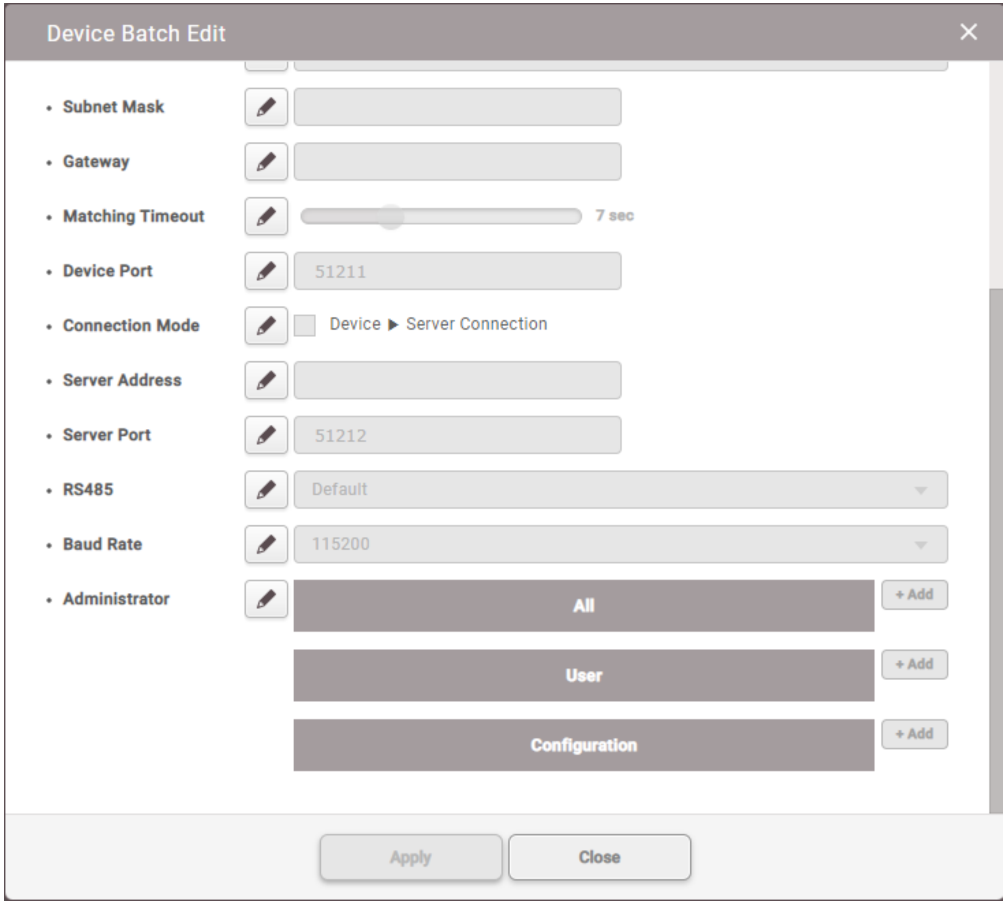
Select Devices / All Devices and click batch edit



Device Batch Edit

Devices (2)

- Use DHCP □ Use DHCP
- Full Access □ Full Access
- Time Zone
- Daylight Saving Time
- Smart Card Layout: None
- Subnet Mask
- Gateway
- Matching Timeout: 7 sec
- Device Port: 51211
- Connection Mode □ Device ▶ Server Connection
- Server Address
- Server Port: 51212
- RS485: Default



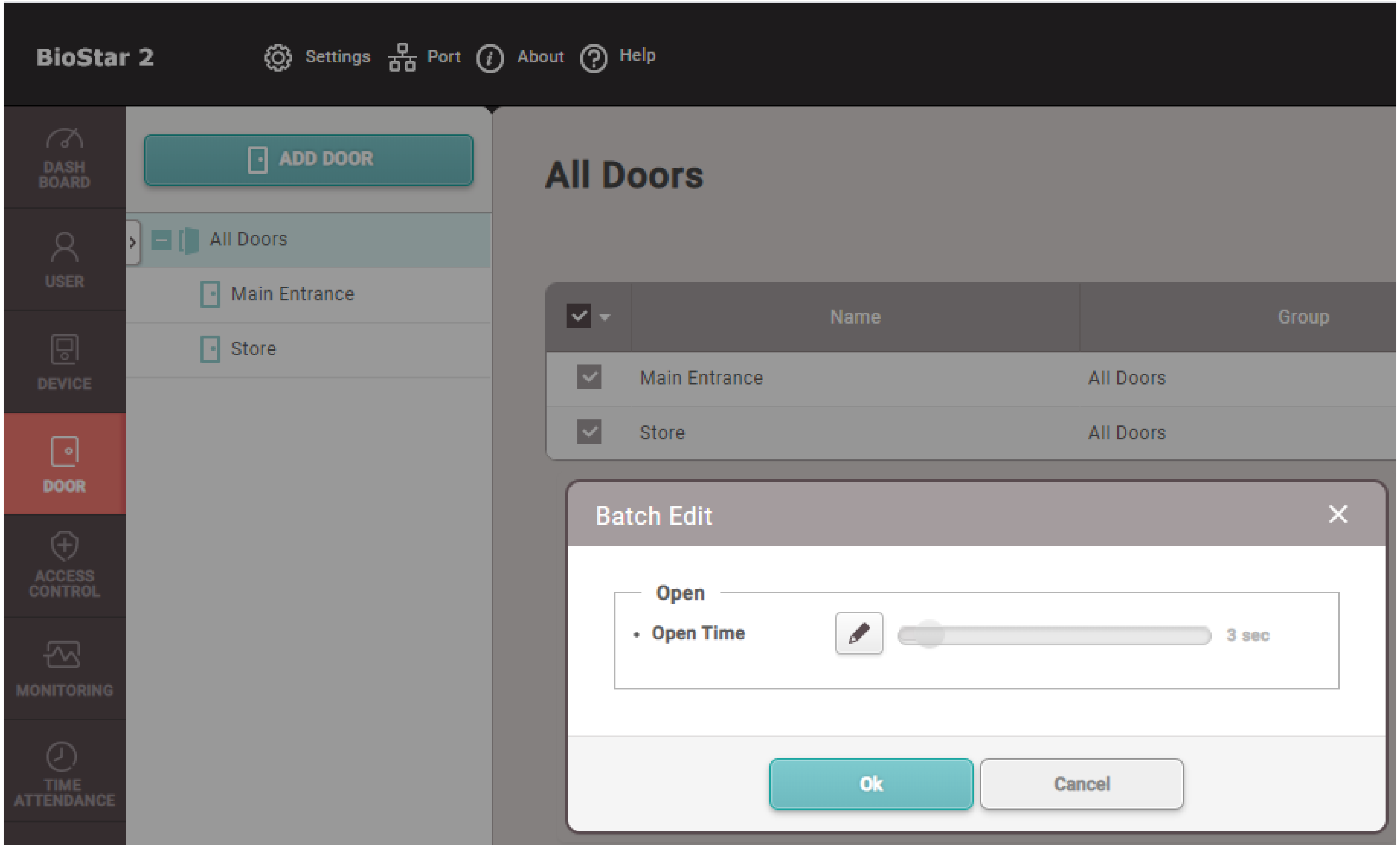
Device Batch Edit

- Subnet Mask
- Gateway
- Matching Timeout: 7 sec
- Device Port: 51211
- Connection Mode □ Device ▶ Server Connection
- Server Address
- Server Port: 51212
- RS485: Default
- Baud Rate: 115200
- Administrator: All + Add; User + Add; Configuration + Add

9 – Batch edit for users, devices, & doors

3. Batch Edit for Doors

Select Doors / All Doors and click batch edit



All Doors

☑	Name	Group
☑	Main Entrance	All Doors
☑	Store	All Doors

Open Time: 3 sec

Demonstration

1. Webinar Goal 2. License 3. After Installation 4. Activate license 5. Add Devices 6. Add Users 7. Add Doors 8.Access Group 9. Batch edit 10. Private Auth. 11. Custom Field 12. Device menu 13. Zones

Demonstration of previous Steps
And
Q&A

Contents

1. Webinar Goal
2. Understanding BioStar2 Access Control License
3. After BioStar2 installation
4. Activate BioStar2 license (online & offline)
5. Add devices (server mode, device mode, network precautions)
6. Add users (finger enrollment precautions to avoid FAR & FRR)
7. Add doors (with 1 reader (IN) for a door and 2 readers (IN & OUT) for another door)
8. Create Access group & Access level
9. Batch edit for users, devices, & doors
10. **Private authentication for users**
11. Custom fields for user profiles
12. Device configuration quick look
13. Understanding zones configuration

10 – Private authentication for users

Normal Authentication:

Authentication means to check, compare, match your live biometric with the stored biometric.

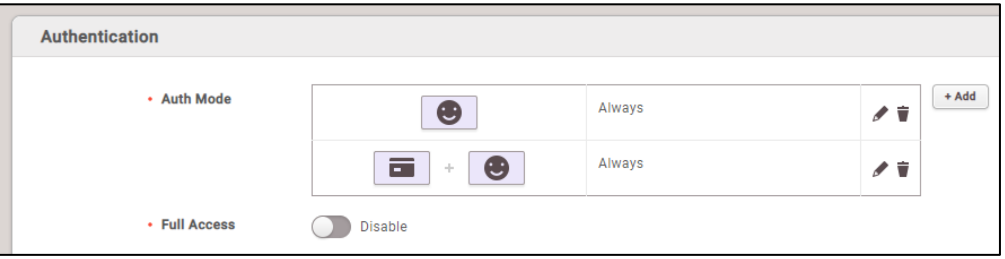
All users will follow the device default authentication.

Each authentication has a schedule.

It is used either for AC or TA

Example:

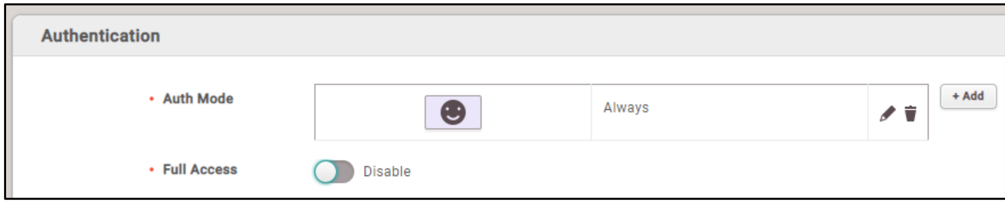
FaceStation2



Authentication

- Auth Mode: ☺ — Always; ▭ + ☺ — Always
- Full Access: ○ Disable

FaceLite



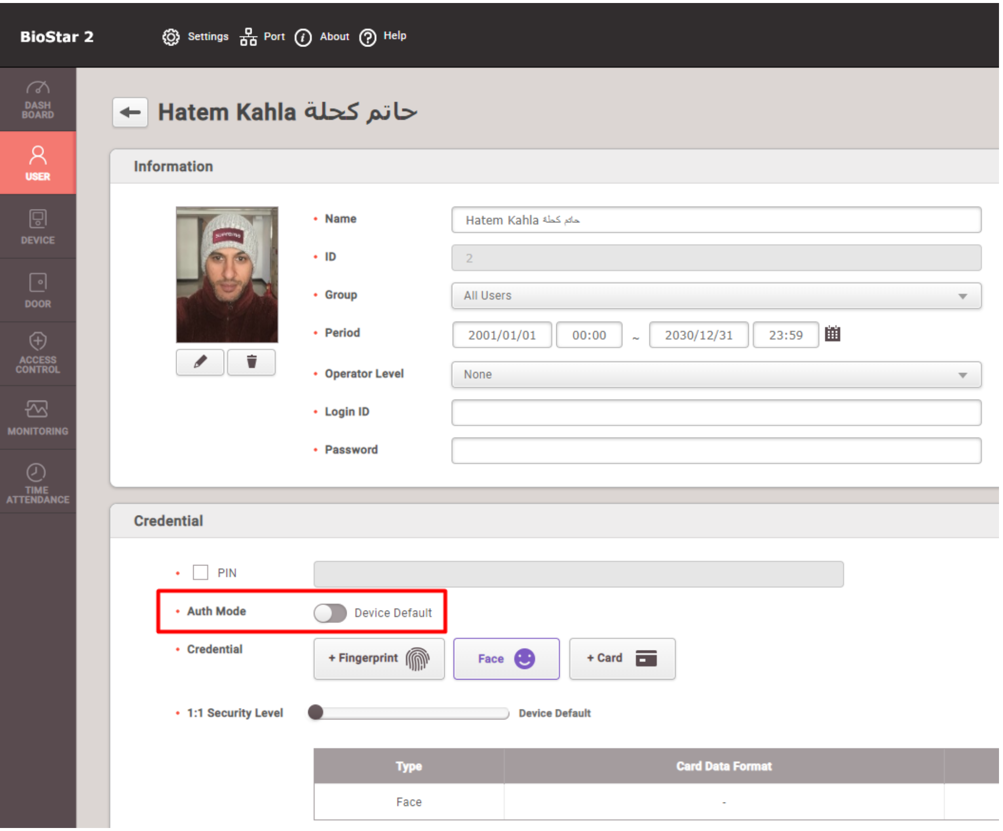
Authentication

- Auth Mode: ☺ — Always
- Full Access: ○ Disable

10 – Private authentication for users

Private Authentication:

The user with private authentication can have additional authentication for him/her only, including the normal authentication or not.
Can be also forced to use only a specific authentication without the normal authentication.



Hatem Kahla حاتم كحلة

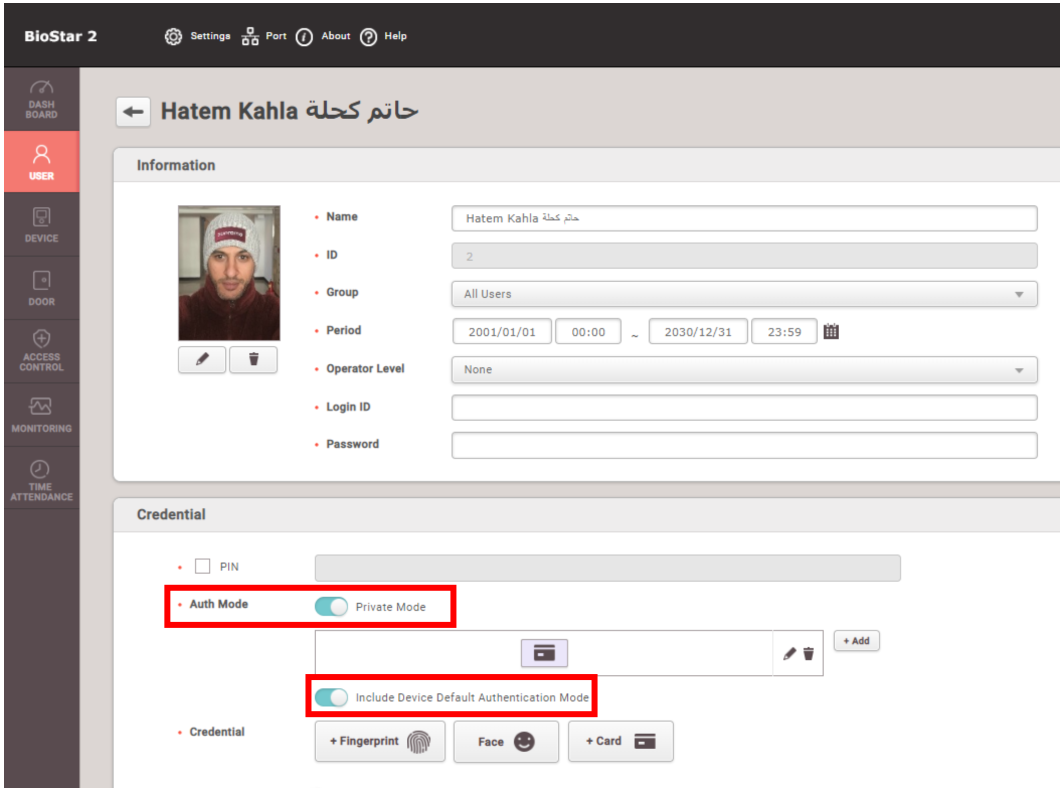
Information

- Name: Hatem Kahla حاتم كحلة
- ID: 2
- Group: All Users
- Period: 2001/01/01 00:00 ~ 2030/12/31 23:59
- Operator Level: None
- Login ID:
- Password:

Credential

- □ PIN
- Auth Mode: Device Default
- Credential: + Fingerprint | Face | + Card
- 1:1 Security Level: Device Default

Type	Card Data Format
Face	-



Hatem Kahla حاتم كحلة

Information

- Name: Hatem Kahla حاتم كحلة
- ID: 2
- Group: All Users
- Period: 2001/01/01 00:00 ~ 2030/12/31 23:59
- Operator Level: None
- Login ID:
- Password:

Credential

- □ PIN
- Auth Mode: Private Mode
- Include Device Default Authentication Mode
- Credential: + Fingerprint | Face | + Card

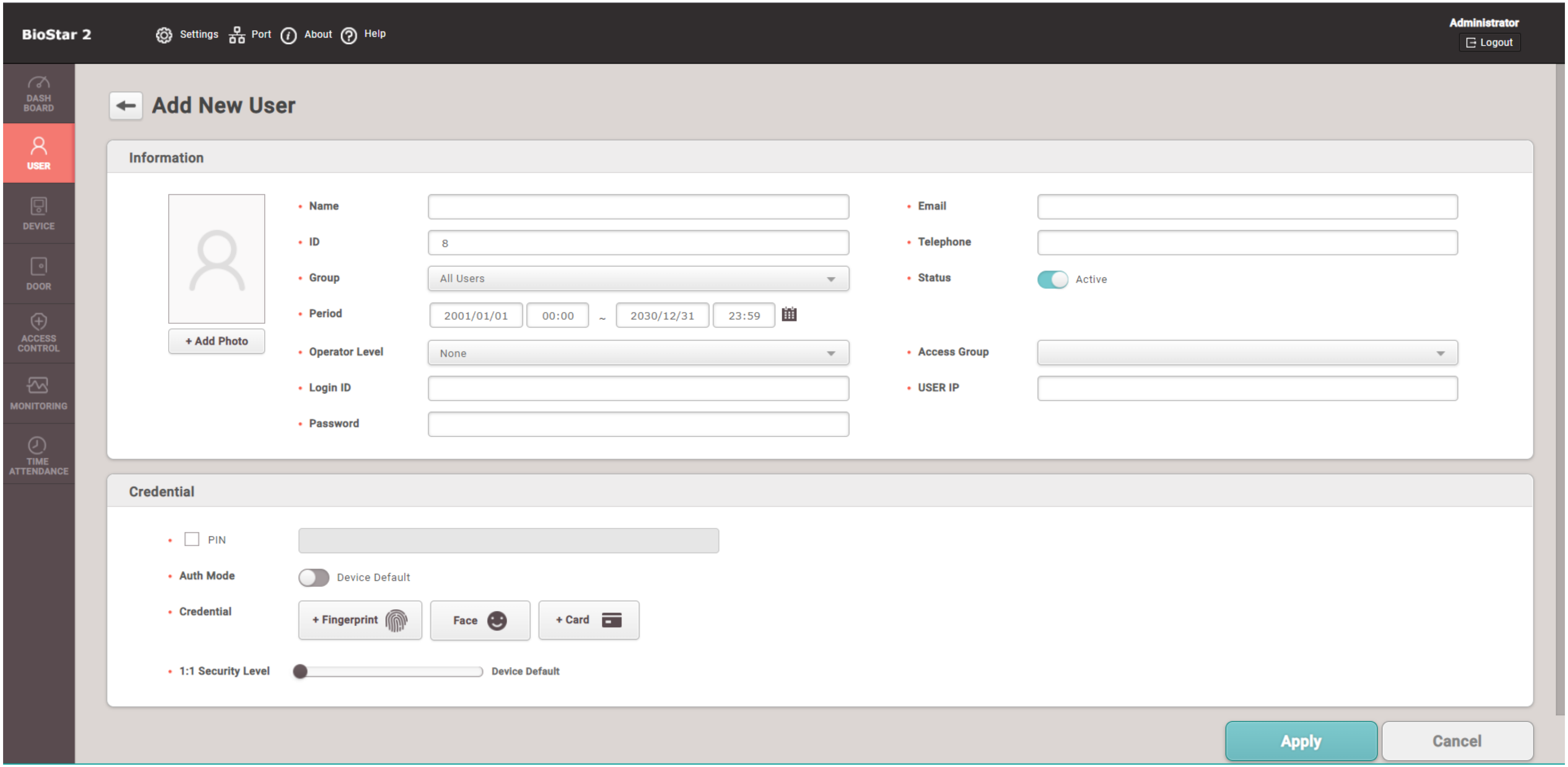
Contents

1. Webinar Goal
2. Understanding BioStar2 Access Control License
3. After BioStar2 installation
4. Activate BioStar2 license (online & offline)
5. Add devices (server mode, device mode, network precautions)
6. Add users (finger enrollment precautions to avoid FAR & FRR)
7. Add doors (with 1 reader (IN) for a door and 2 readers (IN & OUT) for another door)
8. Create Access group & Access level
9. Batch edit for users, devices, & doors
10. Private authentication for users
11. **Custom fields for user profiles**
12. Device configuration quick look
13. Understanding zones configuration

11 – Custom fields for user profiles

Custom Field ?

Additional field in the user profile information additional to the default fields below:



Add New User

Information

• Name		• Email	
• ID	8	• Telephone	
• Group	All Users	• Status	Active
• Period	2001/01/01 00:00 ~ 2030/12/31 23:59		
• Operator Level	None	• Access Group	
• Login ID		• USER IP	
• Password			

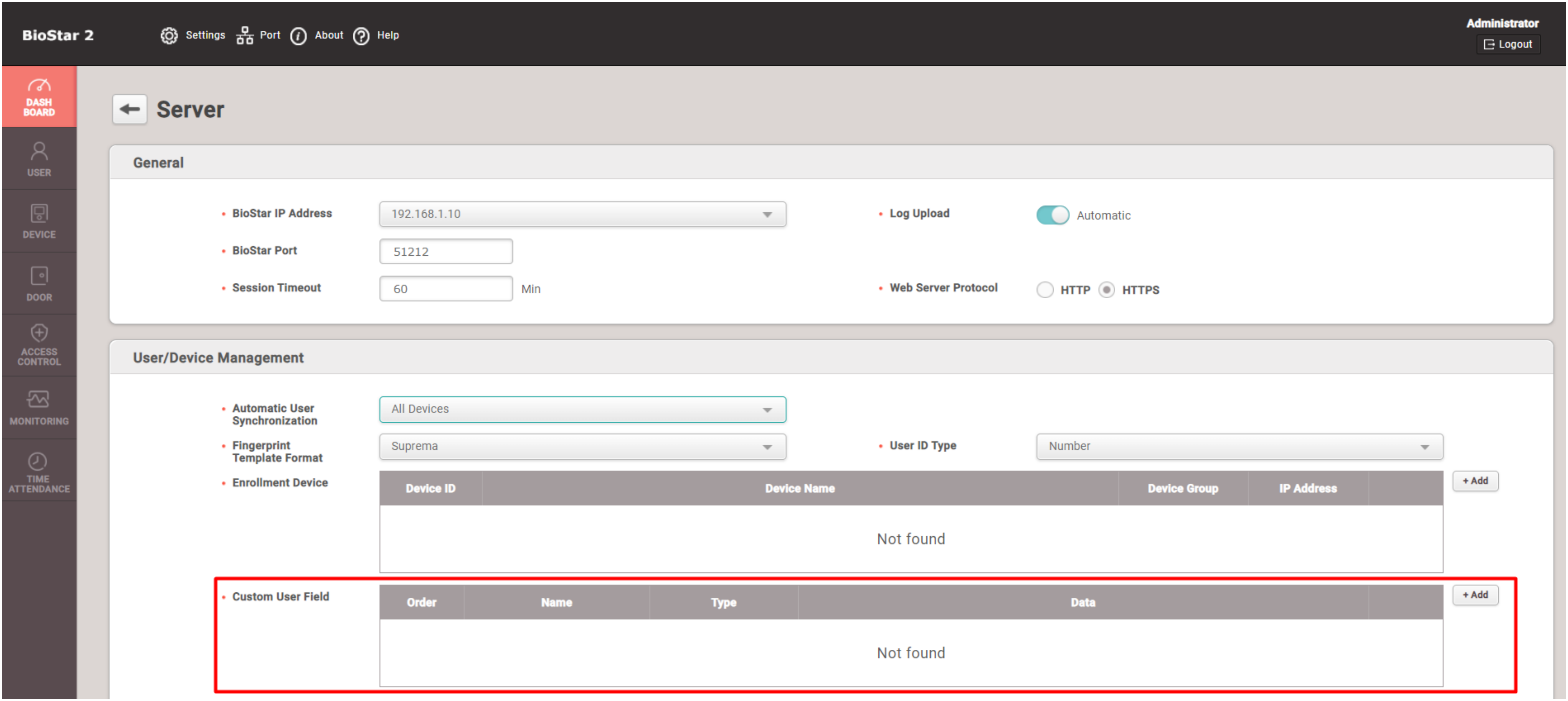
Credential

• □ PIN	
• Auth Mode	Device Default
• Credential	+ Fingerprint · Face · + Card
• 1:1 Security Level	Device Default

11 – Custom fields for user profiles

How to add Custom Field?

Go to Settings → SERVER → add custom field



Server

General

- BioStar IP Address: 192.168.1.10
- BioStar Port: 51212
- Session Timeout: 60 Min
- Log Upload: Automatic
- Web Server Protocol: ○ HTTP ● HTTPS

User/Device Management

- Automatic User Synchronization: All Devices
- Fingerprint Template Format: Suprema
- User ID Type: Number
- Enrollment Device

Device ID	Device Name	Device Group	IP Address
Not found			

+ Add

- Custom User Field

Order	Name	Type	Data
Not found			

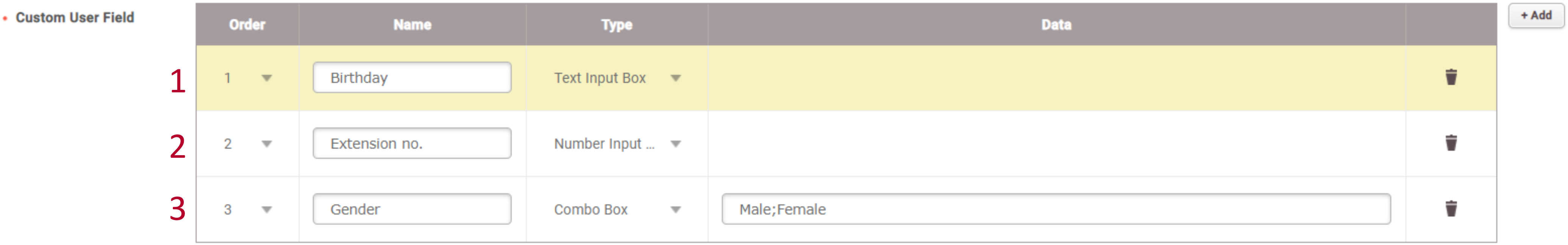
+ Add

11 – Custom fields for user profiles

How to add Custom Field? (Cont'd)

Go to Settings → SERVER → add custom field → Add

You can add up-to 10 custom fields and there is 3 Types

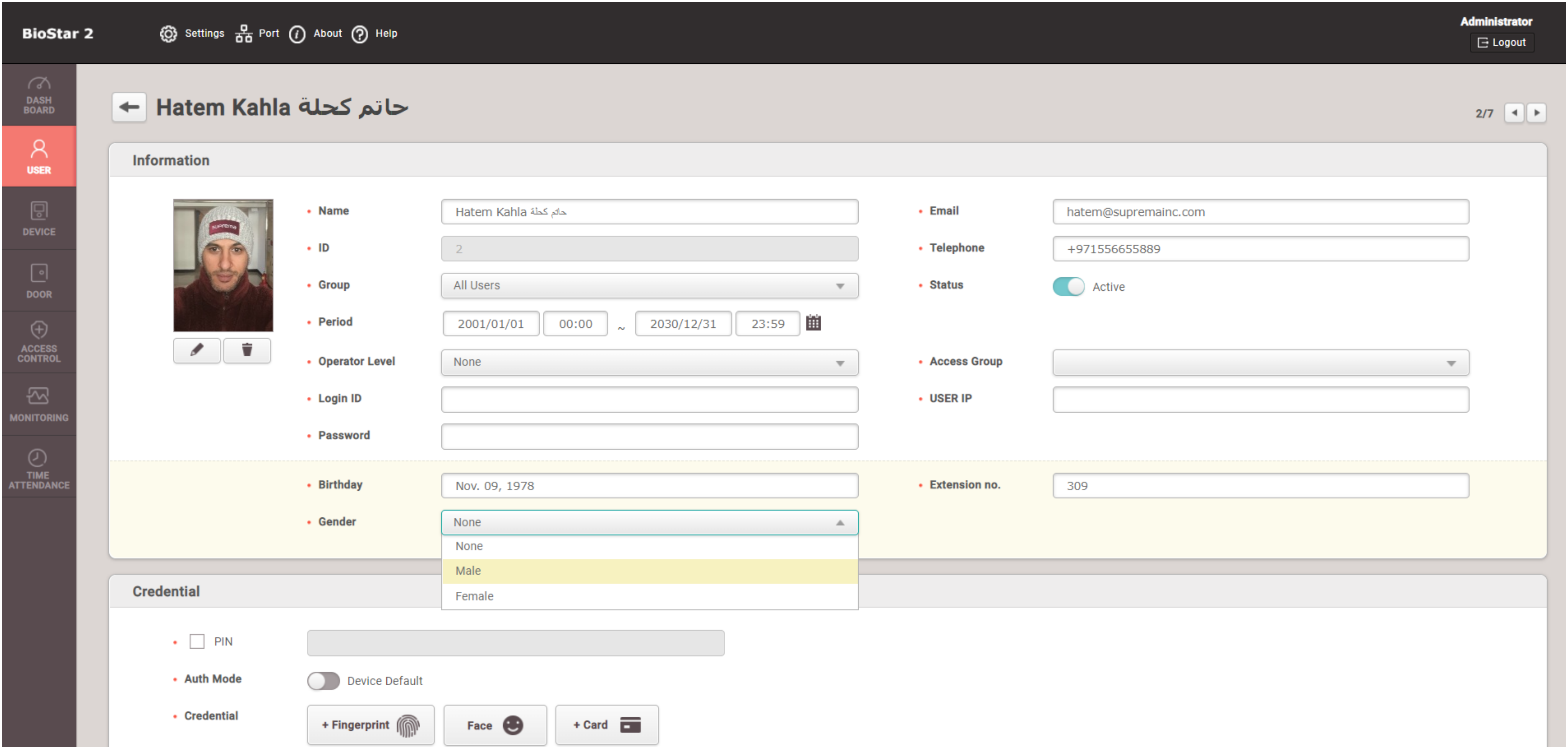


Order	Name	Type	Data
1	Birthday	Text Input Box	
2	Extension no.	Number Input ...	
3	Gender	Combo Box	Male;Female

1. **Text input Box**: you can type alphanumeric (letters & numbers) in this field
2. **Number Input Box** : you can type numbers only in this field
3. **Combo Box (Drop menu):** you can add up to 20 items with 32 characters each, and each item is separated by a semicolon (;).

11 – Custom fields for user profiles

Example:



Hatem Kahla حاتم كحلة

Information

Name	Hatem Kahla حاتم كحلة	Email	hatem@supremainc.com
ID	2	Telephone	+971556655889
Group	All Users	Status	Active
Period	2001/01/01 00:00 ~ 2030/12/31 23:59		
Operator Level	None	Access Group	
Login ID		USER IP	
Password			
Birthday	Nov. 09, 1978	Extension no.	309
Gender	None		

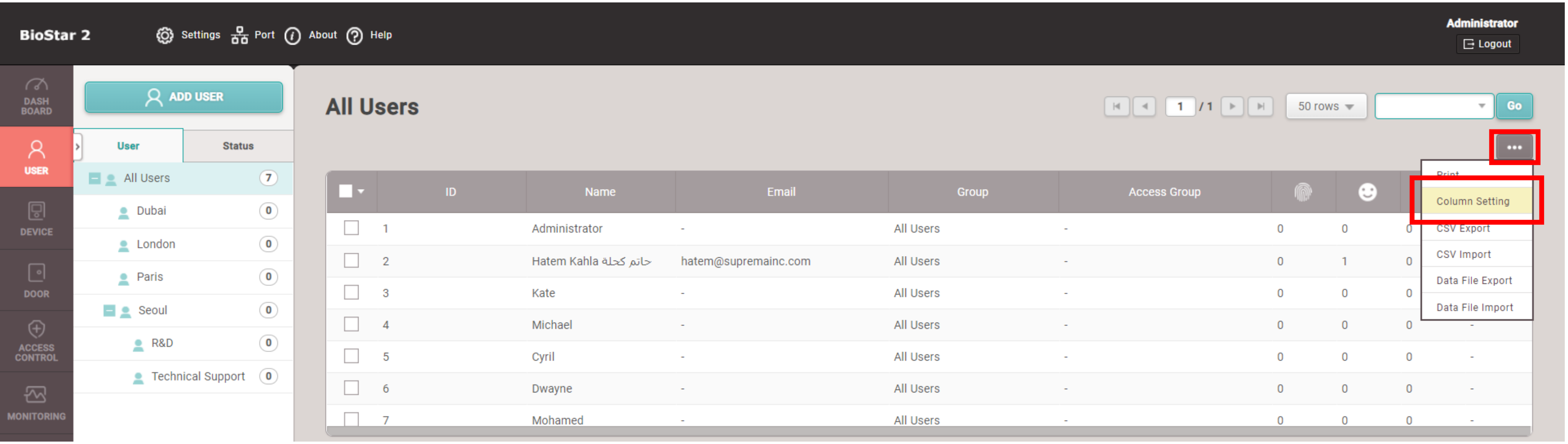
Gender options: None, Male, Female

Credential

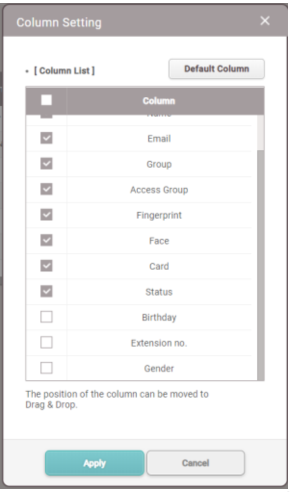
- □ PIN
- Auth Mode: Device Default
- Credential: + Fingerprint, Face, + Card

11 – Custom fields for user profiles

You can add those custom fields to the user menu view columns :



□	ID	Name	Email	Group	Access Group				
□	1	Administrator	-	All Users	-	0	0	0	
□	2	Hatem Kahla حاتم كحلة	hatem@supremainc.com	All Users	-	0	1	0	
□	3	Kate	-	All Users	-	0	0	0	
□	4	Michael	-	All Users	-	0	0	0	-
□	5	Cyril	-	All Users	-	0	0	0	-
□	6	Dwayne	-	All Users	-	0	0	0	-
□	7	Mohamed	-	All Users	-	0	0	0	-



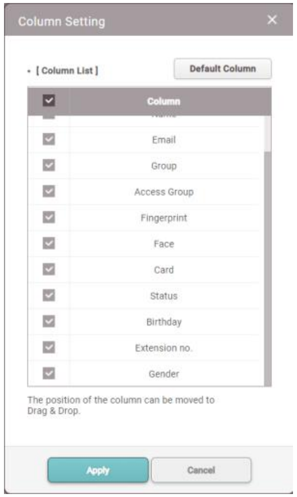
Column Setting

• [Column List] Default Column

□	Column
☑	Email
☑	Group
☑	Access Group
☑	Fingerprint
☑	Face
☑	Card
☑	Status
□	Birthday
□	Extension no.
□	Gender

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

Apply Cancel



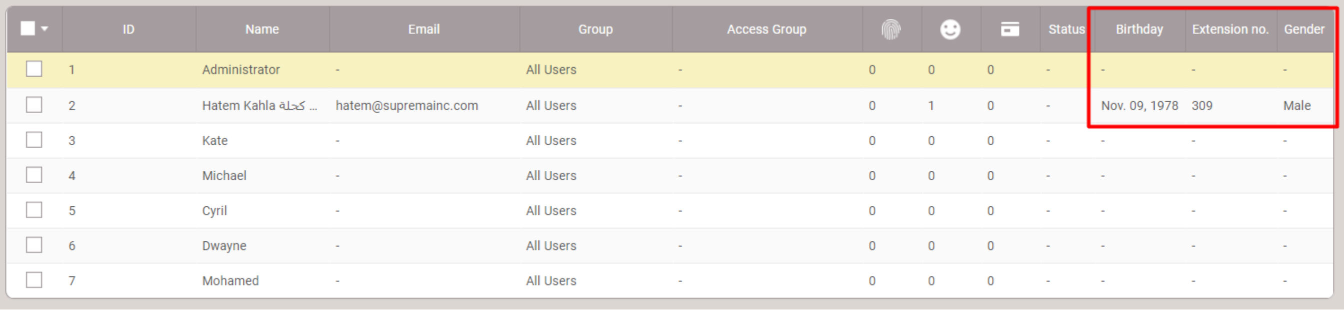
Column Setting

• [Column List] Default Column

☑	Column
☑	Email
☑	Group
☑	Access Group
☑	Fingerprint
☑	Face
☑	Card
☑	Status
☑	Birthday
☑	Extension no.
☑	Gender

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

Apply Cancel



□	ID	Name	Email	Group	Access Group				Status	Birthday	Extension no.	Gender
□	1	Administrator	-	All Users	-	0	0	0	-	-	-	-
□	2	Hatem Kahla كحلة ...	hatem@supremainc.com	All Users	-	0	1	0	-	Nov. 09, 1978	309	Male
□	3	Kate	-	All Users	-	0	0	0	-	-	-	-
□	4	Michael	-	All Users	-	0	0	0	-	-	-	-
□	5	Cyril	-	All Users	-	0	0	0	-	-	-	-
□	6	Dwayne	-	All Users	-	0	0	0	-	-	-	-
□	7	Mohamed	-	All Users	-	0	0	0	-	-	-	-

Demonstration

1. Webinar Goal 2. License 3. After Installation 4. Activate license 5. Add Devices 6. Add Users 7. Add Doors 8.Access Group 9. Batch edit 10. Private Auth. 11. Custom Field 12. Device menu 13. Zones

Demonstration of previous Steps
And
Q&A

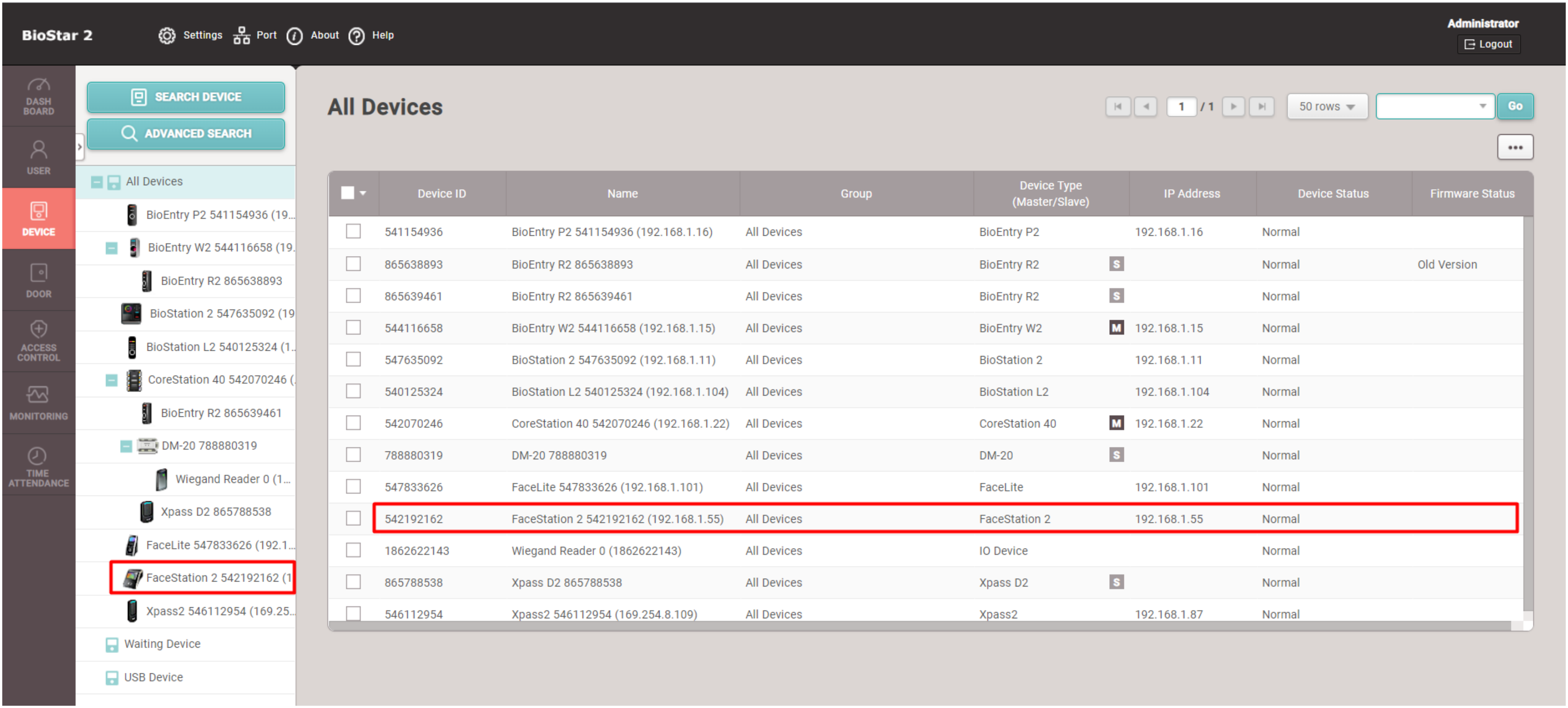
Contents

1. Webinar Goal
2. Understanding BioStar2 Access Control License
3. After BioStar2 installation
4. Activate BioStar2 license (online & offline)
5. Add devices (server mode, device mode, network precautions)
6. Add users (finger enrollment precautions to avoid FAR & FRR)
7. Add doors (with 1 reader (IN) for a door and 2 readers (IN & OUT) for another door)
8. Create Access group & Access level
9. Batch edit for users, devices, & doors
10. Private authentication for users
11. Custom fields for user profiles
12. **Device configuration quick look**
13. Understanding zones configuration

12 – Device configuration quick look

Device Menu

To access the device menu, one click on the device you want to access its configuration within the below red areas:



- All Devices
  - BioEntry P2 541154936 (19...
  - BioEntry W2 544116658 (19...
    - BioEntry R2 865638893
  - BioStation 2 547635092 (19
  - BioStation L2 540125324 (1...
  - CoreStation 40 542070246 (...
    - BioEntry R2 865639461
    - DM-20 788880319
      - Wiegand Reader 0 (1...
    - Xpass D2 865788538
  - FaceLite 547833626 (192.1...
  - FaceStation 2 542192162 (1
  - Xpass2 546112954 (169.25...
- Waiting Device
- USB Device

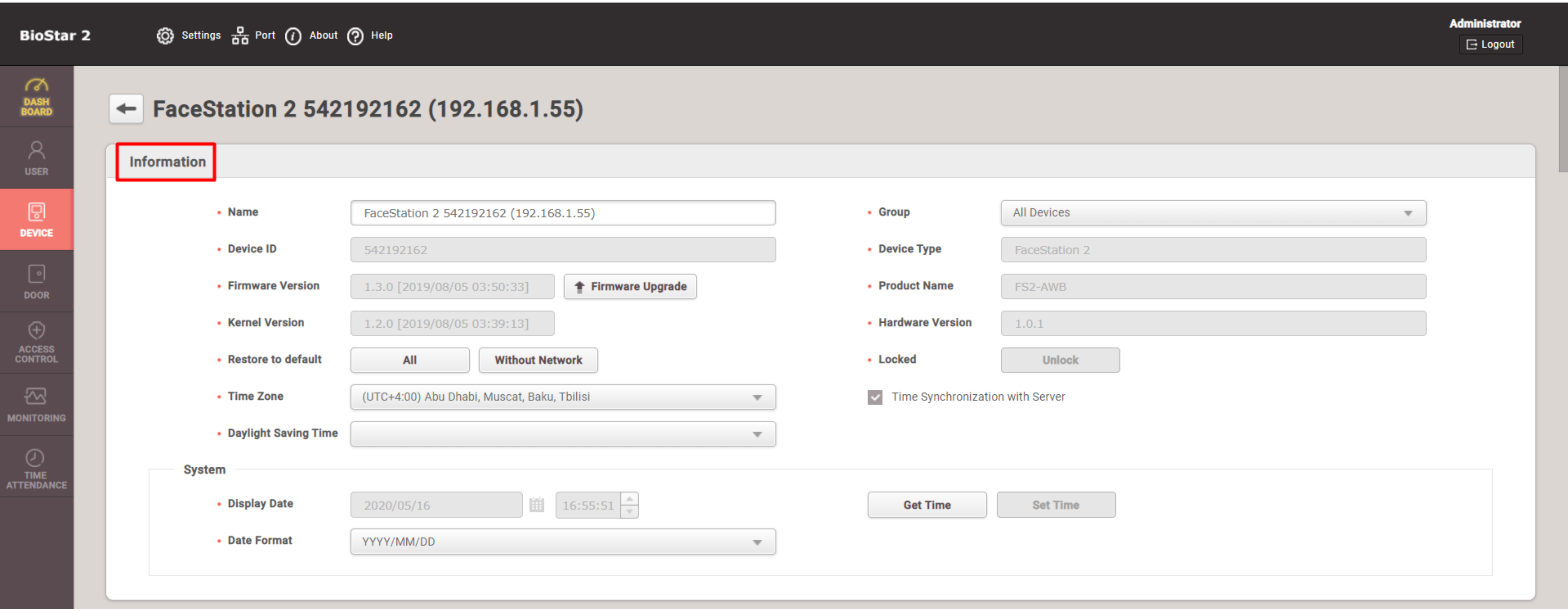
All Devices

□	Device ID	Name	Group	Device Type (Master/Slave)		IP Address	Device Status	Firmware Status
□	541154936	BioEntry P2 541154936 (192.168.1.16)	All Devices	BioEntry P2		192.168.1.16	Normal	
□	865638893	BioEntry R2 865638893	All Devices	BioEntry R2	S		Normal	Old Version
□	865639461	BioEntry R2 865639461	All Devices	BioEntry R2	S		Normal	
□	544116658	BioEntry W2 544116658 (192.168.1.15)	All Devices	BioEntry W2	M	192.168.1.15	Normal	
□	547635092	BioStation 2 547635092 (192.168.1.11)	All Devices	BioStation 2		192.168.1.11	Normal	
□	540125324	BioStation L2 540125324 (192.168.1.104)	All Devices	BioStation L2		192.168.1.104	Normal	
□	542070246	CoreStation 40 542070246 (192.168.1.22)	All Devices	CoreStation 40	M	192.168.1.22	Normal	
□	788880319	DM-20 788880319	All Devices	DM-20	S		Normal	
□	547833626	FaceLite 547833626 (192.168.1.101)	All Devices	FaceLite		192.168.1.101	Normal	
□	542192162	FaceStation 2 542192162 (192.168.1.55)	All Devices	FaceStation 2		192.168.1.55	Normal	
□	1862622143	Wiegand Reader 0 (1862622143)	All Devices	IO Device			Normal	
□	865788538	Xpass D2 865788538	All Devices	Xpass D2	S		Normal	
□	546112954	Xpass2 546112954 (169.254.8.109)	All Devices	Xpass2		192.168.1.87	Normal	

12 – Device configuration quick look

Device Menu (Ex. FaceStation2)

1. Information



FaceStation 2 542192162 (192.168.1.55)

Information

- Name: FaceStation 2 542192162 (192.168.1.55)
- Device ID: 542192162
- Firmware Version: 1.3.0 [2019/08/05 03:50:33]
- Kernel Version: 1.2.0 [2019/08/05 03:39:13]
- Restore to default: All | Without Network
- Time Zone: (UTC+4:00) Abu Dhabi, Muscat, Baku, Tbilisi
- Daylight Saving Time:
- Group: All Devices
- Device Type: FaceStation 2
- Product Name: FS2-AWB
- Hardware Version: 1.0.1
- Locked: Unlock

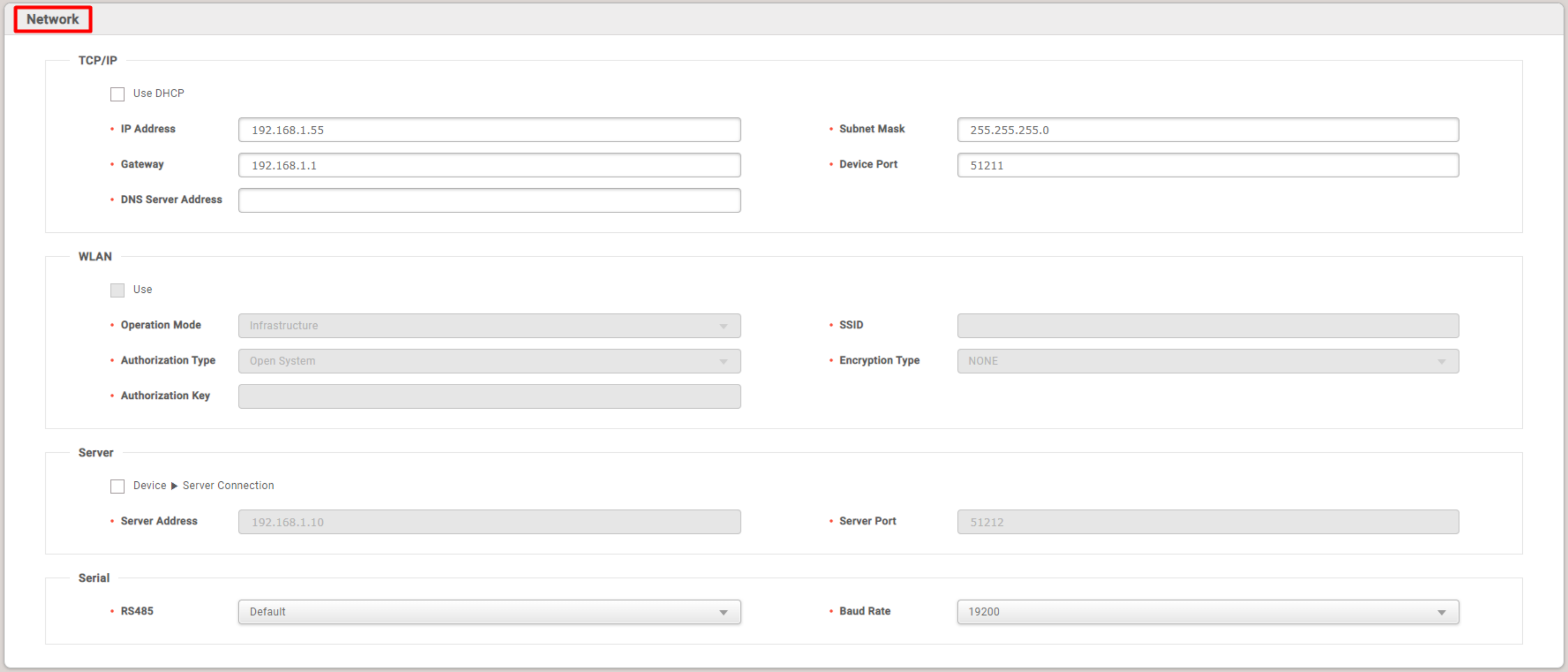
☑ Time Synchronization with Server

System

- Display Date: 2020/05/16 16:55:51
- Date Format: YYYY/MM/DD

Device Menu (Ex. FaceStation2)

2. Network



Network

TCP/IP

□ Use DHCP

• IP Address	192.168.1.55	• Subnet Mask	255.255.255.0
• Gateway	192.168.1.1	• Device Port	51211
• DNS Server Address			

WLAN

□ Use

• Operation Mode	Infrastructure	• SSID	
• Authorization Type	Open System	• Encryption Type	NONE
• Authorization Key			

Server

□ Device ▶ Server Connection

• Server Address	192.168.1.10	• Server Port	51212

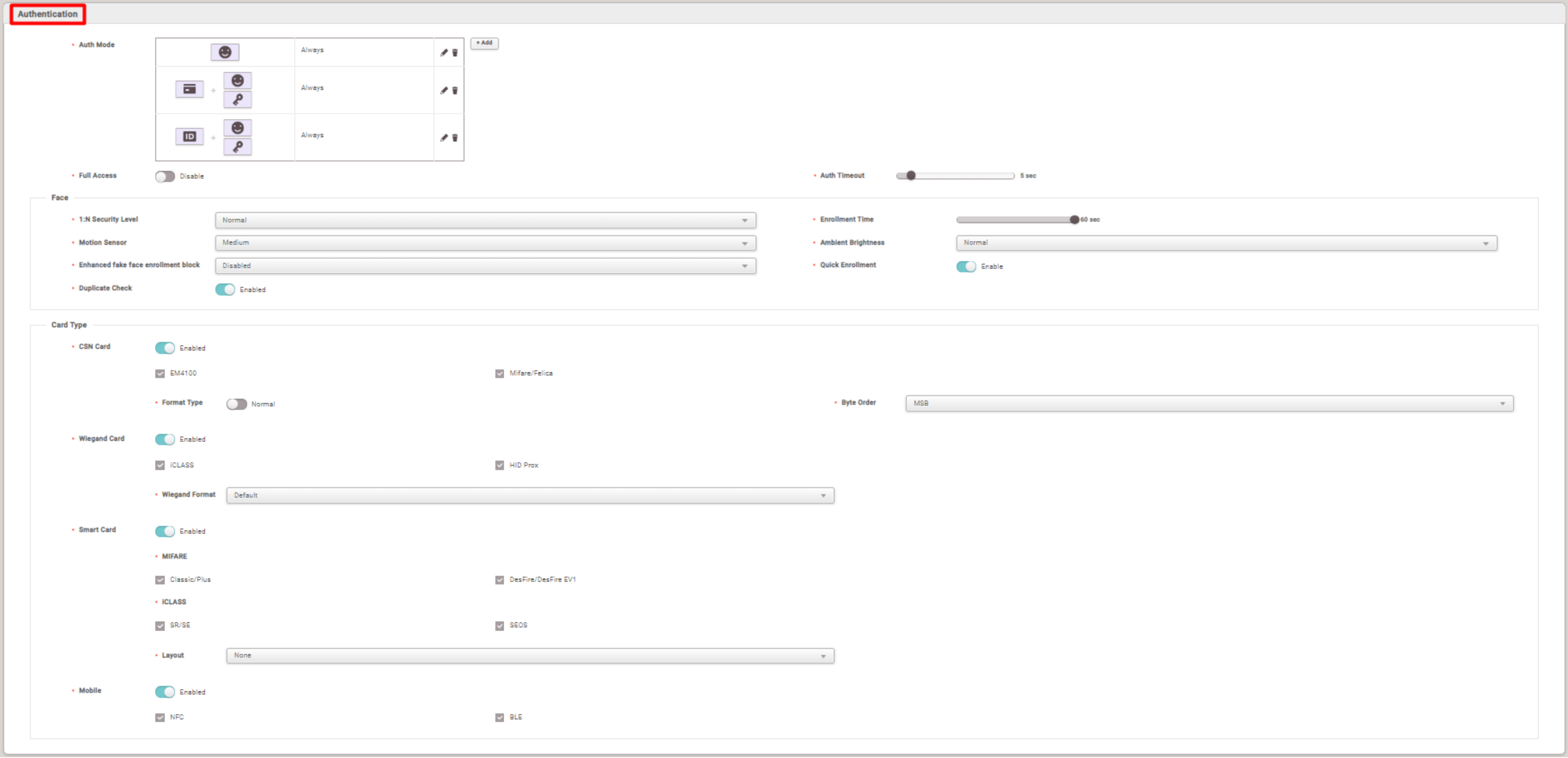
Serial

• RS485	Default	• Baud Rate	19200

12 – Device configuration quick look

Device Menu (Ex. FaceStation2)

3. Authentication



- Auth Mode
  - Always
  - Always
  - Always
- Full Access: Disable
- Auth Timeout: 5 sec

Face

- 1:N Security Level: Normal
- Motion Sensor: Medium
- Enhanced fake face enrollment block: Disabled
- Duplicate Check: Enabled
- Enrollment Time: 60 sec
- Ambient Brightness: Normal
- Quick Enrollment: Enable

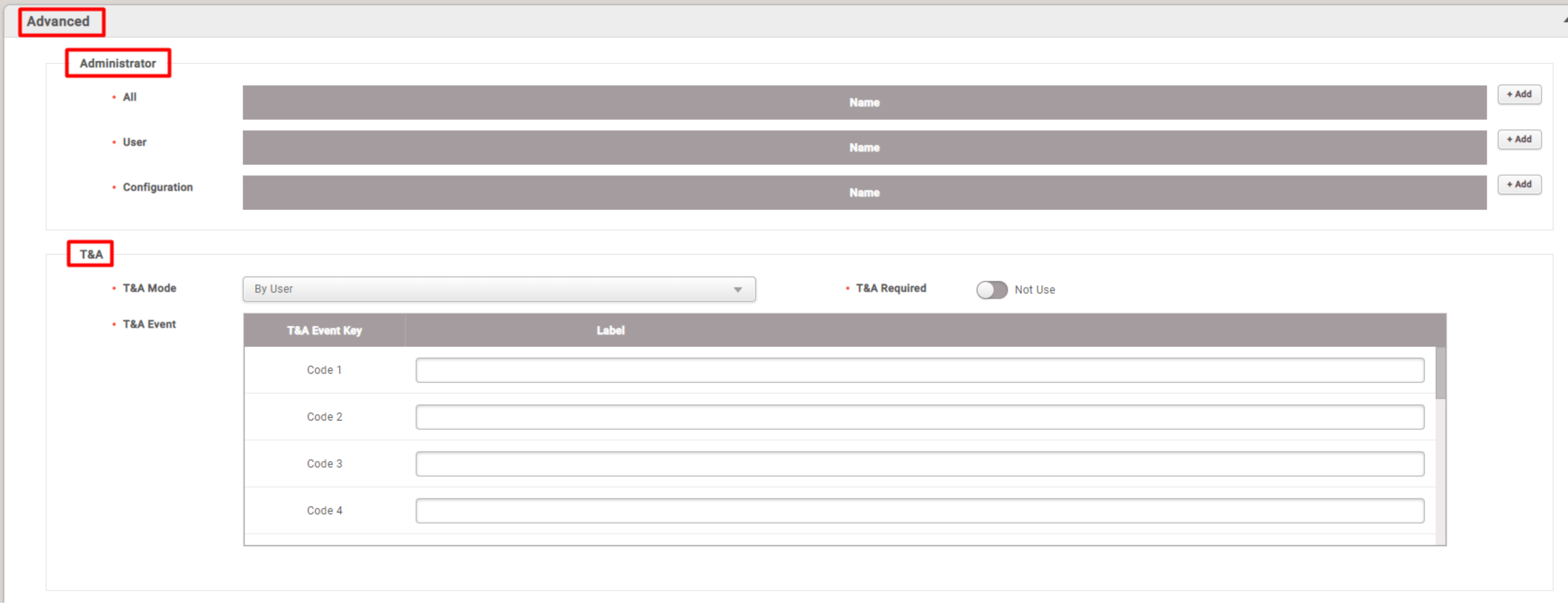
Card Type

- CSN Card: Enabled
  - ☑ EM4100 ☑ Mifare/Felica
  - Format Type: Normal
  - Byte Order: MSB
- Wiegand Card: Enabled
  - ☑ iCLASS ☑ HID Prox
  - Wiegand Format: Default
- Smart Card: Enabled
  - MIFARE
  - ☑ Classic/Plus ☑ DesFire/DesFire EV1
  - ICLASS
  - ☑ SR/SE ☑ SEOS
  - Layout: None
- Mobile: Enabled
  - ☑ NFC ☑ BLE

Device Menu (Ex. FaceStation2)

4. Advanced:

4.1 Administrator
4.2 T&A



Advanced

Administrator

- All — Name — + Add
- User — Name — + Add
- Configuration — Name — + Add

T&A

- T&A Mode: By User
- T&A Required: Not Use
- T&A Event

T&A Event Key	Label
Code 1	
Code 2	
Code 3	
Code 4	

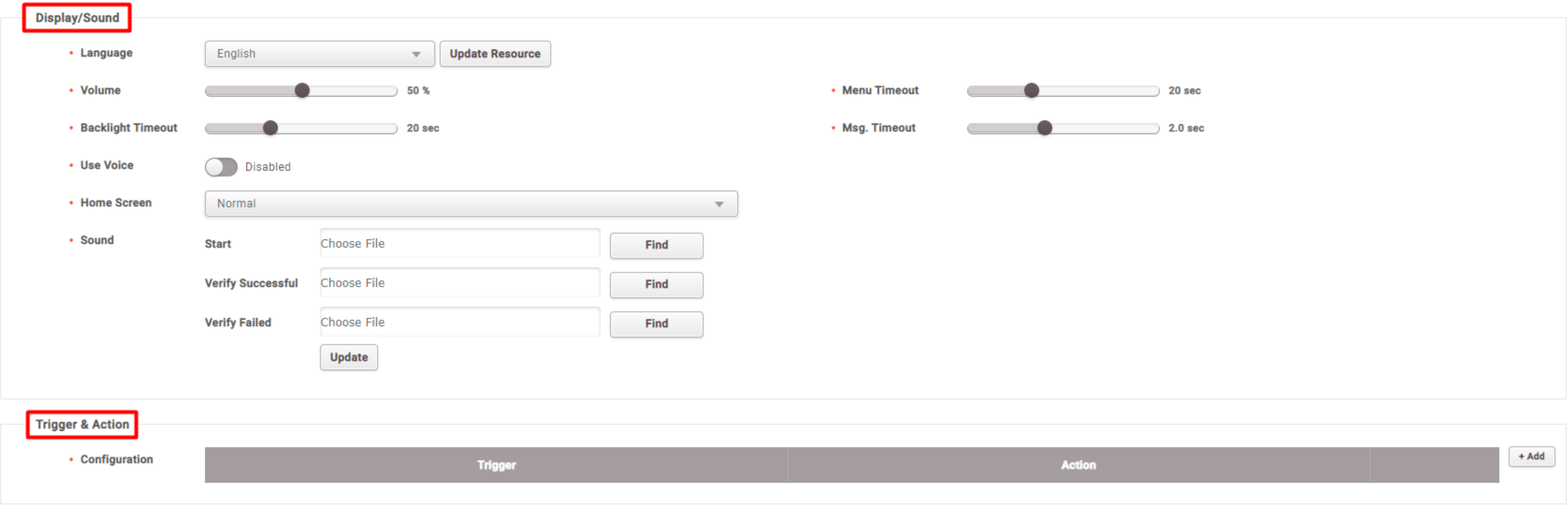
12 – Device configuration quick look

Device Menu (Ex. FaceStation2)

4. Advanced:

4.3 Display/Sound

4.4 Trigger & Action



Display/Sound

- Language: English — Update Resource
- Volume: 50 %
- Menu Timeout: 20 sec
- Backlight Timeout: 20 sec
- Msg. Timeout: 2.0 sec
- Use Voice: Disabled
- Home Screen: Normal
- Sound
  - Start: Choose File — Find
  - Verify Successful: Choose File — Find
  - Verify Failed: Choose File — Find
  - Update

Trigger & Action

- Configuration

Trigger	Action	

+ Add

12 – Device configuration quick look

Device Menu (Ex. FaceStation2)

4. Advanced:

4.5 Image Log
4.6 Wiegand

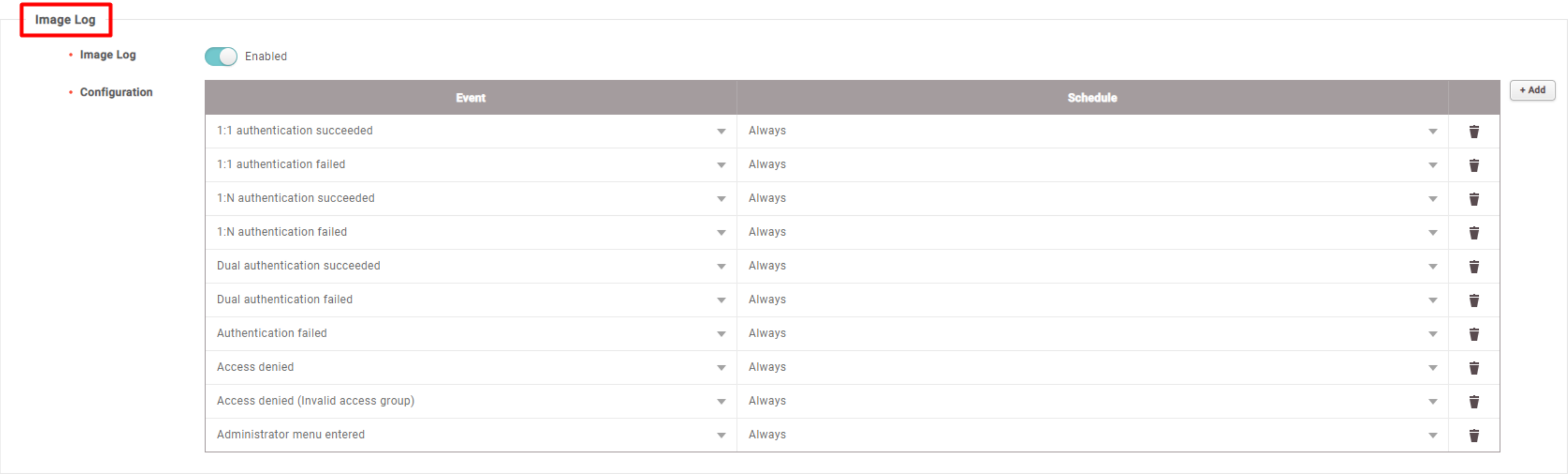
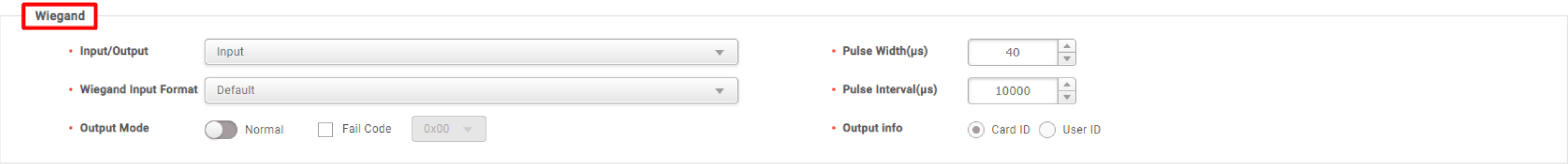


Image Log

- Image Log: Enabled
- Configuration

Event	Schedule
1:1 authentication succeeded	Always
1:1 authentication failed	Always
1:N authentication succeeded	Always
1:N authentication failed	Always
Dual authentication succeeded	Always
Dual authentication failed	Always
Authentication failed	Always
Access denied	Always
Access denied (Invalid access group)	Always
Administrator menu entered	Always



Wiegand

- Input/Output: Input
- Wiegand Input Format: Default
- Output Mode: Normal □ Fail Code 0x00
- Pulse Width(μs): 40
- Pulse Interval(μs): 10000
- Output info: ● Card ID ○ User ID

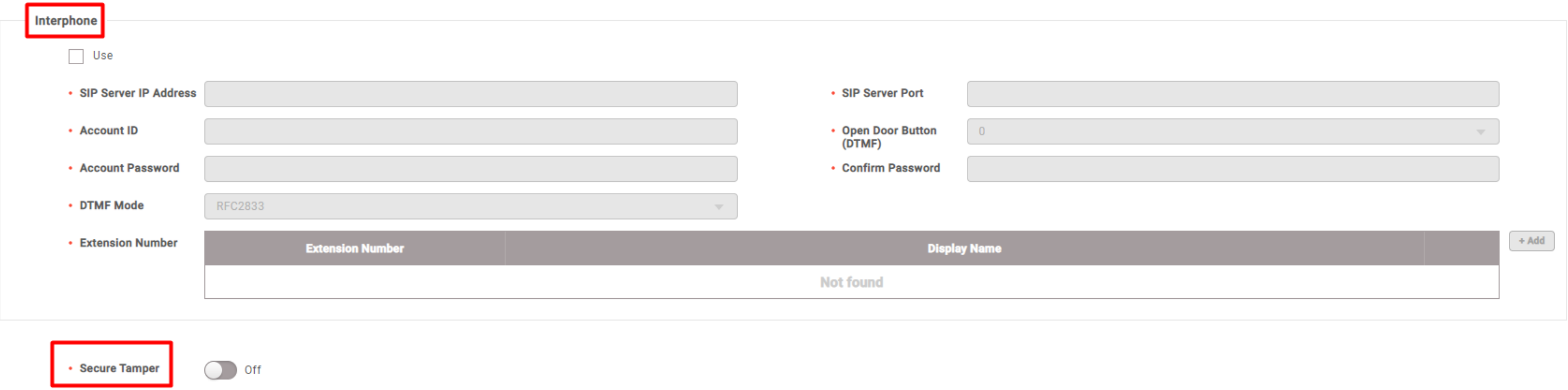
12 – Device configuration quick look

Device Menu (Ex. FaceStation2)

4. Advanced:

4.7 Interphone

4.8 Secure Tamper



Interphone

□ Use

• SIP Server IP Address		• SIP Server Port	
• Account ID		• Open Door Button (DTMF)	0
• Account Password		• Confirm Password	
• DTMF Mode	RFC2833		

• Extension Number

Extension Number	Display Name
Not found	

+ Add

• Secure Tamper Off

Demonstration

Demonstration of previous Steps
And
Q&A

Contents

1. Webinar Goal
2. Understanding BioStar2 Access Control License
3. After BioStar2 installation
4. Activate BioStar2 license (online & offline)
5. Add devices (server mode, device mode, network precautions)
6. Add users (finger enrollment precautions to avoid FAR & FRR)
7. Add doors (with 1 reader (IN) for a door and 2 readers (IN & OUT) for another door)
8. Create Access group & Access level
9. Batch edit for users, devices, & doors
10. Private authentication for users
11. Custom fields for user profiles
12. Device configuration quick look
13. **Understanding zones configuration**

13 – Understanding zones configuration

Zones

Q: Do we require a license to use Zones?

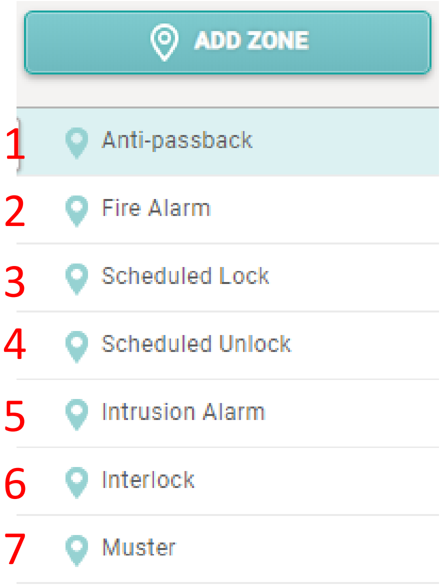
YES

Q: Which version of License should we use?

Standard

What are the zones in BioStar2?

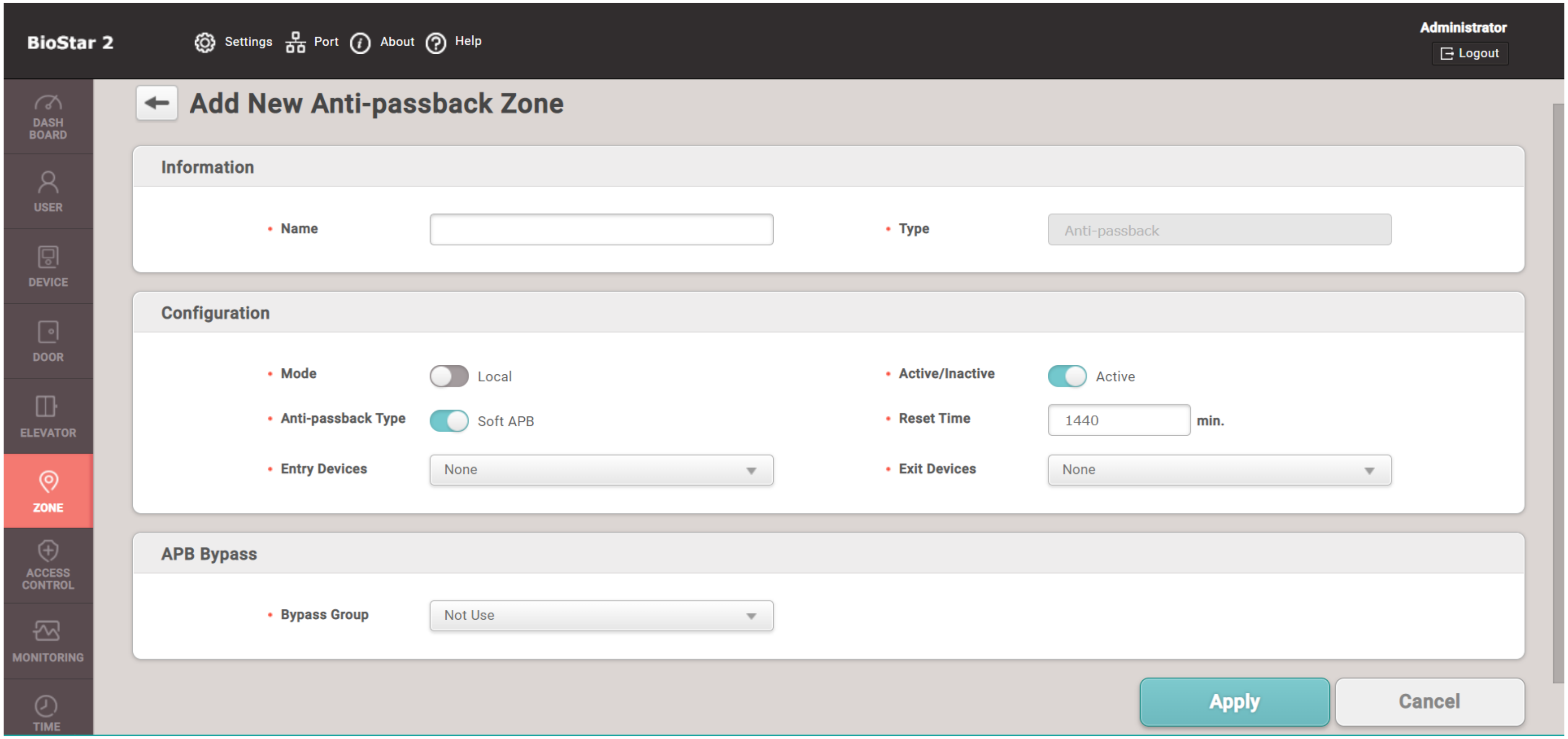
1. Anti-passback
2. Fire Alarm
3. Scheduled Lock
4. Scheduled Unlock
5. Intrusion Alarm
6. Interlock
7. Muster



1. Anti-Passback Zone

Anti-passback can help prevent the users from using an access card to enter and then passing the card over to another user. It can also prevent unauthorized persons who have entered by following users with access privileges from getting out on their own. This feature is available when both an entry device and an exit device are installed.

Configuration steps Link



Add New Anti-passback Zone

Information

- Name
- Type: Anti-passback

Configuration

- Mode: Local
- Active/Inactive: Active
- Anti-passback Type: Soft APB
- Reset Time: 1440 min.
- Entry Devices: None
- Exit Devices: None

APB Bypass

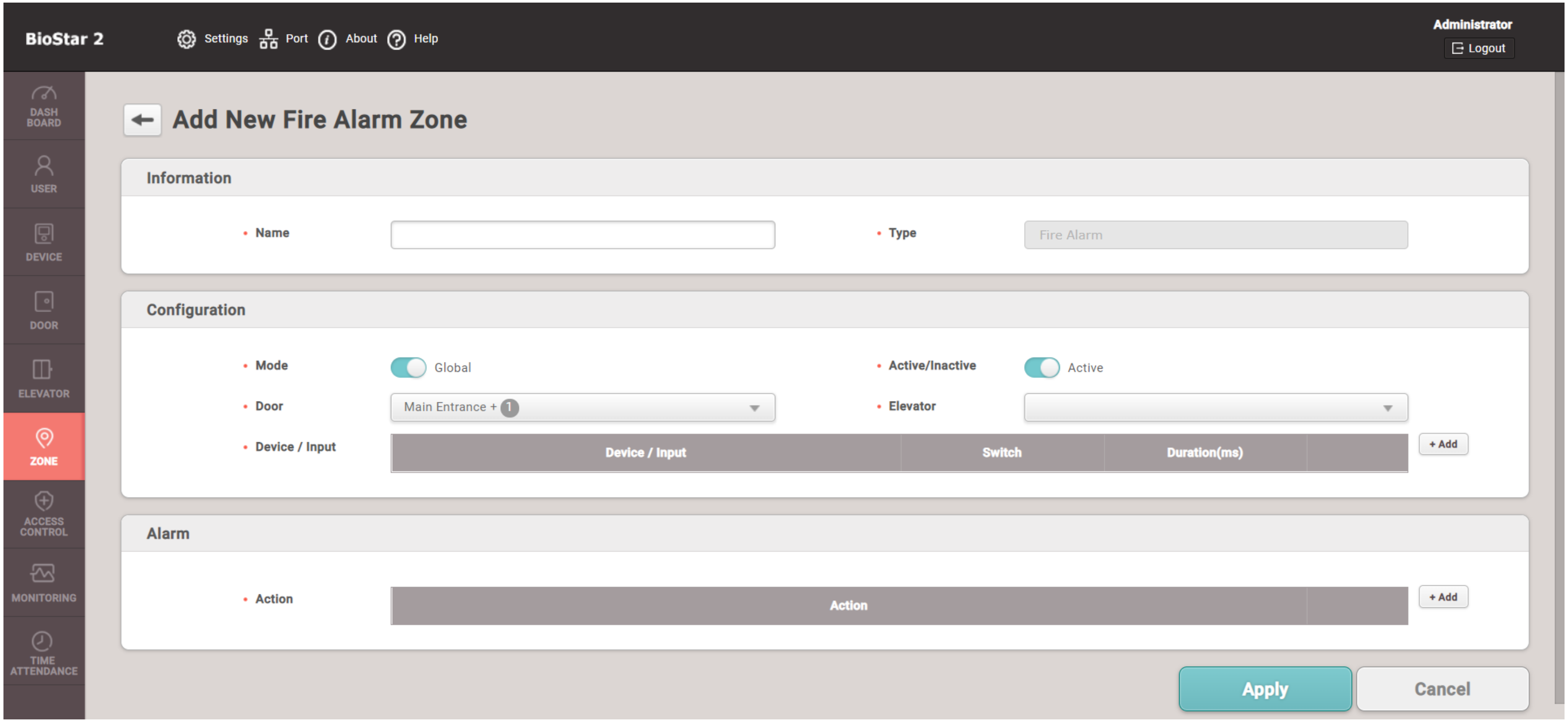
- Bypass Group: Not Use

Apply Cancel

2. Fire Alarm Zone

A zone set to open all the doors and/or elevators configured within this zone in the event of a fire trigger received.

Configuration steps Link



Add New Fire Alarm Zone

Information

- Name
- Type: Fire Alarm

Configuration

- Mode: Global
- Active/Inactive: Active
- Door: Main Entrance + 1
- Elevator
- Device / Input

Device / Input	Switch	Duration(ms)

+ Add

Alarm

- Action

Action

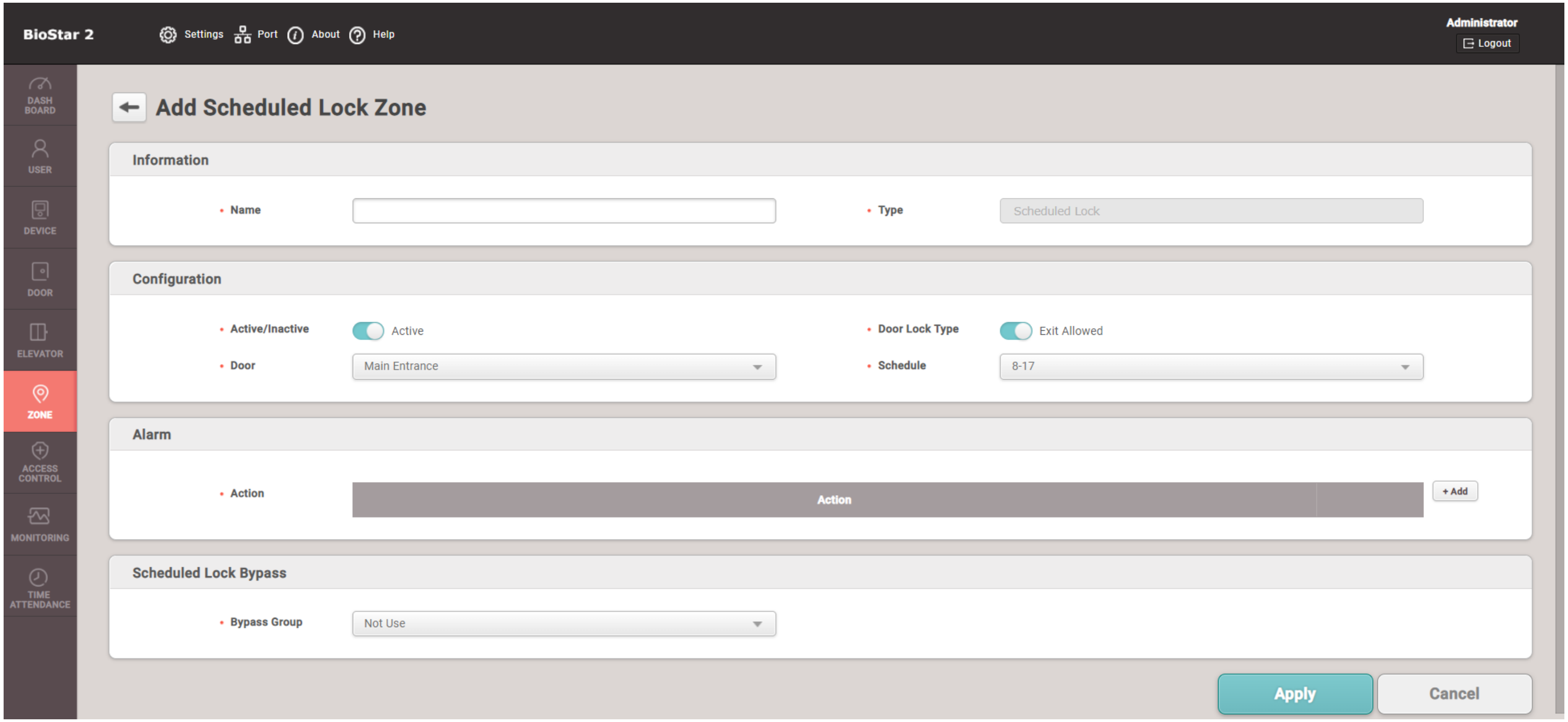
+ Add

Apply Cancel

3. Scheduled Lock Zone

A function that locks the door configured in this zone according to a schedule.

Configuration steps Link



Add Scheduled Lock Zone

Information

- Name:
- Type: Scheduled Lock

Configuration

- Active/Inactive: Active
- Door Lock Type: Exit Allowed
- Door: Main Entrance
- Schedule: 8-17

Alarm

- Action: Action

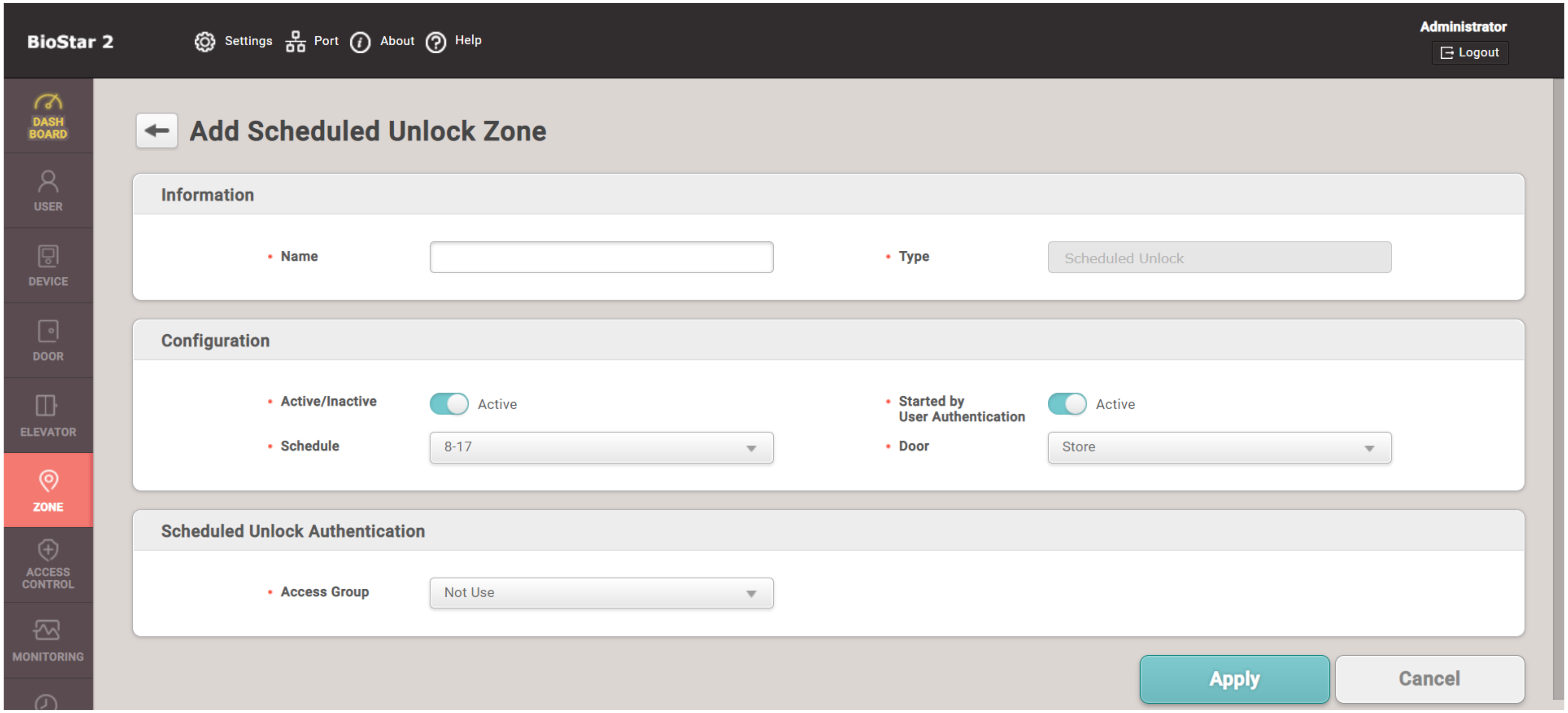
Scheduled Lock Bypass

- Bypass Group: Not Use

4. Scheduled Unlock Zone

A function that unlocks the door configured in this zone according to a schedule.

Configuration steps Link



Add Scheduled Unlock Zone

Information

- Name:
- Type: Scheduled Unlock

Configuration

- Active/Inactive: Active
- Started by User Authentication: Active
- Schedule: 8-17
- Door: Store

Scheduled Unlock Authentication

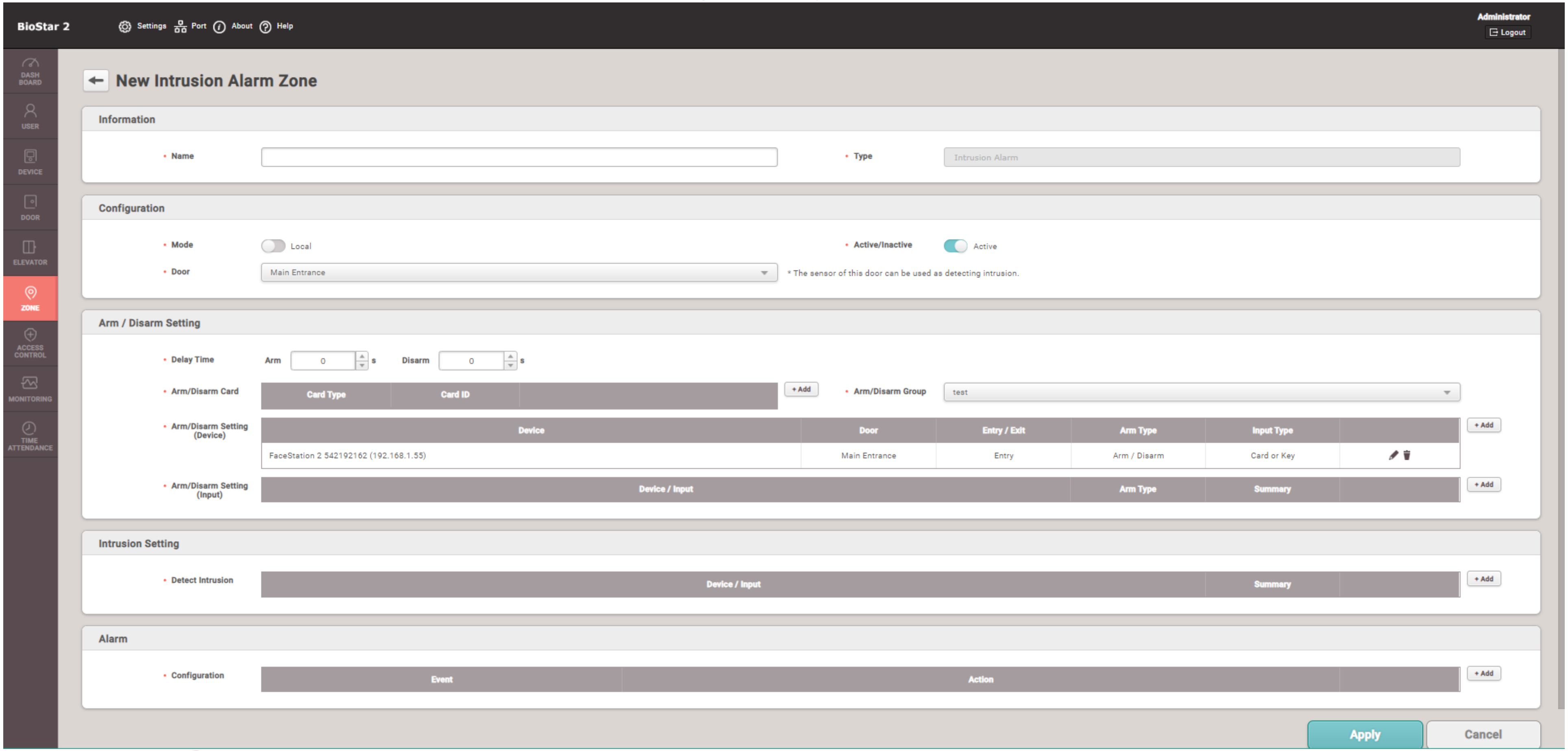
- Access Group: Not Use

Apply | Cancel

5. Intrusion Alarm Zone

A zone set to emit a warning sound or relay signal if an unauthorized person attempts an intrusion after Arm.

Configuration steps Link



New Intrusion Alarm Zone

Information

- Name:
- Type: Intrusion Alarm

Configuration

- Mode: Local
- Active/Inactive: Active
- Door: Main Entrance
- * The sensor of this door can be used as detecting intrusion.

Arm / Disarm Setting

- Delay Time: Arm 0 s Disarm 0 s
- Arm/Disarm Card

Card Type	Card ID

- Arm/Disarm Group: test
- Arm/Disarm Setting (Device)

Device	Door	Entry / Exit	Arm Type	Input Type
FaceStation 2 542192162 (192.168.1.55)	Main Entrance	Entry	Arm / Disarm	Card or Key

- Arm/Disarm Setting (Input)

Device / Input	Arm Type	Summary

Intrusion Setting

- Detect Intrusion

Device / Input	Summary

Alarm

- Configuration

Event	Action

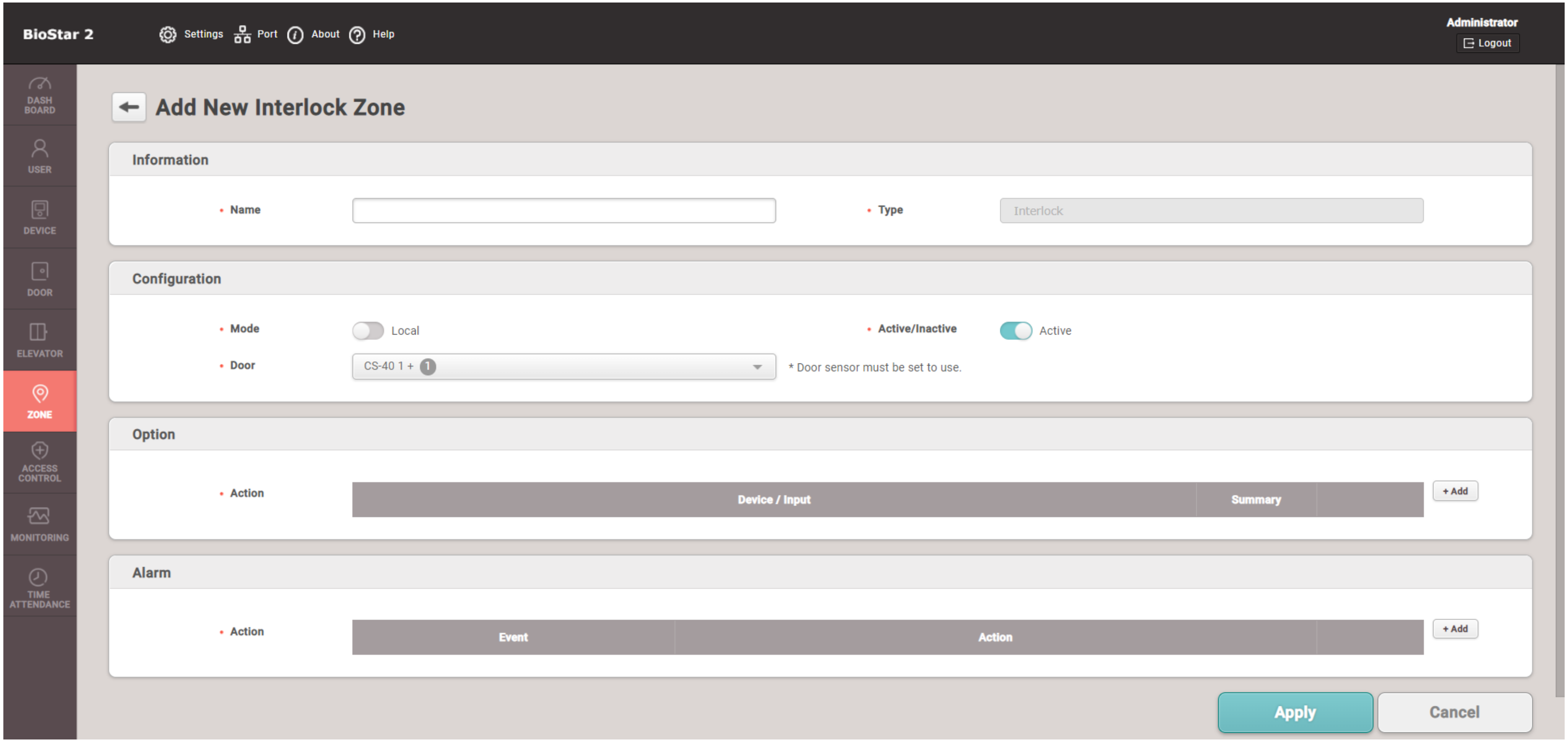
6. Interlock Zone

A zone between **two or three or even four** doors.
In this zone, if one door is open or has been unlocked, the rest of the doors will be locked.

Configuration steps Link

Precaution

Only with **CoreStation**



Add New Interlock Zone

Information

- Name
- Type: Interlock

Configuration

- Mode: Local
- Active/Inactive: Active
- Door: CS-40 1 + 1

* Door sensor must be set to use.

Option

- Action

Device / Input	Summary	

+ Add

Alarm

- Action

Event	Action	

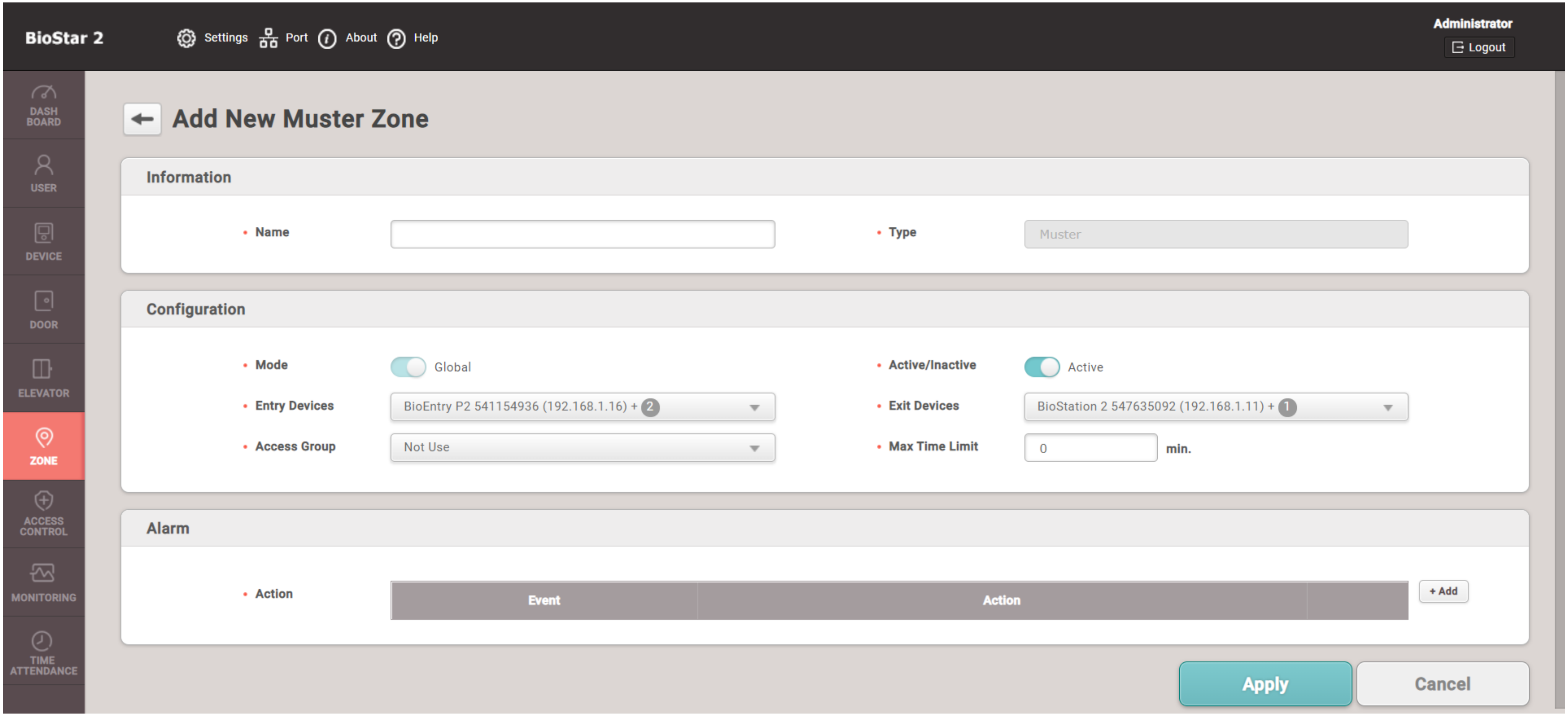
+ Add

Apply Cancel

7. Muster Zone

The muster zone is used as a place where users gather when an emergency occurs. It can also be used for the purpose of monitoring the number of users and list of users in a specific area, or for notifying the manager of alarms and alerts when a user stays in a specific area for a long time.

Configuration steps Link


Add New Muster Zone

Information

- Name:
- Type: Muster

Configuration

- Mode: Global
- Active/Inactive: Active
- Entry Devices: BioEntry P2 541154936 (192.168.1.16) + 2
- Exit Devices: BioStation 2 547635092 (192.168.1.11) + 1
- Access Group: Not Use
- Max Time Limit: 0 min.

Alarm

- Action

Event	Action

Demonstration of previous Steps
And
Q&A

Poll (your Opinion Maters) and Questions & Answers

suprema
SECURITY & BIOMETRICS

20 Years of Innovation

Thank you

suprema
SECURITY & BIOMETRICS

20 Years of Innovation