BioStar 2

v2.5 New Feature

Kate Yu

Contents

Introduction

FAQ

DISCLAIMER

This presentation contains information that is confidential and proprietary to Suprema Inc. and is solely for the use of Suprema Inc. personnel. No part of it may be used, circulated, quoted, or reproduced for distribution outside Suprema Inc. If you are not the intended recipient of this report, you are hereby notified that the use, circulation, quoting, or reproducing of this report is strictly prohibited and may be unlawful. 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.

Introduction

1.Excluded Features

1. Oracle DBMS & Internet explorer

2.Improved Features

1. Better default security : Admin password setting & HTTPS Default
2. Login credential
3. Automatic sync to devices for reconnected device
4. Adding available alert event & trigger event : Network disconnection
5. Adding slave device as fingerprint enrollment device
6. Monitoring menu changes

3.New feature

1. FW update alert message
2. New devices : CoreStation, BioEntry R2, and BioEntry P2
3. New functions: Alarm Zone, Audit Trail, and Video
4. Mobile card widget function

1.Excluded Features

Excluded system requirement

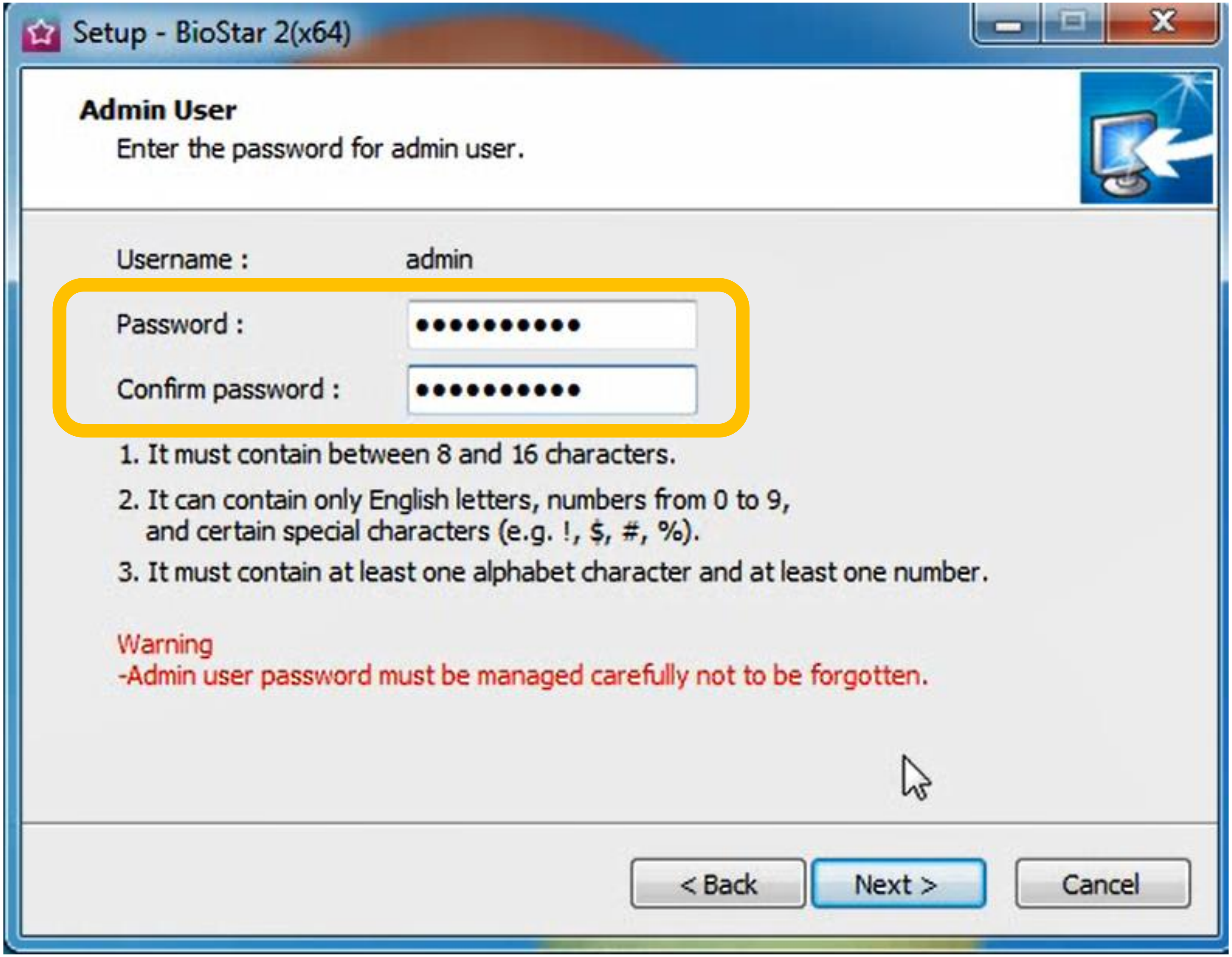
- Oracle DBMS
- Internet Explorer

	v2.4.1	v2.5
DBMS	MariaDB Microsoft SQL Server 2012 ORACLE DATABASE	MariaDB Microsoft SQL Server 2012
Web Browser	chrome Internet Explorer	chrome

2. Improved features

Better Default Security

- Default admin password has to be configured on install



Admin User

Enter the password for admin user.

Username : admin

Password : ●●●●●●●●●●●

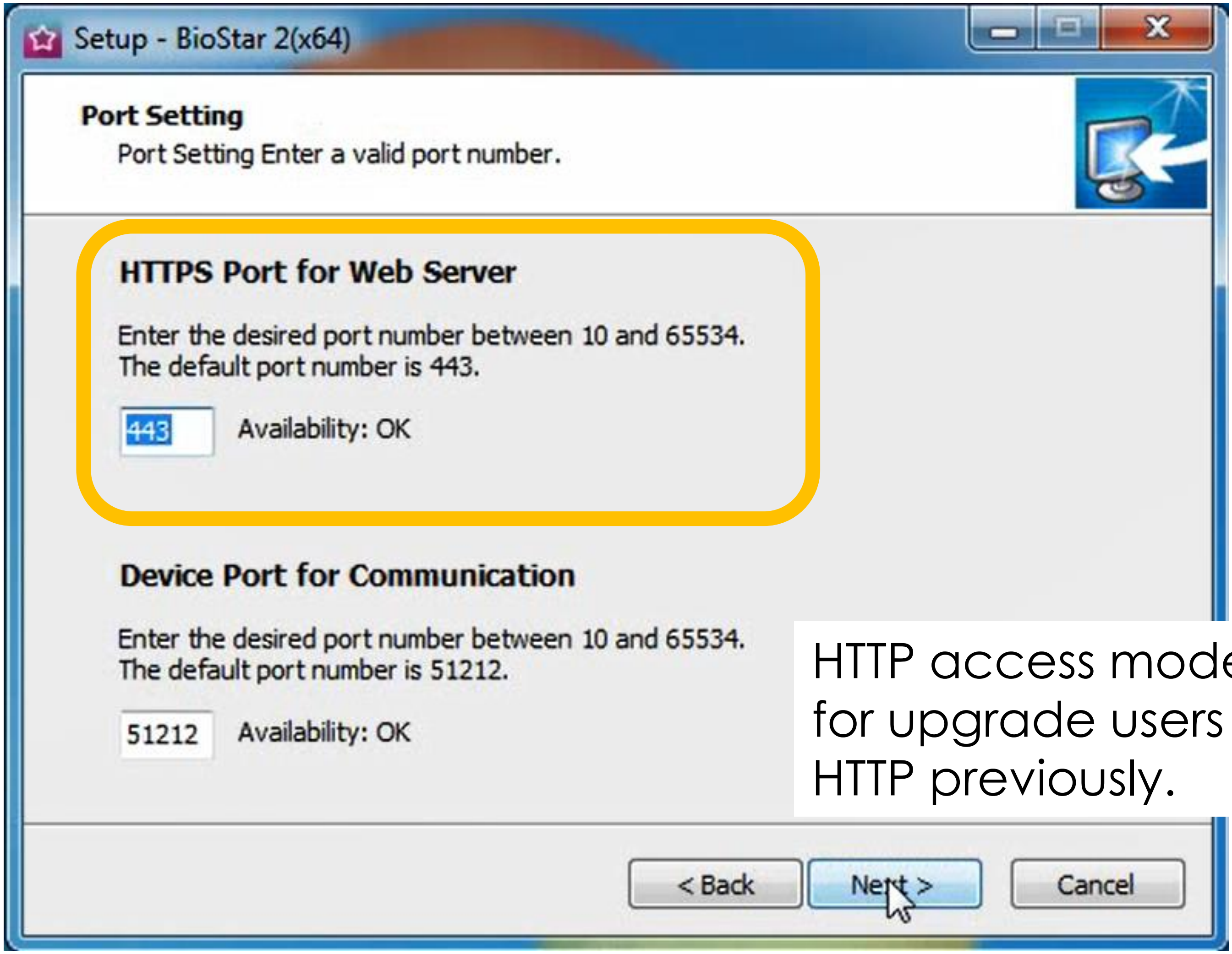
Confirm password : ●●●●●●●●●●●

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

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

Better Default Security

- HTTPS setting by default
- HTTP is still configurable after installation



Port Setting

Port Setting Enter a valid port number.

HTTPS Port for Web Server

Enter the desired port number between 10 and 65534.
The default port number is 443.

443 Availability: OK

Device Port for Communication

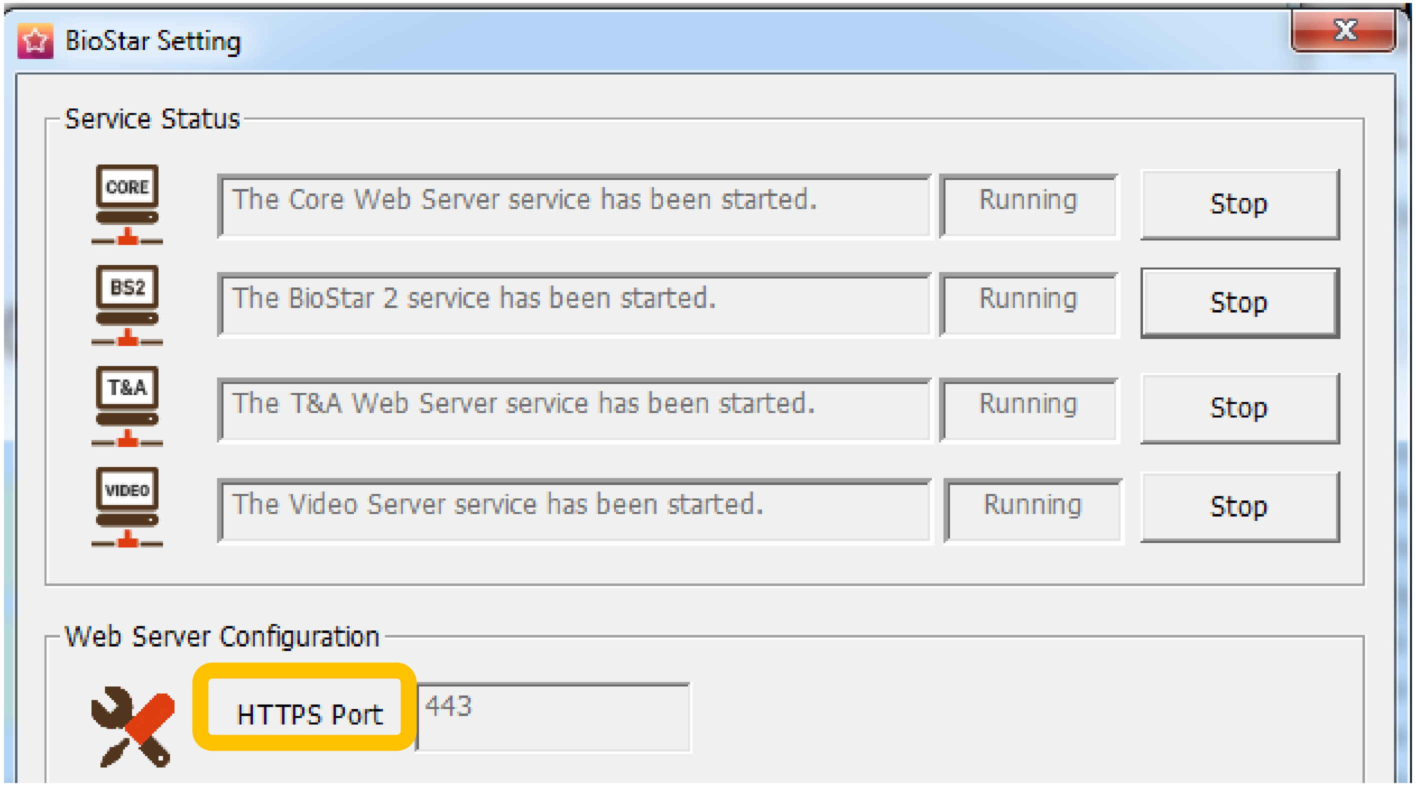
Enter the desired port number between 10 and 65534.
The default port number is 51212.

51212 Availability: OK

HTTP access mode will be maintained for upgrade users who have been using HTTP previously.

Better Default Security

- HTTPS port will be configured on BioStar Setting after BioStar2 v2.5 installation



BioStar Setting

Service Status

The Core Web Server service has been started. Running

The BioStar 2 service has been started. Running

The T&A Web Server service has been started. Running

The Video Server service has been started. Running

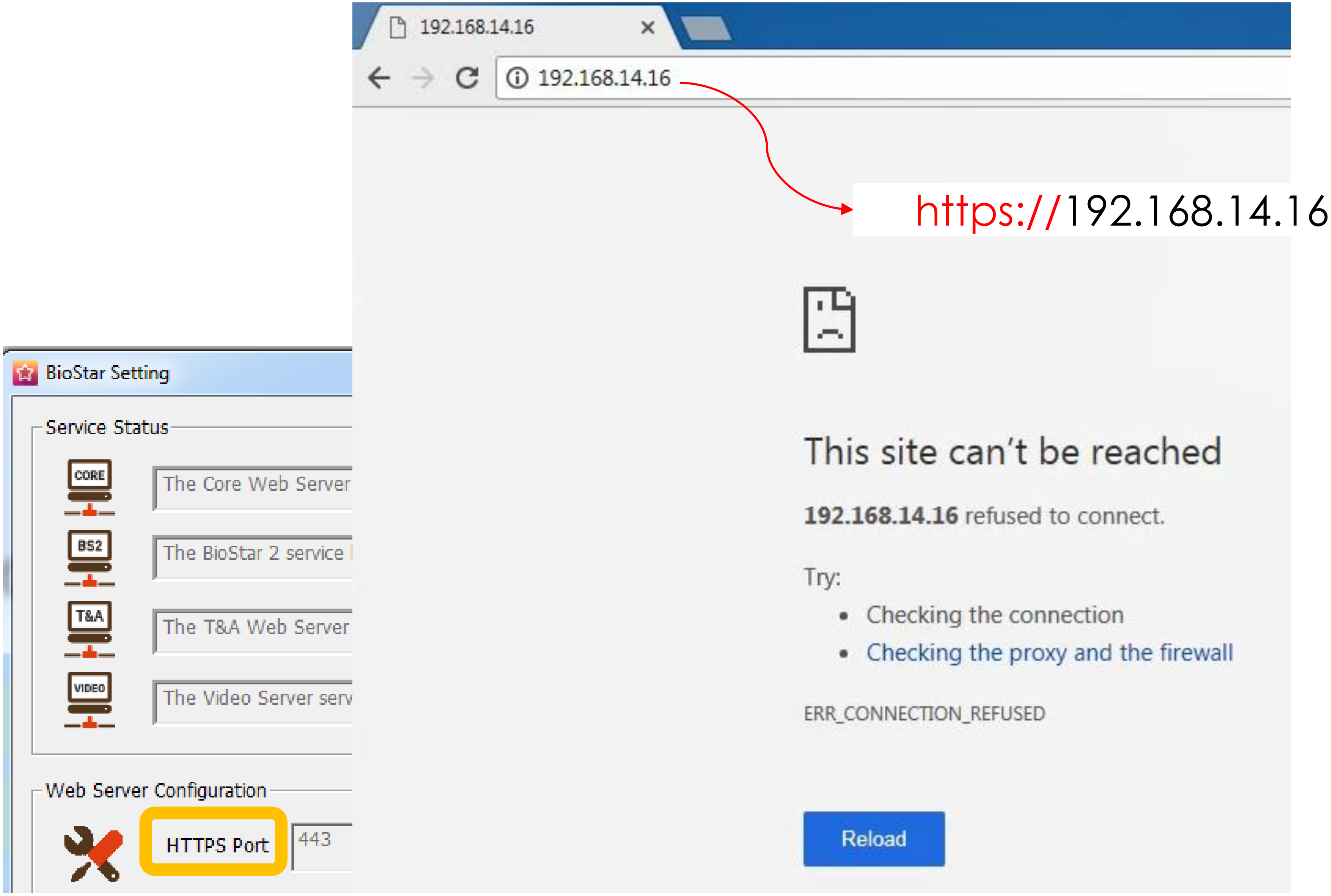
Web Server Configuration

HTTPS Port 443

! Default HTTPS port : 443
Default HTTP port: 80
Above ports can be changed by Biostar Setting

Better Default Security

- Need to enter **https://** at first time



https://192.168.14.16

This site can’t be reached

192.168.14.16 refused to connect.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_REFUSED

BioStar Setting

Service Status

The Core Web Server

The BioStar 2 service

The T&A Web Server

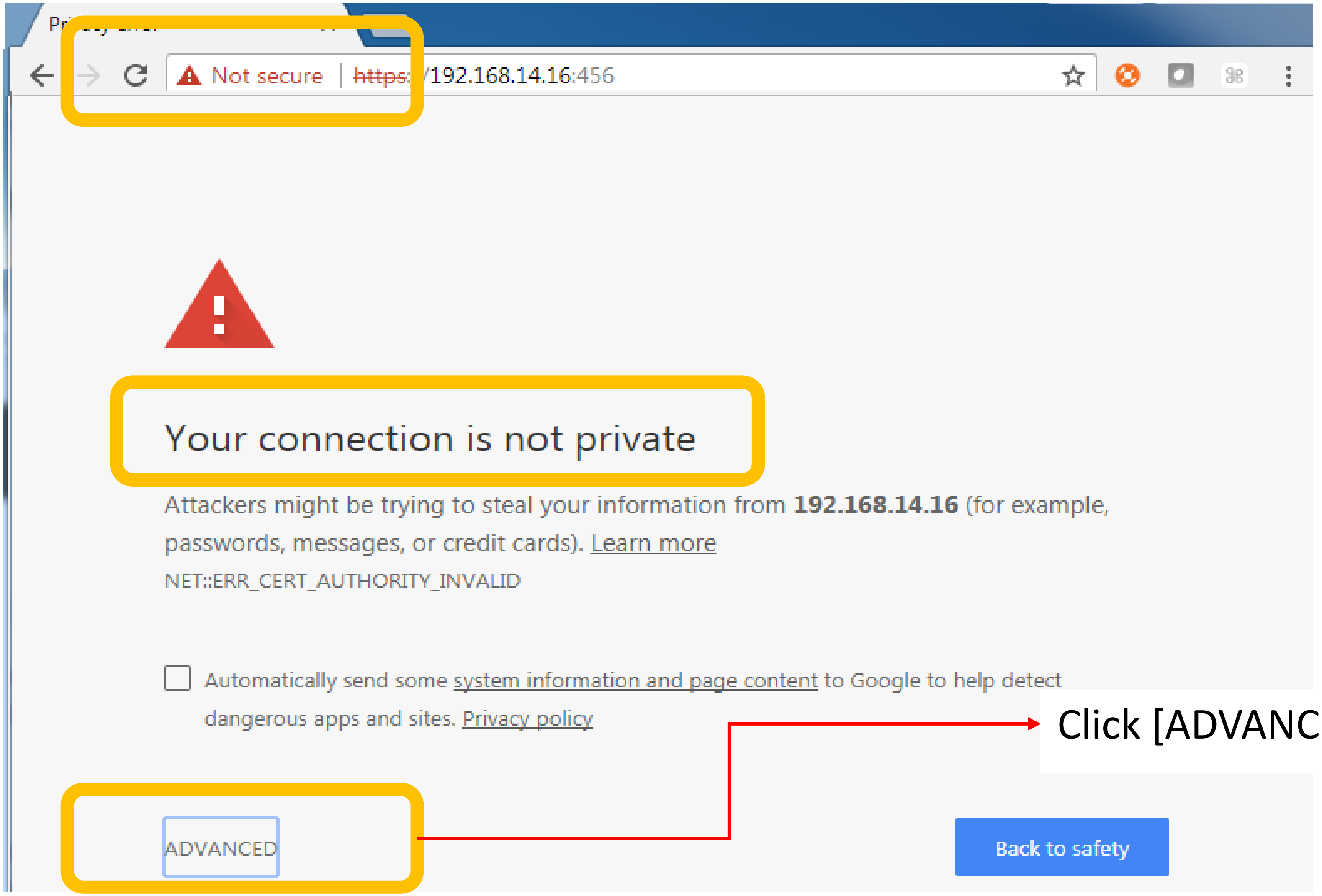
The Video Server serv

Web Server Configuration

HTTPS Port: 443

Better Default Security

- Initial page will appear as not secure
- Need to download certification



Your connection is not private

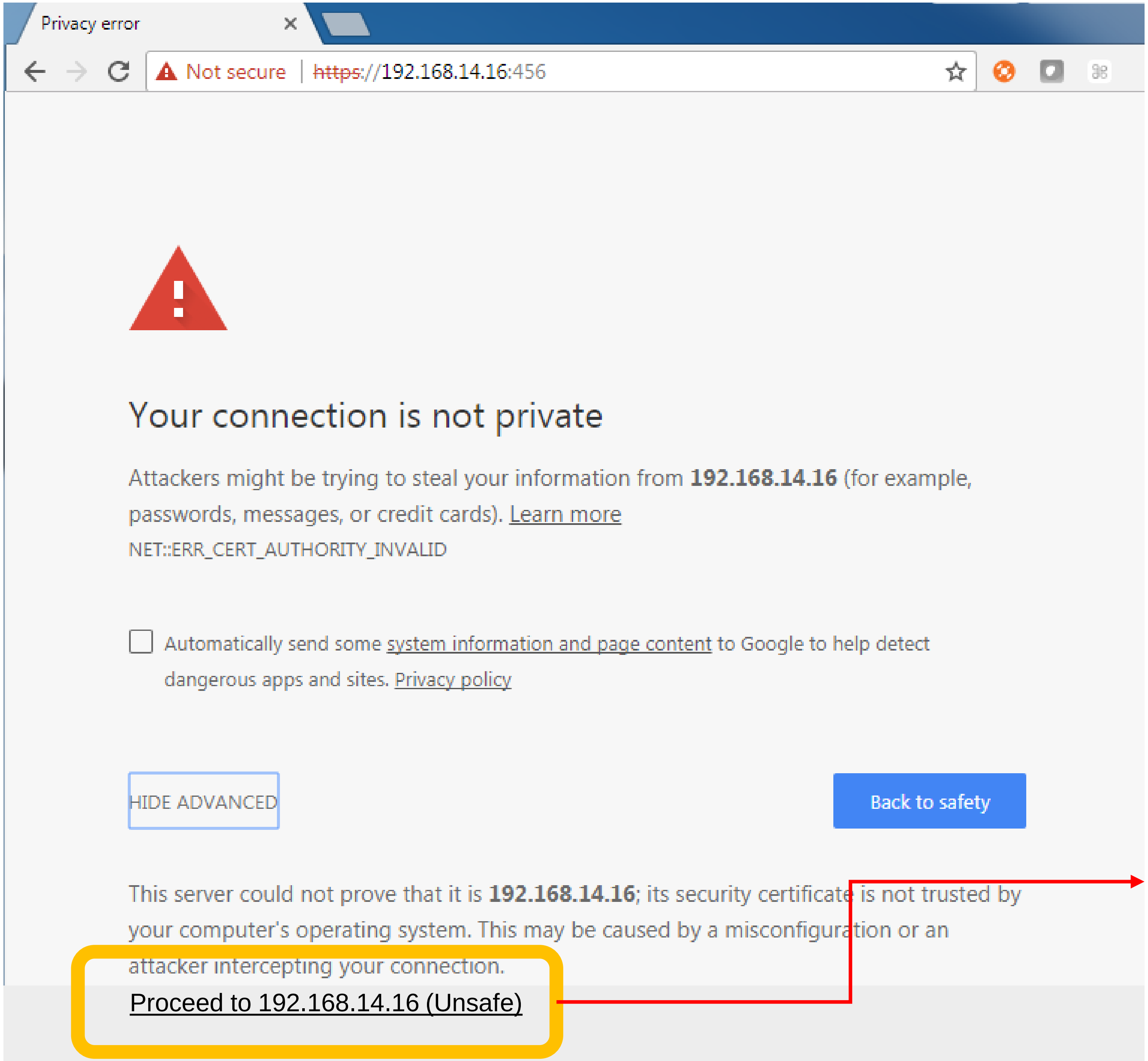
Attackers might be trying to steal your information from **192.168.14.16** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

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

Click [ADVANCED]

Better Default Security



Your connection is not private

Attackers might be trying to steal your information from **192.168.14.16** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

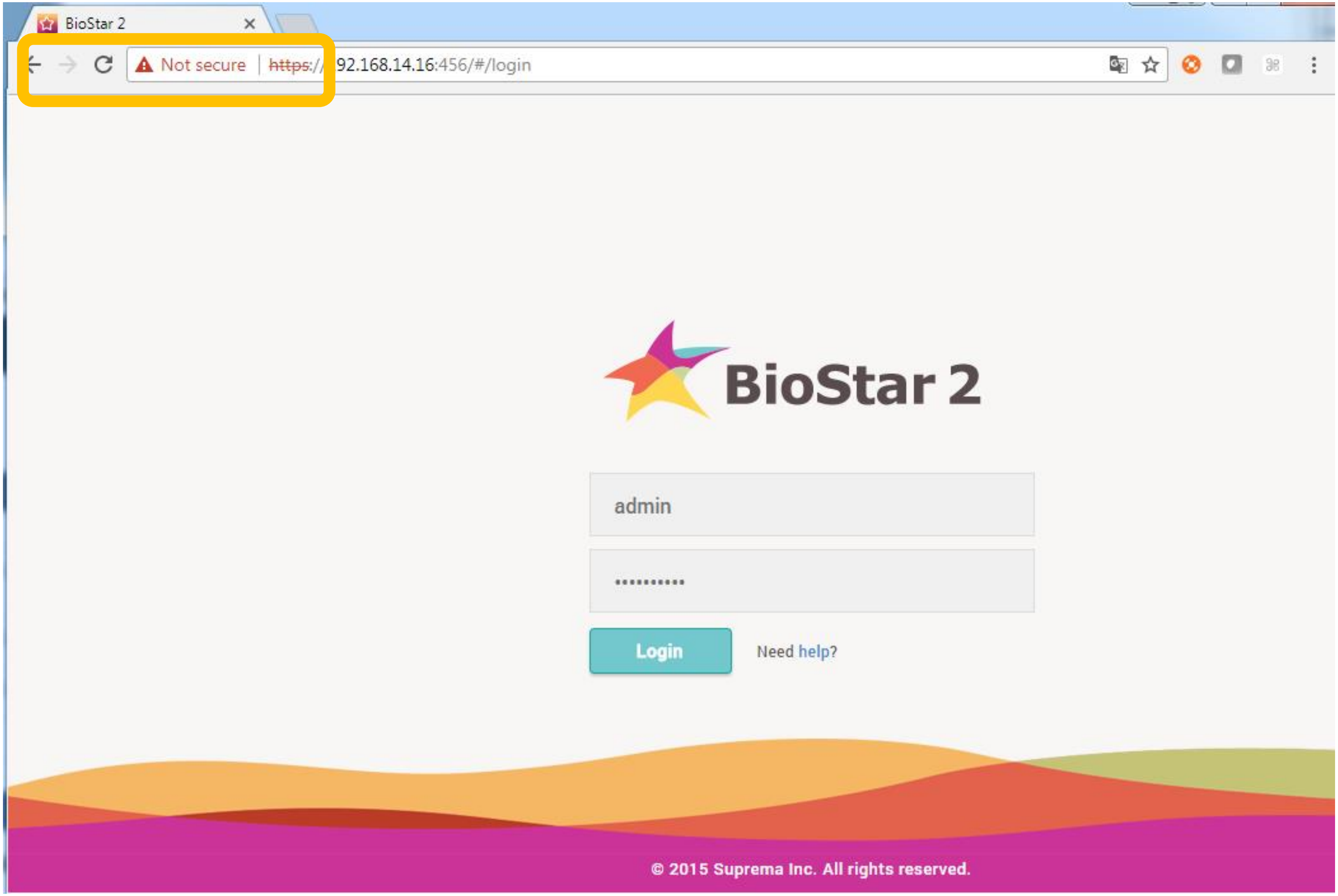
□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

This server could not prove that it is **192.168.14.16**; 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.

Proceed to 192.168.14.16 (Unsafe)

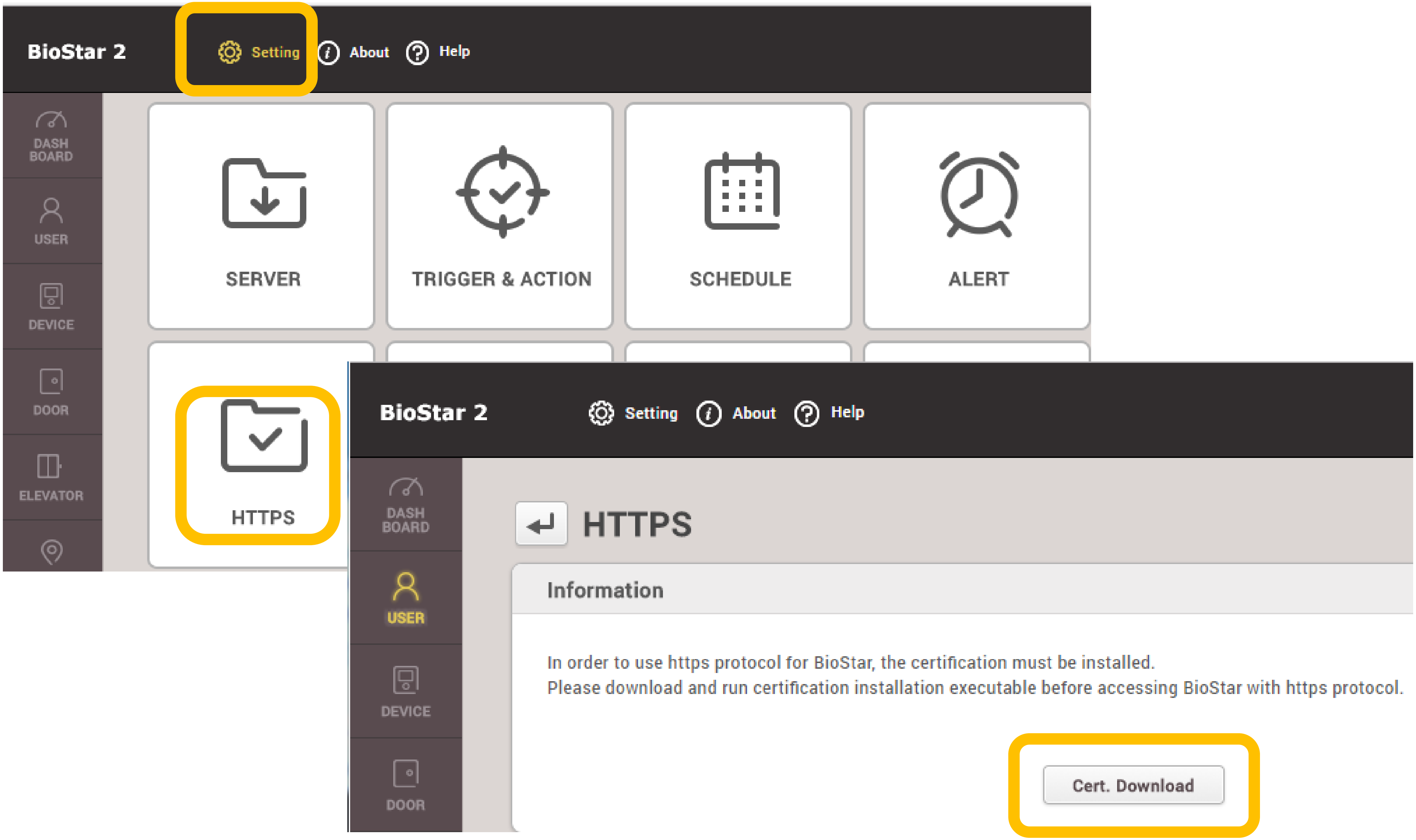
Click [Proceed..] to connect Biostar2 client

Better Default Security



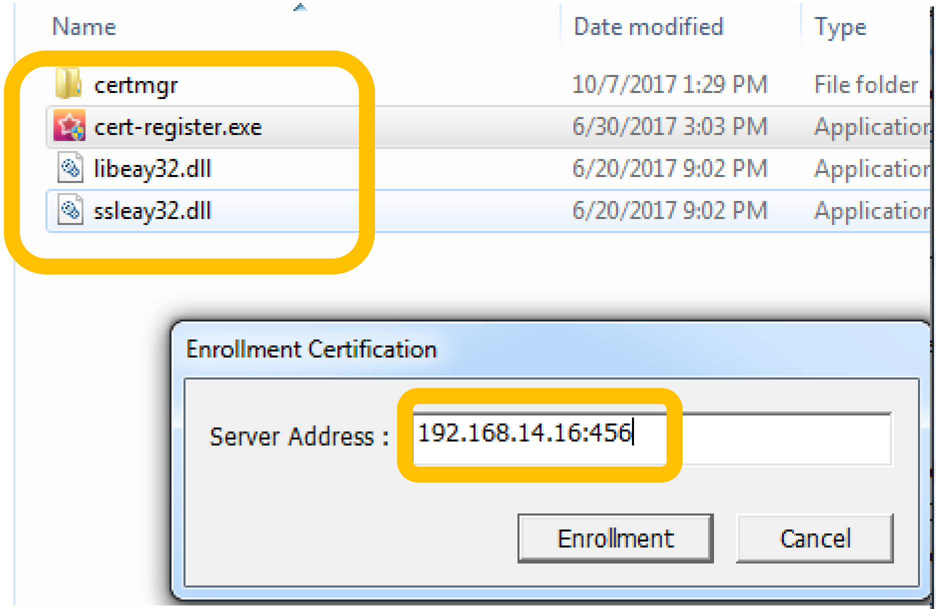
BioStar 2
Not secure
~~https~~://92.168.14.16:456/#/login
BioStar 2
admin
••••••••••••
Login
Need help?
© 2015 Suprema Inc. All rights reserved.

Better Default Security



In order to use https protocol for BioStar, the certification must be installed.
Please download and run certification installation executable before accessing BioStar with https protocol.

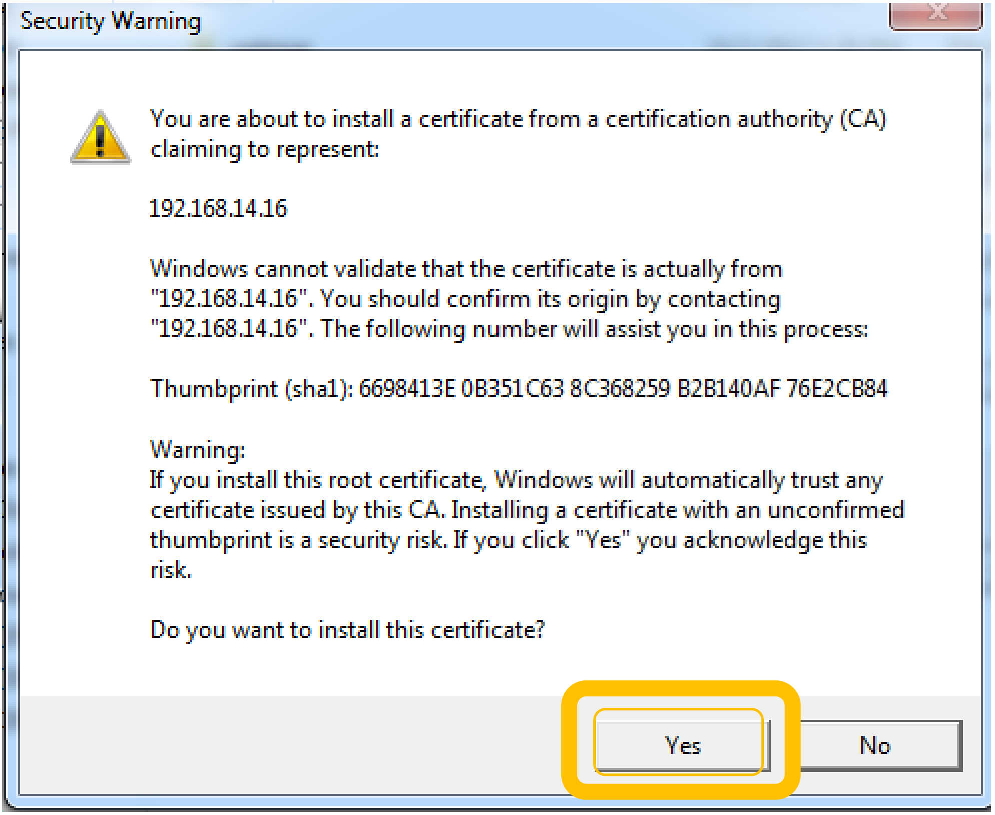
Better Default Security



Name	Date modified	Type
certmgr	10/7/2017 1:29 PM	File folder
cert-register.exe	6/30/2017 3:03 PM	Applicatior
libeay32.dll	6/20/2017 9:02 PM	Applicatior
ssleay32.dll	6/20/2017 9:02 PM	Applicatior

Enrollment Certification

Server Address : 192.168.14.16:456



Security Warning

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

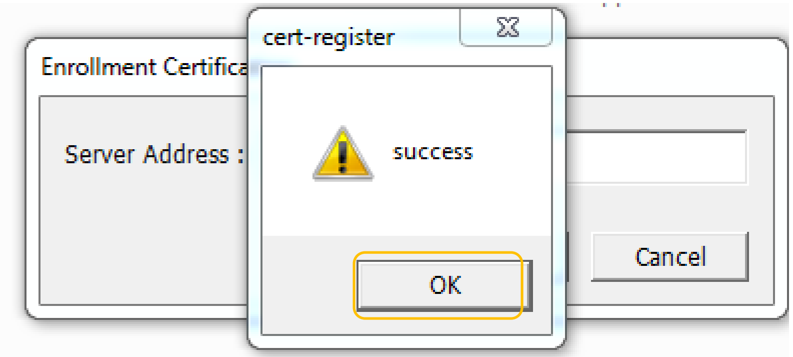
192.168.14.16

Windows cannot validate that the certificate is actually from "192.168.14.16". You should confirm its origin by contacting "192.168.14.16". The following number will assist you in this process:

Thumbprint (sha1): 6698413E 0B351C63 8C368259 B2B140AF 76E2CB84

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?



Enrollment Certifica

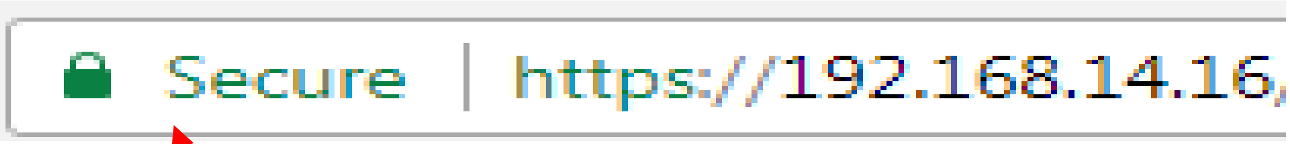
Server Address :

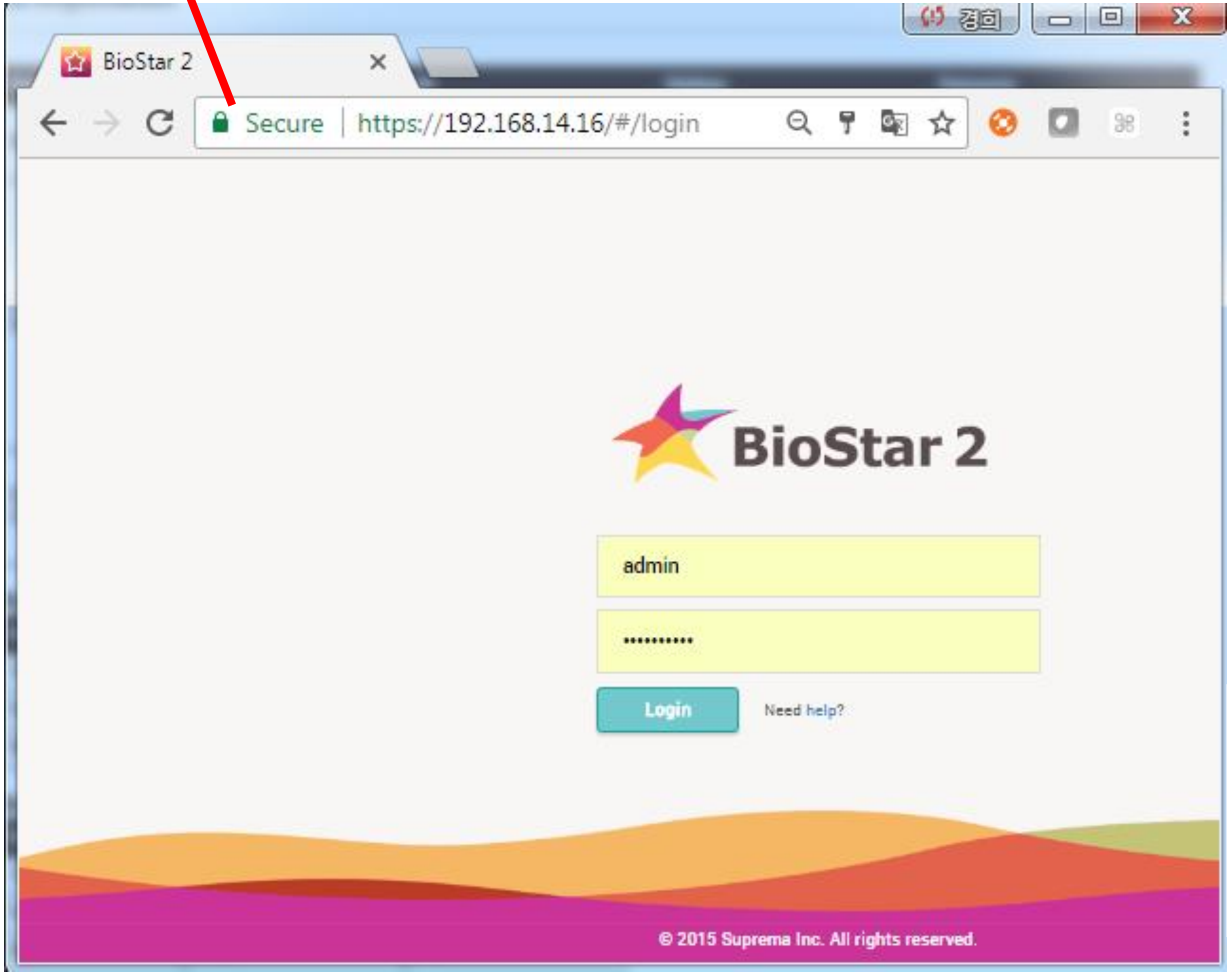
cert-register

success

http://kb.supremainc.com/knowledge/doku.php?id=en:2xfaq_how_to_change_from_http_to_https&s[]=https

Better Default Security




BioStar 2
Secure
https://192.168.14.16/#/login
BioStar 2
Login
Need help?
© 2015 Suprema Inc. All rights reserved.

admin

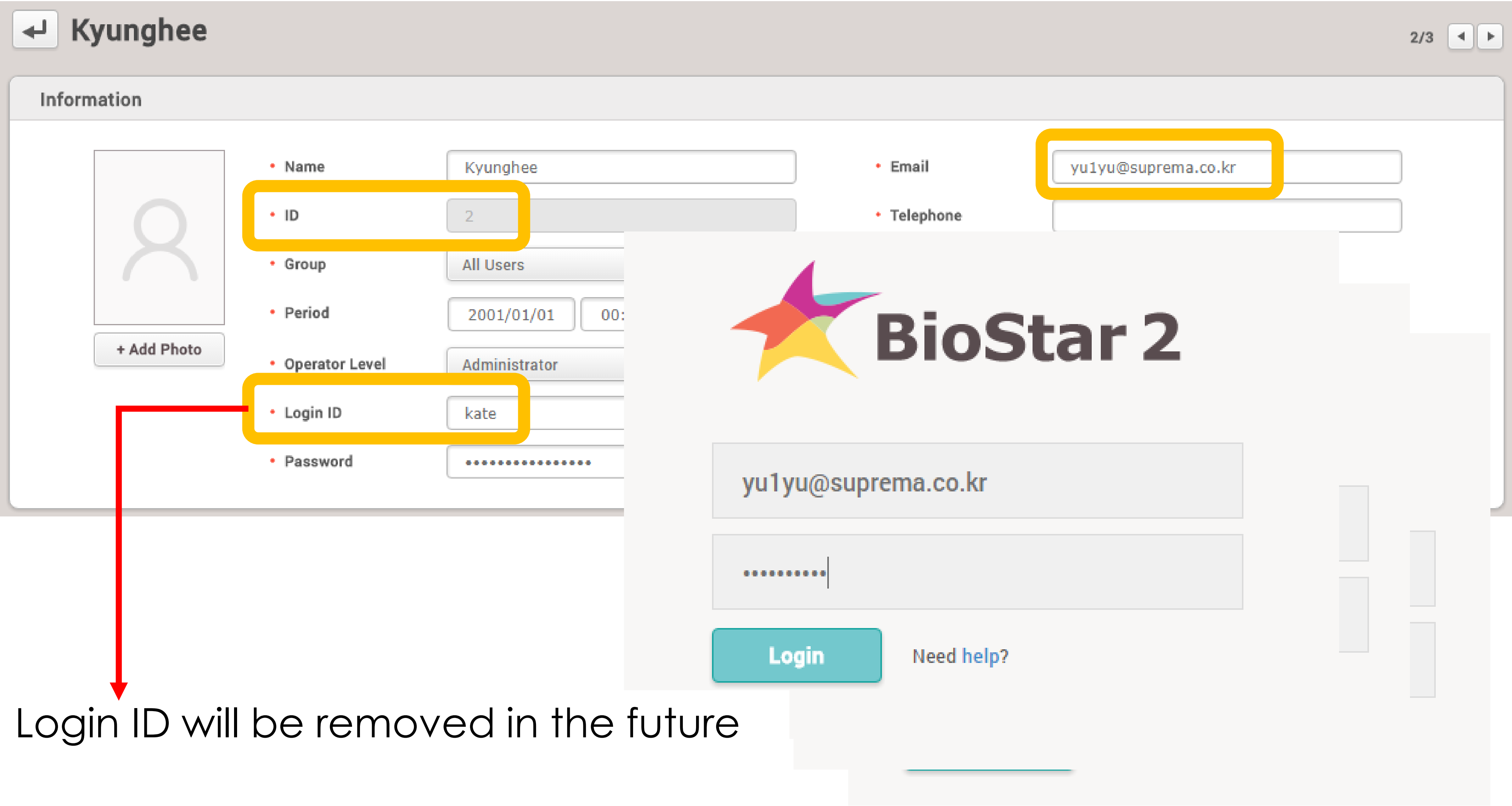
••••••••••

* For a private certificate, Please refer the following link

http://support.supremainc.com/solution/articles/24000005211--biostar-2-how-to-apply-a-private-certificate-for-https/en

Login credential

- BioStar2 v2.5 supports to login with ID, Email, or Login ID



Kyunghee 2/3

Information

- Name: Kyunghee
- ID: 2
- Group: All Users
- Period: 2001/01/01 00:
- Operator Level: Administrator
- Login ID: kate
- Password: ••••••••••••••••
- Email: yu1yu@suprema.co.kr
- Telephone:

BioStar 2

yu1yu@suprema.co.kr

••••••••••

Login ID will be removed in the future

Automatic Device Sync

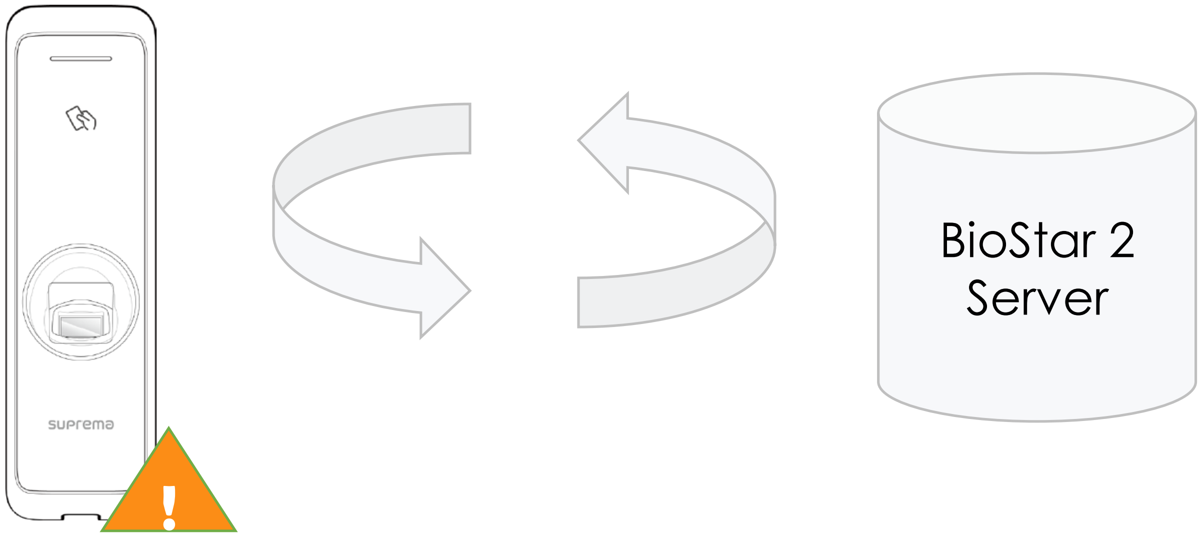
- BioStar v2.5 synchronizes automatically as soon as disconnected devices are reconnected.

  * Synchronization with server: user, access group, door, zone data

Automatic Device Sync

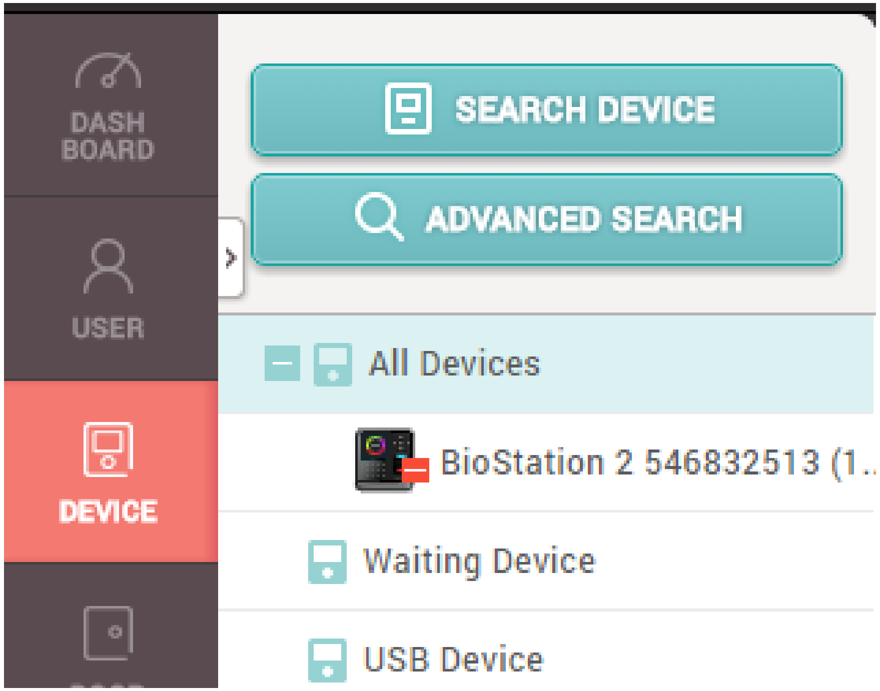
- Device did not sync automatically in lower BioStar 2 versions after reconnection

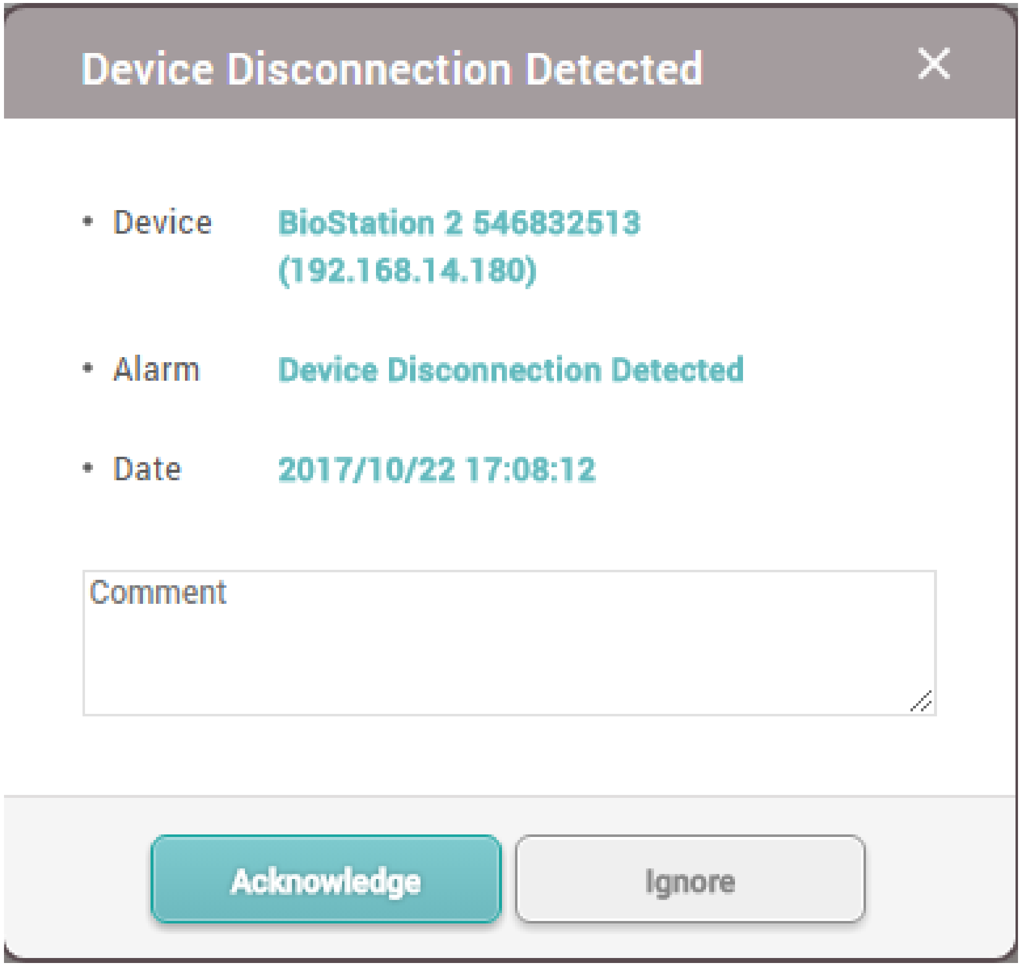
- Previous versions required admin to click sync again every time device reconnected



Adding necessary alert event

- BioStar2 v2.5 can make an alert for device disconnection detection





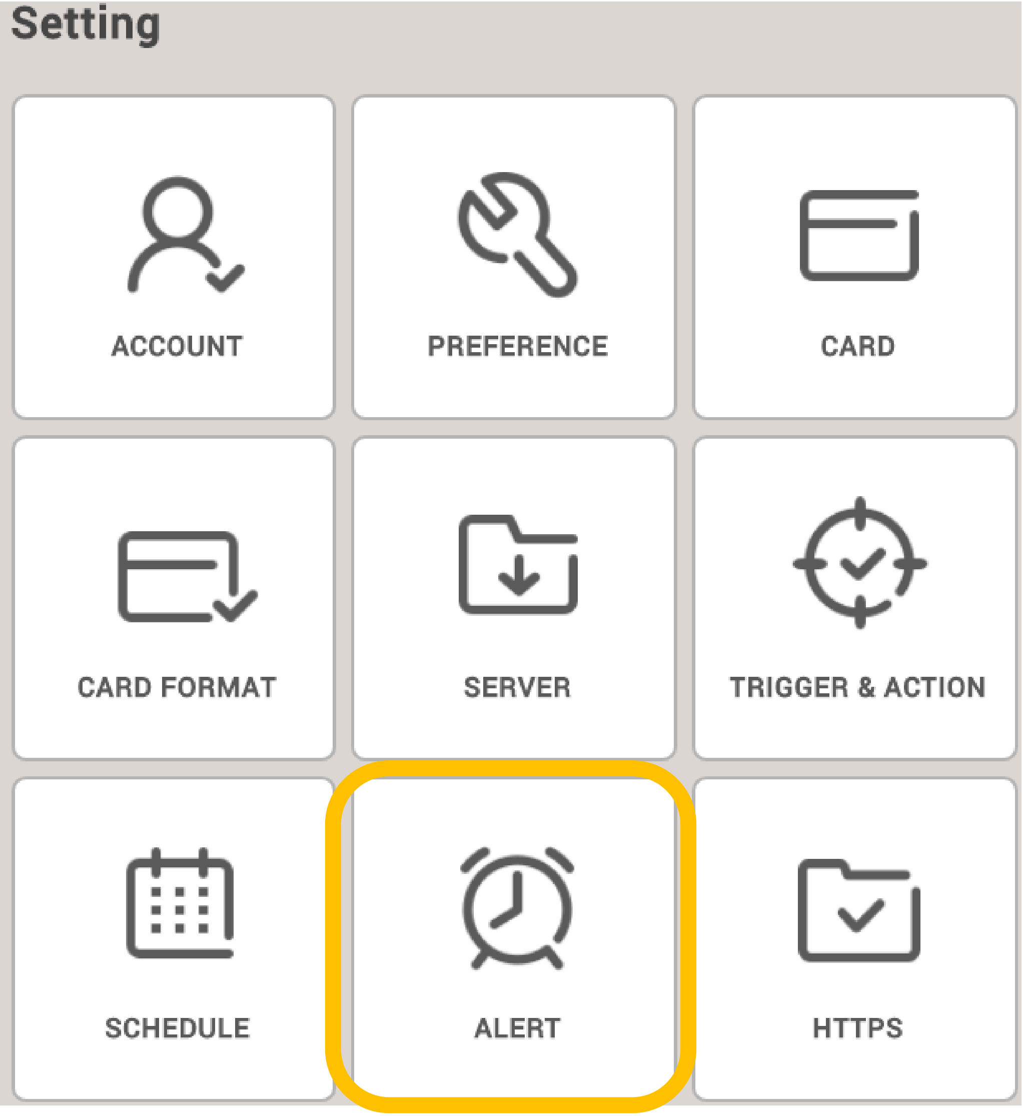
Device Disconnection Detected

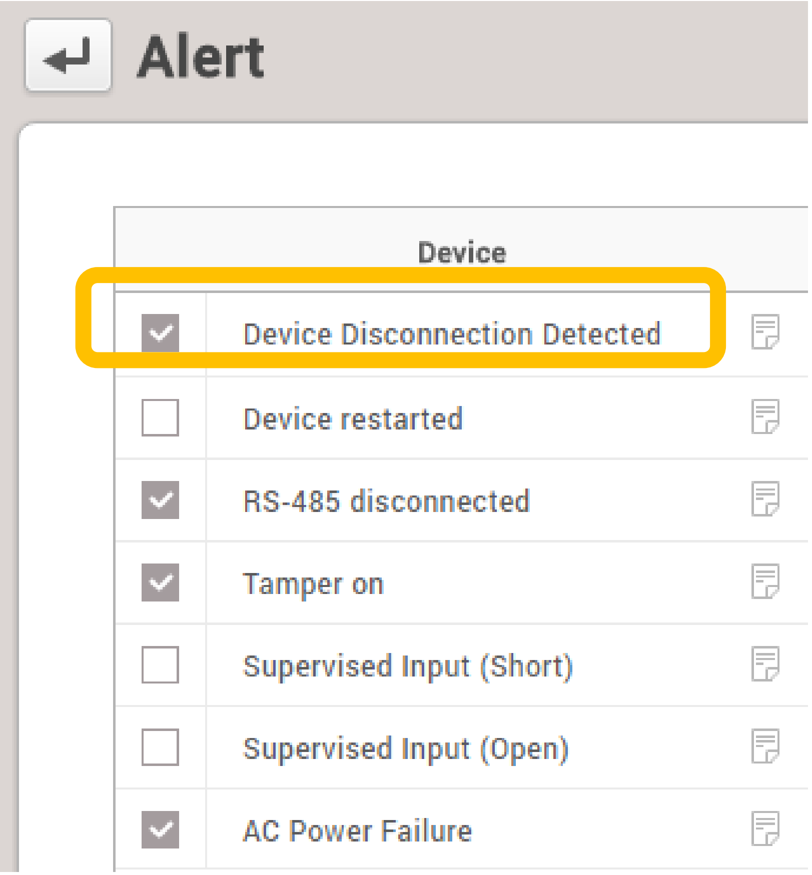
- Device BioStation 2 546832513 (192.168.14.180)
- Alarm Device Disconnection Detected
- Date 2017/10/22 17:08:12

http://kb.supremainc.com/knowledge/doku.php?id=en:how_to_configure_an_alert_pop-up_message_when_a_device_is_disconnected

Adding necessary alert event

- Configuration : Setting > Alert> Device Disconnection Detected

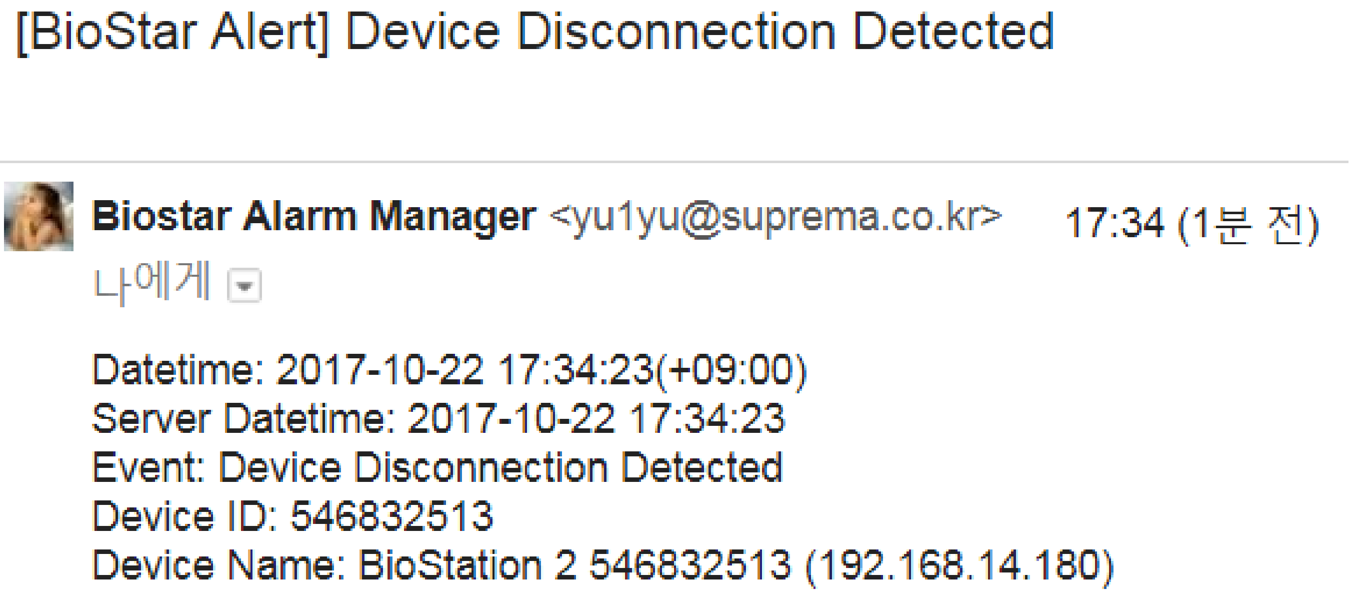




	Device
☑	Device Disconnection Detected
□	Device restarted
☑	RS-485 disconnected
☑	Tamper on
□	Supervised Input (Short)
□	Supervised Input (Open)
☑	AC Power Failure

Adding necessary Trigger & Action

- BioStar2 v2.5 can make an email alert for device disconnection detection



[BioStar Alert] Device Disconnection Detected

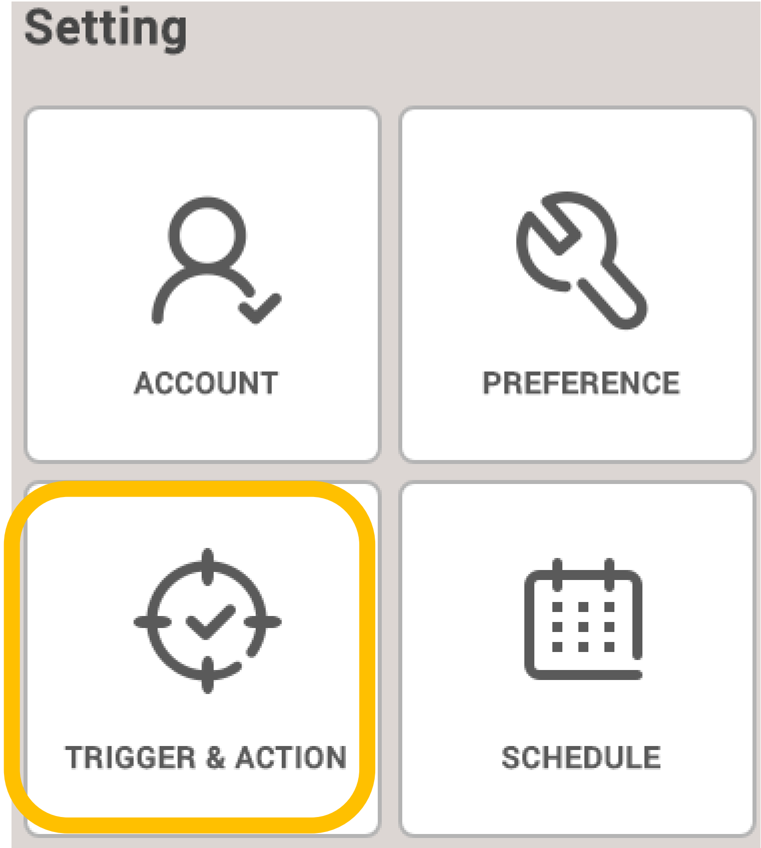
Biostar Alarm Manager <yu1yu@suprema.co.kr> 17:34 (1분 전)

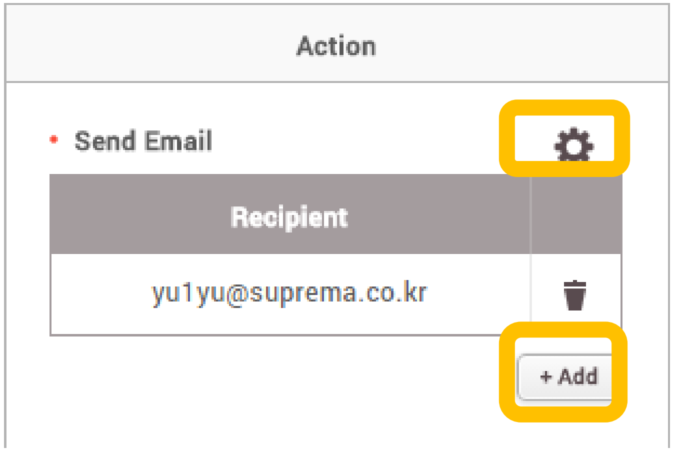
나에게

Datetime: 2017-10-22 17:34:23(+09:00)
Server Datetime: 2017-10-22 17:34:23
Event: Device Disconnection Detected
Device ID: 546832513
Device Name: BioStation 2 546832513 (192.168.14.180)

Trigger & Action

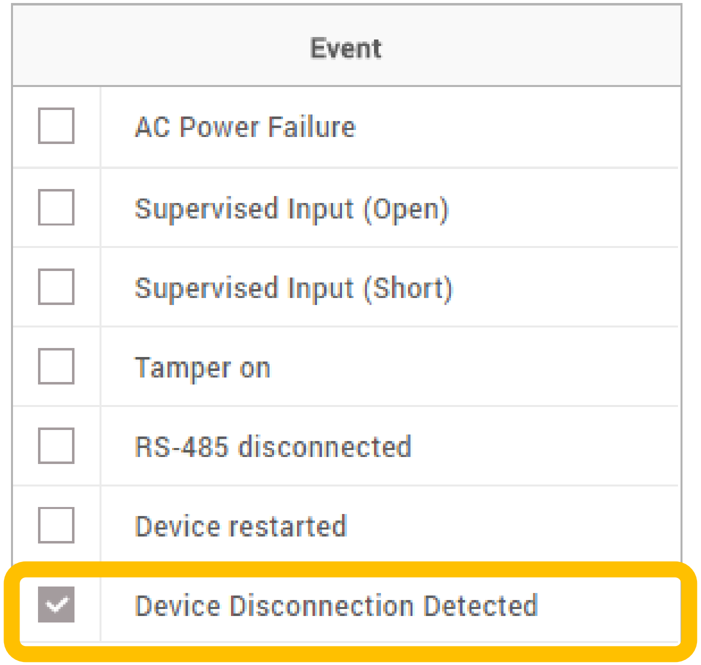
- Configuration : Setting > Trigger& Action > Device Disconnection Detected




Action

- Send Email

Recipient	
yu1yu@suprema.co.kr	

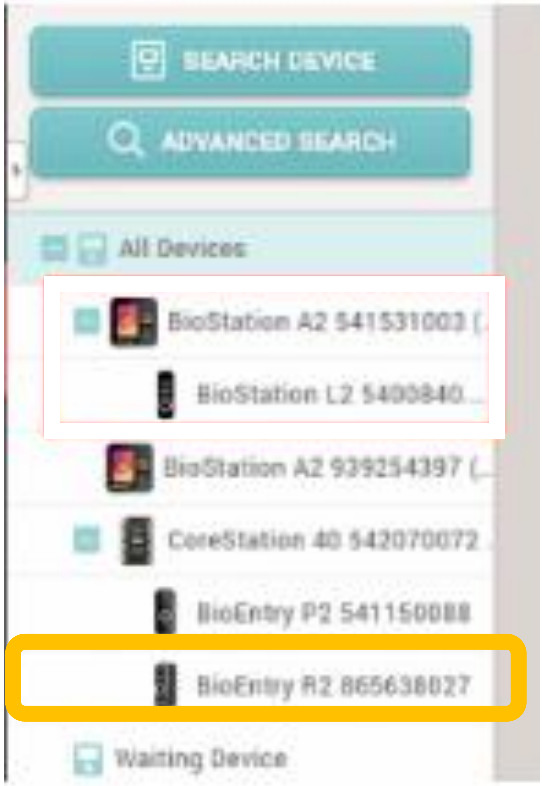

Event

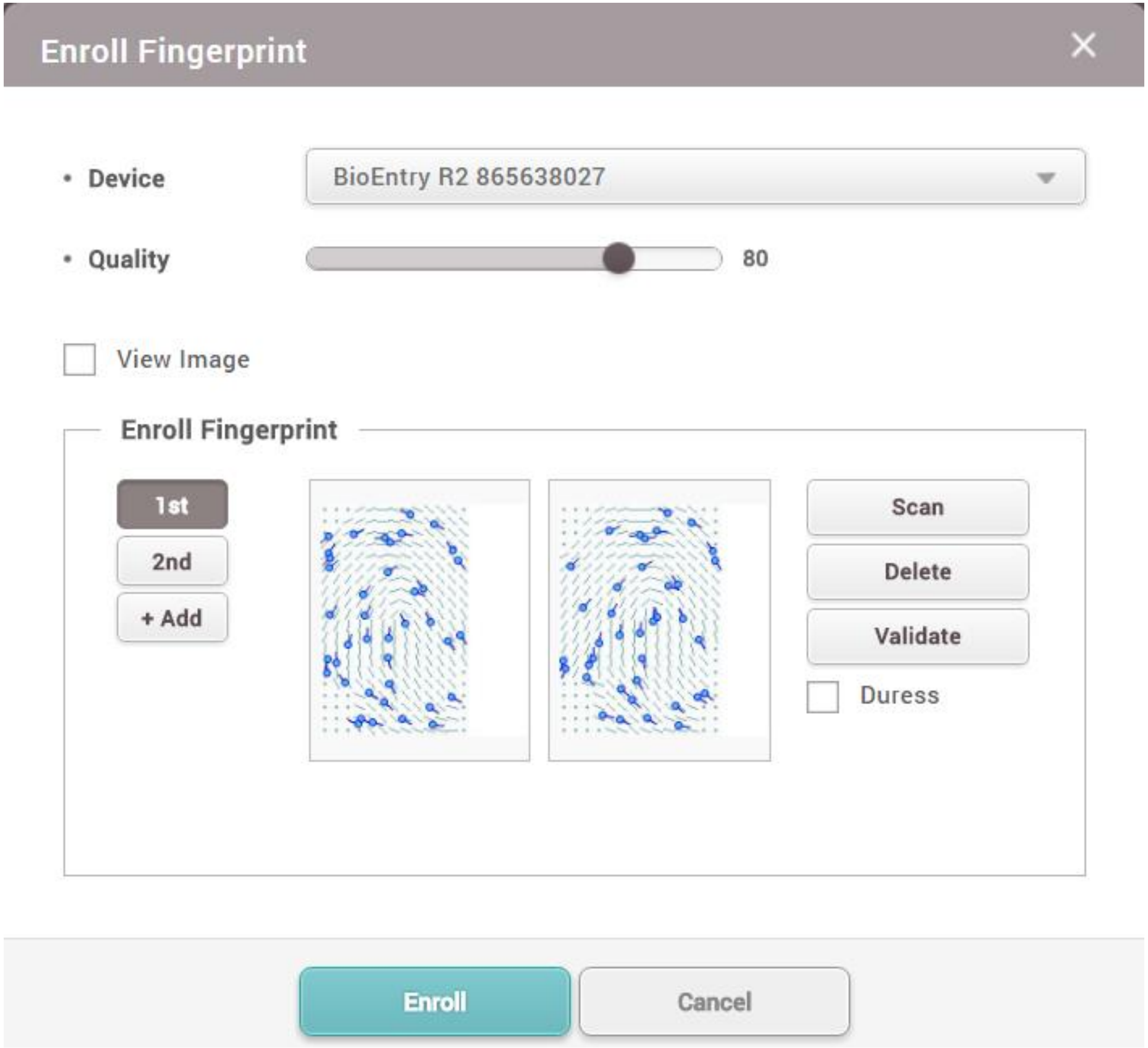
□ AC Power Failure
□ Supervised Input (Open)
□ Supervised Input (Short)
□ Tamper on
□ RS-485 disconnected
□ Device restarted
☑ Device Disconnection Detected

http://kb.supremainc.com/knowledge/doku.php?id=en:how_to_send_email_when_a_device_is_disconnected

Fingerprint Enrollment

- Slave Device was not chosen in lower BioStar 2 versions




Enroll Fingerprint

- Device: BioEntry R2 865638027
- Quality: 80

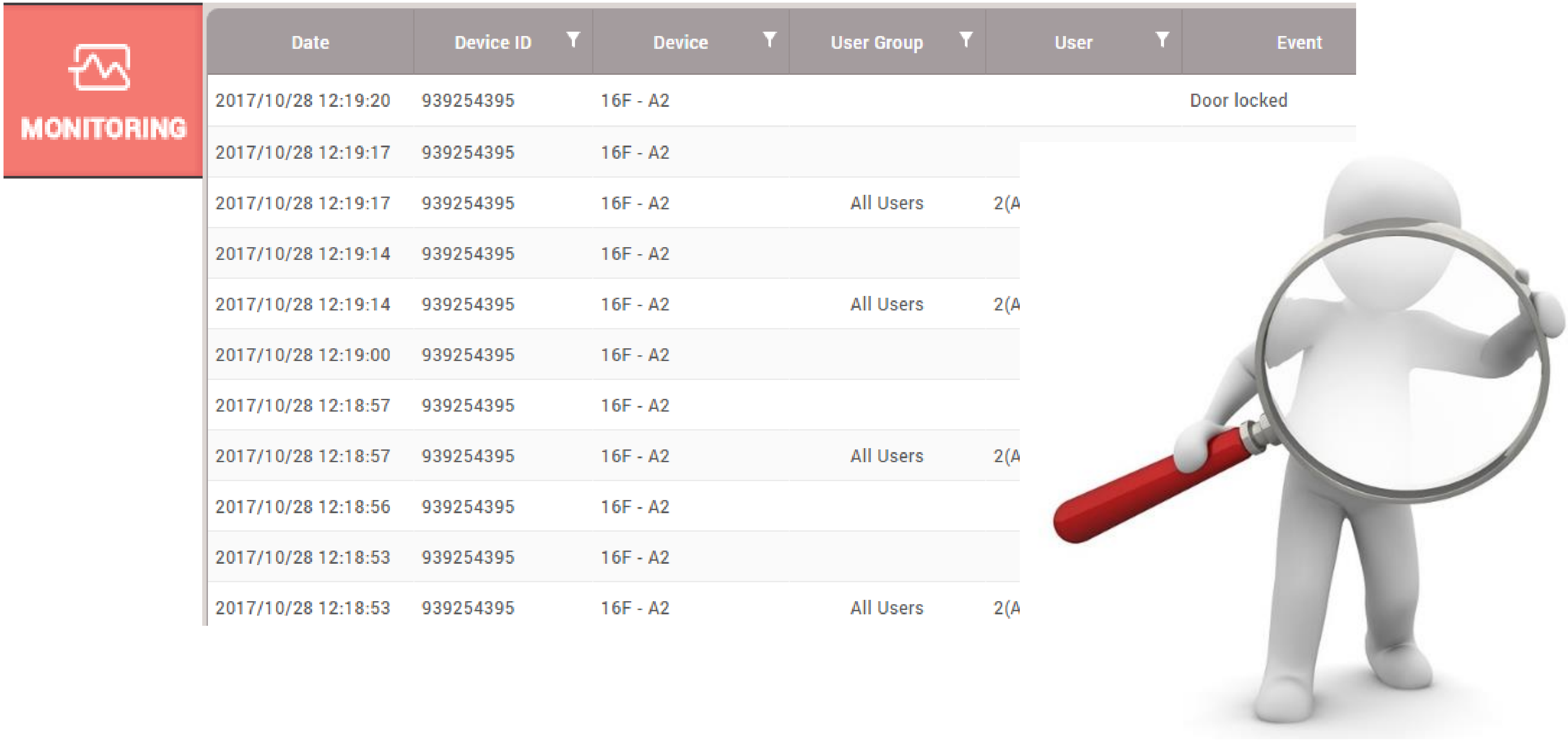
□ View Image

Enroll Fingerprint

□ Duress

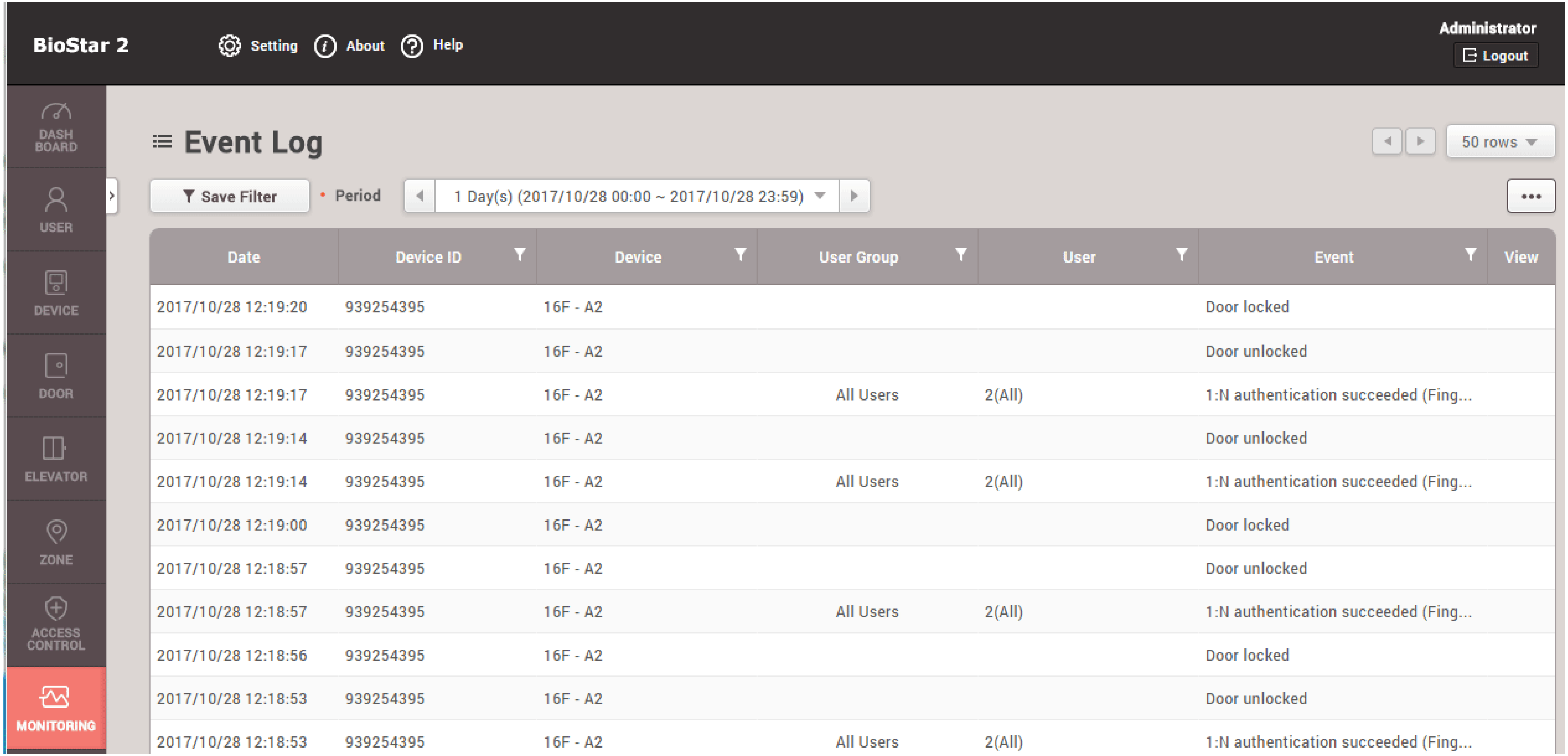
Monitoring

- Convenient log event search
- Improved page navigation of Event Log
- T&A Key event confirmation from Event Log of Monitoring menu



Date	Device ID	Device	User Group	User	Event
2017/10/28 12:19:20	939254395	16F - A2			Door locked
2017/10/28 12:19:17	939254395	16F - A2			
2017/10/28 12:19:17	939254395	16F - A2	All Users	2(A	
2017/10/28 12:19:14	939254395	16F - A2			
2017/10/28 12:19:14	939254395	16F - A2	All Users	2(A	
2017/10/28 12:19:00	939254395	16F - A2			
2017/10/28 12:18:57	939254395	16F - A2			
2017/10/28 12:18:57	939254395	16F - A2	All Users	2(A	
2017/10/28 12:18:56	939254395	16F - A2			
2017/10/28 12:18:53	939254395	16F - A2			
2017/10/28 12:18:53	939254395	16F - A2	All Users	2(A	

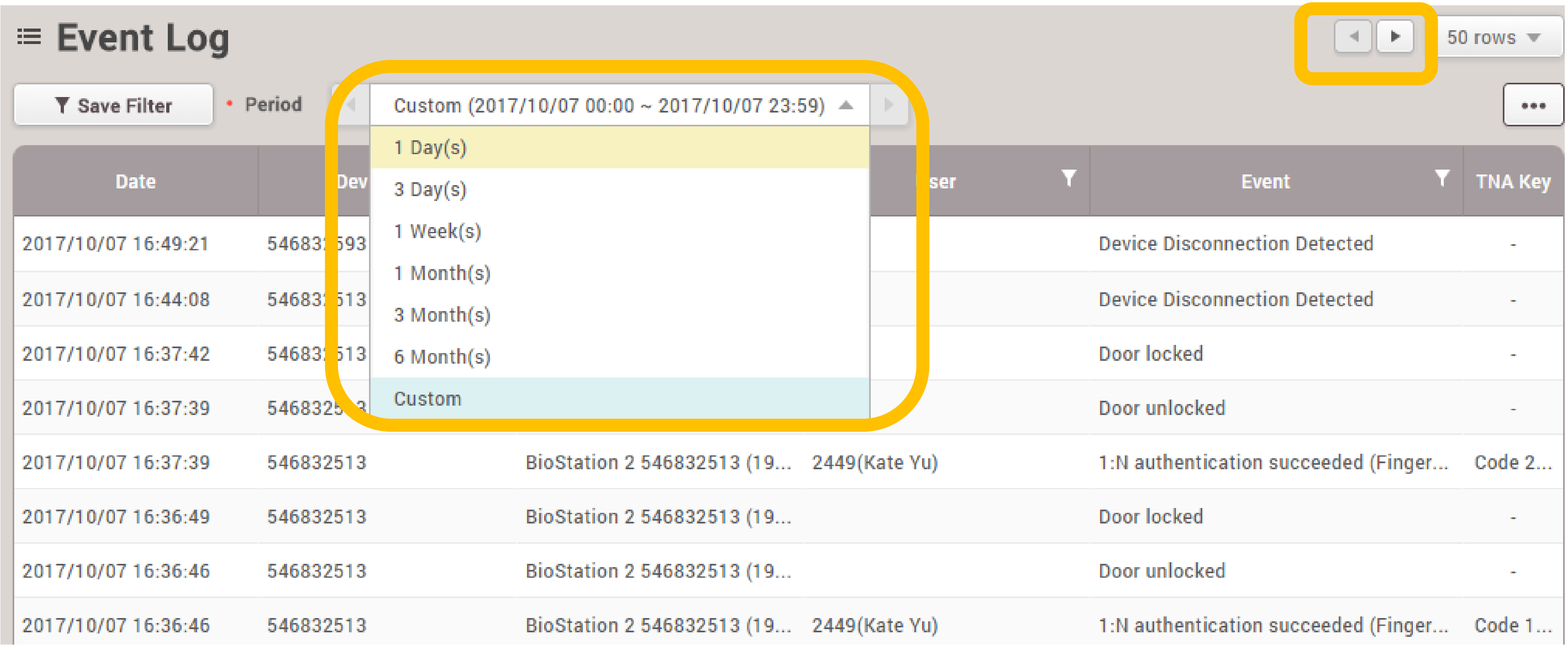
Monitoring



Date	Device ID	Device	User Group	User	Event	View
2017/10/28 12:19:20	939254395	16F - A2			Door locked	
2017/10/28 12:19:17	939254395	16F - A2			Door unlocked	
2017/10/28 12:19:17	939254395	16F - A2	All Users	2(All)	1:N authentication succeeded (Fing...	
2017/10/28 12:19:14	939254395	16F - A2			Door unlocked	
2017/10/28 12:19:14	939254395	16F - A2	All Users	2(All)	1:N authentication succeeded (Fing...	
2017/10/28 12:19:00	939254395	16F - A2			Door locked	
2017/10/28 12:18:57	939254395	16F - A2			Door unlocked	
2017/10/28 12:18:57	939254395	16F - A2	All Users	2(All)	1:N authentication succeeded (Fing...	
2017/10/28 12:18:56	939254395	16F - A2			Door locked	
2017/10/28 12:18:53	939254395	16F - A2			Door unlocked	
2017/10/28 12:18:53	939254395	16F - A2	All Users	2(All)	1:N authentication succeeded (Fing...	

Monitoring

- Confirms log event in accordance with configured period
- Confirm log event with page navigation button



Event Log

50 rows

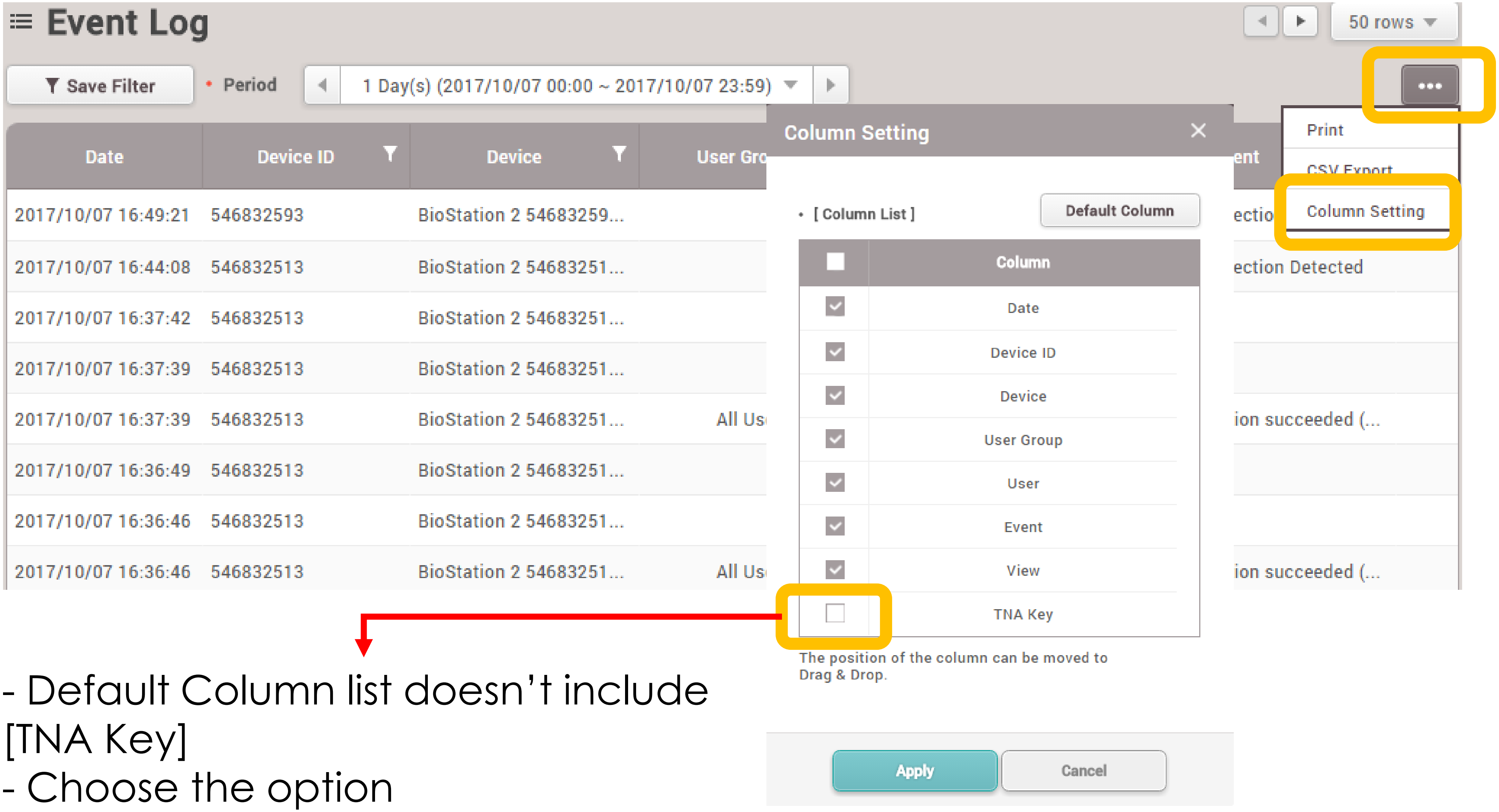
Save Filter

Period: Custom (2017/10/07 00:00 ~ 2017/10/07 23:59)

Date	Dev		ser	Event	TNA Key
2017/10/07 16:49:21	54683 593			Device Disconnection Detected	-
2017/10/07 16:44:08	54683 513			Device Disconnection Detected	-
2017/10/07 16:37:42	54683 513			Door locked	-
2017/10/07 16:37:39	5468325 3			Door unlocked	-
2017/10/07 16:37:39	546832513	BioStation 2 546832513 (19...	2449(Kate Yu)	1:N authentication succeeded (Finger...	Code 2...
2017/10/07 16:36:49	546832513	BioStation 2 546832513 (19...		Door locked	-
2017/10/07 16:36:46	546832513	BioStation 2 546832513 (19...		Door unlocked	-
2017/10/07 16:36:46	546832513	BioStation 2 546832513 (19...	2449(Kate Yu)	1:N authentication succeeded (Finger...	Code 1...

Monitoring

- Available column setting is added : T&A key



Event Log

Date	Device ID	Device	User Gro	ent
2017/10/07 16:49:21	546832593	BioStation 2 54683259...		ectio
2017/10/07 16:44:08	546832513	BioStation 2 54683251...		ection Detected
2017/10/07 16:37:42	546832513	BioStation 2 54683251...		
2017/10/07 16:37:39	546832513	BioStation 2 54683251...		
2017/10/07 16:37:39	546832513	BioStation 2 54683251...	All Us	ion succeeded (...
2017/10/07 16:36:49	546832513	BioStation 2 54683251...		
2017/10/07 16:36:46	546832513	BioStation 2 54683251...		
2017/10/07 16:36:46	546832513	BioStation 2 54683251...	All Us	ion succeeded (...

Column Setting

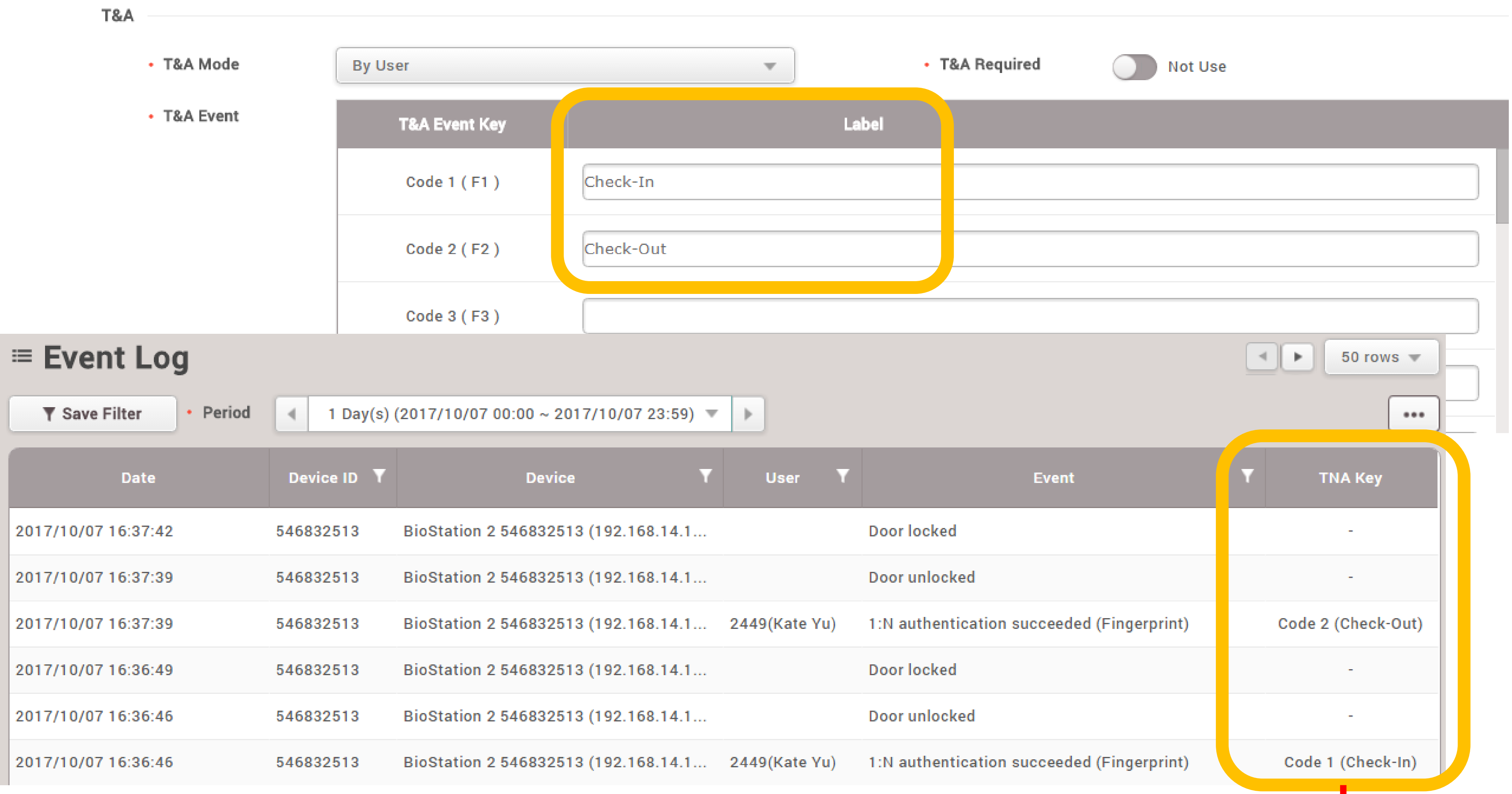
• [Column List] Default Column

□	Column
☑	Date
☑	Device ID
☑	Device
☑	User Group
☑	User
☑	Event
☑	View
□	TNA Key

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

- Default Column list doesn't include [TNA Key]
- Choose the option

Monitoring



T&A

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

T&A Event Key	Label
Code 1 (F1)	Check-In
Code 2 (F2)	Check-Out
Code 3 (F3)	

Event Log

- Period: 1 Day(s) (2017/10/07 00:00 ~ 2017/10/07 23:59)

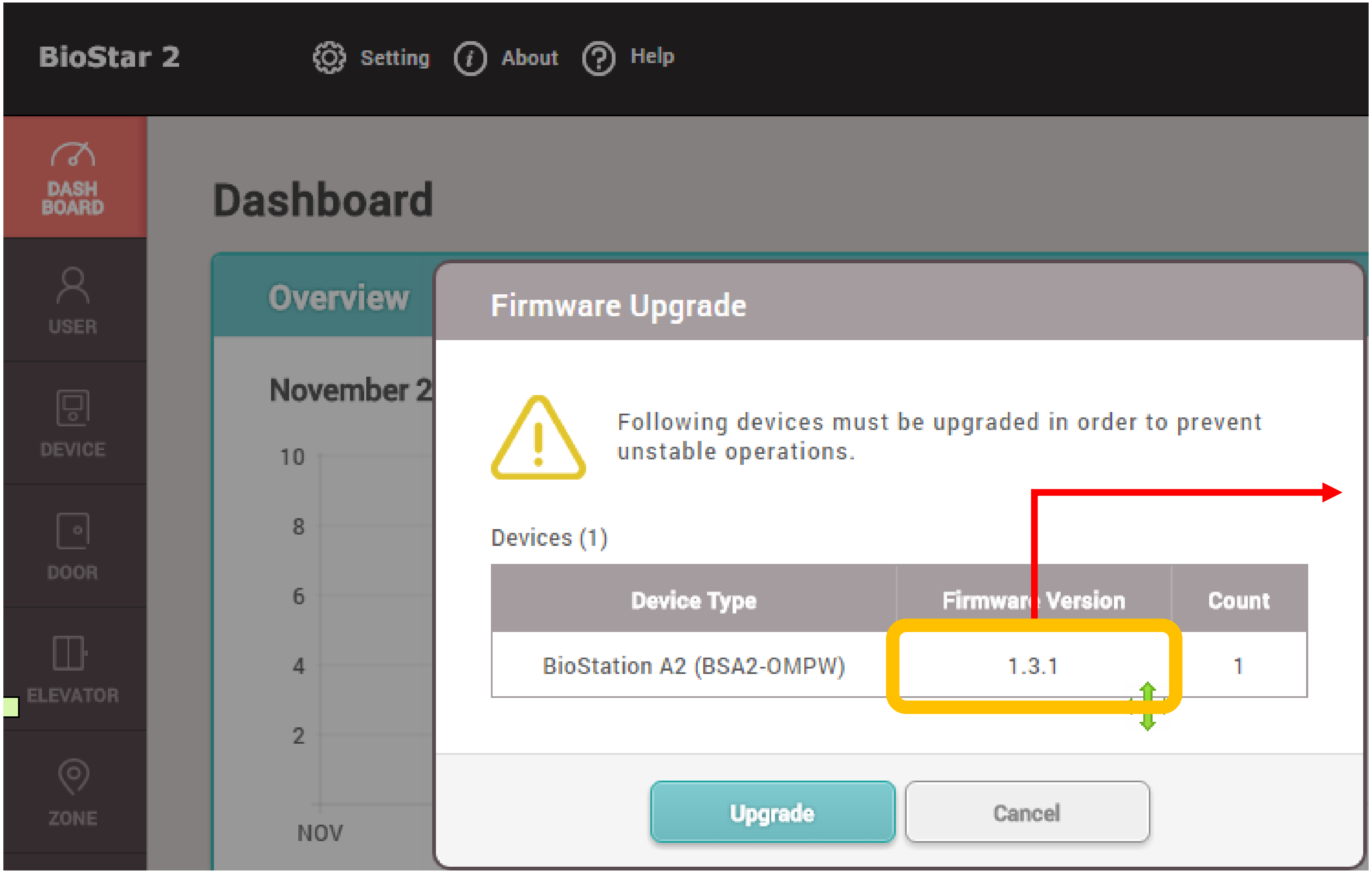
Date	Device ID	Device	User	Event	TNA Key
2017/10/07 16:37:42	546832513	BioStation 2 546832513 (192.168.14.1...		Door locked	-
2017/10/07 16:37:39	546832513	BioStation 2 546832513 (192.168.14.1...		Door unlocked	-
2017/10/07 16:37:39	546832513	BioStation 2 546832513 (192.168.14.1...	2449(Kate Yu)	1:N authentication succeeded (Fingerprint)	Code 2 (Check-Out)
2017/10/07 16:36:49	546832513	BioStation 2 546832513 (192.168.14.1...		Door locked	-
2017/10/07 16:36:46	546832513	BioStation 2 546832513 (192.168.14.1...		Door unlocked	-
2017/10/07 16:36:46	546832513	BioStation 2 546832513 (192.168.14.1...	2449(Kate Yu)	1:N authentication succeeded (Fingerprint)	Code 1 (Check-In)

- Check if a label is properly set
- TNA key field will indicate T&A Event Key with the label

3. New features

FW update Alert message

- BioStar2 v2.5 makes an alert message if the device firmware is old version



Firmware Upgrade

Following devices must be upgraded in order to prevent unstable operations.

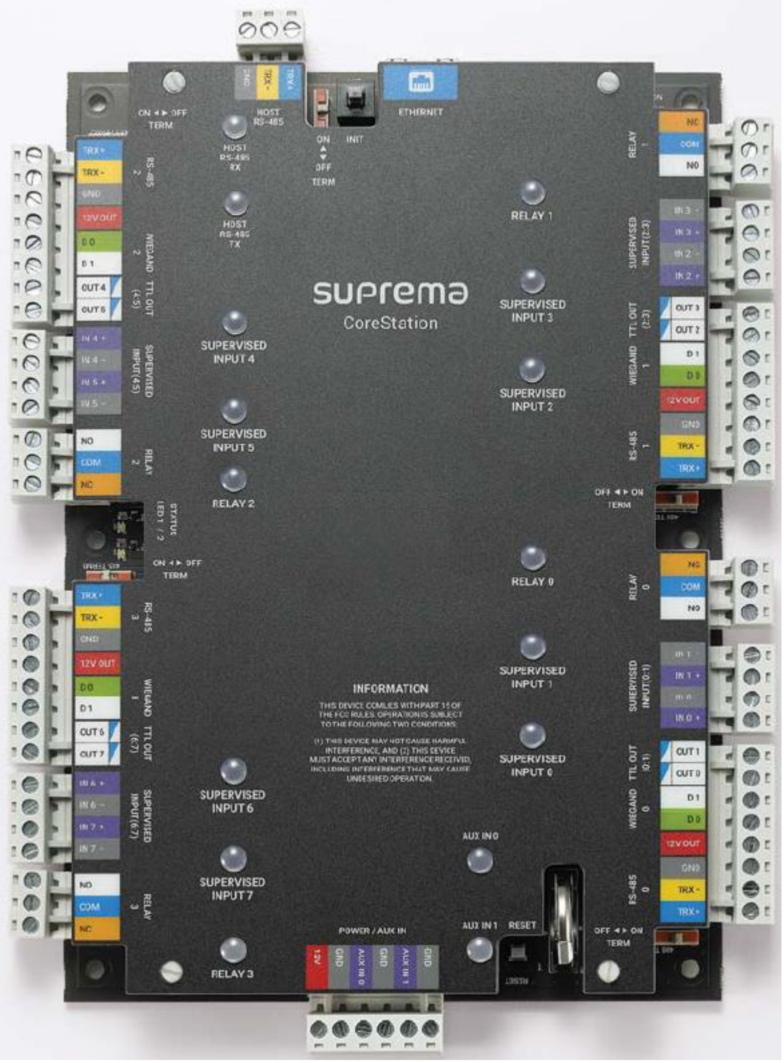
Devices (1)

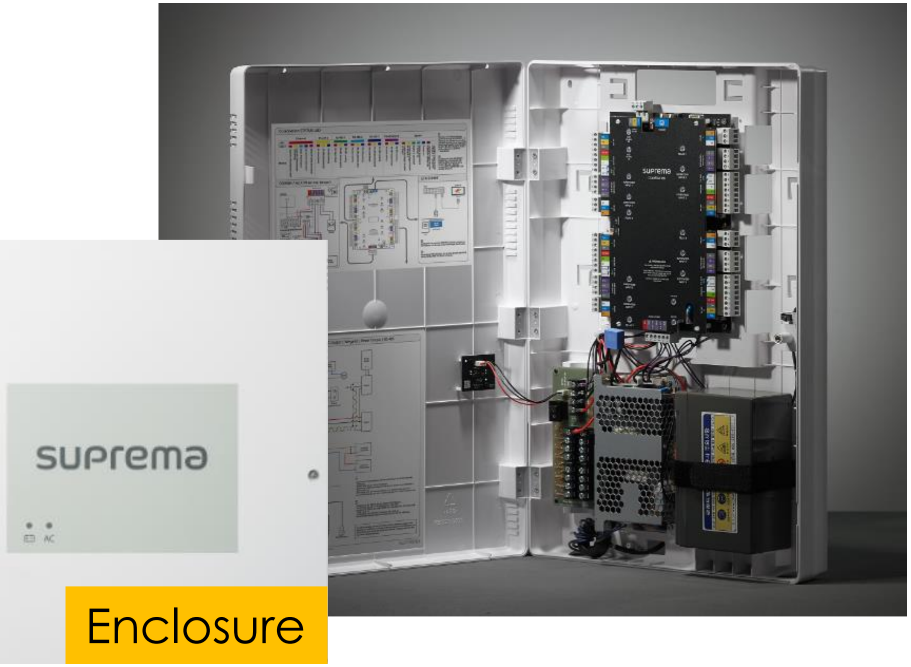
Device Type	Firmware Version	Count
BioStation A2 (BSA2-OMPW)	1.3.1	1

Upgrade old firmware

CoreStation

- Master controller managing slave devices with RS485 connection
- 4 relay, 4 wiegand, 8 supervised input, 5 RS485 channels



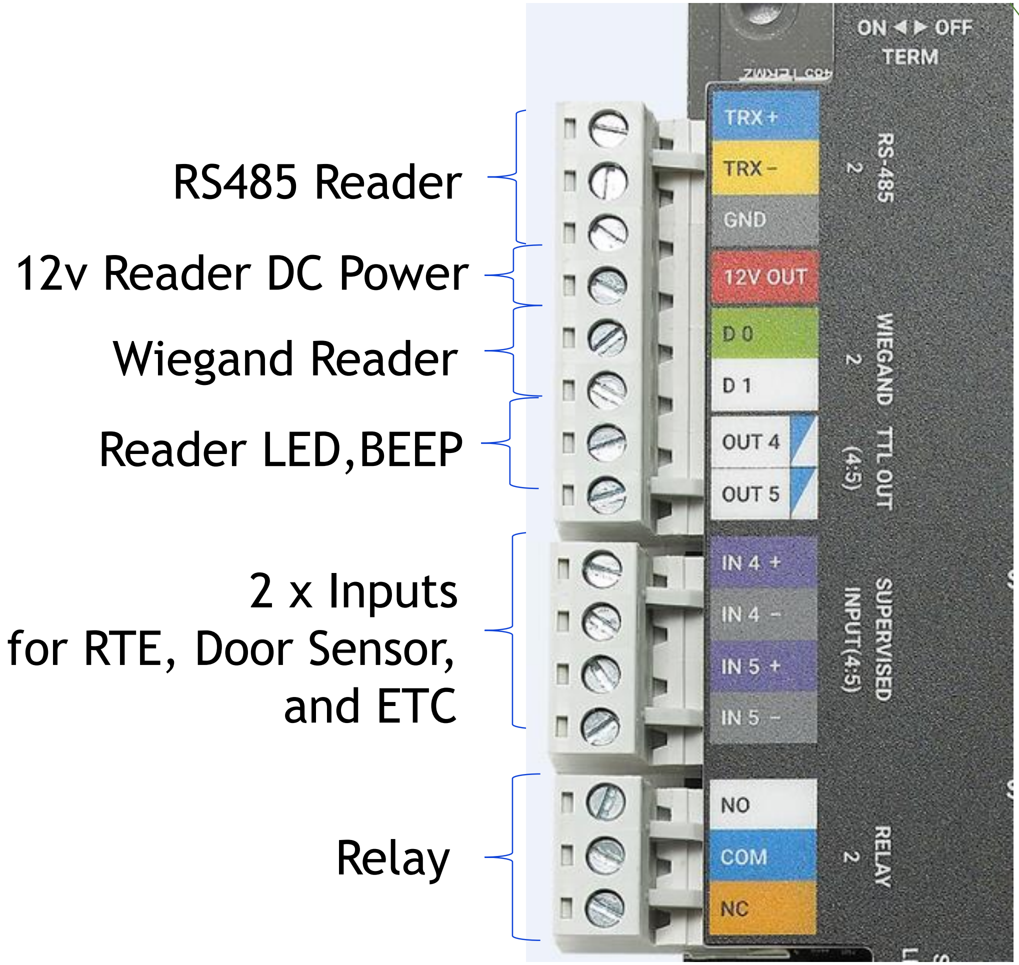


Enclosure

FaceStation2 cannot be used as slave device

CoreStation

- Master controller managing slave devices with RS485 connection
- 4 relay, 4 wiegand, 8 supervised input, 5 RS485 channels



RS485 Reader

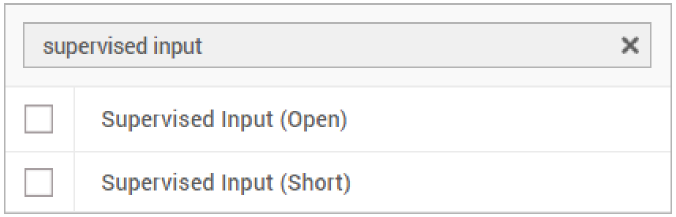
12v Reader DC Power

Wiegand Reader

Reader LED,BEEP

2 x Inputs
for RTE, Door Sensor,
and ETC

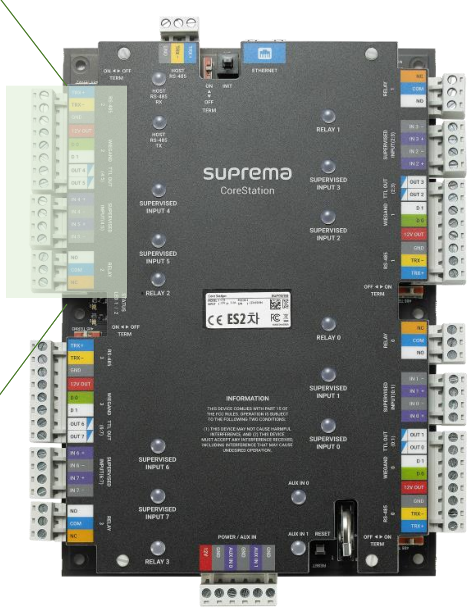
Relay



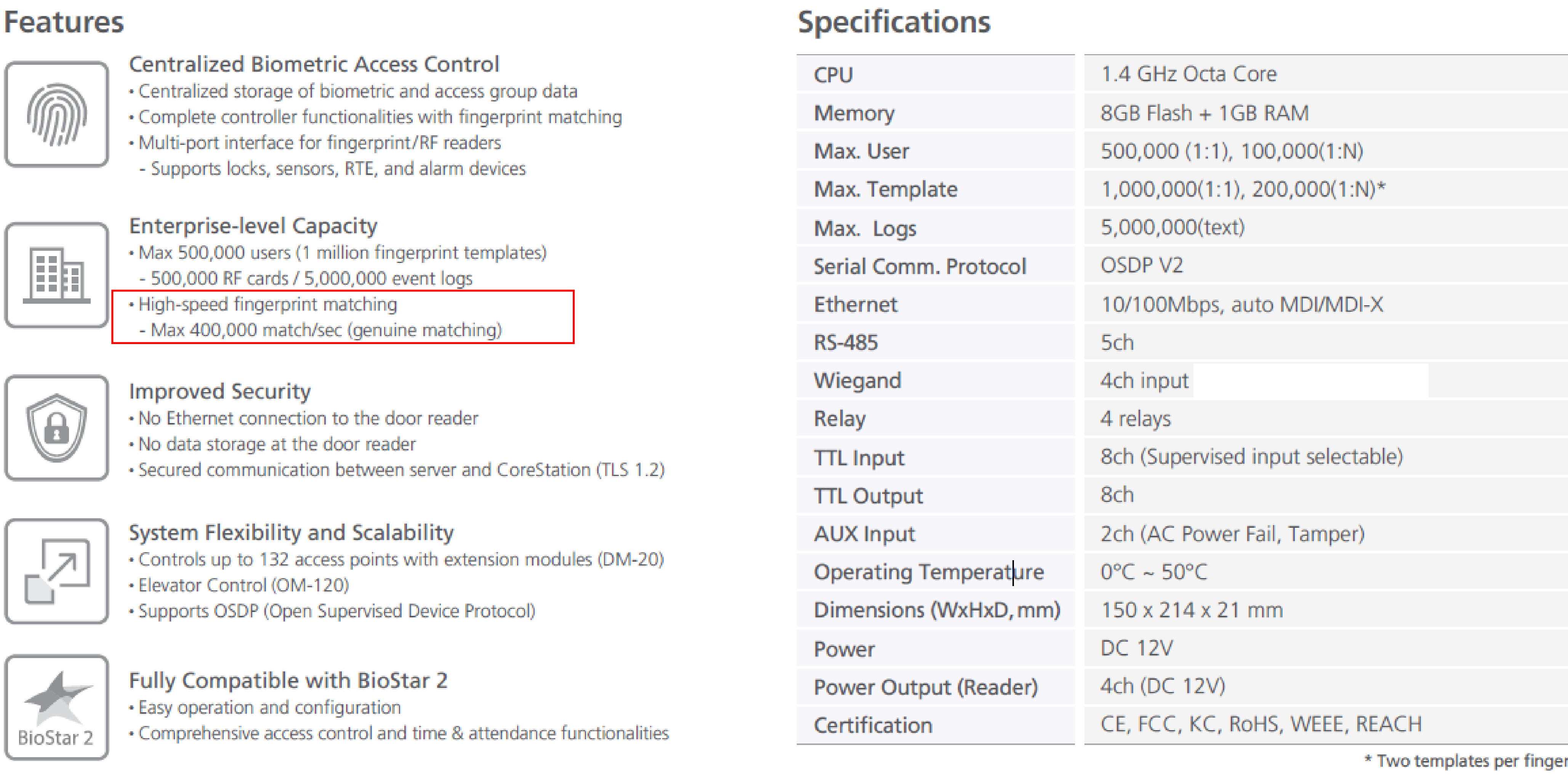
supervised input ✕

□	Supervised Input (Open)
□	Supervised Input (Short)

4 x Reader Interface
Input/Output/Relay/Wiegand/Power



CoreStation



Features

Centralized Biometric Access Control

- Centralized storage of biometric and access group data
- Complete controller functionalities with fingerprint matching
- Multi-port interface for fingerprint/RF readers
  - Supports locks, sensors, RTE, and alarm devices

Enterprise-level Capacity

- Max 500,000 users (1 million fingerprint templates)
  - 500,000 RF cards / 5,000,000 event logs
- High-speed fingerprint matching
  - Max 400,000 match/sec (genuine matching)

Improved Security

- No Ethernet connection to the door reader
- No data storage at the door reader
- Secured communication between server and CoreStation (TLS 1.2)

System Flexibility and Scalability

- Controls up to 132 access points with extension modules (DM-20)
- Elevator Control (OM-120)
- Supports OSDP (Open Supervised Device Protocol)

Fully Compatible with BioStar 2

- Easy operation and configuration
- Comprehensive access control and time & attendance functionalities

Specifications

CPU	1.4 GHz Octa Core
Memory	8GB Flash + 1GB RAM
Max. User	500,000 (1:1), 100,000(1:N)
Max. Template	1,000,000(1:1), 200,000(1:N)*
Max. Logs	5,000,000(text)
Serial Comm. Protocol	OSDP V2
Ethernet	10/100Mbps, auto MDI/MDI-X
RS-485	5ch
Wiegand	4ch input
Relay	4 relays
TTL Input	8ch (Supervised input selectable)
TTL Output	8ch
AUX Input	2ch (AC Power Fail, Tamper)
Operating Temperature	0°C ~ 50°C
Dimensions (WxHxD, mm)	150 x 214 x 21 mm
Power	DC 12V
Power Output (Reader)	4ch (DC 12V)
Certification	CE, FCC, KC, RoHS, WEEE, REACH

* Two templates per finger

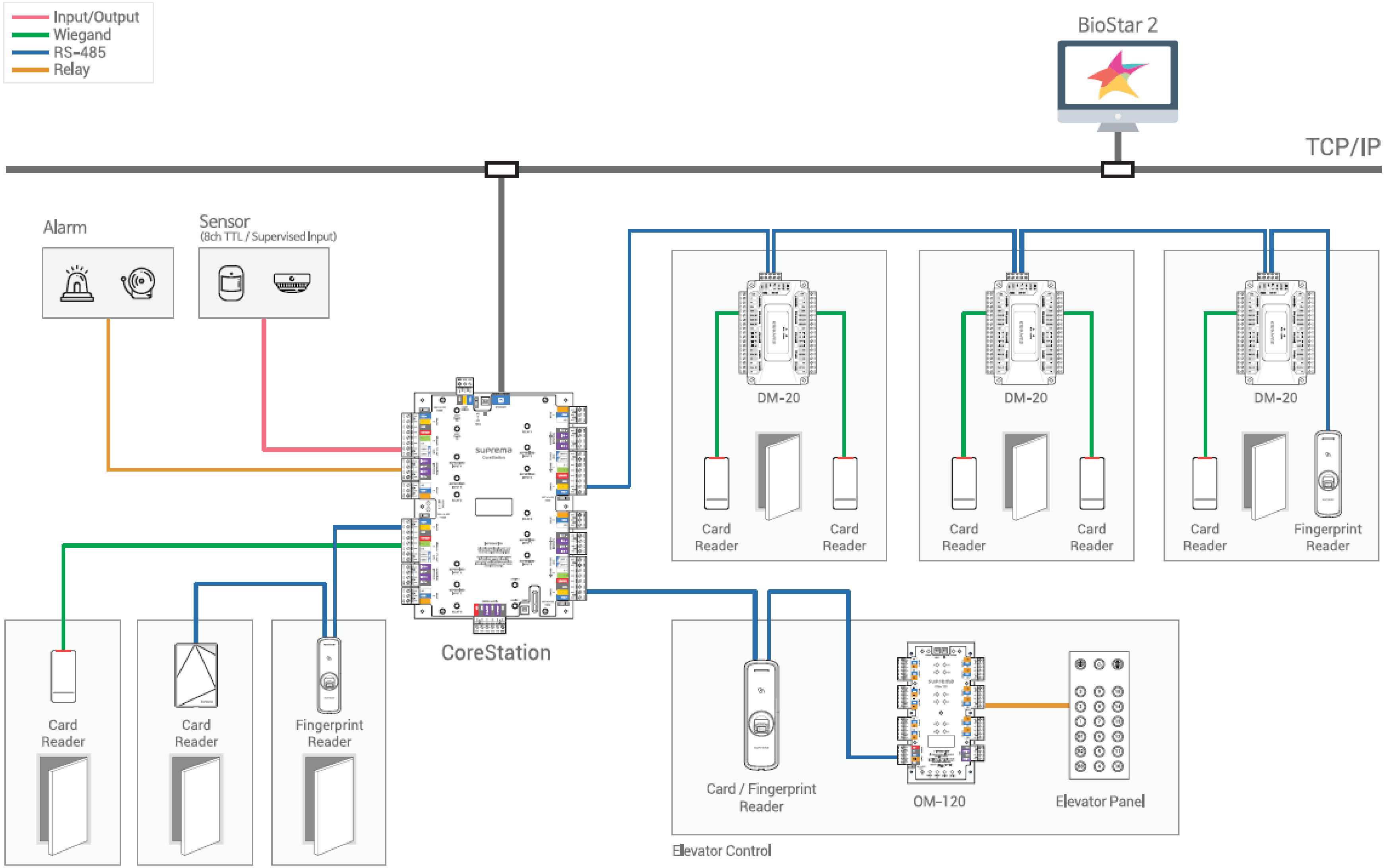
CoreStation

Main Specifications

Max.User	500,000 (1:1), 100,000 (1:N)
Max.Template	1,000,000 (1:1), 200,000 (1:N)*
Max.Logs	5,000,000 (text)
RS485	5 Channel
Wiegand	4 input/output (selectable)
Relay	4 Channel
TTL Input	8 Channel
TTL Output	8 Channel
AUX Input	2 Channel (AC Power Fail, Tamper)
Slave Connection	Max 64 slave devices
Power Output	4 Channel

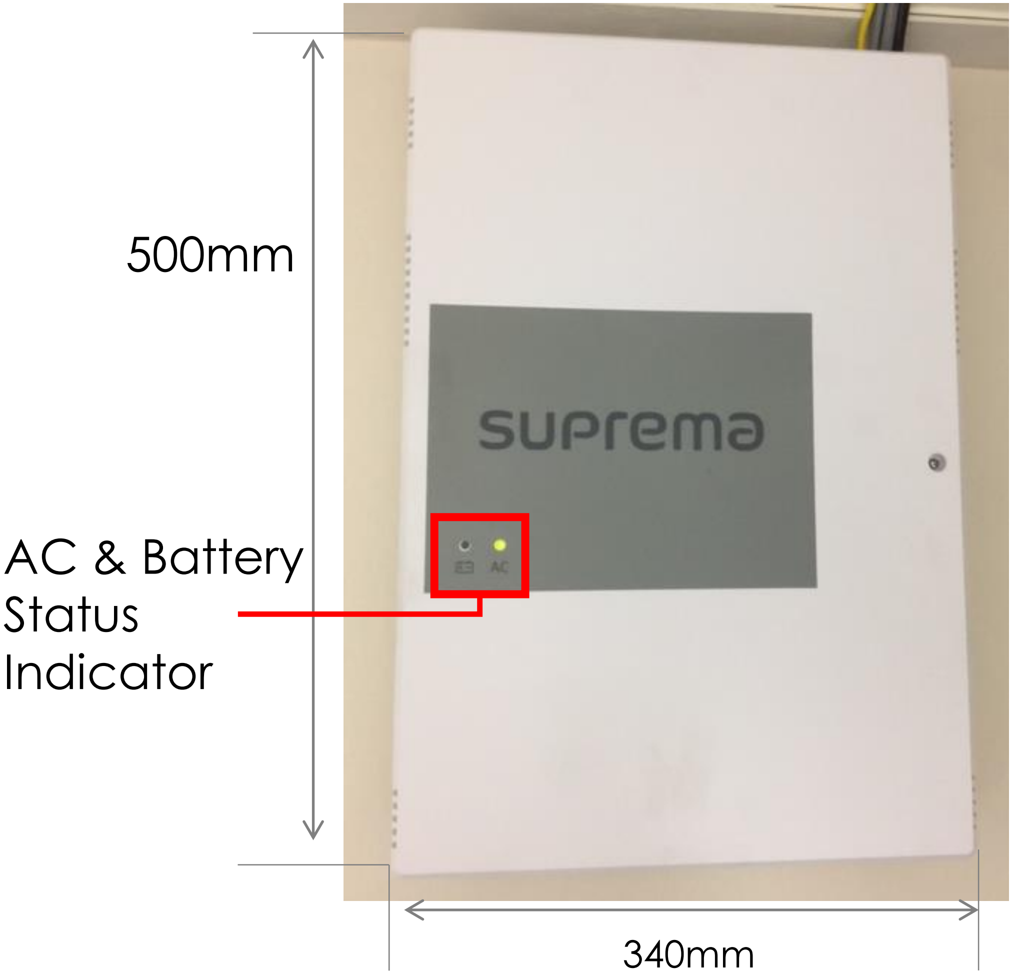
CoreStation

System Configurations



CoreStation

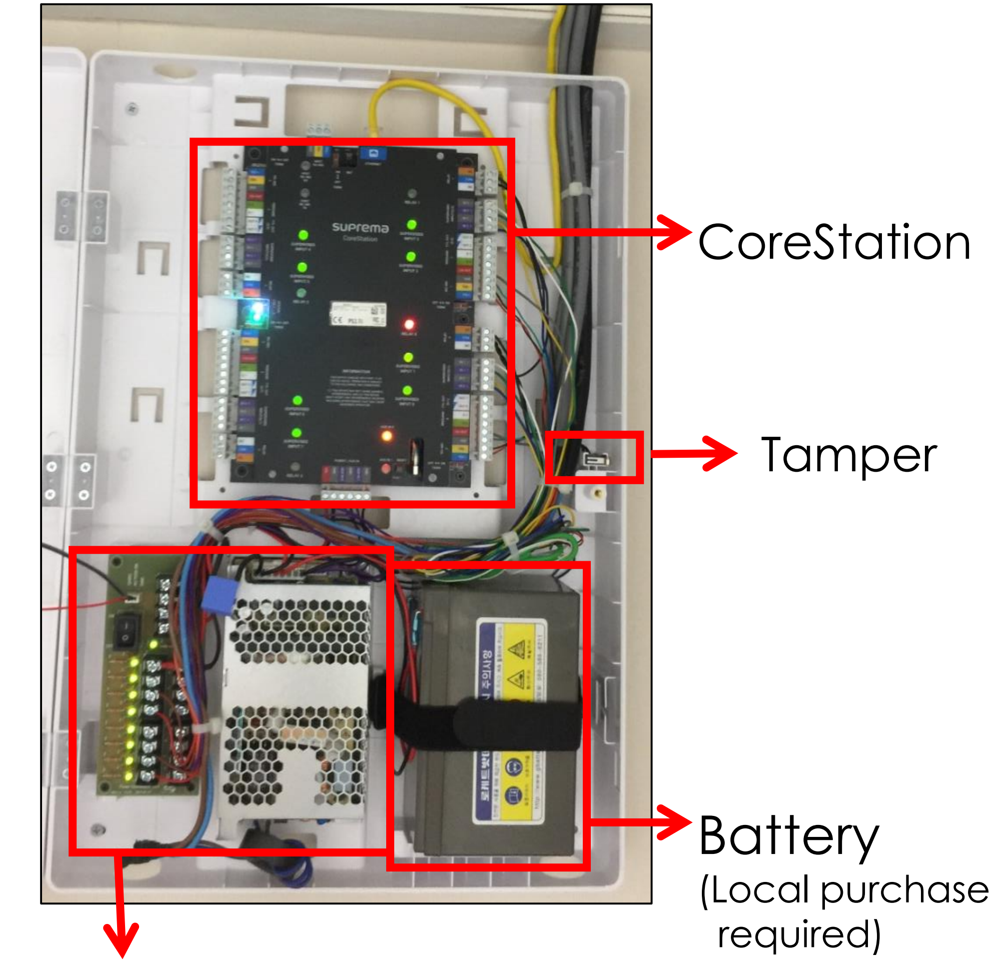
- Optional enclosure



500mm

340mm

AC & Battery Status Indicator



CoreStation

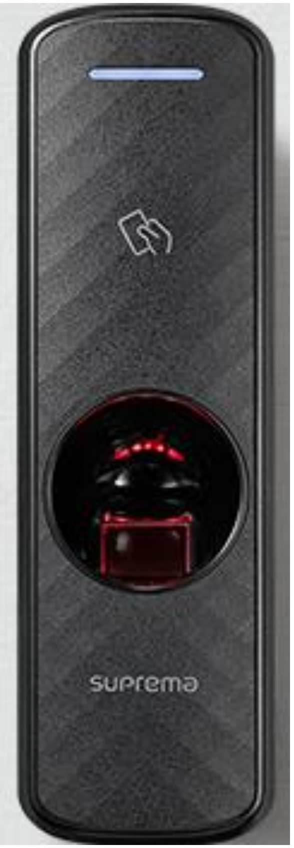
Tamper

Battery
(Local purchase required)

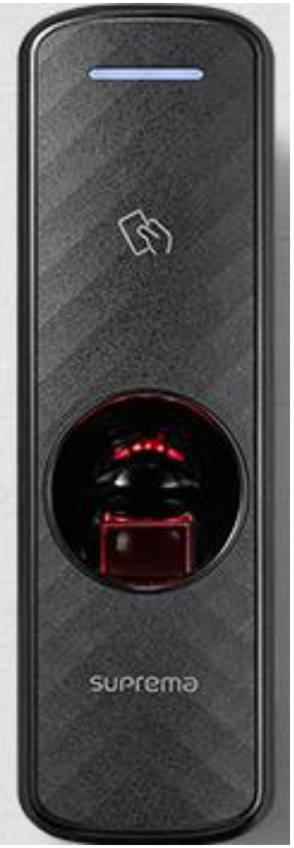
PSU & Power Distribution board
*Lock DC power can be provided

Knowledge Check

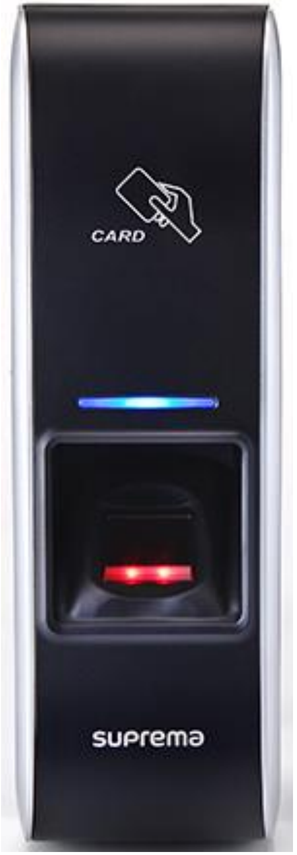
Which product is BioEntry R2?



[✓ A]

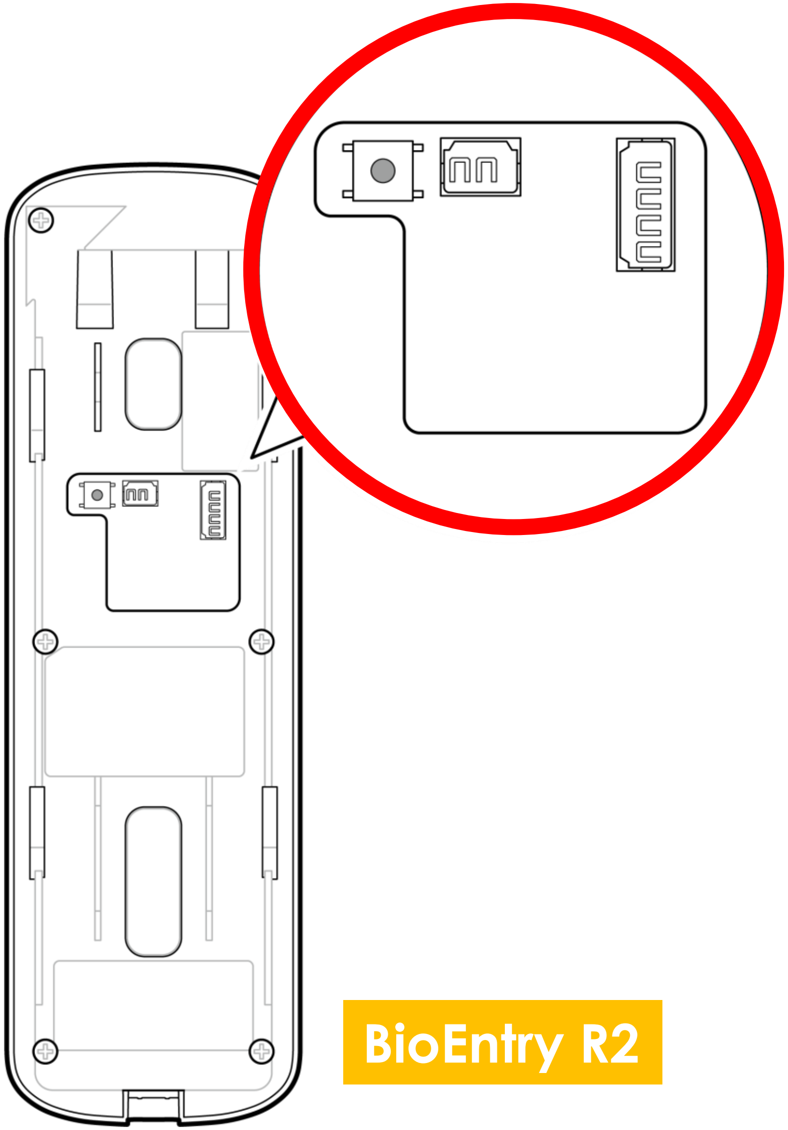


[✓ B]

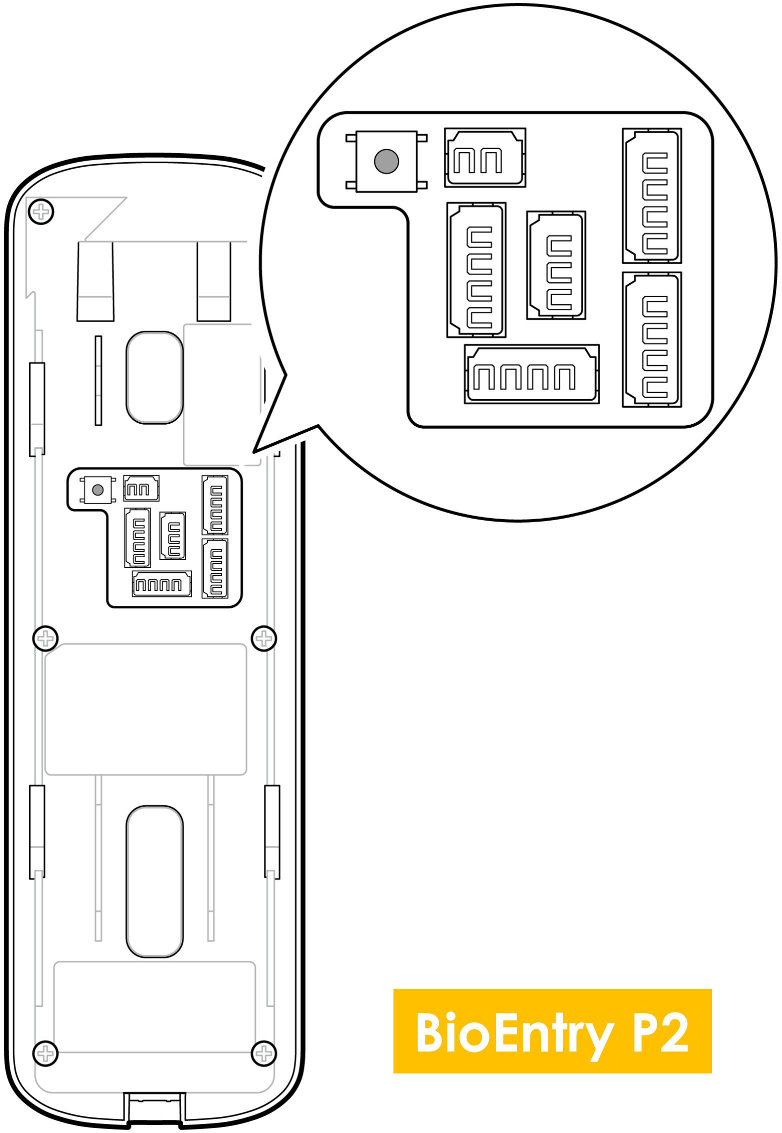


C

BioEntry R2 & P2



BioEntry R2

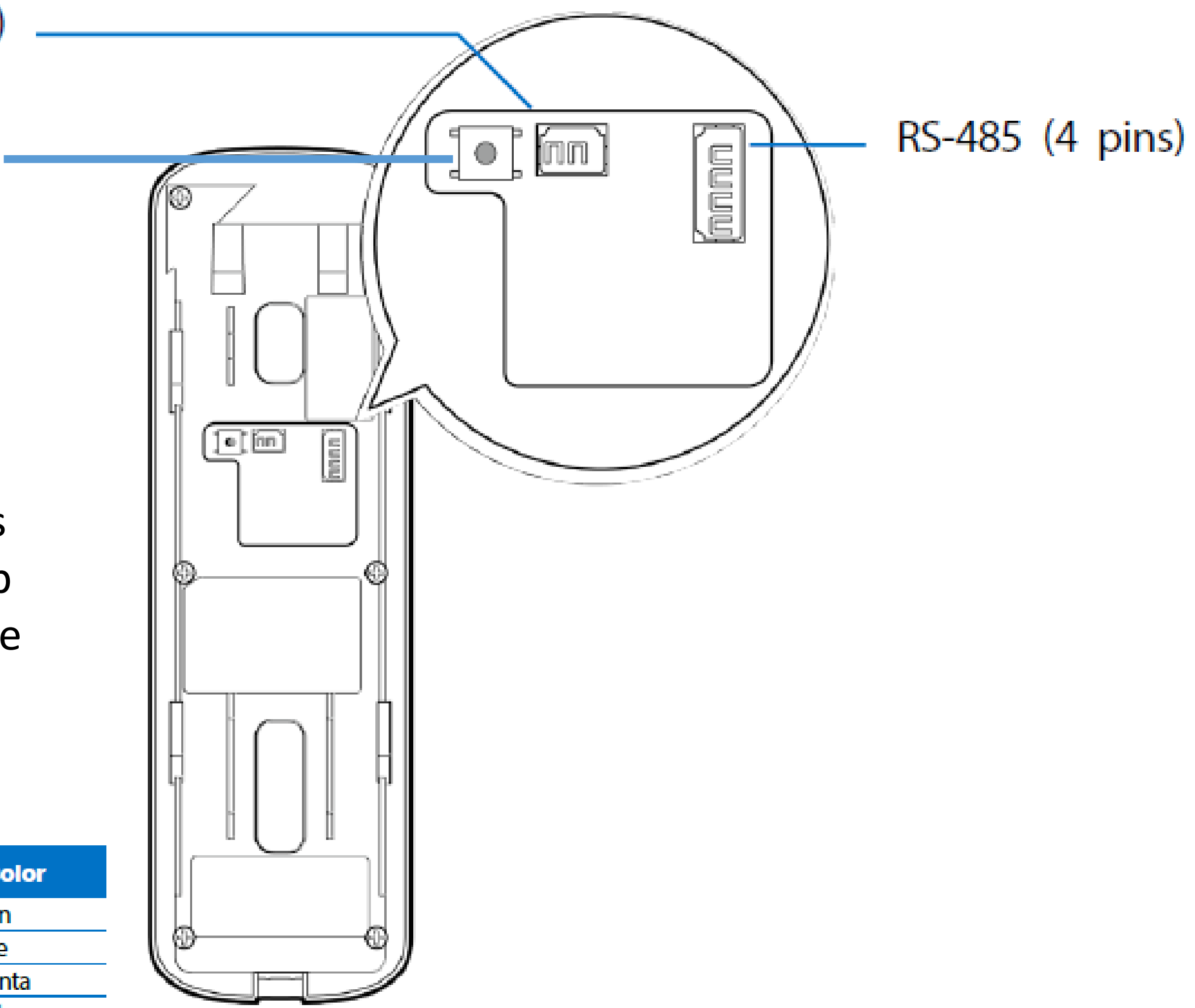


BioEntry P2

BioEntry R2

- For use with Corestation
- Only RS-485 connection
- Same exterior as P2

BioEntry R2



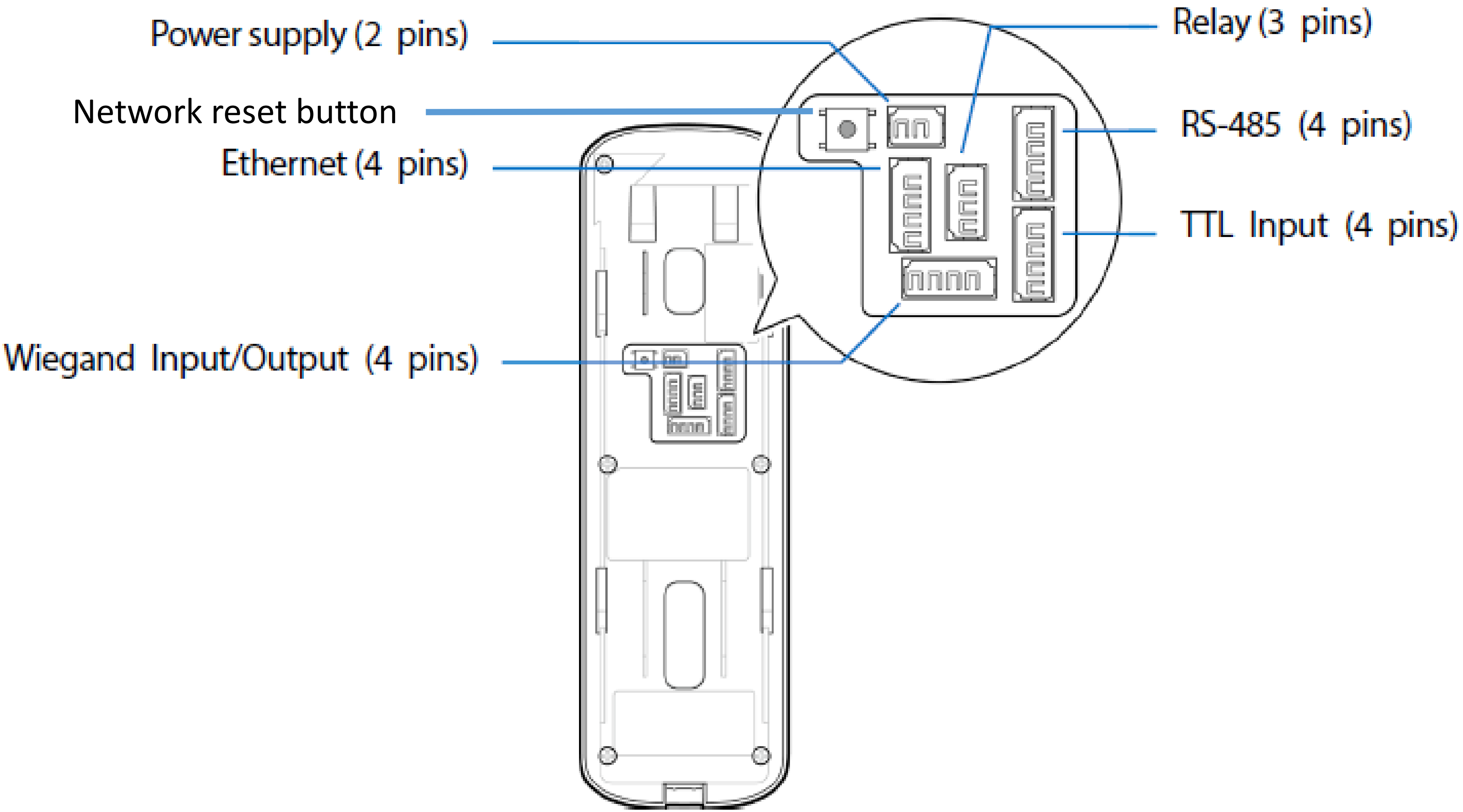
Depending on the number of times the reset button was pressed, the b aud rate changes. You can recognize the baud rate according to the LED color.

The number of times	Baud Rate	LED Color
1	9600	Cyan
2	19200	Blue
3	38400	Magenta
4	57600	White
5	115200	Red

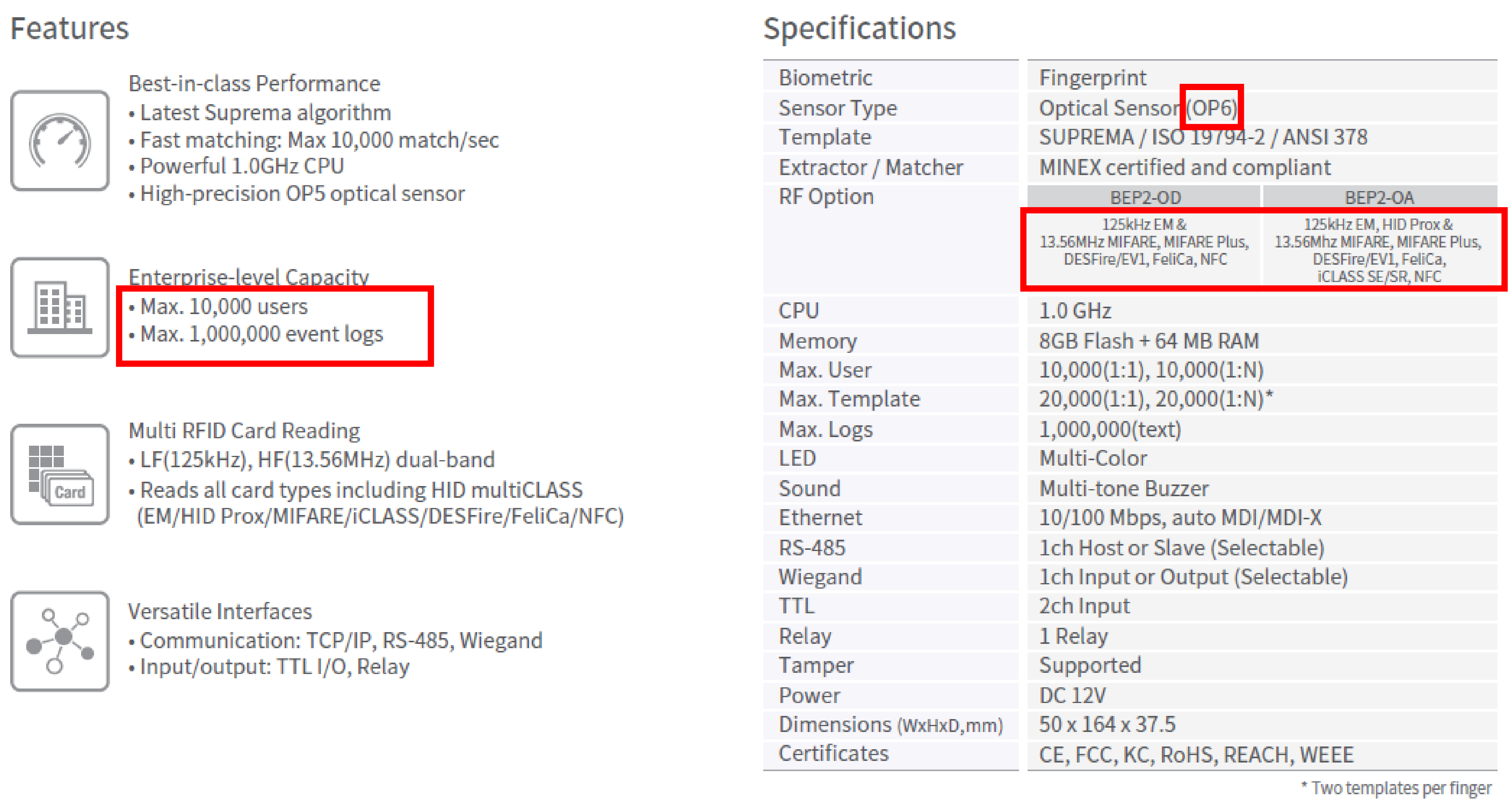
BioEntry P2

- Next model of BioEntry Plus
- 10,000 match/sec
- Max 10,000 users

BioEntry P2


Power supply (2 pins)
Network reset button
Ethernet (4 pins)
Wiegand Input/Output (4 pins)
Relay (3 pins)
RS-485 (4 pins)
TTL Input (4 pins)

BioEntry P2



Features

Best-in-class Performance

- Latest Suprema algorithm
- Fast matching: Max 10,000 match/sec
- Powerful 1.0GHz CPU
- High-precision OP5 optical sensor

Enterprise-level Capacity

- Max. 10,000 users
- Max. 1,000,000 event logs

Multi RFID Card Reading

- LF(125kHz), HF(13.56MHz) dual-band
- Reads all card types including HID multiCLASS (EM/HID Prox/MIFARE/iCLASS/DESFire/FeliCa/NFC)

Versatile Interfaces

- Communication: TCP/IP, RS-485, Wiegand
- Input/output: TTL I/O, Relay

Specifications

Biometric	Fingerprint	
Sensor Type	Optical Sensor (OP6)	
Template	SUPREMA / ISO 19794-2 / ANSI 378	
Extractor / Matcher	MINEX certified and compliant	
RF Option	BEP2-OD	BEP2-OA
	125kHz EM & 13.56MHz MIFARE, MIFARE Plus, DESFire/EV1, FeliCa, NFC	125kHz EM, HID Prox & 13.56Mhz MIFARE, MIFARE Plus, DESFire/EV1, FeliCa, iCLASS SE/SR, NFC
CPU	1.0 GHz	
Memory	8GB Flash + 64 MB RAM	
Max. User	10,000(1:1), 10,000(1:N)	
Max. Template	20,000(1:1), 20,000(1:N)*	
Max. Logs	1,000,000(text)	
LED	Multi-Color	
Sound	Multi-tone Buzzer	
Ethernet	10/100 Mbps, auto MDI/MDI-X	
RS-485	1ch Host or Slave (Selectable)	
Wiegand	1ch Input or Output (Selectable)	
TTL	2ch Input	
Relay	1 Relay	
Tamper	Supported	
Power	DC 12V	
Dimensions (WxHxD,mm)	50 x 164 x 37.5	
Certificates	CE, FCC, KC, RoHS, REACH, WEEE	

* Two templates per finger

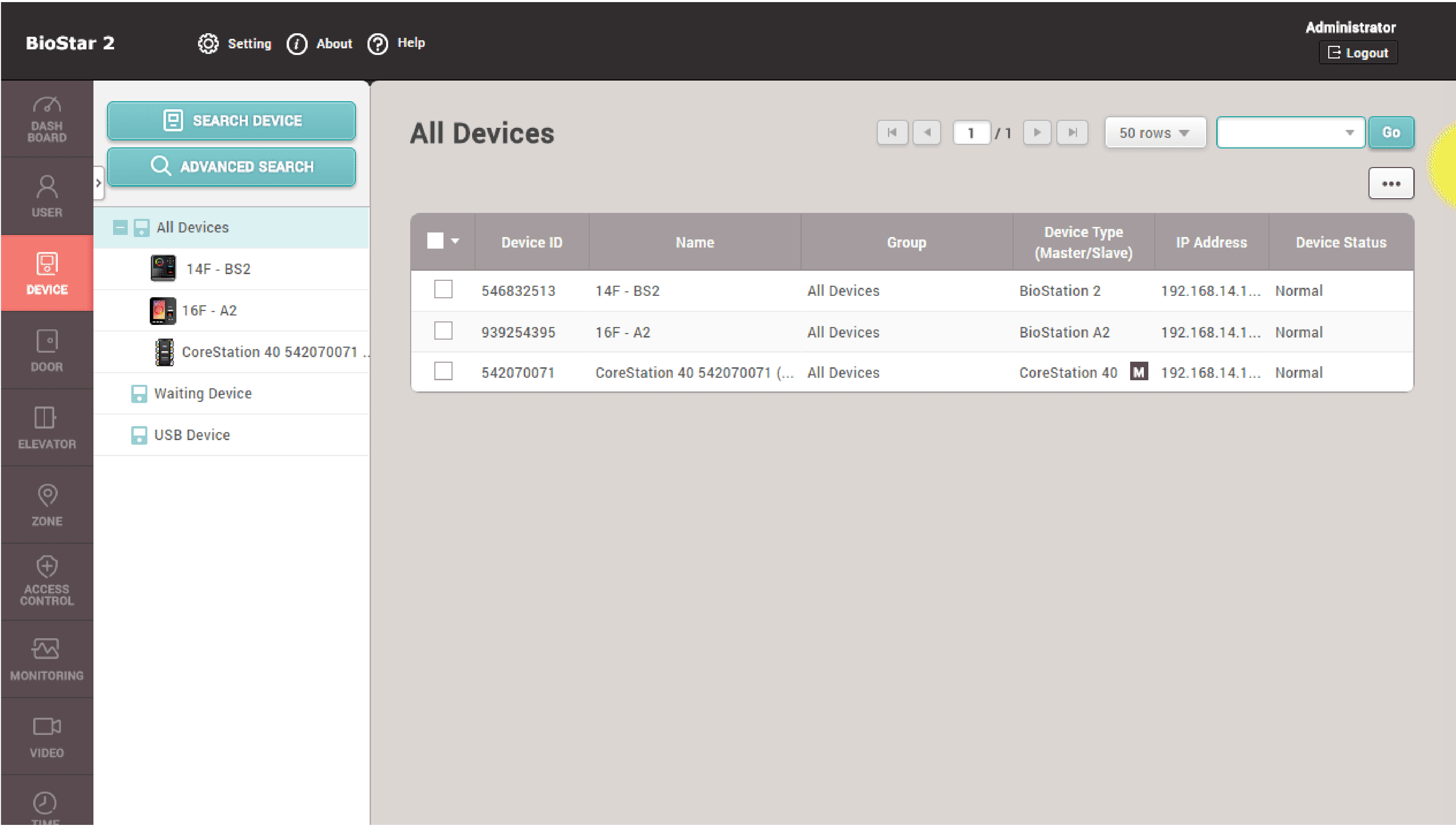
Spec Comparison I

Category		BioEntry P2 BEP2–OD	BioEntry P2 BEP2–OA	BioEntry R2 BER2–OD
Dimension		50 x 164 x 37.5	50 x 164 x 37.5	50 x 164 x 37.5
Memory(RAM)		64MByte	64MByte	32MByte
Storage(Flash)		2GByte	2GByte	32MByte
Finger Detect		O	O	O
Finger Matching		O	O	X
Finger Print	Sensor	OP6	OP6	OP6
RF Card	Mifare	O	O	O
	FeliCa	O	O	O
	iClass	X	O	X
	EM	O	O	O
	HID Prox	X	O	X
I/O	WIEGAND	In/Out - 1port	In/Out - 1port	X
	TTL	Input 2 port	Input 2 port	X
	Relay	1 ch(1A)	1 ch(1A)	X
Operating Temp.		-20 ~ +50 ℃	-20 ~ +50 ℃	-20 ~ +50 ℃
Sound	Alert	Buzzer	Buzzer	Buzzer
	VoIP	X	X	X
	Interphone	X	X	X
Certifications		KC/CE/FCC/RoHS/REACH/WEEE	KC/CE/FCC/RoHS/REACH/WEEE	KC/CE/FCC/RoHS/REACH/WEEE
Comm	Ethernet	O	O	X
	RS485	1 ch	1 ch	1 ch

Spec Comparison II

		BioEntry P2		BioEntry R2
		BEP2-OD	BEP2-OA	BER2-OD
Finger Matching		O	O	X
RF	Mifare, Felica	○	○	○
	iClass	X	○	X
	EM	○	○	○
	HID	X	○	X
IO	Wiegand	○	○	X
	INPUT	2 INPUT	2 INPUT	X
	Relay	○	○	X
Comm.	Ethernet	○	○	X
	RS485	1 CH	1 CH	1 CH

Demo.

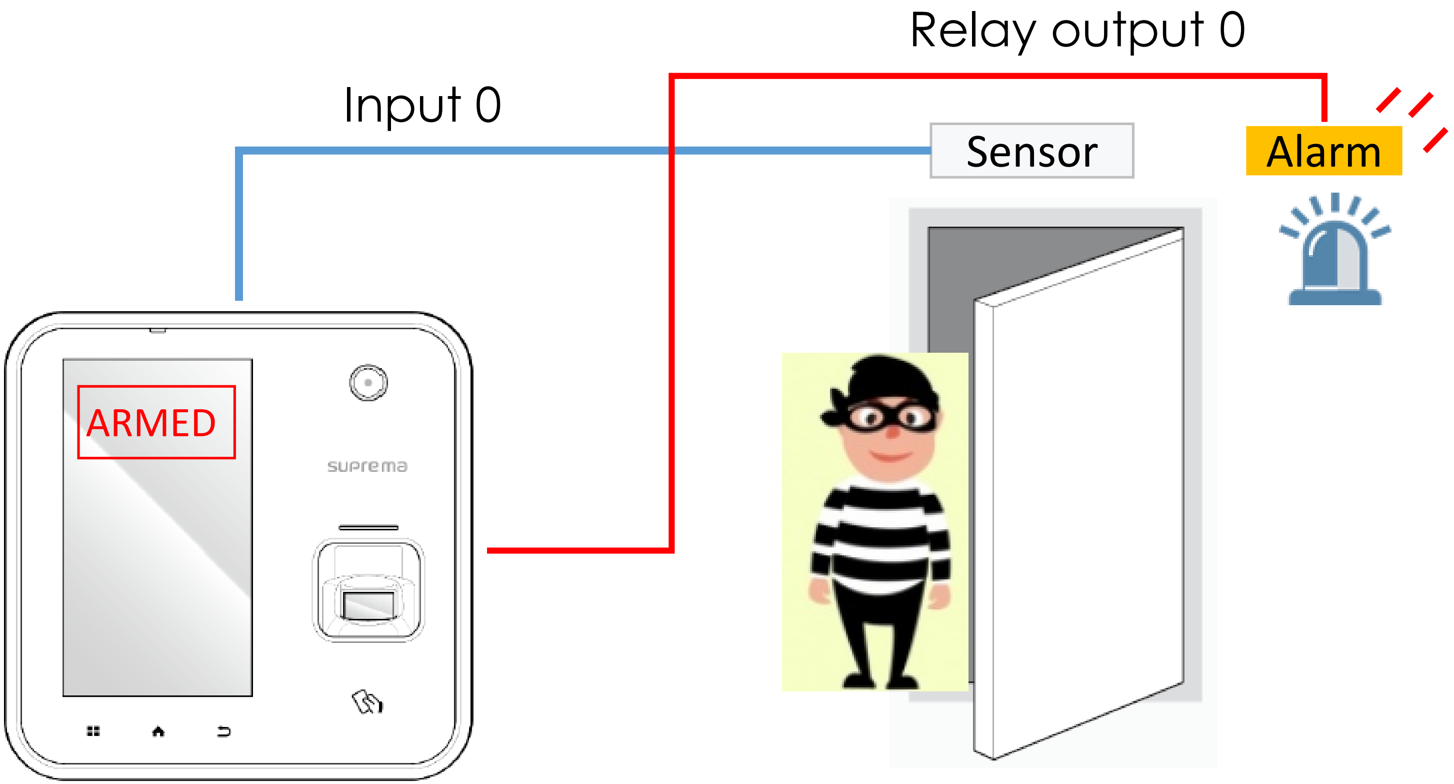


All Devices

□	Device ID	Name	Group	Device Type (Master/Slave)	IP Address	Device Status
□	546832513	14F - BS2	All Devices	BioStation 2	192.168.14.1...	Normal
□	939254395	16F - A2	All Devices	BioStation A2	192.168.14.1...	Normal
□	542070071	CoreStation 40 542070071 (...	All Devices	CoreStation 40 M	192.168.14.1...	Normal

Alarm Zone

- Zone for sensing intrusion with the sensor on armed status

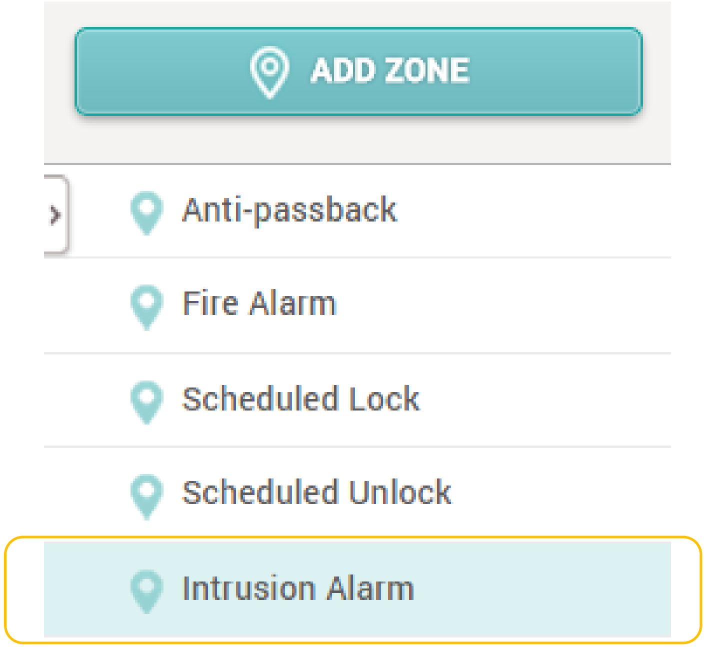


Thief icon designed by All-Free-Download.Com

Alarm Zone

- Initially supported devices: BS2, A2, CoreStation, P2, R2
- Supported in the future: L2, W2, FS2
  * entry devices are not supported
- Only local zone (RS-485) is supported for now

* BS2 and A2 are available to download from Suprema website.

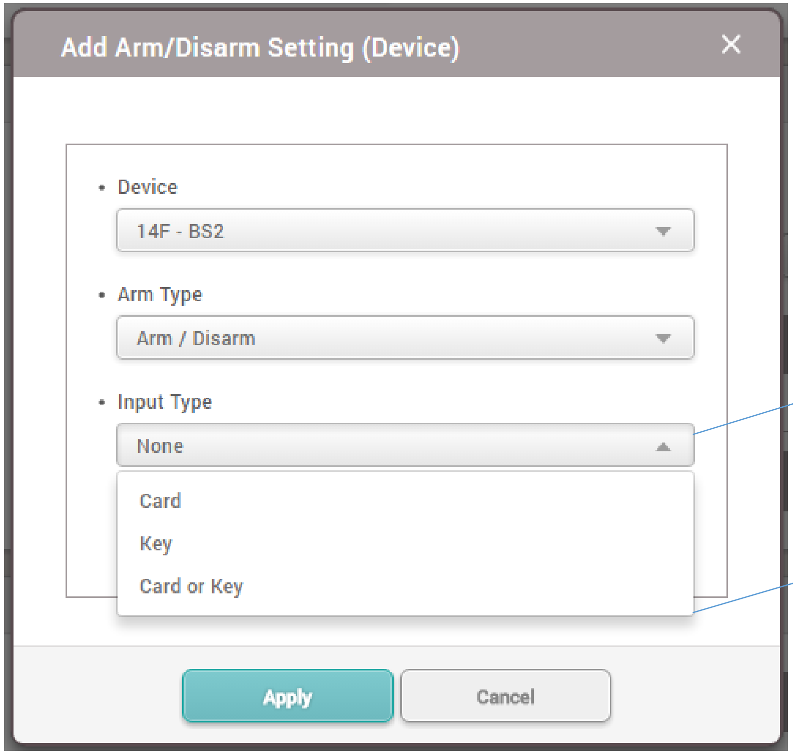


Supported firmware list

BioStation2 1.5.0
BioStation A2 1.4.0
CoreStation 40 1.0
BioEntry P2 1.0
BioEntry R2 1.0

Alarm Zone

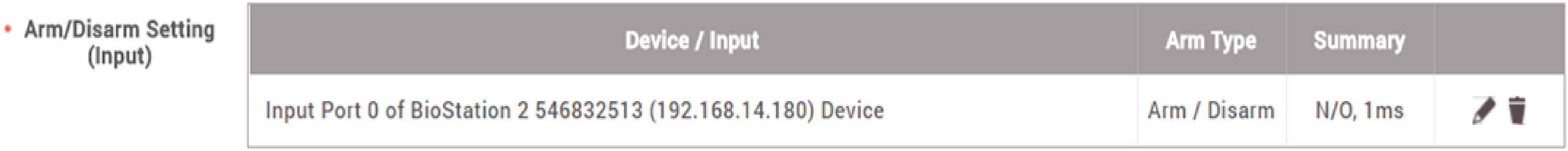
Arm / Disarm Methods



Add Arm/Disarm Setting (Device)

- Device: 14F - BS2
- Arm Type: Arm / Disarm
- Input Type: None

Card
Key
Card or Key

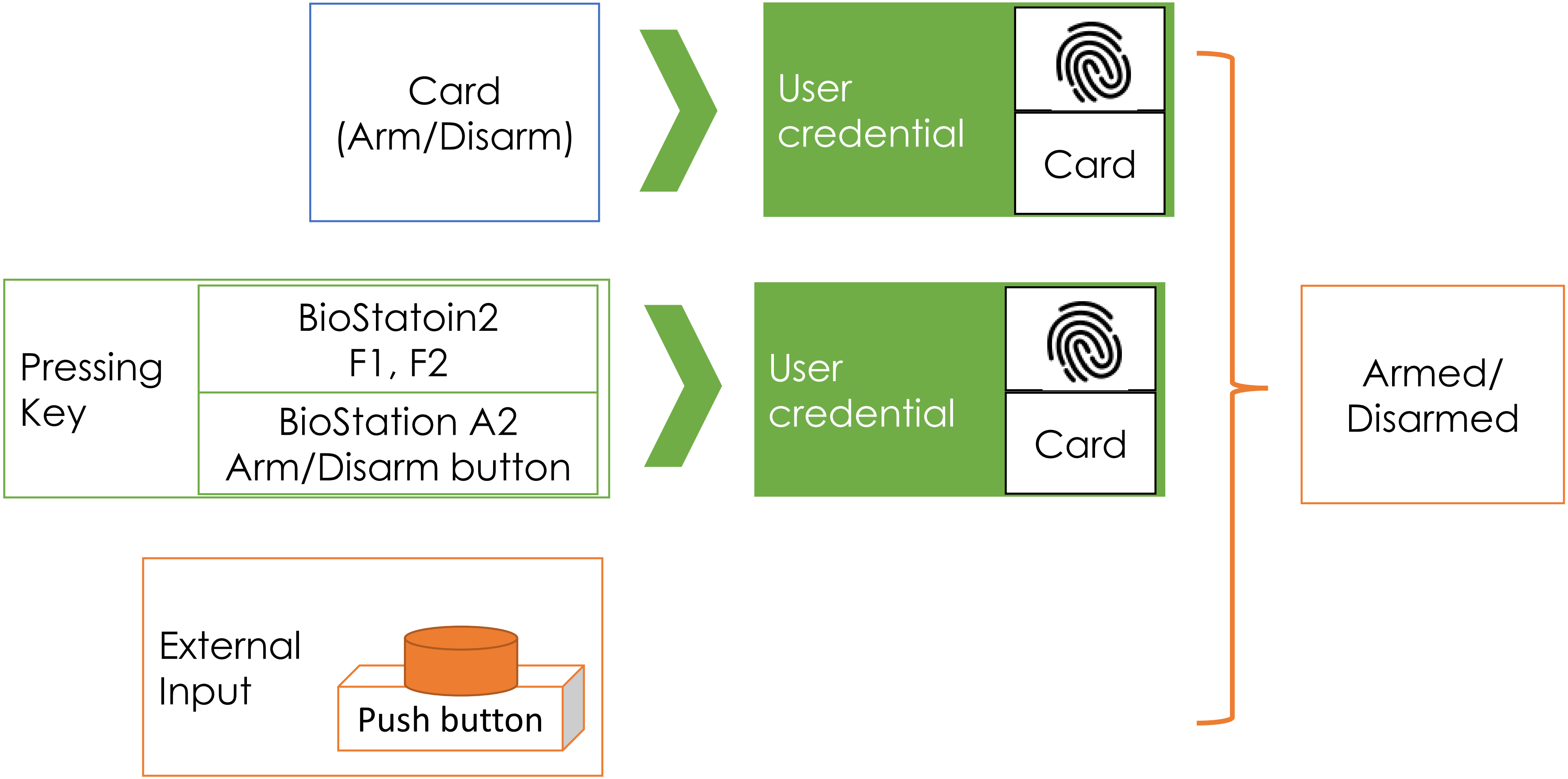


- Arm/Disarm Setting (Input)

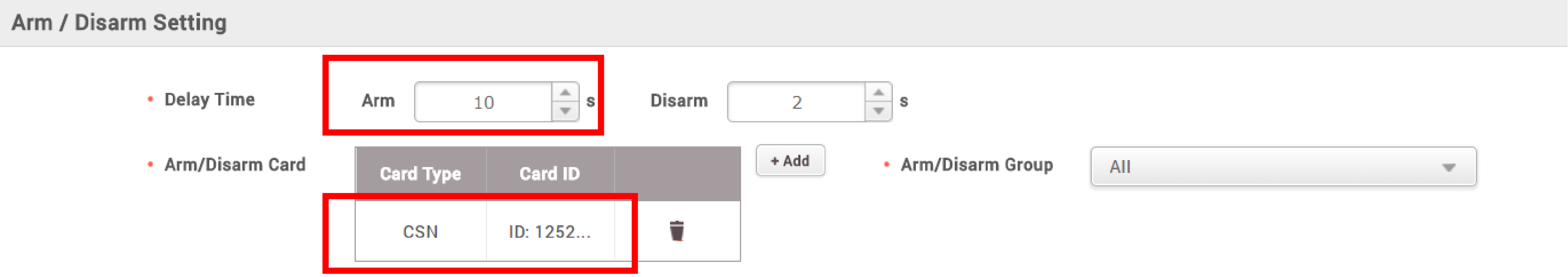
Device / Input	Arm Type	Summary	
Input Port 0 of BioStation 2 546832513 (192.168.14.180) Device	Arm / Disarm	N/O, 1ms	

Alarm Zone

Arm / Disarm Methods



Alarm Zone

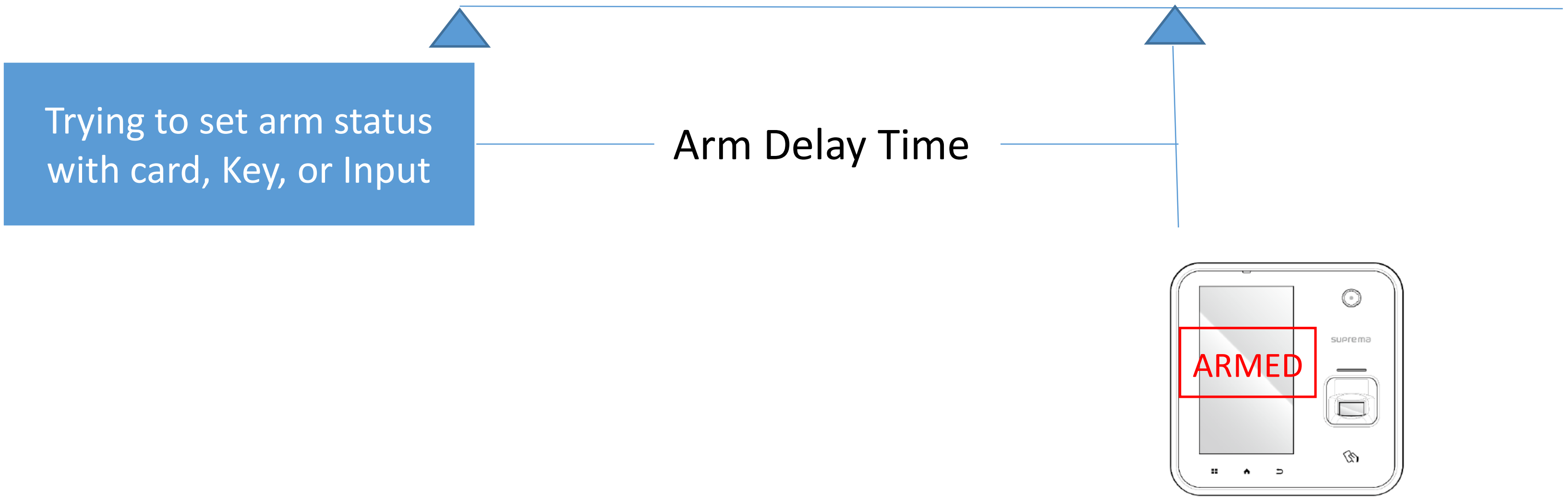


Arm / Disarm Setting

- Delay Time: Arm 10 s Disarm 2 s
- Arm/Disarm Card: + Add

Card Type	Card ID
CSN	ID: 1252...

- Arm/Disarm Group: All

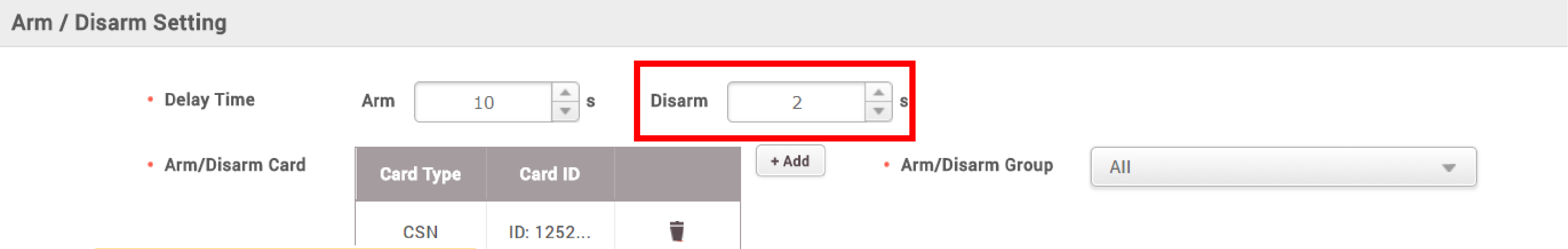


Trying to set arm status with card, Key, or Input

Arm Delay Time

You can't assign same Arm/Disam card to another Alarm Zone.

Alarm Zone



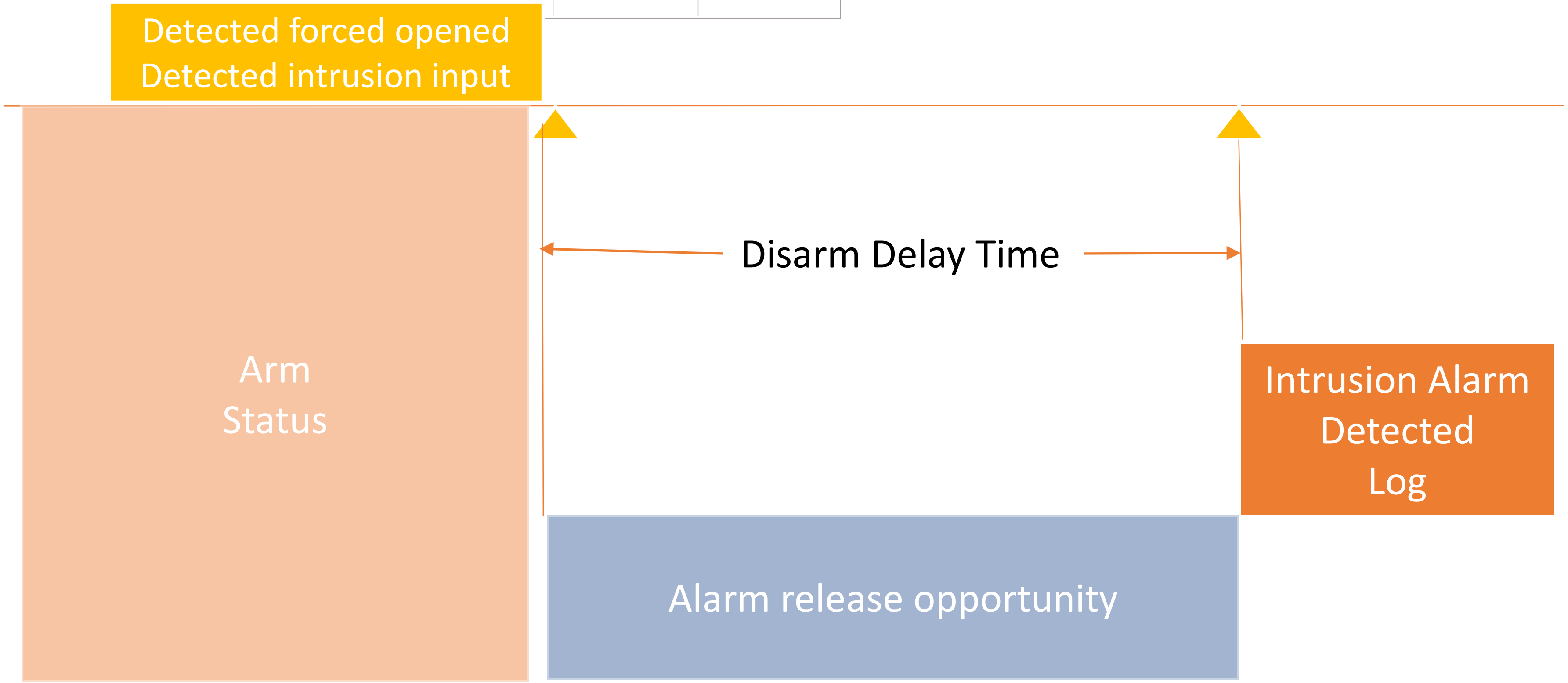
Arm / Disarm Setting

- Delay Time: Arm 10 s, Disarm 2 s
- Arm/Disarm Card

Card Type	Card ID	
CSN	ID: 1252...	

+ Add

- Arm/Disarm Group: All



Detected forced opened
Detected intrusion input

Arm
Status

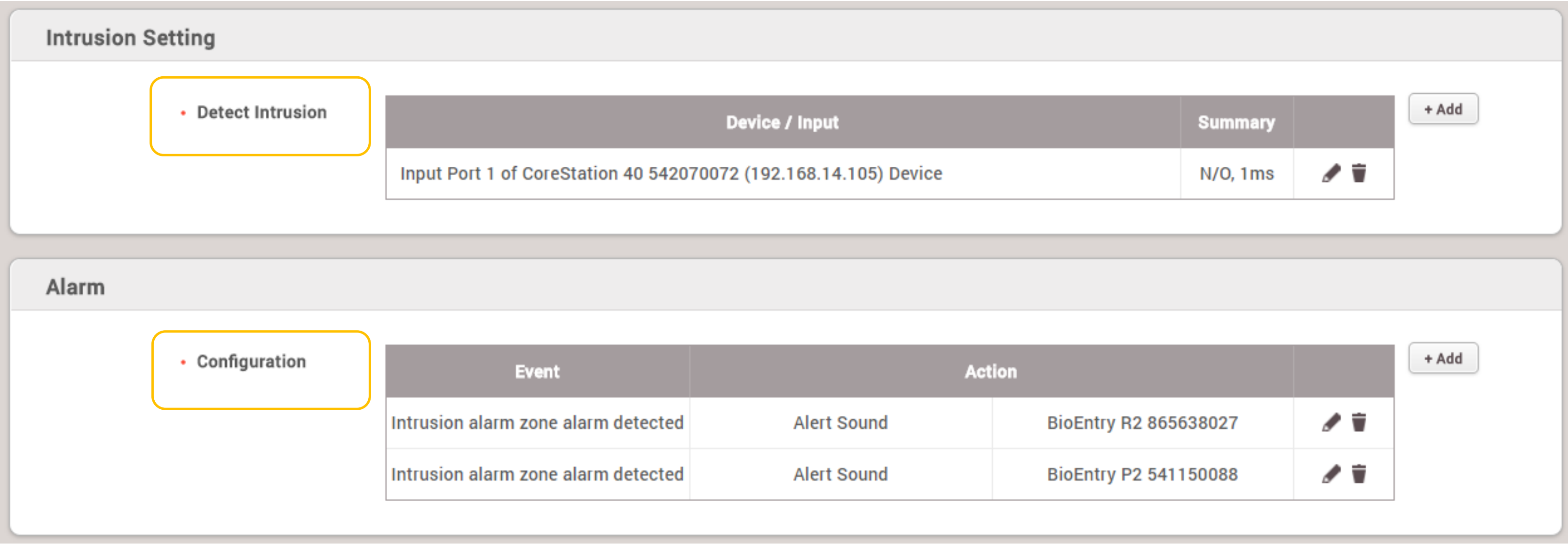
Disarm Delay Time

Intrusion Alarm
Detected
Log

Alarm release opportunity

Alarm Zone

- Input or door sensor can be used to detect intrusion
- Alarm action (output / sound) configurable based on various alarm events



Intrusion Setting

• Detect Intrusion

Device / Input	Summary	
Input Port 1 of CoreStation 40 542070072 (192.168.14.105) Device	N/O, 1ms	

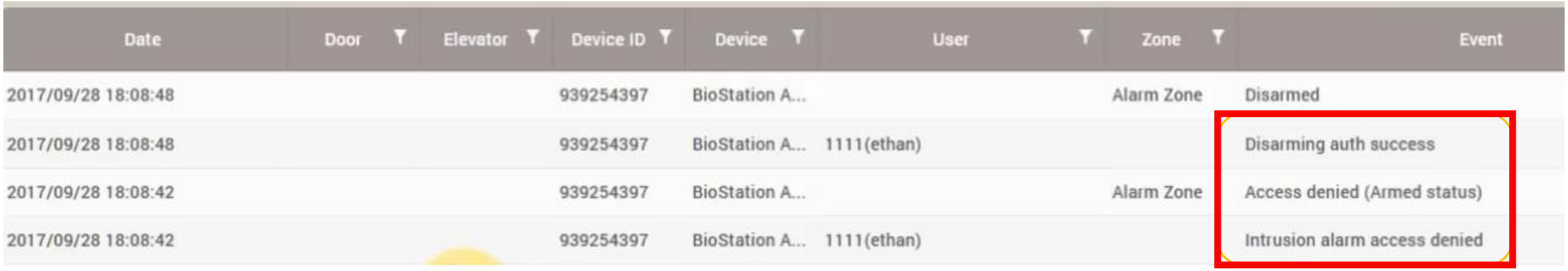
+ Add

Alarm

• Configuration

Event	Action		
Intrusion alarm zone alarm detected	Alert Sound	BioEntry R2 865638027	
Intrusion alarm zone alarm detected	Alert Sound	BioEntry P2 541150088	

+ Add



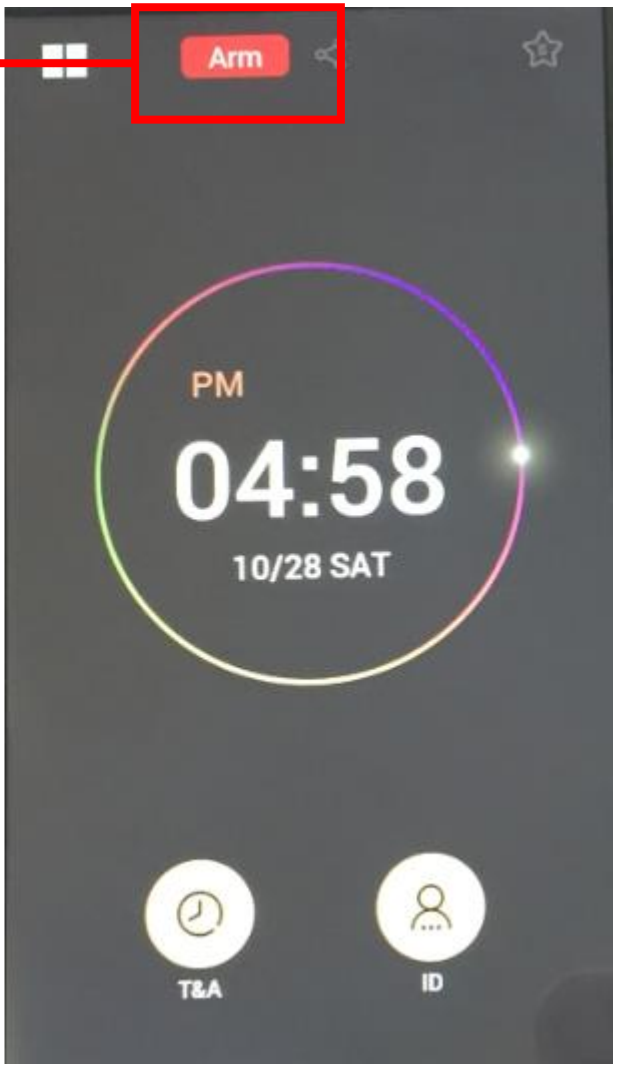
Date	Door	Elevator	Device ID	Device	User	Zone	Event
2017/09/28 18:08:48			939254397	BioStation A...		Alarm Zone	Disarmed
2017/09/28 18:08:48			939254397	BioStation A...	1111(ethan)		Disarming auth success
2017/09/28 18:08:42			939254397	BioStation A...		Alarm Zone	Access denied (Armed status)
2017/09/28 18:08:42			939254397	BioStation A...	1111(ethan)		Intrusion alarm access denied

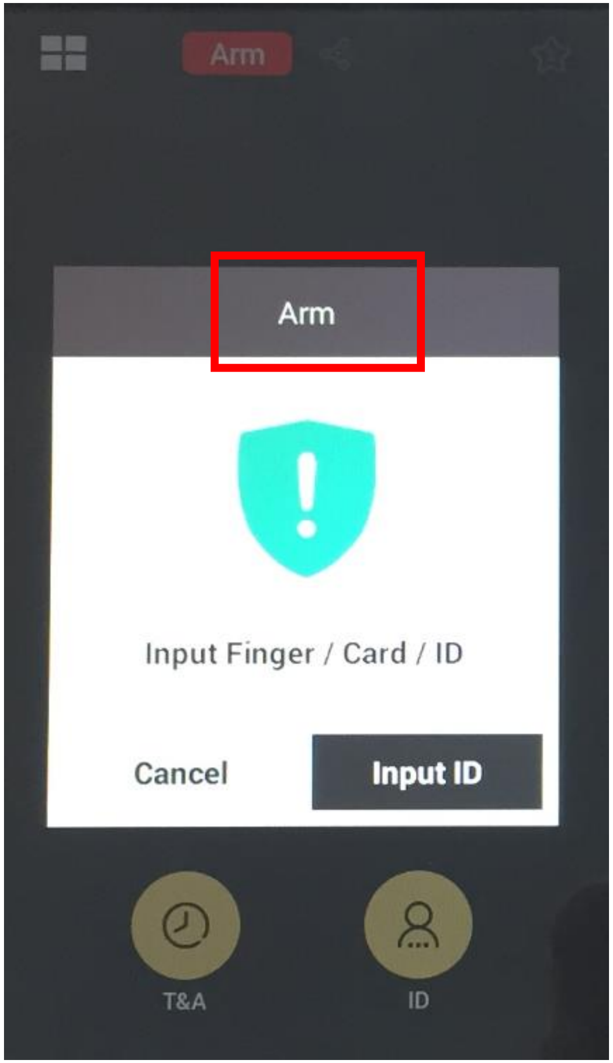
On authentication attempt during arm status

Alarm Zone

BioStation A2

Arm

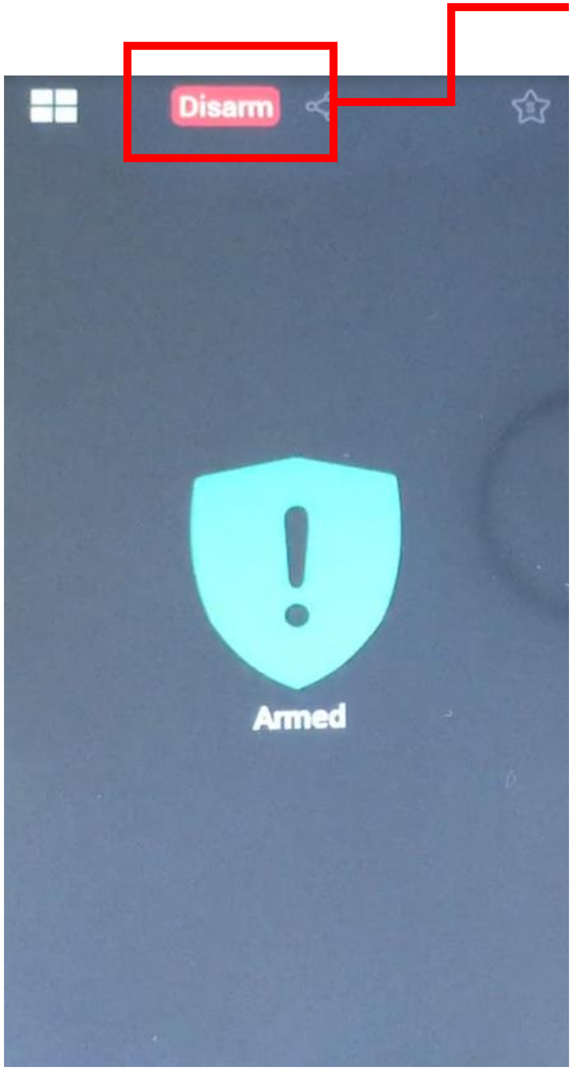




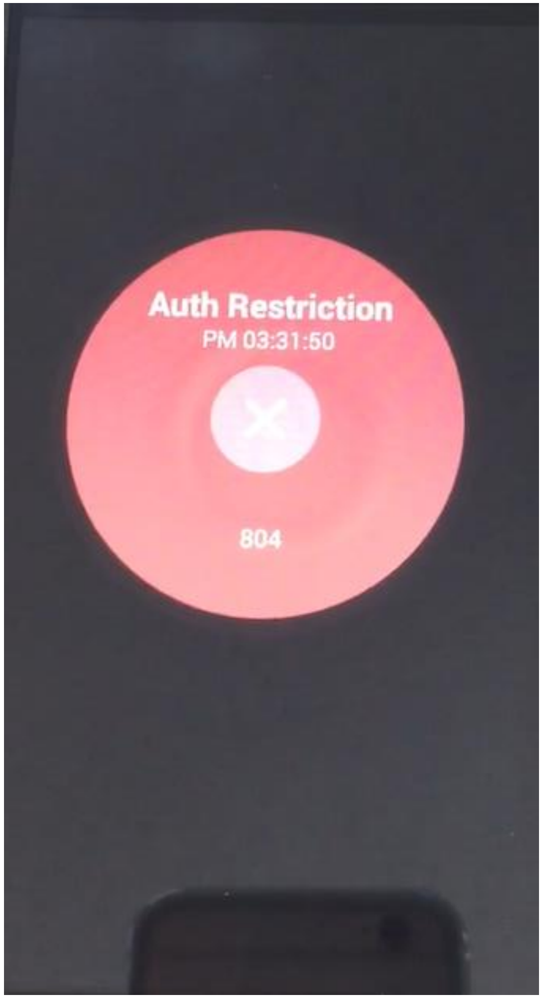
Input Finger / Card / ID

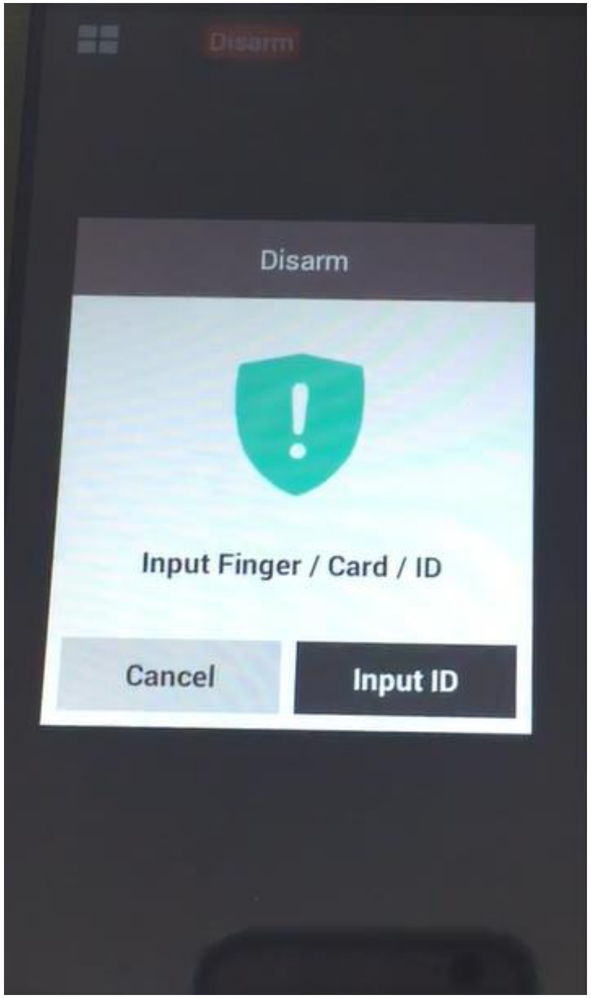
Alarm Zone

BioStation A2



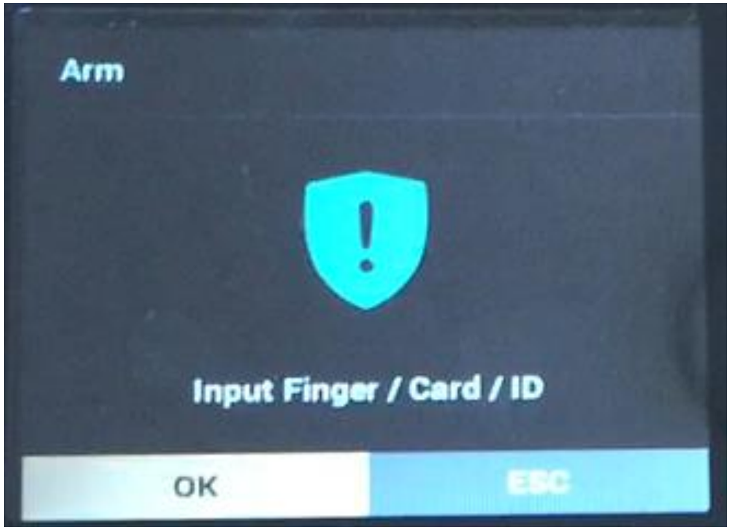
Disarm



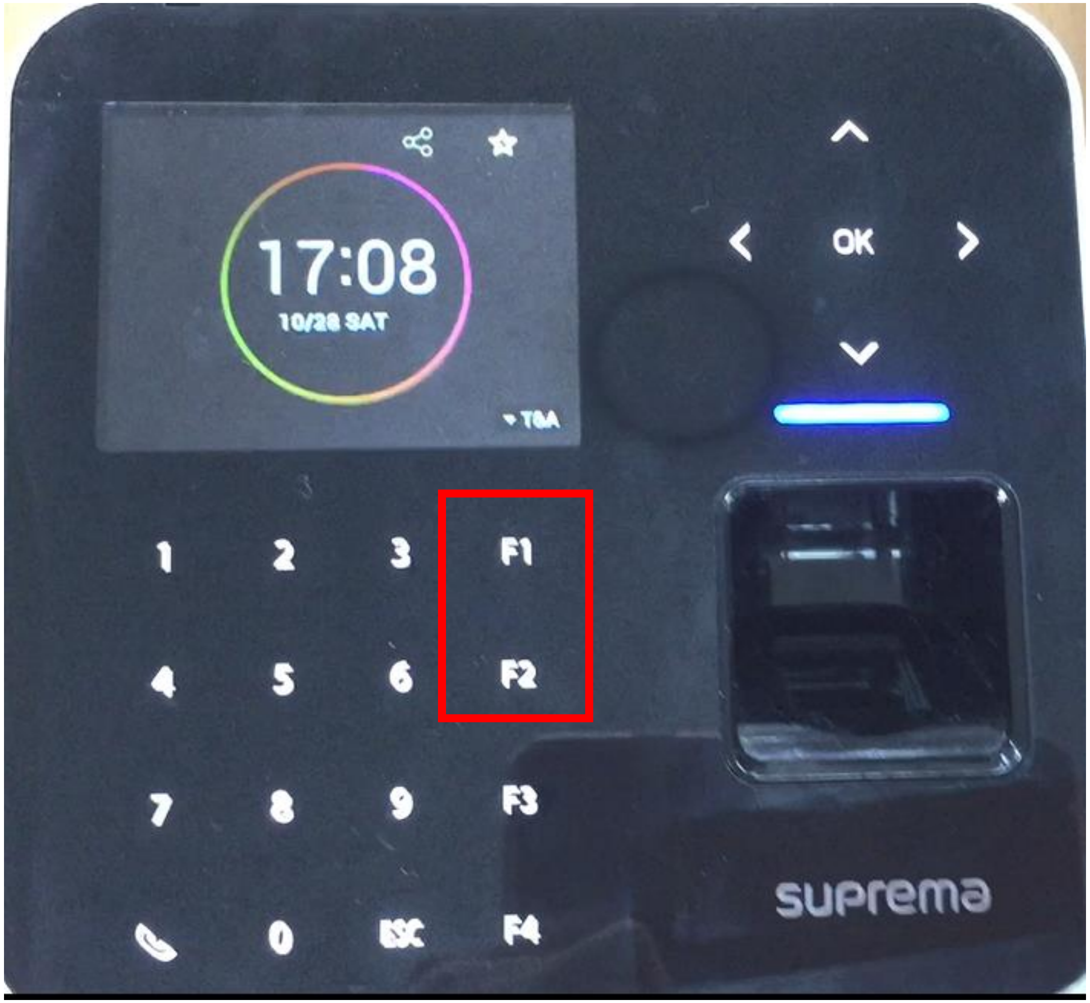


Alarm Zone

BioStation 2


Arm

Input Finger / Card / ID

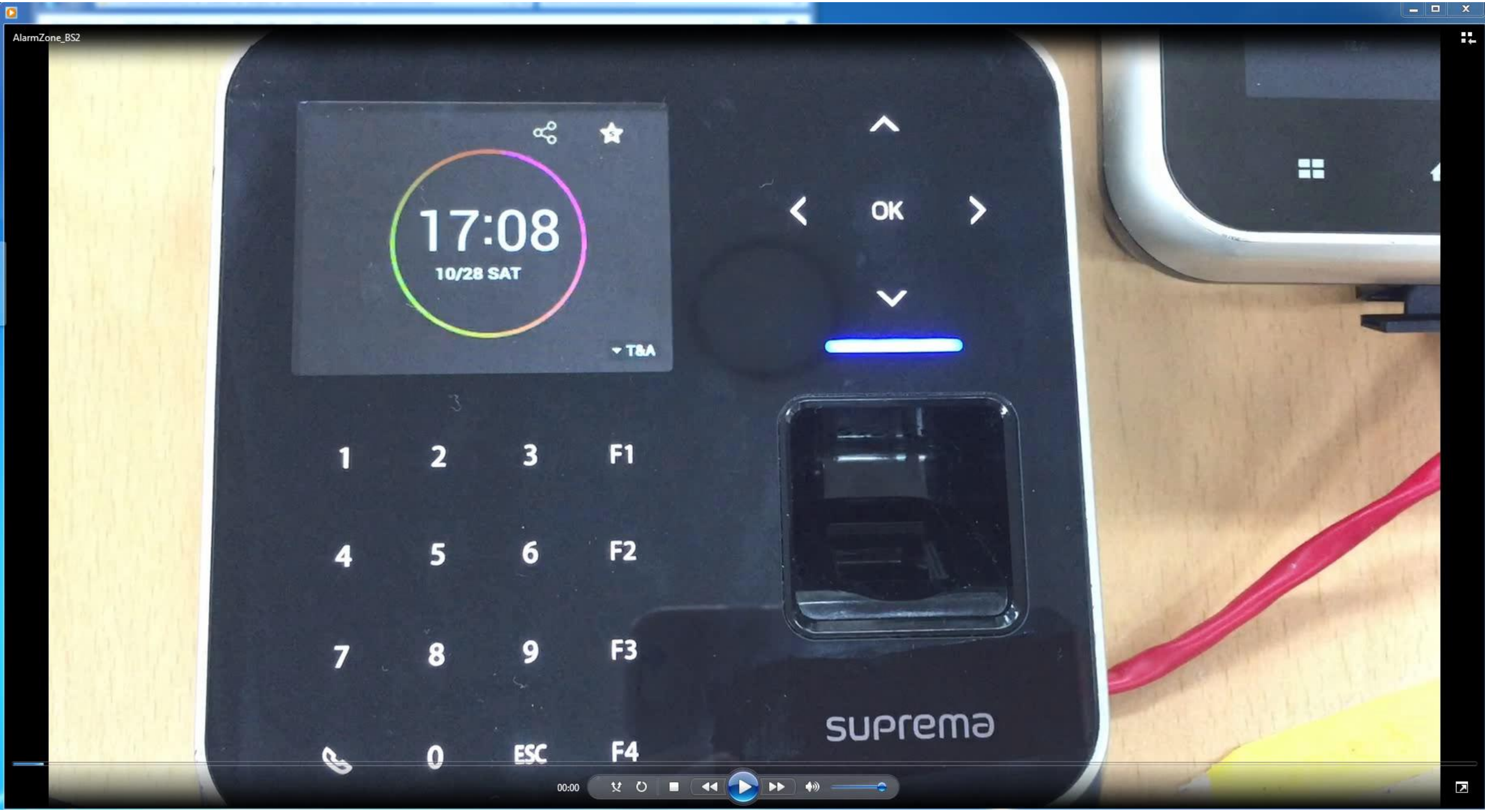


BioStation 2 key below is default key to use Intrusion Alarm Zone

It can be also used as T&A key

F1: Arm Key
(Press and hold F1 till beep sound)
F2: Disarm Key
(Press and hold F2 till beep sound)

Alarm Zone


AlarmZone_BS2
17:08
10/28 SAT
T&A
OK
1
2
3
F1
4
5
6
F2
7
8
9
F3
0
ESC
F4
suprema
00:00

Audit Trail

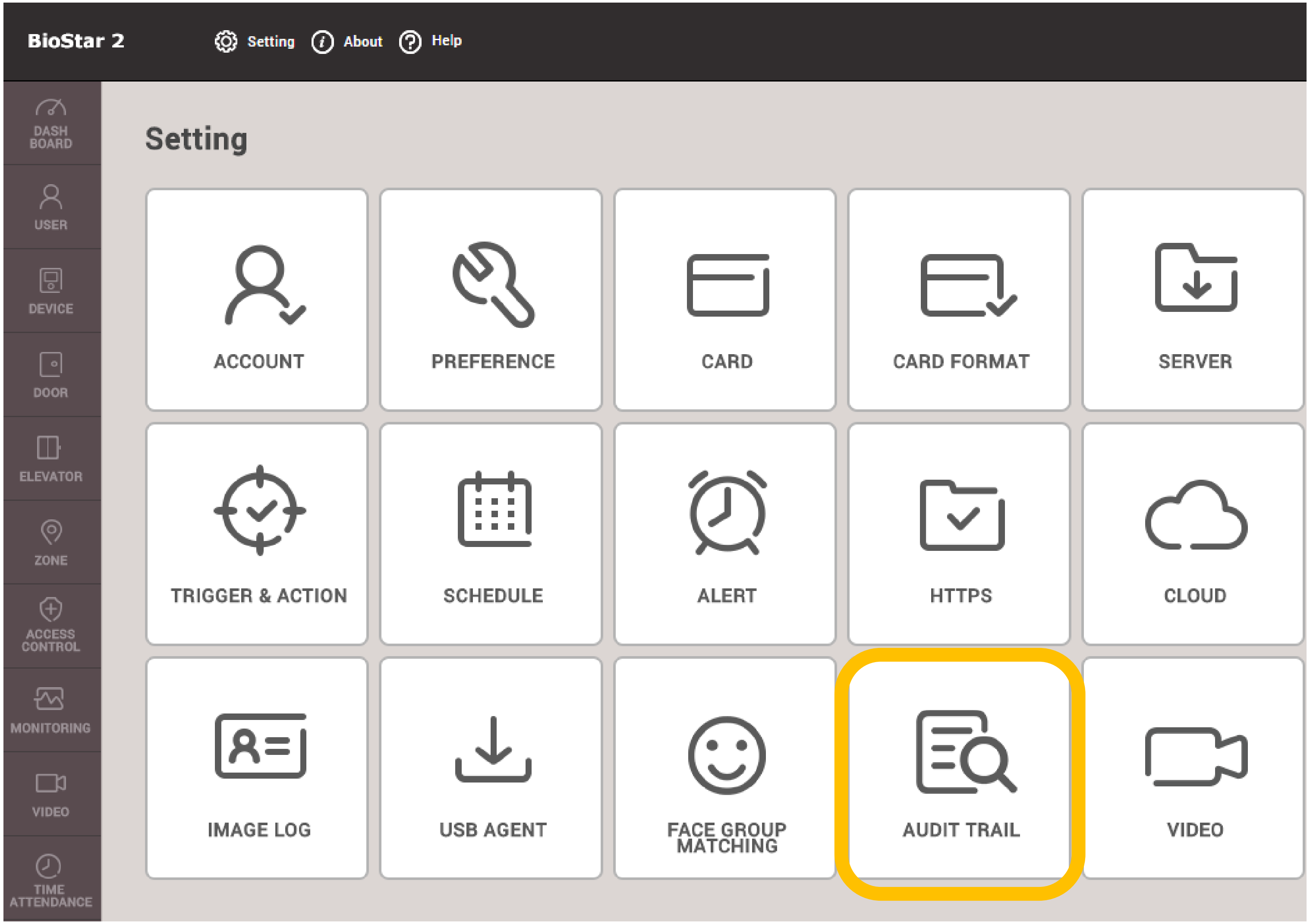
What is Audit Trail of BioStar2?

- Help you to check that which data is created, modified or deleted by the system administrator who login to BioStar 2
- It will not show what value it was changed to

Audit Trail

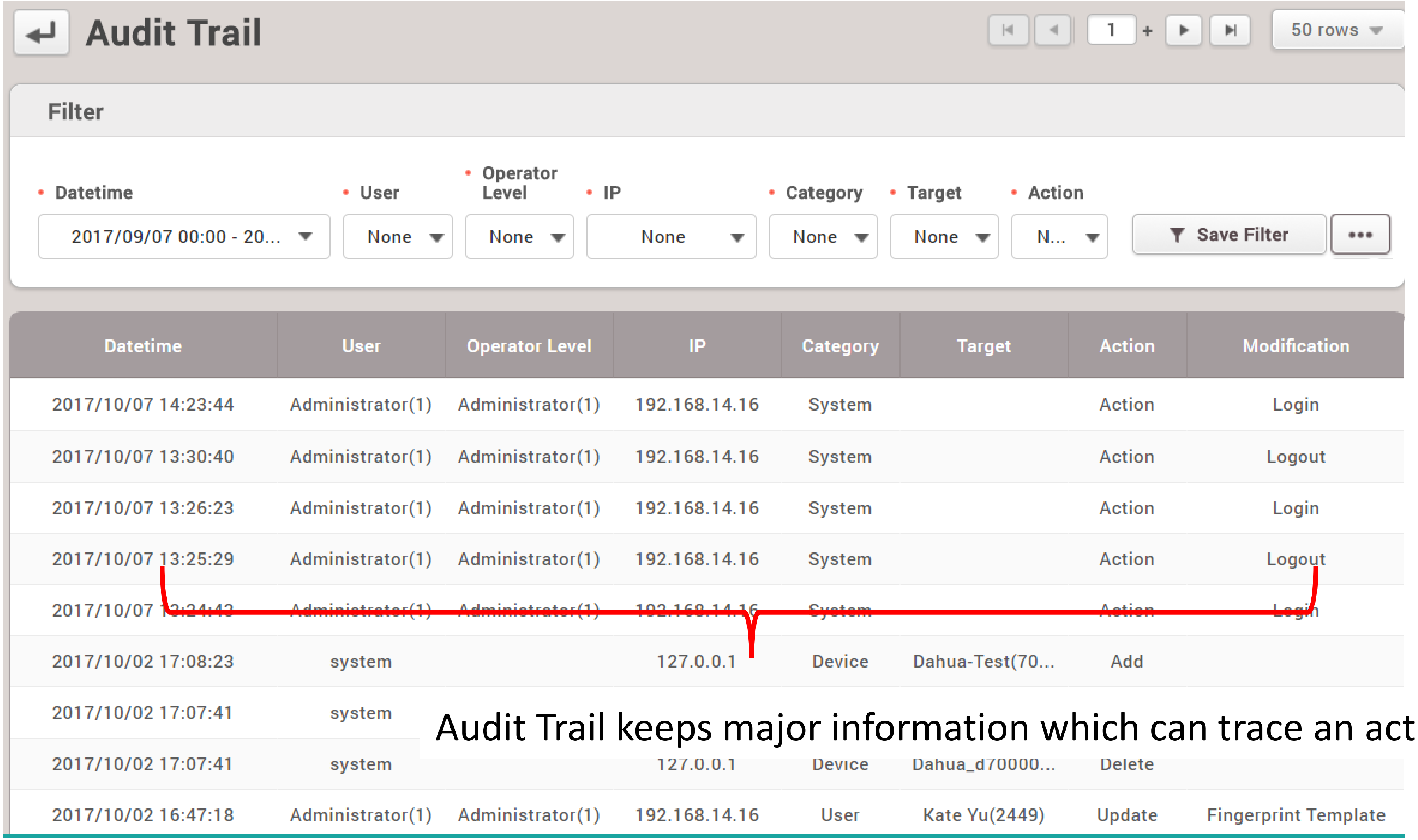
Audit Trail

- Go to Setting>AUDIT TRAIL



Audit Trail

- Check the records from Audit Trail List



Audit Trail

1 + 50 rows

Filter

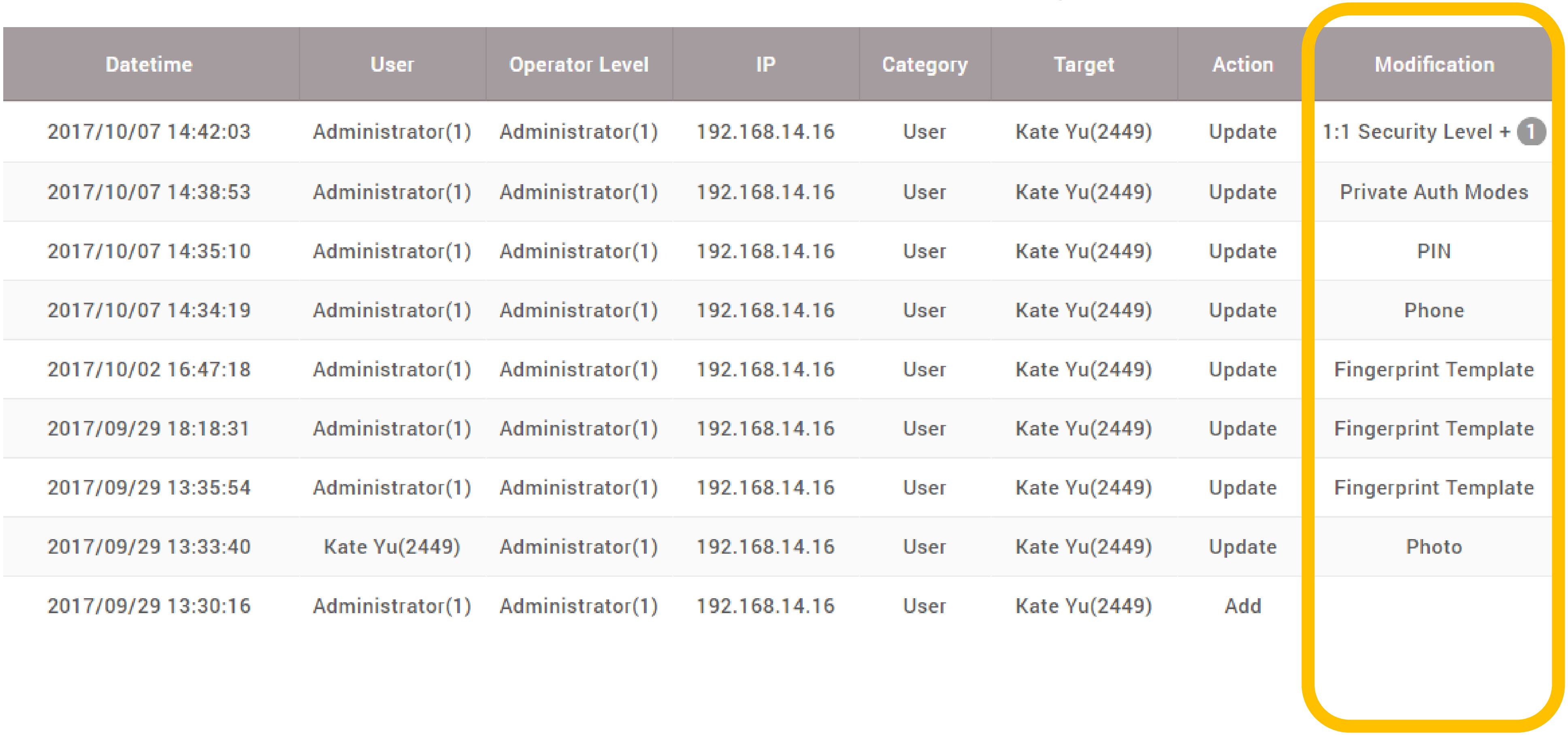
• Datetime	• User	• Operator Level	• IP	• Category	• Target	• Action
2017/09/07 00:00 - 20...	None	None	None	None	None	N...

Datetime	User	Operator Level	IP	Category	Target	Action	Modification
2017/10/07 14:23:44	Administrator(1)	Administrator(1)	192.168.14.16	System		Action	Login
2017/10/07 13:30:40	Administrator(1)	Administrator(1)	192.168.14.16	System		Action	Logout
2017/10/07 13:26:23	Administrator(1)	Administrator(1)	192.168.14.16	System		Action	Login
2017/10/07 13:25:29	Administrator(1)	Administrator(1)	192.168.14.16	System		Action	Logout
2017/10/07 13:24:43	Administrator(1)	Administrator(1)	192.168.14.16	System		Action	Login
2017/10/02 17:08:23	system		127.0.0.1	Device	Dahua-Test(70...	Add	
2017/10/02 17:07:41	system						
2017/10/02 17:07:41	system		127.0.0.1	Device	Dahua_d70000...	Delete	
2017/10/02 16:47:18	Administrator(1)	Administrator(1)	192.168.14.16	User	Kate Yu(2449)	Update	Fingerprint Template

Audit Trail keeps major information which can trace an action

Audit Trail

- Audit trail of Biostar2 is optimized for user changes

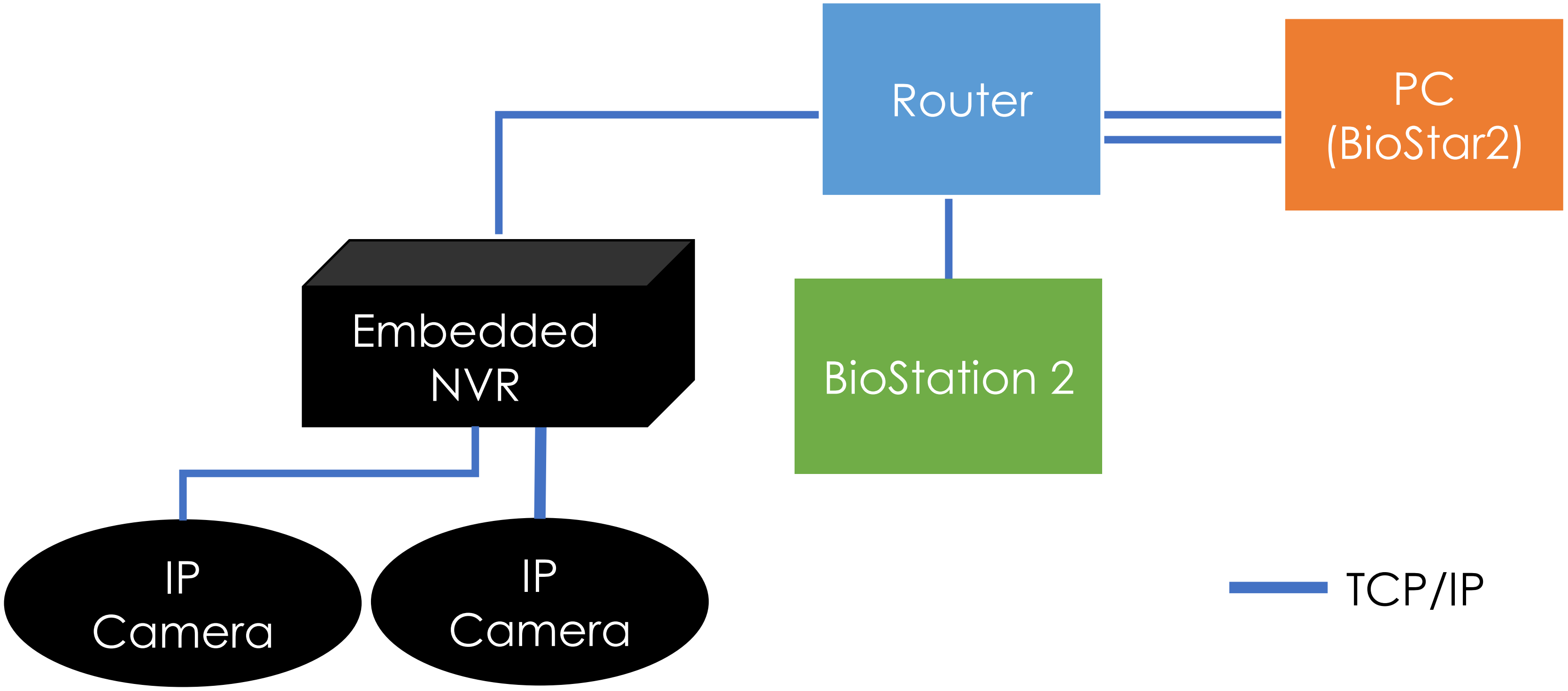


Datetime	User	Operator Level	IP	Category	Target	Action	Modification
2017/10/07 14:42:03	Administrator(1)	Administrator(1)	192.168.14.16	User	Kate Yu(2449)	Update	1:1 Security Level + 1
2017/10/07 14:38:53	Administrator(1)	Administrator(1)	192.168.14.16	User	Kate Yu(2449)	Update	Private Auth Modes
2017/10/07 14:35:10	Administrator(1)	Administrator(1)	192.168.14.16	User	Kate Yu(2449)	Update	PIN
2017/10/07 14:34:19	Administrator(1)	Administrator(1)	192.168.14.16	User	Kate Yu(2449)	Update	Phone
2017/10/02 16:47:18	Administrator(1)	Administrator(1)	192.168.14.16	User	Kate Yu(2449)	Update	Fingerprint Template
2017/09/29 18:18:31	Administrator(1)	Administrator(1)	192.168.14.16	User	Kate Yu(2449)	Update	Fingerprint Template
2017/09/29 13:35:54	Administrator(1)	Administrator(1)	192.168.14.16	User	Kate Yu(2449)	Update	Fingerprint Template
2017/09/29 13:33:40	Kate Yu(2449)	Administrator(1)	192.168.14.16	User	Kate Yu(2449)	Update	Photo
2017/09/29 13:30:16	Administrator(1)	Administrator(1)	192.168.14.16	User	Kate Yu(2449)	Add	

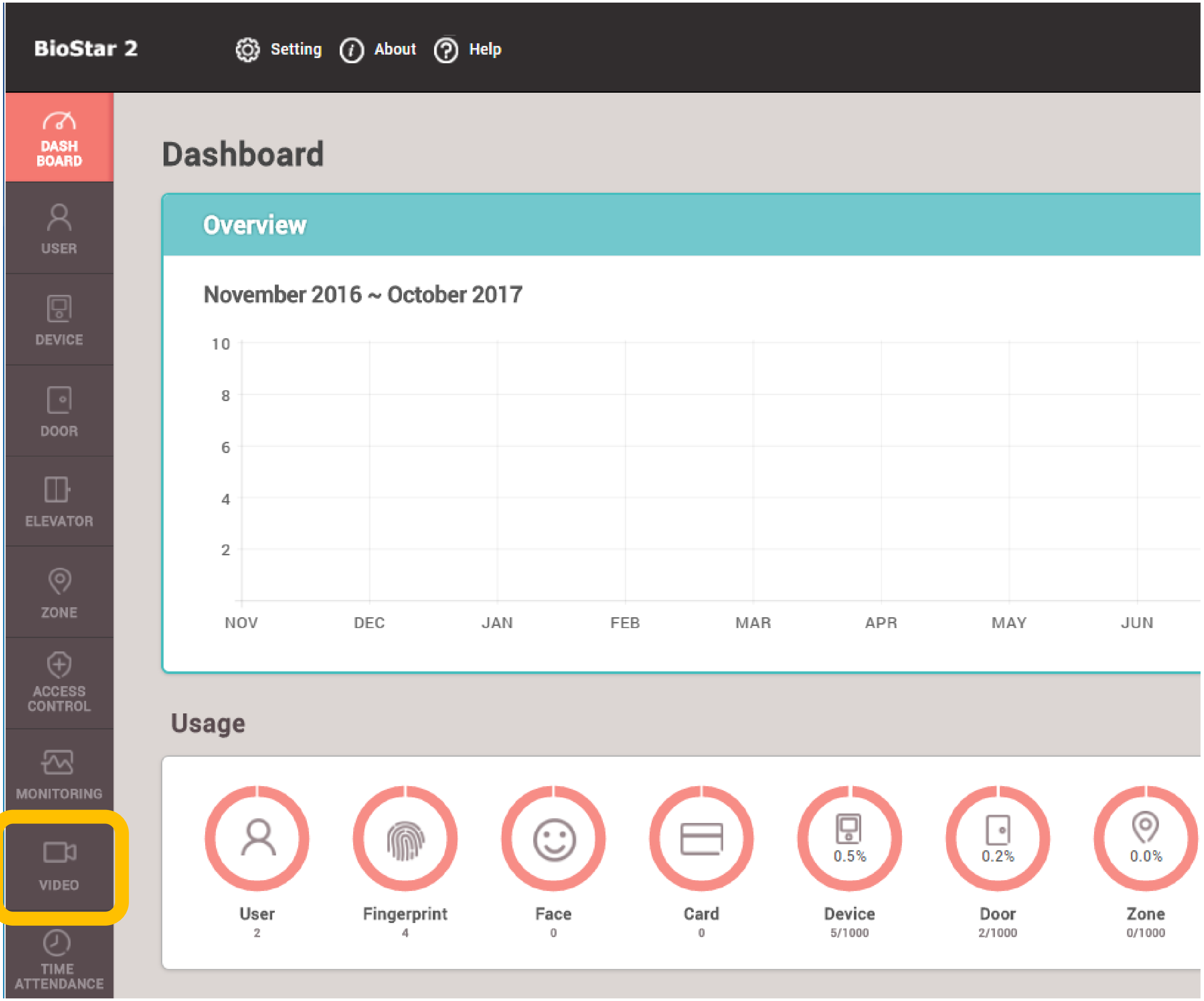
Video

What is Video feature of BioStar2?

- It’s simple integration to see recorded video and picture from NVR
- These recorded contents will be shown **after 3 mins**
- Realtime monitoring is not supported



Video

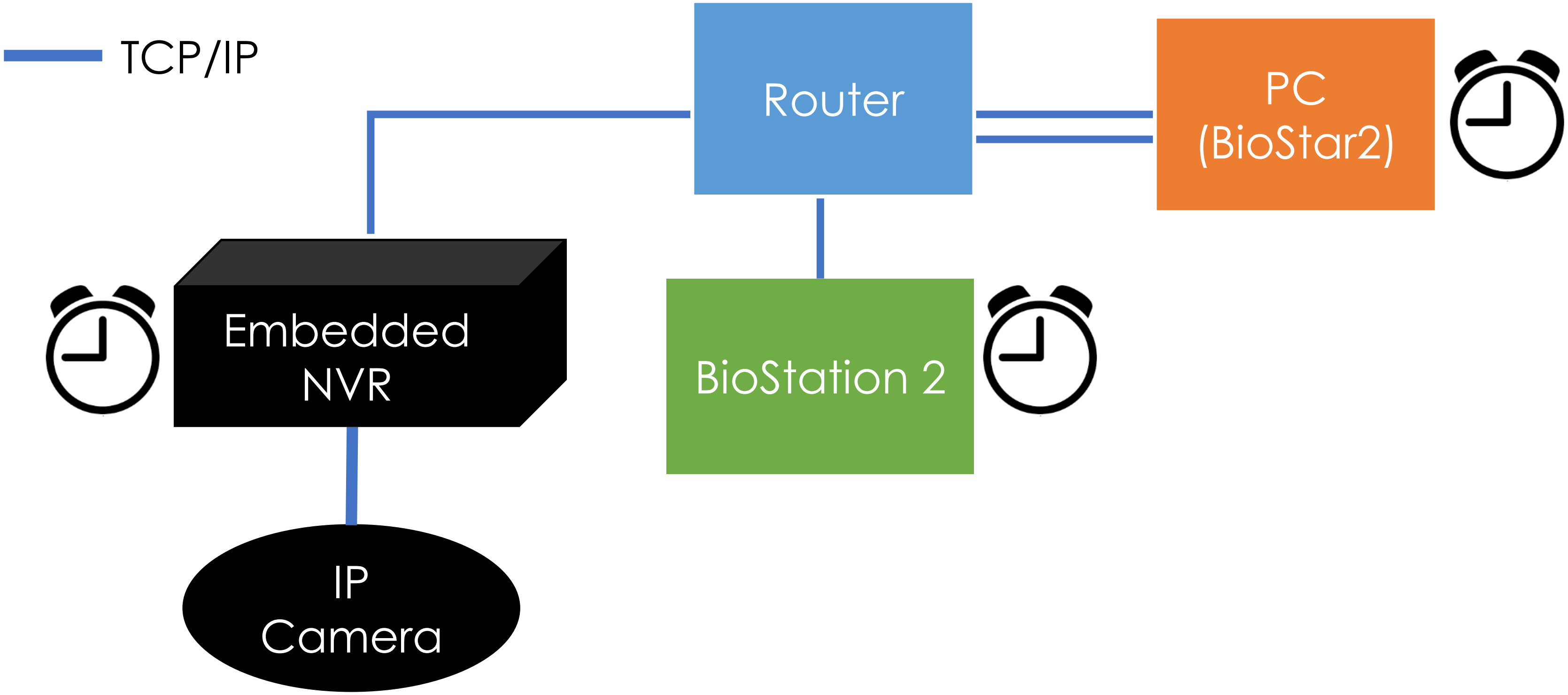


Needed License
Biostar2
AC Standard

Video

Integrate event of door and IP camera which is connected to NVR

- Supported NVR: ACTi, Dahua, Hikvision
- Set Network Time Protocol (NTP) and timezone of NVR
    - Server Address: time.windows.com
- NVR should be recording when event of door occurs



Video

Confirm the following information and check your NVR connection with BioStar2 2.5 before you proceed your project

1. Hikvision NVR

1) SDK version: v5.2.771

2) Tested NVR list : DS-7608NI-E2, DS-7616NI-E2, iVMS4200 v2.4(PC-NVR)

2. Dahua NVR

1) SDK version: v2.14.50523

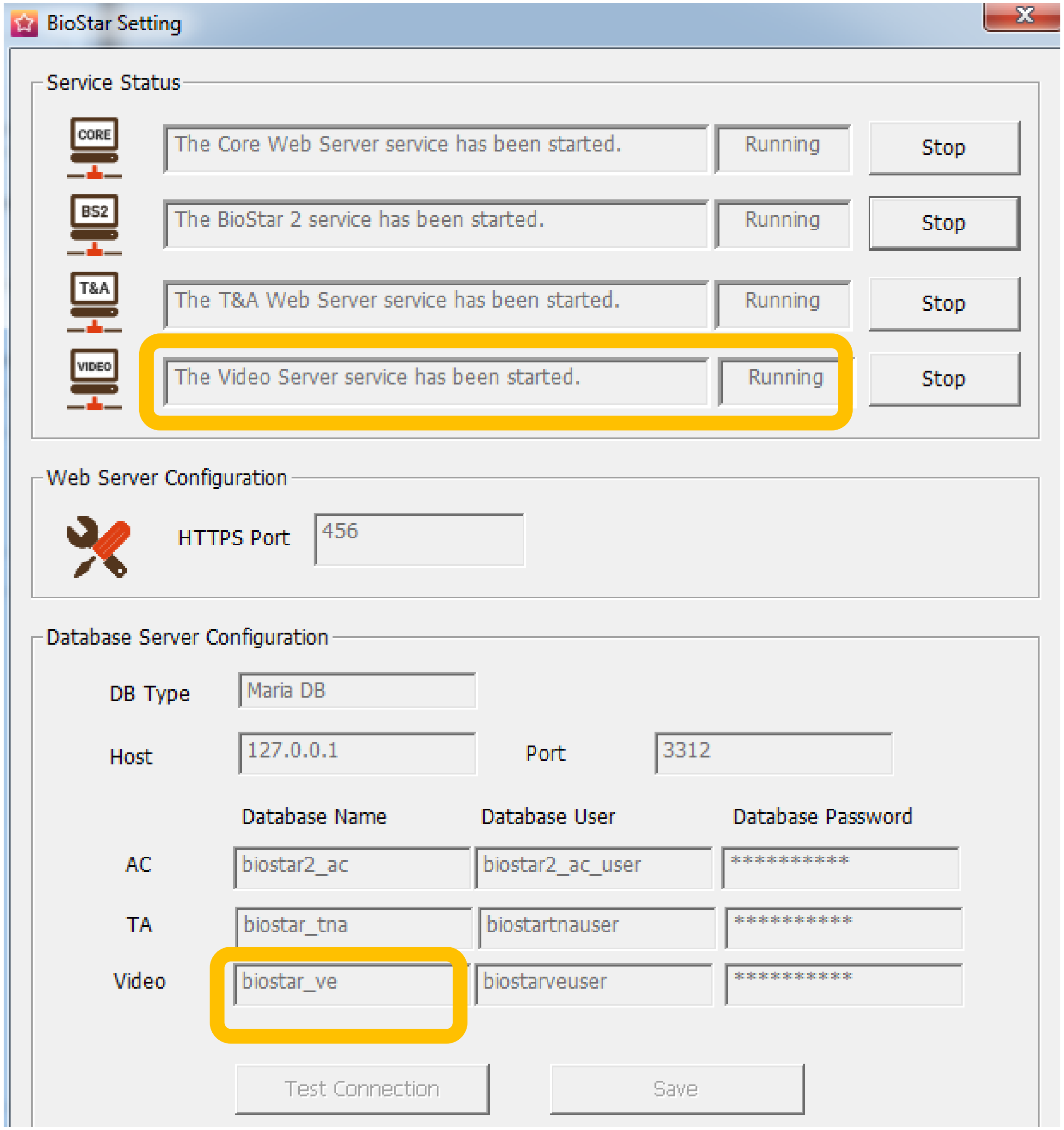
2) Tested NVR list : DH-NVR608-32-4K, DH-NVR4416, SmartPSS V1.13.1.R.20160504(PC-NVR)

3. Acti NVR

1) SDK version: v3.0.12.42

2) Tested NVR list : NVR3 V.3.0.13.27_20161128 Enterprise(PC-NVR)

Video



BioStar Setting

Service Status

CORE	The Core Web Server service has been started.	Running	Stop
BS2	The BioStar 2 service has been started.	Running	Stop
T&A	The T&A Web Server service has been started.	Running	Stop
VIDEO	The Video Server service has been started.	Running	Stop

Web Server Configuration

HTTPS Port: 456

Database Server Configuration

DB Type: Maria DB

Host: 127.0.0.1 Port: 3312

	Database Name	Database User	Database Password
AC	biostar2_ac	biostar2_ac_user	**********
TA	biostar_tna	biostartnauser	**********
Video	biostar_ve	biostarveuser	**********

Supported environment

- **Maria DB**
- **x64 machine**

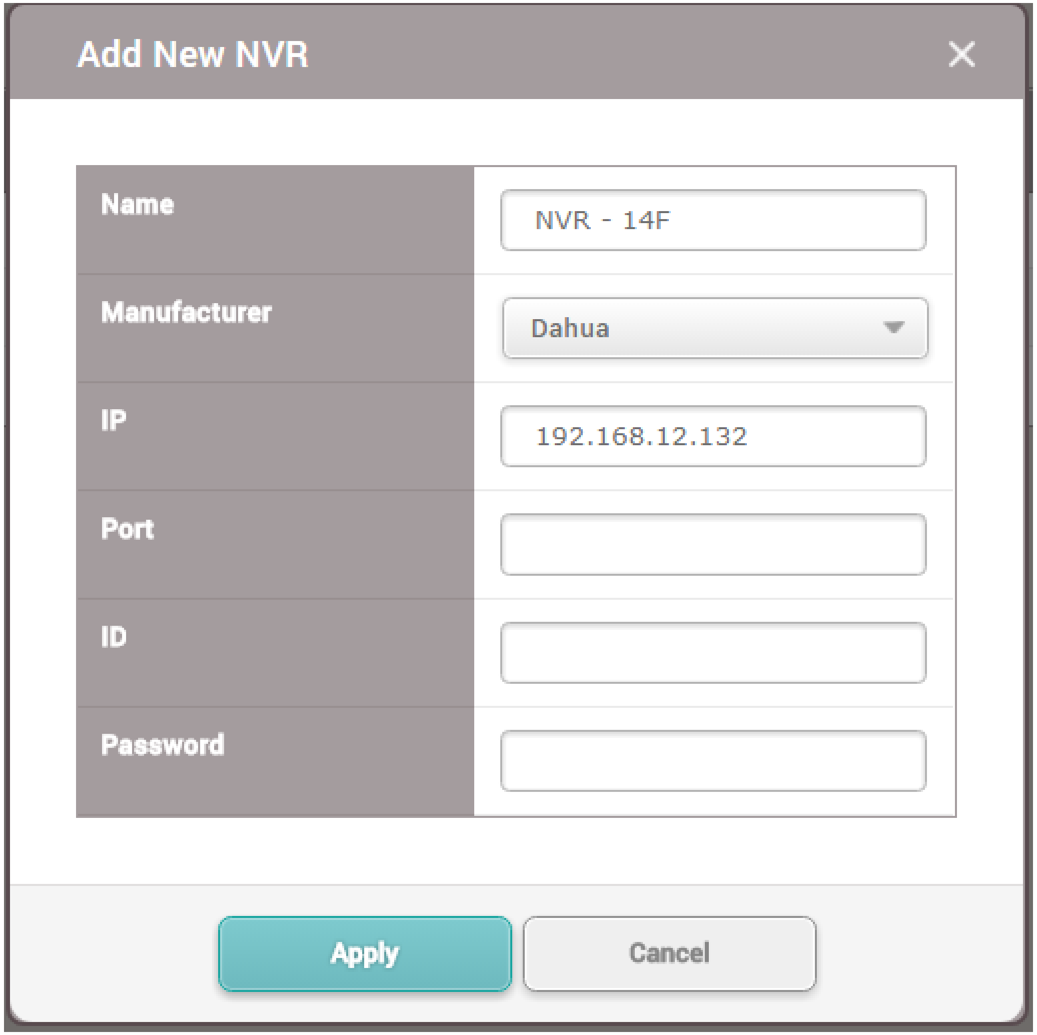
Non-supported environment

- MS SQL
- x86 machine

Video

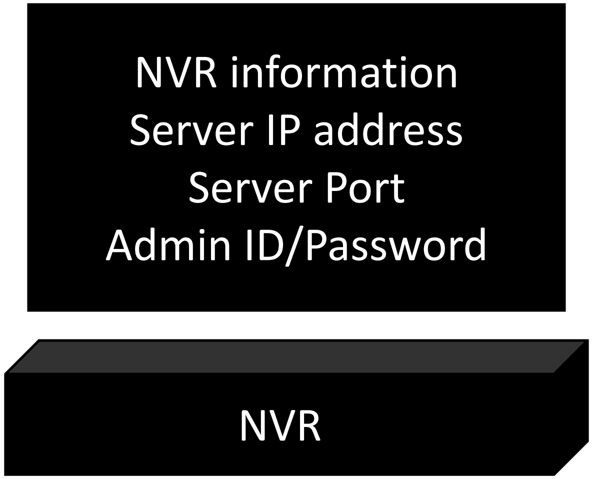
Configuration

- To add NVR on BioStar2, go to Video>Add New NVR



Add New NVR

Name	NVR - 14F
Manufacturer	Dahua
IP	192.168.12.132
Port	
ID	
Password	

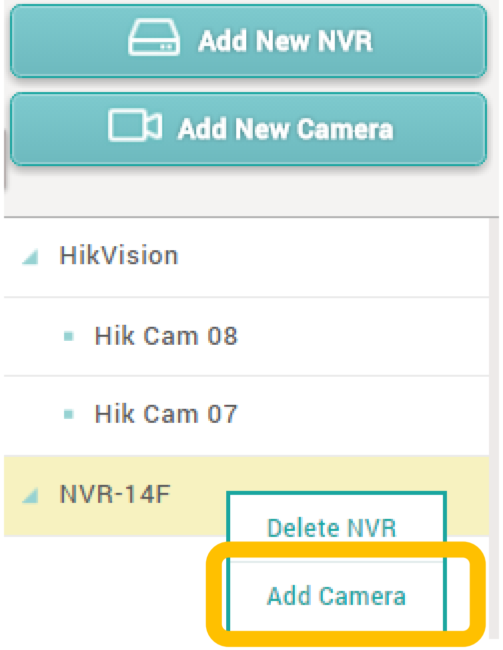


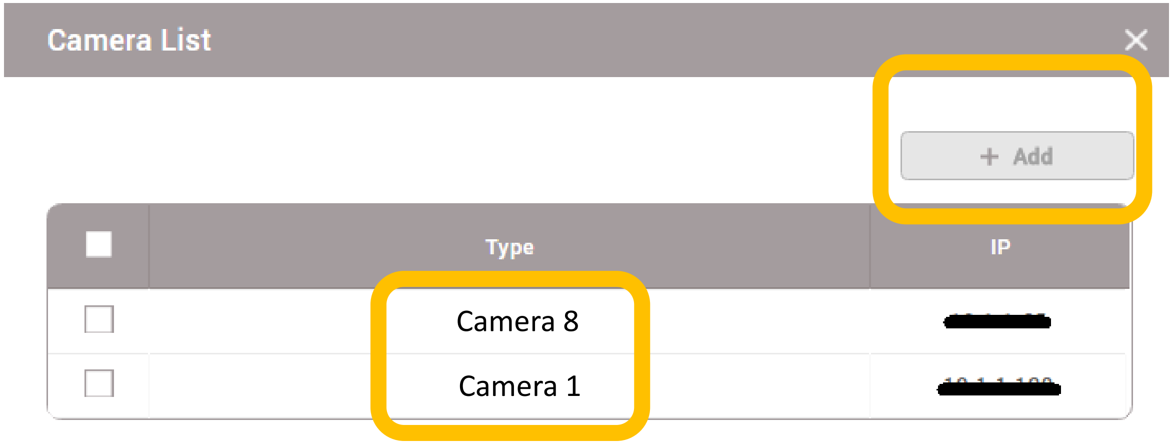
NVR information
Server IP address
Server Port
Admin ID/Password

Video

Configuration

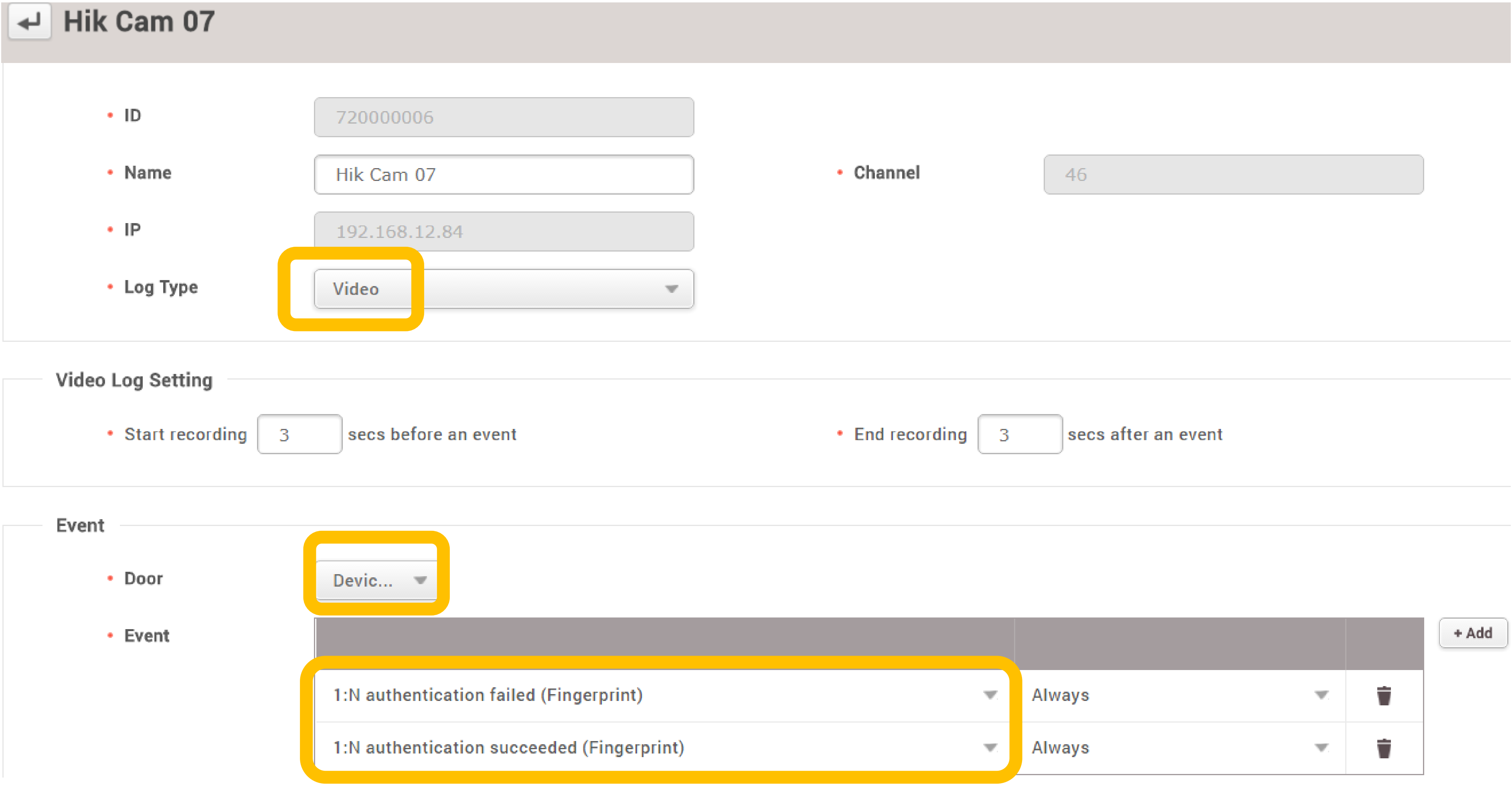
- Add camera after adding NVR





□	Type	IP
□	Camera 8	[redacted]
□	Camera 1	[redacted]

Video



↵ Hik Cam 07

- ID: 720000006
- Name: Hik Cam 07
- Channel: 46
- IP: 192.168.12.84
- Log Type: Video

Video Log Setting

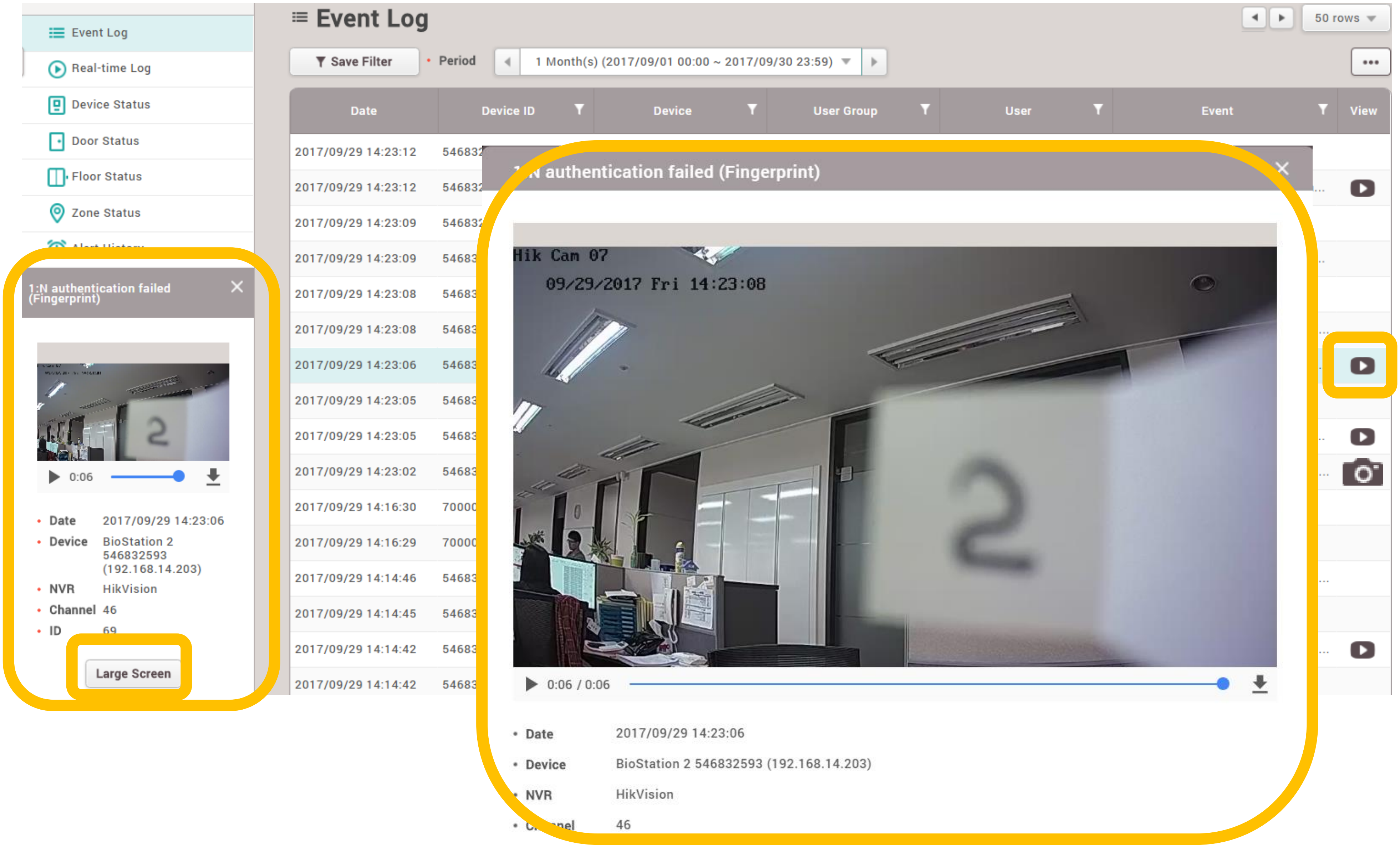
- Start recording 3 secs before an event
- End recording 3 secs after an event

Event

- Door: Devic...
- Event

1:N authentication failed (Fingerprint)	Always	🗑
1:N authentication succeeded (Fingerprint)	Always	🗑

Video



Event Log

Date	Device ID	Device	User Group	User	Event	View
2017/09/29 14:23:12	546832					
2017/09/29 14:23:12	546832					
2017/09/29 14:23:09	546832					
2017/09/29 14:23:09	54683					
2017/09/29 14:23:08	54683					
2017/09/29 14:23:08	54683					
2017/09/29 14:23:06	54683					
2017/09/29 14:23:05	54683					
2017/09/29 14:23:05	54683					
2017/09/29 14:23:02	54683					
2017/09/29 14:16:30	70000					
2017/09/29 14:16:29	70000					
2017/09/29 14:14:46	54683					
2017/09/29 14:14:45	54683					
2017/09/29 14:14:42	54683					
2017/09/29 14:14:42	54683					

1:N authentication failed (Fingerprint)

0:06

- Date 2017/09/29 14:23:06
- Device BioStation 2 546832593 (192.168.14.203)
- NVR HikVision
- Channel 46
- ID 69

1:N authentication failed (Fingerprint)

Hik Cam 07
09/29/2017 Fri 14:23:08

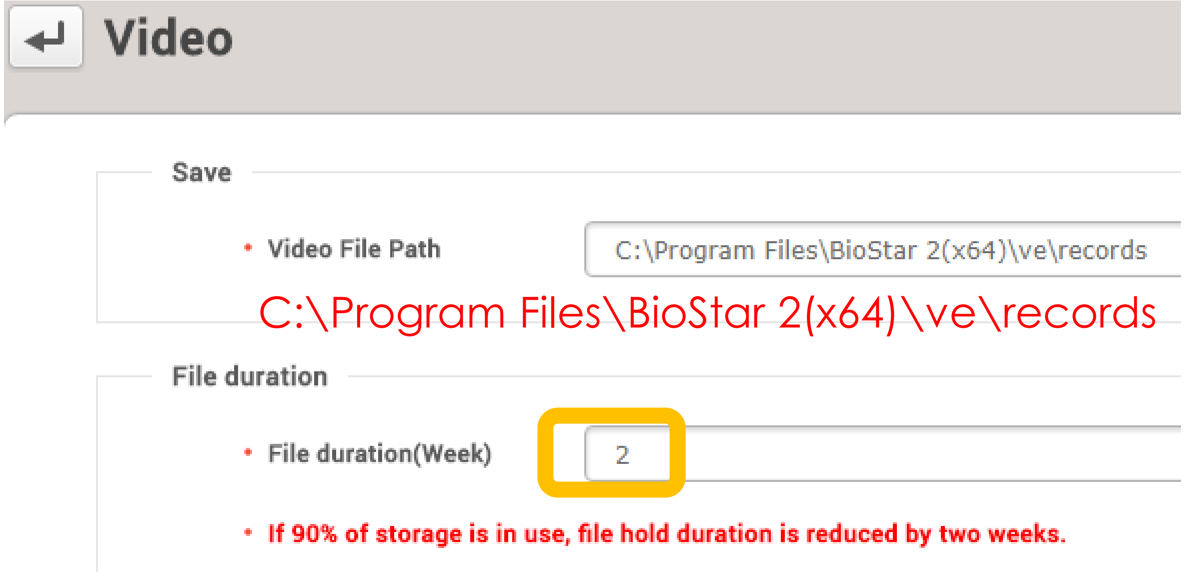
0:06 / 0:06

- Date 2017/09/29 14:23:06
- Device BioStation 2 546832593 (192.168.14.203)
- NVR HikVision
- Channel 46

Video

Caution

- System administrator should manage the storage of HDD
- These files will be kept for minimum 2 weeks as default parameter
- The period can be adjusted more than 2 weeks (Maximum 15 weeks)



↵ Video

Save

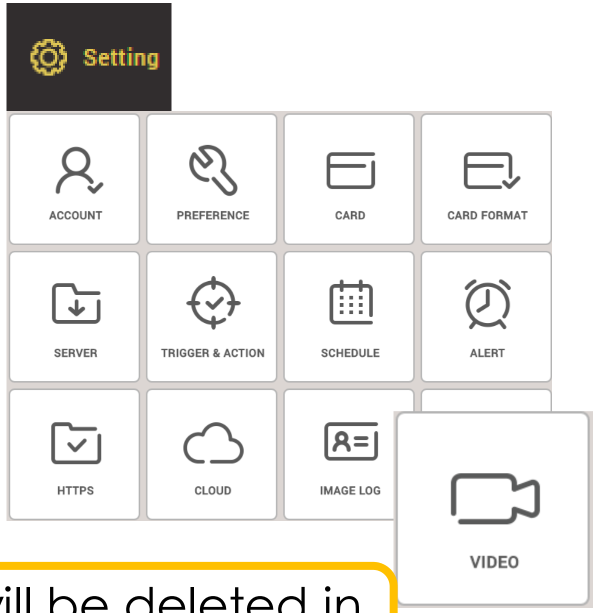
- Video File Path: C:\Program Files\BioStar 2(x64)\ve\records

C:\Program Files\BioStar 2(x64)\ve\records

File duration

- File duration(Week): 2

- If 90% of storage is in use, file hold duration is reduced by two weeks.



- If using storage of C drive is 90%, past recording files will be deleted in accordance with BioStar2 setting

(ex, if the oldest file is 2017-10-01 08 AM, files which is from 2017-10-01 8 AM to 2017-10-15 8 AM will be deleted automatically)

Mobile Card - Widget

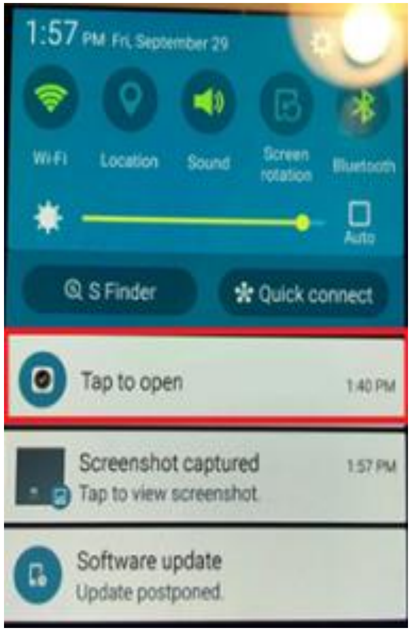
Convenient Mobile Card option with BLE
- Supported BLE device

FS2-AWB

Android

-Tap to open

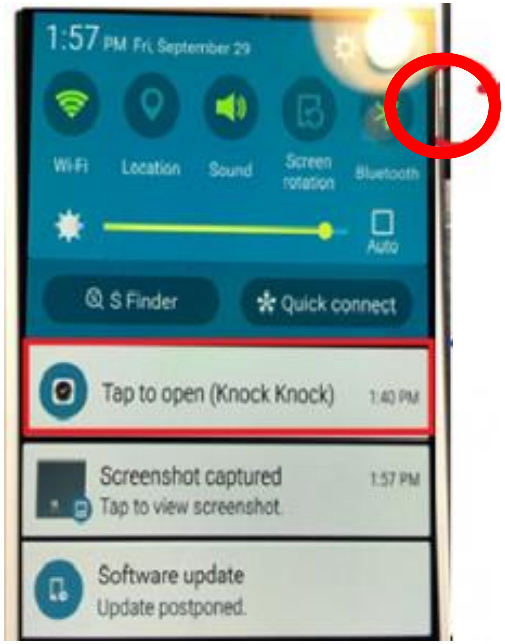
-Tap to open (Knok Knok)



Tap to open 1:40 PM

Screenshot captured 1:57 PM
Tap to view screenshot

Software update
Update postponed



Tap to open (Knock Knock) 1:40 PM

Screenshot captured 1:57 PM
Tap to view screenshot

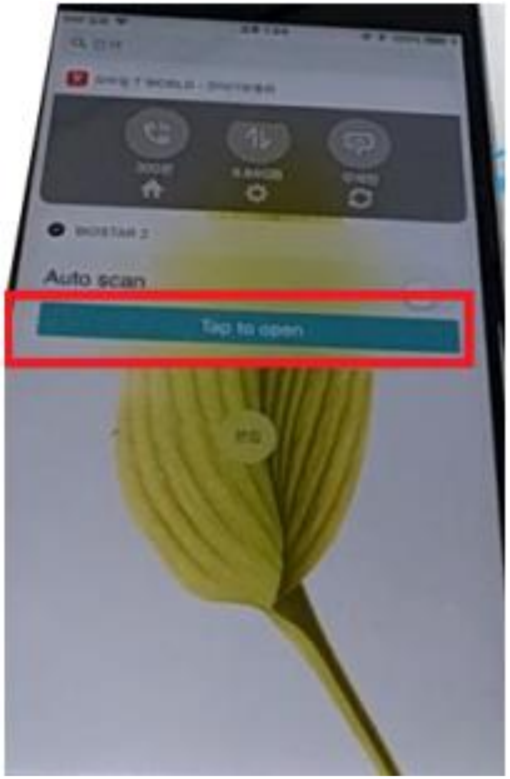
Software update
Update postponed

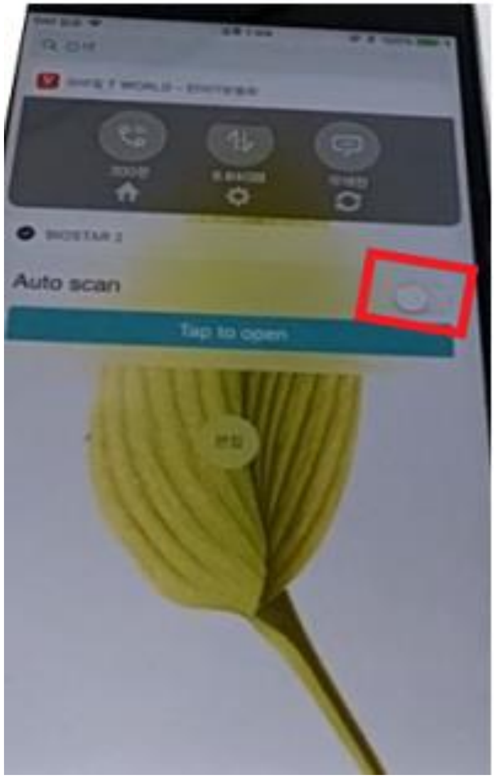
Mobile Card - Widget

iOS

-Tap to open

-Tap to open(Auto Scan)





http://kb.supremainc.com/knowledge/doku.php?id=en:how_to_use_mobile_app_widget_function

Next features

BioStar2 v2.6

- Muster Zone
- Interlock Zone
- BioMini Plus2
- Daylight Saving Time

When

- March-2018

FAQ : Frequently Asked Questions

Frequently Asked Questions

Q.1

Does BioStar2 support BioMini Combo or BioMini Slim?

BioMini Combo

BioMini Slim

A.1

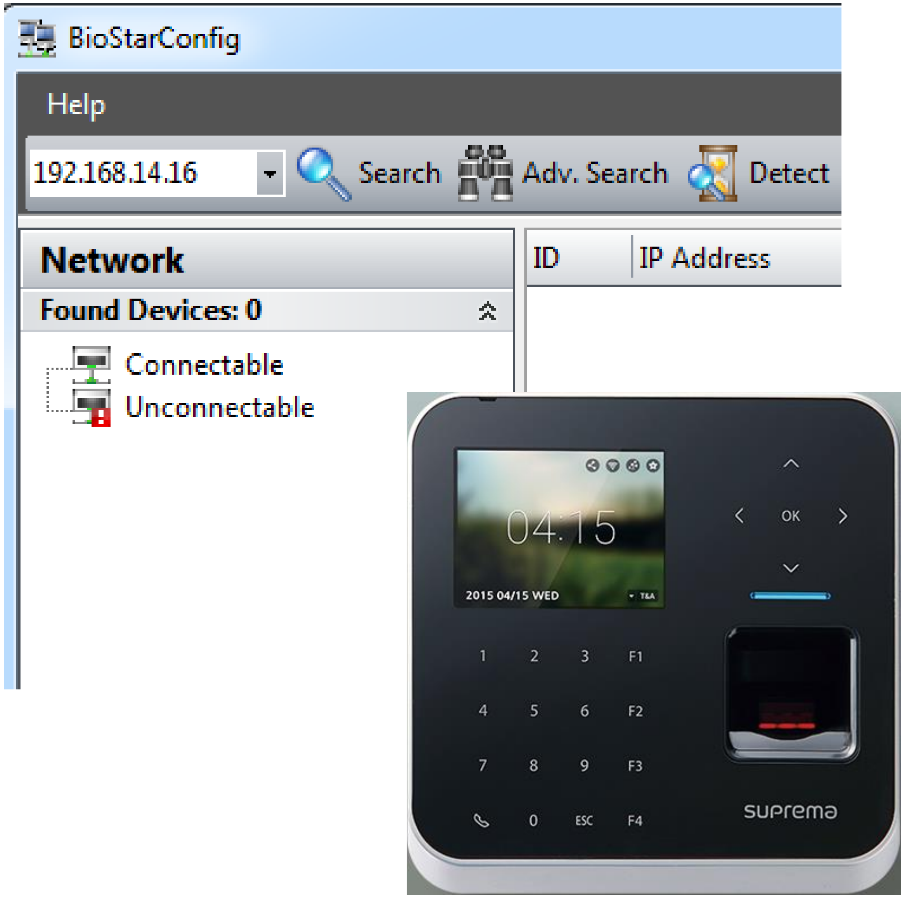
BioStar2 supports BioMini only.

BioMini

Frequently Asked Questions

Q.2

Can we use BioStar Config Tool for V2 devices?



A.2

Unfortunately, no.

It's not compatible with BioStar Config.

We are going to make new Bio Star Config Tool for V2 device.

Frequently Asked Questions

Q.3

When is BioStar 1.92 SDK released?

BioStar 1.9 SDK

V1 device

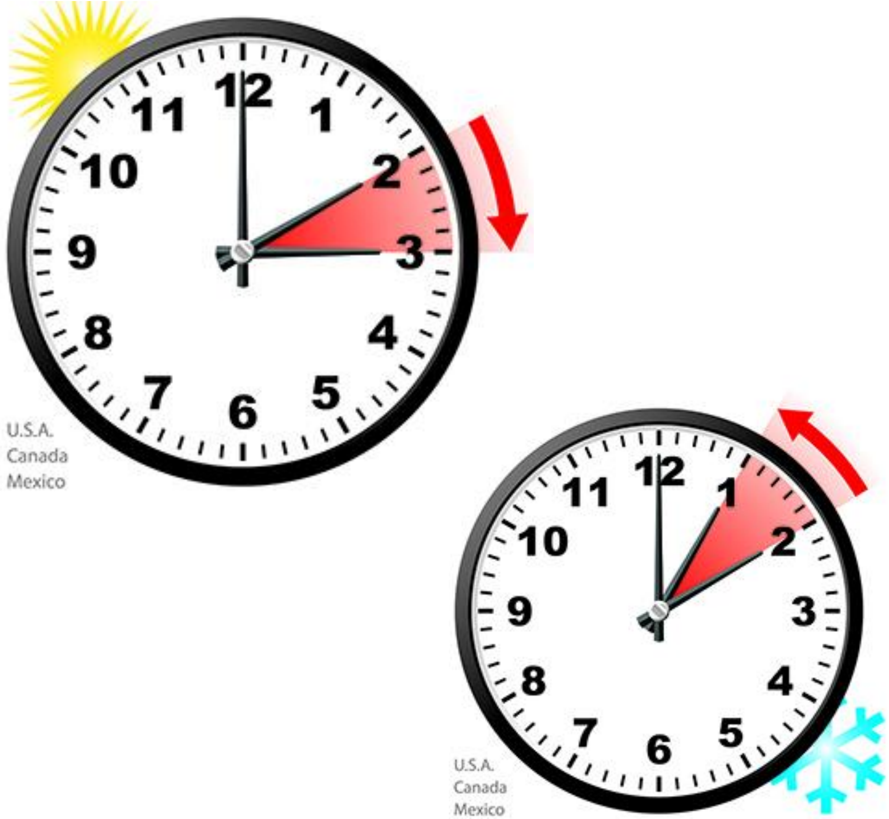
A.3

We do not have BioStar 1.92 SDK. Final version is v1.9 SDK. There will be not any updated version of v1.9 SDK.

Frequently Asked Questions

Q.4

Does Biostar2 support **D**aylight **S**aving **T**ime?



A.4

Unfortunately, no.

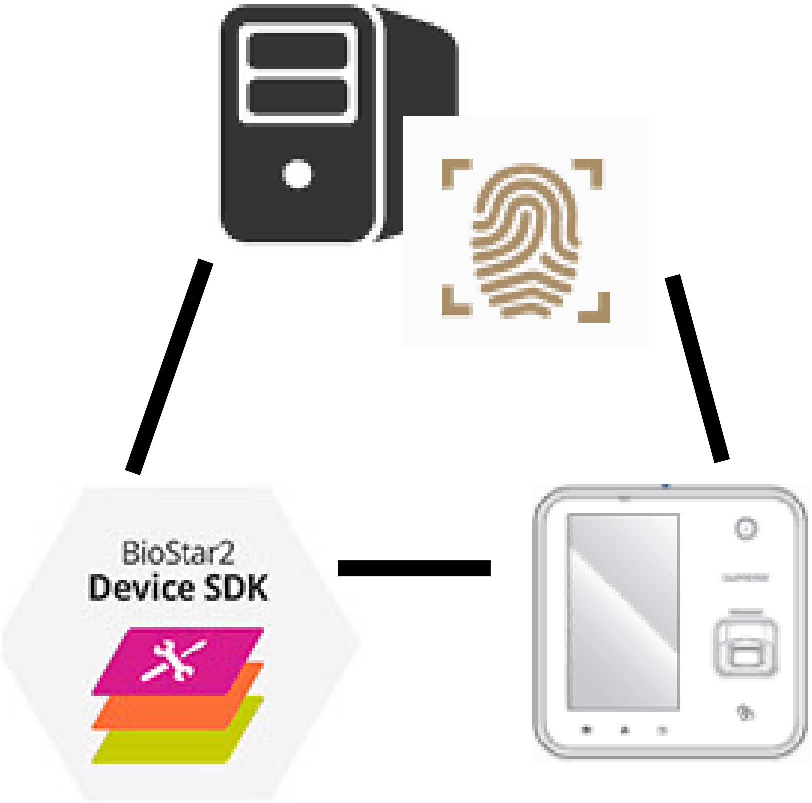
We are going to support DST in the future.

http://support.supremainc.com/support/solutions/articles/24000005681--biostar-2-daylight-savings-time-summer-time-issue

Frequently Asked Questions

Q.5

Could we develop Server Matching using BioStar2 SDK?



A.5

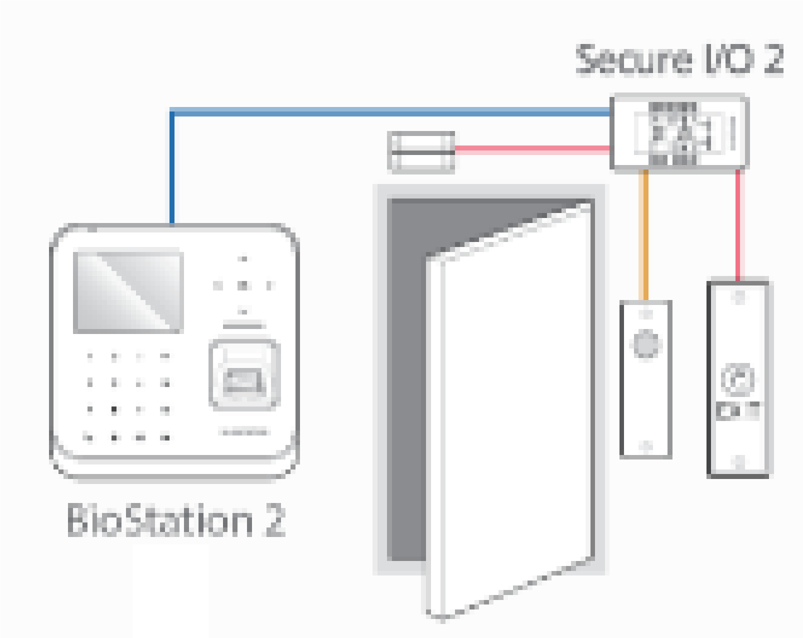
BioStar2 Device SDK doesn't have fingerprint matching algorithm.

You should have other SDK which is called as Image SDK.

Frequently Asked Questions

Q.6

Does BioStar 1.92 support Unlock time & lock time for a door setting using V2 devices?



A.6

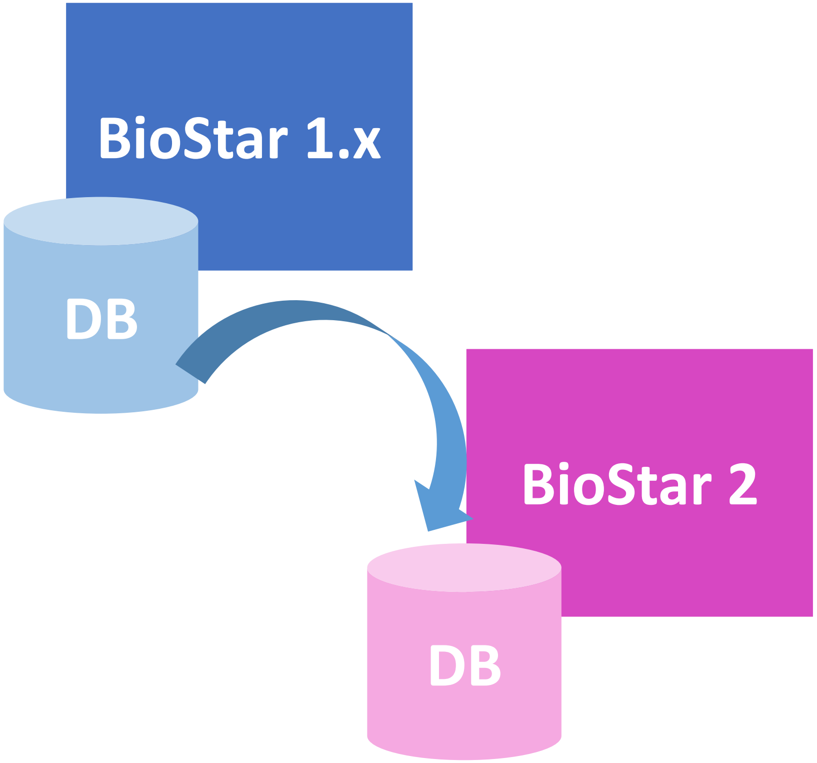
No, it is not supported.

We added this feature to BioStar v1.93.

Frequently Asked Questions

Q.7

Can we upgrade BioStar 1.x to BioStar 2.x?



A.7

It's not possible to upgrade from Biostar 1.x to BioStar2.x directly.

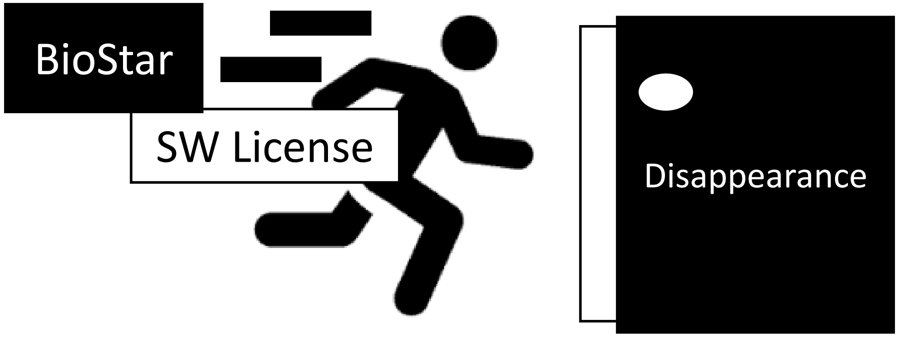
If possible, connect V2 device to BioStar 1.92 and transfer all user i nformation to the device.

Frequently Asked Questions

Q.8

BioStar 1.x SW license has been deleted suddenly.

Could you inform me how we can resolve the issue?

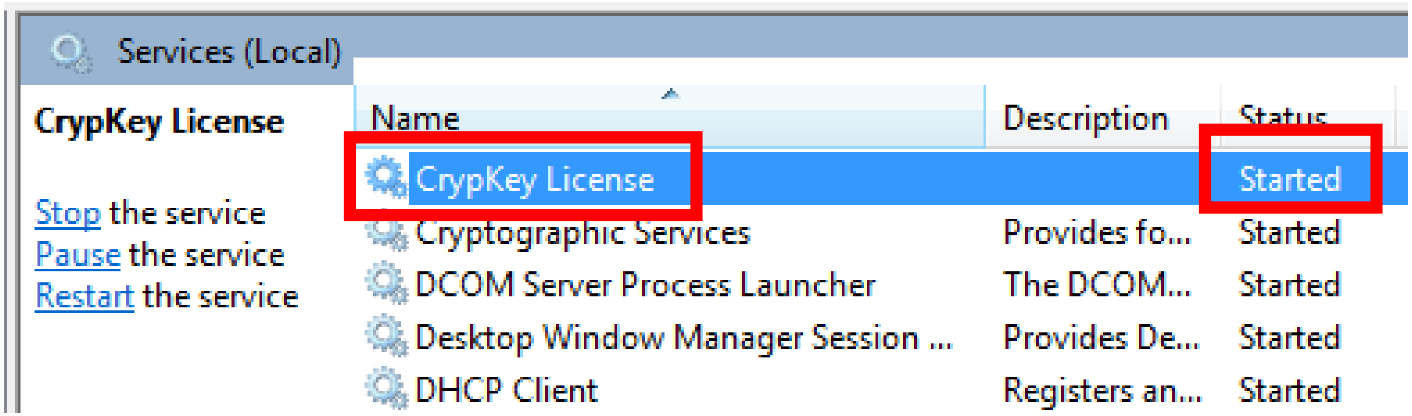

BioStar

SW License

Disappearance

A.8

Confirm if CrypKey License is running and start the license.


Services (Local)

CrypKey License

Stop the service
Pause the service
Restart the service

Name	Description	Status
CrypKey License		Started
Cryptographic Services	Provides fo...	Started
DCOM Server Process Launcher	The DCOM...	Started
Desktop Window Manager Session ...	Provides De...	Started
DHCP Client	Registers an...	Started

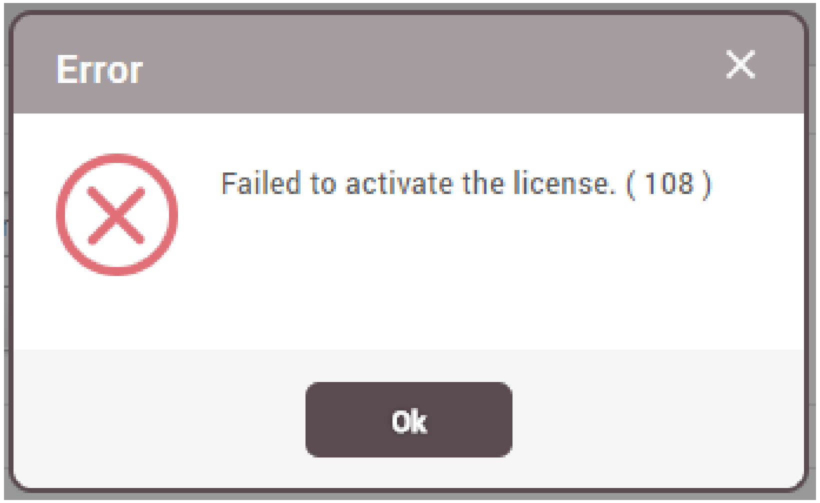
Running icon designed by https://icons8.com/license/

Frequently Asked Questions

Q.9

I’ve got (-108) error during BioStar2 license activation.

How can we resolve the issue?



Error

Failed to activate the license. (108)

A.9

There are three possibilities.

1) Already activated

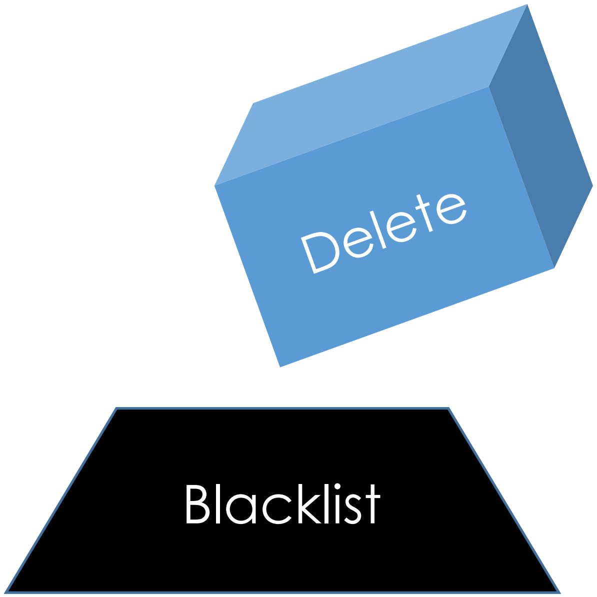
2) Can’t access license server via Internet

3) Incorrect license key

Frequently Asked Questions

Q.10

Can I delete card number from Blacklist?



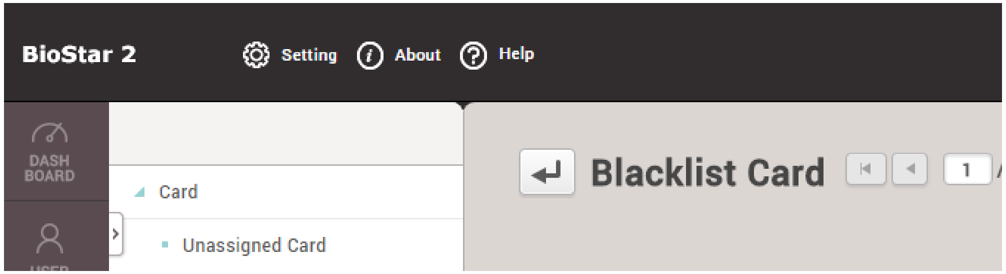
Delete

Blacklist

A.10

Unfortunately, no.
It's not possible.

We are going to improve the blacklist card management to next version of biostar 2.



Thank you!