

BioStar 2.8.6

ADMINISTRATOR GUIDE

Version 1.8.6
English

EN 102.00.BS2 V1.8.6A

Contents

Chapter 1	BioStar 2 Overview	1
	License	2
	Versions	4
Chapter 2	Installation	30
	Minimum System Requirements	30
	Installing BioStar 2	31
Chapter 3	Login	41
	Changing server status of BioStar 2	42
	Changing port of BioStar 2	43
	Changing database of BioStar 2	45
Chapter 4	Before Using	47
Chapter 5	Dashboard	49
Chapter 6	Device	50
	Adding and Managing Device Groups	52
	Basic Search and Registration	53
	Advanced Search and Registration	55
	Wiegand Device Search and Registration	56
	Slave Device Search and Registration	56
	Managing Users Registered with Devices	57
	Upgrading Firmware	58
	Editing Device Settings and Information	59
	Information	60
	Network	62
	Authentication	64
	Advanced Settings	69
	Thermal & Mask	80
	DM-20	83
	OM-120	84
	CoreStation	84
	Wiegand Device	89
Chapter 7	Door	90
	Adding and Managing Door Groups	91

Contents

	Adding Doors	93
	Information	93
	Configuration	93
	Option	95
	Anti-passback	96
	Alarm	97
	Editing Doors	98
Chapter 8	Elevator	98
	Adding and Managing Elevator Groups	99
	Adding Elevators	100
	Information	101
	Detail	101
	Option	103
	Alarm	104
	Editing Elevators	104
Chapter 9	Access Control	105
	Adding and Managing Access Levels	106
	Adding and Managing Access Groups	107
	Adding and Managing Floor Levels	108
	Access Group Status	109
Chapter 10	Users	110
	Adding and Managing User Groups	111
	Adding User Information	113
	Export/Import CSV	116
	Export/Import User Information	119
	Adding User Credentials	120
	Adding PIN	121
	Auth Mode	121
	Enroll Fingerprint	123
	Enroll Face	124
	Enroll Visual Face	126
	Enroll Card	130
	Enroll Mobile Access Card	136
	Transferring User Information to Devices	138
	Deleting User from Devices	139
	Editing User Information	140

Contents

	Managing Long-term Idle Users	141
Chapter 11	Zone	142
	Anti-passback Zone	143
	Fire Alarm Zone	145
	Scheduled Lock Zone	146
	Scheduled Unlock Zone	147
	Intrusion Alarm Zone	148
	Interlock Zone	152
	Muster Zone	154
Chapter 12	Monitoring	155
	List View	156
	Event Log	157
	Real-time Log	159
	Live Video View	160
	Device Status	161
	Door Status	162
	Floor Status	163
	Zone Status	164
	Alert History	165
	Graphic Map View	166
	Adding and Managing Graphic Map Groups	167
	Adding and Managing Graphic Maps	168
Chapter 13	Video	170
	Adding NVRs	171
	Adding IP Cameras	173
	Editing IP Camera Settings	174
Chapter 14	Time & Attendance	175
	Shift	177
	Time Code	177
	Shift	178
	Schedule Template	183
	Rule	185
	Schedule	187
	Report	190
	Editing T&A Records	194
	Setting	196

Contents

Chapter 15

Visitor	197
Applying to Visit	198
Applying to First Visit	198
Applying to Visit Using Existing Info	201
Managing Visitors	202
Managing Registered Visitors	203
Managing Check In Visitors	207
Managing Check Out Visitors	208
Managing All Visitors	209
Deleting Personal Data Expired	210

Chapter 16

BioStar 2 Settings	211
Account	211
Adding Custom Account Level	213
Preference	216
Card	217
Changing Wiegand Card Data Format	218
Card Format	218
Wiegand	219
Smart / Mobile Card	220
Server	221
Trigger & Action	227
Schedules	229
Alert	231
HTTPS	232
Cloud	232
Image Log	234
USB Agent	235
Face Group Matching	236
Audit Trail	237
Video	238
Daylight Saving Time	239
Security	240
Active Directory	244
Active Directory Encryption	246
Visitor	247

Contents

	Mobile Access	251
	Airfob Portal	253
	Configuring Mobile Access	254
	Email Contents	255
Chapter 17	Troubleshooting	258
Chapter 18	Appendix	258
	Disclaimers	258
	Copyright Notice	259
	Open Source License	259
	Software End User License Agreement(EULA)	319

1 BioStar 2 Overview

BioStar 2 is a web-based access control management system which is OS-independent and can be used anywhere.

BioStar 2 expands its versatility even further with its support for access control and time & attendance module, API, Mobile App, and Device SDK solutions.

License

Versions

Access Control

Items		Details
Device	Max. Device	1,000
	Max. Slave per Master (RS-485)	31 (Up to 8 Fingerprint Devices)
	RS-485 Protocol	OSDP Supported
	Multi-Door Control	Supported
	Device Admin Level	All / User / Config
	Auto Reconnection to Server	Direct & Server mode
	USB Enrollment Device	BioMini, BioMini Plus 2, DUALi DE-620
	Daylight Saving Time	Supported
User	Max. Card per User	8
	Max. Fingerprint per User	10
	Auto User Sync to Device	Supported
	Access-on-Card	Supported
	Secure Credential	Supported
	iCLASS Seos Card	Supported
	Inactive User Report	Supported
	Custom Fields	Supported
Access Control	Max. Access Level	2,048 (Depends on the device)
	Max. Access Group	2,048 (Depends on the device)
	Max. Access Group per User	16
	Max. Door per Access Level	128
	Auto Access Group Sync to Device	Supported
	Access Group Report by Door/User/Elevator	Supported
Elevator (Floor Management)	Max. Floor per Elevator	192
	Max. Floor Level	2,048
	Dual Auth	Supported

1 BioStar 2 Overview

	Items	Details
	Anti-passback Zone	Supported
	Fire Alarm Zone	Supported
Zone	Max. Zones	100
	Max. Device per Zone	1,000 Global, 32 Local
	Anti-passback	Door APB, Global, Local
	Fire Alarm	Global, Local
	Scheduled Unlock/Lock	Supported (Local)
	Intrusion Alarm	Supported (Local)
	Interlock	Supported (Local)
	Muster	Supported (Global)
	Dashboard	Supported
	Server Matching	Supported
Advanced	Audit Trail	Supported
	Video Log	Supported
	Local API Server	Supported
	BioStar 2 Mobile App	Supported (User, Door, Monitoring, Alarm)
	Mobile Access	Supported

Time Attendance

Items	Details
Number of Shifts	Unlimited
Number of Schedules	Unlimited
Number of User per Schedule	Unlimited
Shift Type	Fixed, Flexible, Floating
Time Card	Supported
Number of Leave per User	Unlimited
Calendar View	Supported



Note

- Check the [License](#) for features that your license supports.

License

You can use more features by registering the activation key after purchasing the BioStar 2 license.

License for Access Control

1 BioStar 2 Overview

Items		Starter (Free)	Basic	Standard	Advanced	Professional	Enterprise
Access Control	Max. User	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
	Max. Device	1,000	1,000	1,000	1,000	1,000	1,000
	Max. Door	5	20	50	100	300	1,000
	Zone	-	-	Supported	Supported	Supported	Supported
	Elevator	-	-	-	Supported	Supported	Supported
	Graphic Map	-	-	-	Supported	Supported	Supported
	Server Matching	-	-	-	Supported	Supported	Supported
	Cloud	-	-	Supported	Supported	Supported	Supported
Accessories	Active Directory	-	-	-	Supported	Supported	Supported

Note

- If there is an AC Standard license already in use, it is replaced by an Advance license.

License for Time Attendance

Items	Starter (Free)	Standard	Advanced	Professional
Number of Users	100	500	1,000	Unlimited

Note

- If there is an Time Attendance license already in use, it is replaced by an Professional license.

License for Video

Items	Starter (Free)	Video License
Video Log	-	Supported

1 BioStar 2 Overview

License for Visitor

Items	Starter (Free)	Visitor License
Visitor Management	-	Supported

Versions

BioStar 2.8.6

New and improved features

Category	Functionality
Device	<ul style="list-style-type: none">▪ Supports server matching for face recognition devices▪ Supports thermal camera on face recognition devices▪ Support FaceStation F2▪ Support BioEntry W2 (Rev 2)

Compatible firmware

- BioLite Net: 2.3.5 or later
 - BioEntry Plus: 2.3.4 or later
 - BioEntry W: 2.3.4 or later
 - Xpass: 2.4.4 or later
 - Xpass S2: 2.4.4 or later
 - BioStation 2: 1.8.0 or later
 - BioStation A2: 1.7.1 or later
 - BioStation L2: 1.6.0 or later
 - BioEntry W2: 1.5.0 or later
 - FaceStation 2: 1.3.1 or later
 - CoreStation: 1.4.0 or later
 - BioEntry P2: 1.4.0 or later
 - BioEntry R2: 1.4.0 or later
 - BioLite N2: 1.3.1 or later
 - XPass D2: 1.3.1 or later
 - XPass D2 (Rev 2): 1.4.1 or later
 - FaceLite: 1.1.0 or later
 - XPass 2: 1.2.1 or later
 - OM-120: 1.2.0 or later
 - Secure I/O 2: 1.3.0 or later
 - DM-20: 1.2.0 or later
-

1 BioStar 2 Overview

BioStar 2.8.5

New and improved features

Category	Functionality
Time & Attendance	<ul style="list-style-type: none">▪ Supports Wiegand devices▪ Improved the Individual Report usability▪ Supports users to update TA reports

Compatible firmware

- BioLite Net: 2.3.5 or later
- BioEntry Plus: 2.3.4 or later
- BioEntry W: 2.3.4 or later
- Xpass: 2.4.4 or later
- Xpass S2: 2.4.4 or later
- BioStation 2: 1.8.0 or later
- BioStation A2: 1.7.1 or later
- BioStation L2: 1.6.0 or later
- BioEntry W2: 1.5.0 or later
- FaceStation 2: 1.3.1 or later
- CoreStation: 1.4.0 or later
- BioEntry P2: 1.4.0 or later
- BioEntry R2: 1.4.0 or later
- BioLite N2: 1.3.1 or later
- XPass D2: 1.3.1 or later
- XPass D2 (Rev 2): 1.4.1 or later
- FaceLite: 1.1.0 or later
- XPass 2: 1.2.1 or later
- OM-120: 1.2.0 or later
- Secure I/O 2: 1.3.0 or later
- DM-20: 1.2.0 or later

BioStar 2.8.4

New and improved features

Category	Functionality
General	<ul style="list-style-type: none">▪ Supplementation of New Local API▪ Improvement of backup and recovery logic for Web-App, CGI server system.conf▪ Exclusion of TLS V1.1 for improved security

BioStar 2 Overview

Category	Functionality
	<ul style="list-style-type: none">▪ Improved Thrift communication logic log▪ Improved security vulnerabilities on Redis
User	<ul style="list-style-type: none">▪ Improved the logic for issuing mobile access cards▪ Improved the logic for issuing mobile access cards using the CSV
Setting	<ul style="list-style-type: none">▪ Stabilization of features for mobile access cards

Compatible firmware

- BioLite Net: 2.3.5 or later
- BioEntry Plus: 2.3.4 or later
- BioEntry W: 2.3.4 or later
- Xpass: 2.4.4 or later
- Xpass S2: 2.4.4 or later
- BioStation 2: 1.8.0 or later
- BioStation A2: 1.7.1 or later
- BioStation L2: 1.5.1 or later
- BioEntry W2: 1.5.0 or later
- FaceStation 2: 1.3.1 or later
- CoreStation: 1.4.0 or later
- BioEntry P2: 1.4.0 or later
- BioEntry R2: 1.4.0 or later
- BioLite N2: 1.3.1 or later
- XPass D2: 1.3.1 or later
- XPass D2 (Rev 2): 1.4.1 or later
- FaceLite: 1.1.0 or later
- XPass 2: 1.2.1 or later
- OM-120: 1.2.0 or later
- Secure I/O 2: 1.3.0 or later
- DM-20: 1.2.0 or later

BioStar 2.8.3

New and improved features

Category	Functionality
General	<ul style="list-style-type: none">▪ Updated language resource files
Device	<ul style="list-style-type: none">▪ Supports FaceStation 2 and FaceLite as a slave of CoreStation▪ Supports Mobile Access on BioLite N2
Elevator	<ul style="list-style-type: none">▪ Improved the scheduled unlock zone function to support elevator

1 BioStar 2 Overview

Category	Functionality
Setting	<ul style="list-style-type: none">▪ Supports Zone in the Admin Item Settings of the custom level

Compatible firmware

- BioLite Net: 2.3.5 or later
- BioEntry Plus: 2.3.4 or later
- BioEntry W: 2.3.4 or later
- Xpass: 2.4.4 or later
- Xpass S2: 2.4.4 or later
- BioStation 2: 1.8.0 or later
- BioStation A2: 1.7.1 or later
- BioStation L2: 1.5.1 or later
- BioEntry W2: 1.4.1 or later
- FaceStation 2: 1.3.1 or later
- CoreStation: 1.4.0 or later
- BioEntry P2: 1.4.0 or later
- BioEntry R2: 1.4.0 or later
- BioLite N2: 1.3.0 or later
- XPass D2: 1.3.0 or later
- XPass D2 (Rev 2): 1.4.0 or later
- FaceLite: 1.1.0 or later
- XPass 2: 1.2.1 or later
- OM-120: 1.1.0 or later
- Secure I/O 2: 1.3.0 or later
- DM-20: 1.2.0 or later

BioStar 2.8.2

New and improved features

Category	Functionality
General	<ul style="list-style-type: none">▪ Fixed local file inclusion (LFI) vulnerability

Compatible firmware

- BioLite Net: 2.3.5 or later
- BioEntry Plus: 2.3.4 or later
- BioEntry W: 2.3.4 or later
- Xpass: 2.4.4 or later
- Xpass S2: 2.4.4 or later
- BioStation 2: 1.8.0 or later

1 BioStar 2 Overview

- BioStation A2: 1.7.1 or later
 - BioStation L2: 1.5.1 or later
 - BioEntry W2: 1.4.1 or later
 - FaceStation 2: 1.3.1 or later
 - CoreStation: 1.3.1 or later
 - BioEntry P2: 1.3.1 or later
 - BioEntry R2: 1.4.0 or later
 - BioLite N2: 1.2.0 or later
 - XPass D2: 1.3.0 or later
 - XPass D2 (Rev 2): 1.4.0 or later
 - FaceLite: 1.1.0 or later
 - XPass 2: 1.2.0 or later
 - OM-120: 1.1.0 or later
 - Secure I/O 2: 1.2.4 or later
 - DM-20: 1.1.5 or later
-

BioStar 2.8.1

New and improved features

Category	Functionality
General	<ul style="list-style-type: none">▪ Supports MS SQL Server 2019
Time & Attendance	<ul style="list-style-type: none">▪ Move the 'In/Out Only' and 'All Punches' options in the Individual Report

Compatible firmware

- BioLite Net: 2.3.5 or later
- BioEntry Plus: 2.3.4 or later
- BioEntry W: 2.3.4 or later
- Xpass: 2.4.4 or later
- Xpass S2: 2.4.4 or later
- BioStation 2: 1.8.0 or later
- BioStation A2: 1.7.1 or later
- BioStation L2: 1.5.1 or later
- BioEntry W2: 1.4.1 or later
- FaceStation 2: 1.3.1 or later
- CoreStation: 1.3.1 or later
- BioEntry P2: 1.3.1 or later
- BioEntry R2: 1.4.0 or later
- BioLite N2: 1.2.0 or later
- XPass D2: 1.3.0 or later

1 BioStar 2 Overview

- XPass D2 (Rev 2): 1.4.0 or later
 - FaceLite: 1.1.0 or later
 - XPass 2: 1.2.0 or later
 - OM-120: 1.1.0 or later
 - Secure I/O 2: 1.2.4 or later
 - DM-20: 1.1.5 or later
-

BioStar 2.8.0

New and improved features

Category	Functionality
General	<ul style="list-style-type: none">▪ DB encryption to enhance security on personal information

Compatible firmware

- BioLite Net: 2.3.5 or later
 - BioEntry Plus: 2.3.4 or later
 - BioEntry W: 2.3.4 or later
 - Xpass: 2.4.4 or later
 - Xpass S2: 2.4.4 or later
 - BioStation 2: 1.8.0 or later
 - BioStation A2: 1.7.1 or later
 - BioStation L2: 1.5.1 or later
 - BioEntry W2: 1.4.1 or later
 - FaceStation 2: 1.3.0 or later
 - CoreStation: 1.3.1 or later
 - BioEntry P2: 1.3.1 or later
 - BioEntry R2: 1.3.1 or later
 - BioLite N2: 1.2.0 or later
 - XPass D2: 1.2.0 or later
 - XPass D2 (Rev 2): 1.4.0 or later
 - FaceLite: 1.1.0 or later
 - XPass 2: 1.1.0 or later
 - OM-120: 1.1.0 or later
 - Secure I/O 2: 1.2.4 or later
 - DM-20: 1.1.5 or later
-

BioStar 2.7.14

BioStar 2 Overview

New and improved features

Category	Functionality
General	<ul style="list-style-type: none">▪ Supports Windows Authentication for MS SQL database server connections▪ Supports MS SQL Server 2017▪ Added the Floor Control API to BioStar 2 API Documents
Device	<ul style="list-style-type: none">▪ Support XPass D2(Rev 2)
Setting	<ul style="list-style-type: none">▪ Enhancement in Mobile Access usage▪ Stabilization of 'Specific Devices' Automatic User Synchronization option

Compatible firmware

- BioLite Net: 2.3.5 or later
- BioEntry Plus: 2.3.4 or later
- BioEntry W: 2.3.4 or later
- Xpass: 2.4.4 or later
- Xpass S2: 2.4.4 or later
- BioStation 2: 1.8.0 or later
- BioStation A2: 1.7.1 or later
- BioStation L2: 1.5.1 or later
- BioEntry W2: 1.4.1 or later
- FaceStation 2: 1.3.0 or later
- CoreStation: 1.3.1 or later
- BioEntry P2: 1.3.1 or later
- BioEntry R2: 1.3.1 or later
- BioLite N2: 1.2.0 or later
- XPass D2: 1.2.0 or later
- FaceLite: 1.1.0 or later
- XPass 2: 1.1.0 or later
- OM-120: 1.1.0 or later
- Secure I/O 2: 1.2.4 or later
- DM-20: 1.1.5 or later

BioStar 2.7.12

New and improved features

Category	Functionality
Time & Attendance	<ul style="list-style-type: none">▪ Support to generate TA reports simultaneously on multiple clients
Setting	<ul style="list-style-type: none">▪ Added the new Suprema Mobile Access▪ Stabilized 'Specific Devices' Automatic User Synchronization option

1 BioStar 2 Overview

Compatible firmware

- BioLite Net: 2.3.5 or later
- BioEntry Plus: 2.3.4 or later
- BioEntry W: 2.3.4 or later
- Xpass: 2.4.4 or later
- Xpass S2: 2.4.4 or later
- BioStation 2: 1.8.0 or later
- BioStation A2: 1.7.0 or later
- BioStation L2: 1.5.1 or later
- BioEntry W2: 1.4.1 or later
- FaceStation 2: 1.3.0 or later
- CoreStation: 1.3.1 or later
- BioEntry P2: 1.3.1 or later
- BioEntry R2: 1.3.1 or later
- BioLite N2: 1.2.0 or later
- XPass D2: 1.2.0 or later
- FaceLite: 1.1.0 or later
- XPass 2: 1.1.0 or later
- OM-120: 1.1.0 or later
- Secure I/O 2: 1.2.4 or later
- DM-20: 1.1.5 or later

BioStar 2.7.11

New and improved features

Category	Functionality
General	<ul style="list-style-type: none">▪ Improved dashboard usability
User	<ul style="list-style-type: none">▪ Added User IP item to User Information
Device	<ul style="list-style-type: none">▪ Supports the alert sound for 'Input(Event Name Change)' in the <Trigger & Action>
Monitoring	<ul style="list-style-type: none">▪ Supports the sorting of lists for the User ID and User Group column of the <Muster Status> page
Setting	<ul style="list-style-type: none">▪ Enhances the system security▪ Added 'Specific Devices(Only devices belonging to the access group)' option to <Automatic User Synchronization>

Compatible firmware

- BioLite Net: 2.3.5 or later

1 BioStar 2 Overview

- BioEntry Plus: 2.3.4 or later
 - BioEntry W: 2.3.4 or later
 - Xpass: 2.4.4 or later
 - Xpass S2: 2.4.4 or later
 - BioStation 2: 1.8.0 or later
 - BioStation A2: 1.7.0 or later
 - BioStation L2: 1.5.1 or later
 - BioEntry W2: 1.4.1 or later
 - FaceStation 2: 1.3.0 or later
 - CoreStation: 1.3.0 or later
 - BioEntry P2: 1.3.1 or later
 - BioEntry R2: 1.3.1 or later
 - BioLite N2: 1.2.0 or later
 - XPass D2: 1.2.0 or later
 - FaceLite: 1.1.0 or later
 - XPass 2: 1.1.0 or later
 - OM-120: 1.1.0 or later
 - Secure I/O 2: 1.2.4 or later
 - DM-20: 1.1.5 or later
-

BioStar 2.7.10

New and improved features

Category	Functionality
Device	<ul style="list-style-type: none">▪ Support FaceLite▪ Support XPass 2
Time & Attendance	<ul style="list-style-type: none">▪ Improve the Custom Level▪ Support to use the custom user field in the T&A report▪ Supports the sorting for entire data in the T&A report▪ Added option to select 'First in & Last Out' or 'All in/Out Punches' to search conditions of the individual report
Visitor	<ul style="list-style-type: none">▪ Support to the USB fingerprint scanner connection (BioMini, BioMini Plus, BioMini Plus 2)
Setting	<ul style="list-style-type: none">▪ Update the resource files of Japanese, Arabic, and Spanish▪ Add Automatic backup function for Setting.conf file

Compatible firmware

- BioLite Net: 2.3.5 or later
- BioEntry Plus: 2.3.4 or later
- BioEntry W: 2.3.4 or later

1 BioStar 2 Overview

- Xpass: 2.4.4 or later
 - Xpass S2: 2.4.4 or later
 - BioStation 2: 1.8.0 or later
 - BioStation A2: 1.7.0 or later
 - BioStation L2: 1.5.0 or later
 - BioEntry W2: 1.4.0 or later
 - FaceStation 2: 1.3.0 or later
 - CoreStation: 1.3.0 or later
 - BioEntry P2: 1.3.0 or later
 - BioEntry R2: 1.3.0 or later
 - BioLite N2: 1.2.0 or later
 - XPass D2: 1.2.0 or later
 - FaceLite: 1.1.0 or later
 - XPass 2: 1.0.1 or later
 - OM-120: 1.1.0 or later
 - Secure I/O 2: 1.2.4 or later
 - DM-20: 1.1.5 or later
-

BioStar 2.7.8

New and improved features

Category	Functionality
Device	<ul style="list-style-type: none">▪ Supports multiple use function of controllers in CoreStation▪ Supports options for selection by card type▪ Supports the fingerprint/face duplicate check▪ Supports Anti-Tailgating▪ Supports setting options for Wiegand authentication result output
Door	<ul style="list-style-type: none">▪ Supports Anti-Tailgating
Visitor	<ul style="list-style-type: none">▪ Supports to search option for visitors using fingerprints
Setting	<ul style="list-style-type: none">▪ Supports user group synchronization in Active Directory▪ Supports Anti-Tailgating

Compatible firmware

- BioLite Net: 2.3.5 or later
- BioEntry Plus: 2.3.4 or later
- BioEntry W: 2.3.4 or later
- Xpass: 2.4.4 or later
- Xpass S2: 2.4.4 or later
- BioStation 2: 1.7.1 or later

1 BioStar 2 Overview

- BioStation A2: 1.6.0 or later
 - BioStation L2: 1.5.0 or later
 - BioEntry W2: 1.4.0 or later
 - FaceStation 2: 1.2.1 or later
 - CoreStation: 1.3.0 or later
 - BioEntry P2: 1.3.0 or later
 - BioEntry R2: 1.3.0 or later
 - BioLite N2: 1.1.0 or later
 - XPass D2: 1.2.0 or later
 - FaceLite: 1.0.0 or later
 - XPass 2: 1.0.0 or later
 - OM-120: 1.1.0 or later
 - Secure I/O 2: 1.2.4 or later
 - DM-20: 1.1.4 or later
-

BioStar 2.7.7

New and improved features

Category	Functionality
General	<ul style="list-style-type: none">▪ Change the license policy
Visitor	<ul style="list-style-type: none">▪ Add the VISITOR menu
Setting	<ul style="list-style-type: none">▪ Add the settings for visitor management

Compatible firmware

- BioLite Net: 2.3.5 or later
- BioEntry Plus: 2.3.4 or later
- BioEntry W: 2.3.4 or later
- Xpass: 2.4.4 or later
- Xpass S2: 2.4.4 or later
- BioStation 2: 1.7.1 or later
- BioStation A2: 1.6.0 or later
- BioStation L2: 1.4.0 or later
- BioEntry W2: 1.3.0 or later
- FaceStation 2: 1.2.1 or later
- CoreStation: 1.2.0 or later
- BioEntry P2: 1.2.0 or later
- BioEntry R2: 1.2.0 or later
- BioLite N2: 1.1.0 or later
- XPass D2: 1.1.0 or later

1 BioStar 2 Overview

- OM-120: 1.1.0 or later
 - Secure I/O 2: 1.2.4 or later
 - DM-20: 1.1.4 or later
-

BioStar 2.7.6

New and improved features

Category	Functionality
General	<ul style="list-style-type: none">▪ Add BioStar 1.x to BioStar 2.x Migration Tool
Monitoring	<ul style="list-style-type: none">▪ Support to the Clear APB for each user
Setting	<ul style="list-style-type: none">▪ Add the event items to IMAGE LOG menu▪ Add the encryption option to Active Directory menu▪ Supports that the administrator can change the port 9000 in FastCGI of Port menu

Compatible firmware

- BioLite Net: 2.3.5 or later
 - BioEntry Plus: 2.3.4 or later
 - BioEntry W: 2.3.4 or later
 - Xpass: 2.4.4 or later
 - Xpass S2: 2.4.4 or later
 - BioStation 2: 1.7.1 or later
 - BioStation A2: 1.6.0 or later
 - BioStation L2: 1.4.0 or later
 - BioEntry W2: 1.3.0 or later
 - FaceStation 2: 1.2.1 or later
 - CoreStation: 1.2.0 or later
 - BioEntry P2: 1.2.0 or later
 - BioEntry R2: 1.2.0 or later
 - BioLite N2: 1.1.0 or later
 - XPass D2: 1.1.0 or later
 - OM-120: 1.1.0 or later
 - Secure I/O 2: 1.2.4 or later
 - DM-20: 1.1.4 or later
-

BioStar 2.7.5

New and improved features

1 BioStar 2 Overview

Category	Functionality
User	<ul style="list-style-type: none">▪ Support to the list sorting for group and status column
Device	<ul style="list-style-type: none">▪ Support to the list sorting for RS-485 column▪ Remove the unsupported AoC events▪ Added an Ambient Brightness option to the FaceStation 2 slave device
Door	<ul style="list-style-type: none">▪ Support to the list sorting for group column
Video	<ul style="list-style-type: none">▪ Remove the unsupported AoC events
Setting	<ul style="list-style-type: none">▪ Add the Active Directory menu▪ Supports that the administrator can change the port 9000 in setting.conf▪ Remove the unsupported AoC events

Compatible firmware

- BioLite Net: 2.3.5 or later
- BioEntry Plus: 2.3.4 or later
- BioEntry W: 2.3.4 or later
- Xpass: 2.4.4 or later
- Xpass S2: 2.4.4 or later
- BioStation 2: 1.7.1 or later
- BioStation A2: 1.6.0 or later
- BioStation L2: 1.4.0 or later
- BioEntry W2: 1.3.0 or later
- FaceStation 2: 1.2.1 or later
- CoreStation: 1.2.0 or later
- BioEntry P2: 1.2.0 or later
- BioEntry R2: 1.2.0 or later
- BioLite N2: 1.1.0 or later
- XPass D2: 1.1.0 or later
- OM-120: 1.1.0 or later
- Secure I/O 2: 1.2.4 or later
- DM-20: 1.1.4 or later

BioStar 2.7.4

New and improved features

Category	Functionality
Device	<ul style="list-style-type: none">▪ Support for Quick Enrollment for FaceStation 2 (FaceStation 2 FW V1.2.2 or later)

1 BioStar 2 Overview

Category	Functionality
Setting	<ul style="list-style-type: none">▪ Limits the use of passwords that contain the same string, consecutive string, and login ID▪ Limits reuse of the same password▪ Support to Spanish and Arabic▪ Expanding the number of custom levels to unlimited

Compatible firmware

- BioLite Net: 2.3.5 or later
- BioEntry Plus: 2.3.4 or later
- BioEntry W: 2.3.4 or later
- Xpass: 2.4.4 or later
- Xpass S2: 2.4.4 or later
- BioStation 2: 1.7.1 or later
- BioStation A2: 1.6.0 or later
- BioStation L2: 1.4.0 or later
- BioEntry W2: 1.3.0 or later
- FaceStation 2: 1.2.1 or later
- CoreStation: 1.2.0 or later
- BioEntry P2: 1.2.0 or later
- BioEntry R2: 1.2.0 or later
- BioLite N2: 1.1.0 or later
- XPass D2: 1.1.0 or later
- OM-120: 1.1.0 or later
- Secure I/O 2: 1.2.4 or later
- DM-20: 1.1.4 or later

BioStar 2.7.3

New and improved features

Category	Functionality
Device	<ul style="list-style-type: none">▪ Increase the number of administrators that can be added per device▪ Change the way new settings are applied when adding administrators using batch edit of devices
Setting	<ul style="list-style-type: none">▪ Support for reconnection of devices configured as a port forwarding

Compatible firmware

- BioLite Net: 2.3.5 or later
- BioEntry Plus: 2.3.4 or later

1 BioStar 2 Overview

- BioEntry W: 2.3.4 or later
- Xpass: 2.4.4 or later
- Xpass S2: 2.4.4 or later
- BioStation 2: 1.7.0 or later
- BioStation A2: 1.6.0 or later
- BioStation L2: 1.4.0 or later
- BioEntry W2: 1.3.0 or later
- FaceStation 2: 1.2.0 or later
- CoreStation: 1.2.0 or later
- BioEntry P2: 1.2.0 or later
- BioEntry R2: 1.2.0 or later
- BioLite N2: 1.1.0 or later
- XPass D2: 1.1.0 or later
- OM-120: 1.1.0 or later
- Secure I/O 2: 1.2.4 or later
- DM-20: 1.1.4 or later

BioStar 2.7.2

New and improved features

Category	Functionality
Monitoring	<ul style="list-style-type: none">▪ Support to Live Video View on Graphic Map▪ Support to viewing Anti-passback Zone and Fire Alarm Zone on Graphic Map
Time & Attendance	<ul style="list-style-type: none">▪ Supports <Allowed a day before/after time> setting for working 24 hours or longer
Setting	<ul style="list-style-type: none">▪ Add the Security menu▪ Change Password Level options▪ Support to the setting for Maximum Password Age and Maximum Password Change Limit▪ Support to the setting options for password failures at login▪ Support to the Storage Path Settings for image logs

Compatible firmware

- BioLite Net: 2.3.5 or later
- BioEntry Plus: 2.3.4 or later
- BioEntry W: 2.3.4 or later
- Xpass: 2.4.4 or later
- Xpass S2: 2.4.4 or later
- BioStation 2: 1.7.0 or later

1 BioStar 2 Overview

- BioStation A2: 1.6.0 or later
 - BioStation L2: 1.4.0 or later
 - BioEntry W2: 1.3.0 or later
 - FaceStation 2: 1.2.0 or later
 - CoreStation: 1.2.0 or later
 - BioEntry P2: 1.2.0 or later
 - BioEntry R2: 1.2.0 or later
 - BioLite N2: 1.1.0 or later
 - XPass D2: 1.1.0 or later
 - OM-120: 1.1.0 or later
 - Secure I/O 2: 1.2.4 or later
 - DM-20: 1.1.4 or later
-

BioStar 2.7.1

New and improved features

Category	Functionality
Device	<ul style="list-style-type: none">▪ Support to Input(Event Name Change) in Trigger & Action▪ Support to the OM-120 Relay time setting value from 1 second
User	<ul style="list-style-type: none">▪ Support for deleting users stored on the device
Monitoring	<ul style="list-style-type: none">▪ Provides the log about whether a user has been updated on the device or the server
Setting	<ul style="list-style-type: none">▪ Supports synchronization of all devices connected to the server when users update the device▪ Adds root password verification procedures during installation and upgrade

Compatible firmware

- BioLite Net: 2.3.5 or later
- BioEntry Plus: 2.3.4 or later
- BioEntry W: 2.3.4 or later
- Xpass: 2.4.4 or later
- Xpass S2: 2.4.4 or later
- BioStation 2: 1.7.0 or later
- BioStation A2: 1.6.0 or later
- BioStation L2: 1.4.0 or later
- BioEntry W2: 1.3.0 or later
- FaceStation 2: 1.2.0 or later
- CoreStation: 1.2.0 or later

1 BioStar 2 Overview

- BioEntry P2: 1.2.0 or later
- BioEntry R2: 1.2.0 or later
- BioLite N2: 1.1.0 or later
- XPass D2: 1.1.0 or later
- OM-120: 1.1.0 or later
- Secure I/O 2: 1.2.4 or later
- DM-20: 1.1.4 or later

BioStar 2.7.0

New and improved features

Category	Functionality
Device	<ul style="list-style-type: none">▪ Support to the number of users, fingerprints, faces, and cards in Manage Users in Device
Access Control	<ul style="list-style-type: none">▪ Support for a larger number of access groups and access groups
Monitoring	<ul style="list-style-type: none">▪ Support to Graphic Map
Time & Attendance	<ul style="list-style-type: none">▪ Support to Working alarm time report▪ Improve the process for generating the time card▪ Support to the separator option in CSV export▪ Support to Floating shift▪ Support to Fixed option in Meal deduction and Break Time▪ Support to Weekend days setting option in Schedule Template
Setting	<ul style="list-style-type: none">▪ Support to Custom Account Level in T&A▪ Support to AES encryption type for DESFire card▪ Support to DESFire Advanced option

Compatible firmware

- BioLite Net: 2.3.5 or later
- BioEntry Plus: 2.3.4 or later
- BioEntry W: 2.3.4 or later
- Xpass: 2.4.4 or later
- Xpass S2: 2.4.4 or later
- BioStation 2: 1.7.0 or later
- BioStation A2: 1.6.0 or later
- BioStation L2: 1.4.0 or later
- BioEntry W2: 1.3.0 or later
- FaceStation 2: 1.2.0 or later
- CoreStation: 1.2.0 or later
- BioEntry P2: 1.2.0 or later

1 BioStar 2 Overview

- BioEntry R2: 1.2.0 or later
 - BioLite N2: 1.1.0 or later
 - XPass D2: 1.1.0 or later
 - OM-120: 1.1.0 or later
 - Secure I/O 2: 1.2.4 or later
 - DM-20: 1.1.4 or later
-

BioStar 2.6.4

New and improved features

Category	Functionality
Setting	<ul style="list-style-type: none">▪ Support to set the same action for different triggers

Compatible firmware

- BioLite Net: 2.3.5 or later
 - BioEntry Plus: 2.3.4 or later
 - BioEntry W: 2.3.4 or later
 - Xpass: 2.4.4 or later
 - Xpass S2: 2.4.4 or later
 - BioStation 2: 1.6.2 or later
 - BioStation A2: 1.5.1 or later
 - BioStation L2: 1.3.2 or later
 - BioEntry W2: 1.2.3 or later
 - FaceStation 2: 1.1.1 or later
 - CoreStation: 1.1.2 or later
 - BioEntry P2: 1.1.2 or later
 - BioEntry R2: 1.1.1 or later
 - BioLite N2: 1.0.2 or later
 - XPass D2: 1.0.2 or later
 - OM-120: 1.0.0 or later
 - Secure I/O 2: 1.2.1 or later
 - DM-20: 1.1.2 or later
-

BioStar 2.6.3

New and improved features

1 BioStar 2 Overview

Category	Functionality
Setting	<ul style="list-style-type: none">▪ Support Admin Item Settings when configuring Custom Account Level

Compatible firmware

- BioLite Net: 2.3.5 or later
- BioEntry Plus: 2.3.3 or later
- BioEntry W: 2.3.3 or later
- Xpass: 2.4.4 or later
- Xpass S2: 2.4.4 or later
- BioStation 2: 1.6.1 or later
- BioStation A2: 1.5.1 or later
- BioStation L2: 1.3.1 or later
- BioEntry W2: 1.2.1 or later
- FaceStation 2: 1.1.1 or later
- CoreStation: 1.1.1 or later
- BioEntry P2: 1.1.1 or later
- BioEntry R2: 1.1.0 or later
- BioLite N2: 1.0.2 or later
- XPass D2: 1.0.1 or later
- OM-120: 1.0.0 or later
- Secure I/O 2: 1.2.1 or later
- DM-20: 1.1.2 or later

BioStar 2.6.2

New and improved features

Category	Functionality
User	<ul style="list-style-type: none">▪ Support the user information export/import by using the external storage (USB)
Video	<ul style="list-style-type: none">▪ Support the real-time video monitoring
Monitoring	<ul style="list-style-type: none">▪ Support the event log import by using the external storage (USB)

Compatible firmware

- BioLite Net: 2.3.5 or later
- BioEntry Plus: 2.3.3 or later
- BioEntry W: 2.3.3 or later
- Xpass: 2.4.4 or later
- Xpass S2: 2.4.4 or later

1 BioStar 2 Overview

- BioStation 2: 1.6.1 or later
 - BioStation A2: 1.5.1 or later
 - BioStation L2: 1.3.1 or later
 - BioEntry W2: 1.2.1 or later
 - FaceStation 2: 1.1.1 or later
 - CoreStation: 1.1.1 or later
 - BioEntry P2: 1.1.1 or later
 - BioEntry R2: 1.1.0 or later
 - BioLite N2: 1.0.2 or later
 - XPass D2: 1.0.1 or later
 - OM-120: 1.0.0 or later
 - Secure I/O 2: 1.2.1 or later
 - DM-20: 1.1.2 or later
-

BioStar 2.6.0

New and improved features

Category	Functionality
General	<ul style="list-style-type: none">▪ Support the Daylight Saving Time(DST)▪ Support the database encryption key management▪ Support the system ports setting▪ Support the system logs management▪ Firmware upgrade notifications supported▪ Change the license policy
User & Card	<ul style="list-style-type: none">▪ Support for the auto-Increase User IDs▪ Support the iCLASS Seos card setting▪ Support the hexadecimal values for the primary and secondary site keys on the smart card▪ Wiegand card search supported from the Unassigned card menu▪ Support for automatic deletion of user information when issuing an AoC card▪ Wiegand Legacy Mode Support▪ Blacklist card deletion support
Device	<ul style="list-style-type: none">▪ Support BioLite N2▪ Support XPass D2▪ Support BioMini Plus 2▪ Support the user information and log deletion when a tamper event occurs (secure tamper)▪ Device reset excluding network settings▪ Wiegand In/Out Support

1 BioStar 2 Overview

Zone	<ul style="list-style-type: none">▪ Support the interlock zone▪ Support the muster zone
Video	<ul style="list-style-type: none">▪ Support MS SQL for Video log▪ Support the video file storage management
Monitoring	<ul style="list-style-type: none">▪ Add door column to event log list

Compatible firmware

- BioLite Net: 2.3.3 or later
- BioEntry Plus: 2.3.3 or later
- BioEntry W: 2.3.3 or later
- Xpass: 2.4.3 or later
- Xpass S2: 2.4.3 or later
- BioStation 2: 1.6.0 or later
- BioStation A2: 1.5.0 or later
- BioStation L2: 1.3.0 or later
- BioEntry W2: 1.2.0 or later
- FaceStation 2: 1.1.0 or later
- CoreStation: 1.1.0 or later
- BioEntry P2: 1.1.0 or later
- BioEntry R2: 1.1.0 or later
- BioLite N2: 1.0.0 or later
- XPass D2: 1.0.0 or later
- OM-120: 1.0.0 or later
- Secure I/O 2: 1.2.1 or later
- DM-20: 1.1.2 or later

BioStar 2.5.0

New and improved features

Category	Functionality
General	<ul style="list-style-type: none">▪ Setting https as the default communication protocol▪ Oracle Database not supported
Device	<ul style="list-style-type: none">▪ Supports CoreStation▪ Supports BioEntry P2▪ Supports BioEntry R2▪ Supports the enrollment of a fingerprint from the slave device(BioLite Net does not support this feature)
Zone	<ul style="list-style-type: none">▪ Supports Intrusion Alarm zone (Local)

1 BioStar 2 Overview

Monitoring	<ul style="list-style-type: none">▪ Event Log, Real-time Log: T&A Key column added▪ Event Log: Supports the period setting▪ Supports video log
Video	<ul style="list-style-type: none">▪ Supports NVRs (ACTi, Dahua, Hikvision)▪ Supports IP cameras
Setting	<ul style="list-style-type: none">▪ Alert: Network disconnection detection alert added▪ Supports Audit Trail

Compatible firmware

- BioLite Net: 2.3.3 or later
- BioEntry Plus: 2.3.3 or later
- BioEntry W: 2.3.3 or later
- Xpass: 2.4.3 or later
- Xpass S2: 2.4.3 or later
- BioStation 2: 1.5.0 or later
- BioStation A2: 1.4.0 or later
- BioStation L2: 1.2.3 or later
- BioEntry W2: 1.1.4 or later
- FaceStation 2: 1.0.3 or later
- CoreStation: 1.0.0 or later
- BioEntry P2: 1.0.0 or later
- BioEntry R2: 1.0.0 or later

BioStar 2.4.1

New and improved features

Category	Functionality
General	<ul style="list-style-type: none">▪ Supports Mobile Card (NFC, BLE)
Device	<ul style="list-style-type: none">▪ Supports FaceStation 2
Time & Attendance	<ul style="list-style-type: none">▪ Enhanced UI/UX▪ Merge the time card with T&A report▪ Display of daily T&A records▪ Time rate setting is excluded from the time code for leave management.▪ Break time is displayed on the time slot when fixed work is used.▪ It is possible to set the Min. Duration and Punch in Time Limit when flexible work is used.
Setting	<ul style="list-style-type: none">▪ Supports Face Group Matching

1 BioStar 2 Overview

Compatible firmware

- BioLite Net: 2.4.0 or later
 - BioEntry Plus: 2.4.0 or later
 - BioEntry W: 2.4.0 or later
 - Xpass: 2.4.1 or later
 - Xpass S2: 2.4.0 or later
 - BioStation 2: 1.4.0 or later
 - BioStation A2: 1.3.0 or later
 - BioStation L2: 1.2.2 or later
 - BioEntry W2: 1.1.2 or later
 - FaceStation 2: 1.0.0 or later
-

BioStar 2.4.0

New and improved features

Category	Functionality
General	<ul style="list-style-type: none">▪ Supports elevator management▪ Supporting Oracle Database 11g, 12c
Device	<ul style="list-style-type: none">▪ Supports OM-120▪ Supports card USB device (DUALi DE-620)▪ Supports secure communication between BioStar 2 and a device
Time & Attendance	<ul style="list-style-type: none">▪ Supports time & attendance report PDF export
Setting	<ul style="list-style-type: none">▪ Change of detailed custom permission setting▪ Supports user ID type setting (numbers/alphanumeric characters)▪ Supports dd/mm/yyyy date format

Compatible firmware

- BioLite Net: 2.4.0 or later
 - BioEntry Plus: 2.4.0 or later
 - BioEntry W: 2.4.0 or later
 - Xpass: 2.4.0 or later
 - Xpass S2: 2.4.0 or later
 - BioStation 2: 1.4.0 or later
 - BioStation A2: 1.3.0 or later
 - BioStation L2: 1.2.2 or later
 - BioEntry W2: 1.1.2 or later
-

1 BioStar 2 Overview

BioStar 2.3.0

New and improved features

Category	Functionality
General	<ul style="list-style-type: none">▪ Supporting a low-resolution monitor▪ Improvement in list page move
User	<ul style="list-style-type: none">▪ Improvement importing/exporting CSV files
Device	<ul style="list-style-type: none">▪ Supporting BioStation A2 video phone (SIP based)▪ Supporting the batch editing the device manager▪ Supporting an additional information display of a device firmware
Door	<ul style="list-style-type: none">▪ Supporting an automatic door setting
Setting	<ul style="list-style-type: none">▪ Supporting Wiegand card's facility code setting▪ Supporting the batch editing the Wiegand card data format▪ Supporting BioStar 2 alert sound's upload and setting (.wav, .mp3)▪ Supporting the custom account level (up to 32)

Compatible firmware

- BioLite Net: 2.3.0 or later
- BioEntry Plus: 2.3.0 or later
- BioEntry W: 2.3.0 or later
- Xpass: 2.3.0 or later
- Xpass S2: 2.3.0 or later
- BioStation 2: 1.3.0 or later
- BioStation A2: 1.2.0 or later
- BioStation L2: 1.1.0 or later
- BioEntry W2: 1.0.0 or later

BioStar 2.2.2

New and improved features

- BioEntry W2 support

Compatible firmware

- BioLite Net: 2.2.3 or later
- BioEntry Plus: 2.2.3 or later
- BioEntry W: 2.2.3 or later
- Xpass: 2.2.3 or later
- Xpass S2: 2.2.3 or later

1 BioStar 2 Overview

- BioStation 2: 1.3.0 or later
 - BioStation A2: 1.1.0 or later
 - BioStation L2: 1.0.0 or later
 - BioEntry W2: 1.0.0 or later
-

BioStar 2.2.1

New and improved features

- BioStation L2 support
- Long-term idle user management
- Access control privilege management per user
- Automatic database backup
- Enrollment device management
- Custom user fields

Compatible firmware

- BioLite Net: 2.2.3 or later
 - BioEntry Plus: 2.2.3 or later
 - BioEntry W: 2.2.3 or later
 - Xpass: 2.2.3 or later
 - Xpass S2: 2.2.3 or later
 - BioStation 2: 1.3.0 or later
 - BioStation A2: 1.1.0 or later
 - BioStation L2: 1.0.0 or later
-

BioStar 2.2.0

New and improved features

- BioStation A2 support
- Access On Card
- Secure Credential Card
- Global Anti-passback zone
- Image Log

Compatible firmware

- BioLite Net: 2.2.3 or later
- BioEntry Plus: 2.2.3 or later
- BioEntry W: 2.2.3 or later
- Xpass: 2.2.3 or later

1 BioStar 2 Overview

- Xpass S2: 2.2.3 or later
 - BioStation 2: 1.2.0 or later
 - BioStation A2: 1.0.0 or later
-

BioStar 2.1.0

New and improved features

- BioStar API
- DM-20 support
- Global Anti-passback zone / Local Fire Alarm zone / Local Anti-passback zone
- More secure login password
- License management
- BioStar 2 Cloud support
- BioStar 2 Mobile support
- Zone status monitoring

Compatible firmware

- BioLite Net: 2.0.4 or later
 - BioEntry Plus: 2.0.4 or later
 - BioEntry W: 2.0.4 or later
 - Xpass: 2.0.4 or later
 - Xpass S2: 2.0.4 or later
 - BioStation 2: 1.0.1 or later
-

BioStar 2.0.1

New and improved features

- BioStation 2 support
- Wireless LAN configuration
- T&A configuration
- Interphone configuration
- Display and sound configuration
- CSV import and export
- Multi-language resource support
- Memory optimization of BioStar 2 server

Compatible firmware

- BioLite Net: 2.0.0 or later
- BioEntry Plus: 2.0.0 or later

1 BioStar 2 Overview

- BioEntry W: 2.0.0 or later
- Xpass: 2.0.0 or later
- Xpass S2: 2.0.0 or later

Before using BioStar 2 to implement an access control system, the BioStar 2 server must be installed on the administrator PC.

The BioStar 2 server receives event logs, user information, etc. from connected devices and stores them.

BioStar 2 can be installed easily. Before installation, please check the [system requirements](#).

The BioStar 2 installation file can be found on the Suprema's home page(www.supremainc.com).

System Requirements

Installing BioStar 2

Minimum System Requirements

Item		Small	Medium	Enterprise
Environment	Total Devices	50	100	1,000
System requirement (Server)	OS	<ul style="list-style-type: none">▪ Windows 7 Home Basic 64bit SP1 or later▪ Windows 7 Home Basic 32bit SP1 or later	<ul style="list-style-type: none">▪ Windows Server 2008 R2 Standard 64bit SP2 or later▪ Windows 7 Home Premium 64bit SP1 or later	<ul style="list-style-type: none">▪ Windows Server 2008 R2 Standard 64bit SP2 or later▪ Windows 7 Home Premium 64bit SP1 or later
	Database	MariaDB 10.1.10, MS SQL Server 2012, MS SQL Server 2014 SP2, MS SQL Server 2016 SP1, MS SQL Server 2017, MS SQL Server 2019		
	CPU	2 GHz Dual Core	4 GHz Quad Core	4 GHz 16 Core
	RAM	8 GB	16 GB	32 GB
	SSD	512 GB	1 TB	1 TB
	Others	Java 1.8.0_201		
System requirement (Client)	CPU	1 GHz	1 GHz	1 GHz
	RAM	4 GB	4 GB	4 GB
	Web Browser	Google Chrome 75 or later		

2 Installation

BioStar 2 Video Extension

Item	Minimum	Recommended
CPU	4 GHz Quad Core	4 GHz Quad Core
RAM	8 GB	16 GB
HDD	2 TB	4 TB

Note

- For the best performance, use only the 64-bit operating system.
- BioStar 2 is optimized for Google Chrome.
- To use the **Video** menu, use the 64bits MariaDB or MS SQL database.
- BioStar 2 supports Windows 7, but Microsoft's technical support for Windows 7 has ended. Be aware of the OS selection when installing the system.
- If you are using Windows 8.1 or Windows Server 2012 R2, install the KB2919355 update by referring to the following web page.
<https://support.microsoft.com/en-us/help/2919355/windows-rt-8-1--windows-8-1--and-windows-server-2012-r2-update-april-2>
- If MS SQL Server and BioStar 2 are installed on different PCs, you should install the Native Client on a PC with BioStar 2 installed.
<https://www.microsoft.com/en-us/download/details.aspx?id=50402>
- Oracle Database is no longer supported. For details, please contact the Suprema Technical Support.

Installing BioStar 2

BioStar 2 supports a 32-bit operating system and a 64-bit operating system. Check the system type of your PC where BioStar 2 is to be installed and carry out its installation accordingly.

Note

- Do not install BioStar 2 on a PC where BioStar 1 is installed. This may cause performance problems.
- If BioStar 2.3.0 is installed on top of a BioStar 2.2.1 or 2.2.2 installation, all information stored in the SQLite database is migrated to a new MariaDB database.
- Upgrading directly from the existing version to the latest version is possible from BioStar 2.6.0 or higher. If the installed version is lower than 2.6.0, installing all versions in a correct sequence until reaching version v2.6.0 is essential.

Current Version	Upgrade Path
2	2.2.1 > 2.3 > 2.4 > 2.4.1 > 2.5.0 > 2.6.x or 2.7.x > 2.8.x
2.2	2.3 > 2.4 > 2.4.1 > 2.5.0 > 2.6.x or 2.7.x > 2.8.x

2 Installation


2.2.1	2.3 > 2.4 > 2.4.1 > 2.5.0 > 2.6.x or 2.7.x > 2.8.x
2.2.2	2.3 > 2.4 > 2.4.1 > 2.5.0 > 2.6.x or 2.7.x > 2.8.x
2.3	2.4 > 2.4.1 > 2.5.0 > 2.6.x or 2.7.x > 2.8.x
2.4	2.4.1 > 2.5.0 > 2.6.x or 2.7.x > 2.8.x
2.5	2.6.x or 2.7.x > 2.8.x
2.6	2.8.x
2.7	2.8.x

- If you are using Windows 8.1 or Windows Server 2012 R2, install the KB2919355 update by referring to the following web page.
<https://support.microsoft.com/en-us/help/2919355/windows-rt-8-1--windows-8-1--and-windows-server-2012-r2-update-april-2>
- If you are using MS SQL 2014 Express, install the Service Pack 2 by referring to the following web page.
<https://www.microsoft.com/en-us/download/details.aspx?id=53168>
- If MS SQL Server and BioStar 2 are installed on different PCs, you should install the Native Client on a PC with BioStar 2 installed.
<https://www.microsoft.com/en-us/download/details.aspx?id=50402>
- When backing up a database from an older version of BioStar 2, disable all services and procedures. Furthermore, if you do not back up and restore the AC database and the TA database together, you will not be able to use the TA database.
- If you want to back up the database of BioStar 2.8.6, be sure to also back up the **enckey** in the **W Program FilesW BioStar 2 (x64)W util** folder. Otherwise, the database will be unavailable.
- The default values for the ports used by BioStar 2 are as follows. If another program occupies the same port, BioStar 2 may not work properly.

Port

• HTTP Port


80



Available

• Web-socket Port


9002



Available

• Database Port


3312



Available

• T&A HTTPS Port


3002



Available

• AC Cloud Port


52000



Available

• HTTPS Port


443



Available

• API Port


9010



Available

• T&A HTTP Port


3000



Available

• T&A Cloud Port


52001



Available

• FastCGI Port

9000



Available

If you use a database configured by the user directly, check the following items before installing BioStar 2.

— MariaDB

2 Installation

- Open the **my.cnf** file and then change some configurations under [mysqld] as shown below.

```
character-set-server=utf8
collation-server=utf8_unicode_ci
max_connections = 600
```

- Open the **my.cnf** file and then add some configurations under [mysqld] as shown below.

```
log_bin_trust_function_creators = 1
group_concat_max_len = 102400
```

- Access MariaDB with the root permission and execute the following command.

```
> GRANT SUPER ON . TO user_id@'localhost' IDENTIFIED BY "password"
> GRANT SUPER ON . TO user_id@'%' IDENTIFIED BY "password";
```

— MS SQL Server

Setting the port

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

Creating the user and database

- a) Log in to the **sa** account using **SQL Server Authentication** in **SQL Server Management Studio**.
- b) Right-click on **Security** and click **New Login**.
- c) Enter the desired name in the **Login Name** field and select **SQL Server Authentication**.
- d) Enter the desired password in the **Password** and **Confirm password** field, and then uncheck the **Enforce password policy**.
- e) Click **OK** to save the settings.
- f) Right-click on **Database** and click **New Database**.
- g) Enter the desired name in the **Database Name** field.
- h) Enter the login name in the **Owner** field. Use the login name set in step c).
- i) In the **Database Files** section, we recommend that set the **Initial Size (MB)** to 3000 and set the **Autogrowth/Maxsize** to **By 10 MB, Unlimited**.

Setting the Windows Authentication database

2 Installation

1. Presetting

If you are using Microsoft Windows Active Directory, complete the presets as below before setting up the Windows Authentication database.

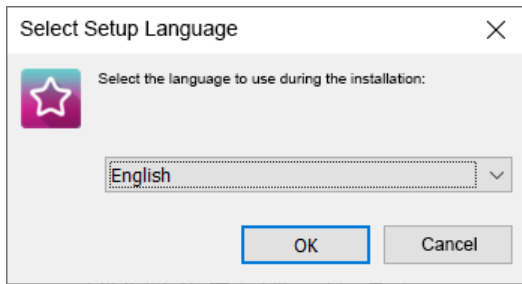
- a) Log in to **SQL Server Management Studio** with an administrator account.
- b) Right-click on **Security** and click **New Login**.
- c) Select **Windows Authentication** and click **Search**.
- d) In the **Select a user or group** window, click **Location**, then select the Active Directory path and click **OK**.
- e) Enter the user name in the object name field, then click **Check Names** > **OK**.
- f) Click **Server Roles** in the **Select a page**.
- g) Select **sysadmin** and click **OK**.
- h) Click **User Mapping** in the **Select a page**.
- i) Select **ac, master, ta, ve** and set the Default Schema to **dbo**.
- j) Click **OK** to save the settings.

2. Setting the database

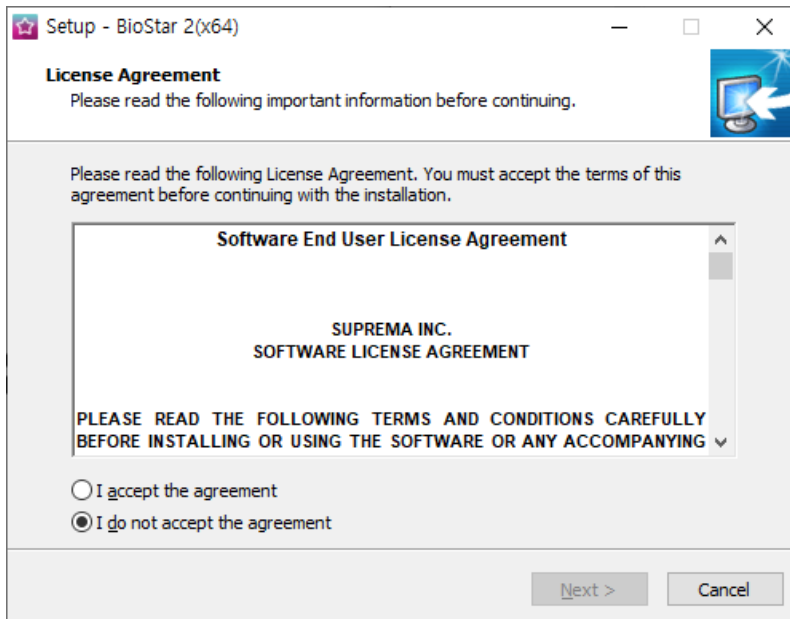
- a) Run **SQL Server Configuration Manager** and click **Client Protocol** under **SQL Native Client Configuration**.
- b) Select **TCP/IP** and check the default port.
- c) Click **Protocols for SQLEXPRESS** under **SQL Server Network Configuration**.
- d) Make sure that the ODBC port is set to the same as the default port in **TCP/IP**.
- e) Log in to **SQL Server Management Studio** by an administrator account.
- f) Click **Security** > **Logins** and then double-click **NT AUTHORITY \ SYSTEM**.
- g) Click **Server Roles** in the **Select a page**.
- h) Select **public, sysadmin**, and then click **OK**.
- i) Click **User Mapping** in the **Select a page**.
- j) Select the **ac, master, ta, ve** databases and click **OK** to save.

- 1) Double-click the downloaded setup program. (ex. 'BioStar 2 Setup.x.x.x.xxx.exe')
- 2) Select a language and click **OK**.

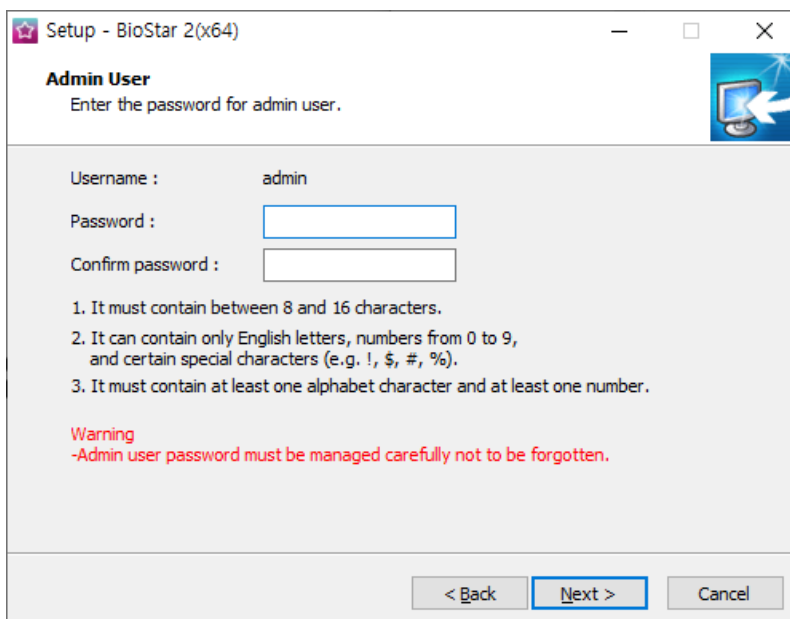
2 Installation



- 3) To continue the installation, select **I accept the agreement** and click **Next**.



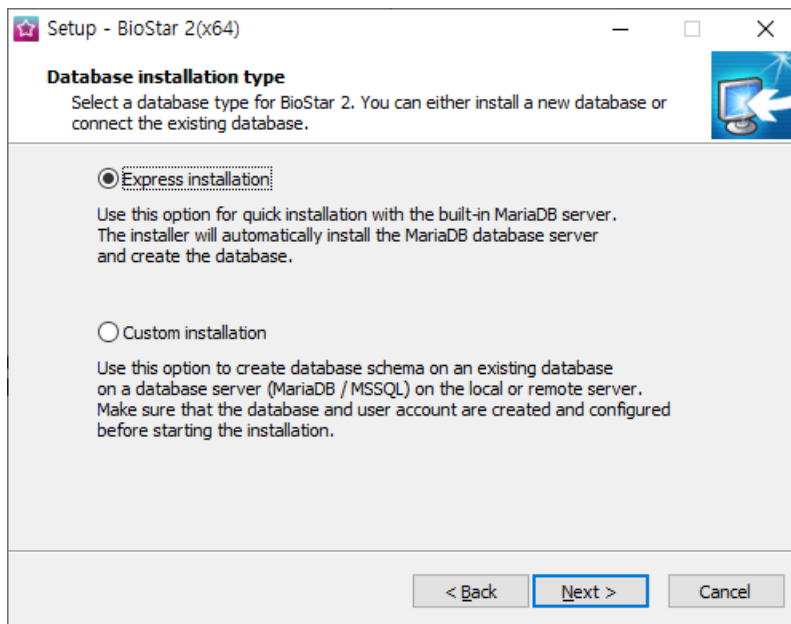
- 4) Enter the password for admin account and click **Next**. The password set in this step will be used when you log in to BioStar 2.



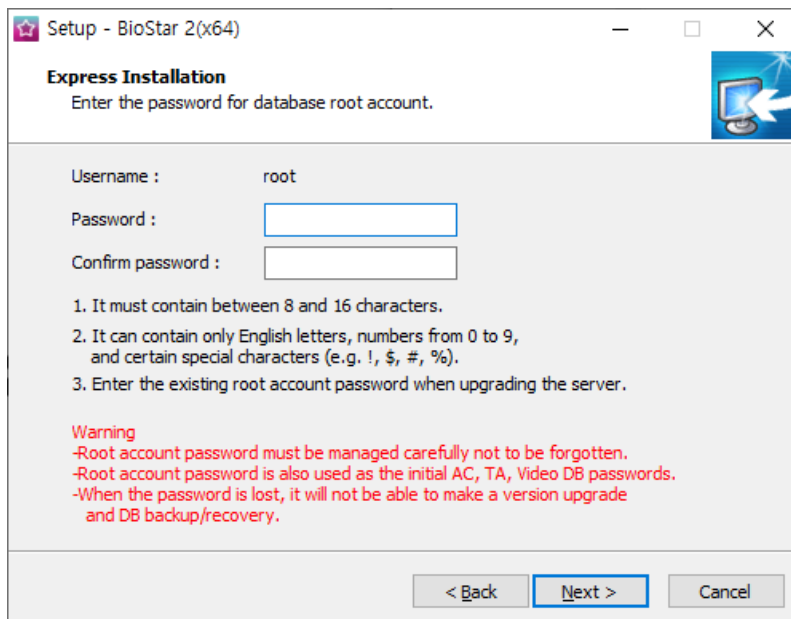
- 5) Install the database to be used in BioStar 2. You can install a new MariaDB or connect it to the already-installed MariaDB. Installing BioStar 2 for the first time, please select **Express Installation**

2 Installation

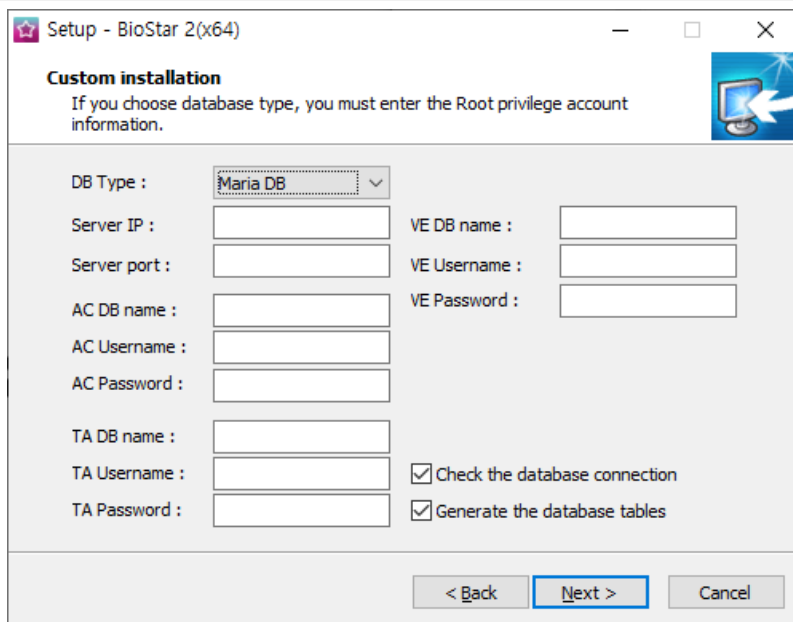
and click **Next**.



- 6) If **Express Installation** has been selected from **Database Installation Type**, enter the database manager's account password and click **Next**. If **Custom Installation** has been selected from **Database Installation Type**, enter the detailed information on the already-configured database and click **Next**.



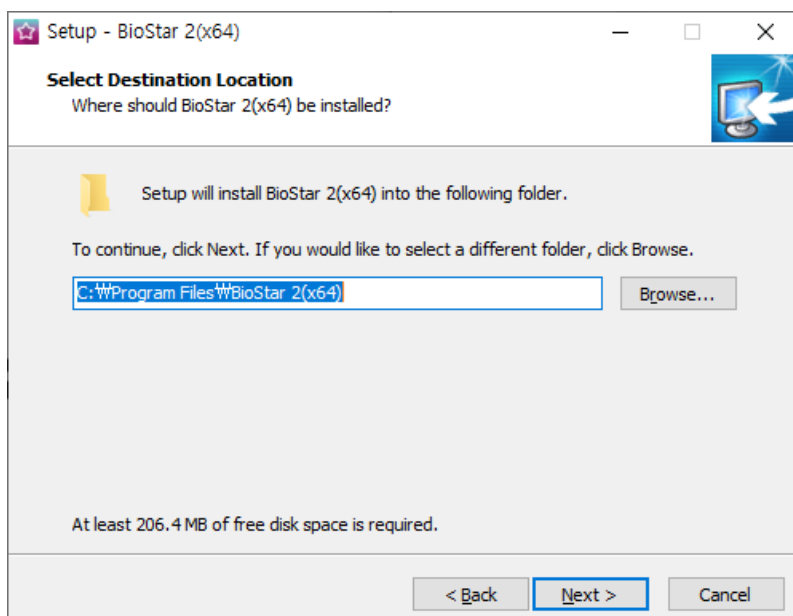
2 Installation



Note

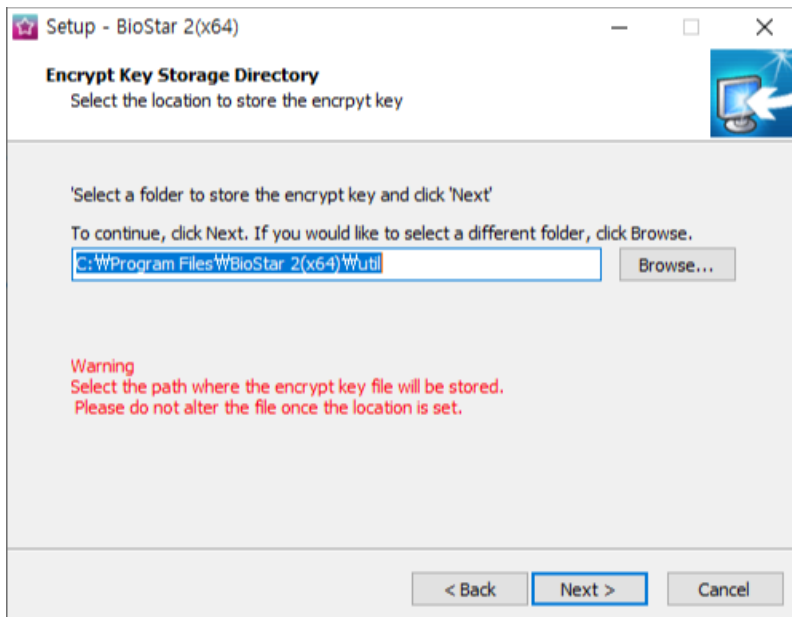
- BioStar 2.8.6 supports the following databases.
 - MariaDB 10.1.10
 - MS SQL Server 2012
 - MS SQL Server 2014 SP2
 - MS SQL Server 2016 SP1
 - MS SQL Server 2017
 - MS SQL Server 2019
- If the database table creation fails when MS SQL Server is set as the **Database Type**, you can create the table by executing the script in **C:\Program Files\BioStar 2 (x64)\dbscript\mysql** folder.

7) Click **Next** after setting a path for BioStar 2 to be installed.



2 Installation

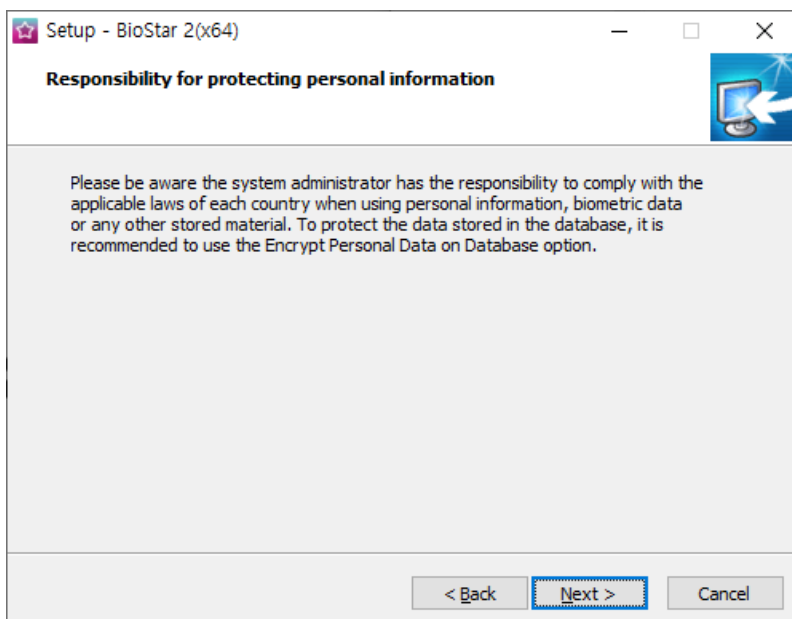
- 8) Click **Next** after setting a path for the encryption key to be stored.



Note

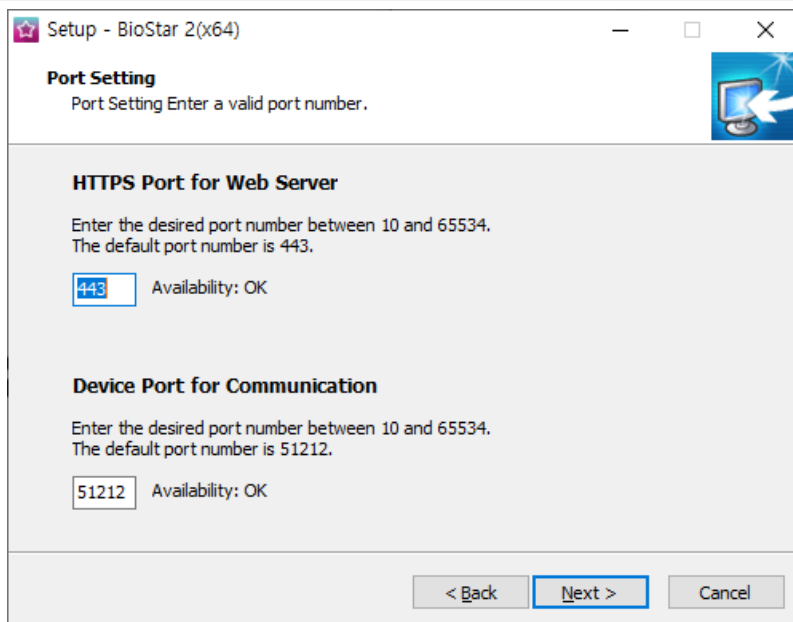
- You can set a path for the encryption key to be stored. However, if the encryption key file is modified or moved after selecting the path, a system error may occur.
- If you delete BioStar 2, the encryption key files will be deleted.

- 9) Read the instructions on the responsibility for protecting personal information stored in the database and click **Next** to continue the installation.



- 10) Enter the port number and click **Next**.

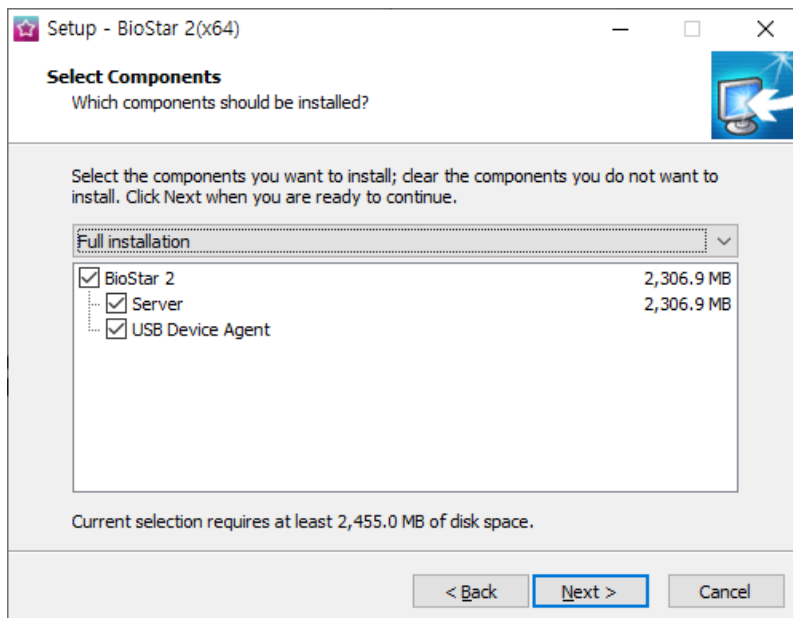
2 Installation



Note

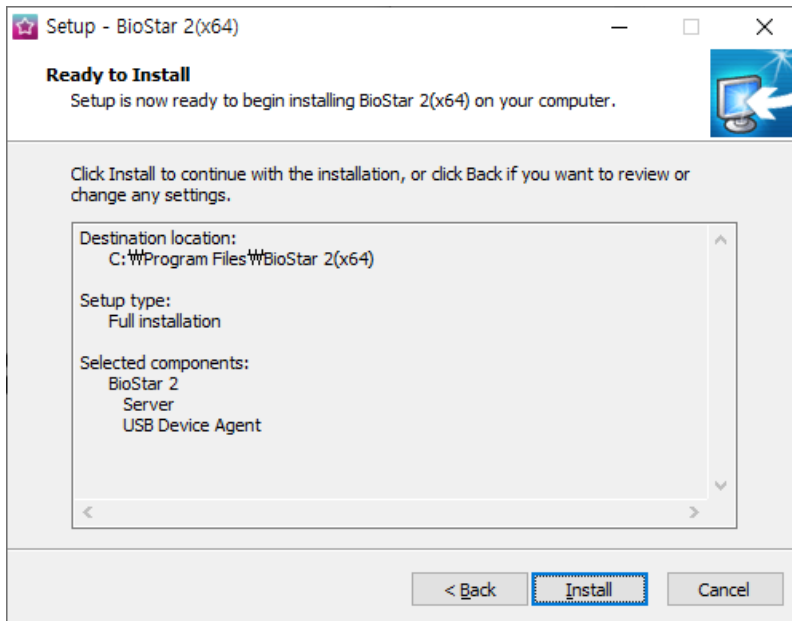
- When you install BioStar 2 on a PC where BioStar 1 is installed, the device port (51212) is not available. In this case, we recommend that you uninstall BioStar 1.

- 9) Select a component of BioStar 2 and click **Next**. If you select **USB Device Agent**, a USB-Agent and a driver for using BioMini, BioMini Plus 2, and DUALi DE-620 will be installed together.

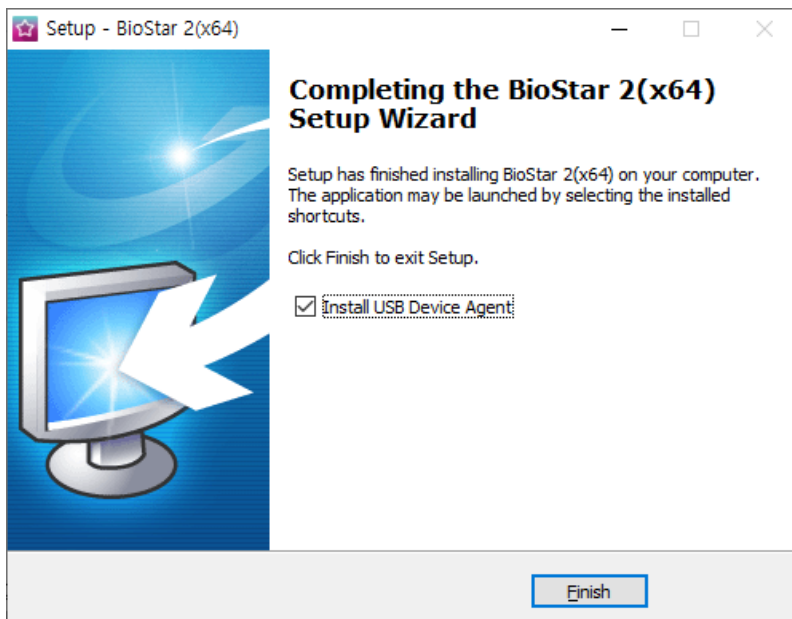


- 10) If ready to install, click **Install**.

2 Installation



- 11) Select whether to install additional program and click **Finish**. Follow on screen instructions to complete.



Note

- The USB Device Agent Certificate provided can be applied to a local network only.
- When another program uses port 443, BioStar-Setting program will be launched automatically and then you can change the port number. For more information, see [Changing port of BioStar 2](#).
- For more information on Database setting changes, see [BioStar 2 Database Change](#).

3 Login

BioStar 2 is a web-based system which can be accessed from anywhere as long as you remember your login ID and password.

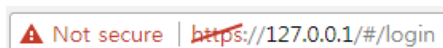
- 1) Run your web browser.
 - We recommend that you use Google Chrome 75 or later.
- 2) Run BioStar 2.
 - If running from the PC installed with BioStar 2, enter '<https://127.0.0.1>' in the address input field of the web browser.
 - If BioStar 2 is installed on another PC, enter '<https://BioStar 2 server IP address>' in the address input field of the web browser.
 - Do not use the 'Localhost' to access the BioStar 2.

Note

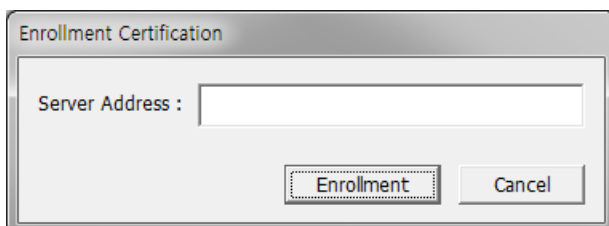
- BioStar 2 uses port 443. If port 443 is used by a program, quit the program and try again. If the program cannot be closed, run 'Biostar Setting' to change the port number. For more information, see [Changing port of BioStar 2](#).
- BioStar 2 uses Java version 1.8.0_201. If BioStar 2 does not run correctly, re-install Java version 1.8.0_201.

<http://www.oracle.com/technetwork/java/javase/downloads/java-archive-javase8-2177648.html>

- 3) Log in with the administrator account. The administrator account ID is 'admin' and when you log in for the first time, **Not secure** warning will be displayed in the address bar.



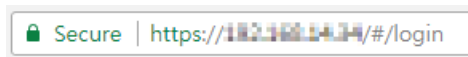
- 4) To use HTTPS properly, register the IP address of the PC where BioStar 2 is installed. Click **Download https certification install program**.
- 5) Unzip the downloaded file and run **cert-register.exe** file. **Enrollment Certification** window will appear.
- 6) Enter the IP address of the PC where BioStar 2 is installed and click **Enrollment**.



- 7) Check the security warning message and click **Yes**.

3 Login

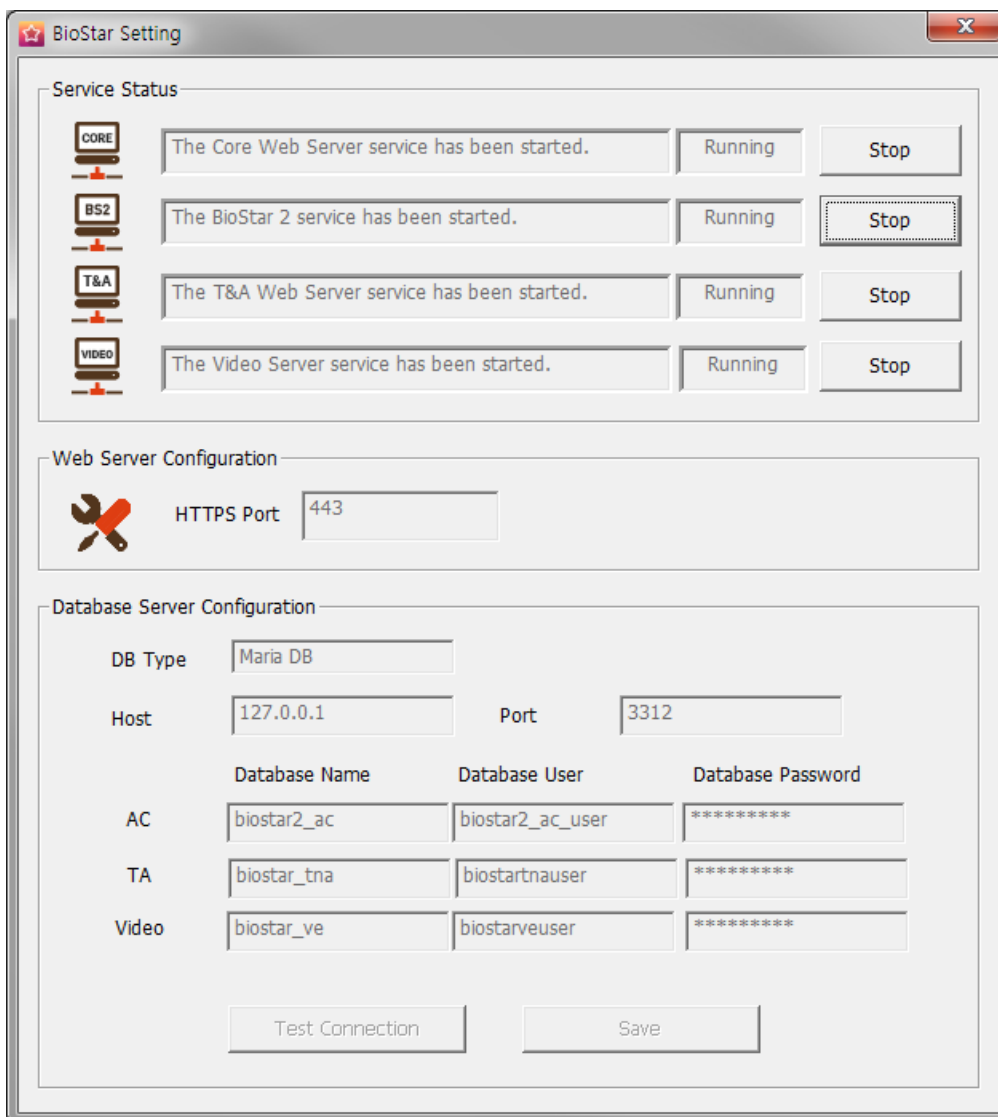
- 8) When you restart the web browser and enter the registered IP address, **Secure** will appear on the address bar of the web browser.



Changing server status of BioStar 2

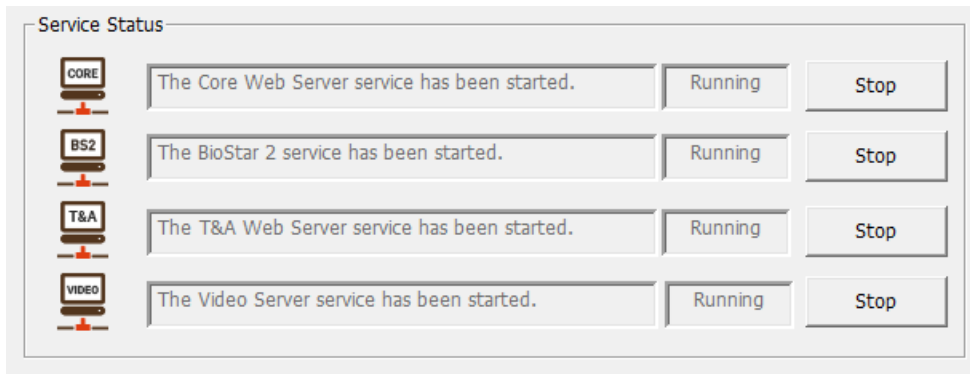
You can check the status of the BioStar 2 server and stop or start the server.

- 1) Click  **Start > All Programs > BioStar 2 > BioStar Setting.**



- 2) Click **Stop** button of the server you want to stop.

3 Login



- 3) Click **Start** button to restart the server.



Note

- If the time setting on the BioStar 2 server has changed, stop and restart the Core Web Server. Otherwise, BioStar 2 may not work properly.

Changing port of BioStar 2

You can change the port used by BioStar 2.

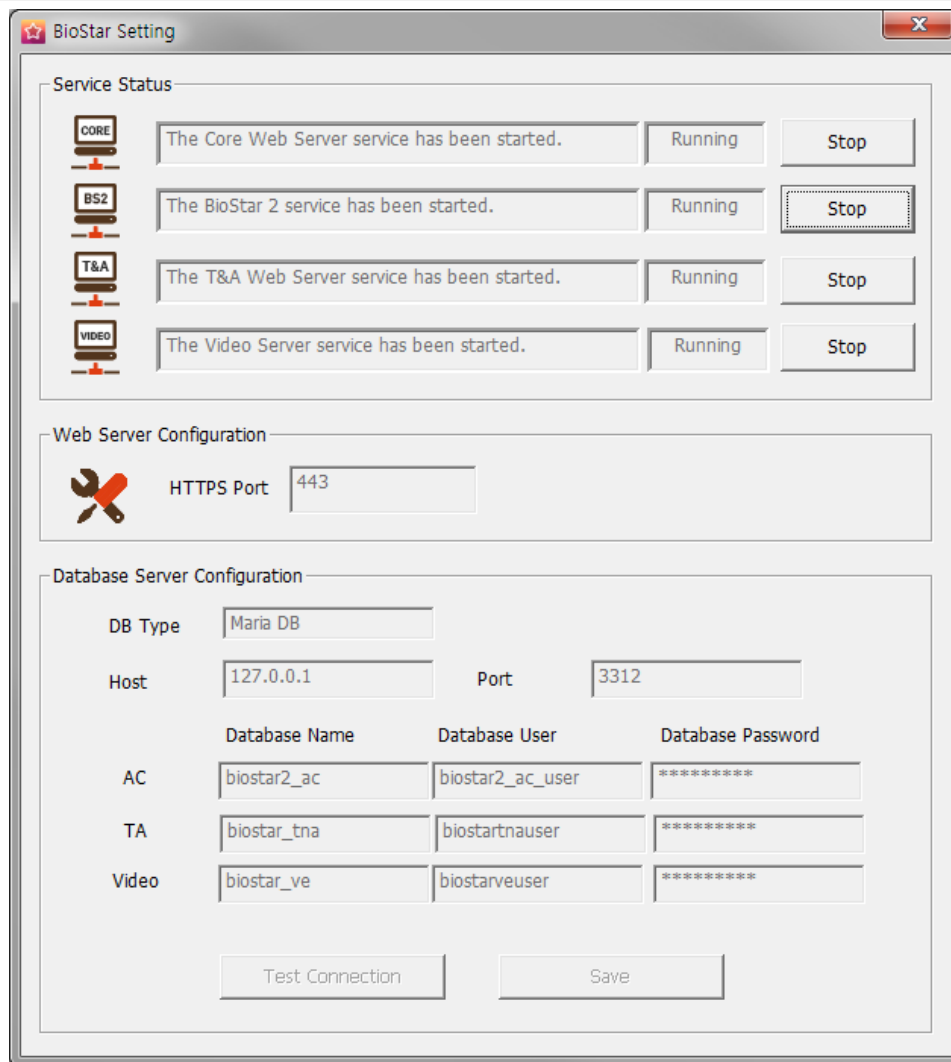
Note

- If you use MS SQL as a database, when changes the port in BioStar 2, you must also change the port manually in the database. Otherwise, BioStar 2 may be disconnected from the database and may not work properly.

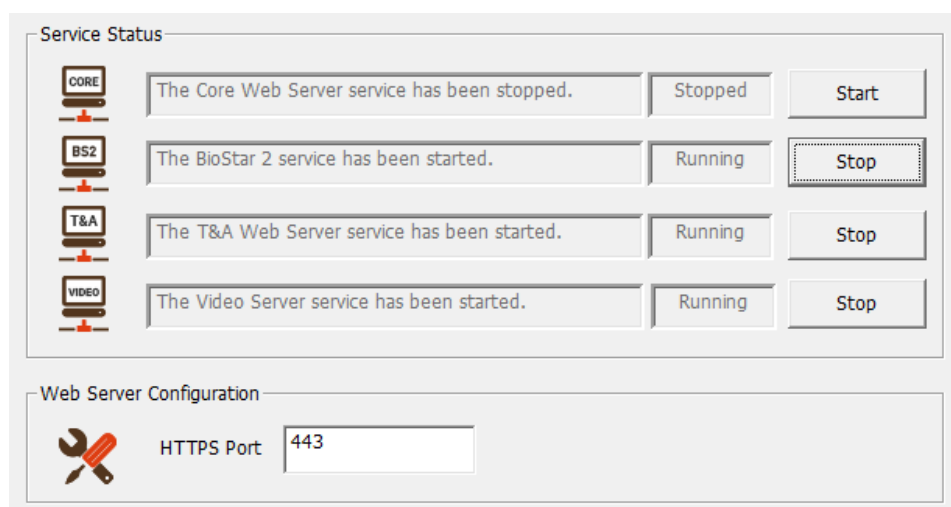
Changing with BioSar Setting (HTTPS port)

- 1) Click  **Start** > **All Programs** > **BioStar 2** > **BioStar Setting**.

3 Login



- 2) Click **Stop** button of Core Web Server.
- 3) Enter the port number in **HTTP port** field.



- 4) Click **Start** button of Core Web Server.
- 5) Run BioStar 2.
 - If using port 450, enter '*IP address::450*'.











3 Login


Changing with BioStar 2 for all port

Note

- The items may vary depending on the type of license that is activated.

- 1) Log in to BioStar 2 and click on the port. All ports in use in BioStar 2 are displayed.

Port			
• HTTP Port	80		Available
• Web-socket Port	9002		Available
• Database Port	3312		Available
• T&A HTTPS Port	3002		Available
• AC Cloud Port	52000		Available
• HTTPS Port	443		Available
• API Port	9010		Available
• T&A HTTP Port	3000		Available
• T&A Cloud Port	52001		Available
• FastCGI Port	9000		Available

- 2) Click the  of the port to change and enter the desired value.
- 3) Click **Apply** to save the settings.

Changing database of BioStar 2

You can change the database settings of BioStar 2.

- 1) Click  **Start** > **All Programs** > **BioStar 2** > **BioStar Setting**.

3 Login

The BioStar Setting window is divided into three main sections:

- Service Status:** Contains four service entries, each with a status icon, a description, a status label, and a control button.

Service	Status	Action
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:** Includes a wrench icon and an HTTPS Port field set to 443.
- Database Server Configuration:** Includes fields for DB Type (Maria DB), Host (127.0.0.1), and Port (3312). It also has a table for database credentials.

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

Buttons for 'Test Connection' and 'Save' are at the bottom.

- 2) Click **Stop** button of Core Web Server and Core Web Server. Database Server Configuration will be enabled.

This is a close-up view of the Database Server Configuration section from the BioStar Setting window. It shows the following fields and controls:

- DB Type: Maria DB
- Host: 127.0.0.1
- Port: 3312
- Database Name, Database User, and Database Password fields for AC, TA, and Video services.
- Buttons: Test Connection and Save.

- 3) Edit the necessary fields. If you are not sure about the each information, contact your system

3 Login

administrator.

- 4) Click **Test Connection** to check if the database has been set properly.
- 5) Click **Save** to save the settings.

BioStar 2 provides web-based services and various functions concerning access control.

Access groups configured in BioStar 2 refer to access privileges. An access group can be configured using a combination of user, access level and door (device) information.

Below is a step-by-step guide on how to use BioStar 2.

☐ Step 1. Register Activation Key

You can use more features by registering the activation key after purchasing the BioStar 2 license.

Related Information

[Server](#)

☐ Step 2. Adding Devices

Add devices to connect to BioStar 2. You can set up an authentication mode for each device type or assign an administrator to each device.

You can also configure actions to be performed according to various events (authentication failure, duress fingerprint authentication, Anti-passback violation, etc.) occurring in the device.

Related Information

[Adding and Managing Device Groups](#)

[Basic Search and Registration](#)

[Advanced Search and Registration](#)

[Slave Device Search and Registration](#)

[Editing Device Settings and Information](#)

☐ Step 3. Adding and Configuring Doors

Add the information on the doors installed with devices. You can configure relay, Anti-passback, dual authentication, alarm, etc.

Related Information

[Adding and Managing Door Groups](#)

[Add Door](#)

4 Before Using

❑ Step 4. Configuring Access Levels

You can create an access level by combining door and schedule information. Multiple doors and schedules can be registered to a single access level.

➤ **Related Information**

[Adding and Managing Access Levels](#)

❑ Step 5. Configuring Access Groups

You can create an access group by combining access level (doors and schedules) and user information. Multiple access levels and users can be registered to a single access group.

➤ **Related Information**

[Adding and Managing Access Groups](#)

❑ Step 6. Adding Users

Add the information to use for access control such as user information, fingerprints, etc. User information can be registered directly on the device or on the PC running BioStar 2. You can also fetch the user information registered within the device to BioStar 2 or transfer the user information registered within BioStar to the device.

➤ **Related Information**

[Adding and Managing User Groups](#)

[Adding User Information](#)

[Adding User Credentials](#)

❑ Step 7. Zone Configuration

You can configure anti-passback and fire alarm zone. The fire alarm can be set to local zone and global zone. Only available when purchasing a standard license.

Related Information

[Zone](#)

[Zone Status](#)

4 Before Using

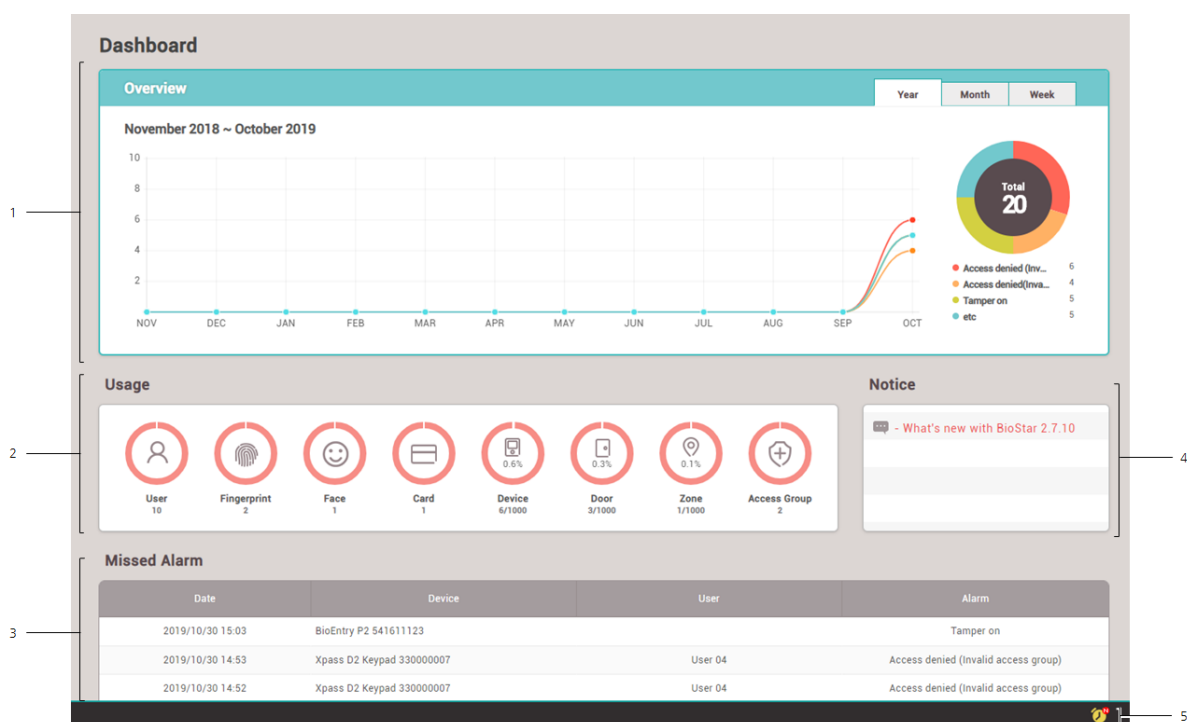
❑ Step 8. Viewing Logs

You can view event logs, device status, door status and alert history, or just view the real-time log information.

🕒 Related Information

Event Log
Real-time Log
Device Status
Door Status
Alert History

The **DASHBOARD** gives you an overview of the major event status, usage status, notice, alarms, etc.



1 Alert Event Status by Period

4 Notice

2 Usage Status

5 Alert List

3 Missed Alarm

📌 Note

- You can set what to display in "Alert Event Status by Period" in the **Setting > Alert**.

5 Dashboard

- 15 alarms that have been missed in the last 6 months are displayed in 'Missed Alarm' in the latest order.
- You can view the list of monitored alerts and write notes by clicking the alert list icon.

Alert List

View History

<<

<

1 / 1

>

>>

50 rows

	Date	Device	User	Alarm
<input type="checkbox"/>	2016/07/25 10:59	BioLiteNet 538101276		RS-485 disconnected
<input type="checkbox"/>	2016/07/25 10:58	BioStation 2 546832590 (192.168.16.108)	kyle	Access denied (Invalid access group)
<input type="checkbox"/>	2016/07/25 10:55	BioStation A2 541531008 (192.168.16.20...		Tamper on

Close

Related Information

Alert History

You can use the **DEVICE** menu to add, delete or edit registered devices, fetch the user information registered within the device to the server or upgrade the firmware.

[Adding and Managing Device Groups](#)

[Basic Search and Registration](#)

[Advanced Search and Registration](#)

[Wiegand Device Search and Registration](#)

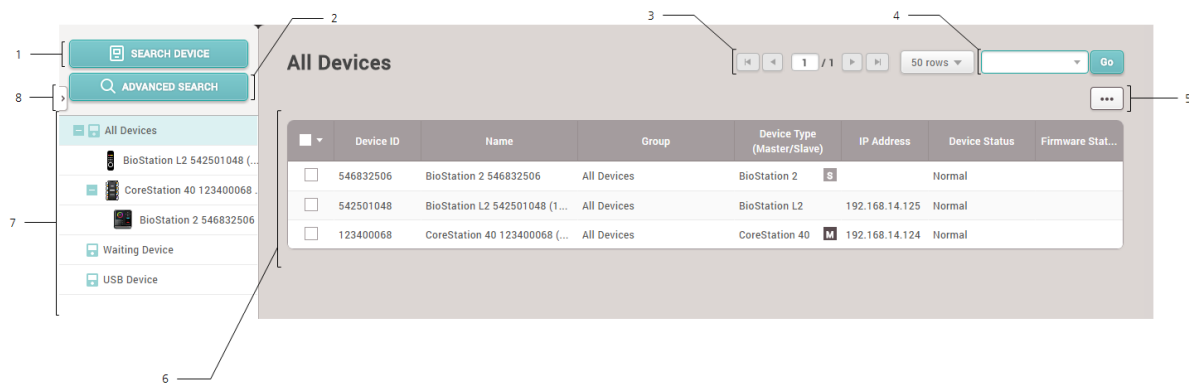
[Slave Device Search and Registration](#)

[Managing Users Registered with Devices](#)

[Upgrading Firmware](#)

[Editing Device Settings and Information](#)

6 Device



1 Basic Search

2 Advanced Search

3 Page Navigation Buttons and Number of List Rows

4 Registered Device Search

5 Function Button (Delete Data & Sync Device, Print, Column Setting)

6 Device List


7 Device and Group List

8 Expand Button

Note

- Registered devices can be searched by **ID, Name, IP Address**.
- Only BioMini can be connected as USB device.

When you select a device on the list, you can use the following functions.

- Reconnect:** Reconnects the selected device. This function is available when only one device is selected.
- Sync Device:** Synchronizes the user and access control information from BioStar 2 with the registered devices. The synchronization will occur based on the information on the server database, and the users that exist on the devices only will be deleted. Click **Manage Users in Device** to retrieve users from the device to the BioStar server.
- Delete Data & Sync Device:** You can delete user related data including users, access groups and schedules on the device and transfer the data on the server to the device. On the device list page, select the target devices, click the Function button () and choose the **Delete Data & Sync Device**.
- Batch Edit:** Edits the information on multiple devices at once. This function is available only when multiple devices are selected.
- Manage Users in Device:** Uploads the user information registered with the device to BioStar 2 or deletes it.
- Firmware Upgrade:** Easily upgrades the firmware of the device.
- Delete Device:** Deletes the selected device from the list. You cannot delete a device that is set as a door or a zone.

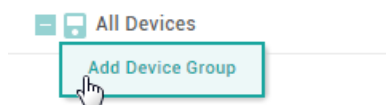
6 Device

Adding and Managing Device Groups

You can register device groups for easy management of multiple devices. Name your device groups according to installation locations of the devices for greater convenience.

— Adding Device Groups

- 1) Click **DEVICE**.
- 2) Right-click on **All Devices** and click **Add Device Group**.



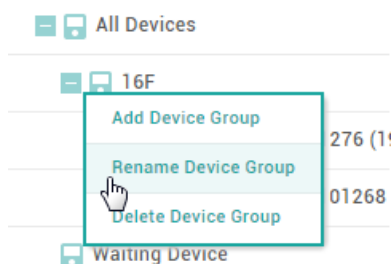
- 3) Enter a name.

📌 Note

- Device groups may be created in up to 8 levels.
- Up to 48 characters may be entered for a device group name.

— Renaming Device Groups

- 1) Click **DEVICE**.
- 2) Right-click on the name of a group you wish to rename and click **Rename Device Group**.



- 3) Enter a name.

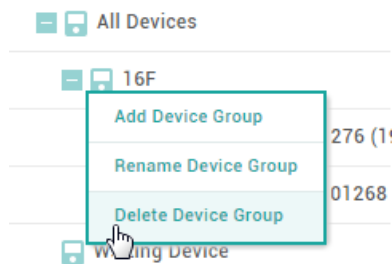
📌 Note

- Up to 48 characters may be entered for a device group name.

— Deleting Device Groups

6 Device

- 1) Click **DEVICE**.
- 2) Right-click on the name of a group you wish to delete and click **Delete Device Group**.



Note

- Deleting a group deletes all devices included in the group.

Basic Search and Registration

You can automatically search for devices connected to BioStar 2 and register them. Before searching for devices, check whether they are correctly connected. When adding multiple devices at once, it will be more convenient to know the location, ID and IP address information of each device in advance.

- 1) Click **DEVICE > SEARCH DEVICE**.
- 2) All available devices are shown. When the user ID type is mismatch with BioStar 2, the user ID type of the device will be automatically changed according to BioStar 2.

Search Device
×

⚙️
Search

Found 7 device(s). 2 device(s) have invalid IP addresses.

<input type="checkbox"/>	Device ID	Name	Group	Device Type (Master/Slave)	IP Address	Status	Secure Mode Status
<input type="checkbox"/>	541531041	BioStation A2 541531041 (...)	All Devices	BioStation A2 M	192.168.16.179	OK	Connectable.
<input type="checkbox"/>	546832590	BioStation 2 546832590 (19...)	All Devices	BioStation 2 M	192.168.16.196	OK	Connectable.
<input type="checkbox"/>	546832437	BioStation 2 546832437 (19...)	All Devices	BioStation 2	192.168.16.193	OK	Connectable.
<input type="checkbox"/>	541531014	BioStation A2 541531014 (...)	All Devices	BioStation A2 M	192.168.16.160	OK	Connectable.
<input type="checkbox"/>	539308121	BioEntryPlus 539308121 (1...)	All Devices	BioEntryPlus M	192.168.16.239	OK	Connectable.
<input type="checkbox"/>	544108056	BioEntry W2 544108056 (192.168.16.238)	All Devices	BioEntry W2 M	192.168.16.238	N/A (192.168.1.23)	Connectable.
<input type="checkbox"/>	542501008	BioStation L2 542501008 (192.168.16.231)	All Devices	BioStation L2	192.168.16.231	N/A (192.168.1.23)	Connectable.

Set IP
Add
Close

- 3) To view newly found devices only, click  and then click **Show New Devices Only**.

6 Device


Search Option

☒ Show New Devices Only

• Timeout(sec)

3

Note

- To hide devices which do not respond within a set period of time, click  and then enter a duration in **Timeout(sec)**.
- If the devices you are looking for are not shown on the list, click **Search** to search for the devices again.

- 4) You may change the **Name** and **Group** of a device found to anything you like. If the IP address of the device cannot be used or otherwise needs to be changed, click **Set IP** to change it.
- 5) To use a dynamic IP address, select **Use DHCP**. To manually enter the **IP Address**, **Subnet Mask** and **Gateway**, deselect the option. To enter the BioStar 2 network information, select **Device** → **Server** and enter the **Server IP** and **Server Port**.

Set IP

ID	Device Type
538102578	BioLiteNet

☒ Use DHCP

- IP Address 192.168.16.207
- Subnet Mask 255.255.255.0
- Gateway 192.168.16.1
- Device Port 51211

☒ Device → Server Connection

- Server IP 192.168.1.6
- Server Port 51212

Apply

Cancel

- 6) To save the IP settings, click **Apply**.
- 7) To register the configured device, click **Add**.
- 8) Select the registered device, and click **Sync Device**.

Note

- If you add a new device, the key of the device changed to the value of the data encryption key

6 Device

on the server. All user data on the device will be deleted when the key is changed.

- If you want to delete user related data including users, access groups and schedules on the device and transfer the data on the server to the device, click the **Delete Data & Sync Device**. On the device list page, select the target devices, click the Function button (⋮) and choose the **Delete Data & Sync Device**.
- After registering a device, you can edit its details by referring to [Editing Device Settings and Information](#).
- To register all waiting devices in the **Waiting Device** group, right-click on the group name and click **Add All Waiting Devices**. To register each device, right-click on the device name and click **Add Waiting Device**.
- If a different user ID type is set for BioStar 2 and a device, change the device setting according to the user ID setting of BioStar 2.
- If the user ID type of BioStar 2 is set with alphanumeric characters, some devices may not be used and/or limitations may occur. For more details, refer to [Server](#).

Advanced Search and Registration

You can register a device by specifying its IP address and port number.

- 1) Click **DEVICE > ADVANCED SEARCH**.
- 2) Enter the IP address and port number of a device to search.
- 3) Click **Search** to view the list of devices found. If the device you are looking for is not shown on the list, click **Search** to search again.

Advanced Search

Device ID	Name	Group	Device Type (Master/Slave)	IP Address
538101276	BioLiteNet 538101276 (192.168.1...	모든 장치	BioLiteNet	192.168.16.230

Search

Add

Cancel

- 4) Select a group to add the found device to and click **Add**.
- 5) Select the registered device, and click **Sync Device**.

Note

- After registering a device, you can edit its details by referring to [Editing Device Settings and Information](#).

6 Device



Wiegand Device Search and Registration

You can easily add Wiegand devices connected to master/slave devices.

- 1) Click **DEVICE**.
- 2) Right-click on the name of a master/slave device to search for Wiegand devices and click **Add Wiegand Device**.
- 3) The list of Wiegand devices connected to the master/slave device is shown.

Add Wiegand Device

DoorModule20 200000013 has 2 wiegand Device(s).

<input checked="" type="checkbox"/>	Wiegand Index	Name
<input checked="" type="checkbox"/>	0	Wiegand Reader 0 (1273741837) 
<input checked="" type="checkbox"/>	1	Wiegand Reader 1 (2347483661) 

Add

Cancel

- 4) Select the device to add, and click **Add**.

Slave Device Search and Registration

You can easily expand your access control system network by adding slave devices to existing master devices. Master devices and slave devices can be connected together via RS-485. Besides regular devices, additional devices such as Secure I/O can be connected.

- 1) Click **DEVICE**.
- 2) Right-click on the name of a master device to search for slave devices and click **Search Slave Device**.
- 3) The list of slave devices connected to the master device is shown. If the devices you are looking for are not shown on the list, click **Search** to search for the devices again.

6 Device

Search Slave Device

×

Search

<input type="checkbox"/>	Device ID	Name	Device Type
<input type="checkbox"/>	538101268	BioLiteNet 538101268	BioLiteNet

BioLiteNet 538101276 (192.168.16.230) has 1 slave Device(s).

Add

Cancel

- 4) Select a group to register the device to and click **Add**.

Note

- If the fingerprint authentication device is the master device, FaceStation 2 cannot be added as a slave device.
- FaceStation 2 cannot be added as a slave device with a different device. FaceStation 2 must be added separately.
- If FaceStation 2 is the master device and a different slave device has been added already, FaceStation 2 cannot be added as a slave device.
- When you connect FaceStation 2 as a slave device while FaceStation 2 is the master device, only one FaceStation 2 can be added as a slave device.

Managing Users Registered with Devices

You can see the number of users, fingerprints, faces, and cards stored in the device.

You can compare the user information stored in the device with the user information registered in BioStar 2, transfer the information to BioStar 2 or delete the information.

Note

- The **Manage Users in Device** function is available only when one device is selected.

- 1) Click **DEVICE**.
- 2) Select a device and click **Manage Users in Device**. A comparison of the user information registered within the device and the user information registered within BioStar 2 is displayed.

6 Device

Manage Users in Device

BioStation A2 541531008 (192.168.14.223)

◀◀

◀

1 / 2

▶

▶▶

50 rows ▼

👤 54

👤 9

😊 0

📄 1

☒ All Users

☐ Different Users

Upload

Delete

<div>☐ ▼</div>	User ID	<div>👤</div>	<div>😊</div>	1:1 Security Le...	Status
<div>☐</div>	50	0	0	Device Default	New User
<div>☐</div>	49	0	0	Device Default	New User
<div>☐</div>	48	0	0	Device Default	New User
<div>☐</div>	47	0	0	Device Default	New User
<div>☐</div>	46	0	0	Device Default	New User
<div>☐</div>	45	0	0	Device Default	New User
<div>☐</div>	44	0	0	Device Default	New User
<div>☐</div>	43	0	0	Device Default	New User

Close

- **Same:** The user's information is the same as the information registered within BioStar 2.
- **Different:** The user's information is different from the information registered with BioStar 2.
- **New User:** The user has not been registered with BioStar 2.

- 3) After selecting user information, click **Delete** to delete it or click **Upload** to upload it to BioStar 2. When you click **Upload**, if BioStar 2 contains user information of the same ID, it can be updated with the information in the device.

Note

- After registering a device, you can edit its details by referring to [Editing Device Settings and Information](#).
- When you delete user information, it is only deleted from the device and the information in BioStar 2 remains intact.

Upgrading Firmware

You can easily upgrade the firmware on any device connected to BioStar 2 without any additional connection or action.

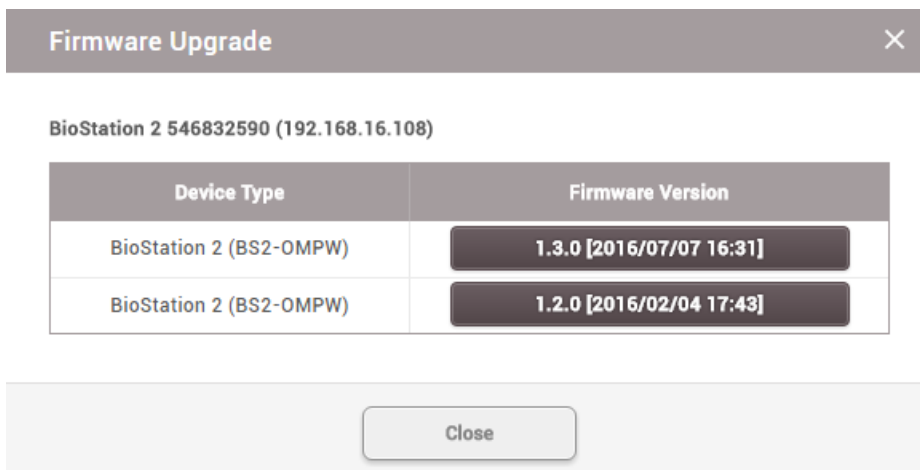
Copy the firmware files that you have downloaded to the following folder. If the folder does not exist, you need to create it.

- 32-Bit Operating Systems: C:\Program Files\BioStar 2\firmware

6 Device

- 64-Bit Operating Systems: C:\Program Files (x86)\BioStar 2\firmware

- 1) Click **DEVICE**.
- 2) Select a device and click **Firmware Upgrade**. Multiple devices of the same type can be batch upgraded.



- 3) Click the firmware version to start the upgrade.

Note

- It is possible to upgrade a number of devices with the same RS-485 mode simultaneously. For example, a number of master devices can be upgraded simultaneously and a number of slave devices can be upgraded simultaneously as well.
- It is possible to upgrade a number of master devices or slave devices that have no master device simultaneously.
- It is not possible to upgrade a number of slave devices which is connected to the same master device simultaneously.

Related Information

[Information](#)

Editing Device Settings and Information

You can edit detailed information of registered devices. For more information on registering devices, see [Basic Search and Registration](#) or [Advanced Search and Registration](#).

The details shown may vary depending on the RS-485 connection type or the device type.

- 1) Click **DEVICE**.

6 Device

- 2) Click a device on the device list to edit.
- 3) Edit the fields by referring to [Information](#), [Network](#), [Authentication](#), [Advanced Settings](#), [DM-20](#) , [OM-120](#), [CoreStation](#) and [Wiegand Device](#).
- 4) To edit information of multiple devices, select multiple devices and click **Batch Edit**.

Device Batch Edit

Devices (2)

- Use DHCP ☐ Use DHCP
- Full Access ☐ Full Access
- Time Zone
- Smart Card Layout
- Subnet Mask
- Gateway
- Matching Timeout
- Device Port
- Connection Mode ☐ Device ☒ Server Connection
- Server Address
- Server Port
- RS485
- Baud Rate

Apply Close

- 5) Click of the field you want to edit and edit the information.
- 6) After editing all information, click **Apply**.

Note

- The fields displayed for **Batch Edit** may vary depending on the device type selected.
- If you select both master devices and slave devices and click **Batch Edit**, only some of the [Authentication](#) and [Display/Sound](#) fields can be edited.

Information

You can enter or edit the name and the group of a device. If a new firmware version is available, you can upgrade to it.

6 Device


1) Edit all fields of the **Information** tab.

The screenshot shows the 'Information' tab of a device management interface. It contains the following fields and controls:

- Name:** CoreStation 40 123400068 (192.168.14.124) (Callout 1)
- Device ID:** 123400068 (Callout 2)
- Firmware Version:** 1.0.0 [2017/03/3...] with a **Firmware Upgrade** button (Callout 3)
- Kernel Version:** 1.0.0 [2017/03/3...] (Callout 4)
- Restore to default:** Buttons for **All** and **Without Network** (Callout 5)
- Time Zone:** (UTC) W. Europe Standard Time, London, Lis... (Callout 6)
- Daylight Saving Time:** (Callout 7)
- Group:** All Devices (Callout 8)
- Device Type:** CoreStation 40 (Callout 9)
- Product Name:** CoreStation (Callout 10)
- Hardware Version:** 1.0.0 (Callout 11)
- Locked:** Unlock button (Callout 12)
- Time Synchronization with Server:** Checked checkbox (Callout 13)
- System:**
 - Display Date:** 2018/03/01 (Callout 14)
 - Time:** 13:54:30 (Callout 15)
 - Buttons:** Get Time and Set Time (Callout 16)

No.	Item	Description
1	Name	Enter a device name.
2	Device ID	View the device ID.
3	Firmware Version	Click Upgrade to install a new firmware version.
4	Kernel Version	View the kernel version.
5	Restore to default	Reset the settings of the device. <ul style="list-style-type: none"> ▪ All: Reset all settings. ▪ Without Network: Reset all settings excluding the network settings.
6	Time Zone	Set the time zone of the device.
7	Daylight Saving Time	Apply the daylight saving time to the device. To add a new daylight saving time rule, see Daylight Saving Time .
8	Group	Change the device group. For more information on adding device groups, see Adding and Managing Device Groups .
9	Device Type	View the device type.
10	Product Name	View the model name.
11	Hardware Version	View the hardware version.
12	Locked	Unlock button will be available when the device is disabled via Trigger & Action .

6 Device

No.	Item	Description
13	Time Synchronization with Server	Select the option to synchronize the time information of the device with the server.
14	Date and Time	Click  to manually set the date and time. If the Time Synchronization with Server option is selected, the date and time cannot be selected manually.
15	Get Time	Click the button to fetch the time set in the device.
16	Set Time	Click the button to apply the time set in BioStar 2 to the device.

2) Click **Apply** to save the settings.

Note

- Make sure to set the correct date and time as they are recorded in the **Event Log** and the **Real-time Log**.

Network

You can configure various connection settings such as TCP/IP and RS-485, etc.

Note

- Editable fields vary depending on the device type.

1) Edit all fields of the **Network** tab.



6 Device

The screenshot shows a 'Network' configuration page with four sections: TCP/IP, WLAN, Server, and Serial. Each section has a corresponding number (1, 2, 3, 4) on the left side of the page.

- TCP/IP (1):** Includes a 'Use DHCP' checkbox (checked), 'IP Address' (192.168.16.107), 'Subnet Mask' (255.255.255.0), 'Gateway' (192.168.16.1), 'Device Port' (51211), and 'DNS Server Address' (empty).
- WLAN (2):** Includes a 'Use' checkbox (unchecked), 'Operation Mode' (Infrastructure), 'SSID' (empty), 'Authorization Type' (Open System), 'Encryption Type' (NONE), and 'Authorization Key' (empty).
- Server (3):** Includes a 'Device - Server Connection' checkbox (checked), 'Server Address' (192.168.16.46), and 'Server Port' (51212).
- Serial (4):** Includes 'RS485' (Master) and 'Baud Rate' (115200).

No.	Item	Description
1	TCP/IP	<p>You can configure the TCP/IP connection settings of the device.</p> <ul style="list-style-type: none"> ▪ Use DHCP: Select this option to allow the device to use a dynamic IP address. If this option is selected, network settings cannot be entered. ▪ IP Address, Subnet Mask, Gateway: Enter network settings of the device. ▪ Device Port: Enter a port to be used by the device. ▪ DNS Server Address: Enter a DNS server address. <p>Note</p> <ul style="list-style-type: none"> ▪ The devices and the firmware versions where a DNS server address can be entered are as follows. <ul style="list-style-type: none"> - BioStation L2 FW 1.0.0 or later - BioStation A2 FW 1.0.0 or later - BioStation 2 FW 1.2.0 or later - BioLite Net FW 2.2.0 or later - BioEntry Plus FW 2.2.0 or later - BioEntry W FW 2.2.0 or later - Xpass FW 2.2.0 or later - Xpass S2 FW 2.2.0 or later - FaceStation 2 FW 1.0.0 or later - BioLite N2 FW 1.0.0 or later - FaceLite FW 1.0.0 or later - XPass 2 FW 1.0.0 or later

6 Device

No.	Item	Description
2	WLAN	<p>Turns on or off the wireless LAN. You can also configure the wireless LAN related settings from the device menu. For the detailed information, refer to the device's user guide.</p> <p> Note</p> <ul style="list-style-type: none">▪ Only for BioStation 2, BioStation A2 and FaceStation 2.
3	Server	<p>You can enter connection settings to use in the server mode.</p> <ul style="list-style-type: none">▪ Device → Server Connection: Select this option to configure the BioStar 2 settings for connecting to the devices. If this option is selected, BioStar 2 server network settings can be entered.▪ Server Address: Enter the IP address or domain name of the BioStar 2 server.▪ Server Port: Enter the port number of the BioStar 2 server. <p> Note</p> <ul style="list-style-type: none">▪ The devices and the firmware versions where a domain address can be entered for the server address are as follows.<ul style="list-style-type: none">- BioStation L2 FW 1.0.0 or later- BioStation A2 FW 1.0.0 or later- BioStation 2 FW 1.2.0 or later- BioLite Net FW 2.2.0 or later- BioEntry Plus FW 2.2.0 or later- BioEntry W FW 2.2.0 or later- Xpass FW 2.2.0 or later- Xpass S2 FW 2.2.0 or later
4	Serial	<p>You can configure the connection mode and baud rate of devices connected over RS-485.</p> <ul style="list-style-type: none">▪ RS-485: Set a RS-485 mode.▪ Baud Rate: Set a baud rate of the RS-485 connection.

2) Click **Apply** to save the settings.

Authentication

You can configure the user authentication settings of the device.

 **Note**

- Editable fields vary depending on the device type.



6 Device

1) Edit all fields of the **Authentication** tab.

The screenshot shows the 'Authentication' tab in the BioStar 2 configuration interface. It is divided into three main sections: 'Authentication', 'Fingerprint', and 'Card Type'.
 1. **Authentication**: Contains a table for adding authentication modes (Fingerprint, Card, ID, etc.) and settings for 'Full Access' (Disable/Enable), 'Server Matching' (Inactive/Active), 'Auth Timeout' (10 sec), and 'Face Detection Level' (Not Use).
 2. **Fingerprint**: Contains settings for '1:N Security Level' (Normal), 'Sensor Sensitivity' (7), 'Template Format' (Suprema), 'View Image' (Disabled), 'Advanced Enrollment' (Enabled), 'Duplicate Check' (Disabled), 'Scan Timeout' (10 sec), '1:N Fast Mode' (Auto), 'Matching Timeout' (5 sec), 'Sensor Mode' (Auto On), and 'Fingerprint LFD' (Not Use).
 3. **Card Type**: Contains settings for 'CSN Card' (Enabled), 'Wiegand Card' (Enabled), 'Smart Card' (Enabled), and 'Mobile' (Enabled). It also includes checkboxes for various protocols like EM4100, Mifare/Felica, iCLASS, HID Prox, Classic/Plus, DesFire/DesFire EV1, SR/SE, SEOS, NFC, and BLE.

No.	Item	Description
1	Auth Mode	<p>You can configure the authentication modes of the device. BioStar 2 can use any combinations of fingerprint, ID, card, PIN and face as authentication modes.</p> <ul style="list-style-type: none"> Click + Add and create an authentication mode by dragging and dropping available options. Select a schedule and click OK to register the authentication mode. If no desired schedule is available, click + Add Schedule to create it. For more information on configuring schedules, see Schedules.





6 Device

No.	Item	Description
2	Full Access	You can grant full access to users registered within the device without setting any access groups.
3	Server Matching	<p>It is possible to set server matching. When Active is set, the authentication is carried out using the user information stored in the PC where BioStar 2 is installed, and when Inactive is set, the authentication is carried out using the user information stored in the device. When using server matching, the server matching of BioStar 2 should be also activated. For more information, refer to Server.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ The devices and the firmware versions where server matching can be used are as follows. <ul style="list-style-type: none"> - CoreStation FW 1.0.0 or later - BioEntry P2 FW 1.0.0 or later - BioEntry W2 FW 1.0.0 or later - BioStation L2 FW 1.0.0 or later - BioStation A2 FW 1.0.0 or later - BioStation 2 FW 1.2.0 or later - BioLite Net FW 2.2.0 or later - BioEntry Plus FW 2.2.0 or later - BioEntry W FW 2.2.0 or later - Xpass FW 2.2.0 or later - Xpass S2 FW 2.2.0 or later - BioLite N2 FW 1.0.0 or later - XPass D2 FW 1.0.0 or later - XPass 2 FW 1.0.0 or later - FaceStation 2 FW 1.4.0 or later ▪ Server Matching is not available for FaceLite.
4	Auth Timeout	<p>When using a combination of multiple credentials in Auth Mode, the system waits for this length of time to authenticate the second credential. Set a timeout period for authenticating the second credential after authenticating the first credential. If the second credential is not authenticated within this time, the authentication fails.</p>
5	Face Detection	<p>You can set an algorithm step for recognizing a face with a camera built in a device when a user tries to authenticate.</p> <p>If it is set to Normal, it can detect a face at an arm's length. If it is set to High, it can detect a face at a shorter distance. If it is set to Not Use, it cannot use the face recognition function.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ Only for BioStation A2.

6 Device

No.	Item	Description
6	Fingerprint / Face	<p>You can configure the detail settings concerning fingerprint authentication.</p> <ul style="list-style-type: none"> ▪ 1:N Security Level: You can set a security level to use for fingerprint or face authentication. The higher the security level is set, the false rejection rate (FRR) gets higher, but the false acceptance rate (FAR) gets lower. ▪ Scan Timeout: You can set a fingerprint scan timeout period. If the fingerprint is not scanned within the set time, the authentication fails. ▪ Sensor Sensitivity: You can set a sensitivity level of the fingerprint recognition sensor. Set the sensor sensitivity higher if you wish to use a higher sensor sensitivity level and obtain more detailed fingerprint information. ▪ 1:N Fast Mode: You can set the fingerprint authentication speed. Select Auto to have the authentication speed configured according to the total amount of fingerprint templates registered within the device. ▪ Template Format: You can view the fingerprint template format. ▪ Matching Timeout: You can set the matching timeout period. If the authentication is not completed within the set time, the authentication fails. ▪ View Image: Displays the image of the fingerprint on the screen during the authentication process. ▪ Sensor Mode: If the option is set to Auto On, the sensor will automatically go on when it detects a finger. If the option is set to Always On, the sensor will always be on. ▪ Advanced Enrollment: Checks the quality of the scanned fingerprint to avoid the poor quality fingerprint template enrollment. The user will be alerted when the quality of the fingerprint scanned is low and given enrollment instructions. ▪ Fingerprint LFD: It is possible to set the live fingerprint detection level. If the live fingerprint detection level is higher, the false rejection rate on actual human fingerprints will increase. ▪ Duplicate Check: You can check for duplicates when registering fingerprints or faces. ▪ Enrollment Time: If a face is not registered during the set time when registering a user's face, the face registration will be canceled. ▪ Motion Sensor: Set the sensitivity for detecting motion near the device. ▪ Ambient Brightness: Sense the brightness near the device and adjust the intensity of IR LED. ▪ Enhanced fake face enrollment block: It is possible to set the Enhanced fake face enrollment block. If the live face detection level is higher, the false rejection rate on actual faces will increase. ▪ Quick Enrollment: Set whether or not to use a Quick Enrollment. When you set this option to Enabled, the face registration procedure is set to 1 step. If you set the option to Disabled, it is set to 3 steps. To register high-quality face templates, disable Quick Enrollment.

6 Device

No.	Item	Description
		<p> Note</p> <ul style="list-style-type: none"> ▪ Fingerprint LFD is available only for BioStation A2, BioStation L2, BioEntry W2 and BioLite N2. ▪ Enrollment Time, Motion Sensor, Ambient Brightness, Enhanced fake face enrollment block and Quick Enrollment is available only for FaceStation 2.
7	Card Type	<p>You can set the type of card used by the device.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ The type of card supported by the device is displayed. <p>▪ CSN Card: You can select the CSN card and format type and set the byte order.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ If Format Type is set to Normal, the device will read the card serial number (CSN). If the option is set to Wiegand, the device will read the card serial number in a Wiegand format that the user has defined. ▪ If Format Type is set to Wiegand, you can select the Wiegand format to be used in the device. To set a new Wiegand format, refer to Wiegand. ▪ When Byte Order is set to MSB, the device reads a card ID from the highest byte to the lowest byte. For example, the highest byte of the card ID 0x12345678 is 0x12 and the device sequentially reads 0x12, 0x34, 0x56 and 0x78. When the option is set to LSB, the device reads a card ID from the lowest byte to the highest byte. <p>▪ Wiegand Card: You can select a Wiegand card type and set the Wiegand format.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ You can select the Wiegand format to be used in the device. To set a new Wiegand format, refer to Wiegand. <p>▪ Smart Card: It is possible to select the smart card layout to be used in the device. To set a new smart card layout, refer to Smart / Mobile Card.</p> <p>▪ Mobile Card: You can set the type of mobile card.</p>

 **Note**

- Changing the fingerprint template format makes all previously stored fingerprints unusable. Be

6 Device

sure to select the correct template format before registering user fingerprints.

- If **Full Access** is set to **Enable**, the device cannot be added to an **Access Level**.

- 2) Click **Apply** to save the settings.

⌕ Related Information

Server

Advanced Settings

You can set the administrator, display/sound and trigger & action.

- 1) Click **Advanced** tab.
- 2) Edit the fields by referring to [Administrator](#), [T&A](#), [Display/Sound](#), [Trigger & Action](#), [Image Log](#), [Wiegand](#), [Interphone](#) and [Camera](#).
- 3) Click **Apply** to save the settings.

📌 Note

- Editable fields vary depending on the device type.

Administrator

You can assign and manage administration rights of the devices.

📌 Note

- You can add and manage up to 1,000 administrators. The number of administrators that can be added depends on the device firmware version.


- 1) Click **+ Add** and select a user.

The screenshot shows the 'Administrator' settings page. On the left, there is a list of three administrators: 'All', 'User', and 'Configuration'. Each entry is preceded by a number (1, 2, 3) and a small red dot. To the right of the list, there are three rows, each with a 'Name' field and a '+ Add' button. The 'Name' fields are currently empty.

6 Device

No.	Item	Description
1	All	The assigned administrators can use all menu functions such as adding and editing users.
2	User	The assigned administrators can manage the user information but cannot change the display, sound, network and RS-485 settings of the device.
3	Configuration	The assigned administrators can change the display, sound, network and RS-485 settings of the device but cannot manage the user information.

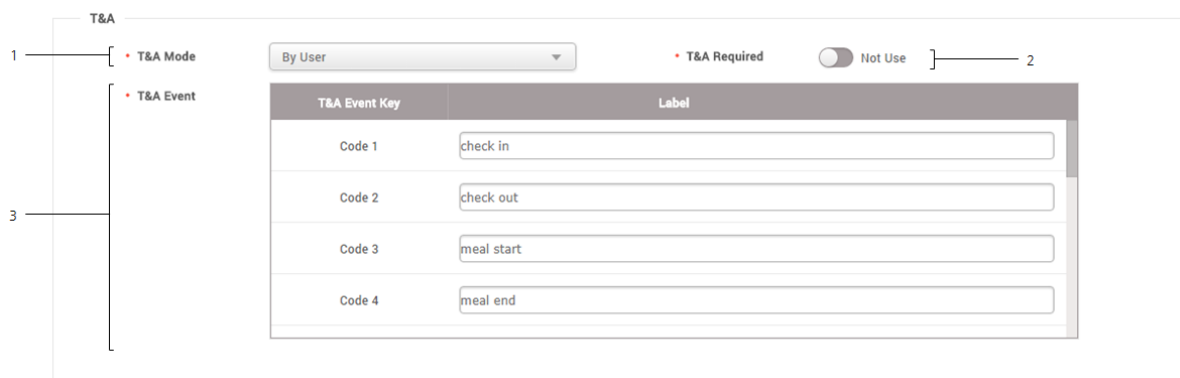
Note

- Click  to delete the registered users.
- The administrator settings configured for each device do not affect the BioStar 2 privileges.

T&A

You can change the device's name of the T&A event or configure the device's T&A Mode.

1) Edit the necessary fields.



No.	Item	Description
1	T&A Mode	<p>You can configure the T&A event settings.</p> <ul style="list-style-type: none"> ▪ Not Use: The user cannot record T&A events. ▪ By User: The user can manually select a T&A event before the authentication. ▪ By Schedule: T&A event automatically changes according to the pre-defined schedule. You can select the schedule under the T&A Event option. ▪ Last Choice: The T&A event that the last user has selected remains unchanged until you change the T&A event manually. ▪ Fixed: The user can use the fixed T&A event only. Configure the T&A

6 Device

No.	Item	Description
		Mode to Fixed and select the event you want to use as fixed.
2	T&A Required	The user will be forced to select a T&A event during the authentication process. The T&A Mode option must be set to By User in order to use the Require T&A option.
3	T&A Event	<p>You can set the name of T&A events or you can add schedules which will be used when you set the T&A Mode as By Schedule.</p> <ul style="list-style-type: none">▪ T&A Key: Lists the keys that you can use for T&A event selection. Choose one of the function keys that you want to edit.▪ Label: You can change the name of the T&A event for the T&A key.▪ Schedule: You can set a schedule for the By Schedule. The T&A mode must be set to By Schedule in order to enable this option. For more Information on configuring new schedules, see Schedules.

Note

- For a device with no LCD screen, T&A Mode can set to Fixed or By Schedule. You can register a fixed T&A event or a T&A event that changes according to the schedule.
Supported devices are BioEntry P2, BioEntry W2, BioEntry Plus, BioEntry W, Xpass, Xpass S2, XPass D2 and XPass 2.

Display/Sound

You can edit display and sound settings of the device. You can configure LED or buzzer action for each event.

Note

- Editable fields may vary depending on the device type.

1) Edit the necessary fields.

— BioEntry P2, BioEntry W2, BioLite Net, BioEntry Plus, BioEntry W, Xpass, Xpass S2, XPass D2, XPass 2

Note

- **Language, Menu Timeout, Backlight Timeout, Mgs. Timeout** can only be used by BioLite Net.

6 Device

Display/Sound

1 Language: English [Update Resource]

2 Volume: ON

3 Menu Timeout: 20 sec

4 Backlight Timeout: 20 sec

5 Msg. Timeout: 2.0 sec

6 LED/Buzzer

Event	LED	Buzzer
Normal	Infinite ON	Infinite OFF
Locked	BLUE 2000 msec	0 msec
RTC Error	CYAN 2000 msec	0 msec
Waiting Input	OFF 0 msec	0 msec
Waiting DHCP	OFF 0 msec	0 msec
Scan Finger	OFF 0 msec	0 msec
Scan Card	OFF 0 msec	0 msec
Auth Success	OFF 0 msec	0 msec
Auth Fail	OFF 0 msec	0 msec
Auth Duress	OFF 0 msec	0 msec

No.	Item	Description
1	Language	Sets the display language of the device. Click Update Resource to transfer a language resource file to the device.
2	Volume	Turns the sound on or off.
3	Menu Timeout	Sets the timeout period for changing from the menu screen to the standby screen.
4	Backlight Timeout	Sets the timeout period for the display backlight to turn off automatically.
5	Msg. Timeout	Sets the timeout period for various messages to disappear automatically.
6	LED/Buzzer	Selects an event and set LED or buzzer actions for the event.

— BioStation 2, BioStation L2, BioLite N2, FaceLite

Display/Sound

1 Language: 한국어 [Update Resource]

2 Volume: 10 %

3 Menu Timeout: 20 sec

4 Theme: Theme 1

5 Backlight Timeout: 20 sec

6 Msg. Timeout: 2.0 sec

7 Use Voice: Disabled

8 Background: Logo [Update] [Add] [Clear]

9 Sound



Start: Choose File [Find]

Verify Successful: Choose File [Find]


Verify Failed: Choose File [Find]

[Update]


6 Device

No.	Item	Description
1	Language	Sets the display language of the device. Click Update Resource to transfer a language resource file to the device.
2	Volume	Controls the volume.
3	Menu Timeout	Sets the timeout for the menu screen.
4	Theme	Changes the style of the device's home screen.
5	Backlight Timeout	Sets the timeout for the backlight.
6	Msg. Timeout	Sets the timeout period for various messages to disappear automatically.
7	Use Voice	Enables voice guidance.
8	Background	<p>Sets the items to be displayed on the device's home screen.</p> <ul style="list-style-type: none"> ▪ Logo: Displays the user's uploaded image on the home screen. You can upload an image by clicking Add. ▪ Notice: Displays messages typed by the administrator. ▪ Slide Show: Displays a slideshow of maximum 10 images. You can upload an image by clicking Add. <p> Note</p> <ul style="list-style-type: none"> ▪ Click Update to apply the configurations to the device instantly. ▪ Clicking Update will not apply when you change the type of the Background. Click Apply to save the configuration.
9	Sound	<p>Configures the sound effect for boot, authentication success, and authentication failure events. Click Find and select a *.wav file(less than 500KB).</p> <p> Note</p> <ul style="list-style-type: none"> ▪ Click Update to apply the configurations to the device in real-time.

6 Device

No.	Item	Description
1	Language	Sets the display language of the device. Click Update Resource to transfer a language resource file to the device.
2	Volume	Controls the volume.
3	Menu Timeout	Sets the timeout for the menu screen.
4	Backlight Timeout	Sets the timeout for the backlight.
5	Msg. Timeout	Sets the timeout period for various messages to disappear automatically.
6	Use Voice	Enables voice guidance.
7	Home Screen	<p>Sets the items to be displayed on the device's home screen.</p> <ul style="list-style-type: none"> ▪ Normal: Displays the default image on the home screen. ▪ Logo: Displays the user's uploaded image on the home screen. You can upload an image by clicking Add. ▪ Notice: Displays messages typed by the administrator. <p> Note</p> <ul style="list-style-type: none"> ▪ Click Update to apply the configurations to the device instantly. ▪ Clicking Update will not apply when you change the type of the Background. Click Apply to save the configuration. ▪ When you set Logo for Home Screen and set Slide Show Enabled, you can display a slideshow of maximum 10 images on the home screen. You can upload an image by clicking Add.

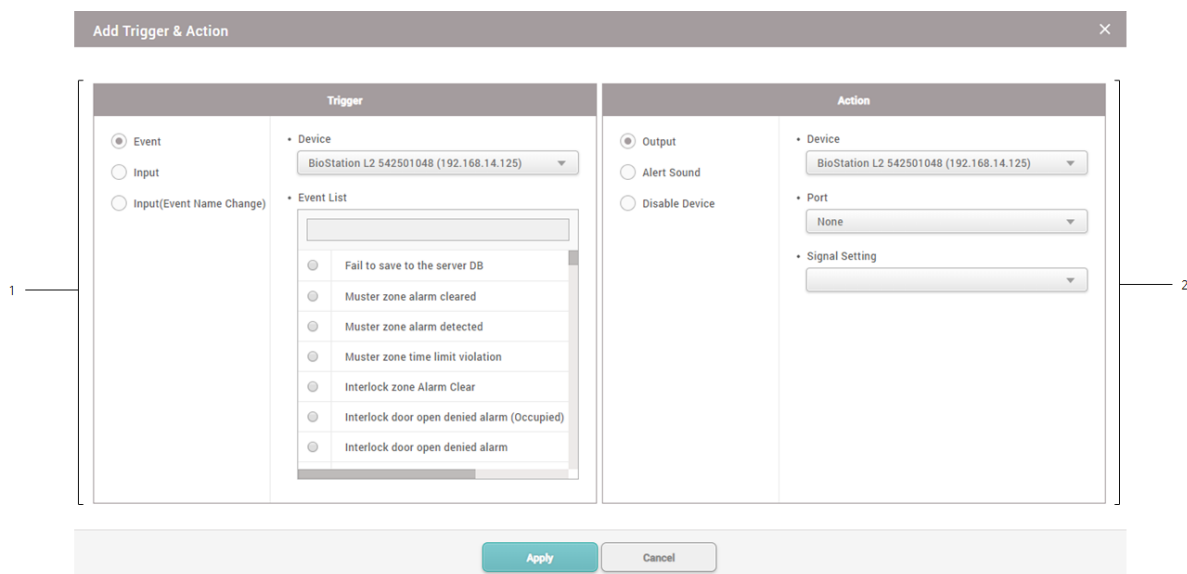
6 Device

No.	Item	Description
8	Sound	<p>Configures the sound effect for boot, authentication success, and authentication failure events.</p> <p>Click Find and select a *.wav file(less than 500KB).</p> <p> Note</p> <ul style="list-style-type: none"> Click Update to apply the configurations to the device in real-time.

Trigger & Action

You can configure triggers and actions for each situation. For instance, you can get all alarms to go off when an authentication fails or disable the device when its RS-485 connection is lost. You can select an event or you can configure the desired triggers and actions.

- 1) Click **+ Add** and configure the settings.



No.	Item	Description
1	Trigger	<p>You can select a pre-defined event or add a user defined trigger.</p> <ul style="list-style-type: none"> Event: You can select a pre-defined event. Input: You can set a user defined trigger by selecting Port, Switch, Duration (ms), and Schedule. Input(Event Name Change): You can set a user defined trigger by selecting Port, Switch, Duration (ms), Schedule and Event Name.

6 Device



		<p> Note</p> <ul style="list-style-type: none"> ▪ If you set the trigger as an event, you can select only one event from the event list. ▪ When configuring a user defined condition by selecting Input or Input(Event Name Change), if no desired schedule is available, click + Add Schedule to create it. For more information on configuring schedules, see Schedules. ▪ When configuring a user defined condition by selecting Input(Event Name Change), if no desired event name is available, click Add Event Name to create it. When the event occurs, the event name is displayed in the Event Log and Real-time Log. ▪ Up to 64 characters may be entered for the event name.
2	Action	<p>You can select a pre-defined action or add a user defined action.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ When configuring a user defined action by selecting Output, if no desired schedule is available, click + Add Schedule to create it. For more information on configuring schedules, see Schedules. ▪ If you set the trigger as Input(Event Name Change), you can set the Action to None.

Image Log

You can set an image log event and schedule to be used in the device. An image log can be used in the device with a built-in camera, and 25 types of event can be used.

 **Note**

- Only for BioStation A2 and FaceStation 2.

- 1) Set **Enabled** for the image log. It is possible to set **Preset** from **Setting > Image Log**. For more information, see [Image Log](#).
- 2) Click **+ Add** and set a desired event and schedule.

6 Device

Image Log

Image Log

Configuration

Enabled

Event	Schedule	
1:1 authentication succeeded	Always	
1:1 authentication failed	Always	
1:1 duress authentication succeeded	Always	
1:N authentication succeeded	Always	
1:N authentication failed	Always	
1:N duress authentication succeeded	Always	
Dual authentication succeeded	Always	
Dual authentication failed	Always	
Authentication failed	Always	
Access denied	Always	
Administrator menu entered	Always	

+ Add

Wiegand

You can define the Wiegand Input/Output.

1) Edit the necessary fields.

Wiegand

1

Input/Output

Input

2

Wiegand Input Format

Default

3

Output Mode

Normal

Fail Code

0x00

Pulse Width(μs)

40

4

Pulse Interval(μs)

10000

5

Output Info

Card ID

User ID

6

No.	Item	Description
1	Input/Output	You can select input/output mode.
2	Wiegand Input Format	You can set a format for Wiegand. For more information on setting a Wiegand format, see Card Format .
3	Output Mode	You can set the Wiegand signal output mode. If it is set to Normal , a card will be scanned in the set Wiegand format. If it is set to ByPass , CSN will be sent regardless of Wiegand authentication. ByPass should be set when using the device without an entrance door control function. If it is set to Normal mode, it is possible to set Fail Code , and select a value to be transmitted when Wiegand card authentication fails.
4	Pulse Width	You can set the pulse width of the Wiegand signal.

6 Device

5	Pulse Interval	You can set the pulse interval of the Wiegand signal.
6	Output info	You can select the information output to the device when the user authenticates.

Secure Tamper

If a tamper event occurs on the device, you can set to delete the entire user information, the entire log, and the security key stored on the device.

- 1) To use the secure tamper, set to **On**.

• Secure Tamper  On *** All the users, logs, and encryption key in the device will be removed at the secure tamper event.**

Interphone

You can set the interphone.

Analog Interphone

SIP Interphone

Analog Interphone

It is possible to set whether or not to use an analog interphone.

Note

- Only for BioStation 2.

- 1) Click **Use** to use a connected intercom.

Interphone

☐ Use

SIP Interphone

It is possible to set whether or not to use a SIP interphone.

Note

6 Device

- Only for BioStation A2 and FaceStation 2.
- It is recommended to use Asterisk for the SIP server.

- 1) Click Use to use a connected interphone.
- 2) Edit the necessary fields.

No.	Item	Description
1	SIP Server IP Address	You can enter the IP address of the SIP server.
2	SIP Server Port	You can set the SIP server port. The default value is 5061.
3	Account ID	You can enter the account ID of the SIP server.
4	Open Door Button(DTMF)	You can set a button for carrying out an entrance door relay.
5	Account Password	You can enter the account password of the SIP server.
6	Confirm Password	Enter the account password one more time.
7	DTMF Mode	You can set the mode for transmitting DTMF signals.
8	Extension Number	You can register up to 16 extension numbers. Click + Add to add an extension number.

Camera

It is possible to set the camera frequency. If you set the frequency incorrectly in the environment where the fluorescent light is used, flickering on the image may occur.

Different camera frequencies are used depending on geographic location. 60 Hz is generally used in

6 Device

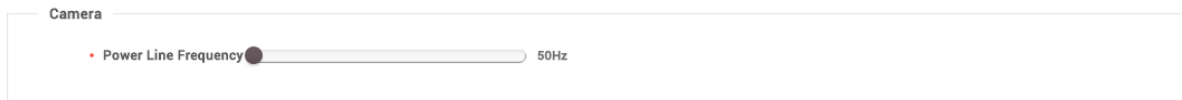
U.S., and 50 Hz is used in all other areas.

For the camera frequency of a given area, contact a sales agent.

Note

- Only for BioStation A2.

- 1) Select the frequency.



Thermal & Mask

You can set the detailed settings of thermal camera and mask detection.

Thermal camera with Suprema face recognition devices measures temperature of users passing the access point and limit the access of users with higher temperature than preset threshold. And the face recognition devices can also detect masks and restrict access to users without masks.

Note


- Only FaceStation 2 and FaceStation F2 support thermal cameras.
- The supported thermal cameras are as follows.
 - TCM10-FS2
 - TCM10-FSF2
- Only FaceStation F2 supports mask detection.

- 1) Edit the necessary items.

6 Device

No.	Item	Description
1	Mask Configuration	<p>You can set whether to use mask detection or not.</p> <ul style="list-style-type: none"> ▪ Mask Detection: You can set whether to use mask detection or not. If you select Use (Deny access when failed to detect mask), it refuses authentication of users who are not wearing a mask and saves event logs. If you select Use (Allow access after leaving log when failed to detect mask) users who are not wearing a mask can authenticate but event logs still be saved. ▪ Mask Detect Level: You can set sensitivity for mask detection.
2	Thermal Camera	<p>You can set options whether to use the thermal camera and edit the detailed settings.</p> <ul style="list-style-type: none"> ▪ Thermal Camera Use: You can set whether to use thermal camera or not. If you select Use (Deny access when exceeded threshold temperature), it refuses authentication of users with elevated temperature than the preset threshold and saves event logs. If you select Use (Allow access after leaving log when exceeded threshold temperature), users with elevated temperature than the preset threshold can authenticate but event logs still be saved. ▪ Celsius/Fahrenheit: Change the unit of temperature. ▪ Threshold Temp. (? / ?): Set the threshold temperature to limit the access. Users with detected temperature over the threshold will be denied access. ▪ Save Temp. Data: Save temperature data. When this mode is Enabled, it saves both authentication and temperature logs. When this mode is

6 Device

No.	Item	Description
		<p>Disabled, it only saves authentication logs.</p> <ul style="list-style-type: none"> ▪ Temp. Fail Sound: Set the alerts to trigger when the temperature is higher than the preset threshold. ▪ Show Infrared Image: Display infrared imaging on the screen of the devices. ▪ Camera Configuration: Configure the thermal camera settings for accurate measurement. <ul style="list-style-type: none"> - Temp. Correction (?): Depending on the device usage environment, the temperature can be calibrated to measure as high or low as a certain value. For example, in an environment where the temperature value is always measured high by 0.1? , set the temperature compensation value to -0.1? . - Distance(cm): Set up the distance between the user and device. - Emission Rate: Set up the emissivity to precisely measure the temperature of the user. - Dynamic ROI: If there are lights in the device field of view, you can set the thermal camera to automatically measure the user's temperature rather than that light. - ROI X(%), ROI Y(%), ROI Width(%), ROI Height(%): If you set Dynamic ROI to Disabled, you can manually set the ROI(Region of Interest). Set the temperature measurement area by adjusting the size and position of ROI. <p> Note</p> <ul style="list-style-type: none"> ▪ It is recommended to maintain the default values of the camera configuration settings for the best performance. The default values of each option are as follows: <ul style="list-style-type: none"> - Distance(cm): The distance may have different default values ? depending on the device. (FaceStation 2: 80 cm / FaceStation F2: 50 cm) - Emission Rate: 0.98 - ROI X(%): 30 - ROI Y(%): 40 - ROI Width(%): 40 - ROI Height(%): 20
3	Thermal & Mask Check Mode	<p>Set the thermal & mask check mode depending on the desired usage.</p> <ul style="list-style-type: none"> ▪ Check after authentication: Measure the temperature or detect the mask after a successful authentication. ▪ Check before authentication: Authentication is performed after checking whether the user is wearing a mask or measuring the temperature. When using this mode, it does not attempt to authenticate user's identity if they does not wear masks or their temperature has been detected to be above the threshold.

6 Device

No.	Item	Description
		<ul style="list-style-type: none"> ▪ Check without authentication: The device may only be used to determine whether a mask is worn or to measure temperature. In this mode, regardless of authentication, all users wearing a mask or below the reference temperature can enter.

- 2) Click **Apply** to save the settings.

DM-20

You can edit detailed settings of registered DM-20.

- 1) Click **DEVICE**.
- 2) Click a DM-20 on the device list to edit.

1

Information

Name

DoorModule20 200000013

Device ID

200000013

Device Type

DoorModule20

Firmware Version

1.0.8

Firmware Upgrade

Product Name

DM20

2

Advanced

Supervised Input

Configuration

Index	Supervised	Supervised Input Resistor
0	<input checked="" type="checkbox"/> Supervised	2.2kΩ
1	<input checked="" type="checkbox"/> Supervised	2.2kΩ
4	<input checked="" type="checkbox"/> Supervised	2.2kΩ
5	<input checked="" type="checkbox"/> Supervised	2.2kΩ

No.	Item	Description
1	Information	<p>You can modify the device's settings.</p> <ul style="list-style-type: none"> ▪ Name: Enter a device name. ▪ Device ID: View the device ID. ▪ Device Type: View the device type. ▪ Firmware Version: Click Firmware Upgrade to install a newer firmware version. ▪ Product Name: View the model name.

6 Device

No.	Item	Description
2	Advanced	You can modify the Supervised Input settings. The DM-20 can oversee the On, Off, Open, and Short status of the device connected to the Supervised Input port, and can set the terminating resistor as 1k Ω , 2.2k Ω , 4.7k Ω , 10k Ω .

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

OM-120

You can edit detailed settings of registered OM-120.

- 1) Click **DEVICE**.
- 2) Click a OM-120 on the device list to edit.

Information	
• Name	OM-120 12345678
• Device ID	12345678
• Device Type	OM-120
• Firmware Version	1.0.0 Firmware Upgrade
• Product Name	OutputModule
• Kernel Version	0.0.0
• Hardware Version	0.0.0

No.	Item	Description
1	Information	<p>You can modify the device's settings.</p> <ul style="list-style-type: none">▪ Name: Enter a device name.▪ Device ID: View the device ID.▪ Device Type: View the device type.▪ Firmware Version: Click Firmware Upgrade to install a newer firmware version.▪ Product Name: View the model name.▪ Kernel Version: View the kernel version.▪ Hardware Version: View the hardware version.

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

CoreStation

You can edit detailed settings of registered CoreStation.

6 Device

- 1) Click **DEVICE**.
- 2) Click a CoreStation on the device list to edit..
- 3) Edit the necessary items.

— Information

Information

Name

CoreStation 40 542070627 (192.168.14.205)

Device ID

542070627

Firmware Version

1.4.0 [2020/05/2...]

Firmware Upgrade

Kernel Version

1.1.1 [2020/05/2...]

Restore to default

All

Without Network

Time Zone

(UTC) W. Europe Standard Time, London, Lis...

Daylight Saving Time

Group

All Devices

Device Type

CoreStation 40

Product Name

CS-40

Hardware Version

1.0.0

Locked

Unlock

Time Synchronization with Server

☒

System


Display Date

2020/07/07

10:00:49

Get Time

Set Time

Item	Description
Information	<ul style="list-style-type: none"> ▪ Name: Enter a device name. ▪ Device ID: View the device ID. ▪ Firmware Version: Click Firmware Upgrade to install a newer firmware version. ▪ Kernel Version: View the kernel version. ▪ Restore to default: Reset the settings of the device. Click All to reset all settings. Click Without Network to reset all settings excluding the network settings. ▪ Time Zone: Set the time zone of the device. You can set a different standard time zone of the device from the time zone of the BioStar 2 server. ▪ Daylight Saving Time: Apply the daylight saving time to the device. To add a new daylight saving time rule, see Daylight Saving Time. ▪ Group: Change the device group. For more information on adding device groups, see Adding and Managing Device Groups. ▪ Device Type: View the device type. ▪ Product Name: View the model name. ▪ Hardware Version: View the hardware version. ▪ Locked: Unlock button will be available when the device is disabled via Trigger & Action. ▪ Time Synchronization with Server: Select the option to synchronize the time information of the device with the server.
System	<ul style="list-style-type: none"> ▪ Display Date: Click  to manually set the date and time. If the Time Synchronization with Server option is selected, the date and time cannot be selected manually. ▪ Get Time: Click the button to fetch the time set in the device. ▪ Set Time: Click the button to apply the time set in BioStar 2 to the

6 Device

Item	Description
	device.

— Network

Network

TCP/IP

☒ Use DHCP

• IP Address

192.168.14.205

• Subnet Mask

255.255.255.0

• Gateway

192.168.14.1

• Device Port

51211

• DNS Server Address

Server

☐ Device → Server Connection

• Server Address

• Server Port

51212

Serial

• RS485

Master

• Baud Rate

Port	Baud Rate
Host	115200
0	115200
1	115200
2	115200
3	115200

Item	Description
TCP/IP	<ul style="list-style-type: none"> ▪ Use DHCP: Select this option to allow the device to use a dynamic IP address. If this option is selected, network settings cannot be entered. ▪ IP Address, Subnet Mask, Gateway: To assign a fixed IP to the device, enter the information of each network. Uncheck Use DHCP and enter the information. ▪ Device Port: Enter a port to be used by the device. This port is used for the communication between BioStar 2 and the device. ▪ DNS Server Address: Enter a DNS server address.
Server	<ul style="list-style-type: none"> ▪ Device → Server Connection: Select this option to configure the BioStar 2 settings for connecting to the devices. If this option is selected, BioStar 2 server network settings can be entered. ▪ Server Address: Enter the IP address or domain name of the BioStar 2 server. ▪ Server Port: Enter the port number of the BioStar 2 server.
Serial	<ul style="list-style-type: none"> ▪ RS-485: You can only use Master. ▪ Baud Rate: Set a baud rate of the RS-485 connection.

— Authentication

6 Device

Authentication

Server Matching
Inactive

Fingerprint

1:N Security Level
Normal

1:N Fast Mode
Auto

Template Format
Suprema

Card Type

CSN Card
Enabled



EM4100
Mifare/Felica

Format Type
Normal

Byte Order
MSB

Mobile
Enabled

NFC
BLE

Item	Description
Authentication	<ul style="list-style-type: none"> ▪ Server Matching: It is possible to set server matching. When Active is set, the authentication is carried out using the user information stored in the PC where BioStar 2 is installed, and when Inactive is set, the authentication is carried out using the user information stored in the device. When using server matching, the server matching of BioStar 2 should be also activated. For more information, refer to Server.
Fingerprint	<ul style="list-style-type: none"> ▪ 1:N Security Level: You can set a security level to use for fingerprint or face authentication. The higher the security level is set, the false rejection rate (FRR) gets higher, but the false acceptance rate (FAR) gets lower. ▪ 1:N Fast Mode: You can set the fingerprint authentication speed. Select Auto to have the authentication speed configured according to the total amount of fingerprint templates registered within the device. ▪ Template Format: You can view the fingerprint template format.
Card Type	<p>You can set the type of card used by the device.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ The type of card supported by the device is displayed. <p>▪ CSN Card: You can select the CSN card and format type and set the byte order.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ If Format Type is set to Normal, the device will read the card serial number (CSN). If the option is set to Wiegand, the device will read the card serial number in a Wiegand format that the user has defined. ▪ If Format Type is set to Wiegand, you can select the

6 Device

Item	Description
	<p>Wiegand format to be used in the device. To set a new Wiegand format, refer to Wiegand.</p> <ul style="list-style-type: none"> When Byte Order is set to MSB, the device reads a card ID from the highest byte to the lowest byte. For example, the highest byte of the card ID 0x12345678 is 0x12 and the device sequentially reads 0x12, 0x34, 0x56 and 0x78. When the option is set to LSB, the device reads a card ID from the lowest byte to the highest byte. Mobile Card: You can set the type of mobile card.

— Advanced

Advanced

Tamper

None

AC Fail

None

Switch Type

Normally Open

Switch Type

Normally Open

Trigger & Action

Configuration

Trigger	Action

Add

Wiegand

Input/Output

Input

Wiegand Input Format

Default

Pulse Width(μs)

40

Pulse Interval(μs)

10000

Supervised Input

Configuration

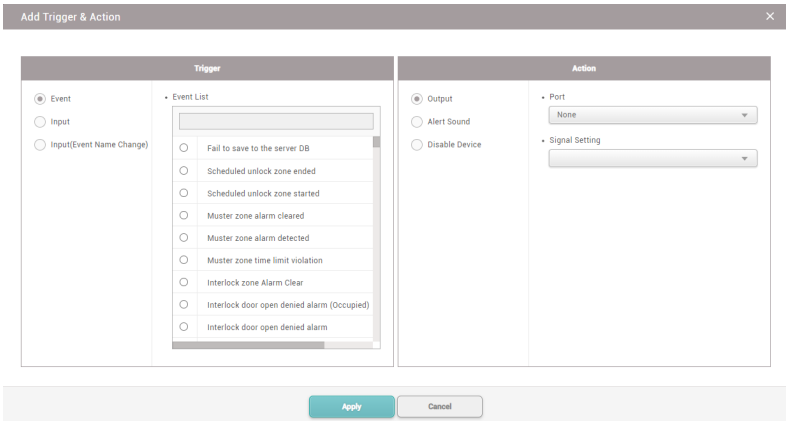
Index	Supervised	Supervised Input Resistor
0	<input type="checkbox"/> Input	
1	<input type="checkbox"/> Input	
2	<input type="checkbox"/> Input	
3	<input type="checkbox"/> Input	
4	<input type="checkbox"/> Input	
5	<input type="checkbox"/> Input	
6	<input type="checkbox"/> Input	
7	<input type="checkbox"/> Input	

Secure Tamper

Off

Item	Description
Advanced	<ul style="list-style-type: none"> Tamper: You can set the AUX port where the tamper is connected. AC Fail: You can set the AUX port that monitors the power input signal.
Trigger & Action	<ul style="list-style-type: none"> Configuration: You can set the operation of the device according to a pre-defined alarm or signal input. For example, you can set to output a signal set by the user or not to use the device when a temper on signal occurs in CoreStation.

6 Device

Item	Description
	
Wiegand	<ul style="list-style-type: none"> ▪ In/Out: You can only use input mode. ▪ Input Format: You can set a format for Wiegand. For more information on setting a Wiegand format, see Card Format. ▪ Pulse Width: You can set the pulse width of the Wiegand signal. ▪ Pulse Interval: You can set the pulse interval of the Wiegand signal.
Supervised Input	You can set the supervised input port of CoreStation to be used as TTL input port and set a resistance value to be used for supervised input. 1k Ω , 2.2k Ω , 4.7k Ω and 10k Ω can be set for the resistance value.
Secure Tamper	If a tamper event occurs on the device, you can set to delete the entire user information, the entire log, and the security key stored on the device.

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

Wiegand Device

You can edit detailed information of registered Wiegand devices.

- 1) Click **DEVICE**.
- 2) Click a Wiegand device on the device list to edit.

6 Device

The screenshot displays the configuration interface for a Wiegand device, organized into three main sections:

- Information (Section 1):** Contains fields for Name (Wiegand Reader 1 (575624497)), Device ID (575624497), Device Type (IO Device), and a Locked status with an Unlock button.
- Authentication (Section 2):** Includes an Operation Schedule dropdown (set to Always), a Matching Timeout slider (set to 5 sec), a Full Access toggle (set to Disable), and a Locked status with an Unlock button.
- Advanced (Section 3):** Contains two sub-sections:
 - Tamper:** Includes a Tamper Port dropdown (set to None) and a Switch Type toggle (set to Normally Open).
 - LED/Buzzer:** Includes a Green LED Port dropdown (set to None) and a Buzzer Port dropdown (set to None).

No.	Item	Description
1	Information	<p>You can modify the settings of the Wiegand device.</p> <ul style="list-style-type: none"> ▪ Name: Enter a device name. ▪ Device ID: View the device ID. ▪ Device Type: View the device type.
2	Authentication	<p>Modify the Wiegand device's authentication settings.</p> <ul style="list-style-type: none"> ▪ Operation Schedule: Configure the activating time for the device. ▪ Full Access: Allows the user to authenticate anytime. This overrides the access group of the user on the master device. ▪ Matching Timeout: You can set the matching timeout period. If the authentication is not completed within the set time, the authentication fails.
3	Advanced	<p>Modify the Wiegand device's tamper switch and LED settings.</p> <ul style="list-style-type: none"> ▪ Tamper Port: Select the input port where the Wiegand device's tamper switch is connected. ▪ Switch Type: Select the tamper switch type for the tamper operation. ▪ Green LED Port: Select the control port for the green LED. ▪ Buzzer Port: Select the control port for the buzzer.

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

You can use the **DOOR** menu to add the information on doors connected to devices.

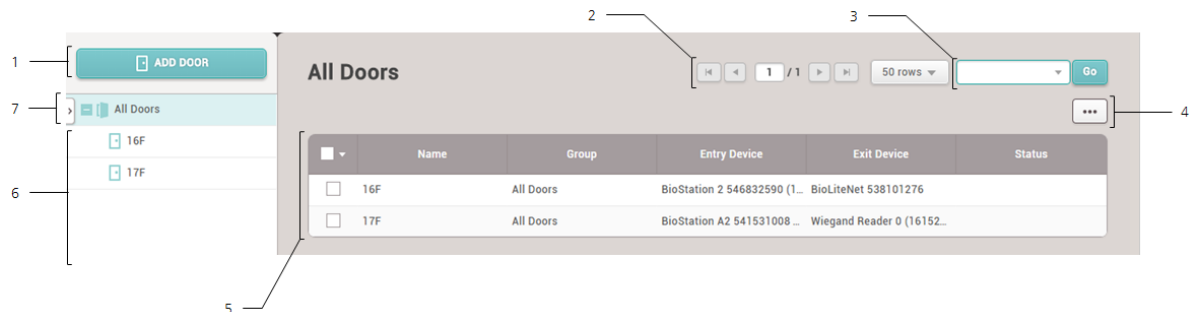
You can configure relay, dual authentication, anti-passback, forced open and held open alarm settings of the device. The door information is then used as a component of the access levels.

Adding and Managing Door Groups

7 Door

Add Door

Editing Doors



- | | |
|---|-----------------------|
| 1 Add Door | 5 Door List |
| 2 Page Navigation Buttons and Number of List Rows | 6 Door and Group List |
| 3 Registered Device Search | 7 Expand Button |
| 4 Function Button (Print, Column Setting) | |

After selecting a door, you can perform the following actions.

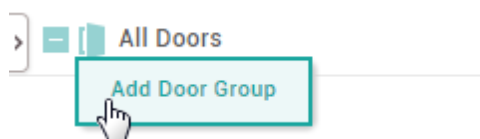
- **Delete Door:** Deletes the selected door from the list.

Adding and Managing Door Groups

You can add groups for easy management of multiple doors. Name your door groups according to door locations or office names for greater convenience.

— Adding Door Groups

- 1) Click **DOOR**.
- 2) Right-click on **All Door Groups** and click **Add Door Group**.



- 3) Enter a group name.

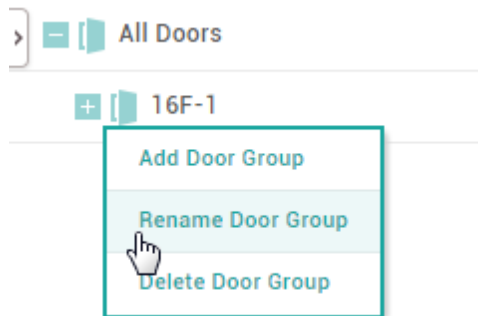
 **Note**

7 Door

- Door groups may be created in up to 8 levels.
- Up to 48 characters may be entered for a door group name.

— Renaming Door Groups

- 1) Click **DOOR**.
- 2) Right-click on the name of a group you wish to rename and click **Rename Door Group**.



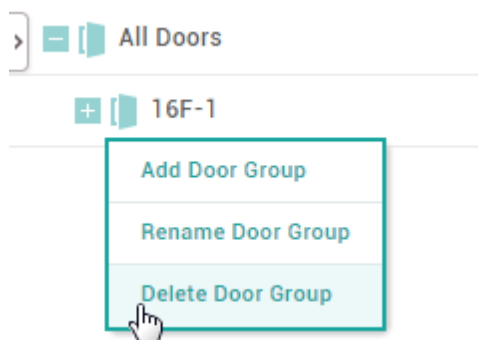
- 3) Enter a name.

Note

- Up to 48 characters may be entered for a door group name.

— Deleting Door Groups

- 1) Click **DOOR**.
- 2) Right-click on the name of a group you wish to delete and click **Delete User Group**.



Note

- Deleting a group deletes all doors in the group.

7 Door

Adding Doors

You can configure the doors to use in your access control installation. You can select an entry device and an exit device, configure Anti-passback settings for improved security, or configure alarms for each door.

- 1) Click **DOOR** and click **ADD DOOR**.
- 2) Configure the settings by referring to [Information](#), [Configuration](#), [Option](#), [Anti PassBack](#) and [Alarm](#).
- 3) After editing all information, click **Apply**.

➤ Related Information

[Basic Search and Registration](#)

[Slave Device Search and Registration](#)

[Adding and Managing Access Levels](#)

Information

You can enter or edit the name, group and description of the door.

- 1) Edit all fields of the **Information** tab.

Information

1

Name

17F-1

Group

All Door Groups

3

2

Description

No.	Item	Description
1	Name	Enter a door name.
2	Group	Set a door group. For more information on adding door groups, see Adding and Managing Door Groups .
3	Description	Enter a short description of the door.

- 2) Click **Apply** to save the settings.

Configuration

You can configure various settings for the device, exit button, door sensor, etc.

7 Door

1) Edit all fields of the **Configuration** tab.

The screenshot shows the 'Configuration' tab with the following fields and settings:

- Entry Device:** Xpass D2 400000005 (Callout 1)
- Door Relay(,):** Relay 0 of CoreStation 40 542070627 (192.1... (Callout 2)
- Exit Button:** Input Port 1 of CoreStation 40 542070627 (1... (Callout 3)
- Door Sensor:** Input Port 1 of CoreStation 40 542070627 (1... (Callout 4)
- Exit Device:** Xpass D2 400000005 (Callout 5)
- Switch:** Normally Open (Callout 4)
- Switch:** Normally Open (Callout 4)
- Use sensor when Entry Confirmed APB enabled:** OFF (Callout 4)

No.	Item	Description
1	Entry device	Select a device to use for entry. You can select a device from the list of registered devices. If no registered device is available, see Basic Search and Registration , Advanced Search and Registration , Wiegand Device Search and Registration , or Slave Device Search and Registration .
2	Door relay	Select a relay to control the door lock.
3	Exit button	Select a port to use for the exit button. <ul style="list-style-type: none"> The Switch can be set to Normally Closed or Normally Open.
4	Door sensor	Select a port to check the door status. <ul style="list-style-type: none"> The Switch can be set to Normally Closed or Normally Open. Use sensor when Entry Confirmed APB enabled: You can set whether to use the door sensor when using Entry Confirmed APB. If Door Sensor is set to None, the Alarm tab cannot be edited.
5	Exit device	Select a device to use at exit. An exit device can only be used when there is a slave device connected. If there is no registered slave device, see Basic Search and Registration , Advanced Search and Registration , Wiegand Device Search and Registration , or Slave Device Search and Registration . <ul style="list-style-type: none"> If no exit device is selected, the Anti Pass Back tab cannot be edited.

2) Click **Apply** to save the settings.

Note

- CoreStation can not be set as either an entry device or an exit device.

Related Information

[Anti Passback](#)


7 Door

Option

You can configure additional options.

- 1) Edit all fields of the **Option** tab.

The screenshot shows the 'Option' configuration tab. It contains three sections: 'Open', 'Dual Authentication', and 'Anti-Tailgating'. The 'Open' section has a slider for 'Open Time' set to 3 seconds. The 'Dual Authentication' section has a dropdown for 'Device' set to 'No device'. The 'Anti-Tailgating' section has a dropdown for 'Sensor' set to 'None'. Numbered callouts 1, 2, and 3 point to the 'Open Time' slider, the 'Device' dropdown, and the 'Sensor' dropdown respectively.

No.	Item	Description
1	Open	<p>You can configure options concerning the opening of the door.</p> <ul style="list-style-type: none">▪ Open Time: Set the duration for which the door will remain open after a user authentication is completed. When the authentication is successful, the relay will be activated for the set time. When this time elapses, the relay no longer sends the signal to the door. <p> Note</p> <ul style="list-style-type: none">▪ Open Time may vary depending on the type of door lock used.▪ Lock when door is closed: When the door sensor detects that the door is closed, the door is locked. This option is not available if Use Automatic Door is set to ON.▪ Use Automatic Door: When using an automatic door as an entrance door, a relay can operate regardless of the status of a door sensor. This option is not available if Lock when door is closed is set to ON.
2	Dual Authentication	<p>You can configure the door to open only when authenticating credentials of two persons (an ordinary user and an administrator).</p> <ul style="list-style-type: none">▪ Device: Select a device to use dual authentication. If No device is selected, the dual authentication mode is disabled.▪ Schedule: Set a schedule to use dual authentication. If no desired schedule is available, click + Add Schedule to create it. For more information on configuring schedules, see Schedules.▪ Approval Type: You can configure the administrator authentication order. Setting to None will require two users to authenticate regardless to

7 Door

No.	Item	Description
		<p>the access group. Setting to Last will require an authentication by a user belonging to an access group that has been set after a normal user authentication.</p> <ul style="list-style-type: none"> ▪ Authentication Group: You can configure a group to which the administrator belongs. ▪ Authentication Timeout: Set a timeout period for authenticating the second credential after the first credential has been authenticated. If the second credential is not authenticated within the timeout period after the first credential has been authenticated, the door will not open.
3	Anti-Tailgating	<p>You can configure the door to detect the tailgating.</p> <ul style="list-style-type: none"> ▪ Sensor: You can select the sensor to detect tailgating.

2) Click **Apply** to save the settings.

Anti-passback

You can use Anti-passback to manage the access history and enhance security.

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. If **Exit Device** is set to **None**, this feature is unavailable.

For more information on configuring exit devices, see [Configuration](#).

Note

- A master device and a slave device should be connected via the RS-485 interface in order to activate the Anti-passback section on the Door page.

1) Edit all fields of the **Anti PassBack** tab.

Anti PassBack

1

Type

Soft APB

Reset Time

1440 min.

2

No.	Item	Description
1	Type	<p>Select an Anti-passback type.</p> <ul style="list-style-type: none"> ▪ None: Select this option to disable the Anti-passback feature. ▪ Soft APB: Select this option to allow entry but set off an alarm or create a log entry in BioStar 2 when Anti-passback is violated.

7 Door

No.	Item	Description
		<ul style="list-style-type: none"> ▪ Hard APB: Select this option to prohibit entry and set off an alarm or create a log entry in BioStar 2 when Anti-passback is violated.
2	Reset Time	You can set a time period for resetting the Anti-passback feature. The maximum possible duration is 7 days (10080 min.). If set to 0, the feature is not reset.

2) Click **Apply** to save the settings.

Alarm

You can configure an alarm to go off or the device to lock when the door is opened by force, held open or an anti-passback violation occurs.

1) Edit all fields of the **Alarm** tab. To add an action, click **+ Add**.

Alarm

1 — [• Held Open

Action

+ Add

2 — [• Held Open Time

3 sec

3 — [• Forced Open

Action

+ Add

4 — [• Anti PassBack

Action

+ Add

No.	Item	Description
1	Held Open	You can configure alarm actions to be taken when the door is held open. Click + Add and select an action. Click OK to add the action.
2	Held Open Time	You can configure the maximum allowed time for the door to remain open.
3	Forced Open	You can configure alarm actions to be taken when the door is opened by force. Click + Add and select an action. Click OK to add the action.
4	Anti-passback	<p>You can configure alarm actions to be taken when an Anti-passback violation occurs. Click + Add and select an action. Click OK to add the action.</p> <ul style="list-style-type: none"> ▪ An exit device must be registered before the Anti-passback setting can be configured.

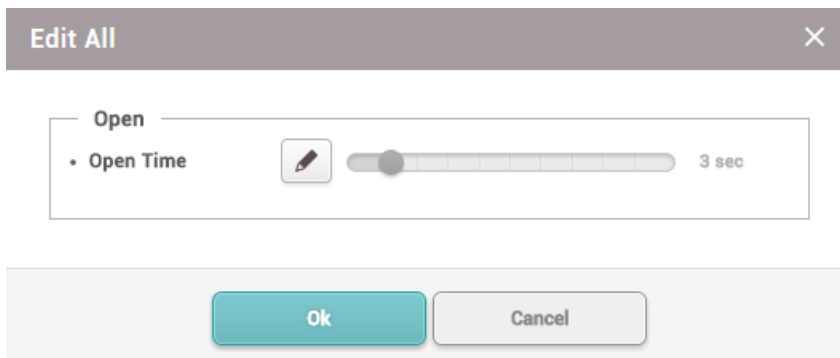
7 Door

- 2) Click **Apply** to save the settings.


Editing Doors

You can edit an existing door or batch edit multiple doors.

- 1) Click **DOOR**.
- 2) In the door list, click a door to edit.
- 3) Edit the details by referring to the instructions in [Adding Doors](#).
- 4) To edit information on multiple doors, select multiple doors and click **Batch Edit**.



The screenshot shows a dialog box titled "Edit All" with a close button (X) in the top right corner. Inside the dialog, there is a section labeled "Open" with a sub-label "• Open Time". To the right of the text is a slider control with a pencil icon on the left and the text "3 sec" on the right. Below the slider is a row of two buttons: "Ok" (highlighted in teal) and "Cancel".

- 4) Click  of the field you want to edit and edit the information.
- 5) After editing all information, click **OK**.

You can configure the elevator to control floors with the access control device and OM-120 by using the **ELEVATOR** menu.

[Adding and Managing Elevator Groups](#)

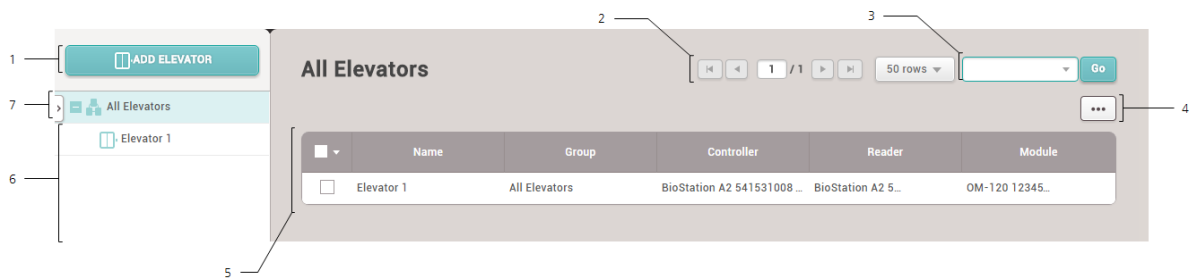
[Adding Elevators](#)

[Editing Elevators](#)

Note

- The **ELEVATOR** menu will appear when the Advanced or higher license is activated.

8 Elevator



- | | |
|---|---------------------------|
| 1 Add Elevator | 5 Elevator List |
| 2 Page Navigation Buttons and Number of List Rows | 6 Elevator and Group List |
| 3 Registered Elevator Search | 7 Expand Button |
| 4 Function Button (Print, Column Setting) | |

After selecting an elevator, you can perform the following actions.

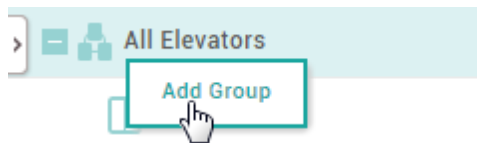
- **Delete Elevator:** Deletes the selected elevator from the list.

Adding and Managing Elevator Groups

You can add groups for easy management of multiple elevators. Name your elevator groups according to elevator locations for greater convenience.

— Adding Elevator Groups

- 1) Click **ELEVATOR**.
- 2) Right-click on **All Elevators** and click **Add Group**.



- 3) Enter a group name.

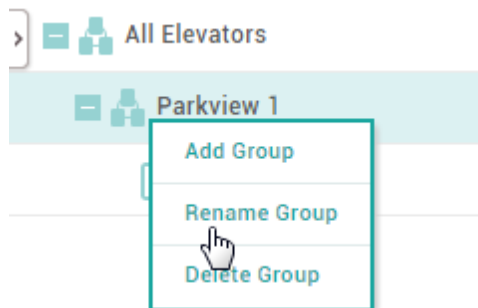
Note

- Elevator groups may be created in up to 8 levels.
- Up to 48 characters may be entered for an elevator group name.

8 Elevator

— Renaming Elevator Groups

- 1) Click **ELEVATOR**.
- 2) Right-click on the name of a group you wish to rename and click **Rename Group**.



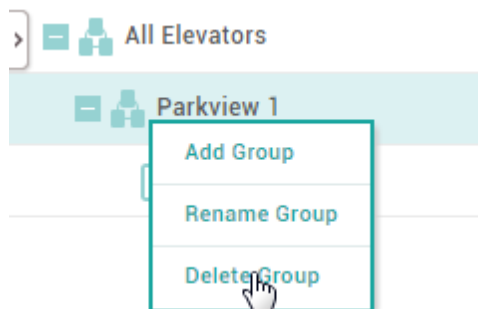
- 3) Enter a name.

Note

- Up to 48 characters may be entered for an elevator group name.

— Deleting Elevator Groups

- 1) Click **ELEVATOR**.
- 2) Right-click on the name of a group you wish to delete and click **Delete Group**.



Note

- Deleting a group deletes all elevators in the group.

Adding Elevators

You can configure the elevators to use for the floor control.

- 1) Click **ELEVATOR** and click **ADD ELEVATOR**.
- 2) Configure the settings by referring to **Information**, **Detail**, **Option**, and **Alarm**.

8 Elevator

- 3) After editing all information, click **Apply**.

Related Information

[Basic Search and Registration](#)

[Slave Device Search and Registration](#)

[Adding and Managing Access Levels](#)

Information

You can enter or edit the name, group and description of the elevator.

- 1) Edit all fields of the **Information** tab.

Information

1

Name

Elevator 1

Group

All Elevators

3

2

Description

No.	Item	Description
1	Name	Enter an elevator name.
2	Group	Set an elevator group. For more information on adding door groups, see Adding and Managing Elevator Groups .
3	Description	Enter a short description of the elevator.

- 2) Click **Apply** to save the settings.

Detail

You can select a device to connect to the elevator and floor information.

Note

- BioEntry Plus, BioEntry W, BioLite Net are not available as a controller.

- 1) Edit all fields of the **Detail** tab.

8 Elevator

Detail

Configuration

1

Controller

BioStation A2 541531008 (192.168...

2

3

Module

OM-120 12345678

Floor

4

Total Number of Floors

12

Apply

Auto-mapping




☐ Auto-mapping

5

6


Floor Settings

Floor Name	Device	Relay Number	
Elevator 1 - 1	OM-120 12345678	Relay 0 of OM-120 12345678 De...	
Elevator 1 - 2	OM-120 12345678	Relay 1 of OM-120 12345678 De...	
Elevator 1 - 3	OM-120 12345678	Relay 2 of OM-120 12345678 De...	
Elevator 1 - 4	OM-120 12345678	Relay 3 of OM-120 12345678 De...	
Elevator 1 - 5	OM-120 12345678	Relay 4 of OM-120 12345678 De...	
Elevator 1 - 6	OM-120 12345678	Relay 5 of OM-120 12345678 De...	
Elevator 1 - 7	OM-120 12345678	Relay 6 of OM-120 12345678 De...	
Elevator 1 - 8	OM-120 12345678	Relay 7 of OM-120 12345678 De...	
Elevator 1 - 9	OM-120 12345678	Relay 8 of OM-120 12345678 De...	
Elevator 1 - 10	OM-120 12345678	Relay 9 of OM-120 12345678 De...	
Elevator 1 - 11	OM-120 12345678	Relay 10 of OM-120 12345678 D...	
Elevator 1 - 12	OM-120 12345678	Relay 11 of OM-120 12345678 D...	

No.	Item	Description
1	Controller	<p>Select a device that controls the elevator access permission.</p> <p> Note</p> <ul style="list-style-type: none"> Only a master device can be selected. You can select it from the list of registered devices. If there is no registered device, refer to Basic Search and Registration.
2	Reader	<p>Select a device you intend to use for authentication.</p> <p> Note</p> <ul style="list-style-type: none"> You can select a device among the master device, slave device, and Wiegand device. OM-120 cannot be set as the reader.
3	Module	<p>Select OM-120 to control the elevator button relay.</p> <p> Note</p> <ul style="list-style-type: none"> Only OM-120 can be selected.
4	Total Number of	Enter the total number of floors that you can move using the elevator.

102

8 Elevator

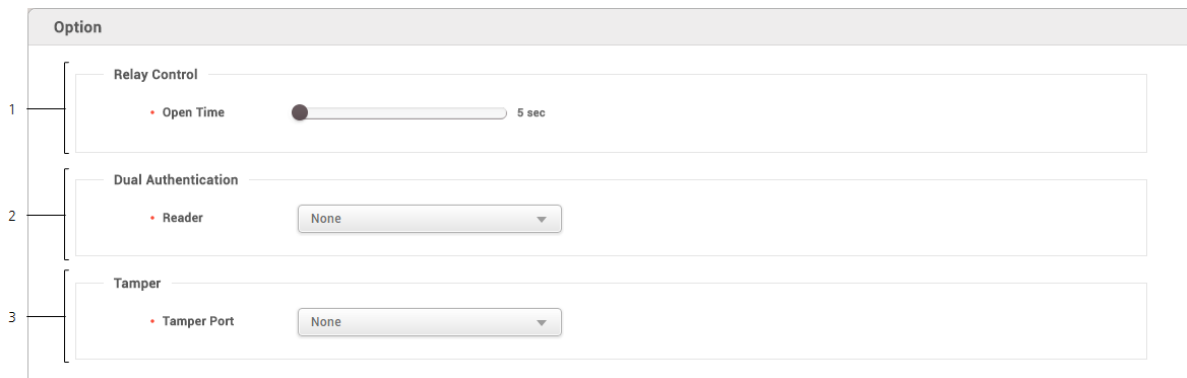
No.	Item	Description
	Floors	 Note <ul style="list-style-type: none"> Up to 192 floors can be entered.
5	Auto-mapping	Select whether or not to use auto-mapping. If Auto-mapping is used, Relay Number is assigned in consecutive order.
6	Floor Settings	You can set the floor name and the relay number to control the floor.

2) Click **Apply** to save the settings.

Option

You can configure additional options.

1) Edit all fields of the **Option** tab.



The screenshot shows the 'Option' tab configuration interface. It contains three main sections, each with a numbered bracket on the left:

- 1** **Relay Control**: Includes a slider for 'Open Time' set to 5 sec.
- 2** **Dual Authentication**: Includes a dropdown menu for 'Reader' currently set to 'None'.
- 3** **Tamper**: Includes a dropdown menu for 'Tamper Port' currently set to 'None'.

No.	Item	Description
1	Relay Control	<p>You can configure options concerning the activating of the relay of the floor.</p> <ul style="list-style-type: none"> Open Time: Set the duration for which the floor button will remain activate after a user authentication is completed. When the authentication is successful, the relay will be activated for the set time. When this time elapses, the relay no longer sends the signal to the relay of the floor.
2	Dual Authentication	<p>You can configure the floor button to activate only when authenticating credentials of two persons (an ordinary user and an administrator).</p> <ul style="list-style-type: none"> Device: Select a device to use dual authentication. If No device is selected, the dual authentication mode is disabled. Schedule: Set a schedule to use dual authentication. If no desired schedule is available, click + Add Schedule to create it. For more

8 Elevator

No.	Item	Description
		<p>information on configuring schedules, see Schedules.</p> <ul style="list-style-type: none">▪ Approval Type: You can configure the administrator authentication order. Setting to None will require two users to authenticate regardless to the access group. Setting to Last will require an authentication by a user belonging to an access group that has been set after a normal user authentication.▪ Authentication Group: You can configure a group to which the administrator belongs.▪ Authentication Timeout: Set a timeout period for authenticating the second credential after the first credential has been authenticated. If the second credential is not authenticated within the timeout period after the first credential has been authenticated, the door will not open.
3	Tamper	You can set a port to output the tamper signal.

- 2) Click **Apply** to save the settings.

Alarm

An action can be set to be performed when tamper input or a separate input signal is detected.

- 1) Edit all fields of the **Alarm** tab. To add an action, click **+ Add**.

The screenshot shows the 'Alarm' configuration window. At the top is a tab labeled 'Alarm'. Below it is a configuration area with a table. The table has two columns: 'Trigger' and 'Action'. To the right of the table is a '+ Add' button. A line with the number '1' points to the configuration area, and a line with the number '2' points to the '+ Add' button.


No.	Item	Description
1	Trigger	Tamper input detection or separate input signal detection can be set.
2	Action	<p>An action can be set to be performed according to the status set under trigger.</p> <p>The floor button of the elevator can be activated, and/or output of a specific signal can be set.</p>

- 2) Click **Apply** to save the settings.

Editing Elevators

You can edit an existing elevator or batch edit multiple elevators.

8 Elevator

- 1) Click **ELEVATOR**.
- 2) In the elevator list, click an elevator to edit.
- 3) Edit the details by referring to the instructions in **Adding Elevators**.
- 4) To edit information on multiple elevators, select multiple elevators and click **Batch Edit**.
- 5) Click  of the field you want to edit and edit the information.
- 6) After editing all information, click **OK**.

You can use the **ACCESS CONTROL** menu to create access levels by configuring doors and access schedules and to configure access groups using access levels and user group information. The configured access groups are then used as components of the access control.

Adding and Managing Access Levels

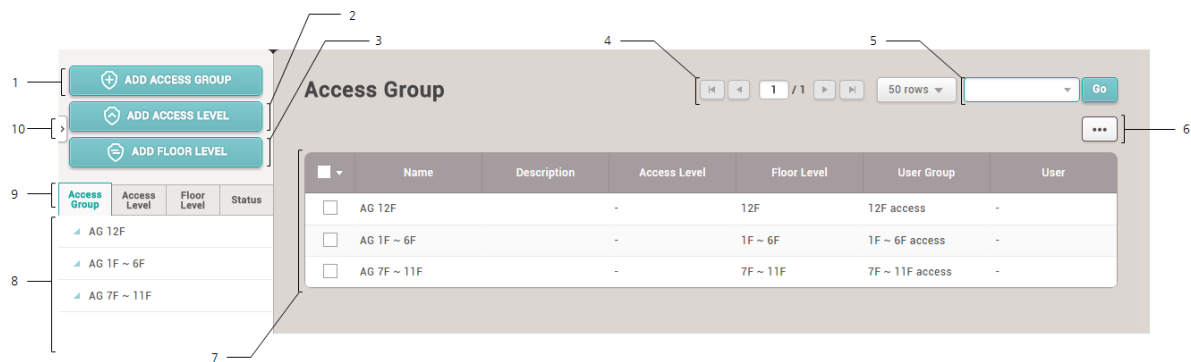
Adding and Managing Access Groups

Adding and Managing Floor Levels

Access Privilege Status

 **Note**

- The **Floor Level** tab and **ADD FLOOR LEVEL** button will appear when the Advanced or higher license is activated.



1 Add Access Group

2 Add Access Level

3 Add Floor Level

4 Page Navigation Buttons and Number of List Rows

6 Function Button (Print, Column Setting)

7 Access Group / Access Level / Floor Level List

8 Access Groups / Access Level / Floor Level Groups

Tab buttons for the Access Group, Access Level, Floor Level and Status list pages

9 Access Control

1 Add Access Group	€ Function Button (Print, Column Setting)
5 Registered Item Search	1 Expand Button (

After selecting an access group or an access level, you can perform the following actions.

- **Delete Access Group:** Deletes the selected access group from the list.
- **Delete Access Level:** Deletes the selected access level from the list.
- **Delete Floor Level:** Deletes the selected floor level from the list.

Adding and Managing Access Levels

You can configure a schedule during which users are allowed to access the door and add it to an access level.

— Adding Access Level

- 1) Click **ACCESS CONTROL > ADD ACCESS LEVEL**.
- 2) Enter **Name** and **Description** for the access level.
- 3) Click **+ Add**.
- 4) Click ▼ to select a door and a schedule.



• Name

• Description

Door	Schedule	
Door 1 ▼	Always ▼	

[+ Add](#)

Note

- Click  to search for an item.
- If no desired door is available, add it by referring to [Adding Doors](#).
- If no desired schedule is available, click **+ Add Schedule** to create it. For more information on configuring schedules, see [Schedules](#).
- Click  to delete an item.

- 5) Click **Apply** to save the settings.

— Editing Access Level

- 1) Click **ACCESS CONTROL > Access Level** tab.
- 2) In the access level list, select an access level to edit.

9 Access Control

- 3) After editing the necessary fields, click **Apply**.

— Deleting Access Level

- 1) Click **ACCESS CONTROL > Access Level** tab.
- 2) In the access level list, select an access level to delete.
- 3) Click **Delete Access Level**.

Adding and Managing Access Groups

You can configure access privileges by using access levels and user group information.

— Adding Access Group

- 1) Click **ACCESS CONTROL > ADD ACCESS GROUP**.
- 2) Enter Name and Description for the access group.
- 3) Click **+ Add** for each field.
- 4) Click ▼ to select an access level, a floor level, a user group or a user.


• Name

• Description

• Access Rule

Access Level	+ Add	Floor Level	+ Add
User Group	+ Add	User	+ Add

Note

- If no desired access level is available, click **+ Add Access Level** to create it. For more information on access levels, see [Adding and Managing Access Levels](#).
 - If no desired floor level is available, click **+ Add Floor Level** to create it. For more information on floor levels, see [Adding and Managing Floor Levels](#).
 - Click  to delete an item.
- 4) Click **Apply** to save the settings.

9 Access Control

— Editing Access Group

- 1) Click **ACCESS CONTROL** > **Access Group** tab.
- 2) In the access group list, select an access group to edit.
- 3) After editing the necessary fields, click **Apply**.

— Deleting Access Group

- 1) Click **ACCESS CONTROL** > **Access Group** tab.
- 2) In the access group list, select an access group to delete.
- 3) Click **Delete Access Group**.

Adding and Managing Floor Levels

You can configure the floor access privileges by using elevators and floor information.

Note

- The **Floor Level** tab and **ADD FLOOR LEVEL** button will appear when the AC standard license is activated.

— Adding Floor Level

- 1) Click **ACCESS CONTROL** > **ADD FLOOR LEVEL**.
- 2) Enter **Name** and **Description** for the floor level.
- 3) Click **+ Add**.
- 4) Click ▼ to select an elevator, a floor name, and a schedule.



• Name

• Description

Elevator	Floor Name	Schedule	
Elevator 1 ▼	Elevator 1 - 1 + 	Always ▼	



Note

- Click  to search for an item.
- If no desired elevator is available, add it by referring to [Adding Elevators](#).
- If no desired schedule is available, click **+ Add Schedule** to create it. For more information on configuring schedules, see [Schedules](#).
- Click  to delete an item.

9 Access Control

- 5) Click **Apply** to save the settings.

— Editing Floor Level

- 1) Click **ACCESS CONTROL > Floor Level** tab.
- 2) In the floor level list, select a floor level to edit.
- 3) After editing the necessary fields, click **Apply**.

— Deleting Floor Level

- 1) Click **ACCESS CONTROL > Floor Level** tab.
- 2) In the floor level list, select a floor level to delete.
- 3) Click **Delete Access Level**.

Access Group Status






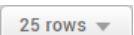
On the Status page, you can view who has the right to access certain doors. You can use a filter or combine filters to narrow down the result. You can also export the result as a CSV file. There are two types of the access privilege status view: by user and by door.

- 1) Click **ACCESS CONTROL > Status**.
- 2) Choose **Door Permission by Door**, **Door Permission by User**, **Elevator permission by Floor**, or **Elevator Permission by User**.
- 3) To view the result of a specific type only, click the ▼ of a column and apply a filter.

The screenshot shows the 'Access Group by Door' table interface. Annotations point to specific UI elements: 1 points to the 'Save Filter' button, 2 points to the pagination controls (showing 1 / 1 and 50 rows), 3 points to the menu icon (three dots), and 4 points to the table header area.

Door Group ▼	Door ▼	Schedule ▼	User ID ▼	User Name ▼	User Group ▼	User Level ▼
All Doors	16F	Always	15	User 006	All Users	None
All Doors	16F	Always	556	User 26	All Users	None
All Doors	16F	Always	33	User 024	All Users	None
All Doors	16F	Always	30	User 021	All Users	None
All Doors	16F	Always	27	User 018	All Users	None
All Doors	16F	Always	24	User 015	All Users	None
All Doors	16F	Always	19	User 010	All Users	None
All Doors	16F	Always	1	Administrator	All Users	Administrator
All Doors	16F	Always	99	kyle	All Users	None

9 Access Control

No.	Item	Description
1	Save Filter Button	Saves the set filter.
2	Page Navigation Buttons and Number of List Rows	<p>You can move a page or set the number of list rows to be displayed on one page.</p> <ul style="list-style-type: none">▪ : Go to the first page.▪ : Go to the previous page.▪  2 / 2: Enter the page number to move to.▪ : Go to the next page.▪ : Go to the last page.▪  25 rows: Set the number of list rows to be displayed on one page.
3	Function Buttons (Print, CSV Export, Column Setting)	You can print the list of logs or save it as a CSV file. Also, the column settings can be modified.
4	Access Privilege Status List	Shows the access privilege status of users.

You can use the **USER** menu to add users to BioStar 2 or to devices and manage their information. You can also add users' fingerprints, manage their authentication credentials such as cards and PINs and use them in access control, or grant administrator privileges.

[Adding and Managing User Groups](#)

[Adding User Information](#)

[Adding User Credentials](#)

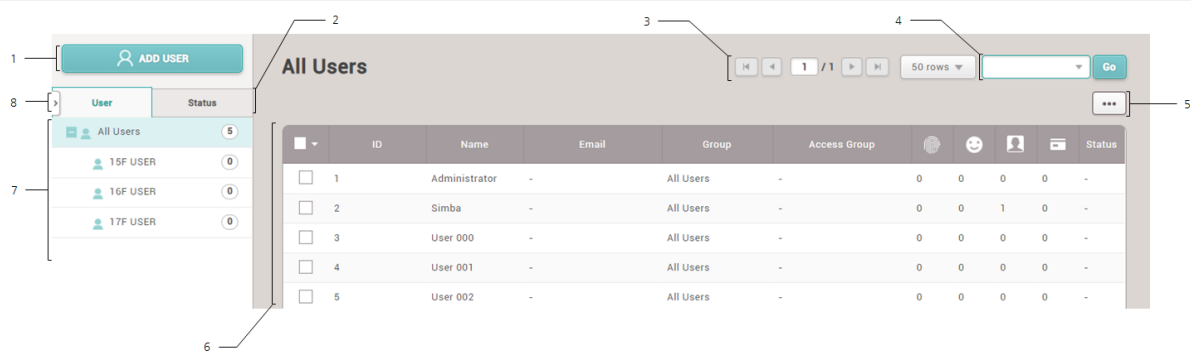
[Enroll Card](#)

[Transferring User Information to Devices](#)

[Editing User Information](#)

[Managing Long-term Idle Users](#)

10 Users



1 Add User

2 Tab buttons for the User and Long-term Idle User list pages

3 Page Navigation Buttons and Number of List Rows

4 Registered User Search

Function Button (Print, Column Setting, CSV Export, CSV Import, Data File Export, Data File Import, Send Visual Face Mobile Enrollment Link)

5 User List

6 User Group

7 Expand Button

Note

- Registered users can be searched by **Name, Email**.
- For more information on Send Visual Face Mobile Enrollment Link, see [Enroll Visual Face](#).

When you select a user, you can perform the following functions.

- Batch Edit:** Batch edits the information on multiple users. This function is available only when multiple users are selected.
- Transfer to Device:** Transfers user information registered with BioStar 2 to devices.
- Delete User:** Deletes the selected user from BioStar 2. User information registered in devices is not deleted.

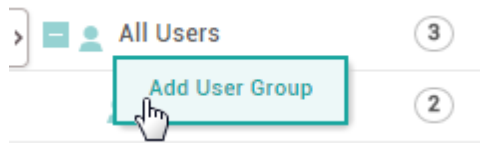
Adding and Managing User Groups

You can add groups for easy management of multiple users. Name your user groups according to users' organizations for greater convenience.

— Adding User Groups

- Click **USER**.
- Right-click on **All User Groups** and click **Add User Group**.

10 Users



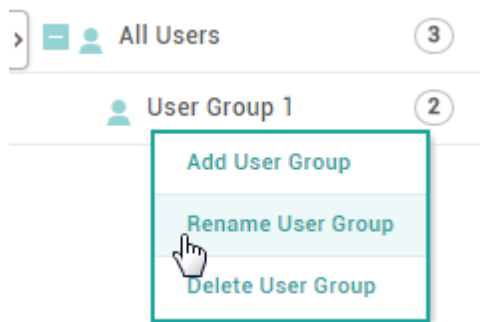
- 3) Enter a group name.

Note

- User groups may be created in up to 8 levels.
- Up to 48 characters may be entered for a user group name.

— Renaming User Groups

- 1) Click **USER**.
- 2) Right-click on the name of a group you wish to rename and click **Rename User Group**.



- 3) Enter a group name.

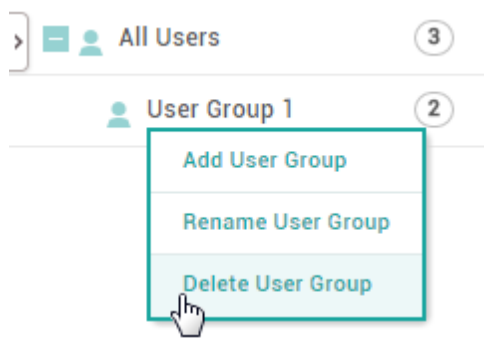
Note

- Up to 48 characters may be entered for a user group name.

— Deleting User Groups

- 1) Click **USER**.
- 2) Right-click on the name of a group you wish to delete and click **Delete User Group**.

10 Users



Note

- Deleting a group deletes all users in the group from BioStar 2.

Adding User Information

You can add photo, name, email, telephone, etc. of a user.
A fingerprint scanner is required for adding users' fingerprints. If a fingerprint scanner is already connected to BioStar 2, you can use the scanner to add fingerprints.






- 1) Click **USER > ADD USER**.
- 2) Enter or select the necessary fields in the **Information** tab.

Note




- The information with must be entered.

No.	Item	Description
1	Photo	<p>Add the user's photo. Click + Add Photo to select the user's photo.</p> <p> Note</p> <ul style="list-style-type: none">▪ Only an image file can be uploaded.

10 Users

No.	Item	Description
2	ID	<p>Enter a unique ID to assign to the user.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ When Number is set for User ID Type in Setting > Server, a number between 1 and 4294967295 can be entered. ▪ When Alphanumeric is set for User ID Type in Setting > Server, a combination of alphabetic characters and numbers can be entered. ▪ Do not use spaces when entering ID. ▪ Numbers or Alphanumeric characters can be set for the user ID type. For more details, refer to Server.
3	Name	<p>Enter the user's name.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ Up to 48 characters may be entered for the user's name.
4	Email	<p>Enter the email address.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ If the mobile access messaging option set as Email, user's email address is required when using the mobile access. ▪ User's email address is required when using visual face mobile enrollment.
5	Telephone	<p>Enter the telephone number.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ If the mobile access messaging option set as Text Message, user's telephone number is required when using the mobile access.
6	Status	You can temporarily deactivate the user's account.
7	Access Group	Set an access group. If no desired access group is available, add it by referring to Adding and Managing Access Groups .
8	USER IP	<p>Enter the user IP. If you register user IP, you can strengthen the security by allowing access only when the IP information registered in the account and the IP information of the PC match.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ The user IP can be entered in the format xxx.xxx.xxx.xxx. Each octet can only be entered in numbers between 0 and 255. ▪ Users whose user IP is not registered can log in regardless of the IP information of the PC.
9	Login ID	Enter the login ID.

10 Users

No.	Item	Description
		 Note <ul style="list-style-type: none"> The login ID appears when you set the Operator Level.
10	Password	<p>Enter the login password. You can change the password level by referring to Server.</p>  Note <ul style="list-style-type: none"> The password appears when you set the Operator Level. The Confirm Password will appear when you enter the password. Enter the password again to confirm.
11	Operator Level	<p>Set a BioStar operator privilege level.</p> <ul style="list-style-type: none"> None: The user has no operator privilege. Administrator: The user can use all menus. User Operator: The user can only use the USER and PREFERENCE menus. Monitoring Operator: The user can use the MONITORING and PREFERENCE menus and only view the DASHBOARD, USER, DEVICE, DOOR, ZONE and ACCESS CONTROL menus. Video Operator: The user can only use the VIDEO menu. T&A Operator: The user can only use the TIME ATTENDANCE menu and only view the USER menu. User: The user can only view own information and T&A records.  Note <ul style="list-style-type: none"> To set a new user permission, refer to Adding Custom Account Level. If you have upgraded from BioStar 2.5.0 to BioStar 2.6.0 and you are using custom account level for monitoring, set operator level again.
12	Period	Set an active period of the account.
13	Group	Select a user group. If no desired user group is available, add it by referring to Adding and Managing User Groups .

- 3) Enter or select the necessary fields in the **Credential** tab and click **Apply**. For more information on adding credentials, see [Adding User Credentials](#).

 **Note**

- You can refer to the **User/Device Management** on the [Server](#) to learn how to add custom user fields for extra user information.

10 Users

🔗 Related Information

[Adding User Credentials](#)

[Enroll Card](#)

[Account](#)

[Server](#)


Export/Import CSV

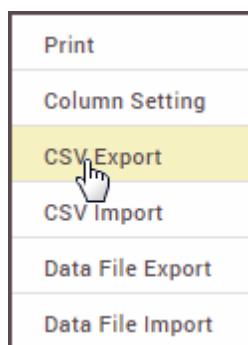
You can export/import user data in CSV files. This feature is useful when you create users in bulk or when you transfer users to another 3rd party systems.

📌 Note

- If a CSV file to import contains data for custom user fields and the fields do not exist on the server, then the data for the fields will be ignored during the import process. You can refer to the [Server](#) to learn how to add custom user fields.
- If you enter the user information in a language other than English or Korean, save the CSV file in UTF-8 format.

— CSV Export

- 1) Select users from the user list you intend to save to a CSV file and click .
- 2) Click **CSV Export**.

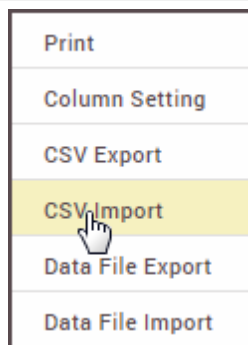


- 3) The CSV file will be downloaded automatically.

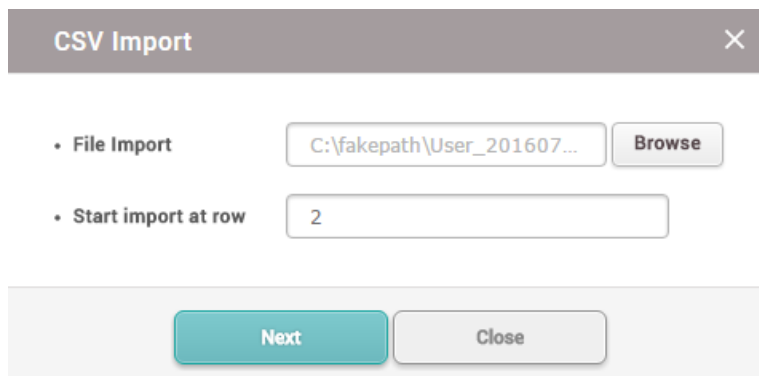
— CSV Import

- 1) Click  and then click **CSV Import**.

10 Users



- 2) Select the CSV file and then click **Open**.
- 3) Set **Start import at row** and then click **Next**.

A dialog box titled 'CSV Import' with a close button (X) in the top right corner. It contains two sections. The first section is labeled 'File Import' and includes a text field with the path 'C:\fakepath\User_201607...' and a 'Browse' button. The second section is labeled 'Start import at row' and includes a text field with the number '2'. At the bottom of the dialog, there are two buttons: 'Next' (teal) and 'Close' (gray).

- 4) The user data field of the CSV file and the user data field of BioStar 2 are mapped and displayed automatically. When you click **Remap**, the fields of the same name will be remapped.

10 Users

CSV Import

×

Remap

CSV Field	User Data Field
user_id	user_id ▼
name	name ▼
phone	phone ▼
email	email ▼
user_group	user_group ▼
start_datetime	start_datetime ▼
expiry_datetime	expiry_datetime ▼
csn	None ▼
csn_mobile	None ▼
26 bit SIA Standard...	None ▼
HID 37 bit-H10302	None ▼
HID 37 bit-H10304	None ▼

Back

Next

Close

- 5) Click **Next** after selecting whether to maintain the user data of which user ID has been already registered to BioStar 2 or overwrite with the CSV file information.

Note

- You can issue Mobile Access Cards via CSV Import. When CSV Import is complete, 1 credit will be deducted per Mobile Access Card in the Airfob Portal. Disable matching if you do not want to issue Mobile Access Cards.
- If the same data as the Mobile Access Card issued to the user who is already registered in BioStar 2 exists in the CSV file, data can be maintained or overwritten, and the existing Mobile Access Card is maintained.
- If there is data different from the mobile access card issued to the user who is already registered in BioStar 2 in the CSV file, the existing Mobile Access Card is maintained if the data is retained, and if overwritten, a new Mobile Access Card is issued to the user.

10 Users

- 6) If an error occurs during the import of CSV file information, you can upload it again after checking only the erroneous CSV data.

Note

- If there are additional columns in the CSV file other than the basic user columns, BioStar 2 will fail to import the CSV file.


Export/Import User Information

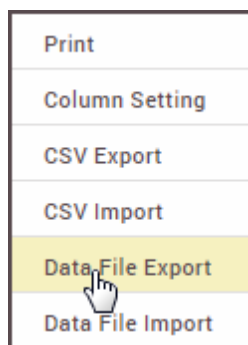
You can store the data file on external storage (USB) and import to BioStar 2 or device. Up to 500,000 users can be moved from server to device or from device to device.

Note

- The exported data file from devices using older firmware version cannot be imported into BioStar 2. Make sure always use the latest version of firmware.
- If the fingerprint template format is different, the data file cannot be imported. For example, the data file exported from a device which uses the Suprema fingerprint template format cannot be imported into a device which uses the ISO fingerprint template format.

— Data File Export

- 1) Select users from the user list you intend to export to a data file and click .
- 2) Click **Data File Export**.



- 3) Select a device type to apply the exported data file. Only devices with USB port is displayed.

10 Users

Data File Export

Please select a device type to apply the exported data file. (Default: BioStation 2)

☒ BioStation2

☐ BioStation A2

☐ FaceStation2

Apply


Cancel

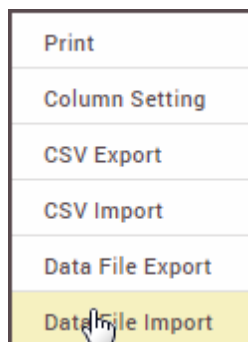
- 4) The data file is automatically downloaded.

Note

- The exported data file includes the profile photo, user ID, name, period, access group, PIN, auth mode, credentials (face, fingerprint, card), 1:1 security level.
- Be sure that the device is selected correctly. Otherwise, the device cannot recognize the data file.

— Data File Import

- 1) Click  and then click **Data File Import**.



- 2) Select the desired file (*.tgz) and then click **Open**.
- 3) A success message will appear on the screen when import successfully.

Adding User Credentials

You can add various user credentials such as PINs, fingerprints and cards.

10 Users

Adding PIN

Auth Mode

Enroll Fingerprint

Enroll Face

Enroll Visual Face

Enroll Card

Enroll Mobile Access Card

Adding PIN

Add a PIN.

- 1) Select the **PIN** option and enter a PIN to use.

• PIN ☒

• Confirm PIN

- 2) For confirmation, enter the PIN again in **Confirm PIN**.
- 3) Click **Apply** to save the settings.

Auth Mode

You can configure an authentication mode for each user.

Select **Device Default** to allow the user to authenticate using the modes configured in [Authentication](#), or select **Private Mode** to assign a unique authentication mode to each user.

- 1) Set **Auth Mode** to **Private Mode**.
- 2) Click **+ Add** and configure the settings.

10 Users

Add New Auth Mode

1

Extended Auth Mode

Not Use

※Extended Auth Mode is only supported by FaceStation F2.

2

Auth Mode

Biometrics

Fingerprint

Face

Card

ID

PIN

Ok

Cancel

No.	Item	Description
1	Extended Auth Mode	<div>Set whether to use Extended Auth Mode. When Extended Auth Mode is set to Use, the auth mode can be combined including both face and fingerprint.</div> <div><div><div></div>Note</div><div><div>Extended Auth Mode is only supported by FaceStation F2.</div></div></div>
2	Auth Mode	<div>Drag and drop authentication methods to use.</div>

3) Click **Apply** to add the authentication mode.

- Note

▪ If **Exclude Device Default Authentication Mode** is set, only the personal authentication mode set in BioStar 2 can be used. If **Include Device Default Authentication Mode** is set, both the authentication mode set in the device and the personal authentication mode set in BioStar 2 can be used.

Auth Mode

Private Mode

+ Add

Include Device Default Authentication Mode

10 Users

Enroll Fingerprint

You can add the user's fingerprints if the device supports fingerprint authentication. Fingerprints can be scanned using a finger scanner or at the installation location.

 **Note**

- Make sure that the user's finger is clean and dry.
- Do not add fingers with wounds or faint fingerprints.

1) Click **+ Fingerprint** and configure the settings.

Enroll Fingerprint

1

+ Device

BioLiteNet 538101276 (192.168.16.213)

2

+ Quality

80

3

☐ View Image

4

+ Add

Enroll Fingerprint

Scan

Delete

Validate

☐ Duress

9

8

7

6

5

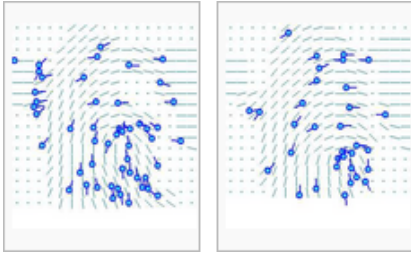
Enroll

Cancel

No.	Item	Description
1	Device	Select a device to enroll the fingerprint with.
2	Quality	Select a fingerprint enrollment quality level. Any fingerprint which does not meet the quality requirement will not be enrolled.
3	View Image	Select this option to view the original image when a fingerprint is scanned.
4	Enroll Fingerprint	Click + Add to add a fingerprint. Up to 10 fingerprints can be added.

123

10 Users

No.	Item	Description
5	Fingerprint Image	<p>This section shows the analysis of the fingerprint enrolled.</p> 
6	Duress	Select this option to add the fingerprint as a duress fingerprint. When threatened by someone to open the door, the user can authenticate using this fingerprint to send an alarm signal to BioStar 2.
7	Validate	It is possible to check if the fingerprint has been enrolled already or not when using the server matching.
8	Delete	Deletes the selected fingerprint.
9	Scan	Click Scan and then place a finger on the fingerprint scanner or the device sensor.

- 2) Click **Enroll** to enroll the fingerprint.
- 3) Set the **1:1 Security Level** and click **Apply**.

Note

- Fingerprints used for regular access should not be registered as duress fingerprints.
- The **View Image** option shows the fingerprint image but does not store it on BioStar.
- If the fingerprint authentication rate is low, delete the existing fingerprint information and add a new fingerprint.
- Use an adequate security level. If **1:1 Security Level** is too high, the fingerprint authentication rate may be too low or the false rejection rate (FRR) may be too high.
- For best fingerprint scanning quality, make sure to cover the entire surface of the fingerprint sensor with the finger. We recommend using the index finger or the middle finger.



Enroll Face

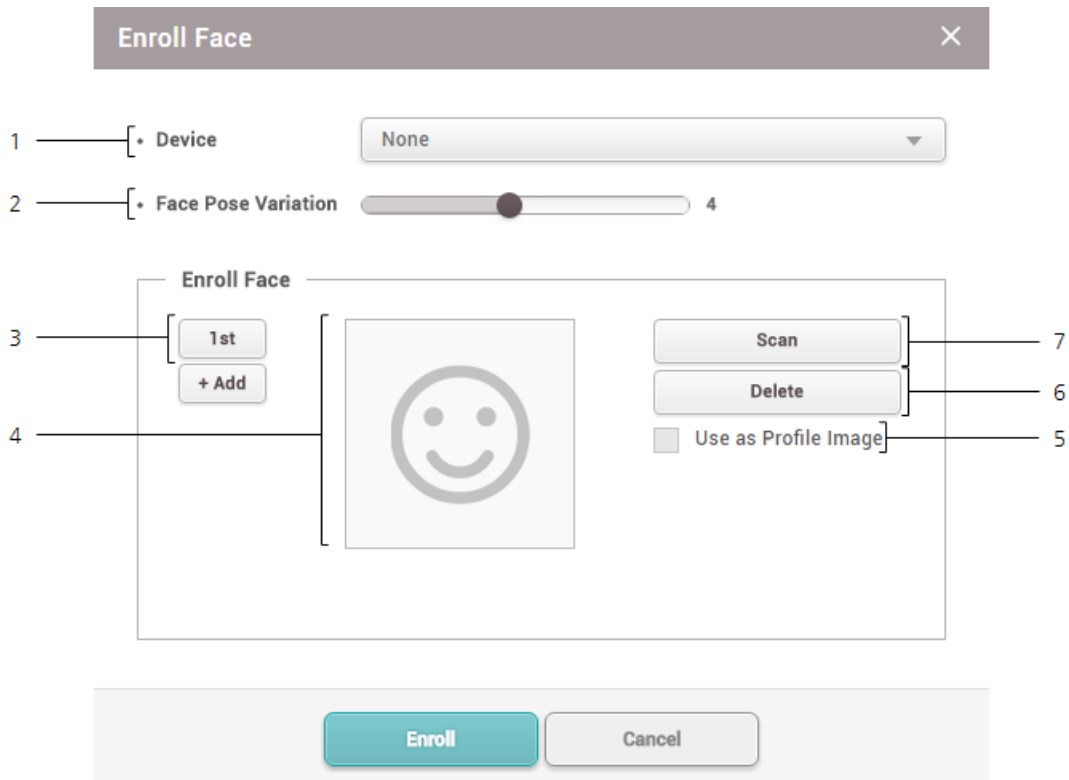
You can add the user's faces if the device supports face authentication.

10 Users

 **Note**

- When registering a face, maintain a distance of 40cm to 80cm between the device and the face.
- Be careful not to change the facial expression. (smiling face, drawn face, wink, etc.)
- If you do not follow the instructions on the screen, the face registration may take longer or may fail.
- Be careful not to cover the eyes or eyebrows.
- Do not wear hats, masks, sunglasses or eyeglasses.
- Be careful not to display two faces on the screen. Register one person at a time.
- It is recommended for a user wearing glasses to register both faces with and without glasses.

1) Click **+ Face** and configure the settings.



No.	Item	Description
1	Device	Select a device to enroll the face with.
2	Face Pose Variation	Set the sensitivity for the position, angle, and distance of a face when registering the face. Set the sensitivity high if you wish to obtain a detailed face template.
3	Enroll Face	Click + Add to add a face. Up to 5 faces can be added.
4	Face Image	View the registered face.
5	Use as	Select the registered face you wish to use as your profile image.

10 Users

No.	Item	Description
	Profile Image	
6	Delete	Deletes the selected face.
7	Scan	Click Scan and then follow the instructions on the device screen to scan.

- 2) Click **Enroll** to enroll the face.
- 3) Set the **1:1 Security Level** and click **Apply**.

Note

- If the face authentication rate is low, delete the existing face information and add a new face.
- Use an adequate security level. If **1:1 Security Level** is too high, the authentication rate may be too low or the false rejection rate (FRR) may be too high.

Enroll Visual Face

Visual Face is a credential that captures the user's face with a visual camera. It is different from face information captured with an infrared camera and is only available on devices that support Visual Face. Visual Face can also be registered non-face-to-face using a user's mobile device.

Note

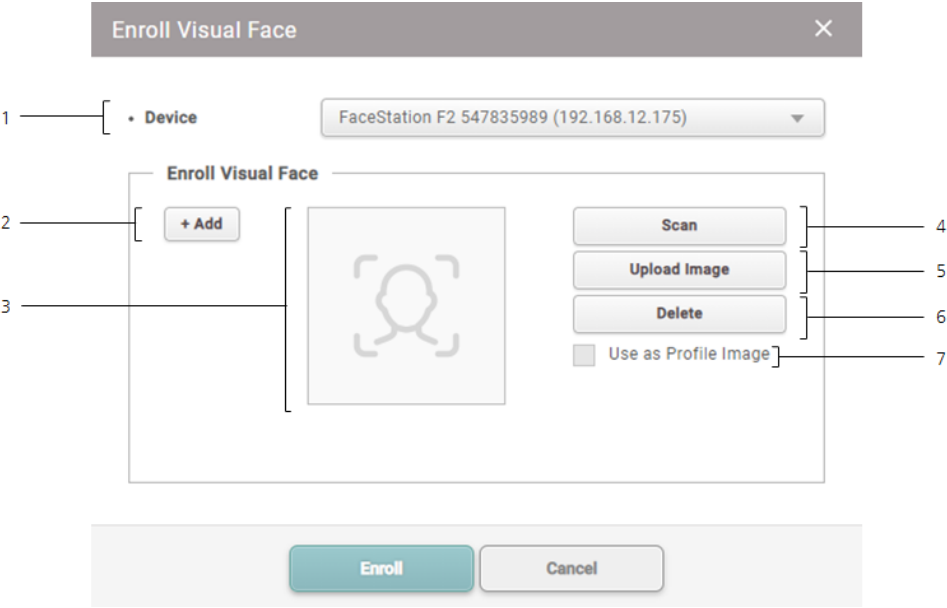
- The devices that can use Visual Face are as follows.
 - FaceStation F2

— Register by Device

You can enroll a visual face by FaceStation F2.

- 1) Click **+ Visual Face** and configure the settings.

10 Users



No.	Item	Description
1	Device	Select a device to enroll the visual face with.
2	Enroll Visual Face	Click + Add to add a visual face. Up to 2 visual faces can be added.
3	Visual Face Image	View the registered visual face.
4	Scan	Click Scan and then follow the instructions on the device screen to scan.
5	Upload Image	Upload the image to use as a visual face. Note <ul style="list-style-type: none">Supported image file formats are JPG and PNG.
6	Delete	Deletes the selected visual face.
7	Use as Profile Image	Select the registered face you wish to use as your profile image.

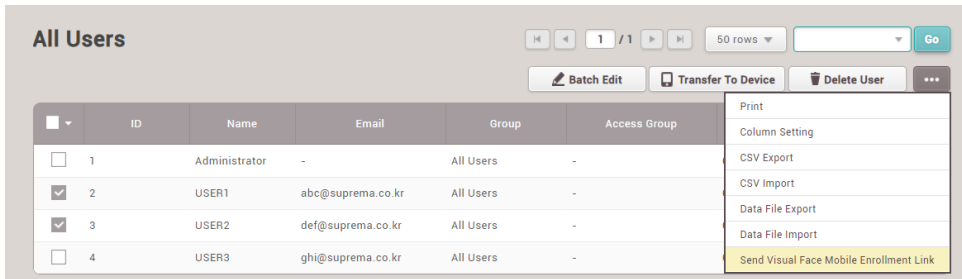
2) Click **Enroll** to enroll the visual face.

— Register by Mobile Device

10 Users

You can send the visible face mobile enrollment link to users via email. Users can access the link from their mobile device and enroll their visual face directly.

- 1) Select users from the user list you intend to enroll the visual face and click .



ID	Name	Email	Group	Access Group
1	Administrator	-	All Users	-
2	USER1	abc@suprema.co.kr	All Users	-
3	USER2	def@suprema.co.kr	All Users	-
4	USER3	ghi@suprema.co.kr	All Users	-

- 2) Select **Send Visual Face Mobile Enrollment Link** and then click **Yes**. The visual face enrollment link will be sent to the email of the selected user. When the user completes the upload, the visual face is enrolled in the user information.

Note

- Complete the email contents setting before using Visual Face Mobile Enrollment. See the [Email Contents](#) for more information.
- You can check whether the email was successfully sent or not in the audit trail. See the [Audit Trail](#) for more information.
- If the user receiving the visual face mobile enrollment link uses an external email application, the language of the email application must be set to the language of their country. If the language does not support Unicode, the text in the email may be broken.
- When the user clicks on Visual Face Mobile Enrollment link, the Visual Face Enrollment Service is executed as follows.
Follow the instructions on the screen to enroll the visual face.

BioStar 2



Visual Face Registration

Register

© 2020 SUPREMA INC. ALL RIGHTS RESERVED.

BioStar 2

Visual Face Registration

BioStar 2 Visual Face Registration is required to send limited personal data on individuals to facilitate the service being provided for the operator. This information is collected by each operator for the purpose of providing templates for biometric authentication to users. All data sent is required and managed by the operator you agree to provide data for this purpose and the manufacturer does not collect any data separately.

Personal information to be sent and managed by operator

BioStar 2 Visual Face Registration sends the minimum personal information required for service delivery. Following information will be sent through the current webpage once the user agrees on uploading the image selected.

- Photo taken from current webpage
- Photo selected by user

Cancel

Next

BioStar 2

Visual Face Registration

Photo

File format : PNG/JPG only (Less than 5MB)

Cancel

Upload

- Supported image file formats are JPG and PNG.
- Visual Face Enrollment link sent will expire after 24 hours.

Enroll Card

You can assign access cards to users or manage the existing cards.
For the types of card supported by the device, refer to the device manual.

- Registering CSN Card
- Registering Wiegand Card
- Registering Smart / Mobile Cards

[Card Enrollment using the USB Agent]

Card Type	CSN	Wiegand	Smart Card
EM	X	X	X
MIFARE	O	X	O
DESFire	O	X	O
FeliCa	O	X	X
HID Prox	X	X	X

10 Users

Card Type	CSN	Wiegand	Smart Card
HID iCLASS	X	X	X

Registering CSN Card

You can register the CSN cards.

- 1) Click **+ Card**.
- 2) Select **CSN** for **Card Type**.

Enroll Card [X]

- Card Type: CSN
- Registration Option: Register by Card Reader
- Device: BioStation 2 546832590 (192.168.16.108)

Information

- Card ID: Read Card

Enroll Cancel

- 3) Select a desired **Registration Option**.

— Register by Card Reader

You can register a card by scanning the card information with the device connected to BioStar 2.

- a) Select **Register by Card Reader** for **Registration Option**.
- b) Select the device to scan a card.
- c) Click **Read Card** and scan a card with the device.

— Assign Card

You can assign a registered card to a user.

- a) Select **Assign Card** for **Registration Option**.
- b) Click the card to be assigned from the list or search for the card.

— Enter Manually

10 Users

You can register a card by entering a card number directly.

- a) Select **Enter Manually** for **Registration Option**.
 - b) Click **Use User ID** or enter directly.
- 4) Click **Enroll** to register a card.

➤ Related Information

[Card Usage Status](#)

[Card Format](#)

Registering Wiegand Card

You can register the Wiegand cards.

- 1) Click **+ Card**.
- 2) Select **Wiegand** for **Card Type**.

Enroll Card [X]

- Card Type: Wiegand
- Card Data Format: 26 bit SIA Standard-H10301
- Registration Option: Register by Card Reader
- Device: BioStation 2 546832590 (192.168.16.108)

Information

- Facility Code: [] Read Card
- Card ID 1: []

[Enroll] [Cancel]

- 3) Set a **Card Data Format**. If no desired card data format is available, see [Wiegand](#) to set a Wiegand format.
- 4) Select a desired **Registration Option**.

— Register by Card Reader

10 Users

You can register a card by scanning the card information with the device connected to BioStar 2.

- a) Select **Register by Card Reader** for **Registration Option**.
- b) Select the device to scan a card. The available devices will be displayed on the top of device list, if no device is available, see **CSN Card Format** of [Authentication](#).
- c) Click **Read Card** and scan a card with the device.

— Assign Card

You can assign a registered card to a user.

- a) Select **Assign Card** for **Registration Option**.
- b) Select the card to be assigned from the list.

Note

- Only the cards with the set **Card Data Format** will be displayed on the list.

— Enter Manually

You can register a card by entering a card number directly.

- a) Select **Enter Manually** for **Registration Option**.
 - b) Enter the **Facility Code** or **Card ID 1**.
- 4) Click **Enroll** to register a card.

Related Information

[Card Usage Status](#)

[Card Format](#)

Registering Smart / Mobile Cards

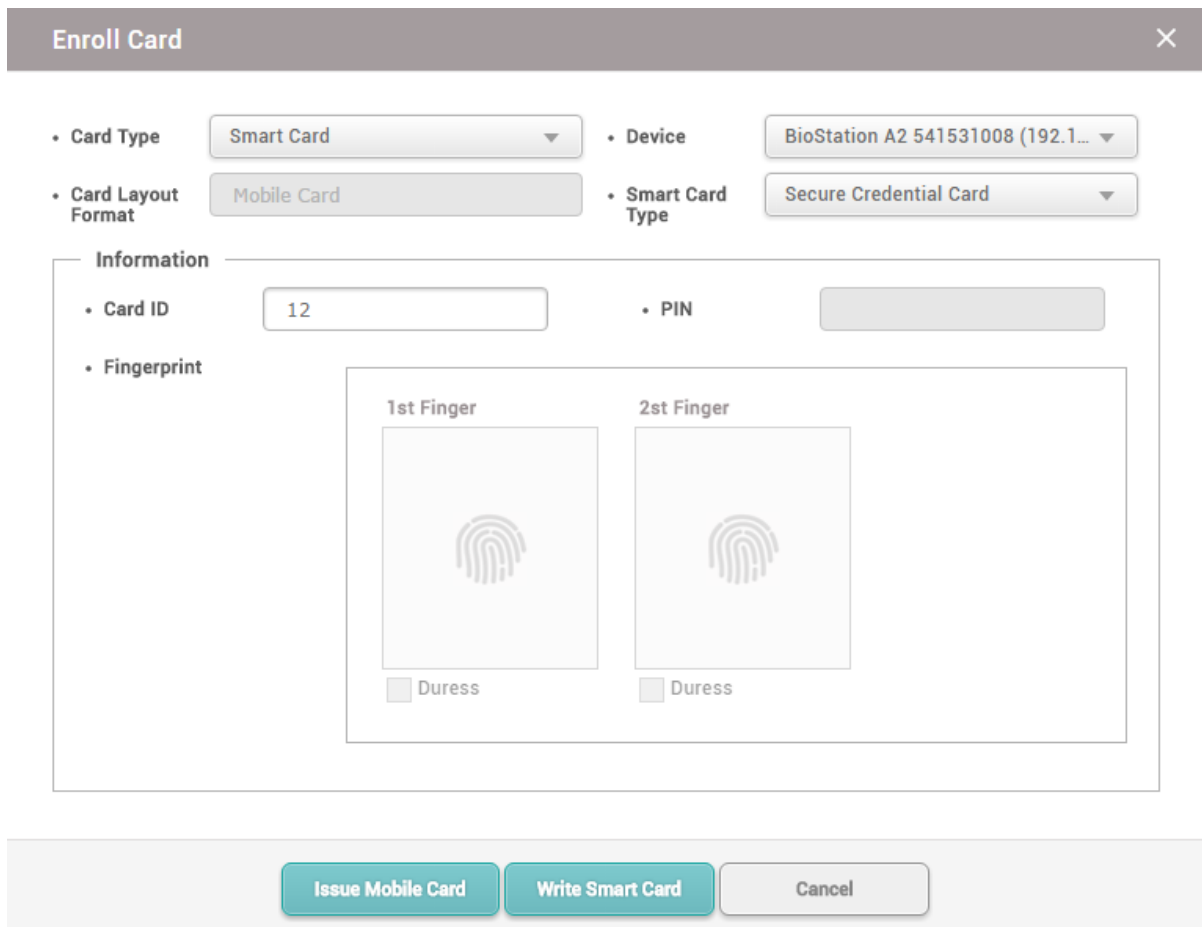
It is possible to enroll the Access on card or Secure credential card.

Note

- To set the mobile card, set **Active** for **Mobile Card Enrollment** on the **User/Device Management** tab of **Setting > SERVER**.
- To issue a smart card or a mobile card, the correct card type must be set. For detailed contents regarding the card type, refer to [Smart / Mobile Card](#).

10 Users

- 1) Click **+ Card**.



- 1) Select **Smart Card** for **Card Type**.
- 2) Select a device where the smart card can be used. To set the smart card layout, refer to **Card ID Format** on [Authentication](#).
- 3) Set **Card Layout Format**. It is possible to set the card layout from [Smart Card](#).
- 4) Select **Smart Card Type**.
 - **Access On Card**: Allows you to save user information (Card ID, PIN, Access Group, Period, and fingerprint templates) on the card.
 - **Secure Credential Card**: Allows you to save user information (Card ID, PIN, and fingerprint templates) on the card. The authentication is unavailable if the fingerprint template and PIN information of the user is not in the card, and the authentication is only available when the user information is stored in the device or BioStar 2. In order to use information stored in BioStar 2, server matching must be activated.
- 5) Select the fingerprint template to be enrolled on the card.
- 6) Clicking **Issue Mobile Card** or **Write Smart Card** will enroll the card.

Note

- If a mobile card has been issued, it can be used only after the issued card is activated through

10 Users

the BioStar 2 Mobile app.

- It is possible to set card ID for the Secure credential card directly.
- The information stored in BioStar 2 is used for the user information to be stored in the smart card. If the new user information is not stored, incorrect user information may be stored in the smart card. Also, if the changed user information is not synchronized with the device, the device may not be able to carry out authentication.

🔗 Related Information

[Card Usage Status](#)

[Card Format](#)

Read/Format Smart Cards

It is possible to format the smart card and record information again.

- 1) Click **+ Card**.

Enroll Card

• Card Type

Read Card

• Device

None

• Card Layout Format

• Smart Card Type

None

Information

• Card ID

• PIN

• Access Group

• Period

• Fingerprint

1st Finger

2st Finger

☐ Duress

☐ Duress

Format Card

Read Card

Cancel

- 2) Select **Read Card** for **Card Type**.
- 3) Select a device which can read the smart card. The list of devices only appears when the smart card layout is set. For setting, refer to **Card ID Format** on [Authentication](#).
- 4) Select **Smart Card Type**.
- 5) **Click** Read Card.
- 6) Check the card information and click **Format Card**.

🔗 **Related Information**

[Card Usage Status](#)

[Card Format](#)

Enroll Mobile Access Card

You can assign the mobile access to users when using the mobile access in conjunction with Suprema Airfob Portal.

Mobile Access Card supports registration either of each user individually or of multiple users at once via CSV Import.

Depending on the issuance method of Mobile Access Card set in the Airfob Portal, the user's email or phone number should be entered.

📌 **Note**

- For more information about using Suprema Airfob Portal and Mobile Access, see [Mobile Access](#).

- 1) Click **+ Mobile**.
- 2) Select a desired **Registration Option**.

— **Assign Card**

Unassigned CSN Mobile cards registered in BioStar 2 can be assigned to users.

- a) Select **Assign Card** for **Registration Option**.

Enroll Card

• Card Type

CSN Mobile

• Registration Option

Assign Card

x

Q

1 / 1

50 rows

Card ID	Type	Status
159609338918850	CSN Mobile	Unassigned
159609675842251	CSN Mobile	Unassigned
159609677396051	CSN Mobile	Unassigned
159609709440751	CSN Mobile	Unassigned
159609747048552	CSN Mobile	Unassigned

Enroll

Cancel

- b) Click the card to be assigned from the list or search for the card.

Enter Manually

CSN Mobile cards can be registered with a card ID entered manually or a random card ID.

- a) Select **Enter Manually** for **Registration Option**.

Enroll Card

• Card Type

CSN Mobile

• Registration Option

Enter Manually

Information

• Card ID

159617081751551

Use User ID

• Input Type

Use random card ID

Enroll

Cancel

- b) If **Input Type** is set as **Use random card ID**, a card ID is automatically generated. Click **Use User ID** to use the user ID as the card ID.
If **Input Type** is set at **Enter manually**, a card ID can be entered manually.

10 Users

Note

- It is recommended to set **Input Type** to **Use random card ID** to prevent duplicate card ID generation.

3) Click **Enroll** to register a mobile access card.

Note

- If the activation code sent to you via email or text message is lost or deleted, you can reissue the activation code by clicking **Reissue**. However, Mobile Access Cards activated in the Airfob Portal cannot be reissued.

Type	Card Data Format	Summary	
CSN Mobile	Mobile Access Card	ID: 159609752740350	<div><div>Reissue</div><div>Block </div></div>

Related Information

[Adding User Information](#)

[Mobile Access](#)

Transferring User Information to Devices

You can transfer user information registered with BioStar 2 to devices.

1) Select a user to transfer and click **Transfer to Device**.

10 Users


Transfer To Device

Users (3)

• Device List

All Devices


16F

 BioLiteNet 538101276 (192.168.16.230)

Overwrite users with different information

Transfer

Cancel

- 2) Select the **Overwrite users with different information** option to overwrite duplicate user information.
- 3) Select devices to transfer the information to. Click  to search for a device.
- 4) Click **Transfer** to transfer the user information.

Related Information

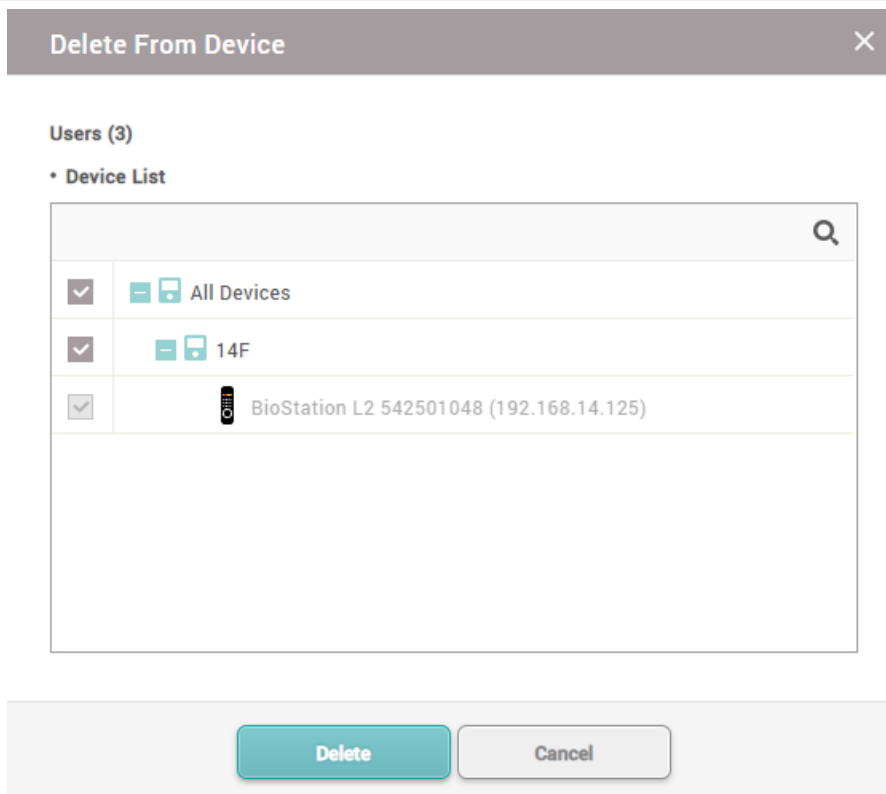
[Managing Users Registered with Devices](#)

Deleting User from Devices

You can delete users from each device registered in BioStar 2.


- 1) Select a user to delete from the device and click **Delete From Device**.

10 Users



Note

- The **Delete From Device** button is activated only when the **Automatic User Synchronization** is set as **Not Used**. You can refer to the [User/Device Management](#) for more detailed information on the Automatic User Synchronization.

- 2) Select devices to delete the users. Click  to search for a device.
- 3) Click **Delete** to delete users.

Note

- When you delete a user, it is only deleted from the device and the user in BioStar 2 remains intact.

Editing User Information

You can edit an existing user or batch edit multiple users.

- 1) In the user list, click a user to edit.
- 2) Edit the details by referring to the instructions in [Adding User Information](#), [Adding User Credentials](#) and [Enroll Card](#).
- 3) To batch edit information of multiple users, select multiple users and click **Batch Edit**.

10 Users

Batch Edit

×

Users (19)

• Group

• Status

Active

• Period

2001/01/01

00:00

~

2030/12/31

23:59


• Access Group

• Operator Level

None

Ok

Cancel

- 4) Click  of a field to edit its information.
- 5) Click **OK** to save the changes.

Note

- You cannot modify the **Operator Level** of "Administrator".

Managing Long-term Idle Users

You can view, edit and delete the users who do not have access events for the recent months.
You can use a filter or combine filters to narrow down the result and export it as a CSV file.

- 1) Click **Status** tab.
- 2) Set the idle period. You can choose from one month to six months.
- 3) You can narrow down the result by setting the filters on the headers of the result table.
- 4) Click **Batch Edit** after selecting multiple users if you want to modify the information of the multiple users.

10 Users

Batch Edit

Users (19)

• Group

• Status

Active

• Period

2001/01/01

00:00

~

2030/12/31

23:59

• Access Group


• Operator Level

None

Ok

Cancel

5) Click **Delete User** after selecting multiple users if you want to delete the multiple users.

 **Note**

- Only users with the operator level of **Administrator** or **User Operator** can use the **Batch Edit** and **Delete User** menu. You can refer to the [Adding User Information](#) for more detailed information on the operator level.

On the **ZONE** page, you can add anti-passback, fire alarm, schedule lock and schedule unlock zones, and configure the settings.

Anti-passback Zone

Fire Alarm Zone


Schedule Lock Zone

Scheduled Unlock Zone

Intrusion Alarm Zone

Interlock Zone

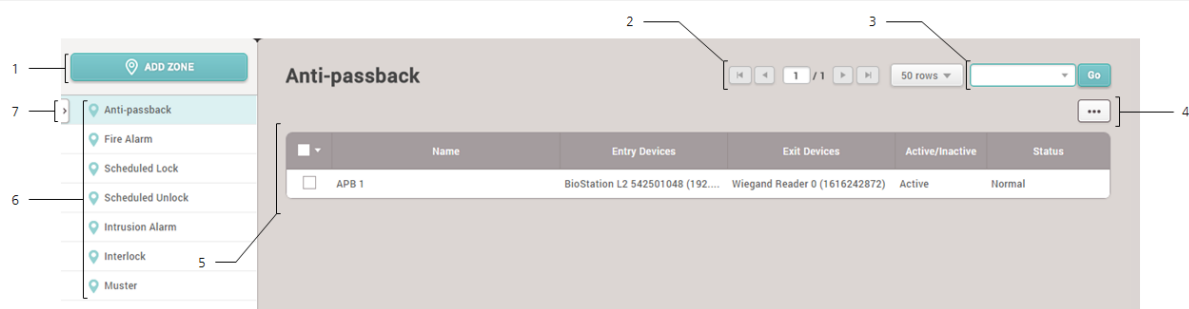
Muster Zone

 **Note**

- The **ZONE** menu will appear when the Advanced or higher license is activated.

142

11 Zone



- | | |
|---|-----------------|
| 1 Add Zone | 5 Zone List |
| 2 Page Navigation Buttons and Number of List Rows | 6 Zone Type |
| 3 Registered Zone Search | 7 Expand Button |
| 4 Function Button (Column Setting) | |

Anti-passback Zone

Anti-passback zone provides an enhanced function than the door based anti-passback feature.

- 1) Click **ZONE** and click **ADD ZONE**.
- 2) Click **Anti-passback** and click **Apply**.

1

Information

Name

APB 1

Type

Anti-passback

2

Configuration

Mode

Global

Anti-passback Type

Soft APB

Entry Confirmed APB

Follows door configuration

Entry Devices

BioStation 2 546832506 (192.168.14.221)

Network Failure Action

Open by auth

Active/Inactive

Active

Reset Time

1440 min.

Exit Devices

Xpass D2 400000005

3

Alarm

Action

Action

+ Add

4

APB Bypass

Bypass Group

Not Use

No.	Item	Description
1	Information	<div>Modify the settings of the anti-passback zone.</div> <ul style="list-style-type: none">Name: Enter an anti-passback name.

11 Zone

No.	Item	Description
		<ul style="list-style-type: none"> ▪ Type: View the zone type.
2	Configuration	<p>Modify the zone settings of the anti-passback.</p> <ul style="list-style-type: none"> ▪ Mode: It is possible to set either Local or Global for the range of zone application. If Local is set, the zone can be set only with the entry devices and devices connected with RS-485, and if Global is set, the zone can be set with all devices enrolled in BioStar 2. ▪ Active/Inactive: You can disable the anti-passback zone. Select Active to enable it. ▪ Anti-passback Type: Select an Anti-passback type. ▪ Reset Time: You can set a time period so that all anti-passback violations can be deleted. This allows the user to be granted access after the time period. The maximum possible duration is 7 days (10080 minutes). If set to 0, anti-passback violations will not be deleted and the users who have previously violated the anti-passback rule will not be granted access. ▪ Entry Confirmed APB: You can set the range to apply the anti-passback. If Entry Confirmed APB is set to ON, the anti-passback is applied according to the actual operation of the door that the entry and exit device are configured. If this option is set to OFF, the rule is applied according to the user's authentication regardless of the door operation. When set to Follows door configuration, the anti-passback rule is applied according to the setting of the Use sensor when Entry Confirmed APB enabled option of the door. ▪ Entry Devices: Select a device to use for entry. You can select a device from the list of added devices. If no registered device is available, see Basic Search and Registration, Advanced Search and Registration, Wiegand Device Search and Registration, or Slave Device Search and Registration. ▪ Exit Devices: Select a device to use at exit. You can select a device from the list of added devices. If there is no registered slave device, see Basic Search and Registration, Advanced Search and Registration, Wiegand Device Search and Registration, or Slave Device Search and Registration. ▪ Network Failure Action: It is possible to set the door operation in case the communication between BioStar 2 and the device where anti-passback is set has been lost. Setting is available when Global is set for Mode. When Open by auth is set, the door opens when the user has been authenticated normally. When Open by auth & record APB log is set, an anti-passback violation alarm occurs and the door opens. When Door locked & record APB log is set, an anti-passback violation alarm occurs and the door does not open.
3	Alarm	Choose the operation to be triggered when an APB violation occurs.
4	APB Bypass	Select an access level. Users who have the access level will not be restricted by the anti-passback rule.

11 Zone

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

Related Information

Anti-passback

Fire Alarm Zone

Configure the fire alarm zone.

- 1) Click **ZONE** and click **ADD ZONE**.
- 2) Click **Fire Alarm** and click **Apply**.

1

Information

Name

Type

Fire Alarm

2

Configuration

Mode

Door

Device / Input

Local

Door 1

Device / Input	Switch	Duration(ms)
Input Port 0 of BioStation 2 546832590 (192.168.16.196) ...	Normally Open	100

Active/Inactive

Elevator

Active

+ Add

3

Alarm


Action

Action

+ Add

No.	Item	Description
1	Information	<div>Modify the settings of the fire alarm zone.</div> <ul style="list-style-type: none">▪ Name: Enter a fire alarm zone name.▪ Type: View the zone type.
2	Configuration	<div>Modify the zone settings of the anti-passback.</div> <ul style="list-style-type: none">▪ Mode: You can set fire alarm in two different modes. Local mode will allow the master device and slave devices that are connected via RS-485 to be selected. Global mode will allow selection of all devices added to BioStar 2.▪ Active/Inactive: Disable the fire alarm zone. Select Active to enable it.

11 Zone

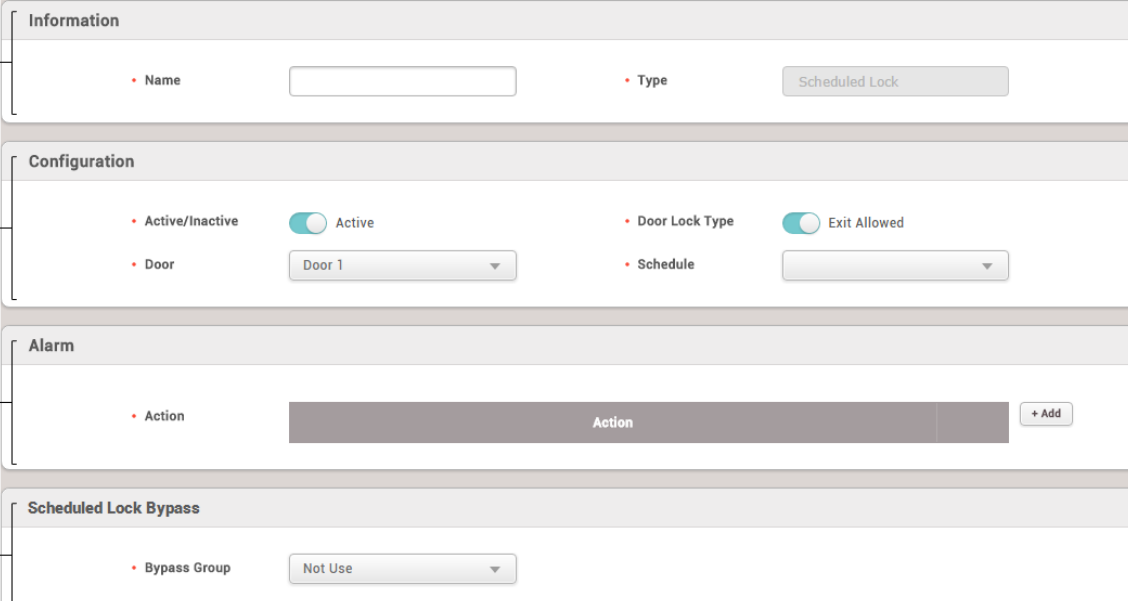
No.	Item	Description
		<ul style="list-style-type: none">▪ Door: Select the doors to include in the fire alarm zone. You can select multiple doors.▪ Elevator: Select the elevators to include in the fire alarm zone. You can select multiple elevators.▪ Device/Input: Click + Add and configure the device to set off the fire alarm signal. <p> Note</p> <ul style="list-style-type: none">▪ When Local is set for Mode, either Door or Elevator can be set as the fire zone.▪ When Global is set for Mode, both Door and Elevator can be set as the fire zone at the same time.
3	Alarm	Choose the operation to be triggered when a fire alarm signal occurs.

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

Scheduled Lock Zone

You can configure the scheduled lock zone. The scheduled lock zone keeps the door locked based on the schedule that has been set.

- 1) Click **ZONE** and click **ADD ZONE**.
- 2) Click **Scheduled Lock** and click **Apply**.



The screenshot displays the configuration interface for a Scheduled Lock Zone, organized into four main sections with numbered callouts:

- 1 Information:** Contains a **Name** text input field and a **Type** dropdown menu currently set to **Scheduled Lock**.
- 2 Configuration:** Includes an **Active/Inactive** toggle switch set to **Active**, a **Door** dropdown menu set to **Door 1**, a **Door Lock Type** toggle switch set to **Exit Allowed**, and a **Schedule** dropdown menu.
- 3 Alarm:** Features an **Action** dropdown menu and a **+ Add** button to add new actions.
- 4 Scheduled Lock Bypass:** Contains a **Bypass Group** dropdown menu currently set to **Not Use**.

11 Zone

No.	Item	Description
1	Information	Modify the settings of the scheduled lock zone. <ul style="list-style-type: none"> ▪ Name: Enter a scheduled lock zone name. ▪ Type: View the zone type.
2	Configuration	Modify the zone settings of the scheduled lock. <ul style="list-style-type: none"> ▪ Active/Inactive: Disable the scheduled lock zone. Select Active to enable it. ▪ Lock Type: You can configure the zone to lock only the entering device, or to lock both entering and exiting device. ▪ Door: Select the doors to include in the scheduled lock zone. You can select multiple doors. ▪ Schedule: Select a schedule. If no desired schedule is available, click + Add Schedule to create it.
3	Alarm	Choose the operation to be triggered when a scheduled lock signal occurs.
4	Scheduled Lock Bypass	Select an access level. Users who have the access level will not be restricted by the scheduled lock rule.

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


Scheduled Unlock Zone

You can configure the scheduled unlock zone. The scheduled unlock zone keeps the door open based on the schedule that has been set.

- 1) Click **ZONE** and click **ADD ZONE**.
- 2) Click **Scheduled Unlock** and click **Apply**.

No.	Item	Description
1	Information	Modify the settings of the scheduled unlock zone.

11 Zone

No.	Item	Description
		<ul style="list-style-type: none"> ▪ Name: Enter a scheduled unlock zone name. ▪ Type: View the zone type.
2	Configuration	<p>Modify the zone settings of the scheduled unlock.</p> <ul style="list-style-type: none"> ▪ Active/Inactive: Disable the scheduled unlock zone. Select Active to enable it. ▪ Started by User Authentication: When set as Active, the user who belongs to the access group must authenticate in the configured schedule to start a schedule unlock. ▪ Door/Elevator: You can set doors or elevators as schedule unlock zones. ▪ Schedule: Select a schedule. If no desired schedule is available, click + Add Schedule to create it. ▪ Door: If you select Door, the door list is activated. Select the doors to include in the scheduled unlock zone. You can select multiple doors. ▪ Elevator: If you select Elevator, the elevator list is activated. Select the elevators to include in the scheduled unlock zone. You can select multiple elevators. ▪ Floor: You can select the floor of the selected elevator. <p> Note</p> <ul style="list-style-type: none"> ▪ If you select an elevator that has already been configured with a different scheduled unlock zone, you cannot set the same floor.
3	Alarm	Choose the operation to be triggered when a scheduled unlock signal occurs.
4	Scheduled Unlock Authentication	You can select the access group where the user belongs who can start a scheduled unlock.

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

Intrusion Alarm Zone

When intrusion alarm zone is used, you can detect trespassing of an unauthorized user to a designated zone without permission.

- 1) Click **ZONE** and click **ADD ZONE**.
- 2) Click **Intrusion Alarm** and click **Apply**.

11 Zone

The screenshot shows a web interface for configuring an intrusion alarm zone. It is divided into five main sections, each indicated by a numbered callout:

- 1 Information:** Contains fields for 'Name' (a text input) and 'Type' (a dropdown menu currently showing 'Intrusion Alarm').
- 2 Configuration:** Contains a 'Mode' toggle set to 'Local', an 'Active/Inactive' toggle set to 'Active', and a 'Door' dropdown menu showing '14F Door 01'. A note states: 'The sensor of this door can be used as detecting intrusion.'
- 3 Arm / Disarm Setting:** Includes 'Delay Time' inputs for 'Arm' (0 s) and 'Disarm' (0 s). It has an 'Arm/Disarm Card' section with 'Card Type' and 'Card ID' fields and an '+ Add' button. There is also an 'Arm/Disarm Group' dropdown set to 'None'. Below these are two tables for 'Arm/Disarm Setting (Device)' and 'Arm/Disarm Setting (Input)', each with columns for 'Device / Input', 'Door', 'Entry / Exit', 'Arm Type', and 'Input Type', and an '+ Add' button.
- 4 Intrusion Setting:** Contains a 'Detect Intrusion' section with a table for 'Device / Input' and 'Summary', and an '+ Add' button.
- 5 Alarm:** Contains a 'Configuration' section with a table for 'Event' and 'Action', and an '+ Add' button.

No.	Item	Description
1	Information	<p>Modify the settings of the intrusion alarm zone.</p> <ul style="list-style-type: none"> ▪ Name: Enter an intrusion alarm zone name. ▪ Type: View the zone type.
2	Configuration	<p>You can change the general settings of an intrusion alarm zone.</p> <ul style="list-style-type: none"> ▪ Mode: You can check the application range of the zone. Only Local mode is supported for intrusion alarm zone, and the zone can be set only with devices connected to the entry device and RS-485. ▪ Active/Inactive: You can disable the intrusion alarm zone. Select Active to enable it. ▪ Door: Select the doors to include in the intrusion alarm zone.
3	Arm / Disarm Setting	<p>You can add an authentication setting for arm and disarm.</p> <ul style="list-style-type: none"> ▪ Delay Time: You can set the delay time to arm or disarm. Arm is the delay time from the authentication to the arm, and Disarm is the delay time from the intrusion detection to the alarm occurs. ▪ Access Card: You can add a card with permission to arm or disarm. You can register up to 128 access cards. ▪ Access Group: You can add an access group with permission to arm or disarm. You can register up to 128 access groups. ▪ Arm/Disarm Setting: You can set the arming and disarming by device or input signal. Click + Add and set each item. <p>Add arming and disarming by device</p>

11 Zone

No.	Item	Description
		<div>Click Device to select a device to control the intrusion alarm zone among the entry and exit devices of the door, and select Arm Type. Card, Key, and Card or Key can be selected for the Input type. Only Card is available as the input type for a device with no LCD screen.</div> <div><div>Add Arm/Disarm Setting (Device) X</div><div><div><div>• Device</div><div>BioStation L2 542501048 (192.168.14.125) ▼</div></div><div><div>• Arm Type</div><div>Arm / Disarm ▼</div></div><div><div>• Input Type</div><div>Card or Key ▼</div></div></div><div><div>Apply</div><div>Cancel</div></div></div> <div><p>Add arming and disarming by input signal</p><p>Click Device to select the device that controls the intrusion alarm zone.</p><p>Click Port and select an input port of the selected device.</p><p>Select Arm Type and set the switch type and the signal duration.</p></div>

11 Zone

No.	Item	Description
		<div><div>Add Arm/Disarm Setting (Input) ×</div><div><div>Setting</div><div><div><div>• Device</div><div>BioStation L2 542501048 ... ▼</div></div><div><div>• Port</div><div>Input Port 0 ▼</div></div><div><div>• Arm Type</div><div>Arm / Disarm ▼</div></div></div><div><div><div>• Switch</div><div><input checked="" type="checkbox"/> Normally Open</div></div><div><div>• Duration(ms)</div><div>100 ▲ ▼</div></div></div></div></div> <div><div>Apply</div><div>Cancel</div></div> <div><div><div>✔</div><div>Note</div></div><div><div>▪ It is activated only when Door is set from Configuration.</div></div></div>
4	Intrusion Setting	<p>You can set the intrusion detection signal. When you click + Add and set as shown in the screen below, the device recognizes the detection of intrusion if N/O sensor connected to input port 0 of BioStation L2 sends a signal for 100(ms).</p>

11 Zone

No.	Item	Description
		<div> <div>Add Intrusion Setting</div> <div> <div>Setting</div> <div> <div> <div>• Device</div> <div>BioStation L2 542501048 ...</div> </div> <div> <div>• Port</div> <div>Input Port 0</div> </div> </div> <div> <div>• Switch</div> <div> <input checked="" type="checkbox"/> Normally Open </div> <div> <div>• Duration(ms)</div> <div>100</div> </div> </div> </div> <div> <div>Apply</div> <div>Cancel</div> </div> <div> <div> <div>☑</div> <div>Note</div> </div> <ul style="list-style-type: none"> It is activated only when Door is set from Configuration. </div> </div>
5	Alarm	<p>Set the alarm action to carry out when a specific event occurs at the intrusion alarm zone.</p> <div> <div> <div>☑</div> <div>Note</div> </div> <ul style="list-style-type: none"> It is activated only when Door is set from Configuration. </div>

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

Interlock Zone

Interlock zone monitors the status of two or more doors by door sensor and relay state to control that one door cannot be opened or close if other doors are open or unlocked. You can also disable access if a user stays within the zone.

11 Zone

 **Note**

- An interlock zone can be configured with up to 4 doors.
- An interlock zone can only set the doors with the devices connected to the CoreStation.
- A device set as an interlock zone cannot be set to another zone.
- A door set as an interlock zone cannot be set to another zone other than the fire alarm zone.

- 1) Click **ZONE** and click **ADD ZONE**.
- 2) Click **Interlock** and click **Apply**.
- 3) Edit the necessary items.

1

Information

Name

Type

Interlock

2

Configuration

Mode

Local

Active/inactive

Active

Door

Door 2

* Door sensor must be set to use.

3

Option

Action

Device / Input

Summary

+ Add

4


Alarm

Action


Event

Action

+ Add

No.	Item	Description
1	Information	<div>Modify the settings of the interlock zone.</div> <ul style="list-style-type: none">▪ Name: Enter an interlock zone name.▪ Type: View the zone type.
2	Configuration	<div>You can change the general settings of an interlock zone.</div> <ul style="list-style-type: none">▪ Mode: You can check the application range of the zone. Only Local mode is supported for interlock zone, and the zone can be set only with devices connected to the CoreStation and RS-485.▪ Active/Inactive: You can disable the interlock zone. Select Active to enable it.▪ Door: Select the doors to include in the interlock zone. You must select at least two doors that are the door sensor is connected.
3	Option	<div>If a user stays in the zone, this option can prevent others from entering the zone.</div> <div> Note</div>

11 Zone

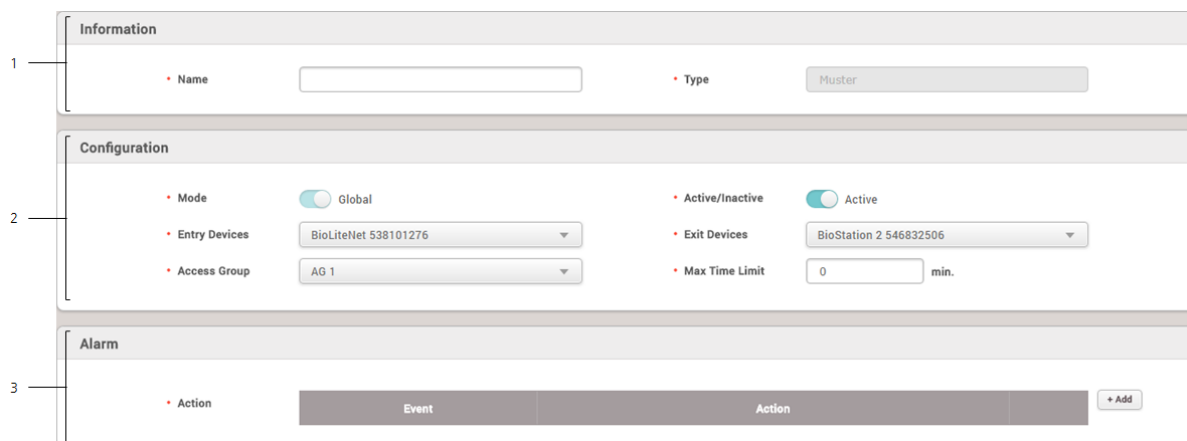
No.	Item	Description
		<ul style="list-style-type: none"> It is activated only when Door is set from Configuration.
4	Alarm	<p>Set the alarm action to carry out when a specific event occurs at the interlock zone.</p> <p> Note</p> <ul style="list-style-type: none"> It is activated only when Door is set from Configuration.

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

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.

- Click **ZONE** and click **ADD ZONE**.
- Click **Muster** and click **Apply**.
- Edit the necessary items.



No.	Item	Description
1	Information	<p>Modify the settings of the muster zone.</p> <ul style="list-style-type: none"> Name: Enter a muster zone name. Type: View the zone type.
2	Configuration	<p>You can change the general settings of a muster zone.</p> <ul style="list-style-type: none"> Mode: You can check the application range of the zone. Only Global mode is supported for muster zone, and the zone can be set with all devices added to BioStar 2. Active/Inactive: You can disable the muster zone. Select Active to

11 Zone

No.	Item	Description
		<p>enable it.</p> <ul style="list-style-type: none">▪ Entry Devices: Select a device to use for entry. You can select a device from the list of added devices. If no registered device is available, see Basic Search and Registration, Advanced Search and Registration, Wiegand Device Search and Registration, or Slave Device Search and Registration.▪ Exit Devices: Select a device to use at exit. You can select a device from the list of added devices. If there is no registered slave device, see Basic Search and Registration, Advanced Search and Registration, Wiegand Device Search and Registration, or Slave Device Search and Registration.▪ Access Group: Set the access group to which the user who will be staying in the muster zone. Up to 16 access groups can be set.▪ Max Time Limit: Set the maximum amount of time that user can stay in the zone. It can be set up to 4320 minutes, and an alarm occurs when the user stays in the muster zone exceeding the specified time.
3	Alarm	<p>Set the alarm action to carry out when a specific event occurs at the muster zone.</p> <p> Note</p> <ul style="list-style-type: none">▪ It is activated only when Entry Devices and Exit Devices is set from Configuration.

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

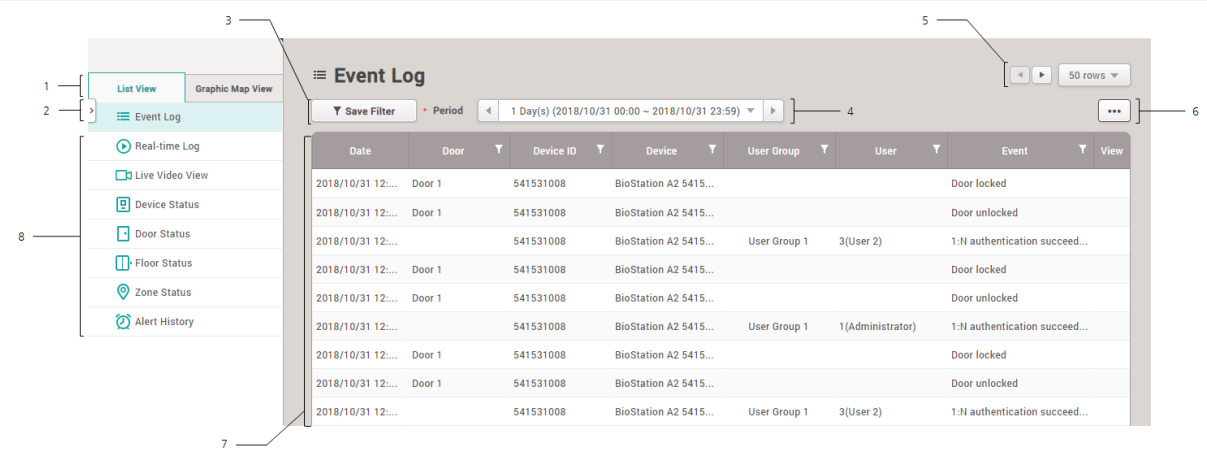
You can use the **MONITORING** menu to view lists of access control events, device and door status, zone status and the alert history.

You can see and control the status of the doors in real-time in the graphic if you add a graphic map.

[List View](#)

[Graphic Map View](#)

12 Monitoring



- 1 Tab buttons for List View and Graphic Map View
- 2 Expand Button
- 3 Save Filter Button
- 4 Search period of Event Log
- 5 Page Navigation Buttons and Number of List Rows
- 6 Function Button (Print, CSV Export, Data File Import, Column Setting)
- 7 List of Selected Monitoring Items
- 8 Monitoring Categories

- Note**
- The **Floor Status**, **Zone Status** and **Graphic Map View** will appear when the AC standard license is activated.
 - The **Live Video View** menu will appear when the Video license is activated.

List View

You can see lists of access control events, device and door status, zone status and the alert history. You can also apply filters to the collected monitoring data and view specific types of monitoring information.

- Event Log
- Real-time Log
- Live Video View
- Device Status
- Door Status
- Floor Status
- Zone Status
- Alert History

12 Monitoring

Note

- The **Floor Status** and **Zone Status** menu will appear when the AC standard license is activated.
- The **Live Video View** menu will appear when the Video license is activated.

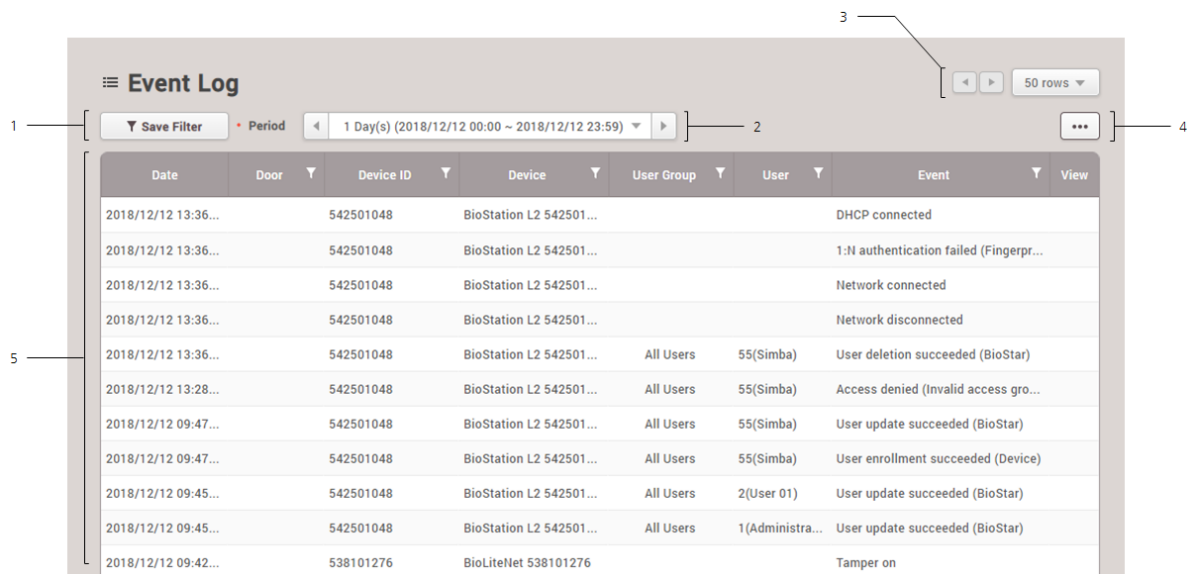
Event Log

You can view all the logs of all past events. You can also apply various filters to sort the displayed data.

Note

- Make sure to check the time and date setting of the device. For more information on configuring device time, see [Information](#).
- When the image log is set, you can view or store a stored image in its actual size.
- Use a separate storage media for the video log. Video logs might not be saved if the video storage space is reduced by the external processing(such as copying files and creating files), To change the path to save video logs, see [Video](#).

- 1) Click **MONITORING > List View > Event Log**.
- 2) To view log entries of a specific type only, click the ▾ of a column and apply a filter.



The screenshot shows the 'Event Log' interface. Callout 1 points to the 'Save Filter' button. Callout 2 points to the 'Period' dropdown menu showing '1 Day(s) (2018/12/12 00:00 ~ 2018/12/12 23:59)'. Callout 3 points to the page navigation buttons (previous, next, and '50 rows' dropdown). Callout 4 points to the column headers. Callout 5 points to the list of event log entries.

Date	Door	Device ID	Device	User Group	User	Event	View
2018/12/12 13:36...		542501048	BioStation L2 542501...			DHCP connected	
2018/12/12 13:36...		542501048	BioStation L2 542501...			1:N authentication failed (Fingerpr...	
2018/12/12 13:36...		542501048	BioStation L2 542501...			Network connected	
2018/12/12 13:36...		542501048	BioStation L2 542501...			Network disconnected	
2018/12/12 13:36...		542501048	BioStation L2 542501...	All Users	55(Simba)	User deletion succeeded (BioStar)	
2018/12/12 13:28...		542501048	BioStation L2 542501...	All Users	55(Simba)	Access denied (Invalid access gro...	
2018/12/12 09:47...		542501048	BioStation L2 542501...	All Users	55(Simba)	User update succeeded (BioStar)	
2018/12/12 09:47...		542501048	BioStation L2 542501...	All Users	55(Simba)	User enrollment succeeded (Device)	
2018/12/12 09:45...		542501048	BioStation L2 542501...	All Users	2(User 01)	User update succeeded (BioStar)	
2018/12/12 09:45...		542501048	BioStation L2 542501...	All Users	1(Administra...	User update succeeded (BioStar)	
2018/12/12 09:42...		538101276	BioLiteNet 538101276			Tamper on	

No.	Item	Description
1	Save Filter Button	Saves the set filter.
2	Period	You can set a desired period and sort event logs.
3	Page Navigation Buttons and	You can move a page or set the number of list rows to be displayed on one page.

12 Monitoring

No.	Item	Description
	Number of List Rows	<ul style="list-style-type: none"> : Go to the first page. : Go to the previous page. : Set the number of list rows to be displayed on one page.
4	Function Buttons (Print, CSV Export, Data File Import, Column Setting)	<p>You can use the additional features with event logs.</p> <ul style="list-style-type: none"> Print the event log Export to CSV file Import the data file Change the column setting <p> Note</p> <ul style="list-style-type: none"> For more information about importing a data file, see Import Event Logs.
5	Event Log	Shows the event log. When an image log exists, it is displayed as and you can view or store a captured image in its actual size in PC.

Note

- When **Log Upload** is set to **Manual**, the user can import the log manually by clicking **Update Log**. For how to change log upload setting, refer to [Server](#).

If **Latest** is set, the log saved after the date of the log saved last in BioStar 2 will be imported from the device, and if **All** is set, all logs of the device will be imported to BioStar 2. You can also set a date range within which to import logs.


Import Event Logs

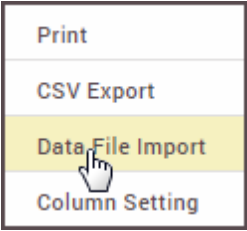
You can view all the logs of all past events. You can also apply various filters to sort the displayed data.

Note

- The exported data file from devices using older firmware version cannot be imported into BioStar 2. Make sure always use the latest version of firmware.
- Only data files exported from FaceStation 2, BioStation A2, and BioStation 2 can be imported.
- Some information of event log may appear as a blank if a door, elevator, or zone is not set by the BioStar 2.

12 Monitoring

1) Click  and then click **Data File Import**.




- 2) Select the desired file (*.tgz) and then click **Open**.
- 3) A success message will appear on the screen when import successfully.

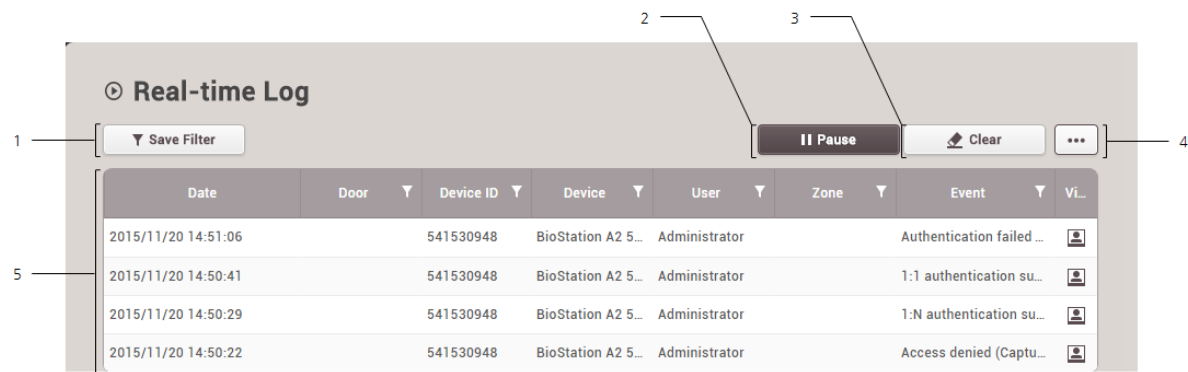
Real-time Log

You can view a log of various events in real time.

 **Note**


- Make sure to check the time and date setting of the device. For more information on configuring the device time, see [Information](#).
- The real-time log can only be viewed while the **Real-time Log** page is displayed. In other words, when the administrator is viewing another page for changing device settings, etc., the real-time log cannot be viewed.
- If **Log Upload** is set to **Manual** in the [Server](#), the real-time log cannot be viewed.
- When the image log is set, you can view or store a stored image in its actual size.

- 1) Click **MONITORING > List View > Real-time Log**.
- 2) To view log entries of a specific type only, click the  of a column and apply a filter.



No.	Item	Description
1	Save Filter Button	Saves the set filter.

12 Monitoring

No.	Item	Description
2	Start/Pause Button	Pauses or starts real-time log collection.
3	Clear Button	Clears the collected log information. To view the entire event log, see Event Log .
4	Function Buttons (Column Setting)	Changes the column setting of the log.
5	Event Log	Shows the event log. When an image log occurs, a notification will pop up on the left side of the browser screen and you can view a captured image in its actual size of store in PC. You can also press  to check.

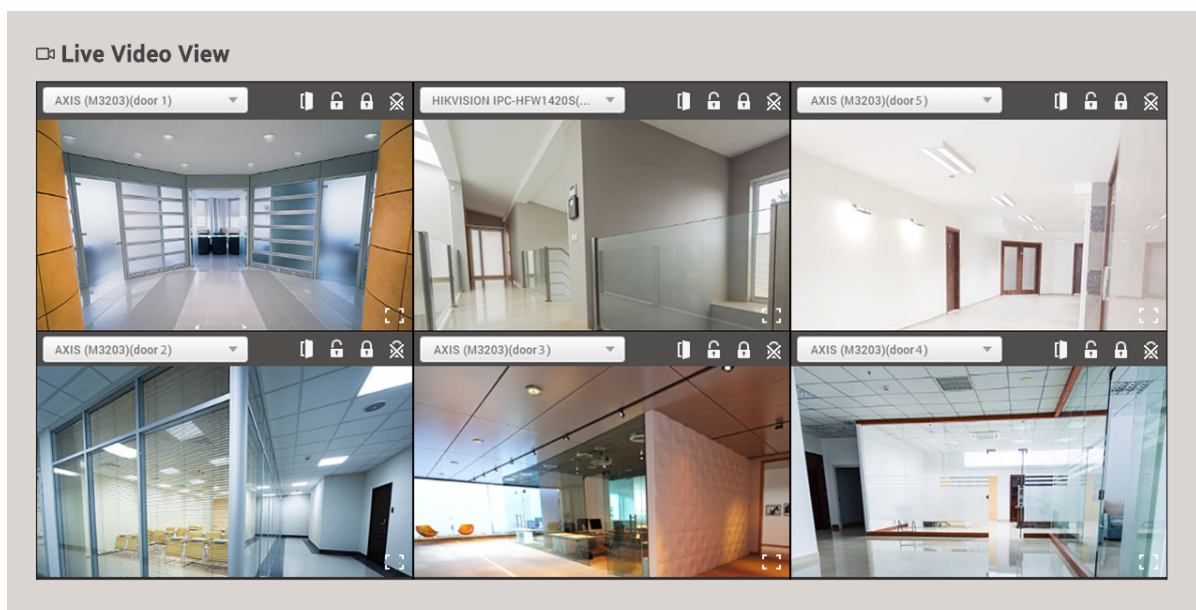
Live Video View

You can see the screen of IP camera set in Video menu and event log set up in real time. In addition, Open, Manual Unlock, Manual Lock, and Release functions are available for the door control function.

Note

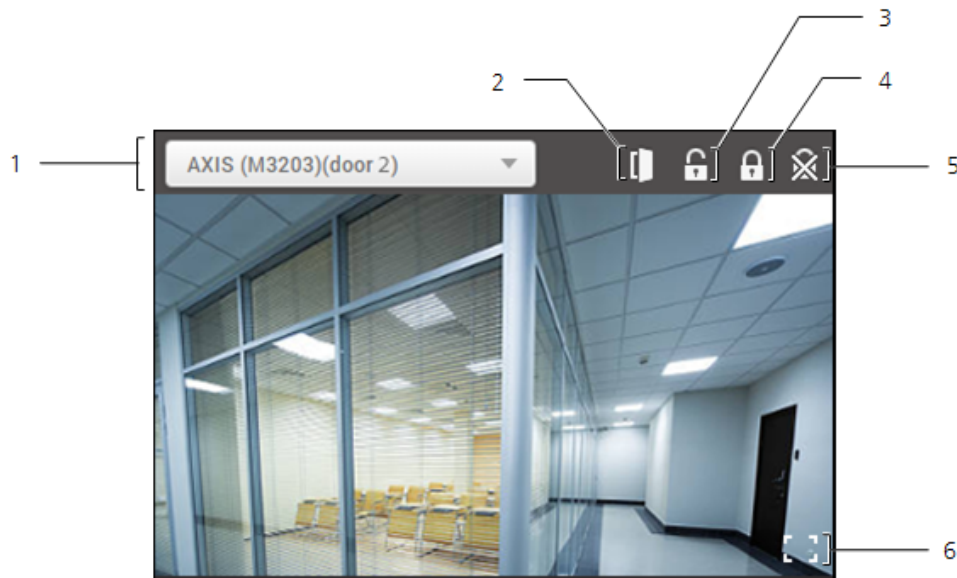
- The **Live Video View** menu will appear when the Video license is activated.
- For more information on registering the NVR and IP camera, see [Video](#).
- IP cameras that do not support the live streaming feature are displayed as "Disconnected".
- PC-NVR does not support the live video view.

1) Click **MONITORING** > **List View** > **Live Video View**.



12 Monitoring

- 2) Refer to the explanation below for how to operate the screen.



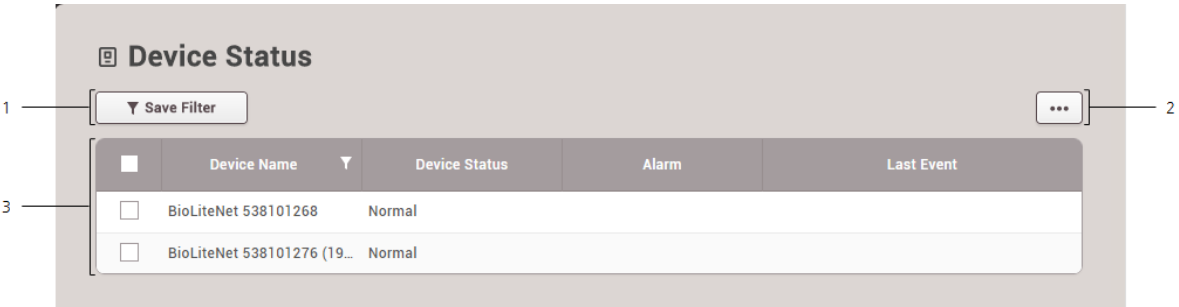
No.	Item	Description
1	IP camera	Select the IP camera to monitor. If there is no desired the IP camera, see Video .
2	Open	Open the door temporarily.
3	Manual Unlock	Unlock the door manually.
4	Manual Lock	Lock the door manually.
5	Release	Release the manual unlock or manual lock.
6	Large size view	The live view screen can be viewed in a large size.

Device Status

You can view various device status information such as the device status, alarm and last event.

- 1) Click **MONITORING > List View > Device Status**.
- 2) To view log entries of a specific type only, click the ▼ of a column and apply a filter.

12 Monitoring



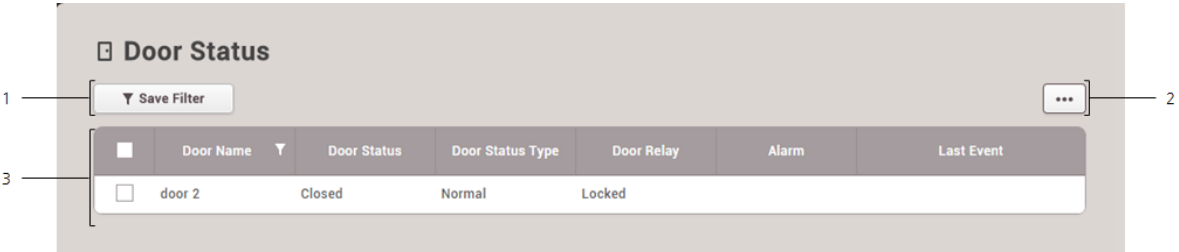
No.	Item	Description
1	Save Filter Button	Saves the set filter.
2	Function Buttons (Column Setting)	Changes the column setting of the log.
3	Status List	Shows the device status list. <ul style="list-style-type: none">Select a device and click Clear Alarm to clear the alarm.

Door Status

You can view various door status information such as the door status, relay status, alarm and last event.

You can also apply various filters to sort the displayed data.

- 1) Click **MONITORING > List View > Door Status**.
- 2) To view log entries of a specific type only, click the ▼ of a column and apply a filter.



No.	Item	Description
1	Save Filter Button	Saves the set filter.
2	Function Buttons (Column Setting)	Changes the column setting of the log.

12 Monitoring

No.	Item	Description
3	Status List	<p>Shows the door status list.</p> <p>The following operations are available for the selected door:</p> <ul style="list-style-type: none">▪ Manual Lock: Click after selecting a door to lock the door manually. If you set Manual Lock, the door will have remained inaccessible even if a user authenticates.▪ Manual Unlock: Click after selecting a door to unlock the door manually. If you set Manual Unlock, the door will have remained accessible even if a user does not authenticate.▪ Release: Release the manual lock or manual unlock set by the administrator.▪ Open: Click after selecting a door to open the door temporarily.▪ Clear Alarm: Clear alarms of all doors. If an alarm is set in the Zone, the alarm may be continuously output even if the door alarm is released. Click Clear Alarm on Zone Status.▪ Clear APB: Reset the anti-passback violation by selecting all or each user.

Note

Refer to below for the explanation on door events.

- **Fire alarm unlocked:** A state where the door designated as a fire alarm zone is unlocked because a fire has broken out.
- **Manual Lock:** A state where the door is locked because the administrator has locked it manually.
- **Manual Unlock:** A state where the door is unlocked and able to enter without an authentication because the administrator has unlocked it manually.
- **Schedule Locked:** A state where the door is locked by the schedule that has been set.
- **Schedule Unlocked:** A state where the door is unlocked by the schedule that has been set.
- **Normal:** A state where a user can enter the door after an authentication.

Floor Status

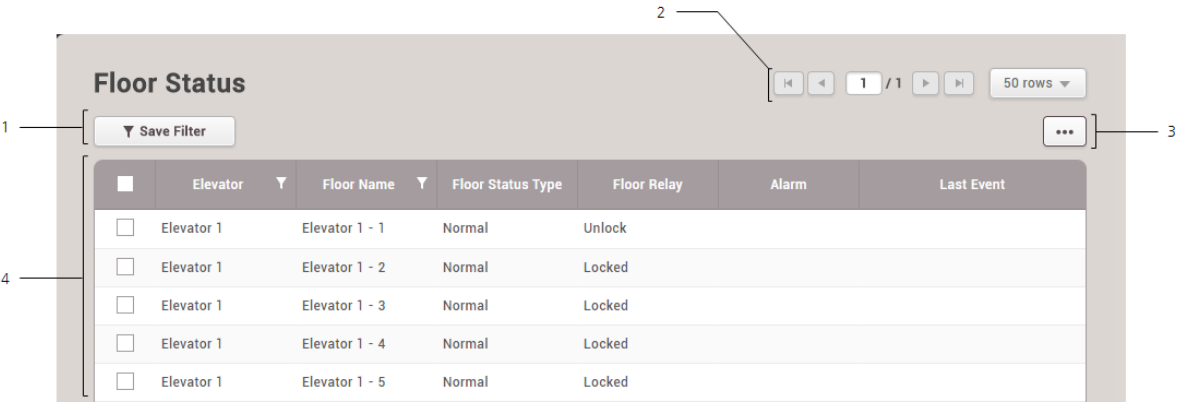
You can view various floor status information such as the floor status, relay status, alarm and last event.

Note

- The **Floor Status** menu will appear when the Advance or higher license is activated.

- 1) Click **MONITORING > List View > Floor Status**.
- 2) To view log entries of a specific type only, click the ▼ of a column and apply a filter.

12 Monitoring



No.	Item	Description
1	Save Filter Button	Saves the set filter.
2	Function Buttons (Column Setting)	Changes the column setting of the log.
3	Status List	<p>Shows the floor status list.</p> <p>The following operations are available for the selected floor:</p> <ul style="list-style-type: none">▪ Manual Lock: Click after selecting a floor to lock the floor manually.▪ Manual Unlock: Click after selecting a floor to unlock the floor manually.▪ Release: Release the manual lock.▪ Open: Click after selecting a floor to open the floor temporarily.▪ Clear Alarm: Clears alarms of all floors.

Zone Status

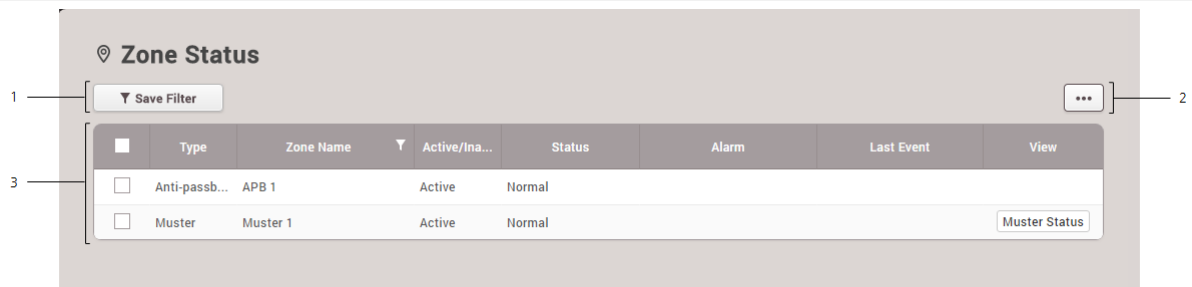
View zone status information such as the zone active status, alarm status, and the last event that has occurred.


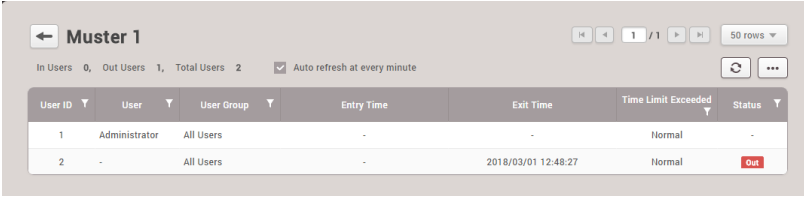
 **Note**

- The **Zone Status** menu will appear when the Standard or higher license is activated.

- 1) Click **MONITORING > List View > Zone Status**.
- 2) To view log entries of a specific type only, click the ▼ of a column and apply a filter.

12 Monitoring



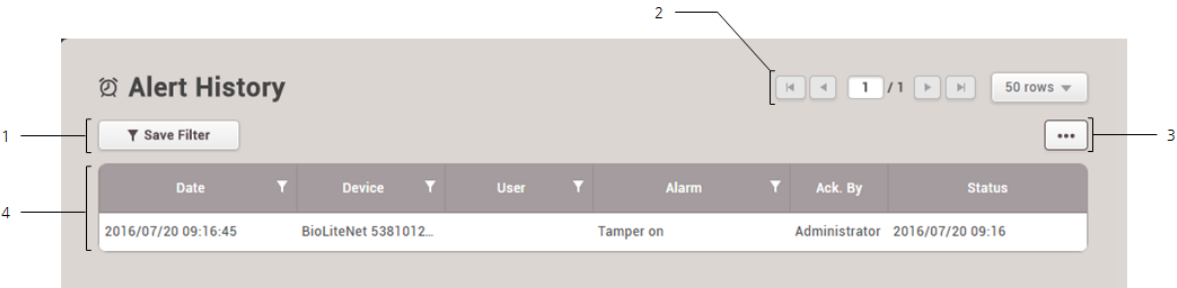
No.	Item	Description
1	Save Filter Button	Saves the set filter.
2	Function Button (Column Setting)	Changes the column setting of the log.
3	Status List	<p>Shows the zone status list.</p> <p>The following operations are available for the selected zone:</p> <ul style="list-style-type: none"> ▪ Clear APB: Reset the anti-passback violation by selecting all or each user. This can be only used when selecting an anti-passback zone. ▪ Clear Alarm: Release the anti-passback violation alarm when selecting an anti-passback zone, and closes the door relays that has been opened by the fire alarm when selecting a fire alarm zone. <p> Note</p> <ul style="list-style-type: none"> ▪ If a muster zone is set, you can check the user's status by clicking the Muster Status. 

Alert History

You can view the history and status of various alerts. You can also apply various filters to sort the displayed data.

- 1) Click **MONITORING > List View > Alert History**.
- 2) To view log entries of a specific type only, click the ▼ of a column and apply a filter.

12 Monitoring



No.	Item	Description
1	Save Filter Button	Saves the set filter.
2	Page Indicator and Navigation Buttons	<p>You can move a page or set the number of list rows to be displayed on one page.</p> <ul style="list-style-type: none">◀: Go to the first page.◀: Go to the previous page.2 / 2: Enter the page number to move to.▶: Go to the next page.▶: Go to the last page.25 rows ▼: Set the number of list rows to be displayed on one page.
3	Function Buttons (Print, Column Setting)	Prints the log or changes the column setting.
4	Alert History	<p>Shows the alert list.</p> <p>Click 📄 to view the alert details.</p>

Graphic Map View

If you add a graphic map, you can see and control the status of the doors in real-time in the graphic. You can control the door and relay using the icons in the door status bar and see the alarm when an event occurs at the door.

Adding and Managing Graphic Map Groups

Adding and Managing Graphic Maps

 **Note**

- The **Graphic Map View** will appear when the AC standard license is activated.

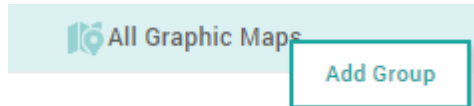
12 Monitoring

Adding and Managing Graphic Map Groups

You can register graphic map groups for easy management of multiple devices. Name your graphic map groups according to door locations or office names for greater convenience.

— Adding Graphic Map Groups

- 1) Click **MONITORING > Graphic Map View**.
- 2) Right-click on **All Graphic Maps** and click **Add Group**.



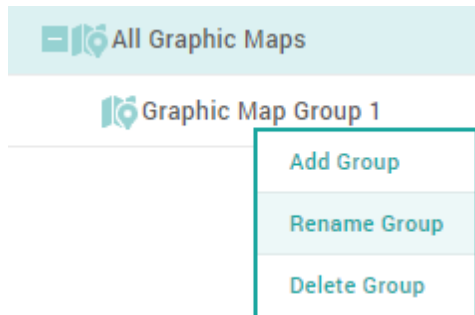
- 3) Enter a group name.

Note

- Graphic map groups may be created in up to 8 levels.
- Up to 48 characters may be entered for a graphic map group name.

Renaming Graphic Map Groups

- 1) Click **MONITORING > Graphic Map View**.
- 2) Right-click on the name of a group you wish to rename and click **Rename Group**.



- 3) Enter a group name.

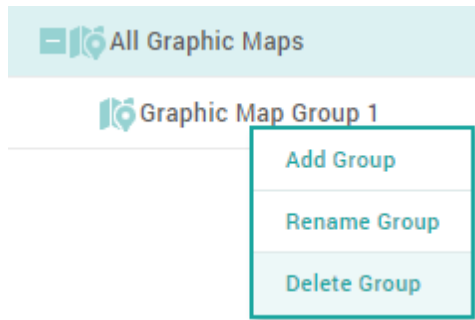
Note

- Up to 48 characters may be entered for a graphic map group name.

Deleting Graphic Map Groups

- 1) Click **MONITORING > Graphic Map View**.
- 2) Right-click on the name of a group you wish to delete and click **Delete Group**.

12 Monitoring



Note

- You cannot delete a group if it contains a graphic map. To delete a group, you must delete all graphic maps belonging to the group.

Adding and Managing Graphic Maps

If you add a graphic map, you can see and control the status of the doors in real-time in the graphic.

Adding Graphic Map

- 1) Click **MONITORING > Graphic Map View**.
- 2) Click **ADD GRAPHIC MAP**.

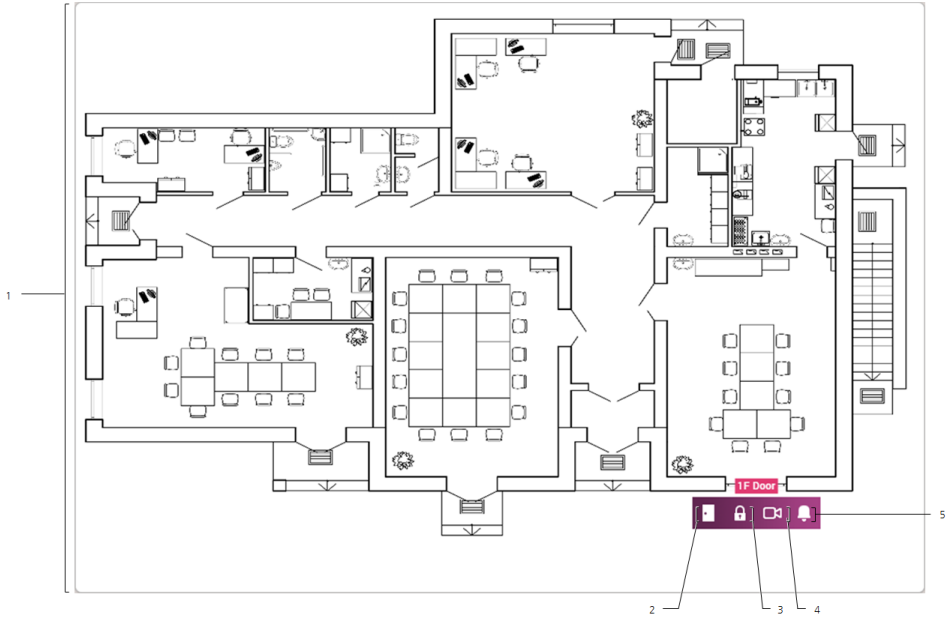
A screenshot of a 'Configuration' form. The form has a title bar 'Configuration' with a close button. It contains four fields: 'Name' (text input), 'Group' (dropdown menu with 'All Graphic Maps' selected), 'Background' (with an 'Upload' button), and 'Door' (dropdown menu). There is also a 'Zone' dropdown menu on the right side of the form.

- 3) Set the name and group of the graphic map.
- 4) Click **Upload** and select the background you want to use as the graphic map.

Note

- The max size of the images that can be used as a background is 5MB.
 - Supported image file formats are BMP, GIF, JPG, JPEG, PNG.
 - If you back up the BioStar 2 database, the image file registered in the graphic map may be deleted. If you want to continue using images registered as a background even after database backup, back up the image files.
- 5) Select the door you want to display on the graphic map from the **Door**. The door status bar appears.

12 Monitoring




N o.	Item	Description
1	Graphic Map	The uploaded background image appears.
2	Door Status	You can see the door status and temporarily open the door.
3	Door Relay	You can lock or unlock the door manually.
4	Live Video View	<div>You can see the screen of the IP camera registered at the door in real time.</div> <div><div><div><div></div></div><div>Note</div></div><div><div>▪</div><div>The Live Video View button is activated only when the camera is registered at the door.</div></div></div>
5	Alarm	You can see or clear the alarm that has occurred on the door.

- 6) Select the zone you want to display on the graphic map from the **Zone**. The Zone status bar appears.

N o.	Item	Description
1	Zone	You can see the type of zone.

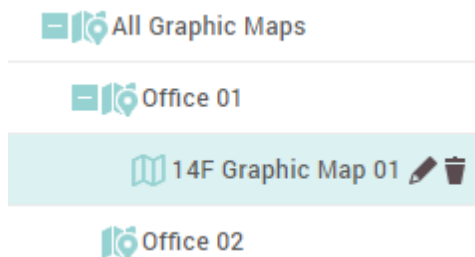
12 Monitoring

N o.	Item	Description
		 Note <ul style="list-style-type: none">▪ The zones can be selected up to 100.
2	Alarm	You can see or clear the alarm that has occurred on the zone.

- 7) Drag the door and zone status bar to the location of the door and zone in the graphic map.
- 8) When setting is finished, click **Apply**.


Editing Graphic Map

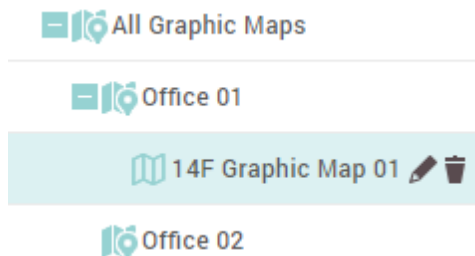
- 1) Click **MONITORING > Graphic Map View**.
- 2) Click  in the graphic map that you want to edit.



- 3) After editing the information you want, click **Apply**.

Deleting Graphic Map

- 1) Click **MONITORING > Graphic Map View**.
- 2) Click  in the graphic map that you want to delete.



- 3) Click **Yes** to delete the selected graphic map.

You can use the **VIDEO** menu to interlock an IP camera with an event of the door. You can set the IP camera to record video or image logs when a set event occurs. Saved videos can be viewed in the **MONITORING** menu.

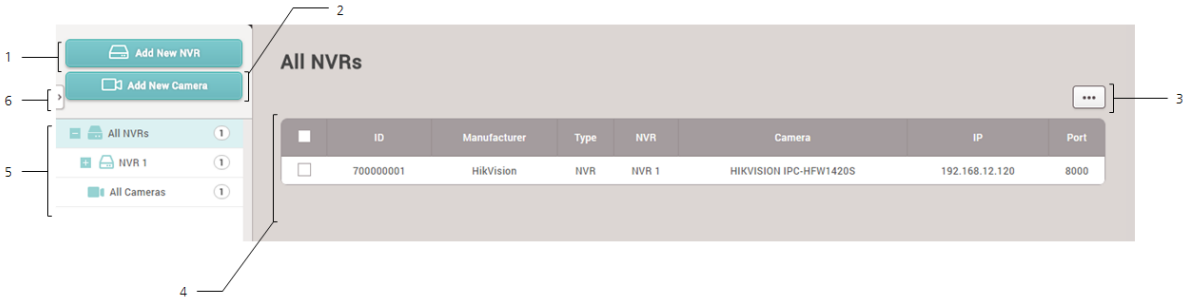
13 Video

Adding NVRs

Adding IP Cameras

 **Note**

- The **VIDEO** menu will appear when the Video license is activated.
- If you connect BioStar 2 using the Cloud, cannot access to the **VIDEO** menu.
- Set the Network Time Protocol (NTP) on a PC with BioStar 2 installed before using the **Video** menu. Go to the **Control Panel > Date and Time** and then click **Change setting** on the **Internet Time** to set up. Use *time.windows.com* for the server address.



- | | |
|------------------------------------|-------------------------------|
| 1 Add NVR | 4 NVR and IP Camera List |
| 2 Add IP Camera | 5 NVR and IP Camera Hierarchy |
| 3 Function Button (Column Setting) | 6 Expand Button |

Adding NVRs

You can add NVR to save video logs or image logs.

 **Note**

- ACTi, Dahua, and Hikvision products can be added for NVR. Before adding NVR, check its manufacturer.
- Set the Network Time Protocol (NTP) to synchronize the time between the BioStar 2 server and the NVR. Use *time.windows.com* for the server address.
- PC-NVR does not support the live video view.
- NVR types that support the live video view are as follows.
 - Dahua: DH-NVR4416-16P, DH-NVR608-32-4K
 - Hikvision: DS-7616NI-E2 / 16P, DS-7608NI-E2 / 8P

13 Video

- 1) Click **VIDEO > Add New NVR**.
- 2) Edit the necessary items.

Add New NVR

Name

Manufacturer

IP

Port

ID

Password

Apply

Cancel

No.	Item	Description
1	Name	Enter the name of NVR.
2	Manufacturer	Select the manufacturer of NVR. ACTi, Dahua and Hikvision products are supported.
3	IP	Enter the IP address of NVR.
4	Port	Enter the port of NVR.
5	ID	<div>Enter the account information (ID) to access NVR.</div> <div><div><div></div></div><div>Note<ul style="list-style-type: none">▪ Enter the default administrator account information for the ID. If you enter the ID after creating a custom administrator account in NVR setting, the function may not work properly.</div></div>
6	Password	Enter the account information (password) to access NVR.

- 3) Click **Apply** to save the changes.

Note

- Contact the system administrator for the detailed information of NVR (**IP, Port, ID, Password**).

13 Video

Adding IP Cameras

You can add an IP camera connected to NVR.

 **Note**

- Before adding an IP camera, add NVR first. For more details, refer to [Adding NVRs](#).
- Set the Network Time Protocol (NTP) to synchronize the time between the BioStar 2 server and the IP camera. Use *time.windows.com* for the server address.

- 1) Click **VIDEO > Add New Camera**.
- 2) Select an added NVR from the list and click **Next**.

Select NVR

• NVR

NVR 1

Next

Cancel

- 3) The list of cameras connected to NVR will appear. Select a camera to add and click **+ Add**. To select a different NVR, click **Prev**.

Camera List

NVR 1

	Type	IP
<input type="checkbox"/>	HIKVISION IPC-HFW1420S	192.168.12.110
<input type="checkbox"/>	AXIS (M3203)	192.168.12.63
<input type="checkbox"/>	112_Amcrest	192.168.12.112
<input type="checkbox"/>	HikVion IP 84	192.168.12.84

Prev

+ Add

Cancel

- 4) After adding the camera, you can set the camera to record a video log according to an event occurring at the door. For more details, refer to [Editing IP Camera Settings](#).

13 Video

Editing IP Camera Settings

You can set the time interval to capture a video log or an image log and link the door and event type to the IP camera.

- 1) In the camera list, click a camera to edit.
- 2) Edit the necessary items.

Information

1

ID

720000001

2

Name

HIKVISION IPC-HFW142...

4

IP

192.168.12.110

5

Log Type

Video

3

Channel

33

Configuration

6

Video Log Setting

Start recording

3

secs before an event

End recording

3

secs after an event

7

Event

Door

▼

Event





Event

Schedule

+ Add

No.	Item	Description
1	ID	You can view the camera ID.
2	Name	You can change the camera name.
3	Channel	You can view the camera channel.
4	IP	You can view the IP address of the camera.
5	Log Type	<div>You can set the log type to be captured by the camera.</div> <div><div><div>▪ None: A video log or an image log is not captured.</div><div>▪ Video: A video log is captured.</div><div>▪ Image: An image log will captured.</div></div><div><div>📌 Note</div><div><div>▪ You can set Video Log Setting or Image Log Setting according to the set Log Type.</div><div>▪ None is set for Log Type, you cannot set the Video Log Setting,</div></div></div></div>

13 Video

No.	Item	Description
		Image Log Setting, and Event.
6	Video Log Setting / Image Log Setting	<p>You can set the time to capture a video log or an image log.</p> <p> Note</p> <ul style="list-style-type: none"> You can set Video Log Setting or Image Log Setting according to the set Log Type. <p>When Log Type is set to Video</p> <p>• Start recording <input type="text" value="3"/> secs before an event • End recording <input type="text" value="3"/> secs after an event</p> <p>When Log Type is set to Image</p> <p>• Capture an image <input type="text" value="3"/> s <input type="text" value="before"/> an event</p> <p> Note</p> <ul style="list-style-type: none"> Recorded video/image logs does not mean the real-time log. It can view after storing in in BioStar 2 database.
7	Event	<p>Select a pre-registered entrance door. Click + Add and set a desired event and schedule.</p> <p> Note</p> <ul style="list-style-type: none"> Door should be set. Only one door can be set per camera. If there is no registered entrance door, register one by referring to Adding Doors. If there is no desired schedule, click Setting > Schedule and register a new schedule. For more details, refer to Schedule. You can delete an added event by clicking .

3) Click **Apply** to save the changes.

You can set the time code, shift, and schedule and/or view time card or report by using the **TIME ATTENDANCE** menu.

[Shift](#)

[Schedule](#)

[Report](#)

[Setting](#)

14 Time & Attendance

Set according to the following order when registering the schedule for the first time.

Step 1. Time code setting

You can set the attendance and leave time code, overtime time code, and the go out/outside work/vacation time code. You can also set the time rate and assign and display a color to make it easily recognizable.

➤ Related information

Time code

Step 2. Shift setting

You can set the service rule on a daily basis (24 hours). The shift includes the time code setting, the start time of day setting and the rounding rule.

➤ Related information

Shift

Step 3. Schedule template setting

You can set the schedule template with the shift on a daily basis. You can also set the weekly and daily schedule template.

➤ Related information

Schedule template

Step 4. Overtime rule setting

This can be used conveniently when the overtime time code has not been added to the shift. Overtime set in the service rule has a start time and an end time, but **Overtime rule** calculates the total time exceeding the range of regular service time. **Overtime rule** can be used conveniently for managing total daily, weekly and monthly overtime hours, and when **Overtime rule** is set, it applies instead of the overtime time code added to the shift.

➤ Related information

14 Time & Attendance

Overtime Rule

Step 5. Schedule setting

You can set the period, user, overtime rule, and vacation schedule to apply to the schedule template set in the previous step.

⌕ Related information

Schedule

Shift

You can set the time code, time segment for time code, schedule template, and overtime rule. These are the main components of T&A management.

Time Code

Shift

Schedule Template

Overtime Rule

Time Code

You can set the time code to be used for worktime calculation. It can be set for T&A records, time code for overtime, and time code for vacation management.

You can assign and use a different time rate for each time code.

- 1) Click **TIME ATTENDANCE > Shift > Time Code**.
- 2) Click **ADD TIME CODE** and set each item.

1

Name

2

Description

3

Type

☒ Attendance management

☐ Overtime management

☐ Leave management

4


Time Rate

1

5

Color

14 Time & Attendance

No.	Item	Description
1	Name	Enter the desired time code name.
2	Description	Enter a brief description of the time code.
3	Type	<p>Set the time code type.</p> <ul style="list-style-type: none">▪ Attendance management: You can set the time code to be used for the T&A record.▪ Overtime management: You can set the time code to be used for overtime.▪ Leave management: You can set the time code to be used for go out, outside work, business trip and vacation. <p> Note</p> <ul style="list-style-type: none">▪ If the time code currently used by shift, Type cannot be changed.▪ If Type is set to Leave management, Time Rate cannot be set.
4	Time Rate	Set the time rate according to the time code. 1 is the default time rate. If 2 is set, it is calculated with twice the hourly pay when the set time code is applied.
5	Color	Set a color to distinguish the time code.

- 3) To save settings, click **Apply**. To add a shift, click **Apply & Next**. To save the settings and add another time code, click **Apply & Add New**.

Related information

Shift

Shift

You can create a shift by applying a different time code for each hour based on a 24 hour cycle. You can select either a fixed working shift , flexible working shift or floating working shift and you can set the start time of day and rounding rule.

- 1) Click **TIME ATTENDANCE > Shift > Shift**.
- 2) Click **ADD SHIFT** and set each item.

14 Time & Attendance

1

Name

2

Description

3

Type

☒ Fixed
 ☐ Flexible
 ☐ Floating

4

Day start time

05

00

☐ Allowed a day before/after time

5

First check-in & Last check-out

☐ No

6

Time segment

Current day

Next day

0

3

6

9

12

15

18

21

24

Time code	Start time	End time	Min. Duration	Action
Attendance man...	<div>09</div> <div>00</div>	<div>18</div> <div>00</div>	<div>04</div> <div>00</div>	

Grace

☐ Use

Add

7

Rounding

☐ Punch in
 ☐ Punch out

8

Meal deduction 1

By Punch

Meal deduction 2

☐ Use



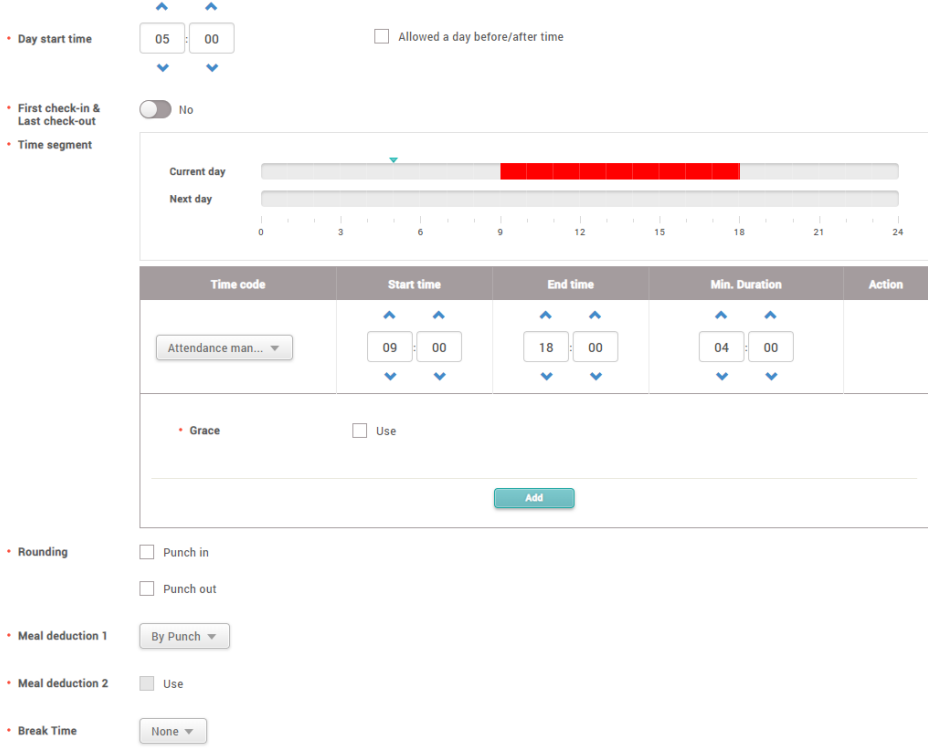

9

Break Time

None

No.	Item	Description
1	Name	Enter the desired shift name.
2	Description	Enter a brief description of the shift.
3	Type	Set the shift type. The detailed setting varies according to the shift type. <ul style="list-style-type: none"> ▪ Fixed: You can set the fixed service to attend and leave at a fixed time. ▪ Flexible: You can set the flexible service with no fixed attendance and leave times. ▪ Floating: You can set the floating service with no fixed attendance and leave times. In this shift type, the shift is automatically applied according to the attendance time.
4	Day Start Time	Set the start time of day. If you use Allowed a day before/after time , you can set Shift for work hours exceeding 24 hours based on the Day start time set.

14 Time & Attendance

No.	Item	Description
		<p> Note</p> <ul style="list-style-type: none"> ▪ Allowed a day before/after time is activated only when you set the type of Shift to Fixed.
5	First check-in & Last check-out	<p>When Yes is set, the first user authentication time is recorded as check-in time, and the last user authentication time is recorded as check-out time.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ If the First check-in & Last check-out is set to Yes, Break by Punch should be set for recording the user's break time.
6	Time segment	<p>When Fixed is selected for Type,</p>  <p>Select the salary code set as T&A record and then set Start time, End time and Min. Duration.</p> <p>You can also set Grace, Rounding, Meal deduction and Break Time. When setting is finished, click Add.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ The Allowed a day The before/after time can be set up to 6 hours. ▪ You can only add one time code set as Attendance management to the shift. ▪ For the time code set as Overtime management, you can only set Start

14 Time & Attendance

No.	Item	Description
		<p>time, End time, Min. Duration, Rounding .</p> <p>When Flexible is selected for Type,</p> <div> <div> <div>Working hours per day</div> <div> <div>08</div> <div>00</div> </div> </div> <div>Options</div> <div> <div>Time code</div> <div>Attendance man...</div> <div> <div>Punch in Time Limit</div> <div>Use</div> <div>Punch out Time Limit</div> <div>Use</div> </div> <div> <div>Meal deduction 1</div> <div>By Punch</div> </div> <div> <div>Meal deduction 2</div> <div>Use</div> </div> <div> <div>Rounding</div> <div>Punch in</div> <div>Punch out</div> </div> <div> <div>Break Time</div> <div>None</div> </div> </div> </div> <p>Set the working hours per day, and then select the time code. You can also set Punch in Time limit, Punch out Time Limit, Meal deduction, Rounding, Break Time.</p> <p>Note</p> <ul style="list-style-type: none"> If Flexible is selected for Type, the time code for overtime cannot be added. <p>When Floating is selected for Type,</p>



14 Time & Attendance

No.	Item	Description										
		<div><div><div><div><div>Segment</div><div><input checked="" type="checkbox"/> Apply leave by this segment</div></div></div><div><div>Time segment</div><div><div><div>Current day</div><div>Next day</div></div><div><div><div>0</div><div>3</div><div>6</div><div>9</div><div>12</div><div>15</div><div>18</div><div>21</div><div>24</div></div></div></div><table><tr><th>Time code</th><th>Start time</th><th>End time</th><th>Min. Duration</th><th>Action</th></tr><tr><td>Attendance man...</td><td>09 : 00</td><td>18 : 00</td><td>04 : 00</td><td></td></tr></table><div><div>Punch in granted time range</div><div><div>05 : 00</div><div>~</div></div><div><div>09 : 00</div></div></div><div><div>Grace</div><div><input type="checkbox"/> Use</div></div><div>Add</div></div><div><div>Rounding</div><div><input type="checkbox"/> Punch in</div><div><input type="checkbox"/> Punch out</div></div><div><div>Meal deduction 1</div><div>By Punch</div></div><div><div>Meal deduction 2</div><div><input type="checkbox"/> Use</div></div><div><div>Break Time</div><div>None</div></div></div></div>	Time code	Start time	End time	Min. Duration	Action	Attendance man...	09 : 00	18 : 00	04 : 00	
Time code	Start time	End time	Min. Duration	Action								
Attendance man...	09 : 00	18 : 00	04 : 00									
		<p>Select the time code and set Start time, End time, Min. Duration, and Punch in granted time range.</p> <p>You can also set Grace, Rounding, Meal deduction, and Break time.</p> <div><div><div><div></div><div>Note</div></div><div><div><div></div><div>You can configure the shift by up to 5 time slots.</div></div><div><div><div></div><div>If you use the floating shift, you must select Apply leave by this segment when setting up a leave management. You can select Apply leave by this segment from the time segment configured as shifts.</div></div><div><div><div></div><div>For the time code set as Overtime management, you can only set Start time, End time, Min. Duration, Rounding.</div></div></div></div></div></div></div>										
7	Rounding	<p>You can set the time rounding rule. Unit is the time to round off to and Point is the time to apply rounding off. For example, 10 minutes are set for Unit and 7 minutes are set for Point, an event occurring at 8:05 is considered to have occurred at 8 and an event occurring at 8:08 is considered to have occurred at 8:10. Select the item which you intend to use, and then set Unit and Point.</p> <div><div><div><div></div><div>Punch in: You can set the rounding rule to process the registered time when an</div></div></div></div>										

☒ Note

- You can configure the shift by up to 5 time slots.
- If you use the floating shift, you must select **Apply leave by this segment** when setting up a leave management. You can select **Apply leave by this segment** from the time segment configured as shifts.
- For the time code set as **Overtime management**, you can only set **Start time**, **End time**, **Min. Duration**, **Rounding**.

14 Time & Attendance

No.	Item	Description
		<p>attendance event is registered earlier/later than the set start time.</p> <ul style="list-style-type: none">▪ Punch out: You can set the rounding rule to process the registered time when a leave event is registered earlier/later than the set end time. <p> Note</p> <ul style="list-style-type: none">▪ Rounding applies in preference to Grace.
8	Meal deduction 1, 2	<p>You can set to deduct meal time from the shift.</p> <ul style="list-style-type: none">▪ By Punch: You can set it to be deducted according to the record registered in the device, without a fixed meal deduction time.▪ Auto: You can set the meal deduction by setting Deduction time and Minimal hours before deduction.▪ Fixed: You can set the fixed meal deduction by setting Start time and End time. <p> Note</p> <ul style="list-style-type: none">▪ You can deduct two meal times from the shift if you use Meal deduction 2.▪ When using the meal deduction type as Auto or Fixed, Meal deduction 1 and Meal deduction 2 can be set only for the same type.
9	Break Time	<p>You can set the break time.</p> <ul style="list-style-type: none">▪ By Punch: You can set it to be confirmed according to the record registered in the device, without a fixed break time. If you select By Punch, you can set Max. allowed break time.▪ Fixed: You can set the fixed break time by setting Start time and End time.

- 3) To save settings, click **Apply**. To add a schedule template, click **Apply & Next**. To save the settings and add another shift, click **Apply & Add New**.

Related information

[Schedule Template](#)

Schedule Template

You can create a weekly and daily schedule by using the set shift.

14 Time & Attendance

- 1) Click **TIME ATTENDANCE > Shift > Schedule Template.**
- 2) Click **ADD SCHEDULE TEMPLATE** and set each item.

1

Name

2

Description

3

Type

Weekly

Daily

4

Weekend days

MON

TUE

WED

THU

FRI

SAT

SUN

* Please select one or consecutive two days.

Shift	Type	Time	Day start time
Daily	Fixed	09:00~18:00	05:00
Flexible	Flexible	8hr 0min	05:00

6

MON

TUE

WED

THU

FRI

SAT

SUN

No.	Item	Description
1	Name	Enter the desired schedule template name.
2	Description	Enter a brief description of the schedule template.
3	Type	You can set either Weekly or Daily for the schedule template, and when Daily is selected, you can set the period to be used repeatedly.
4	Weekend days	You can set the days of the week that you want to use as the weekend.
5	Shift	You can view the list of set service rules.
6	Schedule	<div>Set drag & drop for the set service rule. To apply all at once, click Copy All.</div> <div><div>📌</div><div>Note<ul style="list-style-type: none">To apply a shift that setting the Allowed a day before/after time, Allowed a day before/after time cannot be set 24 hours before Day start time on Shift the day before.</div></div>

- 3) To save settings, click **Apply**. To add a schedule, click **Apply & Next**. To save the settings and add another schedule template, click **Apply & Add New**.

14 Time & Attendance

 **Related information**

Overtime Rule

Rule

This can be used conveniently when the overtime time code has not been added to the shift. Overtime set in the shift has a start time and an end time, but **Rule** calculates the total time exceeding the range of regular working time. **Rule** can be used conveniently for managing total daily, weekly and monthly overtime hours, and when **Rule** is set, it applies instead of the overtime time code added to the shift.

- 1) Click **TIME ATTENDANCE > Shift > Rule**.
- 2) Click **ADD RULE** and set each item.

1

Name

2

Description

3

Overtime

☒ Not Use

☐ Daily overtime

☐ Weekly overtime

☐ Monthly overtime

☐ Weekend overtime

Time Code

None

Day start time

0500

☐ First check-in & Last check-out

☐ Holiday overtime

Time Code

None


Day start time

0500

☐ First check-in & Last check-out

No.	Item	Description
1	Name	Enter the desired overtime rule name.
2	Description	Enter a brief description of the overtime rule.
3	Overtime	Set the overtime rule. Daily overtime, Weekly overtime, Monthly overtime rules can set the overtime time code to be applied after the regular working time, and a different overtime time code can be applied after a certain time. You can

14 Time & Attendance

No.	Item	Description
		<p>also limit the overtime hours for an employee by setting the maximum overtime hours.</p> <p>When you set as follows, the 'Overtime management' time code applies from 5 PM to 11 PM if the normal working time is from 8 AM to 5 PM, and the 'Overtime management' time code applies from 11 PM to 2 AM. Also, the maximum overtime hours for an employee for one day is limited to 9 hours, and the daily payroll is calculated only using the record of providing work until 2 AM.</p> <div> <input type="radio"/> Not Use <input checked="" type="radio"/> Daily overtime </div> <div> Apply Overtime manag... after 8 hour(s) 0 minute(s) Apply Overtime manag... after 6 hour(s) 0 minute(s) of [Overtime management] Max overtime 9 hour(s) </div> <div> <input type="radio"/> Weekly overtime <input type="radio"/> Monthly overtime </div> <div>  Note <ul style="list-style-type: none"> Total working time does not include break time or meal time. </div> <p>For Weekend overtime and Holiday overtime rules, Time code and Day start time can be set, and only First check-in & Last check-out can be set.</p> <div> <input checked="" type="checkbox"/> Weekend overtime </div> <div> Time Code None Day start time 05 : 00 <input type="checkbox"/> First check-in & Last check-out </div> <div> <input checked="" type="checkbox"/> Holiday overtime </div> <div> Time Code None Day start time 05 : 00 <input type="checkbox"/> First check-in & Last check-out </div>

- 3) To save settings, click **Apply**. To add a schedule, click **Apply & Next**. To save the settings and add another rule, click **Apply & Add New**.

14 Time & Attendance

 **Related information**

Schedule

Schedule

You can create a service schedule by assigning the set schedule template, overtime rule, period, and holiday to a user.

You can also add a temporary schedule or personal vacation to the created service schedule.

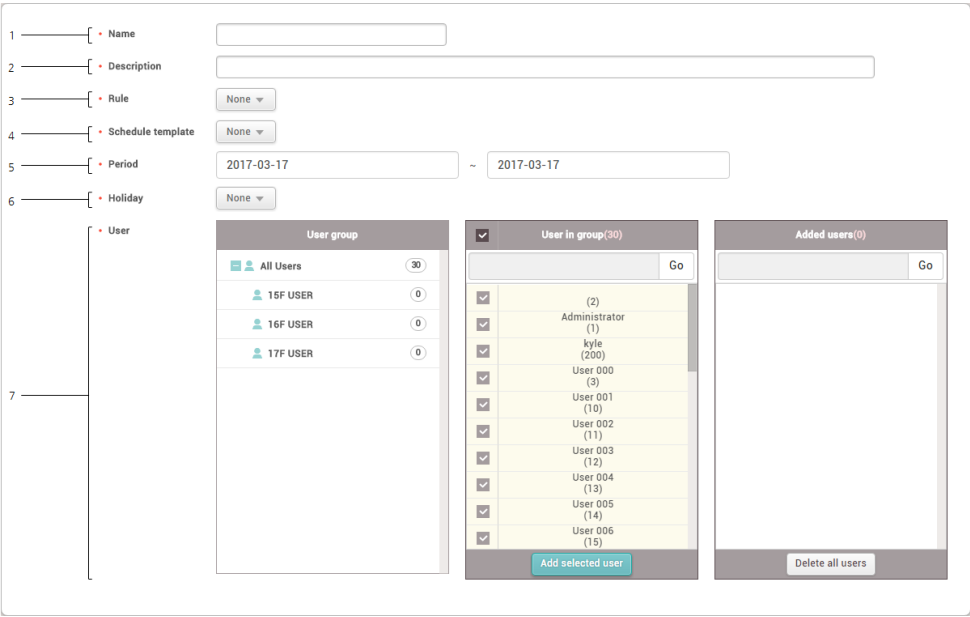
 **Note**

- Before creating a schedule, check if the **Time Code**, **Shift**, **Schedule Template**, and **Holiday** which you will use have been created correctly.

— Adding & deleting a schedule

You can create a service schedule for a registered user.





- Click **TIME ATTENDANCE > Schedule**.
- Click **Add** and set each item.



The screenshot shows a web form for creating a schedule. It has seven numbered sections on the left: 1. Name (text input), 2. Description (text input), 3. Rule (dropdown menu, currently 'None'), 4. Schedule template (dropdown menu, currently 'None'), 5. Period (date range input, currently '2017-03-17' to '2017-03-17'), 6. Holiday (dropdown menu, currently 'None'), and 7. User (a complex section with three panels). The 'User' section includes a 'User group' panel with 'All Users' (30), '15F USER' (0), '16F USER' (0), and '17F USER' (0). A 'User in group(30)' panel shows a list of users with checkboxes, including 'Administrator (1)', 'kyle (200)', and several 'User 000' through 'User 006' entries. An 'Added users(0)' panel is empty. Buttons for 'Go', 'Add selected user', and 'Delete all users' are present.

No.	Item	Description
1	Name	Enter the desired schedule name.

14 Time & Attendance

No.	Item	Description
2	Description	Enter a brief description of the schedule.
3	Rule	<p>Select the set overtime rule.</p> <p>When the overtime rule is set, the overtime service salary code set to the service rule will not apply. If you do not wish use it, set None.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ If there is no desired overtime rule, set one by referring to the Overtime Rule.
4	Schedule Template	<p>Select the set schedule template.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ If there is no desired schedule template, set one by referring to the Schedule Template. ▪ Once schedule template is set, it cannot be changed.
5	Period	<p>Set the period to collect T&A events.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ Once the start date is set, it cannot be changed. The end date can be changed, and when it is changed to a date which is earlier than the set date, leave events for the changed period will be deleted.
6	Holiday	<p>Select the set vacation schedule. If you do not wish use it, set None.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ If there is no desired vacation schedule, add a vacation schedule by referring to the Schedule.
7	User	Add a user to apply the rule.

- 3) To save settings, click **Apply**.
- 4) To delete a schedule, select the schedule you wish to delete from the list, and then click **Delete schedule**.

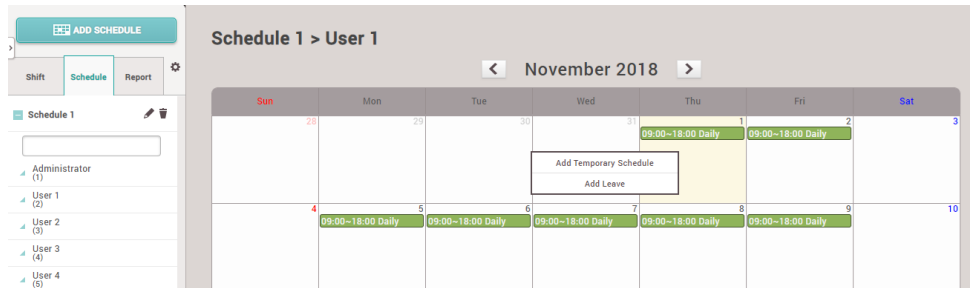
— Adding & deleting a temporary schedule


If you have already registered schedule. you can set a different service rule to a user

14 Time & Attendance

temporarily.

- 1) Select a user assigned to the schedule from the list and click a date on the calendar.



- 2) Select **Add Temporary Schedule** and set each item. To apply it to other users equally, add a user by clicking .

[kyle] Temporary Schedule

Name

Shift

regular shift


Period

2016-12-01

~

2016-12-01

Apply to Other User(s)



Apply

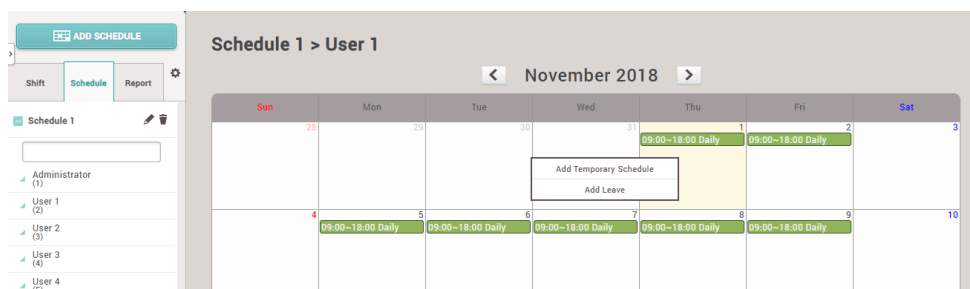
Cancel

- 3) When you click **Apply**, the shift for the set period will be changed.
- 4) To delete a temporary schedule, click the service schedule of the set temporary schedule, and then click **Yes**.


— Adding & deleting a leave

You can add a user's personal leave schedule.

- 1) Select a user assigned to the schedule from the list and click a date on the calendar.




14 Time & Attendance

- 2) Select **Add Leave** and set each item. To apply it to other users equally, add a user by clicking .

Edit Leave

User 1(2)

Date	2018-11-01(Thu)		
Leave	Leave management		
Use Time	<input type="checkbox"/>		
Start Date	<input type="text" value="2018-11-01"/>	End Date	<input type="text" value="2018-11-01"/>
Leave Hours	1day(s)		
Apply to Other User(s)			
Approver Comments	<div></div>		

Ok

Cancel

- 3) When you click **OK**, the leave will be registered on the set period.
- 4) To delete a leave, click the registered leave and click **Yes**.

Note

- If there is no desired leave management Time code, add one by referring to the **Time Code**.

Report

You can create a T&A report with T&A events of a user collected through the system, and edit or export time records as a CSV file or a PDF file.

7 preset report filters can be used conveniently, or the administrator can set the filter manually.

Before Using the Multilingual Report

BioStar 2 supports Korean and English language. To use multilingual report, please check the following.

Font Setting

1. Go to [C:\Program Files\BioStar 2(x64)\ta\dist\setup\report_fonts].
2. Create a folder with the language name you want to use. Refer to the ISO 639-1 standard for language name. For example, to use Spanish, create a folder named "es".
3. Copy and paste the font file into the folder you created. Only one TrueType Font is supported.

14 Time & Attendance

PDF View Setting

1. Click the link to install the PDF viewer on Google Chrome.

<https://chrome.google.com/webstore/detail/pdf-viewer/oemmndcbldboiebfnladdacbfmadadm>

— Before Updating the Report

BioStar 2 uses MariaDB as the default database. If you are using MS SQL database, please check the following.

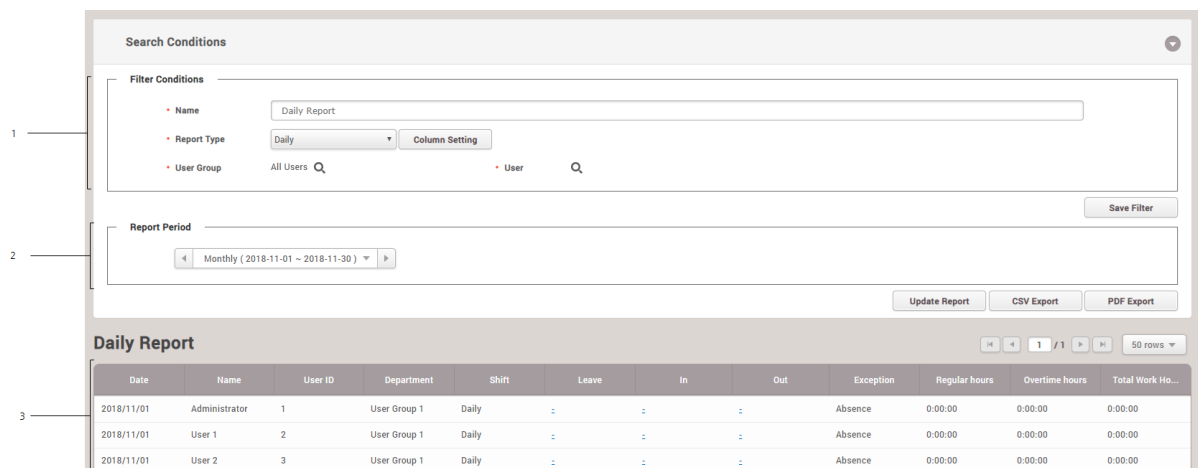
When using BioStar 2 with MS SQL database, your PC's memory usage will accumulate each time you update the report if there are a large number of registered users. Reset Max Server Memory for the MS SQL database.

1. Run **Microsoft SQL Server Management Studio**.
2. Right-click BioStar 2 database in **Object Explorer** and click **Property**.
3. Click **Memory** and then decrease the value of **Max Server Memory**.

Note

- For more information on MariaDB and MS SQL Server settings, see [Installing BioStar 2](#).

- 1) Click **TIME ATTENDANCE > Report**.
- 2) To use a preset filter list, select a desired filter type, set either **User Group** or **User** and click **Update Report**.
- 3) To register a new filter, click **ADD FILTER** and set each item.



Search Conditions

Filter Conditions

- Name: Daily Report
- Report Type: Daily
- User Group: All Users

Report Period: Monthly (2018-11-01 ~ 2018-11-30)


Update Report CSV Export PDF Export

Daily Report

Date	Name	User ID	Department	Shift	Leave	In	Out	Exception	Regular hours	Overtime hours	Total Work Ho...
2018/11/01	Administrator	1	User Group 1	Daily	-	-	-	Absence	0:00:00	0:00:00	0:00:00
2018/11/01	User 1	2	User Group 1	Daily	-	-	-	Absence	0:00:00	0:00:00	0:00:00
2018/11/01	User 2	3	User Group 1	Daily	-	-	-	Absence	0:00:00	0:00:00	0:00:00

No.	Item	Description
1	Filter Conditions	Set a new T&A report.

14 Time & Attendance

No.	Item	Description
		<ul style="list-style-type: none"> ▪ Name: Enter the desired report name. ▪ Report Type: Select the desired report type. Daily, Daily Summary, Individual, Individual Summary, Leave, Exception, Modified Punch Log History, Working alarm time reports are available. ▪ Column Setting: Change or hide the order of columns in the report table. ▪ Filter: This function is enabled only when Leave or Exception is set for Report Type, and detailed conditions for leave or exception records can be selected. ▪ User Group / User: Select a user group or a user to create a report. ▪ Save Filter: Save the set T&A report as the filter.
2	Report Period	<p>Set the period of report.</p> <ul style="list-style-type: none"> ▪ Period: Set the period for creating a report to Daily, Weekly, Monthly, or Custom. ▪ In/Out Only: Select to output only the check-in and check-out logs of the user to the report. ▪ All Punches: Select to output all punches of the user to the report. <p> Note</p> <ul style="list-style-type: none"> ▪ In/Out Only and All Punches are enabled only in Individual Report. ▪ Update Report: Update the report table to the most recent information. ▪ CSV Export: Save the created report as a CSV file. ▪ PDF Export: Save the created report as a PDF file.
3	Report	View the created report.

Adding the Working alarm time report

You can update the report for users who have reached their specified working hours, or notify the administrator by email.

You can update the Working alarm time report weekly.

- 1) Click **TIME ATTENDANCE > Report > Working alarm time Report**.
- 2) Set each item in **Filter Conditions** and **Report Period** and then click **Update Report**.
- 3) Set Automated Email if you want to send an email notification to the administrator for users who have reached their specified working hours.



14 Time & Attendance

The screenshot shows the 'Search Conditions' dialog box with the following details:

- Filter Conditions:**
 - Name: Working alarm time Report
 - Report Type: Working alarm time
 - Working alarm time: 40
 - User Group: User
 - Buttons: Save Filter
- Report Period:**
 - Period: Weekly (2018-10-29 ~ 2018-11-04)
 - Buttons: Update Report, CSV Export, PDF Export
- Automated Email:**
 - Email: ☒
 - Day of Week: THU
 - Time: 5:00
 - Recipient: 1
 - Buttons: Edit

No.	Item	Description
1	Filter Conditions	<p>Set a new T&A report.</p> <ul style="list-style-type: none"> ▪ Name: Enter the desired report name. ▪ Report Type: Select the desired report type. ▪ Column Setting: Change or hide the order of columns in the report table. ▪ Working alarm time: Set the time to generate Working alarm time report. ▪ User Group / User: Select a user group or a user to create a report. ▪ Save Filter: Save the set T&A report as the filter.
2	Report Period	<p>Set the period of report.</p> <ul style="list-style-type: none"> ▪ Period: Set the period for creating a report. ▪ Update Report: Update the report table to the most recent information. ▪ CSV Export: Save the created report as a CSV file. ▪ PDF Export: Save the created report as a PDF file.
3	Automated Email	<p>You can notify about users who have reached their specified working hours for the administrator by email.</p> <ul style="list-style-type: none"> ▪ Email: Click to send an email to an administrator automatically. ▪ Day of Week: You can set the days of the week to send an email to administrators. ▪ Time: You can set the time to send an email to administrators. ▪ Recipient: You can add an administrator's email address that receives the email.

14 Time & Attendance

No.	Item	Description
		 Note <ul style="list-style-type: none"> You need to configure Filter Conditions and then save the filter in order to set up Automated Email. You can set the sender information for automatically sent emails in .

Editing T&A Records

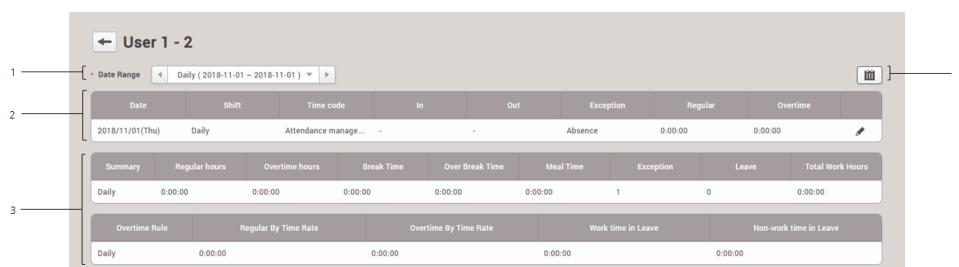
You can modify T&A records by clicking the created report table.

Note

- In order to modify T&A records, a report must be created first. For details about the creation of a report, refer to [Report](#).
- The attendance and leave record of a user whose T&A schedule has not been registered cannot be modified.





- Click a row to modify the record from the created report table.
- Modify a T&A record or add a leave according to the desired method.

— Modifying in the List



No.	Item	Description
1	Period	You can set the period for the T&A record to be displayed as a list.
2	Daily T&A record	You can view the daily T&A record.

14 Time & Attendance

No.	Item	Description
		 Note <ul style="list-style-type: none"> You can add, modify or delete a T&A record by clicking In/Out time. Click  after clicking In/Out time to modify the registered T&A record. When you click OK, changes will be saved. You can add a leave by clicking . To add a leave, the Time Code set as Leave management is necessary. You can click  of the added leave to delete it.
3	T&A record summary	You can view T&A records according to the set period.
4	View in calendar button	You can view T&A records in a calendar.

— Modifying in the calendar

User 1 - 2

All

Work time

Shift

Regular

Overtime

Exception

Leave

Holiday

<

November 2018

>

Sun

Mon

Tue

Wed

Thu

Fri

Sat

0:00:00

0:00:00 (Daily)

0:00:00

0:00:00

0:00:00

0:00:00

0:00:00

0:00:00

0:00:00 (Daily)

0:00:00

0:00:00

0:00:00

0:00:00

0:00:00

0:00:00

0:00:00 (Daily)

0:00:00

0:00:00

0:00:00

0:00:00

0:00:00

0:00:00

0:00:00 (Daily)

0:00:00

0:00:00

0:00:00

0:00:00

0:00:00

0:00:00

0:00:00 (Daily)

0:00:00

0:00:00

0:00:00

0:00:00

0:00:00

0:00:00

0:00:00 (Daily)

0:00:00

0:00:00

0:00:00

0:00:00

0:00:00

Summary

Regular hours

Overtime hours

Break Time

Over Break Time

Meal Time

Exception

Leave

Total Work Hours

Monthly

0:00:00

0:00:00

0:00:00

0:00:00

0:00:00

1

0

0:00:00

Overtime Rule

Regular By Time Rate

Overtime By Time Rate

Work time in Leave

Non-work time in Leave

-




0:00:00

0:00:00

0:00:00


0:00:00

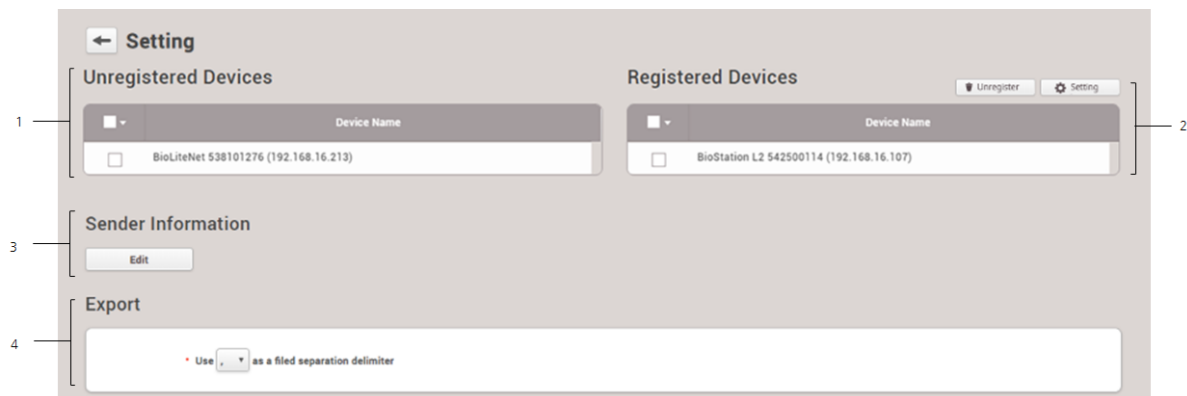
14 Time & Attendance

No.	Item	Description
1	Event Type	You can click each event type to display or hide on the calendar.
2	Month	You can move to the previous or next month by clicking < or >.
3	Daily T&A record	<p>You can view the daily T&A record.</p> <p> Note</p> <ul style="list-style-type: none"> You can add, modify or delete a T&A record by clicking the work time (white). You can modify the registered T&A record by clicking , and when you click OK, changes will be saved. You can add a leave by clicking the shift (gray). To add a leave, the Time Code set as Leave management is necessary. You can click  of the added leave to delete it.
4	T&A record summary	You can view monthly the T&A record.
5	View in list button	You can view T&A records in a list.

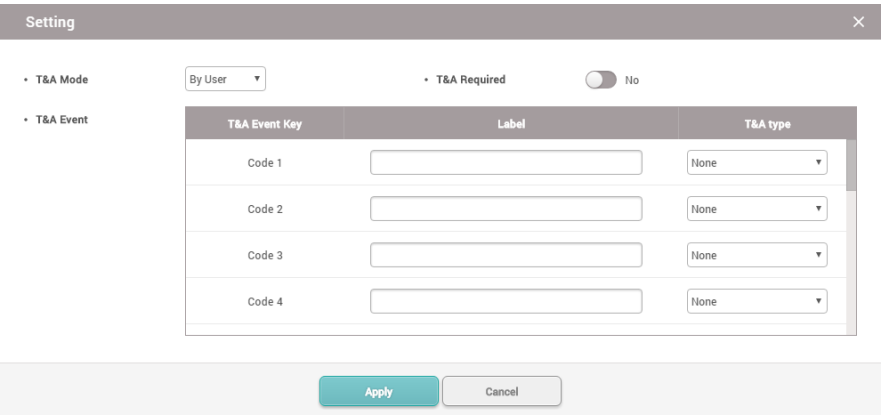
Setting

You can register a device used for T&A management or set the user list synchronization option.

- 1) Click **TIME ATTENDANCE** > .
- 2) Set each item.



14 Time & Attendance

No.	Item	Description
1	Unregistered Devices	This is the list of devices for which T&A management is available. Select the desired device and click + Register to register the selected device as a T&A management device.
2	Registered Devices	<p>This is the list of T&A management devices being used currently. To cancel registration, select the desired device and click Unregister.</p> <p>You can also change the T&A setting of a registered device by clicking Setting. For details, refer to the device's T&A.</p> <p>T&A type is a setting to map the T&A Event Key and T&A event type(Check In, Check Out, Break Start, Break End, Meal Time Start, Meal Time End).</p> 
3	Sender Information	You can set the sender information to use when sending out notification emails.
4	Export	You can select the delimiter of the document when exporting T&A report to CSV export.

Note

- When a registered device is deleted in **DEVICE** menu, the registered T&A management device will be also deleted automatically.

You can manage the access of visitors by using the **VISITOR** menu.

You can also set up a PC where visitors can apply for a visit.

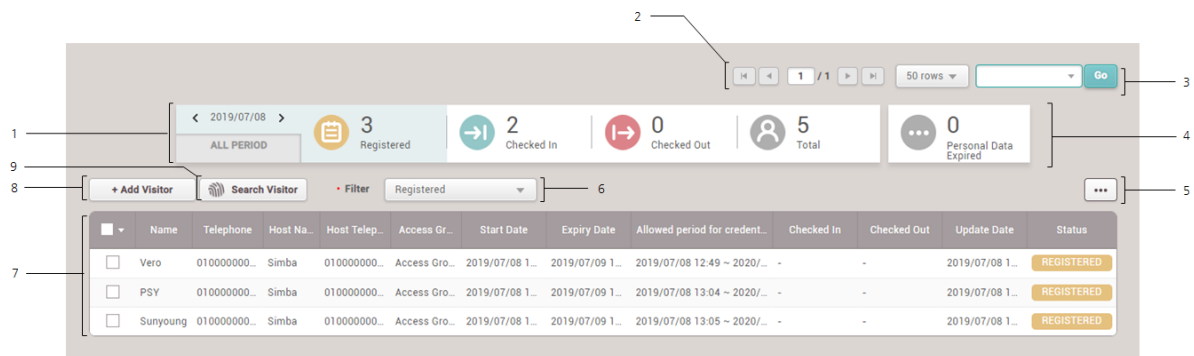
Applying to Visit

Managing Visitors

Note

15 Visitor

- The **VISITOR** menu will appear when the Visitor license is activated.



- | | |
|---|--------------------------------|
| 1 Period and Number of Visitors by Status | 6 Filter of Visitors by Status |
| 2 Page Navigation Buttons and Number of List Rows | 7 List of Visitors by Status |
| 3 Search for Visitors in List of Selected | 8 Add Visitor Button |
| 4 List of Visitors Expired the Personal Data | 9 Search Visitor Button |
| 5 Function Button (Column Setting) | |

Applying to Visit

Visitors can view and accept the terms and conditions or the privacy policy for access.

Visitors with a visit record can also apply for a visit by reusing previously registered information, such as their name, telephone number, and fingerprint.

Applying to First Visit

Applying to Visit Using Existing Info

Note

- You can access the visit application page on the visiting PC. If there is not the shortcut of the visit application page on the visiting PC, create the shortcut by referring to [Visit PC Settings](#).

Applying to First Visit

If you are visiting for the first time, apply for a visit on the visit application page.

15 Visitor

 **Note**

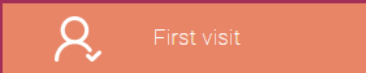
- You can access the visit application page on the visiting PC. If there is not the shortcut of the visit application page on the visiting PC, create the shortcut by referring to [Visit PC Settings](#).

If you visit the site for the first time, apply to visit on the visit application page.


1) Run the visit application page on the visiting PC.

Welcome


For the first visit, please click the button below to register your visit.



If you have already visited, please fill in the information below.

 Search

Or



Search

2) Click **First visit**.

3) Check and accept the terms and conditions or the privacy policy for access and then click **Next**.

4) Enter or select the necessary fields.

Registration Information

1

Visitor

Name

Telephone

2

Host

Name


Telephone

3

Entry Information



Zone

Period

No.	Item	Description
1	Visitor	<div>Enter the visitor's information.</div> <div><ul style="list-style-type: none">▪ Name: Enter the name.▪ Telephone: Enter the telephone number.</div> <div><div> Note</div><div><ul style="list-style-type: none">▪ If the Custom Visitor Field is set in the VISITOR setting, that fields are activated.▪ Up to 48 characters may be entered for a name.</div></div>

199

15 Visitor

No.	Item	Description
2	Host	<p>Enter the host's information.</p> <ul style="list-style-type: none"> ▪ Name: Enter the name. ▪ Telephone: Enter the telephone number. <p> Note</p> <ul style="list-style-type: none"> ▪ Up to 48 characters may be entered for a name.
3	Entry Information	<p>Set the zone and period to visit.</p> <ul style="list-style-type: none"> ▪ Zone: Set the access group. ▪ Period: Set the period for visit. <p> Note</p> <ul style="list-style-type: none"> ▪ Only access groups of sites assigned to visiting PC in VISITOR setting are displayed.

5) Click **Next**.

6) Set the credentials.



1 — [• Fingerprint + Fingerprint 

2 — [• Card ☐ No request

No.	Item	Description
1	Fingerprint	Click + Fingerprint to use the fingerprint authentication. And enroll the fingerprint.
2	Card	Set the card to Request to use the card authentication. And get a card from the visitor operator.

7) Click **Next**.

8) To apply for a visit, click **Register**.

Related Information

Visitor

Applying to Visit Using Existing Info

15 Visitor

Applying to Visit Using Existing Info

Visitors with a visit record can also apply for a visit by reusing previously registered information, such as their name, telephone number, and fingerprint.

— Search by name and telephone number

If you have visited the site, you can use your existing visit information again to request a visit.

- 1) Run the visit application page on the visiting PC.

The screenshot shows a visit application interface. On the left, a purple box with the word 'Welcome' in white. Below it, text says 'For the first visit, please click the button below to register your visit.' At the bottom of this box is an orange button with a person icon and the text 'First visit'. To the right, a white box contains the text 'If you have already visited, please fill in the information below.' Below this text are two input fields: 'Name' and 'Phone Number'. To the right of these fields is a vertical line with the word 'Or' in the middle. To the right of the 'Or' line is a pink box with a fingerprint icon and a 'Search' button at the bottom. Below the 'Name' and 'Phone Number' fields is a teal button with a magnifying glass icon and the text 'Search'.

- 2) Enter the name and telephone number and then click **Search**.
- 3) Check and accept the terms and conditions or the privacy policy for access and then click **Next**.
- 4) Check the Registration Information. If there are items that need to be modified, modify each item by referring to [Applying to first visit](#) and click **Next**.
- 5) Check the Credential. If there are items that need to be modified, modify each item by referring to [Applying to first visit](#) and click **Next**.
- 6) To apply for a visit, click **Register**.

Search by fingerprint

If you have a fingerprint registered in the site of visit, you can search the fingerprint and apply for a visit using the existing visit information.

- 1) Run the visit application page on the visiting PC.

15 Visitor

The image shows two parts of a visitor management system interface. On the left is a 'Welcome' screen with a maroon background. It says 'Welcome' in large white letters, followed by 'For the first visit, please click the button below to register your visit.' and an orange button with a person icon and the text 'First visit'. On the right is a search interface. It has the heading 'If you have already visited, please fill in the information below.' Below this are two input fields: 'Name' and 'Phone Number'. To the right of these fields is a vertical line with the word 'Or' in the middle. To the right of the line is a pink box containing a fingerprint icon and a 'Search' button at the bottom. Below the 'Name' and 'Phone Number' fields is a teal button with a magnifying glass icon and the text 'Search'.

- 2) Click **Search** at the bottom of the fingerprint icon.
- 3) Scan your fingerprint to search the registered visitor.
- 4) If the visitor information is correct, click **Yes**.

The image shows a 'Confirm' dialog box with a grey header and a close button (X) in the top right corner. Inside the dialog, there is a green checkmark icon on the left. To its right, the text reads: 'Name : Vero', 'Phone: 01000000001', and 'Is it correct? Please check the information.' At the bottom of the dialog, there are two buttons: 'Yes' and 'No'.

- 5) Check and accept the terms and conditions or the privacy policy for access and then click **Next**.
- 6) Check the Registration Information. If there are items that need to be modified, modify each item by referring to [Applying to first visit](#) and click **Next**.
- 7) Check the Credential. If there are items that need to be modified, modify each item by referring to [Applying to first visit](#) and click **Next**.
- 8) To apply for a visit, click **Register**.

Related Information

[Visitor](#)

[Applying to First Visit](#)

Managing Visitors

You can check the list of visitors and manage the check in and check out of them. You can also add, delete, or modify visitor information.

15 Visitor

- Managing Registered Visitors
- Managing Check In Visitors
- Managing Checked Out Visitors
- Managing All Visitors
- Deleting Personal Data Expired

 **Note**

- The **VISITOR** menu will appear when the Visitor license is activated.

Managing Registered Visitors

You can approve a visit or edit the registration information. You can also add or delete visitors.

— Approve the Visit

You can approve a visit.

- 1) Click **VISITOR**.
- 2) Click a visitor in the **Registered**.
- 3) Check the information of the visitor and then click **Check in**.

Visitor

Name

Shannon

Telephone

01000000003

Host

Name

Simba

Telephone

01000000000

Name	Telephone	Choose
Simba	01000000000	<div>Choose</div>

Entry Information

Access Group

Access Group

Period

2019/06/04 10:00 ~ 2019/06/05 10:00

Credential

Card

No request

Credential

+ Fingerprint

Edit

Check in

Cancel

 **Note**

- If there are items that need to be modified, modify each item and click **Edit**.

- 4) Check the **Registration Information** and then click **Approve** to approve the

visit.

The form is titled "Registration Information" and contains several sections:

- Privacy Policy:** Includes a "View terms" button and a status "Did not agree".
- Visitor Information:** Fields for Name (Shannon) and Telephone (01000000003).
- Entry Information:** Fields for Access Group (Access Group) and Period (2019/06/04 10:00 ~ 2019/06/05 10:00).
- Host:** Fields for Name (Simba) and Telephone (01000000000).
- Credential:** Fields for Fingerprint and Card (No request).

At the bottom, there are four buttons: "Cancel", "Prev", "Approve", and "Approve and register card".

Note

- The **Approve** button is deactivated for visitors who did not agree to the terms and conditions when applying for a visit. Click **View terms** to provide the visitor with the terms and conditions and request the agreement. If a visitor does not accept the terms and conditions, the visitor will be restricted from visiting.
- If a card device is set on the visiting PC, the **Approve and register card** button is activated. Click **Approve and register card** to approve the visit and issue an access card.

The "Enroll Card" dialog box has a close button (X) in the top right corner. It contains the following elements:

- Registration Option:** A dropdown menu currently set to "Register by Card Reader".
- Information:** A section containing:
 - Facility Code:** An input field with a "Read Card" button next to it.
 - Card ID 1:** An input field.
- Buttons:** "Enroll" and "Cancel" buttons at the bottom.

a) Select a desired Registration Option.

Register by Card Reader

You can register a card by scanning the card information with the device connected to the visiting PC.

- Select **Register by Card Reader** for **Registration Option**.

15 Visitor

- b) Click **Read Card** and scan a card with the device.

Enter Manually

You can register a card by entering a card number directly.

- a) Select **Enter Manually** for **Registration Option**.
- b) Enter the **Facility Code** or **Card ID 1**.

- b) Click **Enroll** to register a card.

Add Visitors



You can add visitors.

- 1) Click **VISITOR**.
- 2) Click **+ Add Visitor**.

The screenshot shows a multi-section form for adding a visitor. Callout 1 points to the 'Visitor' section with 'Name' and 'Telephone' fields. Callout 2 points to the 'Host' section with 'Name' and 'Telephone' fields, and a table below showing 'Not found'. Callout 3 points to the 'Entry Information' section with 'Access Group' and 'Period' fields. Callout 4 points to the 'Credential' section with 'Card' and 'Fingerprint' options. At the bottom right are 'Register' and 'Cancel' buttons.

No	Item	Description
1	Visitor	<div>Enter the visitor's information.</div> <div><div>▪ Name: Enter the name.</div><div>▪ Telephone: Enter the telephone number.</div></div> <div><div>📌 Note</div><div><div>▪ If the Custom Visitor Field is set in the VISITOR setting, that fields are activated.</div></div></div>

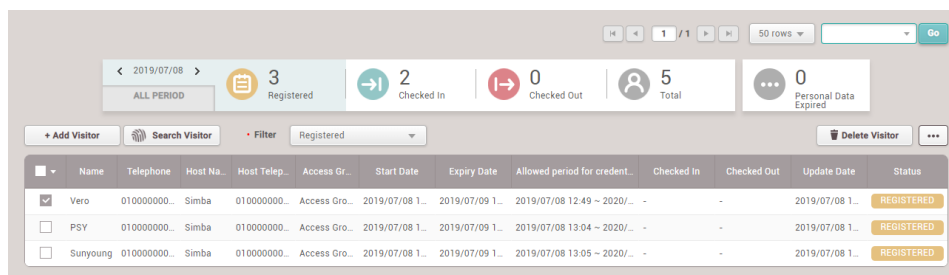
15 Visitor

No.	Item	Description
		<ul style="list-style-type: none"> Up to 48 characters may be entered for a name.
2	Host	<p>Enter the host's information.</p> <ul style="list-style-type: none"> Name: Enter the name. Telephone: Enter the telephone number. <p> Note</p> <ul style="list-style-type: none"> Up to 48 characters may be entered for a name. When you enter the name or telephone number, a list of users with information that matches is displayed. Click Choose to set a user of that list to the host.
3	Entry Information	<p>Set the zone and period to visit.</p> <ul style="list-style-type: none"> Zone: Set the access group. Period: Set the period for visit. <p> Note</p> <ul style="list-style-type: none"> Only access groups of sites assigned to visiting PC in VISITOR setting are displayed.
4	Credential	<p>Set the credentials.</p> <ul style="list-style-type: none"> Card: Set the card to Request to use the card authentication. Credential: Click + Fingerprint to use the fingerprint authentication. And enroll the fingerprint.

- Click **Register** to complete adding visitors.

Delete Visitors

- Click **Visitor**.
- Click a visitor to delete in the **Registered**.



The screenshot shows the 'Registered' tab of the Visitor Management System. At the top, there are summary statistics: 3 Registered, 2 Checked In, 0 Checked Out, 5 Total, and 0 Personal Data Expired. Below this is a table with columns: Name, Telephone, Host Name, Host Telephone, Access Group, Start Date, Expiry Date, Allowed period for credential, Checked In, Checked Out, Update Date, and Status. Three visitors are listed: Vero, PSY, and Sunyoung, all with a status of 'REGISTERED'.

	Name	Telephone	Host Name	Host Telephone	Access Group	Start Date	Expiry Date	Allowed period for credential	Checked In	Checked Out	Update Date	Status
<input checked="" type="checkbox"/>	Vero	0100000000	Simba	0100000000	Access Gro...	2019/07/08 1...	2019/07/09 1...	2019/07/08 12:49 ~ 2020/...	-	-	2019/07/08 1...	REGISTERED
<input type="checkbox"/>	PSY	0100000000	Simba	0100000000	Access Gro...	2019/07/08 1...	2019/07/09 1...	2019/07/08 13:04 ~ 2020/...	-	-	2019/07/08 1...	REGISTERED
<input type="checkbox"/>	Sunyoung	0100000000	Simba	0100000000	Access Gro...	2019/07/08 1...	2019/07/09 1...	2019/07/08 13:05 ~ 2020/...	-	-	2019/07/08 1...	REGISTERED

- Click **Delete Visitor** and then click **Yes**.

15 Visitor

Note

- The **Delete Visitor** button is activated if you click ☐ (check box).
- You can delete visitors only in the **Registered**.

Related Information

[Applying to Visit](#)

[Managing Check In Visitors](#)

[Managing Check Out Visitors](#)

[Visitor](#)

Managing Check In Visitors

You can check which visitors have been checked in and edit the registration information of them. And you can also let the visitors check out.

- 1) Click **VISITOR**.
- 2) Click a visitor in the **Checked In**.
- 3) Check the information of the visitor and then click **Check Out**.

15 Visitor

← Jacey

Visitor

Name

Jacey

Telephone

01000000002

Host

Name

Simba

Telephone

01000000000

Name	Telephone	Choose
Simba	01000000000	<div>Choose</div>

Entry Information

Access Group

Access Group

Period

2019/06/04 10:00 ~ 2019/06/05 10:00

Credential

Credential

+ Fingerprint

+ Card

Edit

Check Out

Cancel



Note

- If there are items that need to be modified, modify each item and click **Edit**.
- You can let the visitors check out in the list. The **Check Out** button is activated if you click ☐ (check box).

< 2019/06/05 >

ALL PERIOD

4 Registered

1 Checked In

4 Checked Out

9 Total

2 Personal Data Expired

+ Add Visitor

Search Visitor

Filter Checked In

Check Out

...

<input checked="" type="checkbox"/>	Name	Telephone	Host N...	Host Telep...	Access Gr...	Start Date	Expiry Date	Allowed period for creden...	Checked In	Checked Out	Update Date	Status
<input checked="" type="checkbox"/>	Jacey	01000000...	Simba	01000000...	Access Gr...	2019/06/04 1...	2019/06/05 1...	2019/06/04 10:03 ~ 2020...	2019/06/04 1...	-	2019/06/04 1...	EXPIRED

Managing Check Out Visitors

You can check which visitors have been checked out and register the visit again using that visitor's registration information.

- 1) Click **VISITOR**.
- 2) In the **Checked Out** list, click the visitor to re-register.
- 3) Click **Edit**.

15 Visitor

Visitor

Name

vero

Telephone

01000000001

Host

Name

Simba

Telephone

01000000000

Name	Telephone	Choose
Simba	01000000000	<div>Choose</div>

Entry Information

Access Group

Access Group

Period

2019/06/04 16:53 ~ 2019/06/05 16:53

Credential

Card

No request

Credential

+ Fingerprint

Type	Card Data Format	Summary	
Fingerprint	-	1	<div><div></div><div></div></div>

Register

Cancel

- 4) If there are items that need to be modified, modify each item and click **Register**.

Managing All Visitors

You can view all visitors that have been registered, checked in, and checked out for the set period. You can also add visitors.

- 1) Click **VISITOR**.
- 2) Click **Total**.

15 Visitor

	Name	Telephone	Host N...	Host Telep...	Access Gr...	Start Date	Expiry Date	Allowed period for creden...	Checked In	Checked Out	Update Date	Status
<input type="checkbox"/>	Jacey	01000000...	Simba	01000000...	Access Gr...	2019/06/04 1...	2019/06/05 1...	2019/06/04 10:03 ~ 2020...	2019/06/04 1...	-	2019/06/04 1...	EXPIRED
<input type="checkbox"/>	Chloe	01000000...	Simba	01000000...	Access Gr...	2019/06/05 1...	2019/06/06 1...	2019/06/05 16:00 ~ 2019...	-	-	2019/06/05 1...	REGISTERED
<input type="checkbox"/>	Julien	01011111...	Simba	01000000...	Access Gr...	2019/06/05 1...	2019/06/06 1...	-	-	-	2019/06/05 1...	REGISTERED
<input type="checkbox"/>	Jacey	01000000...	Simba	01000000...	Access Gr...	2019/06/05 1...	2019/06/06 1...	-	-	-	2019/06/05 1...	REGISTERED
<input type="checkbox"/>	SY	01000000...	Simba	01000000...	Access Gr...	2019/06/05 1...	2019/06/06 1...	-	-	-	2019/06/05 1...	REGISTERED
<input type="checkbox"/>	Shannon	01000000...	Simba	01000000...	Access Gr...	2019/06/04 1...	2019/06/05 1...	2019/06/05 13:48 ~ 2019...	-	2019/06/05 1...	2019/06/05 1...	CHECKED OUT
<input type="checkbox"/>	vero	01000000...	Simba	01000000...	Access Gr...	2019/06/05 1...	2019/06/06 1...	2019/06/05 14:00 ~ 2019...	-	2019/06/05 1...	2019/06/05 1...	CHECKED OUT
<input type="checkbox"/>	PSY	01000001...	Simba	01000000...	Access Gr...	2019/06/04 1...	2019/06/05 1...	2019/06/04 17:05 ~ 2019...	-	2019/06/05 1...	2019/06/05 1...	CHECKED OUT
<input type="checkbox"/>	Sunyoung	01000000...	Simba	01000000...	Access Gr...	2019/06/04 1...	2019/06/05 1...	2019/06/04 17:05 ~ 2019...	-	2019/06/05 1...	2019/06/05 1...	CHECKED OUT

Note

- You can approve the visit and add visitors in **Total**. For more details, refer to [Managing Registered Visitors](#).
- You can manage the checked in or checked out visitors in **Total**. For more details, refer to [Managing Check In Visitors](#) or [Managing Check Out Visitors](#).

Deleting Personal Data Expired

You can delete the visitors that have the personal data expired.

Note

- Only users with the operator level of Administrator can view the list of visitors who have expired. You can refer to the [Adding User Information](#) for more detailed information on the operator level.

- Click **VISITOR**.
- Click **Personal Data Expired**. The visitors that have personal data expired is displayed.

	Name	Telephone	Host N...	Host Telep...	Access Gr...	Start Date	Expiry Date	Allowed period for creden...	Checked In	Checked Out	Update Date	Status
<input checked="" type="checkbox"/>	PSY	01000001...	Simba	01000000...	Access Gr...	2019/06/04 1...	2019/06/05 1...	2019/06/04 17:05 ~ 2019...	-	-	2019/06/04 1...	EXPIRED
<input type="checkbox"/>	Sunyoung	01000000...	Simba	01000000...	Access Gr...	2019/06/04 1...	2019/06/05 1...	2019/06/04 10:03 ~ 2019...	2019/06/05 0...	2019/06/05 0...	2019/06/05 0...	CHECKED OUT

Note

15 Visitor

- For more information on configuring the period for the credential, see [Terms & Visitor Settings](#).

- 3) Click ☐ (check box) to select the visitors you want to delete.
- 4) Click **Delete personal data** and then click **Yes**.

You can use the **Setting** menu to configure user privileges, language, time, date, access card management, server connection, doors, etc.

The modifiable items may differ depending on the user permission.

Account

Preferences

Card

Card Format

Server

Trigger & Action

Schedules

Alert

HTTPS

Cloud

Image Log

USB Agent

Face Group Matching

Audit Trail

Video

Daylight Saving Time

Security

Active Directory


Visitor

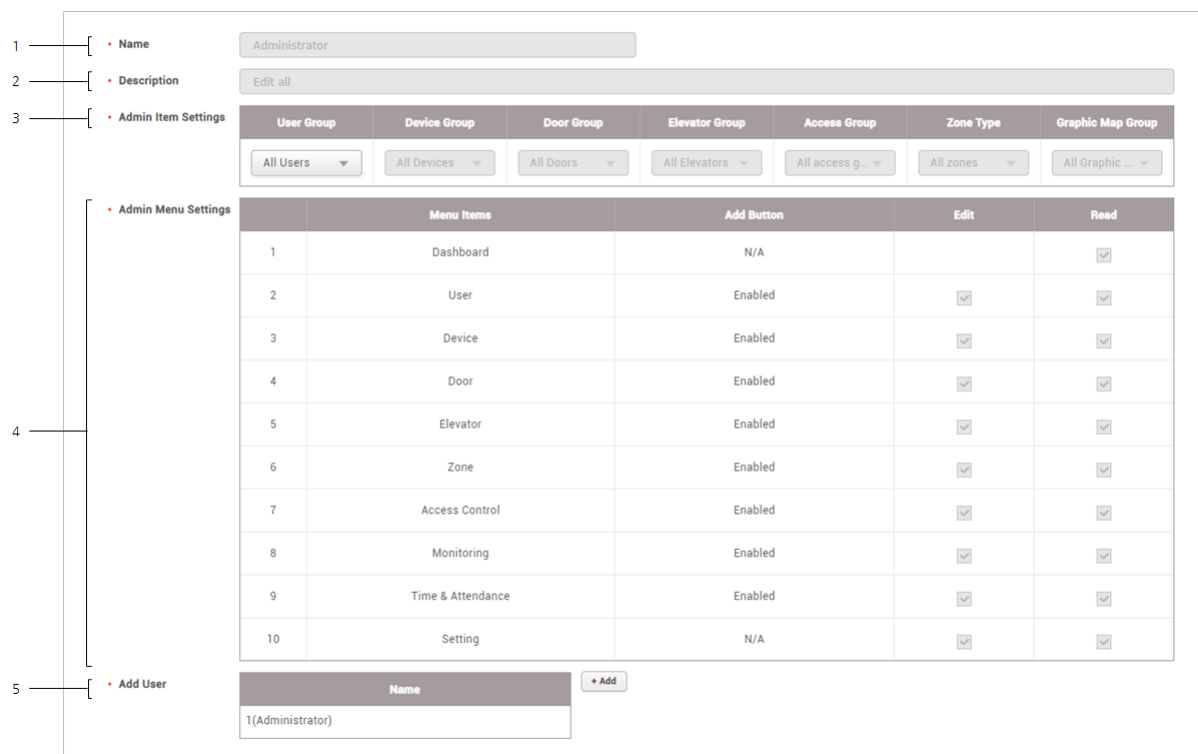
Mobile Access

Account

You can assign BioStar 2 operator account levels to registered users.

16 BioStar 2 Settings

- 1) Click **Settings > ACCOUNT**.
- 2) Click an account type. Depending on the type of license activated, the account type may vary.
 - **Administrator:** The user can use all menus.
 - **User Operator:** The user can only use the **USER** and **PREFERENCE** menus.
 - **Monitoring Operator:** The user can use the **MONITORING** and **PREFERENCE** menus and only view the **DASHBOARD, USER, DEVICE, DOOR, ZONE** and **ACCESS CONTROL** menus.
 - **Video Operator:** The user can only use the **VIDEO** menu.
 - **T&A Operator:** The user can only use the **TIME ATTENDANCE** menu and only view the **USER** menu.
 - **User:** The user can only view own information and T&A records.
 - **Visitor Operator:** The user can only use the **VISITOR** menu.
- 3) Click **+ Add** and select a user or click  to search for a user.




The screenshot displays the BioStar 2 Settings interface for account configuration. On the left, a sidebar contains five numbered items: 1. Name, 2. Description, 3. Admin Item Settings, 4. Admin Menu Settings, and 5. Add User. The main content area is divided into sections corresponding to these items. The 'Name' section shows 'Administrator' in a text box. The 'Description' section has an 'Edit all' button. The 'Admin Item Settings' section features a grid of dropdown menus for 'User Group', 'Device Group', 'Door Group', 'Elevator Group', 'Access Group', 'Zone Type', and 'Graphic Map Group', each with a default selection like 'All Users' or 'All Devices'. The 'Admin Menu Settings' section contains a table with 10 rows of menu items and their permissions. The 'Add User' section shows a list of users with a '+ Add' button.

	User Group	Device Group	Door Group	Elevator Group	Access Group	Zone Type	Graphic Map Group
	All Users	All Devices	All Doors	All Elevators	All access g...	All zones	All Graphic ...

	Menu Items	Add Button	Edit	Read
1	Dashboard	N/A		<input checked="" type="checkbox"/>
2	User	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Device	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	Door	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Elevator	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
6	Zone	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7	Access Control	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Monitoring	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
9	Time & Attendance	Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10	Setting	N/A	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

The 'Add User' section shows a list of users with a '+ Add' button.

Name	+ Add
1 (Administrator)	

No.	Item	Description
1	Name	Shows the account level name.
2	Description	Show a brief description of the account level.
3	Admin Item Settings	Show the group assigned the permission.
4	Admin Menu Settings	Shows the assigned privileges.
5	Add User	Shows the list of users assigned with the privileges. Click + Add to add a user. <ul style="list-style-type: none"> ▪ Click  to delete the registered users.

16 BioStar 2 Settings

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

Note

- If privileges have already been assigned while adding or editing users, the assigned users are shown on the list.
- Unless a user with the privilege for **Edit** saves settings after changing the detailed settings of each menu, the user with a **Read** privilege only can see the previous information yet to be modified.

Related Information

[Editing User Information](#)

[Adding Custom Account Level](#)

Adding Custom Account Level

You can assign BioStar 2 operator privilege levels to registered users.

Note

- The **Admin Menu Settings** may vary depending on the type of license that is activated.

- 1) Click **Settings > ACCOUNT**.
- 2) Click **ADD CUSTOM LEVEL**.
- 3) Enter or select the necessary items. Depending on the type of license activated, the account type may vary.

16 BioStar 2 Settings

1 — [• Name

2 — [• Description

3 — [• Admin Item Settings


User Group	Device Group	Door Group	Elevator Group	Access Group	Zone Type	Graphic Map Group
All Users ▼	All Devices ▼	All Doors ▼	All Elevators ▼	All access g... ▼	All zones ▼	All Graphic ... ▼

4 — [• Admin Menu Settings


	Menu Items	Add Button	Edit	Read
1	Dashboard	N/A		<input type="checkbox"/>
2	User	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
3	Device	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
4	Door	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
5	Elevator	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
6	Zone	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
7	Access Control	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
8	Monitoring	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
9	Time & Attendance	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
10	Setting	N/A	<input type="checkbox"/>	<input type="checkbox"/>

5 — [• Add User

Name + Add

No.	Item	Description
1	Name	Enter the desired account level name.
2	Description	Enter a brief description of the account level.
3	Admin Item Settings	<p>Set the detailed permission for each item. You can select groups to assign the edit and read permissions for each menu.</p> <p>Admin Item Settings can be set for User Group, Device Group, Door Group, Elevator Group, Access Group, Zone Type, Graphic Map Group and it can be set based on the already created group information.</p> <p>If there is no group you want, add a new group to that menu. For details about the creation of a group, refer to Adding and Managing User Groups, Adding and Managing Device Groups, Adding and Managing Door Groups, Adding and Managing Elevator Groups, Adding and Managing Access Groups, Adding and Managing Graphic Map Groups.</p>
4	Admin Menu Settings	<p>Set the edit and read permissions for the menu. A different permission can be set according to each menu.</p> <ul style="list-style-type: none"> ▪ Edit: The permission to add, edit, and delete the items of the menu. ▪ Read: The permission to read the items of the menu. <p> Note</p> <ul style="list-style-type: none"> ▪ If you assign the edit permission to each menu, Add Button will be enabled. However, there is no Add Button in Dashboard and Setting menu, so it is displayed as N/A. And Add button in Access Control menu is only enabled when Access Group is set as All access groups in Admin Item Settings and the edit permission is assigned.

16 BioStar 2 Settings

No.	Item	Description
5	Add User	<p>You can add or view the users assigned with the privilege. If you want to add a user, click + Add to add a user.</p> <ul style="list-style-type: none"> Click  to delete the registered users.

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

Note

- Refer to the following example for configuring **Admin Item Settings** and **Admin Menu Settings**.

User Group	Device Group	Door Group	Elevator Group	Access Group	Zone Type	Graphic Map Group
User Group 01 ▼	Device Grou... ▼	Door Group ... ▼	All Elevators ▼	AC Group ▼	All zones ▼	All Graphic ... ▼
2	User		Disabled		<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	Device		Disabled		<input type="checkbox"/>	<input checked="" type="checkbox"/>
4	Door		Enabled		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Elevator		Disabled		<input type="checkbox"/>	<input checked="" type="checkbox"/>
6	Zone		Disabled		<input type="checkbox"/>	<input type="checkbox"/>
7	Access Control		Disabled		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
8	Monitoring		Disabled		<input type="checkbox"/>	<input checked="" type="checkbox"/>

- **User:** You can see the user information in the 'User Group 01'. However, you cannot add a new user or edit existing users.
- **Device:** You can see the device information in the 'Device Group 01'. However, you cannot add a new device or edit existing devices.
- **Door:** The setting of doors included in the 'Door Group 01' can be edited or deleted. You can edit the device of the door included in 'Door Group 01'. You can also add a new door to 'Door Group 01'.
- **Elevator:** You can see the setting of all the elevators. However, you cannot add a new elevator or edit existing elevators.
- **Zone:** You do not have permission.
- **Access Control:** The setting of access groups included in the 'AC Group' can be deleted. You can add or delete users and user groups to 'AC Group'.
- **Monitoring:** You can see the access control events of the devices included in 'Device Group 01'. And you can see the device and door status zone status and the alert history. You can also see a graphic map of 'All Graphic Maps'. However, you cannot control each status.
- If the configuring for **Admin Item Settings** and **Admin Menu Settings** do not match, the permission will not be assigned for that item. If you select the item of the menu by the account to which this custom permission was assigned, the '**Permission Denied**' message is displayed.

16 BioStar 2 Settings

- You can add an unlimited number of custom account levels.

Preference

You can change language, time zone, time/date format, and upload a sound file to be used as an alert.

- Click **Settings > PREFERENCE**.
- Edit the necessary fields.

1

Language / Time Zone

• Language

English

• Time Zone

(UTC+9:00) Seoul, Tokyo, Osaka, Sapporo, Y...

• Daylight Saving Time

2

Date/Time

• Date Format

yyyy/mm/dd

• Time Format

hh:mm

3

Sound


• Alert

Sound Name	File Size	File Format	Play
Not found			

+ Add

No.	Item	Description
1	Language / Time Zone	<p>You can configure the BioStar 2 language and time zone settings.</p> <ul style="list-style-type: none">Language: Select a language to use.Time Zone: Select a time zone to use.Daylight Saving Time: Select the daylight saving time to apply to BioStar 2 server. If no registered daylight saving time, see Daylight Saving Time.
2	Date/Time Format	<p>You can configure the date and time format to use in BioStar 2.</p> <ul style="list-style-type: none">Date Format: Changes the date format.Time Format: Changes the time format.
3	Sound	<p>You can upload a sound file to use in BioStar 2.</p> <p>a) Click + Add.</p>

16 BioStar 2 Settings

No.	Item	Description
		<div><div>Add Sound ×</div><div><ul style="list-style-type: none">• Sound Name <input type="text"/>• File Size 0 KB• File Format• Sound Name <input type="button" value="Browse"/><p>• Sound Files must be .wav or .mp3 format and a maximum of 10 MB.</p><div><input type="button" value="Add"/> <input type="button" value="Close"/></div></div><p>b) Click Browse to select a file. c) Select .wav file or .mp3 file and then click Open. d) Click Add to upload</p><p> Note</p><ul style="list-style-type: none">▪ Sound files must be .wav or .mp3 format.▪ A maximum file size is 10MB.</div>

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

➤ Related Information

Alert

Card

You can view the card status, assigned users, blacklist, etc.

- 1) Click **Setting** > **CARD**. The list of registered cards is shown.

Card Type	Card ID	Status	User ID	User Name
CSN	1225051669057584	Assigned	2	User 1
CSN	4276710323	Unassigned	-	-
CSN	989777499	Unassigned	-	-
CSN	1217252008448048	Unassigned	-	-
CSN	1234938686282624	Unassigned	-	-
CSN	308871143	Unassigned	-	-

- 2) Click **Unassigned Card**, **Activated Card** or **Blacklist Card** to view the list of corresponding

16 BioStar 2 Settings

cards.

Note


- If a card is blocked, the card information will appear in **Blacklist Card** list. To unblock the card, select a card and click **Unblock**.

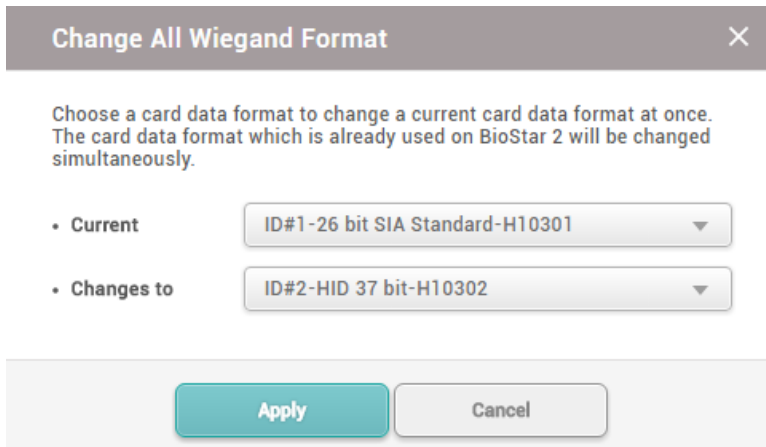
Changing Wiegand Card Data Format

You can change the Wiegand card data formats in use simultaneously.

Note

- The data format of the card already assigned to the user will be changed.

- 1) Click **Settings > CARD**.
- 2) Click  and then select **Change All Wiegand Format**.
- 3) Select a card data format to be changed from the list of **Current** and select a desired card data format from the list of **Changes to**.



The dialog box titled "Change All Wiegand Format" has a close button (X) in the top right corner. Below the title bar, there is a descriptive text: "Choose a card data format to change a current card data format at once. The card data format which is already used on BioStar 2 will be changed simultaneously." Below this text, there are two dropdown menus. The first is labeled "Current" and shows "ID#1-26 bit SIA Standard-H10301". The second is labeled "Changes to" and shows "ID#2-HID 37 bit-H10302". At the bottom of the dialog, there are two buttons: "Apply" (highlighted in teal) and "Cancel".

- 4) Click **Apply** to change the card data format.

Card Format

It is possible to set the Wiegand type of the card or the website key and layout of the smart / mobile card.

- 1) Click **Settings > CARD FORMAT**.

16 BioStar 2 Settings


- 2) Configuring the settings by referring to information, **Wiegand** and **Smart / Mobile Card**.

Wiegand

You can configure the format for reading card data. The card data is processed in the set Wiegand format.

 **Note**

- The data format of the card already assigned to the user will be changed.

- 1) Click **Settings > CARD FORMAT**.
- 2) Click **Wiegand**.
- 3) Click  from the list and then configure the settings.

Information

1

Name

2


Description

3

Total Bits


4

ID Field

	Start Bit	End Bit	Size	
ID0			0	


5

Parity Bits

Position	Type	Start Bit	End Bit	Size	
	Odd			0	

+ Add

+ Add

No.	Item	Description
1	Name	Enter a Wiegand format name.
2	Description	Enter a short description.
3	Total Bits	Enter the total bit count.
4	Facility Code Field	You can set whether or not to use a facility code. If you want to use a facility code, click <input type="checkbox"/> (check box) and enter a start bit and end bit.
4	ID Field	Enter a start bit and end bit of the ID to use. Click + Add to add an ID field.
5	Parity Bits	<div>Set parity bits. Click + Add to add a parity bit.</div> <div><div> Note</div><div><ul style="list-style-type: none">▪ You must enter the total bit to add a parity bit.</div></div>

- 3) Click **Apply** to add the Wiegand format.

16 BioStar 2 Settings

 **Note**

- Pre-defined formats cannot be edited or deleted.

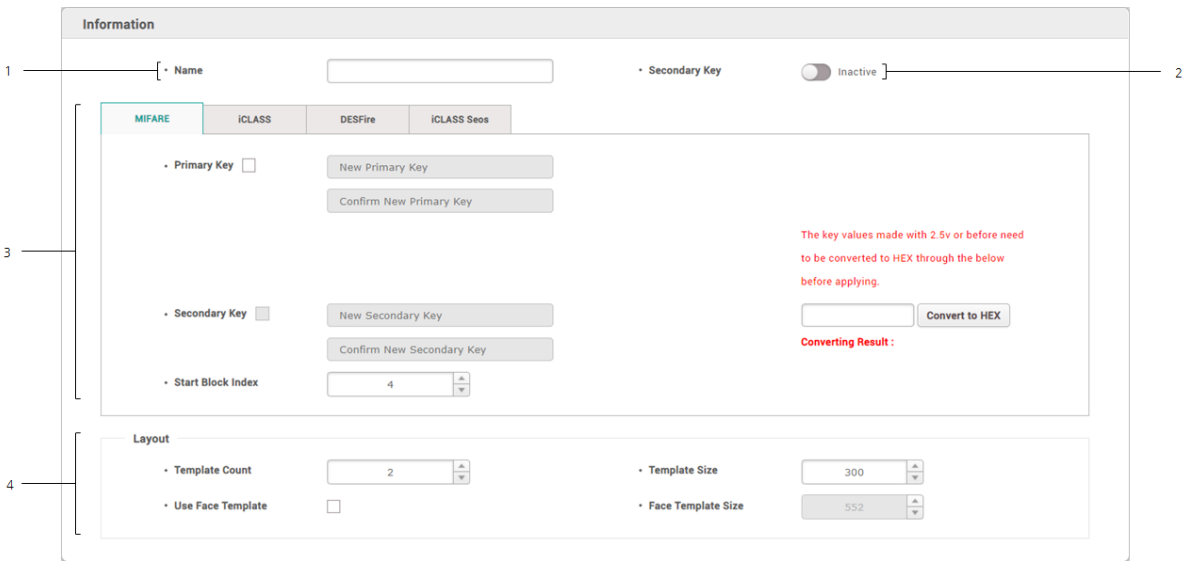
Smart / Mobile Card

It is possible to set the layout of smart cards such as MIFARE, iCLASS, DESFire, iCLASS Seos and mobile.

 **Note**



- To set the mobile card, set **Active** for **Mobile Card Enrollment** on the **User/Device Management** tab of **Setting > SERVER**.

- 1) Click **Settings > CARD FORMAT**.
- 2) Click **ADD SMART CARD** and configure the setting.



No.	Item	Description
1	Name	Enter the name of the smart card.
2	Secondary Key	It is possible to set whether or not to use the secondary website key. If Active is set, you can set Secondary Key . When a secondary site key is set, authentication is carried out using the secondary website key when the basic site key of the card does not match.
3	Smart Card Setting	It is possible to set the structure of smart cards such as MIFARE, iCLASS, DESFire, iCLASS Seos and mobile. The primary site key and the secondary site key support only HEX values. In the field on the right side of the screen, enter the key value and click Convert to HEX . Use the converted value as your site key.

16 BioStar 2 Settings

No.	Item	Description
		<ul style="list-style-type: none"> ▪ DESFire Advanced: You can use a DESFire card issued by a third-party. Setting is available only for DESFire. <p> Note</p> <ul style="list-style-type: none"> ▪ To use DESFire Advanced, enter the information for App Master Key, App Master Key Index, File Read Access Key, File Read Access Key Index, File Write Access Key, File Write Access Key Index, App ID, File ID, and Encryption Type correctly. ▪ Primary Key: Key which encrypts the communication between the smart key and the card reader. ▪ Secondary Key: It is possible to set secondary website key. ▪ Start Block Index: Select the start block where each template will be saved. This block is the index of block where user information will be saved. If the user already has the smart key, set available block for saving. Setting is available only for MIFARE and iCLASS. ▪ App ID: Set the application ID. This plays a role of directory which includes file ID. Setting is available only for DESFire. ▪ File ID: Set the file ID. Setting is available only for DESFire. ▪ Encryption Type: It is possible to set the encryption type to DES/3DES or AES. Setting is available only for DESFire. ▪ ADF Address Value: ADF address where digital credential is stored and only the iCLASS Seos card is available.
4	Layout	<p>It is possible to change the layout where user information and fingerprint information are recorded.</p> <ul style="list-style-type: none"> ▪ Template Count: Set the number of fingerprint templates to be included in the layout. ▪ Template Size: Set the number of bytes used by the fingerprint template. ▪ Use Face Template: Select whether to use the face template. ▪ Face Template Size: Set the number of bytes used by the face template. <p> Note</p> <ul style="list-style-type: none"> ▪ Face templates are only available on FaceStation F2.

3) Click **Apply** to enroll a smart card setting.

Server

16 BioStar 2 Settings

You can configure the BioStar 2 server information, user management, device management and automatic upgrade settings.

1) Click **Settings** > **SERVER** and configure the settings.

General

General

- BioStar IP Address: Any
- BioStar Port: 51212
- Session Timeout: 60 Min
- Log Upload: Automatic
- Web Server Protocol: HTTP ☐ HTTPS ☒

Item	Description
General	<p>You can configure the general information on BioStar 2.</p> <ul style="list-style-type: none">▪ BioStar IP Address: Set the server IP address. Change the setting to use a specific IP address.▪ BioStar Port: Set the server port.▪ Session Timeout: Set a session timeout period. If there is no activity on BioStar 2 for the set time after logging in, the session is logged out automatically.▪ Log Upload: Select an event log upload method. If real-time communication with the server is difficult, set this to Manual.▪ Web Server Protocol: Set a server communication protocol.


User/Device Management

User/Device Management

- Automatic User Synchronization: All Devices
- Fingerprint Template Format: Suprema
- Enrollment Device: Not found
- Mobile Card Enrollment: Inactive
- User ID Type: Number
- Custom User Field: Not found
- Delete personal & credential data when issuing an AoC: Inactive
- AC event log storage duration: Inactive 60 day(s)

Item	Description
User/ Device Manage	You can configure the user synchronization and fingerprint template format settings.

16 BioStar 2 Settings

Item	Description
ment	<ul style="list-style-type: none"> ▪ Automatic User Synchronization: Change the user information synchronization method. Select All Devices to have the user information automatically synchronized with the server. Select All Devices(Including user update from device) to have the user information changed on the device automatically synchronized to all devices that registered on the server. Select Specific Devices(Only devices belonging to the access group) to automatically synchronize only the devices belonging to the access group with the changes. ▪ Mobile Card Enrollment: Set to Enabled to use the mobile card. ▪ Fingerprint Template Format: Set the fingerprint template format. Available options include SUPREMA, ISO and ANSI378. If there are still user fingerprint template remaining in the device, selecting a different format is not possible. ▪ User ID Type: Use of Number or Alphanumeric can be set for user ID. When Alphanumeric is set for User ID Type, BioLite Net, BioEntry Plus and BioEntry W cannot be used. In addition, all users saved in Xpass and Xpass S2 will be deleted and all settings except for the network will be initialized. ▪ Enrollment Device: You can designate certain devices that you frequently use for fingerprint and card enrollment as an enrollment device. Click the + Add and choose the devices. ▪ Custom User Field: You can add custom user fields for extra user information and these fields appear on the User page. There are three types of custom user fields: Number Input Box, Text Input Box and Combo Box. If you choose the Combo Box for a custom user field, you can add up to 20 items with 32 characters each, and each item is separated by a semicolon (;). ▪ Delete personal & credential data when issuing an AoC: If you issue an AoC card which stores user's credentials on the smart card, you can set BioStar 2 to delete user's data and credential information automatically. ▪ AC event log storage duration: You can set the period for storing the access control event logs. <p> Note</p> <ul style="list-style-type: none"> ▪ If you select Automatic User Synchronization as Specific Devices(Only devices belonging to the access group), users stored in the device that do not belong to the access group cannot be managed by the server. If you use this option, go to DEVICE menu and click Delete Data & Sync Device for each device to

16 BioStar 2 Settings

Item	Description
	<p>proceed with the synchronization.</p> <ul style="list-style-type: none"> ▪ Even if you select Automatic User Synchronization as Specific Devices(Only devices belonging to the access group), Access groups set up for special purposes, such as the following, will be synchronized regardless of the device's access group. <ul style="list-style-type: none"> - Dual authentication access group set up in the Devices and Elevators - Bypass Group in the Anti-passback Zone - Bypass Group in the Scheduled Lock Zone - Scheduled Unlock Authentication Group in the Scheduled Unlock Zone - Arm/Disarm Group in the Intrusion Alarm Zone ▪ Even if you select Automatic User Synchronization as Specific Devices(Only devices belonging to the access group), Users set to device administrator will be synchronized regardless of the access group. ▪ NFC card is supported with the below conditions. <ul style="list-style-type: none"> - Mobile device OS: Android 5.0 Lollipop or later - BioStar 2 Mobile 2.4.1 or later - Xpass S2: XPS2M-V2 FW 2.4 or later - BioStation 2: BS2-OMPW, BS2-OIPW FW 1.4 or later - BioStation A2: BSA2-OMPW, BSA2-OIPW FW 1.3 or later - BioStation L2: BSL2-OM FW 1.2 or later - BioEntry W2: BEW2-OAP, BEW2-ODP FW 1.1 or later - FaceStation 2: FS2-D, FS2-AWB FW 1.0 or later - BioLite N2: BLN2-ODB, BLN2-OAB, BLN2-PAB FW 1.0 or later - XPass D2: XPD2-MDB, XPD2-GDB, XPD2-GKDB FW 1.0 or later - FaceLite: FL-DB FW 1.0 or later - XPass 2: XP2-MDPB, XP2-GDPB, XP2-GKDPB FW 1.0 or later ▪ BLE card is supported with the below conditions. <ul style="list-style-type: none"> - Mobile device OS: Android .0 Lollipop or later / iOS 9.0 or later - BioStar 2 Mobile 2.4.1 or later - FaceStation 2: FS2-AWB FW 1.0 or later - BioLite N2: BLN2-ODB, BLN2-OAB, BLN2-PAB FW 1.0 or later - XPass D2: XPD2-MDB, XPD2-GDB, XPD2-GKDB FW 1.0 or later - FaceLite: FL-DB 1.0 or later - XPass 2: XP2-MDPB, XP2-GDPB, XP2-GKDPB FW 1.0 or later

16 BioStar 2 Settings

Item	Description
	<div><ul style="list-style-type: none">▪ When User ID Type is changed from Alphanumeric to Number, all user information registered on BioStar 2 should be deleted.▪ The devices and the firmware versions where the User ID Type can be changed are as follows.<ul style="list-style-type: none">- CoreStation FW 1.0.0 or later- FaceStaion 2 FW 1.0.0 or later- FaceLite FW 1.0.0 or later- BioEntry W2 FW 1.1.0 or later- BioStation L2 FW 1.2.0 or later- BioStation A2 FW 1.3.0 or later- BioStation 2 FW 1.4.0 or later- BioLite N2 FW 1.0.0 or later- BioEntry P2 FW 1.0.0 or later- BioEntry R2 FW 1.0.0 or later- XPass 2 FW 1.0.0 or later- XPass D2 FW 1.0.0 or later- Xpass FW 2.4.0 or later- Xpass S2 FW 2.4.0 or later▪ If you change the value in the Order field, the position of the custom field on the User page changes.▪ For a number input field, a number from 0 to 4294962795 is allowed and characters are not allowed.<div><div>• ex - Number Input Bo..</div><div></div></div>▪ For a text input field, up to 32 characters are allowed.<div><div>• ex - Text Input Box</div><div></div></div>▪ For a combo box field, the items that have been set to the field are displayed as item. If you want to configure a combo box field as shown in the screenshot below, you need to enter <i>Option 1;Option 2;Option 3;Option 4</i> in the data field.<div><div>• ex - Combo Box</div><div><div>Option 1</div><div>None</div><div>Option 1</div><div>Option 2</div><div>Option 3</div><div>Option 4</div></div></div></div>

16 BioStar 2 Settings

License

Access Control

Applied License

Enterprise

Issued to

PSY

Expiry date

None

Time Attendance

Activate License Online

Name

Activation Key

Activate

Activate License Offline

Request offline key

Activate

Video

Activate License Online

Name

Activation Key

Activate

Activate License Offline

Request offline key

Activate

Visitor

Activate License Online

Name

Activation Key

Activate

Activate License Offline

Request offline key

Activate

Item	Description
License	<p>You can activate the purchased license.</p> <p>To activate the license online, click Activate after entering your name and the activation key that you've received from Suprema.</p> <p>To activate the license offline, click Request offline key, then the Activate License Offline dialog will appear. Follow the instructions on the dialog.</p>

Server Matching

Server Matching

Use Server Matching

Inactive

Fast Mode

Active

Max. Simultaneous Server Matching Count

2 / 4

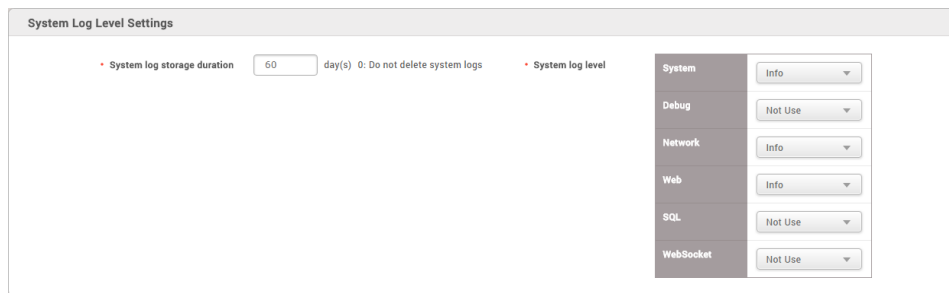
Security Level

1 / 1,000,000

Item	Description
Server Matching	<p>You can configure server matching. If you use server matching, the user's fingerprint will be matched from BioStar 2, not the device.</p> <p>The Server Matching will appear when the Advance or higher license is activated.</p> <ul style="list-style-type: none">Use Server Matching: Activates/Deactivates server matching.Max. Simultaneous Server Matching Count: You can configure how many matchings can be done simultaneously.Fast Mode: You can configure the fingerprint matching speed.Security Level: You can configure the server matching's security level. The higher the security level is set, the more the false rejection rate (FRR) can occur.

System Log Level Settings

16 BioStar 2 Settings



System Log Level Settings

System log storage duration: 60 day(s) 0: Do not delete system logs

System log level:

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

Item	Description
System Log Level Settings	<p>You can set the duration and log level of the system log to be stored in the database. The system log storage period can be set up to 120 days, and logs is not deleted when setting to 0.</p> <p>System logs are managed according to pre-defined categories, and the log level is divided into Trace, Debug, Info, Warning, and Error. The high level contains all lower level logs. For example, when set to Trace, you can store the logs including Debug, Info, Warning, and Error logs.</p>

- 2) Click **Apply** to save the settings.

Note

- Please inquire your network administrator for any help necessary with the web server protocol configuration.

Related Information

[Real-time Log](#)

Trigger & Action

You can set the device or BioStar to do a specific operation when a specific event has occurred at the devices, doors and zones.

- 1) Click **Settings > TRIGGER & ACTION**.
- 2) Click **ADD TRIGGER & ACTION** and configure the settings.


16 BioStar 2 Settings

The screenshot shows the BioStar 2 Settings window for configuring a trigger and action. The interface is divided into six numbered sections:

- 1. Name:** A text input field for naming the trigger and action.
- 2. Schedule:** A dropdown menu for selecting a schedule.
- 3. Device, Door, Zone:** Radio buttons for selecting the type of trigger (Device, Door, or Zone) and a list of available devices/doors/zones.
- 4. Event:** A list of events that can trigger the action, with checkboxes for selection.
- 5. Device and BioStar 2:** A tabbed interface for selecting the device or BioStar 2 server that will perform the action.
- 6. Action:** Two dropdown menus for selecting the output and signal to be sent when the event occurs.

No.	Item	Description
1	Name	Enter a name of the trigger & action.
2	Schedule	<p>Select a schedule.</p> <p>Note</p> <ul style="list-style-type: none"> When configuring a user defined condition by selecting Input, if no desired schedule is available, click + Add Schedule to create it. For more information on configuring schedules, see Schedules.
3	Device, Door, Zone	<p>Select a device/door/zone at which a specific event will be monitored. Multiple devices/doors/zones can be selected. The devices/doors/zones work independently even when they are disconnected from the BioStar server.</p> <p>Note</p> <ul style="list-style-type: none"> The Zone will appear when the Advance or higher license is activated.
4	Triggering Event	Set a triggering event. At least one event must be selected.
5	Device and BioStar 2	Select a device which performs the action. You can select a device or BioStar 2 to perform an action.
6	Action	Set a signal to send when the selected triggering event occurs. You can also set an email to which the log will be sent from BioStar 2.

16 BioStar 2 Settings

No.	Item	Description
		<ul style="list-style-type: none">• Select BioStar and click  to configure the email server information.• To add an email address, click + Add and enter an email address. Click OK to add the recipient.

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

 **Note**

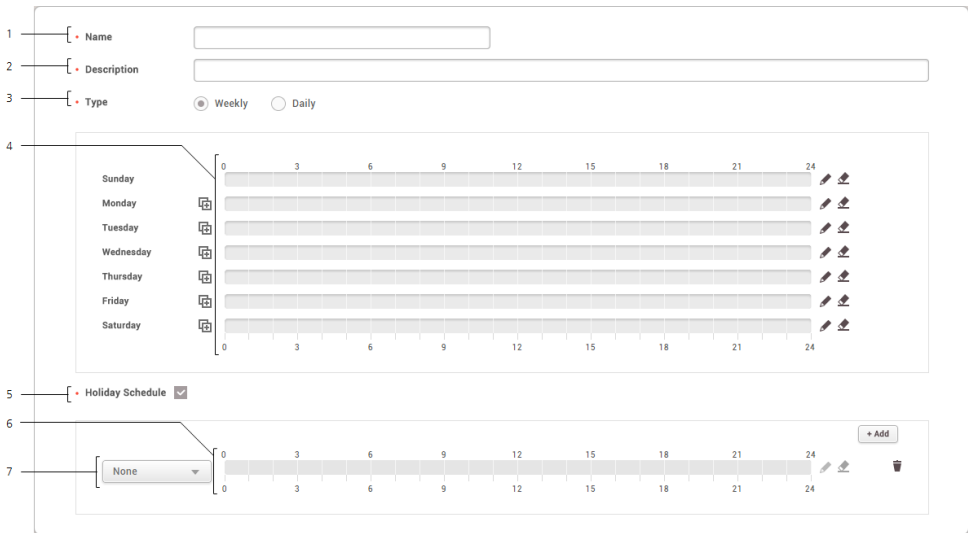
- For more information on email server information, contact your system administrator.

Schedules

You can add access schedules and holiday schedules.

— Adding New Schedule

- 1) Click **Settings > SCHEDULE**.
- 2) Click **ADD SCHEDULE**.
- 3) Enter the required information into the fields and set a schedule for each day of the week.



No.	Item	Description
1	Name	Enter a name of the schedule.
2	Description	Enter a short description of the schedule.
3	Type	For schedule type, select Weekly or Daily . When set to

16 BioStar 2 Settings

No.	Item	Description
		Daily , Cycle and Start Date can be selected.
4	Time Slots	<p>Click on time slots to set a desired schedule and click OK.</p> <div> <div>Input Schedule</div> <div> <div>Schedule</div> <div>Monday</div> <div>Clear</div> </div> <div> <div>Time Slot 1</div> <div></div> <div>:</div> <div></div> <div>~</div> <div></div> <div>:</div> <div></div> </div> <div> <div>Time Slot 2</div> <div></div> <div>:</div> <div></div> <div>~</div> <div></div> <div>:</div> <div></div> </div> <div> <div>Time Slot 3</div> <div></div> <div>:</div> <div></div> <div>~</div> <div></div> <div>:</div> <div></div> </div> <div> <div>Time Slot 4</div> <div></div> <div>:</div> <div></div> <div>~</div> <div></div> <div>:</div> <div></div> </div> <div> <div>Time Slot 5</div> <div></div> <div>:</div> <div></div> <div>~</div> <div></div> <div>:</div> <div></div> </div> </div> <div> <div>Ok</div> <div>Cancel</div> </div>

4) Click **Apply** to add the holiday schedule.

+ Adding Holiday Schedule


16 BioStar 2 Settings


Alert

You can set the alarm type and message to display when a specific event has occurred at the devices, doors and zones. You can adjust settings so that BioStar 2 can play the uploaded sound file upon the occurrence of alarms.

1) Click **Settings > ALERT**.

Device	Door	Zone	Authentication
<input type="checkbox"/> Device Disconnection Det...	<input checked="" type="checkbox"/> Forced door opened	<input checked="" type="checkbox"/> Anti-passback zone alarm...	<input type="checkbox"/> 1:1 authentication failed
<input type="checkbox"/> Device restarted	<input checked="" type="checkbox"/> Held door opened	<input checked="" type="checkbox"/> Fire alarm zone alarm det...	<input checked="" type="checkbox"/> 1:1 duress authentication s...
<input checked="" type="checkbox"/> RS-485 disconnected	<input type="checkbox"/> Forced door open alarmed	<input checked="" type="checkbox"/> Scheduled lock zone alar...	<input type="checkbox"/> 1:N authentication failed
<input checked="" type="checkbox"/> Tamper on	<input type="checkbox"/> Held door open alarmed	<input checked="" type="checkbox"/> Intrusion alarm detected	<input checked="" type="checkbox"/> 1:N duress authentication s...
<input type="checkbox"/> Supervised Input (Short)		<input checked="" type="checkbox"/> Interlock door open denie...	<input checked="" type="checkbox"/> Access denied (Invalid acce...
<input type="checkbox"/> Supervised Input (Open)		<input checked="" type="checkbox"/> Interlock door open denie...	<input checked="" type="checkbox"/> Access denied (Disabled user)
<input checked="" type="checkbox"/> AC Power Failure		<input checked="" type="checkbox"/> Muster zone alarm detected	<input checked="" type="checkbox"/> Access denied (Invalid period)
			<input checked="" type="checkbox"/> Access denied (Blacklist)
			<input checked="" type="checkbox"/> Access denied (Hard Anti-pa...
			<input checked="" type="checkbox"/> Access denied (Forced lock ...
			<input checked="" type="checkbox"/> Access denied (Soft anti-pa...
			<input checked="" type="checkbox"/> Fake Fingerprint Detected

- 2) Select event types to display on the screen.
- 3) Click  and enter a message to display on the screen. If you have uploaded the sound file to play upon the occurrence of a corresponding event, select it from the list of **Sound File** and set the **Play Options**. If there is no sound file to play, upload it with reference to the **Sound of Preference**.


Alert Message 


• Name

Alert Message


• Message

• Sound File

alert 



• Play Options

Once 

Apply

Cancel

16 BioStar 2 Settings

- 4) Click **Apply** to save the alert messages.
- 5) Click **Apply** to save the changes.

➤ Related Information

Preference

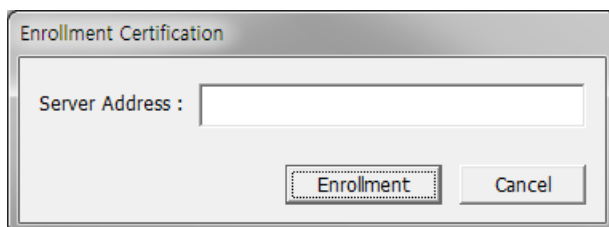
HTTPS

In order to connect BioStar 2 through HTTPS, it is necessary to register the IP address where BioStar 2 is installed and install the certificate. For correct network connection, install the certificate before using BioStar 2.

📌 Note

- BioStar 2.5.0 uses HTTPS as the default communication protocol.

- 1) Click **Settings > HTTPS**.
- 2) Click **Cert. Download**.
- 3) Unzip the downloaded file and run **cert-register.exe** file. **Enrollment Certification** window will appear.



- 4) Enter the IP address of the PC where BioStar 2 is installed and click **Enrollment**.
- 5) Check the security warning message and click **Yes**.
- 6) When you restart the web browser and enter the registered IP address, **Secure** will appear on the address bar of the web browser.

Cloud

You need to configure the cloud settings in order to access your BioStar 2 server remotely (outside of the local network). Additionally, the cloud settings should be done in order to use the BioStar 2 Mobile app.

📌 Note

16 BioStar 2 Settings

- The Cloud will be available when the Standard or higher license is activated.
- If you use BioStar 2 Cloud, cannot connect to BioStar 2 through Internet Explorer or Edge.
- If you connect BioStar 2 using the Cloud, cannot access to the **VIDEO** menu.

- 1) Click **Settings > CLOUD**.
- 2) Edit the necessary fields.

The screenshot shows the 'General' tab of the BioStar 2 Cloud Settings. It includes a 'Cloud Use' toggle set to 'Use'. Below it, 'Subdomain Name' is 'suprema' and 'Administrator e-mail' is 'suprema@suprema.co.kr'. The 'Advanced' tab shows 'Cloud Server Address' as 'api.biostar2.com', 'Port Used By Cloud' as '52000', and 'Version' as 'v2'.

No.	Item	Description
1	Cloud Use	<p>To use the cloud set it as Use. If you set as Not Use, it will be unable to access BioStar 2 using BioStar 2 Mobile.</p> <p> Note</p> <ul style="list-style-type: none">▪ If you set Cloud Use as Use, Password Level should be set as Medium or Strong. For more information, see Server.
2	Subdomain Name	<p>Enter the subdomain for usage. You can use the subdomain to access BioStar 2 using BioStar 2 Mobile.</p> <p>The subdomain is a unique value for identification same as user ID, so use a unique word such as company names.</p>
3	Administrator e-mail	<p>Enter the cloud administrator email.</p>
4	Cloud Server Address	<p>The Cloud server's address. Normally set as default.</p>
5	Version	<p>The Cloud server's version. Normally set as default.</p>
6	Port Used By Cloud	<p>This is the port number the cloud uses. Normally set as default (52000).</p> <p>If the cloud does not operate normally, modify the inbound and outbound rules from the firewall setting on the PC where BioStar 2 is installed. For more information, contact the system administrator.</p> <ul style="list-style-type: none">▪ Ports to be added to the inbound rule: BioStar 2 server port (Default value: 80, user-specification), BioStar 2 cloud port (Default value: 52000, user-specification)▪ Ports to be added to the outbound rule: 4443, all ports used by ngrok

16 BioStar 2 Settings

3) Click **Apply** to save the changes.

 **Note**

- E-mail transfer may take up to 10 minutes.
- For the cloud, BioStar server must always be turned on. If the server loses more than one week of connection, you must proceed with a re-register process via email.

Image Log

It is possible to set the default value which can be added when using the delete option of image log and an image log from the device.

- 1) Click **Settings > Image Log**.
- 2) Edit the necessary fields.

1

Preset

• Configuration

Event	Schedule	
1:1 authentication succeeded	Always	
1:1 authentication failed	Always	
1:1 duress authentication succeeded	Always	
1:N authentication succeeded	Always	
1:N authentication failed	Always	
1:N duress authentication succeeded	Always	
Dual authentication succeeded	Always	
Dual authentication failed	Always	
Authentication failed	Always	
Access denied	Always	
Administrator menu entered	Always	

+ Add

2

Delete Option

• Delete Option

None

3



User Profile Image Option

• Display user profile image when there is no image log for the events

☐

No.	Item	Description
1	Preset	It is possible to set the default setting to be used when adding an image log to the device. It is possible to add an event and schedule to delete by clicking + Add .

16 BioStar 2 Settings

No.	Item	Description
		 Note <ul style="list-style-type: none">▪ If there is no desired schedule, set a desired condition by clicking + Add Schedule.
2	Delete Option	<p>It is possible to set the delete condition of image log.</p> <ul style="list-style-type: none">▪ Delete Option: It is possible to set the condition to delete an image log.▪ Amount of Image Log: It is possible to set the unit of condition set at Delete Option.▪ Delete Cycle: It is possible to set the cycle to carry out the delete condition of image log set from Delete Option and Amount of Image Log.
3	User Profile Image Option	<p>If this option is on, the profile image registered for a user is displayed on the Event Log and Real-time Log pages when there are user related events. This option is particularly useful when you have devices that do not have a built-in camera.</p>  Note <ul style="list-style-type: none">▪ Even if the user profile image option is on, the image captured from the device camera is displayed when there is an image log for the event.

3) Click **Apply** to save the changes.

Note

- The default setting set from **Setting > Image Log** does not apply to the device. To add or change an image log of the device, refer to [Image Log](#).

USB Agent

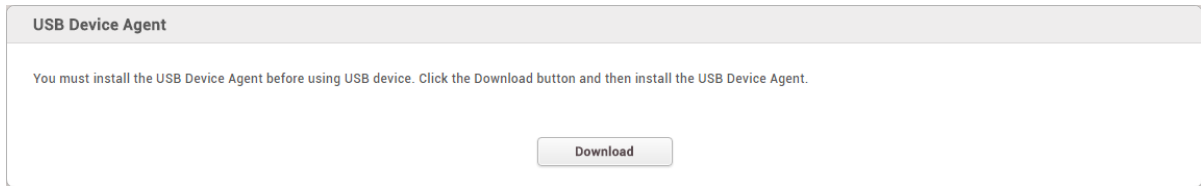
If you want to use the USB Device when logging into BioStar 2 from a client PC, installing the USB Device Agent is required.

Note

- If **User Account Control** is enabled in Windows, USB Agent cannot be run automatically. Disable the User Account Control or run as administrator.

16 BioStar 2 Settings

- 1) Click **Settings** > **USB AGENT**.
- 2) Download the file by clicking **Download**, and install it.



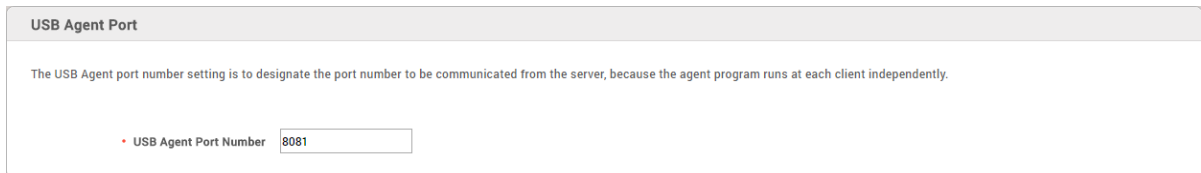
The screenshot shows a web interface titled "USB Device Agent". Below the title, there is a text instruction: "You must install the USB Device Agent before using USB device. Click the Download button and then install the USB Device Agent." At the bottom right of the panel, there is a button labeled "Download".

- 3) Select the byte order of USB card device.



The screenshot shows a web interface titled "Byte Order of USB Card Device". Below the title, there is a text instruction: "Byte order is applied to CSN card type only." Below this, there is a label "Byte Order" followed by a dropdown menu currently set to "MSB".

- 4) Set the port that the USB Agent will use.



The screenshot shows a web interface titled "USB Agent Port". Below the title, there is a text instruction: "The USB Agent port number setting is to designate the port number to be communicated from the server, because the agent program runs at each client independently." Below this, there is a label "USB Agent Port Number" followed by a text input field containing the value "8081".

- 5) Click **Apply** to save the changes.

Face Group Matching

Face group matching is the function used to specify a matching group based on the user groups set in BioStar 2 and authenticate users in that manner.

Note

- Up to 10 matching groups can be created.
- Each group can include up to 3,000 face templates.
- The total number of face templates in the matching group cannot exceed 5,000.

- 1) Click **Settings** > **Face Group Matching**.
- 2) Edit the necessary fields.

16 BioStar 2 Settings

General

1 — [• Group Matching ☒ Use

2 — [• Group Matching Device Settings

3 — [• Matching Group Settings

Device ID	Device Name	Device Group	IP Address	
4	FaceStation 2 4 (192.168.16.208)	All Devices	192.168.16.208	

+ Add

Order	Group Name	User Group	Number of Faces	
1 ▾	<input type="text" value="15F"/>	<input type="text" value="15F USER"/> ▾	4 / 3000	
2 ▾	<input type="text" value="16F"/>	<input type="text" value="16F USER"/> ▾	4 / 3000	
3 ▾	<input type="text" value="17F"/>	<input type="text" value="17F USER"/> ▾	1 / 3000	

+ Add

No.	Item	Description
1	Group Matching	<p>Set whether or not to use Group Matching.</p> <p> Note</p> <ul style="list-style-type: none">▪ To disable the group matching while it is being used, all devices set previously and the group settings must be deleted.
2	Group Matching Device Settings	<p>Set a device to use the group matching. Only FaceStation 2 can be added.</p>
3	Matching Group Settings	<p>Click + Add and set Group Name and User Group.</p> <p> Note</p> <ul style="list-style-type: none">▪ Up to 10 matching groups can be created.▪ A number of user groups can be set for one matching group.▪ If the number of face templates included in the user group exceeds 3,000, it cannot be set as a matching group.

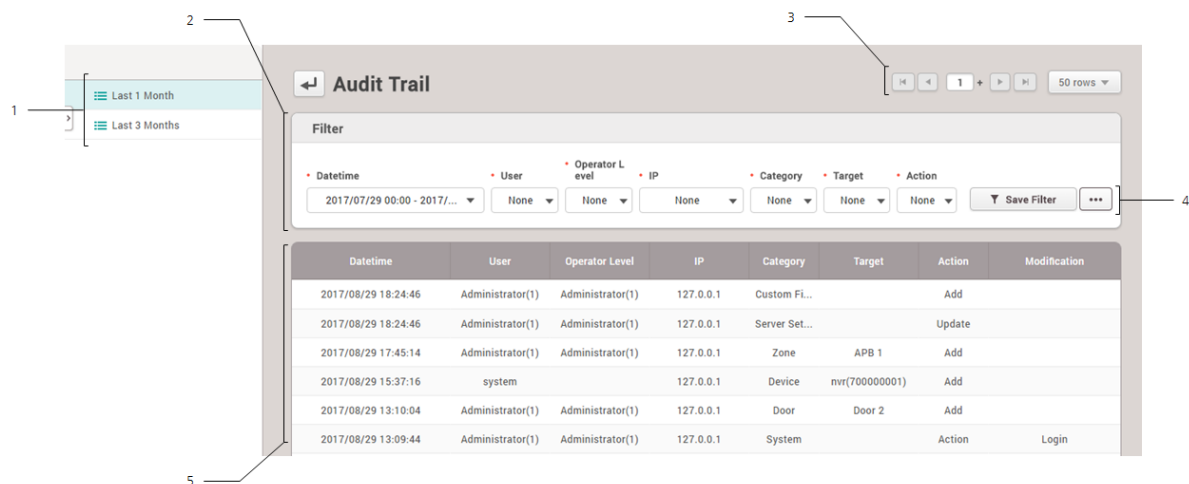
3) Click **Apply** to save the changes.

Audit Trail

Audit trail tracks user access information as well as all the information changed in the system. You can set a filter for each item for sorting.

1) Click **Settings > Audit Trail**.

16 BioStar 2 Settings



No.	Item	Description
1	Period	You can set the previous 1 month or 3 months conveniently for the period.
2	Filter	You can set conditions for each filter item. Click Save Filter to save the filter.
3	Page Navigation Buttons and Number of List Rows	<p>You can move a page or set the number of list rows to be displayed on one page.</p> <ul style="list-style-type: none">◀: Go to the first page.◀◀: Go to the previous page.2 / 2: Enter the page number to move to.▶▶: Go to the next page.▶: Go to the last page.25 rows ▼: Set the number of list rows to be displayed on one page.
4	Function Buttons (CSV Export, Column Setting)	You can save the list of audit list as a CSV file or changes the column setting.
5	Audit List	Shows the audit list.

Video

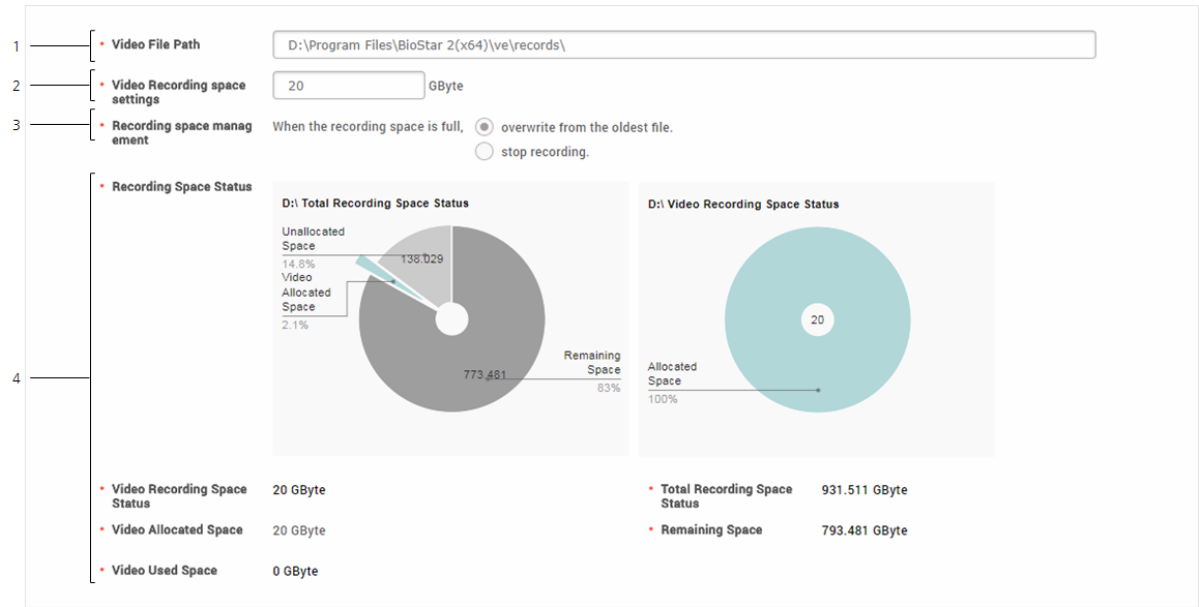
You can set the path to save video files and the storage duration.

 **Note**

- The **VIDEO** menu will appear when the Video license is activated.
- Use a separate storage media for the video log. Video logs might not be saved if the video storage space is reduced by the external processing(such as copying files and creating files),

16 BioStar 2 Settings

- 1) Click **Settings > Video**.
- 2) Edit the necessary items.



No.	Item	Description
1	Video File Path	You can change the path to save a video file. It is recommended to use a separate storage media for saving files securely.
2	Video Recording space settings	You can set the recording space to store video files.
3	Recording space management	If there is insufficient storage space, you can set the file processing method.
4	Recording Space Status	You can view the video storage space status.

- 3) Click **Apply** to save the changes.

Daylight Saving Time

Daylight Saving Time (DST) is a function that adjusts the time to better utilize natural daylight.

16 BioStar 2 Settings

- 1) Click **Settings** > **Daylight Saving Time**.
- 2) Click **+ Add**.
- 3) Edit the necessary items and click **Add**.

Add Daylight Saving Time

• Name

DST

• Start Date/Time

03

▼

Month

1

▼

Week

SUN

▼

Day of Week

01:00

▲

▼

• End Date/Time

11

▼

Month

2

▼

Week

SUN

▼

Day of Week

01:00

▲

▼

Add

Close

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

 **Note**

- You cannot edit or delete a daylight saving time that is already in use.

Security

You can set the password level and the maximum password age. You can also set the maximum invalid attempts and the maximum password change limit.

- 1) Click **Settings** > **SECURITY**.
- 2) Edit the necessary items.

— Login Password

Login Password

Password Level

Medium

Maximum Password Age

Inactive

Maximum Invalid Attempts




Inactive

Maximum Password Change Limit

Inactive

Item	Description
Password Level	<p>Set the policy for the password complexity for BioStar 2 login.</p> <ul style="list-style-type: none">▪ Low: You can enter up to 32 characters.

16 BioStar 2 Settings

Item	Description
	<ul style="list-style-type: none"> ▪ Medium: You must combine 8 to 32 alphabetic characters (a to z), numbers, and at least one alphabetic capital (A to Z). ▪ Strong: You must combine 10 to 32 alphabetic characters (a to z), numbers, at least one alphabetic capital (A to Z), and symbols. <p> Note</p> <ul style="list-style-type: none"> ▪ If Cloud Use set to Use, you can only use Medium or Strong.
Maximum Password Age	<p>You can set the period for which you want to use the password. If the Maximum Password Age is exceeded, a password change request message is displayed at login.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ You can set the Maximum Password Age from 1 day to 180 days.
Maximum Invalid Attempts	<p>You can set the Maximum Invalid Attempts and the time limit. If you enter the wrong password more than the set number of times, you will not be able to log in for the time limit.</p>
Maximum Password Change Limit	<p>You can set the Maximum Password Change Limit.</p> <p> Note</p> <ul style="list-style-type: none"> ▪ You can set the Maximum Password Change Limit up to 10 times.

— Advanced Security Settings

Advanced Security Settings

• Encrypt Personal Data on Database

☒ Use

• Personal Data Encryption Key

Change

• Secure communication with device

☒ Use

• Use external certificates




☐ Not Use

• Device Hashkey Management

☐ Not Use

Item	Description
Encrypt Personal Data on Database	<p>When Use is set for Encrypt Personal Data on Database, all sensitive data including credential data and personal information will be stored in the database as encrypted. If this option is set as Not Use, the encrypted data will be decrypted and the user's personal information will be stored in an unencrypted state.</p>

16 BioStar 2 Settings

Item	Description
	<p> Note</p> <ul style="list-style-type: none"> Items to be encrypted when using Encrypt Personal Data on Database are as follows. <ul style="list-style-type: none"> - Profile image - User ID - Name - Phone number - User IP - Email information for sender and recipients - Login ID - Login password - Face template - Fingerprint template - Card ID - Smart card layout key - Custom information for user and visitor - Image log files
Personal Data Encryption Key	<p>You can set the personal data encryption key. Click Change and set a new encryption key. If changing the encryption key, the existing data will be re-encrypted.</p> <p> Note</p> <ul style="list-style-type: none"> You can enter the encryption key with 32 characters using letters, numbers, and symbols.
Secure communication with device	<p>The communication between BioStar 2 and a device can be protected using a certificate.</p> <p>When Use is set for Secure communication with device, BioStar 2 creates and sends a certificate to the device. The device can use a secure channel for exchanging data with BioStar 2 using this certificate. In order to use an external certificate, Root certificate, Public key certificate, and Private key files must be uploaded.</p> <p>If Device Hashkey Management set to Use, you can set a new data encryption key and administrator password.</p> <p> Note</p> <ul style="list-style-type: none"> The devices and the firmware versions where the secure communication can be set are as follows. <ul style="list-style-type: none"> - FaceStation 2 FW 1.1.0 or later - BioStation A2 FW 1.5.0 or later - BioStation 2 FW 1.6.0 or later

16 BioStar 2 Settings

Item	Description
	<ul style="list-style-type: none"> - BioStation L2 FW 1.3.0 or later - BioLite N2 FW 1.0.0 or later - BioEntry P2 FW 1.1.0 or later - BioEntry W2 FW 1.2.0 or later - FaceLite FW 1.0.0 or later - XPass 2 FW 1.0.0 or later - CoreStation FW 1.1.0 or later <ul style="list-style-type: none"> ▪ BioStar 2 creates or deletes a certificate according to the setting status of Secure communication with device, and the same certificate as the previous certificate will not be created. For example, if the setting of Secure communication with device is changed in the order of [Use - Not Use], the created certificate will be deleted automatically. When the setting is changed in the order of [Use - Not Use - Use], the operation of [Create A certificate - Delete A certificate - Create B certificate] is carried out. ▪ If the device is disconnected from the network physically while using the secure communication of BioStar 2, do not turn off the secure communication option. In such a case, the certificate of BioStar 2 will be deleted, and the device will not be able to connect again. To connect it again, the certificate saved in the device must be deleted or the device must be reset to factory default. For more details, refer to the manual of the device.

Session Security



Item	Description
Simultaneous Connection Allow	You can set whether to allow simultaneous connections using the same account. If you set Simultaneous Connection Allow to Inactive , a previously logged in user will be logged out when attempting to connect to the same account simultaneously.

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

16 BioStar 2 Settings

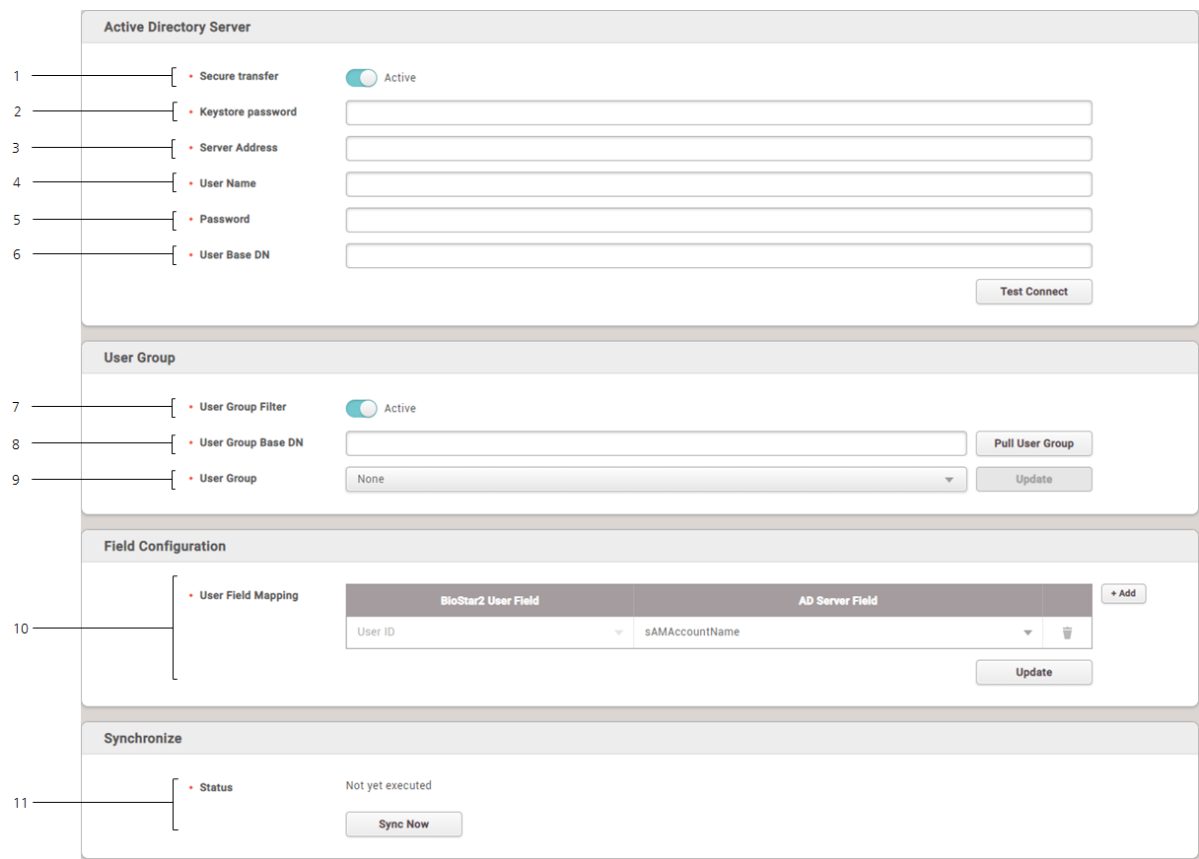
Active Directory

You can synchronize user data stored in Microsoft Windows Active Directory to BioStar 2.

 **Note**

- The Active Directory setting will appear when the AC Advanced license is activated.
- The Active Directory is available for a system environment with Windows Server 2008 R2 or later.
- To use the Active Directory, set the **User ID Type** to **Alphanumeric** by referring to [User/Device Management](#).

- 1) Click **Settings > ACTIVE DIRECTORY**.
- 2) Edit the necessary items.




The screenshot shows the 'Active Directory' configuration page. It has four main sections: 'Active Directory Server', 'User Group', 'Field Configuration', and 'Synchronize'. Numbered callouts 1 through 11 point to specific settings:

- 1: Secure transfer toggle (Active)
- 2: Keystore password field
- 3: Server Address field
- 4: User Name field
- 5: Password field
- 6: User Base DN field
- 7: User Group Filter toggle (Active)
- 8: User Group Base DN field
- 9: User Group dropdown (None)
- 10: User Field Mapping table with columns 'BioStar2 User Field' and 'AD Server Field'. It shows 'User ID' mapped to 'sAMAccountName'.
- 11: Synchronize Status (Not yet executed)

No.	Item	Description
1	Secure transfer	You can use the encryption when communicating with a Windows Active Directory server. Install Active Directory Certificate Services and set the keystore password by referring to Active Directory Encryption .
2	Keystore password	Enter the Windows Active Directory server encryption key store password. This can be only used when activating the Secure transfer .

16 BioStar 2 Settings

No.	Item	Description															
3	Server Address	Enter the server address for Windows Active Directory.															
4	User Name	Enter the user name used by Windows Active Directory.															
5	Password	Enter the password used by Windows Active Directory.															
6	Base DN	<p>Enter the base domain name for Windows Active Directory.</p> <p>You can find the base domain name in the following way.</p> <p>a) Run the Active Directory Administrative Center.</p> <p>b) Right-click on the node where user data is stored, and then click Property.</p> <p>c) In the property window, click Expand and then click Attribute Editor.</p> <p>d) View the value of distributedName.</p>															
7	User Group Filter	You can enable or disable synchronization by user group.															
8	User Group Base DN	Enter the base domain name of the user group for Windows Active Directory. This can be only used when activating the User Group Filter .															
9	User Group	Select the user group to synchronize. This can be only used when activating the User Group Filter .															
10	User Field Mapping	<p>You can map data fields in Windows Active Directory to user fields in BioStar 2.</p> <p>The user fields to be mapped can be set as shown below.</p> <div> <div>• User Field Mapping</div> <table> <thead> <tr> <th>BioStar2 User Field</th><th>AD Server Field</th><th></th></tr> </thead> <tbody> <tr> <td>User ID</td><td>sAMAccountName</td><td>⌵ ⌵</td></tr> <tr> <td>User Name</td><td>displayName</td><td>⌵ ⌵</td></tr> <tr> <td>Email</td><td>mail</td><td>⌵ ⌵</td></tr> <tr> <td>Telephone</td><td>telephoneNumber</td><td>⌵ ⌵</td></tr> </tbody> </table> <div>+ Add</div> <div>Update</div> </div> <p>a) Click + Add to add a user field slot.</p> <p>b) Set the BioStar 2 User Field and AD Server Field to map the correct data to the user field in BioStar 2.</p> <p>c) Click Update to apply user field mapping settings.</p> <p> Note</p> <ul style="list-style-type: none"> The User ID field is a static item and cannot be deleted. 	BioStar2 User Field	AD Server Field		User ID	sAMAccountName	⌵ ⌵	User Name	displayName	⌵ ⌵	Email	mail	⌵ ⌵	Telephone	telephoneNumber	⌵ ⌵
BioStar2 User Field	AD Server Field																
User ID	sAMAccountName	⌵ ⌵															
User Name	displayName	⌵ ⌵															
Email	mail	⌵ ⌵															
Telephone	telephoneNumber	⌵ ⌵															
11	Synchronize	Click Sync Now to synchronize the user data. The last synchronization time and date are displayed.															

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

16 BioStar 2 Settings

Active Directory Encryption

You can use the encryption when communicating with a Windows Active Directory server.
Set according to the following order when using the encryption for the first time.

Step 1. Installing Active Directory Certificate Services

To use Windows Active Directory server encryption communication, you must install the Active Directory Certificate Services.

The Active Directory Certificate Services can be installed as follows:

- 1) On the PC where the Windows Active Directory server is installed, run **Server Manager**, and then click **Manage > Add Roles and Features**.
- 2) On **Before You Begin**, click **Next**.
- 3) On **Select Installation Type**, select **Role-Based or feature-based installation** and then click **Next**.
- 4) On **Select destination server**, select **Select a server from the server pool**, check the server, and click **Next**.
- 5) On **Select Server Roles**, select **Active Directory Certificate Services** and click **Next**.
- 6) When a pop-up window appears, view the details and click **Add Features > Next**.
- 7) View the details of **Active Directory Certificate Services** and click **Next**.
- 8) On **Confirm installation selections**, click **Install**. When installation is complete, click **Configure Active Directory Certificate Services on the destination server**.
- 9) When **AD CS Configuration wizard** appears, view the details and click **Next**.
- 10) On **Role Services**, click **Certification Authority > Next**.
- 11) On the **Setup Type** page, select **Enterprise CA** and click **Next**.
- 12) On the **Specify the type of the CA** page, select **Root CA** and click **Next**.
- 13) On the **Specify the type of the private key** page, select **Create a new private key** and click **Next**.
- 14) Set the **Cryptography for CA**, **CA Name**, and **Validity Period**, and then click **Next**.
- 15) On the **CA Database** page, set the **folder location for the certificate database** and the **certificate database log** and then click **Next**.
- 16) On **Confirmation** page, view the details of Active Directory Certificate Services and click **Configure**.

Step 2. Connecting IDAPS

- 1) Click **Start > Run**.
- 2) Enter **ldp** in the input field.
- 3) When the **Ldp-disconnected** window appears, click **Connect**.

16 BioStar 2 Settings

- 4) Fill in **Server** and **Port** fields and select **SSL**. And then click **OK**.

Step 3. Copying the root certificate

- 1) Run Command Prompt on the PC where the Windows Active Directory server is installed.
- 2) Enter **certutil -ca.cert client.crt** command to copy the root certificate.
- 3) Enter **keytool -import -keystore ad.jks -file client.crt** command to convert the server certificate to .jks format.
- 4) Save the .jks-formatted server certificate to the BioStar 2 installation path.

Visitor

You can configure visiting sites and PCs. You can also set the terms and conditions for visitors. And You can create the information fields that you want to know from the visitors by using the Custom Visitor Field.

 **Note**

- The **VISITOR** setting will appear when the Visitor license is activated.
- Activate the **Automatic User Synchronization** or **Use Server Matching** option to use the **VISITOR**.

- 1) Click **Settings > VISITOR**.
- 2) Set the necessary items.

Site Settings

Site Settings

• Site


Name	Access Group	Card Use	Card Type	Card Data Format	
Suprema 01	Acces...	<input checked="" type="checkbox"/>	CSN	None	
Suprema 02	Acces...	<input checked="" type="checkbox"/>	Wiegand	26 bit ...	

+ Add

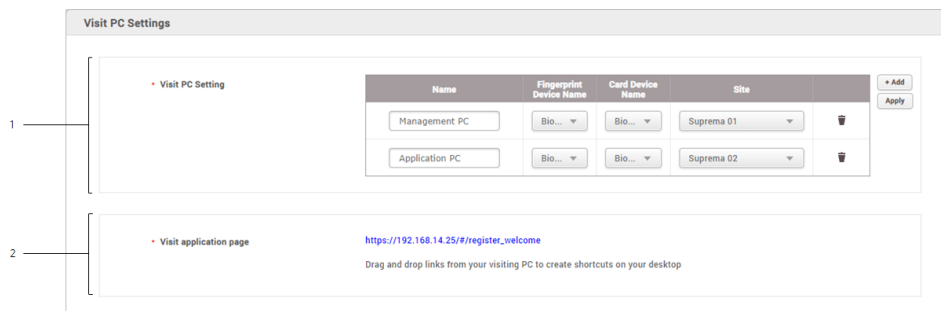
Apply


Item	Description
Site	<p>You can set the access group to use in the visiting PC and managing PC of each site.</p> <p>You can also set whether or not to use cards. If you are using a card, you can also set Card Type and Card Data Format.</p> <ul style="list-style-type: none">▪ Name: You can set the name of site.▪ Access Group: You can select the access group to assign to the visitor.▪ Card Use: You can set whether or not to use a card.▪ Card Type: You can select the type of card to use in the site. The

16 BioStar 2 Settings

Item	Description
	<p>card type is activated only when you select Card Use.</p> <ul style="list-style-type: none"> ▪ Card Data Format: You can configure the format for reading card data. The Card Data Format is activated only when you set the Card Type to Wiegand. <p> Note</p> <ul style="list-style-type: none"> ▪ Up to 48 characters may be entered for a site name. <p>Click Apply to save the setting of the site.</p>

Visit PC Settings



No	Item	Description
1	Visit PC Setting	<p>You can set the visiting PC and managing PC.</p> <ul style="list-style-type: none"> ▪ Name: You can set the name of the visiting PC and managing PC. ▪ Fingerprint Device Name: Select a device to enroll visitors' fingerprints when visitors access the site using the fingerprint authentication. ▪ Card Device Name: Select a device to issue the card to visitors when visitors access the site using the card authentication. ▪ Site: Select a site to manage the visit on the visiting PC. <p> Note</p> <ul style="list-style-type: none"> ▪ Up to 48 characters may be entered for a name of the visiting PC. ▪ You can use the fingerprint and card device at the same time. You can select only one for each. ▪ You can only select one site per PC.

16 BioStar 2 Settings

No.	Item	Description
		Click Apply to save the setting of the Visit PC Setting.
2	Visit application page	You can create a shortcut icon of Visit application page on the desktop of the visiting PC. Drag and drop the link to the desktop of the visiting PC.

Visit PC Select

Visit PC Select

Visit PC Select

Visiting PC

Apply

Item	Description
Visit PC Select	You can select the PC set in Visit PC Setting and assign it to the current PC. Click Apply to save the setting.

Terms & Visitor Settings

Terms & Visitor Settings

Accept Terms and Conditions Settings

1

Insert your Terms and Access Conditions

Apply

2

Insert your sentence of Accept Terms and Conditions

Insert your Privacy Policy

Insert your sentence of Accept Privacy Policy

3

Allowed period for credential

365

Day(s)

Visitor Settings

4

Guide to Completion of Visit



Please fill in the instructions when you complete your visit

5








Default access period for visitor

1

Day(s)

No.	Item	Description
1	Terms and Conditions	You can set the terms and conditions for visitors. Click  to activate the input field and enter the contents of terms and conditions.  Note <ul style="list-style-type: none">Up to 65,535 characters may be entered for

16 BioStar 2 Settings

No	Item	Description
		<p>the sentence of terms and conditions.</p> <ul style="list-style-type: none"> Up to 64 characters may be entered for the sentence of accept terms and conditions.
2	Privacy Policy	<p>You can set the privacy policy for visitors.</p> <p>Click  to activate the input field and enter the privacy policy.</p> <p> Note</p> <ul style="list-style-type: none"> Up to 65,535 characters may be entered for the sentence of privacy policy. Up to 64 characters may be entered for the sentence of accept privacy policy.
3	Allowed period for credential	<p>You can set the period for keeping personal data that visitors provide when they visit.</p> <p>Click  to activate the input field and enter the number of days to keep personal data.</p> <p> Note</p> <ul style="list-style-type: none"> You can delete the visitors that have the personal data expired in VISITOR menu.
4	Guide to Completion of Visit	<p>You can set the guide to appear on the screen as a pop-up when a visitor completes an application for a visit.</p> <p>Click  to activate the input field and enter the guide for visitors.</p> <p> Note</p> <ul style="list-style-type: none"> Up to 65,535 characters may be entered for the sentence of guide. If you do not enter the sentence of a guide, nothing will be displayed on the screen when visitors complete their visit application.
5	Default access period for visitor	<p>You can set the access period for visitors.</p> <p>Click  to activate the input field and enter the default access period for visitors.</p>

16 BioStar 2 Settings

Custom Visitor Field

Custom Visitor Field

Custom Visitor Field Settings

Order	Name	Type	Data	
1	purpose of visit	Text Input Box		

+ Add

Apply

Item	Description
Custom Visitor Field Settings	<p>You can add custom visitor fields for extra visitor information and these fields appear on the visit application page.</p> <ul style="list-style-type: none">▪ Order: You can set the order of the Custom Visitor Field.▪ Name: You can set the name of the Custom Visitor Field.▪ Type: You can choose the Text Input Box, Number Input Box or Combo Box.▪ Data: Enter the options to appear in the combo boxes. Each item is separated by a semicolon (;). Data is only activated when Type is set to Combo Box. <div><div><div>📋</div><div>Note</div></div><ul style="list-style-type: none">▪ For a Text Input Box, characters and numbers are allowed.<div><div>Purpose of visit</div><div></div></div>▪ For a Number Input Box, numbers are allowed and characters are not allowed.<div><div>Number of visitors</div><div></div></div>▪ For a Combo Box, the items that have been set to the field are displayed as item. If you want to configure a combo box field as shown in the screenshot below, you need to enter Option 1;Option 2;Option 3;Option 4 in the data field.<div><div>Option</div><div><div>None</div><div>None</div><div>Option1</div><div>Option2</div><div>Option3</div><div>Option4</div></div></div><div>Click Apply to save the setting of the Custom Visitor Field.</div></div>

Mobile Access

By linking BioStar 2 and Airfob Portal, you can issue the mobile access cards to users in BioStar 2. Users can be issued mobile access cards through a link received by email or SMS without signing up for

16 BioStar 2 Settings

Airfob Portal or registering mobile access cards separately.

Note

- The devices and the firmware versions that can use the mobile access are as follows.
 - XPass 2 FW 1.1.0 or later
 - XPass D2(Rev 2) FW 1.4.0 or later
 - BioLite N2 FW 1.3.0 or later
 - BioEntry W2(Rev 2) FW 1.6.0 or later

You can set up Suprema Mobile Access as shown below.

Step 1. Join Airfob Portal and open site

In Airfob Portal, you can set up mobile access cards and registration devices, and manage sites and credits.

Related information

[Airfob Portal](#)

Step 2. Configure the Mobile Access in BioStar 2

You can set whether to use the mobile access and manage settings related to Airfob Portal.
You can also register devices to use mobile access cards.

Related information

[Configuring Mobile Access](#)

Step 3. Registering Devices

You can register devices to use mobile access directly from the Airfob Pass application or BioStar 2.

Related information

[Configuring Mobile Access](#)

Step 4. Issuing Mobile Access Card

You can issue mobile access cards to users registered with BioStar 2.

16 BioStar 2 Settings

To issue a mobile access card to a user, you must enter user information based on the messaging option.

Related information

[Adding User Information](#)

[Enroll Mobile Access Card](#)

Airfob Portal

In Airfob Portal, you can set up mobile access cards and registration devices, and manage sites and credits.

- 1) Access the Airfob Portal(<https://mc.suprema.io>).
- 2) Click **Get Started** to sign up and create a site.
- 3) Enter the Airfob Portal administrator's email address in the Email input field and click **Get Started**. The authentication code will be sent to the email address you entered.
- 4) Enter the authentication code you received in the authentication code field and click **Confirm**.

Note

- The authentication code is a 6 digit number.

- 5) Check the Privacy and Terms and click **Agree**.
- 6) Set the password and nickname to use in the Airfob Portal and click **Create Account**. Creating the account will be completed.
- 7) Click **Sign In**.
- 8) Enter the email and password, then click **Sign In**.
- 9) Click **Create Site** to open the site.

Note

- Site means an organization or company that uses the mobile access.

- 10) Set the name and country of the site, and then click **Next**.
- 11) Select the site type.

Note

- You can select types either **Dynamic** or **Regular** depending on the type of sites or situations.
 - **Dynamic**: This type allows you to reissue, revoke, or stop mobile access cards or specify the expiration date of it. It deducts credits according to the period of use or devices. Dynamic can be used in gyms, libraries, or shared facilities where it provides membership services.

16 BioStar 2 Settings

- **Regular:** This type can be used permanently until an administrator deletes the access authority. It deducts credits according to the number of issuances. Regular can be used in companies as employee ID cards or access cards.

- 12) Click **Create**. Creating the site will be completed.
- 13) Click the site name to access the Airfob Portal of the site.

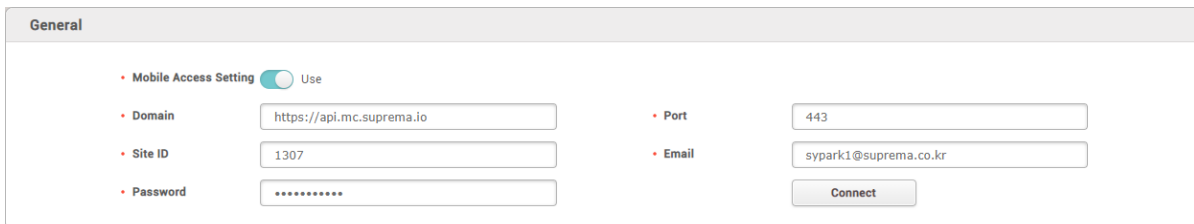
Note


- For more information on using the Airfob Portal, see the Airfob Portal(<https://mc.suprema.io>).

Configuring Mobile Access

You can set whether to use the mobile access and manage settings related to Airfob Portal.
You can also register devices to use mobile access cards.

- 1) Click **Settings > MOBILE ACCESS**.
- 2) Edit the necessary items.



Item	Description
General	<ul style="list-style-type: none">▪ Mobile Access Setting: You can set whether to use the mobile access. If you set the Mobile Access Setting to Use, you can issue mobile access cards to users. <p> Note</p> <ul style="list-style-type: none">▪ To use Mobile Access with BioStar 2, complete the Airfob Portal sign-up and initial setup first.▪ BioStar 2 only supports regular card sites. <ul style="list-style-type: none">▪ Domain: You can see the domain address of the Airfob Portal.▪ Port: You can see the port number of the Airfob Portal.▪ Site ID: Enter the site ID that you created in the Airfob Portal. You can find the site ID in the Site & License menu of the Airfob Portal.▪ Email: Enter the email address of the mobile access administrator.▪ Password: Enter the password of the mobile access administrator.▪ Device Registration: You can register devices to use the mobile access. Device Registration appears when you complete entering the Domain, Port, Site ID, Email, and Password, and then click Connect to successfully connect to the Airfob Portal.

16 BioStar 2 Settings

Item

Description

• Device Registration

Device ID	Device Name	Device Group	IP Address	
Not found				

Click **+ Add** to add devices to use the mobile access. The list of devices registered in BioStar 2 is displayed.

Enrollment Device

50 rows

Go

	Device ID	Name	Group	IP Address
<input type="checkbox"/>	547832712	FaceLite 547832712 (192.168.14.240)	All Devices	192.168.14.240
<input type="checkbox"/>	547833190	Xpass2 Keypad 547833190 (192.168.14.233)	All Devices	192.168.14.233



Add

Close

Select the device and click **Add**.

• Device Registration

Device ID	Device Name	Device Group	IP Address	
547833190	Xpass2 Keypad 547833190 (192.168.14.233)	All Devices	192.168.14.233	<div><div></div><div></div></div>

The devices that have been added to the list of devices are displayed. Click  to resend the mobile access certificate. Click  to delete the registered device.

Note

- The devices and the firmware versions that can use the mobile access are as follows.
 - XPass 2 FW 1.1.0 or later
 - XPass D2(Rev 2) FW 1.4.0 or later
 - BioLite N2 FW 1.3.0 or later
 - BioEntry W2(Rev 2) FW 1.6.0 or later
- You can also register devices using the Airfob Pass application.
- If you delete the registered device, the mobile access certificate sent to the device will be deleted.

Email Contents

You can set contents such as title, body, and signature of email to which the visual face mobile

16 BioStar 2 Settings

enrollment link will be sent.

 **Note**

- Before setting an email contents, activate the **Cloud**. The Cloud will available when the Standard or higher license is activated.
- Enter user's email address in the **user information** to use visual face mobile enrollment.

- 1) Click **Settings > EMAIL CONTENTS**.
- 2) Edit the necessary items.

Email Contents Setting

1

Email Title

2

Email Body

3

Email Signature

4

SMTP Setting

SMTP setting

5

Test Mail Recipient Address

Send Email

No.	Item	Description
1	Email Title	Enter the title of the email.
2	Email Body	Enter the body of the email.
3	Email Signature	Enter the signature of the email.
4	SMTP Setting	Set the SMTP(Simple Mail Transfer Protocol) for sending emails.

16 BioStar 2 Settings

No.	Item	Description
		<div> <div>SMTP Option ×</div> <div> <div>Sender Information</div> <ul style="list-style-type: none"> • SMTP Server Name <input type="text"/> • Description <input type="text"/> • Server Address <input type="text"/> • Port(default:25) <input type="text" value="25"/> • User Name <input type="text"/> • Password <input type="password"/> • Security Type <input type="text" value="SSL"/> • Sender <input type="text"/> <div> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </div> </div> <ul style="list-style-type: none"> ▪ SMTP Server Name: Enter the SMTP server name. ▪ Description: Enter the description. ▪ Server Address: Enter the SMTP server address. SMTP server address is the same form as 'smtp. Email Service Provider.com', and you can check it on the settings screen of email to use as an SMTP . ▪ Port(default:25): Enter the port number of the SMTP server. you can check it on the settings screen of email to use as an SMTP. ▪ User Name: Enter the account of the SMTP service. ▪ Password: Enter the password of the SMTP service. ▪ Security Type: Select security type. ▪ Sender: Enter the email address of the sender. <p><input checked="" type="checkbox"/> Note</p> <ul style="list-style-type: none"> ▪ For more information on SMTP information, contact your system administrator. </div>
5	Test Mail Recipient Address	Enter an email address to receive the test email and click Send Email .

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

17 Troubleshooting

For any inquiries or technical support concerning BioStar 2, please contact the Suprema Technical Support Team (support.supremainc.com).

For efficient technical support, please provide the following information.

- Company name, your name and job title, country information (regional information), contact information and the best time to reach you
- Current BioStar 2 version and device models (examples: BioStar 2 V1.0.233, BioLite Net)
- Details of the error message
- BioStar 2 system log
- Description of your symptom and problem

This section provides the disclaimers, copyright notice, and software end user license agreement of Suprema.

[Disclaimers](#)

[Copyright Notice](#)

[Open Source License](#)

[Software End User License Agreement\(EULA\)](#)

Disclaimers

- The information contained in this Guide is provided in regard to the Suprema product.
- Your right of usage is recognized only for products included in sales agreements and conditions guaranteed by Suprema. No license rights over other intellectual properties mentioned in this Guide are recognized.
- Suprema makes no representations or warranties concerning infringement of patents, copyrights or other intellectual property rights as well as merchantability and fitness of the product for a particular purpose in regard to the sale or use of the Suprema product.
- Do not use the Suprema product in medical, life-saving and life-sustaining situations or in situations where malfunction of the product could lead to personal injury or loss of life. However, if an accident occurs while the purchaser is using the product in any of the situations stated above, even if shortcomings are discovered in the design or production process of the product and are claimed as a point of major negligence, employees, subsidiaries, branches, affiliates, or distributors of Suprema shall not be liable and shall not

18 Appendix

make reimbursements for any direct or indirect costs or expenses associated, including lawyer fees.

- Suprema may change the product standards and specifications at any time without any adequate notice for improvements in stability, performance or design of the product. Designers should keep in mind that features or descriptions marked as 'to be implemented' or 'to be defined' are always subject to change. Suprema will implement or define such features or descriptions in a near future and shall not be liable for any consequent problems, including problems of compatibility.
- If you wish to obtain the latest specification documentation before you place an order for the product, please contact Suprema, a sales agent of Suprema or a regional distributor.

Copyright Notice

Copyright of this documentation is reserved by Suprema. All other product names, trademarks, registered trademarks are the property of their respective owners.

Open Source License

MariaDB LGPL client libraries for C and Java

The LGPL license

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts
as the successor of the GNU Library Public License, version 2, hence
the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom
to share and change it. By contrast, the GNU General Public Licenses
are intended to guarantee your freedom to share and change free

18 Appendix

software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of

18 Appendix

any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

18 Appendix

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run. **TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION**

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and

18 Appendix

what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- * a) The modified work must itself be a software library.
- * b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- * c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- * d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If

18 Appendix

identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

18 Appendix

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

18 Appendix

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- * a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)
- * b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.
- * c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- * d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- * e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is

18 Appendix

normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

- * a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
- * b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

18 Appendix

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the

18 Appendix

original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU

18 Appendix

FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. END OF TERMS AND CONDITIONS.

MariaDB Server

The GPL license

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

=====

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

18 Appendix

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

18 Appendix

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
 - a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
 - b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
 - c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required

18 Appendix

to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
 - a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - b. Accompany it with a written offer, valid for at least three years, to give any third-party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you

18 Appendix

received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance

18 Appendix

by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY

18 Appendix

OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

=====

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

ONE LINE TO GIVE THE PROGRAM'S NAME AND A BRIEF IDEA OF WHAT IT DOES.
Copyright (C) YYYY NAME OF AUTHOR

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19YY NAME OF AUTHOR
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it

18 Appendix

under certain conditions; type ``show c'` for details.

The hypothetical commands ``show w'` and ``show c'` should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ``show w'` and ``show c'`; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
``Gnomovision'` (which makes passes at compilers) written by James Hacker.

SIGNATURE OF TY COON, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Node.js

Node.js is licensed for use as follows:

''''

Copyright Node.js contributors. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR

18 Appendix

IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This license applies to parts of Node.js originating from the <https://github.com/joyent/node> repository:

Copyright Joyent, Inc. and other Node contributors. All rights reserved. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

The Node.js license applies to all parts of Node.js that are not externally maintained libraries.

The externally maintained libraries used by Node.js are:

- c-ares, located at `deps/cares`, is licensed as follows:

Copyright 1998 by the Massachusetts Institute of Technology.
Copyright (C) 2007-2013 by Daniel Stenberg

Permission to use, copy, modify, and distribute this

18 Appendix

software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

- HTTP Parser, located at `deps/http_parser`, is licensed as follows:

`http_parser.c` is based on `src/http/nginx_http_parse.c` from NGINX copyright Igor Sysoev.

Additional changes are licensed under the same terms as NGINX and copyright Joyent, Inc. and other Node contributors. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

- ICU, located at `deps/icu`, is licensed as follows:

ICU License - ICU 1.8.1 and later

18 Appendix

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1995-2016 International Business Machines Corporation and others

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

All trademarks and registered trademarks mentioned herein are the property of their respective owners.

Third-Party Software Licenses

This section contains third-party software notices and/or additional terms for licensed third-party software components included within ICU libraries.

1. Unicode Data Files and Software

COPYRIGHT AND PERMISSION NOTICE

Copyright © 1991-2016 Unicode, Inc. All rights reserved.

Distributed under the Terms of Use in

<http://www.unicode.org/copyright.html>.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the "Data Files") or Unicode software and any associated documentation (the "Software") to deal in the Data Files or Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Data Files or Software, and to permit persons to whom the Data Files or Software are furnished to do so, provided that

(a) this copyright and permission notice appear with all copies of the Data Files or Software,

(b) this copyright and permission notice appear in associated documentation, and

(c) there is clear notice in each modified Data File or in the Software as well as in the documentation associated with the Data File(s) or Software that the data or software has been modified.

THE DATA FILES AND SOFTWARE ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS.

IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in these Data Files or Software without prior written authorization of the copyright holder.

2. Chinese/Japanese Word Break Dictionary Data (cjdict.txt)

The Google Chrome software developed by Google is licensed under
the BSD license. Other software included in this distribution is

18 Appendix

```
# provided under other licenses, as set forth below.
#
# The BSD License
# http://opensource.org/licenses/bsd-license.php
# Copyright (C) 2006-2008, Google Inc.
#
# All rights reserved.
#
# Redistribution and use in source and binary forms, with or without
# modification, are permitted provided that the following conditions are met:
#
# Redistributions of source code must retain the above copyright notice,
# this list of conditions and the following disclaimer.
# Redistributions in binary form must reproduce the above
# copyright notice, this list of conditions and the following
# disclaimer in the documentation and/or other materials provided with
# the distribution.
# Neither the name of Google Inc. nor the names of its
# contributors may be used to endorse or promote products derived from
# this software without specific prior written permission.
#
#
# THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
# CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES,
# INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
# MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
# DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE
# LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
# CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
# SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
# BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
# LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
# NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
# SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
#
#
# The word list in cjdict.txt are generated by combining three word lists
# listed below with further processing for compound word breaking. The
# frequency is generated with an iterative training against Google web
# corpora.
#
# * Libtabe (Chinese)
# - https://sourceforge.net/project/?group\_id=1519
```

18 Appendix

```
# - Its license terms and conditions are shown below.
#
# * IPADIC (Japanese)
# - http://chasen.aist-nara.ac.jp/chasen/distribution.html
# - Its license terms and conditions are shown below.
#
# -----COPYING.libtabe ---- BEGIN-----
#
# /*
# * Copyright (c) 1999 TaBE Project.
# * Copyright (c) 1999 Pai-Hsiang Hsiao.
# * All rights reserved.
# *
# * Redistribution and use in source and binary forms, with or without
# * modification, are permitted provided that the following conditions
# * are met:
# *
# * . Redistributions of source code must retain the above copyright
# * notice, this list of conditions and the following disclaimer.
# * . Redistributions in binary form must reproduce the above copyright
# * notice, this list of conditions and the following disclaimer in
# * the documentation and/or other materials provided with the
# * distribution.
# * . Neither the name of the TaBE Project nor the names of its
# * contributors may be used to endorse or promote products derived
# * from this software without specific prior written permission.
# *
# * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
# * "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
# * LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS
# * FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE
# * REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
# * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
# * (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
# * SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
# * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
# * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
# * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
# * OF THE POSSIBILITY OF SUCH DAMAGE.
# */
#
# /*
# * Copyright (c) 1999 Computer Systems and Communication Lab,
```

18 Appendix

```
# *      Institute of Information Science, Academia
# *      Sinica. All rights reserved.
# *
# * Redistribution and use in source and binary forms, with or without
# * modification, are permitted provided that the following conditions
# * are met:
# *
# * . Redistributions of source code must retain the above copyright
# * notice, this list of conditions and the following disclaimer.
# * . Redistributions in binary form must reproduce the above copyright
# * notice, this list of conditions and the following disclaimer in
# * the documentation and/or other materials provided with the
# * distribution.
# * . Neither the name of the Computer Systems and Communication Lab
# * nor the names of its contributors may be used to endorse or
# * promote products derived from this software without specific
# * prior written permission.
# *
# * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
# * "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
# * LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS
# * FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE
# * REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
# * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
# * (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
# * SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
# * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
# * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
# * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
# * OF THE POSSIBILITY OF SUCH DAMAGE.
# */
#
# Copyright 1996 Chih-Hao Tsai @ Beckman Institute,
# University of Illinois
# c-tsai4@uiuc.edu http://casper.beckman.uiuc.edu/~c-tsai4
#
# -----COPYING.libtabe-----END-----
#
#
# -----COPYING.ipadic-----BEGIN-----
#
# Copyright 2000, 2001, 2002, 2003 Nara Institute of Science
# and Technology. All Rights Reserved.
```

18 Appendix

```
#
# Use, reproduction, and distribution of this software is permitted.
# Any copy of this software, whether in its original form or modified,
# must include both the above copyright notice and the following
# paragraphs.
#
# Nara Institute of Science and Technology (NAIST),
# the copyright holders, disclaims all warranties with regard to this
# software, including all implied warranties of merchantability and
# fitness, in no event shall NAIST be liable for
# any special, indirect or consequential damages or any damages
# whatsoever resulting from loss of use, data or profits, whether in an
# action of contract, negligence or other tortuous action, arising out
# of or in connection with the use or performance of this software.
#
# A large portion of the dictionary entries
# originate from ICOT Free Software. The following conditions for ICOT
# Free Software applies to the current dictionary as well.
#
# Each User may also freely distribute the Program, whether in its
# original form or modified, to any third party or parties, PROVIDED
# that the provisions of Section 3 ("NO WARRANTY") will ALWAYS appear
# on, or be attached to, the Program, which is distributed substantially
# in the same form as set out herein and that such intended
# distribution, if actually made, will neither violate or otherwise
# contravene any of the laws and regulations of the countries having
# jurisdiction over the User or the intended distribution itself.
#
# NO WARRANTY
#
# The program was produced on an experimental basis in the course of the
# research and development conducted during the project and is provided
# to users as so produced on an experimental basis. Accordingly, the
# program is provided without any warranty whatsoever, whether express,
# implied, statutory or otherwise. The term "warranty" used herein
# includes, but is not limited to, any warranty of the quality,
# performance, merchantability and fitness for a particular purpose of
# the program and the nonexistence of any infringement or violation of
# any right of any third party.
#
# Each user of the program will agree and understand, and be deemed to
# have agreed and understood, that there is no warranty whatsoever for
# the program and, accordingly, the entire risk arising from or
```

18 Appendix

```
# otherwise connected with the program is assumed by the user.
#
# Therefore, neither ICOT, the copyright holder, or any other
# organization that participated in or was otherwise related to the
# development of the program and their respective officials, directors,
# officers and other employees shall be held liable for any and all
# damages, including, without limitation, general, special, incidental
# and consequential damages, arising out of or otherwise in connection
# with the use or inability to use the program or any product, material
# or result produced or otherwise obtained by using the program,
# regardless of whether they have been advised of, or otherwise had
# knowledge of, the possibility of such damages at any time during the
# project or thereafter. Each user will be deemed to have agreed to the
# foregoing by his or her commencement of use of the program. The term
# "use" as used herein includes, but is not limited to, the use,
# modification, copying and distribution of the program and the
# production of secondary products from the program.
#
# In the case where the program, whether in its original form or
# modified, was distributed or delivered to or received by a user from
# any person, organization or entity other than ICOT, unless it makes or
# grants independently of ICOT any specific warranty to the user in
# writing, such person, organization or entity, will also be exempted
# from and not be held liable to the user for any such damages as noted
# above as far as the program is concerned.
#
# -----COPYING.ipadic-----END-----
```

3. Lao Word Break Dictionary Data (laodict.txt)

```
# Copyright (c) 2013 International Business Machines Corporation
# and others. All Rights Reserved.
#
# Project: http://code.google.com/p/lao-dictionary/
# Dictionary: http://lao-dictionary.googlecode.com/git/Lao-Dictionary.txt
# License: http://lao-dictionary.googlecode.com/git/Lao-Dictionary-LICENSE.txt
#         (copied below)
#
# This file is derived from the above dictionary, with slight
# modifications.
# -----
# Copyright (C) 2013 Brian Eugene Wilson, Robert Martin Campbell.
# All rights reserved.
```

18 Appendix

```
#
# Redistribution and use in source and binary forms, with or without
# modification,
# are permitted provided that the following conditions are met:
#
#
# Redistributions of source code must retain the above copyright notice, this
# list of conditions and the following disclaimer. Redistributions in
# binary form must reproduce the above copyright notice, this list of
# conditions and the following disclaimer in the documentation and/or
# other materials provided with the distribution.
#
#
# THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
# "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
# LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS
# FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE
# COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT,
# INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
# (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
# SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
# HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
# STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
# ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
# OF THE POSSIBILITY OF SUCH DAMAGE.
# -----
```

4. Burmese Word Break Dictionary Data (burmesedict.txt)

```
# Copyright (c) 2014 International Business Machines Corporation
# and others. All Rights Reserved.
#
# This list is part of a project hosted at:
# github.com/kanyawtech/myanmar-karen-word-lists
#
# -----
# Copyright (c) 2013, LeRoy Benjamin Sharon
# All rights reserved.
#
# Redistribution and use in source and binary forms, with or without
# modification, are permitted provided that the following conditions
# are met: Redistributions of source code must retain the above
# copyright notice, this list of conditions and the following
```

18 Appendix

```
# disclaimer. Redistributions in binary form must reproduce the
# above copyright notice, this list of conditions and the following
# disclaimer in the documentation and/or other materials provided
# with the distribution.
#
# Neither the name Myanmar Karen Word Lists, nor the names of its
# contributors may be used to endorse or promote products derived
# from this software without specific prior written permission.
#
# THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
# CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES,
# INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF
# MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
# DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS
# BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
# EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED
# TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
# DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
# ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR
# TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF
# THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
# SUCH DAMAGE.
# -----
```

5. Time Zone Database

ICU uses the public domain data and code derived from Time Zone Database for its time zone support. The ownership of the TZ database is explained in BCP 175: Procedure for Maintaining the Time Zone Database section 7.

7. Database Ownership

```
#
# The TZ database itself is not an IETF Contribution or an IETF
# document. Rather it is a pre-existing and regularly updated work
# that is in the public domain, and is intended to remain in the
# public domain. Therefore, BCPs 78 [RFC5378] and 79 [RFC3979] do
# not apply to the TZ Database or contributions that individuals make
# to it. Should any claims be made and substantiated against the TZ
# Database, the organization that is providing the IANA
# Considerations defined in this RFC, under the memorandum of
# understanding with the IETF, currently ICANN, may act in accordance
# with all competent court orders. No ownership claims will be made
```

18 Appendix

```
# by ICANN or the IETF Trust on the database or the code. Any person
# making a contribution to the database or code waives all rights to
# future claims in that contribution or in the TZ Database.
''''
```

- libuv, located at deps/uv, is licensed as follows:

```
''''
```

```
libuv is part of the Node project: http://nodejs.org/
libuv may be distributed alone under Node's license:
```

```
=====
```

Copyright Joyent, Inc. and other Node contributors. All rights reserved.
Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to
deal in the Software without restriction, including without limitation the
rights to use, copy, modify, merge, publish, distribute, sublicense, and/or
sell copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS
IN THE SOFTWARE.

```
=====
```

This license applies to all parts of libuv that are not externally
maintained libraries.

The externally maintained libraries used by libuv are:

- tree.h (from FreeBSD), copyright Niels Provos. Two clause BSD license.

- inet_pton and inet_ntop implementations, contained in src/inet.c, are
copyright the Internet Systems Consortium, Inc., and licensed under the ISC
license.

18 Appendix

- stdint-msvc2008.h (from msinttypes), copyright Alexander Chemeris. Three clause BSD license.
- pthread-fixes.h, pthread-fixes.c, copyright Google Inc. and Sony Mobile Communications AB. Three clause BSD license.
- android-ifaddrs.h, android-ifaddrs.c, copyright Berkeley Software Design Inc, Kenneth MacKay and Emergya (Cloud4all, FP7/2007-2013, grant agreement n° 289016). Three clause BSD license.

""""

- OpenSSL, located at deps/openssl, is licensed as follows:

""""

Copyright (c) 1998-2016 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following

18 Appendix

acknowledgment:

"This product includes software developed by the OpenSSL Project
for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
OF THE POSSIBILITY OF SUCH DAMAGE.

=====

====

This product includes cryptographic software written by Eric Young
(eyay@cryptsoft.com). This product includes software written by Tim
Hudson (tjh@cryptsoft.com).

''''

- Punycode.js, located at `lib/punycode.js`, is licensed as follows:

''''

Copyright Mathias Bynens <<https://mathiasbynens.be/>>

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE

18 Appendix

LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

- V8, located at `deps/v8`, is licensed as follows:

This license applies to all parts of V8 that are not externally maintained libraries. The externally maintained libraries used by V8 are:

- PCRE test suite, located in `test/mjsunit/third_party/regexp-pcre/regexp-pcre.js`. This is based on the test suite from PCRE-7.3, which is copyrighted by the University of Cambridge and Google, Inc. The copyright notice and license are embedded in `regexp-pcre.js`.
- Layout tests, located in `test/mjsunit/third_party/object-keys`. These are based on layout tests from `webkit.org` which are copyrighted by Apple Computer, Inc. and released under a 3-clause BSD license.
- Strongtalk assembler, the basis of the files `assembler-arm-inl.h`, `assembler-arm.cc`, `assembler-arm.h`, `assembler-ia32-inl.h`, `assembler-ia32.cc`, `assembler-ia32.h`, `assembler-x64-inl.h`, `assembler-x64.cc`, `assembler-x64.h`, `assembler-mips-inl.h`, `assembler-mips.cc`, `assembler-mips.h`, `assembler.cc` and `assembler.h`. This code is copyrighted by Sun Microsystems Inc. and released under a 3-clause BSD license.
- Valgrind client API header, located at `third_party/valgrind/valgrind.h`. This is released under the BSD license.

These libraries have their own licenses; we recommend you read them, as their terms may differ from the terms below.

Further license information can be found in LICENSE files located in sub-directories.

Copyright 2014, the V8 project authors. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

18 Appendix

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

- zlib, located at deps/zlib, is licensed as follows:

zlib.h -- interface of the 'zlib' general purpose compression library
version 1.2.8, April 28th, 2013

Copyright (C) 1995-2013 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be

18 Appendix

misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly

Mark Adler

jloup@gzip.org

madler@alumni.caltech.edu

""""

- npm, located at `deps/npm`, is licensed as follows:

""""

The npm application

Copyright (c) npm, Inc. and Contributors

Licensed on the terms of The Artistic License 2.0

Node package dependencies of the npm application

Copyright (c) their respective copyright owners

Licensed on their respective license terms

The npm public registry at <https://registry.npmjs.org>

and the npm website at <https://www.npmjs.com>

Operated by npm, Inc.

Use governed by terms published on <https://www.npmjs.com>

"Node.js"

Trademark Joyent, Inc., <https://joyent.com>

Neither npm nor npm, Inc. are affiliated with Joyent, Inc.

The Node.js application

Project of Node Foundation, <https://nodejs.org>

The npm Logo

Copyright (c) Mathias Pettersson and Brian Hammond

"Gubblebum Blocky" typeface

Copyright (c) Tjarda Koster, <https://jelloween.deviantart.com>

Used with permission

The Artistic License 2.0

Copyright (c) 2000-2006, The Perl Foundation.

Everyone is permitted to copy and distribute verbatim copies

18 Appendix

of this license document, but changing it is not allowed.

Preamble

This license establishes the terms under which a given free software Package may be copied, modified, distributed, and/or redistributed. The intent is that the Copyright Holder maintains some artistic control over the development of that Package while still keeping the Package available as open source and free software.

You are always permitted to make arrangements wholly outside of this license directly with the Copyright Holder of a given Package. If the terms of this license do not permit the full use that you propose to make of the Package, you should contact the Copyright Holder and seek a different licensing arrangement.

Definitions

"Copyright Holder" means the individual(s) or organization(s) named in the copyright notice for the entire Package.

"Contributor" means any party that has contributed code or other material to the Package, in accordance with the Copyright Holder's procedures.

"You" and "your" means any person who would like to copy, distribute, or modify the Package.

"Package" means the collection of files distributed by the Copyright Holder, and derivatives of that collection and/or of those files. A given Package may consist of either the Standard Version, or a Modified Version.

"Distribute" means providing a copy of the Package or making it accessible to anyone else, or in the case of a company or organization, to others outside of your company or organization.

"Distributor Fee" means any fee that you charge for Distributing this Package or providing support for this Package to another party. It does not mean licensing fees.

"Standard Version" refers to the Package if it has not been modified, or has been modified only in ways explicitly requested

18 Appendix

by the Copyright Holder.

"Modified Version" means the Package, if it has been changed, and such changes were not explicitly requested by the Copyright Holder.

"Original License" means this Artistic License as Distributed with the Standard Version of the Package, in its current version or as it may be modified by The Perl Foundation in the future.

"Source" form means the source code, documentation source, and configuration files for the Package.

"Compiled" form means the compiled bytecode, object code, binary, or any other form resulting from mechanical transformation or translation of the Source form.

Permission for Use and Modification Without Distribution

(1) You are permitted to use the Standard Version and create and use Modified Versions for any purpose without restriction, provided that you do not Distribute the Modified Version.

Permissions for Redistribution of the Standard Version

(2) You may Distribute verbatim copies of the Source form of the Standard Version of this Package in any medium without restriction, either gratis or for a Distributor Fee, provided that you duplicate all of the original copyright notices and associated disclaimers. At your discretion, such verbatim copies may or may not include a Compiled form of the Package.

(3) You may apply any bug fixes, portability changes, and other modifications made available from the Copyright Holder. The resulting Package will still be considered the Standard Version, and as such will be subject to the Original License.

Distribution of Modified Versions of the Package as Source

(4) You may Distribute your Modified Version as Source (either gratis or for a Distributor Fee, and with or without a Compiled form of the Modified Version) provided that you clearly document how it differs from the Standard Version, including, but not limited to, documenting

18 Appendix

any non-standard features, executables, or modules, and provided that you do at least ONE of the following:

(a) make the Modified Version available to the Copyright Holder of the Standard Version, under the Original License, so that the Copyright Holder may include your modifications in the Standard Version.

(b) ensure that installation of your Modified Version does not prevent the user installing or running the Standard Version. In addition, the Modified Version must bear a name that is different from the name of the Standard Version.

(c) allow anyone who receives a copy of the Modified Version to make the Source form of the Modified Version available to others under

(i) the Original License or

(ii) a license that permits the licensee to freely copy, modify and redistribute the Modified Version using the same licensing terms that apply to the copy that the licensee received, and requires that the Source form of the Modified Version, and of any works derived from it, be made freely available in that license fees are prohibited but Distributor Fees are allowed.

Distribution of Compiled Forms of the Standard Version
or Modified Versions without the Source

(5) You may Distribute Compiled forms of the Standard Version without the Source, provided that you include complete instructions on how to get the Source of the Standard Version. Such instructions must be valid at the time of your distribution. If these instructions, at any time while you are carrying out such distribution, become invalid, you must provide new instructions on demand or cease further distribution. If you provide valid instructions or cease distribution within thirty days after you become aware that the instructions are invalid, then you do not forfeit any of your rights under this license.

(6) You may Distribute a Modified Version in Compiled form without the Source, provided that you comply with Section 4 with respect to the Source of the Modified Version.

18 Appendix

Aggregating or Linking the Package

(7) You may aggregate the Package (either the Standard Version or Modified Version) with other packages and Distribute the resulting aggregation provided that you do not charge a licensing fee for the Package. Distributor Fees are permitted, and licensing fees for other components in the aggregation are permitted. The terms of this license apply to the use and Distribution of the Standard or Modified Versions as included in the aggregation.

(8) You are permitted to link Modified and Standard Versions with other works, to embed the Package in a larger work of your own, or to build stand-alone binary or bytecode versions of applications that include the Package, and Distribute the result without restriction, provided the result does not expose a direct interface to the Package.

Items That are Not Considered Part of a Modified Version

(9) Works (including, but not limited to, modules and scripts) that merely extend or make use of the Package, do not, by themselves, cause the Package to be a Modified Version. In addition, such works are not considered parts of the Package itself, and are not subject to the terms of this license.

General Provisions

(10) Any use, modification, and distribution of the Standard or Modified Versions is governed by this Artistic License. By using, modifying or distributing the Package, you accept this license. Do not use, modify, or distribute the Package, if you do not accept this license.

(11) If your Modified Version has been derived from a Modified Version made by someone other than you, you are nevertheless required to ensure that your Modified Version complies with the requirements of this license.

(12) This license does not grant you the right to use any trademark, service mark, tradename, or logo of the Copyright Holder.

(13) This license includes the non-exclusive, worldwide, free-of-charge patent license to make, have made, use, offer to sell,

18 Appendix

sell, import and otherwise transfer the Package with respect to any patent claims licensable by the Copyright Holder that are necessarily infringed by the Package. If you institute patent litigation (including a cross-claim or counterclaim) against any party alleging that the Package constitutes direct or contributory patent infringement, then this Artistic License to you shall terminate on the date that such litigation is filed.

(14) Disclaimer of Warranty:

THE PACKAGE IS PROVIDED BY THE COPYRIGHT HOLDER AND CONTRIBUTORS 'AS IS' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES. THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT ARE DISCLAIMED TO THE EXTENT PERMITTED BY YOUR LOCAL LAW. UNLESS REQUIRED BY LAW, NO COPYRIGHT HOLDER OR CONTRIBUTOR WILL BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING IN ANY WAY OUT OF THE USE OF THE PACKAGE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

""""

- GYP, located at tools/gyp, is licensed as follows:

""""

Copyright (c) 2009 Google Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- * Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT

18 Appendix

OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

- marked, located at tools/doc/node_modules/marked, is licensed as follows:

Copyright (c) 2011-2014, Christopher Jeffrey (<https://github.com/chjj/>)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

- cpplint.py, located at tools/cpplint.py, is licensed as follows:

Copyright (c) 2009 Google Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above

18 Appendix

copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

- ESLint, located at tools/eslint, is licensed as follows:

ESLint

Copyright jQuery Foundation and other contributors, <https://jquery.org/>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

18 Appendix

- gtest, located at deps/gtest, is licensed as follows:

""""

Copyright 2008, Google Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- * Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

""""

- node-weak, located at test/gc/node_modules/weak, is licensed as follows:

""""

Copyright (c) 2011, Ben Noordhuis <info@bnoordhuis.nl>

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF

18 Appendix

MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

boost

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

// Copyright Joe Coder 2004 - 2006.

// Distributed under the Boost Software License, Version 1.0.

glog

Copyright (c) 2008, Google Inc.

All rights reserved.

18 Appendix

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

GoAhead

Copyright (c) 20XX GoAhead Software, Inc. All Rights Reserved.

gtest

Copyright 2008, Google Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

iconv

the libiconv and libcharset libraries and their header files are under LGPL.
- refer to <http://www.gnu.org/licenses/lgpl.html>

libfcgi

This FastCGI application library source and object code (the "Software") and its documentation (the "Documentation") are copyrighted by Open Market, Inc ("Open Market"). The following terms apply to all files associated with the Software and Documentation unless explicitly disclaimed in individual files.

Open Market permits you to use, copy, modify, distribute, and license this Software and the Documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this Software and Documentation may be copyrighted by their authors and need not follow the licensing terms described here. If modifications to this Software and Documentation have new licensing terms, the new terms must be clearly indicated on the first page of each file where they apply.

OPEN MARKET MAKES NO EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE SOFTWARE OR THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN

18 Appendix

NO EVENT SHALL OPEN MARKET BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY DAMAGES ARISING FROM OR RELATING TO THIS SOFTWARE OR THE DOCUMENTATION, INCLUDING, WITHOUT LIMITATION, ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OR SIMILAR DAMAGES, INCLUDING LOST PROFITS OR LOST DATA, EVEN IF OPEN MARKET HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS". OPEN MARKET HAS NO LIABILITY IN CONTRACT, TORT, NEGLIGENCE OR OTHERWISE ARISING OUT OF THIS SOFTWARE OR THE DOCUMENTATION.

libjpeg

This package contains C software to implement JPEG image encoding, decoding, and transcoding. JPEG is a standardized compression method for full-color and gray-scale images.

The distributed programs provide conversion between JPEG "JFIF" format and image files in PBMPLUS PPM/PGM, GIF, BMP, and Targa file formats.

The core compression and decompression library can easily be reused in other programs, such as image viewers. The package is highly portable C code; we have tested it on many machines ranging from PCs to Crays.

We are releasing this software for both noncommercial and commercial use.

Companies are welcome to use it as the basis for JPEG-related products.

We do not ask a royalty, although we do ask for an acknowledgement in product literature (see the README file in the distribution for details).

We hope to make this software industrial-quality --- although, as with anything that's free, we offer no warranty and accept no liability.

For more information, contact jpeg-info@jpegclub.org.

microzip

the microzip libraries and their header files are under LGPL.

- refer to <http://www.gnu.org/licenses/lgpl.html>

minizip

MiniZip - Copyright (c) 1998-2010 - by Gilles Vollant - version 1.1 64 bits from Mathias Svensson

18 Appendix

Credits

Gilles Vollant - Original MiniZip author
Even Rouault - ZIP64 unzip Support
Daniel Borca - BZip Compression method support in unzip
Mathias Svensson - ZIP64 zip support
Mathias Svensson - BZip Compression method support in zip

License

Condition of use and distribution are the same than zlib :

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

nginx

/*

- * Copyright (C) 2002-2014 Igor Sysoev
- * Copyright (C) 2011-2014 Nginx, Inc.
- * All rights reserved.
- *
- * Redistribution and use in source and binary forms, with or without
- * modification, are permitted provided that the following conditions
- * are met:

18 Appendix

```
* 1. Redistributions of source code must retain the above copyright
*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
*
* THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*/
```

OpenSSL

LICENSE ISSUES

=====

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

```
/*
=====
==
* Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
```

18 Appendix

- * are met:
- *
- * 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
- *
- * 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in
* the documentation and/or other materials provided with the
* distribution.
- *
- * 3. All advertising materials mentioning features or use of this
* software must display the following acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
- *
- * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without
* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
- *
- * 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
- *
- * 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"
- *
- * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
- *

=====

18 Appendix

==

*

* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).

*

*/

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

* All rights reserved.

*

* This package is an SSL implementation written

* by Eric Young (eay@cryptsoft.com).

* The implementation was written so as to conform with Netscapes SSL.

*

* This library is free for commercial and non-commercial use as long as

* the following conditions are aheared to. The following conditions

* apply to all code found in this distribution, be it the RC4, RSA,

* lhash, DES, etc., code; not just the SSL code. The SSL documentation

* included with this distribution is covered by the same copyright terms

* except that the holder is Tim Hudson (tjh@cryptsoft.com).

*

* Copyright remains Eric Young's, and as such any Copyright notices in

* the code are not to be removed.

* If this package is used in a product, Eric Young should be given attribution

* as the author of the parts of the library used.

* This can be in the form of a textual message at program startup or

* in documentation (online or textual) provided with the package.

*

* Redistribution and use in source and binary forms, with or without

* modification, are permitted provided that the following conditions

* are met:

* 1. Redistributions of source code must retain the copyright

* notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright

* notice, this list of conditions and the following disclaimer in the

* documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software

* must display the following acknowledgement:

* "This product includes cryptographic software written by

18 Appendix

```
*   Eric Young (eay@cryptsoft.com)"
*   The word 'cryptographic' can be left out if the routines from the library
*   being used are not cryptographic related :-).
*   4. If you include any Windows specific code (or a derivative thereof) from
*   the apps directory (application code) you must include an acknowledgement:
*   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
*   THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
*   ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
*   IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
*   ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
*   FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
*   DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
*   OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
*   HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
*   LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
*   OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
*   SUCH DAMAGE.
*
*   The licence and distribution terms for any publically available version or
*   derivative of this code cannot be changed.  i.e. this code cannot simply be
*   copied and put under another distribution licence
*   [including the GNU Public Licence.]
*/
```

PCRE

PCRE LICENCE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 8 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C++ wrapper functions, and a just-in-time compiler that can be used to optimize pattern matching. These are both optional features that can be omitted when the library is built.

18 Appendix

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel
Email local part: ph10
Email domain: cam.ac.uk

University of Cambridge Computing Service,
Cambridge, England.

Copyright (c) 1997-2014 University of Cambridge
All rights reserved.

PCRE JUST-IN-TIME COMPILATION SUPPORT

Written by: Zoltan Herczeg
Email local part: hzmester
Email domain: freemail.hu

Copyright(c) 2010-2014 Zoltan Herczeg
All rights reserved.

STACK-LESS JUST-IN-TIME COMPILER

Written by: Zoltan Herczeg
Email local part: hzmester
Email domain: freemail.hu

Copyright(c) 2009-2014 Zoltan Herczeg
All rights reserved.

THE C++ WRAPPER FUNCTIONS

Contributed by: Google Inc.

18 Appendix

Copyright (c) 2007-2012, Google Inc.

All rights reserved.

THE "BSD" LICENCE

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

End

sqlcipher

Copyright (c) 2008, ZETETIC LLC

All rights reserved.

18 Appendix

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of the ZETETIC LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY ZETETIC LLC "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL ZETETIC LLC BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

sqlite

Anyone is free to copy, modify, publish, use, compile, sell, or distribute the original SQLite code, either in source code form or as a compiled binary, for any purpose, commercial or non-commercial, and by any means.

TiddlyWiki

Copyright (c) UnaMesa Association 2004-2007

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY

websocketpp

WebSocket++ is an open source (BSD license)

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

zlib

(C) 1995-2013 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

18 Appendix

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly Mark Adler
jloup@gzip.org madler@alumni.caltech.edu

SIL

Copyright (c) 1994-2008, SIL International (<http://www.sil.org/>).

This Font Software is licensed under the SIL Open Font License, Version 1.1, with Reserved Font Names "Lateef" and "SIL".

This license is copied below, and is also available with an FAQ at:
<http://scripts.sil.org/OFL>

SIL OPEN FONT LICENSE Version 1.1 - 26 February 2007

PREAMBLE

The goals of the Open Font License (OFL) are to stimulate worldwide development of collaborative font projects, to support the font creation efforts of academic and linguistic communities, and to provide a free and open framework in which fonts may be shared and improved in partnership with others.

The OFL allows the licensed fonts to be used, studied, modified and redistributed freely as long as they are not sold by themselves. The fonts, including any derivative works, can be bundled, embedded, redistributed and/or sold with any software provided that any reserved names are not used by derivative works. The fonts and derivatives, however, cannot be released under any other type of license. The requirement for fonts to remain under this license does not apply to any document created using the fonts or their derivatives.

18 Appendix

DEFINITIONS

"Font Software" refers to the set of files released by the Copyright Holder(s) under this license and clearly marked as such. This may include source files, build scripts and documentation.

"Reserved Font Name" refers to any names specified as such after the copyright statement(s).

"Original Version" refers to the collection of Font Software components as distributed by the Copyright Holder(s).

"Modified Version" refers to any derivative made by adding to, deleting, or substituting -- in part or in whole -- any of the components of the Original Version, by changing formats or by porting the Font Software to a new environment.

"Author" refers to any designer, engineer, programmer, technical writer or other person who contributed to the Font Software.

PERMISSION & CONDITIONS

Permission is hereby granted, free of charge, to any person obtaining a copy of the Font Software, to use, study, copy, merge, embed, modify, redistribute, and sell modified and unmodified copies of the Font Software, subject to the following conditions:

- 1) Neither the Font Software nor any of its individual components, in Original or Modified Versions, may be sold by itself.
- 2) Original or Modified Versions of the Font Software may be bundled, redistributed and/or sold with any software, provided that each copy contains the above copyright notice and this license. These can be included either as stand-alone text files, human-readable headers or in the appropriate machine-readable metadata fields within text or binary files as long as those fields can be easily viewed by the user.
- 3) No Modified Version of the Font Software may use the Reserved Font Name(s) unless explicit written permission is granted by the corresponding Copyright Holder. This restriction only applies to the primary font name as presented to the users.
- 4) The name(s) of the Copyright Holder(s) or the Author(s) of the Font Software shall not be used to promote, endorse or advertise any Modified Version, except to acknowledge the contribution(s) of the

18 Appendix

Copyright Holder(s) and the Author(s) or with their explicit written permission.

5) The Font Software, modified or unmodified, in part or in whole, must be distributed entirely under this license, and must not be distributed under any other license. The requirement for fonts to remain under this license does not apply to any document created using the Font Software.

TERMINATION

This license becomes null and void if any of the above conditions are not met.

DISCLAIMER

THE FONT SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF COPYRIGHT, PATENT, TRADEMARK, OR OTHER RIGHT. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, INCLUDING ANY GENERAL, SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF THE USE OR INABILITY TO USE THE FONT SOFTWARE OR FROM OTHER DEALINGS IN THE FONT SOFTWARE.

Software End User License Agreement(EULA)

SUPREMA INC.

SOFTWARE LICENSE AGREEMENT

PLEASE READ THE FOLLOWING TERMS AND CONDITIONS CAREFULLY BEFORE INSTALLING OR USING THE SOFTWARE OR ANY ACCOMPANYING DOCUMENTATION (COLLECTIVELY, THE "SOFTWARE").

THE TERMS AND CONDITIONS OF THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") GOVERN USE OF THE SOFTWARE UNLESS YOU AND SUPREMA INC ("COMPANY") HAVE EXECUTED A SEPARATE AGREEMENT GOVERNING USE OF THE SOFTWARE.

Company is willing to license the Software to you only upon the condition that you accept all the terms contained in this Agreement. By installing or using the Software, you have indicated that you understand this Agreement and accept all of its terms. If you are accepting the terms of this Agreement on behalf of a company or other legal entity, you represent and warrant that you have the authority to bind that company or other legal entity to the terms of this Agreement, and, in such event, "you" and "your" will refer to that company or other legal entity. If you do not accept all the terms of this Agreement, then

18 Appendix

Company is unwilling to license the Software to you, and you must return the Software to Company for a full refund, if you have paid for the license to the Software, or, if Company has made the Software available to you without charge, you must destroy all copies of the Software. Your right to return the Software for a refund expires 30 days after the date of purchase.

1. Grant of License.

Conditioned upon your compliance with the terms and conditions of this Agreement, Company grants you a non-exclusive, non-transferable, revocable license to Execute (as defined herein) the executable form of the Software on or in connection with hardware products sold by the Company, solely for your internal business purposes. You may make a single copy of the Software for backup purposes, provided that you reproduce on it all copyright and other proprietary notices that are on the original copy of the Software. Company reserves all rights in the Software not expressly granted to you in this Agreement. For purposes of this Agreement, "Execute" and "Execution" means to load, install, and run the Software in order to benefit from its functionality as designed by Company.

2. Restrictions.

Except as expressly specified in this Agreement, you may not: (a) copy (except in the course of loading or installing) or modify the Software, including but not limited to adding new features or otherwise making adaptations that alter the functioning of the Software; (b) transfer, sublicense, lease, lend, rent or otherwise distribute the Software to any third party; or (c) make the functionality of the Software available to multiple users through any means, including but not limited to by uploading the Software to a network or file-sharing service or through any hosting, application services provider, service bureau, software-as-a-service (SaaS) or any other type of services. You acknowledge and agree that portions of the Software, including but not limited to the source code and the specific design and structure of individual modules or programs, constitute or contain trade secrets of Company and its licensors. Accordingly, you agree not to disassemble, decompile or reverse engineer the Software, in whole or in part, or permit or authorize a third party to do so, except to the extent such activities are expressly permitted by law notwithstanding this prohibition.

3. Ownership.

The copy of the Software is licensed, not sold. You own the media on which the Software is recorded, but Company retains ownership of the copy of the Software itself, including all intellectual property rights therein. The Software is protected by copyright laws and the related regulations of your jurisdictional countries, the copyright law of the Republic of Korea, and international treaties. You will not delete or in any manner alter the copyright, trademark, and other proprietary rights notices or markings appearing on the Software as delivered to you.

4. Term.

The license granted under this Agreement remains in effect for a period of 75 years, unless earlier terminated in accordance with this Agreement. You may terminate the license at any time by destroying all copies of the Software in your possession or control. The license granted under this Agreement will automatically terminate, with or without notice from Company, if you breach any term of this Agreement. Upon termination, you must at Company's option either promptly destroy or return to

18 Appendix

Company all copies of the Software in your possession or control.

5. Limited Warranty.

Company warrants that, for [thirty (30)] days following the date of purchase (or delivery, if Company has made the Software available to you without charge), the Software will perform in all material respects in accordance with any accompanying documentation ("Documentation"). As your sole and exclusive remedy and Company's entire liability for any breach of this limited warranty, Company will at its option and expense promptly correct or replace the Software so that it conforms to this limited warranty. Company does not warrant that the Software will meet your requirements, that the Software will operate in the combinations that you may select for Execution, that the operation of the Software will be error-free or uninterrupted, or that all Software errors will be corrected. The warranty set forth in this Section 5 does not apply to the extent that Company provides you with the Software (or portions of the Software) for beta, evaluation, testing or demonstration purposes.

6. DISCLAIMER.

THE LIMITED WARRANTY SET FORTH IN SECTION 5 IS IN LIEU OF AND COMPANY EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES AND CONDITIONS, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT, AND ANY WARRANTIES AND CONDITIONS ARISING OUT OF COURSE OF DEALING OR USAGE OF TRADE. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED FROM COMPANY OR ELSEWHERE WILL CREATE ANY WARRANTY OR CONDITION NOT EXPRESSLY STATED IN THIS AGREEMENT.

7. Limitation of Liability.

COMPANY'S TOTAL LIABILITY TO YOU FROM ALL CAUSES OF ACTION AND UNDER ALL THEORIES OF LIABILITY WILL BE LIMITED TO ANY REFUND THE LOCAL DISTRIBUTOR OR INSTALLER MAY PROVIDE IN REGARDS TO THE DIRECT DAMAGES UP TO AND LIMITED TO THE AMOUNT PAID FOR THE SOFTWARE. IN NO EVENT WILL COMPANY BE LIABLE TO YOU FOR ANY SPECIAL, INCIDENTAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF DATA, BUSINESS, PROFITS OR ABILITY TO EXECUTE) OR FOR the cost of procuring substitute products ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR THE EXECUTION OR PERFORMANCE OF THE SOFTWARE, WHETHER SUCH LIABILITY ARISES FROM ANY CLAIM BASED UPON CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, AND WHETHER OR NOT COMPANY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE. THE FOREGOING LIMITATIONS WILL SURVIVE AND APPLY EVEN IF ANY LIMITED REMEDY SPECIFIED IN THIS AGREEMENT IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

8. Indemnities

You shall indemnify Company and hold Company harmless from and against, and shall defend against, any and all claims, including, but not limited to, the claim in relation to the infringement of the third party's Intellectual Property and damages of every kind for injury to or death of any person or persons and for damage to or loss of property.

18 Appendix

9. Export Law.

You agree to comply fully with all export or import controls imposed by the country of origin, destination or use, including regulations under such laws. You agree not to export or re-export (directly or indirectly) to ensure that neither the Software nor any technical data related thereto nor any direct product thereof are exported or re-exported directly or indirectly in violation of, or used for any purposes prohibited by, such laws and regulations.

10. Governing Law.

This Agreement will be governed by and construed in accordance with the laws of the Republic of Korea, without regard to or application of conflict of laws rules or principles. The United Nations Convention on Contracts for the International Sale of Goods will not apply.

11. Arbitration.

In the event of any dispute controversy or claim arising out of, or in connection with, or relating to this Agreement, or the breach, termination or invalidity of this Agreement, all attempts shall be made to solve it through mutual consultation in a spirit of confidence and integrity. If all attempts so made through mutual consultations have proved to be of no help within a reasonable time, arbitration rather than legal proceedings shall solve it. The matter shall be referred to the Korean Commercial Arbitration Board (43rd Fl., Trade Tower 159, Samsung-dong, Kangnam-ku, Seoul 135-729, Korea) using the Rules of Arbitration of the International Chamber of Commerce. The award of the arbitrators shall be final and binding upon the parties. The award shall be enforceable by any court having jurisdiction over the party against whom the award has been rendered or where any assets of the party against whom the award has been rendered can be located. The arbitrator(s) will be entitled to award attorneys' fees, costs and expenses incurred in connection with any dispute, controversy or claim arising out of, or in connection with, or relating to this Agreement, or the breach, termination or invalidity of this Agreement (including but not limited to costs and expenses associated with procuring expert witnesses), to the prevailing party in any arbitration.

12. General.

You may not assign or transfer this Agreement or any rights granted hereunder, by operation of law or otherwise, without Company's prior written consent, and any attempt by you to do so, without such consent, will be void. Except as expressly set forth in this Agreement, the exercise by either party of any of its remedies under this Agreement will be without prejudice to its other remedies under this Agreement or otherwise. All notices or approvals required or permitted under this Agreement will be in writing and delivered by confirmed facsimile transmission, by overnight delivery service, or by certified mail, and in each instance will be deemed given upon receipt. All notices or approvals will be sent to the addresses set forth in the applicable ordering document or invoice or to such other address as may be specified by either party to the other in accordance with this section. The failure by either party to enforce any provision of this Agreement will not constitute a waiver of future enforcement of that or any other provision. Any waiver, modification or amendment of any provision of this Agreement will be effective only if in writing and signed by authorized representatives of both parties. If any provision of this Agreement is held to be unenforceable or invalid, that provision will be enforced to the maximum extent possible, and the other provisions will remain in full force and effect. This Agreement is the

18 Appendix

complete and exclusive understanding and agreement between the parties regarding its subject matter, and supersedes all proposals, understandings or communications between the parties, oral or written, regarding its subject matter, unless you and Company have executed a separate agreement. Any terms or conditions contained in your purchase order or other ordering document that are inconsistent with or in addition to the terms and conditions of this Agreement are hereby rejected by Company and will be deemed null.

13. Contact Information.

If you have any questions regarding this Agreement, you may contact Suprema at sales@supremainc.com.

Index

1

- 1:N fast mode 64
- 1:N Security Level 64

A

- Access Group 107
- Access Group Status 109
- Access level 106
- Access on Card 133
- Activate the purchased license 221
- Adding Custom Account Level 213
- Adding holiday 229
- Adding PIN 121
- Adding schedule 229
- Adding User Information 113
- Advanced device search 55
- Advanced Enrollment 64
- Alert 231
- Alert History 165
- Alert List 49
- All log 157
- Analog Interphone 78
- Anti passback 97
- Anti-passback 96
- Anti-passback Bypass 143
- Anti-passback Zone 143
- Assigning CSN Card 131
- Assigning Wiegand Card 132
- Audit Trail 237
- Auth Tieout 64
- Automatic meal deduction 178
- Automatic user information syncing setting 221

B

- Background setting 71
- Basic device search 53
- Batch editing device information 59
- Batch editing doors 98
- Batch editing user information 140
- Before using 47
- BioMini Enrollment Package 235
- BioStar 2 date/time setting 216
- BioStar 2 language setting 216
- BioStar 2 Mobile app 232
- BioStar 2 preferences 216

C

- Camera Frequency 79
- Card Format 218
- Card list 217
- Changing database of BioStar 2 45
- Changing port of BioStar 2 43
- Changing server status of BioStar 2 42
- Cloud 232
- CSN Card 131
- CSV 116
- Custom User Field 221

D

- Dashboard 49
- Database Backup 221
- Daylight Saving Time 239
- Delete Data & Sync Device 53
- DESFire 133, 135, 220
- Device - administrator 69
- Device - authentication 64
- Device - display/sound 71
- Device - information 60
- Device - network 62
- Device - trigger & action 75
- Device administrator setting 69
- Device auth mode 64
- Device configuration 59
- Device language setting 71
- Device Status 161
- Device volume 71
- DM-20 83
- Door - configuration 93
- Door - information 93
- Door - option 95
- Door alarm 97
- Door Group 91
- Door relay 93
- Door sensor 93
- Door Status 162
- Dual authentication mode 95
- Duress 123

E

- Elevator 98
- Elevator - Alarm 104
- Elevator - Detail 101
- Elevator - Information 101
- Elevator - Option 103

Index

Elevator Group 99
Enroll Fingerprint 123
Enrollment Device 221
Entry device 93
Event Log 157
Event Status by Period 49
Exit button 93
Exit device 93

F

Face Detection Level 64
Fingerprint LFD 64
Fire Alarm Zone 145
First check-in & Last check-out 178
Fixed Shift 178
Flexible Shift 178
Floating Shift 178
Floor Status 163
Format Smart Card 135

G

General server setting 221
Grace 178
Graphic Map 166, 167, 168
Group 52, 111

H

Hard APB 96
HTTPS 232

I

iCLASS 133, 135, 220
Image Log 76, 234
Installing BioStar 2 31
Intercom 78
Interlock Zone 152
Intrusion Alarm Zone 148
IP Camera 173

L

Log upload method setting 221
Login 41
login password 240
Long-term Idle User 141

M

Managing Users Registered with Devices 57
Matching Timeout 64
MIFARE 133, 135, 220
Missed Alarm 49
Mobile Card 220
Mobile Credential 251
Mobile Credential Partial 251
Muster Zone 154

N

Notice 49
NVR 171

O

OM-120 84
Overtime Rule 185

P

password level 240
Personal auth mode 121

R

Read Smart Card 135
Real-time Log 159
Registering CSN Card 131
Registering Wiegand Card 132
Report 190
Rounding 178
RS-485 settings 62

S

Scan Timeout 64
Schedule Template 183
Scheduled Lock 146
Scheduled Unlock 147
Secure communication with device 221
Secure Credential Card 133
Secure Tamper 78
Sensor Mode 64
Sensor Sensitivity 64
Seos 220
Server Matching 64, 221
session security 240
Session timeout setting 221

Index

Shift 178
SIP Interphone 78
Slave device search 56
Slave devices 56
Smart Card 133, 220
Soft APB 96
Supported card list 130
Sync Device 53
System Requirements 30
system security 240

T

T&A 175
T&A Device 196
T&A Schedule 187
TCP/IP settings 62
Template format 64
Time Card 194
Time Code 177
Transferring User Information to Devices 138
Trigger & Action 227
Troubleshooting 258

U

Upgrading Firmware 58
User - BioStar privilege setting 113
User account privilege setting 211

V

Version Information 4
Video Setting 238

W

Wiegand 77, 219
Wiegand Card 132
Wiegand Card Data Format 218
Wiegand Device 89
Wiegand Device Search and Registration 56
WLAN 62

Z

Zone Status 164

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang- gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA
Tel: +82 31 783 4502 | Fax: +82 31 783 4503 | Inquiry: sales_sys@supremainc.com

©2020 Suprema Inc. Suprema and identifying product names and numbers herein are registered trade marks of Suprema, Inc. All non-Suprema brands and product names are trademarks or registered trademarks of their respective companies. Product appearance, build status and/or specifications are subject to change without notice.