

Terminal de Acceso / RFID, BLE, QR / Táctil 4" / IP65 / Cámara 2 MP / PoE

SKU: XS2QAPB Marca: SUPREMA Categoría: Proximidad (125 KHz)

Garantía: 3 años

$28,926.41

Precios con IVA incluido

DESCRIPCIÓN

La X-Station 2 es una terminal de control de acceso multitecnología diseñada para entornos profesionales que requieren flexibilidad en métodos de autenticación. Soporta tarjetas RFID en 125 kHz y 13.56 MHz (MIFARE, MIFARE Plus, DESFire EV1/EV2, FeliCa y HID Prox), credenciales móviles mediante Bluetooth y códigos QR. Incorpora un procesador quad-core de 1.5 GHz con 1 GB de RAM, pantalla táctil IPS de 4 pulgadas y cámara de 2 MP para registro visual de eventos. Su arquitectura incluye arranque seguro, protocolo OSDP y protección IP65, garantizando integridad de datos y operatividad en condiciones ambientales exigentes. La alimentación PoE, conectividad Ethernet y salida Wiegand facilitan su despliegue e integración con sistemas de control de acceso existentes.

Desempeño
CPU: Quad Core 1.5 GHz
RAM: 1 GB
Pantalla táctil IPS: 4'
Cámara: 2 MP para registro de eventos
Protocolo: OSDP
Arranque seguro
RFID: 125 kHz EM, 13.56 MHz MIFARE / MIFARE Plus / DESFire EV1 / EV2 / FeliCa
Opciones RF con HID: 125 kHz EM HID Prox, 13.56 MHz
Acceso móvil mediante Bluetooth
Lectura de códigos QR

Físicas / Eléctricas
Alimentación: PoE
Conectividad: Ethernet
Salida: Wiegand
Grado de protección: IP65 (resistente al polvo y agua)

Contenido del Paquete
Terminal X-Station 2 (XS2QAPB)
Accesorios de montaje

MEMORIA TÉCNICA · XS2QAPB

Número de parte de esta ficha: XS2QAPB. La información corresponde a esta variante.

X-Station 2
USER GUIDE
Version 1.03
English
EN 102.00.XS2 V1.03A
- CONTENTS Safety instructions 3
Instructional icons 3
Introduction 6
Components 6
Name and function of each part 7
Cables and connectors 8
How to scan a QR code/barcode 9
Admin Menu 10
All Menus 10
User 11
Registering user information 11
Modifying User Information 12
Delete All Users 12
View User Usage 12
Authentication 13
Auth Mode 13
Modifying Auth Mode 13
Delete Auth Mode 14
Add Auth Mode 14
Operation 14
QR/Barcode Operation 15
T&A Mode 15
Display & Sound 16
Network 17
Network Settings 17
Ethernet 17
Server 18
Serial Setting 18
Device 19
Relay 19
Date & Time 19
Daylight Saving Time 20
Device Info 21
Memory Info 21
USB Memory 22
Secure Tamper 23
Restart Device 23
Restore Default 23
User ID Type 23
Event Log 24
Search Log 24
Delete All Logs 24
View Log Usage 25
Troubleshooting 26
Checklist before reporting a failure 26

- CONTENTS Product specifications 27
Dimensions 29
XS2-QAPB, XS2-QDPB 29
XS2-APB, XS2-DPB 29
FCC compliance information 30
EU Declaration of Conformity (CE) 30
Appendices 31
Disclaimers 31
Open Source License 32
GNU General Public License 32
TERMS AND CONDITIONS 33
BoringSSL License 39
OpenSSL License 39
Original SSLeay License 40
Licenses for support code 41
Apache License 42

Safety instructions
Safety instructions
Please read this safety instructions before you use the product to prevent injury to yourself and others and to prevent property damage. The term ‘product’ in this manual refers to the product and any items provided with the product.
Instructional icons
Warning: This symbol indicates situations that could result in death or severe injury.
Caution: This symbol indicates situations that may result in moderate injury or property damage.
- Note: This symbol indicates notes or additional information.
- Warning
Installation
Do not install or repair the product arbitrarily.
- This may result in electric shock, fire, or product damage.
- Damages caused by any modifications or failure to follow installation instructions can void your manufacturer’s warranty.
Do not install the product in a place with direct sunlight, moisture, dust, soot, or a gas leak.
- This may result in electric shock or fire.
Install the product in a well-ventilated and cool place away from direct sunlight to prevent overheating when installing it outside.
Do not place the product inside the sealed enclosure when installing it outside.
- It increases the internal temperature of the enclosure and this may result in electric shock, fire, or malfunction.
Do not install the product in a location with heat from an electric heater.
- This may result in fire due to overheating.
Install the product in a dry location.
- Humidity and liquids may result in electric shock or product damage.
Do not install the product in a location where it will be affected by radio frequencies.
- This may result in fire or product damage.
Operation
Keep the product dry.
- Humidity and liquids may result in electric shock, fire, or product damage.
Do not use damaged power supply adaptors, plugs, or loose electrical sockets.
- Unsecured connections may cause electric shock or fire.
Do not bend or damage the power cord.
- This may result in electric shock or fire.

Safety instructions
- Caution
Installation
Do not install the product under direct sunlight or UV light.
- This may result in product damage, malfunction, discoloration, or deformation.
Do not install the power supply cable in a location where people pass by.
- This may result in injury or product damage.
Do not install the product near magnetic objects, such as a magnet, TV, monitor (especially CRT), or speaker.
- The product may malfunction.
Keep the minimum distance between products when installing multiple products.
- The product may be affected by radio frequencies emitted by other products and the product may malfunction.
Use only a power supply adaptor of either D.C 24 V and 800 mA or higher or D.C 12 V and 1,500 mA or higher.
- If the right power supply is not used, the product may malfunction.
Use a separate power supply for the Secure I/O 2, electric lock, and the product.
- If connecting and using the same power supply, the product may malfunction.
Do not connect and use the power supply and Power over Ethernet (PoE) simultaneously.
- The product may malfunction.
Make sure that the cable cover is completely closed after connecting it to the product to maintain the water-resistant and dust-resistant features (IP65 rating). It is recommended to use the enclosure if the product is installed outside.
- The product may malfunction if the water-resistant and dust-resistant features are damaged.
Operation
Do not drop the product or cause impacts to the product.
- The product may malfunction.
Do not disconnect the power supply while upgrading the firmware of the product.
- The product may malfunction.
Do not disclose the password to others and change it regularly.
- This may result in illegal intrusion.
Do not press buttons on the product by force or do not press them with a sharp tool.
- The product may malfunction.
Do not store your product in very hot or very cold places. It is recommended to use your product at temperatures from -20 °C to 50 °C.
- The product may malfunction.
When cleaning the product, mind the following.
- Wipe the product with a clean and dry towel.
- If you need to sanitize the product, moisten the cloth or the wipe with a proper amount of rubbing alcohol and gently clean all exposed surfaces including fingerprint sensor. Use rubbing alcohol (containing 70% Isopropyl alcohol) and a clean, non-abrasive cloth like lens wipe.
- Do not apply liquid directly to the surface of the product.
Do not use the product for anything other than its intended use.
- The product may malfunction.

Safety instructions
RTC battery
Discard the battery according to the appropriate regional or international waste regulations. Discard the battery according to the appropriate regional or international waste regulations.

Introduction
Introduction
Components
XS2-QAPB
XS2-QDPB
XS2-APB
XS2-DPB
Device and Wall Bracket
(XS2-QAPB, XS2-QDPB)
Device and Wall Bracket

(XS2-APB, XS2-DPB)
Drilling Template
Cables Diode 120 Ω resistor
Ferrite Core PVC Anchor x2 Fixing Screw x2
Bracket Fixing Screw
(Star Shaped)
201.00.XS2 V1.00A
X-Station 2
Compact RFID & QR Code Terminal
Open Source Software
Linux Kernel GPL
BoringSSL
Original SSLeay
AOSP Apache
306.00 V1.00AG
Cable Cover Shrink Tube Quick Guide
Open Source Software
Guide
- Components may vary according to the installation environment.
- When assembling the product with the bracket, you can use the included bracket fixing screw (Star Shaped)
instead of the product fixing screw for enhanced security.
and refer to the installation guide.

Introduction
Name and function of each part
Camera
LCD screen
RF card and
mobile access card
authentication unit
QR code/Barcode
authentication unit
USB (Type-C) cable slot
Cable connector
Speaker
Name Description
Camera Captures actual images.
LCD screen Provides UI for operation.
RF card and mobile access card
authentication unit
Part to scan a RFID card or mobile access card for entrance.
QR code/Barcode
authentication unit
Part to scan a QR code or barcode for entrance.
USB (Type-C) cable slot Connects the USB cable.
Cable connector
Connects cables.
- Power supply
- Ethernet + PoE
- RS-485
- Wiegand input and output
- TTL input
- Relay
Speaker Delivers sound.
Only XS2-QAPB and XS2-QDPB models support barcode and QR code authentication.

Introduction
Cables and connectors
- 1 21 22 2
Cable PIN Name Color
RJ-45
(Ethernet +
PoE)
1 ENET TXP White
3 ENET TXN Orange
5 ENET RXP Black
7 ENET RXN Yellow
TTL input
9 TTL GND Gray
11 TTL IN0 Purple
13 TTL IN1 Brown
RS-485
15 485 GND White (Black stripe)
17 485 TRXN Yellow (Black stripe)
19 485 TRXP Blue (White stripe)
Wiegand
21 WG D1 White
22 WG D0 Green
20 WG GND Black
Relay
18 RLY NO Gray (White stripe)
16 RLY NC Orange (White stripe)
14 RLY COM Green (White stripe)
Power
12 PWR +VDC Red
10 PWR GND Black (White stripe)
RJ-45
(Ethernet +
PoE)
8 VB2 Brown
6 VB2 Blue
4 VB1 Green
2 VB1 Red

Introduction
How to scan a QR code/barcode
You can issue a QR code/barcode to a user and use it as an authentication method. Scan the QR code/barcode properly
by following the instructions on the screen to increase the recognition rate.
5-20 cm
- Keep 5 cm to 20 cm of distance between the QR code/Barcode
authentication unit of the device and the QR code/barcode.
- Hold the smartphone with the screen facing towards the QR/
Barcode code authentication unit and place the guide beam at
the center of the QR code.
- When authenticating with the QR code/barcode downloaded
to your smartphone, adjust the brightness of your smartphone
so that the device can read the QR code/barcode clearly.
- If you do not follow the instructions on the screen, it may take

a long time to scan the QR code/barcode, or it may fail.
- Only XS2-QAPB and XS2-QDPB models support QR code/barcode authentication.
- You can issue QR codes only on BioStar 2. For more information on how to issue a QR code/barcode, refer to BioStar 2 Administrator's manual.
- 10
Admin Menu
Admin Menu
All Menus
1 Press and authenticate with the Admin level credential.
2 Select the desired menu.
If the administrator has not been designated, the menu screen will be displayed when you press .
- 11
User
User
Registering user information
The user information including credentials can be registered.
1 Press and authenticate with the Admin level credential.
2 Select USER → , and choose a credential you want to register.
There are two steps for the user registration. Some options are available after the credential has been registered.
- : Take a picture of a user with the built-in camera.
- Name: Enter the username.
- ID: Enter a number between 1 and 429467295 to register as the user ID. If User ID Type set to Alphanumeric, a combination of alphanumeric characters and symbols (_, -) can be used for the ID. Up to 32 characters can be input.
- Card / QR Code: Register a card for user authentication. Press
- and scan the card which will be assigned to the
user. To register an additional card, press again. You can issue QR codes only on BioStar 2.
- PIN: Enter the PIN you wish to use. Enter the PIN you wish to use, and then enter the same PIN again for confirmation. Enter a number between 4 and 16 digits to prevent leaking.
- Operator Level: Select the level you wish to assign to a user.
Available menus vary according to the set user level.
- None: This is the general user level and menus cannot be accessed.
- Administrator: All menus can be accessed.
- Configuration: AUTHENTICATION, DISPLAY & SOUND, NETWORK, DEVICE, and EVENT LOG menus can be accessed.
- User Management: USER and EVENT LOG menu can be accessed.
- Period: Set an expiry date to use the user account.
- Access Group: Select an access group for the user. Access groups can be registered only in BioStar 2.
- Private Auth Mode: Change the authentication method according to the user.
- 12
User
Modifying User Information
User Management or Administrator can modify the registered user information. A card can be added, and PIN and level can be modified.
1 Press
- and authenticate with the Admin level credential.
2 Select USER → .
3 Select your search terms. You can search for a user by All, User ID, Name, and Card / QR Code.
4 Select a user you wish to modify.
5 Modify the information by referring to Registering user information and press OK.
- To delete a user, select and then press OK.
Access Group can be registered in BioStar 2. For detailed contents regarding registering an access group, refer to the BioStar 2 Administrator Manual.
Delete All Users
You can delete all registered users at once.
1 Press
- and authenticate with the Admin level credential.
2 Select USER → .
3 Check Delete All to delete all registered users and press OK.
4 When you press OK, all registered users will be deleted.
View User Usage
You can see the number of registered users, and cards at a glance.
1 Press and authenticate with the Admin level credential.
2 Select USER → . User usage information appears.
- 13
Authentication
Authentication
Auth Mode
Modifying Auth Mode
You can set the authentication method and schedule according to each credential. You can set up to 3 auth modes.
1 Press and authenticate with the Admin level credential.
2 Select AUTHENTICATION → Auth Mode.
3 Select the authentication mode to modify.
4 When you press , the selected credential will be deleted, and when you press , available credentials to be added will be displayed on the screen.
5 Set the desired auth mode and select a schedule.
Category Description
Card / QR Code
- : Mode to use a card or QR code only.
- + : Mode to authenticate with a card or QR code, and then enter PIN.
User ID
- + : Mode to enter ID and then enter PIN.
6 When you press OK, settings will be saved.
- The icon image may differ depending on the model you use.
- A schedule can be set in BioStar 2. If there is no set schedule, only can be selected.
- For detailed contents regarding setting a schedule, refer to BioStar 2 Administrator's manual.
- 14
Authentication
Delete Auth Mode
1 Press and authenticate with the Admin level credential.
2 Select AUTHENTICATION → Auth Mode.
3 Press and select the authentication mode to delete. You can select multiple options.
4 Press OK. To delete the selected option, press OK. Or, press Cancel to cancel the deletion.
Add Auth Mode
You can register up to 3 auth modes.
1 Press and authenticate with the Admin level credential.
2 Select AUTHENTICATION → Auth Mode.
3 Press .
4 Set the desired auth mode by pressing , and then select a schedule.
5 When you press OK, the auth mode will be added.
Operation
1 Press and authenticate with the Admin level credential.
2 Press AUTHENTICATION and then modify items below Operation.
- Face Detection: When you set Face Detection, X-Station 2 can detect real face, and authentication can be done only when a face is detected after authenticating with a card, QR code, or PIN.
- Auth Timeout: If the authentication is not completed during a set time, the authentication will fail. You can set a time between 3 seconds and 20 seconds.
- Server Matching: When you set Server Matching, the user authentication is not carried out in the device,

but instead is carried out in BioStar 2. Server Matching can be useful when there is a large amount of user information in the device or you do not wish to publicly expose the device where user credential information is saved.
- 15
Authentication
QR/Barcode Operation
1 Press and authenticate with the Admin level credential.
2 Press AUTHENTICATION and then modify items below QR/Barcode Operation.
- QR/Barcode: Set to use QR code or Barcode to authenticate.
- QR/Barcode Scan Timeout: If you do not scan the QR code or Barcode within the set time, the authentication will fail. You can set a time between 4 seconds and 10 seconds.
T&A Mode
You can set how to register T&A Mode.
1 Press
- and authenticate with the Admin level credential.
2 Press AUTHENTICATION and then modify items below T&A Mode.
3 Select and set the desired item.
- T&A Mode: Set the method to use T&A mode.
- T&A Code: You can register T&A events. Select T&A Code → to register a T&A event and set an icon, name of T&A event, and schedule.
- T&A Required: Set to require a user to select a T&A event when authenticating.
- Fixed T&A Key: Set to use only a T&A event selected by the administrator. This option can be used when Fixed is set for T&A Mode.
- Job Code: Select whether to use Job Code.
4 To save settings, press OK.
- 16
Display & Sound
Display & Sound
You can change the display and sound settings of the device.
1 Press and authenticate with the Admin level credential.
2 Select DISPLAY & SOUND.
3 Change the desired item.
- Home Screen: Select items to be displayed in the background of the home screen.
- Language: Set the language you wish to use.
- Device Private Msg.: Set whether to use a Private Message, which will be displayed on the screen when the user authenticates. You can set Device Private Msg. by using the BioStar 2 Device SDK.
- Server Private Msg.: Set whether to use a Private Message, which will be displayed on the screen when the user authenticates. You can set the Server Private Msg. by using the BioStar 2 API. If you have not set it on the server, the device does not display a message when authentication is successful even if Server Private Msg. is enabled on the device.
- Screen Saver: Set this option to use the screen saver feature. It reduces unnecessary energy consumption by lowering the brightness of the LCD screen when the device is not in use.
- Menu Timeout: Set the time (sec) for the menu screen to disappear automatically. If there is no button input during a set time, the screen will return to the home screen.
- Message Timeout: Set the time (sec) for a setting complete message or information message to disappear automatically.
- Backlight Timeout: Set the time (second) to turn off the lighting of LCD screen.
- Voice Instruction: Set to use the voice instruction instead of alarm sounds.
- Volume: Set the volume.
Refer to the BioStar 2 Device SDK webpage on the Suprema Knowledge Base website (kb.supremainc.com/bs2sdk/) for more information on the BioStar 2 Device SDK.
- 17
Network
Network
Network Settings
You can change the network settings of the device.
Ethernet
1 Press and authenticate with the Admin level credential.
2 Select NETWORK → Ethernet.
3 Change the desired item.
- DHCP: Set whether to use DHCP. If DHCP setting is disabled, the user can modify Port, IP Address, Gateway, Subnet Mask, and DNS.
- Device Port: Set the device port.
- IP Address: View the IP address of the device. To modify, disable DHCP setting.
- Gateway: View the gateway of the device. To modify, disable DHCP setting.
- Subnet Mask: View the subnet mask of the device. To modify, disable DHCP setting.
- DNS: Set the DNS server address.
4 To save settings, press OK.
- 18
Network
Server
1 Press and authenticate with the Admin level credential.
2 Select NETWORK → Server.
3 Change the desired item.
- Device → Server: You can send a connection signal from the device to a server with the input information directly. When you select Server
→ Device, Server IP, Server URL and Server Port cannot be entered.
- Server IP: Enter the IP address of the PC on which BioStar 2 is installed. Input is accepted only when Device → Server is set for Connection Mode.
- Server URL: Enter server URL instead of Server IP. Input is accepted only when Device → Server is set for Connection Mode.
- Server Port: Enter the port of the PC on which BioStar 2 is installed. Input is accepted only when Device -> Server is set for Connection Mode.
4 To save settings, press OK.
Serial Setting
1 Press
- and authenticate with the Admin level credential.
2 Select NETWORK.
3 Change the desired item.
- RS-485: Select the RS-485 mode.
- Baud Rate: Select the desired baud rate.
4 To save settings, press OK.
- 19
Device
Device
Relay
You can set the open time and the input port of the exit button in the device.
1 Press and authenticate with the Admin level credential.
2 Select DEVICE → Relay.
- Relay: You can set whether relay is enabled or not. To set the open time and the input port of the exit button, activate this option.
- Open Time: Set the duration for the door to remain open when standard user authentication has been carried out.
- Exit Button: Select the input port where the exit button is connected.
- Switch: Select the relay type (N/O or N/C).
Date & Time
You can set the open time and the input port of the exit button in the device.
1 Press

- and authenticate with the Admin level credential.
2 Select DEVICE → Date & Time.
3 Change the desired item.
- Date & Time: Check the current date and time. To modify it manually, disable Time Sync.
- Time Zone: Set the time reference of the current location.
- Time Sync: Synchronize the server and the time. If you wish to synchronize the server and the time, enable Time Sync.
- Date Format: Set the date format. You can select among YYYY/MM/DD, MM/DD/YYYY and DD/MM/YYYY.
- Time Format: Set the time format. You can select either 24-Hour or AM/PM.
- 20
Device
Daylight Saving Time
You can use the device by applying daylight saving time. Set the start and end time correctly.
1 Press and authenticate with the Admin level credential.
2 Select DEVICE → Daylight Saving Time and press to add additional daylight-saving time.
3 Select the desired item and change the setting.
- Name: Set the name of daylight-saving time.
- Start Month / Start Week / Start Day / Start Time: Set details of when the daylight-saving time option begins.
- End Month / End Week / End Day / End Time: Set details of when the daylight-saving time ends.
4 To save settings, press OK.
- 21
Device
Device Info
You can view the model name, device ID, serial number, firmware version of device ID, and MAC address.
1 Press and authenticate with the Admin level credential.
2 Select DEVICE → Device Info. You can view the information including Model Name, Device ID, Serial No., HW, FW, Kernel, and MAC .
Memory Info
View the status of memory usage.
1 Press and authenticate with the Admin level credential.
2 Select DEVICE → Memory Info. You can view the memory usage status of the device.
- 22
Device
USB Memory
Connect USB Memory and import user information to the device or export log and user information from the device. Upgrade the firmware.
1 Press
- and authenticate with the Admin level credential.
2 Select DEVICE → USB Memory.
3 Select the desired item and change the setting.
- Import: Import user information from the connected USB memory.
- Export: Select information you wish to export to the connected USB memory.
- FW Upgrade: Upgrade the firmware if the firmware files are saved in the connected USB memory.
The type of supported USB memory is as follows. If you use a different type of USB memory, the function may not operate normally.
- Samsung Electronics: SUM-LSB 8 GB, SUM-PSB 8 GB, SUM-PSB 16 GB, SUM-BSG 32 GB
- LG Electronics: XTICK J3 WINDY 8 GB, SMART USB MU1 White 8 GB, MU 1 USB 32 GB, MU28GBC 32 GB, XTICK MOBY J1 16 GB
- SanDisk: Cruzer 16 GB, Cruzer Blade CZ50 4 GB, Cruzer Blade CZ50 32 GB, CZ48 Ultra USB 3.0 64 GB, CZ80 USB3.0 64 GB, CZ52 64 GB, Cruzer Glide Z60 128 GB, Cruzer Force CZ71 32 GB
- Sony: Micro Vault Click 8 GB, MicroVault CLICK 16 GB, USM-SA1 32 GB
- Transcend: JetFlash 760 8 GB, JetFlash 760 32 GB, JetFlash 500 8 GB
- Memorette: MINI500 8 GB
- A-DATA: S102 PRO 8 GB
- Trigem Pastel 8 GB
The supported USB flash drives listed above were all tested with USB Type-A. To connect these USB flash drives to X-Station 2, a separate USB Type-C gender is required.
- 23
Device
Secure Tamper
When the tamper is turned on, you can set to delete the entire user, the entire log, and the security key.
1 Press and authenticate with the Admin level credential.
2 Select DEVICE.
3 Activate Secure Tamper to delete data of all registered users, all logs, and secure keys when a temper event occurs.
Restart Device
The user can restart the device.
1 Press and authenticate with the Admin level credential.
2 Select DEVICE → Restart Device.
3 To restart the device, press OK. To return to the previous screen, press Cancel.
Restore Default
Device settings, network settings, and operator levels will be reset.
1 Press and authenticate with the Admin level credential.
2 Select DEVICE → Restore Default.
- All settings: You can reset all settings stored on the device. Press OK to reset all device settings.
- Keep Network Settings: You can reset all settings except network settings. Press OK to reset all settin