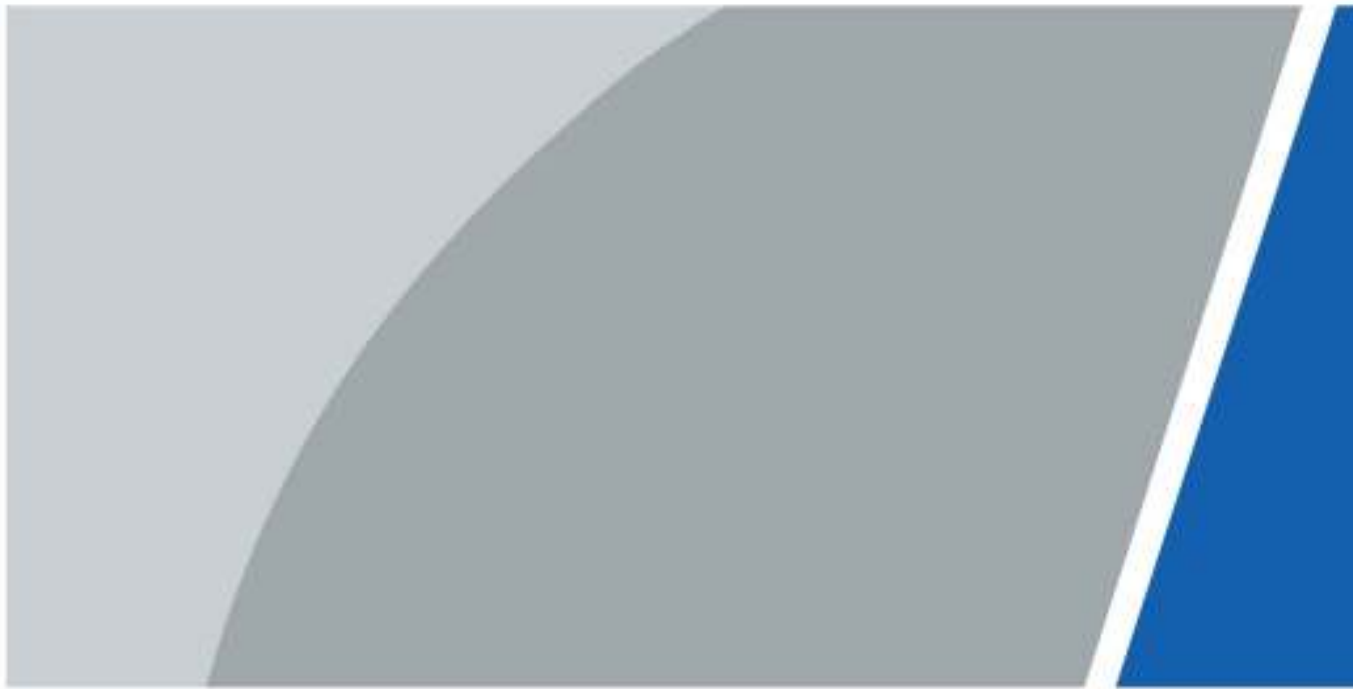


Access Standalone

Quick Start Guide








Foreword

General

This manual introduces the installation and basic operations of the Access Standalone (hereinafter referred to as "the Device").

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 TIPS	Provides methods to help you solve a problem or save you time.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	September 2021

Privacy Protection Notice

As the access controller user or data controller, you might collect the personal data of others such as their face, fingerprints, and car plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions.

For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.

- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the access controller.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Device, hazard prevention, and prevention of property damage. Read carefully before using the Device, comply with the guidelines when using it, and keep the manual safe for future reference.

Operating Requirements



- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.
- Only use the device within the rated power range.
- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquid on top of the device to avoid liquids flowing into it.
- Do not disassemble the device.

Installation Requirements



WARNING

- Connect the Device to the adapter before power on.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to the power requirements of the Device.
- Do not connect the Device to more than one power supply. Otherwise, the Device might become damaged.



- Observe all safety procedures and wear required protective equipment provided for your use while working at heights.
- Keep the Device on a stable place to prevent it from falling.
- Do not expose the Device to direct sunlight or heat sources.
- Do not install the Device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the Device.
- Use the power adapter or case power supply provided by the Device manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the Device label.
- Connect class I electrical appliances to a power socket with protective earthing.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Structure	1
2 Wiring and Installation	2
2.1 Environment Requirements	2
2.2 Wiring	3
2.3 Installation	3
3 Local Configurations	5
3.1 Initialization	5
3.2 Adding Users	5
4 Web Configurations	7
4.1 Logging in on Computer	7
4.2 Logging in on Phone	8
Appendix 1 Fingerprint Registration Instructions	9
Appendix 2 Cybersecurity Recommendations	10

1 Structure

Figure 1-1 Dimensions (1) (mm [inch])

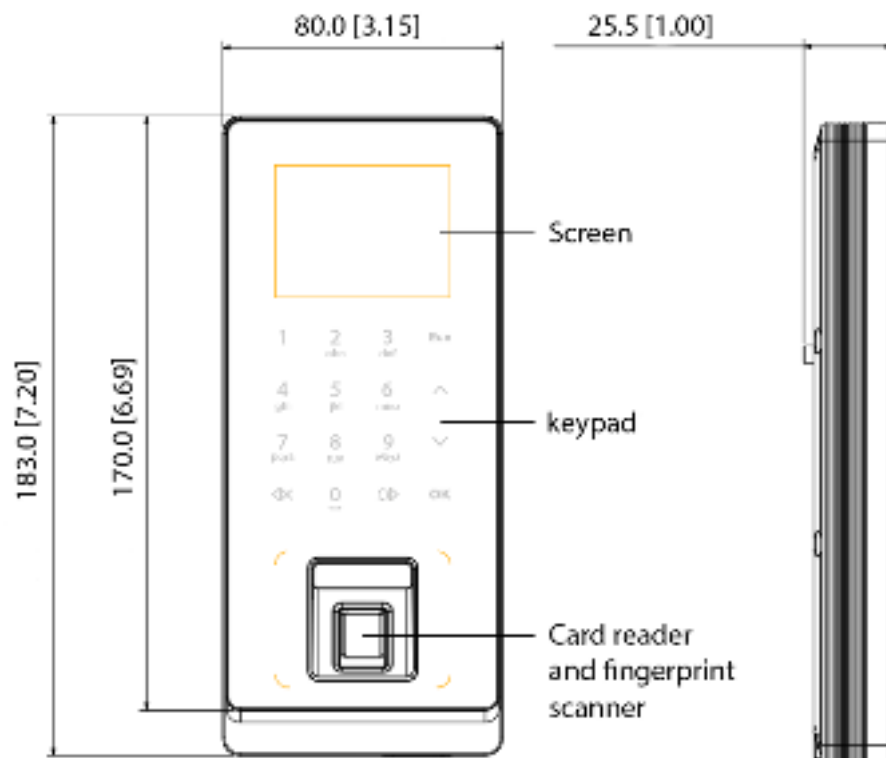
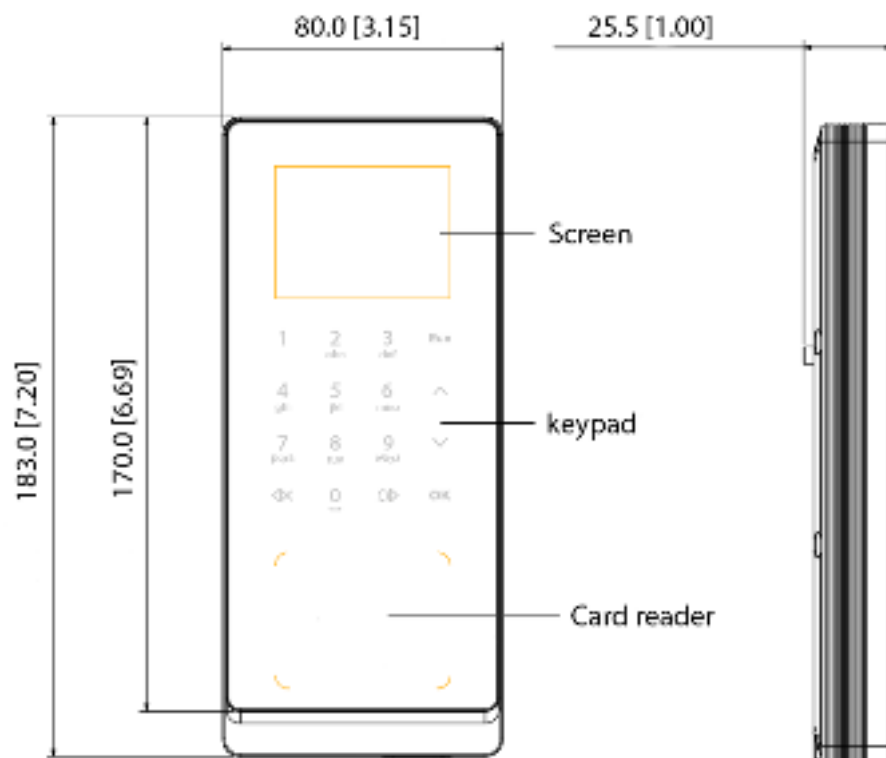


Figure 1-2 Dimensions (2) (mm[inch])



2 Wiring and Installation

2.1 Environment Requirements

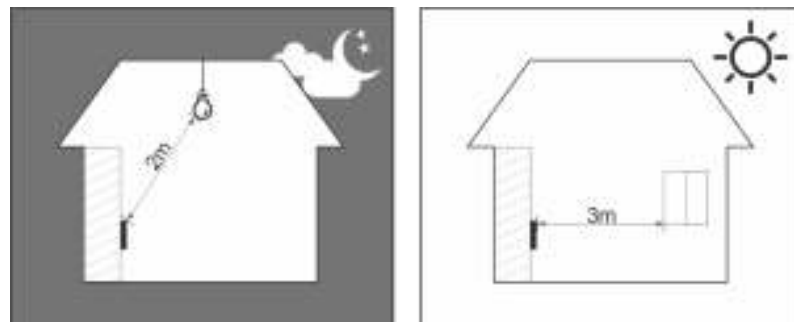
- The illumination 0.5 m from the device should not be less than 100 lx.

Figure 2-1 Installation Environment



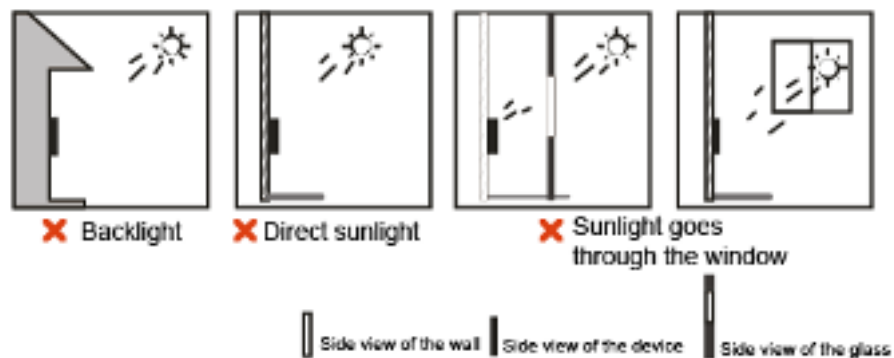
- We recommend installing the device indoors, 3 m away from the windows or doors, and 2 m away from any light source.

Figure 2-2 Installation Position



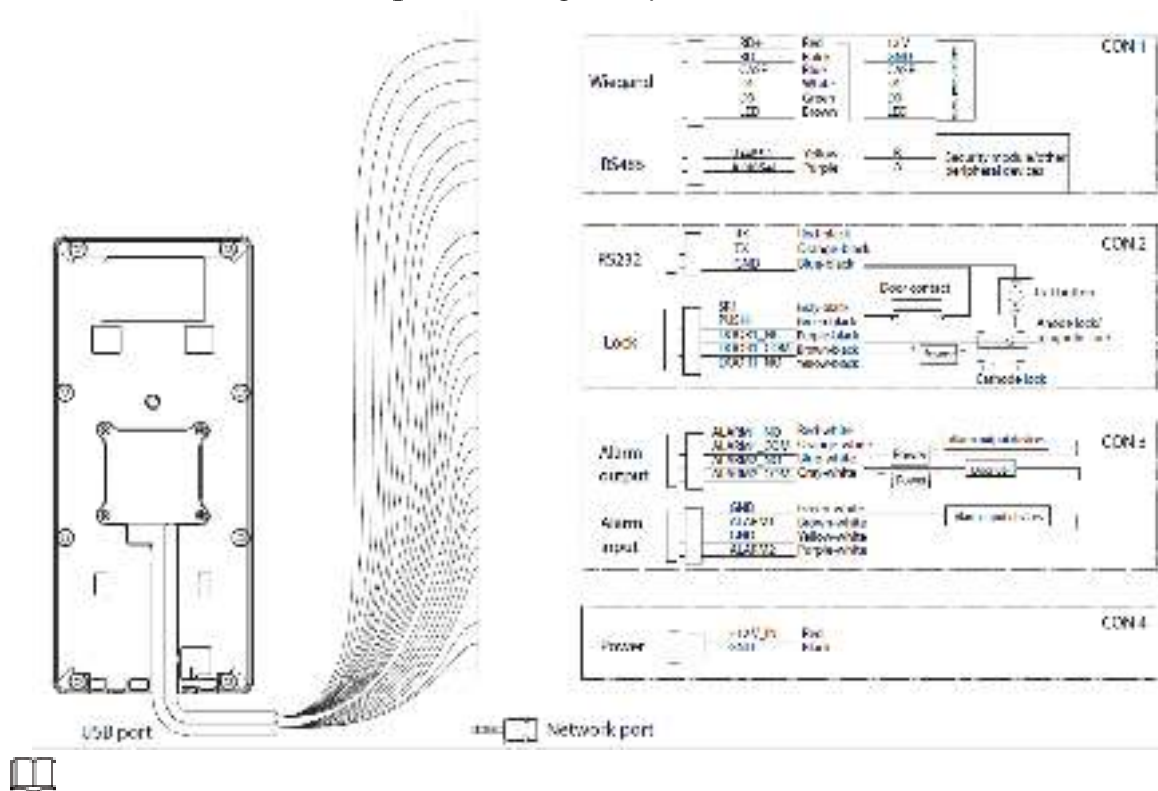
- Do not expose the device to backlight, sunlight, or place it near any light.

Figure 2-3 Places not recommended



2.2 Wiring

Figure 2-4 Wiring description

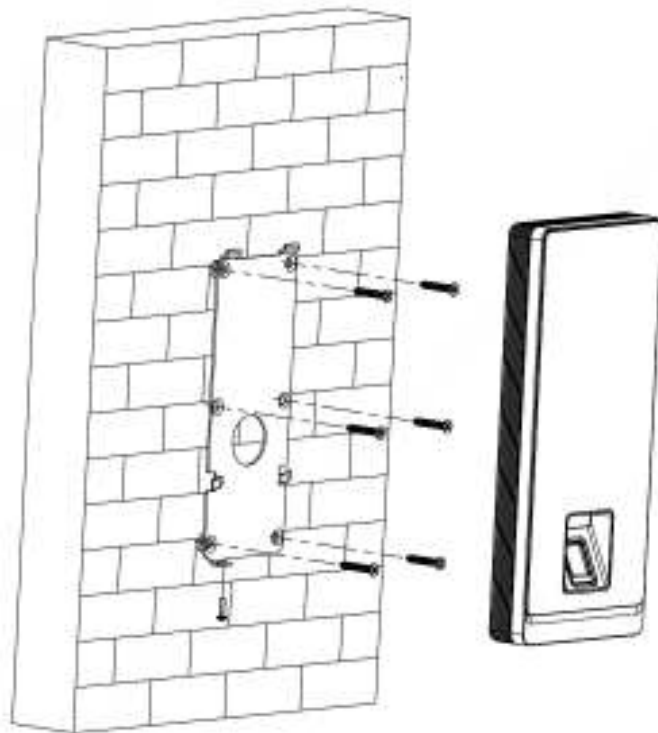


- On the web portal, select **Config Mgmt > Features** to check whether **Security Module** is enabled. If it is enabled, you need to purchase a matched security module and it requires a separate power supply.
- When the security module is enabled, the door exit button, lock and fire linkage will be invalid.

2.3 Installation

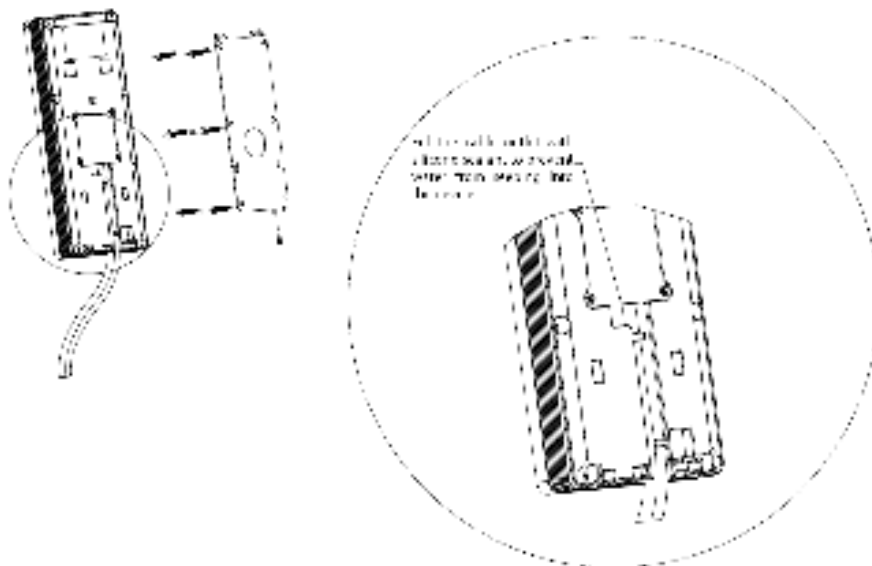
This section uses a device with the fingerprint function as an example. We recommend you to install the Device 1.2 m–1.6 m above the ground (from the center of the lens to the ground).

Figure 2-5 Install the device on the wall



- Step 1** Mark holes on the wall according to the bracket. Drill six screw holes and one cable outlet in the wall. Put expansion bolts in the holes.
- Step 2** Use screws to fix the bracket to the wall.
- Step 3** Wire the device. See "2.2Wiring".
- Step 4** Fit the device on the hooks of the bracket.
- Step 5** Tighten the screw at the bottom of the device.
- Step 6** (Optional) Apply silicone sealant to the cable outlet.

Figure 2-6 Apply silicone sealant



3 Local Configurations

3.1 Initialization

For first-time use or after restoring factory defaults, you need to set a password and link your email address for the admin account. You also need to set the time zone of the Device. You can use the admin account to log in to the main menu of the Device, configure the Device, and log in to the web interface and SmartPSS AC.

Figure 3-1 Initialize the device



- If you forget the administrator password, send a reset request to your linked e-mail address.
- The password must consist of 8 to 32 non-blank characters and contain at least two types of the following characters: upper case, lower case, numbers, and special characters (excluding ' " ; : &). Set a high-security password by following the password strength prompt.

3.2 Adding Users

Step 1 On the standby interface, the arrow buttons to select , and then tap **OK**.

Step 2 Log in with the administrator account, and then select **User > New User**.




The interfaces in this manual are only for reference, and might differ from the actual product.

Figure 3-2 Add a new user

New User(1/2)		New User(2/2)	
User ID	1	Permission	User >
Name		Period	255-Default
FP	0	Holiday Plan	255-Default
Card	0	Valid Date	2037-12-31
PWD		User Type	General >

Step 3 Configure the parameters.

Table 3-1 Description of user parameters

Parameter	Description
ID.	Each user ID is unique. It can be 18 characters of numbers, letters, or the their combination.
Name	You can enter names with a maximum of 32 characters (including numbers, symbols, and letters).
Fingerprint	<p>Each user can add up to 3 fingerprints. Follow the on-screen prompts and voice prompts to add fingerprints.</p> <p>You can enable the duress fingerprint function under each fingerprint. After the duress alarm function is enabled, an alarm will be triggered if the door is unlocked by the duress fingerprint.</p>  <ul style="list-style-type: none">• We do not recommend setting the first fingerprint as the duress fingerprint.• Only certain models support the fingerprint function.
Card	<p>You can register five cards for each user. On the card registration interface, swipe your card, and then the card information will be read by the Device.</p> <p>You can enable the duress card function on the card registration interface. After the duress alarm function is enabled, an alarm will be triggered if the door is unlocked by the duress card.</p>
PWD	Enter password to unlock the door. The maximum length of the ID digits is 8.
Permission	<p>You can select a user permission for the new user.</p> <ul style="list-style-type: none">■ Users only have door unlock permission.■ Administrators can configure the Device and unlock the door.
Period	A user can only unlock the door within the defined period. The default value is 255, which means the user can unlock the door at any time.
Holiday Plan	A user can only unlock the door within the defined period. The default value is 255, which means the user can unlock the door at any time.
Valid Date	Define a period during which the user has door access control.
User Type	<ul style="list-style-type: none">■ General: General users can unlock the door normally.■ Blocklist: When users in the blocklist unlock the door, service personnel receive a notification.■ Guest: Guests can unlock the door within a defined period or for a certain amount of times. After the defined period expires or the unlocking times runs out, they cannot unlock the door.■ Patrol: Paroling users can have their attendance tracked, but they have no unlocking permissions.■ VIP: When the VIP user unlocks the door, service personnel receives a notification. The VIP user is not restricted by unlock modes, such as Multi-card and Time Section.■ Others: When they unlock the door, the door will stay unlocked for 5 more seconds.■ Custom User 1/2: Same as General.

Step 4 After you have configured all the parameters, tap **Esc**.

Step 5 Tap **OK** to save the settings.

4 Web Configurations

On the web interface, you can configure and update the Device. For details, see "Access Standalone User's Manual". Here only describe the login operation on the web.

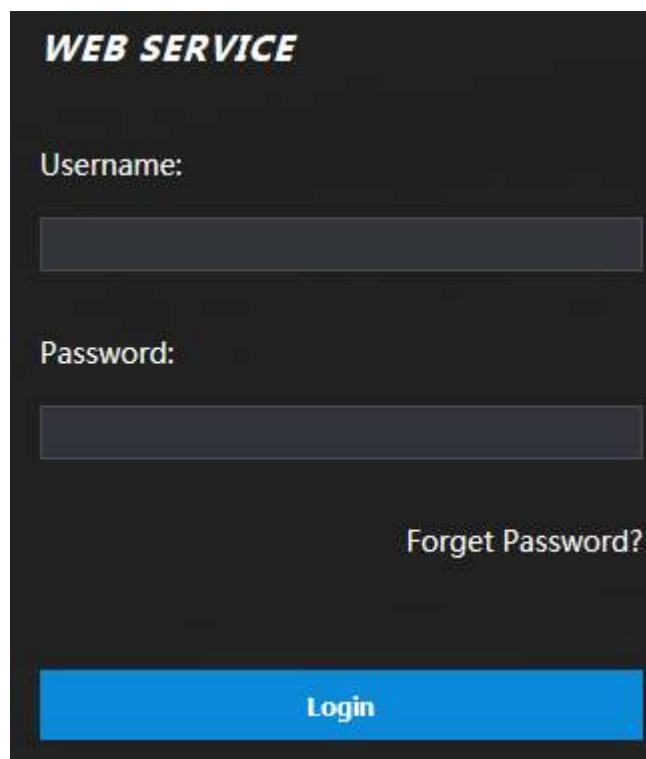
4.1 Logging in on Computer

Step 1 Go to the IP address (192.168.1.108 by default) of the Device in a browser, and press the Enter key.



- Make sure that the computer is on the same LAN as the Device.

Figure 4-1 Login



Step 2 Enter the user name and password.



- The default administrator name is admin, and the password is the one you set during initialization. We recommend you to change the administrator password regularly to increase security.
- If you forgot the administrator password, click **Forget Password?** to reset it.

Step 3 Click **Login**.

4.2 Logging in on Phone

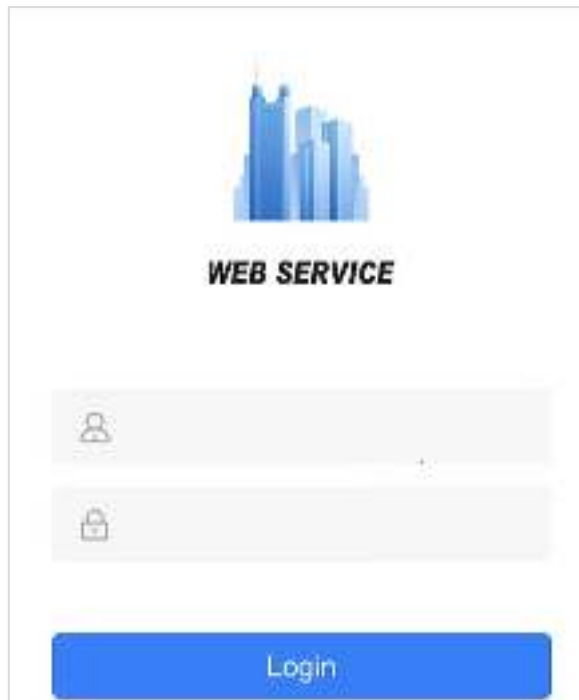
Make sure the Device is on the same LAN as your phone. Connect the Device to your phone hotspot or connect the Device and your phone to the same router.



Only certain parameters can be configured on the web portal if you log in on a phone.

Step 1 Go to the IP address (192.168.1.108 by default) of the Device in the browser.

Figure 4-2 Login



Step 2 Enter the user name and password.



- The default administrator name is admin, and the password is the one you set during initialization. We recommend you to change the administrator password regularly to increase security.

Step 3 Click **Login**.

Appendix 1 Fingerprint Registration Instructions

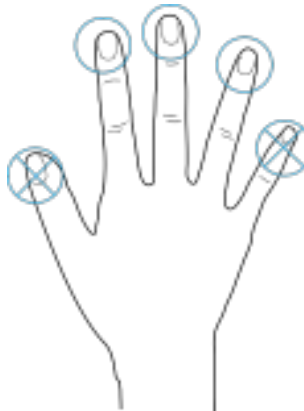
Before register your fingerprints, pay attention to the following:

- Make sure that your fingers are clean and dry.
- Press your finger on the center of the fingerprint scanner.
- Do not put the fingerprint sensor in a place with intense light, high temperature, and high humidity.
- If your fingerprints are unclear, use other unlocking methods.

Fingers Recommended

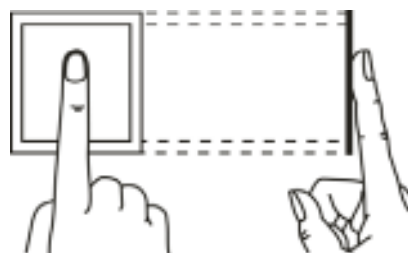
Forefingers, middle fingers, and ring fingers are recommended. Thumbs and little fingers cannot be put at the recording center easily.

Appendix Figure 1-1 Recommended fingers

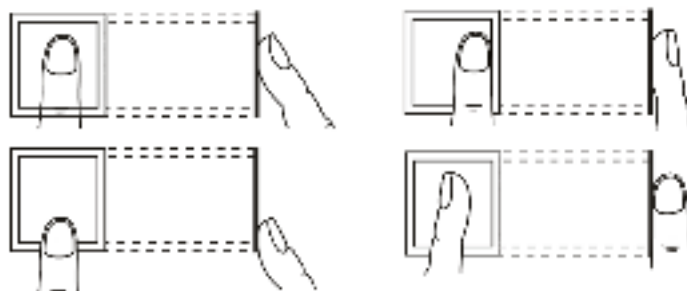


How to Press Your Fingerprint on the Scanner

Appendix Figure 1-2 Correct



Appendix Figure 1-3 Wrong



Appendix 2 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use overlapped characters, such as 111, aaa, etc.;

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. Physical Protection

We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. Audio and Video Encrypted Transmission

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. Network Log

Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. Construct a Safe Network Environment

In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.