

Access Standalone

Quick Start Guide








Foreword

General

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

Safety Instructions

The following categorized signal words with defined meaning 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 Date
V1.0.2	Updated the manual.	October 2022
V1.0.1	Add recommended installation height.	June 2020
V1.0.0	First release.	March 2020

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.

- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our 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 the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

This chapter describes the contents covering proper handling of the standalone, hazard prevention, and prevention of property damage. Read these contents carefully before using the standalone, comply with them when using, and keep it well for future reference.

Operation Requirement

- Do not place or install the standalone in a place exposed to sunlight or near the heat source.
- Keep the standalone away from dampness, dust or soot.
- Keep the standalone installed horizontally on the stable place to prevent it from falling.
- Do not drop or splash liquid onto the standalone, and make sure there is no object filled with liquid on the standalone to prevent liquid from flowing into the standalone.
- Install the standalone in a well-ventilated place, and do not block the ventilation of the standalone.
- Operate the standalone within the rated range of power input and output.
- Do not disassemble the standalone.
- Transport, use and store the standalone under the allowed humidity and temperature conditions.

Electrical Safety

- Improper battery use might result in fire, explosion, or inflammation.
- When replacing battery, make sure the same model is used.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the standalone; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Connect the device (I-type structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Dimensions and Components	1
2 Installation	3
2.1 Cable Connection	3
2.2 Device Installation	3
3 System Operation	6
3.1 Initialization.....	6
3.2 Adding New Users	7
4 Web Operation	10
5 Mobile Phone Operation	11
Appendix 1 Cybersecurity Recommendations	12

1 Dimensions and Components

Figure 1-1 Front view (mm [inch])

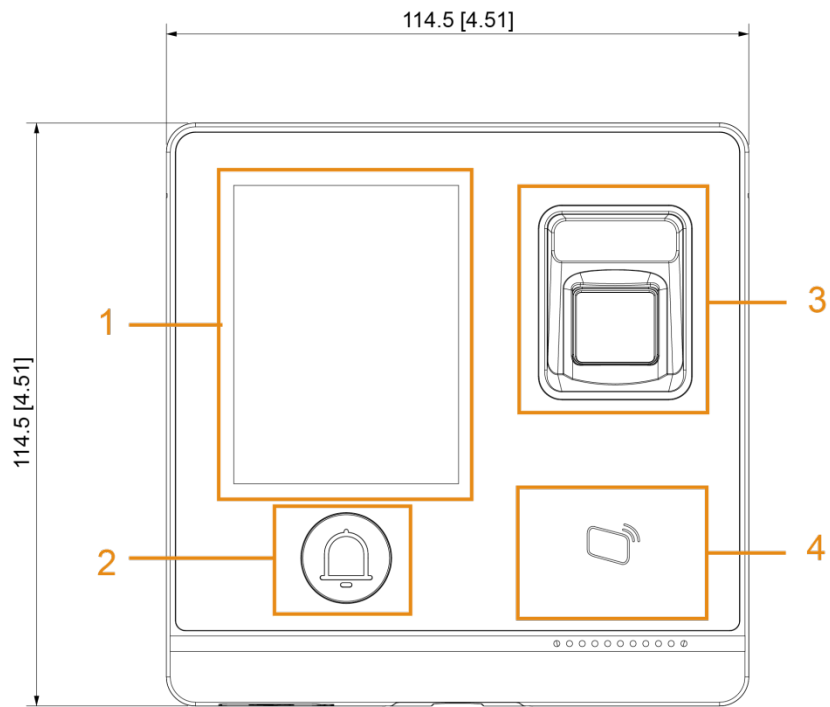


Figure 1-2 Back view (mm [inch])

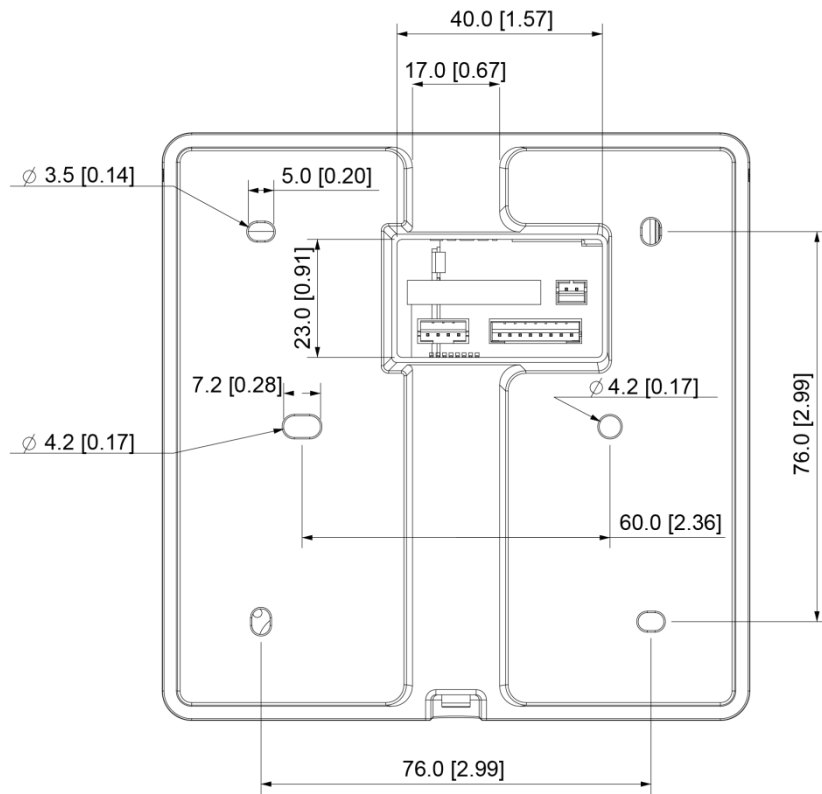


Figure 1-3 Side and bottom view (mm [inch])

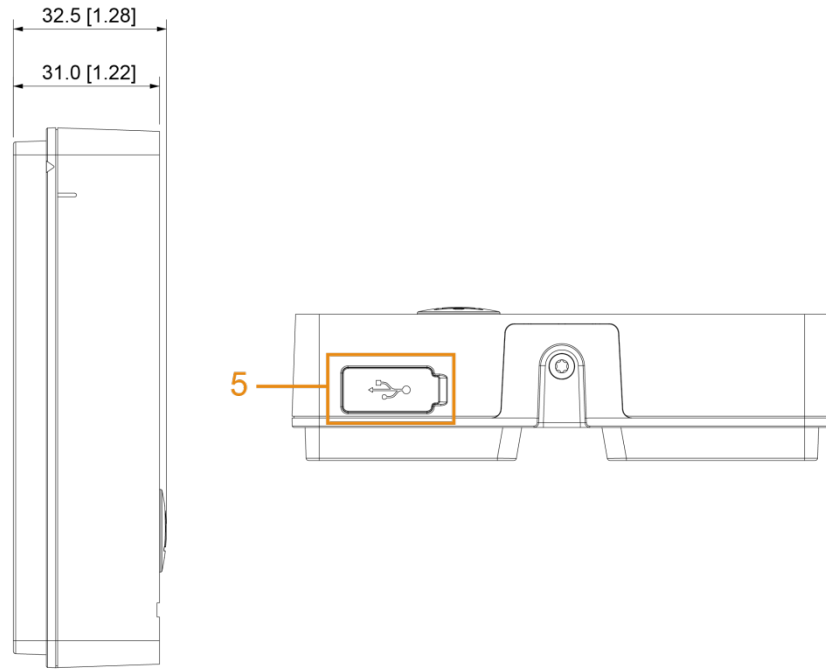


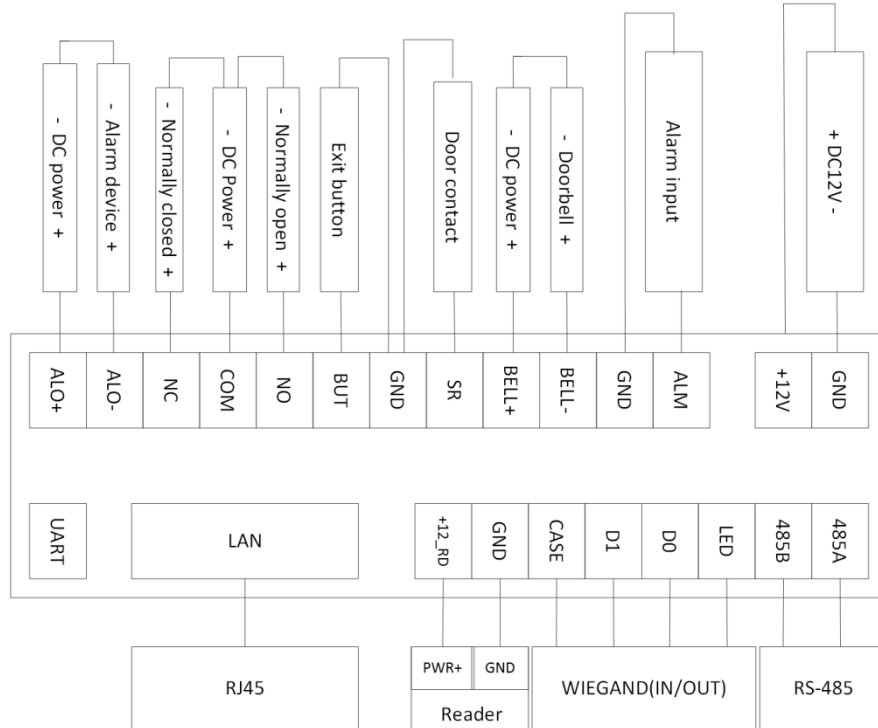
Table 1-1 Component description

No.	Name
1	VA area
2	Doorbell button
3	Fingerprint sensor
4	Card swiping area
5	USB port

2 Installation

2.1 Cable Connection

Figure 2-1 Cable connection



2.2 Device Installation

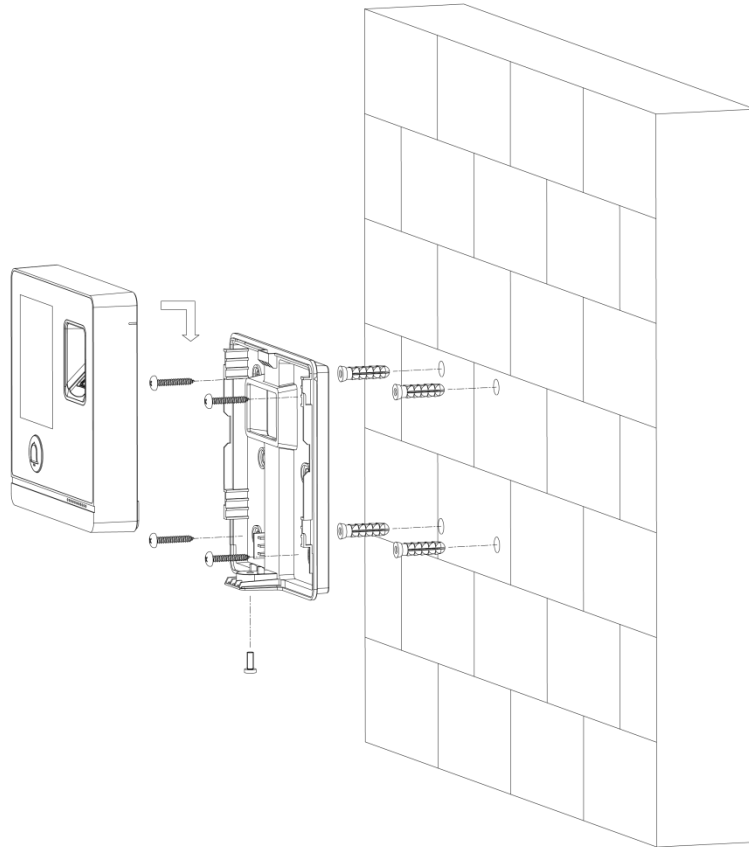


The recommended installation height is 1.4–1.6 meters.

The standalone supports surface installation and concealed installation.

Surface installation

Figure 2-2 Surface installation

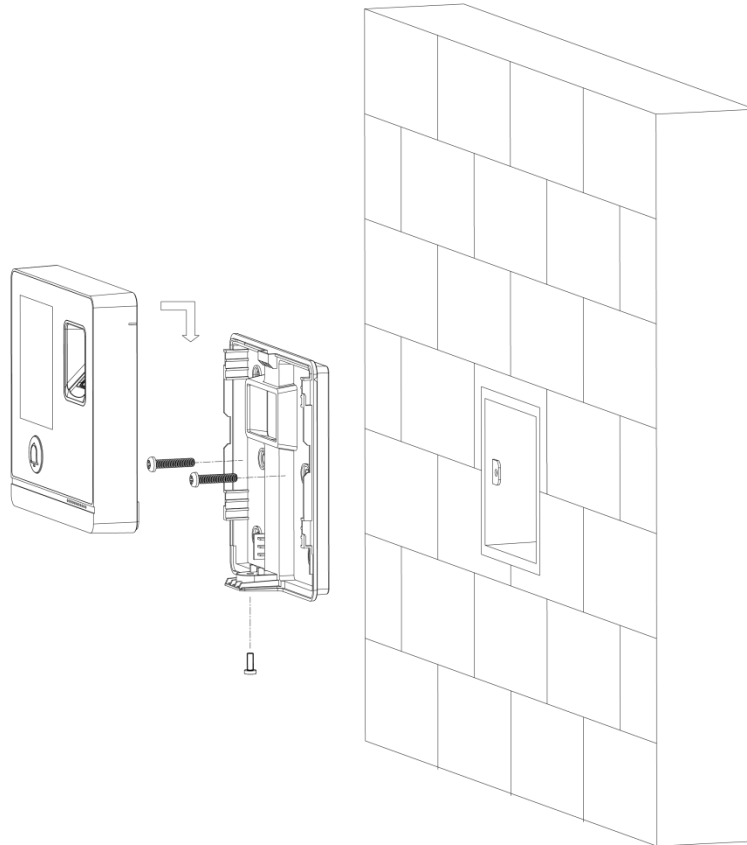


Installation Procedure

- Step 1 Stick installation map on the wall, and then drill holes according to hole positions on the map.
- Step 2 Insert expansion bolt into installation holes.
- Step 3 Fix the rear cover onto the wall with self-tapping screws.
- Step 4 Put machine screws through the bottom hole; lock the front cover on to the rear cover.

Concealed installation

Figure 2-3 Concealed installation



Installation Procedure

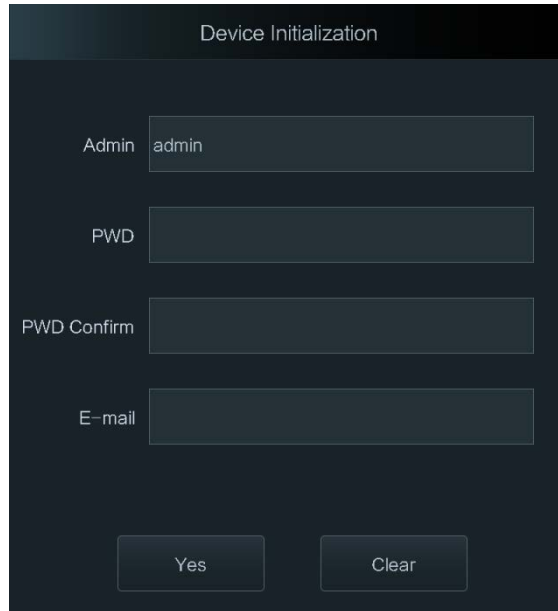
- Step 1 Draw the cables through the outlet.
- Step 2 Fix the back cover on the mounted box with screws.
- Step 3 Neaten the cables and buckle the front cover onto the back cover.

3 System Operation

3.1 Initialization

Administrator password and an email should be set the first time the standalone is turned on; otherwise the standalone cannot be used.

Figure 3-1 Initialization



Device Initialization

Admin admin

PWD

PWD Confirm

E-mail

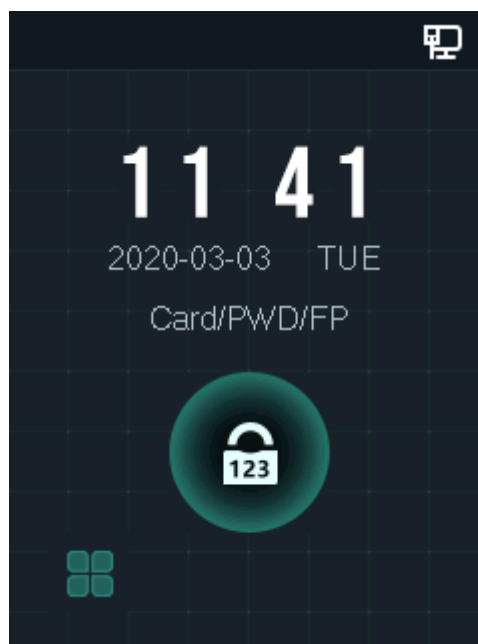
Yes Clear



- The administrator password can be reset through the email address you entered if the administrator forgets the administrator password.
- The password should consist of 8 to 32 non-blank characters and contain at least two types of characters among upper case, lower case, number, and special character (excluding ' " ; : &).

After the initialization is completed, the standby interface is displayed.

Figure 3-2 Standby interface



3.2 Adding New Users

You can add new users by entering their user IDs, names, importing fingerprint, passwords, selecting their user levels, and more.


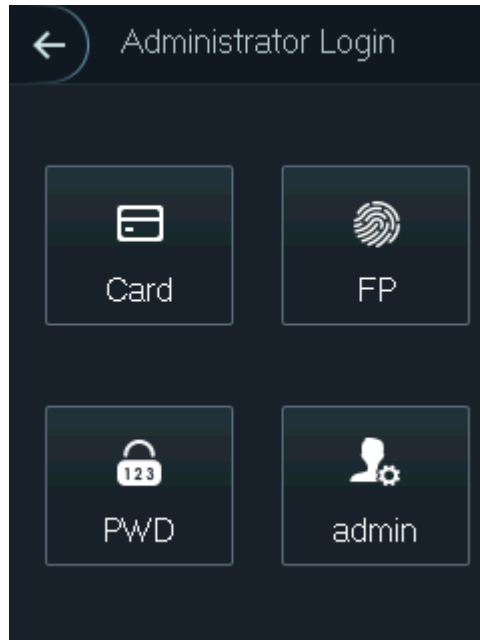
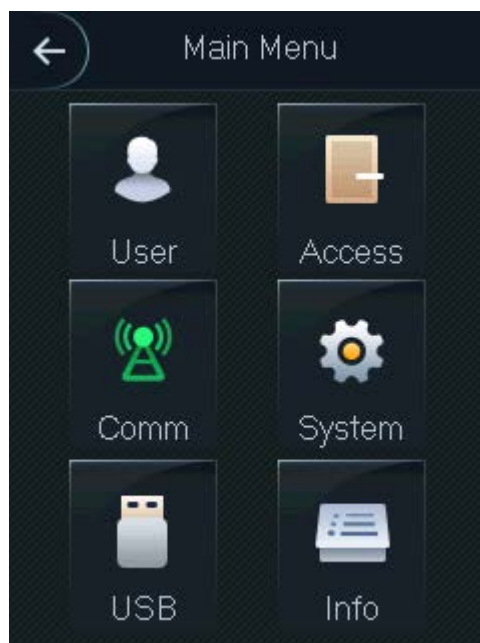
Step 1 Tap  on the standby interface.




Figure 3-3 Administrator login



Step 2 Select a main menu entering method.

Figure 3-4 Main menu



Step 3 Tap , and then tap 


The following figure is for reference only, and the actual interface shall prevail.

Figure 3-5 New user

Parameter	Value
User ID	1
Name	
FP	0
Card	0
PWD	
Permission	User

Step 4 Configure parameters on the interface.

Table 3-1 New user parameter description

Parameter	Description
User ID	You can enter user IDs. The IDs consist of 18 characters (including numbers and letters, but not special characters), and each ID is unique.
Name	You can enter names with at most 32 characters (including numbers, symbols, and letters).
FP	Fingerprint registration. Record the user's fingerprints.
Card	Card registration. Record the card information.
PWD	The door unlocking password. The maximum length of the ID digits is 8.
Permission	Set the user's permission: User or Admin . <ul style="list-style-type: none"> ● User: User only has the permission to unlock the door. ● Admin: Admin has the permission to unlock the door and configure the parameters.
Period	You can set a period in which the user can unlock the door. For detailed period settings, see the configuration manual.
Holiday Plan	You can set a holiday plan in which the user can unlock the door. For detailed holiday plan settings, see the configuration manual.
Valid Date	You can set a period during which the unlocking information of the user is valid.
User Type	<ul style="list-style-type: none"> ● General: General users can unlock the door normally. ● Restricted: When users in the blocklist unlock the door, service personnel will get a prompt. ● Guest: Guests are allowed to unlock the door certain times in certain periods. Once they exceed the maximum times and periods, they cannot unlock the door again. ● Patrol: Patrolling users can get their attendance tracked, but they have no unlock authority. ● VIP: When VIP unlocks the door, service personnel will get a prompt. ● Other: When special users unlock the door, there will be a delay of 5 seconds before the door is closed.
Use Time	When the user level is Guest , you can set the maximum number of times that the guest can unlock the door.

Step 5 After you have configured all the parameters, tap  to save the configuration.

4 Web Operation

The standalone can be configured and operated on the web. Through the web you can set parameters including network parameters, video parameters, and standalone parameters; and you can also maintain and update the system.

Login

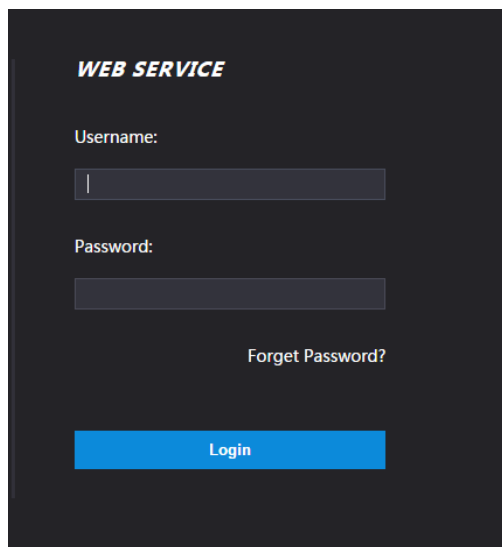


You need to set a password and an email address before logging in to the web for the first time.

Password that you set is used to log in to the web, and the email is used to retrieve passwords.

Step 1 Open IE web browser, enter the IP address (192.168.1.108 by default) of the standalone in the address bar, and then press Enter.

Figure 4-1 Login



Step 2 Enter the username and password.



- The default username of administrator is admin, and the password is the login password after initializing the standalone. Modify the administrator password regularly and keep it properly for security.
- If you forget the administrator login password, you can click **Forget Password?** to reset it. See the user manual.

Step 3 Click **Login**.

The homepage of the web is displayed.

5 Mobile Phone Operation

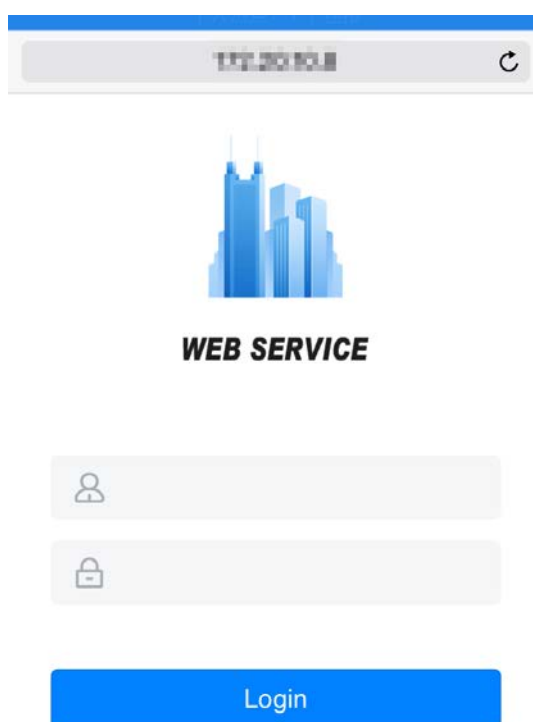
The standalone can be configured and operated on the mobile phone. Through the mobile phone you can set parameters including network parameters, video parameters, and standalone parameters; and you can also maintain and update the system.

Login

Step 1 Connect the device and mobile phone to the same network.

Step 2 Open the browser on the mobile phone, enter the IP address (it is displayed on the Wi-Fi interface, and 192.168.1.108 by default) of the standalone in the address bar, and then press Enter.

Figure 5-1 Login



Step 3 Enter the username and password.



The default username of administrator is admin, and the password is the login password after initializing the standalone. Modify the administrator password regularly and keep it properly for security.

Step 4 Click **Login**.

The homepage of the web is displayed.

Appendix 1 Cybersecurity Recommendations

1 Mandatory actions to be taken for basic device network security:

1. Use Strong Passwords

Appendix 2 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.

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

1. Physical Protection

Appendix 3 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

Appendix 4 We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

Appendix 5 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

Appendix 6 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

Appendix 7 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

Appendix 8 We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. MAC Address Binding

Appendix 9 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

Appendix 10 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

Appendix 11 If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

Appendix 12 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

Appendix 13 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.

Appendix 14 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

Appendix 15 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

Appendix 16 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.