



Network Transmission (Wireless Product)

FAQ



Foreword

This FAQ manual provides solutions and operation instructions for common device faults, parameter setting questions, and misunderstandings encountered in the actual use environment.

The descriptions in this document need to be analyzed in combination with the actual on-site device and are not to be regarded as the sole method of handling. If you have any questions, please contact the relevant technical support.

Symbols

The following symbols might appear in the manual.

Symbol	Description
 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, reductions in performance, or unpredictable results.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.1	- Added wireless bridge issues. - Added 4G/5G router issues. - Updated wireless AP and AC issues.	July 2026
V1.0.0	First release.	July 2024

Privacy Protection Notice

As the device user, you might collect the personal data of individuals such as their names, email addresses, face images, audio and fingerprints. You shall be fully responsible for any activities associated with processing personal data. You commit to comply with your local privacy protection laws and regulations to protect the legitimate rights and interests of individuals, and shall implement measures which are required by applicable law, including but not limited to, providing clear and comprehensive information to individuals before processing their personal data, obtaining consent from individuals when necessary, informing individuals of the existence of the surveillance area, and providing required contact information.

Intelligent Product Usage Statement

Intelligent products utilize AI technology to effectively enhance security. The intelligent recognition and alarm functions of the product might be affected by factors such as environmental lighting, camera angles, object obstructions, and network delays, potentially leading to false alarms, missed alerts, or response delays. This intelligent product is solely intended to be used as a security assistance tool. The results from performing identification are for reference only and do not constitute absolute guarantee of personal or property safety. Users need to combine these products with necessary physical security measures to enhance overall protection. Except as otherwise provided by laws or in the event of intentional or gross negligence on the part of the company, the company shall not be liable for any losses caused by the aforementioned factors not attributable to the company.

About the Manual

- This manual is provided for general reference only. Discrepancies might exist between the product and this manual, including but not limited to printed, electronic, or any other editions.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. Specifications and documentation are subject to change without prior notice. For the latest versions, as well as legal notices, consult the printed manual, the product webpage, our official website, or scan the QR code to access the electronic edition.
- The manual will be updated as necessary to reflect product changes and applicable legal requirements. These updates will not diminish your statutory rights, nor will they remove or weaken the safety information or essential instructions provided at the time of purchase.
- Although we make every effort to ensure accuracy, errors or deviations in descriptions of functions, operations, or technical data might occur. If there is any uncertainty or controversy, we reserve the right of final explanation.
- All trademarks, registered trademarks and company names referenced in this manual are the property of their respective owners.

Table of Contents

Foreword.....	I
1 Wireless Bridge Issues.....	1
1.1 How Many STAs can the Access Point Support.....	1
1.2 Elevator Bridge Signal Loss Beyond the 15th Floor.....	1
1.3 Network Transmission Abnormalities When Bridges are too Close.....	2
1.4 Severe Packet Loss When Pinging the Bridge from a Computer.....	3
1.5 Precautions for Connecting Different Models of Bridges.....	3
1.6 Poor Signal Strength after Bridge Connection.....	3
1.7 High Latency Despite Good Signal Strength After STA and Access Point Association.....	3
1.8 The DIP Switch Function on the Bridge.....	4
1.9 How to Select the Elevator Bridge Bandwidth.....	4
1.10 Signals of Mobile Base Stations are Affected by Elevator Bridges.....	4
1.11 Whether the Management IP Address of the Connected Bridges Need to be in the Same Segment.....	4
1.12 Frequently-Used Password to Log in to Web Manager of the Wireless Bridge.....	4
2 Wireless AP and AC.....	5
2.1 The Concept of Fat and Thin APs.....	5
2.2 Common Networking Methods for Fat and Thin APs.....	5
2.3 Differences Between Local Forwarding and Centralized Forwarding.....	5
2.4 Whether the EAC Series Supports Multiple VLANs.....	5
2.5 How to Configure the EAC Series for Multiple VLANs.....	5
2.6 Whether Roaming can be Achieved without an AC.....	6
2.7 AP Deployment Standards.....	6
2.8 What is the Default Management Address.....	6
2.9 How to Reset the Password if You Forgot it.....	6
2.10 How to Restore the Device to the Factory Settings.....	6
2.11 How to Make AP Device Online on an ER Series Router.....	6
2.12 Whether AC and AP Support VLAN.....	6
2.13 How to Upgrade the Router.....	7
2.14 How to Optimize Wireless Interference.....	7
2.15 What Determines the Number of AP devices that a Router can Manage.....	7
2.16 How to Handle Abnormality of the Web Manager.....	7
3 Concept Introduction.....	8
3.1 Differences Between Bridges and Switches.....	8
3.2 Differences Between Bridges and Routers.....	8
3.3 Why a Device with IP 192.168.1.251 cannot Communicate with a Gateway at IP 192.168.1.1 and Subnet Mask 255.255.255.128.....	8
4 4G/5G Router Issues.....	9

4.1 What are the Uplink and Downlink Speeds of a 4G Router.....	9
4.2 What are the Uplink and Downlink Speeds of a 5G Router.....	9
4.3 Terminal cannot Access the Internet after Connecting to the Router.....	9
4.4 Coverage Range of Omnidirectional Antennas.....	9
4.5 5G Router Fails to Negotiate 5G Connection.....	9
4.6 Router SIM Card cannot be Recognized.....	9
4.7 Router cannot Access the Internet after being Powered On.....	10
4.8 How to Reset Router Login Password.....	10
4.9 Terminal Device cannot Connect to the Router.....	10
Appendix 1 Security Commitment and Recommendation.....	12

1 Wireless Bridge Issues

1.1 How Many STAs can the Access Point Support

Theoretically, an access point can support any number of STAs within its coverage area. However, considering bandwidth limitations, the more STAs that connect, the weaker the bandwidth performance becomes. It is recommended to have a ratio of 1:3 (one access point to three STAs) at most, and it should not exceed a ratio of 1:8.

1.2 Elevator Bridge Signal Loss Beyond the 15th Floor

Possible Causes

- The bridge installation location is inappropriate.
- There are obstructions between the devices.

Solutions

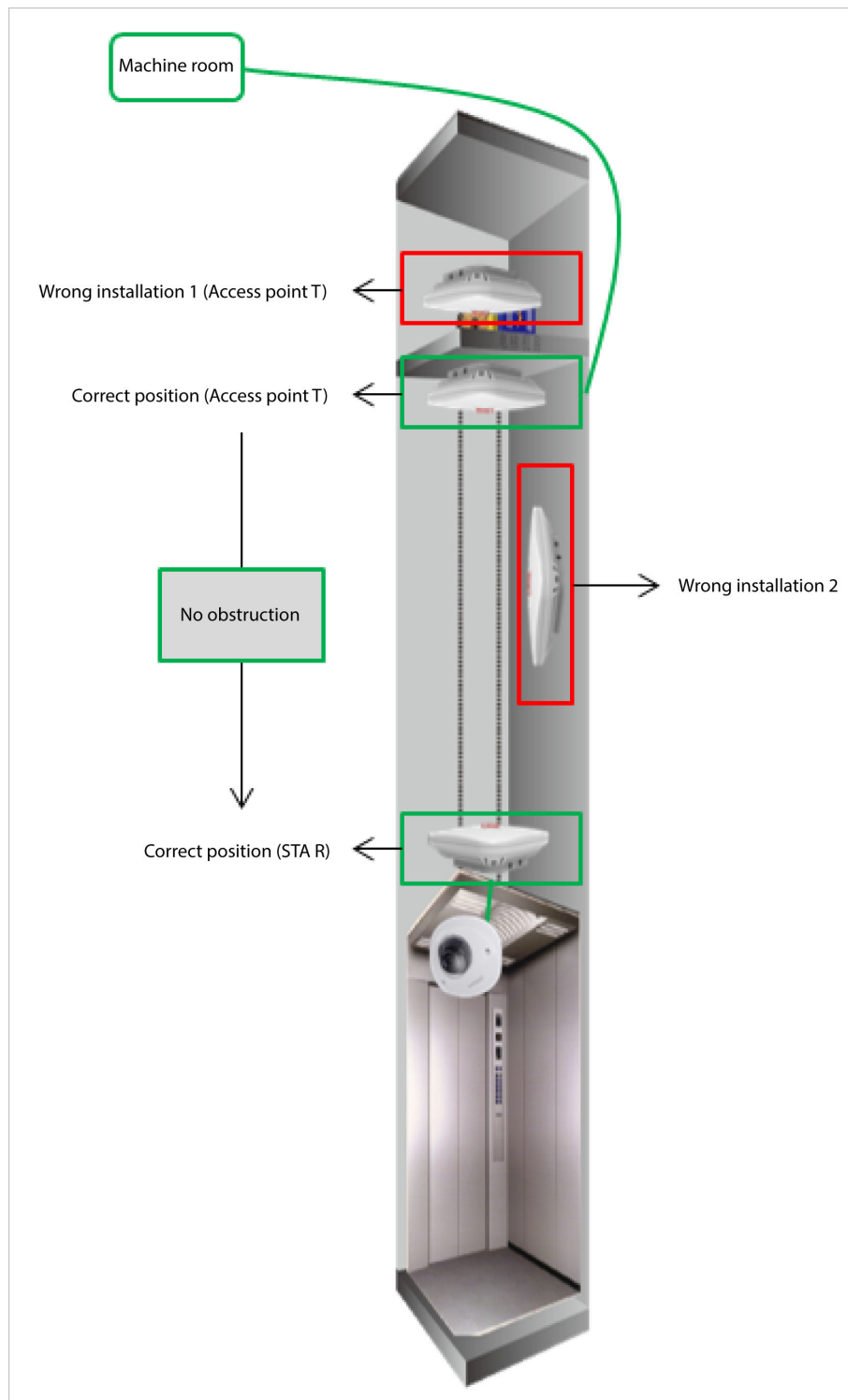
Adjust the installation location of the bridge.

Check if the problem is resolved. If not, contact technical support.



- Elevator bridges must be installed in pairs. The T unit acts as the access point, installed at the top of the elevator shaft and connected to the machine room. While the R unit acts as the STA, installed on the elevator car and connected to the cameras inside the car.
- There should be no obstructions between the 2 devices. Position 1 in the diagram represents an incorrect installation.
- Elevator bridges use directional antennas. The access point and STA should be installed facing each other. Position 2 in the diagram represents an incorrect installation.

Figure 1-1 Bridge installation location diagram



1.3 Network Transmission Abnormalities When Bridges are too Close

When bridges are too close to each other, signal overflow may occur. It is recommended to reduce the transmission power of the devices.

1.4 Severe Packet Loss When Pinging the Bridge from a Computer

Check the bridge signal strength and noise floor. If the environmental interference is relatively small, the noise floor of the received signal of the bridge is usually between -90 dBm and -100 dBm. In long-distance or high-interference environments, the noise value may increase to between -75 dBm and -85 dBm.

1.5 Precautions for Connecting Different Models of Bridges

Ensure that the bridge protocols are consistent. For example, the DH-PFM881 supports IEEE802.11 b/g/n, while the DH-PFM880E supports IEEE802.11 a/n/ac. When connecting, the mode should be adjusted to 802.11n.

1.6 Poor Signal Strength after Bridge Connection

Possible Causes

- The antennas of the two devices are not aligned.
- There are obstructions between the devices.
- Wireless interference exists between the devices.
- The device's output power is not set to maximum.

Solutions

1. Align the antennas of the two devices and check if the problem is resolved.
2. Check for obstructions between the devices. If obstructions are found, remove them or change the installation location of the devices and check if the problem is resolved.
3. Adjust the device frequency and channel width and check if the problem is resolved.
4. Log in to the device's web interface, go to the **Wireless Basic Settings** page, and set the device's output power to maximum.
5. Check if the problem is resolved. If not, contact technical support.

1.7 High Latency Despite Good Signal Strength After STA and Access Point Association

Possible Causes

- Wired link failure, such as poor-quality network cables or loose connections.
- Co-channel or adjacent-channel wireless interference in the surrounding environment.

Solutions

1. Replace the network cables with high-quality ones and ensure all connections are secure.
2. Adjust the device frequency and channel width.

3. Check if the problem is resolved. If not, contact technical support.

1.8 The DIP Switch Function on the Bridge

Dial the DIP code to the corresponding letter to select whether the current device is on the STA side or the Host side (access point).

C = STA (camera end, STA side), H = Host (recorder end, access point).

1.9 How to Select the Elevator Bridge Bandwidth

- If the on-site wireless environment is complex, select 20 MHz.
- If the on-site wireless environment is simple, select 40 MHz.

1.10 Signals of Mobile Base Stations are Affected by Elevator Bridges

The high-frequency part of the elevator bridge in the 2.4G frequency band partially overlaps with the signal transmitted by the mobile base station. It is sufficient to appropriately reduce the bandwidth and select low frequency band.

1.11 Whether the Management IP Address of the Connected Bridges Need to be in the Same Segment

It can be both in the same segment and different segments. When in the same segment, make sure that the IP address of the connected bridge and that of the client should be different.

1.12 Frequently-Used Password to Log in to Web Manager of the Wireless Bridge

Table 1-1 User and password

User name	Password
admin	admin123
admin	admin
root	admin

2 Wireless AP and AC

2.1 The Concept of Fat and Thin APs

Fat APs usually come with their own complete operating systems and are standalone network devices that can perform functions such as dial-up and routing, for example, wireless routers.

Thin APs remove many loaded functions such as routing, DNS, and DHCP server from fat APs, retaining only the wireless access part.

2.2 Common Networking Methods for Fat and Thin APs

Fat APs can be used independently and are suitable for small and micro enterprises and home use.

Thin APs need to be used in conjunction with an AC (Access Controller) and are suitable for small and medium-sized office networks. The AC centrally configures and manages thin APs.

2.3 Differences Between Local Forwarding and Centralized Forwarding

The networking solution of AC with thin APs has become the mainstream wireless local area network (WLAN) networking mode. Local forwarding and centralized forwarding are two traffic forwarding models based on this solution.

- Centralized forwarding means that all data is sent to the AC for centralized processing and then forwarded by the AC.
- Local forwarding means that all data does not need to be processed by the AC but is forwarded locally by the AP.

2.4 Whether the EAC Series Supports Multiple VLANs

Yes.

2.5 How to Configure the EAC Series for Multiple VLANs

Deployment method: the EAC series are deployed in bypass mode.

1. VLANX is used as the AP management VLAN.
2. The VLAN ID in the AP is set to the corresponding service VLAN.
3. The switch port connected to the EAC must be configured as access VLANX.
4. The path from the core switch to the AP should be set as trunk. The service VLAN should be tagged, and the PVID should be set to X.



X indicates the VLAN ID.

2.6 Whether Roaming can be Achieved without an AC

Roaming cannot be achieved without an AC.

- Without an AC, terminals will only actively disconnect from the previous AP signal and reconnect to a new AP signal when the AP signal is extremely weak, resulting in a poor user experience and no roaming capability.
- With an AC, the AC will proactively select a better AP signal for the terminal based on its location, avoiding signal interruption and thus achieving roaming.

We recommend using an AC for centralized management to enable roaming for connected terminals.

2.7 AP Deployment Standards

To avoid mutual interference between signals, we recommend keeping at least 1 meter between APs and Wi-Fi devices.

2.8 What is the Default Management Address

- Domain name: dahuanetwork.com
- IP address: 192.168.10.1

2.9 How to Reset the Password if You Forgot it

Reset it through the email address configured during device initialization.

2.10 How to Restore the Device to the Factory Settings

- Press the Reset button on the device for 5 seconds until the system indicator is solid on.
- Log in to the web manager, select **Local Device Config** > **System Management** > **System Settings** > **Configurations Management**, and then click **Restore** to restore the device to the factory settings.

2.11 How to Make AP Device Online on an ER Series Router

Make sure that the ER series router has enabled the AP function by default and the AC and AP networks are accessible.

The AP can automatically come online in the AC and will automatically synchronize the configuration information in the AC, making it plug-and-play.

2.12 Whether AC and AP Support VLAN

AC in ER series and AP in EAP series support VLAN function, which can be configured in **Network Management** > **Wired** > **LAN Config**.

2.13 How to Upgrade the Router

- Update the device on the web manager: local upgrade or online upgrade.
- Update the device on the DoLynk Care.

2.14 How to Optimize Wireless Interference

Configure the AP channel to a non-overlapping channel on the ER series router (for example, adjust the 2.4G channel to 1, 6, 11, and the bandwidth to 20 MHz), and appropriately adjust the AP transmission power according to the actual environment to reduce wireless interference.

2.15 What Determines the Number of AP devices that a Router can Manage

The number of AP devices that a router can manage is determined by the specific router model, and there is no need to purchase additional licenses.

2.16 How to Handle Abnormality of the Web Manager

Close this web page, and then reopen it in the browser.

3 Concept Introduction

3.1 Differences Between Bridges and Switches

The basic functions of a LAN switch are the same as those of a bridge, including frame forwarding, frame filtering, and spanning tree algorithm functions. The differences between them are as follows:

- Operation mode: When a switch operates, it allows multiple channels between groups of ports to work simultaneously. The functionality of a switch goes beyond that of a single bridge; it is a collection of multiple bridge functions. While a bridge typically has two ports, a switch has a high-density port configuration.
- Segmentation capability: A switch can support multiple ports and can divide a network system into more physical segments, resulting in higher overall network bandwidth. In contrast, a bridge, which only supports two ports, has a very limited ability to segment the network physically.
- Transmission rate: Compared to a bridge, a switch has a faster data transmission rate.
- Frame forwarding method: A bridge uses a per-frame forwarding method, meaning each data frame is received and forwarded to the target network without any processing. In contrast, a switch has a forwarding table (also known as a MAC address table) that allows it to forward data frames only to the target port based on the destination MAC address, thereby improving forwarding efficiency.

3.2 Differences Between Bridges and Routers

- Bridges are Layer 2 devices, while routers are Layer 3 devices.
- Bridges can only connect two identical networks, whereas routers can connect different networks.
- Bridges do not isolate broadcasts, but routers can. A bridge, also known as a bridging device, is a store-and-forward device that interconnects LANs at the link layer. It receives MAC frames from one LAN, disassembles, checks, and verifies them, and then reassembles them in the format of another LAN before sending them to its physical layer. As a link-layer device, a bridge does not process headers added by protocols above the data link layer.

3.3 Why a Device with IP 192.168.1.251 cannot Communicate with a Gateway at IP 192.168.1.1 and Subnet Mask 255.255.255.128

Subnet mask defines network segment range. A subnet mask of 255.255.255.128 indicates that the usable IP addresses in the 192.168.1.0 subnet are 192.168.1.1 to 192.168.1.127. Since 192.168.1.251 is outside this range, it cannot communicate with the gateway.

4 4G/5G Router Issues

4.1 What are the Uplink and Downlink Speeds of a 4G Router

The theoretical downlink speed is 100 Mbps, and the uplink speed is 50 Mbps. The actual speeds depend on the surrounding network environment and the SIM card used.

4.2 What are the Uplink and Downlink Speeds of a 5G Router

The theoretical downlink speed is 1920 Mbps, and the uplink speed is 600 Mbps. The actual speeds depend on the surrounding network environment and the SIM card used.

4.3 Terminal cannot Access the Internet after Connecting to the Router

Solutions:

1. If the terminal is connected to the router via a wired connection, it is recommended to use DHCP mode to obtain a dynamic IP address.
2. If the terminal uses a static IP address, the gateway address must be set to the IP address of the router's LAN port.

4.4 Coverage Range of Omnidirectional Antennas

When using omnidirectional antennas, the maximum coverage range is 100 meters in an unobstructed and interference-free environment.

4.5 5G Router Fails to Negotiate 5G Connection

Confirm the 5G base station coverage in your area. You can perform a comparative test using the same data SIM card on a 5G mobile phone.

4.6 Router SIM Card cannot be Recognized

Some products do not support hot-swapping of SIM cards. The SIM card must be inserted before powering on the device. Insert the card first, then power on the device.

4.7 Router cannot Access the Internet after being Powered On

- Some devices can choose between wired and cellular connections for internet access. If using a wired WAN port, ensure that the WAN port settings match those provided by the ISP. If using cellular data, ensure that no device is connected to the wired WAN port, or set the cellular connection's priority to 1 in the port settings.
- The cellular module requires some time to initialize. Wait until the 5G or 3G/4G indicator light turns on before attempting to access the internet. If the light does not turn on after a while, log in to the WEB interface and click **Quick Detection** on the **Status Management** page to preliminarily determine the cause.

4.8 How to Reset Router Login Password

During device initialization, you are prompted to enter a reserved phone number. You can reset the password using the phone number as prompted. If the phone number is no longer in use, press and hold the reset button on the side of the device for more than 5 seconds. When all the indicator lights turn on and then off, it indicates that the reset is successful. You can then reinitialize the device to set a new password and reserved phone number.

4.9 Terminal Device cannot Connect to the Router

Wired Connection is Available, but Wi-Fi Connection is not Available

1. Confirm whether the password is correct.
2. Confirm the encryption method. If the encryption method is WPA3-AES, modify it to WPA/WPA2-PSK.



The devices with older version do not support WPA3-AES.

3. Reconnect the devices at a position about 1 meter away from the router and without any walls blocking it.
4. If there are any additional terminal devices, connect them to Dahua router to confirm whether the connection can be successful. If there are routers from other manufacturers, connect them to routers from other manufacturers to confirm whether the connection can be successful, so as to check whether there is a problem with the terminal devices.
5. Restart the router and reconnect them.

Wi-Fi Connection is Available, but Wired Connection is not Available

1. Make sure the terminal device is correctly inserted into the LAN port. Insert the terminal device to all LAN ports to confirm whether it can connect normally.
2. Disable and enable the wired network card of the terminal device and then reconnect.
3. Check if the crystal head of the network cable is damaged. Replace the network cable to check if it works properly.
4. Restart the router and reconnect them.

Neither Wi-Fi Connection nor Wired Connection is Available

1. Restore the router to factory settings, complete the configuration according to the wizard, and then reconnect.
2. Follow the steps from Wired Connection is Available, but Wi-Fi Connection is not Available and Wi-Fi Connection is Available, but Wired Connection is not Available.

Appendix 1 Security Commitment and Recommendation

Zhejiang Dahua Vision Technology Co., Ltd. (hereinafter referred to as "Dahua") attaches great importance to cybersecurity and privacy protection, and continues to invest special funds to comprehensively improve the security awareness and capabilities of Dahua employees and provide adequate security for products. Dahua has established a professional security team to provide full life cycle security empowerment and control for product design, development, testing, production, delivery and maintenance. While adhering to the principle of minimizing data collection, minimizing services, prohibiting backdoor implantation, and removing unnecessary and insecure services (such as Telnet), Dahua products continue to introduce innovative security technologies, and strive to improve the product security assurance capabilities, providing global users with security alarm and 24/7 security incident response services to better protect users' security rights and interests. At the same time, Dahua encourages users, partners, suppliers, government agencies, industry organizations and independent researchers to report any potential risks or vulnerabilities discovered on Dahua devices to Dahua PSIRT, for specific reporting methods, please refer to the cyber security section of Dahua official website.

Product security requires not only the continuous attention and efforts of manufacturers in R&D, production, and delivery, but also the active participation of users that can help improve the environment and methods of product usage, so as to better ensure the security of products after they are put into use. For this reason, we recommend that users safely use the device, including but not limited to:

Account Management

1. Use complex 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: 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 repeating characters, such as 111, aaa, etc.

2. Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. Enable account lockout function

The account lockout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. Set and update password reset information in a timely manner

Dahua device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. **Enable HTTPS**

It is recommended that you enable HTTPS to access Web services through secure channels.

2. **Encrypted transmission of audio and video**

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

3. **Turn off non-essential services and use safe mode**

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

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

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

4. **Change HTTP and other default service ports**

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allowlist**

It is recommended that you turn on the allowlist function, and only allow IP in the allowlist to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.

2. **MAC address binding**

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. **Build a secure network environment**

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
- According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
- Establish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

It is recommended to check online users regularly to identify illegal users.

2. **Check device log**

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

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

Software Security

1. **Update firmware in time**

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

We recommend you to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188