




dahua Ethernet Switch 16&24-port Cloud Managed Switch User Guide

[Home](#) » [Dahua](#) » dahua Ethernet Switch 16&24-port Cloud Managed Switch User Guide 

Contents

- [1 dahua Ethernet Switch 16&24-port Cloud Managed Switch](#)
- [2 Foreword](#)
- [3 Important Safeguards and Warnings](#)
- [4 Overview](#)
 - [4.1 Introduction](#)
 - [4.2 Features](#)
- [5 Port and Indicator](#)
- [6 Installation](#)
- [7 Initializing and Adding the Switch](#)
 - [7.1 Initializing the Switch](#)
 - [7.2 Adding the Switch](#)
- [8 Related Information](#)
- [9 Appendix](#)
- [10 Documents / Resources](#)
- [11 Related Posts](#)



dahua Ethernet Switch 16&24-port Cloud Managed Switch








Foreword

General

This manual introduces the installation, functions and operations of the 16&24-port cloud managed switch (hereinafter referred to as “the Switch”). Read carefully before using the device, and keep the manual safe for future reference.

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, 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 PoE description.	March 2023
V1.0.0	First release.	March 2023

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license 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 device.
- 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, and comply with the guidelines when using it.

Transportation Requirements

Transport the device under allowed humidity and temperature conditions.

Storage Requirements

Store the device under allowed humidity and temperature conditions.

Installation Requirements

- Do not connect the power adapter to the device while the adapter is powered on.
- Strictly comply with the local electrical safety code and standards. Make sure that the ambient voltage is stable and meets the power supply requirements of the device.
- Personnel working at heights must take all necessary measures to ensure personal safety including wearing a helmet and safety belts.
- Do not place the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Put the device in a well-ventilated place, and do not block its ventilation.
- Use an adapter or cabinet power supply provided by the manufacturer.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- Do not connect the device to two or more kinds of power supplies, to avoid damage to the device.
- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.

- The device must be grounded by a copper wire with a cross-sectional area of 2.5 mm² and a ground resistance no more than 4 Ω.
- Voltage stabilizer and lightning surge protector are optional depending on the actual power supply on site and the ambient environment.
- To ensure heat dissipation, the gap between the device and the surrounding area should not be less than 10 cm on the sides and 10 cm on top of the device.
- When installing the device, make sure that the power plug and appliance coupler can be easily reached to cut off power.

Operation Requirements

- Do not disassemble the device without professional instruction.
- Operate the device within the rated range of power input and output.
- Make sure that the power supply is correct before use.
- Make sure the device is powered off before disassembling wires to avoid personal injury.
- Do not unplug the power cord on the side of the device while the adapter is powered on.
- Use the device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Operating temperature: -10 °C to +55 °C (+14 °F to +131 °F).
- This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- Do not block the ventilator of the device with objects, such as a newspaper, table cloth or curtain.
- Do not place an open flame on the device, such as a lit candle.

Maintenance Requirements

- Power off the device before maintenance.
- Mark key components on the maintenance circuit diagram with warning signs.

Overview

Introduction

Cloud managed switch is a layer-2 commercial switch. With its long-distance PoE function, it can supply power to devices up to 250 meters away. The Switch has PoE red port functions with the PoE power supply as high as 90 W. The PoE total power of the 16-port switch is as high as 240 W, and the 24-port switch is as high as 360 W. In addition, based on the DoLink Care Cloud Server, this Switch can be managed through the DoLink Care app, the network topology diagram function can be used to quickly locate the problem. The Switch is applicable for uses in different scenarios, including homes, factories and offices.

In Extend Mode, the transmission distance of the PoE port is up to 250 meters but the transmission rate drops to 10 Mbps. The actual transmission distance might vary due to power consumption of connected devices or the cable type and status.

Features

- 16/24 × 100/1000 Mbps PoE Ethernet ports, 2 × 100/1000 Mbps Ethernet ports, and 2 × 1000 Mbps optical ports (Combo).
- The gray ports conform with IEEE802.3af and IEEE802.3at standards, the orange ports conform with Hi-PoE standard and the red ports conform with IEEE802.3bt standards.
- Supports network topology visualization.
- Supports 250 m long-distance power supply.

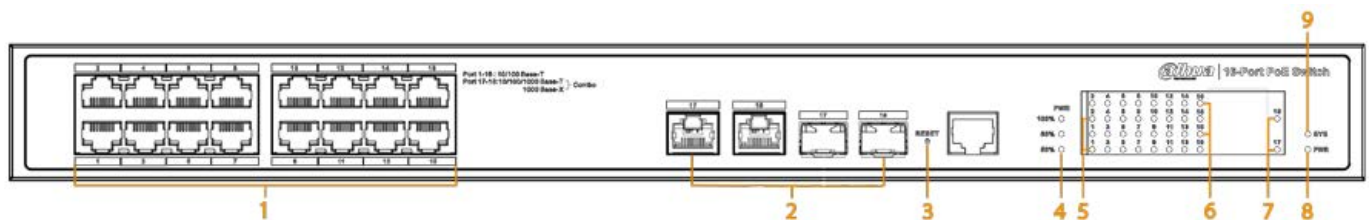
In Extend Mode, the transmission distance of the PoE port is up to 250 meters but the transmission rate drops to 10 Mbps. The actual transmission distance might vary due to power consumption of connected devices or the cable type and status.

- Features mobile management by app.
- Supports LLDP (Link Layer Discovery Protocol).
- Supports DHCP (Dynamic Host Configuration Protocol) Client.
- Desktop mount and rack mount.

Port and Indicator

Front Panel

The following figure uses a 16-port 100 Mbps cloud managed switch as an example, and might differ from the actual product.



No.	Name	Description
1	PoE ports	16/24 × 10/100 Mbps or 10/100/1000 Mbps self-adaptive Ethernet ports.
2	Uplink ports	10/100/1000 Mbps self-adaptive Ethernet ports and 1000 Mbps optical ports.
3	Reset button	Press and hold it for more than 5 seconds, and release after the panel status indicators all turn on to restore the Switch to default settings.
4	PoE output power indicator	<ul style="list-style-type: none"> Only solid green: PoE output power ≤ 50%. Solid green and red: 50% < PoE output power ≤ 80%. Solid green, yellow and red: 80% < PoE output power.
5	Link/Act indicator	<ul style="list-style-type: none"> On: Connected to device. Off: Not connected to device. Flashing: Transmitting data.
6	PoE port status indicators	<ul style="list-style-type: none"> On: Powered by PoE. Off: Not powered by PoE.
7	Uplink port status (Link) indicators	<ul style="list-style-type: none"> On: Connected to device. Off: Not connected to device.
8	Power indicator	<ul style="list-style-type: none"> On: Power on. Off: Power off.
9	System status indicator (SYS)	<ul style="list-style-type: none"> Indicator flashes quickly (1 second interval): Start up. Indicator flashes slowly (2 seconds interval): Normal operation.

Rear Panel



No.	Name	Description
1	DIP switch	—
2	Power port	Supports 53 VDC.
3	Ground terminal	<p>Connecting GND.</p> <ul style="list-style-type: none"> ● Normal GND connection of the Switch guarantees device lightning protection and anti-interference. You must connect the GND cable before powering on the Switch and power off the Switch before disconnecting the GND cable. ● The sectional area of the GND cable must be more than 2.5 mm^2, and the GND resistance must be less than 4Ω.

Installation

Preparation

- Select an appropriate installation method as needed.
- Install the Switch on a solid and flat surface.
- Leave around 10 cm of open space around the Switch for heat dissipation and to ensure good ventilation.

Desktop Mount

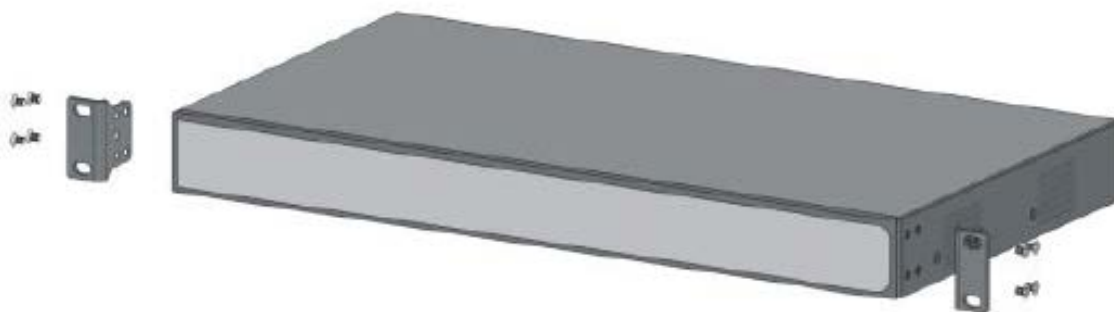
The Switch supports desktop mount. You can directly place it on a solid and flat desktop.

Rack Mount

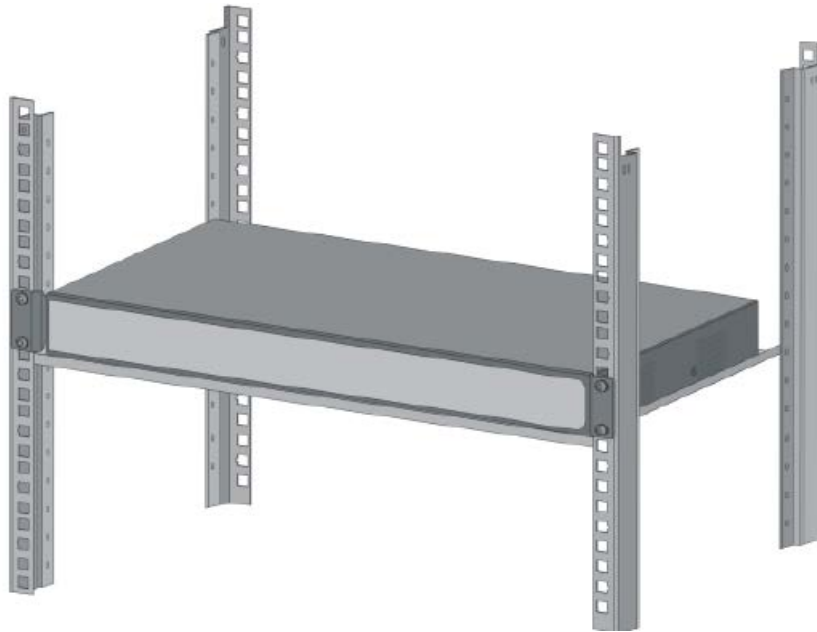
The Switch supports rack mount.

Procedure

- **Step 1** Attach the mounting brackets to the Switch (one on each side), and fix them with the provided screws.



- **Step 2** Fix the Switch onto the rack.



Initializing and Adding the Switch

Initializing the Switch

Background Information

You can initialize devices and modify the IP address of devices using the ConfigTool.

- ConfigTool can be downloaded from the Dahua official website, and the link is <https://support2.dahuasecurity.com/en>.
- Device initialization is required for first-time use or after the Switch has been reset.
- Device initialization is available only when the Switch (IP address is 192.168.1.110 by default) and the computer are on the same network segment.
- Plan the network segment properly to connect the Switch to the network.

Procedure

- **Step 1** Double-click “ConfigTool.exe” to open the tool.
- **Step 2** Tap Search Setting.
- **Step 3** Enter the start IP address and end IP address of the network segment on which you want to search for devices, and then tap OK.

Setting

×

☒ Current Segment Search
 ☒ Other Segment Search

Start IP

192 . 168 . 1 . 1

End IP

192 . 168 . 1 . 255


Username


admin

Password

•••••

OK

- Step 4 Tap  on the Modify IP screen, and search for devices on the network segment that you have arranged.

 Configtool

Modify IP

Device Upgrade

Device Config


System Settings

Password Reset

Building Config

CGI Protocol

51 Device(s) found



Search Setting

⌵

—

×

Initialize

Batch Modify IP

Import

Export

Manual Add

Delete

Search

<input checked="" type="checkbox"/>	NO.	Status	Type	Model	IP	MAC	Version	Operate
<input checked="" type="checkbox"/>	1	Uninitialized	TS		192.168.1.110		V1.000.000...	Edit Details Web

You have selected 1 device(s)

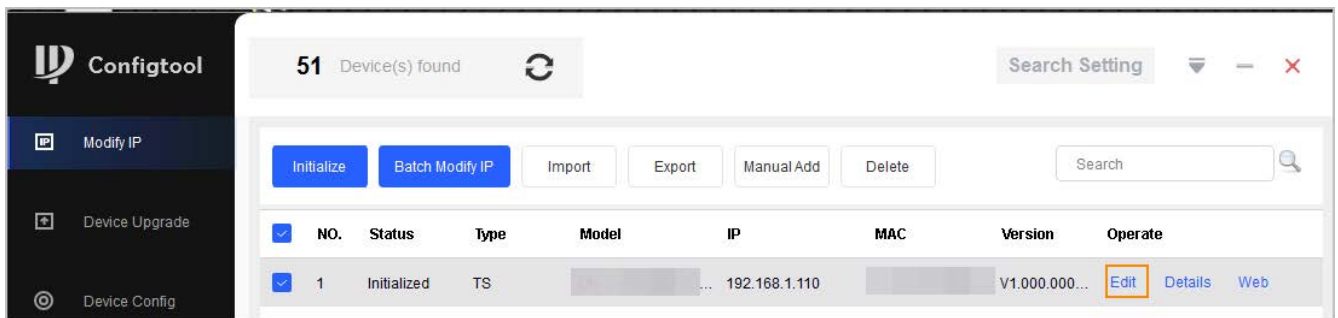
☒ Uninitialized

☐ Initialized

IPv4

IPv6

- Step 5 Select the devices that need initialization, and then tap Initialize.



- **Step 9** Tap Static mode, and then enter target IP, subnet mask, and gateway.

The Switch target IP address must be on the same network segment as the computer.

Modify IP Address

Mode

☒ Static
 ☐ DHCP

Target IP

Subnet Mask

Gateway

OK

Selected number of devices: 1

- **Step 10** Tap OK.

Adding the Switch

Scan the QR code and add the Switch to the DoLink Care app.

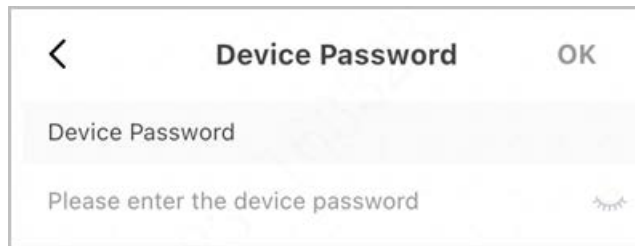
Procedure

- **Step 1** Open the DoLink Care app.
- **Step 2** Tap + on the upper-right corner of the Home screen, and scan the QR code of the Switch.



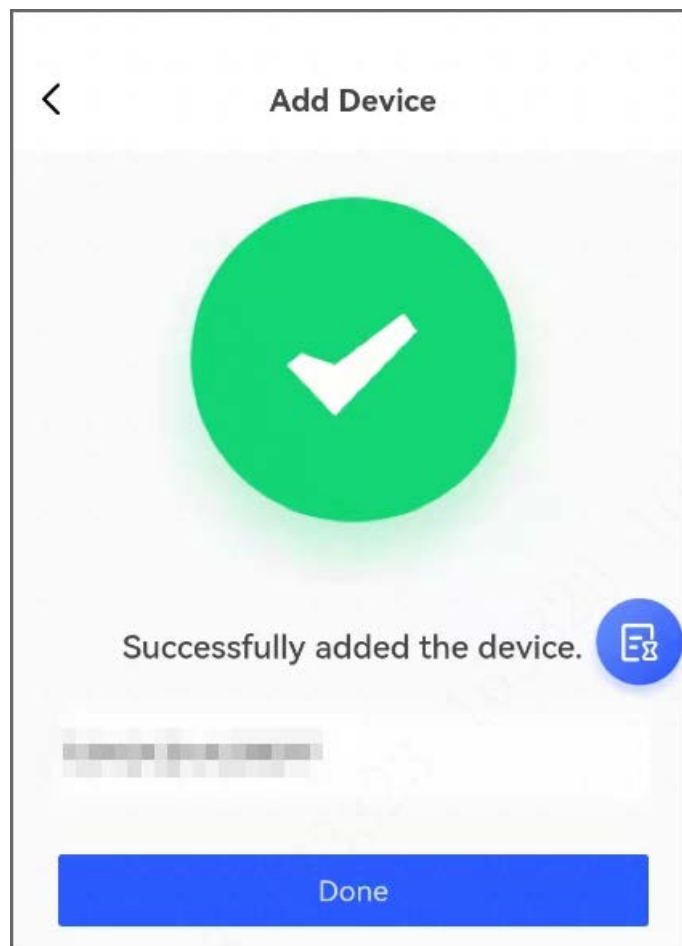
- **Step 3** If the Switch has not been initialized, you need to enter the SC password on the label, and then tap OK. Enter the device password, and then tap OK.

If the Switch has been initialized, you do not need to enter the SC password. Enter the device password, and then tap OK.



- **Step 4** Tap Done.

Select Me > HELP > User's_Manual in DoLynk Care for more details.



Related Information

Scan the QR code below to get the DoLynk Care app.



Appendix

Appendix 1 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 from Dahua 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.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

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

Documents / Resources

 Ethernet Switch 16&24-port Cloud Managed Switch Quick Start Guide  <small>Dahuang Dahua Technology Co., Ltd. 1/12</small>	<p>dahua Ethernet Switch 16&24-port Cloud Managed Switch [pdf] User Guide</p> <p>Ethernet Switch 16 24-port Cloud Managed Switch, Ethernet, Switch 16 24-port Cloud Managed Switch, Cloud Managed Switch, Managed Switch</p>
--	--