Splicing Controller

Quick Start Guide



V1.0.0

Foreword

General

This manual introduces the installation, functions and operations of the splicing controller (hereinafter referred to as the "device"). Read carefully before using the device, and keep the manual safe for future reference.

Models

- DSCON8000-S13 (5U Case)
- DSCON8000-S24 (8U Case)

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
V1.0.0	First release.	August 2026

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.

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.

Transportation Requirements



- Transport the device under allowed humidity and temperature conditions.
- Do not transport the device with its front panel facing down.

Storage Requirements



Store the device under allowed humidity and temperature conditions.

Installation Requirements

 **DANGER**

-  Electrical Hazard

  Preventive measures: Make sure the power is off when you put your hand into the device.
- Stability Hazard

  Possible result: The rack might fall down and cause serious personal injury.

  Preventive measures (including but not limited to):
  - ◇ Before extending the rack to the installation position, read the installation instructions.
  - ◇ When the Device is installed on the slide rail, do not place any load on it.
  - ◇ Do not retract the slide rail while the Device is installed on it.

 **WARNING**

-  Rotating Fan Blades Hazard

  Avoid touching the fan blades, especially when they are moving.
- ⚠ Before installation, disconnect all the power cords.
- Use a cable tie to bundle the cables after they are connected to avoid risk of short circuits, overheating and electrocution caused by tangled cables.



- The device must be installed in a location that only professionals can access. Non-professionals are not allowed to enter the installation area.
- When installing the device, make sure that the power plug can be easily reached to cut off the power.
- A 5 A overcurrent protection device is required to be installed in the external power circuit of the product as a circuit breaker. Make sure the protection device is close to the product, offering safety of cutting power during maintenance.
- Install the device near a power socket for emergency disconnect.
- An easily accessible safety disconnect switch must be incorporated into the external power supply circuit during installation.
- Make sure the product is installed by trained professionals and it must be installed in locations that only professionals can access.
- To ensure heat dissipation, the gap between the device and the surrounding area should not be less than 5 cm on the sides and 1 cm on top of the device.
- Do not block the ventilator of the device with objects, such as newspaper, table cloth or curtains.
- Do not put open flames, such as a lit candle, on the device.
- Prevent liquid from dripping or splashing on the device. Do not put any objects filled with liquid, such as a vase, on top of the device.
- Do not place or install the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, or soot.
- Make sure the device is installed stably and levelly, allowing normal status for internal tremor resistant modules.
- 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.
- An independent protective grounding terminal is designed at the lower-right corner of the product. Make sure the terminal is reliably grounded during installation.
- Connect the cables in sequence when linking the circuit, and connect the power cable last to avoid damaging the device.
- Make sure the negative binding post of the battery is disassembled while the device is being wired.
- Please follow the electrical requirements to power the device.
  - Following are the requirements for selecting a power adapter.
    - The power supply must conform to the requirements of IEC 60950-1 and IEC 62368-1 standards.
    - The voltage must meet the SELV (Safety Extra Low Voltage) requirements and not exceed ES-1 standards.
    - When the power of the device does not exceed 100 W, the power supply must meet LPS requirements and be no higher than PS2.
  - We recommend using the power adapter provided with the device.

- When selecting the power adapter, the power supply requirements (such as rated voltage) are subject to the device label.

Operation Requirements

DANGER

- The Device or remote control contains button batteries. Do not swallow the batteries due to the risk of chemical burns.

  Possible result: The swallowed button battery can cause serious internal burns and death within 2 hours.

  Preventive measures (including but not limited to):

  - Keep new and used batteries out of reach of children.
  - If the battery compartment is not securely closed, stop using the product immediately and keep out of reach of children.
  - Seek immediate medical attention if a battery is believed to be swallowed or inserted inside any part of the body.
- Battery Pack Precautions

  Preventive measures (including but not limited to):

  - Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.
  - Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.
  - Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
  - Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.

WARNING

- Operating the device in a domestic environment may cause radio interference.
- Place the device in a location that children cannot easily access.
- When the redundant power supply is optional, use the power supply of the same manufacturer and model as the original one of the product.
- High Current

  Preventative measure: Ground the screw of the device to protective ground before you power it on.
- Do not use multiple devices together to avoid generating high current.

  Preventative measure: Ground the device to protective ground before you power it on.

- Use the device under the allowed humidity and temperature conditions.
- Use the device within the rated range of power input and output.
- Operating temperature: –10 °C to +50 °C (14 °F to 122 °F).
- Do not disassemble the device.
- Do not plug or unplug RS-232, RS-485 or the audio/video signal cable with the power on to avoid damaging the ports.

Maintenance Requirements

DANGER

Replacing unwanted batteries with the wrong type of new batteries might result in explosion.

Preventive measures (including but not limited to):

- Replace unwanted batteries with new batteries of the same type and model to avoid the risk of fire and explosion.
- Dispose of the old batteries as instructed.

WARNING

- A blown fuse does not ensure disconnection of subsequent circuit. Please be cautious during maintenance.
- Power off the device before maintenance.
- The device can only be used with batteries possessing internal protection. To prevent explosion, dispose of the old batteries as instructed.
- Make sure to use the same model when replacing the battery to avoid fire or explosion.

- The device casing provides protection for internal components. Use a screwdriver to loosen the screws before detaching the casing. Make sure the casing is put back and fixed to the original spot before power on and use the device again.
- Damp dust on the circuit board might cause the device to short circuit, resulting in device damage. Make sure to regularly clear dust from the circuit board, connectors and the case with a brush.

Table of Contents

Foreword....I
Important Safeguards and Warnings....III
1 Overview....1
1.1 Product Introduction....1
1.2 Main Case....1
1.2.1 DSCON8000-S13 (5U Case)....1
1.2.2 DSCON8000-S24 (8U Case)....2
2 Device Appearance and Installation Connection....5
2.1 Unpacking Inspection....5
2.2 Device Installation....5
2.2.1 Installation Environment....5
2.2.2 Installation Steps....6
2.3 Startup....7
3 Basic Operations....8
3.1 Touchscreen Operations (DSCON8000-S13)....8
3.1.1 Device Initialization and Login....8
3.1.2 Configuring the Network and LCD screen....8
3.2 Touchscreen Operations (DSCON8000-S24)....10
3.3 Initialization and Login....11
Appendix 1 Security Recommendation....14

1 Overview

1.1 Product Introduction

The series of DSCON splicing controllers is designed with an FPGA frame that boasts high performance and bandwidth. It features a minimal interaction design with flexible combinations of input and output boards. This device supports various large-screen control functions including image stitching, roaming, and scene tours, as well as image processing capabilities such as image acquisition, background image display, and dynamic subtitles.

This device is widely used in professional audio and video display fields such as command centers, exhibition halls, lecture rooms, meeting rooms, and more.

1.2 Main Case

1.2.1 DSCON8000-S13 (5U Case)

The splicing controller DSCON8000-S13 is a 19-inch 5U rack-mounted main case, including service board slots, power ports, and intelligent temperature-controlled fans. The front panel indicators are used to display the device operating status.

Figure 1-1 Front panel



The rear panel includes the following components.

- Case air inlet.
- 6 intelligent temperature control fans with hot-swappable fan frame modules.
- Function card slots: A total of 13, sequentially numbered for the installation of function cards.

  ◇ Preview cards can be used in output slots.

  ◇ Decoding extension cards can be used in slots 1, 3, 5, 7, 9, and 11.

◇ The VI0401EHP UHD capture card and VI0801HH HD capture card have their performance halved when used in slot 13.

Table 1-1 Function card slot description

Slot Number	Function
Slots 1/3	Dedicated to capture cards and labeled **IN**.
Slots 5/7/9/11/13	Shared between capture cards and output cards, and labeled **IN/OUT**.
Slots 2/4/6/8/10	Dedicated to output cards and labeled **OUT**.
Slot 12	Shared between control cards and output cards and labeled **M/OUT**.

- 1 dedicated slot for the main control card, labeled **M**.
- 1 dedicated slot for the switching card, labeled **N**.
- Dual power supply module design, supporting redundancy with hot standby (single power supply included; dual power supply optional).

When disconnecting the power cord, for devices with a dual power supply, you need to unplug 2 power cords.

Figure 1-2 Rear panel



1.2.2 DSCON8000-S24 (8U Case)

The splicing controller DSCON8000-S24 is a 19-inch 8U rack-mounted main case, including service board slots, power ports, and intelligent temperature-controlled fans. The front panel indicators are used to display the device operating status.

Figure 1-3 Front panel



The rear panel includes the following components.

- Case air inlet.
- 8 intelligent temperature control fans with hot-swappable fan frame modules.
- Function card slots: A total of 24, sequentially numbered for the installation of function cards.

  ◇ Preview cards can be used in output slots.

  ◇ Decoding extension cards can be used in slots 1, 3, 5, 13, 15, and 17.

  ◇ The VI0401EHP UHD capture card and VI0801HH HD capture card have their performance halved when used in shared input/output slots.

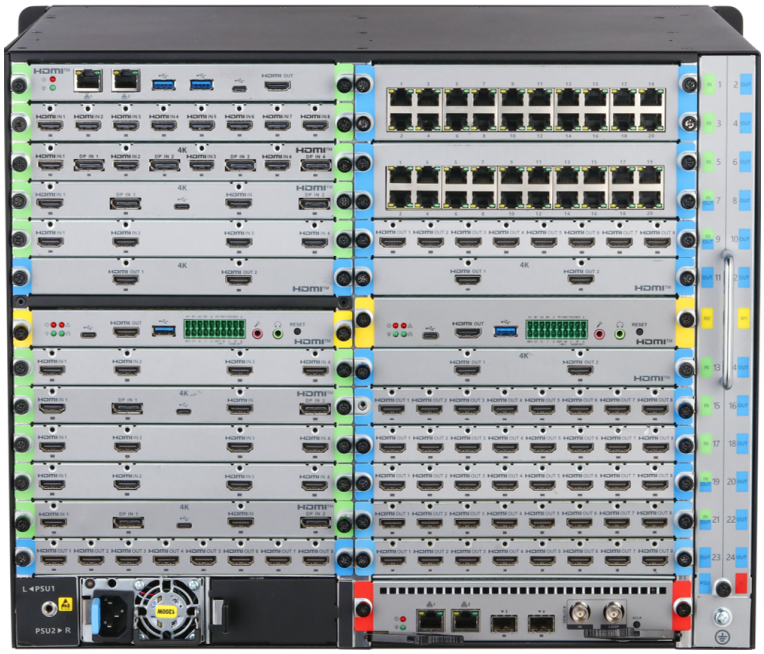
Table 1-2 Function card slot description

Slot Number	Function
Slots 1/3/5/13/15/17	Dedicated to input slots and labeled **IN**.
Slots 7/9/19/21	Shared between input slots and output slots, and labeled **IN/OUT**.
Slots 2/4/6/8/10/11/12/14/16/18/20/22/23/24	Dedicated to output slots and labeled **OUT**.

- 2 dedicated slots for control cards and labeled **M1, M2** , with **M1** as the factory default.
- 1 dedicated slot for the switching card, labeled **N**.
- Dual power supply module design, supporting redundancy with hot standby (single power supply included; dual power supply optional).

When disconnecting the power cord, for devices with a dual power supply, you need to unplug 2 power cords.

Figure 1-4 Rear panel



2 Device Appearance and Installation Connection

2.1 Unpacking Inspection

Upon receiving the device, check it according to the following steps.

Procedure

Step 1 Check whether there is any visible damage.

The protective material of the device package can resist most accidental collisions during transportation.

Step 2 Open the product packaging and check whether all included accessories are present. After confirmation, remove the protective film from the device.

Step 3 Open the case to check if the front-panel data cables, power cord, and the motherboard connections are secure. Additionally, ensure that the main control card, the control card, and the function card inside the case are properly inserted.

The label at the side of the case contains the device serial number and other information. The information is required when contacting after-sales service. Keep the label intact. Do not remove or discard it; otherwise, you may be unable to receive after-sales service.

2.2 Device Installation

2.2.1 Installation Environment

The splicing controller is typically installed in the central machine room, and the selection of its installation site must comply with relevant national and regional standards for data center construction.

As the device is a standard rack-mount device fixed inside the cabinet, observe the following precautions during installation and operation:

- Ensure that the cabinet is sufficiently sturdy to support the weight of the splicing controller and its accessories, while avoiding uneven mechanical loads that might pose risks.
- Provide sufficient clearance for audiovisual cable routing, maintaining a minimum bend radius no less than 5 times the external diameter of the cable.
- Maintain proper ventilation with recommended ground clearance exceeding 50 cm beneath the device.

Power Supply Requirements

- The rated current of DSCON8000-S13 is 8 A, rated power is ≤ 550 W. Its rated voltage ranges from 100 VAC to 240 VAC.
- The rated current of DSCON8000-S24 is 10 A/5 A, rated power is ≤ 1200 W. Its rated voltage ranges from 100 VAC to 240 VAC.

Anti-Interference Requirements

- The on-site power supply system must implement effective measures to prevent grid interference.
- The working ground shall not be shared with the grounding devices of electrical equipment or lightning protection grounding systems, and should be kept as far apart as possible.
- Keep the device away from high-power wireless transmission stations, radar systems, and high-frequency and high-current devices.
- If necessary, use electromagnetic shielding methods for anti-interference purposes.

Environmental Requirements

Table 2-1 Environmental requirements description

Type	Normal Operating Specifications
Ambient temperature	• Operating: 5 °C to 35 °C (mainstream) • Computer room standard recommends 18 °C to 28 °C.
Relative humidity	8% to 90% RH, no condensation allowed.
Dust/cleanliness	The main computer room must meet the requirement of particle size ≥0.5 μm; dust <3.5×10^7 particles/m^3.

2.2.2 Installation Steps

Background Information

The device is delivered with the main control card installed by default.

Procedure

Step 1 Insert the function card and blank panel as needed, and then tighten the screws.

Under full load conditions, inserting a blank panel is not required. However, in non-full load scenarios, blank panels must be inserted to avoid potential operational impact.

Step 2 Properly ground the grounding terminal of the splicing controller.

⚠

To ensure the safety of both personnel and the device, the splicing controller and any connected devices through cables (such as large screens, computers, and more) must be grounded. When most devices are directly grounded through power supplies, no additional grounding is required for the grounding terminal on the device.

Step 3 Connect necessary cables (such as Ethernet cable and HDMI cable) according to actual requirements.

Step 4 Power on the device to start it.

2.3 Startup

Plug in the power cord, and then the power indicator lights up. The startup page is displayed after the power switch is turned on.

Pay attention to the following matters when starting up.

- Ensure that the input voltage of the power supply is within the range of 100 VAC to 240 VAC and 47 Hz to 63 Hz. Verify that the power cord is securely connected before turning on the power switch.
- We recommend providing a stable power input with minimal interference (as per national standards). This will help ensure the stable operation and prolonged lifespan of the device. Additionally, it will greatly benefit external devices, such as cameras. If possible, using UPS power would be the optimal choice.

3 Basic Operations

3.1 Touchscreen Operations (DSCON8000-S13)

3.1.1 Device Initialization and Login

Procedure

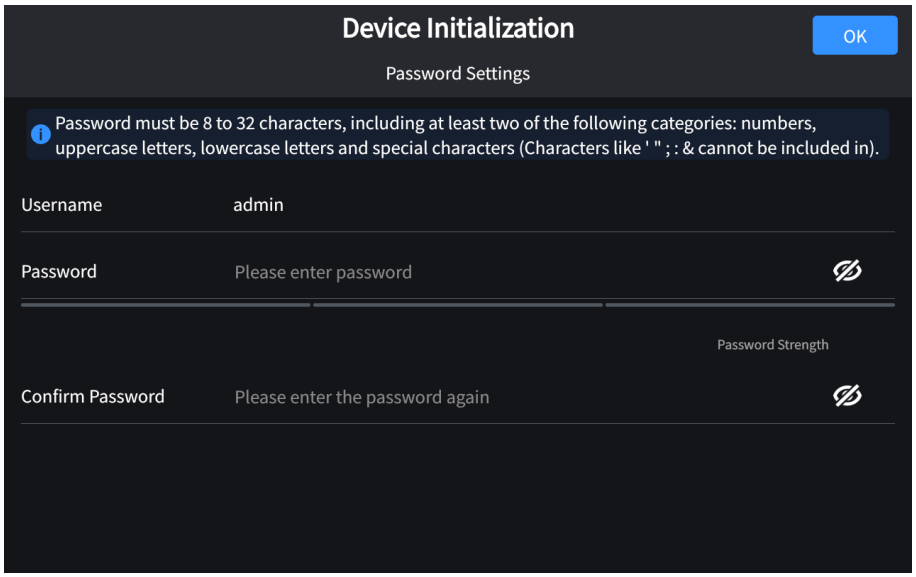
Step 1 Connect the power cord and wait for the device to start up.

Once the device powers on, it proceeds to the initialization page.

Step 2 Set and confirm the password, and then tap **OK**.

- Set a high-security password according to the password strength prompt.
- The password must be 8 to 32 non-blank characters, including at least 2 of the following categories: numbers, uppercase letters, lowercase letters, and special characters (excluding ', ", ;, :, &). The passwords must be the same.

Figure 3-1 Set password



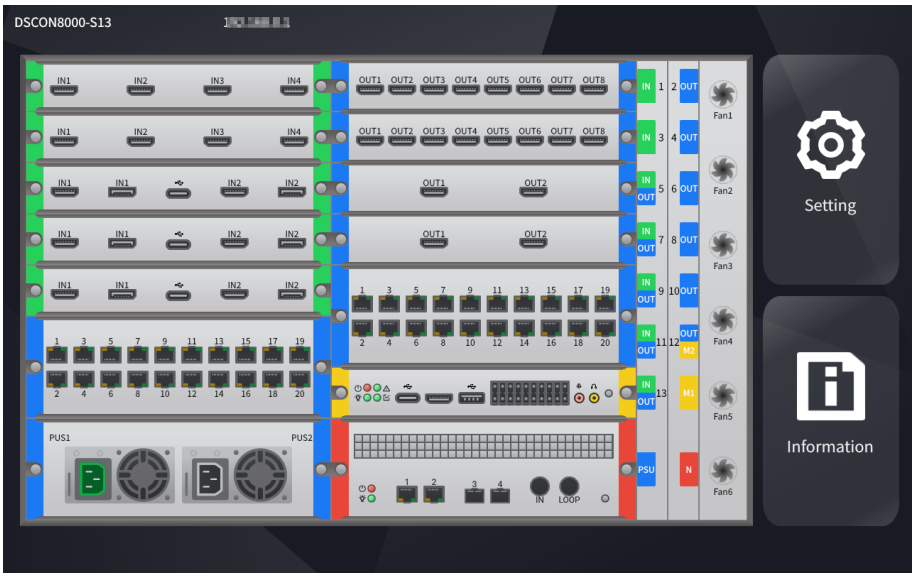
Step 3 On the login page, enter your username and password, and then tap **Login**.

3.1.2 Configuring the Network and LCD screen

Network Settings

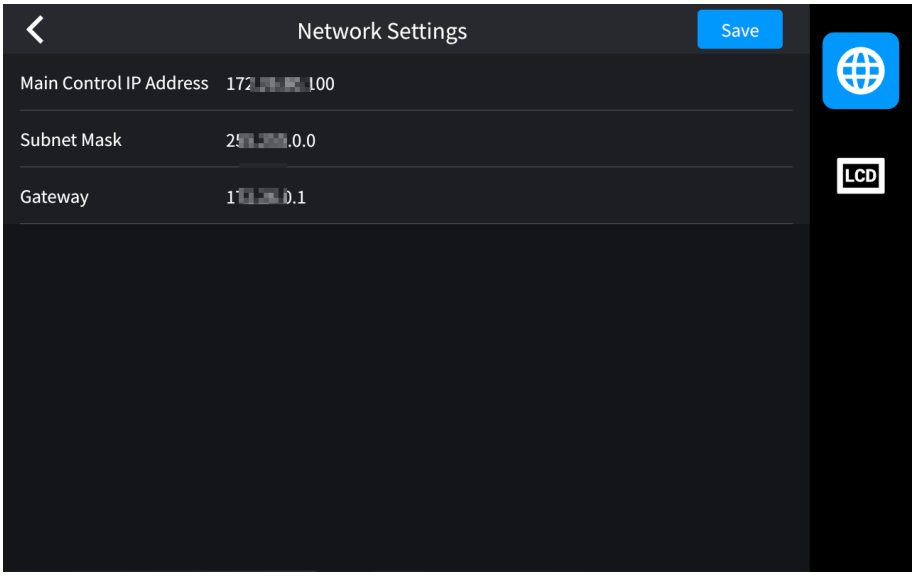
1. On the home page, tap **Setting**.

Figure 3-2 Home page



2. Configure the IP address, subnet mask and gateway, and then tap **Save**.

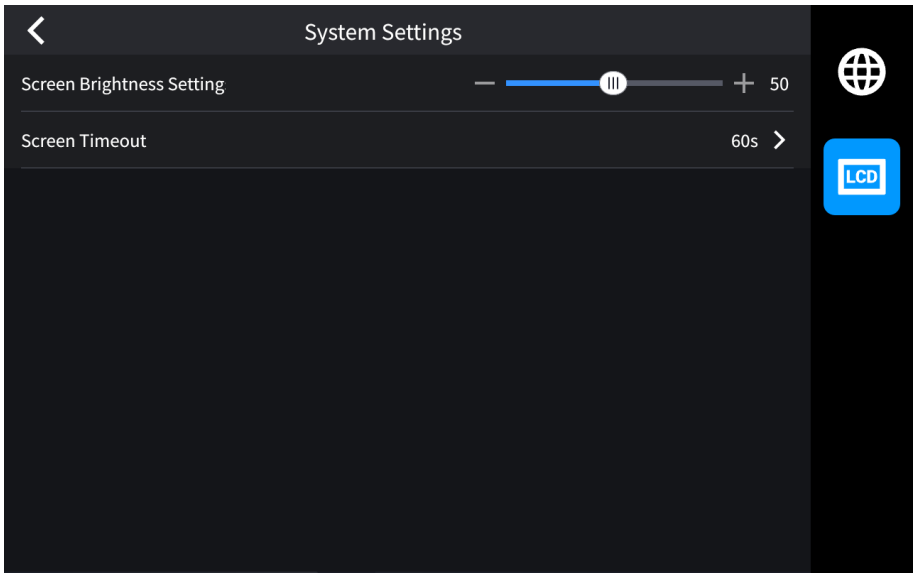
Figure 3-3 Network settings



LCD Settings

1. Tap **LCD**.
2. Adjust the screen brightness and set the screen timeout time.

Figure 3-4 Configure LCD screen



3.2 Touchscreen Operations (DSCON8000-S24)

The front panel LCD screen of the device supports viewing information such as device version and IP address.

Prerequisites

The device has been initialized through the webpage.

Procedure

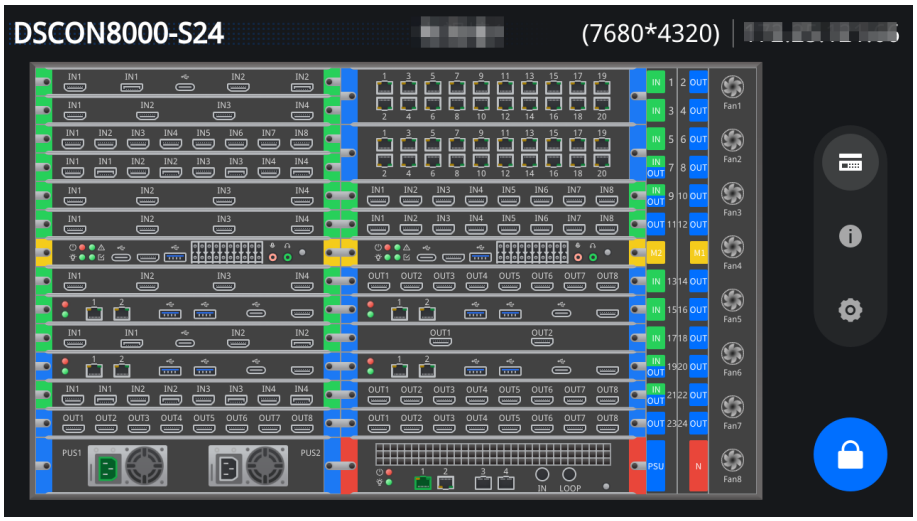
Step 1 Connect the power cord and wait for the device to start up.

After the device is powered on, the device enters the main page ( ), which displays the information of the device's rear panel.

Step 2 Tap to unlock the device.

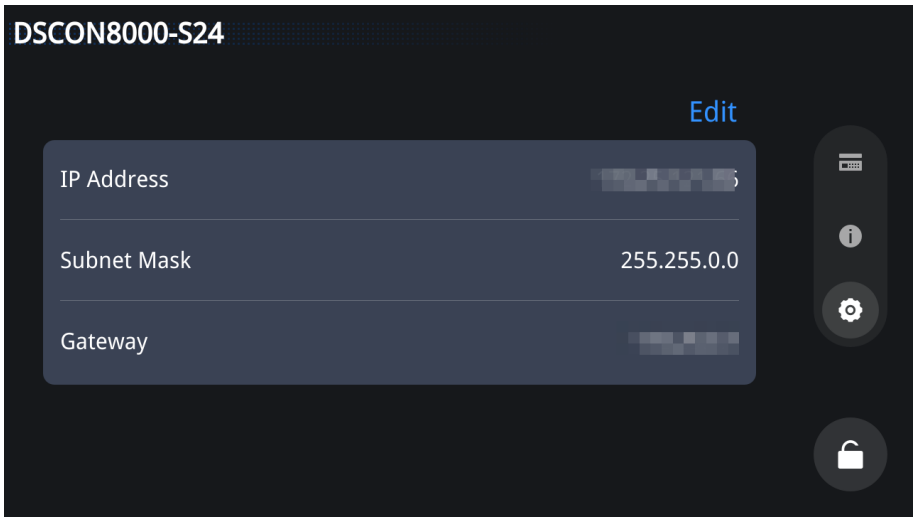
After unlocking, tap to lock the device.

Figure 3-5 Unlock



Step 3 Tap to view the device IP information.

Figure 3-6 View IP address



Step 4 Modify the device IP address.

1. Tap **Edit** on the IP address page.
2. Enter the username (admin) and password.
3. Modify the IP address, subnet mask, and gateway information.
4. Tap **OK**.

3.3 Initialization and Login

Procedure

Step 1 Enter the IP address of the device (for example 192.168.1.108) in the address bar of the browser, and then press the Enter key.

Step 2 Enter and confirm the new admin password.

- You need to configure your own password for the first-time login.
- The password must consist of 8–32 non-blank characters and contain at least 2 types of the following characters: Uppercase, lowercase, numbers, and special characters (excluding ', ", ;, :, &). The new password and confirmation password must match.
- Set a high-security password according to the password strength prompt.

Step 3 Click **OK**.

Step 4 Enter the username and password, and then click **Login**.

The video wall page is displayed by default.

Refer to the corresponding user manual for detailed device information.

Figure 3-7 Home page

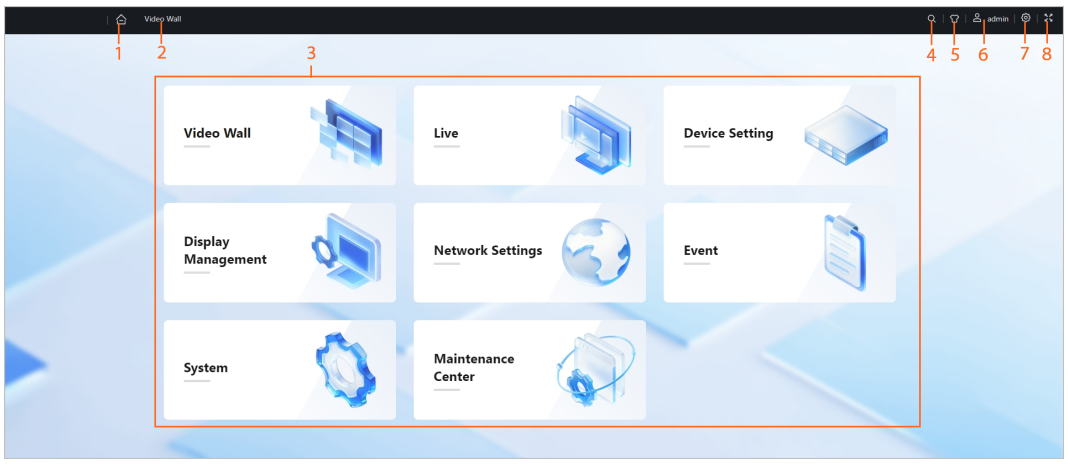


Table 3-1 Description of the homepage

No.	Name	Description
1	Home page	Click it to return to the home page menu.
2	Function tabs	Click it to enter the corresponding function configuration page. Click ✕ to close the corresponding tab.
3	Application functions	Click each application function to enter the corresponding configuration page.
4	Search	Enter a function name keyword to search and quickly navigate to the corresponding configuration page. 

No.	Name	Description
5	Theme	Switch between dark and light themes. The default is light. Screenshots in this document use the light theme.
6	Log out	Click it, and then select **Logout** to return to the login page.
7	System configuration	Click it to select the function menu to configure the system.
8	Full screen	Click it to display the page in full screen. Click again to exit full screen.

Appendix 1 Security Recommendation

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**

   The 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, it is recommended 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**

   It is recommended 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).