



iLinksView Network Management Platform

Quick Start Guide

V1.0.2

Foreword

General

This manual introduces the functions and operations of the iLinksView Network Management Platform (hereinafter referred to as "the Device").

Models

Name	Model
iLinksView Network Management Platform	DH-ILS1000

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 Time
V1.0.2	Modified company address.	August 2023
V1.0.1	Updated the figure of the rear panel.	December 2022
V1.0.0	First release.	Sep 2019

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

The manual helps you to use our product properly. To avoid danger and property damage, read the manual carefully before using the product, and we highly recommend you to keep it well for future reference.

Operating Requirements

- Do not expose the device directly to the sunlight, and keep it away from heat.
- Do not install the device in the damp environment, and avoid dust and soot.
- Make sure the device is in horizontal installation, and install the device on solid and flat surface to avoid falling down.
- Avoid liquid spattering on the device. Do not place object full of liquid on the device to avoid liquid flowing into the device.
- Install the device in the well-ventilated environment. Do not block the air vent of the device.
- Use the device at rated input and output voltage.
- Do not disassemble the device without professional instruction.
- Transport, use, and store the device in allowed ranges of humidity and temperature.

Power Supply Requirements

- Use the battery properly to avoid fire, explosion, and other dangers.
- Replace the battery with battery of the same type.
- Use locally recommended power cord in the limit of rated specifications.
- Use the standard power adapter. We will assume no responsibility for any problems caused by nonstandard power adapter.
- The power supply shall meet the SELV requirement. Use the power supply that conforms to Limited Power Source, according to IEC60950-1. Refer to the device label.
- Adopt GND protection for I-type device.
- The coupler is the disconnecting apparatus. Keep it at the angle for easy to operate.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Introduction.....	1
1.1 Overview	1
1.2 Functions.....	1
2 Device Structure	2
2.1 Product Dimensions.....	2
2.2 Specification	3
2.3 Interface Description	4
3 Device Initialization	6
3.1 Setting Password for Admin	6
3.2 Startup Wizard.....	7
4 Device Reboot and Reset	10
4.1 Rebooting the Device.....	10
4.2 Resetting the Device.....	10
Appendix 1 Cybersecurity Recommendations	12

1 Introduction

1.1 Overview

iLinksView Network Management Platform is a product based on hardware platform and designed for network problem location, network fault detection, network operation and maintenance.

The product has a friendly operation interface and is easy to use. It supports Dahua switch and mainstream third-party switch products, provides real-time management of device information, and greatly improves the speed of network fault resolution. It can be widely used in security projects, and help project implementation and maintenance personnel quickly pinpoint network problems and ensure the safe operation of the network.

1.2 Functions

The product mainly includes the following functions:

- Support Dahua switch and mainstream third-party switch products, and support the discovery of terminal devices such as IPC, NVR.
- Support automatic generation of network topology, and display device status and detailed information.
- Support intelligent analytics of switches, including running time, port dynamics, alarm log and other information.
- Support device management of switches, terminal devices and PoE switches.
- Support various types of statistics and display of alarm information.
- Support statistics and display of CPU and memory utilization rate of the system.

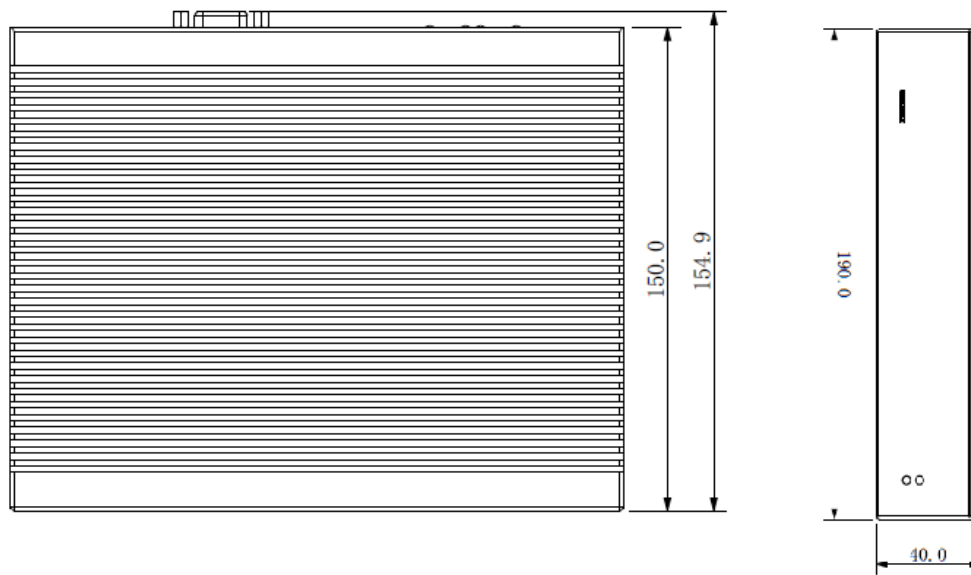
2 Device Structure

This chapter describes the product dimensions, specification and interfaces of the Device.

2.1 Product Dimensions

The appearance and dimensions of the Device are shown in Figure 2-1.

Figure 2-1 Product dimensions (mm)



2.2 Specification

For the specification of the Device, see Table 2-1.

Table 2-1 Parameter list

Specification	Parameters
CPU (Intel)	Braswell N3060
Dimensions	155 mm × 135 mm × 30 mm
Memory	2 GB
Storage	32 GB
Input/output port	4 USB ports 1 HDMI port 1 VGA port 2 RJ45 ports  The two RJ45 ports are the same IP, and the default IP is 192.168.1.110. Only one RJ45 port is allowed for a device.
Ethernet port rate	10 M / 100 M / 1000 M
Power supply	12 V / 4 A
Static voltage	2 KV
Working temperature	-10°C to 55°C
Humidity	0 – 90%
Power	15 W
Supported device	1000 switches 10,000 terminal devices

2.3 Interface Description

Interfaces of the Device are shown in Figure 2-2. For details, see Table 2-2.

The Device can be used only by connecting the network cable and the power cable.

Figure 2-2 Rear panel

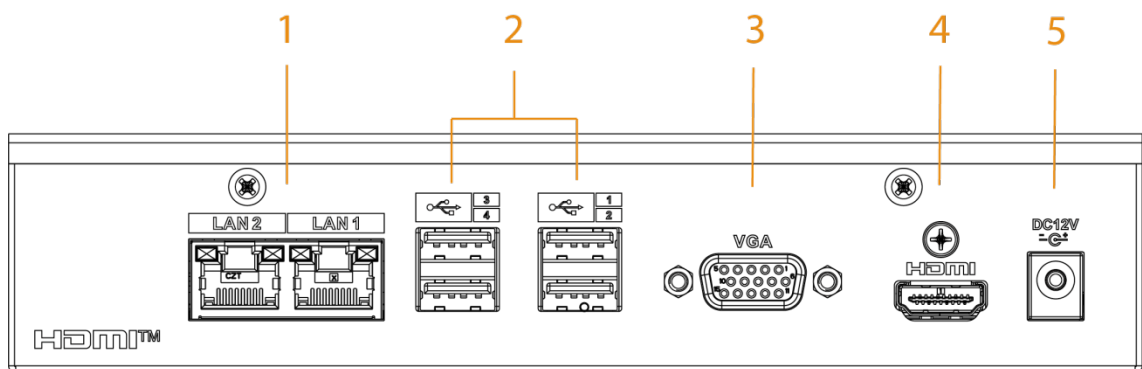


Table 2-2 Interface description

No.	Name	Description
1	Ethernet port	RJ45 network port, one device can only connect to one RJ45 network port.
2	USB port	Connects to the external devices such as keyboard, mouse, and USB storage device.  This interface is only used for initializing the Device, and it cannot be used when the Device is running.
3	VGA port	Outputs analog video data to the connected display with VGA port.  This interface is only used for initializing the Device, and it cannot be used when the Device is running.
4	HDMI port	High definition audio and video signal output port. The port outputs the uncompressed high definition video and multi-channel audio data to the connected display with HDMI port.  This interface is only used for initializing the Device, and it cannot be used when the Device is running.
5	Power port	Connects to power source.

3 Device Initialization

After the Device connects to the network and power source, you can log in to the web interface.

If it is your first time to log in to the Web interface, you need to set password for admin and initialize the Device.

3.1 Setting Password for Admin

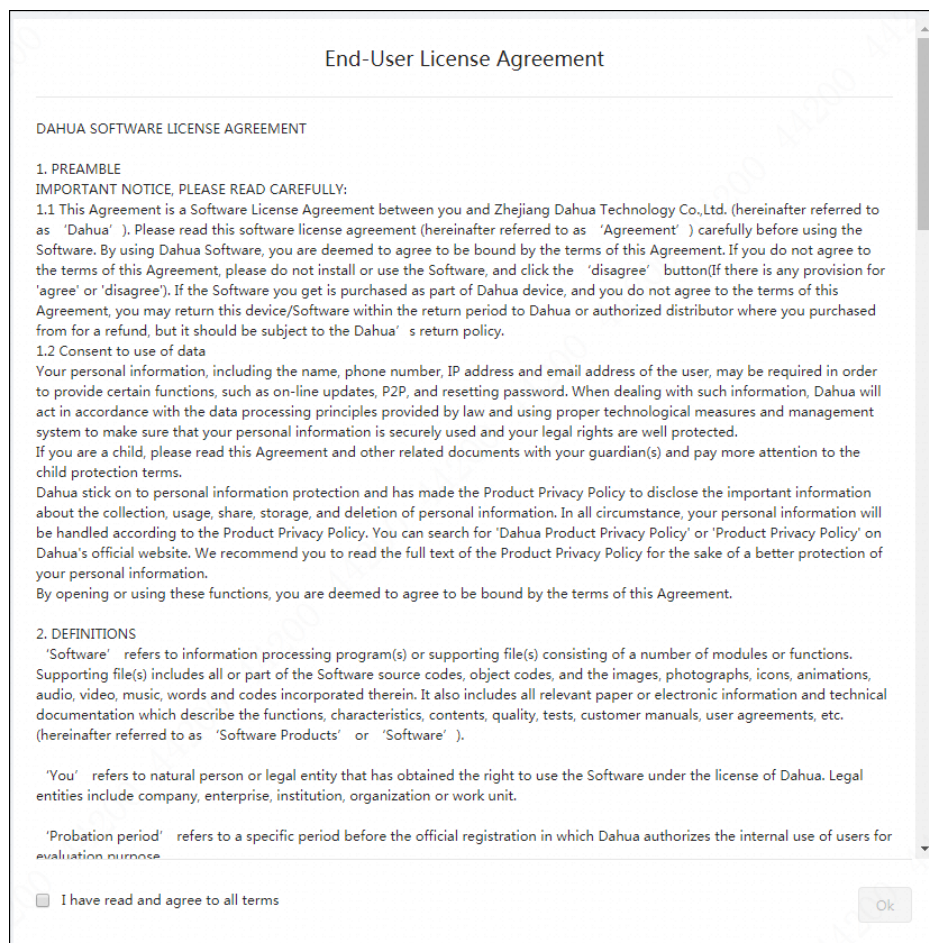
If it is your first time to use the Device after purchase or reset, you need to set a login password of the administrator user (admin by default).

Step 1 Open the browser, enter IP address of the Device (the default IP is 192.168.1.110) and then press **Enter** key.

The **End-User License Agreement** interface is displayed.

Step 2 Confirm the license agreement, select **I have read and agree to all terms** check box after confirmation, and then click **Ok**.

Figure 3-1 End-user license agreement



End-User License Agreement

DAHUA SOFTWARE LICENSE AGREEMENT

1. PREAMBLE

IMPORTANT NOTICE, PLEASE READ CAREFULLY:

1.1 This Agreement is a Software License Agreement between you and Zhejiang Dahua Technology Co., Ltd. (hereinafter referred to as 'Dahua'). Please read this software license agreement (hereinafter referred to as 'Agreement') carefully before using the Software. By using Dahua Software, you are deemed to agree to be bound by the terms of this Agreement. If you do not agree to the terms of this Agreement, please do not install or use the Software, and click the 'disagree' button (If there is any provision for 'agree' or 'disagree'). If the Software you get is purchased as part of Dahua device, and you do not agree to the terms of this Agreement, you may return this device/Software within the return period to Dahua or authorized distributor where you purchased from for a refund, but it should be subject to the Dahua' s return policy.

1.2 Consent to use of data

Your personal information, including the name, phone number, IP address and email address of the user, may be required in order to provide certain functions, such as on-line updates, P2P, and resetting password. When dealing with such information, Dahua will act in accordance with the data processing principles provided by law and using proper technological measures and management system to make sure that your personal information is securely used and your legal rights are well protected.

If you are a child, please read this Agreement and other related documents with your guardian(s) and pay more attention to the child protection terms.

Dahua stick on to personal information protection and has made the Product Privacy Policy to disclose the important information about the collection, usage, share, storage, and deletion of personal information. In all circumstance, your personal information will be handled according to the Product Privacy Policy. You can search for 'Dahua Product Privacy Policy' or 'Product Privacy Policy' on Dahua's official website. We recommend you to read the full text of the Product Privacy Policy for the sake of a better protection of your personal information.

By opening or using these functions, you are deemed to agree to be bound by the terms of this Agreement.

2. DEFINITIONS

'Software' refers to information processing program(s) or supporting file(s) consisting of a number of modules or functions. Supporting file(s) includes all or part of the Software source codes, object codes, and the images, photographs, icons, animations, audio, video, music, words and codes incorporated therein. It also includes all relevant paper or electronic information and technical documentation which describe the functions, characteristics, contents, quality, tests, customer manuals, user agreements, etc. (hereinafter referred to as 'Software Products' or 'Software').

'You' refers to natural person or legal entity that has obtained the right to use the Software under the license of Dahua. Legal entities include company, enterprise, institution, organization or work unit.

'Probation period' refers to a specific period before the official registration in which Dahua authorizes the internal use of users for evaluation purpose.

☐ I have read and agree to all terms

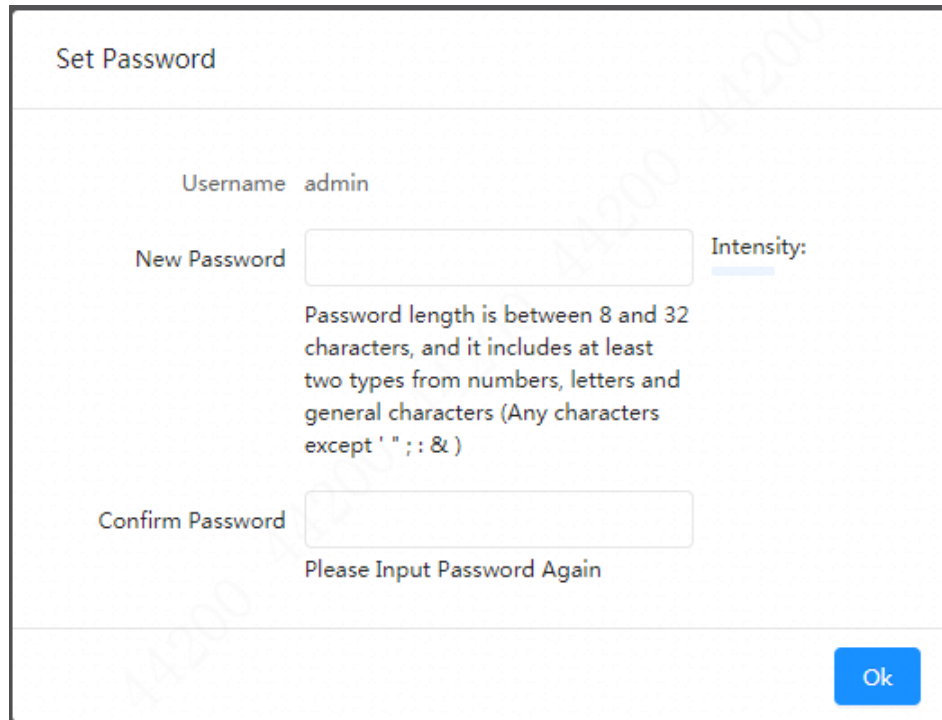
Ok

Step 3 Set the login password for admin.

The password must 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 ' ' ; : &).

Enter a strong password according to the password strength prompt.

Figure 3-2 Set password

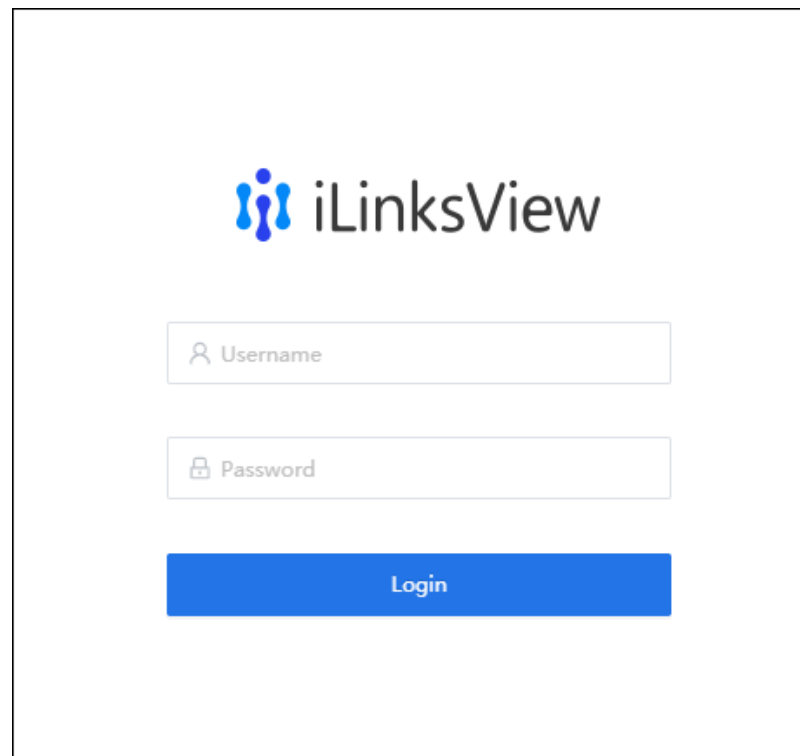


The 'Set Password' interface shows the username 'admin'. It has a 'New Password' field with an 'Intensity' indicator and a 'Confirm Password' field. A password policy note states: 'Password length is between 8 and 32 characters, and it includes at least two types from numbers, letters and general characters (Any characters except ' ' ; : &)'. An 'Ok' button is at the bottom right.

Step 4 Click **Ok** to save the configuration.

Step 5 The user login interface is displayed.

Figure 3-3 User login



The 'iLinksView' login interface features the logo at the top. Below it are two input fields: 'Username' (with a person icon) and 'Password' (with a lock icon). A blue 'Login' button is positioned at the bottom.

3.2 Startup Wizard

If it is your first time to log in, you will enter the **Setup Wizard** interface, which can help you quickly configure network segment of the network devices and network settings of the system.

Step 1 Log in to iLinksView.

Figure 3-4 Web login



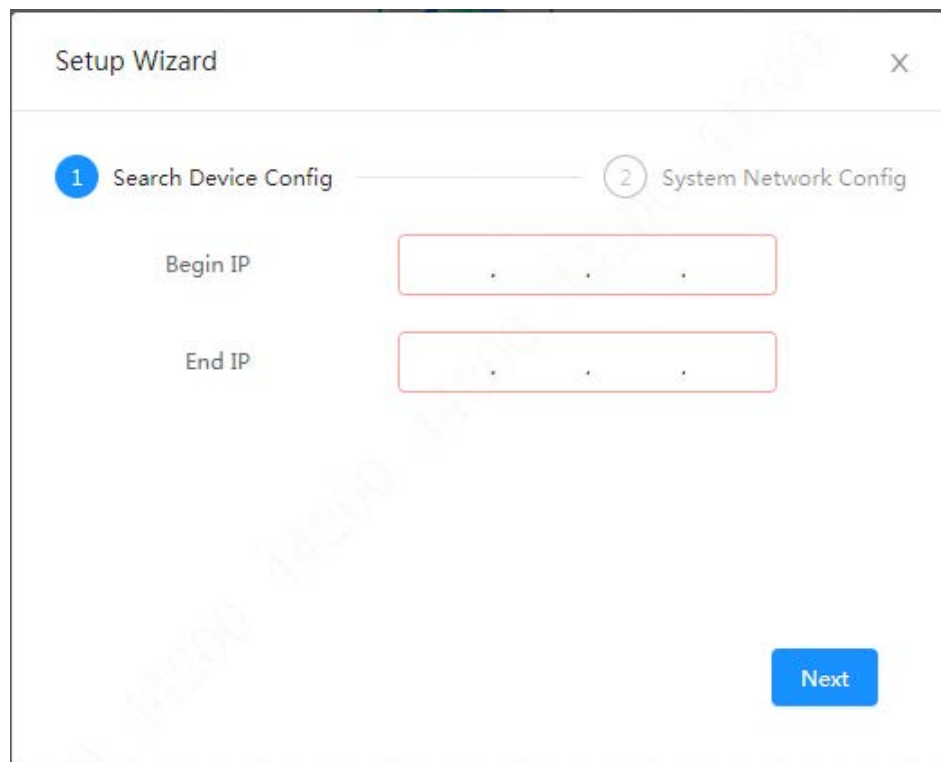
The image shows the iLinksView web login interface. At the top, there is a logo consisting of three blue dots arranged in a triangular pattern, followed by the text "iLinksView". Below the logo, there are two input fields. The first field has a user icon and the text "admin". The second field has a lock icon and a series of dots representing a password. Below these fields is a blue button with the text "Login".

Step 2 Configure network segment of the network devices.

On the **Setup Wizard** interface, enter **Begin IP** and **End IP**, and click **Next**.

The system will search devices within the segment.

Figure 3-5 Configuring search IP address



The image shows the "Setup Wizard" interface. At the top, there is a title bar with the text "Setup Wizard" and a close button (X). Below the title bar, there are two steps: "1 Search Device Config" and "2 System Network Config". The "1 Search Device Config" step is currently active. Below the steps, there are two input fields: "Begin IP" and "End IP". Each field has a red border and contains three dots, indicating that the IP address has not been entered yet. At the bottom right of the interface, there is a blue button with the text "Next".

Step 3 Configure system network.

On the **System Network Setting** interface, enter IP address, subnet mask, default gateway and DNS.



DNS is not required.

Figure 3-6 System network settings

Step 4 Click **OK** to complete the network configuration.

4 Device Reboot and Reset

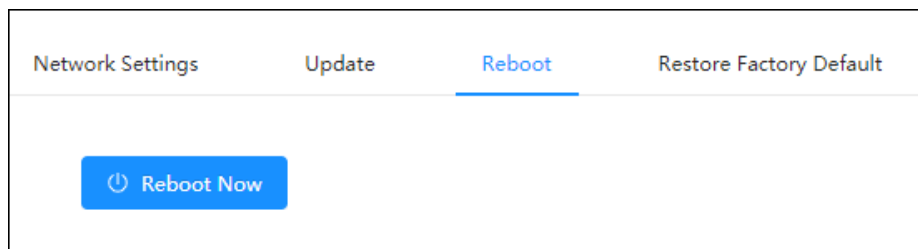
4.1 Rebooting the Device

Step 1 Log in to iLinksView.

Step 2 Click  on the upper right corner, and then select **Reboot**.

Step 3 Click **Reboot Now**.

Figure 4-1 Reboot



4.2 Resetting the Device

Refer to the following two ways to reset the Device.

On Web Interface

Step 1 Log in to iLinksView.

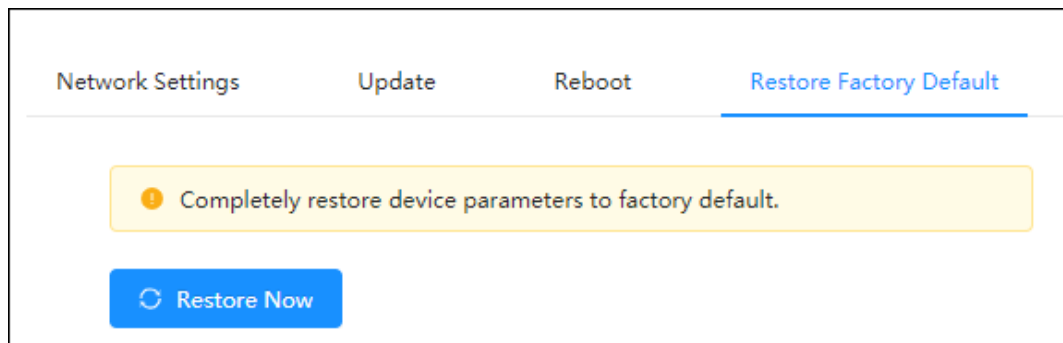
Step 2 Click  on the upper right corner, and then select **Restore Factory Default**.

Step 3 Click **Restore Now**.



IP address will not be changed when you reset the system on the Web interface.

Figure 4-2 System reset on web interface



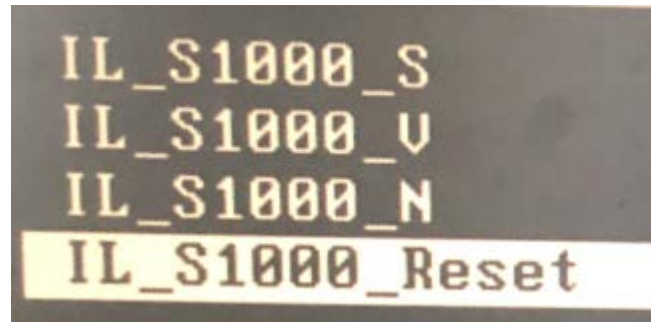
On the Device

Step 1 Connect the external monitor (VGA port) and keyboard (USB port) to the Device.

Step 2 Connect the power source, hold down keypad (↑), and go to the system reset interface.

Step 3 Select **IL_S1000_Reset**, and then press **Enter** key.

Figure 4-3 System reset on the Device



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.

ENABLING A SAFER SOCIETY AND SMARTER 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