

iLinksView Network Management Platform

User's Manual

V1.0.0

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

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
	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
	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
V1.0.0	First release.	November 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 dissemble 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	
Important Safeguards and Warnings	111
1 Introduction	1
1.1 Overview	1
1.2 Functions	1
2 Device Structure	3
2.1 Product Dimensions	3
2.2 Specification	4
2.3 Port Description	4
3 Web Configuration	6
3.1 Login	6
3.1.1 Setting Password for Admin	6
3.1.2 Startup Wizard	8
3.2 Network Management	11
3.2.1 Discovering Device	11
3.2.2 Device Management	12
3.3 AI Analysis	14
3.4 Dynamic View	15
3.5 Alarm Message	20
3.5.1 Real-time Message	20
3.5.2 Ignore Message	20
4 System Settings	21
4.1 Basic Settings	21
4.1.1 Basic Information	21
4.1.2 Network Settings	21
4.1.3 Updating the Device	22
4.1.4 Rebooting the Device	23
4.1.5 Resetting the Device	23
4.1.6 Configuring Import and Export	24
4.2 Global Configuration	24
4.2.1 Alarm Management	24
4.2.2 Performance Management	25
4.2.3 SNMP	26
4.3 Safety Management	26
4.3.1 HTTPS	26
4.3.2 SSH	27
4.4 Firewall	27
4.5 Language Setting	28
4.6 System Log	28
4.7 Modifying Password	29
4.8 Logout	30
Appendix 1 Cybersecurity Recommendations	31

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 the most popular 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

This Device mainly contains the following functions.

Device Discovery

- Support Dahua switch and the most popular third-party switch products.
- Support discovery of terminal devices such as IPC, NVR.

AI Analysis

- Status monitoring of switches and terminal devices.
- Alarm statistics and display.
- Statistics of port flow and total bandwidth.
- Statistics and display of switch operation time.

Dynamic View

- Automatic generation of network topology.
- Display connection relationship of devices in the network and details of link load.
- Display status and details of switches and terminal devices.

Device Management

- Support classified display and detailed information display of switches and terminal devices.
- Support export of terminal device information.
- Support direct access to a device by the IP address on the iLinksView platform.

Platform Management

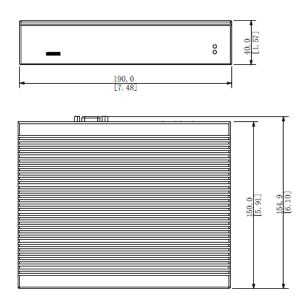
- Support IP address configuration of the iLinksView platform, and view of software and hardware version information.
- Support configuration of alarm threshold.
- Support collection and display of the system logs.



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[inch])



2.2 Specification

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

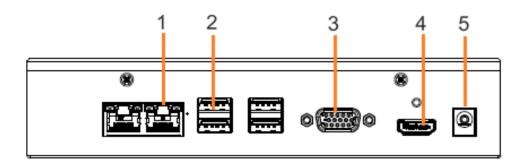
Specification	Parameters	
Dimensions	155 mm × 135 mm × 30 mm	
Memory	2 GB	
Storage	32 GB	
	4 USB ports	
	1 HDMI port	
	1 VGA port	
Input/output port	• 2 RJ45 ports	
	• The two RJ45 ports are the same IP, and the default IP is	
	192.168.1.110.	
	 Only one RJ45 port is allowed for a device. 	
Ethernet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

Table 2-1 Parameter list

2.3 Port Description

Ports of the Device are shown in Figure 2-2. For details, see Table 2-2. Power on the Device after it is connected to network and power.

Figure 2-2 Rear panel



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

Table 2-2 Port description



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

 \square

Use the following browsers to log in to the web interface:

- Firefox (version 69.0.1 or later)
- Google (version 77.0.3865.120 or later)
- IE (version 11 or later)

3.1 Login

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

3.1.1 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).

<u>Step 1</u> 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.

<u>Step 2</u> 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	
INPORTANT NOTICE, PLEASE READ CAREFULLY: 1.1 This Agreement is a Software License Agreement between you and Zhejiang Dahua Technology Co.,Ltd. (he as 'Dahua'). Please read this software license agreement (hereinafter referred to as 'Agreement') carefully Software. By using Dahua Software, you are deemed to agree to be bound by the terms of this Agreement. If y the terms of this Agreement, please do not install or use the Software, and click the 'disagree' button(If ther 'agree' or 'disagree'). If the Software you get is purchased as part of Dahua device, and you do not agree to the Agreement, you may return this device/Software within the return period to Dahua or authorized distributor wi	y before using the ou do not agree to re is any provision for e terms of this
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 I to provide certain functions, such as on-line updates, P2P, and resetting password. When dealing with such infi act in accordance with the data processing principles provided by law and using proper technological measure system to make sure that your personal information is securely used and your legal rights are well protected.	ormation, Dahua will
If you are a child, please read this Agreement and other related documents with your guardian(s) and pay more child protection terms.	e attention to the
Dahua stick on to personal information protection and has made the Product Privacy Policy to disclose the imp about the collection, usage, share, storage, and deletion of personal information. In all circumstance, your pers be handled according to the Product Privacy Policy. You can search for 'Dahua Product Privacy Policy' or 'Produ Dahua's official website. We recommend you to read the full text of the Product Privacy Policy for the sake of a your personal information.	onal information will uct Privacy Policy' on
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 modu Supporting file(s) includes all or part of the Software source codes, object codes, and the images, photographs audio, video, music, words and codes incorporated therein. It also includes all relevant paper or electronic infor documentation which describe the functions, characteristics, contents, quality, tests, customer manuals, user ag (hereinafter referred to as 'Software Products' or 'Software').	, icons, animations, rmation and technical
'You' refers to natural person or legal entity that has obtained the right to use the Software under the licens entities include company, enterprise, institution, organization or work unit.	e of Dahua. Legal
'Probation period' refers to a specific period before the official registration in which Dahua authorizes the in evaluation purpose	iternal use of users for
I have read and agree to all terms	

<u>Step 3</u> 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

Username	admin		
New Password		Intensity:	
	Password length is between 8 and 32		
	characters, and it includes at least		
	two types from numbers, letters and		
	general characters (Any characters except ' " ; : &)		
Confirm Password			
	Please Input Password Again		

<u>Step 4</u> Click **OK** to save the configuration. The user login interface is displayed.

Figure 3-3 User login

🚺 iLinksView
A Username
🗄 Password
Login

3.1.2 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

<mark>1</mark> iLinksView	
A admin	
⊕ ••••••	
Login	

<u>Step 2</u> Configure network segment of the network devices.

On the **Setup Wizard** interface, enter **Begin IP** and **End IP**, and then click **Next**. The system will search devices within the segment.

Figure 3-5 Configuring search IP address

Setup Wizard	×
1 Search Device Config	2 System Network Config
Begin IP	
End IP	
	Next

<u>Step 3</u> 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

Setup Wizard						×
Search for Device Config			2	Syst	tem Ne	etwork Settings
IP Address	-	-				
Subnet Mask	100	30			F	
Default Gateway						
DNS						
				Pre	evious	ок

<u>Step 4</u> Click **OK** to complete the network configuration. The homepage is displayed. See Figure 3-7. Figure 3-7 Homepage

1 iLinksView			2	⊛ A admin © 10
	AI Analysis	Dynamic View	Network Management	
	Alarm Message			

 \square

- After the initialization, you can just log in to the web interface with the username and password.
- You can click the module icons to go to the corresponding module interfaces.

3.2 Network Management

You can discover and view the detailed information of switches and terminal devices, such as IPC and NVR.

3.2.1 Discovering Device

You can discover, manage and analyze switches and terminal devices.

3.2.1.1 Setting Network Segment

You can set the network segment to search and add switches and terminal devices to the iLinksView platform.

 \square

Only the Dahua devices will be automatically discovered.

Step 1 Log in to iLinksView.

Step 2 Click Network Management > Network Adding > Search Network Segment.

Step 3 Click Add.

The Network Segment Search interface is displayed.

Figure 3-8 Network segment search

Network Segment Search								
Start IP								
End IP	N							
	Cancel OK							

<u>Step 4</u> Enter Start IP and End IP, and then click OK.

Figure 3-9 Search network segment

Add	Delete		
	Start IP	End IP	Operation
	172.26.2.0	172.262.255	2
	• Click 🖉	to modify start IP and end IP.	

Click ¹ to delete the network segment.

3.2.1.2 Searching SNMP Switch

When the switch cannot be discovered in batch through the network segment search, you can add it manually.

 \square

- Confirm that SNMP of the switch is configured.
- Switches that meet the SNMP settings of the iLinksView platform can be discovered directly through the network segment search, and does not need to be added manually. For SNMP settings of the iLinksView platform, refer to 4.2.3 SNMP.
- Step 1 Log in to iLinksView.
- <u>Step 2</u> Click Network Management > Network Adding > SNMP Switch.
- Step 3 Click Add.

The Add interface is displayed. See Figure 3-10.

Figure 3-10 Add a switch.

Add		×
IP :	N . N . I . I	
SNMP Version :	V2 V	
Community:		
	Cancel	к

Step 4 Enter IP, SNMP Version and Community of the switch.

 \square

IP, SNMP Version and Community should be the same as the switch setting. Step 5 Click OK.

3.2.2 Device Management

3.2.2.1 Terminal Device

You can view the detailed information of IPCs, NVRs and other devices, such as name, type, mode, IP, MAC, manufacturer and status.

Step 1 Log in to iLinksView.

<u>Step 2</u> Click Network Management > Terminal Device.

The Terminal Device interface is displayed. See Figure 3-11.

Figure 3-11 Terminal device

Device Type All	V Device Status All	✓ Enter IP, Mac, and name	ne. Q Del	ete Export Refresh			
Name	Туре	Mode	IP	MAC	Manufacturer	Status	Operation
3L06397SAU00068	IPC	(4) (disc)((0,0))	0.004	100000000000000000000000000000000000000	Private	 Online 	Û
NVR	NVR	(+************************************	1000		Private	• Online	Ū

- Click the IP address to go to the login interface of the device.
- You can search devices by IP, MAC and name.
- Click ¹ to delete the switch.
- Click Export to export the device information as csv format.
- Select one or more devices, and then click **Delete** to delete the selected devices.

3.2.2.2 Switch Management

You can view the detailed information of switches, such as name, mode, SN, IP, MAC and status.

- Step 1 Log in to iLinksView.
- <u>Step 2</u> Click Network Management > Switch Management.

The **Switch Management** interface is displayed. See Figure 3-12.

Figure 3-12 Switch management

Device Status	All	∨ Enter IP, Mae	c, and name. Q	Delete Refresh	1					
Nan	me	Mode	SN	IP	Mac	Subnet Mask	Software Version	Operation Duration	Status	Operation
164	IPOE	16 Ports PoE Switch	000000000000000000000000000000000000000		0.000.000.000		1.001.0000000.1.R	7day(s)6hour(s)32minute(s)	 Online 	© 1
SWI	тсн	4 Ports PoE Switch	000000000000000000000000000000000000000			10.000	1.001.0000003.0.R	1day(s)2hour(s)5minute(s)	 Online 	© İ

- Click the IP address to go to the login interface of the device.
- You can search devices by IP, MAC and name.
- Click ⁽¹⁰⁾ to view the details of the switch port information.
- Click to delete the selected switch.
- Select one or more switches, and then click **Delete** to delete the selected switches.

3.2.2.3 PoE Management

You can view the power consumption of switches, including total and used power consumption. And you can also remote control the PoE switch.

- <u>Step 1</u> Log in to iLinksView.
- <u>Step 2</u> Click Network Management > PoE Management.

The **PoE Management** interface is displayed. See Figure 3-13.

Figure 3-13 PoE Management

2.7%	3.2 已使用(W) 总功率(W)										421P 172.2
										,	I□(4/7
PoE总开关 🌑											

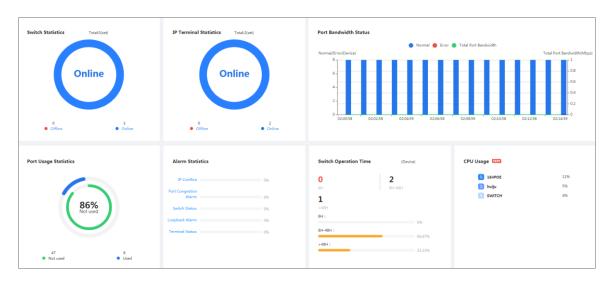
- Power consumption display of PoE switches: Display the total and used power consumption of the current switch.
 - ♦ When the used power consumption is blow 50% of the total power consumption, the status bar indicates green;
 - ♦ When the used power consumption is between 50% and 80% of the total power consumption, the status bar indicates yellow;
 - ♦ When the used power consumption is above 80% of the total power consumption, the status bar indicates red.
- PoE management: Recover terminal devices by remotely control the PoE switch.

3.3 Al Analysis

Al analysis is used for real-time analysis of network, which is convenient for troubleshooting and locating network problems.

In the homepage of the iLinksView platform, click **Al Analysis**, and the **Al Analysis** interface is displayed. See Figure 3-14. For Al analysis module description, see Table 3-1.

Figure 3-14 AI analysis



No.	Module	Description
		Display the number of online and offline switches.
1	Switch Statistics	You can click Online or Offline to directly go to the Switch
		Management interface to view the details of the online or offline switches.
		Display the number of online and offline IP terminal devices.
2	IP Terminal Statistics	You can click Online or Offline to directly go to the Terminal
2		Device interface to view the details of the online or offline
		terminal devices.
		Display the number of normal and abnormal ports and the total
	Port Bandwidth Status	port bandwidth of the switch.
3		• The number of normal ports is displayed in blue;
Ū		• The number of abnormal ports is displayed in red;
		• The total port bandwidth is displayed in green.
		Move the mouse over the histogram to view the specific value.
4	Port Usage Statistics	Display the number of used and unused ports of all switches.
		Alarm types include: IP Conflict, Port Congestion Alarm, Switch
5	Alarm Statistics	Status, Loopback Alarm and Terminal Status.
	Alarm Otatistics	You can click the alarm type to go to the Alarm Message
		interface to view the details.
6	Switch Operation Time	Switch operation time is classified as follows: less than 8 hours,
0		8–48 hours and more than 48 hours.
7	CPU Usage	Display the top 9 switches with most CPU usages.

Table 3-1 AI analysis module description

3.4 Dynamic View

Display the connection relationship of devices in the current network, and devices include IPCs, NVRs, switches and the iLinksView platform. When a device is discovered and added to the platform, the platform will automatically draw a topology graph to visually display the connection relationship between the switch and the device. For the icon description of the topology graph, refer to Table 3-2.

In the homepage of the iLinksView platform, click **Dynamic View** to view the topology graph of the current devices. Move the mouse over the link to view the details.

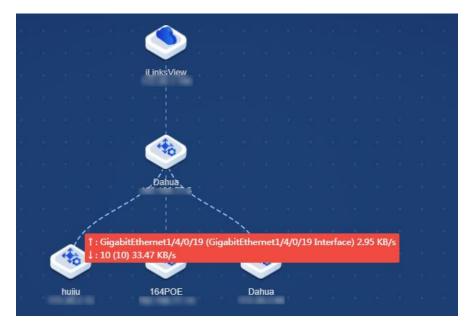


Figure 3-15 Dynamic view

Table 3-2 lcons

Icons	Description	lcon	Description
	Unmanaged switch (online)	*	Unmanaged switch (offline)
40	Managed switch (online)	40°	Managed switch (offline)
	NVR (online)	0.000	NVR (offline)
	IPC (online)		IPC (offline)
	Unknown devices (online)		Unknown devices (offline)

• Search a device At the top right corner of the **Dynamic View** interface, enter IP address or name of a

device, click, and you can search a specific device.

View detail information of a device
 Double-click the device icon to view the detail information of the device. See Figure 3-16.

Figure 3-16 Device details

Details		×
Device Information	Port Traffic	
Device Name	: 4PoE	
Device Model	: 4 Ports PoE Switch	
SN	:	
Software Version	: 1.001.000003.0.R	
IP		
MAC	:	
Subnet Mask	:	
Operation Duration	: 19hour(s)58minute(s)	
Status	: Online	

• View traffic of a switch port

Double-click the switch icon, click **Port Traffic**, and select a port. And you can view the bandwidth details. See Figure 3-17. For port description, refer to Table 3-3.

To display the received and sent flow, move mouse to the specific location of the bandwidth graph.

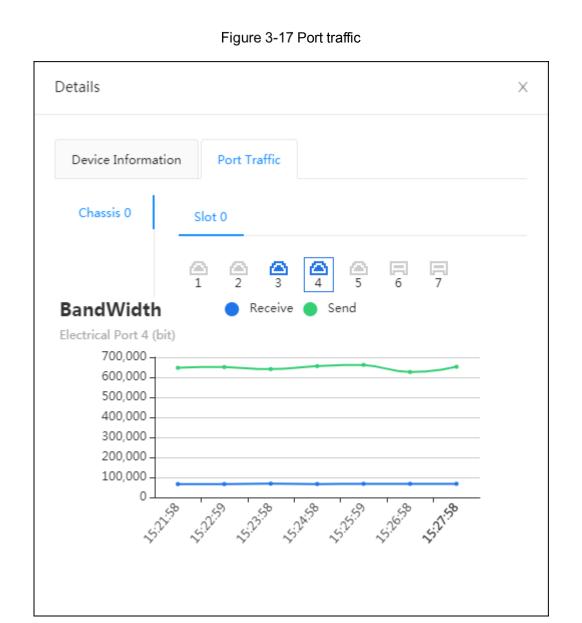


Table 3-3 Port description

Icon	Description	Icon	Description
	Ethernet port (online)		Ethernet port (offline)
	Fiber port (online)		Fiber port (offline)
?	Unknown ports (online)	P •	Unknown ports (offline)

View link details and modify port name
 Double-click a link to view the link details and modify port name. See Figure 3-18.

Figure 3-18 Link details

Details	×
Uplink Device :	Dahua
Uplink Port No.:	GigabitEthernet1/4/0/24
Uplink Port Name:	GigabitEthernet1/4/0/24 Interface
Downlink Device :	switch123
Downlink Port No.:	10
Downlink Port Name :	10
	Cancel
	10

- If the downlink device is a terminal device, modifying the port name will synchronously change the name of the terminal device.
- If the uplink device is the iLinksView platform, the port name cannot be modified.
- Device Collapse

When there are nodes under the device, click the device icon to collapse the nodes, and only the number of nodes is shown. See Figure 3-19.



Figure 3-19 Device collapse

3.5 Alarm Message

The platform displays the alarm message when a switch alarm occurs.

You can configure types of alarm messages. For details, refer to 4.2.1 Alarm Management.

To help troubleshooting problems, you can click at the upper right corner or **Alarm Message** in the homepage of the iLinksView platform to view details of the alarm message.

3.5.1 Real-time Message

Step 1 Log in to iLinksView.

<u>Step 2</u> Click Alarm Message > Real-time Message.

Step 3 Set the filtering condition to view the alarm details. See Figure 3-20.

Figure 3-20 Real-time message

Alarm Type All 🗸	Start date - End date - Delete Ignore Export Clear Refresh		
Alarm Type	Log Content	Time	Operation
IP Conflict	[Switch-ic IP conflict exists. [Conflicting Devicemac : 3csef8csf8:38	2019-11-07 09:43:19	Θ
Switch Status	ip = Offline	2019-11-07 09:41:45	Θ
IP Conflict	[Switch-ipVlan:1] IP conflict exists. [Conflicting Devicemac : 9c:14:63:45:	2019-11-07 09:28:18	Θ

- Select an alarm message, and then click **Delete** or ¹ to delete the message.
- Select an alarm message, and then click Ignore or ^O to ignore the message.
 Click Alarm Message > Ignore Message to view the ignored messages.
- Click **Export** to export the alarm messages as csv format.
- Click Clear to remove all messages.

3.5.2 Ignore Message

You can view the ignored message in the Ignore Message interface.

Step 1 Log in to iLinksView.

<u>Step 2</u> Click Alarm Message > Ignore Message.

Step 3 Set the filtering condition to view the ignored messages. See Figure 3-21.

Figure 3-21 Ignore message

Alarm Type	All V	Start date ~ End date 🖹 Delete Export Clear Refresh		
	Alarm Type	Log Content	Time	Operation
	Port Congestion Alarm	ip: Port-5 ExitDirectionCongestion Speed[10.78Mb/s]	2019-11-07 10:07:58	•
	IP Conflict	[Switch-ip] Vlan:1] IP conflict exists. [Conflicting Devicemac : 4c:11:bf:24	2019-11-06 20:22:17	•

- Select a message, and then click **Delete** or \Box to delete the message.
- Click Export to export the ignored messages as csv format.
- Click Clear to remove all ignored messages.

4 System Settings

4.1 Basic Settings

4.1.1 Basic Information

You can view the basic information of the iLinksView platform, such as CPU usage, device model and SN.

Log in to iLinksView, and then click *at the upper right corner to view the basic information* of the platform. See Figure 4-1.

Figure 4-1 Basic information

-O- CPU Usage -O- Memory Usage	Device Model DH-ILS1000
	SN
30	Software Version 1.000.000000.3.R 2019-11-6
25	MAC Address
15-	Security Baseline Version V1.4
5	System Time 2019-11-07 10:15:04 🗇 Sync PC
0 04:14:16 04:49:27 05:24:37 05:59:48 06:34:58 07:10:08 07:45:19 08:20:29 08:55:39 09:30:50 10:06:00	

4.1.2 Network Settings

You can configure the network of the Platform, including IP address, subnet mask, default gateway and DNS.

Step 1 Log in to iLinksView, and then click 2 at the upper right corner.

<u>Step 2</u> Click Basic Settings > Network Settings.

The Network Settings interface is displayed.

Network Settings	Update	Rebo	oot	Restore Facto	ry Default	Confi	g Import Export	
IP Address					1			
Subnet Mask	-		-					
Default Gateway					1			
DNS	а.		10					
	Apply							

Figure 4-2 Network settings

Step 3 Configure network as needed, and then click Apply.

4.1.3 Updating the Device

Import the upgrading file to upgrade the Device. You can get the upgrading file from technical support.

 \square

- Export the configuration file for backup before upgrade, and then import it after the upgrade is completed. For details, refer to 4.1.6 Configuring Import and Export.
- Use the upgrading file with SDA, for example, General_IL_S1000_Chn_SDA_V1.000.0000000.1.R.190911.BIN.
- Do not disconnect the power or network, or reboot or shutdown the Device during upgrade.



Upgrading with the wrong version might cause unavailability of the Device and data loss. Please operate carefully.

- Step 1 Log in to iLinksView, and then click or at the upper right corner.
- <u>Step 2</u> Click **Basic Settings > Update**.

The **Update** interface is displayed.

Figure 4-3 Upgrade

Network Settings	Update	Reboot	Restore Factory Default	Config Import Export	
Import Update file				Browse	Update now

<u>Step 3</u> Click **Browse**, and then select the upgrading file. <u>Step 4</u> Click **Update now**.

4.1.4 Rebooting the Device

Step 1	Log in to iLinksView.			
<u>Step 2</u>	Click 🧿 on the upp	er right corner	, and then sele	ect Reboot .
<u>Step 3</u>	Click Reboot Now.			
		Figure 4-4	Reboot	
	Network Settings	Update	Reboot	Restore Factory Default

4.1.5 Resetting the Device

Refer to the following two ways to reset the Device.

① Reboot Now

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 4-5 System reset on web interface

Network Settings	Update	Reboot	Restore Factory Default
Omple	tely restore device pa	arameters to factory	y default.
C Restore	Now		

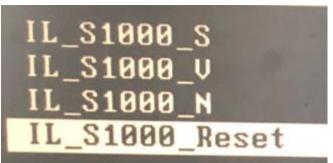
On the Device

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

<u>Step 2</u> Connect the power source, hold down keypad (\uparrow), and go to the system reset interface.

Step 3 Select IL_S1000_Reset, and then press Enter key.

Figure 4-6 System reset on the Device



4.1.6 Configuring Import and Export

You can import the configuration from other devices to the current device or export the configuration of the current device to local.

Step 1 Log in to iLinksView, and then click 2 at the upper right corner.

<u>Step 2</u> Click **Basic Settings > Config Import and Export**. The **Config Import and Export** interface is displayed.

Figure 4-7 Configure import and export

Network Settings	Update	Reboot	Restore Factory Default	Config Import Export		
Select File				Browse	Config Import	Export

<u>Step 3</u> Import or export configuration.

- Import configuration
 - 1. Click **Browse** to select the file you want to import.
 - 2. Click Config Import.
- Export configuration Click **Export** to export the configuration of the Device.

4.2 Global Configuration

4.2.1 Alarm Management

You can set the alarm types that the iLinksView platform can receive. If the alarm type is not enabled, the platform will not receive the corresponding alarm message even if this type of alarm occurs.

Step 1 Log in to iLinksView, and then click 2 at the upper right corner.

<u>Step 2</u> Click Global Config > Alarm Management.

The Alarm Management interface is displayed. See Figure 4-8.

Figure 4-8	Alarm m	anagement

Alarm Management	Perf	ormance Mar	nagement	SNMP	
IP Conflict Alarm					
Switch Status Alarm	ı				
Terminal Status Ala	rm				
Loopback Alarm					
Port Congestion Ala	arm		Threshold	90	(90-100)%
ОК					

Step 3 Set alarm types that you want to enable and threshold, and then click OK.



Loopback Alarm is valid only when the loop protection of the switch is enabled.

4.2.2 Performance Management

You can set the period of device discovery and deletion.

Step 1 Log in to iLinksView, and then click or at the upper right corner.

Step 2 Click Global Config > Performance Management.

The **Performance Management** interface is displayed.

Figure 4-9 Performance management

Alarm Management	Performance Management	SNMP
Device Discovery Pe	riod 1	(1-10)minute(s)
Device Delete Period	d 4	(4-43200)minute(s)
ок		

Step 3 Set Device Discovery Period and Device Delete Period, and then click OK.



Device Delete Period must be set to 4 times or above of Device Discovery Period.

4.2.3 SNMP

SNMP is used to set the general switch protocol. After the setting is completed, the switches that match the protocol can be discovered and added directly to the iLinksView platform. And you do not need to search and add them separately.

Step 1 Log in to iLinksView, and then click 2 at the upper right corner.

<u>Step 2</u> Click Global Config > SNMP.

The **SNMP** interface is displayed.

Figure 4-10 SNMP

Alarm Management	Performance Management	SNMP
SNMP Version	V2 ~	
Community	public	
Port	161	(1-65535)
ок		

Step 3 Enter SNMP Version, Community and Port, and then click OK.

4.3 Safety Management

4.3.1 HTTPS

You can log in to the web interface of iLinksView by HTTPS, which ensures the security of communication data, and guards the user information and device security.

Ш

- If it is your first time to use HTTPS or after you change the IP address of the Device, you need to create the server certificate and then download and install the root certificate.
- If you want to log in to the web interface of iLinksView on a new PC by HTTPS, please ensure that the root certificate is installed on the new PC.
- The HTTPS setting takes effect after the iLinksView platform restarts.

Step 1 Log in to iLinksView, and then click 2 at the upper right corner.

Step 2 Click Safety Management.

Figure 4-11 Safety management

нттру С	
SSH C	
Create Server Certificate	Download Root Certificate

Step 3 Enable HTTPS.

<u>Step 4</u> The confirmation dialog box is prompted, and then click **OK**. Figure 4-12 Confirm to restart

?	Prompt			
	Settings will take effect after the Are you sure to change the con the application?			
		Cancel	ОК	

4.3.2 SSH

After SSH is enabled, you can access the iLinksView platform background through SSH connection tool, which facilitates remote debugging by technical personnel.

Step 1 Log in to iLinksView, and then click 2 at the upper right corner.

- Step 2 Click Safety Management.
- Step 3 Enable SSH as needed.

4.4 Firewall

You can set the white list and black list of the platform by adding IPs or IP segments.

- Step 1 Log in to iLinksView, and then click or at the upper right corner.
- Step 2 Click Firewall.
- Step 3 Enable Firewall.

Figure 4-13 Enable firewall

	White List Black List	
Add	Delete	
	Ib	Operation
		No Data
ОК	Refresh	

Step 4Select White List or Black List.Step 5Click Add.

Add		Х
Т	ype: IP	~
	IP	
		Cancel OK

Figure 4-14 Add IP

<u>Step 6</u> Enter the IP or IP segment. <u>Step 7</u> Click **OK**.

4.5 Language Setting

Step 1 Log in to iLinksView, and then click of at the upper right corner.

Step 2 Select English.

4.6 System Log

You can view details of user operation, such as login and logout.

Step 1 Log in to iLinksView, and then click of at the upper right corner.

Step 2 Click System Log.

Figure 4-15 System log

Start date ~ End date Clear			
Log Content	Log Type	Operator	Time
Address:	LogOut	admin	2019-11-07 11:14:01
Data/SHD; Enable:No->Yes;	SaveConfig	admin	2019-11-07 11:13:45
Addres Type:Web3.0;	LogIn	admin	2019-11-07 11:11:55
Address	LogOut	admin	2019-11-07 11:08:03

- You can filter logs according to start date and end date.
- Click **Export** to export logs as csv format.
- Click Clear to remove all logs.

4.7 Modifying Password

There are two ways to change the user password.

By User Management

- Step 1 Log in to iLinksView, and then click of at the upper right corner.
- Step 2 Click User Management.
- Step 3 Click 2
- <u>Step 4</u> Enter the old password and new password, confirm the new password, and then click **OK**. See Figure 4-16.



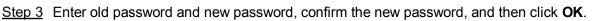
Modify Password		×
Old Password:		
New Password		
Confirm Password		
	Cancel	ОК

By Admin Icon

<u>Step 1</u> Log in to iLinksView, and then click

A admin at the upper right corner.

Step 2 Select Modify password.



4.8 Logout

A admin

<u>Step 1</u> Log in to iLinksView, and then click at the upper right corner.

<u>Step 2</u> Select Logout, and the system redirects to the login interface.

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 on how to create a more secured security system.

Mandatory actions to be taken for basic equipment 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 equipment (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 equipment 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 equipment network security:

1. Physical Protection

We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment 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 equipment (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 equipment 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. Enable Whitelist

We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.

8. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.

9. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

10. 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.

11. 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.

12. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

13. Network Log

Due to the limited storage capacity of the equipment, 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.

14. Construct a Safe Network Environment

In order to better ensure the safety of equipment 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.

Поставщик систем безопасности TELECAMERA.RU

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. Address: No.1199, Bin'an Road, Binjiang District, Hangzhou, P.R. China Postcode: 310053 Tel: +86-571-87688883 Fax: +86-571-87688815 Email: overseas@dahuatech.com Website: www.dahuasecurity.com