Tiandy

MicroSense AI Box

User Manual



ISO 9001:2008
ISO 14001:2004

Thank you for choosing our production

Please read this manual carefully before using this product

Preface

Thank you very much for purchasing our products. If you have any questions or needs, please feel free to contact us.

Applicable Model

This manual applies to the following models:

product line	product model	product name
AI Box	TC-P5820 Configuration: SQ	MicroSense AI Box

disclaimer

- This manual may contain inaccuracies, discrepancies in product functionality or operation, or printing errors. We will update this manual as product features evolve and regularly improve the described software and hardware products. Updates will be reflected in the latest version of this manual without prior notice.
- As our company continuously adopts new technologies, our products are updated in real time. No separate notice will be given for any upgrades.
- This manual serves solely as a reference guide for customers and does not guarantee complete consistency with the actual product; the final application shall be based on the physical product.
- The components, parts, and accessories listed in this manual do not constitute the standard configuration of the equipment; please refer to the packing list for detailed specifications.

- All text, tables, and images in this manual are protected by applicable national laws and may not be reproduced without authorization.

About Default

- Default administrator account for the device upon factory shipment: admin
- Default administrator password upon device delivery: admin (Please change the administrator password promptly)
- Default IP address for the device upon factory shipment: 192.168.1.3

symbol description

The symbols appearing in this article are explained as follows:

symbol	explain
	Indicates a moderate or low potential hazard that, if not avoided, may cause minor to moderate injuries to individuals.
	This indicates potential risks. Ignoring this text may result in device damage, data loss, reduced performance, or unforeseen consequences.
	Represents additional information to the main text, emphasizing and supplementing it.

catalogue

1. Product Function Overview 5 6
2. Essential Reading for Operation 6 6
2.1. Panel Introduction and Description 6 6
3. Installation and Connection 8 8
3.1. Installation Notes 8 8
4. Web Interface Operations 10 10
4.1. Operating Environment 10 10
4.2. IE Settings 10 10
4.3. Login Device 11 11
4.4. Video Preview 14 14
4.5 Understanding the Details 15 16
4.6 Configuration 16 16
4.6.1 Channel Management 16 16
4.6.2 Video Parameters 21 21
4.6.3 Network Configuration 23 23
4.6.4 Zhimiao Configuration 30 30
4.6.5 System Settings 39 39
4.6.6 System Maintenance 44 44

1. Product Function Overview

Introduce the key functional features users should know when using the server.

basic function

- Supports network device connectivity, including network cameras, network dome cameras, and third-party network cameras.
- Supports private protocols, ONVIF, and RTSP connections.

Local Monitoring

- Supports single-screen video preview.
- Supports up to one video preview.

Other Local Features

- Administrators can create multiple operational users and set their permissions, which can be refined down to individual services.
- Supports manual or automatic device time adjustment.

Network Functions

- Supports TCP/IP protocol clusters and protocols such as DHCP, DDNS, and NTP.
- Supports system maintenance operations such as remote upgrade programs and reboots.

explain ：

- Product Features: This section lists the main features supported by our servers. Functions may vary depending on model specifications and configurations; please refer to the physical product for details.

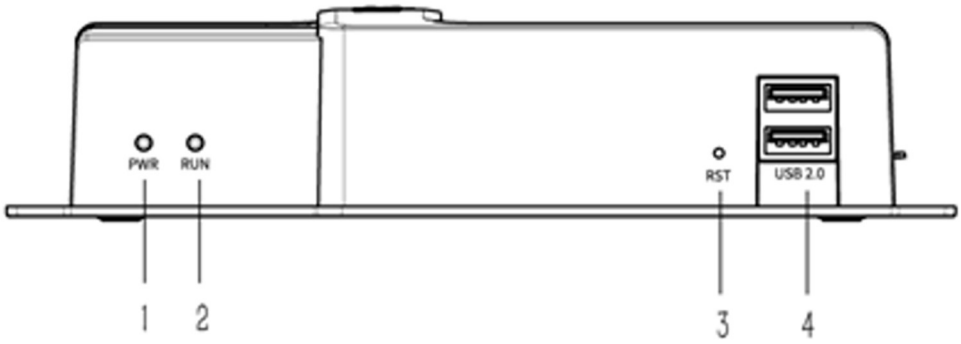
2. Essential Operations

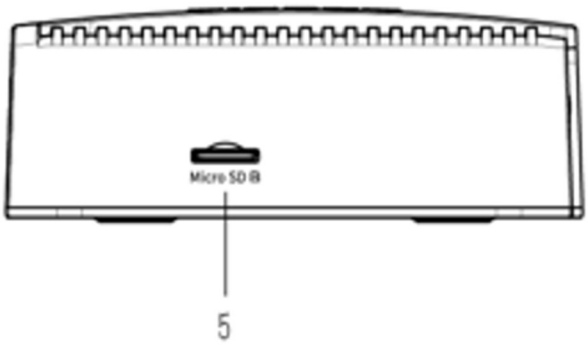
Introduce the components and accessories users must understand before using the server: front and rear panels, mouse, and how to operate the device with these components and accessories.

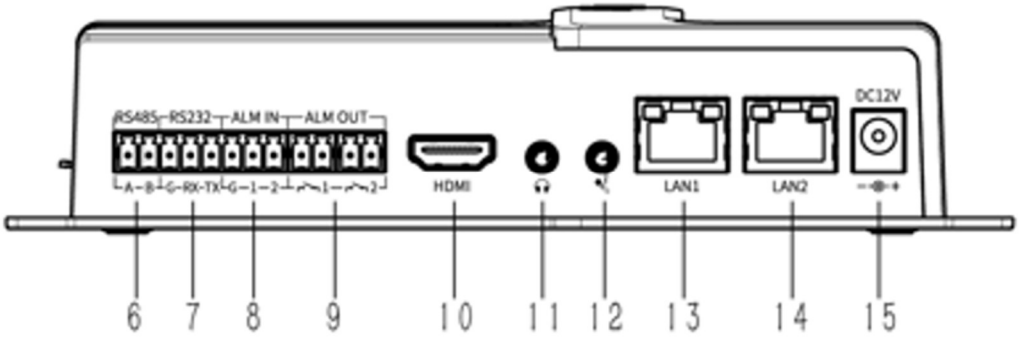
2.1. Panel Introduction and Description

Introduction to device panel interface specifications.

The interface is shown below:



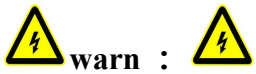




No.	Key Name	Identifier	Function Description
1	Power Indicator	PWR	Steady light indicating device startup
2	Power Supply Light	RUN	Green light, customizable
3	Reset Button	RST	Reserved
4	USB 2.0	USB2.0	USB ×2
5	Micro SD	Micro SD	Reserved
6	RS-485	RS485	Reserved
7	RS-232	RS232	Debug serial port
8	Alarm Input	ALM IN	Reserved
9	Alarm Output	ALM OUT	Reserved
10	HDMI	HDMI	Reserved video interface
11	Audio Output (3.5mm)	🎧	Reserved
12	Intercom Input (3.5mm)	—	Reserved
13	RJ45	LAN1	Default IP: 192.168.1.3
14	RJ45	LAN2	Default IP: 192.168.2.3, supports POE AT/AF
15	Power Interface	DC12V	Input via DC 12V power adapter

3. Installation and Connection

3.1. Installation Notes



Improper battery replacement may cause explosion; users are advised not to replace it directly. If replacement is necessary, use only batteries of the same type or equivalent type.

Please note the following during installation:

- Do not place containers containing liquids (e.g., cups) on the server.
- Install the server in a well-ventilated location. When installing multiple devices, keep them at least 2 cm apart.
- Keep the server operating within the permitted temperature range (0°C to +55°C) and humidity range (10% to 90%).
- When cleaning the equipment, always disconnect the power cord and completely cut off the power supply.
- Dust on server circuit boards can cause short circuits when moistened. Regularly use a soft-bristled brush to clean the circuit boards, connectors, chassis, and fans. If dirt is difficult to remove, wipe it off with a water-diluted neutral cleaner and dry thoroughly.
- When cleaning equipment, do not use volatile solvents such as alcohol, benzene, or diluents. Avoid strong or abrasive cleaning agents, as they may damage surface coatings.
- Ensure that no hazards arise due to uneven mechanical loads.

- Ensure there is sufficient installation space for video and audio cables; the cable bending radius should be at least 5 times the cable's outer diameter.
- Ensure the server is properly grounded.

explain ：

- When you receive this product, verify its contents against the Equipment Packaging List inside the box. If you find any damage to items or missing components, contact your dealer immediately.

4. WEB Interface Operations

4.1. Java runtime environment Java

It is recommended to run on Windows 7 or later operating systems. To ensure optimal performance and functionality, verify that the following settings are correctly configured after successful installation:

(1) Set the display resolution to 1024×768 or higher, and color to Enhanced Color (32-bit). For details on configuring display resolution and color, see Windows Help or Online Help.

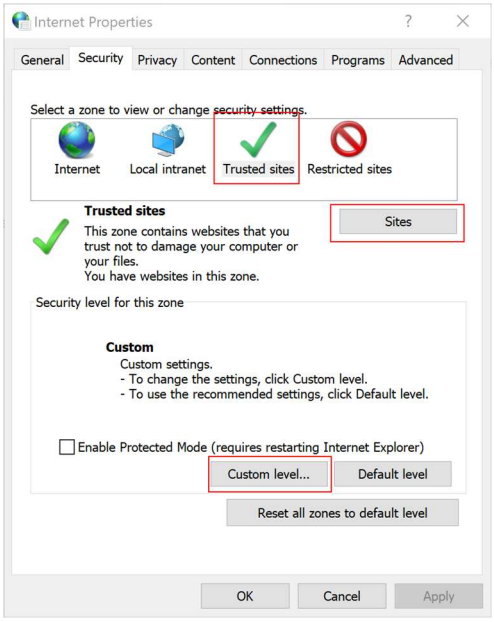
(2) Ensure that the required font, Songti, is installed on the Windows operating system. If the system interface displays incorrectly, it may be due to missing or corrupted fonts; reinstall them.

4.2. IE set up

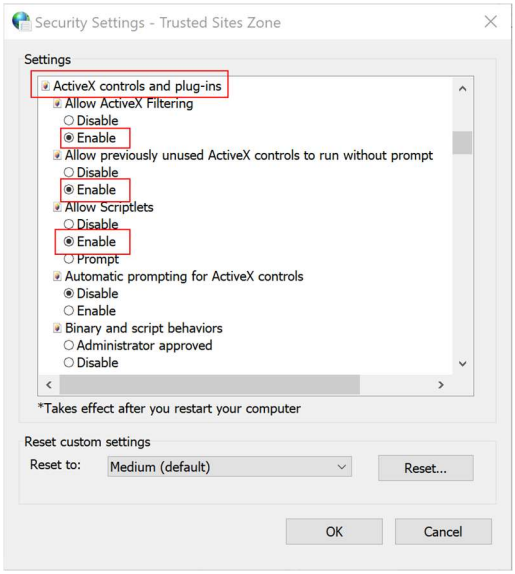
If you're using this series of online video products for the first time, you need to download the ActiveX control. Before downloading, configure your IE browser accordingly to ensure successful installation.

Note: Use the built-in IE browser in Windows (version 8.0 or later). Except for Firefox and Google Chrome, avoid using third-party browsers or any IE extensions such as Maxthon or World Window, as we cannot guarantee proper login functionality with these applications.

When your computer connects to the camera for the first time, go to Internet Options> Security> Trusted Sites> Sites and add the camera's IP address to the Trusted Sites list. Then set Custom Levels and enable all options under ActiveX Controls and Plugins to ensure the control downloads and runs properly.



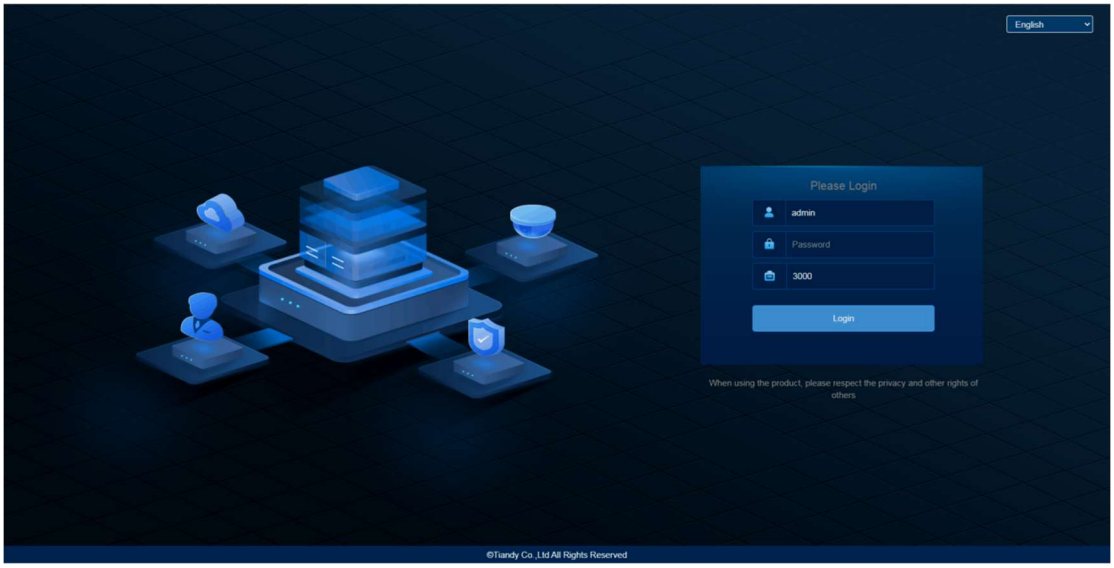
IE Browser – Internet Options



Trusted Sites – Custom Levels

4.3. Log in to Device

The device's default IP address is 192.168.1.3, subnet mask: 255.255.255.0, and gateway: 192.168.1.1. Set your computer's IP to the same subnet as the device's IP—for example, set it to 192.168.1.3 to access the device via IE. Open IE, enter the network video device's IP address in the address bar, and click "Go" to log in.



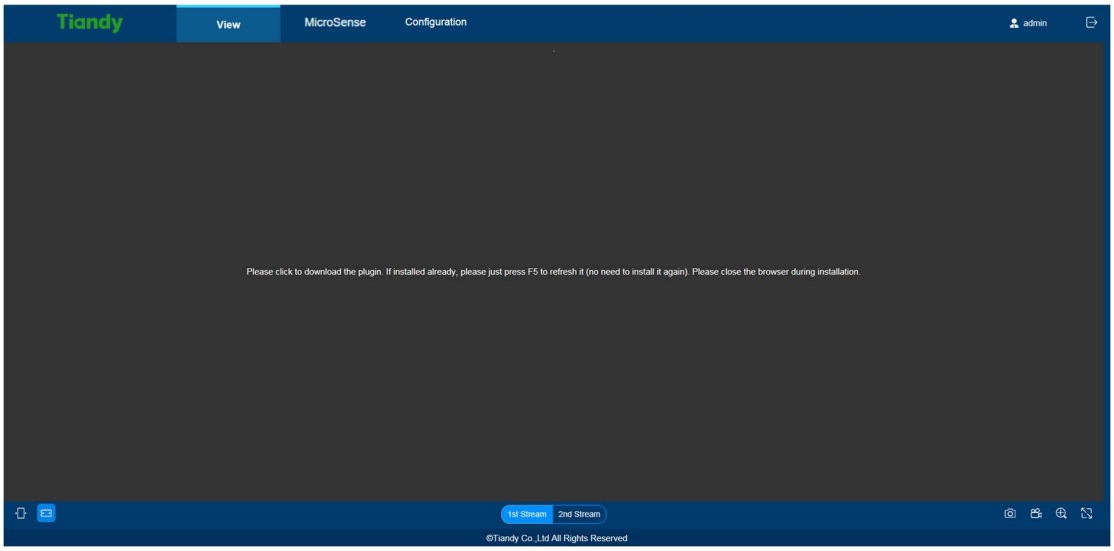
IE login interface

Enter the correct username and password in the login window, click "Login", and you will soon enter the preview interface.

explain ：

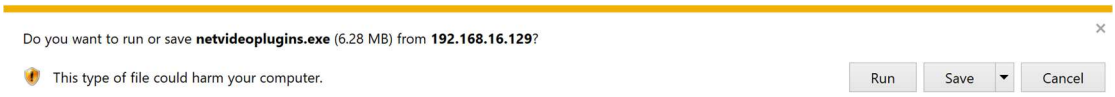
If you change the device port number, enter the correct value; the default is 3000.

If you are using it for the first time, you will see the following interface.



Download Control Prompt Page

Click the text link to open the Save or Run dialog box, as shown below. Select "Save" to download netvideoplugins.exe locally; select "Run" to automatically install Swallow.exe after completion.



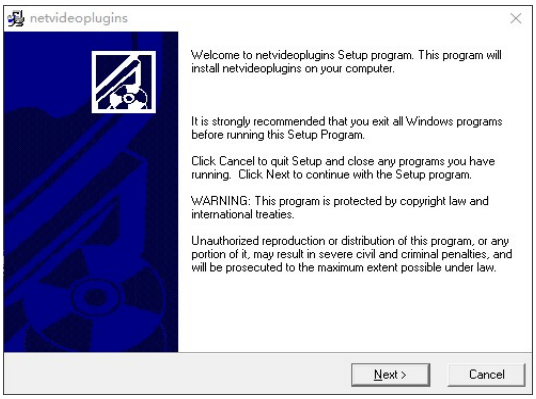
Save or run the control interface

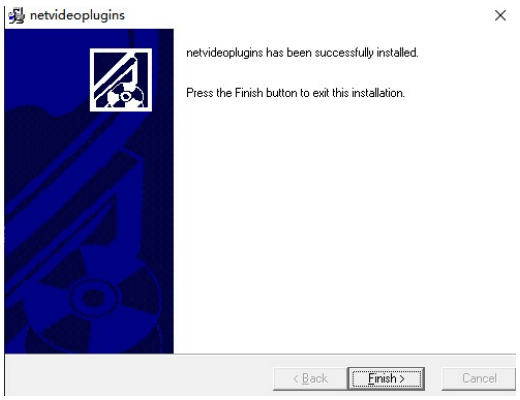
After downloading the control, you need to install it. A dialog box will appear with the Control Installation Program interface; click the Run button as shown below.

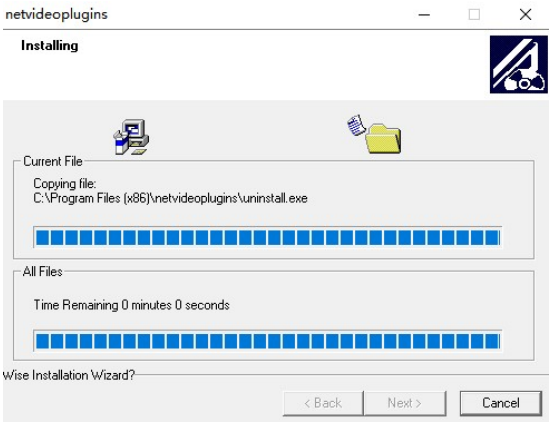


Operation Control Installation Program Interface

When the control installation interface appears, click the Next button as shown below.

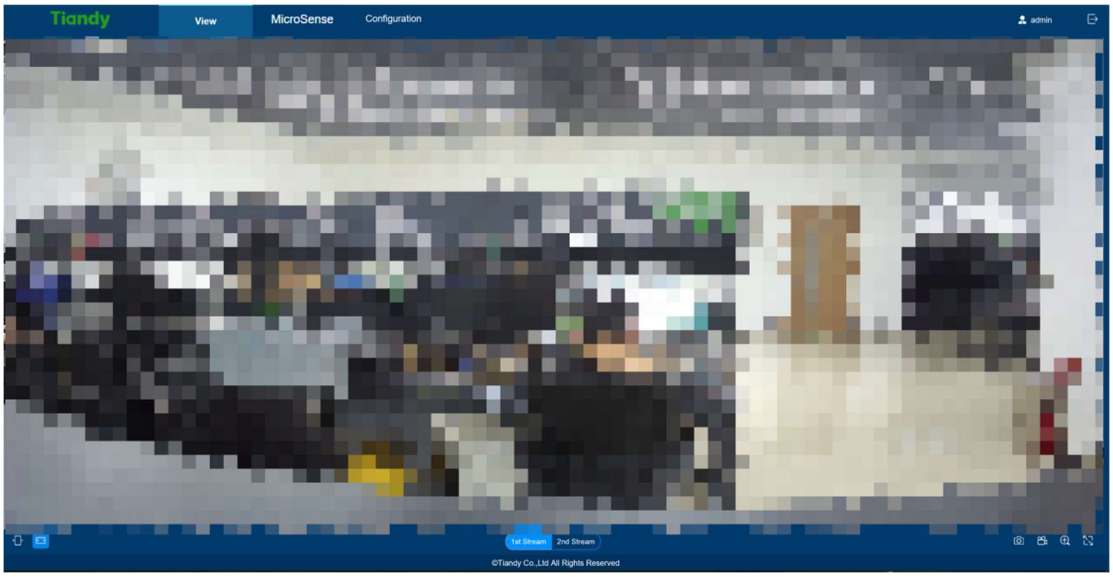






Installation Controls Interface

After the plugin is installed, refresh your browser to view the preview image as shown below.



Video Preview Interface

After logging in, click the icon at the top of the interface to switch between different views or execute relevant commands.

icon	explain
preview	Click this icon to enter the Preview interface.
Perceiving the subtle details	Click this icon to enter the "MicroSense" interface.
configure	Click this icon to enter the System Configuration interface. This interface allows you to configure network settings, channels, MicroSense, and system settings.
admin	Displays the username for this login. (This icon is for display only; do not click it)
	Click this icon to log out of your current account.

Note: To ensure your information security, please change your initial password!

4.4. Video Preview

After successful login, the system displays the [Preview] interface by default. In

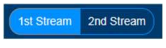
this interface, users can view a real-time preview video of the added camera.

On other interfaces, users can click the [Preview] button at the top to return to the video preview interface.

explain ：

Double-click the video to display it in full screen. Double-click again or press the Esc key to exit full screen mode.

Video Preview Interface Button Functions:

icon	explain
	Fixed aspect ratio: Click to enable. The video will play in the fixed aspect ratio of the front-end device.
	In the adaptation window, click Enable to play the video at the window's aspect ratio.
	Local capture: Click to enable. Captures images from the selected window and saves them locally. (You can modify the local save path in System Configuration-> System Settings-> Local Settings.)
	Local recording: Click Enable to record the video from the selected window and save it locally. (You can modify the local save path in Configuration-> System Settings-> Local Settings.)
	Electronic Zoom Button: When enabled, click the left mouse button to select the area you want to enlarge and view it.
	Full-screen display button: Click the icon to bring the video surveillance screen to full screen. Double-click the video frame to exit full-screen mode.
	Switch between main and secondary streams: Click the icon to change the main or secondary stream for the current preview video.

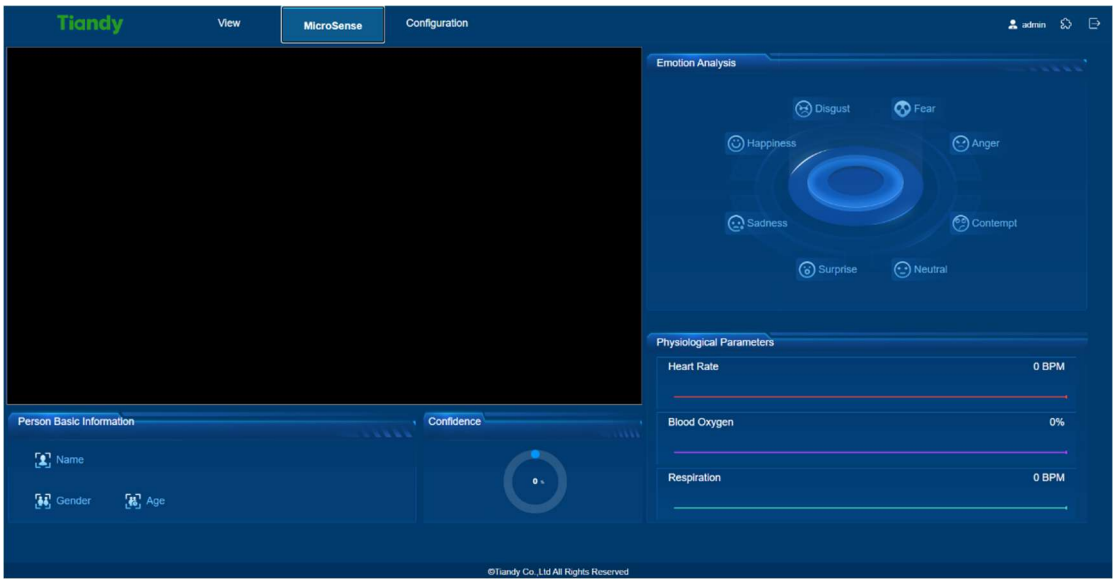
pay attention to

(1) All icons are valid when pressed.

4.5 Recognizing the Subtle Details

Click the [MicroSense] button to enter the [MicroSense] interface. Here, you can

view basic information, expression analysis, physiological parameters, and confidence levels of individuals in the video.



MicroSense Interface

explain ：

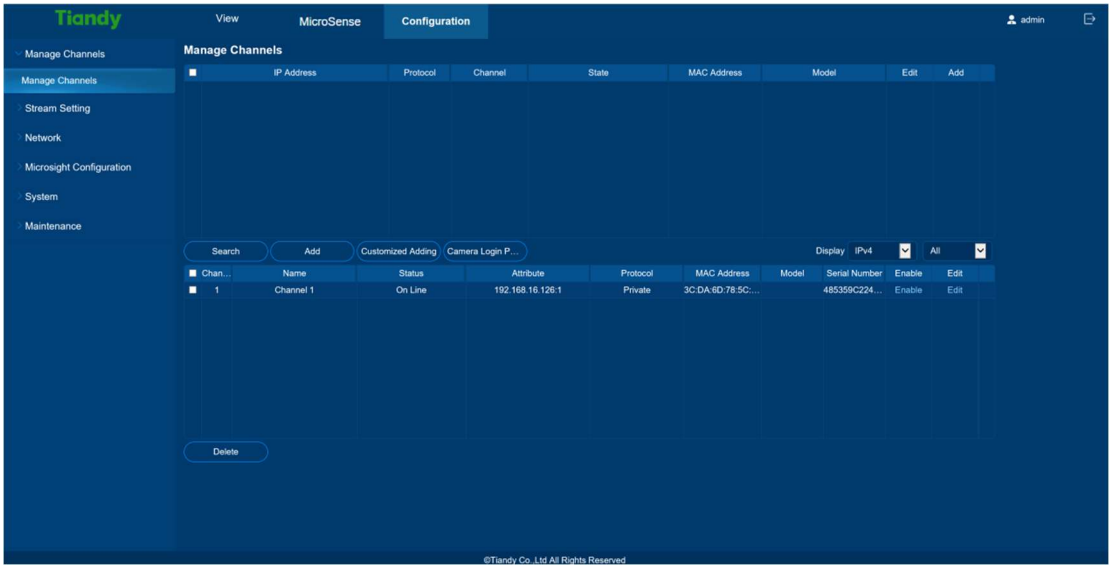
This page can display personnel basic information, physiological parameters, confidence scores, and facial expression analysis results only after enabling the algorithm on the Configuration> MicroSense Configuration> Algorithm Configuration page.

4.6 Configuration

Click the [Configure] button to enter the configuration interface. This interface displays commonly used functions such as network IP settings, time settings, and user management.

4.6.1 Channel Management

On the Channel Management page, click Search Camera Device and enter the correct password to add a camera.



Channel Management Page

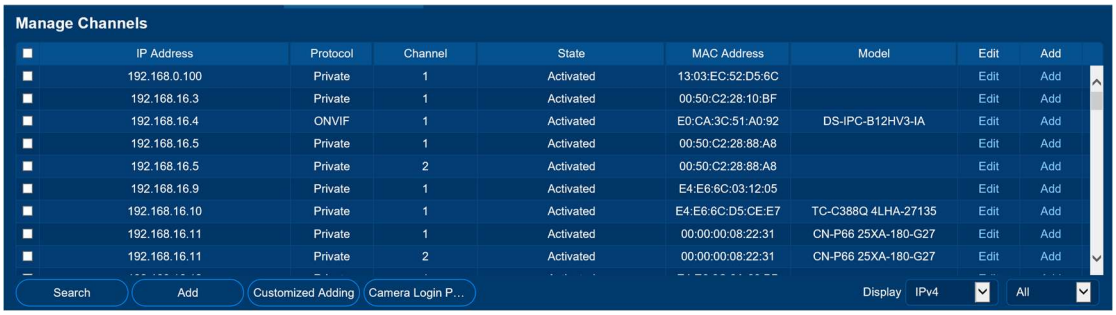
Basic operations are shown in the table below:

icon	explain
search	Click the search icon to search all cameras on the network and sort them by IP address in ascending order.
add	Select the devices found in search and click Add to add cameras to the box. If the number of selected cameras exceeds the number of supported connection channels, a message will appear: No extra available channels. Delete some channels manually.
Custom Addition	Click Custom Add to go to the custom add page. You can customize protocol types and connection modes.
Camera Login Password	Click Camera Login Password to enter your camera password. All added cameras will use this password for login after saving.
Display Filter	You can modify filter conditions: IPv4 or IPv6 addresses, all, private, or ONVIF connection method (default: IPv4 All).
delete	Select the added cameras and click Delete to remove them from the current device.
Enable/Disable	Click to switch between enabled and disabled states. The camera connects normally when enabled; it disconnects when disabled.
edit	Click the Edit button to modify the IP address, username, password, and

	other details of the added camera.

4.6.1.1 Search and Add Channels

Click the search icon to search all cameras on the network and sort them by IP address in ascending order.



search result

explain ：

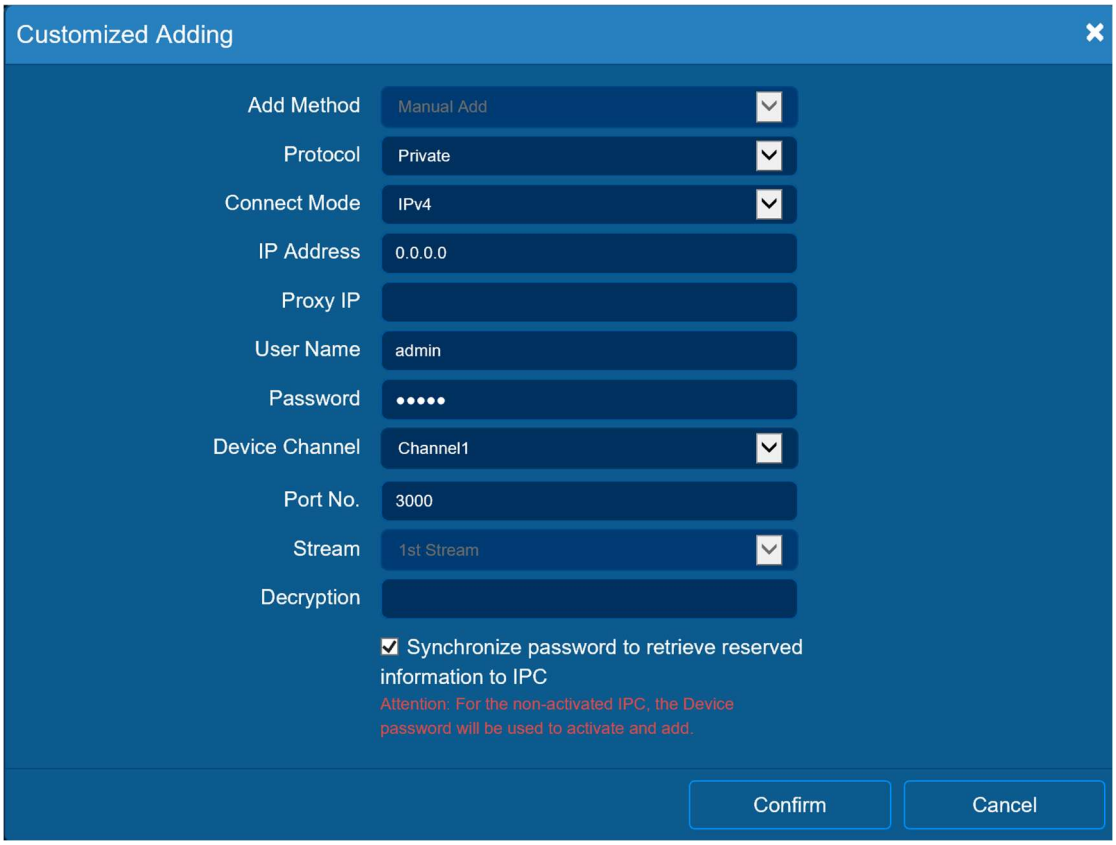
If the [Camera Login Password] is not configured in , the system will use the NVR password by default when adding a device.

The status bar displays whether the device is activated and whether it has been added by other NVR devices.

Only some devices in the can indicate whether they have been added by other devices; please refer to the actual status.

4.6.1.2 Custom Addition

Customize the add page to select different protocol types and connection methods.



Customize the Add/Edit Interface

Basic operations are shown in the table below:

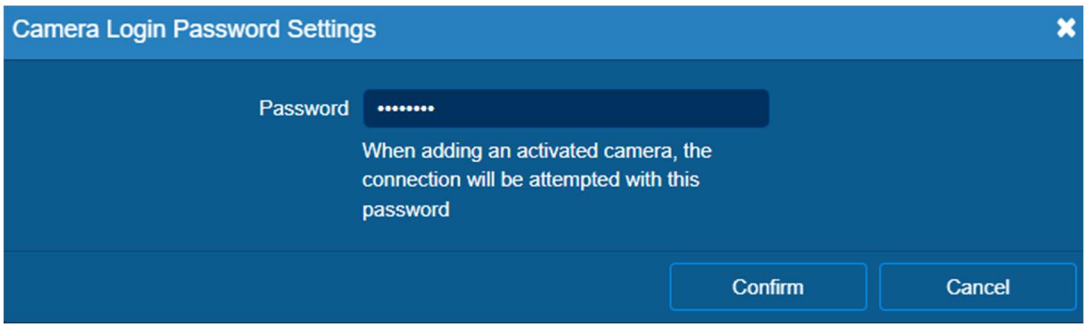
icon	explain
channel	The box supports adding only one channel, so Channel 1 is displayed at the channel position.
adding mode	The default addition method for custom additions is manual; disabling it cannot be changed.
protocol type	The types include Private Protocol, ONVIF Protocol, and RTSP.
Connection Mode	The types include IPv4, IPv6, and EasyDDNS.
IP address	Enter an IPv4 or IPv6 address; the default is 0.0.0.0
agent IP	Enter the camera's proxy IP
user name	Enter the camera username
password	Enter the camera login password
Device Channel	Select the camera channel you want to add.
Bitrate Type	The main stream is displayed by default and cannot be changed when

	grayed out.
port number	The default port number is 3000; modify it according to the camera's actual port number.
Decrypt Password	When the camera is encrypted for video, you can enter a password at the decryption field. The default decryption setting applies after adding the camera.
confirm	Click the Confirm button to save changes on this page.
cancel	Click the Cancel button to discard changes on this page and close the pop-up window.

pay attention to ：

- For devices using private protocols, available connection modes include IPv4, IPv6, and Easy DDNS.
- When the device type uses the ONVIF protocol, available connection modes include IPv4 and IPv6.
- The connection mode is not displayed when the device type is RTSP.
- Sync password recovery details: Sync the password recovery details configured on IPC, such as phone number.

4.6.1.3 Camera Login Password Configuration



Camera Login Password Setting Page

pay attention to ：

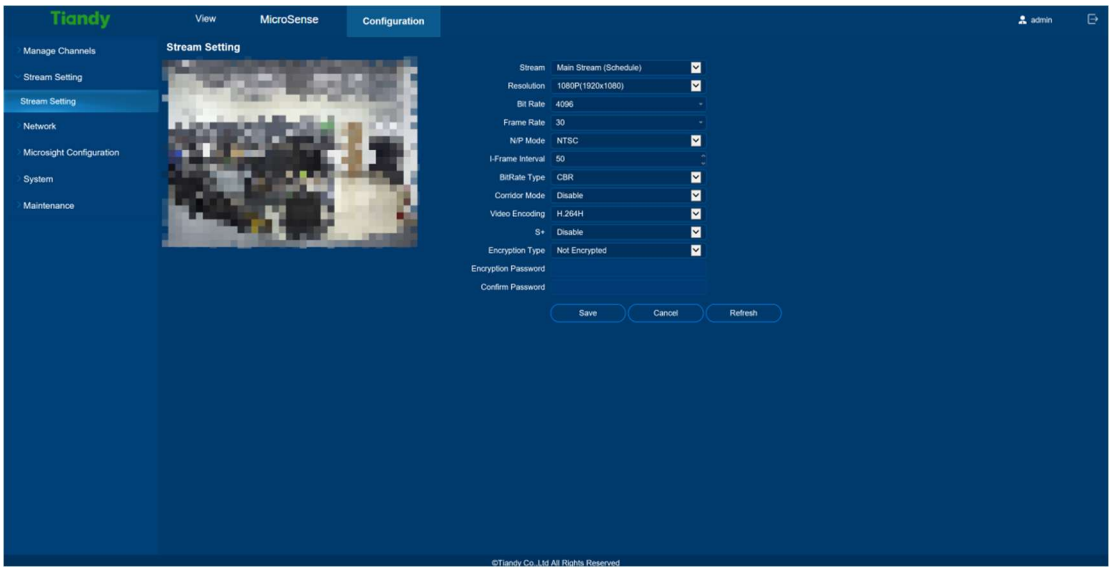
After configuring your login password, adding a device will use the configured password; otherwise, the NVR password will be used.

4.6.2 Video Parameters

4.6.2.1 Video Parameters

In the video parameters interface, you can configure video parameter settings for each point and synchronize them to the front end.

1.1.1.1.1. video parameter



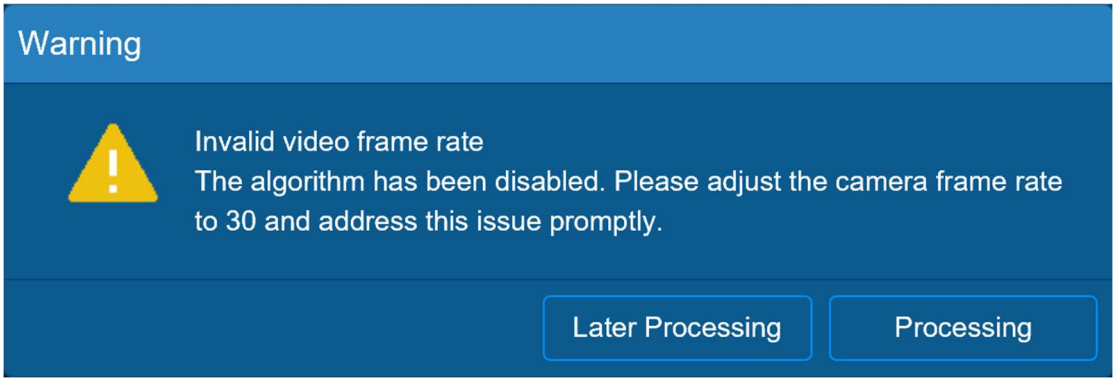
Video Parameters Interface

Basic operations are shown in the table below:

icon	explain
Service Selection	Select the service name with parameters to set.
Point Selection	Select the points to set.
Flow Type	Select pure video or audio-video.
resolution ratio	Set the video resolution (maximum supported resolutions vary by model).
Bitrate	Set the video bitrate in kb/s. Range: 32 to 16384 kb/s. Tip: Select the desired resolution from the Resolution dropdown list to switch the bitrate to the specified value. When Compression Mode is Fixed Bitrate, the Bitrate represents the actual bitrate of the stream; when Compression Mode is Variable Bitrate, the Bitrate represents the

	maximum allowed bitrate for the stream. (Supported bitrates vary slightly by model; refer to the actual specifications)
frame rate	Set the frame rate of the current video. Under the [PAL] format, some models support 50 frames; with wide dynamic range enabled, the maximum supports 25 frames. Under the [NTSC] format, some models support 60 frames; with wide dynamic range enabled, the maximum supports 30 frames.
standard	You can choose PAL or NTSC.
I-frame Rate	You can set the number of frames between every two I-frames, ranging from 10 to 100.
compress mode	Set either fixed-bitrate or variable-bitrate compression. With fixed-bitrate, video data volume remains stable, ensuring consistent bandwidth usage during network transmission; with variable-bitrate, data volume varies according to video complexity, conserving bandwidth when scenes are repetitive. Variable-bitrate offers multiple levels, where higher levels result in greater average bitrates.
video coding	Set the video encoding format. H.265 uses less bandwidth, but some browsers or players do not support it.
S+	Switch the drop-down list to enable or disable S+. When enabled, features such as compression mode, video quality, I-frame rate, and key areas will be unavailable.
preserve	Click Enable to save current data and synchronize it to the corresponding front-end device.
resetting	Click Enable to restore the last saved parameters.
renovate	Click Enable to allow re fetching of front-end parameters.

Note: After enabling the algorithm, the channel format must be N-mode 30 frames; otherwise, a prompt will appear.

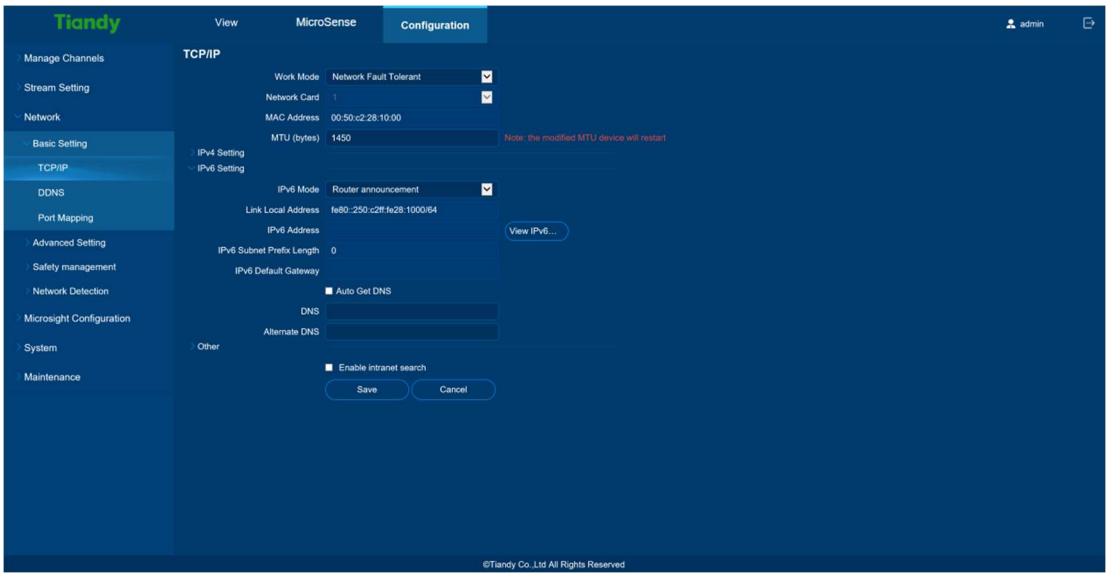


4.6.3 Network Configuration

The network configuration interface primarily allows you to configure your device's network settings, such as IP addresses, DNS configurations, and blacklists/whitelist rules.

4.6.3.1 Basic Settings

4.6.3.1.1 TCP/IP Configuration



TCP/IP Configuration Interface

[Auto-assign IP Address]: Set whether the DHCP server automatically assigns an IP address to the device.

[IPv4]: Set the device's IP address, subnet mask, and gateway.

[IPv6]: The device supports IPv6. Users can view the device's IPv6 address and subnet mask on the page.

[DNS]: Set the DNS server address.

[Physical Address]: Shows the device's physical address.

[MTU]: Set the MTU size (range: 500–1500; default: 1500). After setting, click [Save] to apply the changes. The settings will take effect after restarting the device.

[HTTP Port]: Enter the [HTTP port number] in the input field on the page, then restart the device to change the HTTP port number.

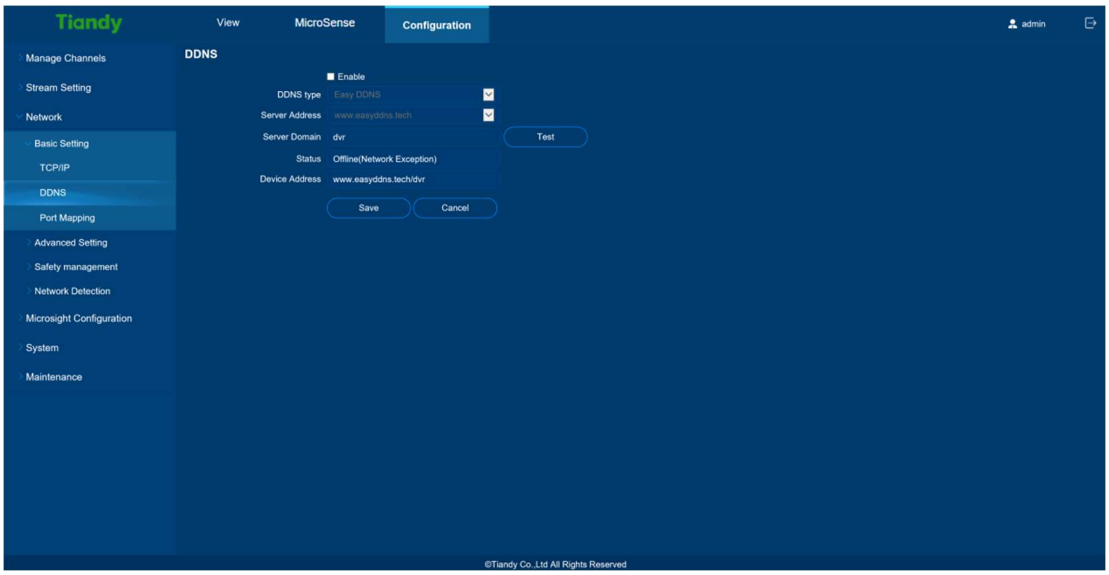
[HTTPS Port]: Enter the [HTTPS port number] in the input field on the page, then restart the device to change the HTTPS port number.

[Save]: Save the current settings.

[Reset]: Restore the last saved parameters.

4.6.3.1.2 DDNS Configuration

DDNS primarily maps users' dynamic IP addresses to a fixed domain name resolution service.



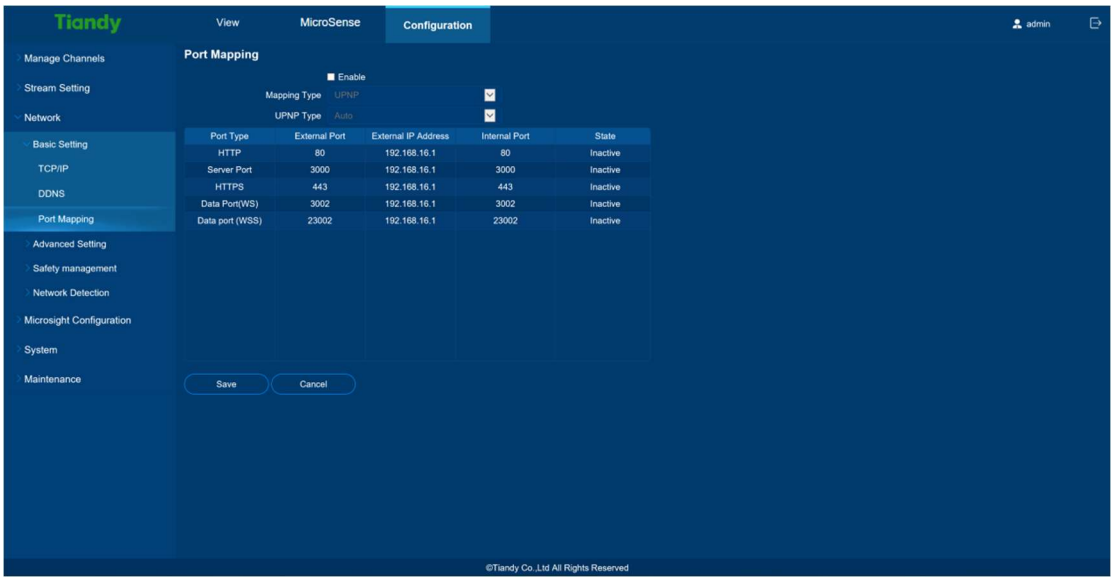
DDNS Configuration Interface

After checking [Enable] DDNS, select the server address to configure, modify the device domain name, set the server address, username, password, and confirmation password, then click Save to configure DDNS network server information. Click Reset to restore the previously saved parameters.

4.6.3.1.3 Port Mapping

Port mapping can primarily be executed on a local network gateway, associating

a specific gateway server port with a corresponding port on a local machine. Accessing the gateway server's configured port from outside the LAN is equivalent to accessing port 80 on an internal machine, enabling device login.



Port Mapping Interface

Enable port mapping to allow network devices to open ports properly. Port mapping modes are "Automatic" and "Manual".

1. Select the "Automatic" mode and enable UPnP; users do not need to perform port mapping on the router—simply activate the UPnP function.

2. Select "Manual" mode, where users must manually configure port mapping on the router. In manual mode, users can specify the external port to map from a public IP address without modifying the device's ports. If the router or gateway does not support UPnP functionality, users may enter the current status of the mapped external port here.

3. The "Status After Port Mapping" field indicates whether the mapping is active, while displaying the external port corresponding to the currently mapped public IP address on the external ports list. Users must use this mapped external port to access network devices over the public network.

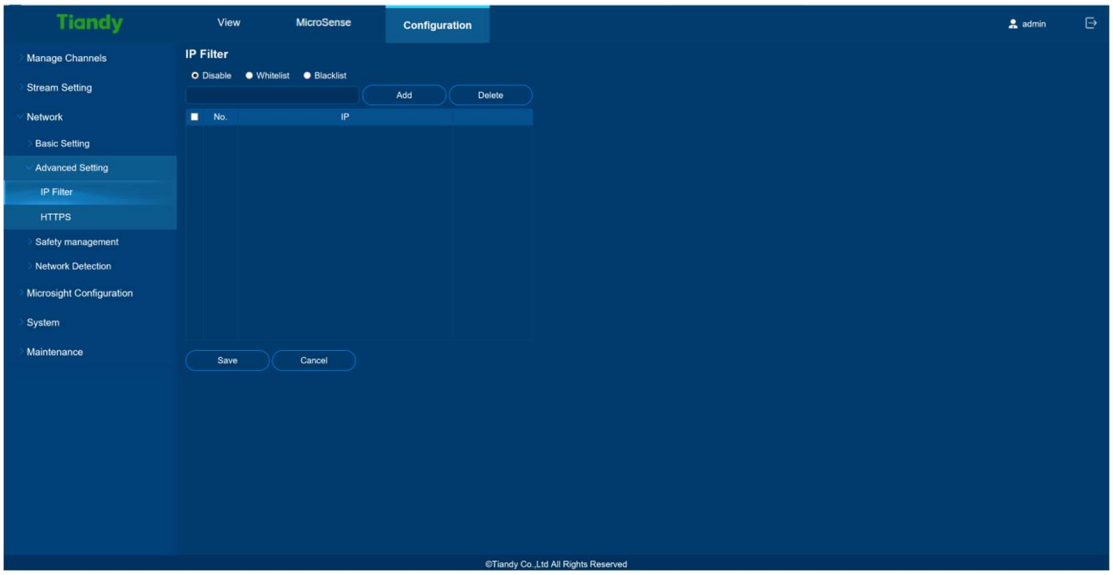
[Save]: Save the current settings.

[Reset]: Restore the last saved parameters.

4.6.3.2 Advanced Settings

4.6.3.2.1 Blacklist and whitelist

An IP firewall, also known as a blacklist/whitelist, provides users with greater flexibility in managing access permissions.



Black and White List Interface

[Unrestricted]: Select the [Unrestricted] radio button to remove blacklist and whitelist restrictions, allowing access from all IPs, not just those in the list.

[White List]: If you want to allow only a few trusted IP addresses to access the device, select the [White List] checkbox, enter each trusted IP address individually, click [Add], and then click [Save] to apply the white list. From this point onward, only IPs specified in the list will be permitted to log in; all login requests from other IPs will be denied, regardless of username or password correctness. You can specify up to 16 trusted IP addresses in the white list.

Note: When adding a whitelist, confirm whether to include the user's IP address.

Blacklist: To block specific IP addresses and prevent access to your device, select the [Blacklist] checkbox, enter each target IP address individually, click [Add], and then click [Save] to apply the blacklist. From this point onward, all login requests from any listed IP address will be denied, regardless of username or password correctness.

Note: When adding a blacklist, confirm whether the current user's IP address has been included.

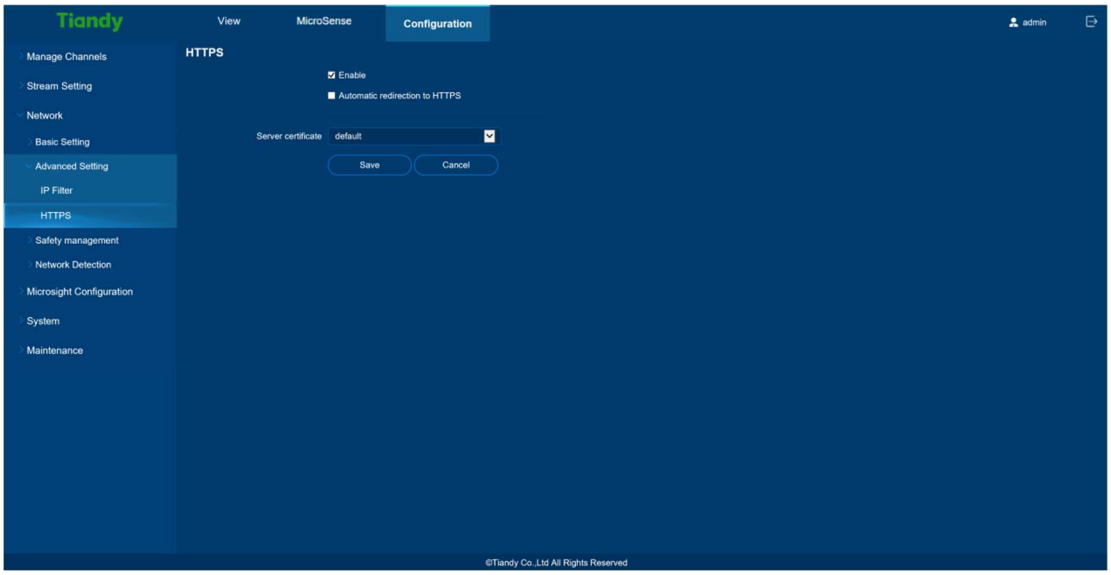
[Delete]: To remove specific IPs from the list, check the checkbox next to each IP and click [Delete]. Note: Do not delete all IPs when removing a whitelist, or devices may fail to log in.

Note: IP filtering only applies when a user logs in for the first time; it does not filter IPs of logged-in users. We strongly recommend restarting the device immediately after configuring the blacklist to block unauthorized IPs.

[Save]: Save the current settings.

[Reset]: Restore the last saved parameters.

4.6.3.2.2 HTTPS



https interface

You can import and install an HTTPS certificate as needed.

[Enable]: Enable HTTPS. When opening a webpage on the device, a pop-up will appear asking you to choose between switching to HTTPS or HTTP.

[Auto Switch to HTTPS]: Auto switches to HTTPS without user selection.

[Server Certificate]: Click the drop-down list and select the server certificate type to install. (Certificates can be managed under [Security Management> Certificate Management])

[Save]: Save current settings;

[Reset]: Restore the last saved parameters.

4.6.3.3 Safety Management

4.6.3.3.1 Certificate Management

Certificate Management Interface

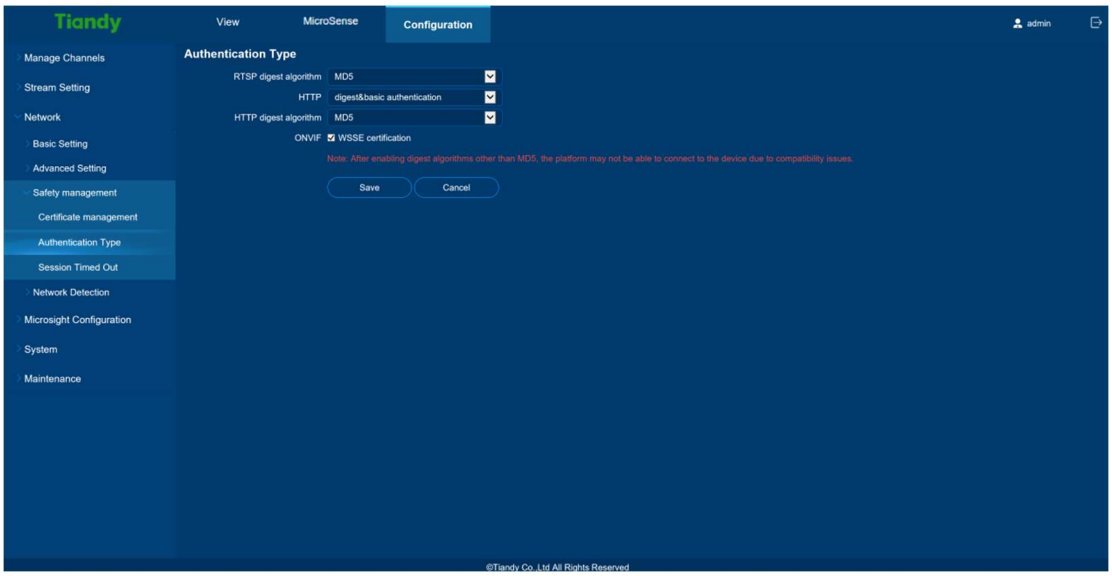
Certificate management manages all certificates on both the server and client sides. These certificates primarily provide a more secure connection for users logging into devices.

[Self-generated Certificate]: The device generates and uses a certificate independently.

Create Certificate Request and Import: The device requests a certificate from the CA authority and automatically imports it for use once obtained.

[Third-party Certificate Import]: Users can import their certificates for device use.

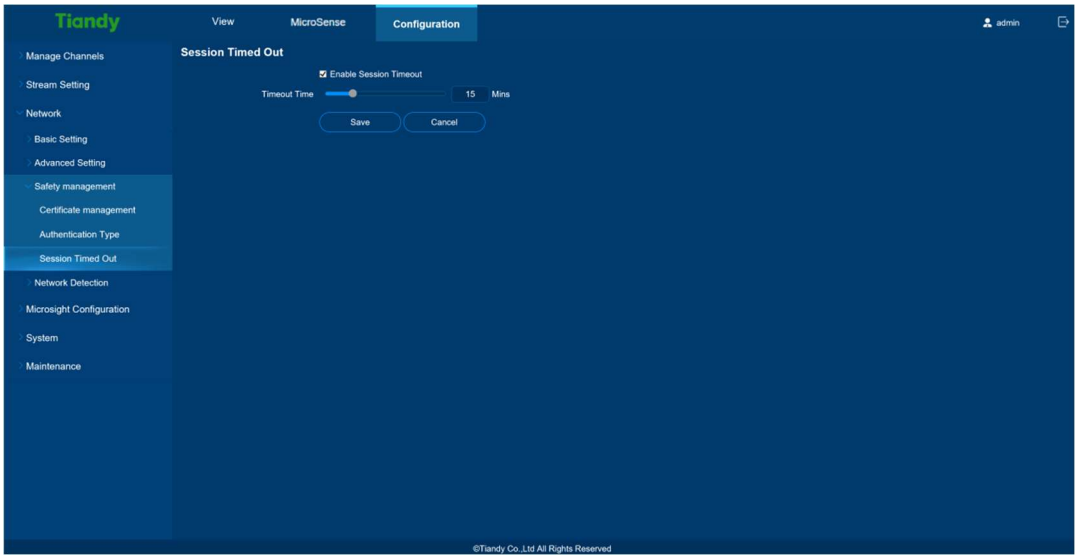
4.6.3.3.2 Types of Certification



International Server Interface

From the drop-down menu, you can select Digest & Basic Authentication or Digest Authentication.

4.6.3.3 Session Timed Out



Session Timeout Interface

The session timeout feature allows users to configure the current interface to automatically exit when no action is performed, enhancing device access security.

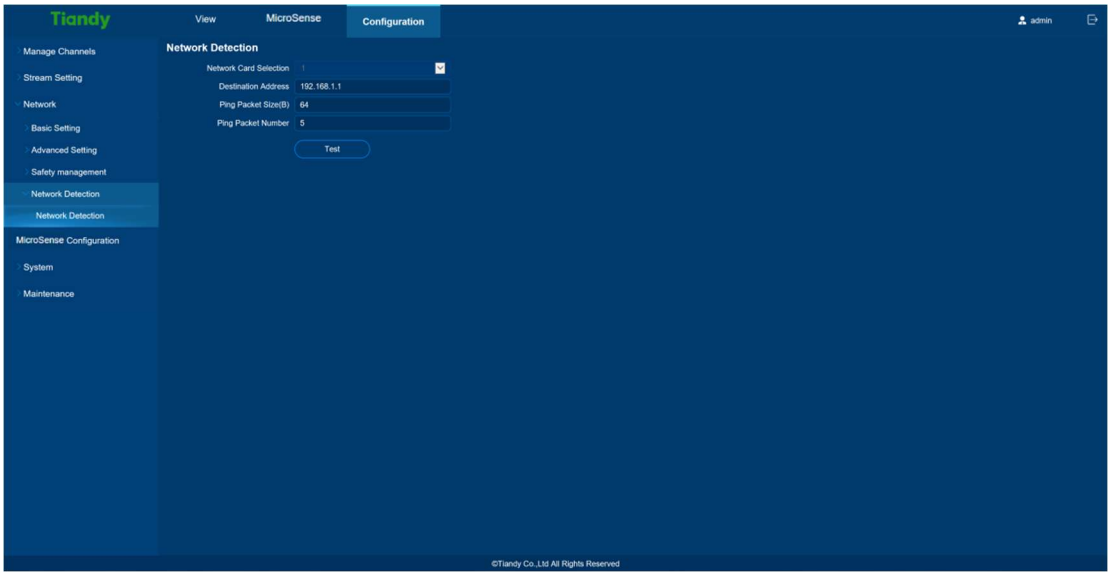
[Enable]: Provides a switch for this feature;

[Timeout]: Sets the maximum time for exiting the interface after timeout, ranging from 1 to 60 minutes.

4.6.3.4 Network Detection

4.6.3.4.1 Network Detection

Network monitoring is primarily used to check the current network status of devices.



Network Monitoring Interface

Network Monitoring Interface

Select the network card to test, enter the destination address, and click the [Test] button to check the network connection. If the network is stable, you will see the average latency and packet loss rate; if the network is unstable, a [Destination Address Unreachable] message will appear.

4.6.4 Fine Configuration

The Microsence Configuration Page is primarily used for configuring algorithms when adding channels.

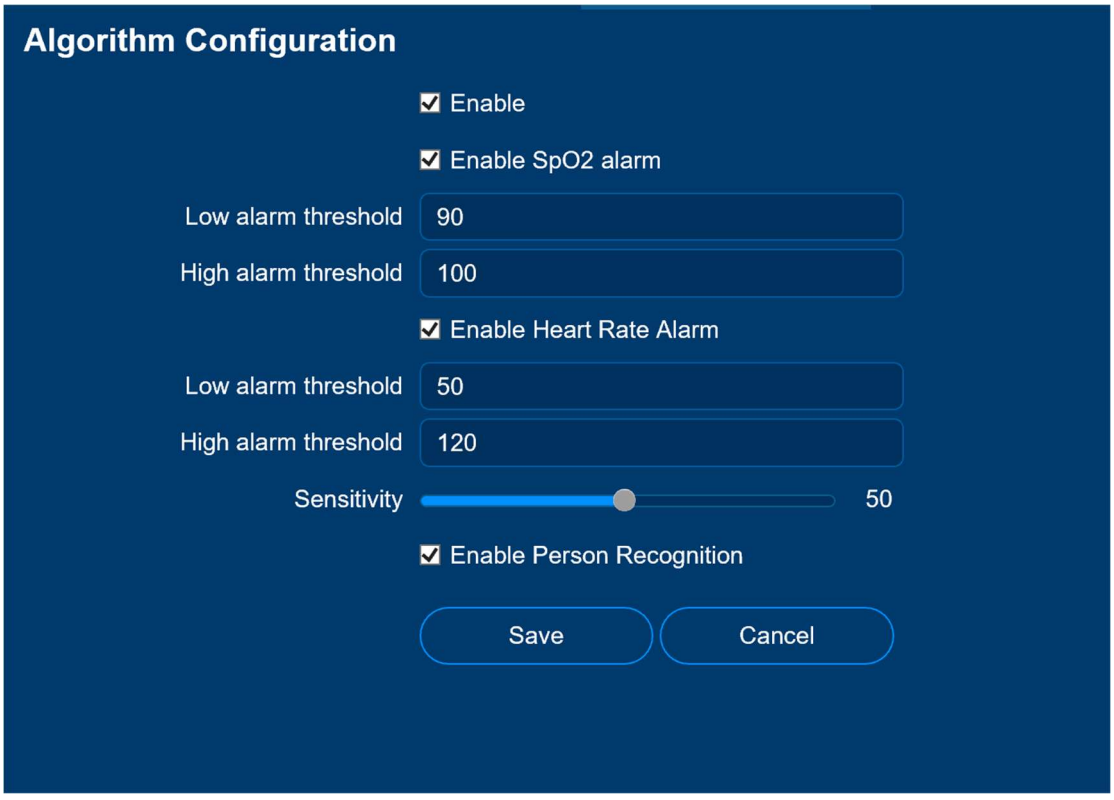
4.6.4.1 Algorithm Configuration

4.6.4.1.1 Algorithm Configuration

Scenario Requirements:

Face width> 400 pixels, face area> 5% of the image area; pitch, yaw, and rotation angles all less than 15° (i.e., frontal view with eye level); upper body clearly visible; image resolution> 4 million pixels

If the device installation does not meet the above requirements, it may affect the detection accuracy of this function.



Micro-analysis Algorithm Configuration Interface Micro-analysis Algorithm

Configuration Interface

The algorithm configuration is as follows:

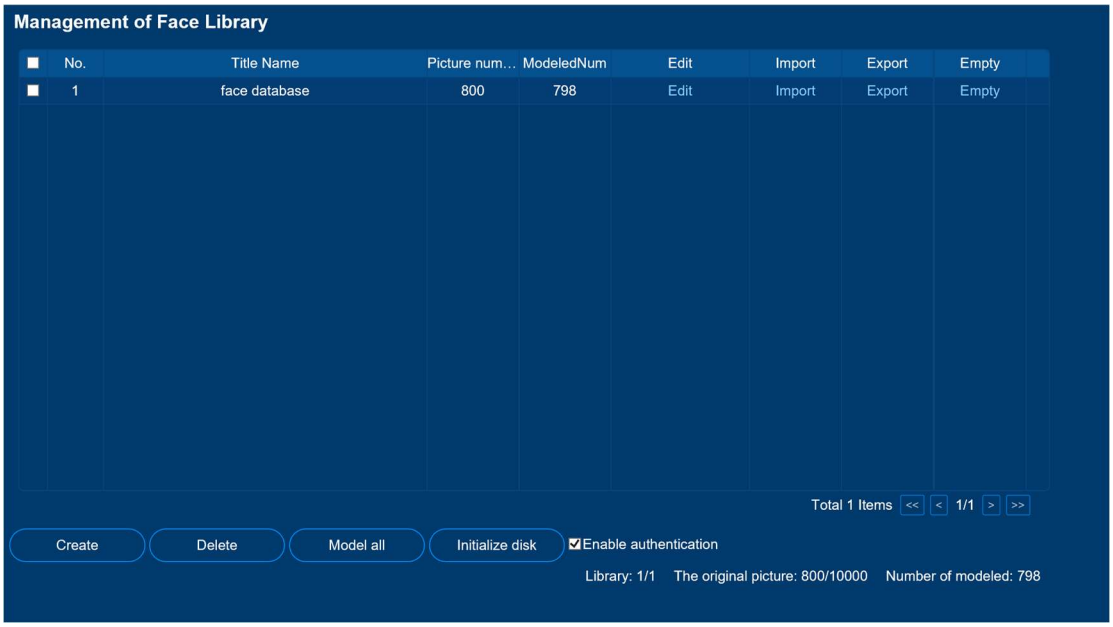
parameter	explain
start using	Algorithm activation button: If not checked, none of the algorithms will be active. When checked, the micro-expression algorithm activates, and other algorithms become active based on their respective activation buttons (this button serves as the master switch for all algorithms; if not selected, other buttons remain inactive).
Enable oxygen saturation alarm	Enable the blood oxygen alarm algorithm by checking the box.
Low Alarm Threshold	Minimum blood oxygen alarm threshold range: 90–100
High Alarm Threshold	Maximum blood oxygen alarm threshold range: 90–100
Enable heart rate alarm	Enable heart rate alarm by checking the box
Low Alarm Threshold	Minimum heart rate alarm threshold range: 50–120
High Alarm Threshold	Maximum heart rate alarm threshold range: 50–120
sensitivity	Sensitivity adjustment, range: 0–100
Enable Person Identification	Check this option to enable person recognition and compare with uploaded facial database images
preserve	Save changes to this page
resetting	The changes were not saved. Click Reset to restore the value to the last saved data

4.6.4.2 Face Database

4.6.4.2.1 Facial Database Management

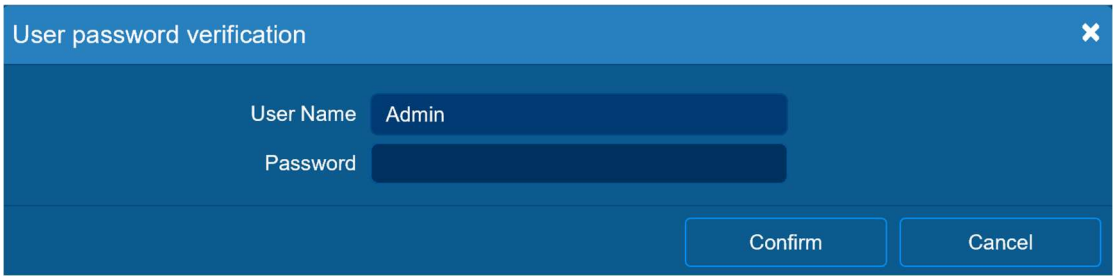
The face database manages face templates by group. You can query existing face data

and manage the template library using the [Add] and [Delete] buttons.

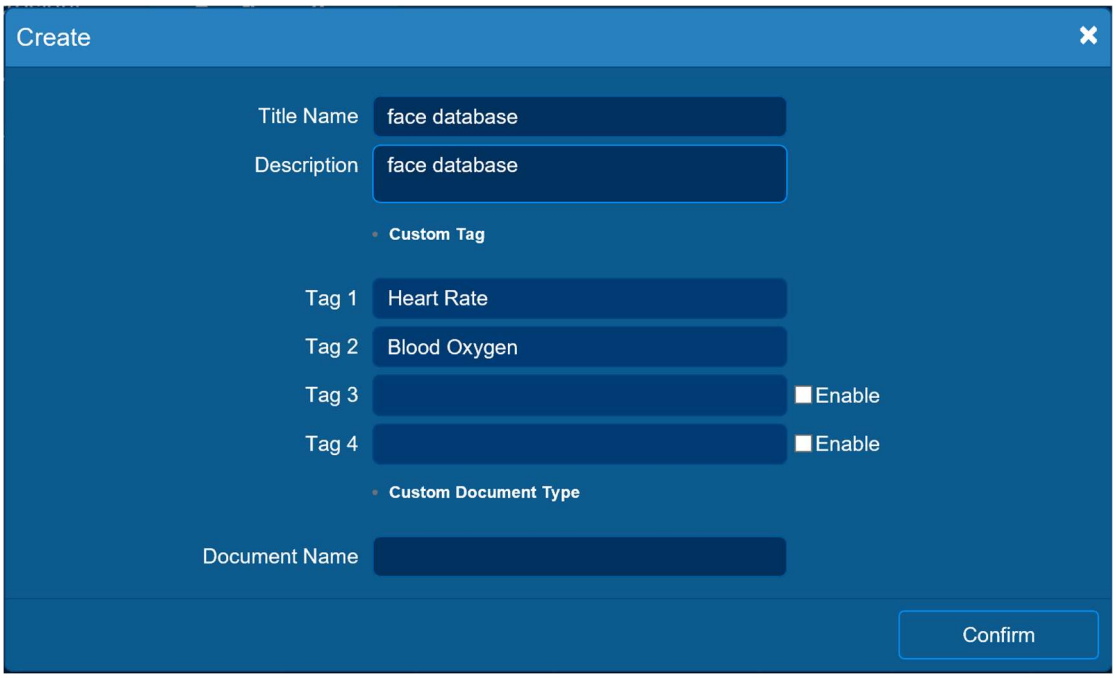


Face Recognition Interface

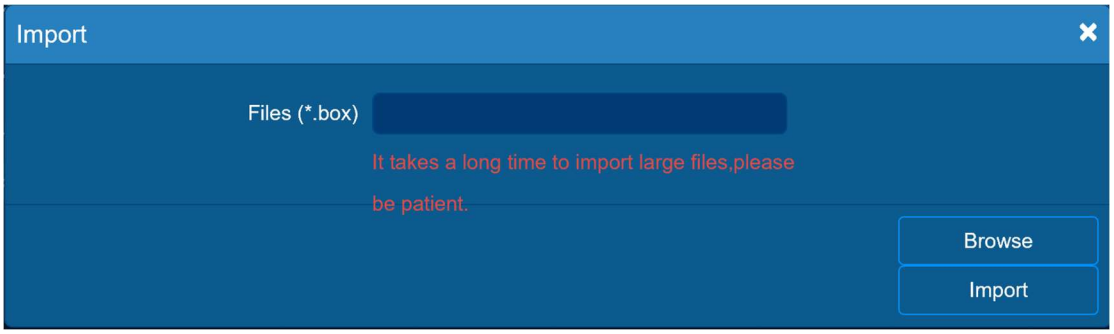
Check [Enable Authentication]. A prompt will appear during operation, as shown below. Enter the correct username and password to proceed. Only administrator users can modify the facial database.



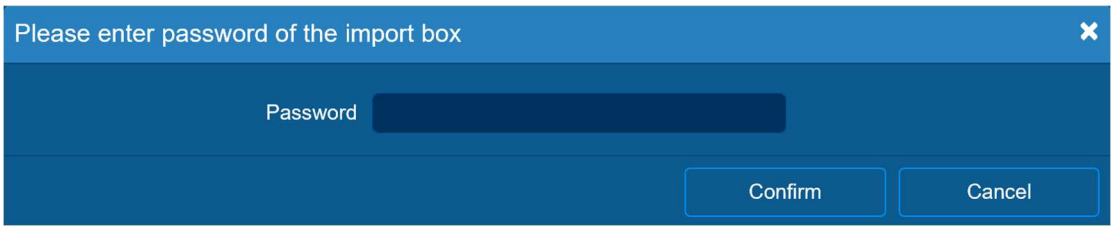
3. Click the [Edit] button to modify the name and description of the face database, as shown below.



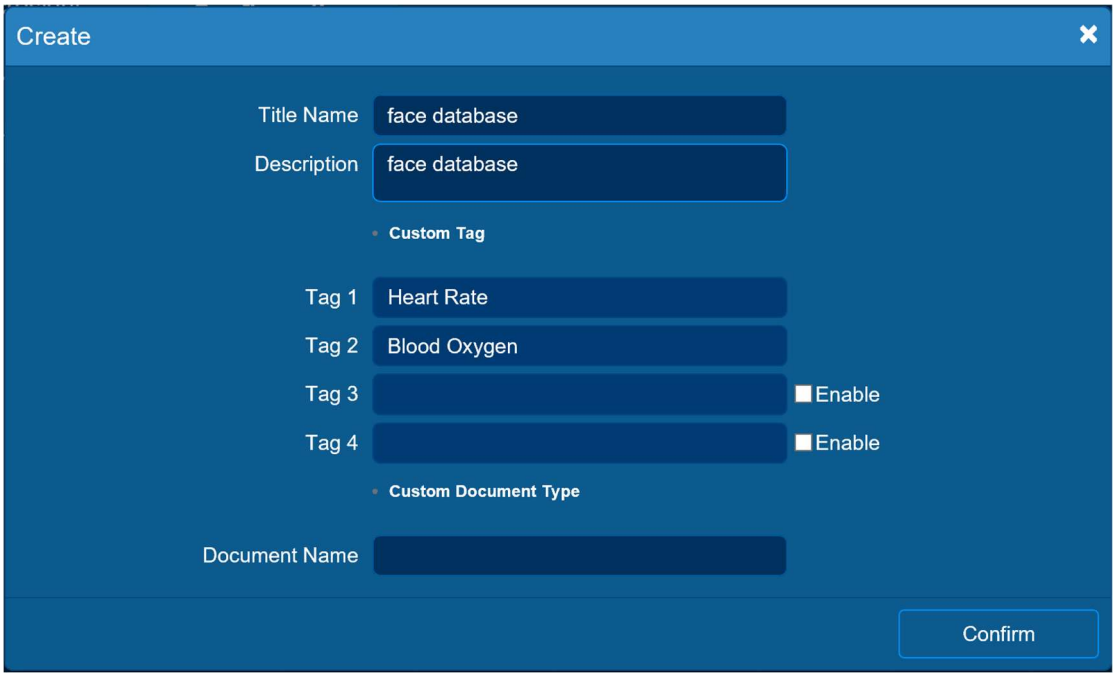
4. In the face database list, click the [Import] button to import a box file containing the face database. Note that the imported file must be in.box format; you need to enter the password for the box file during importation, as shown below.



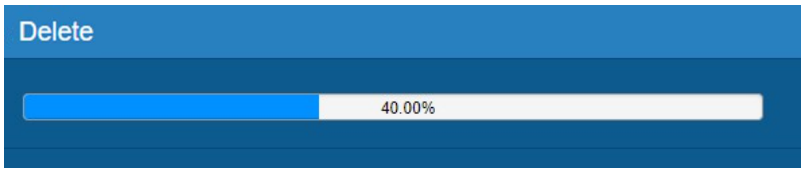
5. In the face database list, click the [Export] button to export a box file containing the face database. Set a password for the box file to import it to your computer disk, as shown below.



7. Click the [Create] button, enter the name and description of the new face database, and complete its addition as shown in the figure below.



8. Select the face database you want to delete, then click the [Delete] button to remove it, as shown below.



9. Click the [Model All] button to model the base maps for all libraries. The number of models can be viewed in the bottom-right corner, as shown below.



4.6.4.2.2 Management of Facial Background Image Libraries

pay attention to ：

Image Requirements:

(1) The image size must be no less than 100×100 and no more than 1080×1920;

(2) The image must be in color and in formats such as jpg or png;

(3) The interpupillary distance should be ≥60 pixels, preferably ≥90 pixels;

(4) The face must be intact with clear, unobstructed images; for example, no mask or sunglasses should be worn, and eyeglass frames must not cover the eyes.

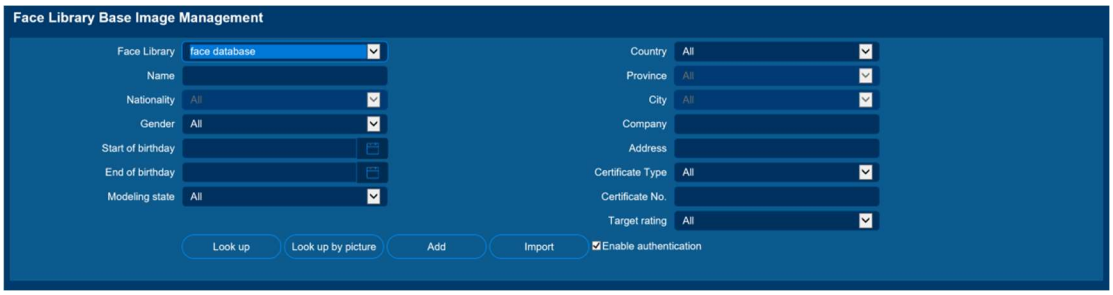
(5) The facial expression in the image should be neutral or smiling; exaggerated expressions are not recommended.

(6) The horizontal rotation angle, pitch angle, and tilt angle of the face are all within

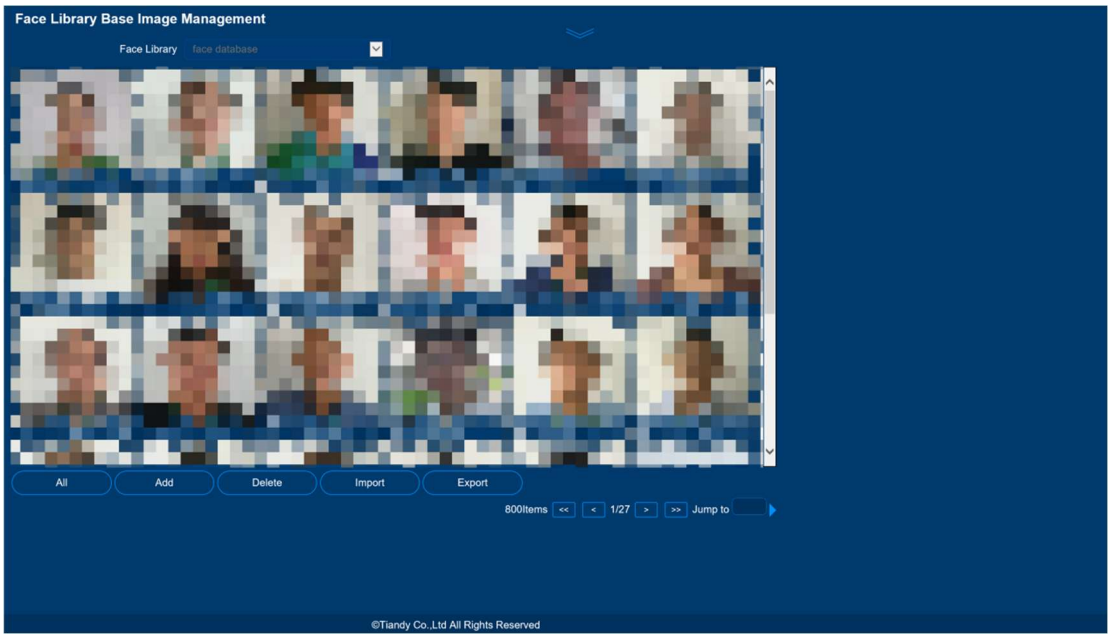
±10 degrees.

Face templates serve as the foundation for facial recognition algorithms. You can search, find by image, or add face templates, and also import them in bulk.

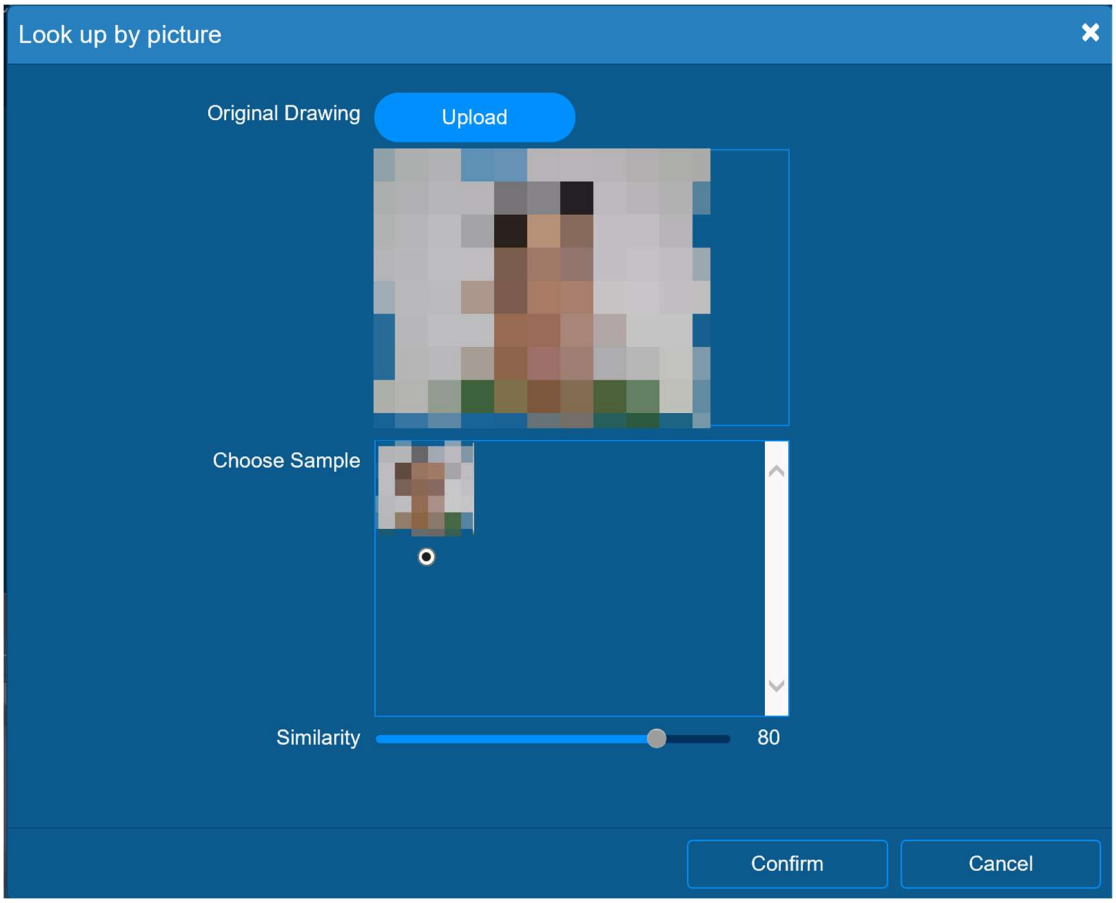
1. Go to [Configuration-> Deep Analysis-> Face Database], and select the Face Background Image Library Management tab as shown below.



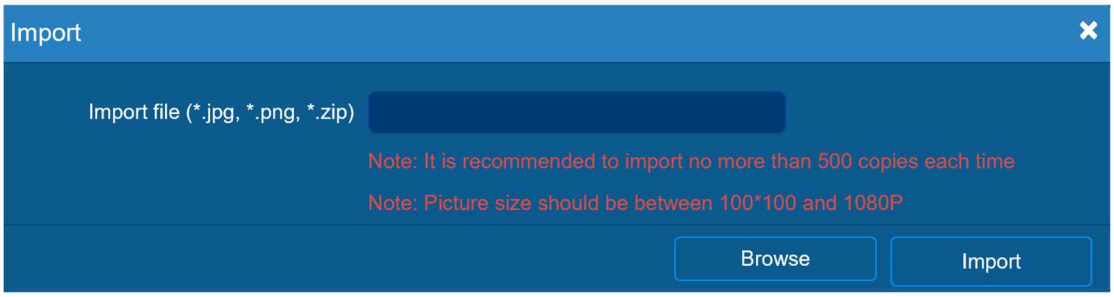
2. [Search Method]: First set your search criteria, then click the [Find] button. Click to display or hide search criteria. Only after searching the background image can you delete, export, or copy the current face library background image to another face library, as shown in the figure below.



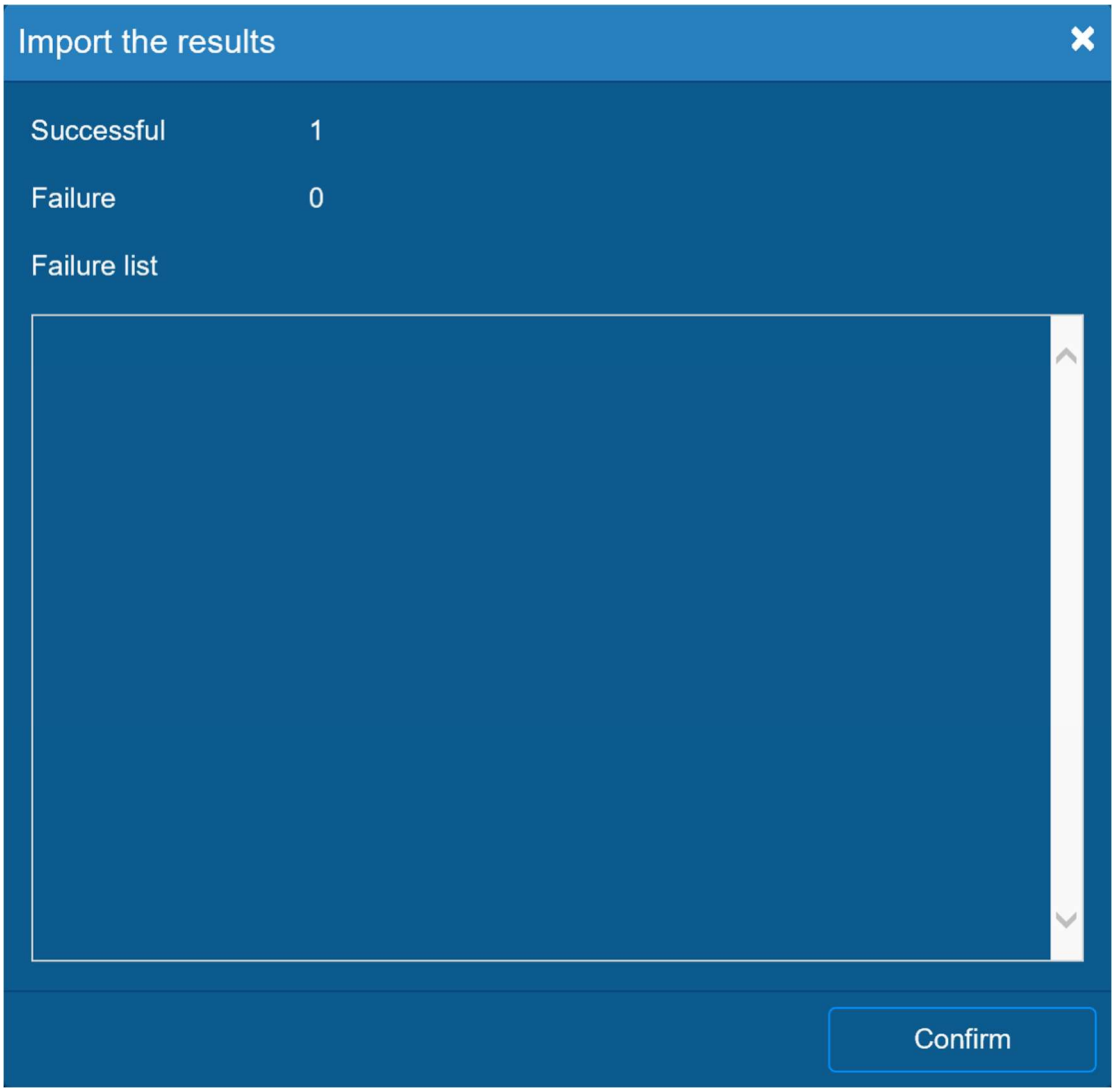
4. Click the [Find by Image] button to select an image from your USB drive or computer disk, then search the face database for the corresponding background image as shown below.



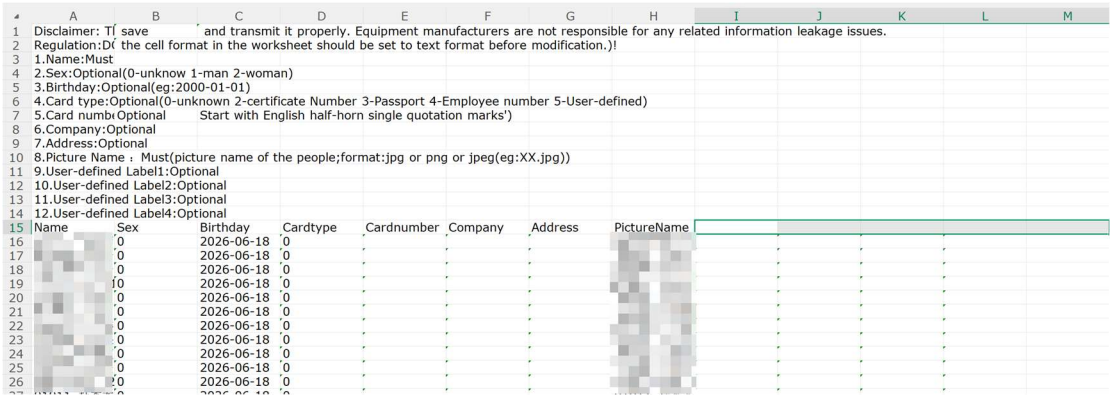
4. Click the [Import] button to select images from a USB drive or local storage and add them to the face database. When selecting a folder, you can include all eligible images within the folder, as shown below.



After importing is complete, a prompt box will appear as shown below.



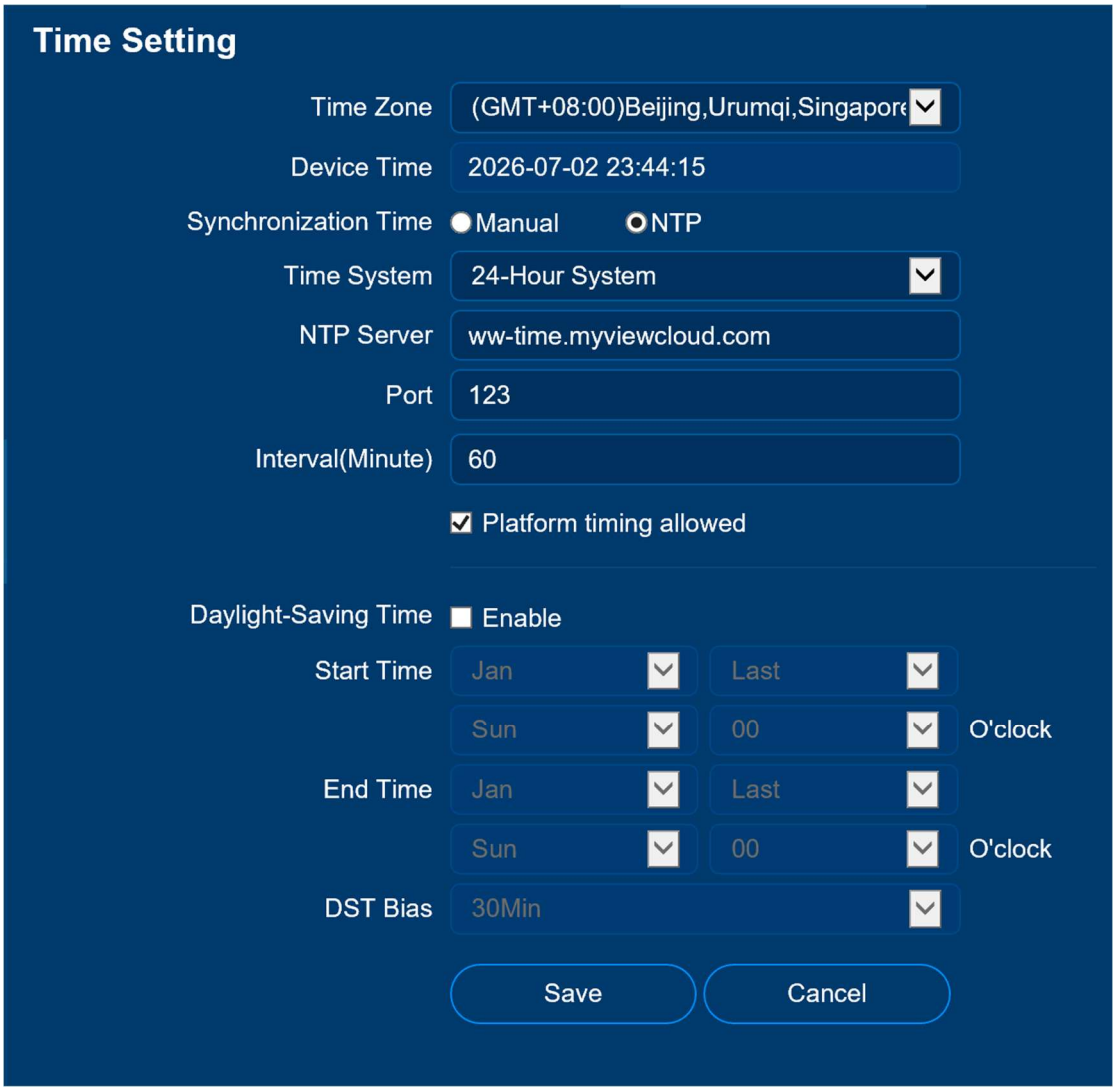
5. After completing the query, click the [Export] button to export the image and its details as shown below.



4.6.5 System Settings

4.6.5.1 System Settings

4.6.5.1.1 Time Settings



Time Settings Interface

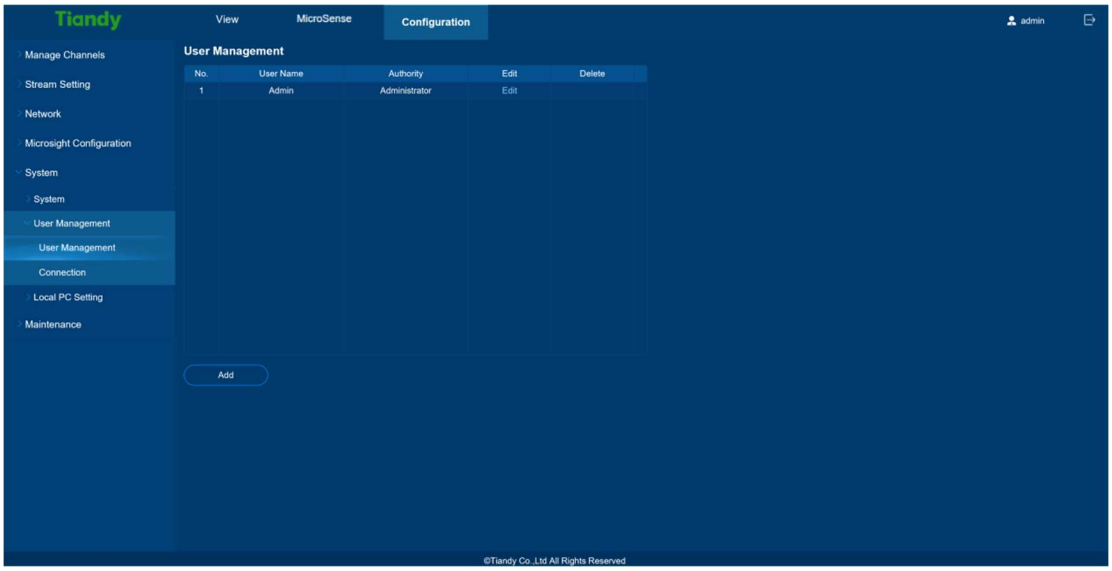
Parameter details are shown in the table below:

parameter	explain
time zone	Users can set the time zone of their device as needed.
Device Time	Show the device's current time

Time Format	Supports both 12-hour and 24-hour formats, displaying time according to the selected format.
Local Time	Displays the current system time and allows you to modify it. Click the "Sync" button to synchronize the time with all device locations.
NTP server	Configure a network time synchronization server. This feature requires the device to be connected to the external network.
port	Configure the port number for the NTP server.
time interval	Configure the time synchronization interval for the NTP server.

4.6.5.2 User Management

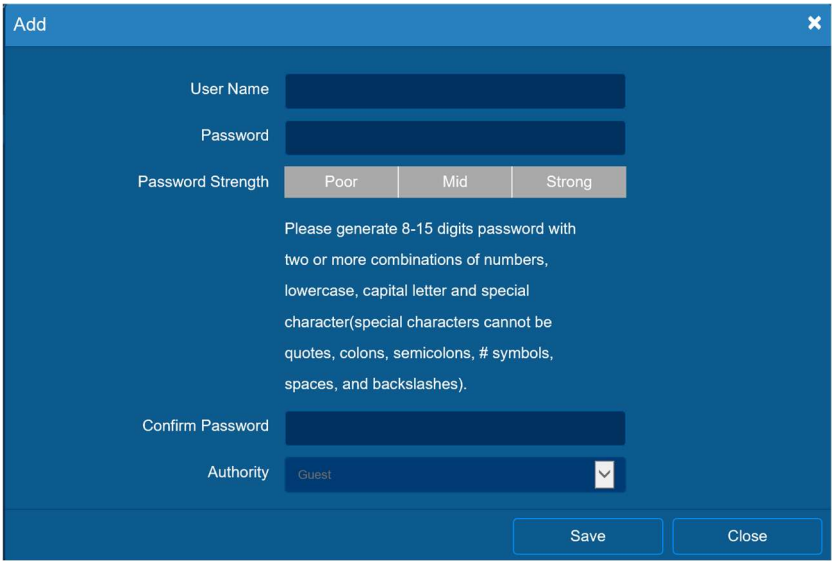
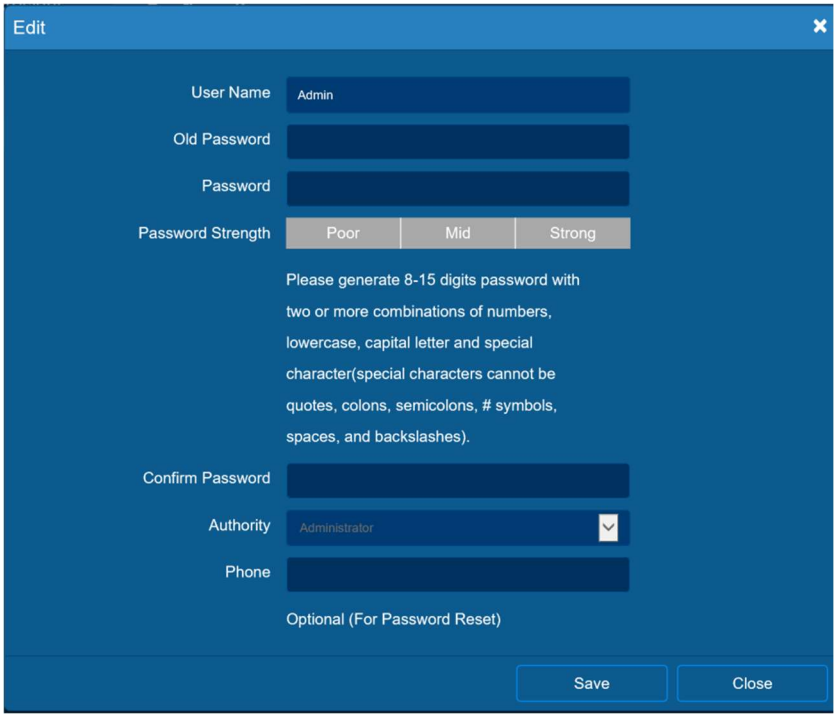
4.6.5.2.1 User Management



User Management Interface

Parameter details are shown in the table below:

parameter	explain
add	Only the administrator account can add new users. You can set a new user's username, password, and permissions as shown

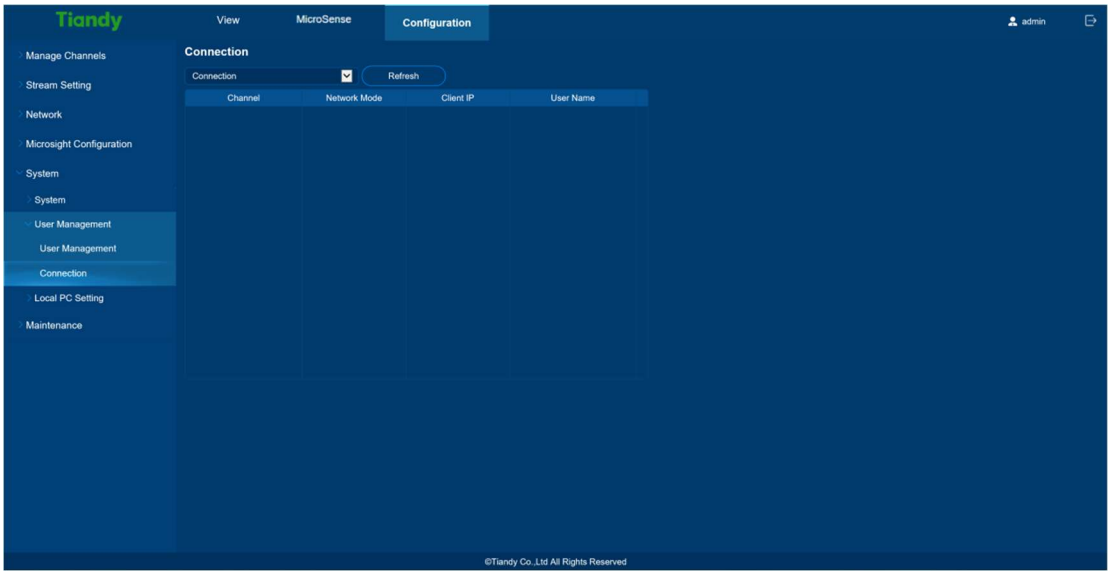
	below:  Description: Supports both "Regular User" and "Administrator" permissions. ● Regular User: Watch Video ● Administrator: View Videos + Device Control + Parameter Settings + User Management
edit	You can change the user's password as shown below: 
delete	You can delete the selected account.

pay attention to ：

Once 1 and user permissions are set, they cannot be modified again. Once 1 and user permissions are set, they cannot be modified again.

2: Add up to 32 users. 2: Add up to 32 users.

4.6.5.2.2 Connection Information



Connection Information Interface

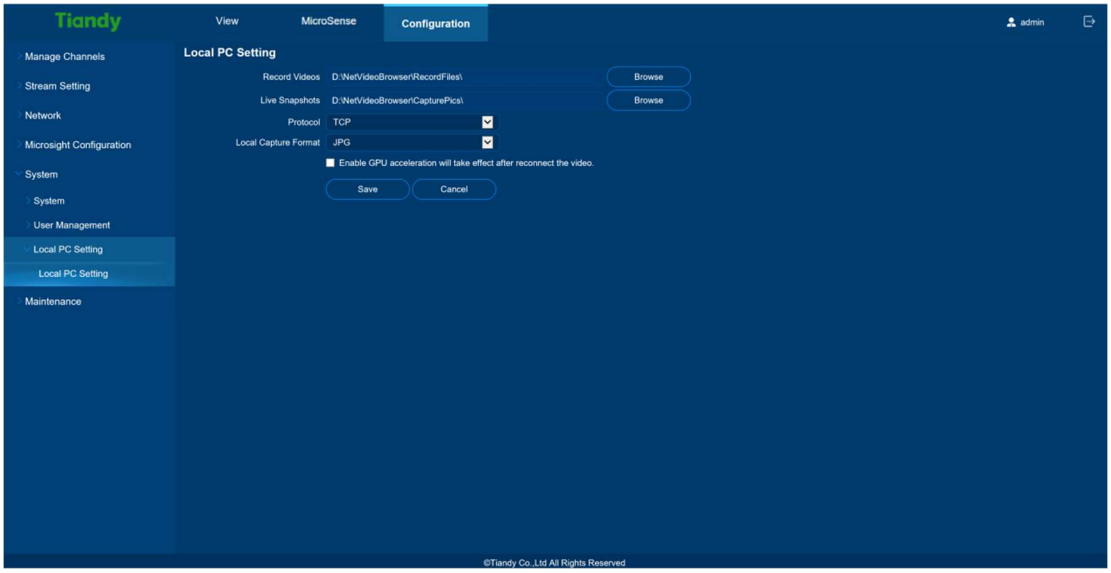
Parameter details are shown in the table below:

parameter	explain
linkage information	The connection information interface displays a detailed list of devices logged in, including service type, network mode, client IP, and username, as shown below. Click the [Refresh] button to update the connection information.
login information	On the login information page, you will see the client's IP address and the username used for login. As shown in the figure below, click the [Refresh] button to update the login information.

4.6.5.3 Local Settings

4.6.5.3.1 Local Settings

On the Local Settings page, configure the device's local storage path and format as shown below:



Local Settings Interface

1. Set the save paths for preview screenshots and video files.
2. Set the protocol type for storage and the local capture format.
3. Click the [Save] button to save the current settings. Click the [Reset] button to restore the last saved parameters.

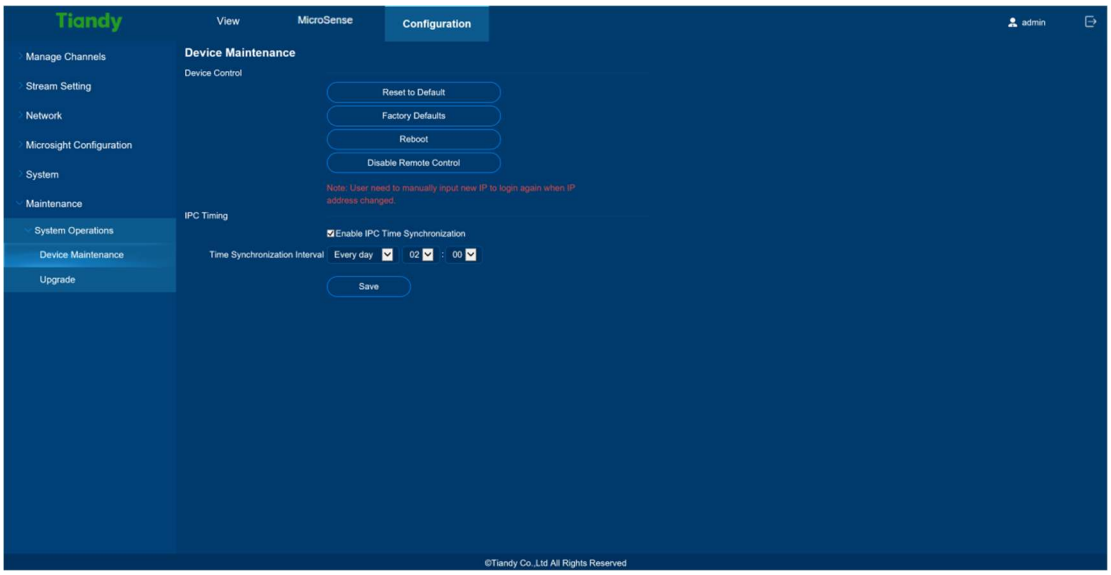
pay attention to ：

This setting only works in IE browser; path information will not display in other browsers.

4.6.6 System Maintenance

4.6.6.1 System Operation and Maintenance

4.6.6.1.1 Equipment Maintenance



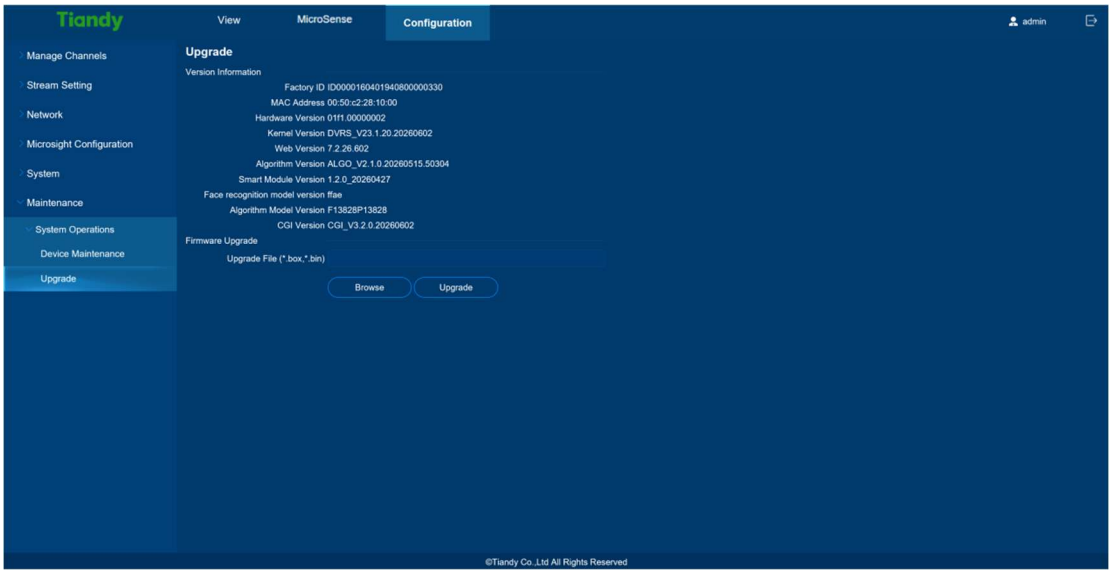
Device Maintenance Interface

Parameter details are shown in the table below:

parameter	explain
DC	Including restoring defaults, restarting the device, shutting down the device, and enabling remote services.
Parameter Import and Export	Supports importing and exporting parameter information for storage, alarms, previews, intelligent analysis, and system settings. If the IP address changes, manually enter the new IP address and log in again.
Log Level	Supports log statistics for system, warning, alarm, and operation types.
Automatic Maintenance	Set the device restart time, which can be configured in years, months, weeks, or days. The device will restart at this time.
Enable IPC Time synchronization	When enabled, the system will synchronize time with connected cameras based on the configured time synchronization cycle.
School Day Cycle	Select the time period: daily, weekly, monthly, annually, or off. Change hours and minutes.

4.6.6.1.2 System Upgrade

The system upgrade interface displays device version information and allows you to perform version upgrades, as shown below:



System Upgrade Interface

Parameter details are shown in the table below:

parameter	explain
Version Information	Show basic information about the device before display and copy/paste it.
Firmware Update	Supports online upgrades for the current device.