6.2.2 Set Defocus Detection

The blurred image caused by lens defocus can be detected. If it occurs, the device can take linkage actions.

Steps

1. Go to **Configuration → Event → Smart Event → Defocus Detection** .
2. Check **Enable**.
3. Set **Sensitivity**. The higher the value is, the more easily the defocus image can trigger the alarm. You can adjust the value according to the actual environment.
4. For the linkage method settings, refer to ***Linkage Method Settings*** .
5. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with models.

6.2.3 Detect Scene Change

Scene change detection function detects the change of surveillance scene. Some certain actions can be taken when the alarm is triggered.

Steps

1. Go to **Configuration → Event → Smart Event → Scene Change Detection** .
2. Click **Enable**.
3. Set the **Sensitivity**. The higher the value is, the more easily the change of scene can be detected. But the detection accuracy is reduced.
4. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
5. Click **Save**.

Note

The function varies according to different models.

6.2.4 Set Face Detection

It helps to detect the face in the detection region. If a face is detected, the device triggers the linkage actions.

Steps

1. Go to **Configuration → Event → Smart Event → Face Detection** .
2. Check **Enable Face Detection**.
3. **Optional:** Highlight to display the face in the image.
   1) Check **Enable Dynamic Analysis For Face Detection**.

2) Go to **Configuration → Local** , set **Rules** to **Enable**.

4. Set **Sensitivity**. The lower the sensitivity is, the profile of the face or unclear face is more difficult to detect.
5. Set the arming schedule and linkage methods. For the information about arming schedule settings, see ***Set Arming Schedule*** . For the information about linkage methods, see ***Linkage Method Settings*** .
6. Click **Save**.

6.2.5 Set Video Loss

This function can detect the video signal loss in time and trigger the linkage action.

Steps

1. Go to **Configuration → Event → Basic Event → Video Loss** .
2. Check **Enable**.
3. Refer to ***Set Arming Schedule*** for setting scheduled time. Refer to ***Linkage Method Settings*** for setting linkage method.
4. Click **Save**.

6.2.6 Set Intrusion Detection

It is used to detect objects entering and loitering in a pre-defined virtual region. If it occurs, the device can take linkage actions.

Steps

1. Go to **Configuration → Event → Smart Event → Intrusion Detection** .
2. Check **Enable**.
3. Select a **Region**. For the detection region settings, refer to ***Draw Area*** .
4. Set rules.

Sensitivity	Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the pre-defined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.
Threshold	Threshold stands for the threshold for the time of the object loitering in the region. If the time that one object stays exceeds the threshold, the alarm is triggered. The larger the value of the threshold is, the longer the alarm triggering time is.
Detection Target	Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including the human and vehicle.

Target Validity If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.

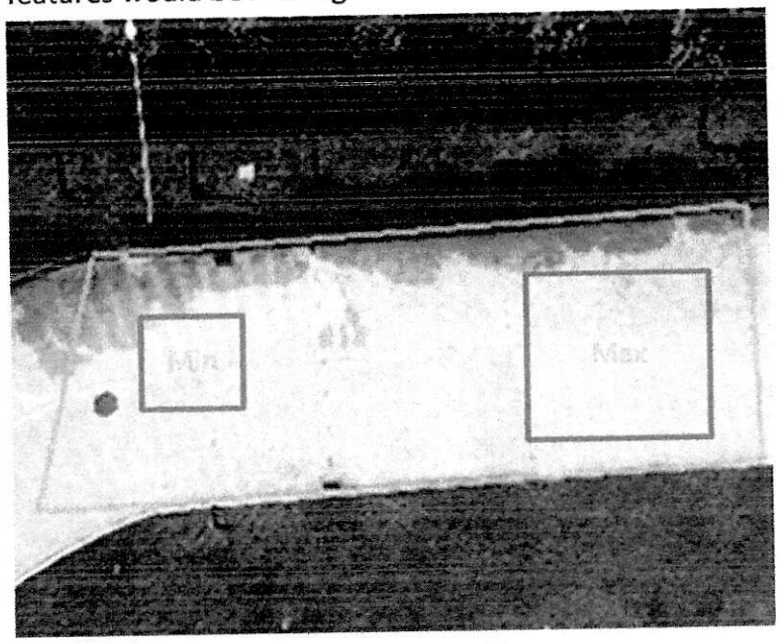


Figure 6-3 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
7. Click **Save**.

6.2.7 Set Line Crossing Detection

It is used to detect objects crossing a pre-defined virtual line. If it occurs, the device can take linkage actions.

Steps

1. Go to **Configuration → Event → Smart Event → Line Crossing Detection** .
2. Check **Enable**.
3. Select one **Line** and set the size filter. For the size filter settings, refer to ***Set Size Filter*** .
4. Click **Draw Area** and a line with an arrow appears in the live video. Drag the line to the location on the live video as desired.
5. Set rules.

Direction It stands for the direction from which the object goes across the line.

A<->B: The object going across the line from both directions can be detected and alarms are triggered.

	A->B: Only the object crossing the configured line from the A side to the B side can be detected. B->A: Only the object crossing the configured line from the B side to the A side can be detected.
Sensitivity	It stands for the percentage of the body part of an acceptable target that goes across the pre-defined line. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the pre-defined line. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.
Detection Target	Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including the human and vehicle.
Target Validity	If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.

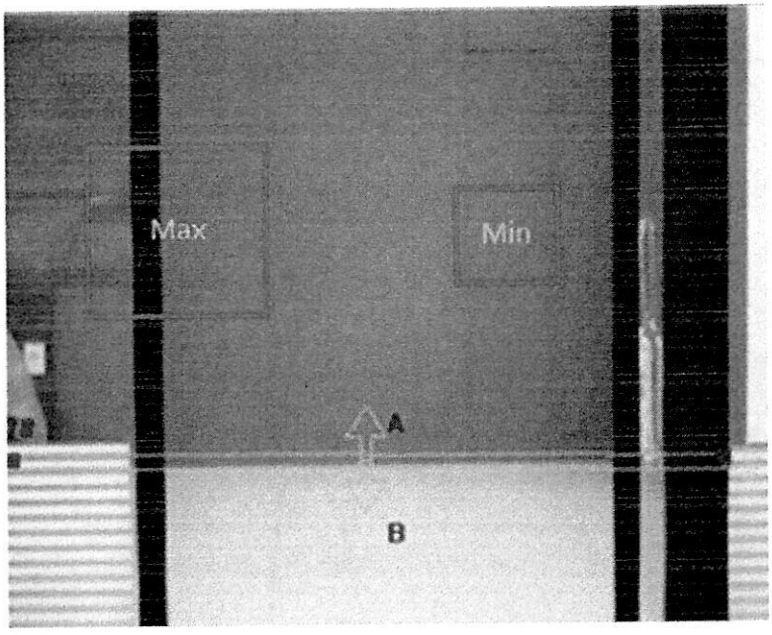


Figure 6-4 Set Rule

6. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
7. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
8. Click **Save**.

6.2.8 Set Region Entrance Detection

It is used to detect objects entering a pre-defined virtual region from the outside place. If it occurs, the device can take linkage actions.

Steps

1. Go to **Configuration → Event → Smart Event → Region Entrance Detection** .
2. Check **Enable**.
3. Select one **Region**. For the region settings, refer to ***Draw Area*** .
4. Set the detection target, sensitivity and the target validity.

Sensitivity	It stands for the percentage of the body part of an acceptable target that goes across the pre-defined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the pre-defined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.
Detection Target	Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including the human and vehicle.
Target Validity	If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.

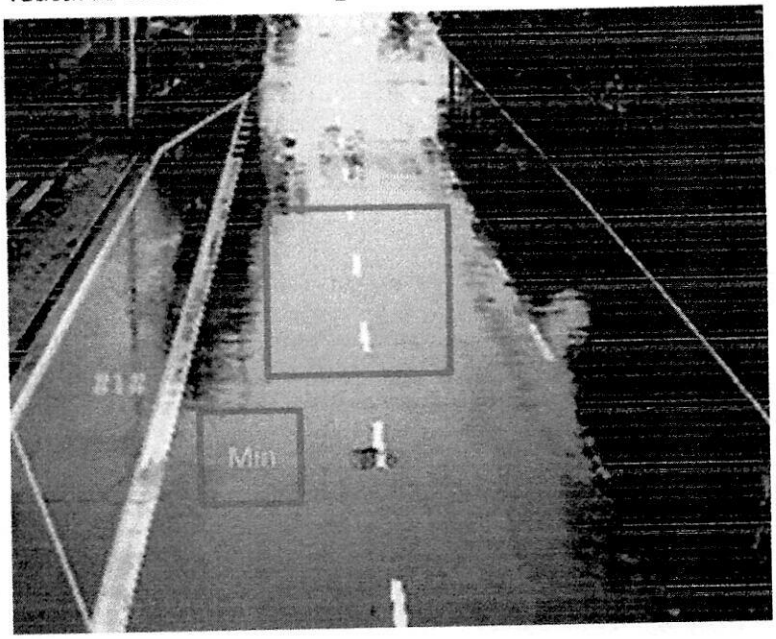


Figure 6-5 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
7. Click **Save**.

6.2.9 Set Region Exiting Detection

It is used to detect objects exiting from a pre-defined virtual region. If it occurs, the device can take linkage actions.

Steps

1. Go to **Configuration → Event → Smart Event → Region Exiting Detection**
2. Check **Enable**.
3. Select one **Region**. For the detection region settings, refer to ***Draw Area*** .
4. Set the detection target, sensitivity and the target validity.

Sensitivity	It stands for the percentage of the body part of an acceptable target that goes across the pre-defined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the pre-defined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.
Detection Target	Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including the human and vehicle.
Target Validity	If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.



Figure 6-6 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .

7. Click **Save**.

6.2.10 Set Unattended Baggage Detection

It is used to detect the objects left over in the pre-defined region. Linkage methods can be triggered after the object is left and stays in the region for a set time period.

Steps

1. Go to **Configuration → Event → Smart Event → Unattended Baggage Detection**.
2. Check **Enable**.
3. Select one **Region**. For the detection region settings, refer to ***Draw Area***.
4. Set rules.

Sensitivity Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that goes across the pre-defined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Threshold It stands for the time of the objects left in the region. Alarm is triggered after the object is left and stays in the region for the set time period.

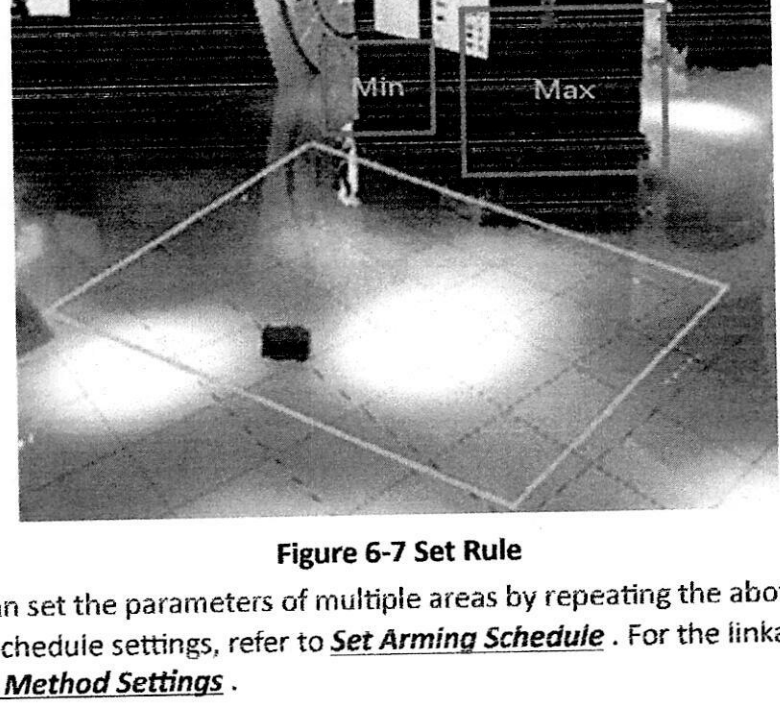


Figure 6-7 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to ***Set Arming Schedule***. For the linkage method settings, refer to ***Linkage Method Settings***.
7. Click **Save**.

6.2.11 Set Object Removal Detection

It detects whether the objects are removed from the pre-defined detection region, such as the exhibits on display. If it occurs, the device can take linkage actions and the staff can take measures to reduce property loss.

Steps

1. Go to **Configuration → Event → Smart Event → Object Removal Detection** .
2. Check **Enable**.
3. Select a **Region**. For the region settings, see ***Draw Area*** .
4. Set the rule.

Sensitivity	It stands for the percentage of the body part of an acceptable target that leaves the pre-defined region. Sensitivity = 100 – S1/ST*100 S1 stands for the target body part that leaves the pre-defined region. ST stands for the complete target body. Example: If you set the value as 60, a target is possible to be counted as a removed object only when 40 percent body part of the target leaves the region.
Threshold	The threshold for the time of the objects removed from the region. If you set the value as 10, alarm is triggered after the object disappears from the region for 10s.

5. **Optional:** Repeat the above steps to set more regions.
6. For the arming schedule settings, see ***Set Arming Schedule*** . For the linkage method settings, see ***Linkage Method Settings*** .
7. Click **Save**.

Note

The function is only supported by certain models. The actual display varies with the models.

6.2.12 Draw Area

This section introduces the configuration of area.

Steps

1. Click **Draw Area**.
2. Click on the live view to draw the boundaries of the detection region, and right click to complete drawing.
3. Click **Save**.

Note

Click **Clear All** to clear all pre-defined areas.

6.2.13 Set Size Filter

This part introduces the setting of size filter. Only the target whose size is between the minimum value and maximum value is detected and triggers alarm.

Steps

1. Click **Max. Size**, and drag the mouse in the live view to draw the maximum target size.
2. Click **Min. Size**, and drag the mouse in the live view to draw the minimum target size.
3. Click **Save**.

Chapter 7 Network Settings

7.1 TCP/IP

TCP/IP settings must be properly configured before you operate the device over network. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting to each other.

Go to **Configuration → Network → Basic Settings → TCP/IP** for parameter settings.

NIC Type

Select a NIC (Network Interface Card) type according to your network condition.

IPv4

Two IPv4 modes are available.

DHCP

The device automatically gets the IPv4 parameters from the network if you check **DHCP**. The device IP address is changed after enabling the function. You can use SADP to get the device IP address.

Note

The network that the device is connected to should support DHCP (Dynamic Host Configuration Protocol).

Manual

You can set the device IPv4 parameters manually. Input **IPv4 Address**, **IPv4 Subnet Mask**, and **IPv4 Default Gateway**, and click **Test** to see if the IP address is available.

IPv6

Three IPv6 modes are available.

Route Advertisement

The IPv6 address is generated by combining the route advertisement and the device Mac address.

Note

Route advertisement mode requires the support from the router that the device is connected to.

DHCP

The IPv6 address is assigned by the server, router, or gateway.

Manual

Input **IPv6 Address, IPv6 Subnet, IPv6 Default Gateway**. Consult the network administrator for required information.

MTU

It stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.

The valid value range of MTU is 1280 to 1500.

DNS

It stands for domain name server. It is required if you need to visit the device with domain name. And it is also required for some applications (e.g., sending email). Set **Preferred DNS Server** and **Alternate DNS server** properly if needed.

Dynamic Domain Name

Check **Enable Dynamic Domain Name** and input **Register Domain Name**. The device is registered under the register domain name for easier management within the local area network.

Note

DHCP should be enabled for the dynamic domain name to take effect.

7.1.1 Multicast

Multicast is a group communication where data transmission is addressed to a group of destination devices simultaneously. After setting multicast, you can send the source data efficiently to multiple receivers.

Go to **Configuration → Network → Basic Settings → Multicast** for the multicast settings.

IP Address

It stands for the address of multicast host.

Stream Type

The stream type of the multicast source.

Video Port

The video port of the selected stream.

Audio Port

The audio port of the selected stream.

FEC Port

The FEC port of the selected stream.

FEC Ratio

The ratio of forward error correction.

7.1.2 Multicast Discovery

Check the **Enable Multicast Discovery**, and then the online network camera can be automatically detected by client software via private multicast protocol in the LAN.

7.2 SNMP

You can set the SNMP network management protocol to get the alarm event and exception messages in network transmission.

Before You Start

Before setting the SNMP, you should download the SNMP software and manage to receive the device information via SNMP port.

Steps

1. Go to the settings page: **Configuration → Network → Advanced Settings → SNMP** .
2. Check **Enable SNMPv1, Enable SNMP v2c** or **Enable SNMPv3**.

Note

The SNMP version you select should be the same as that of the SNMP software.
And you also need to use the different version according to the security level required. SNMP v1 is not secure and SNMP v2 requires password for access. And SNMP v3 provides encryption and if you use the third version, HTTPS protocol must be enabled.

3. Configure the SNMP settings.
4. Click **Save**.

7.3 Set SRTP

The Secure Real-time Transport Protocol (SRTP) is a Real-time Transport Protocol (RTP) internet protocol, intended to provide encryption, message authentication and integrity, and replay attack protection to the RTP data in both unicast and multicast applications.

Steps

1. Go to **Configuration → Network → Advanced Settings → SRTP** .
2. Select **Server Certificate**.
3. Select **Encrypted Algorithm**.
4. Click **Save**.

Note

- Only certain device models support this function.
- If the function is abnormal, check if the selected certificate is abnormal in certificate management.

7.4 Port Mapping

By setting port mapping, you can access devices through the specified port.

Before You Start

When the ports in the device are the same as those of other devices in the network, refer to ***Port*** to modify the device ports.

Steps

1. Go to **Configuration → Network → Basic Settings → NAT** .
2. Select the port mapping mode.

Auto Port Mapping	Refer to ***Set Auto Port Mapping*** for detailed information.
Manual Port Mapping	Refer to ***Set Manual Port Mapping*** for detailed information.

3. Click **Save**.

7.4.1 Set Auto Port Mapping

Steps

1. Check **Enable UPnP™**, and choose a friendly name for the camera, or you can use the default name.
2. Select the port mapping mode to **Auto**.
3. Click **Save**.

Note

UPnP™ function on the router should be enabled at the same time.

7.4.2 Set Manual Port Mapping

Steps

1. Check **Enable UPnP™**, and choose a friendly name for the device, or you can use the default name.
2. Select the port mapping mode to **Manual**, and set the external port to be the same as the internal port.
3. Click **Save**.

What to do next

Go to the router port mapping settings interface and set the port number and IP address to be the same as those on the device. For more information, refer to the router user manual.

7.4.3 Set Port Mapping on Router

The following settings are for a certain router. The settings vary depending on different models of routers.

Steps

1. Select the **WAN Connection Type**.
2. Set the **IP Address, Subnet Mask** and other network parameters of the router.
3. Go to **Forwarding → Virtual Severs** , and input the **Port Number** and **IP Address**.
4. Click **Save**.

Example

When the cameras are connected to the same router, you can configure the ports of a camera as 80, 8000, and 554 with IP address 192.168.1.23, and the ports of another camera as 81, 8001, 555, 8201 with IP 192.168.1.24.

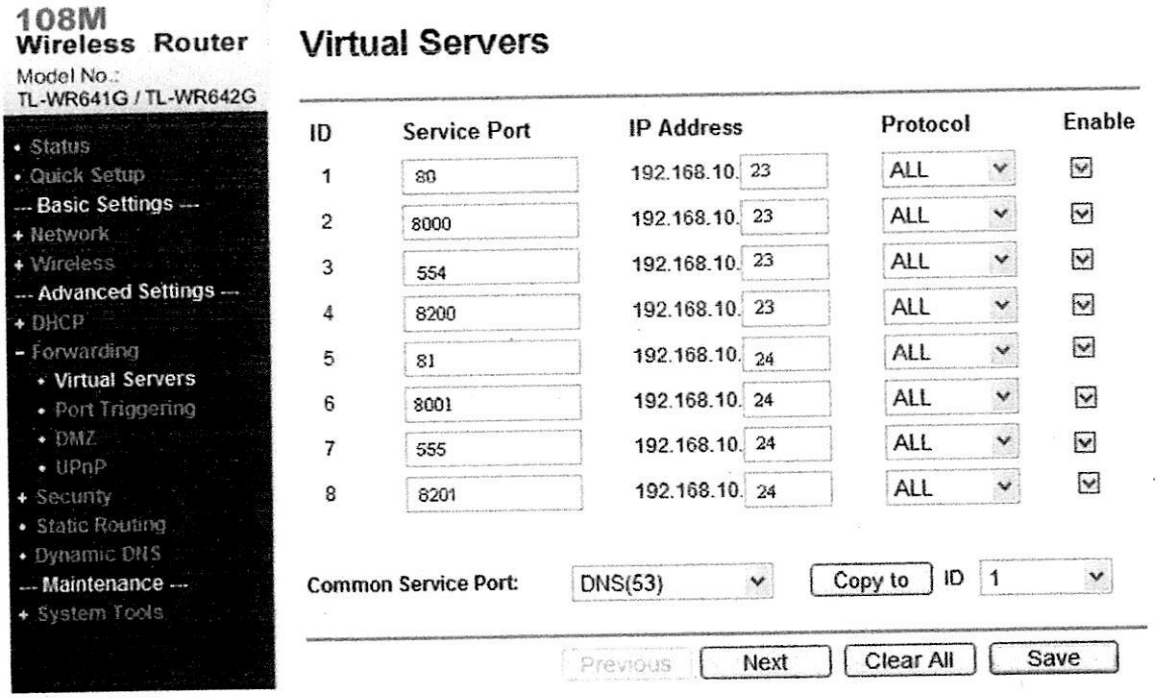


Figure 7-1 Port Mapping on Router

Note

The port of the network camera cannot conflict with other ports. For example, some web management port of the router is 80. Change the camera port if it is the same as the management port.

7.5 Port

The device port can be modified when the device cannot access the network due to port conflicts.

Caution

Do not modify the default port parameters at will, otherwise the device may be inaccessible.

Go to **Configuration → Network → Basic Settings → Port** for port settings.

HTTP Port

It refers to the port through which the browser accesses the device. For example, when the **HTTP Port** is modified to 81, you need to enter ***http://192.168.1.64:81*** in the browser for login.

HTTPS Port

It refers to the port through which the browser accesses the device with certificate. Certificate verification is required to ensure the secure access.

RTSP Port

It refers to the port of real-time streaming protocol.

SRTP Port

It refers to the port of secure real-time transport protocol.

Server Port

It refers to the port through which the client adds the device.

Enhanced SDK Service Port

It refers to the port through which the client adds the device. Certificate verification is required to ensure the secure access.

WebSocket Port

TCP-based full-duplex communication protocol port for plug-in free preview.

WebSockets Port

TCP-based full-duplex communication protocol port for plug-in free preview. Certificate verification is required to ensure the secure access.

Note

- Enhanced SDK Service Port, WebSocket Port, and WebSockets Port are only supported by certain models.
- For device models that support that function, go to **Configuration → Network → Advanced Settings → Network Service** to enable it.

7.6 Access to Device via Domain Name

You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name.

Before You Start

Registration on the DDNS server is required before configuring the DDNS settings of the device.

Steps

1. Refer to ***TCP/IP*** to set DNS parameters.
2. Go to the DDNS settings page: **Configuration → Network → Basic Settings → DDNS** .
3. Check **Enable DDNS** and select **DDNS type**.

   DynDNS

   Dynamic DNS server is used for domain name resolution.

   NO-IP

   NO-IP server is used for domain name resolution.
4. Input the domain name information, and click **Save**.
5. Check the device ports and complete port mapping. Refer to ***Port*** to check the device port , and refer to ***Port Mapping*** for port mapping settings.
6. Access the device.

By Browsers	Enter the domain name in the browser address bar to access the device.
By Client Software	Add domain name to the client software. Refer to the client manual for specific adding methods.

7.7 Access to Device via PPPoE Dial Up Connection

This device supports the PPPoE auto dial-up function. The device gets a public IP address by ADSL dial-up after the device is connected to a modem. You need to configure the PPPoE parameters of the device.

Steps

1. Go to **Configuration → Network → Basic Settings → PPPoE** .
2. Check **Enable PPPoE**.
3. Set the PPPoE parameters.

   Dynamic IP

   After successful dial-up, the dynamic IP address of the WAN is displayed.

   User Name

   User name for dial-up network access.

   Password

   Password for dial-up network access.

Confirm

Input your dial-up password again.

4. Click **Save**.
5. Access the device.

By Browsers	Enter the WAN dynamic IP address in the browser address bar to access the device.
By Client Software	Add the WAN dynamic IP address to the client software. Refer to the client manual for details.

Note

The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the camera. To solve the inconvenience of the dynamic IP, you need to get a domain name from the DDNS provider (e.g. DynDns.com). Refer to ***Access to Device via Domain Name*** for detail information.

7.8 Wireless Dial

Data of audio, video and image can be transferred via 3G/4G wireless network.

Note

The function is only supported by certain device models.

7.8.1 Set Wireless Dial

The built-in wireless module offers dial-up access to the Internet for the device.

Before You Start

Get a SIM card, and activate 3G/4G services. Insert the SIM card to the corresponding slot.

Steps

1. Go to **Configuration → Network → Advanced Settings → Wireless Dial** .
2. Check to enable the function.
3. Click **Dial Parameters** to configure and save the parameters.
4. Click **Dial Plan**. See ***Set Arming Schedule*** for detailed information.
5. **Optional:** Set **Allowlist**. See ***Set Allowlist*** for detailed information.
6. Click **Dial Status**.

Click Refresh	Refresh the dial status.
Click Disconnect	Disconnect the 3G/4G wireless network.

When the **Dial Status** turns to **Connected**, it means a successful dial.

7. Access the device via the **IP Address** of the computer in the network.

- Input the IP address in the browser to access the device.
- Add the device in client application. Select **IP/Domain**, and input IP address and other parameters to access the device.

7.8.2 Set Allowlist

Add the mobile phone number of administrator to the allowlist in order to receive alarm message from the device.

Steps

1. Go to allowlist settings page: **Configuration → Advanced Configuration → Wireless Dial → Allowlist**.
2. Check **Enable SMS Alarm**.
3. Click + in the allowlist.
   1) Input the mobile phone number to receive alarm message.
   2) Check **Reboot via SMS**.
   3) Select the certain events, and the mobile phone can receive the alarm message when the event happens.
   4) Click **Save**.
   5) **Optional:** Repeat the steps above to set multiple recipients.

✎	Modify the allowlist parameters.
×	Delete the allowlist that already set.
Send Test SMS	Send a message to the mobile phone for test.

4. Click **Save**.

7.9 Wi-Fi

Connect the device to wireless network by setting Wi-Fi parameters.

Note

This function is only supported by certain device models.

7.9.1 Connect Device to Wi-Fi

Before You Start

Refer to the user manual of wireless router or AP to set SSID, key, and other parameters.

Steps

1. Go to TCP/IP settings page: **Configuration → Network → Basic Configuration → TCP/IP**.
2. Select **Wlan** to set the parameters. Refer to ***TCP/IP*** for detailed configuration.

Note

For stable use of Wi-Fi, it is not recommended to use DHCP.

3. Go to Wi-Fi settings page: **Configuration → Network → Advanced Configuration → Wi-Fi** .
4. Set and save the parameters.
   1) Click **Search**.
   2) Select a **SSID**, which should be the same as that of wireless router or AP.

      The parameters of the network is automatically shown in **Wi-Fi**.
   3) Select the **Network Mode** as **Manage**.
   4) Input the key to connect the wireless network. The key should be that of the wireless network connection you set on the router.

What to do next

Go to TCP/IP settings page: **Configuration → Network → Basic Configuration → TCP/IP** , and click **Wlan** to check the **IPv4 Address** and log in the device.

7.10 Set Network Service

You can control the ON/OFF status of certain protocol as desired.

Steps

Note

This function varies according to different models.

1. Go to **Configuration → Network → Advanced Settings → Network Service** .
2. Set network service.

   WebSocket & WebSockets

   WebSocket or WebSockets protocol should be enabled if you use Google Chrome 57 and its above version or Mozilla Firefox 52 and its above version to visit the device. Otherwise, live view, image capture, digital zoom, etc. cannot be used.

   If the device uses HTTP, enable WebSocket.

   If the device uses HTTPS, enable WebSockets.

   When you use WebSockets, select the **Server Certificate**.

   Note

   Complete certificate management before selecting server certificate. Refer to ***Certificate Management*** for detailed information.

   SDK Service & Enhanced SDK Service

   Check **Enable SDK Service** to add the device to the client software with SDK protocol.

Check **Enable Enhanced SDK Service** to add the device to the client software with SDK over TLS protocol.

When you use Enhanced SDK Service, select the **Server Certificate**.

Note

- Complete certificate management before selecting server certificate. Refer to ***Certificate Management*** for detailed information.
- When set up connection between the device and the client software, it is recommended to use Enhanced SDK Service and set the communication in Arming Mode to encrypt the data transmission. See the user manual of the client software for the arming mode settings.

TLS (Transport Layer Security)

The device offers TLS1.1 and TLS1.2. Enable one or more protocol versions according to your need.

Bonjour

Uncheck to disable the protocol.

3. Click **Save**.

7.11 Set Open Network Video Interface

If you need to access the device through Open Network Video Interface protocol, you can configure the user settings to enhance the network security.

Steps

1. Go to **Configuration → Network → Advanced Settings → Integration Protocol** .
2. Check **Enable Open Network Video Interface**.
3. Click **Add** to configure the Open Network Video Interface user.

Delete Delete the selected Open Network Video Interface user.

Modify Modify the selected Open Network Video Interface user.

4. Click **Save**.
5. **Optional:** Repeat the steps above to add more Open Network Video Interface users.

7.12 Set ISUP

When the device is registered on ISUP platform (formerly called Ehome), you can visit and manage the device, transmit data, and forward alarm information over public network.

Steps

1. Go to **Configuration → Network → Advanced Settings → Platform Access** .
2. Select **ISUP** as the platform access mode.
3. Select **Enable**.

4. Select a protocol version and input related parameters.
5. Click **Save**.

   Register status turns to **Online** when the function is correctly set.

7.13 Set Alarm Server

The device can send alarms to destination IP address or host name through HTTP, HTTPS, or ISUP protocol. The destination IP address or host name should support HTTP, HTTP, or ISUP data transmission.

Steps

1. Go to **Configuration → Network → Advanced Settings → Alarm Server** .
2. Enter **Destination IP or Host Name**, **URL**, and **Port**.
3. **Optional:** Check **Enable** to enable ANR.
4. Select **Protocol**.

   Note

   HTTP, HTTPS, and ISUP are selectable. It is recommended to use HTTPS, as it encrypts the data transmission during communication.
5. Click **Test** to check if the IP or host is available.
6. Click **Save**.

7.14 Access Camera via Hik-Connect

Hik-Connect is an application for mobile devices. Using the App, you can view live image, receive alarm notification and so on.

Before You Start

Connect the camera to network with network cables.

Steps

1. Get and install Hik-Connect application by the following ways.
   - Visit ***https://appstore.hikvision.com*** to download the application according to your mobile phone system.
   - Visit the official site of our company. Then go to **Support → Tools → Hikvision App Store** .
   - Scan the QR code below to download the application.

Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways.

- Visit *https://appstore.hikvision.com/static/help/index.html* to refer to the troubleshooting.
- Visit *https://appstore.hikvision.com/*, and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

2. Start the application and register for a Hik-Connect user account.
3. Log in after registration.
4. In the app, tap "+" on the upper-right corner and then scan the QR code of the camera to add the camera. You can find the QR code on the camera or on the cover of the Quick Start Guide of the camera in the package.
5. Follow the prompts to set the network connection and add the camera to your Hik-Connect account.

   For detailed information, refer to the user manual of the Hik-Connect app.

7.14.1 Enable Hik-Connect Service on Camera

Hik-Connect service should be enabled on your camera before using the service.

You can enable the service through SADP software or Web browser.

Enable Hik-Connect Service via Web Browser

Follow the following steps to enable Hik-Connect Service via Web Browser.

Before You Start

You need to activate the camera before enabling the service.

Steps

1. Access the camera via web browser.
2. Enter platform access configuration interface. **Configuration → Network → Advanced Settings → Platform Access**
3. Select Hik-Connect as the **Platform Access Mode**.
4. Check **Enable**.
5. Click and read "Terms of Service" and "Privacy Policy" in pop-up window.
6. Create a verification code or change the old verification code for the camera.

   Note

   The verification code is required when you add the camera to Hik-Connect service.

7. Save the settings.

Enable Hik-Connect Service via SADP Software

This part introduce how to enable Hik-Connect service via SADP software of an activated camera.

Steps

1. Run SADP software.
2. Select a camera and enter **Modify Network Parameters** page.
3. Check **Enable Hik-Connect**.
4. Create a verification code or change the old verification code.

Note

The verification code is required when you add the camera to Hik-Connect service.

5. Click and read "Terms of Service" and "Privacy Policy".
6. Confirm the settings.

7.14.2 Set Up Hik-Connect

Steps

1. Get and install Hik-Connect application by the following ways.
   - Visit ***https://appstore.hikvision.com*** to download the application according to your mobile phone system.
   - Visit the official site of our company. Then go to **Support → Tools → Hikvision App Store** .
   - Scan the QR code below to download the application.

Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways.

- Visit ***https://appstore.hikvision.com/static/help/index.html*** to refer to the troubleshooting.
- Visit ***https://appstore.hikvision.com/*** , and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

2. Start the application and register for a Hik-Connect user account.
3. Log in after registration.

7.14.3 Add Camera to Hik-Connect

Steps

1. Connect your mobile device to a Wi-Fi.
2. Log into the Hik-Connect app.
3. In the home page, tap "+" on the upper-right corner to add a camera.
4. Scan the QR code on camera body or on the *Quick Start Guide* cover.

Note

If the QR code is missing or too blur to be recognized, you can also add the camera by inputting the camera's serial number.

5. Input the verification code of your camera.

Note

- The required verification code is the code you create or change when you enable Hik-Connect service on the camera.
- If you forget the verification code, you can check the current verification code on **Platform Access** configuration page via web browser.

6. Tap **Connect to a Network** button in the popup interface.
7. Choose **Wired Connection** or **Wireless Connection** according to your camera function.

Wireless Connection	Input the Wi-Fi password that your mobile phone has connected to, and tap **Next** to start the Wi-Fi connection process. (Locate the camera within 3 meters from the router when setting up the Wi-Fi.)
Wired Connection	Connect the camera to the router with a network cable and tap **Connected** in the result interface.

Note

The router should be the same one which your mobile phone has connected to.

8. Tap **Add** in the next interface to finish adding.

For detailed information, refer to the user manual of the Hik-Connect app.

Chapter 8 Arming Schedule and Alarm Linkage

Arming schedule is a customized time period in which the device performs certain tasks. Alarm linkage is the response to the detected certain incident or target during the scheduled time.

8.1 Set Arming Schedule

Set the valid time of the device tasks.

Steps

1. Click **Arming Schedule**.
2. Drag the time bar to draw desired valid time.

   Note

   Up to 8 periods can be configured for one day.
3. Adjust the time period.
   - Click on the selected time period, and enter the desired value. Click **Save**.
   - Click on the selected time period. Drag the both ends to adjust the time period.
   - Click on the selected time period, and drag it on the time bar.
4. **Optional:** Click **Copy to...** to copy the same settings to other days.
5. Click **Save**.

8.2 Linkage Method Settings

You can enable the linkage functions when an event or alarm occurs.

8.2.1 Trigger Alarm Output

If the device has been connected to an alarm output device, and the alarm output No. has been configured, the device sends alarm information to the connected alarm output device when an alarm is triggered.

Steps

1. Go to **Configuration → Event → Basic Event → Alarm Output** .
2. Set alarm output parameters.

   Automatic Alarm For the information about the configuration, see ***Automatic Alarm*** .

   Manual Alarm For the information about the configuration, see ***Manual Alarm*** .
3. Click **Save**.

Manual Alarm

You can trigger an alarm output manually.

Steps

1. Set the manual alarm parameters.

   Alarm Output No.

   Select the alarm output No. according to the alarm interface connected to the external alarm device.

   Alarm Name

   Edit a name for the alarm output.

   Delay

   Select **Manual**.

2. Click **Manual Alarm** to enable manual alarm output.
3. **Optional:** Click **Clear Alarm** to disable manual alarm output.

Automatic Alarm

Set the automatic alarm parameters, then the device triggers an alarm output automatically in the set arming schedule.

Steps

1. Set automatic alarm parameters.

   Alarm Output No.

   Select the alarm output No. according to the alarm interface connected to the external alarm device.

   Alarm Name

   Custom a name for the alarm output.

   Delay

   It refers to the time duration that the alarm output remains after an alarm occurs.

2. Set the alarming schedule. For the information about the settings, see ***Set Arming Schedule*** .
3. Click **Copy to...** to copy the parameters to other alarm output channels.
4. Click **Save**.

8.2.2 FTP/NAS/Memory Card Uploading

If you have enabled and configured the FTP/NAS/memory card uploading, the device sends the alarm information to the FTP server, network attached storage and memory card when an alarm is triggered.

Refer to ***Set FTP*** to set the FTP server.

Refer to ***Set NAS*** for NAS configuration.

Refer to ***Set New or Unencrypted Memory Card*** for memory card storage configuration.

8.2.3 Send Email

Check **Send Email**, and the device sends an email to the designated addresses with alarm information when an alarm event is detected.

For email settings, refer to ***Set Email*** .

Set Email

When the email is configured and **Send Email** is enabled as a linkage method, the device sends an email notification to all designated receivers if an alarm event is detected.

Before You Start

Set the DNS server before using the Email function. Go to **Configuration → Network → Basic Settings → TCP/IP** for DNS settings.

Steps

1. Go to email settings page: **Configuration → Network → Advanced Settings → Email** .
2. Set email parameters.
   1) Input the sender's email information, including the **Sender's Address**, **SMTP Server**, and **SMTP Port**.
   2) **Optional:** If your email server requires authentication, check **Authentication** and input your user name and password to log in to the server.
   3) Set the **E-mail Encryption**.
      - When you select **SSL** or **TLS**, and disable STARTTLS, emails are sent after encrypted by SSL or TLS. The SMTP port should be set as 465.
      - When you select **SSL** or **TLS** and **Enable STARTTLS**, emails are sent after encrypted by STARTTLS, and the SMTP port should be set as 25.

      Note

      If you want to use STARTTLS, make sure that the protocol is supported by your email server. If you check the **Enable STARTTLS** while the protocol is not supported by your email sever, your email is sent with no encryption.
   4) **Optional:** If you want to receive notification with alarm pictures, check **Attached Image**. The notification email has 3 attached alarm pictures about the event with configurable image capturing interval.
   5) Input the receiver's information, including the receiver's name and address.
   6) Click **Test** to see if the function is well configured.
3. Click **Save**.

8.2.4 Notify Surveillance Center

Check **Notify Surveillance Center**, the alarm information is uploaded to the surveillance center when an alarm event is detected.

8.2.5 Trigger Recording

Check **Trigger Recording**, and the device records the video about the detected alarm event.

For recording settings, refer to ***Video Recording and Picture Capture***

8.2.6 Flashing Light

After enabling **Flashing Light** and setting the **Flashing Light Alarm Output**, the light flashes when an alarm event is detected.

Set Flashing Alarm Light Output

When events occur, the flashing light on the device can be triggered as an alarm.

Steps

1. Go to **Configuration → Event → Basic Event → Flashing Alarm Light Output** .
2. Set **Flashing Duration**, **Flashing Frequency** and **Brightness**.

   Flashing Duration

   The time that the flashing lasts when one alarm happens.

   Flashing Frequency

   The rate at which the light flashes. High frequency, medium frequency, low frequency, and normally on are selectable.

   Brightness

   The brightness of the light.
3. Set the arming schedule. See ***Set Arming Schedule*** for details.
4. Click **Save**.

Note

Only certain device models support the function.

8.2.7 Audible Warning

After enabling **Audible Warning** and setting **Audible Alarm Output**, the built-in speaker of the device or connected external speaker plays warning sounds when an alarm happens.

For audible alarm output settings, refer to ***Set Audible Alarm Output*** .

Note

The function is only supported by certain camera models.

Set Audible Alarm Output

When the device detects targets in the detection area, audible alarm can be triggered as a warning.

Steps

1. Go to **Configuration → Event → Basic Event → Audible Alarm Output** .
2. Select **Sound Type** and set related parameters.
   - Select **Prompt** and set the alarm times you need.
   - Select **Warning** and its contents. Set the alarm times you need.
   - Select **Custom Audio**. You can select a custom audio file from the drop-down list. If no file is available, you can click **Add** to upload an audio file that meets the requirement. Up to three audio files can be uploaded.
3. **Optional:** Click **Test** to play the selected audio file on the device.
4. Set arming schedule for audible alarm. See ***Set Arming Schedule*** for details.
5. Click **Save**.

Note

The function is only supported by certain device models.

Chapter 9 System and Security

It introduces system maintenance, system settings and security management, and explains how to configure relevant parameters.

9.1 View Device Information

You can view device information, such as Device No., Model, Serial No. and Firmware Version.

Enter **Configuration → System → System Settings → Basic Information** to view the device information.

9.2 Search and Manage Log

Log helps locate and troubleshoot problems.

Steps

1. Go to **Configuration → System → Maintenance → Log** .
2. Set search conditions **Major Type, Minor Type, Start Time,** and **End Time.**
3. Click **Search.**

   The matched log files will be displayed on the log list.
4. **Optional:** Click **Export** to save the log files in your computer.

9.3 Simultaneous Login

The administrator can set the maximum number of users logging into the system through web browser simultaneously.

Go to **Configuration → System → User Management** , click **General** and set **Simultaneous Login.**

9.4 Import and Export Configuration File

It helps speed up batch configuration on other devices with the same parameters.

Enter **Configuration → System → Maintenance → Upgrade & Maintenance** . Choose device parameters that need to be imported or exported and follow the instructions on the interface to import or export configuration file.

9.5 Export Diagnose Information

Diagnose information includes running log, system information, hardware information.

Go to **Configuration → System → Maintenance → Upgrade & Maintenance** . Check desired diagnose information and click **Diagnose Information** to export corresponding diagnose information of the device.

9.6 Reboot

You can reboot the device via browser.

Go to **Configuration → System → Maintenance → Upgrade & Maintenance** , and click **Reboot**.

9.7 Restore and Default

Restore and Default helps restore the device parameters to the default settings.

Steps

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance** .
2. Click **Restore** or **Default** according to your needs.

Restore	Reset device parameters, except user information, IP parameters and video format to the default settings.
Default	Reset all the parameters to the factory default.

Note

Be careful when using this function. After resetting to the factory default, all the parameters are reset to the default settings.

9.8 Upgrade

Before You Start

You need to obtain the correct upgrade package.

Caution

DO NOT disconnect power during the process, and the device reboots automatically after upgrade.

Steps

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance** .
2. Choose one method to upgrade.

Firmware	Locate the exact path of the upgrade file.

Firmware Directory Locate the directory which the upgrade file belongs to.

3. Click **Browse** to select the upgrade file.
4. Click **Upgrade**.

9.9 View Open Source Software License

Go to **Configuration → System → System Settings → About Device** , and click **View Licenses**.

9.10 Wiegand

Note

This function is only supported by certain camera models.

Check **Enable** and select the protocol. The default protocol is SHA-1 26bit.

If enabled, the recognized license plate number will be output via the selected Wiegand protocol.

9.11 Metadata

Metadata is the raw data that the camera collects before algorithm processing. It provide the option to users to explore various data usages.

Note

The function is only supported by certain device models.

Go to **Configuration → System → Metadata Settings** to enable metadata uploading of the desired function.

Smart Event

The metadata of the smart event includes the target ID, target coordinate, time, etc.

9.12 Time and Date

You can configure time and date of the device by configuring time zone, time synchronization and Daylight Saving Time (DST).

9.12.1 Synchronize Time Manually

Steps

1. Go to **Configuration → System → System Settings → Time Settings** .
2. Select **Time Zone**.

3. Click **Manual Time Sync.**.
4. Choose one time synchronization method.
   - Select **Set Time**, and manually input or select date and time from the pop-up calendar.
   - Check **Sync. with computer time** to synchronize the time of the device with that of the local PC.
5. Click **Save**.

9.12.2 Set NTP Server

You can use NTP server when accurate and reliable time source is required.

Before You Start

Set up a NTP server or obtain NTP server information.

Steps

1. Go to **Configuration → System → System Settings → Time Settings** .
2. Select **Time Zone**.
3. Click **NTP**.
4. Set **Server Address, NTP Port** and **Interval**.

   Note

   Server Address is NTP server IP address.
5. Click **Test** to test server connection.
6. Click **Save**.

9.12.3 Synchronize Time by Satellite

Note

This function varies depending on different devices.

Steps

1. Enter **Configuration → System → System Settings → Time Settings** .
2. Select **Satellite Time Sync.**.
3. Set **Interval**.
4. Click **Save**.

9.12.4 Set DST

If the region where the device is located adopts Daylight Saving Time (DST), you can set this function.

Steps

1. Go to **Configuration → System → System Settings → DST** .
2. Check **Enable DST**.
3. Select **Start Time, End Time** and **DST Bias**.
4. Click **Save**.

9.13 Set RS-485

RS-485 is used to connect the device to external device. You can use RS-485 to transmit the data between the device and the computer or terminal when the communication distance is too long.

Before You Start

Connect the device and computer or termial with RS-485 cable.

Steps

1. Go to **Configuration → System → System Settings → RS-485** .
2. Set the RS-485 parameters.

Note

You should keep the parameters of the device and the computer or terminal all the same.

3. Click **Save**.

9.14 Set RS-232

RS-232 can be used to debug device or access peripheral device. RS-232 can realize communication between the device and computer or terminal when the communication distance is short.

Before You Start

Connect the device to computer or terminal with RS-232 cable.

Steps

1. Go to **Configuration → System → System Settings → RS-232** .
2. Set RS-232 parameters to match the device with computer or terminal.
3. Click **Save**.

9.15 Power Consumption Mode

It is used to switch the power consumption when the device is working.

Note

The function is only supported by certain camera models.

Go to **Configuration → System → System Settings → Power Consumption Mode** , select the desired power consumption mode.

Full Consumption Mode

The device works with all the functions enabled.

Low Consumption Real-Time Mode

The device DSP works normally. It records the videos with the main stream at the half frame rate, and supports the remote login, preview and the configuration.

Low Power Sleep

When the device power is lower than **Threshold of Low Power Sleep Mode**, the device enters sleep mode.

When the device power is recovered to 10% above the threshold, the device enters the user configuration mode.

Scheduled Sleep

If the device is during **Scheduled Sleep Time**, it enters the sleep mode, otherwise it enters the user configuration mode.

Note

For the scheduled sleep schedule settings, see ***Arming Schedule and Alarm Linkage*** .
The device supports the timing wake. For the details, see ***Set Timing Wake*** .

9.16 External Device

For the device supporting external devices, including the supplement light, wiper on the housing and the LED light, you can control them via the Web browser when it is used with the housing. External devices vary with models.

Brightness

Adjust **Low Beam Brightness** and **High Beam Brightness** according to the actual scene.

Timing

The LED light will be turned on by the schedule you set. You should set **Start Time** and **End Time**.

Auto

The LED light will be turned on according to the environment illumination.

9.16.1 Supplement Light Settings

You can set supplement light and refer to the actual device for relevant parameters.

Smart Supplement Light

Smart supplement light avoids over exposure when the supplement light is on.

Supplement Light Mode

When the device supports supplement light, you can select supplement light mode.

IR Mode

IR light is enabled.

White Light Mode

White light is enabled.

Mix Mode

Both IR light and white light are enabled.

Off

Supplement light is disabled.

Brightness Adjustment Mode

Auto

The brightness adjusts according to the actual environment automatically.

Manual

You can drag the slider or set value to adjust the brightness.

9.16.2 Heater

You can enable heater to remove fog around the lens of the device.

Go to **Configuration → System → System Settings → External Device** and select the mode as required.

9.17 Security

You can improve system security by setting security parameters.

9.17.1 Authentication

You can improve network access security by setting RTSP and WEB authentication.

Go to **Configuration → System → Security → Authentication** to choose authentication protocol and method according to your needs.

RTSP Authentication

Digest and digest/basic are supported, which means authentication information is needed when RTSP request is sent to the device. If you select **digest/basic**, it means the device supports digest or basic authentication. If you select **digest**, the device only supports digest authentication.

RTSP Digest Algorithm

MD5, SHA256 and MD5/SHA256 encrypted algorithm in RTSP authentication. If you enable the digest algorithm except for MD5, the third-party platform might not be able to log in to the device or enable live view because of compatibility. The encrypted algorithm with high strength is recommended.

WEB Authentication

Digest and digest/basic are supported, which means authentication information is needed when WEB request is sent to the device. If you select **digest/basic**, it means the device supports digest or basic authentication. If you select **digest**, the device only supports digest authentication.

WEB Digest Algorithm

MD5, SHA256 and MD5/SHA256 encrypted algorithm in WEB authentication. If you enable the digest algorithm except for MD5, the third-party platform might not be able to log in to the device or enable live view because of compatibility. The encrypted algorithm with high strength is recommended.

Note

Refer to the specific content of protocol to view authentication requirements.

9.17.2 Set IP Address Filter

IP address filter is a tool for access control. You can enable the IP address filter to allow or forbid the visits from the certain IP addresses.

IP address refers to IPv4.

Steps

1. Go to **Configuration → System → Security → IP Address Filter** .
2. Check **Enable IP Address Filter.**
3. Select the type of IP address filter.

   Forbidden IP addresses in the list cannot access the device.

   Allowed Only IP addresses in the list can access the device.
4. Edit the IP address filter list.

   Add Add a new IP address or IP address range to the list.

   Modify Modify the selected IP address or IP address range in the list.

   Delete Delete the selected IP address or IP address range in the list.
5. Click **Save.**

9.17.3 Set HTTPS

HTTPS is a network protocol that enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **Configuration → Network → Advanced Settings → HTTPS** .
2. Check **Enable** to access the camera via HTTP or HTTPS protocol.
3. Check **Enable HTTPS Browsing** to access the camera only via HTTPS protocol.
4. Select the **Server Certificate**.
5. Click **Save**.

Note

If the function is abnormal, check if the selected certificate is abnormal in **Certificate Management**.

9.17.4 Set QoS

QoS (Quality of Service) can help improve the network delay and network congestion by setting the priority of data sending.

Note

QoS needs support from network device such as router and switch.

Steps

1. Go to **Configuration → Network → Advanced Configuration → QoS** .
2. Set **Video/Audio DSCP**, **Alarm DSCP** and **Management DSCP**.

Note

Network can identify the priority of data transmission. The bigger the DSCP value is, the higher the priority is. You need to set the same value in router while configuration.

3. Click **Save**.

9.17.5 Set IEEE 802.1X

IEEE 802.1x is a port-based network access control. It enhances the security level of the LAN/ WLAN. When devices connect to the network with IEEE 802.1x standard, the authentication is needed.

Go to **Configuration → Network → Advanced Settings → 802.1X** , and enable the function.

Set **Protocol** and **EAPOL Version** according to router information.

Protocol

EAP-LEAP, EAP-TLS, and EAP-MD5 are selectable

EAP-LEAP and EAP-MD5

If you use EAP-LEAP or EAP-MD5, the authentication server must be configured. Register a user name and password for 802.1X in the server in advance. Input the user name and password for authentication.

EAP-TLS

If you use EAP-TLS, input Identify, Private Key Password, and upload CA Certificate, User Certificate and Private Key.

EAPOL Version

The EAPOL version must be identical with that of the router or the switch.

9.17.6 Control Timeout Settings

If this function is enabled, you will be logged out when you make no operation (not including viewing live image) to the device via web browser within the set timeout period.

Go to **Configuration → System → Security → Advanced Security** to complete settings.

9.17.7 Search Security Audit Logs

You can search and analyze the security log files of the device so as to find out the illegal intrusion and troubleshoot the security events.

Steps

Note

This function is only supported by certain camera models.

1. Go to **Configuration → System → Maintenance → Security Audit Log** .
2. Select log types, **Start Time**, and **End Time**.
3. Click **Search**.

   The log files that match the search conditions will be displayed on the Log List.
4. **Optional:** Click **Export** to save the log files to your computer.

9.17.8 Security Reinforcement

Security reinforce is a solution to enhance network security. With the function enabled, risky functions, protocols, ports of the device are disabled and more secured alternative functions, protocols and ports are enabled.

Go to **Configuration → System → Security → Advanced Security** . Check **Security Reinforcement**, and click **Save**.

9.17.9 SSH

Secure Shell (SSH) is a cryptographic network protocol for operating network services over an unsecured network.

The SSH function is disabled by default.

Caution

Use the function with caution. The security risk of device internal information leakage exists when the function is enabled.

9.18 Certificate Management

It helps to manage the server/client certificates and CA certificate, and to send an alarm if the certificates are close to expiry date, or are expired/abnormal.

Note

The function is only supported by certain device models.

9.18.1 Create Self-signed Certificate

Steps

1. Click **Create Self-signed Certificate**.
2. Follow the prompt to enter **Certificate ID**, **Country/Region**, **Hostname/IP**, **Validity** and other parameters.

   Note

   The certificate ID should be digits or letters and be no more than 64 characters.
3. Click **OK**.
4. **Optional:** Click **Export** to export the certificate, or click **Delete** to delete the certificate to recreate a certificate, or click **Certificate Properties** to view the certificate details.

9.18.2 Create Certificate Request

Before You Start

Select a self-signed certificate.

Steps

1. Click **Create Certificate Request**.
2. Enter the related information.
3. Click **OK**.

9.18.3 Import Certificate

Steps

1. Click **Import**.
2. Click **Create Certificate Request**.
3. Enter the **Certificate ID**.
4. Click **Browser** to select the desired server/client certificate.
5. Select the desired import method and enter the required information.
6. Click **OK**.
7. **Optional:** Click **Export** to export the certificate, or click **Delete** to delete the certificate to recreate a certificate, or click **Certificate Properties** to view the certificate details.

Note

- Up to 16 certificates are allowed.
- If certain functions are using the certificate, it cannot be deleted.
- You can view the functions that are using the certificate in the functions column.
- You cannot create a certificate that has the same ID with that of the existing certificate and import a certificate that has the same content with that of the existing certificate.

9.18.4 Install Server/Client Certificate

Steps

1. Go to **Configuration → System → Security → Certificate Management** .
2. Click **Create Self-signed Certificate, Create Certificate Request** and **Import** to install server/client certificate.

Create self-signed certificate	Refer to ***Create Self-signed Certificate***
Create certificate request	Refer to ***Create Certificate Request***
Import Certificate	Refer to ***Import Certificate***

9.18.5 Install CA Certificate

Steps

1. Click **Import**.
2. Enter the **Certificate ID**.
3. Click **Browser** to select the desired server/client certificate.
4. Select the desired import method and enter the required information.
5. Click **OK**.

Note

Up to 16 certificates are allowed.

9.18.6 Enable Certificate Expiration Alarm

Steps

1. Check **Enable Certificate Expiration Alarm**. If enabled, you will receive an email or the camera links to the surveillance center that the certificate will expire soon, or is expired or abnormal.
2. Set the **Remind Me Before Expiration (day)**, **Alarm Frequency (day)** and **Detection Time (hour)**.

Note

- If you set the reminding day before expiration to 1, then the camera will remind you the day before the expiration day. 1 to 30 days are available. Seven days is the default reminding days.
- If you set the reminding day before expiration to 1, and the detection time to 10:00, and the certificate will expire in 9:00 the next day, the camera will remind you in 10:00 the first day.

3. Click **Save**.

9.19 User and Account

9.19.1 Set User Account and Permission

The administrator can add, modify, or delete other accounts, and grant different permission to different user levels.

Caution

To increase security of using the device on the network, please change the password of your account regularly. Changing the password every 3 months is recommended. If the device is used in high-risk environment, it is recommended that the password should be changed every month or week.

Steps

1. Go to **Configuration → System → User Management → User Management** .
2. Click **Add**. Enter **User Name**, select **Level**, and enter **Password**. Assign remote permission to users based on needs.

Administrator

The administrator has the authority to all operations and can add users and operators and assign permission.

User

Users can be assigned permission of viewing live video, setting PTZ parameters, and changing their own passwords, but no permission for other operations.

Operator

Operators can be assigned all permission except for operations on the administrator and creating accounts.

Modify Select a user and click **Modify** to change the password and permission.

Delete Select a user and click **Delete**.

Note

The administrator can add up to 31 user accounts.

3. Click **OK**.

9.19.2 Simultaneous Login

The administrator can set the maximum number of users logging into the system through web browser simultaneously.

Go to **Configuration → System → User Management** , click **General** and set **Simultaneous Login**.

9.19.3 Online Users

The information of users logging into the device is shown.

Go to **Configuration → System → User Management → Online Users** to view the list of online users.

Chapter 10 Allocate VCA Resource

VCA resource offers you options to enable certain VCA functions according to actual needs. It helps allocate more resources to the desired functions.

Steps

1. Go to **Configuration → System → System Settings → VCA Resource** .
2. Select desired VCA function.
3. Save the settings.

Note

Some VCA functions are mutually exclusive. When certain function or functions are selected and saved, others will not be hidden.

10.1 Road Traffic

Motor vehicle, non-motor vehicle, and pedestrian can be detected and captured when they enter the set lane to realize rapid detection and comprehensive surveillance of the targets on road.

Note

Only certain device models support this function.

10.1.1 Set Vehicle Detection

The vehicle that enters the set lane can be detected and the picture of the vehicle and its license plate can be captured and stored. Alarm will be triggered and capture can be uploaded.

Before You Start

Go to **Configuration → System → System Settings → VCA Resources** , and select **Road Traffic.**

Steps

1. Go to **Configuration → Road Traffic → Detection Configuration** , and select **Vehicle Detection** as detection type.
2. Check **Enable.**
3. Select the lane number.
4. Click and drag the lane line to set its position, or click and drag the line end to adjust the length and angle of the line.
5. Adjust the zoom ratio of the camera so that the size of the vehicle in the image is close to that of the red frame. Only the position of red frame is adjustable.

Note

Only 1 license plate can be captured at one time for each lane.

6. Select **Region** and **Country/Region**.
7. Select the license plate information upload mode.

Entrance/Exit	The license plate information of the detected vehicle will be uploaded when the vehicle passes the detection area and triggers the detection in entrance/ exit.
City Street	The license plate information of the detected vehicle will be uploaded when the vehicle passes the detection area and triggers the detection in city streets.
Alarm Input	It means the input alarm will trigger a license plate capture and recognition action.

Note

- When Alarm Input is selected, the alarm input A<-1 will automatically be assigned to trigger vehicle detection and its alarm type is always NO.
- If the A<-1 alarm input is used to trigger vehicle detection, it can not be used for other basic events.
- When Alarm Input is selected and saved, previously configured linkage method for A<-1 will be canceled.

8. Select the **Detection mode**.
9. Check **Remove Duplicated License Plates** ans set the **Time Interval**. The default time interval is 4 minutes.

Note

Up to 8 license plates are supported.

10. Set arming schedule and linkage method. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
11. Click **Save**.

10.1.2 Set Mixed-Traffic Detection Rule

The motor vehicle, non-motor vehicle, and pedestrian that enter the set lane can be detected, and the picture of targets can be captured and stored. Alarm will be triggered and capture can be uploaded.

Before You Start

Go to **Configuration → System → System Settings → VCA Resources** , and select **Road Traffic**.

Steps

1. Go to **Configuration → Road Traffic → Detection Configuration** , and select **Mixed-traffic Detection** as detection type.
2. Check **Enable**.
3. Select the lane number.
4. Select **Region** and **Country/Region**.
5. Set arming schedule and linkage method. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
6. Click **Save**.

10.1.3 Uploading Pictures Settings

You can set the image parameters of the captured images in vehicle detection and mixed-traffic detection.

Go to **Configuration → Road Traffic → Picture** .

Picture Quality

The larger the value is, the clearer the picture is, but larger storage space is also required.

Picture Size

The larger the value is, the larger the storage space is needed. And the level of network transmission requirement is also higher.

License Plate Enhancement

The larger the value is, the clearer the license plate is, but larger storage space is also required.

Check **License Plate Enhancement** and set the level. The default level is 50.

Overlay

You can overlay camera, device or vehicle information on the captured image and click ↑ ↓ to adjust the order of overlay texts.

For camera settings, go to **Configuration → Road Traffic → Camera** to set relevant parameters and click **Save**.

10.1.4 Camera Settings

You can set the parameters of each camera for better management.

Go to **Configuration → Road Traffic → Camera** to set relevant parameters and click **Save**.

10.1.5 Import or Export Blocklist & Allowlist

You can import and export the blocklist and allowlist as desired, and check the list content in this interface.

Steps

1. Click **Browse** to open the PC local directory.
2. Find the blocklist & allowlist file and click to select it. Click **Open** to confirm.

Note

- The file to import should corresponds with the file template that is required by the camera. You are recommended to export an empty blocklist & allowlist file from the camera as the template and fill in the content.
- The file should be in the .xls format and the cell format should be Text.

3. Click **Import** to import the selected file.
4. Click **Export** to open the PC local directory.
5. Select a directory in your PC local directory.
6. Name the file in the file name text filed.
7. Click **Save**.

10.2 Face Capture

The device can capture the face that appears in the configured area, and the face information will be uploaded with the captured picture as well.

Note

- For device that supports face capture, you need to enable the function in **VCA Resource**. Refer to ***Allocate VCA Resource*** for details.
- Face capture is only supported by certain models.

10.2.1 Set Face Capture

The face that appears in the configured area can be captured.

Before You Start

To enable the function, go to **VCA Resource** and select **Face Capture**.

Steps

1. Go to **Configuration → Face Capture** .
2. For shield region settings, refer to ***Set Shield Region*** .
3. Select **Rule** and check **Rule**.
4. Input the min. pupil distance in the text field, or click ▫ to draw the min. pupil distance.

   Min. Pupil Distance

   The min. pupil distance refers to the minimum area between two pupils, and it is basic for the device to recognize a face.
5. Input the max. pupil distance in the text field, or click ▫ to draw the max. pupil distance.

6. Click ⬡ to draw the detection area you want the face capture to take effect. Draw area by left-clicking end-points in the live view window, and right-clicking to finish the area drawing. It is recommended that the drawn area occupies 1/2 to 2/3 of the live view image.
7. For the arming schedule settings, refer to ***Set Arming Schedule*** . For the linkage method settings, refer to ***Linkage Method Settings*** .
8. Click **Save**.
9. For overlay and capture settings, refer to ***Overlay and Capture*** . For advanced parameters settings, refer to ***Face Capture Algorithms Parameters*** .

Result

You can view and download captured face images in **Picture**. Refer to ***View and Download Picture*** for details.

10.2.2 Overlay and Capture

Choose to configure capture parameters and the information you want to display on stream and picture.

Display VCA info. on Stream

Display smart information on stream, including the target and rules information.

Display Target info. on Alarm Picture

Overlay the alarm picture with target information.

Target Picture Settings

Custom, Head Shot, Half-Body Shot and Full-Body Shot are selectable.

Note

If you select **Custom**, you can customize **width**, **head height** and **body height** as required.

You can check **Fixed Value** to set the picture height.

Background Picture Settings

Comparing to target picture, background picture is the scene image offers extra environmental information. You can set the background picture quality and resolution. If the background image need to be uploaded to surveillance center, check **Background Upload**.

People Counting Overlay

Select flow overlay type.

Select the daily reset time. Click **Manual Reset** if you want to reset right now.

Camera

You can set **Device No.** and **Camera Info.** for the camera, which can be overlaid on captured picture.

Text Overlay

You can check desired items and adjust their order to display on captured pictures by ↓ ↑ .

The content of **Device No.** and **Camera Info** should be on the same page.

10.2.3 Face Capture Algorithms Parameters

It is used to set and optimize the parameters of the algorithm library for face capture.

Go to **Configuration → Face Capture → Advanced Configuration → Parameters** .

Face Capture Version

It lists the version of the algorithms library.

Detection Parameters

Generation Speed

The speed to identify a target. The higher the value, the faster the target will be recognized. Setting the value quite low, and if there was a face in the configured area from the start, this face will not be captured. It can reduce the misinformation of the faces in the wall painting or posters. The default value of 3 is recommended.

Sensitivity

The sensitivity to identify a target. The higher the value is, the easier a face will be recognized, and the higher possibility of misinformation would be. The default value of 3 is recommended.

Capture Parameters

Best Shot

The best shot after target leave the detection area.

Capture Times

It refers to the capture times a face will be captured during its stay in the configured area. The default value is 1.

Capture Threshold

It stands for the quality of face to trigger capture and alarm. Higher value means better quality should be met to trigger capture and alarm.

Quick Shot

You can define quick shot threshold and max. capture interval.

Quick Shot Threshold

It stands for the quality of face to trigger quick shot.

Face Exposure

Check the checkbox to enable the face exposure.

Reference Brightness

The reference brightness of a face in the face exposure mode. If a face is detected, the camera adjusts the face brightness according to the value you set. The higher the value, the brighter the face is.

Minimum Duration

The minimum duration of the camera exposures the face.

Note

If the face exposure is enabled, please make sure the WDR function is disabled, and the manual iris is selected.

Face Filtering Time

It means the time interval between the camera detecting a face and taking a capture action. If the detected face stays in the scene for less than the set filtering time, capture will not be triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the detected face when the face keeps staying in the scene for 5 seconds.

Note

The face filtering time (longer than 0s) may increase the possibility of the actual capture times less than the set value above.

Restore Default

Click **Restore** to restore all the settings in advanced configuration to the factory default.

10.2.4 Set Shield Region

The shield region allows you to set the specific region in which the set smart function rule is invalid.

Steps

1. Select **Shield Region**.
2. Click ○ to draw shield area. Repeat this step above to set more shield regions.
3. **Optional:** Click ✕ to delete the drawn areas.
4. Click **Save**.

Chapter 11 Smart Display

It can display the captured pictures when enabling smart functions.

Note

The function is only supported by certain device models.

Layout Preview

Click and select **Layout Preview**. Select the contents according to your needs. When you select real-time analysis, you can select the contents only for real-time analysis.

Detection Attribute

Click and select **Detection Attribute**. When you enable this function, the attribute information of target analysis can be displayed and the information you select will be displayed in the attribute analysis area.

Chapter 12 EPTZ

EPTZ (Electronic PTZ) is a high-resolution function that digitally zooms and pans into portions of the image, with no physical camera movement. If you want to use the EPTZ function, make sure you have select the **Fourth Stream** in the live view. Fourth stream and EPTZ should be both enabled simultaneously.

Note

The function is only supported by certain device models.

12.1 Patrol

Steps

1. Go to **Configuration → EPTZ** .
2. Check **Enable EPTZ**.
3. Check **Fourth Stream**.
4. Select **Patrol** in **Application**.
5. Click **Save**.

What to do next

For the detailed information about the patrol settings, see the PTZ operations on live view page.

12.2 Auto-Tracking

Steps

1. Go to **Configuration → EPTZ** .
2. Check **Enable EPTZ**.
3. Check **Fourth Stream**.
4. Select **Auto-tracking** in **Application**.
5. Click **Detection Area** to start drawing.
6. Click on the live video to specify the four vertexes of the detection area, and right click to complete drawing.
7. Set rules.

Detection Target	Human and vehicle are available. If the detection target is not selected, all the detected targets will be tracked, including the human and vehicle.

Note

Only certain camera models support this function.

Sensitivity	It stands for the percentage of the body part of an acceptable target that is tracked. Sensitivity = 100 - S1/ST × 100. S1 stands for the target body part that enters the pre-defined area. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the target can be tracked.

8. Click **Save**.

Appendix A. Device Command

Scan the following QR code to get device common serial port commands.

Note that the command list contains the commonly used serial port commands for all Hikvision network cameras.

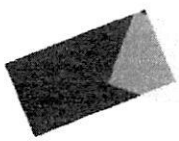


Appendix B. Device Communication Matrix

Scan the following QR code to get device communication matrix.

Note that the matrix contains all communication ports of Hikvision network cameras.





See Far, Go Further

3569

HIKVISION

DS-6900UDI(B) Series
HD Video and Audio Decoder

User Manual

© 2020 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

This Manual is the property of Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision"), and it cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise expressly stated herein, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual, any information contained herein.

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (https://www.hikvision.com/).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks Acknowledgement

- ***HIKVISION*** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Regulatory information

FCC information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

CE This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

Applicable Model

Series	Model
DS-6900UDI Decoder	DS-6901UDI(B)
	DS-6904UDI(B)
	DS-6908UDI(B)
	DS-6910UDI(B)
	DS-6912UDI(B)
	DS-6916UDI(B)

About the Default

Item	Default Value
User name	admin
Device IP address	192.0.0.64
SSH login	User name: admin Password: same as the device

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
NOTE	Provides additional information to emphasize or supplement important points of the main text.
WARNING	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Instructions

WARNING

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- Use the power adapter delivered with the device only.
- The socket-outlet shall be installed near the equipment and shall be easily accessible.
- Please make sure that the plug is firmly connected to the power socket.
- The equipment must be connected to an earthed mains socket-outlet.
- The equipment has been designed, when required, modified for connection to an IT power distribution system.
- This equipment is not suitable for use in locations where children are likely to be present.
- CAUTION: Risk of explosion if the battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.
  ATTENTION: Risque d'explosion si la batterie est remplacée par un type incorrect. Mettre au rebus les batteries usagées selon les instructions.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
- Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.

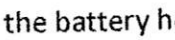
-  identifies the battery holder itself and identifies the positioning of the cell(s) inside the battery holder. + identifies the positive terminal(s) of equipment which is used with, or generates direct current. - identifies the negative terminal(s) of equipment which is used with, or generates direct current.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
- If the product does not work properly, please contact your dealer or the nearest service center.
- Never attempt to disassemble the product yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)
- Please enhance the protection for personal information and data security as the device may be confronted with the network security problems when it is connected to the Internet. Please contact your dealer or the nearest service center once you find that there may be the network security problems.
- The USB port of the equipment is used for connecting to a mouse, a keyboard, or a USB flash drive only.
- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not expose the device to the explosive situation.
- Keep clean and dry on the surface of the device.
- Do not touch the exposed connection points or components when the device is powered on.
- Do not place any naked flame sources, such as lit candles, on the device.
- Do not place any objects containing water or liquids on the device. Prevent the device from water dropping or splashing.
- Place the device in a well-ventilated, dust-free environment. Ensure that the air vents are not covered by any objects such as newspapers, tablecloths, or curtains.
- Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
- If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

Table of Contents

Chapter 1 Introduction 1
1.1 Description 1
1.2 Features 1
Chapter 2 Panels and Connections 3
2.1 Front Panel 3
2.2 Rear Panel 6
Chapter 3 Device Activation 10
3.1 Activating via SADP Software 10
3.2 Activating via Web Browser 11
Chapter 4 Network Configuration 13
4.1 Configuring Basic Network Settings 15
4.2 Configuring Security Control 15
Chapter 5 Decoding Parameters Configuration 17
5.1 Configuring Stream Settings 17
5.2 Configuring Transparent Channel 17
5.3 Configuring Synchronous Output Settings 18
5.4 Configuring Personalized Settings 19
Chapter 6 Decoding Operation 21
6.1 Configuring Encoding Devices 21
6.1.1 Adding an Encoding Device 21
6.1.2 Modifying an Encoding Device 24
6.1.3 Deleting an Encoding Device 25
6.2 Configuring Video Wall 25
6.3 Configuring Decoding Output 26
6.3.1 Configuring BNC Output 27
6.3.2 Configuring HDMI Output 28
6.4 Decoding Video on Video Wall 30
6.4.1 Interface Description 30
6.4.2 Dragging Channels to the Video Wall 31
6.4.3 Openning Window via Coordinate 32
6.4.4 Managing Decoding 34

6.4.5 Switching Encoding Channel 36
6.4.6 Configuring Auto-Switch of Cameras 37
6.4.7 Roaming Window 37
6.4.8 Zooming in/out Roaming Windows 38
6.4.9 Configuring Scene 40
Chapter 7 User Management 42
Chapter 8 System Configuration 44
8.1 Checking Device Information 44
8.2 Configuring Time Settings 44
8.3 Configuring RS-232 Serial Port 46
8.4 Configure RS-485 Serial Port 47
Chapter 9 System Maintenance 48
9.1 Importing Configuration Files 48
9.2 Exporting Configuration Files 48
9.3 Upgrading the Device 49
9.4 Restoring the Default Settings 49
9.5 Rebooting the Device 49
Chapter 10 Decoder Configuration and Operation by Client Software 50
10.1 Decode and Display Directly 50
10.2 View Settings 52
10.2.1 Add View Group 52
10.2.2 Add View 53
10.2.3 Set Schedule for Displaying Views on Smart Wall 53
10.3 Perform View Auto-Switch 54
10.4 Auto-Switch Cameras in One Window 55
10.5 Create a Roaming Window 55
10.6 View Alarm's Related Video on Smart Wall 56
10.7 View and Export Window No. and Camera ID 57
Chapter 11 Appendix 58
11.1 FAQ 58
11.2 List of Third-Party IP Cameras Access 59

Chapter 1 Introduction

1.1 Description

Designed for the high-definition video monitoring system, DS-6900UDI(B) Decoder is developed on the basis of embedded hardware platform, ensuring high reliability and stability of system running.

DS-6900UDI(B) Decoder is capable of simultaneous decoding video for 8-ch@24MP, 16-ch@12MP, 32-ch@8MP, 48-ch@5MP, 80-ch@3MP, 128-ch@1080p simultaneous decoding, and outputting decoded video via BNC, VGA, or HDMI interfaces, and it also supports multiple video stream formats like H.265, H.264+, Hik264, H.264 and MPEG4. The decoded video can be displayed on video wall or large screen.

1.2 Features

Powerful Decoding Capability

- DS-6901UDI(B) provides HDMI, VGA, and BNC output interfaces.
- Up to 8-ch decoding at 24 MP resolution (DS-6916UDI(B)).
- DS-6904UDI(B), DS-6908UDI(B), DS-6910UDI(B), DS-6912UDI(B), DS-6916UDI(B) provide HDMI (adaptable to DVI-D) and BNC output interfaces.
- Up to 4K (3840 × 2160@30 Hz) via HDMI interface (only for even interface), and up to 1080p@60 Hz via VGA interface.
- H.265+/H.265, H.264+/Hik264/H.264, MPEG4 and MJPEG video stream formats.
- PS, RTP, TS, ES, HIK encapsulation formats.
- Supports window opening and window roaming.
- Supports two-window division mode.
- You can double click the roaming window to zoom in or out for one roaming window or divided roaming sub-window.
- Three encoding levels: baseline, main, and high-profile.
- G.722, G711A, G726, G711U, MPEG2-L2, and AAC audio stream formats.
- Accessible by panoVu network camera.
- Accessible by 2.4 MP DeepinView camera.
- Accessible by thermal network camera and you can view the temperature measurement, dynamic fire source detection, ship detection and VCA information in live view and playback.
- You can enable or disable the smart information for the thermal network camera.

Multiple Decoding Control Modes

- Two decoding modes: active decoding and passive decoding.
- Decoding output of remote video files.
- Decoding on video wall by directly linking cameras or by stream media forwarding.
- Gets stream and decodes via URL.
- Remotely controls PTZ of DVR or DVS via transparent channel.
- Two-way audio via client software.
- Supports multi-screen control with PC installed with RSC server.
- Supports Wi-Fi module access to display the signal from iOS/Android mobile phone or pad on video wall.
- Wi-Fi can be enabled via the Web browser or client software. You can get stream and decode the video on the video wall when Wi-Fi is enabled if no wired network can be accessed.
- Configurable LED width and height parameters when the LED is connected.
- Regular and irregular virtual screen configurable to display multiple signal sources and get rid of the restriction of physical screen.
- LCD output type configurable for the BNC and VGA outputs; LCD and LED output types configurable for HDMI outputs.
- You can configure what the video wall show when decoding ends and streaming fails via the Web browser and client software.
- Auto-switch of sub-stream configurable via the Web browser and client software.

Integrated Capability

- Decoding video/audio stream accessed by ONIVF, RTP/RTSP protocols.
- Provides complete software development kit (SDK) for third-party developers.
- Port link aggregation technology (Ethernet Channel).

Maintenance Management

- Remotely get, configure, export and import parameters.
- Remotely reboot, restore default settings and upgrading via web browser or client software.

Chapter 2 Panels and Connections

2.1 Front Panel

- Front panel of DS-6901UDI(B)

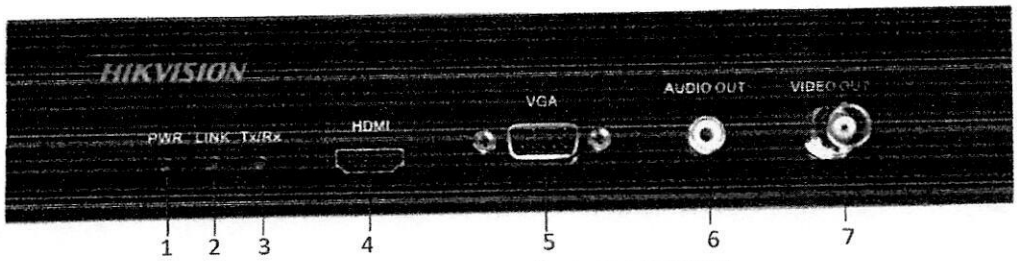


Figure 2-1 Front Panel of DS-6901UDI(B)

Table 2-1 Description of DS-6901UDI(B) Front Panel

No.	LED Indicator & Interface	Description
1	POWER	Power LED indicator
2	LINK	Network connection LED indicator
3	Tx/Rx	Data transmitting/receiving status LED indicator
4	HDMI	HDMI video output
5	VGA	VGA video output
6	AUDIO OUT	Audio output, 3.5mm connector
7	VIDEO OUT	Video output, BNC connector

- Front Panel of DS-6904UDI(B)

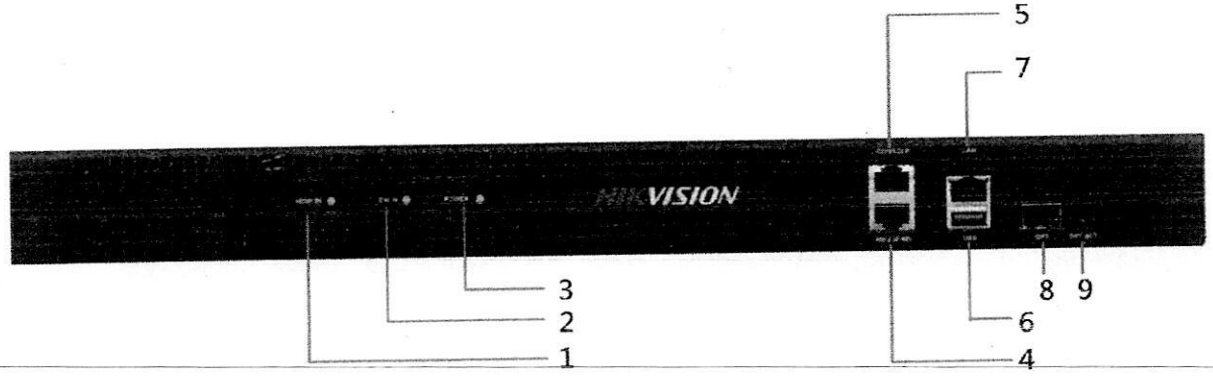


Figure 2-2 Front Panel of DS-6904UDI(B)

Table 2-2 Description of DS-6904UDI(B) Front Panel

No.	LED Indicator & Interface	Description
1	HDMI IN	HDMI input indicator
2	DVI IN	DVI input indicator
3	Power	Power indicator
4	RS-232/485	Connect to RS-232/485 devices, e.g., PC , etc.
5	CONSOLE	Debugging interface
6	USB	USB 2.0 interface
7	LAN	10/100/1000 Mbps Ethernet interface
8	OPT	10/100/1000 Mbps optical interface
9	OPT ACT	Optical interface indicator

- Front Panel of DS-6908UDI(B)

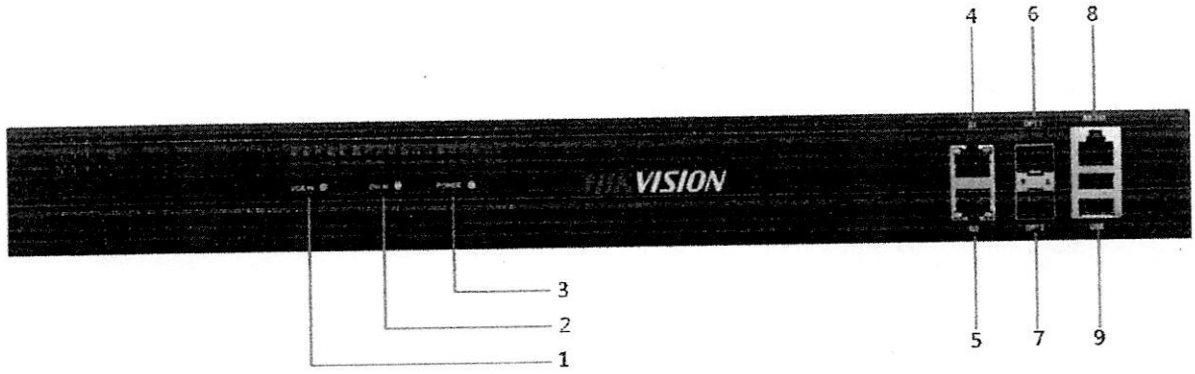


Figure 2-3 Front Panel of DS-6908UDI(B)

Table 2-3 Description of DS-6908UDI(B) Front Panel

No.	LED Indicator & Interface	Description
1	VGA IN	VGA input indicator
2	DVI IN	DVI input indicator
3	POWER	Power indicator
4	G1	10/100/1000 Mbps Ethernet interface 1
5	G2	10/100/1000 Mbps Ethernet interface 2
6	OPT1	10/100/1000 Mbps optical interface 1
7	OPT2	10/100/1000 Mbps optical interface 2
8	RS-232	Connect to RS-232 devices, e.g., PC, etc.
9	USB	USB 2.0 interface

- Front Panel of DS-6910/6912/6916UDI(B)

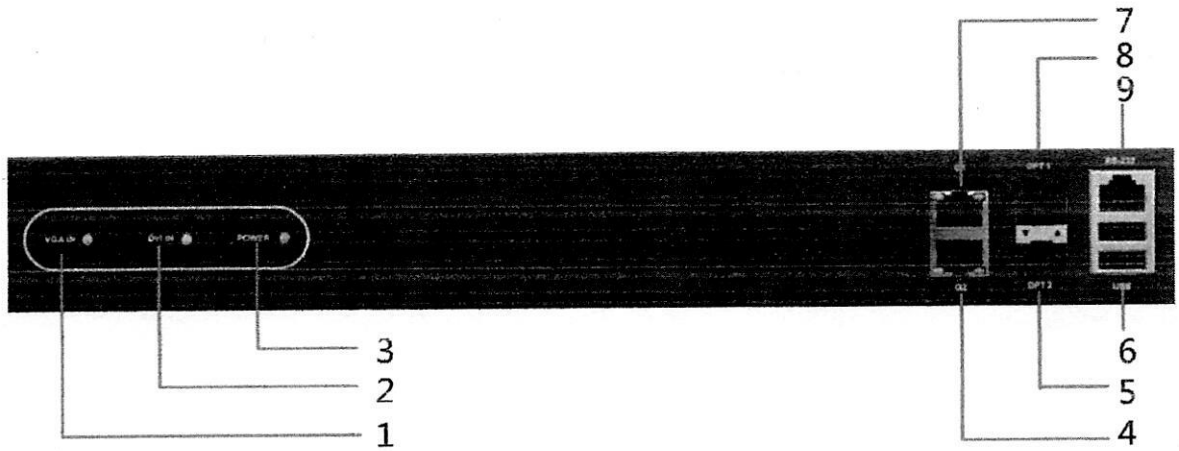


Figure 2-4 Front Panel of DS-6916UDI(B)

Table 2-4 Description of DS-6916UDI(B) Front Panel

No.	LED Indicator & Interface	Description
1	VGA IN	VGA input signal indicator
2	DVI IN	DVI input signal indicator
3	POWER	Power indicator
4	G2	10/100/1000 Mbps Ethernet interface 2
5	OPT2	10/100/1000 Mbps optical interface 2
6	USB	USB 2.0 interface
7	G1	10/100/1000 Mbps Ethernet interface 1
8	OPT1	10/100/1000 Mbps optical interface 1
9	RS-232	Connect to RS-232 devices, e.g., PC, etc.

2.2 Rear Panel

- Rear Panel of DS-6901UDI(B)

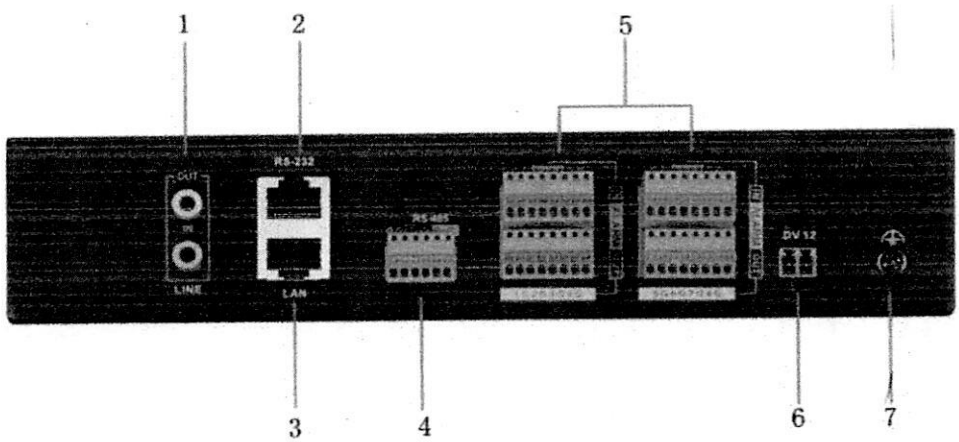


Figure 2-5 Rear Panel of DS-6901UDI(B)

Table 2-5 Description of DS-6901UDI(B) Rear Panel

No.	Interface	Description
1	LINE IN/OUT	Two-way audio input/output, 3.5 mm connector
2	RS-232	Connect to RS-232 devices, e.g., PC, etc.
3	LAN	10/100/1000 Mbps Ethernet interface
4	RS-485	Connect to RS-485 devices, e.g., keyboard, etc.

5	ALARM IN	8 alarm inputs
	ALARM OUT	8 alarm outputs
6	DV 12	Power supply (12 VDC)
7	[redacted]	GND

- Rear Panel of DS-6904UDI(B)

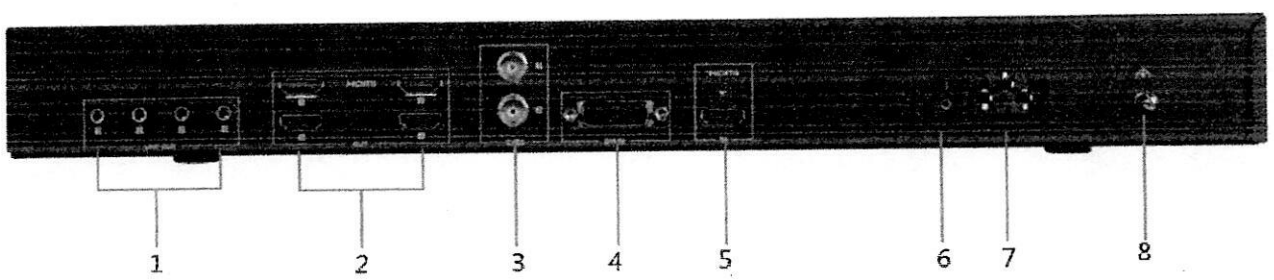


Figure 2-6 Rear Panel of DS-6904UDI(B)

Table 2-6 Description of DS-6904UDI(B)

No.	Interface	Description
1	LINE OUT	BNC connector
2	HDMI OUT	HDMI video output interface
3	CVBS	CVBS video output interface
4	DVI IN	DVI video input interface
5	HDMI IN	HDMI video input interface
6	Power switch	Power on or power off the device
7	Power	Power indicator
8	[redacted]	GND

- Rear Panel of DS-6908UDI(B)

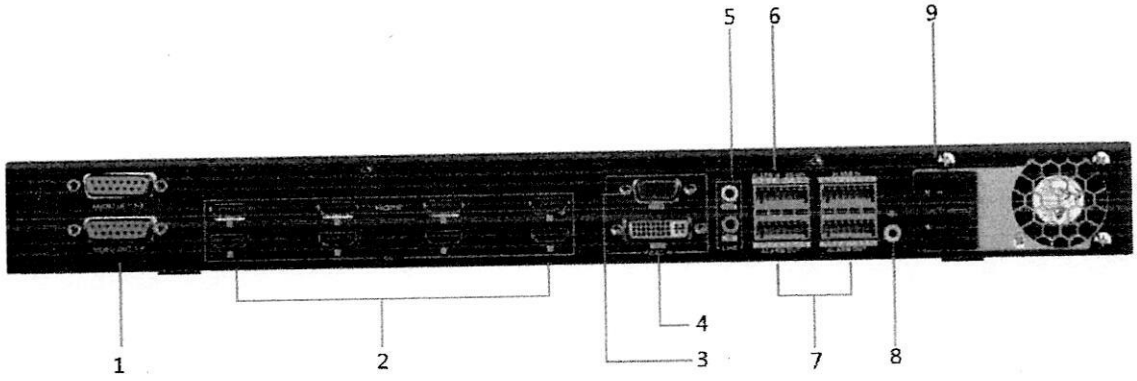


Figure 2-7 Rear Panel of DS-6908UDI(B)

Table 2-7 Description of DS-6908UDI(B) Rear Panel

No.	Interface	Description
1	AUDIO/VIDEO OUT	BNC connector
2	HDMI OUT	HDMI video output interface
3	VGA VIDEO IN	VGA video input interface
4	DVI VIDEO IN	DVI video input interface
5	LINE IN/OUT	Two-way audio input/output, 3.5mm connector
6	RS-485	Connect to RS-485 devices, e.g., keyboard, etc.
7	ALARM IN	8 alarm inputs
	ALARM OUT	8 alarm outputs
8	[redacted]	GND
9	Power	Power input

- Rear Panel of DS-6916UDI(B)

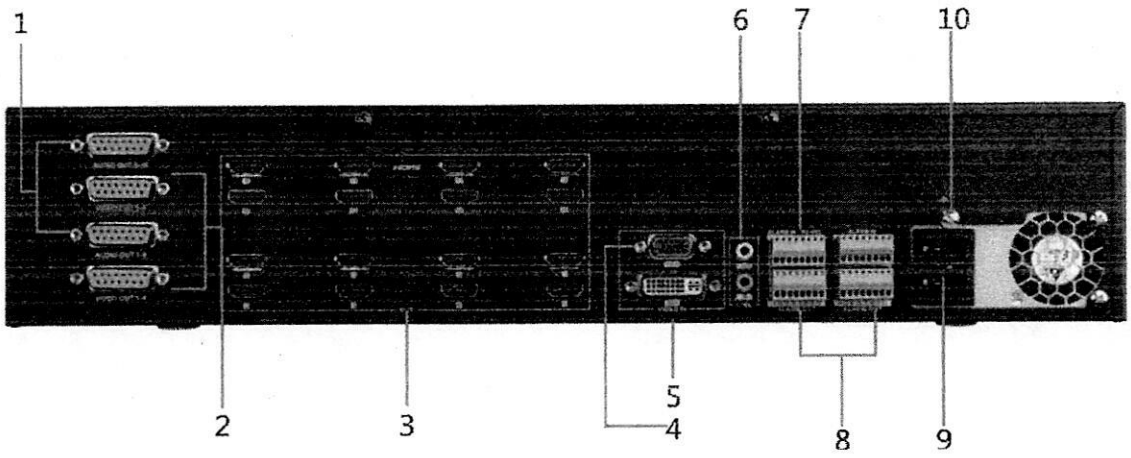


Figure 2-8 Rear Panel of DS-6916UDI(B)

Table 2-8 Description of DS-6916UDI(B) Rear Panel

No.	Interface	Description
1	AUDIO OUT	BNC connector
2	VIDEO OUT	BNC connector
3	HDMI OUT	HDMI video output interface
4	VGA VIDEO IN	VGA video input interface
5	DVI VIDEO IN	DVI video input interface
6	LINE IN/OUT	Two-way audio input/output, 3.5mm connector
7	RS-485	Connect to RS-485 devices, e.g., keyboard, etc.
8	ALARM IN	8 alarm inputs
	ALARM OUT	8 alarm outputs
9	Power	Power input
10	■	GND

NOTE

DS-6910UDI(B) provides 10 HDMI output interfaces, DS-6912UDI(B) provides 12 HDMI output interfaces and other interfaces are the same with DS-6916UDI(B).

Chapter 3 Device Activation

Purpose

You are required to activate the decoder first by setting a strong password for it before you can use the device. You can configure the basic network parameters.

Activation via Web Browser and Client Software are all supported.

NOTE

For the first-time user, the default user name of DS-6900UDI(B) is *admin*, and the default IP address is 192.0.0.64.

3.1 Activating via SADP Software

SADP software is used for detecting the online device, activating the camera, and resetting the password.

Get the SADP software from the supplied disk or the official website, and install the SADP according to the prompts. Follow the steps to activate the camera.

Step 1 Run the SADP software to search the online devices.

Step 2 Check the device status from the device list, and select the inactive device.

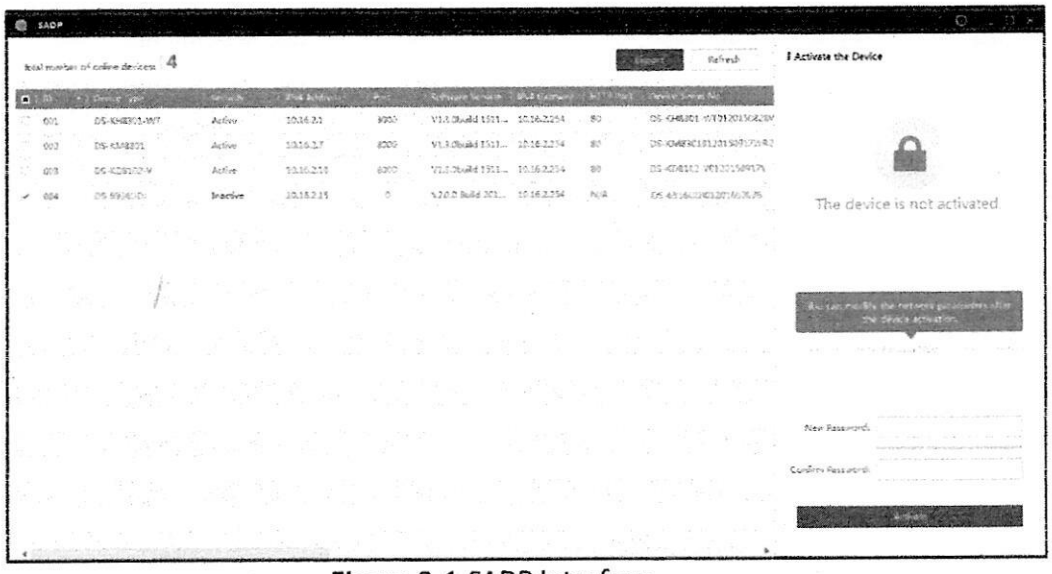


Figure 3-1 SADP Interface

Step 3 Create a password and input it in the password field, and confirm the password.

Step 4 Click **Activate** to activate the device.

WARNING

STRONG PASSWORD RECOMMENDED–We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Step 5 Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.

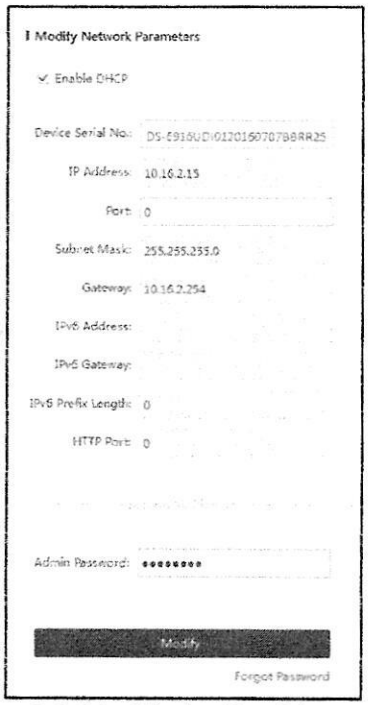


Figure 3-2 Modify the IP Address

Step 6 Input the password and click the **Modify** button to activate your IP address modification.

3.2 Activating via Web Browser

Step 1 Power on the decoder, and connect the decoder to the network.

Step 2 Input the IP address into the address bar of the web browser, and click Enter to enter the activation interface.

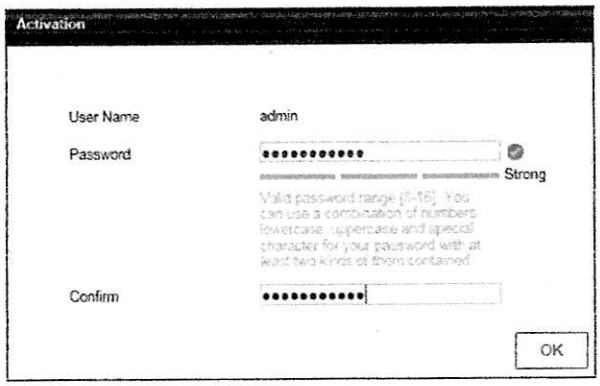


Figure 3-3 Activation Interface

Step 3 Create a password and input the password into the password field.

WARNING

STRONG PASSWORD RECOMMENDED–We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

Step 4 Confirm the password.

Step 5 Click **OK** to save the password and enter the live view interface.

Chapter 4 Network Configuration

NOTE

You shall acknowledge that the use of the product with the Internet access might be under network security risks. For avoidance of any network attacks and information leakage, please strengthen your own protection. If the product does not work properly, contact with your dealer or the nearest service center.

Purpose

You shall configure the basic network, DDNS, and Wi-Fi settings before other operations. In this chapter, the network configuration of the decoder by the Web browser is provided.

NOTE

The tested Web browsers include: IE 8.0+, Chrome 18.0+, Firefox 5.0+, and Safari 5.02+.

Step 1 Open the Web browser and input the IP address of Decoder (e.g., http://192.168.0.0).

Step 2 Log in to the device.

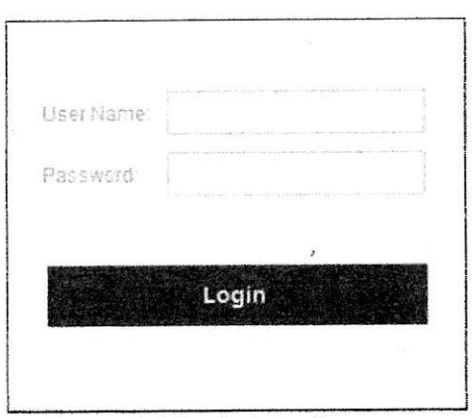


Figure 4-1 Login Interface

- If the device has not been activated, you need to active the device first before login.

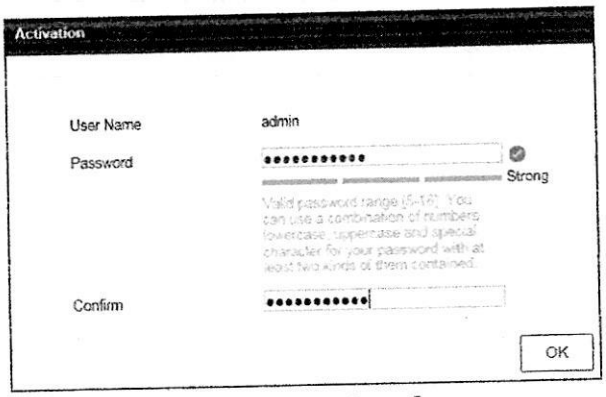


Figure 4-2 Activation Interface

WARNING

STRONG PASSWORD RECOMMENDED–We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters.) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

- If the device is already activated, input the user name and password in the login interface, and click the **Login** button.

The following interface is shown after successful login.

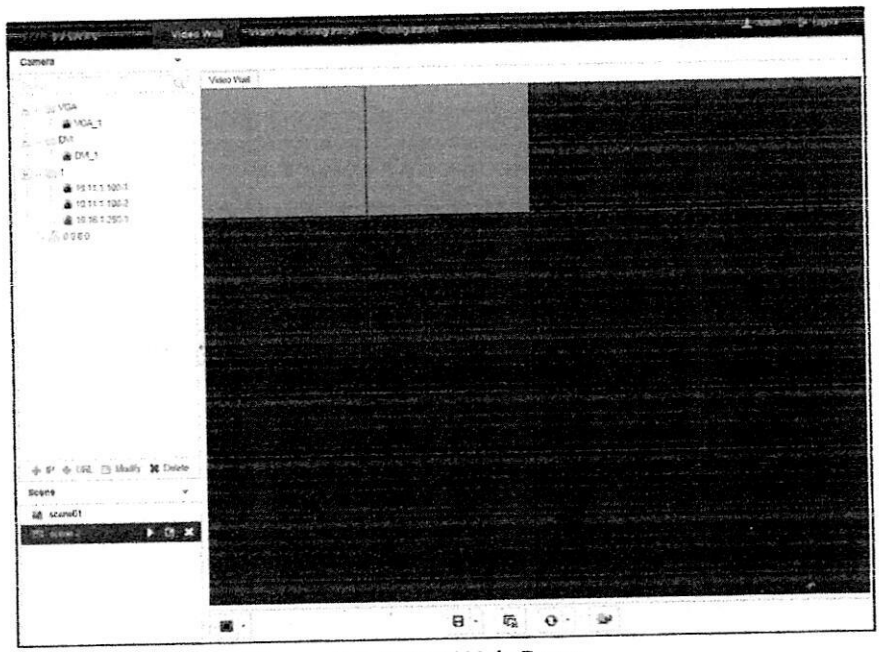


Figure 4-3 Enter Web Page

4.1 Configuring Basic Network Settings

Purpose

You can set the network parameters for the decoder in the parameter configuration interface.

Step 1 Click **Configuration > Network > TCP/IP** to enter the general network settings interface.

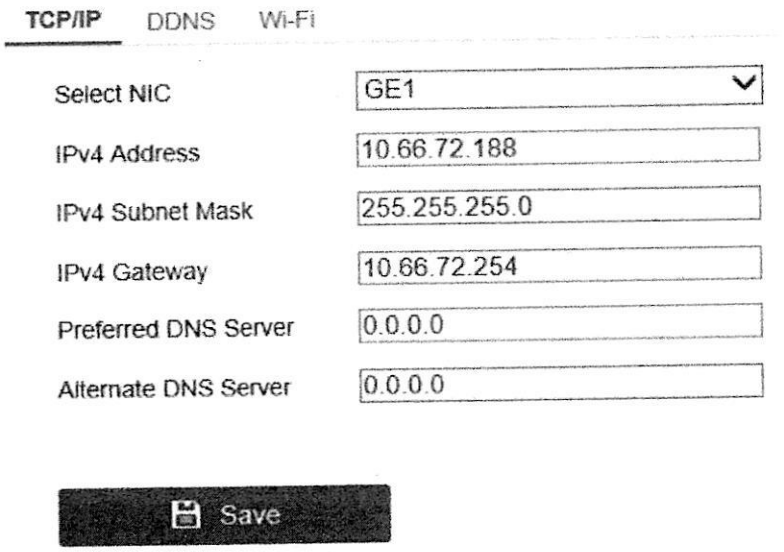


Figure 4-4 Configure Basic Network Settings

Step 2 Set the network parameters, including the NIC, IP Address, Subnet Mask, Gateway, and DNS Server.

NOTE

The DS-6904/6908/6910/6912/6916UDI provides multiple NICs for selection.

Step 3 Click **Save** to save the settings.

4.2 Configuring Security Control

Purpose

You can disable SSH, SADP, or HTTPS to enhance the access security, e.g., when you are in the untrusted network environment.

Step 1 Go to **Configuration > Security Control**.

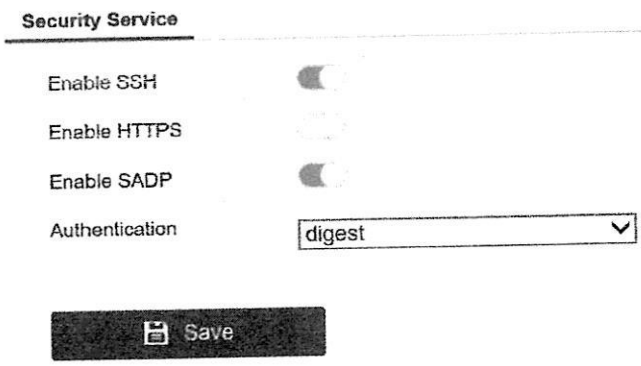


Figure 4-5 Security Service

Step 2 Uncheck **Enable SSH**, **Enable SADP**, or **Enable HTTPS** to disable the services.

NOTE

- By default, SSH is disabled, and SADP and HTTPS are enabled.
- The login user name for SSH is *root*, and the password is the same with that of the admin.

Step 3 Select **Authentication** as **digest** or **digest/basic**. **Digest** is an encryption transmission mechanism, and **basic** is not. Select **digest** to enable the encryption mechanism, and select **digest/basic** to enable both the two mechanism.

Step 4 Click **Save**.

Chapter 5 Decoding Parameters Configuration

5.1 Configuring Stream Settings

Purpose

The stream configuration refers to the auto stream switch between main stream and sub-stream.

Step 1 Click **Configuration > Decoding Configuration > Stream Configuration** to enter stream configuration interface.

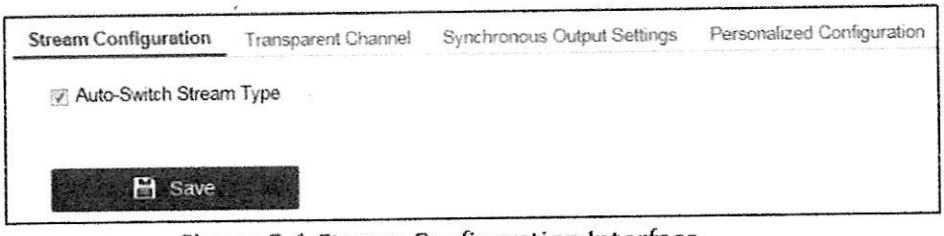


Figure 5-1 Stream Configuration Interface

Step 2 Check the check box of **Auto-Switch Stream Type** to enable auto switch between main stream and sub-stream.

Step 3 Click **Save** button to save the settings.

NOTE

When a screen is split into more than 16 windows, the main stream will automatically switch to sub-stream to lower the bandwidth.

5.2 Configuring Transparent Channel

Purpose

The Transparent Channel refers to the transmission channel used for forwarding data between the decoder and the encoder without operating on the data.

Step 1 Click **Configuration > Decoding Configuration > Transparent Channel** to enter transparent channel settings interface.

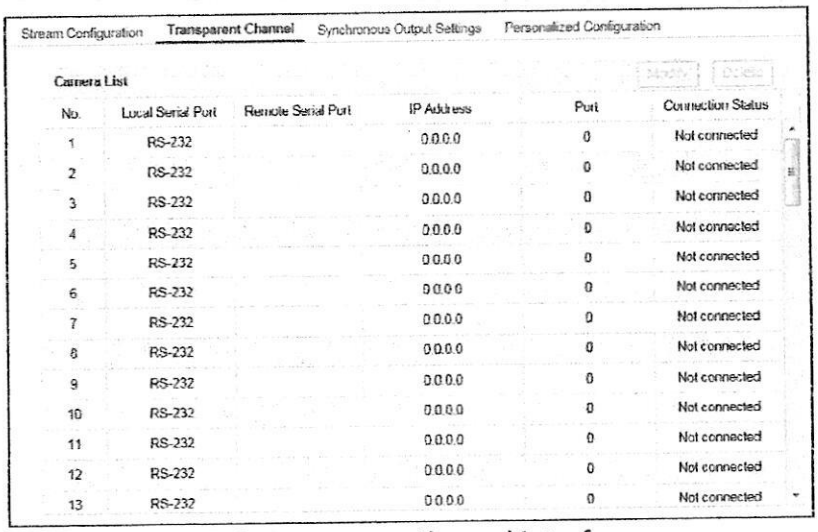


Figure 5-2 Transparent Channel Interface

Step 2 Select a transparent channel from the list to configure.

Step 3 Click **Modify** to modify the parameters of the selected transparent channel.

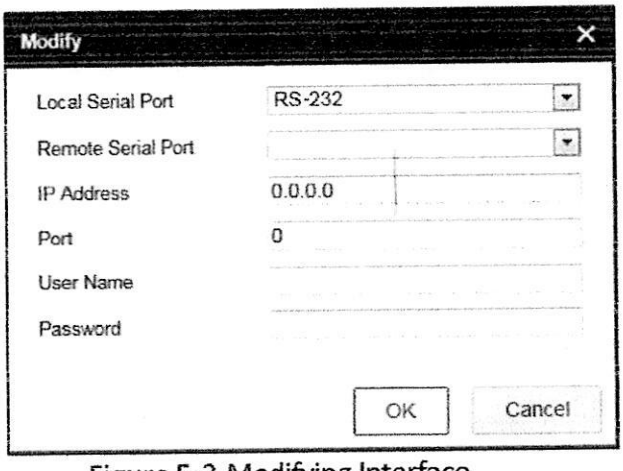


Figure 5-3 Modifying Interface

Step 4 Select the **Local Serial Port** and the **Remote Serial Port** to RS-485 or RS-232.

Local Serial Port: The serial port used as the transparent channel by the decoder.

Remote Serial Port: The serial port used as the transparent channel by the encoding device.

NOTE

You can click **Delete** to delete the selected channel.

5.3 Configuring Synchronous Output Settings

Purpose

All video outputs of the device can be configured to be synchronous.

Step 1 Click **Configuration** > **Decoding Configuration** > **Synchronous Output Settings** to enter the Synchronous Output Settings interface.

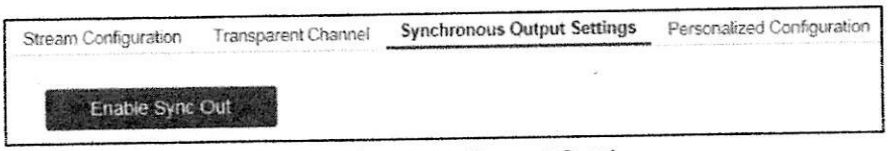


Figure 5-4 Synchronous Output Settings

Step 2 Click the **Enable Sync Out** button to enable the synchronization of all outputs. The following message box pops up.

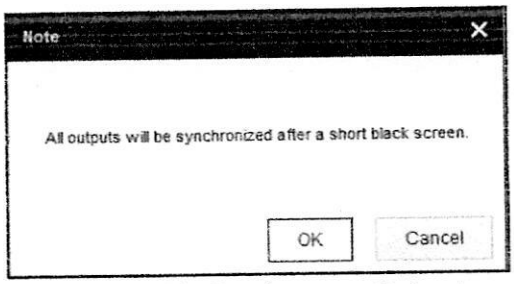


Figure 5-5 Enable Synchronous Output

Step 3 Click **OK** to confirm the settings.

5.4 Configuring Personalized Settings

Purpose

You can set the stopped decoding image and failed streaming image for the personalized configuration.

Step 1 Click **Configuration** > **Decoding Configuration** > **Personalized Configuration** to enter the personalized configuration interface.

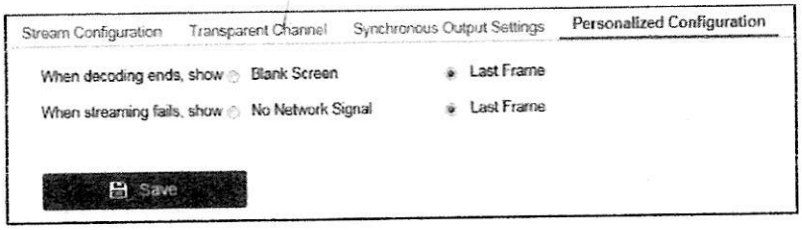


Figure 5-6 Personalized Configuration

Step 2 Select **Blank Screen** or **Last Frame** when decoding ends. If you select **Blank Screen**, the screen will change blank when the decoding ends. If you select **Last Frame**, the screen will show the last frame when the decoding ends.

Step 3 Select **No Network Signal** or **Last Frame** when streaming fails. If you select **No Network Signal**, the screen will show the cause of the failure when streaming fails. If you select **Last Frame**, the screen will show the last frame when streaming fails.

Step 4 Click **Save** to save the settings.

Chapter 6 Decoding Operation

6.1 Configuring Encoding Devices

6.1.1 Adding an Encoding Device

Purpose

You can add an encoding device via IP address or URL.

- **Adding an Encoding Device via IP Address**

Step 1 Click **IP** to add encoding devices.

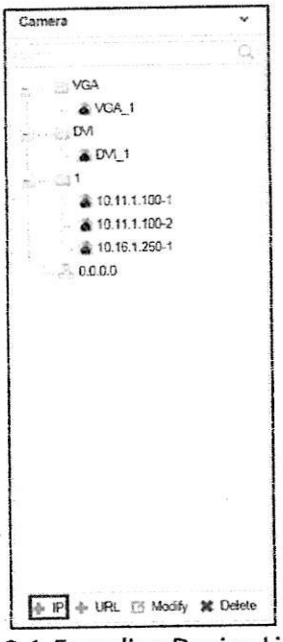


Figure 6-1 Encoding Device List

Step 2 Input **Device Name, Type, Port, User Name, Password** and **Channel Number** and select the **Transmission Protocol, Area Name,** and **Device Manufacturer**. Decide whether to enable **Stream Encryption** and input the encryption password. Check the checkbox of **Get Stream by Stream Media** to lower the network load of the device.

NOTE

- You can add device by IP or DDNS. If you select DDNS, you need to enter the domain name and ensure that you have configured the DNS server. For details, see section 4.1 Configuring Basic Network Settings.
- If **Stream Encryption** is enabled, you need to input the encryption password so you can remotely watch live videos of encrypted camera streams.

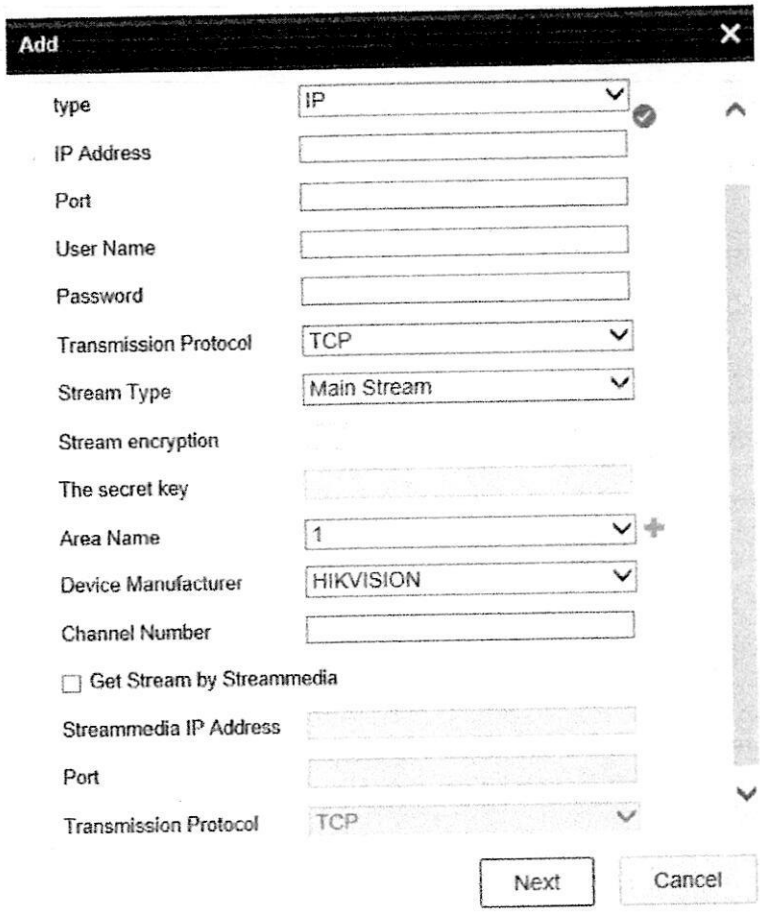


Figure 6-2 Add Device via IP Address

Step 3 (Optional) You can also click ✚ to add a new area and click 🖫 to save the area.

Step 4 Click **Next** to select the channel. The channel(s) displayed here depend(s) on the **Channel Number** you input on the previous page.

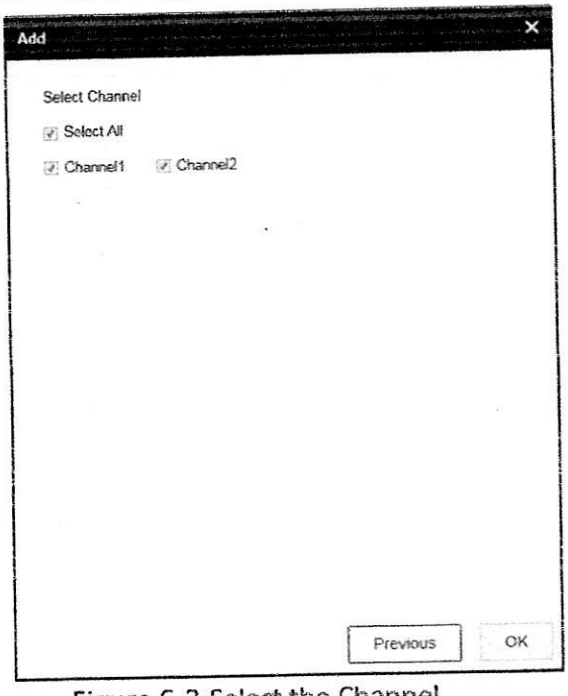


Figure 6-3 Select the Channel

Step 5 Click **OK** to save the settings and add the device.

- **Adding an Encoding Device via URL**

Step 1 Click **URL** to add encoding devices.

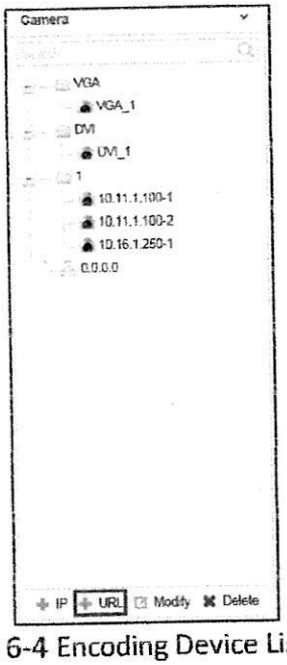


Figure 6-4 Encoding Device List

Step 2 Input the **Device Name** and **URL**. Select the **Area Name** from the dropdown list or click + to add a new area. Decide whether to enable **Stream Encryption** and input the encryption password.

NOTE

- An example of the URL format is as follows:

rtsp://10.9.1.233:554/h264/ch1/main/av_stream/?username=admin?password=hik12345?linkmode=tcp

In the above URL, **10.9.1.233** indicates the device IP, **admin** indicates the user name, **hik12345** indicates the password, and **tcp** indicates the stream transport protocol. The transport protocol can be set as tcp, udp, and mcast.

- If **Stream Encryption** is enabled, you need to input the encryption password so you can remotely watch live videos of encrypted camera streams.

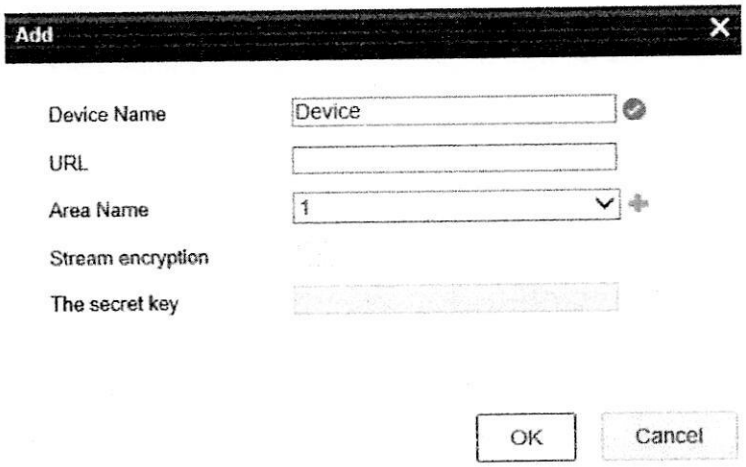


Figure 6-5 Add Device via URL

Step 3 Click **OK** to save the settings.

6.1.2 Modifying an Encoding Device

Step 1 Select one area or one encoding device, and click **Modify** to modify corresponding parameters.

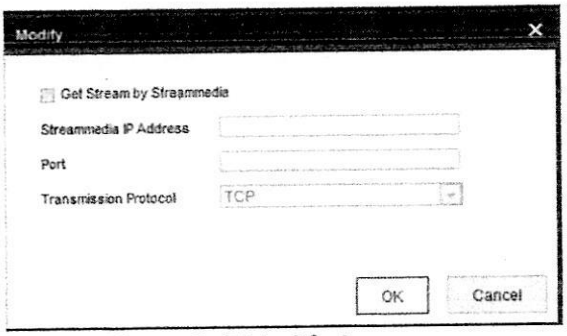


Figure 6-6 Modify Area

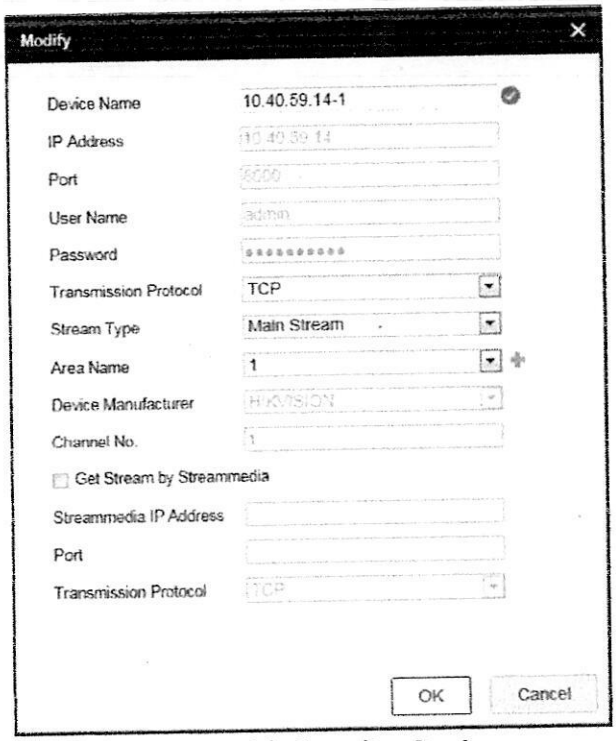


Figure 6-7 Modify Encoding Device

Step 2 Click **OK** to save the new settings.

6.1.3 Deleting an Encoding Device

Step 1 Select one area or one encoding device and click **Delete** to pop up the note interface below.

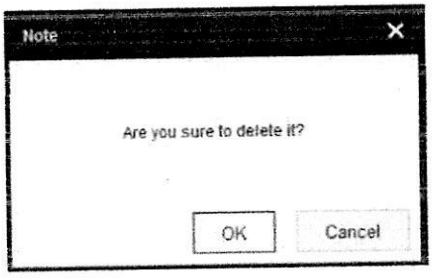


Figure 6-8 Deleting Note

Step 2 Click **OK** to delete it.

6.2 Configuring Video Wall

Purpose

To realize the display of the decoded video on the video wall, you must set the video wall configuration first so as to link the video output with video wall.

Step 1 Click **Video Wall Configuration** to enter the corresponding interface.

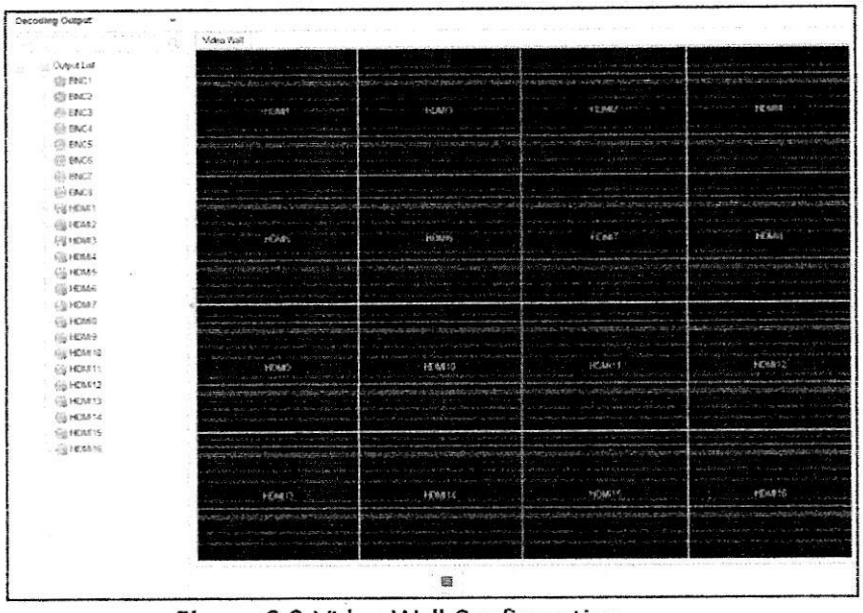


Figure 6-9 Video Wall Configuration

Step 2 You can use the default video wall layout or click to add a new layout. Input the number of screens in row and column and up to 16 × 20 split screens are available.

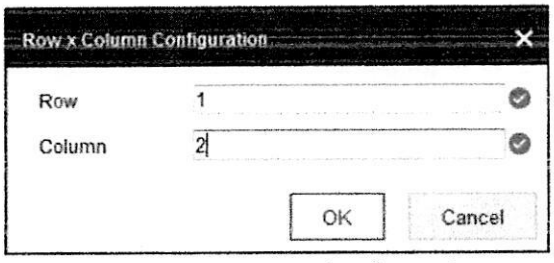


Figure 6-10 Screen Layout Configuration

Step 3 Click **OK** to finish the adding of the video wall information.

Step 4 Drag the output channels from the left-side list to the display screen.

Step 5 Move the cursor to the window, and the icon automatically appears in the upper-right comer of the window. Click to close the window.

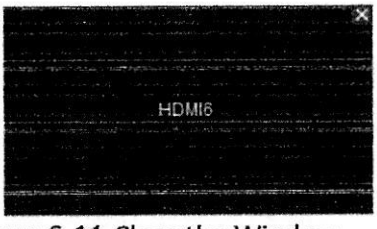


Figure 6-11 Close the Window

6.3 Configuring Decoding Output

Purpose

In the output list, there are two kinds of video output signals, respectively BNC and HDMI. You can configure the resolution and output mode.

6.3.1 Configuring BNC Output

Step 1 Click **Video Wall Configuration** to enter the corresponding interface. Right click one of the BNC signal sources.

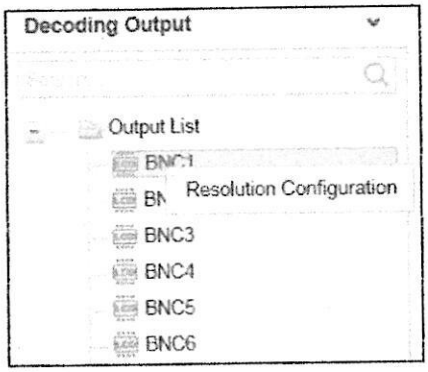


Figure 6-12 BNC Decoding Output

Step 2 Right click one of BNC signal sources and select **Resolution Configuration** to pop up the interface as below.

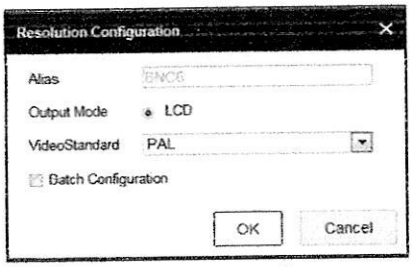


Figure 6-13 Resolution Configuration

Step 3 Select the resolution from the **LCD Resolution** drop-down list. PAL and NTSC are selectable.

Step 4 Check the checkbox of **Batch Configuration** to set the same configuration for other outputs with same signal source.

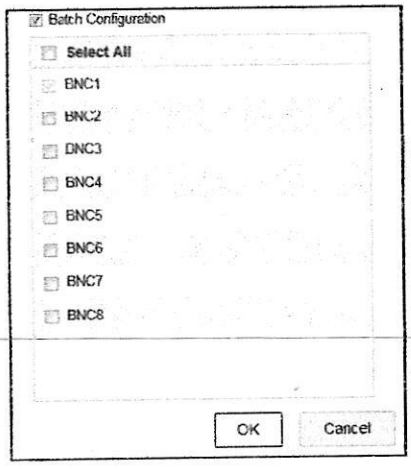


Figure 6-14 Batch Configuration

Step 5 Click **OK** to save the settings.

6.3.2 Configuring HDMI Output

Step 1 Right click one of the HDMI signal sources.

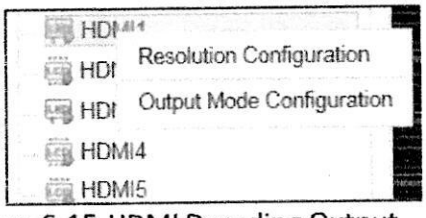


Figure 6-15 HDMI Decoding Output

Step 2 Click **Resolution Configuration** to enter the interface below.

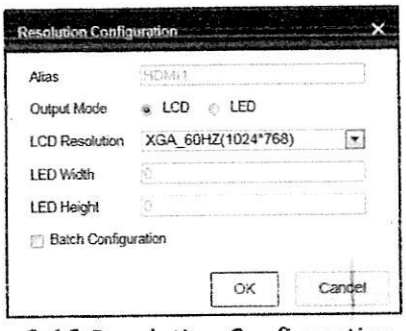


Figure 6-16 Resolution Configuration

Step 3 Select the **Output Mode** and set the corresponding parameters. You can select LCD and LED.

- LCD
  1. Select the **Output Mode** to LCD.
  1. Select the resolution from the **LCD Resolution** drop-down list.

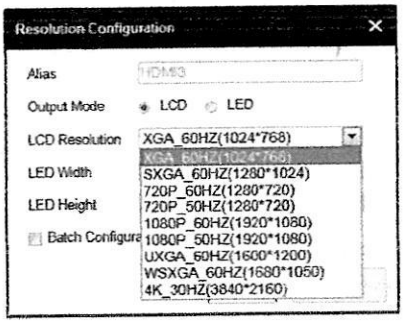


Figure 6-17 Set LCD Resolution

- LED
  1. Select the **Output Mode** to LED.
  1. Input the **LED Width** and **LED Height** in the corresponding text fields.

Figure 6-20 Output Mode Configuration

Step 7 Select the output mode to HDMI or DVI.

Step 8 Check the checkbox of **Batch Configuration** to set the same configuration for other HDMI outputs.

Step 9 Click **OK** to save the settings.

6.4 Decoding Video on Video Wall

Purpose

You can decode the video of the encoding devices on the video wall by dragging the channel directly or opening window via coordinate.

6.4.1 Interface Description

Click **Video Wall** to enter the video wall interface.

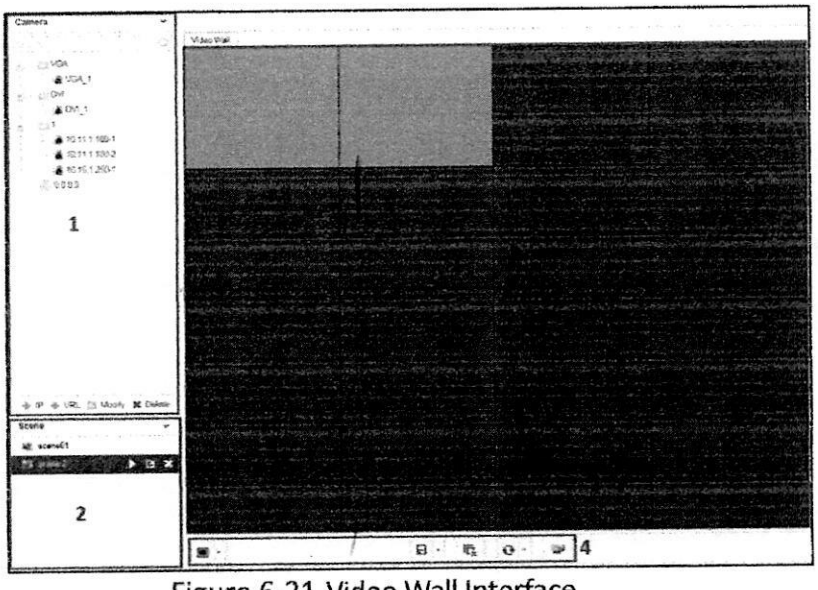


Figure 6-21 Video Wall Interface

Refer to the following figure for the video wall description.

Table 6-1 Description of Video Wall

No.	Description
1	**Encoding Device List:** The encoding devices added in the Web
2	**Scene:** The Web supports up to 8 scenes by default, capable of independent scene configuration and fast switching.
3	**Video Wall:** Video wall operation interface
4	**Shortcut Toolbar:** Select decoding screen layout. Save the scene Delete all windows Refresh all windows If two decoding windows overlap with each other, click the icon to switch the upper window to the bottom.

6.4.2 Dragging Channels to the Video Wall

Step 1 Drag the channel from the left side list to realize the decoding in the selected window.

You can also drag an area file to the video wall to decode the added encoding devices in the area file on the video wall.

NOTE

- You cannot drag an area file to the video wall across the LCD and LED outputs.
- If there are more than 3 encoding devices in an area, when you drag the area file to the video wall, the note pops up to remind you that no more window can be opened or the total area of layers in single-screen has reached the limit. Only the first 3 encoding devices in the area file can be decoded on the video wall.

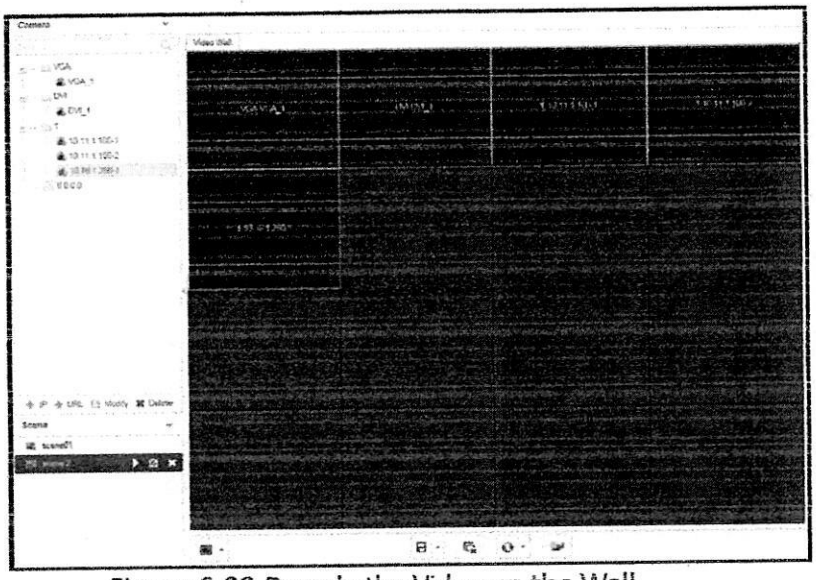


Figure 6-22 Decode the Video on the Wall

Step 2 Select one decoding window and click to set the decoding screen layout.

1/2/4/6/8/9/12/16/25/36 window division modes are available.

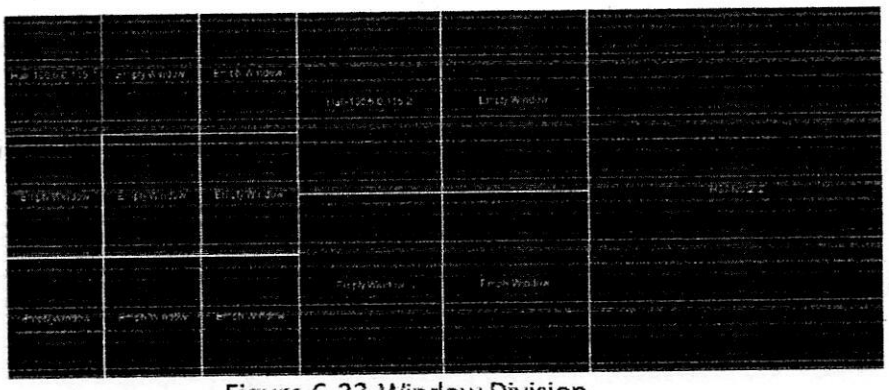


Figure 6-23 Window Division

6.4.3 Openning Window via Coordinate

Step 1 Select one encoding device and right-click it to pop up the interface below.

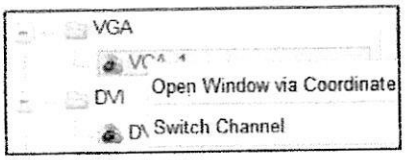


Figure 6-24 Right-Click Menu

Step 2 Click **Open Window via Coordinate.**

Step 3 Select the **Window Opening Mode**. LCD and LED are selectable.

- **Opening Window via Coordinate for LCD Output**

  1) Select the **Window Opening Mode** as **LCD**.

  2) Enter the **Left Margin, Right Margin, Width** and **Height** in the corresponding text fields.

  3) Click **OK** to save the settings.

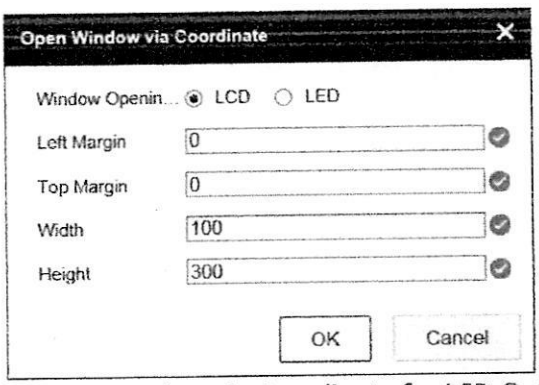


Figure 6-25 Open Window via Coordinate for LCD Output

  4) The window will be opened in the LCD area.

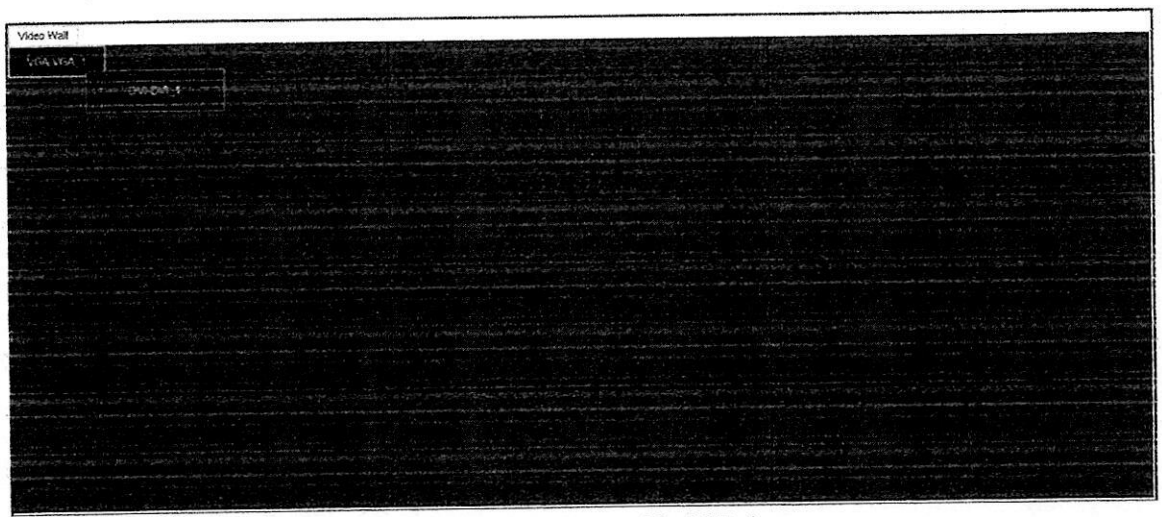


Figure 6-26 Window Opened in LCD Area

- **Opening Window via Coordinate for LED Output**

1) Select the **Window Opening Mode** as **LED**.

2) Select the **LED** area.

   The area number depends on the HDMI decoding output configuration. For the adjacent HDMI outputs, if the resolution is configured to be LED, and the LED width or height is same, they can be seen as one area. You can refer to *Chapter 6.3.2 Configuring HDMI Output*.

3) Enter the **Left Margin**, **Right Margin**, **Width** and **Height** in the corresponding text fields.

4) Click **OK** to save the settings.

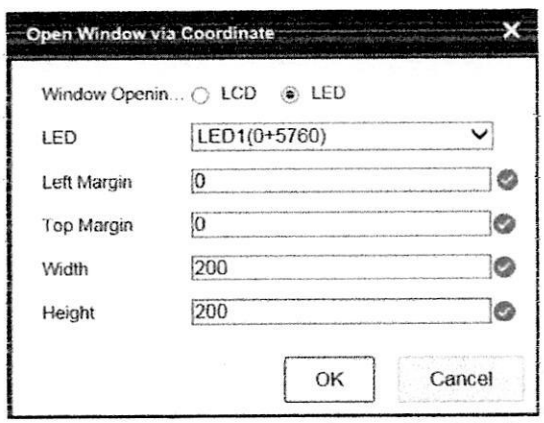


Figure 6-27 Open Window via Coordinate for LED Output

5) The window will be opened in the LED area.

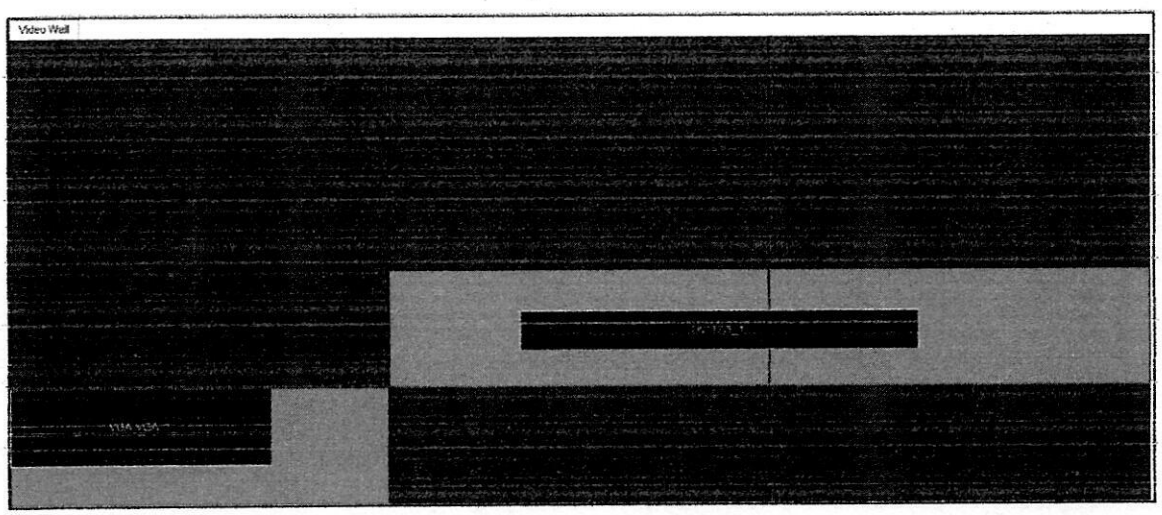


Figure 6-28 Window Opened in LED Area

6.4.4 Managing Decoding

Right-click the selected window and the Decoding Management interface pops up.

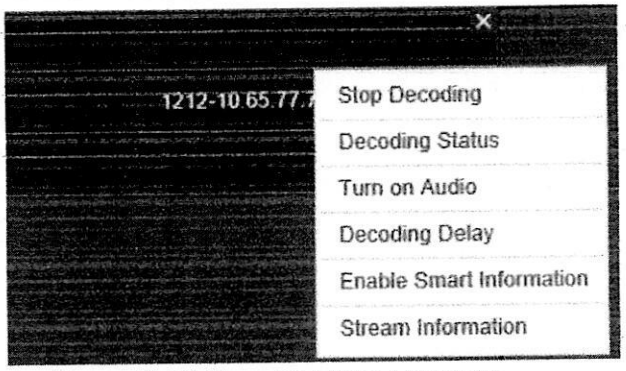


Figure 6-29 Decoding Management

- **Stop Decoding**

  Click the button to stop decoding.

- **Decoding Status**

  1. Click the button to enter the decoding status interface.
  2. View the decoding status.

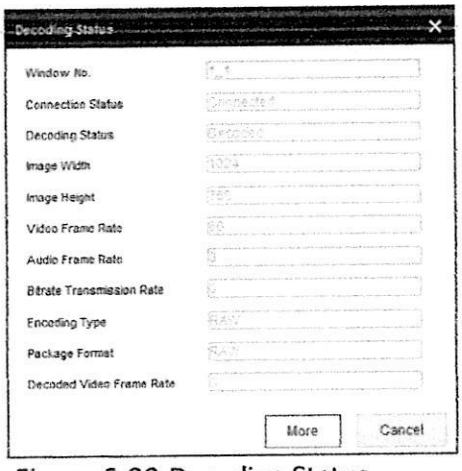


Figure 6-30 Decoding Status

3. Click **More** to check the decoding information of each channel.

Window..	Connection Status	Decoding Status	Image Width	Image Height	Video Frame Rate	Audio Frame Rate	Bitrate Transmission..	Encoding Type	Package Format	Decoded Video Fram...
1_1	Connected	Decoded	1280	720	59	0	0	RAW	RAW	10954
2_1	Connected	Decoded	1280	720	59	0	0	RAW	RAW	10446
3_1	Not connected	Not decoded	0	0	0	0	0	UNKNOWN	UNKNOWN	0
4_1	Not connected	Not decoded	0	0	0	0	0	UNKNOWN	UNKNOWN	0

Figure 6-31 Check More Decoding Status Information

- **Turn on Audio**

  1. Click the button to enter the interface below.

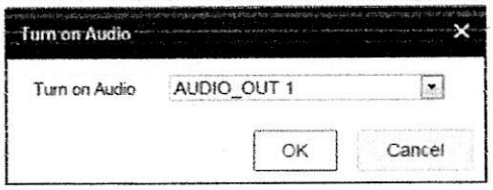


Figure 6-32 Turn on Audio

2. Select from the dropdown list to enable the audio in the corresponding window.
3. Click **OK** to save the settings.

- **Decoding Delay**

1. Click the button to enter the decoding delay interface.
2. Select the type of decoding delay. The default mode is the same with medium real time and fluency.

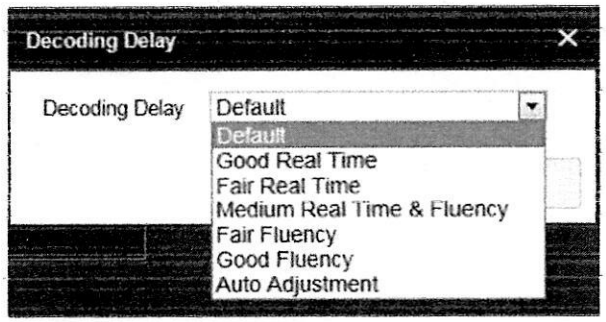


Figure 6-33 Decoding Delay

3. Click **OK** to save the settings.

- **Enable Smart Information**

1. Click the button to enable smart information.
2. (Optional) Click **Disable Smart Information** to disable the function.

NOTE

For the normal IP camera, the smart information refers to the VCA information. For the thermal network camera, the smart information refers to the VCA and the temperature, dynamic fire source detection and ship detection information.

- **Stream Information**

Click the button to view stream information such as host name and transport protocol.

6.4.5 Switching Encoding Channel

Purpose

You can switch the encoding channel to display on the selected decoding window.

Step 1 Select a decoding window and select an encoding channel from the left side list.