

USB 3.0 Area Scan Camera

User's Manual








Foreword

General

This manual introduces the functions and operations of the USB 3.0 area scan camera (hereinafter referred to as "the camera").

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	July 2021

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and car plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The contents of this manual are for reference only, and timely update cannot be guaranteed. Slight differences might be found between the manual and the product. If you have any questions, please contact the technical support of the corresponding area.
- We are not liable for losses incurred due to operating the product in ways that are not in

compliance with the manual.

- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section describes the contents covering proper handling of the device, hazard prevention, and prevention of property damage. Read these contents carefully before using the device, comply with them when using, and keep the manual well for future reference.

Operation Requirements

- Transport, use and store the device under allowed humidity and temperature conditions.
- Prevent liquids from splashing or dripping on the device. Make sure that there are no objects filled with liquids on top to avoid liquids flowing into the device.
- Do not disassemble the device.
- Only use the device within the rated power range.
- Make sure that the power supply of the device works properly before use.
- Do not pull out the power cable of the device while it is powered on.

Installation Requirements

- Observe all safety procedures and wear required protective equipment provided for your use while working at height.
- Do not expose the device to direct sunlight or heat source.
- Do not install the device in humid, dusty or smoky places.
- Install the device in a well-ventilated place, and do not block the ventilator of the device.
- Strictly abide by local electrical safety standards, and make sure that the voltage in the area is steady and conforms to power requirements of the device.
- Use the power adapter or case power supply provided by the device manufacturer.
- Connect the device with the adapter before power on.
- Do not connect the device to more than one power supply. Otherwise, the device might be damaged.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and no higher than PS2. Note that power supply requirements are subject to the device label.
- Connect the class I electrical appliance to a power socket with protective earthing.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Product Information	1
1.1 Overview	1
1.2 Highlight	1
1.3 Typical Networking Topology.....	1
1.4 Operating Environment.....	1
2 Installation	2
2.1 Downloading the Client	2
2.2 Connecting Camera	2
3 Function Parameter	4
3.1 Frame Rate.....	4
3.1.1 Influential Facts for Frame Rate	4
3.1.2 Frame Rate.....	4
3.2 Acquisition mode.....	5
3.3 Trigger Mode.....	6
3.3.1 Trigger Type.....	6
3.3.2 Trigger Source	7
3.4 Flat Field Correction	8
3.5 Trigger Delay	10
3.6 Output Signal	10
3.7 IO Feature.....	11
3.7.1 Two-way I/O Circuit.....	11
3.7.2 Opto-isolated Input	13
3.7.3 Opto-isolated Output.....	13
3.8 IO Smoothing	15
3.9 Black Level	15
3.10 Gain.....	16
3.10.1 Analog Gain.....	16
3.10.2 Digital Gain	17
3.11 White Balance.....	17
3.12 Gamma	18
3.13 Testimage (Test Mode).....	19
Appendix 1 Cybersecurity Recommendations	20

1 Product Information

1.1 Overview

The USB 3.0 area scan camera adopts high performance photosensitive chip and transmits non-compressed image data through USB data port. It complies with USB Vision protocol and GenICam standard. Meeting the requirements of most industrial applications, the camera can work stably in various poor environments, which makes it an industrial camera with high stability at low cost. You can configure parameters and collect data by MV Viewer client.

1.2 Highlight

- Global shutter and rolling shutter CMOS.
- Strong ISP algorithm supported.
- FPN correction is available on certain models.
- High image quality.
- High performance at low cost.
- Shutter mode and global reset are available on certain models.
- Color camera supports interpolation, white balance, color correction matrix, chromaticity and saturation.
- Outputs multiple image data formats such as ROI, Binning and mirror.
- Conform to CE, FCC, UL and RoHS.
- Global shutter high frame rate CMOS models, Global shutter high quality CCD models.
- CCD supports static correction, dynamic fusion, image quality enhance by algorithm and Smear inhibition.
- CMOS supports FFC.
- Defective pixel correction. Custom defective data import is available.
- Wide voltage input meets USB Vision V3.0 protocol and GenICam

1.3 Typical Networking Topology

For industrial cameras, the most typical networking method is point-to-point, which means that between the host and the camera, there is no network media but only a USB cable.

One host can connect to multiple cameras through multiple USB ports or switches.

Figure 1-1 Typical Networking Topology



1.4 Operating Environment

- Operating temperature: -30°C to 50°C (-22°F to $+122^{\circ}\text{F}$).
- Operating humidity: 20%–80% (non-condensing).
- Storage temperature: -30°C to $+80^{\circ}\text{C}$ (-22°F to 176°F).
- Storage humidity: 20%–80% (non-condensing).
- Install the camera indoor on stable surface with reasonable dissipation space around it.
- Air circulation ensured.

2 Installation

2.1 Downloading the Client

Log in to <http://download.huaraytech.com/pub/sdk/>, download and install MV Viewer onto your PC.

2.2 Connecting Camera

Step 1 Open MV Viewer to configure and operate on the camera.

Step 2 Click all attributes to start configuration.

Figure 2-1 Main interface

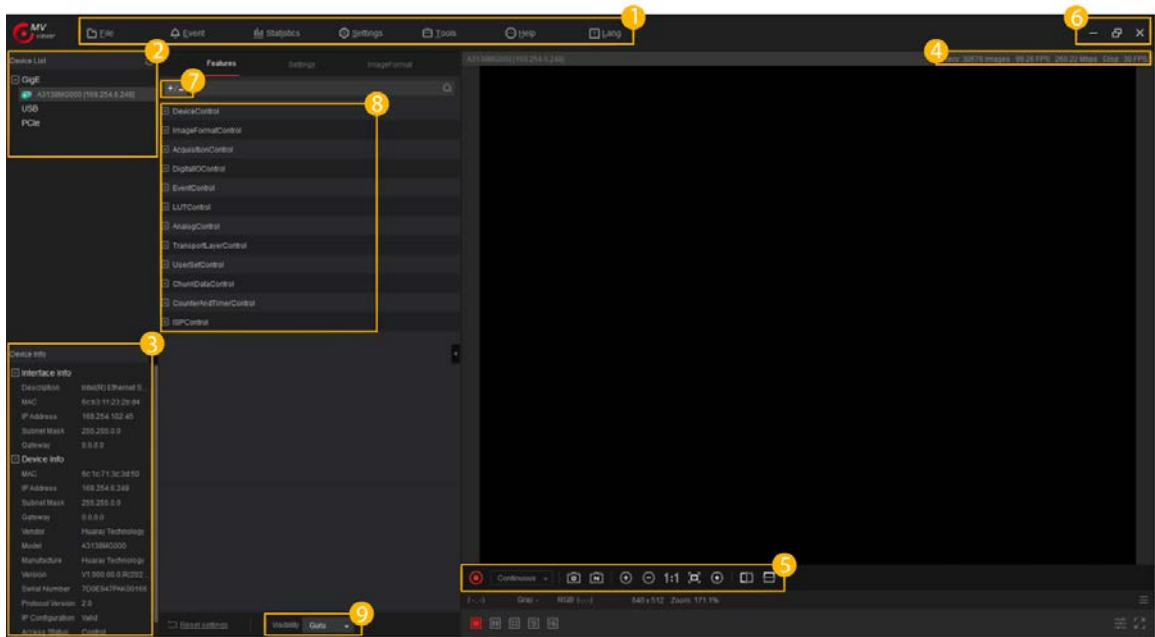





Table 2-1 Parameter description

No.	Parameter	Description
1	Menu	See Table 2-2 for details.
2	Device list	Includes GigE, USB, CameraLink and PCIe cameras.
		 : Click the icon to manually refresh the online device information.
		 : Device to be connected.
		 : Device is connected. MV Viewer can only connect and operate on one camera at a time.
3	Device information	Interface information and device information of the selected device.
4	Image configuration	Includes video stream, image stream, display stream, image position, gray level and RGB value.

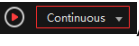










No.	Parameter	Description
5	Tool bar	 : Play/stop. Click ▾ and select play mode among continuous, single frame and multiple frames as needed.  You can only select play mode when the video is paused.  : Save single or multiple frames of images.  : Zoom in or out the image.  : Displays the image in 1:1 ratio or as the window size.  When the image is zoomed in or out, click  can restore the image to windows size.  : The mirror of image in the vertical or horizontal direction.
6	Window operation menu	 : Maximize/restore/minimize the image window.  : Close MV Viewer.
7	Parameter information	 : Display or hide all function parameter information.
8	Function parameters	Select and configure specific function parameters.
9	Operation level	Click ▾ to select characters among Beginner , Expert or Guru from the drop-down list as needed. Each character corresponds to slightly different sets of parameters.

Table 2-2 Menu parameter description

Menu		Description
File	Open File	Select File > Open File , and then select a file, click Open .
	Open Recent	Select File > Open Recent , 10 files which have been opened recently are displayed. Click one file to open it.
	Save	Save the changes of the current file.
	Save as	Save the current file to a different path with a different name.
Event	Event	Notifications for events such as device parameter update, event message channel and stream cache.
Statistics	Statistics	Integrates data such as the configured collection frame rate, bandwidth, number of received images, frame loss rate and number of error images.

3 Function Parameter

This section takes on the functions of the industrial camera.



- Industrial cameras support 3 user levels, including Beginner, Expert and Guru. Each corresponds to slightly different sets of parameters.
- Grayed out parameters cannot be changed under the current running mode.

3.1 Frame Rate

Frame rate, in area scan cameras, indicates the number of images the camera outputs every second.

3.1.1 Influential Facts for Frame Rate

- Bandwidth: The bigger the bandwidth, the bigger the transmission data volume and the higher the frame rate.
- Pixel format: Different pixel formats takes up different amount of storage. Under the same environment, the more storage is occupied, the lower the frame rate becomes.
- Image resolution: Relates to the camera sensor features, affected by the image size as well. With the smaller image size, the frame rate gets higher.
- Exposure time: The longer the exposure time, the lower the frame rate.

3.1.2 Frame Rate

- **AcquisitionFrameRateEnable** is the parameter for enabling frame rate acquisition. **True** means enable and **False** means disable.

Figure 3-1 Configure frame rate

AcquisitionFrameRate	1.00000 Hz
AcquisitionFrameRateEnable	True
	False
	True

- **AcquisitionFrameRate** defines capture rate of frames.
- **ResultingFrameRateAbs** defines the largest speed of capturing frames allowed.



When the value of **AcquisitionFrameRate** exceeds that of **ResultingFrameRateAbs**, the camera captures images at the frame rate of **ResultingFrameRateAbs** value. Opposite of that, the camera captures images at the frame rate of **AcquisitionFrameRate** value.

Figure 3-2 Frame acquisition rate

Features		Settings	ImageFormat
AcquisitionFrameCount	1		
AcquisitionFrameRate	600.00000 Hz		
AcquisitionFrameRate...	False		
AcquisitionStatusSelector	FrameTriggerWait		
AcquisitionStatus	False		
TriggerSelector	FrameStart		
TriggerMode	Off		
TriggerSoftware	{Command}		
TriggerSource	Software		
TriggerActivation	{Not Available}		
TriggerDelay	0.00000 us		
TriggerMultiplier	100		
LightTriggerDelay	0.00000 us		
ExposureMode	Timed		
ExposureTargetBrightn...	50		
ExposureAuto	Off		
ExposureTime	1,000.00000 us		
ResultingFrameRateAbs	439.81177 Hz		

3.2 Acquisition mode

Acquisition mode of the camera includes **Continuous**, **Single Frame** and **MultiFrame**. Configurations are as follows.

Figure 3-3 Acquisition mode settings

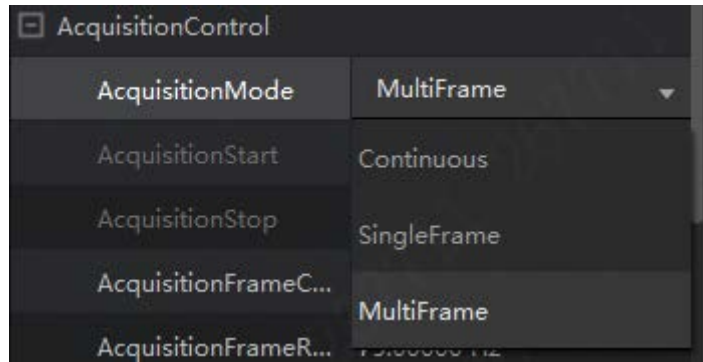


Table 3-1 Description of acquisition mode parameters

Parameter	Working Principle
Single Frame	The camera starts capturing and stops after one capture.
Continuous	<ul style="list-style-type: none"> The camera starts and keeps capturing. Manual operation is required for stopping the capture.
MultiFrame	<p>You can set the number of frames to be captured in AcquisitionFrameCount (1–255).</p> <ul style="list-style-type: none"> The camera starts and keeps capturing. You can manually stop capturing before the set volume is reached.

AcquisitionFrameCount needs to be configured for **MultiFrame**. Enter a reasonable number as needed.

3.3 Trigger Mode

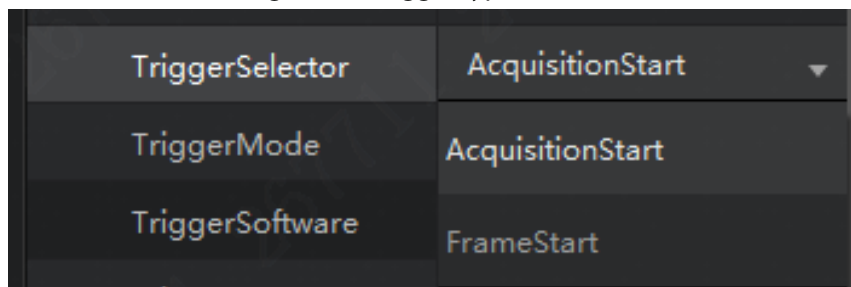
The trigger mode of the camera includes **SoftwareTrigger** (software trigger) and **LineN** (hardware trigger).

3.3.1 Trigger Type

Select **FrameStart** (frame trigger) or **AcquisitionStart** (image capture trigger) under **TriggerSelector**.

- **FrameStart**: Single frame capture. One trigger signal captures one frame.
- **AcquisitionStart**: Continuous capture. One signal triggers continuous captures.

Figure 3-4 Trigger type



3.3.2 Trigger Source

- Software trigger: Trigger signal comes from software.
- Hardware trigger: Trigger signal comes from external devices through I/O port. For the detailed number of signal channels for each camera I/O port, refer to the electrical specifications of the camera.



Specified 6-pin cable is recommended.

Figure 3-5 Electrical Specification

Definitions of camera 6-pin ports:

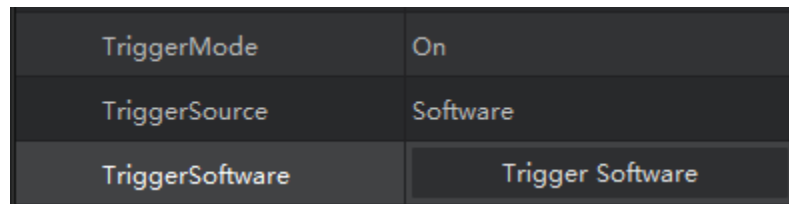
Color	Pin	Description	Features
Blue	1	-	+9VDC to 24VDC power supply
Red	2	Line1	Opto-isolated input
Gray	3	Line2	GPIO (I/O can be configured for non-isolated software) ¹
Black	4	Line0	Opto-isolated output
Green	5	-	Opto-isolated signal ground (ISO_GND)
Brown	6	-	Camera DC power ground and GPIO signal ground (GND)

Step 1 Enable **TriggerMode**.

Step 2 Set **TriggerSource** to **Software**.

Each click on **TriggerSoftware** gets a frame.

Figure 3-6 Software trigger



Step 3 (Optional) Set **TriggerSource** to **LineN**.

Each trigger signal from external devices gets a frame.

Step 4 When hardware trigger is enabled, you can select trigger signal through **TriggerActivation**.

- RisingEdge: Triggered by signal rising edge.
- FallingEdge: Triggered by signal falling edge.

Step 5 You can send the trigger signal as needed after setting the trigger source.

Figure 3-7 Trigger source



3.4 Flat Field Correction

The image quality can be affected by uneven light, fixed-pattern noise of the sensor and noise of uneven responses during using the area scan cameras. FFC (Flat Field Correction) is needed for these situations.

It is mainly for ensuring image balance when applied to area scan cameras.

FFC works by combination of 3 corrections.

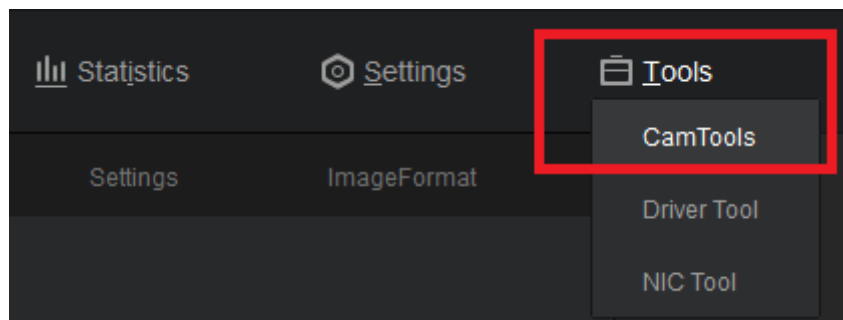
- In dark field, correct fixed-pattern noise.
- In Bright field, correct uneven response.
- In Bright field, correct uneven lens or light.



The ratio between the maximum and the minimum brightness of the image which needs FFC cannot exceed 2.

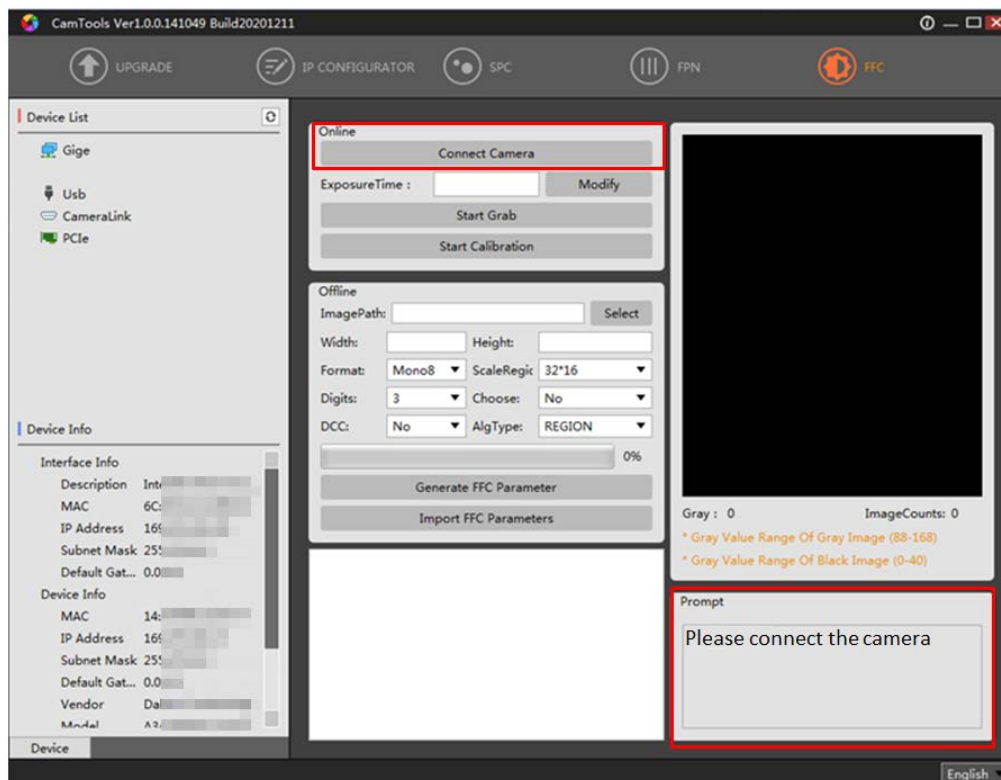
Step 1 Select **Tools > Camtools** on the top.

Figure 3-8 Camera tools



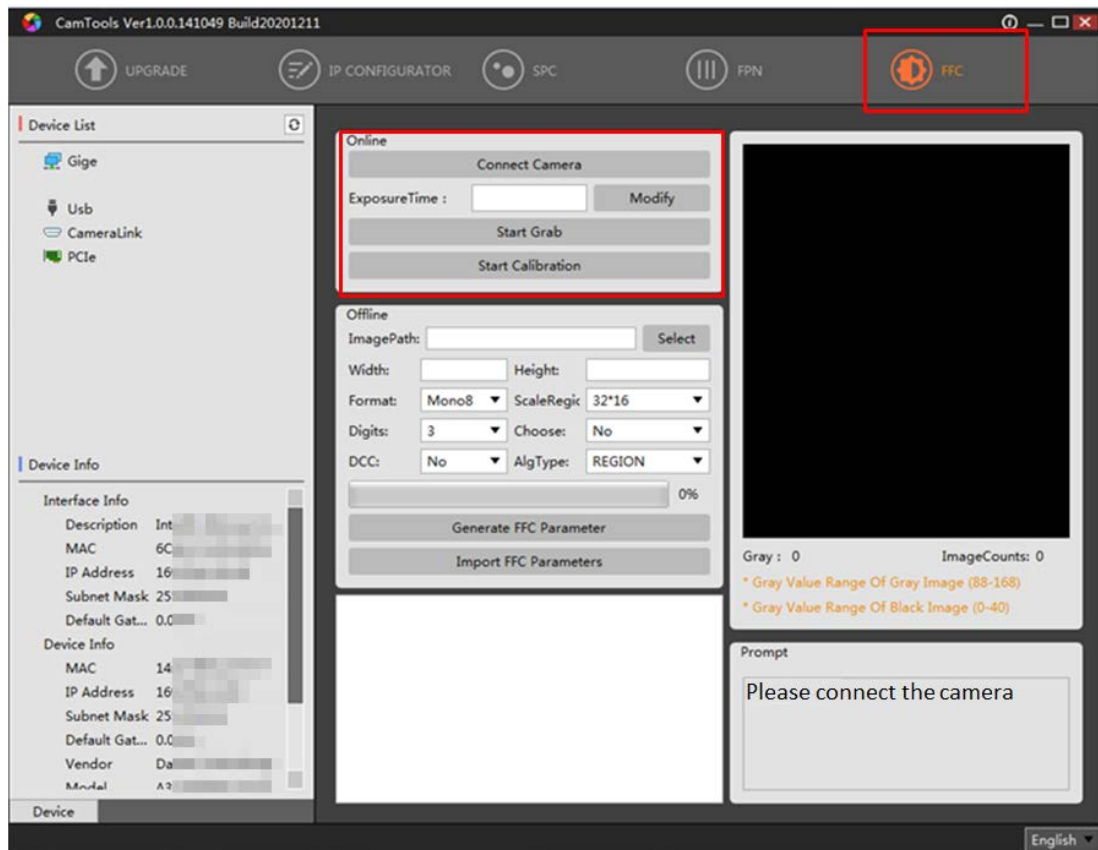
Step 2 Click **FFC** at the upper-right corner.

Figure 3-9 FFC interface



Step 3 After entering the FFC interface, there will be step-by-step instructions prompting at the lower-right corner.

Figure 3-10 FFC operation

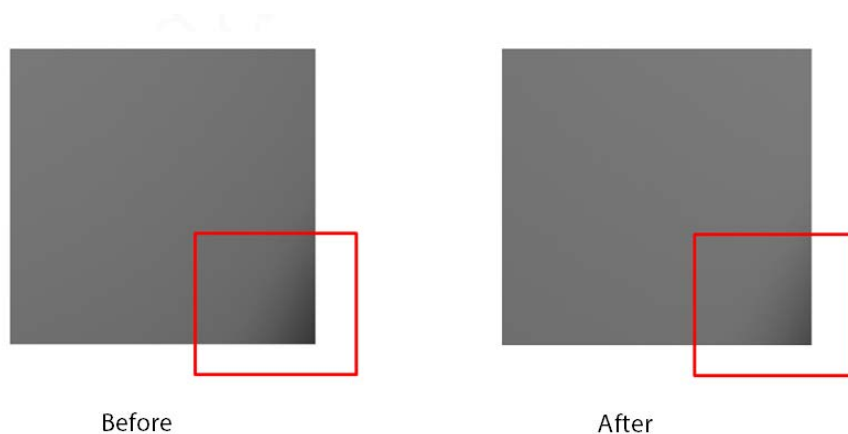


Step 4 Follow the on-screen instructions to complete FFC.

Step 5 **FFCEnable** dialog box pops up after completing online FFC with ON/OFF option for you to disable it.

Step 6 After the correction, you can see the difference on the brightness of the dark part of the image.

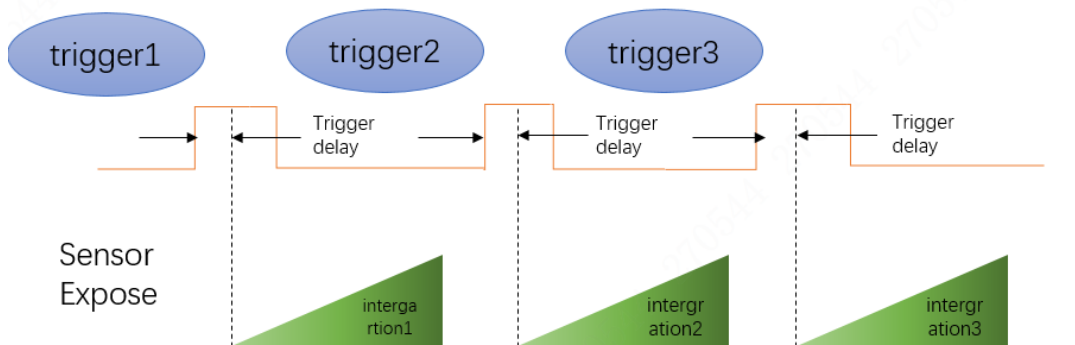
Figure 3-11 Correction effect



3.5 Trigger Delay

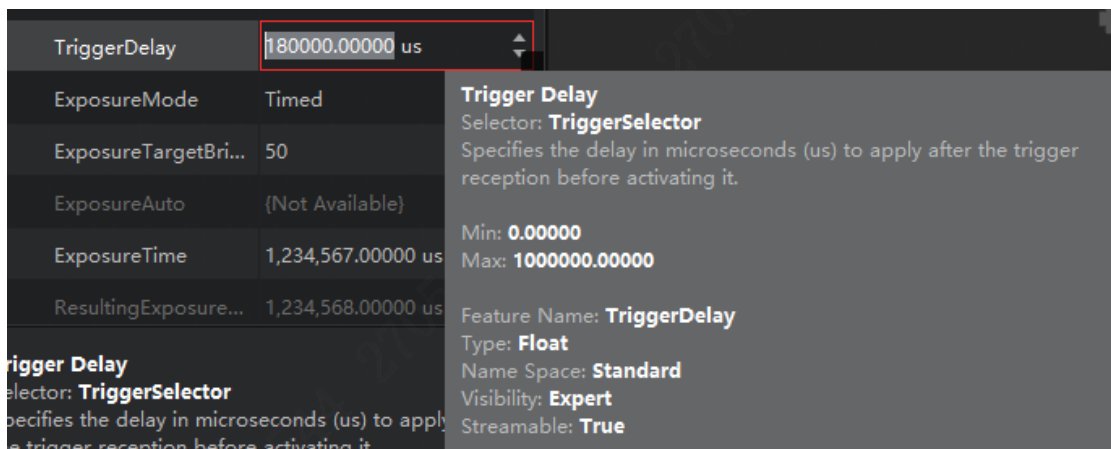
You can set delay time from the camera receiving the trigger signal to responding to the signal to capture.

Figure 3-12 Principle of trigger delay



The trigger signal is rising edge in the following figure. The delay time is configured through **Trigger Delay** with μs as unit and ranges from $0 \mu\text{s}$ – $1000000 \mu\text{s}$, namely, 0 s – 1 s .

Figure 3-13 Configure trigger delay



3.6 Output Signal

USB camera contains one opto-isolated output **Line 0** and one **Line 2** which can be set to input or output.

Step 1 Under **Digital IO Control**, set **Line 2** as **Line Selector**.

Step 2 Set **Line Mode** to **Output**.

Figure 3-14 Set output signal Line2



The output signal triggered by the camera can be used as switch on/off signal to control external devices such as alarm light, light source and PLC. Trigger signal can be sent out through electrical level reversal and **Output** signal. Configure parameters by **Digital IO Control**.

3.7 IO Feature

3.7.1 Two-way I/O Circuit

Line2 is a bidirectional I/O which can be used as input or output signal.



- The external circuit must be able to input up to 2 mA sink current with voltage under 0.8 VDC. No more than 100 uA sink current for high level input.
- Up to 50 mA sink current when the IO port is used as output.

Figure 3-15 GPIO input

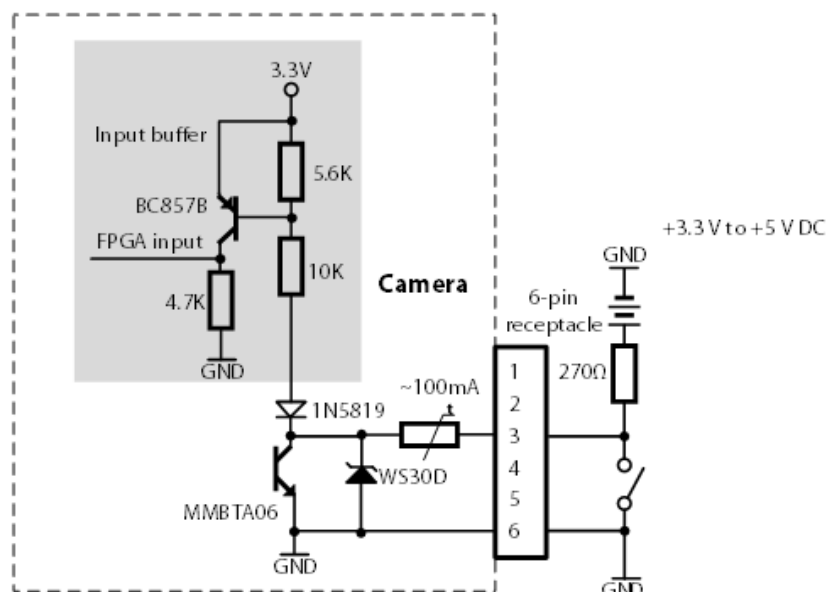


Figure 3-16 5 VTTL logic level input circuit

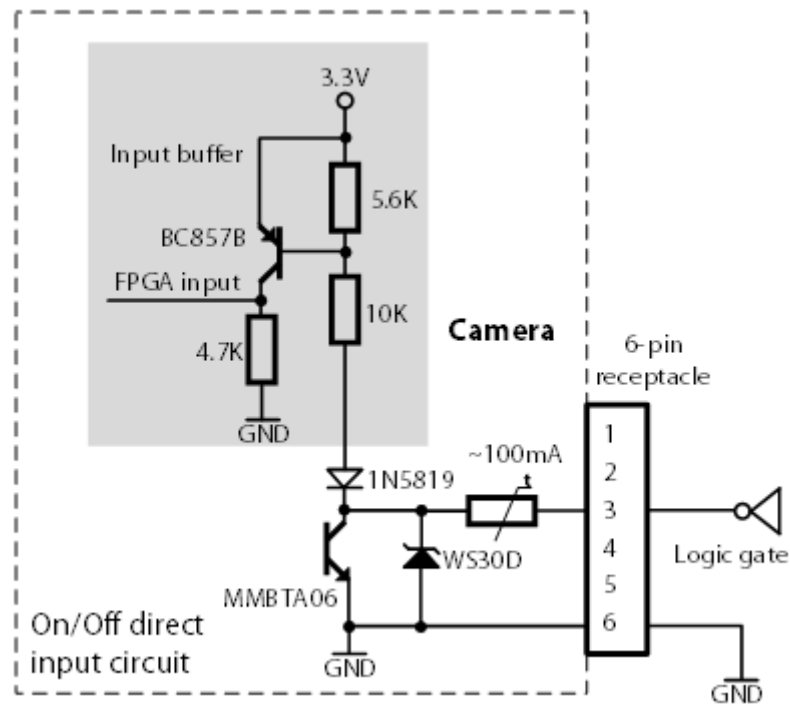


Figure 3-17 GPIO output

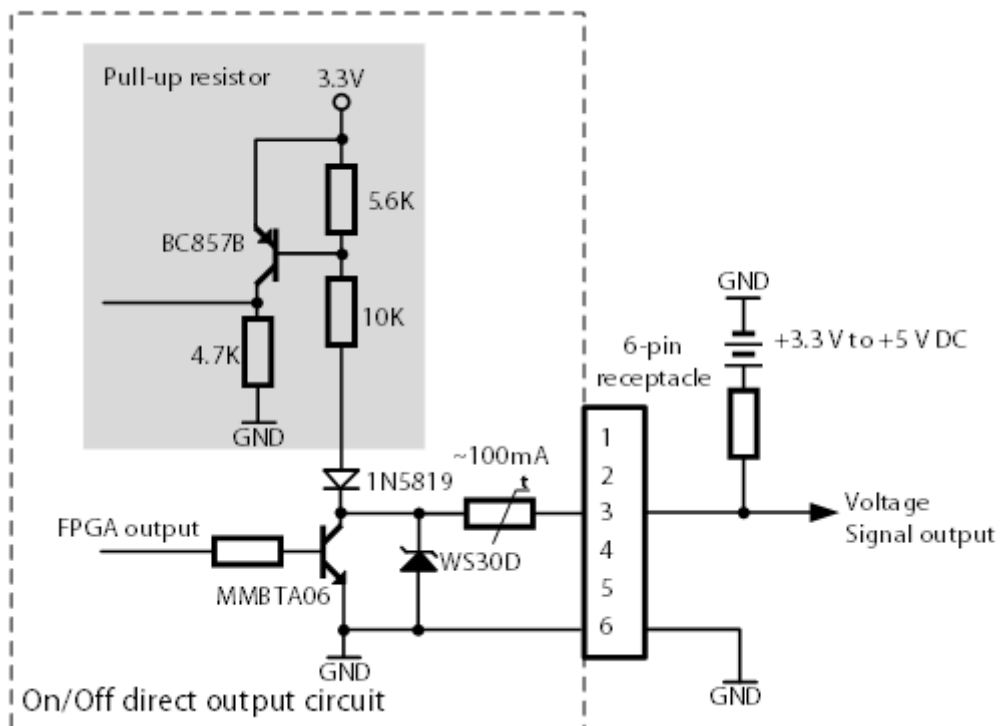


Table 3-2 Electrical specifications of the two-way I/O circuit

Voltage	Description
+30.0 VDC	Extreme voltage. Output voltage cannot exceed the value. Otherwise, the device might be damaged.
+3.3 to +24 VDC	The security working voltage range when output.
< 3.3 VDC	Possible error on I/O output.

3.7.2 Opto-isolated Input

Opto-isolator can realize one-way transmission of signal due to that the optocoupler is transmitted in one way. One-way transmission separates the input and output end completely, which eliminates the influence output signals have on the input end, leading to high anti-interference performance and strong working stability of the opto-isolator.

Line1 of the camera I/O signal is opto-isolated input and can sustain up to 25 mA current. For detailed circuit, see Figure 3-18.

Figure 3-18 Line1 internal circuit

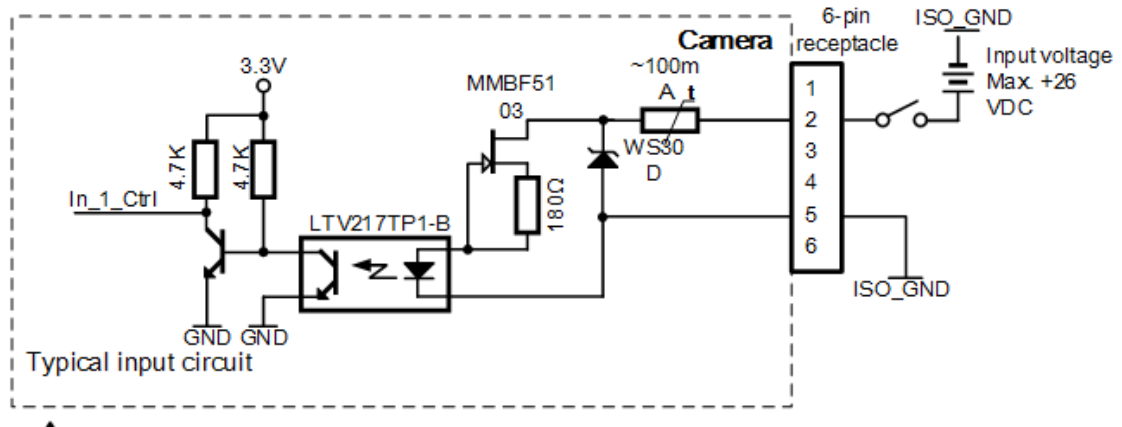


Table 3-3 Opto-isolated input circuit description

Input Voltage	Description	Remarks
30 VDC	Extreme voltage. Input voltage cannot exceed the value. Otherwise, the device might be damaged.	The extreme voltage of opto-isolated input is 25 VDC, and security working voltage range is 0–18 VDC for the 29 mm × 29 mm × 42 mm GigE camera.
0–24 VDC	Security working voltage range for I/O input.	
0–1.4 VDC	Logic 0.	
> 1.4–2.2 VDC	The input status reverses, and the logic status inside the voltage range is unsure.	
> 2.2 VDC	Logic 1.	

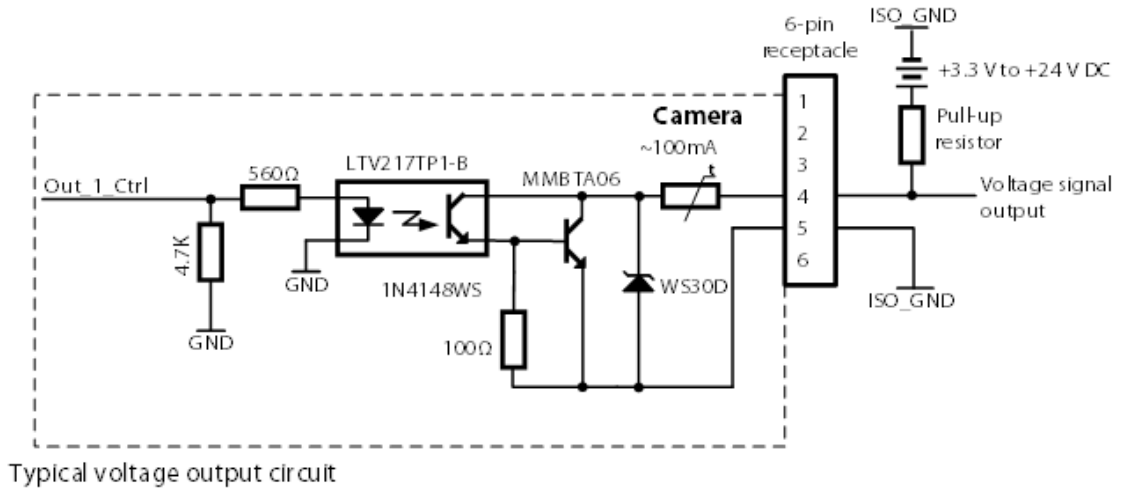


- Avoid the input voltage being inside 1–1.5 V, under which the circuit is not stable.
- The breakdown voltage is 30 V. keep the voltage stable.
- The sink current of the opto-isolated I/O input port is 5 mA–15 mA.

3.7.3 Opto-isolated Output

Line0 of the camera I/O signal is opto-isolated output. Refer to Figure 3-19 for detailed internal circuit.

Figure 3-19 Internal circuit of Line0

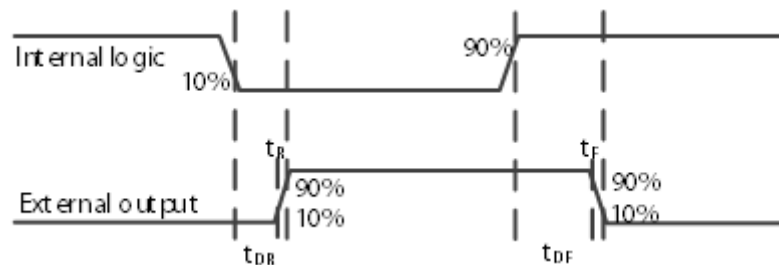


The highest output current of Line0 is 25 mA.

The pull-up resistance value complies with the maximum allowed current of the opto-isolated output port under the defined voltage. The larger the resistance value, the smaller the optocoupler forward voltage drop, the more slowly the output wave changes and the weaker the ability to power external devices. The recommended optocoupler value is 270 Ω, 560 Ω and 1 kΩ when the voltage is 5 V, 12 V and 24 V respectively.

The rising and falling time, delay time of rising and falling edge are shown as Figure 3-20 when the pull-up voltage is 1 kΩ.

Figure 3-20 Delay time of rising and falling



The electrical specifications of the opto-isolated output are shown in below table Table 3-4 when the external voltage is 3.3 V and resistance is 1 kΩ.

Table 3-4 Output trigger time

External Voltage (V)	Rising Time t_R (us)	Falling Time t_F (us)	Rising Edge Trigger Delay t_{DR} (us)	Falling Edge Trigger Delay t_{DF} (us)
5	19.70	3.20	39.9	8.06
12	24.06	5.22	44.8	11.8
24	30.11	8.10	44.8	53.2

- The optocoupler output delay is the time delay from FPGA internal logic output to external opto-isolated output pin.
- Rising edge trigger delay is the time delay from the 10% of the FPGA pin output level to the 90% of the external output signal amplitude.
- Falling edge trigger delay is the time delay from the 90% of the FPGA pin output level to the 10% of the external output signal amplitude.

- Rising time is the time delay from the 10% of the external output signal amplitude to 90%.
- Falling time is the time delay from the 90% of the external output signal amplitude to 10%.
- Values mentioned above are measured when the environment temperature is 25°C.



The maximum allowed continuous current for the opto-isolated output port is 50 mA. Any current exceeds the extreme value might result in port damage.

3.8 IO Smoothing

LineDebouncerTimeAbs: IO port smoothing. Only available under input mode, it filters the level signals of the cable connected to the corresponding port based on the defined value. If the signal value is lower than the defined value, it will be filtered.

For example, set the **LineDebouncerTimeAbs** value to 1500 us.

Figure 3-21 Configure filter value

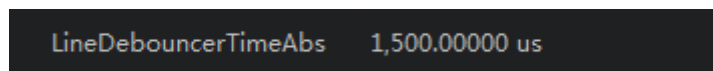


Figure 3-22 Before smoothing

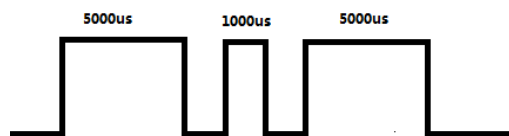


Figure 3-23 After smoothing



When the **LineDebouncerTimeAbs** value is higher than that of the high-low level, as the above example, the smoothing level is higher than 5000 us, the camera has no stream. Do not set the **LineDebouncerTimeAbs** value higher than that of the high-low level.

3.9 Black Level

The camera supports black level which can adjust the gray level deviation of the output data and decides the average gray level when the sensor is not photosensitive. Different ADC bit depth modes corresponds to different black level parameter range of the camera.

Configure black level.

Step 1 Select **Once** or **Continuous** under **Analog Control** > **Black Level Enable**.

Step 2 Enter the value in **BlackLevel** as needed.

Figure 3-24 Configure black level

BlackLevelAuto	Off
BlackLevelSelector	All
BlackLevel	50

3.10 Gain

Gain contains analog gain and digital gain. Analog gain can amplify the analog signal, and digital gain can amplify the signal after ADC (Analog to Digital Conversion).

Analog gain amplifies the signal, with higher value comes the stronger gain, higher brightness and more noises. Digital gain amplifies signals after ADC, same as analog gain, the higher the value, the stronger the gain, the higher the brightness and the more the noise. Compares to analog gain, the noise of digital gain is even more.

3.10.1 Analog Gain

Analog gain parameter settings include **Off**, **Once** and **Continuous**.

Table 3-5 Working principle of gain

Analog Mode	Gain	Parameter	Working Mode
Manual	Off		Adjusts analog gain based on the set value of GainRaw .
Automatic once	Once		Runs analog gain adjustment automatically for a period and then stops based on the current situation.
Continuous	Continuous		Runs analog gain adjustment continuously and automatically based on the current situation.

Select GainAuto mode.

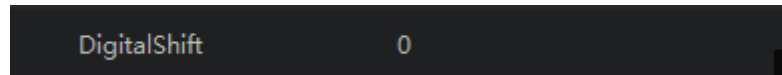
Figure 3-25 GainAuto mode

GainSelector	All
GainAuto	Off
GainRaw	Off
	Once
	Continuous

3.10.2 Digital Gain

Set the DigitalShift parameter among 0–4. The higher the value, the stronger the gain, the higher the brightness and the more the noise.

Figure 3-26 Digital Gain



3.11 White Balance

White balance renders the intensities of colors on images captured under different lights through adjusting the corresponding R/G/B value. It keeps the white parts of the image white under different color temperature.

White balance supports **Off**, **Once** and **Continuous** mode.

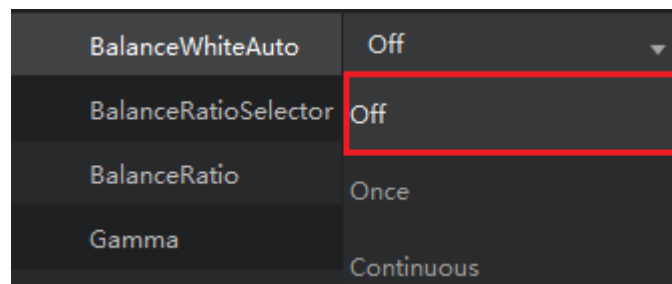
Table 3-6 Configure white balance.

WB mode	Parameter	Working Mode
Manual	Offz	Manually set the value of Red, Green and Blue channels under BlackRatioSelector and BalanceRatio .
Automatic once	Once	Runs white balance adjustment automatically for a period and then stops based on the current situation.
Continuous	Continuous	Runs white balance adjustment continuously and automatically based on the current situation.

You can use white balance to correct the image when the color is much different from the actual objects.

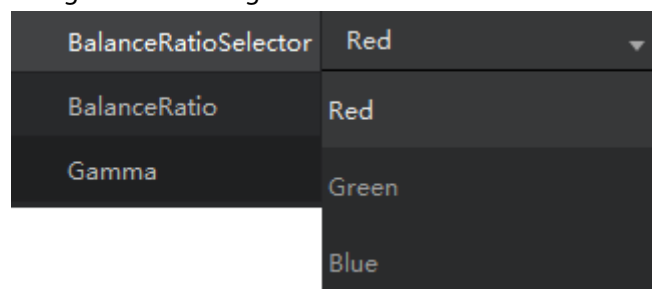
Step 1 Set **BalanceWithAuto** to **Off**.

Figure 3-27 Configure BalanceWithAuto



Step 2 Select R/G/B channels to be adjusted under **BlackRatioSelector**.

Figure 3-28 Configure BlackRatioSelector



Step 3 Adjust the **BalanceRatio** to a reasonable value among 0–15. Do the same for R/G/B.

Figure 3-29 Configure BalanceRatio

BalanceRatio	2.04266
--------------	---------

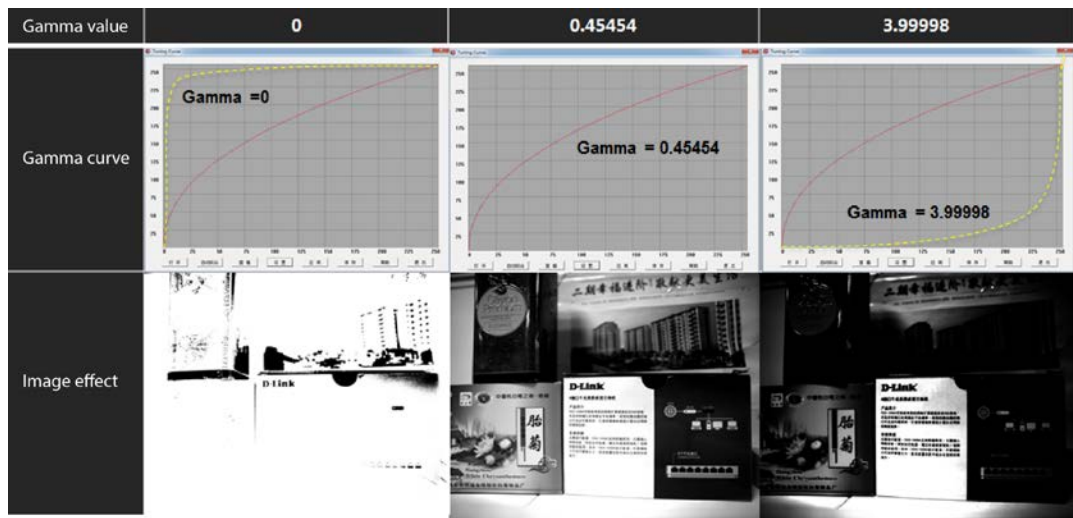


- Save the parameters after correction to avoid repeated configuration in case of unexpected occasions.
- You need to do white balance correction again if the light source or color temperature changes on the camera position.

3.12 Gamma

Gamma is used to correct the influence caused by nonlinear response of monitors on image. The smaller the value, the brighter the image. Gamma coefficient ranges from 0 to 3.99998.

Figure 3-30 Gamma value



Step 1 Set **GammaEnable** to **True**.

Figure 3-31 GammaEnable

GammaEnable	True
Gamma	False
	True

Step 2 Adjust Gamma value until the brightness meets the requirements.

Figure 3-32 Adjust Gamma value

Gamma	1.00000
-------	---------

Step 3 Gamma value is not valid when setting **GammaEnable** to **False**.

Figure 3-33 Cannot select Gamma

Gamma	{Not Available}
-------	-----------------



Gamma and **LookUpTable** are on opposite sides. When Gamma is enabled, LUT is unavailable. To make it available, set Gamma value to 1.

3.13 Testimage (Test Mode)

The camera supports test mode. When the test mode is enabled, the camera outputs images set by internal programs instead of images captured in real time. When the real-time images are abnormal, you can check whether the images output from test mode have the same issue to locate the problem. The test mode is disabled and the camera outputs real-time captured images by default.

- You can enable the test mode from **Image Format Control > Test ImageSelector**.
- After enabling it, the image displayed on the application window of the capture card switches to test image (decided by test mode).



Supported test images vary from different models.

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use overlapped characters, such as 111, aaa, etc.;

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. Physical Protection

We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. MAC Address Binding

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

8. Assign Accounts and Privileges Reasonably

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

9. Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. Audio and Video Encrypted Transmission

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. Secure Auditing

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

12. Network Log

Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. Construct a Safe Network Environment

In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.