

User Guide

GU-CI-Series

www.grundig-security.com

Content

1	Overvie	w5
	1.1 Ran	ge of Application5
	1.2 Ope	erating Environment
2	Devid	ce Connection
	2.1	Connecting to a PC
	2.2	Connecting Through a Router/Switch
3	Setti	ng an IP-Address with the GU-SW-IP-FINDER Tool7
4	Login	ı from Web Client
	4.1	Accessing Camera from Web Client 8
	4.2	Login for the First Time
	4.3	General Login
	4.4	Recover Password 10
	4.4.1	Security Question Configuration10
	4.4.2	Certificate of Authorization
	4.4.3	Super Code11
	4.5	Password Expire
5	Insta	lling Plug-in13
6	Live	View14
	6.1	Live View Menu
	6.2	Recording Status
7	Playb	back17
	7.1	General Playback
	7.2	Image Search
	7.3	Playback by Tag
	7.4	Smart
	7.5	AI
	7.5.1	Face Search 22

7.5.3 Perimeter Intrusion & Line Crossing. 7.5.4 Repeat Visitors. 7.5.5 Face Attendance 7.5.6 License Plate Detection 7.5.7 Intrusion. 7.5.8 Region Entrance 7.5.9 Region Entrance 7.5.9 Region Entrance 7.5.9 Region Entrance 7.5.9 Region Entrance 8.1 Live View 8.2 Image Control 8.3 Privacy Zone 8.4 ROI 8.5 Recording Parameters 8.5.1 Encode Parameters 8.5.2 Record 8.5.3 Capture 8.6 Event Setup 8.6.1 Parameter Setup 8.6.2 Alarm Setup 8.6.3 Retup 8.7.4 Statistics 8.8 Network Settings 8.8.1 Basic Settings 8.8.2 Email Configuration	23	7.5.2	
7.5.5 Face Attendance 7.5.6 License Plate Detection 7.5.7 Intrusion 7.5.8 Region Entrance 7.5.9 Region Exiting 8 Remote Setting 8.1 Live View 8.2 Image Control 8.3 Privacy Zone 8.4 ROI 8.5 Recording Parameters 8.5.1 Encode Parameters 8.5.2 Record 8.5.3 Capture 8.6 Event Setup 8.6.1 Parameter Setup 8.6.2 Alarm Setup 8.7.1 Setup 8.7.2 Recognition 8.7.3 Alarm Setup 8.7.4 Statistics 8.8 Network Settings 8.8.1 Basic Settings 8.8.2 Email Configuration		7.5.3	
7.5.6 License Plate Detection 7.5.7 Intrusion 7.5.8 Region Entrance 7.5.9 Region Exiting 8 Remote Setting 8.1 Live View 8.2 Image Control 8.3 Privacy Zone 8.4 ROI 8.5 Recording Parameters 8.5.1 Encode Parameters 8.5.2 Record 8.5.3 Capture 8.6 Event Setup 8.6.1 Parameter Setup 8.6.2 Alarm Setup 8.7.1 Setup 8.7.2 Recognition 8.7.3 Alarm Setup 8.7.4 Statistics 8.8 Network Settings 8.8.1 Basic Settings 8.8.2 Email Configuration	24	7.5.4	
7.5.7 Intrusion		7.5.5	
7.5.8 Region Entrance	29	7.5.6	
7.5.9 Region Exiting 8 Remote Setting. 8.1 Live View 8.2 Image Control. 8.3 Privacy Zone 8.4 ROI 8.5 Recording Parameters. 8.5.1 Encode Parameters. 8.5.2 Record. 8.5.3 Capture 8.6.4 Parameter Setup. 8.6.1 Parameter Setup. 8.6.2 Alarm Setting. 8.7 Al 8.7.1 Setup. 8.7.2 Recognition 8.7.3 Alarm Setup 8.7.4 Statistics. 8.8 Network Settings. 8.8.1 Basic Settings. 8.8.2 Email Configuration	29	7.5.7	
8 Remote Setting		7.5.8	
8.1 Live View 8.2 Image Control 8.3 Privacy Zone 8.4 ROI 8.5 Recording Parameters 8.5.1 Encode Parameters 8.5.2 Record 8.5.3 Capture 8.6 Event Setup 8.6.1 Parameter Setup 8.6.2 Alarm Setting 8.7 Al 8.7.1 Setup 8.7.2 Recognition 8.7.3 Alarm Setup 8.7.4 Statistics 8.8 Network Settings 8.8.1 Basic Settings 8.8.2 Email Configuration		7.5.9	
8.2 Image Control		8 Remo	8
8.3 Privacy Zone		8.1	
8.4 ROI		8.2	
8.5 Recording Parameters. 8.5.1 Encode Parameters. 8.5.2 Record. 8.5.3 Capture . 8.6 Event Setup . 8.6.1 Parameter Setup. 8.6.2 Alarm Setting. 8.7.4 Statistics. 8.8 Network Settings. 8.8.1 Basic Settings. 8.8.2 Email Configuration		8.3 [
8.5.1 Encode Parameters. 8.5.2 Record 8.5.3 Capture 8.5.3 Capture 8.6 Event Setup 8.6.1 Parameter Setup 8.6.2 Alarm Setting 8.7 Al 8.7.1 Setup 8.7.2 Recognition 8.7.3 Alarm Setup 8.7.4 Statistics 8.8 Network Settings 8.8.1 Basic Settings 8.8.2 Email Configuration		8.4 (
8.5.2 Record		8.5	
8.5.3 Capture 8.6 Event Setup 8.6.1 Parameter Setup 8.6.2 Alarm Setting 8.7 Al 8.7.1 Setup 8.7.2 Recognition 8.7.3 Alarm Setup 8.7.4 Statistics 8.8 Network Settings 8.8.1 Basic Settings 8.8.2 Email Configuration		8.5.1	
8.6 Event Setup 8.6.1 Parameter Setup 8.6.2 Alarm Setting 8.7 Al 8.7.1 Setup 8.7.2 Recognition 8.7.3 Alarm Setup 8.7.4 Statistics 8.8 Network Settings 8.8.1 Basic Settings 8.8.2 Email Configuration	39	8.5.2	
 8.6.1 Parameter Setup	41	8.5.3	
8.6.2 Alarm Setting 8.7 Al 8.7.1 Setup 8.7.2 Recognition 8.7.3 Alarm Setup 8.7.4 Statistics 8.8 Network Settings 8.8.1 Basic Settings 8.8.2 Email Configuration	42	8.6	
8.7 Al 8.7.1 Setup 8.7.2 Recognition 8.7.3 Alarm Setup 8.7.4 Statistics 8.8 Network Settings 8.8.1 Basic Settings 8.8.2 Email Configuration	42	8.6.1	
 8.7.1 Setup 8.7.2 Recognition	46	8.6.2	
 8.7.2 Recognition 8.7.3 Alarm Setup 8.7.4 Statistics 8.8 Network Settings 8.8.1 Basic Settings 8.8.2 Email Configuration 	50	8.7	
 8.7.3 Alarm Setup 8.7.4 Statistics 8.8 Network Settings 8.8.1 Basic Settings 8.8.2 Email Configuration	50	8.7.1	
8.7.4 Statistics 8.8 Network Settings 8.8.1 Basic Settings 8.8.2 Email Configuration	67	8.7.2	
 8.8 Network Settings 8.8.1 Basic Settings 8.8.2 Email Configuration 	72	8.7.3	
8.8.1 Basic Settings	76	8.7.4	
8.8.2 Email Configuration		8.8	
	80	8.8.1	
	83	8.8.2	
8.8.3 FTP		8.8.3	

9	Local Se	ettings 100
	8.10.4	System Information
	8.10.3	System Maintenance
	8.10.2	Multi-user Management
	8.10.1	General
8.	10 Sy	stem Settings
	8.9.2	Audio Management
	8.9.1	Disk Management
8.	9 De	evice Management
	8.8.9	Event Push Platform
	8.8.8	RTMP
	8.8.7	IP Filter
	8.8.6	HTTPS
	8.8.5	Dynamic Domain Name
	8.8.4	RTSP

Introduction

Thank you for purchasing a Grundig product. Before installing or connecting the product, please read first the following documents which you can find in printed form in the product package:

- Legal Disclaimer
- Safety Instructions
- Installation Manual and/or Quick Guide for the respective product model

Further information about the product like Data Sheets, CE Documents, etc. can also be found on our Web page <u>www.grundig-security.com</u>.

This User Guide is a manual for IP Cameras. Please see in the table of **Model Overview** the applicable models. Please read this User Guide carefully and retain it for future use.

Model Overview

This User Guide is for the following products:

GU-CI-AC5617E	GU-CI-AC5617V	GU-CI-AC5617T	GU-CI-AP12616F
GU-CI-AC5637E	GU-CI-AC5637V	GU-CI-AC5637T	GU-CI-AP20527Q
GU-CI-AC8616E	GU-CI-AC8616V	GU-CI-AC8616T	GU-CI-AT32637Q
	GU-CI-AP4634V	GU-CI-AP4634T	GU-CI-AP8616Q
	GU-CI-AC5617W	GU-CI-AP5634T	GU-CI-AP5647P

1 Overview

1.1 Range of Application

The network cameras with powerful image processing capacity may be applied at various public places such as mall, supermarket, school, factory and workshop, as well as in environments requiring HD video image such as bank and traffic control system, as shown below:



Figure 1.1 Application

1.2 Operating Environment

System: Windows XP/Windows 7/ Windows 8/ Windows 10/ Windows 11/MacOS 10 or above.

CPU: Intel I3 or above

Memory: 2 GB or above

Video memory: 1 GB or above

Display: 1024×768 or above

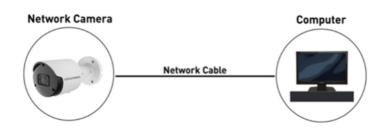
Browsers:IE10 and above, Chrome 57 and above, Firefox 52 and above, Edge 41 and above, Safari 12 and above.

2 Device Connection

An IP camera can be connected in two ways:

2.1 Connecting to a PC

Directly connect an IP camera to a PC through a network cable, connect the power input to the DC 12V adapter, and set the IP addresses of the PC and the IP camera on the same network segment. If the network is running properly, the IP camera will communicate with the PC within one minute after turned on.





2.2 Connecting Through a Router/Switch

This connection method is used when an IP camera is connected to the Internet where the IP camera and PC are connected to the LAN ports of a router/switch and the gateway of the camera is set to the IP address of the router.

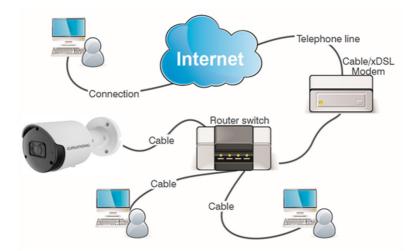


Figure 2.2 Connecting with Router

3 Setting an IP-Address with the GU-SW-IP-FINDER Tool

Step 1. Run Device Config Tool Run Device Config Tool role click Search to get the information of the IPCs in this LAN as shown in the

figure below, and locate your desired IPC based the P2P or MAC address of the camera.

GR	undi	IG													? – ×
Search	Upgrad	de Confi	g Stream	n Config	SD Config Reco	very Import/Exp	port Reboot h	ange Passwor					Filtration	IP	*
No.	IP	Media Port	Web Port	Channel	Device Name	Device Type	Device Version	Net Mask	Gateway	MAC	Network Mode	P2P ID	Status		
1	<u>192.168.0.41</u>	9000	80	1	GU-CI-AP5647P	GU-CI-AP5647P	V40.45.8.2.4.1_240429	255.255.128.0	192.168.1.1	00-23-63-A4-BE-16	DHCP	J3LVFFRLZLL45			
2	<u>192.168.0.42</u>	9000	80	16	GU-RN-AP8216N	GU-RN-AP8216N	V8.2.4.1-20240527	255.255.128.0	192.168.1.1	A4-DA-22-A8-00-74	DHCP	37UBURBVHJ61			
3	<u>192.168.0.43</u>	9000	80	1	GU-CI-AP5634T	GU-CI-AP5634T	V34.45.8.2.4_240509	255.255.128.0	192.168.1.1	A4-DA-22-A8-25-38	DHCP	IV31K5M7BZNG			
4	<u>192.168.0.48</u>	9000	80	1	GU-CI-AP4634T	GU-CI-AP4634T	V30.45.8.2.4.1_240508	255.255.128.0	192.168.1.1	A4-DA-22-A8-25-22	DHCP	63JNLFTLLRZN			
5	192.168.0.49	9000	80	1	GU-CI-AC5637V	GU-CI-AC5637V	V31.35.8.2.4_231228	255.255.128.0	192.168.1.1	A4-DA-22-A8-00-4A	DHCP	AZGGGNL2H1Z			
6	192 168.0.51	9000	80	1	GU-CI-AC8616V	GU-CI-AC8616V	V26.34.8.2.3_230419	255.255.128.0	192.168.1.1	A4-DA-22-A8-00-66	DHCP				
7	<u>192 168 0 54</u>	9000	80	8	GU-RN-AC8108P	GU-RN-AC8108P	V8.2.3.2-20231026	255.255.128.0	192.168.1.1	A4-DA-22-A8-0E-F4	DHCP	53UP43EZTBH3J			
8	<u>192.168.0.70</u>	9000	80	1	IPCamera	IPCamera	V31.35.8.2.4_231229	255.255.128.0	192.168.1.1	A4-DA-22-A8-24-97	DHCP	393F6W7MWW			
9	<u>192.168.0.72</u>	9000	80	1	GU-CI-AC4634V	GU-CI-AP5647P	V43.45.8.2.4.1_240419	255.255.128.0	192.168.1.1	A4-DA-22-A8-1F-E3	DHCP	(61C8G3R7HEM			
10	192.168.0.194	9000	80	1	GU-CI-AC5617T	GU-CI-AC5617T	V31.35.8.2.4.1_240425	255.255.128.0	192.168.1.1	A4-DA-22-A8-00-25	Static	'RFWKJ9WKTXA			
11	192.168.0.196	9000	80	1	GU-CI-AP12617F	GU-CI-AP12617F	V21.45.8.2.4.1_240429	255.255.128.0	192.168.1.1	00-23-63-A6-D9-06	DHCP	'1P3SGT4EVFUT			
12	192.168.1.250	9000	80	1	IP CAMERA	IP CAMERA	V31.35.8.2.4.1_240425	255.255.0.0	192.168.1.1	00-23-63-A4-BE-17	Static	YN6CRU4VH55			
13	<u>192.168.2.16</u>	9000	80	1	GU-CI-AC5637E	GU-CI-AC5637E	V31.35.8.2.3_230325	255.255.255.0	192.168.2.0	A4-DA-22-A8-00-3A	Static				

Note: The default IP address of the camera is 192.168.0.100, the default username is admin.

Step 2. Select the corresponding device, enter your username and password, edit the corresponding network information, and click Modify to save changes.

Note: Change the Network Mode to DCHP to get the IP address if the current network supports DHCP.

earch	Upgrai	te Config	Stream	Config 0	SD Config Reco	very Import/Exp	ort Rebool h	ange Passwor					Filtration	IP
No.	IP	Media Port	Web Port	Channel	Device Name	Device Type	Device Version	Net Mask	Gateway	MAC	Network Mode	P2P ID	Status	
1	<u>192.168.0.41</u>	9000	80	1	GU-CI-AP5647P	GU-CI-AP5847P	V40.45.8.2.4.1_240429	255.255.128.0	192.168.1.1	00-23-63-A4-BE-16	DHCP	J3LVFFRLZLL45		
	192 168 0.42	9000	80	16	GU-RN-AP8216N	GU-RN-AP8216N	V8.2.4.1-20240527	255.255.128.0	192.168.1.1	A4-DA-22-A8-00-74	DHCP	17UBURBVHU61		
3	192.168.0.43	9000	80	1	GU-CI-AP5634T	GU-CI-AP5634T	V34.45.8.2.4_240509	255.255.128.0	192,168.1.1	A4-DA-22-A8-25-38	DHCP	4V31K5M7BZNG		
4	192 168 0.48	9000	80	1	GU-CI-AP4634T	GU-CI-AP4634T	V30.45.8.2.4.1_240508	255,255,128.0	192.168.1.1	A4-DA-22-A8-25-22	DHCP	63JINLFTLLRZN		
5	192.168.0.49	9000	80	1	GU-CI-AC5637V	GU-CI-AC5637V	V31.35.8.2.4_231228	255.255.128.0	192.168.1.1	A4-DA-22-A8-00-4A	DHCP	AZGGGNL2H1Z		
6	192 168 0.51	9000	80	1	GU-CI-AC8616V	GU-CI-AC8616V	V26.34.8.2.3_230419	255.255.128.0	192.168.1.1	A4-DA-22-A8-00-66	DHCP			
7	192 168 0.54	9000	80	8	GU-RN-AC8108P	GU-RN-AC8108P	V8.2.3.2-20231026	255.255.128.0	192,168,1,1	A4-DA-22-A8-0E-F4	DHCP	33UP43EZTBH3J		
8	192.168.0.70	9000	80	1	IPCamera	IPCamera	V31.35.8.2.4_231229	255.255.128.0	192.168.1.1	A4-DA-22-A8-24-97	DHCP	393F6W7MWW		
9	192.168.0.72	9000	80	1	GU-CI-AC4634V	GU-CI-AP5647P	V43.45.8.2.4.1_240419	255.255.128.0	192.168.1.1	A4-DA-22-A8-1F-E3	DHCP	351C8G3R7HEM		
10	192 168 0 194	9000	80	1	GU-CI-AC5617T	GU-CI-AC5617T	V31.35.8.2.4.1_240425	255.255.128.0	192,168.1.1	A4-DA-22-A8-00-25	Static	RFWKJBWKTXA		
11	192 168.0 195	9000	80	1	GU-CI-AP12617F	GU-CHAP12617F	V21.45.8.2.4.1_240429	255.255.128.0	192.168.1.1	00-23-63-A5-D9-06	DHCP	1P3SGT4EVFUT		
12	192 168 1 250	9000	80	1	IP CAMERA	IP CAMERA	V31.35.8.2.4.1_240425	255.255.0.0	192.168.1.1	00-23-63-A4-BE-17	Static	YN6CRU4VH55		
13	192 168 2 16	9000	80	1	GU-CI-AC5637E	GU-CI-AC5637E	V31.35.8.2.3_230325	255.255.255.0	192.168.2.0	A4-DA-22-A8-00-3A	Static			
er info			Device I	nfo 2.168.0.41		Web Port 80		168.1.1 Net Mas						G

4 Login from Web Client

4.1 Accessing Camera from Web Client

Use Device Config Tool to search the IPCs in the current network. As shown in the following figure, directly click an IP address and use your IE browser to login to the corresponding camera.

1 122182.0.11 900 80 1 OUCAP58/TP 0.0CAP58/TP 0.	Search	The second second						port Rebool in					Filtration	IP
2 12 192	No.	IP	Prostanting and and a		Channel	Device Name	Device Type	Device Version	Net Mask	MAC			Status	
0 0														
4 192,180.48 900 00 1 0U-CH-P463AT CU-CH-P463AT V0 458.24_21,246590 255.5128 192,181.11 AL-0A-22-A6-2522 DHCP SUMLFILEZM. 5 52,180.48 900 90 1 0U-CH-P663T7 V0 458.24_23.2222 255.5128 192,181.11 AL-0A-22-A6-044 DHCP SZ0GONL2H7Z. 6 192,180.254 900 90 1 0U-CH-C65977 V0 CH-AC65977 V0 23.22203102 255.5128 192,181.11 AL-0A-22-A6-0454 DHCP SZ0GONL2H7Z. 7 192,180.254 900 00 1 0U-CH-AC69197 V0 23.222031028 255.5128 192,181.11 AL-0A-22-A6-0644 DHCP SJ0H3ETIBHJJ 0 122,158.0.272 900 00 1 PCamera V3135.82.4_231229 255.5128 192,181.11 AL-0A-22-A6-0644 DHCP SJ0H3ETIBHJJ 1 192,158.0.272 900 00 1 OU-CH-A65477 GU-CH-A65477 V135.8.2.4_124049 2555.128 192,181.11 AL-0A-22-A6-045 SB6C														
6 192.198.028 900 90 1 0U-0A-05937V 0U-0A-05937V 103.58.4_231228 255.55.128 192.198.11 A4-0A-22-A9-04-A DHOP AZDGORL2H1Z 6 192.198.051 900 90 1 0U-0A-05917V 013.58.24_231228 255.55.128 192.198.11 A4-0A-22-A9-04-A DHOP AZDGORL2H1Z 7 192.198.054 900 90 9 0U-0A-00819V 002.0A-02819V 252.55.128 192.198.11 A4-0A-22-A9-04-4 DHOP 3UPAIEZTBHUJ 8 192.198.027 900 90 1 DU-CA-00817V V313.58.24_231229 255.55.128 192.198.11 A4-0A-22-A9-074 DHOP 3UPAIEZTBHUJ 9 192.198.027 900 80 1 OU-CA-06917V V313.58.24_1240419 255.55.128 192.198.11 A4-0A-22-A9-075 SBMC RVFWU9HKTMA 1 192.198.027 9000 80 1 OU-CA-06917T V313.58.24.1_24428 255.55.128 192.198.11 A4-0A-22-A9-075 SBMC RVFWU9HKTMA														
0 1 0U-CAC0616V V02.348.21_20419 255.512.8 192.181.1 A40A2A40464 DHCP 7 152.188.054 900 90 9 0U-CAC0616V V02.34.20231026 255.512.8 192.181.1 A40A2A40464 DHCP SUPARATION 7 152.188.054 900 90 9 0U-CAC0616V V02.32-20231026 255.512.8 192.181.1 A40A2A40464 DHCP SUPARATION 8 152.188.073 900 60 1 PCamera PCamera V13.58.24_2.312.29 255.512.8 192.181.1 A40A22A4047 DHCP 307603776MW 9 192.188.073 900 80 1 GU-CAC65177 V13.58.24_1.240419 255.512.8 192.181.1 A40A22A40475 DHCP 307603776M 1 192.158.0134 900 80 1 GU-CAC65177 V13.58.24_1.240429 2555.128 192.181.11 A40A22A40455 SBMC FV7WU9MKTXA 1 192.158.0134 900 80 1 GU-CAC95177 V14.5														
7 192 118.054 900 80 8 GURN-AC8108P GURN-AC8108P QL2.3-20231028 255.55.128 192.181.1 A+0-A-22-A9-6F4 DHCP SUPCETTENSU 8 192.188.070 900 90 1 PCamera PCamera V3135.82.4_231229 255.55.128 192.181.1 A+0-A22-A9-6F4 DHCP 30JF08/TMWW 9 192.188.070 900 90 1 OU-CA-D6504V GUC-AP564TP V3135.82.4_1.2404P1 255.55.128 192.181.1 A+0-A22-A9-47P DHCP 30JG03RTHEM 10 192.188.072 900 60 1 GUC-AP564TP V3135.82.4_1.2404P1 255.55.128 192.181.1 A+0-A22-A9-47P DHCP 30JG03RTHEM 10 192.188.012 900 60 1 GUC-AP561TT V3135.82.4_1.2404P1 2555.55.55.55.55.55.55.55.55.55.55.55.55												AZGGGNL2H1Z		
0 1 IPCamera IPCamera V3158.2.4_231229 255 55.58.0 192.188.11 A4-0A-22-A6-447 DHCP 393F6W718Ww 0 1 0U-CA-D6934V OU-CA-D6944V OU-CA-D6944V V3158.8.2.4_234249419 255 55.58.0 192.188.11 A4-0A-22-A6-447 DHCP 393F6W718Ww 1 1 102-16A-D6934V OU-CA-D69547F V3158.8.2.4.1_2A0419 255 55.18.0 192.188.11 A4-0A-22-A6-47E DHCP 3106038714EM 1 1 152.188.0.128 600 60 1 GU-CA-D695177 V3158.8.2.4.1_2A0425 2555.528.0 192.188.11 A4-0A-22-A6-025 Static 7FWKJ9WKTXA 1 112.1580.128 600 60 1 GU-CA-P12517F V3145.8.2.4.1_2A0429 2555.528.0 192.188.11 0-0-23-63-A6-06-06 DHCP 'PISGT4EVFUT 1 112.1580.128 600 60 1 IPCAMERA V3158.8.2.4.1_2A0429 2555.528.0 192.188.11 0-0-23-63-A6-06-06 DHCP 'PISGT4EVFUT 1 12.1582.158.1150 0000<														
9 192:158.0.72 8000 80 1 GU-CH-AC4534V GU-CH-AP5647P V31.45.8.2.4 1_240419 255:255.128.0 192.168.1.1 A4-DA-22-A8-IF-E3 DHCP ISTGR3R7HEML. 10 192:158.0.194 8000 80 1 GU-CH-AC5517T V3135.8.2.4 1_240429 255:255.128.0 192.168.1.1 A4-DA-22-A8-IF-E3 DHCP ISTGR3R7HEML. 11 192:158.0.194 8000 80 1 GU-CH-AP12817F V3135.8.2.4 1_240429 255:255.128.0 192.168.1.1 A4-DA-22-A8-0255 Static RFWKU9WKT0A 11 192:158.0.194 8000 80 1 GU-CH-AP12817F V3135.8.2.4 1_240429 255:255.128.0 192.168.1.1 04-23-83-86D4-05 DHCP 193SGR4EVPUT 11 192:158.1250 8000 80 1 GU-CH-AP12817F V3135.8.2.4 1_240429 255:255.128.0 192.168.1.1 04-23-83-46D4-05 DHCP 193SGR4EVPUT 12 192:158.1250 8000 80 1 IP CAMERA V3135.8.2.4 1_240429 255:255.00 192.168.1.1 04-23-83-46E+17 </td <td></td>														
10 192:168.0.194 8000 80 1 GU-CH-AC5617T GU-CH-AC5617T V3135.8.2.4.1_240425 255:255.128.0 192:168.11 A4-DA-22-A6-00-25 Static TR/WKJBWKTXA 11 192:168.0.199 8000 80 1 GU-CH-AP12617F GU-CH-AP12617F V21:45.8.2.4.1_240429 255:255.128.0 192:168.11 04-23-63-A6-06-05 DHCP **1933GT4E/FUT 11 192:158.0.199 8000 80 1 GU-CH-AP12617F V21:45.8.2.4.1_240429 255:255.128.0 192:168.11 04-23-63-A6-06-05 DHCP **1933GT4E/FUT 12 192:158.1250 8000 80 1 IP CAMERA V31:35.8.2.4.1_240425 255:255.0 192:168.11 04-23-63-A4-0E-17 State ************************************								0.50						
11 152:158.0.195 9000 80 1 GU-CHAP12617F GU-CHAP12617F V21.45.8.2.4.1.240429 255:255.128.0 192:168.1.1 00-23-63.46-D9-06 DHCP '1P39G74EVPUT 112 152:168.1250 9000 80 1 IP-CAMERA IP-CAMERA V31.35.8.2.4.1_240425 255:255.0.0 192:168.1.1 00-23-63.44-DE-17 State: '1NHORR/WHY55														
) 12 112 118 1250 8000 80 1 IP CAMERA IP CAMERA V3135 8.2.4 1_240425 255 255 0.0 182 168.1.1 00-23-63-44-8E-17 Static 3116CRU41H65														
] 13 <u>192.158.2.15</u> 8000 80 1 GU-CI-AC5537E GU-CI-AC5537E V31.35.8.2.3_230325 255.255.0 192.168.2.0 A4-DA-22-A9-00-3A Bsute				80	1			V31.35.8.2.4.1_240425		00-23-63-A4-BE-17	Static	NN6CRU4VH55		

As an alternative, you can open your IE browser and type the following information into the address bar: HTTP://ip:web port. As shown in the figure above, the IP address of the device to be accessed is 192.168.0.41, the web port No.is 80, and the combined URL is http://192.168.0.41:80.

Note: In practical applications, the default HTTP access mode is port 80.

4.2 Login for the First Time

Firstly, access the camera from a web client, you need to set a password for the camera in order to complete the activation operation. The web client will display the screen as shown in Figure 4.2.1. Hover over the password entry box to prompt for the password requirement:

The length of the password should be 8~16 characters. It should contain at least two combinations of upper-case letters, lower case letters, numbers and special characters.

Password and username cannot be set the same.

	Password		
New Password			
			۵
Password Strength			
Confirm Password			
			ок

Figure 4.2.1 Password

Set a new password and click OK to save your change. The web client will display the screen as shown in Figure 4.2.2. Users can open the corresponding recover password method by checking the box, or cancel the setting directly without checking the box, and do not enable the recover password function.

	Recover Password	
Security Question Configuration		
Security Question 1	Your father's name?	
Answer		
Security Question 2	Your mother's name?	
Answer		
Security Question 3		
Answer		
Certificate of authorization		
Super code(Not recommended)		
	OK Cancel	

Figure 4.2.2 Recover

(1) Security Question Configuration: To change the user password by question verification, check the Security Question Configuration, select three questions among 15 questions, and set the answers at a maximum length of 64 characters to recover your password.

(2) Certificate of authorization: To change the user password by using a certificate, check the Certificate of authorization, and click Export to download the certificate.txt file.

③ Super code (Not recommended): This method is to calculate a super code allowing to changing the user password by using the MAC address of the camera and camera time. You are not advised to enable this function as the MAC address of the camera is broadcast over the network, and the system time of the camera can be directly obtained when you login from the web client and use Super code to change the user password.

Note: Keep your verification information properly when the recover password function is enabled.



4.3 General Login

After accessing from the web client, you will be directed to the login screen as shown in Figure 4.3.1. Then, input your username and password, and click Login to access the operation screen. At the same time, you can select your desired language upon login.



Figure 4.3.1 Login

4.4 Recover Password

When the recover password function is enabled, if you forget the login information, you can click Recover Password to enter the Recover Password screen. You can check security question configuration, certificate of authorization, or super code upon first login to recover your password.

4.4.1 Security Question Configuration

You can change the user password by setting security questions on the Recover Password screen, as shown in Figure 4.4.1. Fill in the answers to security questions. You can directly change the user password.

Verification Mode	Security Question Verification	
Security Question 1		
Answer		
Security Question 2		
Answer		
Security Question 3		
Answer		
New Password		
Password Strength		
Confirm Password		
	OK Cancel	

Figure 4.4.1 security Questions

4.4.2 Certificate of Authorization

When you set security questions upon first login, you will be asked to download the certificate.txt when you choose to recover the user password by using Certificate of authorization. On the Recover Password screen, click the

Recover Password and import the certificate.txt file to reset the password, as shown in Figure 4.4.2. Click Import and select the certificate.txt file. Then, enter a new password to change the user password.

	Recover Password	
Verification Mode	Security Question Verification	
Security Question 1		
Active		
Security Question 2		
Acouse		
Security Question 3		
Acouser		
New Password		
Password Strength		
Confirm Password		
	OK Cancel	

Figure 4.4.2 Recover

4.4.3 Super Code

A super code is an insecure way to recover the password. The super code is calculated based on the MAC address of the camera and the time of the super verification code according to certain rules. Then the user password can be changed by entering the verification code.

	Recover Password	
Verification Mode	Super Code	
Super code		
New Password		
Password Strength		
Confirm Password		
	OK	

Figure 4.4.3 Super Code

4.5 Password Expire

Security risks may arise if you use the same password for a long period of time. To this end, the program records the time when the password was changed last time. The system will ask you whether to change the password again if the current login time is 90 days later after the last password change time.

When you decide to change the password, the screen as shown in Figure 4.5.1 displays. As instructed on the screen, use your old password for verification and set a new password.



Password New Password Password servely Password Strength Cov Confirm Password
Pressent Strength Low
Passand Shergh Passand Shergh Lov
Pasavad Straigh Low
Confirm Password
OK Carol

Figure 4.5.1 Password Expire



5 Installing Plug-in

An image can be normally previewed only when the plug-in is installed when you login from your IE browser. Download and install the plug-in as instructed on the screen as shown in Figure 5.1.1.

GRUNDIG	Live	Playback	Remote Setting	Local Settings	• 🙂
ManSteam SubStream MobieStream					5
Live video can be played only after the player plug in is installed. Download and install the player if you have installed the player, n	estart your brows	er. (Allow the player			
▷ □ □ □ ₽ 0 Q Φ ♀					

Figure 5.1.1

Note: Skip the plugin installation when you access the web client from Safari 12 and above, Chrome 57 and above, Firefox 52 and above and Edge 41.

6 Live View

6.1 Live View Menu

The web client enters the login live view upon login, as shown in the figure below.

Note: Features may vary depending on product models.

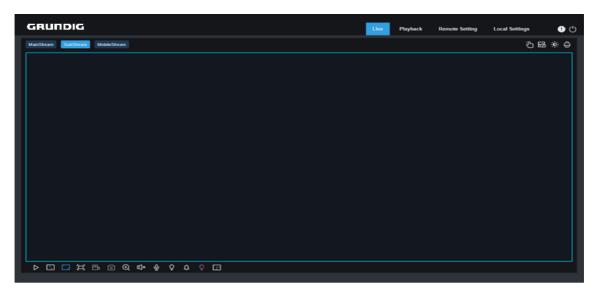


Figure 6.1 Live View

Stream switching menu: Switch the picture quality of the current live view at the upper left corner:

Main stream: HD picture, but higher requirements on bandwidth and PC performance.

Sub stream: Moderate requirements on bandwidth and PC performance, but lower picture quality when compared with main stream.

Mobile stream: Lowest requirements on bandwidth and PC performance, and lowest picture quality.

Main switching bar: Switches web function screens. The web client provides four menus: Live, Playback, Remote Setting, Local Settings.



Info: Displays the information about the active user, web version and plugin version.

Manual Alarm: Enable/disable the manual alarm (Note: for cameras with alarm I/O function only).

2 Al alarm: Open the alarm push bar on the right to display the captured images during face detection and human & vehicle detection.

Color: Adjust current image settings, such as image saturation and sharpness.



0

PTZ Setting: PTZ settings and re-focusing.

FRUNDIG





Recording & alarm status: Displays alarm and recording status of the camera. For details, check Section 6.2.



Stop/Play: Play and stop the preview of the current stream.



Original Proportions: Displays the current live view in its original proportion.



Stretch: Displays the current live view in a way that stretches the display area.

Full Screen: Displays the live view in full screen. You can double-click the screen to enable or disable the function, and press Esc to exit the full screen mode.



Record: Manually record the stream in preview.



Capture: Manually capture the image of the current stream.



Digital Zoom: Zoom in a certain area of the display.



Audio: Turn on/off or adjust the audio in preview.



Voice Intercom: Communicate with the camera.



Light: Manually turn on/off the white light.



Siren: Manually turn on/off the siren.



Warning Light: Turn on/off the red and blue lights

Pixel Counter: Select an area to check its pixel size in the stream.



Add Tag: Add a label, click to add a label.

Intelligent **Popup Info:** Prompt some alarm information in the lower right corner.

Fisheye: Enter/exit fisheye mode, please check section 6.3.

6.2 Recording Status

The recording status is a simple presentation of the current alarm at the web client and indicates whether the recording is normal. A variety of alarms can be stored at a time, as described below:

No icon: The memory card functions are normal but no recording is executing.

^R: camera is normal recording.

Note: When the camera is recording an alarm, the icon will disappear, but the normal recording process continues.

- ^H: The memory card is abnormal. Please check the memory card.
- M : A motion alarm is in progress but the motion alarm recording is not turned on.
- M : A motion alarm is in progress and the motion alarm recording is turned on.
- An I/O alarm is in progress, but the I/O alarm recording is not turned on.
- I : An I/O alarm is in progress, and the I/O alarm recording is turned on.
- PIR : A PIR alarm is in progress, but the PIR alarm recording is not turned on.
- PIR : A PIR alarm is in progress, and the PIR alarm recording is turned on.
- S : An intelligent alarm is in progress, but the intelligent alarm recording is not turned on.

Note: Intelligent alarms include face, human, and vehicle alarms.

S : An intelligent alarm is in progress, and the intelligent alarm recording is turned on.

7 Playback

The camera not only need to be able to show us images in real time, but also save the image information so that we can call it up when needed.

7.1 General Playback

The playback function mainly includes general video search and AI search, as shown in the following figure.

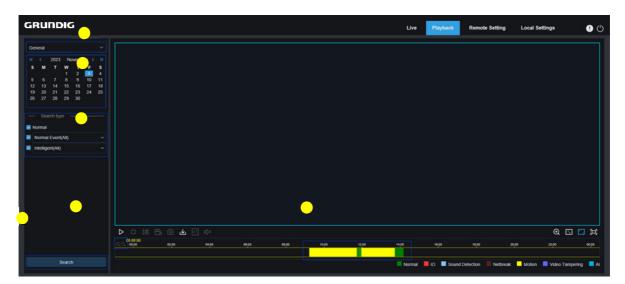


Figure 7.1.1 Playback

1.Switch search mode: Switch search functions, as shown in the figure above. General is selected by default to search for general recording files. You can switch to AI image search by referring to the following part in this section.

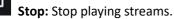
2.Date: Set the date to search for recording files, click Search, you will be prompted with the dates with available recording files.

3.Search type: Displays the search types supported by the camera. You can search for only part of recording files as required.

4.Playback process bar: Display and search for recording files stored in the memory card according to search settings.



Pause/Play: Pause/play streams.





Forward by One Frame: Play one frame with one click.



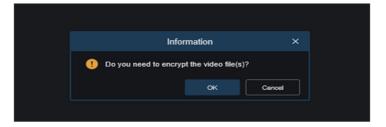
[0]

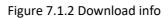
Record: Manually record the stream in preview.

Capture: Manually capture the image of the current stream.



Download: Download the searched recording file. (Note: When downloading RF format records, a Pop-up window will ask if encryption is required. AVI and MP4 formats will not have a pop-up window.)





×1 **Speed:** Supports playing at a speed of 1/8,1/4,1/2,1, X2, X4, X8, X16.

Audio: Turn on/off or adjust stream sound.

Playback progress bar: The time bar on the bottom displays the current playback progress bar and playback progress in different colors based on the search results.

Ð

٩Þ

Digital Zoom: Zoom in a certain area of the stream.



Original Proportions: Displays the current live view in its original proportion.



Stretch: Displays the current live view in a way that stretches the display area.



Full Screen: Displays the playback stream in full screen. You can double-click the screen to enable or disable the function, and press Esc to exit the full screen mode.

Zooming in/out playback progress bar: By default, the progress bar displays the progress within 24 hours.By zooming in and out the progress bar, you can jump to the corresponding playback position more accurately. You can also use the mouse wheel to zoom in/out the progress bar.

7.2 Image Search

 CRUIDIC
 Lva
 Pospess
 Rendo Setting
 Lcal Setting
 Cal Setting
 C

When the auto capture function is enabled, you can search and play pictures on this screen.

Figure 7.2.1 Image Search

1.Switch search mode: Switch the current search function. The current Search Mode is Picture.

2.Date: Set the date to search for pictures. By clicking Search, you will be prompted with the dates for which recording files are available.

3.Search time: Set the time to search for pictures, allowing users to search for pictures in a specific period of time.

4.Search type: Select the picture capture type you want to search for, or check "All Type" to select all pictures (Default select all).

5.Search: Click Search to start searching images.

6.Search Result Display Area: Displays the desired search results. Double-click on a picture will play the video after and before the picture.

7.Search results Flip: scroll through search results at the lower right corner.

7.3 Playback by Tag

This screen allows to view all previously added tags and edit, play back, or delete them.



GRUNDIG					H	Live Playback Remote Setting	g Local Settings	0
Tag	No.	Name	Date	Time	Playback	Edit	Delete	
Start time		Tag	11/11/2022	00:00:02				
2022-11-11 00 : 00 : 00		Tag	11/11/2022	08.15.53			Ē	
End time		Tag	11/11/2022	10.19.46			8	
2022-11-11 23 : 59		Tag	11/11/2022	10:41:53				
•				•		•		
Search							R < 1 / 1 >	28

Figure 8.3.1 Playback Tag

- 1.Switch search mode: Switch the current search function. The current Search Mode is Tag.
- 2.Start time: Set the start time to search for tags.
- **3.End time:** Set the end time to search for tags.
- **4.Keyword:** Search for tags with keywords.
- **5.Search:** Click Search to start searching.
- 6.Search Result Display Area: Displays the desired search results.
- Click the button to playback events, click the button to change event name, click the Save button to

display the Modify Success prompt dialog box, and click the 💼 button to delete this event.

7.Search results Flip: Scroll through search results at the lower right corner.

7.4 Smart

Login from a browser without the need of plugin to start smart playback, as shown in the figure below:

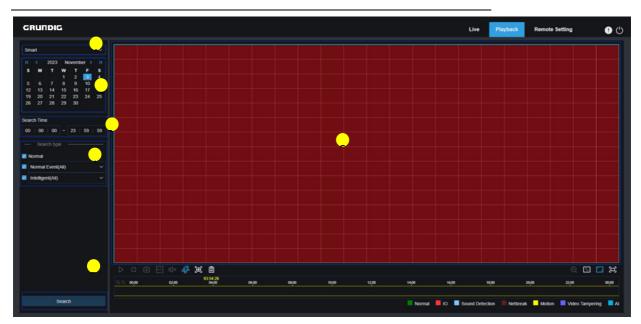


Figure 7.4.1 Smart Playback

This function can identify whether an alarm is triggered by human in daily life. If yes, the alarm will be shown in blue in the playback time bar on the bottom.

1. Switch search mode: Switch the current search function. The current Search Mode is Smart.

2. Date: Set the date to search for smart events. By clicking Search, you will be prompted with the dates for which recording files are available.

3. Search time: Set the time for searching for events.

4. Search type: Displays the search types supported by the camera. You can search for only part of recording files as required.

- 5. Search: Click Search to start searching.
- 6. Search Result Display Area: Displays the desired search results.



Pause/Play: Pause/play streams.



Stop: Stop playing streams.



Capture: Manually capture the image of the current stream.



Speed: Supports playing at a speed of 1/8,1/4,1/2,1, X2, X4, X8, and X16.



Audio: Turn on/off or adjust stream sound.

Add Default Tag: Add default tags. Mark the video playback start time at the current time in the current



channel and click this icon to add tags.

Ø? Add Tag: Add custom tags. When you click this icon to add a tag, a custom window will appear and you can specify a name for this tag.



Smart: Click this icon to enter the Smart area setting screen.



All: Click on All will set the full screen as the Smart detection area.



Delete: Click on **Delete All** will clear the entire area.



Digital Zoom: Zoom in a certain area of the stream.

Original Proportions: Displays the current live view in its original proportion.

Stretch: Displays the current live view in a way that stretches the display area.

(C Full Screen: Displays the playback stream in full screen. You can double-click the screen to enable or disable the function, and press Esc to exit the full screen mode.

7.5 AI

7.5.1 Face Search

The camera performs face recognition stores the obtained face information to the TF card, and saves the imagerelated information. You can quickly retrieve captured faces meeting user requirements and easily locate corresponding videos. The face search and playback screen is shown below.



Figure 7.5.1.1 Face Search



1. Switch search mode: Switch the current search function. The current Search Mode is Face Detection.

2. Start time: Set the start time to search for captured faces.

3. End time: Set the end time to search for captured faces.

4. Face Feature: The Face Features box is unchecked by default. When enabled, only face images captured when the face Feature detection function is turned on are searched. The firmware can recognize five face attributes, including gender, age, mask, glasses, and expression.

5. Alarm Group: The camera matches face images to the corresponding group according to the settings of the face database when capturing face images. This setting allows to search for images of only the groups you want.

6. Search: Search for face data according to settings.

7. Add: Add images to the camera for comparison purpose. You can add local images and captured images.

8. Delete: Delete currently added images.

9. Similarity: Set the lowest similarity of feature values of matching faces when using the Compare function.

10.Compare: Search for captured faces according to the set search time, group in which captured images are located, and selected reference face image for comparison.

11. Add Image Display Area: Displays images that are currently added and available for comparison.

12. Search Result Display Area: On the right side will display captured images searched by using Search and Compare.Double-click on a picture will play the video after and before the picture.

7.5.2 Pedestrian and Vehicle Search

Similar to the face capture function, the camera can distinguish humans or vehicles, and record them according to the required situation, which can be used to search for the required records. The interface effect is shown in the figure below. The screen is shown in the figure below.

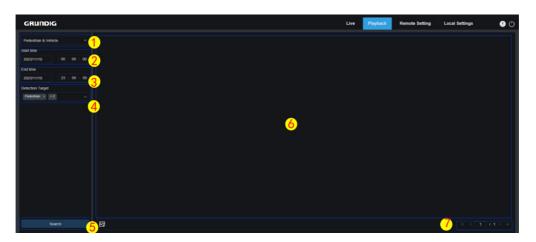


Figure 7.5.2.1 P & V Search

1.Switch search mode: Switch the current search function. The current Search Mode is Pedestrian & Vehicle.

2.Start time: Set the start time to search for Pedestrian and Vehicle images.

3.End time: Set the end time to search for Pedestrian and Vehicle images.

4.Detection Type: Select human or vehicle images as needed, or select both.

5.Search: Search for Pedestrian and Vehicle images according to search settings.

6.Search Result Display Area: Displays the desired search results. Double-click on a picture will play the video after and before the picture.

7.Search results Flip: Scroll through search results at the lower right corner.

7.5.3 Perimeter Intrusion & Line Crossing

With the development of technology, Perimeter Intrusion & Line Crossing is not only compatible with the old method to alarm targets entering the warning area, but also adds Pedestrian and Vehicle detection function, which only alarms human or vehicle targets and records image or video information for easy search and viewing. The screen is shown in the figure below.

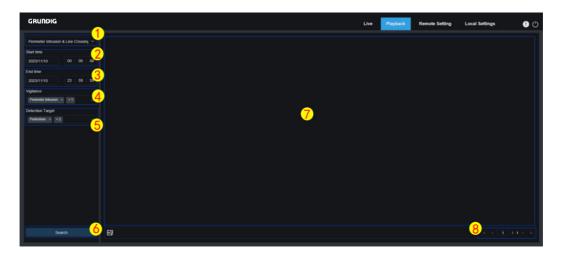


Figure 7.5.3.1 PI & LC Search

1.Switch search mode: Switch the current search function. The current search Mode is Perimeter Intrusion & Line Crossing.

2.Start time: Set the start time to search for Pedestrian and Vehicle images.

3.End time: Set the end time to search for Pedestrian and Vehicle images.

4.Vigilance: Select Perimeter Intrusion or Line Crossing or both as the capture method.

5.Detection Target: Select human or vehicle images as needed, or select both.

6.Search: Search for Pedestrian and Vehicle images according to search settings.

7.Search Result Display Area: Displays the desired search results. Double-click on a picture will play the video after and before the picture.

8.Search results Flip: Scroll through search results at the lower right corner.

7.5.4 Repeat Visitors

The face recognition function can not only provide alarms in real time, but also deeply dig into data to meet customer needs. For example, a camera is installed in a certain area of the mall, the repeat visitors function allows to check whether a customer stops to check out goods in this area. You can also monitor an area to check if a

suspected target is frequently seen in that area. The repeat customer function screen is shown in the figure below.

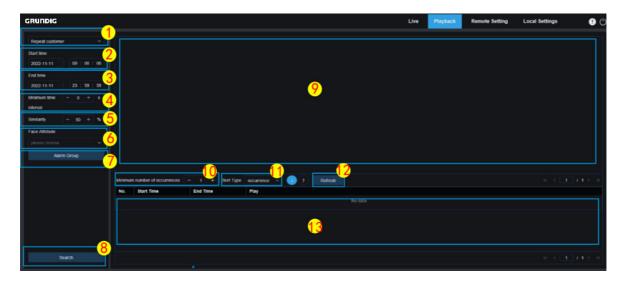


Figure 7.5.4.1 Visitors

1.Switch search mode: Switch the current search function. The current Search Mode is Repeat customer.

2.Start time: Set the start time to search for face images.

3.End time: Set the end time to search for face images.

4.Minimum time interval: Set the minimum time interval of capturing the same object twice to increase the search accuracy.

5.Similarity: Set the lowest similarity between other images and the reference image while matching repeat customers.

Note: This setting takes effect only when Alarm Group is unchecked for the current function.

6.Face Features: Filter searched images according to facial characteristic values.

Note: The search will be applied on all images when this option is not set. When this option is set,only captured images with Face Features enabled are searched.

7.Alarm Group: Identify repeat customers according to group settings in the database.

Note: All images will be searched when no group limitations are set. In this case, the similarity setting takes effect. Stranger information will be ignored when group limitations are set.

8.Search: Search for the information of captured images according to settings.

9.Search Result Display Area: Displays the search results in a stacked manner. Double-click on the displayed image information will list the stacked images on the bottom, and click on the corresponding image again will jump to its quick playback.

10.Minimum number of occurrences: Filter search results by number of occurrences. You have to click Refresh to update the display.

11. Sort Type: Sort search results chronologically or by capture count in ascending or descending sequence. You have to click Refresh to update the display.

12. Refresh: Refresh the sorting in your IE according to Minimum number of occurrences and Sort Type.

13. Secondary Search Result Display Area: Displays captured images of selected objects in the form of event list according to the information selected in the search result display area. You can click the Play button to go to quick playback.

7.5.5 Face Attendance

In addition to the repeat customer function, the face recognition function also provides the face attendance function. The face attendance (FA) function is used to retrieve face matching status in different groups (excluding stranger group) saved in the memory card in a specified period of time, and generate attendance results according to capture records. The functional screen is shown in the figure below.

GRUNDIG		4							Live	Playback	Remote Setting	Local Settings	0 0
Face attendance	Working	g day Mon. × +4	ľ				Duty	y Time 08 : 30 : 00 ~ 17	7:30:00			Refresh	Export
Search time mode	No.	Name	Group	Detail	11-10	11-11	Late	Leave Early			Absence		
Day	1	F2604@[g2_f18]	Allow List		5	0							
	2	123	Block List	B1	60	0							
2022-11-10 3 2022-11-11 4	3	bojunfang_0_0_[g3_f181]	Group 1	8	0	0							
Import type By group	4	caixunquan_0_0_[g3_f182]	Group 1	Ð	0	0							14
0	5	caojinzhi_0_0_[g3_f183]	Group 1	B	0	0							
Alarm Group	6	censhuangrong_0_0_[g3_f1 84]	Group 1	B									
	7	chenfang_0_0_[g3_f185]	Group 1	8	0	0							
	8	chengxiangqian_0_0_[g3_f1 86]	Group 1	8	0	0	0	0			2		
		•	we Early 👘 😒	Late and Le	ave Early 07:27:0	Absence 1 06:30:00	° <mark>15</mark>				20.00		
9 Search		00500 62.06	04.00	06:00		08.00	10.06	1208	* 14:00	16.00	1900 20	06 22:00	3460

Figure 7.5.5.1 Face Attendance

1. Switch search mode: Switch the current search function. The current Search Mode is Face Attendance.

2. Select Time Mode: Options include day, week, month, customize, and today. After you select a type, the system will automatically change the start date and end date. If day is selected, the end date and start date will be automatically synchronized. If week is selected, the start date and end date will be automatically changed to Monday and Sunday of the week to which the selected date belongs. If month is selected, the start date and end date will be automatically changed to the first and last day of the month to which the selected date belongs. If customize is selected, the search date is customizable. If today is selected, the start date and end date will be changed to the current date.

3. Start Date: Set the start date for searching by face attendance.

4. End Date: Set the end date for searching by face attendance.

5. Import type: Select import type, including by group and by face. The former takes all the people in the existing group as detection objects to search for matching results. The latter selects people in a certain group to search for matching results.

6. Alarm Group: When by group is selected, face attendance results will be searched by groups in the database.

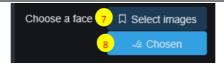


Figure 7.5.5.2 Select Image

When **by Face** is selected, the screen will change to the menu shown in the figure above.

7. Select images: Select and click the face image to be detected. The window shown below is displayed.

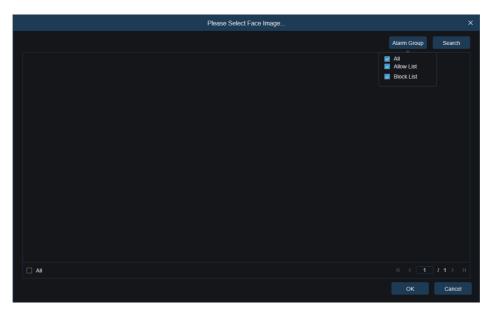


Figure 7.5.5.3 Select Image

Click **Alarm Group** to select a group and click Search again to search for all face images in this group. Select the face image for face attendance detection, and click **OK**. The face image will be added to the **Chosen** list. You can click **Cancel** to close this window.

8. Displays a list of selected face images. You can click Chosen to display the window shown in the figure below Select a face image and click **Delete**.

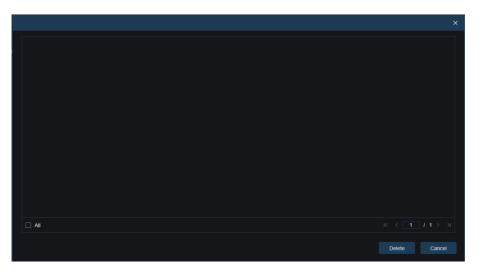


Figure 7.5.5.4 Delete Image

The face image will be deleted from the list. You can also click All to select all face images. You can click Cancel to

close this window.

9. Search: Search face attendance information according to settings.

10. Working Day: Set working day here.

11. Duty Time: Set duty time here.

12. Refresh: After changing attendance parameters, you can click Refresh to refresh search results.

13. Export: Click Export to export results to your PC.

Attendance Results:" \leftarrow " indicates leave early," \rightarrow " indicates late, both indicates late and leave early," \vee " indicates normal attendance, and " \circ " indicates absence. The green lines indicate the start and end time of attendance.

14. Secondary Search Result Display Area: Clicking on a person will display detailed time information at the lower right.



Figure 7.5.5.5 Detailed Information

15. Secondary display area for search results: Clicking on a person will display detailed time information down the right-hand side. The time-point that matches this person will be marked with a red bar. Click on the red bar will jump to the corresponding quick replay.

16. Click the **Detail** icon to check details. You can click the **playback** icon to go to quick replay.

1 Name 2021/	04/23				
n Duty	No.	Channel	Start time	End time	Playback
tatus Leave Early N DUTY 08:26:57	1	IP CH3	2021-4-23 08:26:57	2021-4-23 08:27:15	
	2	IP CH1	2021-4-23 08:26:58	2021-4-23 08:27:18	
YK W HAR STOR	3	IP CH1	2021-4-23 08:27:19	2021-4-23 08:27:24	
	4	IP CH3	2021-4-23 08:27:19	2021-4-23 08:27:22	
	5	IP CH3	2021-4-23 08:27:24	2021-4-23 08:30:05	
	6	IP CH1	2021-4-23 08:27:25	2021-4-23 08:30:06	
ff Duty		IP CH3	2021-4-23 08:30:13	2021-4-23 08:30:15	
atus Leave Early	8	IP CH3	2021-4-23 08:30:21	2021-4-23 08:30:22	
FF DUTY 12:56:43	9	IP CH3	2021-4-23 08:41:15	2021-4-23 08:41:24	
() () () () () () () () () () () () () (10	IP CH1	2021-4-23 08:42:26	2021-4-23 08:47:34	⊳
	11	IP CH3	2021-4-23 08:47:18	2021-4-23 08:47:32	
	12	IP CH3	2021-4-23 10:36:54	2021-4-23 10:37:30	
	5 4				

Figure 7.5.5.6 Secondary Display

You can click the arrow at the lower right corner to scroll through results.

7.5.6 License Plate Detection

When the license plate detection function is enabled for the IPC, an alarm will be triggered for recognized license plates, and images or videos will be recorded for easy search and viewing. The screen is shown in the figure below.

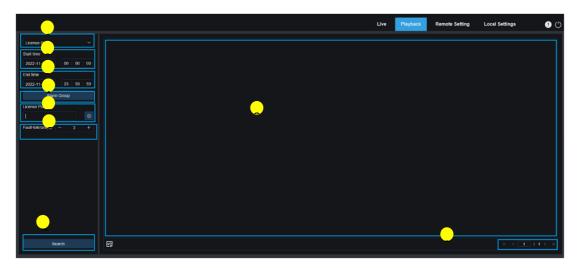


Figure 7.5.5.7 License Plate

1.Switch search mode: Switch the current search function. The current Search Mode is License Plate.

2.Start time: Set the start time to search for captured license plates.

3.End time: Set the end time to search for captured license plates.

4.Alarm Group: Recognize license plates by groups in the database.

Note: All images will be searched when no group limitations are set. In this case, the similarity setting takes effect. Unknown license plates will be ignored when group limitations are set.

5.License Plate: Filter and query license plates.

6.Fault-tolerant: Fault-tolerant rate. For example, three characters are set as the querying criteria. When the license plate number is **B594SB** in the allow list in the group, an alarm will also be triggered when the vehicle with license plate number **B734KB** approaches the surveillance area. That is, a license plate number has 0-3 characters different from that in the database will be recognized.

7.Search: Search for captured license plates according to settings.

8.Search Result Display Area: Displays the desired search results. Double-click on a picture will play the video after and before the picture.

9.Search results Flip: Scroll through search results at the lower right corner.

7.5.7 Intrusion

When the camera enabled the Intrusion function, it will alarm the target that enters into the intrusion of the alert area. Record video or capture picture information for easy search and view. Its interface is shown in the following figure.

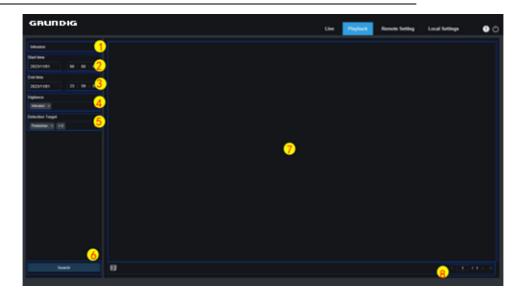


Figure 7.5.5.8 Intrusion

1.Switch search mode: Switch the current search function. The current Search Mode is Intrusion.

2.Start time: Set the start time to search for Intrusion snapshot.

3.End time: Set the end time to search for Intrusion snapshot.

4.Vigilance: Select Intrusion as the capture method.

5.Detection Type: Select Intrusion images as needed, or select both.

6.Search: Search for Intrusion images according to search settings.

7.Search Result Display Area: Displays the desired search results. Double-click on a picture will play the video after and before the picture.

8.Search results Flip: Scroll through search results at the lower right corner.

7.5.8 Region Entrance

When the camera enabled Region Entrance function, it will alarm the target that enters into the intrusion of the alert area. Record video or capture picture information for easy search and view. Its interface is shown in the following figure.

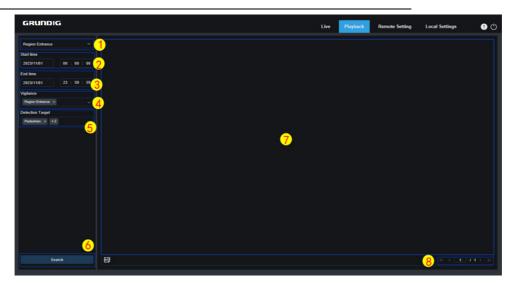


Figure 7.5.5.9 Region Entrance

1.Switch search mode: Switch the current search function. The current Search Mode is Region Entrance.

2.Start time: Set the start time to search for Region Entrance images.

3.End time: Set the end time to search for Region Entrance images.

4.Vigilance: Select Region Entrance as the capture method.

5.Detection Type: Select Region Entrance images as needed, or select both.

6.Search: Search for Region Entrance images according to search settings.

7.Search Result Display Area: Displays the desired search results. Double-click on a picture will play the video after and before the picture.

8.Search results Flip: Scroll through search results at the lower right corner.

7.5.9 Region Exiting

When the camera turns on Region Exiting function, Alarm triggered and detect targets leaving the guarded area. Record video or capture picture information for easy search and view. Its interface is shown in the following figure.

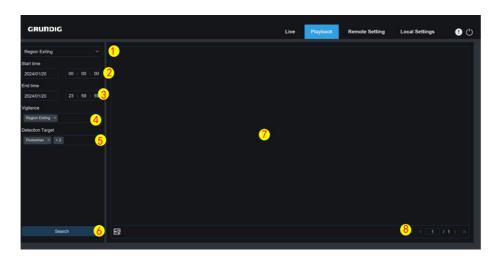


Figure 7.5.5.10 Region Exiting

1.Switch search mode: Switch the current search function. The current Search Mode is Region Exiting.

2.Start time: Set the start time to search for Region Exiting images.

3.End time: Set the end time to search for Region Exiting images.

4.Vigilance: Select Region Exiting as the capture method.

5.Detection Type: Select Region Exiting images as needed, or select both.

6.Search: Search for Region Exiting images according to search settings.

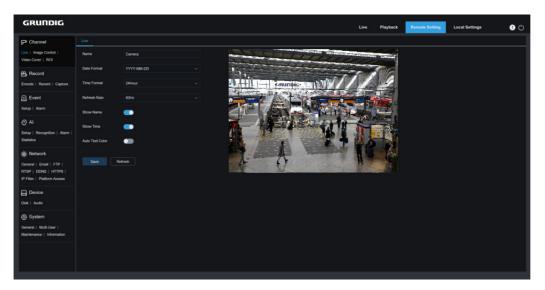
7.Search Result Display Area: Displays the desired search results. Double-click on a picture will play the video after and before the picture.

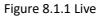
8.Search results Flip: Scroll through search results at the lower right corner.

8 Remote Setting

8.1 Live View

On the Live view, you can set channel name, device time, time standard, as well as camera information display. The view is shown in the figure below.





Name: Set the channel name of the camera displayed on the OSD.

Date Format: Set the date format of the camera displayed on the OSD, including MM/DD/YYYY, YYYY-MM-DD, and DD/MM/YYYY.

Time Format: Set the hour format of the camera on the OSD, including 12-Hour and 24-Hour.

Flicker Control: Set the image refresh rate, including 60 Hz and 50 Hz, corresponding to N and P respectively.

Show Name: Set whether to display channel name on images.

Show Time: Set where to display channel time on images.

OSD Self-adaptive: The OSD font color of the camera time and channel name is self-adaptive. The color switches between white and black based on the image background to ensure clear display.

Channel Name Display Location: Set the location where the channel name appears by dragging its location on the image.

Time Display Location: Set the location where the channel time appears by dragging its location on the image.

Alarm Statistic Display Location: Set the location where alarm statistic appears by dragging its location on the image. This setting is available only when the alarm statistic display function is enabled.

Save: Save the current changes.

Refresh: Refresh parameters on the current view.

8.2 Image Control

Image control is to directly control and modify graphic parameters, such as color to black mode, wide dynamic range, backlight compensation, etc. The view is shown in below figure.

GRUNDIG					Live	Playback	Remote Setting	Local Settings	
P Channel	Image Control								
we Image Control Ideo Cover ROI	Image Setting	Full Color Mode	A TWO INTO AND A REAL		And Intelligence	Grand Colorado	2		
B Record	White Light	Automatic mode	1.	in the state	-	-16			
ncode Record Capture	Sensitivity			GRUNDIG - MANY	1/1				
Event			ALL STREET LINE			E 11.	1		
ietup Alarm	Corridor Mode	Disable				3-1-1			
9 AI	Angle Adjustment			a desan see	2. 4	1.1.1.1	1		
- letup Recognition Alarm itatistics		Disable			14 1				
) Network	Exposure Compensation	Disable			1				
eneral Email FTP ITSP DONS HTTPS	White Balance	Automatic mode	₹¥ I	0		1			
P Filter Platform Access	Shutter	Automatic mode							
Device	Time Exposure								
Nsk Audio	Delog Mode								
) System Seneral Multi-User	3D Noise Reduction	Automatic mode							
taintenance Information									

Figure 8.1.2 Image Control

GRUNDIG						Live	Playback	Remote Setting	Local Settings	0
🖓 Channel	Image Control									
Live Image Control Video Cover ROI	Image Setting	Day/Night Mode		4	Carry	11-03 14	26.57	/.		
B Record	IR-CUT Mode	Image		1	10000					
Encode Record Capture	IR-CUT Sensitivity 🔮			A	1000060					
Event		Manual			and the second					
Setup Alarm	Low Beam Light		0 100							
() AI	High Beam Light		•100							
Setup Recognition Alarm Statistics					1000000					
Network	Corridor Mode	Disable					-			
General Email FTP	Angle Adjustment									
RTSP DONS HTTPS IP Filter Platform Access	Mirror	Disable					- /			
Device	Exposure Compensation	Disable								
Disk Audio	White Balance	Automatic mode								
System	Shutter	Automatic mode								
General Multi-User										

Figure 8.1.3 IR-settings

-	Image Control					
P Channel	image Control					
Live Image Control Video Cover ROI	Image Setting Advanced	Smart Illumination	~ •	Camera	0323-11-01163382	
B Record	Corridor Mode	Disable		0.0000		
Encode Record Capture	Angle Adjustment			0005880		
፼ Event Setup∣Alarm	Mirror	Disable		10000		
⊘ AI	Exposure Compensation	Disable				
Setup Recognition Alarm Statistics	White Balance	Automatic mode				
Network	Shutter	Automatic mode				/
General Email FTP RTSP DDNS HTTPS	Time Exposure					
IP Filter Platform Access	3D Noise Reduction	Automatic mode				
Device	Save Det	fault Refresh				
System						
General Multi-User Maintenance Information						

Figure 8.1.4 Image Settings

Image Setting: Set camera mode. There are three mode options.

Full Color Mode: The camera works in Full Color Mode.

Day/Night Mode: The camera works in Day/Night Mode.

Smart Illumination: In this mode, when the camera triggers an alarm in night vision mode, it will link with the warm light to fill in the light, and the image will be in color. The camera will return back to night mode after the alarm ends.

White Light: Set the fill-in light for the white light in Full Color Mode. There are four mode options.

Automatic mode: In Automatic Mode, the camera automatically adjusts the intensity of the fill-in light according to ambient illumination.

Manual: In Manual Mode, the fill-in light is applied on the environment with a fixed brightness value.

Schedule: In Schedule Mode, the white light is automatically switched on and off for fill-in as scheduled.

OFF: Disable the white light.

Sensitivity: Sensitivity 0-3. The degree to which the camera is sensitive to ambient light. The higher the value is, the higher the sensitivity is.

Light Distance: Ranging from 0 to 100 and used to adjust the brightness of the fill-in light. The higher the value is, the higher the brightness is.

IR-CUT Mode: Set the day/night switching mode of the camera in Day/Night Mode.There are five mode options.

Auto: Automatically controls the Switching mode. Among them, color to b/w is judged by images and b/w to color is judged by light sensitivity to ambient light.

Day: Forced Color mode will not be switched to b/w.

Night: Forced B/W mode will not be switched to color.

Image: Similar to the Auto Mode, color to B/W and B/W to color are judged by images (for non-photosensitive models).

Schedule: Switch between b/w and color as scheduled. If this function is enabled, the start time and end time for night vision shall be set.

IR-LED: Set the fill-in light effect of the IR light at night vision. There are three mode options.

SmartIR: Intelligently control the fill-in light intensity of the IR light according to focal length and overexposure condition.

Manual: Manual Mode in which the fill-in light is applied in the form of the set brightness of the IR light.

OFF: No fill-in light is applied for any light.

Low/High Beam Light: manually adjust the first group IR light brightness (0 to100, of which 0 indicates that the IR light is off and 100 indicates the highest brightness).

High Beam Light: Manually adjust the second group IR light (Only support by varifocals camera) brightness (0 to100, of which 0 indicates that the IR light is off and 100 indicates the highest brightness).



Corridor Mode: Corridor Mode.

Angle Trad: Image rotation setting. The camera is reverse to the presetting in some usage scenarios. For example, the camera is designed to be hung upside down, but in practice it is used flatwise. Set this value to adjust the image.

Mirror: Set the mirror mode to adjust the picture effect. There are four mode options.

Disable: Disable the Mirror Mode.

Vertical: Set the Mirror Mode in the vertical direction to interact the image on the picture up and down.

Horizontal: Set the Mirror Mode in the horizontal direction to interact the image on the picture left and right.

All: Enable Vertical and Horizontal at the same time. The effect is similar to that of 180° rotation, but the implementation principle is different.

Exposure Compensation: Set firmware performance when backlight. There are four mode options.

WDR: Wide dynamic range in which the picture is uniformly balanced based on the setting and both light and dark areas can be clearly distinguished.

HLC: Highlight compensation in which the objects in the highlighted area are clearer in the picture (applicable for some models).

Back Light: Backlight compensation in which the objects in the dark area are clearer.

Disable: An image will not be optimized with backlight on.

White Balance: White balance is a measure of the accuracy of white produced by mixing red, green, and blue. There are two mode options.

Automatic mode: Adjust the white light using default parameters.

Manual: Actively set the synthetic gained white light of red, green, and blue.

Shutter: Set the shutter exposure time. There are two mode options.

Automatic mode: The program automatically selects a proper exposure time according to the Time Exposure setting.

Manual: Allows to directly use the Time Exposure setting.

Note: Deselect the flickerless option of the exposure time in shutter manual mode, and select the option in shutter auto mode. If you switch the shutter to manual mode, the exposure time is switched automatically to 1/100 or 1/120.

Time Exposure: Set the exposure time of the camera and use this parameter in combination with Shutter. When the exposure time is too long, there may be overexposure. When the exposure time is too short, the picture may be dark.

3D Noise Reduction: Reduce image noise by setting this parameter to obtain a clearer picture. There are three mode options.

Automatic mode: In this mode, the camera will automatically select the noise reduction effect according to algorithms.

OFF: Disable the noise reduction function.

Manual: Allows to manually set the noise reduction coefficient to reduce image noise.

Defog: Foggy will lead to deteriorated images. The defog function can optimize image rendering in foggy days. There are three settings:

OFF: Disable the defog function.

Automatic mode: In this mode, the camera automatically judges the defog effect.

Manual: Allows to manually set the defog value.

Save: Save parameter changes to an image.

Default: Restore image parameters to default settings.

Refresh: Refresh image parameters.

8.3 Privacy Zone

In practical applications, if areas that can be monitored by the camera are not suitable for monitoring and recording, you can use this function to occlude these areas. This feature will allow users to create 4 or 6 (depending on model) privacy zones of any size and location. The screen is shown in the figure below.

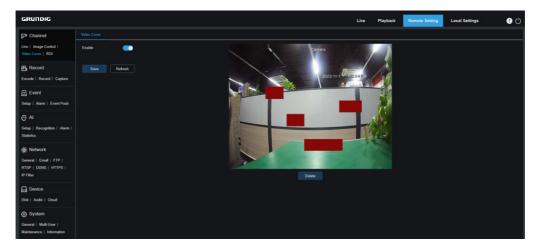


Figure 8.3.1 Privacy Zone

Enable: Enable the privacy zone function.

Tampering Area Setting: Set the areas to be masked in the monitoring screen. The masked blocks are red while setting and will turn to black after they take effect. You can set up to 6 (depending on model) blocks.

Delete: Delete selected blocks.

8.4 ROI

ROI (sensitive area) is a region of interest selected from the video area. This area can be set to a different frame rate and sharpness than the unselected area.

Note: This feature is mutually exclusive with H.264+ and H.265+ encoding types and cannot be enabled at the same time.

GRUNDIG				lve Playb	ack Remote Setting	Local Settings	• O
P Channel	ROI						
Live Image Control Video Cover ROI	Stream Type	MainStream		and a second			
B Record	Region ID		21.	in the	8		
Encode Record Capture	Enable Region	•					
Event	ROI Level	Lowest					
Setup Alarm Event Push	Non-ROI Fps(1~29)			51			
 Q Al Enter Becognition Aleren Statistics (i) Notwork General Entel FTP RTSP DONS HTTPS P Filter D Davice Diak Audio Churd (i) Enterm 	Save	takush	La constanti de la constanti de La constanti de la constanti de				
System General Multi-User Maintenance Information							

Figure 8.4.1 ROI Settings

frame rate of non-region of interest

Note: not supported from all models.

If the video code type is H264+ or H265+, the ROI function and the type are mutually exclusive. Therefore, the ROI function cannot be enabled, as shown in the following figure:

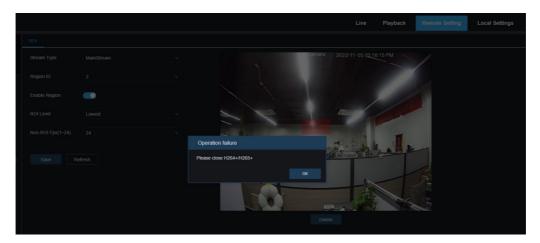


Figure 8.4.2 Operation failed

Enabling ROI does not take effect when Sub-Stream is in MJPEG format

Note: ROI is not supported from all models.

8.5 Recording Parameters

This menu allows to configure preview parameters and recording parameters.

8.5.1 Encode Parameters

This menu allows to configure the image quality for video recording or network transmission. In general, "Main

Stream" defines the quality parameters of recorded videos that will be stored in the HDD, "Sub Stream" defines the quality parameters of live videos that are remotely accessed from for example the web client and VMS, and "Mobile Stream" (can be turned off) defines the quality parameters of live views that are remotely accessed and viewed from mobile devices.

GRUNDIG				Live	Playback	Remote Setting	Local Settings	• •
P Channel	MainStream SubS	Itream MobileStream						
Live Image Control Video Cover ROI	Resolution							
B Record								
Encode Record Capture	Video Code Type							
Event	Video Code Level	Main Profile						
Setup Alarm	Bitrate Control							
 Al Setup Recognition Alarm 	Bitrate Mode	Predefined						
Statistics	Bitrate							
Network General Email FTP RTSP DDNS HTTPS IP Filter Platform Access	Audo Save R	wheeh						
Device								
System General Multi-User Maintenance Information								

Figure 8.5.1.1 Stream Settings

Resolution: This parameter defines the resolution of a recording image.

FPS: This parameter defines the frame rate of recording in your IPC.

Video Code Type: Channel decoding types. The options include H.264, H.265, H.264+, H.265+, and MJPEG (MJPEG only exists in Sub Stream mode).

Video Code Level: Video quality levels. The options include Bestline, Main Profile, and High Profile (for H.265, only Main Profile is available).

Bitrate Control: Select a bit rate level. For a simple scenario, a constant bit rate is preferred. For a complicated scenario such as a busy street, a variable bit rate is preferred.

Bitrate Mode: To manually set a bit rate, select the "Custom" Mode. To select a preset bit rate, select the "Preset" Mode.

Bitrate: This parameter corresponds to the data transmission speed used by the IPC to record a video. Recording in a higher bit rate will gain better image quality.

I Frame Interval: Set an I-frame interval.

Audio: Select this option if you want to record both audio and video and connect your microphone to IPC or use a camera with audio capability.

8.5.2 Record

8.5.2.1 Recording Parameters

This menu allows to set recording parameters.

GRUNDIG		Live	Playback	Remote Setting	Local Settings	! ()
P ^{II} Channel	Record Schedule					
Live Image Control Video Cover ROI	Steam Mode MainSteam v					
Encode Record Capture	Record C					
Event Setup : Alarm	Netrus C					
Al Setup Recognition Alarm Statistics	See Rotes					
Oeneral Email FTP RTSP DDNS HTTPS IP Filter Platform Access						
Device						
System General Multi-User Maintenance Information						

Figure 8.5.2.1.1 Record Parameter

Stream Mode: Select a Recording Mode, that is, video stream to be saved in the memory card. The main stream is selected by default.

Record: Select this option to start recording.

PreRecord: If this option is enabled, the IPC will start recording a few seconds before an alarm event occurs. This option is recommended if your main recording type is based on motion detection or I/O alarm.

Netbreak: If this option is selected, recording continues even when the network is disconnected or network failure occurs.

8.5.2.2 Schedule

ecording is performed only within the selected time period. You can drag your cursor to mark areas.

This menu allows to specify when the IPC starting recording. You can set a recording plan in the recording schedule. The recording is performed only within the selected time period. You can drag your cursor to mark areas.





8.5.3 Capture

8.5.3.1 Capture Settings

GRUNDIG					Live	Playback	Remote Setting	Local Settings	0 C
P Channel	Capture Captu	ure Schedule							
Live Image Control Video Cover ROI	Normal Interval	10 Min							
B Record	Alarm Interval								
Encode Record Capture	Auto Cepture	-							
Event Setup Alarm		Refresh							
 Al Setup Recognition Alarm Statistics 									
Network General Email FTP RTSP DDNS HTTPS IP Filter Platform Access									
Device									
System General Multi-User Maintenance Information									



Normal Interval: Normal capture interval, used to specify the capture interval in normal recording.

Alarm Interval: Alarm capture interval, used to specify the capture interval when motion detection, I/O alarm, or PIR is triggered.

Auto Capture: Automatic capture.

8.5.3.2 Capture Schedule

This menu allows to specify when the IPC capture images. You can set a capture plan in the capture schedule. The capture is performed only within the selected time period. You can drag your cursor to mark areas.

GRUNDIG											Live	Playback	Remote Setting	Local Settings	• •
P Channel	Capture	Capture Sche	duk												
Live Image Control Video Cover IROI	SUN	•	2	•	•	10	12	14	16	18	20	22	24		
Ercode Record Capture	MON												Normal Motion		
Event	TUE														
Setup Alarm															
Setup Recognition Alarm Statistics		Refres	A. Mart		-				0						
Network General Email FTP RTSP DONS HTTPS IP Filter Platform Access		. Nation													
Device															
System General Multi-User Maintenance Information															



Normal: When the area is marked green, the channel performs normal capture on the area in the corresponding

time period.

Motion: When the area is marked yellow, the channel performs motion capture on the area in the corresponding time period.

IO: When the area is marked red, the channel performs I/O alarm capture on the area in the corresponding time period.

PIR: When the area is marked purple, the channel performs PIR alarm capture on the area in the corresponding time period.

No Capture: When the area is marked black, the channel will not perform capture in this time period.

8.6 Event Setup

8.6.1 Parameter Setup

8.6.1.1 Motion Detection

This menu allows to configure motion detection parameters. When motion is detected, a series of alarms will be triggered, such as sending an email alert with attached images from the camera (if this option is enabled) and a push notification via the app.

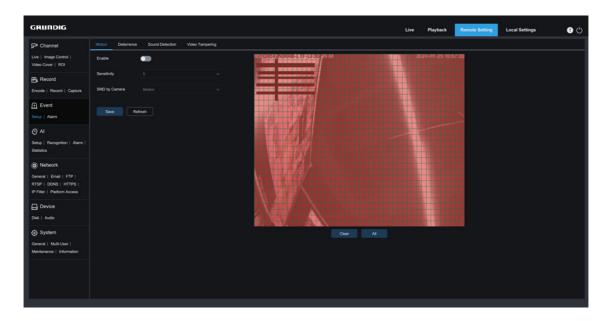


Figure 8.6.1.1.1 Motion

You can drag the left mouse button to delimit the detection area in the right window. An alarm will be triggered only when motion is detected in this area.

Enable: Enable or disable motion detection.

Sensitivity: Set the sensitivity of motion detection. The higher the value, the higher the sensitivity.

Target Detection: Intelligent motion detection. You can set the target detection type and area. The motion

detected in the area can trigger an alarm. The detection type includes the following four options: Motion, Pedestrian, Vehicle and Pedestrian & Vehicle (Note: Only some models support target detection. The default detection type is Pedestrian).

8.6.1.2 Deterrence

This menu allows to configure white light deterrence parameters when the camera supports white light and the image control is set to Day/Night Mode.When the alarm linking to deterrence is triggered, the white light will be automatically turned on for deterrence purpose as shown in the figure below:

undig					Live	Playback	Remote Setting	Local Settings	
annel	Motion Deterrence	Siren Sound Detection	n Video Tampering				ar		
Image Control Cover ROI	Light								
Record	Duration		Ĵ (5 - 180)						
code Record Capture	Deterrence Mode								
Event	Warning Light								
tup Alarm	Warning Light Duration		<u>(5 ~ 180)</u>						
) Al Hup Recognition arm Statistics	Save Deta	ut Refresh							
Network Internal Email FTP ITSP DONS HTTPS P Filter Platform Access									
Device									
System									

Figure 8.6.2.1.1 Deterrence

Note: When the camera supports white light and image control is set to Full Color Mode, the white light parameters such as **Light** become unavailable; when image control is set to Day/Night Mode, all parameters on this screen are available. When the image control is set to **Smart Illumination** mode, all parameters of this interface are grayed out and cannot be set.

Light: White light deterrence switch.

Duration: set the duration of white light deterrence.

Deterrence Mode: White light Deterrence Mode. There are two mode options:

Light Warning: The white light is steady on during deterrence.

Light Strobe: The white light blinks at a set frequency during deterrence.

Warning Light: Turn on or turn off warning light.

Warning Light Duration: Set the warning light duration.

8.6.1.3 Siren

When the camera supports siren, you can set the siren deterrence parameters on this screen. When an alarm linking to deterrence is triggered, the siren is automatically turned on for deterrence purpose, as shown in the following figure.

GRUNDIG		Live	Playback	Remote Setting	Local Settings	•
🖵 Channel	Motion Deterrence Siren Sound Detection V	ideo Tampering				
Live Image Control Video Cover ROI	Siren 🗩					
B Record	Siren Type Alarm1					
Encode Record	Siren Volume	9				
Event Setup Alarm	Siren Duration 5					
() AI	Save Refresh					
Setup Alarm Statistics						
Network						
General Email FTP RTSP DDNS HTTPS						
IP Filter Platform Access						
Device						
Disk Audio						
System						
General Multi-User Maintenance Information						

Figure 8.6.1.3.1 Siren

Siren: Turn on/off the siren.

Siren Type: Set the siren file type.

By default, there are two files for users to configure. You can customize and import three siren audio files (the audio file format should be **.wav** and **.pcm**, audio sampling rate can't exceed 8000Hz, and the file size is not larger than 256K).

Siren Level: Set the siren level.

Siren Duration: Set the siren duration.

8.6.1.4 Sound Detection

An alarm will be triggered when the camera detects that the connected audio has changed and the requirement of alarm detection is met.

GRUNDIG				ı	ive Playb	ack	Remote Setting	Local Settings	•
Channel Live Image Control Video Cover ROI	Enable 🧰		Video Tampering						
Encode Record	Rise 🧰	•	50						
Event Setup Alarm	Sound Intensity		50						
Al Setup Alarm Statistics	Decline Sensitivity	•	50						
Network General Email FTP RTSP DONS HTTPS IP Filter Platform Access		Refresh							
Device									
System General Muti-User Maintenance Information									

Figure 8.6.1.4.1 Sound Detection



Enable: enable or disable audio detection.

Rise: Volume rise switch. When this option is turned on, an alarm will be triggered only when the volume rises steeply.

Rise Sensitivity: Rise sensitivity. The higher the value, the easier it is to trigger an alarm.

Sound Intensity: Send sound intensity. This setting is the sound threshold. The larger the threshold, the louder the sound is required to trigger a rise alarm, and vice versa.

Decline: Volume decline switch. When this option is turned on, an alarm will be triggered only when the volume declines steeply.

Decline Sensitivity: Decline sensitivity. The higher the value, the easier it is to trigger an alarm.

Schedule: Set a sound alarm schedule. A sound alarm will be triggered only within the planned time.



Figure 8.6.1.4.2 Schedule

8.6.1.5 Video Tampering

Detects the live view tampering and trigger an alarm.

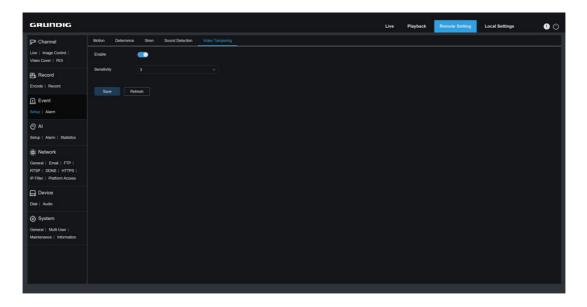


Figure 8.6.1.5.1 Video Tampering

Enable: enable or disable video tampering detection.

8.6.2 Alarm Setting

This menu allows to set the actions to be performed when an alarm is triggered.

8.6.1.6 Motion Detection

GRUNDIG						Live	Playback	Remote Setting	Local Settings	90
Live Image Control	Motion NO 5	Sound Detection	Video Tampering							
	Latch Time									
Encode Record Capture	Post Recording									
Event	Send Email	•								
Setup Atarm	Event Push Platform	•								
🤿 AI	Alarm Out	•••								
Setup Recognition Alarm Statistics	Light	•								
(a) Network	Warn Light	-								
General Email FTP RTSP DONS HTTPS	Siren	•								
IP Filter Platform Access	FTP Picture Upload									
Device	FTP Video Upload	•••								
Disk Audio	Enable Record	-								
System										
General Multi-User Maintenance Information		chedule Ref	esh							

Figure 8.6.1.6.1 Motion

Latch Time: Set the duration for triggering an external alarm when motion is detected.

Post Recording: Set the duration of continuous recording after an event occurs. The options include 5s, 10s, 20s, and 30s. The default duration is set to 5s.

Send Email: The camera automatically sends an Email when it detects motion.

Event push Platform: If this option is set to ON, this type of information will be pushed to the client when an alarm is triggered.

Alarm Out: Optional. If your device supports connection to an external alarm device, you can turn on this switch to activate the external alarm device.

Light: If this option is set to ON, the white light will be turned on for deterrence when an alarm is triggered.

Warn Light: If this option is set to ON, the warning light will be turned on for deterrence when an alarm is triggered.

Siren: If this option is set to ON, the siren will be turned on for deterrence when an alarm is triggered.

FTP Picture Upload: Upload alarm pictures to the FTP server.

FTP Video Upload: Upload alarm videos to the FTP server.

Enable Record: If this option is turned on, this kind of recording will be enabled when an alarm is triggered.

Schedule: Set the scheduled time when an alarm acts. An alarm action is triggered only within the scheduled time.

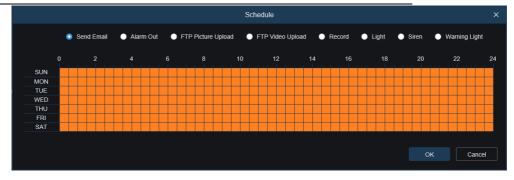
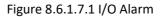


Figure 8.1.8.6.2 Schedule

8.6.1.7 I/O Alarm

This function is available only when your camera supports I/O sensors and connected to an external I/O alarm device.

GRUNDIG					Live	Playback	Remote Setting	Local Settings	0 C
🖓 Channel	Motion 10 5	Sound Detection Video	Tampering						
Live Image Control Video Cover ROI	Alarm Type								
B Record	Latch Time								
Encode Record Capture	Post Recording								
Event	Send Email	•••							
Setup Alarm	Event Push Platform	•							
Al Setup Recognition	Alarm Out	•••							
Alarm Statistics	Light	-							
(a) Network	Warn Light	-							
General Email FTP RTSP DONS HTTPS	Siren	•							
IP Filter Platform Access	FTP Picture Upload	•••							
Device	FTP Video Upload	•							
System	Enable Record	•							
General Multi-User									



Latch Time: Set the duration for triggering an external alarm when an alarm is detected.

Post Recording: Set the duration of continuous recording after an event occurs. The options include 5s, 10s, 20s, and 30s.The default duration is set to 5s.

Send Email: The device automatically sends you an Email when it detects an alarm.

Event push Platform: If this option is set to ON, an information will be pushed to the client when an alarm is triggered.

Alarm Out: Optional. If your device supports connection to an external alarm device, you can turn on this switch to activate the external alarm device.

Light: If this option is set to ON, the white light will be turned on for deterrence when an alarm is triggered.

Warn Light: If this option is set to ON, the warning light will be turned on for deterrence when an alarm is triggered.

Siren: If this option is set to ON, the siren will be turned on for deterrence when an alarm is triggered.

FTP Picture Upload: Upload alarm pictures to the FTP server.

FTP Video Upload: Upload alarm videos to the FTP server.

Enable Record: If this option is turned on, the recording will be enabled when an alarm is triggered.

Schedule: Set the scheduled time when an alarm acts. An alarm action is triggered only within the scheduled time.



Figure 8.6.1.7.2 Schedule

8.6.1.8 Sound Alarm

GRUNDIG					Live	Playback	Remote Setting	Local Settings	90
P Channel	Motion I/O	Sound Detection Vide	eo Tampering						
Live Image Control Video Cover ROI	Latch Time								
음 Record	Post Recording								
Encode Record Capture	Send Email	•••							
Event	Event Push Platform	•••							
Setup Alarm	Alarm Out	•••							
Al Setup Recognition	FTP Picture Upload	•							
Alarm Statistics	FTP Video Upload	•••							
General Email FTP	Enable Record	•							
RTSP DDNS HTTPS IP Filter Platform Access		chedule Refresh							
Device									
Disk Audio									
System									
General Multi-User									

Figure 8.6.1.8.1 Sound Alarm

Latch Time: Set the duration for triggering an external alarm when a sound alarm is triggered.

Post Recording: Set the duration of continuous recording after an event occurs. The options include 5s, 10s, 20s, and 30s.The default duration is set to 5s.

Send Email: The device automatically sends you an Email when it detects a sound alarm.

Event push Platform: If this option is set to ON, an information will be pushed to the client when an alarm is triggered.

Alarm Out: Optional. If your device supports connection to an external alarm device, you can turn on this switch to activate the external alarm device.

FTP Picture Upload: Upload alarm pictures to the FTP server.

FTP Picture Video: Upload alarm videos to the FTP server.

Enable Record: If this option is turned on, a recording will be enabled when an alarm is triggered.

Schedule: Set the scheduled time when an alarm acts. An alarm action is triggered only within the scheduled time.



Figure 8.6.1.8.2 Schedule

8.6.1.9 Video Tampering

GRUNDIG				Live	Playback	Remote Setting	Local Settings	9 C
P Channel	Motion IO	Sound Detection Vide	o Tampering					
Live Image Control Video Cover ROI	Latch Time							
B Record	Post Recording							
Encode Record Capture	Send Email	-						
Event	Event Push Platform	•••						
Setup Alarm	Alarm Out	•••						
Al Setup Recognition	Light	•						
Alarm Statistics	Warn Light	-						
(a) Network	Siren	-						
General Email FTP RTSP DONS HTTPS IP Filter Platform Access	FTP Picture Upload	•						
Device	Enable Record	•						
System	Save S	chedule Refresh						
General Multi-User								

Figure 8.6.1.9.1 Video Tampering

Latch Time: Set the duration for triggering an external alarm when a manipulation is detected.

Post Recording: Set the duration of continuous recording after an event occurs. The options include 5s, 10s, 20s, and 30s.The default duration is set to 5s.

Send Email: The device automatically sends an Email when it detects a manipulation.

Event push Platform: If this option is set to ON, an information will be pushed to the client when an alarm is triggered.

Alarm Out: Optional.If your device supports connection to an external alarm device, you can turn on this switch to activate the external alarm device.

Light: If this option is set to ON, the white light will be turned on for deterrence when an alarm is triggered.

Warn Light: If this option is set to ON, the warning light will be turned on for deterrence when an alarm is triggered.

Siren: If this option is set to ON, the siren will be turned on for deterrence when an alarm is triggered.

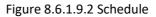
FTP Picture Upload: Upload alarm pictures to the FTP server.

FTP Video Upload: Upload alarm videos to the FTP server.

Enable Record: If this option is turned on, a recording will be enabled when an alarm is triggered.

Schedule: Set the scheduled time when an alarm acts. An alarm action is triggered only within the scheduled time.





Note: Video tampering alarm is not supported on all models.

8.7 AI

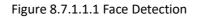
8.7.1 Setup

To use the AI alarm function, enable the alarm function in the Setup menu. Enabling the function consumes the computing power of the camera. Due to the limited performance of the camera. Some AI functions are not supported to be turned on at the same time, please refer to the relevant restriction tips of the specific model.

8.7.1.1 Face Detection

Face detection function. First, the camera detects the face and obtain the capture image that meets the requirements. Then, the face feature data of the capture image is calculated by the face model algorithm and then compared with that in the face database. Finally, an alarm is triggered. To do this, you need to enable the face detection function.

GRUNDIG										Live	Playback	Remote	Setting	Local Settings	0	0
🖓 Channel	Face Detection	Pedestrian & Vehicle	Perimeter Intrusion	Line Crossing	Object Detection	Cross Counting	Heat Map	Crowd Density	Queue Longth	License Plate	Rare Sound	Intrusion 1	Tegion Entrance	Region Exiting	Schedule	
Live Image Control Video Cover RCI		nd agree to intelligent Visio			1		Gerrieria 25	23-11-06 09 58 23								
B Record	Enable	-10							5							
Encode Record Capture	Dynamic Marking	•														
Event	Face Enhance	6 0														
Sellap Alarm	Face Features O	40			1965											
🔿 Al Senge i Recognition i Alaem i	Snap Mode					-		1								
Statistics	Apply Mode						-	-	100							
(1) Network General Email FTP RTSP DONS HTTPS	Min Pixel	2 H				-										
IP Filter Plattern Access	Max Pinel															
Device	Detection Mode	Hybrid Mode														
System	Trigger Mode															
General Multi-User Maintenance Information	Detection Area															
		Rebesh														



Service Agreement: Face Recognition Algorithm Agreement will automatically pop up when logging in for the first time, and the user can check to agree or not. If you do not click the apply button, it will appear every time you login. Before turning on the face detection switch, you must check to agree to the agreement, otherwise the face detection function cannot be used.

Enable: Enable the face detection function.

Dynamic Marking: Displays the face detection box and used to turn on or off the detection rule line (supported by some models).

Face Enhance: Face enhancement switch to increase the capture effect of moving objects. It will also adjust the brightness of the recognized face closest to the camera to optimize the capture effect (supported by some models).

Face Features: recognize the features of the detected face image, including age, gender, mask, glasses, expression, and so on.

Note: To use the Face Features alarm, enable this function.

Snap Mode: Set the snap mode. You can receive push notifications in live view or connect an NVR to check the image effect. The program supports three Snap Modes.

Optimal Mode: The camera only pushes an image that it considers best from detecting an object until the object disappears.

RealTime Mode: When detecting an object, the camera immediately pushes an image, and then pushes the best image when the object disappears.

Interval Mode: set the snap number and the snap and push interval as required. The options for Snap Num include 1,2,3, and unlimited. The Snap Frequency ranges from 1s to 255s. For example, when the snap frequency is set to 5s, an image is pushed at 5s, 10s and 15s when the object is detected.

Apply Mode: Screen the captured images. That is, only the captured images that meet angle setting will be pushed. There are three mode options.

Frontal View: Only the frontal view of an object is pushed.

Multi Angle: Choose to push images containing only side faces.

Customize: Customize the angle of an object for which images can be pushed. If this function is enabled, Roll Range, Pitch Range, Yaw Range, and Picture Quality options, as well as Frontal Default and Multi Default buttons will be available.

Roll Range: Set the roll range of the captured face image in the 3D model. When the angle does not meet the setting limit, face detection can be carried out but the image will not be pushed.

Pitch Range: Set the pitch range of the captured face image in the 3D model. When the angle does not meet the setting limit, face detection can be carried out but the image will not be pushed.

Yaw Range: Set the yaw angle of the captured face image in the 3D model. When the angle does not meet the setting limit, face detection can be carried out but the image will not be pushed.

Picture Quality: High quality images are good for filtering out detected non-face images.

Frontal Default Apply Mode: Selecting Customize displays the control, setting the values for Push Angle to Range: 30, Pitch Range: 30, Yaw Range: 45, and Picture Quality: 100.

Multi Default Apply Mode: Selecting Customize displays the control, setting the values for Push Angle to Range: 180, Pitch Range: 180, Yaw Range: 180, and Picture Quality: 100.

Min Pixel: Based on the 1080p resolution, filter out faces lower than the setting in the snap screen. The default

resolution is 64×64 pixels, and the setting range is 32 to 1080 pixels. When the mouse is moved to the progress bar, the right image preview shows the actual size of the pixel box. You can also drag the pixel box to set it. When the mouse is moved away for 5 seconds, the pixel box in the image preview disappears.

Max Pixel: Based on the 1080p resolution, filter out faces greater than the setting in the snap screen. The default resolution is 640×640 pixels, and the setting range is 320 to 1080 pixels. When the mouse is moved to the progress bar, the right image preview shows the actual size of the pixel box. You can also drag the pixel box to set it. When the mouse is moved away for 5 seconds, the pixel box in the image preview disappears.

Detection Mode: Filter the performance of detected objects in the camera. There are two mode options.

Hybrid Mode: Allow do face detection for all objects in the view.

Motion Mode: Allow to filter out motionless faces, such as such as portraits and statues in the scene.

Trigger Mode: Set the detection rule type. There are two rule types.

Rectangle: Allows to detect only face objects in the set area.

Line: In this mode, face objects are tracked only when the detection line is crossed according to settings.

Detection Area: Setting options are changed when the detection area is used to recognize objects by default. There are two modes.

Full Screen: All areas that can be monitored by the camera are detected.

User-defined: Only user-defined boxed areas are detected.

The Rule Type setting option is available only when the line-crossing detection mode is used. There are $A \rightarrow B$ and $B \rightarrow A$ detection Trigger Modes.

Rule Line Setting Area: Supports setting the detection area of 3-8 sides, or detecting the trigger line.

8.7.1.2 Pedestrian & Vehicle

Pedestrian detection and vehicle detection function, used to recognize pedestrian or vehicles in the view, generate an alarm, and record capture images, according function settings.

GRUNDIG					Live Playback Remote Setting ()
다 Channel	Face Detection Hur		imeter Intrusion Detection	Line Crossing Detection Rare Sound Detection	Stationary Object Detection Cross Counting Heat Map Intrusion Region Entrance Region Exiting Al Schedule
Live Image Control Video Cover ROI	Enable		License Plate Detection	Rare Sound Detection	Exag Cam 23/12/2024
Encode Record Capture	Sensitivity	60	Ĵ (1 - 100)		
Event	Dynamic Marking				
Setup Alarm	Snap Mode	Default			
Al Setup Recognition Alarm Statistics	Min Pixel	64 64 640	1080		
) Network	Max Pixel	320	1080		
General Email FTP RTSP CLOUD DDNS HTTPS IP Filter Platform Access	Detection Target	Pedestrian Motor Vehicle Non-motorized Vehicle		1	
Device	Detection Mode 🔮	Motion Mode			

Figure 8.7.1.2.1 Pedestrian & Vehicle

Enable: Enable the pedestrian and vehicle detection function.

Sensitivity: With higher detection sensitivity, pedestrian or vehicle objects can be detected easier, but false alarms may be easily generated.

Dynamic Marking: Displays the pedestrian and vehicle detection box and used to turn on or off **the detection rule line.**

Snap Mode: set the snap mode. You can receive push notifications in live view or connect an NVR to check the image effect. The program supports three Snap Modes.

Default: The camera pushes only one pedestrian or vehicle image from detecting an object until the object disappears.

RealTime Mode: When detecting an object, the camera immediately pushes one image, and then pushes another image when the object disappears.

Interval Mode: push images at a set interval.

Snap Num: Images for the same object as determined by the camera will be pushed 1,2,3, or unlimited times at an interval set in Snap Frequency.

Snap Frequency: Images will be pushed based on the set time upon appearance of an object or since the last push.

Min Pixel: Based on the 1080p resolution, filter out pedestrian or vehicle objects lower than the setting in the view. When the mouse is moved to the progress bar, the right image preview shows the actual size of the pixel box. You can also drag the pixel box to set it. When the mouse is moved away for 5 seconds, the pixel box in the image preview disappears.

Max Pixel: Based on the 1080p resolution, filter out pedestrian or vehicle objects greater than the setting in the view. When the mouse is moved to the progress bar, the right image preview shows the actual size of the pixel box. You can also drag the pixel box to set it. When the mouse is moved away for 5 seconds, the pixel box in the image preview disappears.

Detection Target: The options include pedestrian, motor vehicle, non-motorized vehicle, and all.

Detection Mode: Filter object behaviors in the detection area. There are two mode options.

Hybrid Mode: Allow to detect all pedestrians or vehicles in the view.

Motion Mode: Allow to filter out motionless pedestrians or vehicles.

Detection Range: Detection area setting. There are two mode options:

Full Screen: All areas that can be monitored by the camera are detected.

User-defined: Only user-defined boxed areas are detected.

Rule Line Setting Area: Supports setting the detection area of 3-8 sides, or detecting the trigger line.

8.7.1.3 Perimeter Intrusion

Perimeter intrusion detection. An alarm is triggered when a specific object enters or leaves the warning area.

GRUNDIG		Live Playback Remote Setting Local Settings 🕕 🖒
Channel Live Image Control Video Cover ROI	Face Detection Predestrian & Vehicle <u>Permeter Influsion</u> Line Crossing Region Entrance Region Exting Schedule	Object Detection Cross Counting Heat Map Crowd Density Queue Length License Plate Rare Sound Intrusion
Record Encode Record Capture	Enable Sensitivity 2 ~	Camera 2023-11-1001.3210
Event	Dynamic Marking 🗾 Detection Target 📓 Podeshtan	
Setup Alarm	Motor Vehicle Non-motorized Vehicle	A 44
Setup Recognition Alarm Statistics	Rule Number 1 🗸 🗸	
General Email FTP RTSP DDNS HTTPS IP Filter Platform Access	Rule Type A>8 ~	
Device	Save Refresh	Deinter All
System General Mutti-User ✓		

Figure 8.7.1.3.1 Perimeter Intrusion

Enable: Turn on or off the perimeter intrusion alarm function.

Sensitivity: Filter small disturbing objects. The higher the sensitivity, the smaller the object can be detected.

Dynamic Marking: Displays the detection box and used to turn on or off the detection rule line.

Detection Target: Set objects for perimeter intrusion detection:

Pedestrian: An alarm is triggered when a pedestrian intrudes the perimeter.

Motor Vehicle: An alarm is triggered when a motor vehicle intrudes the perimeter.

Non-motorized Vehicle: An alarm is triggered when a non-motorized vehicle intrudes the perimeter.

Rule Number: Allows to select a rule line number. The PID function Allow to set four detection rule lines.

Rule Enable: Turn on or off rule lines. Each rule line has an independent enable switch that is associated with the currently selected Rule Number.

Rule Type: Specifies the rule to trigger rules. There are $A \rightarrow B$, $B \rightarrow A$, and $A \leftarrow A$ bline-crossing rules whose settings are related to the currently selected Rule Number.

Rule Line Setting Area: Allows to set and view edited rule lines.

Delete: Allow to delete selected rule Lines in the rule line setting area.

Delete All: Allow to delete all rule lines.

8.7.1.4 Line Crossing

Line-crossing detection function. An alarm is triggered when a specific object crosses the preset detection line.

GRUNDIG										Live	Playback	Remo	te Setting	Local Settings	0	Ф
Channel	Face Detection	Pedestrian & Vehicle	Perimeter Intrusion	Line Crossing	Object Detection	Cross Counting	Heat Map	Crowd Density	Queue Length	License Plate	Rare Sound	Intrusion	Region Entrance	Region Exiting	Schedule	
Live Image Control Video Cover ROI	Enable	-			B		Caniera 20	23-11-06 11 13:20								
Record Encode Record Capture	Dynamic Marking Sensitivity	-		- 50					Ĩ							
D Event	Target Validity															
Setup Alarm	Min Poel	64						• •								
Setup Recognition Alarm Statistics	Max Porel	320	640					-	1							
Several Email FTP RTSP DONS HTTPS IP Filter Platform Access	Detection Target	 Pedestrian Motor Vehicle Non-molorized 	Vehicle				weeks Down	40 AS								
Device	Rule Number Rule Enable	•														
System General Multi-User Maintenance Information	Rule Type Save	A+8 Refresh														

Figure 8.7.1.4.1 Line Crossing

Enable: Enables the line-crossing detection function.

Sensitivity: The sensitivity is related to the percentage of the target that enters the area; the higher the sensitivity setting of Line Crossing, the more likely the alarm will be triggered. For example, if it is set to 100%, the alarm will be triggered when the detection target has just touched the boundary of the set area. If set to 50%, the alarm is triggered after 50% of the detection target has already crossed the boundary of the set area.

Dynamic Marking: Displays the detection box and used to turn on or off the detection rule line.

Target Validity: The similarity between the detection target and the set detection type.1 represents a similarity of 80% or more, 2 represents a similarity of 60% or more, 3 represents a similarity of 40% or more, 4 represents a similarity of 20% or more.

Min Pixel: Based on the 1080p resolution, filter out pedestrian or vehicle objects lower than the setting in the view. When the mouse is moved to the progress bar, the right image preview shows the actual size of the pixel box. You can also drag the pixel box to set it. When the mouse is moved away for 5 seconds, the pixel box in the image preview disappears.

Max Pixel: Based on the 1080p resolution, filter out pedestrian or vehicle objects greater than the setting in the view. When the mouse is moved to the progress bar, the right image preview shows the actual size of the pixel box. You can also drag the pixel box to set it. When the mouse is moved away for 5 seconds, the pixel box in the image preview disappears.

Detection Target: Set objects for perimeter intrusion detection:

Pedestrian: A perimeter intrusion alarm is triggered only for pedestrians.

Motor Vehicle: A perimeter intrusion alarm is triggered only for motor vehicles.

Non-motorized Vehicle: A perimeter intrusion alarm is triggered only for non-motorized vehicles.

Rule Number: Allows to select a rule line number. Allows to set four detection rule lines.

Rule Enable: Turn on or off rule lines. Each rule line has an independent enable switch that is associated with the currently selected Rule Number.

Rule Type: Specifies the rule to trigger rule lines. There are $A \rightarrow B$, $B \rightarrow A$, and $A \leftarrow A$ bline-crossing rules whose

settings are related to the currently selected Rule Number.

Rule Line Setting Area: Allows to set, modify, and view edited rule lines.

Delete: Allows to delete selected rule Lines in the rule line setting area.

Delete All: Allows to delete all rule lines.

8.7.1.5 Object Detection

An alarm will be triggered when there are items left or lost in the monitored scene.

GRUNDIG								Live	Playback	Remote Setting	Local Settings	0
P Channel	Face Detection	Pedestrian & Vehicle	Perimeter Intrusion	Line Crossing	Object Detection	Cross Counting	Heat Map	Crowd Density	Queue Leng	ph License Plate	Rare Sound Intrusion	
Live Image Control	Region Entrance	Region Exiting	Schedule									
Video Cover ROI	Enable				1000		Camera 20	23-11-10 01 32-	49			
B Record	Sensitivity											
Encode Record Capture												
Event	Dynamic Marking	-					11.epecy			0		
Setup Alarm	Rule Number											
() Al	Rule Enable	-				(I)						
Setup Recognition												
Alarm Statistics	Rule Type	Legacy										
(a) Network								-				
General Email FTP RTSP DONS HTTPS	Save	Refresh			-		-					
IP Filter Platform Access												
Device												
Disk Audio												
System												
General Multi-User												

Figure 8.7.1.5 Object Detection

Enable: T urn on or off the SOD function.

Sensitivity: Filter small disturbing objects. The higher the sensitivity, the smaller the object can be detected.

Dynamic Marking: Displays the detection box and used to turn on or off the detection rule line.

Rule Number: Allows to select a rule line number. The LCD function allows to set four detection rule lines.

Rule Enable: Turn on or off rule lines. Each rule line has an independent enable switch that is associated with the currently selected Rule Number.

Rule Type: Specifies the rule to trigger rule lines. You can set to trigger an alarm when an item is left or lost in the detection area. There are three rules including Legacy, Lost, and Lost & Legacy whose settings are related to the currently selected Rule Number.

Rule Line Setting Area: Allows to set, modify, and view edited rule lines.

Delete: Allows to delete selected rule Lines in the rule line setting area.

Delete All: Allows to delete all rule lines.

8.7.1.6 Cross Counting

Cross counting (CC) statistics function. Record the line-crossing information of a specific object in the monitored area. Set a crossing line. There are A and B areas on two sides of the set line. For example, the triggering rule for the rule line is $A \rightarrow B$. When an object enters from area A and crosses the detection line, in is increased by 1 when the

object leaves area B. When the object enters from area B and crosses the detection line, out is increased by 1 when the object leaves area A. When the increase is to be calculated, an alarm is triggered only when the current IN count minus the out count is greater than or equal to the set Alarm Number, as shown in the following figure.

GRUNDIG						Live	Playback	Remote Setting	Local Settin	PS 🙂
🖓 Channel	Face Detection	Pedestrian & Vehicle Pe	rimeter Intrusion Line Crossing	Object Detection	Cross Counting Heat Map	Crowd Densit	y Queue Leng	th License Plate	Rare Sound	Intrusion
Live Image Control	Region Entrance	Region Exiting Schedu	*							
Adeo Cover ROI	Enable			1000	Camera 20	925-11-10 01 33	120			
B Record	Sensitivity									
ncode Record Capture										
Event	Dynamic Marking	-								
Setup Alarm	Detection Target	Pedestrian								
() AI	Alarm Number		Ĵ (1 - 255)							
Setup Recognition										
Warm Statistics	Start Time			10.000						
Network	End Time							2		
ieneral Email FTP TSP DONS HTTPS				-			/			
P Filter Platform Access	Rule Number									
Device	Rule Enable	-								
Disk Audio	Rule Type									
) System										
Seneral Multi-User	Save	Refresh Reset Count								

Figure 8.7.1.6 Cross Counting

Enable: Enables the cross-counting statistics function.

Sensitivity: Filters small disturbing objects. The higher the sensitivity, the smaller the object can be detected. This can also be used to detect distant objects in the scene.

Dynamic Marking: Displays the detection box and used to turn on or off the detection rule line.

Type: Set the type of objects to be recognized in the cross-counting detection. There are three modes. Switchover or saving operation will clear the current count.

Motion: All objects, including pedestrians, vehicles, and cartons, will be detected.

Pedestrian: Only pedestrian objects will be recognized.

Motor Vehicle: Only motor vehicle objects will be recognized.

Non-motorized Vehicle: Only non-motorized vehicle objects will be recognized.

Alarm Number: Set conditions to trigger an alarm. The camera will trigger a cross-counting alarm when the count is updated and the in count minus the out count is greater or equal to the current setting.

Start Time: The time when the line-crossing detection function starts to work every day.

Start Time: The time when the line-crossing detection function stops working every day.

Rule Number: Only one detection rule line is supported for cross counting.

Rule Enable: Turn on or off the current rule line.

Rule Type: Set the direction to increase the in/out trigger count, that is, $A \rightarrow B$ and $B \rightarrow A$. For example, if $A \rightarrow B$ is selected, the in-count increases when the monitored object enters area A and leaves area B, and the out-count increases when the monitored object enters area B and leaves area A.

Reset Count: Clear the currently displayed count.

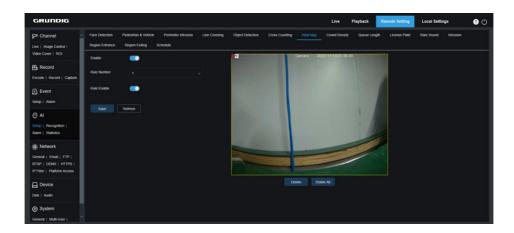


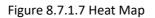
Line-crossing Setting Area: Allow to set the rule line for cross counting detection in this area.

Count Area: Displays cross counting statistics. For details, refer to Adjusting Display Location in Section 8.1.

8.7.1.7 Heat Map

You can set all areas or a specific area to detect the people activity information in the specified area. You can also save and upload changes at an interval of 10 minutes. The heat map can intuitively present people distribution in temporal and spatial dimensions for good understanding of activity degrees in each area in the scene. This function only supports data recording, not alarming.





Enable: Turn on or off the HM statistics.

Rule Number: Only one detection rule line is supported for HM.

Rule Enable: Turn on or off the current rule line.

Monitoring Area Setting: Set the areas for collecting heat statistics. By default, all areas are selected.

8.7.1.8 Crowd detection

Performs people counting and identify number of people in the monitored area. An alarm is triggered when the number of people exceeds the preset value.

GRUNDIG										Um	Playback	Reno	ote Setting	Local Settings		00
₽ Channel	Face Detection	Pedestrian & Vehicle	Perimeter Indusion	Line Crossing	Object Detection	Cross Counting	Heat Map	Crowd Density	Queue Length	License Plate	Rare Sound	Intrusion	Region Entrance	Region Exting	Schedule	
Live Image Control Video Cover ROI	Enable	-			Pre de O Avalació	. 10/	Cartora 22	23-11-06 13:39:24								
B Record	Sensibility								1							
Encode Record Capture	Dynamic Marking				-											
Deteo Airem	Min Pinel	32														
(O) Al	Max Ploat		1						1							
Swhip Recognition Alarm Statistics	Max Detection No	mber 50					-	1								
(g): Network	Detection Area	User defined														
General Email FTP RTSP DONS HTTPS	Rule Number					~										
IP Filter Platform Access	Rule Enable	-				De	Ante Dela	Nr A8								
Device																
Disk Audio	Save	Refeat														
System																
General Multi-User Maintenance Information																

Figure 8.7.1.8 Crowd Detection



Enable: Turn on or off the crowd detection function.

Sensitivity: Filter small disturbing objects. The higher the sensitivity, the smaller the object can be detected.

Dynamic Marking: Displays the detection box and used to turn on or off the detection rule line.

Min Pixel: Based on the 1080p resolution, filter out objects with heads smaller than the setting in the view. When the mouse is moved to the progress bar, the right image preview shows the actual size of the pixel box. You can also drag the pixel box to set it. When the mouse is moved away for 5 seconds, the pixel box in the image preview disappears.

Max Pixel: Based on the 1080p resolution, filter out objects with heads larger than the setting in the view. When the mouse is moved to the progress bar, the right image preview shows the actual size of the pixel box. You can also drag the pixel box to set it. When the mouse is moved away for 5 seconds, the pixel box in the image preview disappears.

Max Detection Number: Maximum number of heads that can be detected in the detection area. An alarm will be triggered when this value is exceeded.

Detection Area: Set the area where the crowd detection function will be applied. There are two modes.

Full Screen: In this mode, all areas covered by the camera will be detected.

User-defined: Only user-defined boxed areas are detected.

Rule Number: This number is displayed when you set a custom detection area. One detection rule line is supported.

Rule Enable: Turn on or off the current rule line. This switch is displayed when you set a custom detection area.

Detection Area Setting: This setting is available when you set a custom detection area. Supports setting the detection area of 3-8 sides.

Count Display Area: Displays the number of people in the current monitored area. For adjustment of display location, see Section 8.1.

8.7.1.9 Queue Length

Queue Length detection function set the people number in the queue and wait time. An alarm will be triggered when the queue is too long or the wait time is too long.

GRUNDIG										Live	Playback	Remo	te Setting	local Settings		• •
P Channel	Face Detection	Pedestrian & Vehicle	Perimeter Intrusion	Line Crossing	Object Detection	Cross Counting	Heat Map	Crowd Density	Queue Length	License Plate	Rare Sound	Intrusion	Region Entrance	Region Exiting	Schedule	
Live Image Control Video Cover ROI	Enable	•			n Daller O Sere		Cart-ara 20.	23-11-00 13 44 11								
B Record	Sensitivity				/											
Encode Record Capture	Dynamic Marking				Liberdefred											
Event Setup Alarm	Min Pixel	2	640													
() AI	Max Pixel	320	11													
Setup Recognition Alarm Statistics	Max Detection Nar	nber 10					-	-								
(a) Network	Max Pro Time			Ĵ (1 ~ 3600)												
General Email FTP RTSP DONS HTTPS IP Filter Platform Access	Delection Area	User-defined				04	ete Dese	to Al								
Device	Rule Number															
Disk Audio	Rule Enable	-														
System		Reliesh														
General Multi-User Maintenance Information																

Figure 8.7.1.9.1 Queue Lenght



Enable: Enable or disable the Queue Length detection function.

Sensitivity: Filter small disturbing objects. The higher the sensitivity, the smaller the object can be detected.

Dynamic Marking: Displays the detection box and used to turn on or off the detection rule line.

Min Pixel: Based on the 1080p resolution, filter out objects with heads smaller than the setting in the view. When the mouse is moved to the progress bar, the right image preview shows the actual size of the pixel box. You can also drag the pixel box to set it. When the mouse is moved away for 5 seconds, the pixel box in the image preview disappears.

Max Pixel: Based on the 1080p resolution, filter out objects with heads larger than the setting in the view. When the mouse is moved to the progress bar, the right image preview shows the actual size of the pixel box. You can also drag the pixel box to set it. When the mouse is moved away for 5 seconds, the pixel box in the image preview disappears.

Max Detection Number: Maximum number of heads that can be detected in the detection area. An alarm will be triggered when this value is exceeded.

Max Pro Time: The maximum duration allowed for people to stay in the detection area. An alarm will be triggered when the set duration is exceeded and no one leaves the detection area (This duration starts from the time when the last person leaves the detection area. If no one leaves within the set duration, the processing will be considered as timeout and an alarm will be triggered).

Note: Counting is restarted only when a target leaves the detection area. Counting will be ignored if the target in the area suddenly disappears. Counting is started only if a target is detected in the detection area.

Detection Range: Set the area where the queue detection function will be applied. There are two modes.

Full Screen: In this mode, all areas covered by the camera will be detected.

User-defined: Only user-defined boxed areas are detected.

Rule Number: Rule line number. This number is displayed when you set a custom detection area. One detection rule line is supported.

Rule Enable: Turn on or off the current rule line. This switch is displayed when you set a custom detection area.

Detection Area Setting: This setting is available when you set a custom detection area. Supports setting the detection area of 3-8 sides.

Detection Area Setting: This setting is available when you set a custom detection area. An octagonal detection area needs to be set.

Count Display Area: Displays the number of people in the current monitored area and queue time. For adjustment of display location, see Section 8.1.

8.7.1.10 License Plate

License plate detection function detects license plates of passing vehicles to determine whether vehicles are registered to the database or not. An alarm will be triggered where necessary. Therefore, the license plate detection function needs to be enabled.

Currently, the license plate detection function is only available for European and American regions.

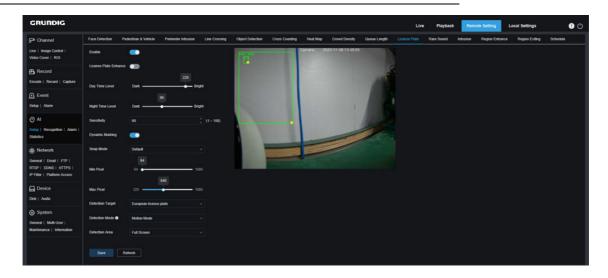


Figure 8.7.1.10.1 LPR Detection

Enable: Enable or disable the license plate detection function.

License plate Enhance: Enable or disable the License plate Enhance function. This function and WDR, HLC, as well as BLC are mutually exclusive. Therefore, they cannot be enabled simultaneously. If the enhancement mode is enabled, the shutter mode and exposure time also cannot be adjusted.

Day Time Level: When IR light is disabled for the camera, the higher the level, the brighter the image. Likewise, the lower the level, the dimmer the image. The level value ranges from 0 to 255 (Some models range from 0 to 150).

Night Time Level: When IR light is enabled for the camera, the higher the level, the brighter the image. Likewise, the lower the level, the dimmer the image. The level value ranges from 0 to 255 (Some models range from 0 to 150).

Note: The level can be adjusted only when License plate and License plate Enhance are both enabled. When the License plate Enhance mode is enabled, the image brightness is adjusted based on the specified value for the day mode and night mode respectively. The two modes do not interfere with each other as they are switched automatically depending on whether the camera IR light is enabled. In addition, the License plate Enhance mode and the exposure compensation of image control, as well as the shutter manual mode are mutually exclusive. Therefore, they cannot be enabled simultaneously. If the License plate Enhance mode is enabled, the time exposure of image control also cannot be changed.

Sensitivity: Filters small disturbing objects. The higher the sensitivity, the easier it is to detect an object.

Dynamic Marking: Displays the detection box and used to turn on or off the detection rule line.

Snap Mode: Set the snap mode. You can receive push notifications in live view or connect an NVR to check the image effect. The program supports three Snap Modes.

Default: The camera pushes only one license plate image from detecting an object until the object disappears.

RealTime Mode: When detecting an object, the camera immediately pushes one image, and then pushes another image when the object disappears.

Interval Mode: Push images at a set interval.

Min pixel: Minimum recognition pixel. Only license plates greater than the set minimum pixel can be recognized. When the mouse is moved to the progress bar, the right image preview shows the actual size of the pixel box. You

can also drag the pixel box to set it. When the mouse is moved away for 5 seconds, the pixel box in the image preview disappears.

Max pixel: Maximum recognition pixel. Only license plates lower than the set maximum pixel can be recognized. When the mouse is moved to the progress bar, the right image preview shows the actual size of the pixel box. You can also drag the pixel box to set it. When the mouse is moved away for 5 seconds, the pixel box in the image preview disappears.

Detection Target: Type of license plates to be detected. There are two type options.

European license plate: License plates in European regions.

American license plate: License plates in American regions.

Detection Mode: License plate detection mode. There are two mode options.

Hybrid Mode: In this mode, static license plates in the view will be detected.

Motion Mode: In this mode, motionless vehicles and their license plates will be filtered out and only license plates in motion will be detected.

Detection Area: Set the area where the license plate detection function will be applied. There are two type options.

Full Screen: Detection in full screen.

User-defined: Only user-defined boxed areas are detected, Supports setting the detection area of 3-8 sides.

8.7.1.11 Rare Sound

Rare Sound detection, here you can set different detection requirements depending on application requirements, for example, baby crying sound, gunshot, and dog barking. An alarm will be triggered when the camera detects the set sound.

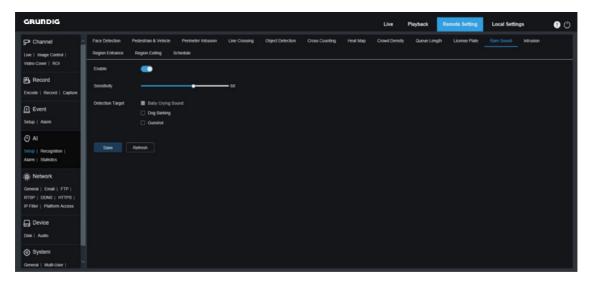


Figure 8.7.1.11.1 Rare Sound

Enable: Turn on or off the sound exception detection function.

Sensitivity: Sensitivity.1 indicates the minimum setting and 100 indicates the maximum setting.

Detection Target: Specify detection type.

Baby Crying Sound: A baby crying sound can be detected if this box is checked.

Dog Barking: A dog barking sound can be detected if this box is checked.

Gunshot: A gunshot sound can be detected if this box is checked.

8.7.1.12 Intrusion

The function will detect whether there is an object in the video to invade the set restricted area. Linkage alarm according to the judgment result.

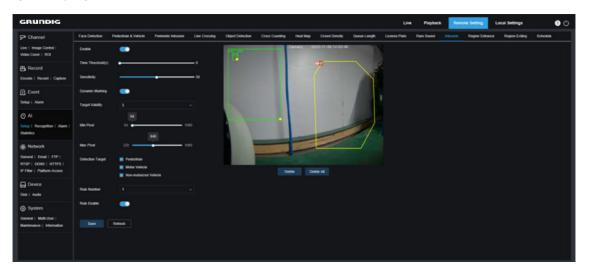


Figure 8.7.1.12.1 Intrusion

Enable: Enable the Intrusion detection function.

Time Threshold(s): Indicates that the alarm is generated after the target enters the alert area and stays there continuously for that amount of time. For example, if it is set to 1, the alarm will be triggered immediately after the target has invaded the area for 1s, and the maximum length of time can be set to 10s.

Sensitivity: The sensitivity is related to the percentage of the target that enters the area; the higher the sensitivity setting of Line Crossing, the more likely the alarm will be triggered. For example, if it is set to 100%, the alarm will be triggered when the detection target has just touched the boundary of the set area. If set to 50%, the alarm is triggered after 50% of the detection target has already crossed the boundary of the set area.

Dynamic Marking: Displays the detection box and used to turn on or off the detection rule line.

Target Validity: The similarity between the detection target and the set detection type.1 represents a similarity of 80% or more, 2 represents a similarity of 60% or more, 3 represents a similarity of 40% or more, 4 represents a similarity of 20% or more.

Min Pixel: Based on the 1080p resolution, filter out pedestrian or vehicle objects lower than the setting in the view. When the mouse is moved to the progress bar, the right image preview shows the actual size of the pixel box. You can also drag the pixel box to set it. When the mouse is moved away for 5 seconds, the pixel box in the image preview disappears.

Max Pixel: Based on the 1080p resolution, filter out pedestrian or vehicle objects greater than the setting in the view. When the mouse is moved to the progress bar, the right image preview shows the actual size of the pixel box.

You can also drag the pixel box to set it. When the mouse is moved away for 5 seconds, the pixel box in the image preview disappears.

Detection Target: Set objects for perimeter intrusion detection:

Pedestrian: A perimeter intrusion alarm is triggered only for pedestrians.

Motor Vehicle: A perimeter intrusion alarm is triggered only for motor vehicles.

Non-motorized Vehicle: A perimeter intrusion alarm is triggered only for non-motorized vehicles.

Rule Number: Allow to select a rule line number. Allow to set four detection rule lines.

Rule Enable: Turn on or off rule lines. Each rule line has an independent enable switch that is associated with the currently selected Rule Number.

Rule Line Setting Area: Allow to set, modify, and view edited rule lines. Supports setting the detection area of 3-8 sides

Delete: Allow to delete selected rule Lines in the rule line setting area.

Delete All: Allow to delete all rule lines.

8.7.1.13 Region Entrance

Region Entrance detection will detect targets entering the area from outside the area can be detected, and targets generated within the area will not generate an alarm, and the alarm will be linked according to the judgment result.

GRUNDIG										Live	Playback	Rem	ote Setting	Local Settings		00
P Channel	Face Detection	Pedestrian & Vehicle	Perimeter Intrusion	Line Crossing	Object Detection	Cross Counting	Heat Map	Crowd Density	Queue Length	License Plate	Rare Sound	Intrusion	Region Entrance	Region Exiting	Schedule	
Live Image Control Video Cover ROI	Enable	•			1			23-11-06 14 26 13								
B Record	Sensibility		•	<u> </u>			00									
Encode Record Capture	Dynamic Marking	-														
Event	Target Validity															
Setup Alarm									Aller							
(O) AI	Min Pixel	64	10						11000							
Selup Recognition Alarm Statistics	Max Pixel		640					-								
(a) Network	Detection Target	Pedestrian				Solution and										
General Email FTP RTSP DONS HTTPS		Motor Vehicle	Vehicle			-										
IP Filter Platform Access	Rule Number					De	nete Dela	te All								
Device																
Disk Audio	Rule Enable	-														
System		Reliesh														
General Multi-User Maintenance Information																
Mantenance (Information																

Figure 8.7.1.13 Region Entrance

Enable: Enable the Intrusion detection function.

Sensitivity: The sensitivity is related to the percentage of the target that enters the area; the higher the sensitivity setting of Line Crossing, the more likely the alarm will be triggered. For example, if it is set to 100%, the alarm will be triggered when the detection target has just touched the boundary of the set area. If set to 50%, the alarm is triggered after 50% of the detection target has already crossed the boundary of the set area.

Dynamic Marking: Displays the detection box and used to turn on or off the detection rule line.

Target Validity: The similarity between the detection target and the set detection type.1 represents a similarity of 80% or more, 2 represents a similarity of 60% or more, 3 represents a similarity of 40% or more, 4 represents a

similarity of 20% or more.

Min Pixel: Based on the 1080p resolution, filter out pedestrian or vehicle objects lower than the setting in the view. When the mouse is moved to the progress bar, the right image preview shows the actual size of the pixel box. You can also drag the pixel box to set it. When the mouse is moved away for 5 seconds, the pixel box in the image preview disappears.

Max Pixel: Based on the 1080p resolution, filter out pedestrian or vehicle objects greater than the setting in the view. When the mouse is moved to the progress bar, the right image preview shows the actual size of the pixel box. You can also drag the pixel box to set it. When the mouse is moved away for 5 seconds, the pixel box in the image preview disappears.

Detection Target: Set objects for perimeter intrusion detection:

Pedestrian: A perimeter intrusion alarm is triggered only for pedestrians.

Motor Vehicle: A perimeter intrusion alarm is triggered only for motor vehicles.

Non-motorized Vehicle: A perimeter intrusion alarm is triggered only for non-motorized vehicles.

Rule Number: Allow to select a rule line number. Allow to set four detection rule lines.

Rule Enable: Turn on or off rule lines. Each rule line has an independent enable switch that is associated with the currently selected Rule Number.

Rule Line Setting Area: Allow to set, modify, and view edited rule lines. Supports setting the detection area of 3-8 sides

Delete: Allow to delete selected rule Lines in the rule line setting area.

Delete All: Allow to delete all rule lines.

8.7.1.14 Region Exiting

Region exiting detection, can detect the target walking from the area to the outside of the area, and the target generated outside the area will not generate an alarm, and the alarm will be linked according to the judgment result.



Figure 8.7.1.14.1 Region Exiting

Enable: Enable the Intrusion detection function.

Sensitivity: The sensitivity is related to the percentage of the target that enters the area; the higher the sensitivity setting, the more likely the alarm will be triggered. For example, if it is set to 100%, the alarm will be triggered when the detection target has just touched the boundary of the set area. If set to 50%, the alarm is triggered after 50% of the detection target has already crossed the boundary of the set area.

Dynamic Marking: Displays the detection box and used to turn on or off the detection rule line.

Target Validity: The similarity between the detection target and the set detection type. 1 represents a similarity of 80% or more, 2 represents a similarity of 60% or more, 3 represents a similarity of 40% or more, 4 represents a similarity of 20% or more.

Min Pixel: Based on the 1080p resolution, filter out pedestrian or vehicle objects lower than the setting in the view. When the mouse is moved to the progress bar, the right image preview shows the actual size of the pixel box. You can also drag the pixel box to set it. When the mouse is moved away for 5 seconds, the pixel box in the image preview disappears.

Max Pixel: Based on the 1080p resolution, filter out pedestrian or vehicle objects greater than the setting in the view. When the mouse is moved to the progress bar, the right image preview shows the actual size of the pixel box. You can also drag the pixel box to set it. When the mouse is moved away for 5 seconds, the pixel box in the image preview disappears.

Detection Target: Set objects for perimeter intrusion detection:

Pedestrian: A perimeter intrusion alarm is triggered only for pedestrians.

Motor Vehicle: A perimeter intrusion alarm is triggered only for motor vehicles.

Non-motorized Vehicle: A perimeter intrusion alarm is triggered only for non-motorized vehicles.

Rule Number: Allow to select a rule line number. Allow to set four detection rule lines.

Rule Enable: Turn on or off rule lines. Each rule line has an independent enable switch that is associated with the currently selected Rule Number.

Rule Line Setting Area: Allow to set, modify, and view edited rule lines. Supports setting the detection area of 3-8 sides

Delete: Allow to delete selected rule Lines in the rule line setting area.

Delete All: Allow to delete all rule lines.

8.7.1.15 Al Schedule

The function of AI schedule, you can enable or disable this function, set the AI enable schedule.

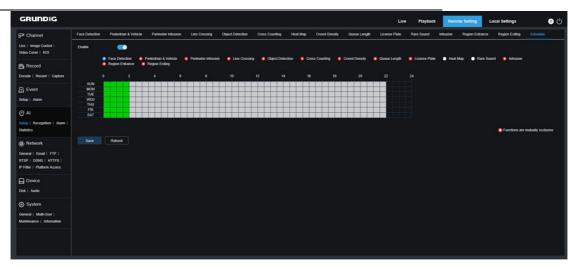


Figure 8.7.1.15.1 AI Schedule

Enable: Enable or disable the AI function schedule.

Functions are mutually exclusive: Functions that are mutually exclusive to the selected functions.

Note:

- Functions that are mutually exclusive cannot be set at the same time. That is, two mutually exclusive AI functions cannot be enabled at the same time. There will be restrictions on this UI.
- After the AI schedule is enabled, all AI function switches for the channel can no longer be manually enabled or disabled and are controlled by the schedule. However, parameters such as sensitivity can be edited.
- When setting up the face detection function schedule for the first time, the user will be prompted to check and agree to the face privacy agreement. If the user unchecks it, the time period corresponding to the face detection function in the AI schedule will be cleared.

8.7.2 Recognition

8.7.2.1 Face Recognition

Face recognition function, the focus is to recognize the identity of a detection object and use base data for comparison. The program establishes a database for face matching using the database management function.

Note: Changes to the database take full effect after the system reloads data for a short period of time.

GRUNDIG				Live Playback	Remote Setting Local Settings
P Channel	Face Database Management	License Plate Management			
Live Image Control		Group Name	Delete	Edit	Enable
Video Cover ROI		Allow List			
B Record		Block List			
Encode Record Capture		Stranger			
0-		Group 1			
Event Setup Alarm Event Push					
Al Setup Recegnition Alarm Statefics Statefics Metwork General Email FTP RESP Dorks HTTPS P Piere Dorkice Disk Audie Cloud System					
General Multi-User Maintenance Information					

Figure 8.7.2.1.1 Face Recognition

Alarm Policy Display: This serves as a policy prompt only in the camera. Green indicates the allow list, red indicates the block list, and colorless indicates the stranger group.

Group Name: Edit, modify, and view the current group name. A group name will be pushed together with an alarm.

Delete: Delete a group. The first three group cannot be deleted.

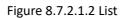
Edit: Open the image setting example for this group. For details, please continue editing the content on the next image.

Enable: Open the face recognition function for data comparison between groups.

Add Group: Allow to add a new database group. Up to 16 database groups can be added.

You can click the **Edit** icon to set the reference for the corresponding group. The view is shown in the figure below.

GRUNDIG							
	caonunguan_0_0		Face Information				
			Name	cabiunguan_0_0_jg	3 (182)		
	Detail Information		Sex	Male		63	
	Move To		Age				
	Edit		Country				
	Delete		Nation				
			ld Code				
			Occupation				
			Phone				
			Email Residence				
			Residence				
			Remark				
		8 K 1					
					Delete		



Added Image Display Area: Displays images that have been added to groups in the face database.

Info: Displays the editing information of the selected image.

Detail Information: Right click event to check the information of the selected image.



Move To ...: Right click event to move the selected image to other groups.

Edit: Right click event to open the editing interface of the selected image to edit the information again.

Delete: Right click event to delete the selected image.

Import: Add new face data in the current group and import local images or captured images by the camera.

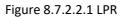
Delete: Delete face data in batches in the database. You can click this icon, select the image to be deleted, and then click the Delete icon again to delete the image.

8.7.2.2 License Plate Recognition

License plate recognition function, the focus is to recognize the identity of a detection object and use base data for comparison. The program establishes a database for license plate matching using the database management function.

Note: Changes to the database take full effect after the system re	eloads data for a short period of tim	ıe.

GRUNDIG				Live Playback	Remote Setting Loc	al Settings	0
P Channel	Face Database Management License	Plate Management					
Live Image Control		Group Name	Delete	Edit		Enable	
Video Cover ROI		Allow List					
B Record		Block List					
Encode Record Capture		Unkown					
Event		Group 1					
Setup Alarm Event Push							
 Al Setup Recognition Alarm Statistica Network 	Add Group, Save Park						
General Email FTP RTSP DDNS HTTPS IP Filter							
Disk Audio Cloud							
General Multi-User Maintenance Information							



Alarm Policy Display: This serves as a policy prompt only in the camera. Green indicates the allow list, red indicates the block list, and colorless indicates the unknown license plate list.

Group Name: Edit, modify, and view the current group name. A group name will be pushed together with an alarm.

Delete: Delete a group. The first three groups cannot be deleted.

Edit: Open the image setting example for this group. For details, please continue editing the content on the next image.

You can click the **Edit** icon to set the reference data for the corresponding group. The view is shown in the figure below.

	Edit	License Plate	Color	Car Brand	Car Type	Owner	Gender	ld Code	Plate Detail		
Record		W5074 PRA	Blue	нјнјн	Volkswagen	GSY5DGDXGH	Male		License Plate	W5074 PRA	
le Record Capture		W5075 PRA	Blue	нјнјн	Volkswagen	GSY5DGDXGH	Male	5174			
		W5076 PRA	Blue	HJHJH	Volkswagen	GSY5DGDXGH	Male	5175	Color	Blue	
vent 🛛		W5077 PRA	Blue	HJHJH	Volkswagen	GSY5DGDXGH	Male	5176	Car Brand	нјнјн	
		W5078 PRA	Blue	НЈНЈН	Volkswagen	GSY5DGDXGH	Male		Car Type	Volkswagen	
Alarm		W5079 PRA	Blue	HJHJH	Volkswagen	GSY5DGDXGH	Male	5178			
u 🖉		W5080 PRA	Blue	нјнјн	Volkswagen	GSY5DGDXGH	Male	5179	Owner	GSY5DGDXGH	
N		W5081 PRA	Blue	HJHJH	Volkswagen	GSY5DGDXGH	Male	5180	Gender	Male	
Recognition Alarm		W5082 PRA	Blue	нјнјн	Volkswagen	GSY5DGDXGH	Male	5181	Phone	2217284	
ics 🛛 🖸		W5083 PRA	Blue	нјнјн	Volkswagen	GSY5DGDXGH	Male	5182			
		W5084 PRA	Blue	нјнјн	Volkswagen	GSY5DGDXGH	Male	5183	ld Code		
Vetwork		W5085 PRA	Blue	HJHJH	Volkswagen	GSY5DGDXGH	Male	5184			
al Email FTP		W5086 PRA	Blue	нјнјн	Volkswagen	GSY5DGDXGH	Male	5185	Occupation		
DONS HTTPS		W5087 PRA	Blue	HJHJH	Volkswagen	GSY5DGDXGH	Male	5186	22222		
er		W5088 PRA	Blue	HJHJH	Volkswagen	GSY5DGDXGH	Male	5187	Residence		
		W5089 PRA	Blue	нјнјн	Volkswagen	GSY5DGDXGH	Male	5188			
Device		W5090 PRA	Blue	нјнјн	Volkswagen	GSY5DGDXGH	Male	5189	51534		
		W5091 PRA	Blue	HJHJH	Volkswagen	GSY5DGDXGH	Male	5190	Remark		
									agregaegea		

Figure 8.7.2.2.2 Edit List

There are three ways to add license plate information: Import, Import From CSV, and Import From Local Capture.

- 1) You can click the **Import** button to manually add individual entries of license plate information.
- 2) You can click the **Import from CSV** button to import one or multiple data entries from CSV. The CSV sheet is formatted as follows:

A B	C D E F	G H I J K	LM	N	0	P	Q	R	S	T	U	V	¥	X	Y	- 7
License FColor	Car BrancCar Type Owner Sex	Id Code Phone OccupaticResidenceRemark														
粤C-3R525blue	HJHJH VolkswageYHJ male	2222 2212211 22222 46461 FFQFQFQ														
A-HP-233 white	HJH NOMAL UYUU male	101 11111 LLLL KKLKLK FQFQWQ														
MCY164J black	BEEB NOMAL QQQQ female															
FLB-360 black	R23R2AD KDGS QRQD female															
MA 5465 Cwhite	TWVAGA 3FSWF FWFFWF female															
GC 9671 Cwhite	RGWTWZGEAWEGWTG WTAZHRT female	105 2, 35E+09 WAWAGEG AGHAG AGEY														
LH66 BUE white	GASRJHDFJWTASDSF ATYDFZDY%male	106 3.47E+08 Ftqta agshsrh agregaege	a													
R21 ROY white	HEH T4T34 AVETAT male	107 SJYTEFG HRJFFXHD STUUROFYKETOKH														
DE14 LVP white	ETUURHS 4YAGRG AERTWYDFEmale	108 45634 VECARGA AFSCS KUKTT														
1218 LGT white	HSHRTHST YEYGD GSY5DGDXGmale	109 4673T387ESGEG SDGSHHRTFTRYRTHFX														
W12 PRA yellow	CRECACAC ACEACE GA4TGZVZ female															
W13 PRA blue	HIHIH WEGWIG GSY5DGDXCmale	112 2212223 22222 46473 FFQFQFQ														
W14 PRA blue	HIHIH WEGWIG GSY5DGDXCmale	113 2212224 22222 46474 F0F0W0														
W15 PRA blue	HJHJH WEGWIG GSY5DGDXCmale	114 2212225 22222 46475 QT#F														
W16 PRA blue	HIHIH WEGWIG GSY5DGDXCmale	115 2212226 22222 46476 GWTTWE														
W17 PRA blue	HJHJH WEGWIG GSY5DGDXCmale	116 2212227 22222 46477 FWFWA														
W18 PRA blue	HJHJH WEGWIG GSY5DGDXCmale	117 2212228 22222 46478 AGEY														
W19 PRA blue	HIHIH WEGWIG GSY5DGDXCmale	118 2212229 22222 46479 agregaege														
W20 PRA blue	HIHIH WEGWIG GSY5DGDXCmale	119 2212230 22222 46480 ETOKH	a													
W21 PRA blue	HJHJH WEGWIG CSY5DCDXCmale	120 2212230 22222 40400 ETORN														
W22 PRA blue	HIHIH WEGWIG GSY5DGDXCmale	120 2212231 22222 40481 KOK11 121 2212232 22222 46482 TRYRTHFX														
W23 PRA blue	HIHIH VEGVIG GSY5DGDXCaale	122 2212233 22222 46483 ¥GAA														
W24 PRA blue	HJHJH WEGWIG GSY5DGDXCmale	123 2212234 22222 46484 FFQFQFQ														
W25 PRA blue	HIHIH WEGWIG GSY5DGDXCmale	125 2212235 22222 46485 F0F0W0														
W26 PRA blue	HIHIH VEGVIC CSY5DCDXCaale	124 2212235 22222 40465 PQPQ4Q 125 2212236 22222 46486 QTWF														
W27 PRA blue	HIHIH VolkswageGSY5DGDXCmale	125 2212230 22222 90980 Q18P 126 2212237 22222 46487 GWTTWE														
W28 PRA blue	HJHJH VolkswageGSY5DGDXCmale	127 2212238 22222 46488 FVFVA														
#29 PRA blue	HJHJH VolkswageGSY5DGDXCmale	128 2212239 22222 46489 ACEY														
W30 PRA blue	HJHJH VolkswageGSY5DGDXCmale	129 2212240 22222 46490 agregaege	8													
W31 PRA blue	HJHJH VolkswageGSY5DGDXCmale	130 2212241 22222 46491 ETOKH														
W32 PRA blue	HJHJH VolkswageGSY5DGDXCmale	131 2212242 22222 46492 KUKTT														
W33 PRA blue	HJHJH VolkswageGSY5DGDXCmale	132 2212243 22222 46493 TRYRTHFX														
W34 PRA blue	HJHJH VolkswageGSY5DGDXGmale	133 2212244 22222 46494 WGAA														
W35 PRA blue	HJHJH VolkswageGSY5DGDXCmale	134 2212245 22222 46495 FFQFQFQ														
W36 PRA blue	HJHJH VolkswageGSY5DGDXCmale	135 2212246 22222 46496 FQFQWQ														
W37 PRA blue	HJHJH VolkswageGSY5DGDXGmale	136 2212247 22222 46497 QTWF														
W38 PRA blue	HJHJH VolkswageGSY5DGDXCmale	137 2212248 22222 46498 GWTTWE														
#39 PRA blue	HJHJH VolkswageGSY5DGDXCmale	138 2212249 22222 46499 FWFWA														
#40 PRA blue	HJHJH VolkswageGSY5DGDXCaale	139 2212250 22222 46500 ACEY														
#41 PRA blue	HIHIH VolkswageGSY5DGDXCmale	140 2212251 22222 46501 agregaege	a													
W40.004 1.1	mann, m.ll	1.41 00100E0 00000 44E00 ETOUT														
 	入5000 ④					1 4										

Figure 8.7.2.2.3 List

Select the license plate file in CSV format you want to import and click the Import button to add it to the group. You can click the Delete button to delete unwanted license plate information, as shown in the figure below.

Image Control Cover												× Enable	
		Status	Edit	License Plate	Color	Car Brand	Car Type	Owner	Gender	Plate Detail			
		0		W5002 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male				
		Ō		W5003 PRA	Blue	нинин	Volkswagen	GSY5DGDXGH	Male	License Plate	W5002 PRA		
		0		W5004 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	Color	Blue		
		0		W5005 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	Car Brand	нјнјн		
		0		W5006 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	Car Type	Volkswagen		
				W5007 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male				
		\odot		W5008 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	Owner	GSY5DGDXGH		
		0		W5009 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	Gender	Male		
				W5010 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	Phone	2217212		
		O		W5011 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	ld Code			
		O		W5012 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	5101			
		O		W5013 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male				
		0		W5014 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	Occupation			
		O		W5015 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	22222			
		0		W5016 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	Residence			
		O		W5017 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	51462			
				W5018 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	Remark			
		O	e_	W5019 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	FFQFQFQ			
	<								< 1 / 278				

Figure 8.7.2.2.4 Import CSV

Note: When more than 5000 data entries will be added, a dialog box indicating "Data entries exceed the upper limit" will appear.

3) You can click the Import From Capture button to import license plate information from a local directory to the database.

									θ
				Please Select Image					
	Start time 2022-10-27		End time 2022-10-2		1Day	~ •			
		2022-10-27 14:59:38	2022-10-27 14:59:53	2022-10-27 14 59 54					
	MK 9903	658:1362	TILIZED IN TELLE	TENDORUS					
		CHI	CHI	СНІ					
Device									
neral Multi-User									

Figure 8.7.2.2.5 Import Capture

You can select the date, duration, and Alarm Group, and then click the **Search** button to retrieve all the license plates saved by the device within this time range.

All: select all license plate information.

	Status	Edit	License Plate W5002 PRA	Color Blue	Car Brand	Car Type Volkswagen	Owner GSY5DGDXGH	Gender Male	Plate Detail			
		0	W5002 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	License Plate	W5018 PRA	-	
		2	W5004 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	Color	Green	-	
		0	W5005 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	Car Brand	нјнјн		
			W5006 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	Car Type	Volkswagen		
			W5007 PRA	Blue	нјнјн	Volkswagen	GSY5DGDXGH	Male				
			W5008 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	Owner	GSY5DGDXGH		
			W5009 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	Gender	Male		
			W5010 PRA	Blue	нјнјн	Volkswagen	GSY5DGDXGH	Male	Phone	2217228		
			W5011 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	ld Code			
			W5012 PRA	Blue	нјнјн	Volkswagen	GSY5DGDXGH	Male	5117			
			W5013 PRA	Blue	нјнјн	Volkswagen	GSY5DGDXGH	Male				
			W5014 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	Occupation			
			W5015 PRA	Blue	нунун	Volkswagen	GSY5DGDXGH	Male	22222			
			W5016 PRA	Blue	нјнјн	Volkswagen	GSY5DGDXGH	Male	Residence			
			W5017 PRA	Blue	нјнјн	Volkswagen	GSY5DGDXGH	Male	51478			
			W5018 PRA	Green	нунун	Volkswagen	GSY5DGDXGH	Male	Remark			
	٢	e	W5019 PRA	Blue	нинин	Volkswagen	GSY5DGDXGH	Male	AGEY			
								< 1 / 278				

Figure 8.7.2.2.6 Import All

You can click a data entry to edit the corresponding license plate information. Then, you can click the **Save** button to save changes. Upon completion of change, will changes to

- 4) **Delete:** check the checkbox next to the license plate information and then click this button to delete the information.
- 5) **Move to...:** Check the checkbox next to the license plate information and then click this button to move the information to other groups.
- 6) You can click the **Export** button to export the information of the entire group and then save it.

1.Enable: Turn on or off the license plate recognition function for data comparison between groups.

2.Add Group: Allow to add a new database group. Up to 16 database groups can be added.

8.7.3 Alarm Setup

Alarm response to AI functions of the camera can be divided into three categories in the implementation dimension:

Category I includes Face Detection, Face Features, Pedestrian & Vehicle, Perimeter Intrusion, Line Crossing, Object Detection, Cross Counting, Crowd Density, Queue Length, License Plate, Rare Sound, Intrusion, Region Entrance, Region Exiting. Alarm response will be generated directly if alarm conditions are met as determined by the camera.

Category II includes Face Recognition and License Plate Recognition. The camera captures an alarm image and recognizes the facial characteristic value or license plate information in the image, then compares it with the information in the database, and finally generates an alarm response according to the alarm group setting.

Category III includes Face Attendance. Automatically search data at a specific time to generate alarm push email.

8.7.3.1 Face Detection, Face Features, Pedestrian & Vehicle, Perimeter Intrusion, Line Crossing, Object

Detection, Cross Counting, Crowd Density, Queue Length, License Plate, Rare Sound, Intrusion,

Region Entrance, Region Exiting

Alarm response will be generated directly if alarm conditions are met as determined by the camera.

GRUNDIG									E	Live Playbaci	Remote Set	ting Local t	lettings	• •
Channel Uve Image Control		Face Recognition are Sound		atures Licens Region Entrance	Plate Recognition Region Exiting	Pedestrian & Vehicle	Perimeter Intrusion	Line Crossing	Object Detection	Cross Counting	Face Attendance	Crowd Density	Queue Length	
Video Cover ROI	Alarm Type	Close												
B Record Encode Record Capture	Latch Time													
Event	Post Recording													
Setup Alarm	Send Email	•												
() AI	Event Push Platform	•												
Setup Recognition Alarm Statistics	Alarm Out	•												
() Network	Light	-												
General Email FTP RTSP DONS HTTPS IP Fiber Platform Access	Warn Light	•												
	Siren	-												
Device Disk Audio	FTP Picture Upload	-												
 System General Multi-User 	FTP Video Upload	•												
Maintenance Information	Save S	ichedule 🗌	Refresh											

Figure 8.7.3.1.1 Alarm Settings

Alarm Type: This option is specific to Face Features alarms. Enable the face attribute recognition function for Face Features alarms according to Section 8.7.1.1. An alarm will be generated to alert whether the detected object wears a mask. There are three mode options.

Close: Face Features alarms are disabled.

NO Mask: An alarm is generated when the detected object is not wearing a mask.

Wear Mask: An alarm is generated when the detected object is wearing a mask.

Latch Time: Specifies the duration of an I/O alarm after the alarm is cleared.

Note: The camera must support the I/O feature and the working time is controlled by the schedule.

Post Recording: Specifies the duration of recording after the alarm is cleared.

Note: The effective time is also controlled by the schedule.

Send Email: Specifies whether to send an email when an alarm is being triggered.

Note: The effective time is also controlled by the schedule.

Event push Platform: If this option is set to ON, this type of information will be pushed to the **client when an alarm is triggered.**

Alarm Out: Specifies whether to enable Latch Time.

Light: White light deterrence switch. When an alarm is triggered, the alarm is reported in accordance with the warning light configuration on the **Deterrence** screen (GUI path: **Remote Setting > Event > Setup > Deterrence**). **Note:** Only **s**ome models support White light.

Warn Light: Warning light deterrence switch. When an alarm is triggered, the alarm is reported in accordance with the warning light configuration on the **Deterrence** screen (GUI path: **Remote Setting > Event > Setup > Deterrence**).

Note: Only some models support warning light.

Siren: Siren deterrence switch. When an alarm is triggered, the alarm is reported in accordance with the siren configuration on the **Siren** screen (GUI path: **Remote Setting > Event > Setup > Siren**).

Note: Only some models support siren deterrence.

FTP Picture Upload: Specifies whether to send pictures to the associated FTP server when an alarm is being triggered. If the alarm is continuously triggered, the pictures will be sent at an interval of 10s until the alarm is cleared.

Note: The effective time is also controlled by the schedule and the FTP server shall be associated in advance.

FTP Video Upload: Specifies whether to send videos to the associated FTP server when an alarm is being triggered. If the alarm is continuously triggered, the videos will be sent at an interval of 10s until the alarm is cleared.

Note: The effective time is also controlled by the schedule and the FTP server shall be associated in advance.

Enable Record: Specifies whether to enable Post Recording.

Schedule: configure the schedule of Send Email, Alarm Out, FTP Picture Upload, FTP Video Upload, Cloud Picture, Cloud Video, Record, Light (Deterrent), and Siren (Deterrent) for the current alarm.

Note: The white light deterrence feature is available for some models.

8.7.3.2 Face Recognition

Face recognition function, the camera captures a face image and retrieve matching face data from the database to obtain the group the object is in. Then, the camera generates an alarm by calling out the alarm setting in this group. Changes to parameters take effect after the system reloads data for a short period of time.

GRUNDIG							Live	Playback	Remote Setting	Local Settings
Channel	Face Detection Queue Length	Face Recognito	n Face Features Lic Rare Sound Intrusion	cense Plate Recognition Pedestriar Region Entrance Region Exit	N& Vehicle Perimeter Intrusion	n Line	Crossing	Object Detection	Cross Counting	Face Attendance Crowd Density
Video Cover ROI			Group Name	Enable	Policy		Simil	larity	Alarm	Alarm Schedule
B Record					Allow					
Encode Record Capture					Deny					
					Stranger					
Event					Allow ~					
etup Recognition tarm Statistics		Refresh								
) Network										
eneral Email FTP TSP DONS HTTPS										
Filter Platform Access										
Device										
Disk Audio										
System										
eneral Multi-User 🎽										

Figure 8.7.3.2.1 Face Recognition

Group Name: Edit, modify, and view the current group name. A group name will be pushed together with an alarm in the live view.

Enable: Specifies whether to enable alarm response settings.

Policy: Alarm policy. The first three groups cannot be edited and other groups can be customized as Allow or Deny.

Similarity: An alarm is triggered when the similarity exceeds the threshold during face matching.

Alarm: Specifies whether to enable group alarm settings.



					Face Attendance	Crowd Density	Queue Length
			Allow List				
	Latch Time	10s			Alarm		
	Lattin nine	105					
	Alarm Out	•					
	Face Capture	_					
	Send Ernail	•					
	FTP Picture Uplo	ad 💽					

Figure 8.7.3.2.2 Allow List

Alarm Schedule: Specifies the effective time of the Send Email, Alarm Out, FTP Picture Upload, and Cloud Picture settings.

Latch Time: Specifies the duration of an I/O alarm after the camera captures the image and successfully retrieves the matched image in the database.

Note: The camera must support the I/O feature and the working time is controlled by the schedule.

Alarm Out Latch Time: Specifies whether to enable settings.

Save Picture: Specifies whether to save face images to the memory card.

This setting is not controlled by the Enable status.

Save the Background: Specifies whether to save face images to the memory card and at the same time save background images.

This setting is not controlled by the Enable status.

Send Email: Specifies whether to send an email when faces in the group are recognized and matched.

Note: The effective time is also controlled by the schedule.

FTP Picture Upload: Specifies whether to send pictures to the associated FTP server when faces in the group are recognized and matched.

Note: The effective time is also controlled by the schedule and the FTP server shall be associated in advance.

Cloud Picture: Specifies whether to send pictures to the associated cloud storage server when faces in the group are recognized and matched.

Note: The effective time is also controlled by the schedule and the cloud storage server shall be associated in advance.

8.7.3.3 Face Attendance

The face attendance (FA) function is used to retrieve face matching status in different groups (excluding stranger group) saved in the memory card in a specified period of time, and generate attendance files according to capture records, and send these files to the associated email address.

GRUNDIG							Live	Playback	Remote Setting	Local Settings	• එ
P Channel	Face Detection	Face Recognition	Face Feature	s License Plate Recognit	on Pedestrian & Vehicle	Perimeter Intrusion	Line Crossing	Object Detection	Cross Counting	Face Attendance	Crowd Density
Live Image Control	Queue Length	License Plate	Rare Sound	Intrusion Region Entranc	e Region Exiting						
Video Cover ROI	Enable										
B Record	Send Email	08 : 30	. 00								
Encode Record Capture	Cond Crital	00.30									
Event	ON DUTY										
Setup Alarm	OFF DUTY	17 : 30									
() AI	UTP DUTT	17 : 30	. 00								
Setup Recognition	Mode	Day									
Alarm Statistics	Working Days										
(a) Network			TUE 🗾 WED	🗖 THU 🗾 FRI 🗌 SAT	SUN						
General Email FTP	Group	AI									
RTSP DDNS HTTPS	Group		II 3 II 4 II	5 2 6 2 7 2 8 2 9	9 🖬 10 📓 11 📓 12 📓	13 🖬 14 🖬 15 💌 1	16				
IP Filter Platform Access											
Device		Refresh									
Disk Audio											
System											
General Multi-User											

Figure 8.7.3.3.1 Face Attendance

Enable: Enable or disable the automatic face attendance file generation function.

Send Email: Specifies the time to send face attendance status. The program will make retrieval at a certain interval. When the retrieval time is greater than the set time, an attendance record file is automatically generated and an email is sent.

Note: No email will be sent if no attendance record is available.

ON DUTY: Specifies the on-duty reference time to generate an attendance file.

OFF DUTY: Specifies the off-duty reference time to generate an attendance file.

Mode: Specifies the time to generate and send an attendance file. There are three mode options.

Day: Allow to send the attendance record file of the day before.

Week: For example, if it is set to Wednesday, the attendance information from last Wednesday to this Tuesday will be sent.

Month: For example, if it is set to the 15th day, the attendance information from the 15th day of the last month to the 14th day of this month will be sent.

Working days: Specifies the on-duty reference working days to generate an attendance file.

Group: Specifies the group subject to attendance check when an attendance file is generated.

Note: This function is unavailable for the stranger group and grayed out for group 3 by default.

8.7.4 Statistics

AI-enabled statistical analysis function.

8.7.4.1 Face Recognition

Face image statistical analysis function, this function allows to retrieve face data statistics stored in the memory card according to search settings. The screen is shown in the figure below.

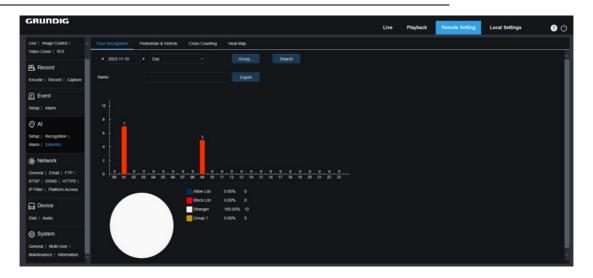


Figure 8.7.4.1.1 Face Recognition Statistic

Time: Specifies the reference time for the Search Mode.

Search Mode: Specify Day, Week, Month, Quarter, and Year as time range for data retrieval.

Group: Specifies the group subject to retrieval when statistical data is being retrieved.

Search: Allow to re-initiate data retrieval according to the current search settings.

Export: You need to give a name to an exported file. Export current search results to an Excel file.

Display Area: Displays search results in a graph below.

8.7.4.2 Pedestrian & Vehicle

Pedestrian and Vehicle statistics, including Pedestrian & Vehicle, Perimeter Intrusion, Line Crossing, Intrusion, Region Entrance, Region Exiting alarms. The screen is shown in the figure below.

GRUNDIG						Live	Playback	Remote Setting	Local Settings	0 ()
Live Image Control	Face Recognition	Pedestrian & Vehicle	Cross Counting	Heat Map						
B Record	4 2023-11-10	• Day		inteligent	Search					
Encode Record Capture	Name									
Event										
Setup Alarm										
© AI	8 6									
Setup Recognition Alarm Statistics										
(a) Network										
General Email FTP RTSP DDNS HTTPS	0 0, 0, 0	<u>0,0,0,0,0</u> 03 04 05 06	0,0,0,0,0,0 07 08 09 10 11	<u>, 0 , 0 , 0 , 0</u> 12 13 14 15	<u>, 0 , 0 , 0 , 0 , 0 , 0 , 0 , 0 , 0 , 0</u>					
IP Filter Platform Access										
Device										
Disk Audio										
General Multi-User Maintenance Information										

Figure 8.7.2.4.1 P & V Statistic

Time: Specifies the reference time for the Search Mode.

Search Mode: Specify Day, Week, Month, Quarter, and Year as time range for data retrieval.

Intelligent: Allow to perform search according to tag type of captured images, including Perimeter Intrusion [Human], Perimeter Intrusion [Motor Vehicle], Perimeter Intrusion [Non-motorized Vehicle], Line Crossing [Human], Line Crossing [Motor Vehicle], Line Crossing [Non-motorized Vehicle], Human, Motor Vehicle, Non-motorized Vehicle , Intrusion[Human], Intrusion[Motor Vehicle], Intrusion[Non-motorized Vehicle], Region Entrance[Human], Region Entrance[Motor Vehicle], Region Entrance[Non-motorized Vehicle], Region Exiting[Human], Region Exiting[Motor Vehicle], Region Exiting[Non-motorized Vehicle].

Search: Allow to re-initiate data retrieval according to the current search settings.

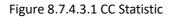
Export: You need to give a name to an exported file. Export current search results to an Excel file.

Display Area: Displays search results in a graph.

8.7.4.3 Cross Counting Statistics

Cross counting statistics function, the screen is shown in the figure below.

GRUNDIG					Live	Playback	Remote Setting	Local Settings	0 C
Live Image Control /	Face Recognition	Pedestrian & Vehicle	Cross Counting	Heat Map					
B Record	Report Type	Daily Report							
Encode Record Capture	Detection Target	Motion							
🕞 Event	Cross Type	Cross in							
Setup Alarm	Name								
@ AI	Date	2023-11-10							
Setup Recognition									
	Column Chart	 Line Chart 							
Alarm Statistics	Column Chart	 Lise Chart 	Statistics time (he	ours)			Cross In		
Alarm Statistics	Column Chart	 Line Chart 	Statistics time (ho 00.00-02.59	ours)			Cross In 0		
Alarm Statistics	Column Chart	Line Chart	00.00-00.59 01.00-01.59						
Alarm Solistics): Network General Email FTP RTSP DONS HTTPS	Column Chart	Line Chart	00 00-00 59 01:00-01:59 02:00-02:59						
Alarm Statistics	Column Chart	Lise Chart	00 00-00 59 01 00-01 59 02 00-02 59 03 00-03 59						
Aarm Statistics): Network Ceneral Email FTP RTSP DONS HTTPS P Filter Platform Access	Column Chart	Lise Chart	00.00-00.59 01.00-01.59 02.00-02.59 03.00-03.59 04.00-04.59						
Nami Statistics Network Ceneral Email FTP RTSP DONS HTTPS P Filter Pattom Access Device	Column Chart	Line Chart	00 00 00 09 59 01 00 01 59 02 00 02 59 03 00 03 59 04 00 04 59 05 00 05 59						
Nami Statistics Network Ceneral Email FTP RTSP DONS HTTPS P Filter Pattom Access Device	Column Chart	 Lite Chart 	00 00 00 09 59 01 00 01 59 02 00 02 59 03 00 03 59 04 00 04 59 05 00 05 59 06 00 06 59						
Alarm Statedics	Column Chart	 Lite Chart 	00 00 00 59 01 00 01 59 02 00 02 59 03 00 03 59 04 00 04 59 05 00 05 59 06 00 06 59 07 00 07 59						
Alam Stutistics (i): Network Deereral Email FTP ETEP Devis HTTPS P Filter Platform Access Device Device Det, Austo	Column Chart	● Line Chart	00.00-00.59 01.00-01.59 02.00-02.59 04.00-04.59 06.00-04.59 06.00-06.59 07.00-07.59 06.00-06.59						
Alam Tantos	Column Chart	Line Chart	00 00 00 59 01 00 01 59 02 00 02 59 03 00 03 59 04 00 04 59 05 00 05 59 06 00 06 59 07 00 07 59						



Report Type: The options include Daily report, Weekly report, Monthly report, and Annual report.

Detection Target: Set your desired alarm model. For example, you cannot retrieve motion-triggered data if alarm models other than motion model are selected. There are three model options including Motion, Person, and Vehicle, corresponding to their function settings.

Cross Type: Allow to search for data according to cross counting (CC) statistics. There are two mode options, including Cross In and Cross Out.

Export: You need to give a name to an exported file. Export current search results to an Excel file.

System time: Specifies the reference time for the selected report type.

Mode: Specifies whether to display graphs in the icon display area in a column or line chart.

Display Area: Displays search results in a graph.

Search: search for data according to current settings.

8.7.4.4 Heat Map

The heat map can intuitively present people distribution in temporal or spatial dimension.

① **Space heat map:** People activity degree in different areas in the view. Red indicates the densest area, meaning the highest activity degree, and blue indicates the lowest dense area.

(2) **Time heat map:** People activity degree in different times in the view. The Y-axis value is the index calculated based on the number of people and the duration of stay. The higher the value is, the higher the activity degree will be. It does not represent the number of people.

The smart camera must be equipped with a SD disk with free space in which heat map information will be stored. The screen is shown in the figure below.

GRUNDIG								Live	Playback	Remote Setting	Local Settings	
P Channel	Face Recognition	Pedestrian & Vehicle	Cross Counting	Heat Map	P.							
Live Image Control Video Cover ROI	Report Type	Daily Report										
B Record	Date	2023-11-10										
Encode Record Capture	Start Time	00.00										
庄 Event	End Time	23.59										
Setup Alarm	Space Heat Map	 Time Heat Map 										
Al Setup Recognition Alarm Statistics	Spatial density legend	L										
Network General Email FTP RTSP DDNS HTTPS IP Filter Platform Access	A.		Camera									
Device	2.1		-		-	-						
System												
General Multi-User Maintenance Information	-				The second							

Figure 8.7.4.4.1 Heat Map

Report Type: The options include Daily report, Weekly report, Monthly report, and Annual report.

Date: Specifies the reference date for data search.

Start Hour: This option is available only for Daily report and used to set the hour to start searching.

End Hour: This option is available only for Daily report and used to set the hour to end searching.

Mode: Specifies the data display mode. There are two mode options including graph and table.

Display Area: Displays the change frequency of monitored areas as a graph, and displays the change frequency of monitored areas in different time periods as a table.

Search: Search for data according to current settings.

8.8 Network Settings

This menu allows to configure network parameters, such as PPPoE, DHCP, and SNMP, of which DHCP is the most common. In most cases, the network type is DHCP unless the static IP address is set manually. If you need an authenticated username and password to connect to the network, select PPPoE.

8.8.1 Basic Settings

8.8.1.1 General

GRUNDIG				Live	Playback	Remote Setting	Local Settings	• •
<table-cell-rows> Channel</table-cell-rows>	General PPPoE	SNMP IEEE802.1X Port (Configuration					
Live Image Control Video Cover ROI	DHCP	•						
B Record	IP Address		Test					
Encode Record Capture	Subnet Mask							
f Event	Gateway							
Setup Alarm	IPv6 DHCP							
Al Setup Recognition Alarm	IPv6 Address	fe80:223.63#fe0a.901b						
Statistics	IPv6 Cateway	fe80:223.638.fe0a.901b/64						
Network General Email FTP								
RTSP DDNS HTTPS IP Filter Platform Access	DNS 2							
Device	IPv6 DNS 1	2001-4860-4860_8888						
Disk Audio	IFv6 DNS 2	2001;4860;4860;8844						
System	Multicast	-						
General Multi-User Maintenance Information	Multicast Address	239.255.255.255	(224.0.0.0-239.255.255.255)					
	Video Encryption Tran	emission						
		Refresh						

Figure 8.8.1.1.1 General

To connect to a router that allows DHCP, check the DHCP box. The router will automatically assign all network parameters to the device. You can also choose to manually set the following parameters for the network:

IP Address: The IP address is the identifier of IPC on the network. It consists of four numbers between 0 and 255 separated by periods, for example, "192.168.001.100".

Subnet Mask: A subnet mask is a network parameter that defines the range of IP addresses that can be used in the network. If the IP address is likened to the street you live on, then the subnet mask is the community. A subnet address also consists of four numbers separated by periods, for example,"255.255.000.000".

Gateway: This address allows IPC to access the network. The format of a gateway address is the same as that of an IP address, for example, "192.168.001.001".

IPv6 Address: The IPv6 address is the identifier of IPC on the network. It consists of eight numbers between 0 and FFFF, separated by colons, f or example, "ABCD:EF01:2345:6789:ABCD:EF01:2345:6789".

DNS1/DNS2: DNS1 is the active DNS server and DNS2 is the standby DNS server. Usually you just need to enter the DNS1 server address.

Main Stream: If this option is enabled, the main stream can be used for multicast.

Multicast Address: Specifies a multicast address. A third-party player can request the camera to send a multicast media stream through the RTSP protocol.

Video Encryption Transmission: Indicates audio/video encryption transmission.

If the IPC is capable of warning you of repeated IP addresses in the same network segment, when IP addresses are

repeatedly used, the following message will pop up when you click the rest icon:

IP Address	172.020.058.037	⊗	Test
	The address is used		
Subnet Mask	255.255.255.000	\otimes	

8.8.1.2 PPPoE

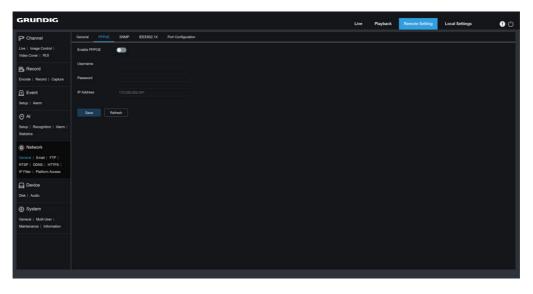


Figure 8.8.1.2.1 PPoE

This is an advanced protocol that allows the IPC to connect to the network more easily via DSL modems. Turn on the "Enable PPPoE" box and then enter the username and password of PPPoE. Click the "Apply" to save data. The system will restart to take PPPoE settings into effect.

8.8.1.3 SNMP

Simple Network Management Protocol (SNMP) is a standard application-layer protocol that is designed to manage nodes such as servers, workstations, routers, switches, and HUBS over IP networks.

GRUNDIG							Live	Playback	Remote Setting	!
다. Channel	General PPPoE	SNMP	IEEE802.1X	Port Configura	ition					
Live Image Control Video Cover ROI	Enable									
멾, Record	SNMP Version									
Encode Record Capture	SNMP Port				(1 ~ 65535)					
Event	Read Community									
Setup Alarm	Write Community									
Ø AI	Trap IP Address									
Setup Recognition Alarm Statistics	Trap Port				(1 ~ 65535)					
Network General Email FTP RTSP CLOUD DDNS HTTPS IP Filter Platform Access	Save Re	fresh								

Figure 8.8.1.3.1 SNMP

Enable: Turn on or off SNMP.

SNMP Version: Specifies the version of the SNMP server. The options include V1, V2 and V1, V2, and V3.

SNMP Port: Specifies the port number of the SNMP server.

Read Community: Specifies the Read Community value of the SNMP server.

Write Community: Specifies the Write Community value of the SNMP server.

Trap IP Address: Specifies the Trap IP address of the SNMP server.

Trap Port: Specifies the Trap port number of the SNMP server.

8.8.1.4 IEEE802.1X

The 802.1x protocol is widely used in Ethernet as the access control mechanism for LAN ports, which mainly solves the problems of authentication and security in Ethernet. The 802.1x protocol is a port-based network access control protocol. "Port-based network access control" refers to the authentication and control of accessed user devices at the port level of the LAN access device. User devices connected to the port can access resources on the LAN if they can pass authentication; If it cannot pass authentication, it cannot access resources on the LAN.

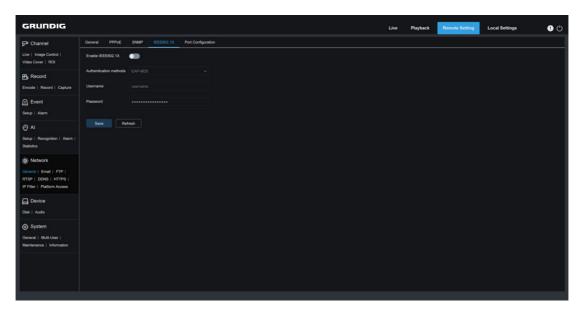


Figure 8.8.1.4 IEEE802.1X

Enable IEEE802.1X: Enable or disable IEEE802.1X.

Authentication Methods: Set the authentication methods of IEEE802.1X.

Username: Set IEEE802.1X authentication username.

Password: Set IEEE802.1X authentication password.

8.8.1.5 Port Configuration

GRUNDIG						Live Playbac	k Remote Setting	Local Settings	9 C
🖵 Channel	General PPPoE	SNMP IEEE802.1X	Port Configuration						
Live Image Control	Server	Inter	nal Port	External Port	Protocol	UPNP Status	Maping St	trategy	UPNP
Video Cover ROI	HTTP Port					Inactive			
B Record	Client Port	9000				Inactive			•
Encode Record Cepture	HTTPS Port	443				Inactive			•10
	RTSP Port	554				Inactive			
Event Setup Alarm	Multicast Port	10000	Ĵ (1024	65535)					
() AI	P2P Switch								
Setup Recognition Alarm Statistics	Save Refre	sh							
(
General Email FTP									
RTSP DONS HTTPS									
IP Filter Platform Access									
Device									
Disk Audio									
Disk Audio									
Device Disk Audio System General Multi-User Maintenance Information									
Disk Audio System General Multi-User									
Disk Audio System General Multi-User									
Disk Audio System General Multi-User									

Figure 8.8.1.5.1 Port

Web Port: This is the port you use to remotely login to the IPC (for example, using a web client). If port 80 is already used by other applications, change the port number.

Client Port: This is the port through which the IPC will send messages (for example, using a mobile application). If default port 9000 is already used by other applications, change the port number.

RTSP Port: The default port number is 554. If it is already used by other applications, change the port number.

HTTPS: It is an HTTP channel aiming for security. On the basis of HTTP, transmission encryption and identity authentication are used to ensure the security of transmission.

UPNP: To remotely login to the device from a web Client, perform port forwarding on the router. Enable this option if your router supports UPnP. In this case, you do not have to manually configure port forwarding on the router. If your router does not support UPnP, make sure that port forwarding is done manually on your router.

Multicast Port: Specifies a multicast port.

P2P Switch: P2P is ineffective if this switch is turned off.

8.8.2 Email Configuration

This menu allows to configure email settings. Complete these settings if you want to receive system notifications via email when an alarm is triggered or your hard drive is full.

GRUNDIG				Live	Playback	Remote Setting	
P Channel	Email Configuration						
Live Image Control Video Cover ROI	Email	-					
B Record	Encryption						
Encode Record Cepture	SMTP Port		1 ~ 65555)				
Event	SMTP Server						
Setup Alarm	Username						
() AI	Password						
Setup Recognition Alarm Statistics	Sender						
() Network	Receiver 1						
General Email FTP RTSP DONS HTTPS	Receiver 2						
IP Filter Platform Access	Receiver 3						
Disk Audio	Interval						
System		Tost Refresh					
General Multi-User Maintenance Information							

Figure 8.8.2.1 E-Mail

Email: Enable or disable email.

Encryption: Enable this option if your email server requires SSL or TLS authentication. Set it to Automatic if you are not sure.

SMTP Port: Specifies the SMTP port number of the email server.

SMTP Server: Specifies the SMTP server address.

UserName: Specifies your email address.

Password: Specifies your email password.

Receiver 1~3: Specifies the email address from which you want to receive event notifications from the IPC.

Interval: Specifies the interval between notification emails on the IPC.

To ensure that all settings are correct, click "**Test Email**". The system will send an email to your inbox. If you receive a test email, the configuration parameters are correct.

8.8.3 FTP

This menu enables you to enable the FTP server, through which you can view pictures and videos uploaded from the IPC to your FTP server.

GRUNDIG		Live	Playback	Remote Setting	•
P Channel					
Live Image Control Video Cover ROI	FT9 Enables C				
Encode Record Capture	Server 1722550.3 Port 21 ① (1~66535)				
Event	Usomane zhorg				
Setup Alarm	Passaord 🗠				
 Al Setup Recognition Alarm Statistics 	Taunder images 🛑				
Network General Email FTP RTSP DDNS HTTPS IP Filter Pattorn Access	Ease Robush				
Device					
System General Muth-User Maintenance Information					

Figure 8.3.3.1 FTP

When option is turned on, alarm videos will be uploaded to the FTP server.

8.8.4 RTSP

Real Time Streaming Protocol (RTSP), RFC2326, is an application layer protocol in the TCP/IP protocol architecture. This protocol defines how one-to-many applications can efficiently transfer multimedia data over IP networks. You can view real-time images using a video player.

RTSP Enable: Enable or disable the RTSP. This protocol is available only when it is turned on.

Anonymous Login: Allow to login as an anonymous user. Authentication is not required for using this protocol if this option is turned on.

GRUNDIG		Live	Playback	Remote Setting	0
🖓 Channel	RTSP				
Live Image Control Video Cover ROI	RT3P Enuble				
B Record	Anonymous Login 💦 👔 (No username or passavord required)				
Encode Record Capture	Metadata Platform None V				
Event	Instruction, nago pri Pulporingsistemento I Stadogen A A Gjoven Internej, 1 (sub Anterni, 2)noble sinemi				
© AI	Save Retrolt				
Setup Recognition Alarm Statistics					
(@) Network					
General Email FTP RTSP OONS HTTPS IP Filter Platform Access					
Device					
Disk Audio					
System					
General Multi-User Maintenance Information					

Figure 8.8.4.1 RTSP



8.8.5 Dynamic Domain Name

This menu allows to configure DDNS settings. DDNS provides a static address to simplify remote connection to the IPC.To use DDNS, you first need to sign up an account on the webpage of the DDNS service provider.

GRUNDIG		Live	Playback	Remote Setting	• •
🖓 Channel	cons				
Live Image Control Video Cover RDI	covs 💷				
B Record	Server NO_P v				
Encode Record Capture	Hostrame				
Event	Username				
Setup Alarm	Password				
() AI					
Setup Recognition Alarm Statistics	Save Tent Refrech				
(@) Network					
General Email FTP RTSP DONS HTTPS					
IP Filter Platform Access					
Device					
Disk Audio					
System					
General Multi-User Maintenance Information					

Figure 8.8.5.1 DDNS

DDNS: Enable or disable DDNS.

Server: Specifies your preferred DDNS server (DDNS_3322, DYNDNS, NO_IP, or even CHANGEIP, DNSEXIT).

Hostname: Specifies the domain name you created on the web page of the DDNS service provider. This is the address you type in the URL bar when you want to connect remotely to the IPC from your PC.

User/Password: Specifies the username and password obtained when you create an account on the web page of the DDNS service provider.

Enter all parameters and then click "**Test DDNS**" to test DDNS settings. If the test result is "Unreachable or DNS error", check whether the network works normally or the DDNS information is correct.

8.8.6 HTTPS

This menu allows to set HTTPS. You can connect your device over HTTPS.

GRUNDIG		Live	Playback	Remote Setting	ڻ
P Channel	нтра				
Live Image Control Video Cover ROI	Certificite Type Custom v				
B Record	Certificate not installed				
Encode Record Capture	Certificate				
Event Setup Alarm					
 Al Setup Recognition Alarm Statistica 	See Relea				
() Network					
General Email FTP RTSP DDNS HTTPS IP Filter Platform Access					
Device					
System General Multi-User Maintenance Information					

Figure 8.8.6.1 HTTPS

Certificate Type: There are two options, including default and custom. The Custom option Allow to connect devices using your own certificate.

Certificate: Select a custom certificate when the Custom option is selected.

Key: Select a custom key file when the Custom option is selected.

8.8.7 IP Filter

The IP filter can be used to set the allow list and block list of devices to be connected.

GRUNDIG		Live	Playback	Remote Setting	• •
P Channel	IP Flar				
Live Image Control Video Cover ROI	Enable				
B Record	Type Enable Allow List Enable Block List				
Encode Record Cepture	Restricted Type Allow List V				
Event					
Setup Alarm	No. Start Address End Address	CON.			
() AI					
Setup Recognition Alarm Statistics	Save Dukto Refeash				
(i) Network					
General Email FTP					
RTSP DDNS HTTPS IP Filter Platform Access					
Device					
Disk Audio					
System					
General Multi-User					
Maintenance Information					

Figure 8.8.7.1 IP Filter

Enable: Enable or disable the IP filter. You can choose to enable the block list or allow list if this option is turned on.

Restricted Type: Select the list to be set (block list or allow list).

Start Address: Specifies the start address.

End Address: Specifies the end address.

8.8.8 RTMP

RTMP function page, turn on the enable switch, fill in the correct server address and then you can push the audio and video streams of the device to the YouTube live server.

GRUNDIG	u	,ive	Playback	Remote Setting	Local Settings	0
P Channel	RTLAP Event Push Platform					
Live Image Control Video Cover ROI	Enate 💿					
B Record	Server Address					
Encode Record Capture	Stream Type MainStream V					
庄 Event	Note Recommended resolution is 1120x1080					
Setup Alarm	After enabling RTMP, if the existing audio or video codect are not supported, the system will automatically change the video codect to H264 or the audio codec to					
() Al	Save Retresh					
Setup Recognition Alarm Statistics						
(a): Network						
General Email FTP RTSP DONS HTTPS						
IP Filter Platform Access						
Device						
Disk Audio						
System						
General Mutti-User						

Figure 8.8.8.1 RTMP

Enable: Enable or disable the RTMP function.

Server Address: The address of the server to be pushed.

Stream Type: Select the video stream to be pushed to the server.

8.8.9 Event Push Platform

Event push can be implemented in two modes: HTTP push mode and UDP push mode. HTTP push mode provides POST method and GET method. UDP push mode provides unicast, multicast, and broadcast methods.

Note: Only some models support the event push function.

8.8.9.1 HTTP Push

GRUNDIG				Live	Playback	Remote Setting	Local Settings	•
P Channel	RTMP Event P	ush Platform						
Live Image Control Video Cover ROI	Enable	•						
멾, Record	Precise	•						
Encode Record Capture	Name							
🖻 Event	Push Way	💿 НТТР 💿 UDP						
Setup Alarm	Usemame							
() AI	Password							
Setup Recognition Alarm Statistics	Server Address							
. Network	Port							
General Email FTP	URL	API/AlarmEvent/EventPush						
RTSP DONS HTTPS IP Filter Platform Access								
	Method	POST						
Disk Audio	Interval	OFF						
System		Refresh						
General Multi-User								

Figure 8.8.9.1.1 HTTP Push



Enable: Enable or disable the event push function.

Precise: Enable or disable the Precise function. When on, pushes once when an alarm is triggered and again when the alarm ends. When it is off, it will only push once when the alarm is triggered.

Name: Set the channel name. Does not support Chinese display.

Push Way: Set the push mode. Both HTTP push mode and UDP push mode are supported. You can select **HTTP** or **UDP** as required.

Username: Set the username. It can be set to NULL if there is not any.

Password: Set the password. It can be set to NULL if there is not any.

Server Address: Set the server address.

Port: Set the server port (port number range:1–65535).

URL: Set the server API. It can be set to NULL if there is not any.

Method: Set the HTTP push method. Both POST and GET methods are supported. Only the HTTP-POST method supports image push. Other methods push notifications only. The alarm type of image push is the same as that in the alarm column of live view on the Web client.

Interval: Set the keep-alive interval. The keep-alive mechanism ensures that a notification is periodically pushed to the client in accordance with the preset time while normal alarm push is not affected. There is no keep-alive mechanism in UDP mode.

8.8.9.2 UDP Push

GRUNDIG				Live	Playback	Remote Setting	Local Settings	0
🖓 Channel	RTMP Event Push	Platform						
Live Image Control Video Cover ROI	Enable	•						
B Record	Precise	•••						
Encode Record Capture	Name							
🖻 Event	Push Way	🔵 HTTP 💿 UDP						
Setup Alarm	UDP Method	Broadcast						
Al Setup Recognition	UDP Address							
Alarm Statistics	UDP Port	5000						
Retwork General Email FTP RTSP DDNS HTTPS IP Filter Platform Access	Save	tresh						
Device								
General Multi-User								

Figure 8.8.9.2.1 UDP Push

Enable: Enable or disable the event push function.

Precise: Enable or disable the Precise function. When on, pushes once when an alarm is triggered and again when the alarm ends. When it is off, it will only push once when the alarm is triggered.

Name: Set the channel name. Does not support Chinese display.

Push Way: Set the push mode. Both HTTP push mode and UDP push mode are supported.You can select **HTTP** or **UDP** as required.

UDP Method: Set the UDP push method. There are three options: Unicast, Multicast, and Broadcast.

Unicast: Enter the IP address and port number of the client UDP server for receiving push notifications. The notifications can be received by this address only.

Multicast: Multiple clients in the same network segment of which the UDP servers use the same UDP address and port number can receive notifications. Other UDP addresses cannot receive notifications.

Broadcast: All UDP servers in the same network segment can receive notifications.

UDP Address: Set the UDP server address.

UDP Port: Set the UDP server port (port number range:1–65535).

8.9 Device Management

8.9.1 Disk Management

This menu allows to check and configure the internal SD-card. Formatting is required only for initial access and when a new SD-card is used.

GRUNDIG							Live	Playback	Renote Setting	Local Settings	00
P Channel	2008										
Live Image Central	101	10.		Serial No.	Operation	Type	Status	Fies /	Tenerally	Press / Tintal (T)	
Video Cover RCH						Read & Write			109G	-by/t0 four	
B Record				NUT		Read & Wills	Normal	*	9490	Deather	
Encode Record Capture	Cvenertie		Auto								
G Event		- Design	ETHER DEAL ACCTS	INCO Referent							
Drig Aven											
O N											
The second second second second second											
Subp (Bosspillon) Asses (Maleises											
Add (manage											
Retwork											
General Creat FTP											
RTSP DONS HTTPS											
PTHE PHONADOM											
Device											
Cost Auto											
(g) System											
General Multi-Liter											



- 1. Format Hard Disk: Select the SD-card to be formatted, and then click Format hard disk. To start formatting, enter your username and password and then click OK.
- 2. Overwrite: This option to overwrite old records in the SD-card when the SD-card is full. If Auto is selected, the oldest data will be automatically overwritten when the SD-card is full. Select OFF if you do not want to overwrite any old videos. If this function is disabled, check the status of the SD-card periodically to ensure that the SD-card is not full.
- **3. ADD NetHDD:** This function Allow to add a network HDD. After a network HDD (NAS) is configured, you can connect the NAS to the Internet to record channel videos or capture images. The AI face database can only be stored in the HDD.



Mounting type: There are two options, including NFS and SMB/CIFS. Among them, NFS does not need username and password, but SMB/CIFS needs.

User Name: Specifies the username of NAS (unavailable in NFS mode).

Password: Specifies the password of NAS (unavailable in NFS mode).

Server IP: Specifies the IP address of NAS.

Directory Name: Specifies the folder where you want to store data in the NAS.

Disk Size: Specifies the size of the network HDD.

Test: Test the connectivity of NAS.

Add NetHDD: Click this option to add NAS.

8.9.2 Audio Management

This menu is used to set the volume of your device.

GRUNDIG								0 C
ive I Image Control I fideo Cover ROI		Seria SC		Add Net				
B Record			Mounting Type	SMB/CIFS				
incode Record Capture			Username Password					
🚹 Event letup Alarm			Server IP	Password cannot be ampty!				
ivent Push			Directory Name	IP formal errot)				
) AI hetup Recognition			Disk Size		(4 - 8192)GB			
larm Statistics								
Notwork				Test	Add NetHDD			
Seneral Email FTP RTSP DONS HTTPS P Filter								
Device								
lisk Audio Cloud								
System								
Seneral Multi-User								

Figure 8.9.2.1 Audio Management

Audio Input Type: Select the audio input type. There are two ways: Mic/In and Line/In. Mic/In means the audio is input through the internal microphone of the camera, Line/In means the audio is input through the tail cable of the camera (supported by some models).

Enable Audio: Enable or disable camera audio.

Output Volume: Specifies the volume of output audio.

Input Volume: Specifies the volume of input audio.

Audio Code Type: Specifies the audio decoding type. There are two options, including G711A and G711U.

8.10 System Settings

You can change system information such as date and time and regions, and change the password and permissions.

8.10.1 General

8.10.1.1 Date and Time

GRUNDIG		Live	Playback Remote Setting	• •
🖵 Channel	Date and Time Daylight Saving Time Privacy Statement			
Live Image Control Video Cover ROI	Time setting mode			
B Record	Date Format YYYY-MM-DD			
Encode Record Capture	Time Zone GMT+8:00			
Event	Time Format 24Hour			
Setup Alarm	System time 2024-01-23 10 : 53 : 4			
() Al	Server Address Erne windows.com			
Setup Recognition Alarm Statistics				
() Network	Save Synchronize computer time Ratheah			
General Email FTP				
RTSP DDNS HTTPS IP Filter Platform Access				
Device				
Disk Audio				
System				
General Multi-User Maintenance Information				

Figure 8.10.1.1 Date & Time

Time settings mode: There are two options including Static and NTP server synchronization. When Static is selected, you have to set the time manually. When NTP server synchronization is selected, the time will be synchronized to the network time.

Date Format: Specifies the date format.

Time Zone: Specifies the time zone associated with your region or city.

Time Format: Specifies your preferred time format.

System Time: Click the box to change the date and time.

Synchronize computer time: Here you can synchronize the time to the computer time.

You cannot set the time manually if NTP server synchronization is selected.

Sever Address: Specifies the automatic time synchronization website.

8.10.1.2 Daylight Saving Time

The Daylight-Saving Time (DST) function enables you to choose when to add daylight saving time to a specific time zone or region.

GRUNDIG		Live	Playback	Remote Setting	• 🙂
P ^I Channel	Date and Time Daylight Saving Time Physicy Statement				
Live Image Control Video Cover ROI	Deylight Saving Time 💿 & Sec by week. 🔶 Sec by date				
B Record	Start Time March The 2nd SUN 14 / 00 : 00				
Encode Record Capture	End Time November V The fat V SUN V 14 : 00 : 00				
Event Setup Alarm	The Ohet Hour C				
() AI	Save Refresh				
Setup Recognition Alarm Statistics					
Network					
General Email FTP RTSP DDNS HTTPS IP Filter Platform Access					
Device					
Disk Audio					
System					
General Multi-User Maintenance Information					

Figure 8.10.1.2 Daylight Saving

Daylight Saving Time: Enable or disable this option if DST is used in your time zone.

Set by week: Specifies the month, weekday, and time when daylight saving time begins and ends, for example, 2:00am on the first Sunday of a month.

Set by date: Specifies the date and time when daylight saving time begins and ends.

Start Time / End Time: Specifies the start time and end time of daylight-saving time.

Time Offset: Specifies the time that daylight saving time adds to your time zone. This is the difference between Universal Time Coordinated (UTC) and your local time.

8.10.1.3 Privacy Statement

GRUNDIG	Live Playback Remote Setting Local Settings 🕕 🔿
Live Image Control A	Date and Time Daylight Saving Time Physics Statement
Video Cover (ROI	Privacy Statement
畕 Record	
Encode Record Capture	"We' fully respect your privacy rights. We hereby formulate this "Privacy Statement" (hereinather referred to as "this Statement") to inform you of how we collect, use, disclose, protect, shore, and transmit your personal data. Please read this Statement carefully, if you have any questions, please let us know.
Event	
Setup Alarm	Personal information refers to various information, recorded electronically or otherwise that can identify the personal identity of a natural person alone or in combination with other information. This Statement sets out how we handle your personal information,
	but it does not cover all processing scenarios. The products or services discussed, mentioned, or introduced in this Statement vary depending on your device hype, model, or geographic location. How specific products or services handle your personal
AI	information, your rights, and how to contact the data controller will be explained by us in the specific privacy notice or supplementary statement published with that product or service. In addition to this Statement, we recommend that you read the relevant
Setup Recognition	privacy notice or supplementary statement when using specific products or services.
Alarm Statistics	This Statement applies only to our IPC series products and their video surveillance-related services.
A	This Statement will help you understand the following:
(a) Network	1. How We Collect and Use Your Personal Information
General Email FTP	II. How We Entrust, Share, Transfer, and Disclose Your Personal Information
RTSP DDNS HTTPS	III. How We Protect Your Personal Information
IP Filter Platform Access	IV: How You Can Manage Your Personal Information
Device	V, How This Statement is updated
Disk Audio	I. How We Collect and Use Your Personal Information
System	1. Personal Information We Collect
	When you use IPC products or services, you may need to provide personal information, and we will only collect and use your personal information for the purposes stated in this statement. The following are examples of the personal information we may
General Multi-User Maintenance Information	ovier.

Figure 8.10.1.3 Privacy

8.10.2 Multi-user Management

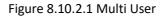
This menu allows to configure username, password, and permissions.

The system supports user types as follows:

ADMIN - **System Administrator:** A system administrator can fully configure the system and can change administrator and user passwords as well as enable/disable password protection.

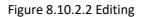
USER - Normal User: A normal user can only access the preview, search, playback and other appropriate functions. You can set multiple users with different system access permissions.

RUNDIG				U	ve Playback	Remote Setting	Local Settings	! 🙂
Live Image Control A	Multi-User							
Video Cover KOI	NO.	Username	Level	Status	Passwo	rd	Policy	
B Record		admin	ADMIN	Enable				
Encode Record Capture		user1	USER	Disable				
		user2	USER	Disable				
Event		user3	USER	Disable				
Setup Alarm		user4	USER	Disable				
		user5	USER	Disable				
() AI		user6	USER	Disable				
Alarm Statistics	Reflesh							
Device								
System								
General Multi-User								



To change an administrator or user password, click the "Edit Password" icon. The password must be at least 8 characters long and a combination of numbers, letters, and symbols. Enter the new password again for confirmation. Save the new password. You will be asked to enter the old password for authentication.

				L	ive Playback	Remote Setting	Local Settings	00
₽ Channel								
Live Image Control			Editing	×				
Video Cover								
🛱 Record		Enable	-					
		Username	user1					
Encode Record Capture								
Event		Password						
Setup Alarm Event Push		Password strength						
Al Setup Recognition Alarm Statistics One Notwork		Confirm	OK Cancel					
General Email FTP RTSP DDNS HTTPS IP Filter								
Device								
Disk Audio Cloud								
System								
General Multi-User Maintenance Information								



- 1. Select one of inactive users and click the "Edit Password" icon.
- 2. Turn on "Enable" to enable users.
- 3. Click "Username" to edit the username.
- 4. Click the field next to **Password** to enter your password.
- 5. Click the field next to **Confirm** to enter your confirm password.

Click **Save**. You will have to enter the administrator password for authentication.

						00
P Channel						
Live Image Control Video Cover	Us			×		
📇 Record	Username	user1				
Encode Record Capture	Parameter					
Event	Live Playback					
Setup Alarm Event Push	□ PTZ □ RTSP					
 Al Setup Recognition Alarm Statistics 			Cancel			
Network General Email FTP RTSP DDNS HTTPS IP Filter						
Device						
System General Multi-User Maintenance Information						

Figure 8.10.2.3 Policy

Set user permissions and check the boxes corresponding to the functions. Click **All** to check all boxes. Click **Clear** to clear all boxes.

8.10.3 System Maintenance

This menu enables you to search for and view system logs, restore factory settings, upgrade the system, export and import system parameters, and configure automatic system restart.

8.10.3.1 Log Management

The system log displays important system events, such as motion alarms and system warnings. You can easily import backup files in the system log to your computer within a set time range.

GRUNDIG							Live	Playback	Remote Setting	Local Settings	! ()
₽ Channel	Log Load Default	Upgrade	Paran	ieter Management	Auto Reboot	Developer Mode				/	
Live Image Control Video Cover	Log Type										
음, Record	Name										
Encode Record Capture	Start Time	04/13/2022									
庄 Event	End Time	04/13/2022									
Setup Alarm	No.			Time		Log Content		Log Info			
() AI			04/1	3/2022 16:38:45		Motion End		Is there a video: ha	s record		
			04/1	3/2022 16:38:35		Motion Start		Is there a video: ha	s record		
Setup Recognition Alarm			04/1	3/2022 16:37:58		Motion End		Is there a video: ha	s record		
Statistics			04/1	3/2022 16:37:46		Login		Operation result: TI User Name: admin IP: 172.20.58.2	e operation was success	u	
			04/1	3/2022 16:37:42		Motion Start		Is there a video: ha	s record		
General Email FTP			04/1	3/2022 16:36:59		Motion End		Is there a video: ha	s record		
RTSP DONS HTTPS			04/1	3/2022 16:36:29		Motion Start		Is there a video: ha	s record		
IP Filter			04/1	3/2022 16:35:44		Motion End		Is there a video: ha	s record		
D Davies			04/1	3/2022 16:35:24		Motion Start		Is there a video: ha	s record		
Device			04/1	3/2022 16:35:09		Motion End		Is there a video: ha	s record		
Disk Audio Cloud											
System General Mutti-User Maintenance Information											

Figure 8.10.3.1.1 Log Files

Log Search and Backup:

- 1. Click the field next to **Start Time** and select the start date and time from the on-screen calendar.
- 2. Click the field next to **End Time** and select the end date and time from the on-screen calendar.
- 3. Select the event type you want to search for from the drop-down list next to Log Type, or select All to view

the entire system log for the selected time range. The type options include: system log, configuration log, warning log, account log, recording log, storage log, and network log.

- 4. Select the event type you want to search for from the drop-down list next to **Minor Type** (this menu is unavailable if ALL is selected for Log Type), or select **All** to view the entire system log for the selected time range. The type options include:
- System: System settings, restart, automatic restart, upgrade, time settings, and NTP.
- Configuration: IPC live control, private area settings, recording mode settings, recording plan settings, main stream settings, network settings, Sub Stream settings, email settings, color settings, motion detection settings, hard disk settings, multi-user settings, NTP settings, image control, mobile stream settings, RTSP settings, IP filter settings, restore factory settings, rare sound detection settings, export settings, and import settings. Event Push settings, Capture settings, Deterrent settings, AI settings, FTP settings, DDNS settings, HTTPS settings, audio settings, Siren settings.
- Alarm: Start of motion detection, end of motion detection, start of I/O alarm, end of I/O alarm, start of Video Tamper, end of Video Tamper, start of Perimeter Intrusion, end of Perimeter Intrusion, start of Line Crossing, end of Line Crossing, start of Object Detection, end of Object Detection, start of Pedestrian & Vehicle, end of Pedestrian & Vehicle, start of Face Detection, end of Face Detection, start of Cross Counting, end of Cross Counting, start of Crowd Density, end of Crowd Density, start of Queue Length, end of Queue Length, start of License plate detection, end of Intrusion, start of Rare Sound, end of Rare Sound, start of Sound Alarm, end of Sound Alarm, start of Intrusion, end of Intrusion, start of Region Entrance, end of Region Exiting.
- Account: login, log out, locked and switch users.
- Recording: Search, playback, and backup.
- **Storage:** Formatting HDD, HDD full, and HDD error.
 - 5. **network:** Network disconnected, network online, network exception, and Network Mode changed.
 - 6. Click Search.
 - 7. Browse system logs from the selected time range:
 - 8. Use the K < / >> I button in the lower right corner of the menu to switch between pages of system log events.

Enter the name of the exported file in the field next to Name. Click Export to create the backup of system logs.

8.10.3.2 Load Default

Reset the device to factory settings. You can choose to reset all the settings at a time, or the settings on a specific menu.

Note: Restoring the default Settings will not delete videos and snapshots stored in the memory card.

GRUNDIG		Live	Playback	Remote Setting	Local Settings	• •
Channel Uve Image Control Video Cover ROI	Log Loss Drivet Upgede Perenter Mangement Auto Reboot Developer Mode M Auto Reboot					
Record Encode Record Capture	III Reard III Coart					
Event Setup Alarm	 Network 					
Al Setup Recognition Alerm Statistice	Except to non-oxisting parameters Al Except to non-oxisting parameters Al Except to non-oxisting parameters Al					
Network General Email FTP RTSP DONS HTTPS IP Filter Platform Access	Eur Reine A					
Device						
System General Multi-User Maintenance Information						

Figure 8.10.3.2.1 Default

Select the item to restore, or All to select all items. Click "Save" to load the default settings for the selected items.

8.10.3.3 System Upgrade

This menu allows to upgrade firmware.

GRUNDIG		Live	Playback	Remote Setting	Local Settings	(
P Channel	Log Load Default Upgrade Parameter Management Auto Reboot					
Live Image Control Video Cover ROI						
B Record	Automatic Detection					
Encode Record Capture	Usemarre					
Event	Password					
Setup Alarm Event Push	FTPH/TTP ut address https://softwareupgrade.atbbs.cn/IPC/NOF					
() AI	protocol./hostnamej.portjipath					
Setup Recognition Alarm Statistics	example: flp://192.168.1.100.25/ipc/upgradePackage					
Network	http://192.168.1.100.80/ipc/upgradePackage					
General Email FTP RTSP DDNS HTTPS	Save Detect Upgrade Refresh					
IP Filter						
Device	Path Upgrade					
Disk Audio Cloud						
System						
General Multi-User Maintenance Information						

Figure 8.10.3.3.1 System Upgrade

Automatic Detection: You can enable this function to automatically detect available updates.

Username: Specifies the username of your FTP server.

Password: Specifies the password of your FTP server.

FTP/HTTP URL address: Specifies the over-the-air upgrade address (no username or password is required for upgrade over HTTP).

Note: The FTP address is in the format as below: ftp://{IP address of FTP server:port}/Upgrade (the name of the folder containing the over-the-air upgrade path of the FTP server).

Save: Click this button to save current settings.

Detect: After the upgrade file is uploaded and the upgrade path is set, you can click Detect to manually detect the over-the-air upgrade file. A message pops up when updates are available, as shown in the figure below:

Live Playback Romoto Settings 🕕 ()
The second se

Figure 8.10.3.3.2 Auto Upgrade

Upgrade: Click this button to start system upgrade.

Place the firmware file (.sw) into the HDD of your PC.

Click "..." next to "Path" to select the firmware file from your PC.

Click the **Upgrade** button to start system upgrade. The system upgrade will take about 2 to 3 minutes. Do not power off the device or close your browser while system upgrade is in progress.

8.10.3.4 Parameter Management

You can export the configured parameters to your PC or import the exported configuration file from your PC to the camera.

GRUNDIG						Live	Playback	Remote Setting	Local Settings	0
P Channel	Log Loed Default	Upgrade	Parameter Management	Auto Reboot	Developer Mode					
Live Image Control Video Cover /ROI	Import File									
B Record	Export file name									
Encode Record Capture										
Event										
Setup Alarm										
() Al										
Setup Recognition Alarm Statistics										
(i) Network										
General Email FTP RTSP DONS HTTPS										
IP Filter Platform Access										
Device										
Disk Audio										
System										
General Multi-User Maintenance Information										

Figure 8.10.3.4 Parameter

Import File: Click the field to display the path window. Select the parameter file and then click **Import** to start importing parameters.

Export File Name: Click the field to enter the name of the file to which parameters are exported. Click **Export** to export parameters.

8.10.3.5 Auto Reboot

This menu enables the system to automatically reboot. You are advised to enable this function to guarantee the stable operation of the device.

GRUNDIG							Li	e Play	yback	Remote Setting	Local Settings	0	Ċ
P Channel	Log Loed Defaul	t Upgrade	Parameter Managemen	Auto Reboot	Developer Mode								
Live Image Control Video Cover RDI	Auto Reboot	•											
Record Encode Record Capture													
Event Setup Alarm													
Al Setup Recognition Alarm Statistics		Retresh	Reboot										
Network General Email FTP RTSP DONS HTTPS IP Filter Platform Access													
Device Dek Audio													
System General Multi-User Maintenance Information													

Figure 8.10.3.5 Reboot

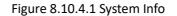
Auto Reboot: Enable or disable auto reboot feature.

Time: Set IPC to reboot by day, week, or month.

8.10.4 System Information

This menu allows to view system information, such as device ID, device model, MAC address, firmware version.

GRUNDIG				Live	Playback	Remote Setting	•
	Information						
Encode Record Capture	Device ID	000000	11 2830				
	Device Name	GU-CI-AP4634T	- <u>1699</u> 268				
Event	Device Type	GU-CI-AP4634T	一些生产				
Setup Alarm	Hardware Version	GU-CI-AP4634T-B					
AI	Software Version	V30.45.8.2.4.1_240508					
Setup Recognition Alarm Statistics	Web Version	V1.4.1.1017_240508					
(MAC Address	A4-DA-22-A8-25-22					
General Email FTP	P2P ID	FJ63JNLFTLLRZNWC111A					
RTSP DDNS HTTPS	Device Serial No	H3X5100015A8					
IP Filter Platform Access	Refresh						
Device							
Disk Audio							
System							
General Multi-User Maintenance Information							



9 Local Settings

This menu allows to set the path for storing videos and downloaded and captured image files, as well as the format of videos and captured images.

Note: skip this page when you access the web client from Safari 12 and later, Chrome 57 and later, Firefox 52 and later, and Edge 41.

GRUNDIG			Live	Playback	Remote Setting	Local Settings	• •
Path configuration							
Record Path	D Device/Record	Ð					
Download P	D D Device Download						
Snapshot Pr							
File type	MP4 V						
Interval Capture Typ	10 V Mi	ute					
Capture Typ	Save						

Figure 9.1 Local Settings

UG-GU-CI-Series-2024-07-03-V6-EN ©ABETECHS GMBH, DÜSSELDORF, GERMANY