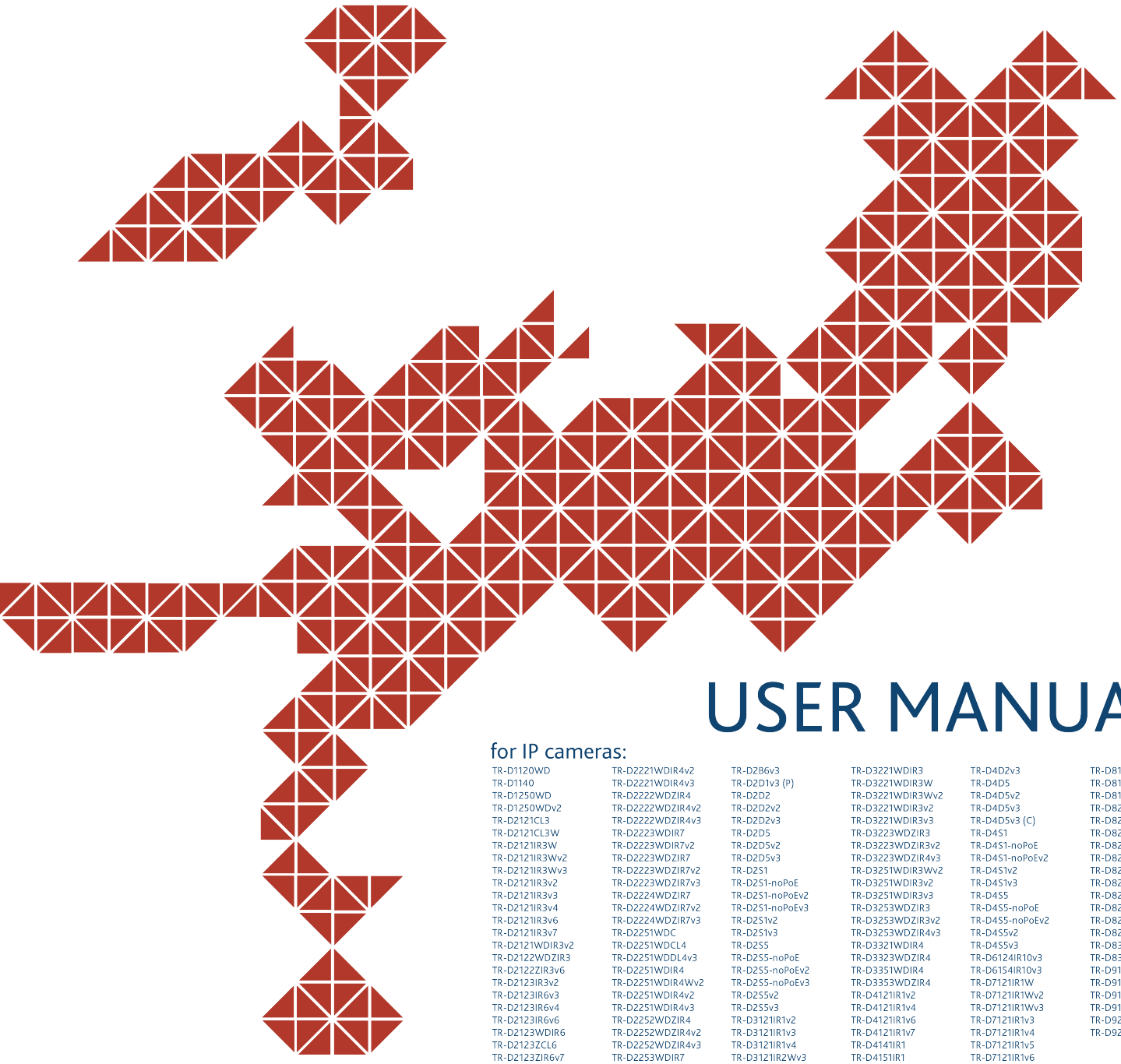


USER MANUAL

for IP cameras:

TR-D1120WD
TR-D1140
TR-D1250WD
TR-D1250WDv2
TR-D2121CL3
TR-D2121CL3W
TR-D2121IR3W
TR-D2121IR3Wv2
TR-D2121IR3Wv3
TR-D2121IR3v2
TR-D2121IR3v3
TR-D2121IR3v4
TR-D2121IR3v6
TR-D2121IR3v7
TR-D2121WDIR3v2
TR-D2122WDZIR3
TR-D2122ZIR3v6
TR-D2123IR3v2
TR-D2123IR6v3
TR-D2123IR6v4
TR-D2123IR6v6
TR-D2123WDIR6
TR-D2123ZCL6
TR-D2123ZIR6v7
TR-D2141IR3
TR-D2142ZIR3
TR-D2143IR3
TR-D2143IR6
TR-D2151CL3v7
TR-D2151IR3
TR-D2151IR3v2
TR-D2151IR3v7
TR-D2152ZIR3
TR-D2152ZIR3v2
TR-D2153IR6
TR-D2153IR6v2
TR-D2153ZCL6v7
TR-D2153ZIR6v7
TR-D2161IR3 (rev.2)
TR-D2163IR6
TR-D2181IR3 (rev.2)
TR-D2183IR6
TR-D2221WDC
TR-D2221WDCL4
TR-D2221WDIR4
TR-D2221WDIR4W
TR-D2221WDIR4Wv2
TR-D2221WDIR4v2
TR-D2221WDIR4v3
TR-D2222WDZIR4
TR-D2222WDZIR4v2
TR-D2222WDZIR4v3
TR-D2223WDIR7
TR-D2223WDIR7v2
TR-D2223WDZIR7
TR-D2223WDZIR7v2
TR-D2223WDZIR7v3
TR-D2224WDZIR7
TR-D2224WDZIR7v2
TR-D2224WDZIR7v3
TR-D2251WDC
TR-D2251WDCL4
TR-D2251WDDL4v3
TR-D2251WDIR4
TR-D2251WDIR4Wv2
TR-D2251WDIR4v2
TR-D2251WDIR4v3
TR-D2252WDZIR4
TR-D2252WDZIR4v2
TR-D2252WDZIR4v3
TR-D2253WDIR7
TR-D2253WDIR7v2
TR-D2253WDZCL7
TR-D2253WDZDL7v3
TR-D2253WDZIR7
TR-D2253WDZIR7v2
TR-D2253WDZIR7v3
TR-D2254WDZIR7v3
TR-D2321WDIR4
TR-D2323WDZIR7
TR-D2324WDZIR9
TR-D2351WDIR4
TR-D2353WDZIR7
TR-D2354WDZIR9
TR-D2B5
TR-D2B5-noPoE
TR-D2B5-noPoEv2
TR-D2B5-noPoEv3
TR-D2B5L
TR-D2B5L-noPoE
TR-D2B5v2
TR-D2B5v3
TR-D2B6
TR-D2B6v2
TR-D2B6v3
TR-D2D1v3 (P)
TR-D2D2
TR-D2D2v2
TR-D2D2v3
TR-D2D5
TR-D2D5v2
TR-D2D5v3
TR-D2S1
TR-D2S1-noPoE
TR-D2S1-noPoEv2
TR-D2S1-noPoEv3
TR-D2S1v2
TR-D2S1v3
TR-D2S5
TR-D2S5-noPoE
TR-D2S5-noPoEv2
TR-D2S5-noPoEv3
TR-D2S5v2
TR-D2S5v3
TR-D3121IR1v2
TR-D3121IR1v3
TR-D3121IR1v4
TR-D3121IR2Wv3
TR-D3121IR2v6
TR-D3121IR3v7
TR-D3122WDZIR2
TR-D3122ZIR2v6
TR-D3123IR2v3
TR-D3123IR2v4
TR-D3123IR2v6
TR-D3123VIR2v2
TR-D3123WDIR2
TR-D3123ZIR3v7
TR-D3141IR1
TR-D3142ZIR2
TR-D3143IR2
TR-D3143VIR2
TR-D3151CL3v7
TR-D3151IR2
TR-D3151IR2v2
TR-D3151IR3v7
TR-D3152ZIR2
TR-D3152ZIR2v2
TR-D3153IR2
TR-D3153IR2v2
TR-D3153ZIR3v7
TR-D3221WDIR3
TR-D3221WDIR3W
TR-D3221WDIR3Wv2
TR-D3221WDIR3v2
TR-D3221WDIR3v3
TR-D3223WDZIR3
TR-D3223WDZIR3v2
TR-D3223WDZIR4v3
TR-D3251WDIR3Wv2
TR-D3251WDIR3v2
TR-D3251WDIR3v3
TR-D3253WDZIR3
TR-D3253WDZIR3v2
TR-D3253WDZIR4v3
TR-D3321WDIR4
TR-D3323WDZIR4
TR-D3351WDIR4
TR-D3353WDZIR4
TR-D4121IR1v2
TR-D4121IR1v4
TR-D4121IR1v6
TR-D4121IR1v7
TR-D4141IR1
TR-D4151IR1
TR-D4151IR1v2
TR-D4151IR1v7
TR-D4161IR1
TR-D4181IR1
TR-D4221WDIR2
TR-D4221WDIR2v2
TR-D4221WDIR2v3
TR-D4251WDIR2v2
TR-D4251WDIR2v3
TR-D4321WDIR2
TR-D4351WDIR2
TR-D4B5
TR-D4B5-noPoE
TR-D4B5-noPoEv2
TR-D4B5L
TR-D4B5L-noPoE
TR-D4B5v2
TR-D4B5v3
TR-D4B6
TR-D4B6v2
TR-D4B6v3
TR-D4D2
TR-D4D2v2
TR-D4D2v3
TR-D4D5
TR-D4D5v2
TR-D4D5v3
TR-D4D5v3 (C)
TR-D4S1
TR-D4S1-noPoE
TR-D4S1-noPoEv2
TR-D4S1v2
TR-D4S1v3
TR-D4S5
TR-D4S5-noPoE
TR-D4S5-noPoEv2
TR-D4S5v2
TR-D4S5v3
TR-D6124IR10v3
TR-D6154IR10v3
TR-D7121IR1W
TR-D7121IR1Wv2
TR-D7121IR1Wv3
TR-D7121IR1v3
TR-D7121IR1v4
TR-D7121IR1v5
TR-D7121IR1v6
TR-D7121IR1v7
TR-D7141IR1
TR-D7151IR1
TR-D7151IR1v7
TR-D7221WDIR2Wv2
TR-D8121CL2
TR-D8121IR2W
TR-D8121IR2Wv2
TR-D8121IR2Wv3
TR-D8121IR2v2
TR-D8121IR2v3
TR-D8121IR2v4
TR-D8121IR2v6
TR-D8121IR3v7
TR-D8121WDIR2v2
TR-D8122ZIR2v6
TR-D8123ZIR3
TR-D8123ZIR4v7
TR-D8141IR2
TR-D8151CL3v7
TR-D8151IR2
TR-D8151IR2v2
TR-D8151IR3v7
TR-D8152ZIR2
TR-D8152ZIR2v2
TR-D8153ZIR4v7
TR-D8221WDC
TR-D8221WDCL3
TR-D8221WDIR3
TR-D8221WDIR3v2
TR-D8221WDIR3v3
TR-D8251WDC
TR-D8251WDCL3
TR-D8251WDDL3v3
TR-D8251WDIR3
TR-D8251WDIR3v2
TR-D8251WDIR3v3
TR-D8321WDIR4
TR-D8351WDIR4
TR-D9141IR2
TR-D9151IR2
TR-D9151IR2v2
TR-D9161IR2
TR-D9251WDIR3
TR-D9251WDIR3v2

TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION 7

1.1 TRASSIR IP camera exterior 7

1.1.1 TRASSIR TR-D1120WD / TR-D1140 7

1.1.2 TRASSIR TR-D1250WD / TR-D1250WDv2 9

1.1.3 TRASSIR TR-D2121IR3v2 / TR-D2121IR3v3 / TR-D2121IR3v4 / TR-D2121WDIR3v2 / TR-D2122WDZIR3 / TR-D2141IR3 / TR-D2142ZIR3 / TR-D2161IR3 / TR-D2181IR3 11

1.1.4 TRASSIR TR-D2121IR3W 13

1.1.5 TRASSIR TR-D2121CL3W 14

1.1.6 TRASSIR TR-D2123ZCL6 / TR-D2153ZCL6v7 / TR-D2224WDZIR7 / TR-D2224WDZIR7v2 / TR-D2253WDZCL7 / TR-D2253WDZDL7v3 15

1.1.7 TRASSIR TR-D2123IR3v2 / TR-D2143IR3 17

1.1.8 TRASSIR TR-D2121IR3v6 / TR-D2122ZIR3v6 / TR-D2151IR3 / TR-D2151IR3v2 / TR-D2152ZIR3 / TR-D2152ZIR3v2 / TR-D2221WDIR4 / TR-D2221WDIR4v2 / TR-D2251WDIR4 / TR-D2251WDIR4v2 19

1.1.9 TRASSIR TR-D2123IR6v3 / TR-D2123IR6v4 / TR-D2143IR6 /TR-D2123WDIR6 / TR-D2163IR6 / TR-D2183IR6 21

1.1.10 TRASSIR TR-D2321WDIR4 / TR-D2351WDIR4 23

1.1.11 TRASSIR TR-D2B6 / TR-D2B6v2 / TR-D4B6 / TR-D4B6v2 25

1.1.12 TRASSIR TR-D2B5-noPoE / TR-D2B5-noPoEv2 / TR-D2B5 / TR-D2B5v2 / TR-D2B5v2 (B) / TR-D4B5-noPoE / TR-D4B5 26

1.1.13 TRASSIR TR-D2B5L / TR-D2B5L-noPoE / TR-D4B5L / TR-D4B5L-noPoE 28

1.1.14 TRASSIR TR-D2B5v3 / TR-D2B5v3 (B) / TR-D2B5-noPoEv3 / TR-D4B5v3 29

1.1.15 TR-D2B6v3 / TR-D4B6v3 31

1.1.16 TRASSIR TR-D2121IR3Wv2 / TR-D2121IR3Wv3 / TR-D2221WDIR4W / TR-D2221WDIR4Wv2 / TR-D2251WDIR4Wv2 32

1.1.17 TRASSIR TR-D2222WDZIR4 / TR-D2222WDZIR4v2 / TR-D2252WDZIR4 / TR-D2252WDZIR4v2 34

1.1.18 TRASSIR TR-D2222WDZIR4v3 / TR-D2252WDZIR4v3 36

1.1.19 TRASSIR TR-D2123IR6v6 / TR-D2153IR6/ TR-D2153IR6v2 / TR-D2223WDIR7/ TR-D2223WDIR7v2 / TR-D2223WDZIR7 / TR-D2223WDZIR7v2 / TR-D2253WDIR7 / TR-D2253WDIR7v2 / TR-D2253WDZIR7 / TR-D2253WDZIR7v2 38

1.1.20 TRASSIR TR-D2323WDZIR7 / TR-D2353WDZIR7 40

1.1.21 TRASSIR TR-D2224WDZIR7v3 / TR-D2254WDZIR7v3 / TR-D2324WDZIR9 / TR-D2354WDZIR9 42

1.1.22 TRASSIR TR-D2123ZIR6v7 / TR-D2153ZIR6v7 TR-D2223WDZIR7v3 / TR-D2253WDZIR7v3 44

1.1.23 TRASSIR TR-D2121IR3v7 / TR-D2151IR3v7 / TR-D2221WDC / TR-D2221WDIR4v3 / TR-D2251WDC / TR-D2251WDIR4v3 46

1.1.24 TRASSIR TR-D2121CL3 / TR-D2221WDCL4 / TR-D2151CL3v7 / TR-D2251WDCL4 / TR-D2251WDDL4v3 48

1.1.25 TRASSIR TR-D2D2 / TR-D2D2v2 / TR-D2D2v3 / TR-D3123IR2v3 / TR-D3123IR2v4 / TR-D3123WDIR2 / TR-D3143IR2 / TR-D4D2 / TR-D4D2v2 / TR-D4D2v3 50

1.1.26 TRASSIR TR-D2D1v3 (P) / TR-D2D5 / TR-D2D5v2 / TR-D2D5v3 / TR-D3121IR1v2 / TR-D3121IR1v3 / TR-D3121IR1v4/ TR-D3141IR1 / TR-D4D5 / TR-D4D5v2 / TR-D4D5v3 52

1.1.27 TRASSIR TR-D2S1 / TR-D2S1v2 / TR-D2S1v3 / TR-D2S1-noPoE / TR-D2S1-noPoEv2 / TR-D2S1-noPoEv3 / TR-D4S1 / TR-D4S1v2 / TR-D4S1-noPoEv2 / TR-D4S1v3 54

1.1.28 TRASSIR TR-D2S5 / TR-D2S5-noPoEv2 / TR-D2S5-noPoEv3/ TR-D2S5v2 / TR-D2S5v3 / TR-D4S5 / TR-D4S5-noPoE / TR-D4S5-noPoEv2 / TR-D4S5v2 / TR-D4S5v3 / TR-D8121IR2v2 / TR-D8121IR2v3 / TR-D8121WDIR2v2 / TR-D8141IR2 / TR-D8121IR2v4 56
1.1.29 TRASSIR TR-D3122WDZIR2 / TR-D3142ZIR2 58
1.1.30 TRASSIR TR-D3121IR2v6 / TR-D3122ZIR2v6 / TR-D3123IR2v6 / TR-D3151IR2 / TR-D3151IR2v2 / TR-D3152ZIR2 / TR-D3152ZIR2v2 / TR-D3221WDIR3/ TR-D3221WDIR3v2 / TR-D3251WDIR3v2 60
1.1.31 TRASSIR TR-D3123VIR2v2 / TR-D3143VIR2 62
1.1.32 TRASSIR TR-D3151CL3v7 64
1.1.33 TRASSIR TR-D3121IR2Wv3 / TR-D3221WDIR3W / TR-D3221WDIR3Wv2 / TR-D3251WDIR3Wv2 66
1.1.34 TRASSIR TR-D3223WDZIR3 / TR-D3223WDZIR3v2 / TR-D3253WDZIR3 / TR-D3253WDZIR3v2 / TR-D3153IR2 / TR-D3153IR2v2 68
1.1.35 TRASSIR TR-D3121IR3v7 / TR-D3151IR3v7 / TR-D3221WDIR3v3 / TR-D3251WDIR3v3 / TR-D3321WDIR4 / TR-D3351WDIR4 70
1.1.36 TRASSIR TR-D3123ZIR3v7 / TR-D3153ZIR3v7 / TR-D3223WDZIR4v3 / TR-D3253WDZIR4v3 / TR-D3323WDZIR4 / TR-D3353WDZIR4 72
1.1.37 TRASSIR TR-D4121IR1v2 / TR-D4121IR1v4 / TR-D4121IR1v6 / TR-D4141IR1 / TR-D4151IR1 / TR-D4151IR1v2 / TR-D4161IR1 / TR-D4181IR1 / TR-D4221WDIR2 / TR-D4221WDIR2v2 / TR-D4221WDIR2v3 / TR-D4251WDIR2v3 74
1.1.38 TRASSIR TR-D4B5v2 / TR-D4B5-noPoEv2 76
1.1.39 TRASSIR TR-D4121IR1v7 / TR-D4151IR1v7 / TR-D4251WDIR2 / TR-D4251WDIR2v2 / TR-D4321WDIR2 / TR-D4351WDIR2 77
1.1.40 TRASSIR TR-D6124IR10v3 / TR-D6154IR10v3 79
1.1.41 TRASSIR TR-D7121IR1W / TR-D7121IR1Wv2 / TR-D7121IR1Wv3 81
1.1.42 TRASSIR TR-D7121IR1v3 / TR-D7121IR1v4 / TR-D7121IR1v5 / TR-D7121IR1v6 / TR-D7121IR1v7 / TR-D7141IR1 / TR-D7151IR1 / TR-D7151IR1v7 / TR-D7251WDIR2Wv2 / TR-D7221WDIR2Wv2 83
1.1.43 TRASSIR TR-D8121IR2W 85
1.1.44 TRASSIR TR-D8121IR2Wv2 / TR-D8121IR2Wv3 86
1.1.45 TRASSIR TR-D8121IR2v6 / TR-D8221WDIR3/ TR-D8221WDIR3v2 / TR-D8122ZIR2v6 / TR-D8251WDIR3 / TR-D8251WDIR3v2 / TR-D8151IR2/ TR-D8151IR2v2 / TR-D8152ZIR2 / TR-D8152ZIR2v2 87
1.1.46 TRASSIR TR-D8121CL2 / TR-D8151CL3v7 / TR-D8221WDCL3 / TR-D8251WDCL3 / TR-D8251WDDL3v3 89
1.1.47 TRASSIR TR-D8121IR3v7 / TR-D8151IR3v7 / TR-D8221WDC / TR-D8221WDIR3v3 / TR-D8251WDC / TR-D8251WDIR3v3 / TR-D8321WDIR4 / TR-D8351WDIR4 91
1.1.48 TRASSIR TR-D8123ZIR3 93
1.1.49 TRASSIR TR-D8123ZIR4v7 / TR-D8153ZIR4v7 95
1.1.50 TRASSIR TR-D9141IR2 / TR-D9161IR2 / TR-D9151IR2 / TR-D9151IR2v2 / TR-D9251WDIR3 / TR-D9251WDIR3v2 97

1.2 Safety instructions....99
1.3 Warranty obligations....100
CHAPTER 2. CONNECTING TRASSIR IP CAMERA....101
2.1 System requirements....101
2.2 Local network connection....101
2.3 IP address configuration....102
2.4 Connecting to the IP camera via the Internet....103
2.5 Confguring ActiveX for Internet Explorer....104
2.6 Reset IP camera settings....106
CHAPTER 3. TRASSIR IP CAMERA CONFIGURATION....107
3.1 Gaining access to IP camera web interface....107
3.2 Preview menu....110
3.2.1 Image settings menu....112
3.3 Archive menu....113
3.4 Configuration menu....115
3.4.1 Base settings menu....115
3.4.2 “System” menu....116
3.4.2.1 “General” menu....117
3.4.2.2 “Date & time” menu....118
3.4.2.3 “Auto maintain” menu....120
3.4.2.4 “Upgrade” menu....121
3.4.2.5 “PTZ” menu....122
3.4.2.6 “Information” menu....123
3.4.2.7 “Log” menu....124
3.4.3 “Network” menu....125
3.4.3.1 “TCP/IP” menu....126
3.4.3.1.1 “Network status” tab....126
3.4.3.1.2 “TCP/IP” tab....127
3.4.3.2 “Port” menu....129
3.4.3.3 “WIFI” menu....131
3.4.3.4 “PPPoE” menu....132
3.4.3.5 “SMTP” menu....133
3.4.3.6 “UpnP” menu....134
3.4.3.7 “DDNS” menu....136
3.4.3.8 “RTSP” menu....136
3.4.3.9 “RTMP” menu....138
3.4.3.10 “VoIP” menu....139
3.4.3.11 “SNMP” menu....140
3.4.3.12 “IEEE 802.1x” menu....141
3.4.3.13 “Trassir Cloud” menu....142
3.4.3.14 “HTTPS” menu....143
3.4.4 “Video & Audio” menu....144
3.4.4.1 “Audio” menu....145

3.4.4.2 “Video” menu....146
3.4.4.2.1 “Working mode” tab....146
3.4.4.2.2 “Video” tab....147
3.4.4.2.3 “Third stream” tab....148
3.4.4.3 “Snapshot” menu....148
3.4.4.4 OSD menu....150
3.4.4.5 “Image settings” menu....151
3.4.4.5.1 “Image” tab....151
3.4.4.5.2 “Schedule” tab....154
3.4.4.5.3 “Day/Night” tab....155
3.4.4.6 “Privacy mask” menu....157
3.4.4.7 ”ROI” menu....158
3.4.5 “Storage” menu....159
3.4.5.1 “Local settings” menu....159
3.4.5.2 “Disk” menu....160
3.4.5.3 “FTP” menu....161
3.4.5.4 “NFS” menu....162
3.4.5.5 “Prerecord settings” menu....163
3.4.5.6 “Schedule” menu....164
3.4.5.6.1 “Record” tab....164
3.4.5.6.2 “Snapshot” tab....166
3.4.5.6.3 “FTP Upload” tab....167
3.4.6 “Event” menu....168
3.4.6.1 “Motion detector” menu....169
3.4.6.1.1 “Detection zone” tab....169
3.4.6.1.2 “Schedule” tab....170
3.4.6.1.3 “Action” tab....171
3.4.6.2 “I/O Alarm” menu....172
3.4.6.2.1 “I/O Alarm” tab....172
3.4.6.2.2 “Schedule” tab....173
3.4.6.2.3 “Action” tab....174
3.4.6.3 “PIR” menu....175
3.4.6.4 “Abnormality” menu....175
3.4.6.4.1 “Network disconnection” tab....175
3.4.6.4.2 “Device startup” tab....176
3.4.7 “Security” menu....177
3.4.7.1 “Manage users” menu....177
3.4.7.2 “IP filter” menu....179
3.4.7.3 “Telnet” menu....181
3.4.8 “Video analytics” menu....182
3.4.8.1 “Facial detection” menu....183
3.4.8.1.1 “Basic settings” tab....184
3.4.8.1.2 “Schedule” tab....185
3.4.8.1.3 “Action” tab....185
3.4.8.2 “People counting” menu....186
3.4.8.2.1 “Basic settings” tab....187

3.4.8.2.2 “Report to FTP” tab....188
3.4.8.2.3 “Quota for Report” tab....190
3.4.8.3 “Human Detection” menu....191
3.4.8.3.1 “Basic settings” tab....192
3.4.8.3.2 “Schedule” tab....193
3.4.8.3.3 “Action” tab....193
3.4.8.4 “Vehicle detection” menu....194
3.4.8.4.1 “Basic settings” tab....194
3.4.8.4.2 “Schedule” tab....195
3.4.8.4.3 “Action” tab....195
3.4.8.5 “Line Crossing” menu....196
3.4.8.5.1 “Basic settings” tab....197
3.4.8.5.2 “Schedule” tab....198
3.4.8.5.3 “Action” tab....198
3.4.8.6 “Intrusion Detection” menu....199
3.4.8.6.1 “Basic settings” tab....200
3.4.8.6.2 “Schedule” tab....201
3.4.8.6.3 “Action” tab....201
3.4.8.7 “Loitering” Menu....202
3.4.8.7.1 “Basic settings” tab....202
3.4.8.7.2 “Schedule” tab....203
3.4.8.7.3 “Action” tab....203
SUPPLEMENT A. CONFIGURING NETWORK SETTINGS ON PC....204
SUPPLEMENT B. UTP CABLING....207
SUPPLEMENT C. ROUTER SETTINGS....208
SUPPLEMENT D. OPERATION ON RTSP AND ONVIF....213
Connecting on RTSP protocol....213
Getting a snapshot from IP camera....215
Connecting on ONVIF standard....216
SUPPLEMENT E. IP CAMERA PLACEMENT....217
SUPPLEMENT F. IPC MANAGER....220
Searching for IP-camera using TRASSIR IPCManager app....220
Additional menu for managing IP camera....222
Upgrading camera with IPC Manager....224
“Configurations” menu....225
“Tools” menu....226

CHAPTER 1. INTRODUCTION

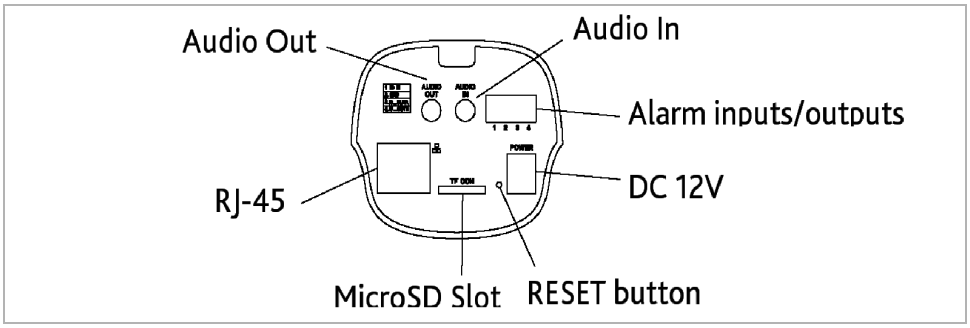
1.1 TRASSIR IP camera exterior

WARNING!

Hereinafter, the model name also refers to all its modifications.
The modification is indicated by a Latin letter in brackets in the model name.

1.1.1 TRASSIR TR-D1120WD / TR-D1140

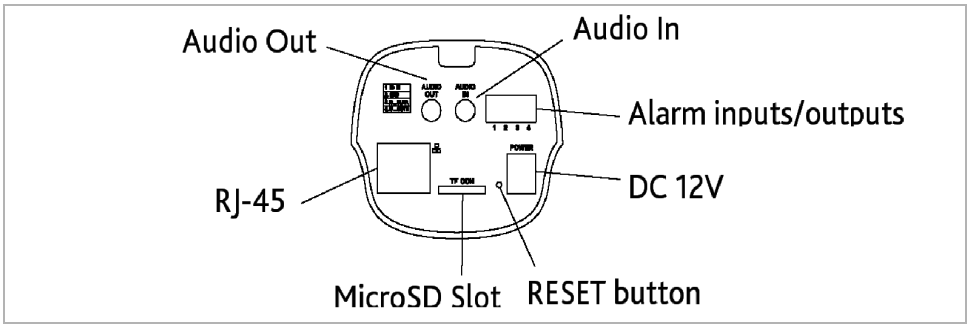
External connectors:



Connector	Description
DC12V	12V power supply connector.
RJ-45	LAN connector.
Audio IN	Microphone Connector.
Audio OUT	Speaker connector.
Alarm inputs/outputs	Alarm inputs and outputs.
MicroSD Slot	Slot for microSD memory card.
RESET Button	Reset to factory defaults.

1.1.2 TRASSIR TR-D1250WD / TR-D1250WDv2

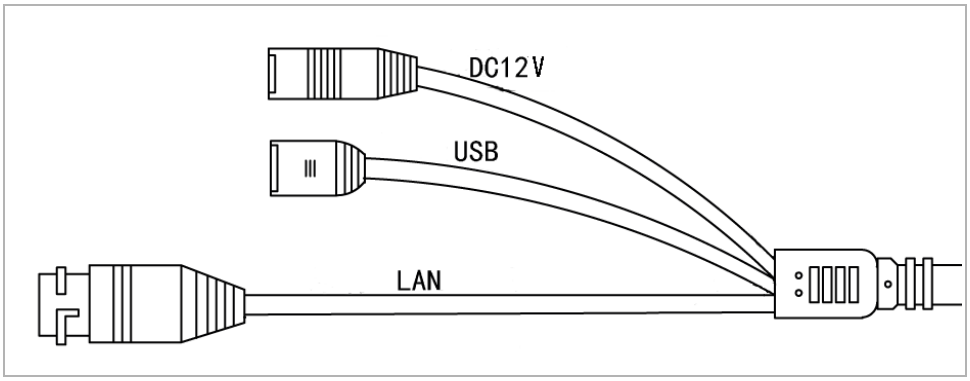
External connectors:



Connector	Description
DC12V	12V power supply connector.
RJ-45	LAN connector.
Audio IN	Microphone Connector.
Audio OUT	Speaker connector.
Alarm inputs/outputs	Alarm inputs and outputs.
MicroSD Slot	Slot for microSD memory card.
RESET Button	Reset to factory defaults.

1.1.3 TRASSIR TR-D2121IR3v2 / TR-D2121IR3v3 / TR-D2121IR3v4 / TR-D2121WDIR3v2 / TR-D2122WDZIR3 / TR-D2141IR3 / TR-D2142ZIR3 / TR-D2161IR3 / TR-D2181IR3

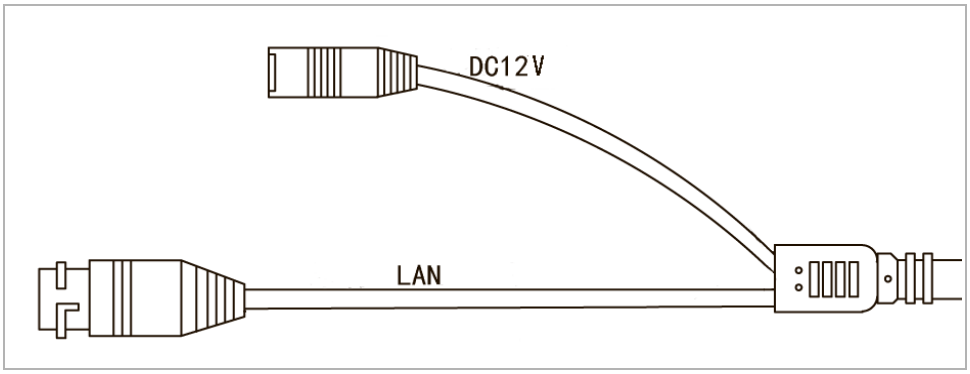
External connectors:



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
USB	USB connector for USBHDD

1.1.4 TRASSIR TR-D2121IR3W

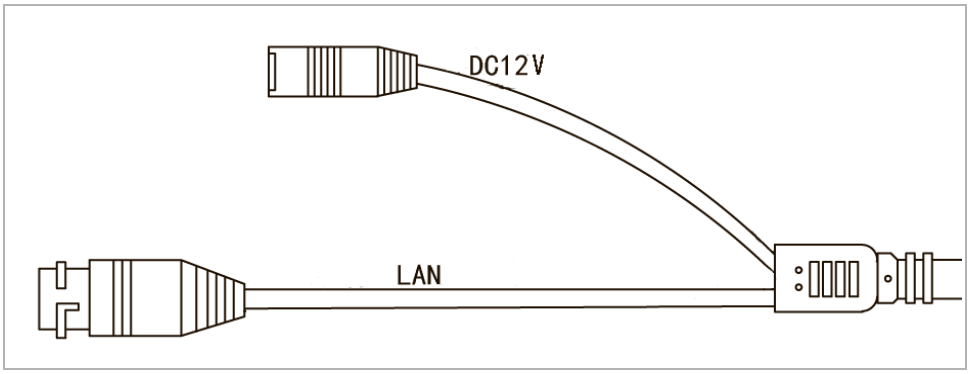
External connectors:



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.

1.1.5 TRASSIR TR-D2121CL3W

External connectors:

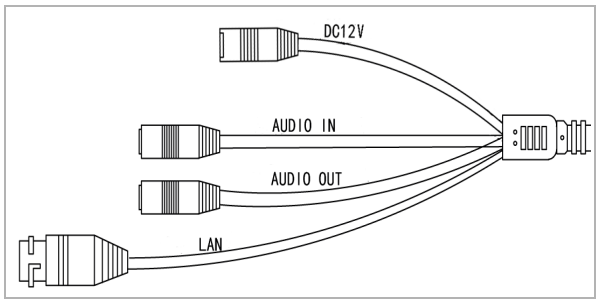


Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.

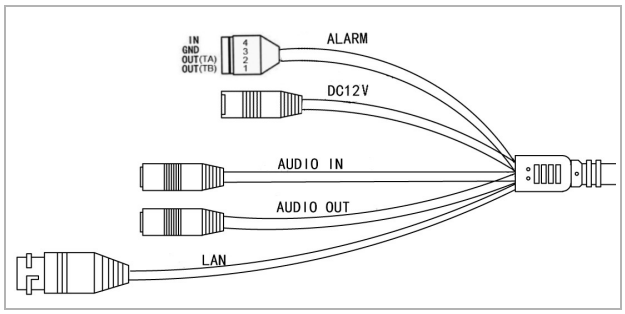
1.1.6 TRASSIR TR-D2123ZCL6 / TR-D2153ZCL6v7 / TR-D2224WDZIR7 / TR-D2224WDZIR7v2 / TR-D2253WDZCL7 / TR-D2253WDZDL7v3

External connectors:

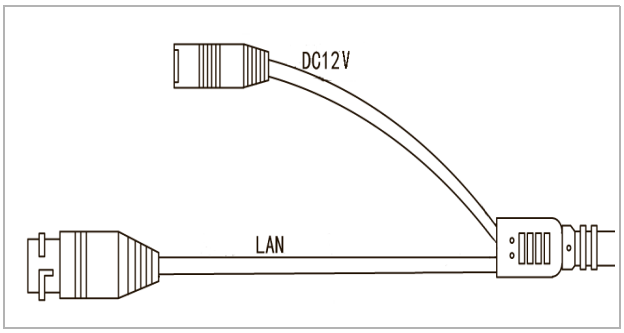
TR-D2153ZCL6v7



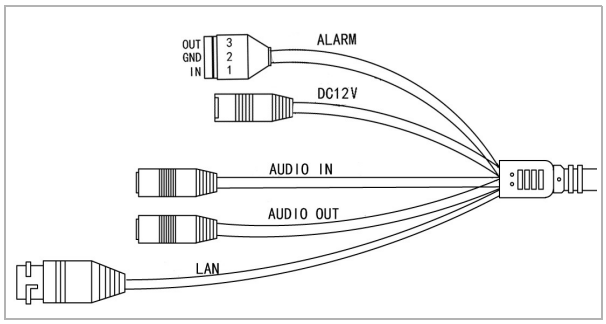
TR-D2224WDZIR7v2 / TR-D2253WDZCL7 / TR-D2253WDZDL7v3



TR-D2123ZCL6



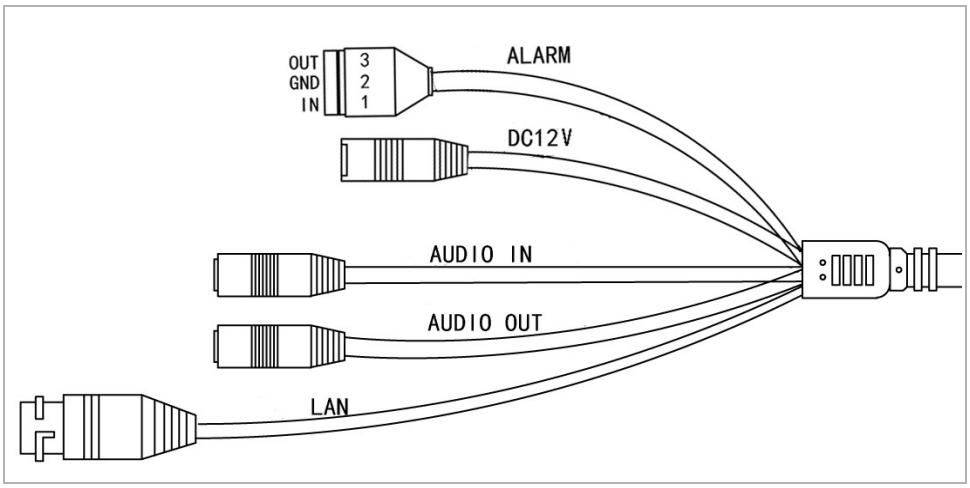
TR-D2224WDZIR7



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
ALARM	Alarm inputs and outputs.

1.1.7 TRASSIR TR-D2123IR3v2 / TR-D2143IR3

External connectors:

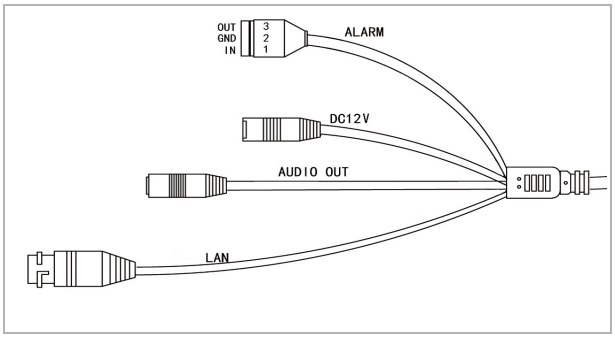


Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
Alarm I/O	Alarm inputs and outputs.

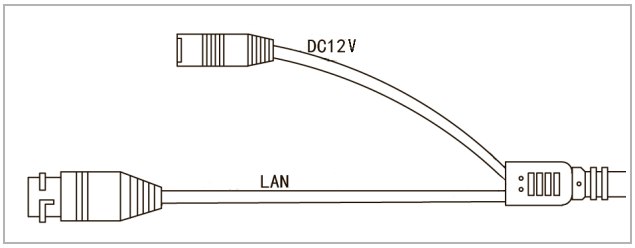
1.1.8 TRASSIR TR-D2121IR3v6 / TR-D2122ZIR3v6 / TR-D2151IR3 / TR-D2151IR3v2 / TR-D2152ZIR3 / TR-D2152ZIR3v2 / TR-D2221WDIR4 / TR-D2221WDIR4v2 / TR-D2251WDIR4 / TR-D2251WDIR4v2

External connectors:

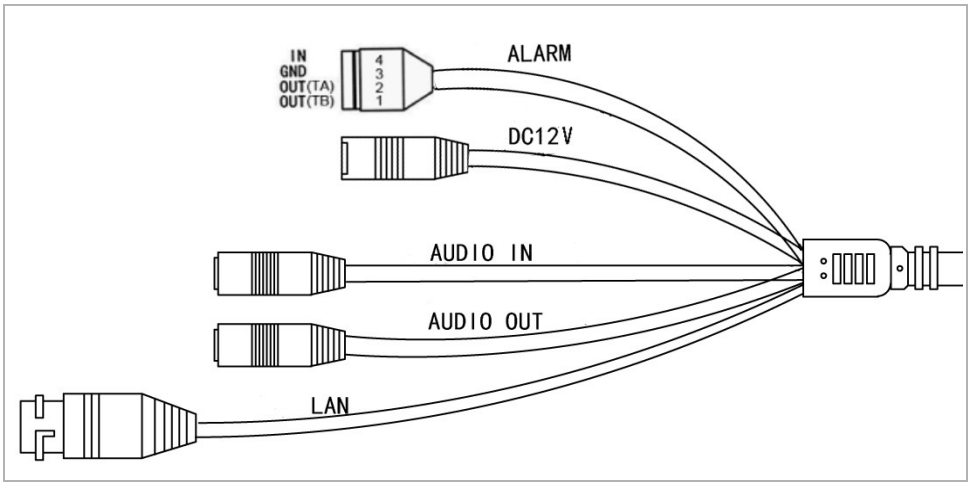
TR-D2221WDIR4 / TR-D2251WDIR4



TR-D2121IR3v6 / TR-D2122ZIR3v6 / TR-D2151IR3 / TR-D2151IR3v2 / TR-D2152ZIR3 / TR-D2152ZIR3v2



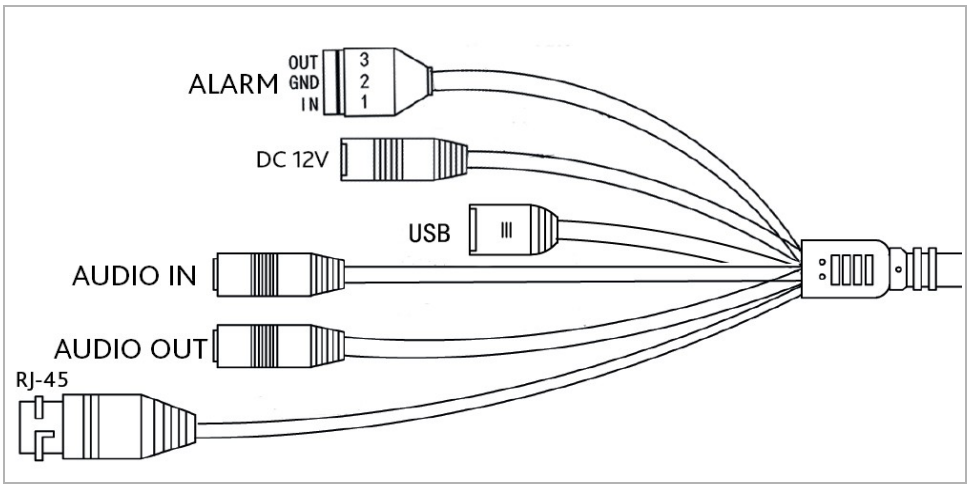
TR-D2221WDIR4v2 / TR-D2251WDIR4v2



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
Alarm I/O	Alarm inputs and outputs.

1.1.9 TRASSIR TR-D2123IR6v3 / TR-D2123IR6v4 / TR-D2143IR6 /TR-D2123WDIR6 / TR-D2163IR6 / TR-D2183IR6

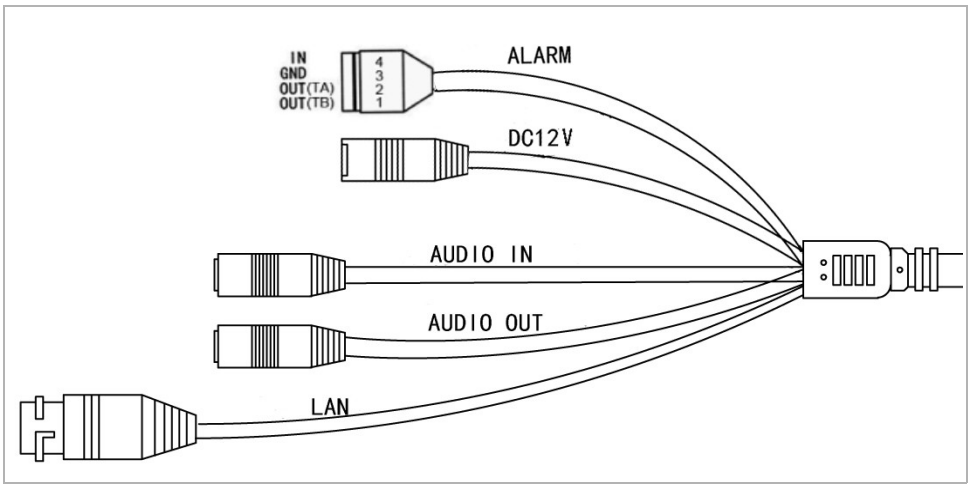
Eternal connectors:



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
Audio OUT	Speaker connector.
AUDIO IN	Active microphone connector.
Alarm I/O	Alarm inputs and outputs.
USB	USB connector for USBHDD

1.1.10 TRASSIR TR-D2321WDIR4 / TR-D2351WDIR4

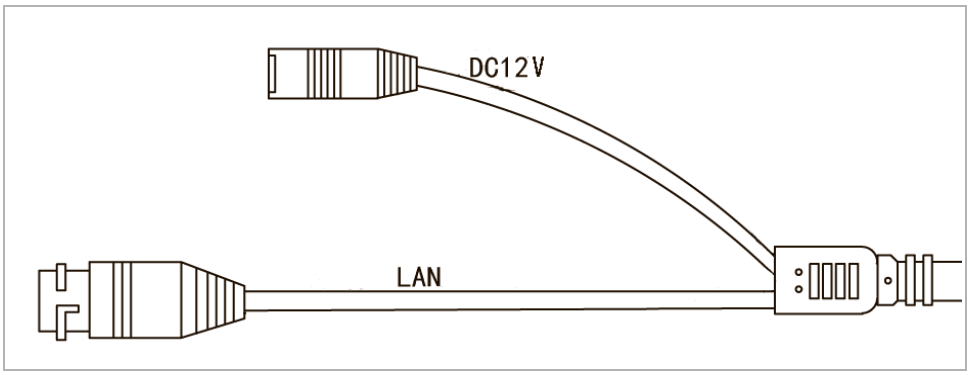
External connectors:



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
ALARM	Alarm inputs and outputs.

1.1.11 TRASSIR TR-D2B6 / TR-D2B6v2 / TR-D4B6 / TR-D4B6v2

External connectors:

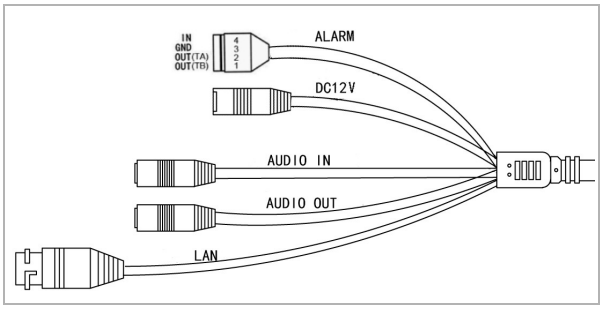


Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.

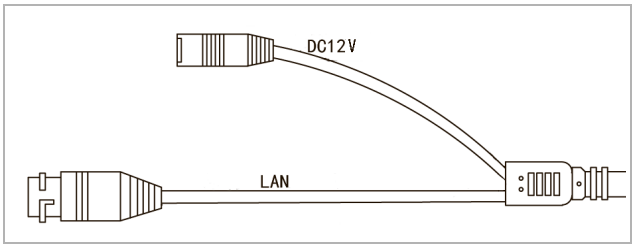
1.1.12 TRASSIR TR-D2B5-noPoE / TR-D2B5-noPoEv2 / TR-D2B5 / TR-D2B5v2 / TR-D2B5v2 (B) / TR-D4B5-noPoE / TR-D4B5

External connectors:

TR-D2B5v2 (B)



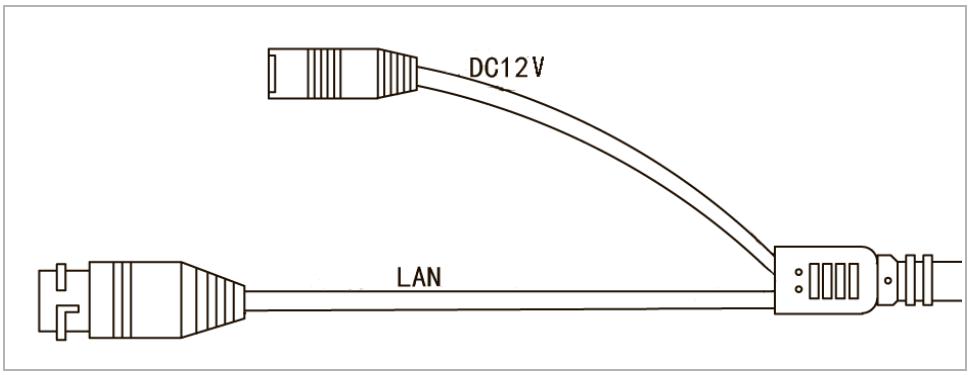
TR-D2B5-noPoE / TR-D2B5-noPoEv2 / TR-D2B5 / TR-D2B5v2 / TR-D4B5-noPoE / TR-D4B5



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
Alarm I/O	Alarm inputs and outputs.

1.1.13 TRASSIR TR-D2B5L / TR-D2B5L-noPoE / TR-D4B5L / TR-D4B5L-noPoE

External connectors:

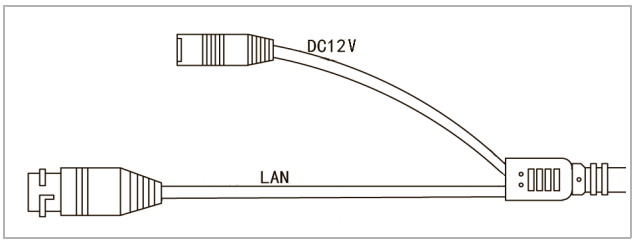


Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.

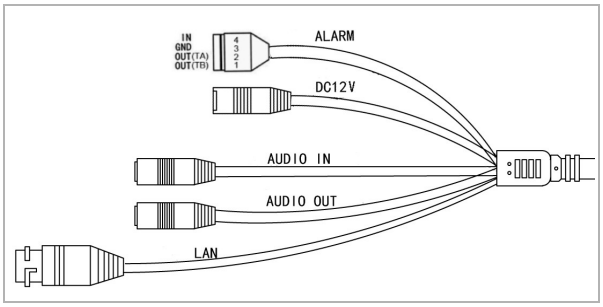
1.1.14 TRASSIR TR-D2B5v3 / TR-D2B5v3 (B) / TR-D2B5-noPoEv3 / TR-D4B5v3

External connectors:

TR-D2B5v3 / TR-D2B5-noPoEv3 / TR-D4B5v3



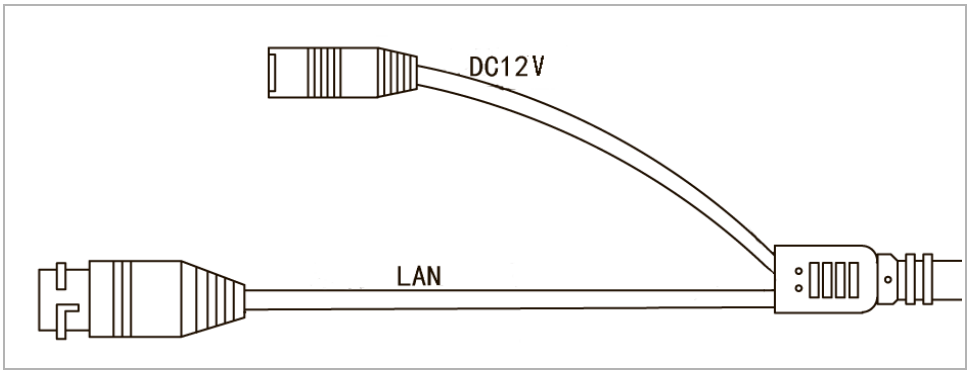
TR-D2B5v3 (B)



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
Alarm I/O	Alarm inputs and outputs.

1.1.15 TR-D2B6v3 / TR-D4B6v3

External connectors:

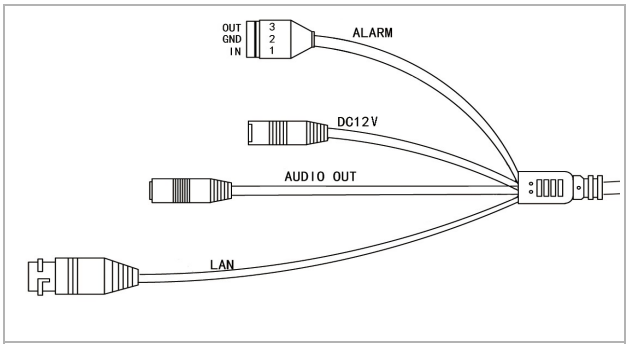


Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.

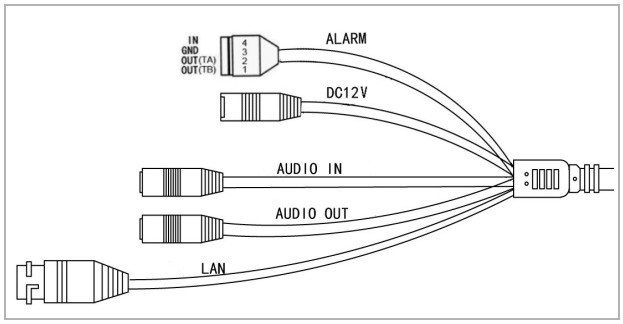
1.1.16 TRASSIR TR-D2121IR3Wv2 / TR-D2121IR3Wv3 / TR-D2221WDIR4W / TR-D2221WDIR4Wv2 / TR-D2251WDIR4Wv2

External connectors:

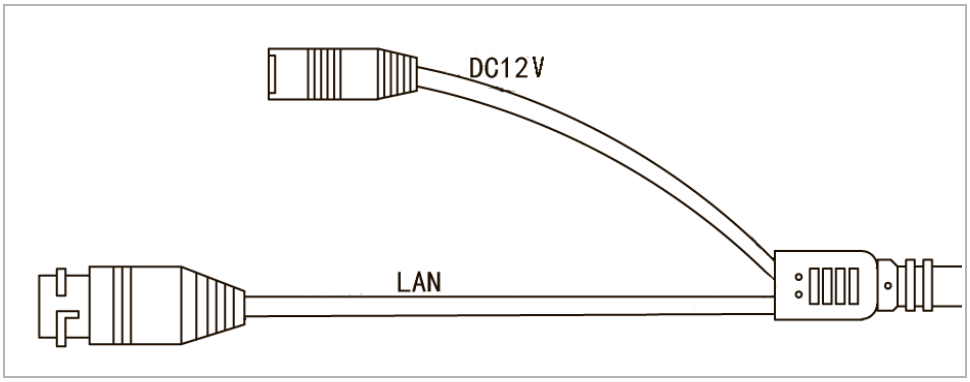
TR-D2221WDIR4W



TR-D2221WDIR4Wv2 / TR-D2251WDIR4Wv2



TR-D2121IR3Wv2 / TR-D2121IR3Wv3

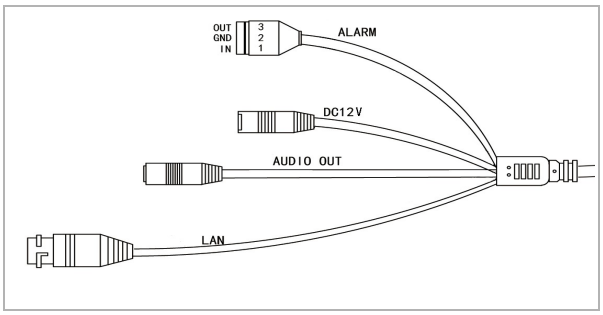


Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
Alarm I/O	Alarm inputs and outputs.

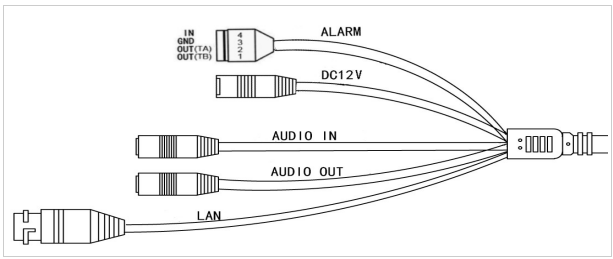
1.1.17 TRASSIR TR-D2222WDZIR4 / TR-D2222WDZIR4v2 / TR-D2252WDZIR4 / TR-D2252WDZIR4v2

External connectors:

TR-D2222WDZIR4 / TR-D2252WDZIR4



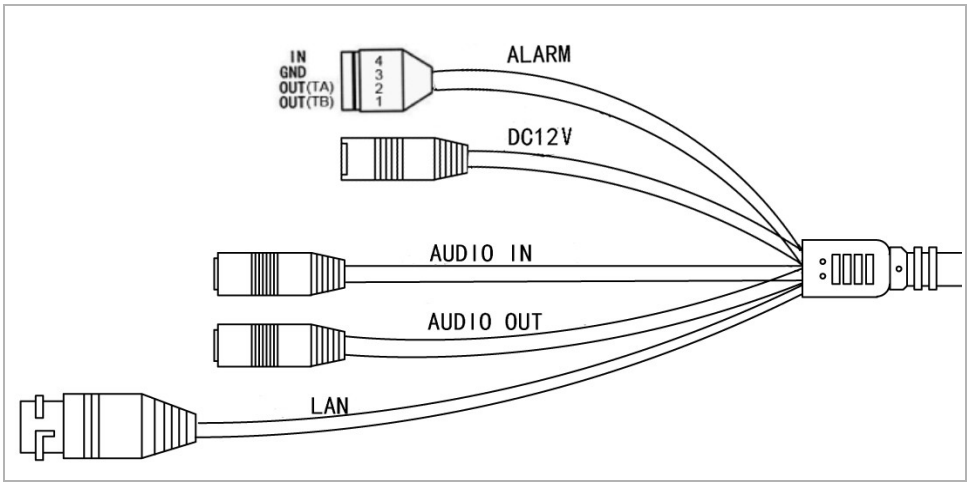
TR-D2222WDZIR4v2 / TR-D2252WDZIR4v2



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
Alarm I/O	Alarm inputs and outputs.

1.1.18 TRASSIR TR-D2222WDZIR4v3 / TR-D2252WDZIR4v3

External connectors:

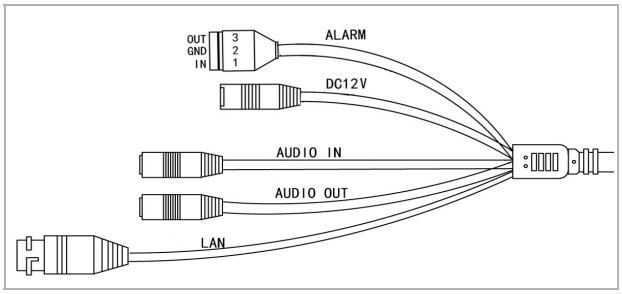


Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
ALARM	Alarm inputs and outputs.

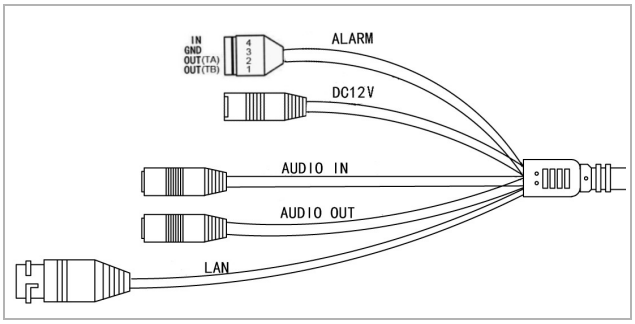
1.1.19 TRASSIR TR-D2123IR6v6 / TR-D2153IR6/ TR-D2153IR6v2 / TR-D2223WDIR7/ TR-D2223WDIR7v2 / TR-D2223WDZIR7 / TR-D2223WDZIR7v2 / TR-D2253WDIR7 / TR-D2253WDIR7v2 / TR-D2253WDZIR7 / TR-D2253WDZIR7v2

External connectors:

TR-D2123IR6v6 / TR-D2153IR6/ TR-D2153IR6v2 / TR-D2223WDIR7 / TR-D2223WDZIR7 / TR-D2253WDIR7 / TR-D2253WDZIR7



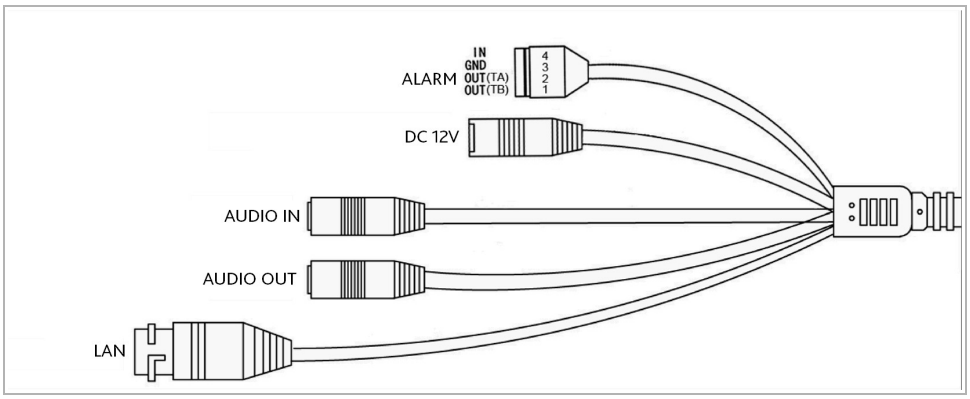
TR-D2223WDZIR7v2 / TR-D2223WDIR7v2 / TR-D2253WDIR7v2 / TR-D2253WDZIR7v2



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
ALARM	Alarm inputs and outputs.

1.1.20 TRASSIR TR-D2323WDZIR7 / TR-D2353WDZIR7

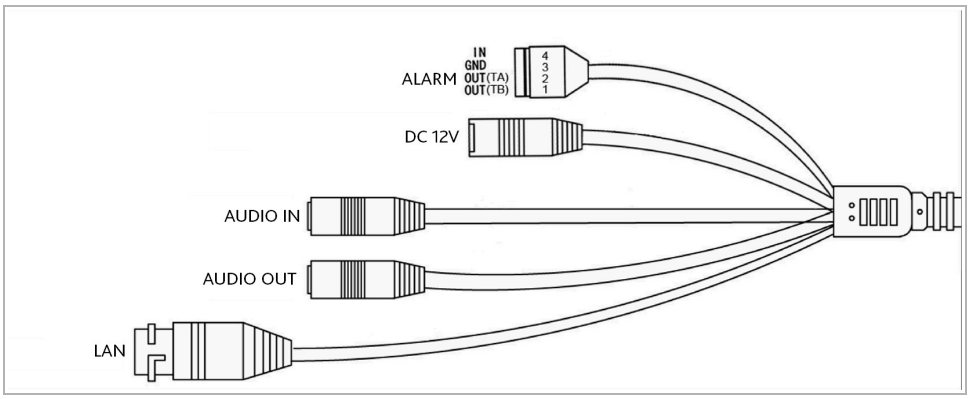
External connectors



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
ALARM	Alarm inputs and outputs.

1.1.21 TRASSIR TR-D2224WDZIR7v3 / TR-D2254WDZIR7v3 / TR-D2324WDZIR9 / TR-D2354WDZIR9

External connectors:

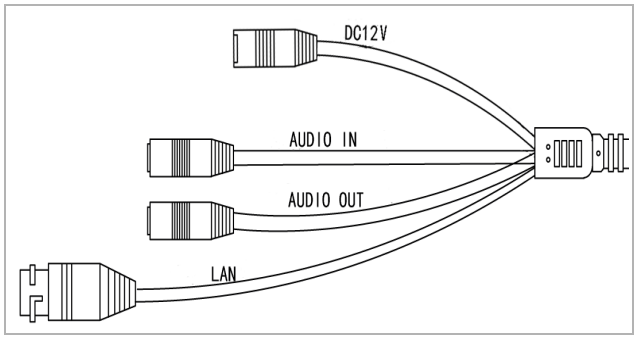


Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
ALARM	Alarm inputs and outputs.

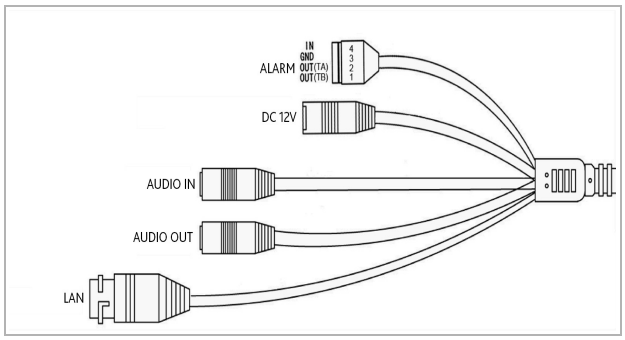
1.1.22 TRASSIR TR-D2123ZIR6v7 / TR-D2153ZIR6v7 TR-D2223WDZIR7v3 / TR-D2253WDZIR7v3

External connectors:

TR-D2123ZIR6v7 / TR-D2153ZIR6v7



TR-D2223WDZIR7v3 / TR-D2253WDZIR7v3

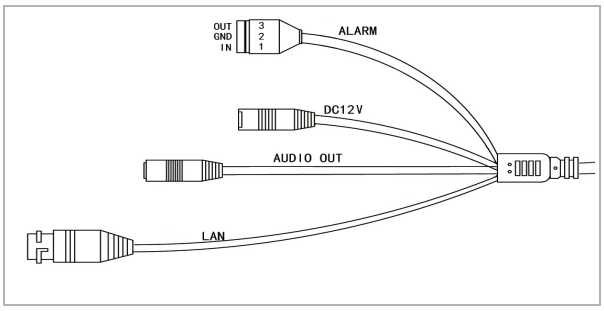


Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
ALARM	Alarm inputs and outputs.

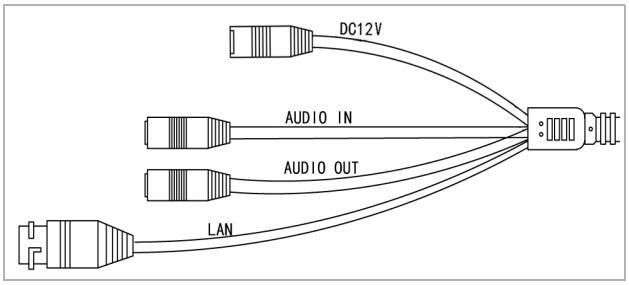
1.1.23 TRASSIR TR-D2121IR3v7 / TR-D2151IR3v7 / TR-D2221WDC / TR-D2221WDIR4v3 / TR-D2251WDC / TR-D2251WDIR4v3

External connectors:

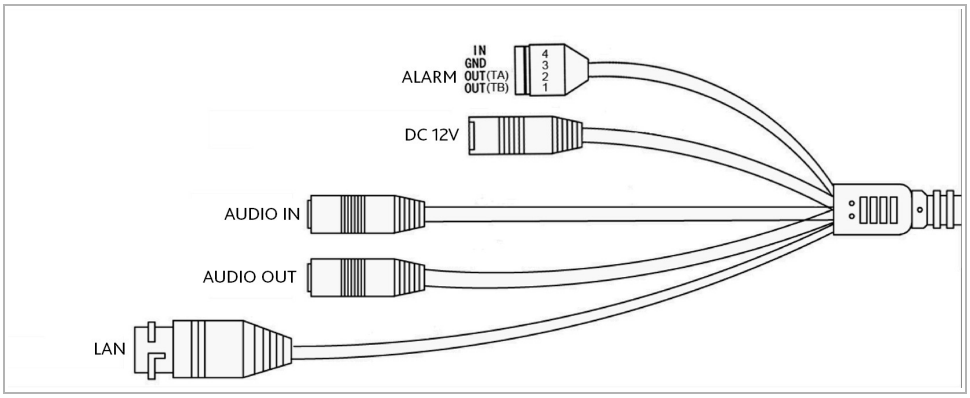
TR-D2221WDC



TR-D2121IR3v7 / TR-D2151IR3v7



TR-D2221WDIR4v3 / TR-D2251WDC / TR-D2251WDIR4v3

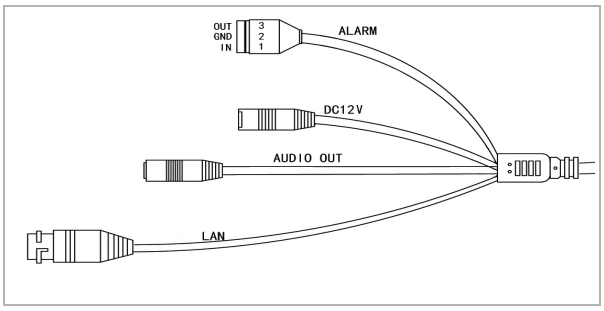


Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
Alarm I/O	Alarm inputs and outputs.

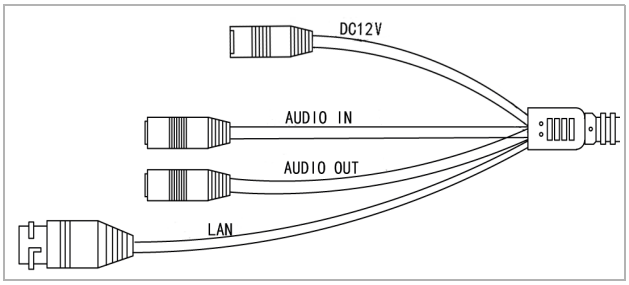
1.1.24 TRASSIR TR-D2121CL3 / TR-D2221WDCL4 / TR-D2151CL3v7 / TR-D2251WDCL4 / TR-D2251WDDL4v3

External connectors:

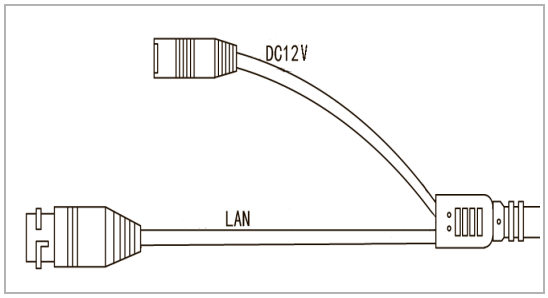
TR-D2151CL3v7



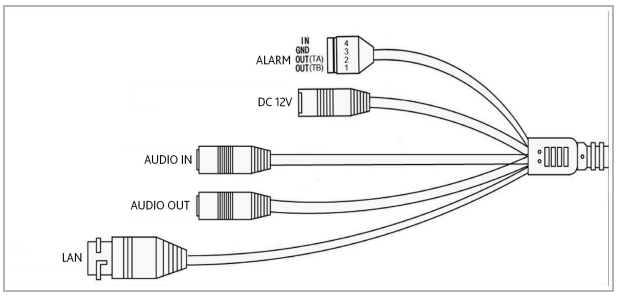
TR-D2221WDCL4



TR-D2121CL3



TR-D2251WDCL4 / TR-D2251WDDL4v3

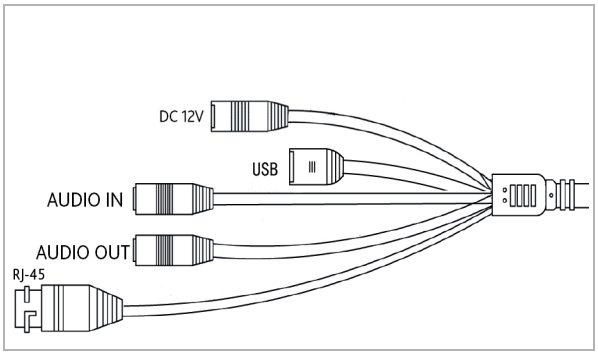


Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
Alarm I/O	Alarm inputs and outputs.

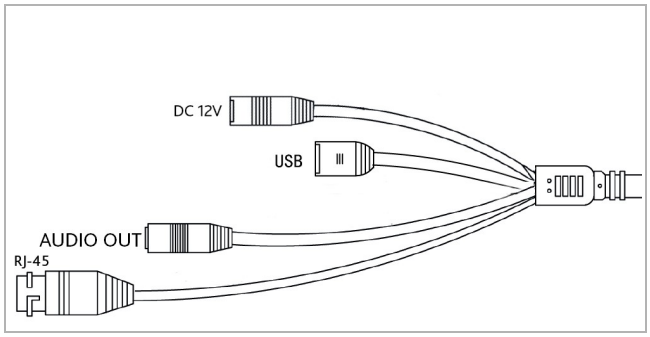
1.1.25 TRASSIR TR-D2D2 / TR-D2D2v2 / TR-D2D2v3 / TR-D3123IR2v3 / TR-D3123IR2v4 / TR-D3123WDIR2 / TR-D3143IR2 / TR-D4D2 / TR-D4D2v2 / TR-D4D2v3

External connectors:

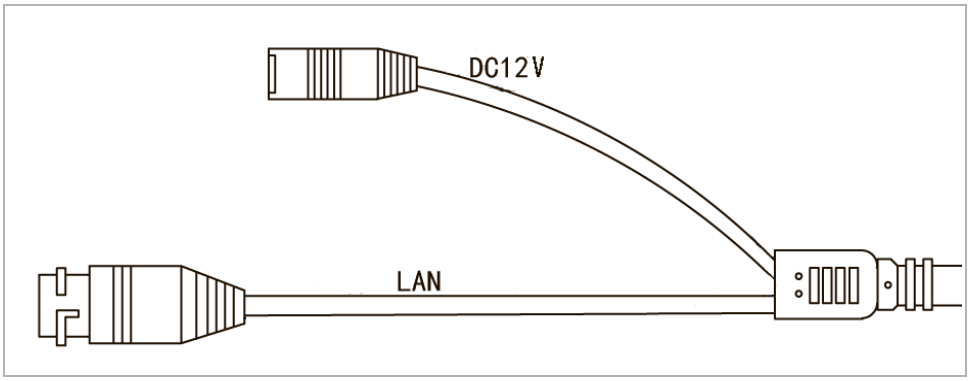
TR-D3123IR2v3 / TR-D3123WDIR2 / TR-D3143IR2



TR-D3123IR2v4



TR-D2D2 / TR-D2D2v2 / TR-D2D2v3 / TR-D4D2 / TR-D4D2v2 / TR-D4D2v3

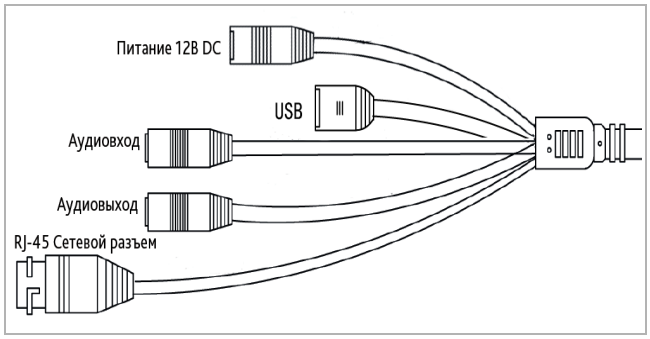


Connector	Description
LAN	LAN connector.
DC12V	12V power supply connector.
USB	USB connector for USBHDD.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.

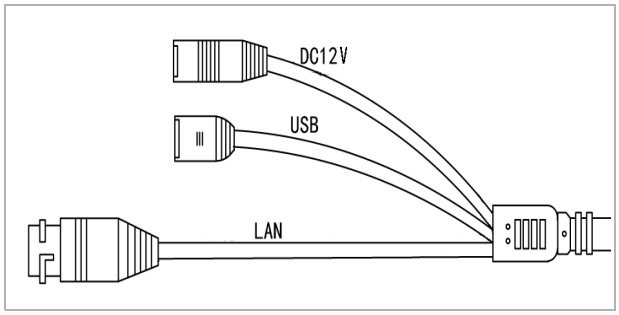
1.1.26 TRASSIR TR-D2D1v3 (P) / TR-D2D5 / TR-D2D5v2 / TR-D2D5v3 / TR-D3121IR1v2 / TR-D3121IR1v3 / TR-D3121IR1v4/ TR-D3141IR1 / TR-D4D5 / TR-D4D5v2 / TR-D4D5v3

External connectors:

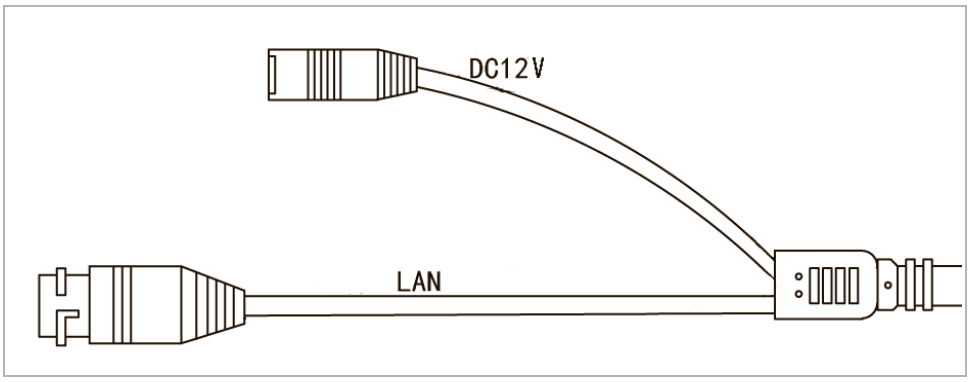
TR-D3141IR1



TR-D3121IR1v2 / TR-D3121IR1v3 / TR-D3121IR1v4



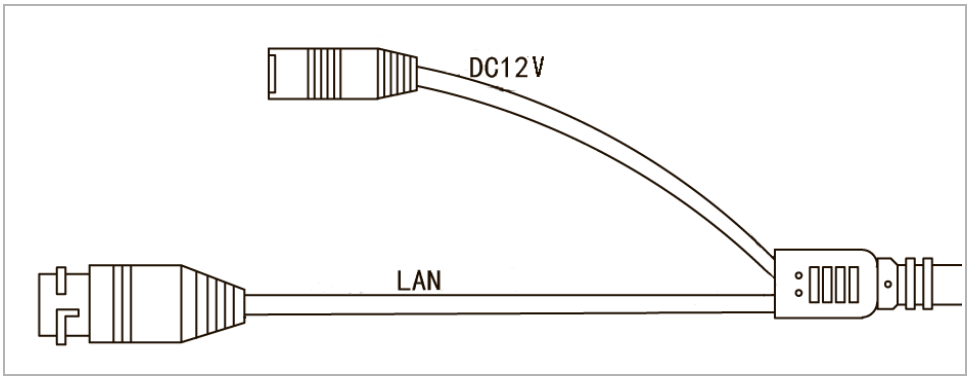
TR-D2D5 / TR-D2D5v2 / TR-D2D1v3 (P) / TR-D2D5v3 / TR-D4D5 / TR-D4D5v2 / TR-D4D5v3



Connector	Description
LAN	LAN connector.
DC12V	12V power supply connector.
USB	USB connector for USBHDD.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.

1.1.27 TRASSIR TR-D2S1 / TR-D2S1v2 / TR-D2S1v3 / TR-D2S1-noPoE / TR-D2S1-noPoEv2 / TR-D2S1-noPoEv3 / TR-D4S1 / TR-D4S1v2 / TR-D4S1-noPoEv2 / TR-D4S1v3

External connectors:

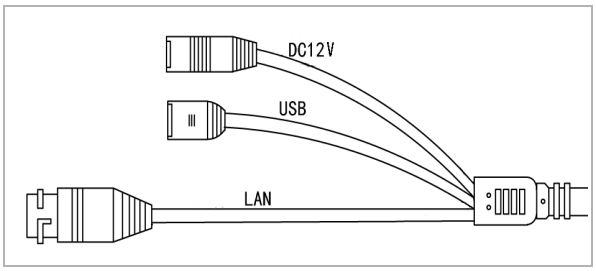


Connector	Description
LAN	LAN connector.
DC12V	12V power supply connector.

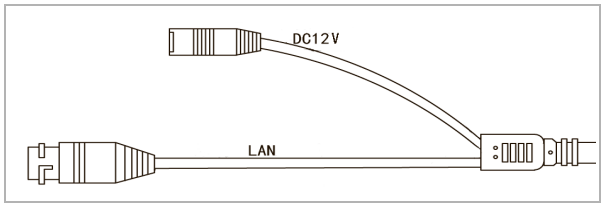
1.1.28 TRASSIR TR-D2S5 / TR-D2S5-noPoEv2 / TR-D2S5-noPoEv3/ TR-D2S5v2 / TR-D2S5v3 / TR-D4S5 / TR-D4S5-noPoE / TR-D4S5-noPoEv2 / TR-D4S5v2 / TR-D4S5v3 / TR-D8121IR2v2 / TR-D8121IR2v3 / TR-D8121WDIR2v2 / TR-D8141IR2 / TR-D8121IR2v4

External connectors:

TR-D8121IR2v2 / TR-D8121IR2v3 / TR-D8121IR2v4 / TR-D8121WDIR2v2 / TR-D8141IR2



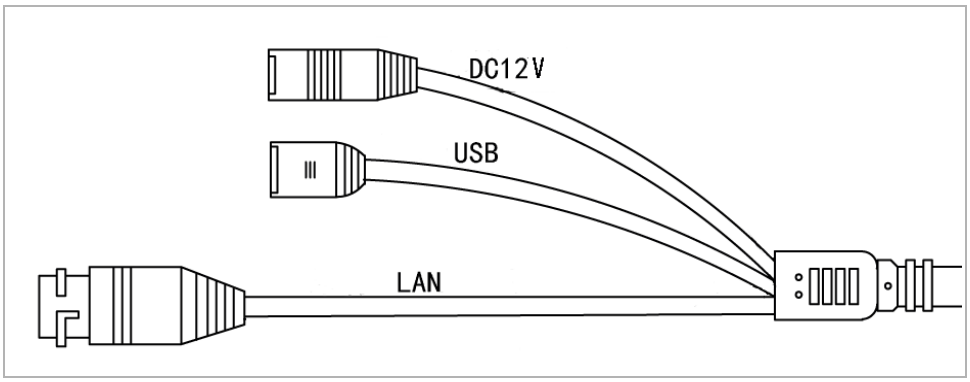
TR-D2S5-noPoEv2 / TR-D2S5 / TR-D2S5v3 / TR-D2S5-noPoEv3 / TR-D4S5 / TR-D4S5-noPoE / TR-D4S5-noPoEv2 / TR-D4S5v2 / TR-D4S5v3



Connector	Description
LAN	LAN connector.
USB	USB connector for USBHDD
DC12V	12V power supply connector.

1.1.29 TRASSIR TR-D3122WDZIR2 / TR-D3142ZIR2

External connectors:

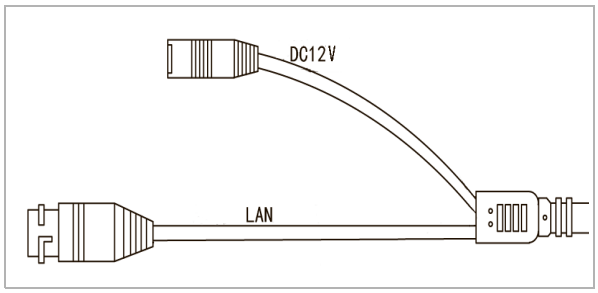


Connector	Description
LAN	LAN connector.
USB	USB connector for USBHDD
DC12V	12V power supply connector.

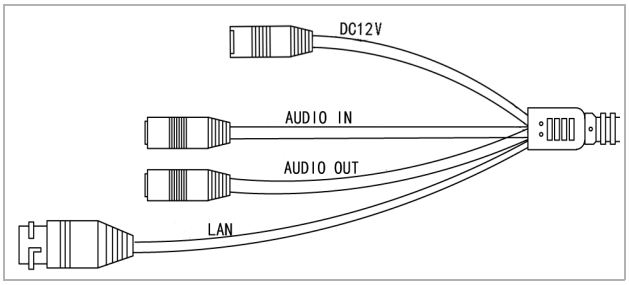
1.1.30 TRASSIR TR-D3121IR2v6 / TR-D3122ZIR2v6 / TR-D3123IR2v6 / TR-D3151IR2 / TR-D3151IR2v2 / TR-D3152ZIR2 / TR-D3152ZIR2v2 / TR-D3221WDIR3/ TR-D3221WDIR3v2 / TR-D3251WDIR3v2

External connectors:

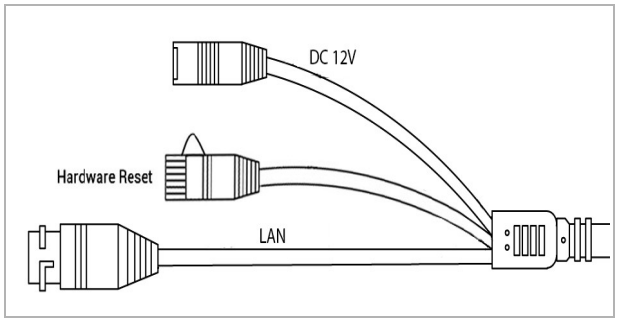
TR-D3121IR2v6 / TR-D3122ZIR2v6 / TR-D3151IR2 / TR-D3152ZIR2 / TR-D3152ZIR2v2



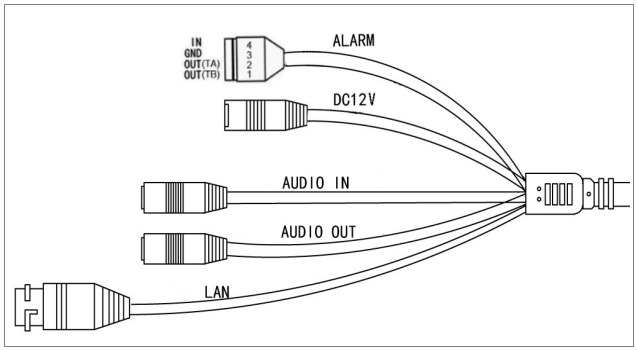
TR-D3123IR2v6



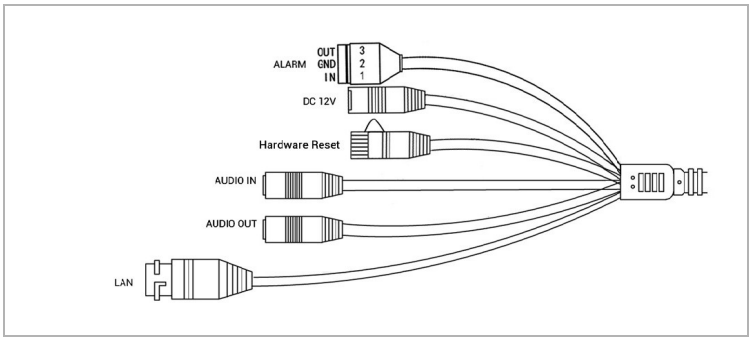
D3151IR2v2



TR-D3221WDIR3v2 / TR-D3251WDIR3v2



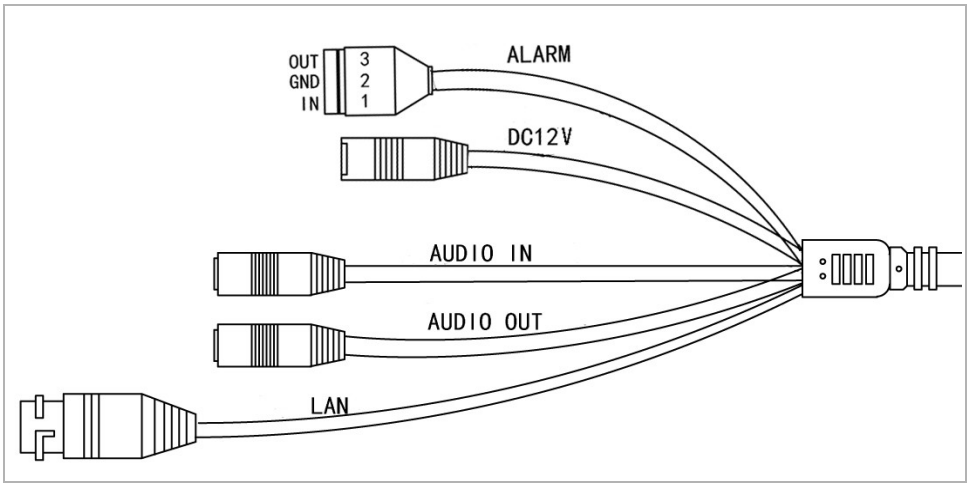
TR-D3221WDIR3



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
RESET	Hardware settings reset (see 2.6).
ALARM	Alarm inputs and outputs.

1.1.31 TRASSIR TR-D3123VIR2v2 / TR-D3143VIR2

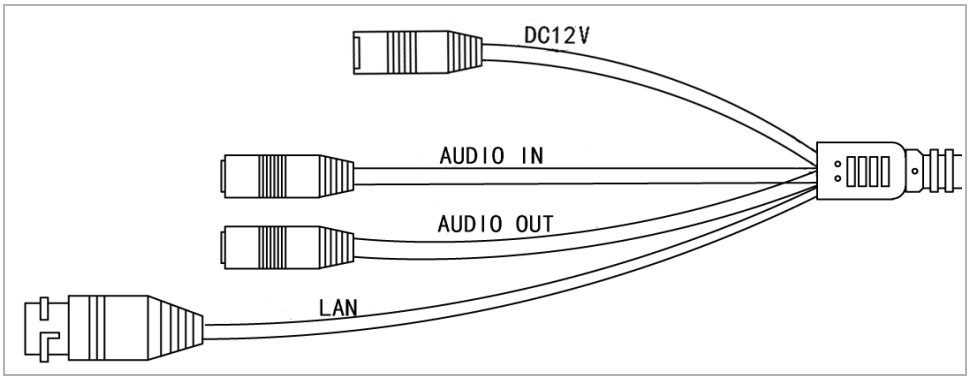
External connectors:



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
ALARM	Alarm inputs and outputs.

1.1.32 TRASSIR TR-D3151CL3v7

External connectors:

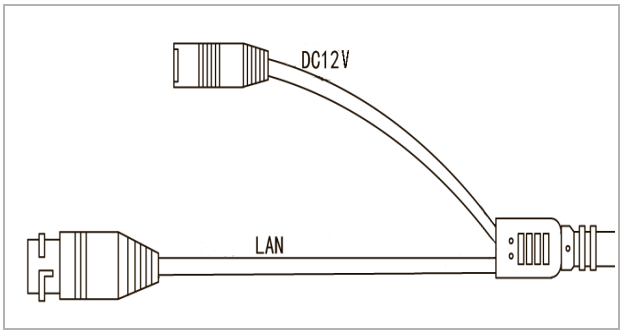


Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.

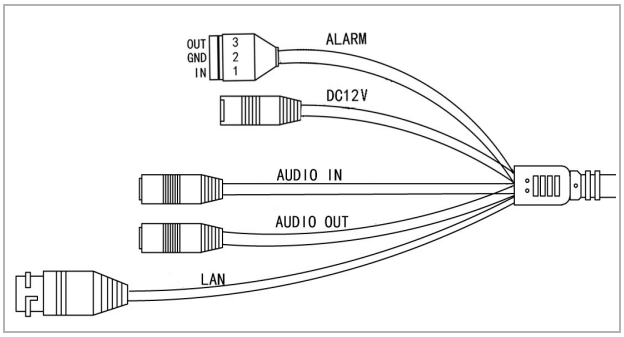
1.1.33 TRASSIR TR-D3121IR2Wv3 / TR-D3221WDIR3W / TR-D3221WDIR3Wv2 / TR-D3251WDIR3Wv2

External connectors:

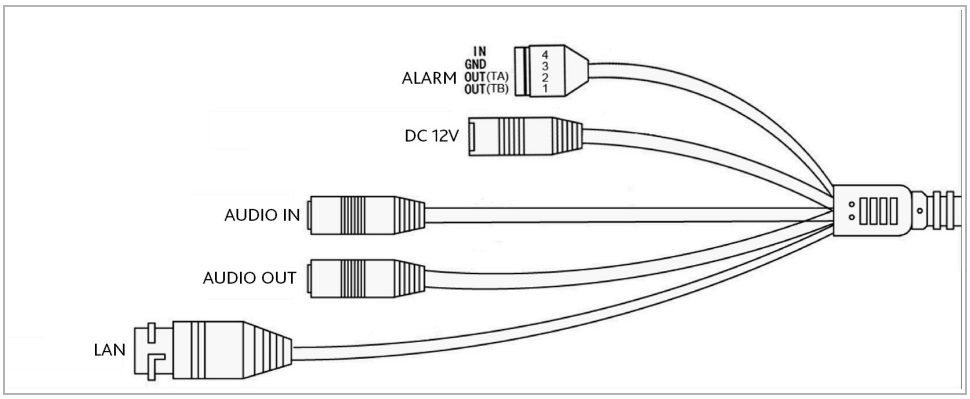
TR-D3121IR2Wv3



TR-D3221WDIR3W



TR-D3221WDIR3Wv2 / TR-D3251WDIR3Wv2

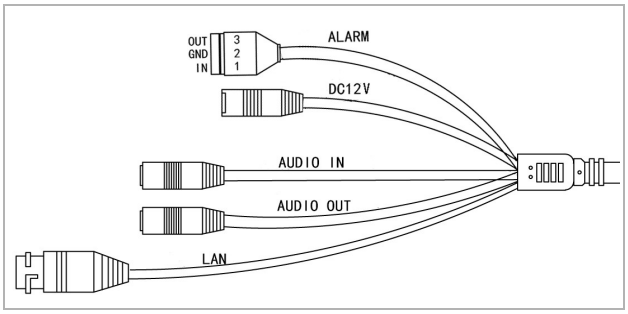


Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
ALARM	Alarm inputs and outputs.

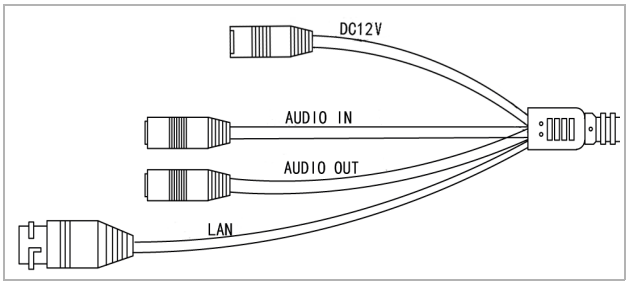
1.1.34 TRASSIR TR-D3223WDZIR3 / TR-D3223WDZIR3v2 / TR-D3253WDZIR3 / TR-D3253WDZIR3v2 / TR-D3153IR2 / TR-D3153IR2v2

External connectors:

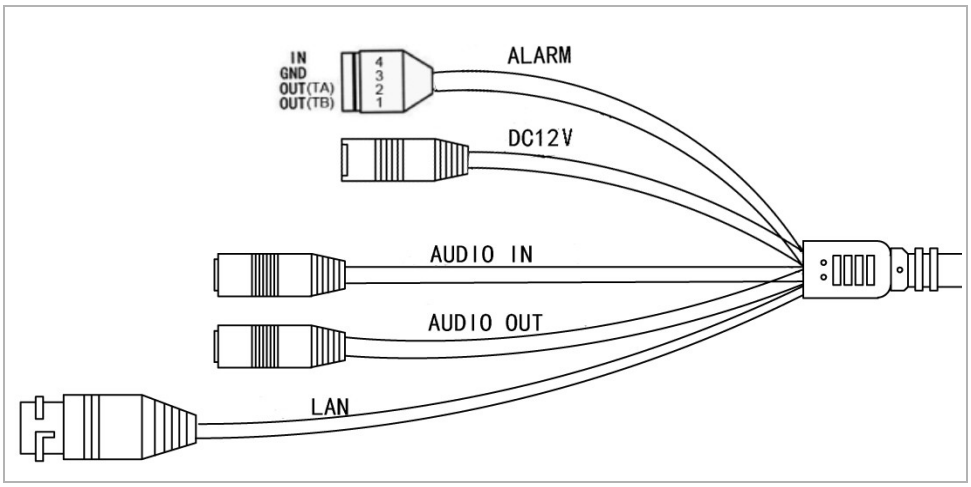
TR-D3153IR2v2 / TR-D3223WDZIR3 / TR-D3253WDZIR3



TR-D3153IR2



TR-D3223WDZIR3v2 / TR-D3253WDZIR3v2

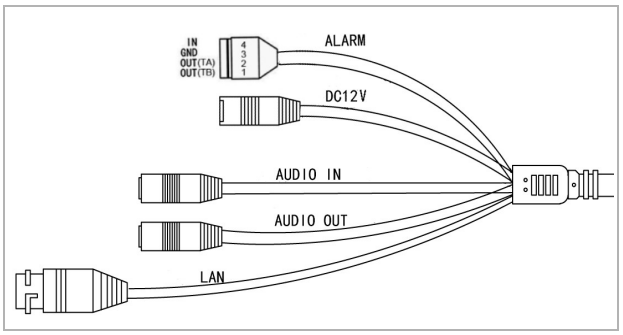


Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
ALARM	Alarm inputs and outputs.

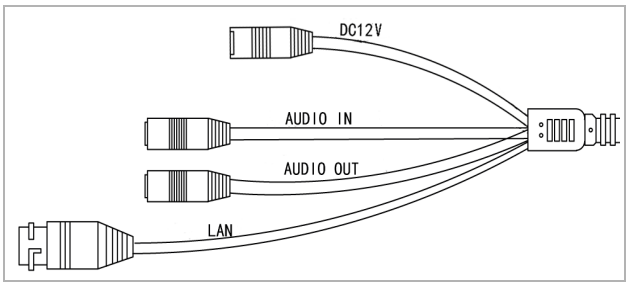
1.1.35 TRASSIR TR-D3121IR3v7 / TR-D3151IR3v7 / TR-D3221WDIR3v3 / TR-D3251WDIR3v3 / TR-D3321WDIR4 / TR-D3351WDIR4

External connectors:

TR-D3221WDIR3v3 / TR-D3251WDIR3v3 / TR-D3321WDIR4 / TR-D3351WDIR4



TR-D3121IR3v7 / TR-D3151IR3v7

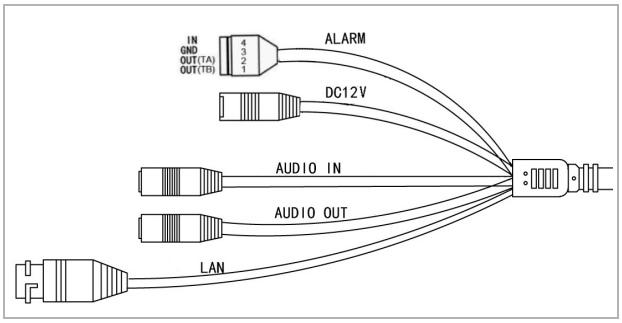


Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
ALARM	Alarm inputs and outputs.

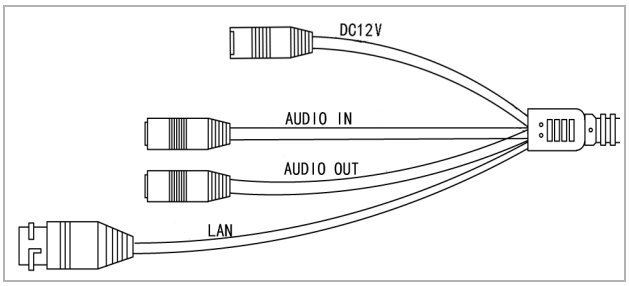
1.1.36 TRASSIR TR-D3123ZIR3v7 / TR-D3153ZIR3v7 / TR-D3223WDZIR4v3 / TR-D3253WDZIR4v3 / TR-D3323WDZIR4 / TR-D3353WDZIR4

External connectors:

TR-D3223WDZIR4v3 / TR-D3253WDZIR4v3 / TR-D3323WDZIR4 / TR-D3353WDZIR4



TR-D3123ZIR3v7 / TR-D3153ZIR3v7

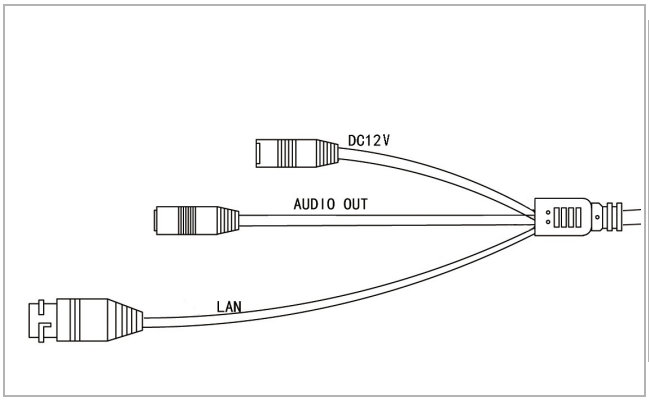


Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
ALARM	Alarm inputs and outputs.

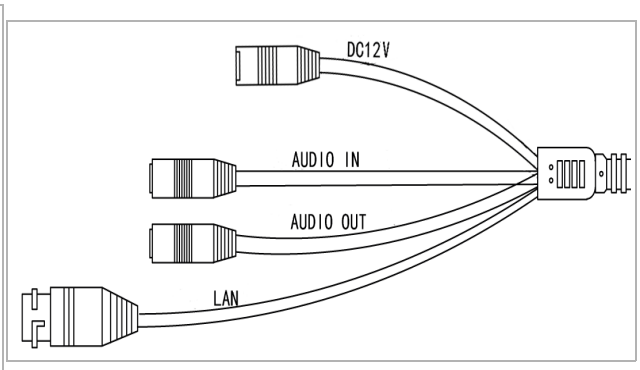
1.1.37 TRASSIR TR-D4121IR1v2 / TR-D4121IR1v4 / TR-D4121IR1v6 / TR-D4141IR1 / TR-D4151IR1 / TR-D4151IR1v2 / TR-D4161IR1 / TR-D4181IR1 / TR-D4221WDIR2 / TR-D4221WDIR2v2 / TR-D4221WDIR2v3 / TR-D4251WDIR2v3

External connectors:

TR-D4121IR1v4



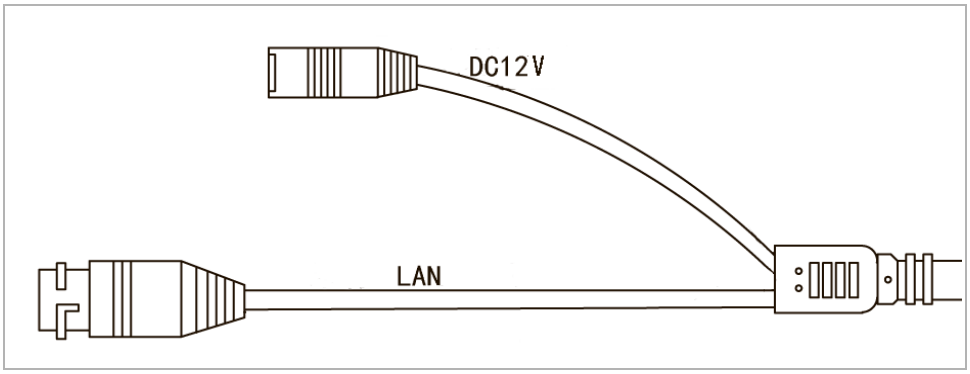
TR-D4121IR1v2 / TR-D4121IR1v6 / TR-D4141IR1 / TR-D4151IR1 / TR-D4151IR1v2 / TR-D4161IR1 / TR-D4181IR1 / TR-D4221WDIR2 / TR-D4221WDIR2v2 / TR-D4221WDIR2v3 / TR-D4251WDIR2v3



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.

1.1.38 TRASSIR TR-D4B5v2 / TR-D4B5-noPoEv2

External connectors:

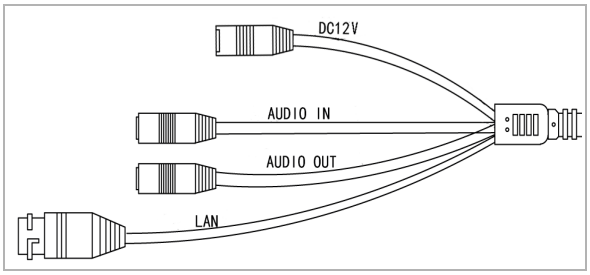


Connector	Description
LAN	LAN connector.
DC12V	12V power supply connector.

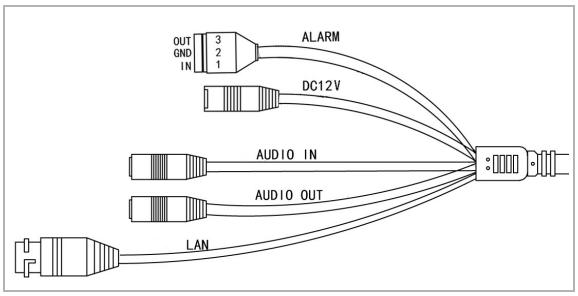
1.1.39 TRASSIR TR-D4121IR1v7 / TR-D4151IR1v7 / TR-D4251WDIR2 / TR-D4251WDIR2v2 / TR-D4321WDIR2 / TR-D4351WDIR2

External connectors:

TR-D4121IR1v7 / TR-D4151IR1v7 / TR-D4251WDIR2 / TR-D4251WDIR2v2



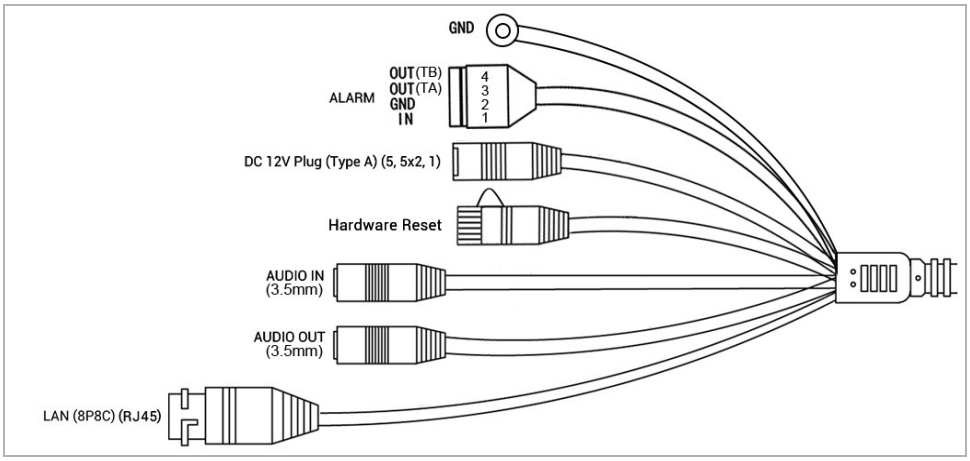
TR-D4321WDIR2 / TR-D4351WDIR2



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
ALARM	Alarm inputs and outputs.

1.1.40 TRASSIR TR-D6124IR10v3 / TR-D6154IR10v3

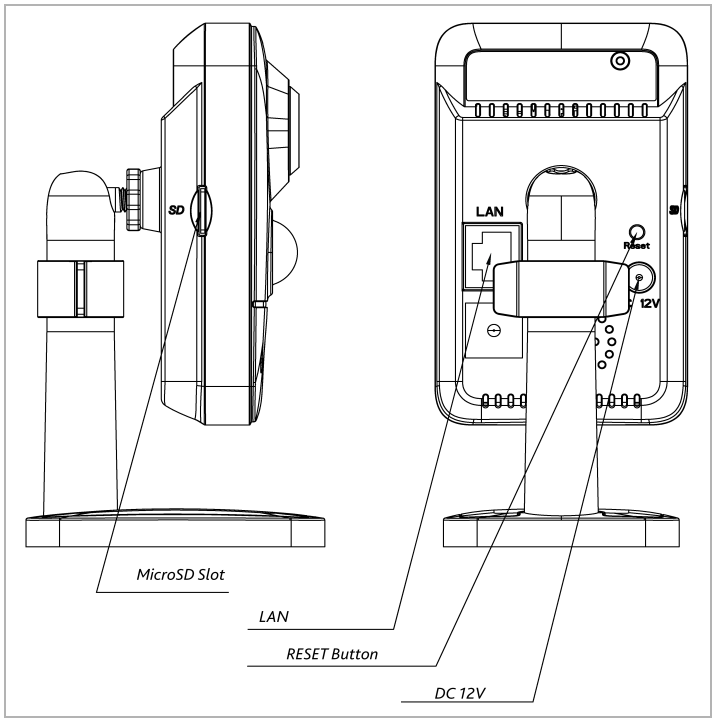
External connectors:



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
ALARM	Alarm inputs and outputs.
Hardware Reset	Hardware settings reset (see 2.6).
GND	Ground connector.

1.1.41 TRASSIR TR-D7121IR1W / TR-D7121IR1Wv2 / TR-D7121IR1Wv3

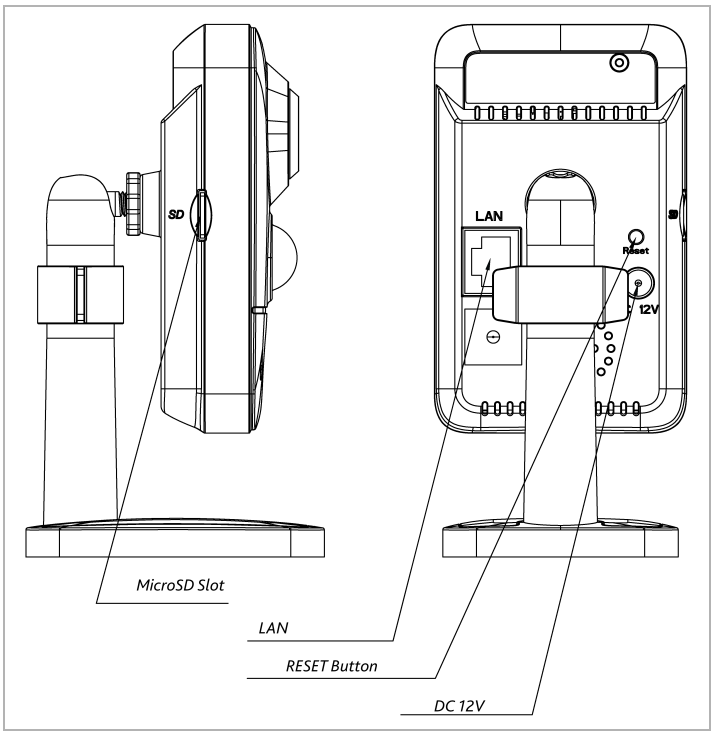
External connectors:



Connector	Description
LAN	LAN connector.
DC 12V	12V DC power connector.
RESET button	Button to reset camera settings to factory defaults.
MicroSD Slot	Slot for microSD memory card.

1.1.42 TRASSIR TR-D7121IR1v3 / TR-D7121IR1v4 / TR-D7121IR1v5 / TR-D7121IR1v6 / TR-D7121IR1v7 / TR-D7141IR1 / TR-D7151IR1 / TR-D7151IR1v7 / TR-D7251WDIR2Wv2 / TR-D7221WDIR2Wv2

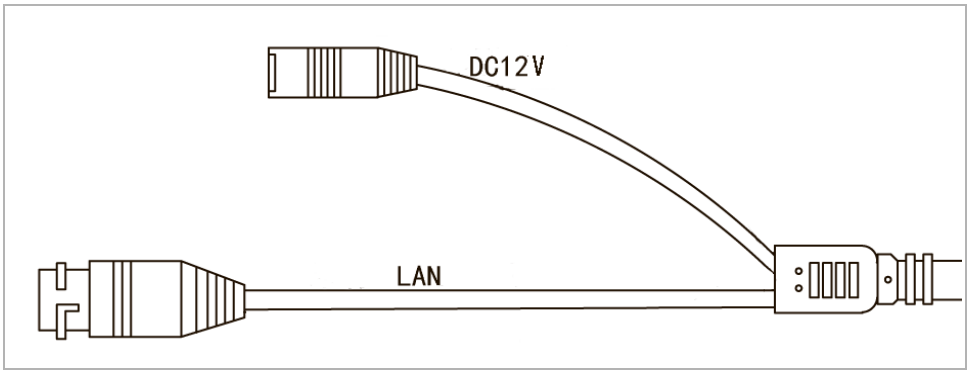
External connectors:



Connector	Description
LAN	LAN connector.
DC 12V	12V DC power connector.
RESET button	Button to reset camera settings to factory defaults.
MicroSD Slot	Slot for microSD memory card.

1.1.43 TRASSIR TR-D8121IR2W

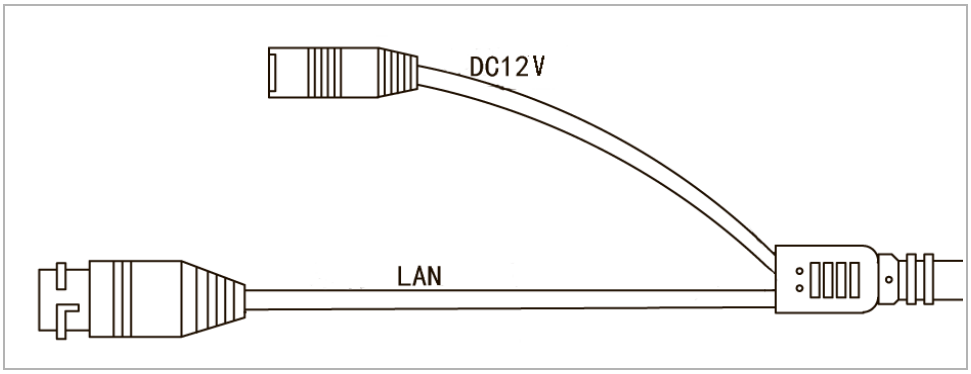
External connectors:



Connector	Description
RJ-45	LAN connector.
DC12V	12V power supply connector.

1.1.44 TRASSIR TR-D8121IR2Wv2 / TR-D8121IR2Wv3

External connectors:

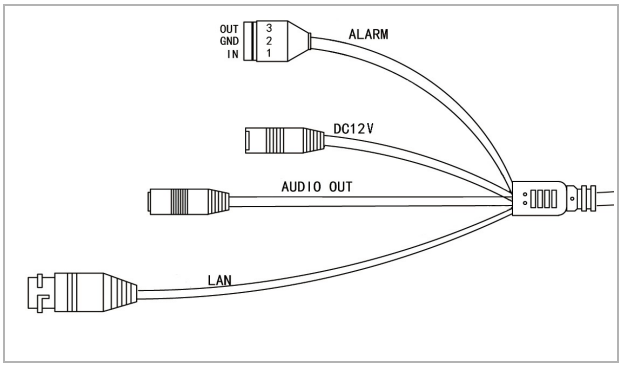


Connector	Description
RJ-45	LAN connector.
DC12V	12V power supply connector.

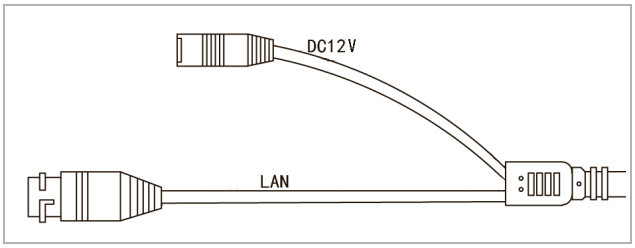
1.1.45 TRASSIR TR-D8121IR2v6 / TR-D8221WDIR3/ TR-D8221WDIR3v2 / TR-D8122ZIR2v6 / TR-D8251WDIR3 / TR-D8251WDIR3v2 / TR-D8151IR2/ TR-D8151IR2v2 / TR-D8152ZIR2 / TR-D8152ZIR2v2

External connectors:

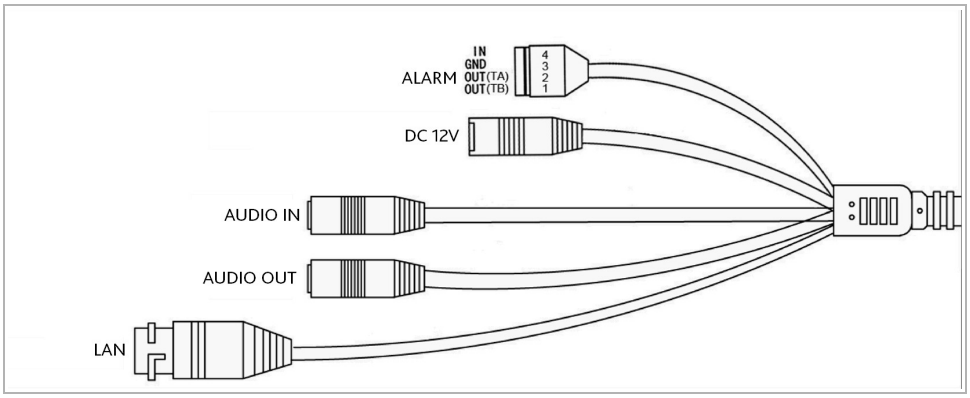
TR-D8221WDIR3 / TR-D8251WDIR3



TR-D8121IR2v6 / TR-D8122ZIR2v6 / TR-D8151IR2/
TR-D8151IR2v2 / TR-D8152ZIR2 / TR-D8152ZIR2v2



TR-D8221WDIR3v2 / TR-D8251WDIR3v2

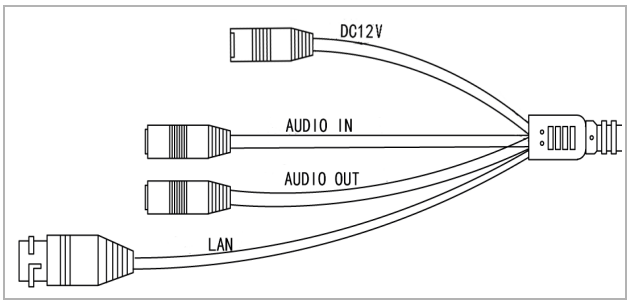


Connector	Description
RJ-45	LAN connector
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
DC12V	12V power supply connector.
Alarm I/O	Alarm inputs and outputs.

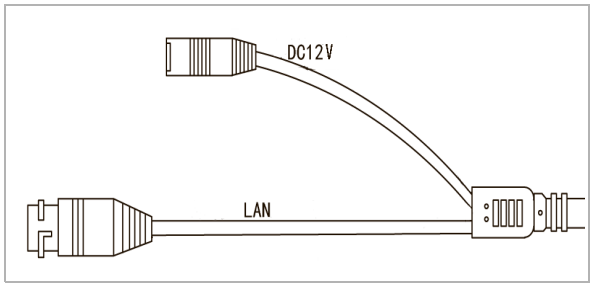
1.1.46 TRASSIR TR-D8121CL2 / TR-D8151CL3v7 / TR-D8221WDCL3 / TR-D8251WDCL3 / TR-D8251WDDL3v3

External connectors:

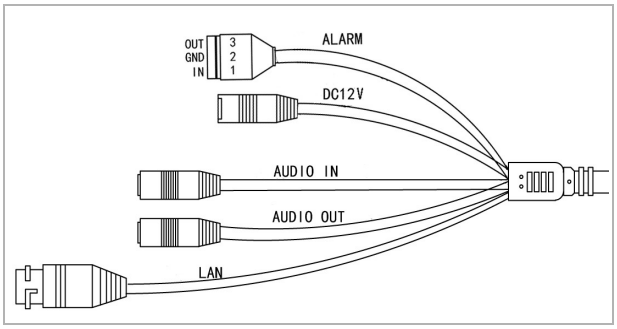
TR-D8151CL3v7



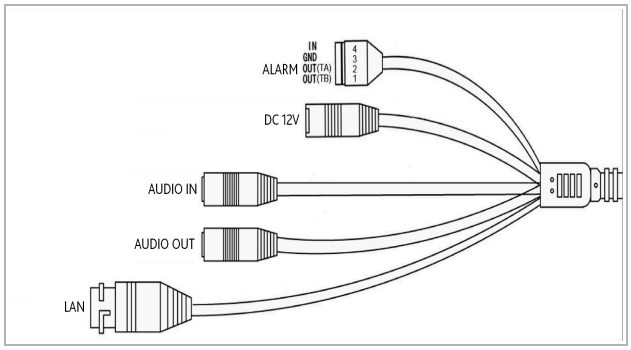
TR-D8121CL2



TR-D8221WDCL3



TR-D8251WDCL3 / TR-D8251WDDL3v3

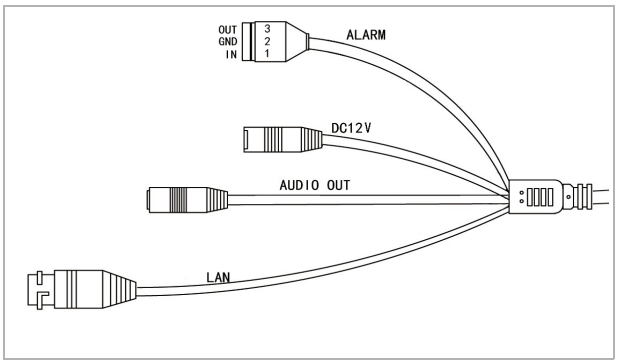


Connector	Description
RJ-45	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
DC12V	12V power supply connector.
Alarm I/O	Alarm inputs and outputs.

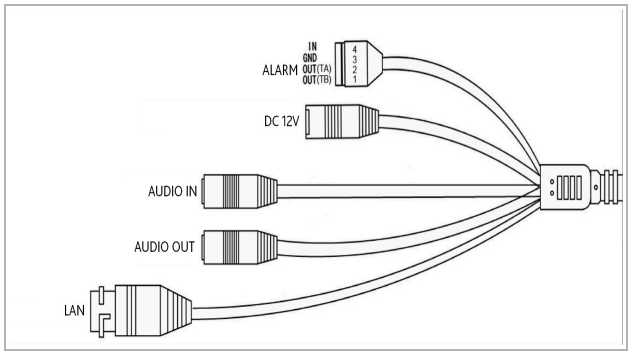
1.1.47 TRASSIR TR-D8121IR3v7 / TR-D8151IR3v7 / TR-D8221WDC / TR-D8221WDIR3v3 / TR-D8251WDC / TR-D8251WDIR3v3 / TR-D8321WDIR4 / TR-D8351WDIR4

External connectors:

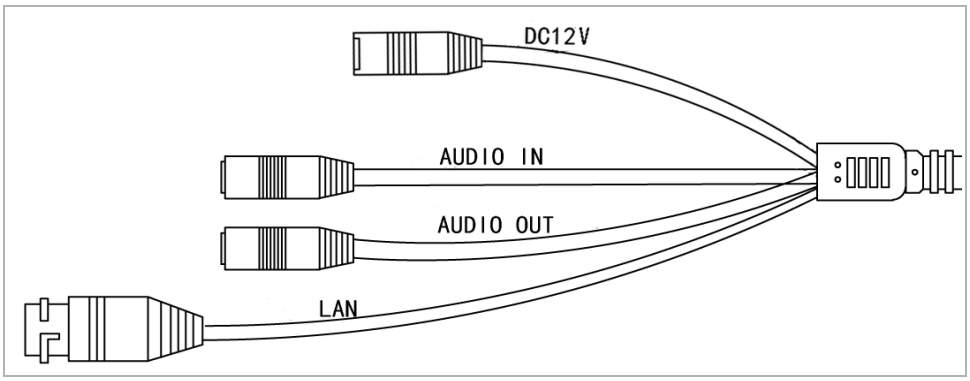
TR-D8221WDC



TR-D8221WDIR3v3 / TR-D8251WDC / TR-D8251WDIR3v3 / TR-D8321WDIR4 / TR-D8351WDIR4



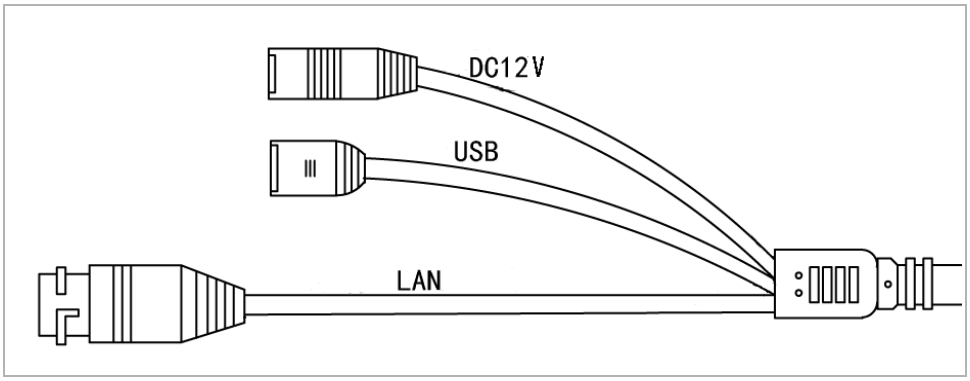
TR-D8121IR3v7 / TR-D8151IR3v7



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
Alarm I/O	Alarm inputs and outputs.

1.1.48 TRASSIR TR-D8123ZIR3

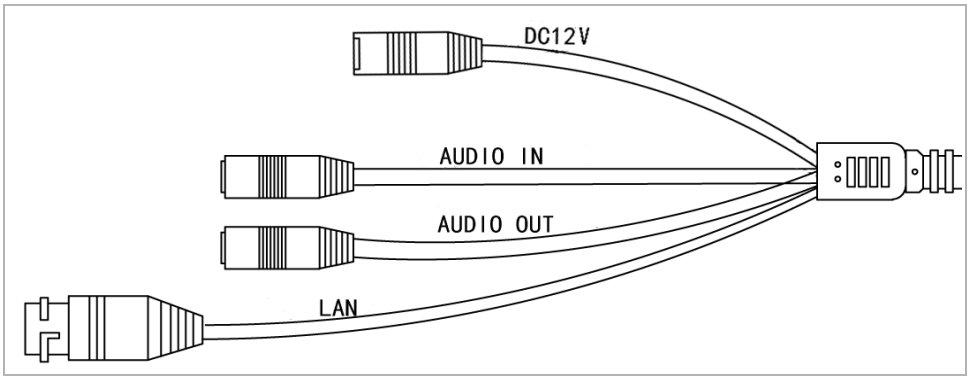
External connectors:



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
USB	USB connector for USBHDD.

1.1.49 TRASSIR TR-D8123ZIR4v7 / TR-D8153ZIR4v7

External connectors:

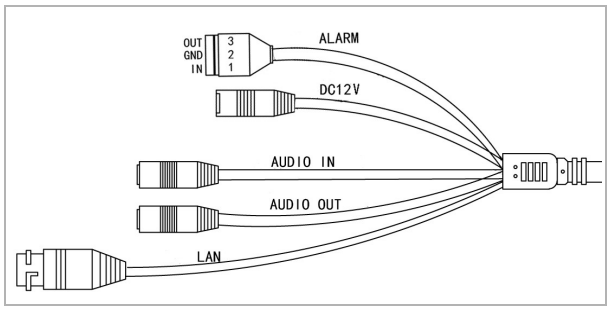


Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.

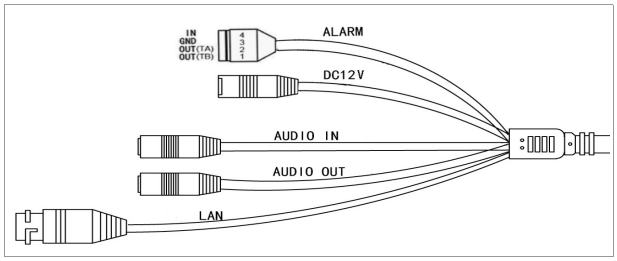
1.1.50 TRASSIR TR-D9141IR2 / TR-D9161IR2 / TR-D9151IR2 / TR-D9151IR2v2 / TR-D9251WDIR3 / TR-D9251WDIR3v2

External connectors:

TR-D9151IR2 / TR-D9151IR2v2 / TR-D9251WDIR3 / TR-D9141IR2 / TR-D9161IR2



TR-D9251WDIR3v2



Connector	Description
DC12V	12V power supply connector.
LAN	LAN connector.
AUDIO OUT	Speaker connector.
AUDIO IN	Active microphone connector.
ALARM	Alarm inputs and outputs.

1.2 Safety instructions

Please, read this manual before connecting and setting up your IP camera.

Check the conformity of the input voltage with the passport details and make sure that the power source is operatig properly.

Use network filters or UPS to increase the reliability of the IP-camera, protect against voltage drops, and ensure uninterrupted power supply.

Do not expose the IP camera to high pressure, shaking, mechanical shock, or strong electromagnetic radiation. Avoid installing the equipment on surfaces subject to vibrations, as this may damage it. When transporting, the IP camera must be placed in its original packaging or packaging the device safety.

Do not touch the sensor module. If necessary, use a clean cloth with a small amount of ethanol. The operation of the sensor may be disrupted by the laser ray, so when using any laser equipment, make sure that the rays do not hit the surface of the matrix. Do not aim the camera at the sun or very bright areas. This can lead to loss of image clarity, and can significantly shorten the life of the sensor module.

Do not expose the camera to extremely high or low temperatures (you can see the specification in the device datasheet).

Do not use the device in dirty rooms with high humidity, as this may result in a fire or an electrical short circuit. Free air exchange is required for proper camera operation.

In cases where the IP camera installation requires opening the housing, the silica gel must be replaced with a spare one from the kit.

Do not expose the equipment to direct sunlight. Do not place it near heat sources such as a stove, heater or radiator (it may result in fire).

The IP camera mounted on a wall or ceiling must be securely fixed.

If case of IP camera malfunction, contact your supplier or the nearest service center. Do not attempt to repair the camera by yourself. (The manufacturer declines the warranty obligations for damages resulting from unauthorized repairs or maintenance.).

1.3 Warranty obligations

The warranty period for cameras is 5 years.

The warranty obligations are valid from the date of sale of the IP camera to the final consumer and throughout the entire warranty period

If the IP camera malfunctions during the warranty period, you are entitled to request a free repair, except for non-warranty cases, in DSSL Service Center.

The warranty is void if the cause of the malfunction of the IP camera is:

- intentional corruption;
- fire, flood, or any other natural disaster;
- power outages;
- violation of technical requirements for placement, connection and operation;
- mechanical damages.

CHAPTER 2. CONNECTING TRASSIR IP CAMERA

2.1 System requirements

To start working with the TRASSIR IP camera, you need a PC connected to the local network:

- on Windows, Mac OS, Linux etc.;
- having Google Chrome, Mozilla Firefox, Safari or any other web browser installed.

2.2 Local network connection

Depending on the model, you can choose one of the following options to connect the IP camera to the local network:

- using a network cable (you can check the description on the connectors in section 1.1);
- using a network cable to any network equipment with the support of PoE technology;
- to WiFi wireless network.

NOTE.

It is not recommended to use switches, injectors and other PoE power supplies that use the Passive PoE standard to power up the cameras.

2.3 IP address configuration

NOTE.

In order to connect to IP camera, you PC should be in the same local network with the camera. You can read a detailed description of the PC settings sequence in Supplement A.

The following network settings should be configured on the IP camera by default:

- IP address: 192.168.1.188;
- Subnet mask: 255.255.0.0;
- Gateway: 192.168.1.1;
- HTTP port: 80;
- user name: admin;
- password: admin.

The example of the network settings:

- IP address: 192.168.1.10;
- Subnet mask: 255.255.0.0.

Start the web browser and try to connect to the IP camera. To do this, type in http://192.168.1.188 into the address bar and press Enter.

Enter user name and password to access web interface (see section. 3.1), after that change the IP camera network settings (see section 3.4.3.1).

NOTE.

If you failed to get access to the IP camera, check you firewall settings and try again.

If the IP address of the camera differs from the default settings, then use the IPCManager utility (see section Searching for IP-camera using TRASSIR IPCManager app).

2.4 Connecting to the IP camera via the Internet

There are several options to access IP camera via the Internet:

- The Internet service provider provides an actual **static** IP address.

  In this case, the provider grants the subscribe a list of network settings: IP address, subnet mask, gateway and DNS server IP address, or PPPoE connection details, which should be specified in the camera settings. Using such a network organization, it is impossible to use an external IP address to connect to several network devices at once, that is, it will be possible to connect to only one IP camera at a time

NOTE.

A static camera IP address and other required parameters are specified in the network settings (see 3.4.3.1).

See PPPoE settings description in 3.4.3.4.

- The Internet service provider allocates an actual external **static** IP address, which is used to connect to an office or home network.

  In this case, to organize the local network, a special device is used - a router (or a NAT server). To access the IP camera from the Internet, you should configure forwarding of the incoming connections from the router (NAT server) to the internal local addresses of IP cameras

NOTE.

See detailed router settings description in «SUPPLEMENT C. Router settings».

- The Internet service provider allocates an actual external **dynamic** IP address. That is upon connection to the Internet the IP address will be different each time. This variant is very common when working through 3G, GPRS or ADSL connection.In thi case you should use DDNS server options.

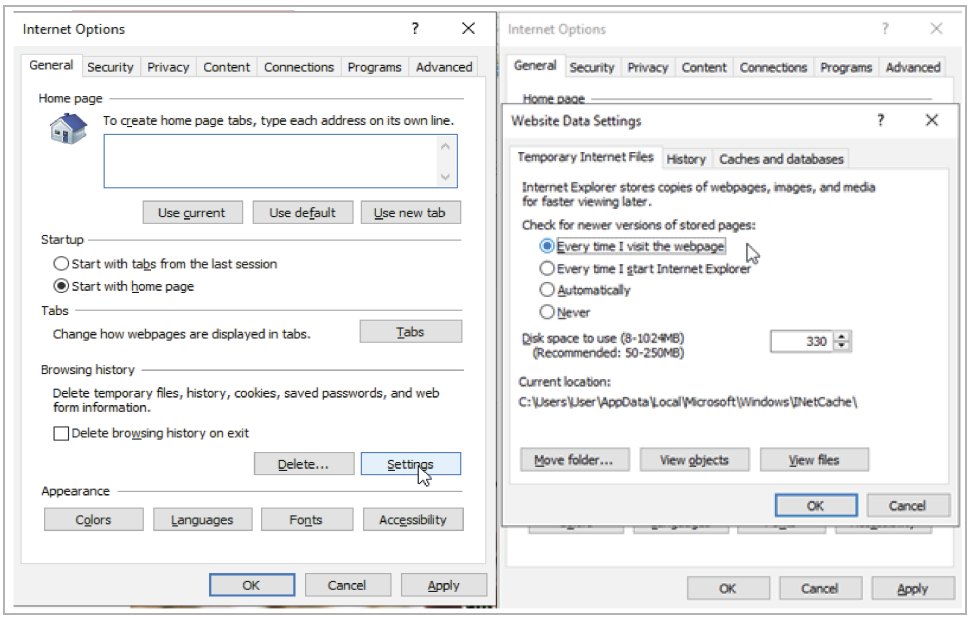
NOTE.

See description of DDNS server in IP camera in 3.4.3.1.

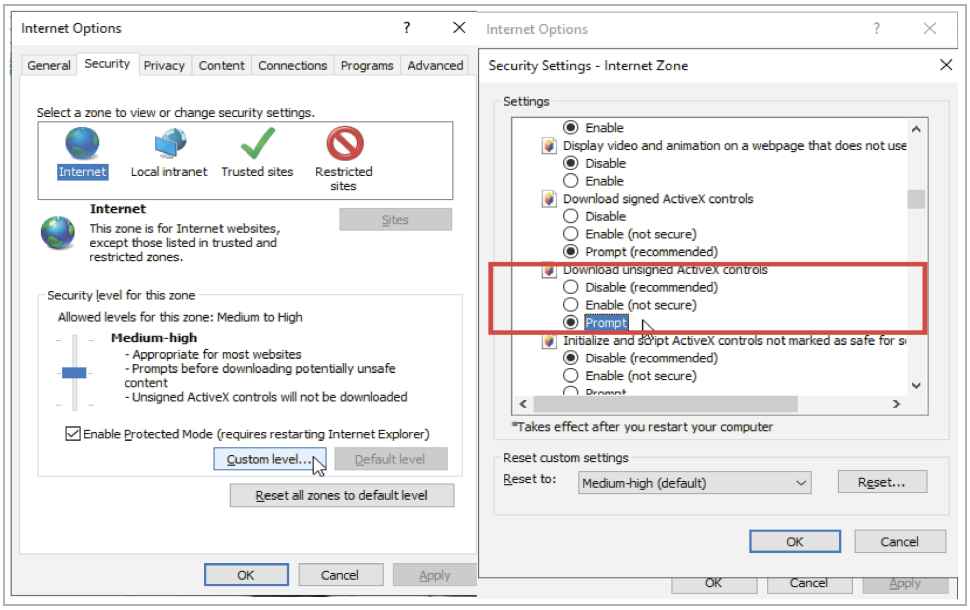
2.5 Confguring ActiveX for Internet Explorer

If you use the Internet Explorer browser to get image from the IP camera, check ActiveX settings before gaining access to the IP camera web interface (see section 3.1).

Open the General tab of the Internet Explorer options. Press Settings in the Browsing History settings group. Select Everytime I visit the webpage in Check for newer versions of the stored page parameters group in Website data settings window.



Open the Security tab, select the Internet area and press the Custom level... button. Select Prompt in Download unsigned ActiveX components.



Press OK in all opened windows to save the changes.

WARNING!

In case the image is absent in the preview window (see section 3.2) of the web interface (see section 3.1) it means ActiveX plugin is not installed. Internet Explorer will offer to download and install ActiveX plugin.

You should run the browser as Administrator to save some settings of the IP camera web interface.

2.6 Reset IP camera settings

There are three ways to reset IP camera settings:

1. Software reset to default values (see section 3.4.2.3).
2. Software reset to factory settings (see section 3.4.2.3).
3. Hardware reset using RESET button.

WARNING!

Software reset to the factory settings and hardware reset set factory default settings on the camera, including IP camera, login and password.

It is recommended to use these methods in case of emergency, if the software reset does not help.

You can perform the hardware reset using RESET button the following:

1. Power the camera on.
2. Press the RESET button (see 1.1) and hold for 10 sec.
3. Release the button. The camera will restart.
4. Try to connect to the IP camera (see 2.3).

CHAPTER 3. TRASSIR IP CAMERA CONFIGURATION

3.1 Gaining access to IP camera web interface.

In case you know IP camera IP address and port, then start Internet Explorer and enter http://<ip>:<port> into the address bar (where <ip> is a camera IP address and <port> is a value of http port). After that press Enter.

NOTE.

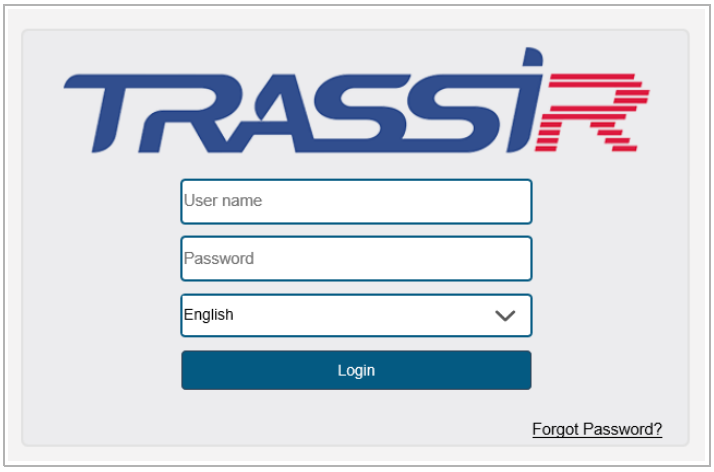
If the <port> is 80, you can omit it. Just enter http://<ip> into the address bar. E.g., http://192.168.1.188.

NOTE.

You can see the description of the IP camera network settings in 3.4.3.1.

Default values:
IP address: 192.168.1.188
Port: 80

In case of successful connection you will see a user authorization window:



Enter user name and password. You can also change the interface language. After that press Login.

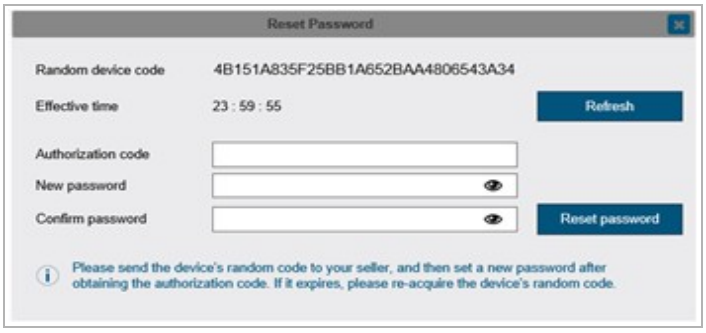
NOTE.

The default setting is described in 3.4.7.1.

Default values:
User name: admin
Password: admin

NOTE.

In order to reset your password press Reset password in the authorization menu. You will see the random device code in the opened window. The Random device code will be valid for 24 hours, it is not allowed to reboot or turn the device off within this time period.



After that contact our technical support via reset@trassir.com and provide the following data in your request:

1. **Full name.**
2. **Contact telephone number.**
3. **You company name.**
4. **Random device code.**
5. **The photo of the sticker on camera.**

As a reply you will receive the authorization code. Enter this code into the corresponding field in the authorization window and create a new password.

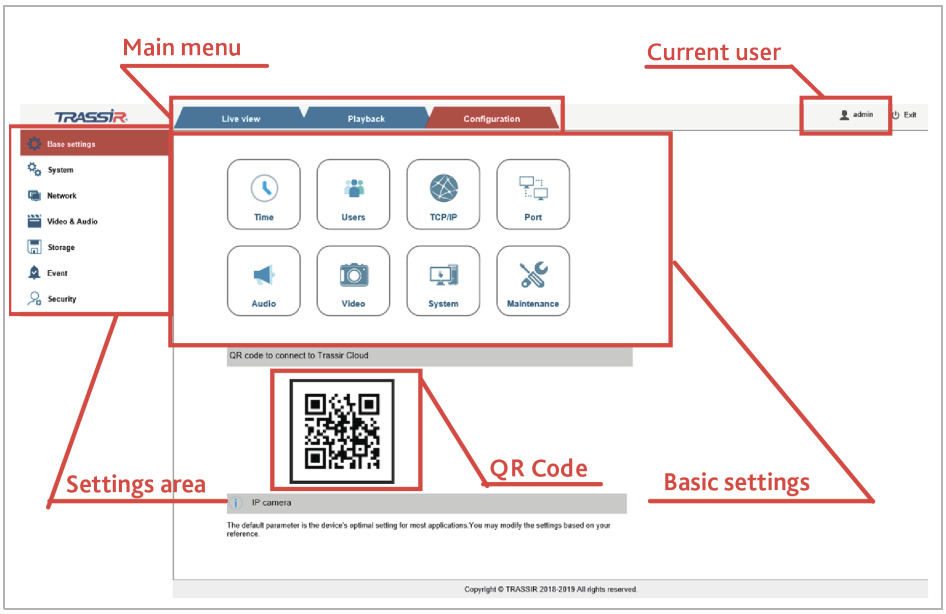
WARNING!

We recommend to change the administrator password (see 3.4.7.1) and IP address (see 3.4.3.1) upon the first connection to the IP camera web interface.

WARNING!

If there is no image from camera check your ActiveX settings in Internet Explorer (see 2.5)

In case of successful authorization in Internet Explorer you will see the settings menu.

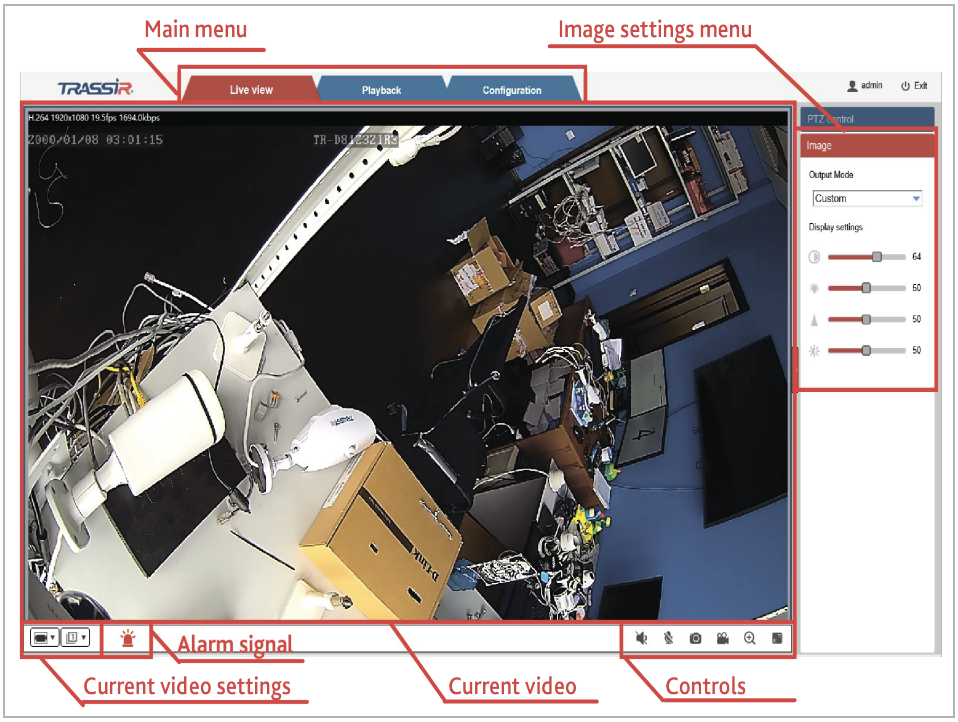


The menu consists of the following areas:

Setting	Description
Basic settings	IP camera main settings buttons.
Current user	Current authorized user. Read more about user settings in section 3.4.7.1.
Main menu	IP camera main menu.
Settings area	Click the tab to open. This area lets you perform basic actions to configure your camera.
QR code	QR code for TRASSIR Cloud connection via TRASSIR Client mobile app. Read more about TRASSIR Cloud connection in section 3.4.3.13 and in TRASSIR User guide.

3.2 Preview menu

This menu lets you check and configure parameters of the camera video. Press Preview to open the menu.



Setting	Description
Menu menu	Main IP camera menu
Image settings menu	Context menu to manage image and video settings (see 3.2.1).
Current video settings	Parameters of the video displayed in current window (see 3.4.4.2).
Current video	Real-time video image transmitted by the camera.
Alarm signal	Alarm signal. Flashes in case of alarm event or motion detection (see sections 3.4.6.1 and 3.4.6.2).

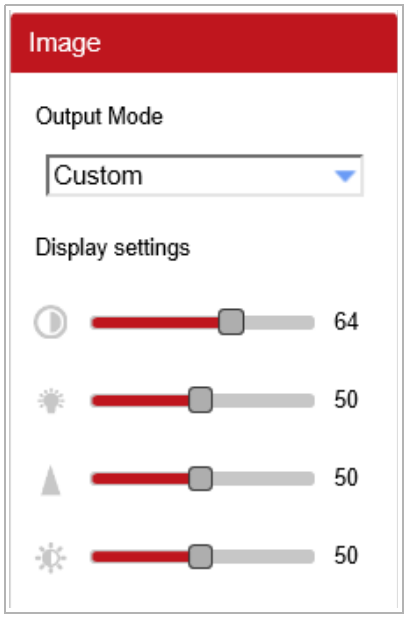
Setting	Description	
Controls	IP camera video controls:	
		Sound on/off
		Enable two-way communication
		Save snapshot
		Record start/stop
		Zoom in
		Fullscreen

NOTE.

Image settings and controls menu are available only in Internet Explorer.
Use Image settings to customize the image in any other browser (see section 3.4.4.5).

3.2.1 Image settings menu

Press in the right part of the Preview menu.



It lets you select and set up the following image settings modes:

- Standard;
- Bright;
- Vivid;
- Gentle;
- Custom.

You can configure the following settings manually when selecting the Custom mode:

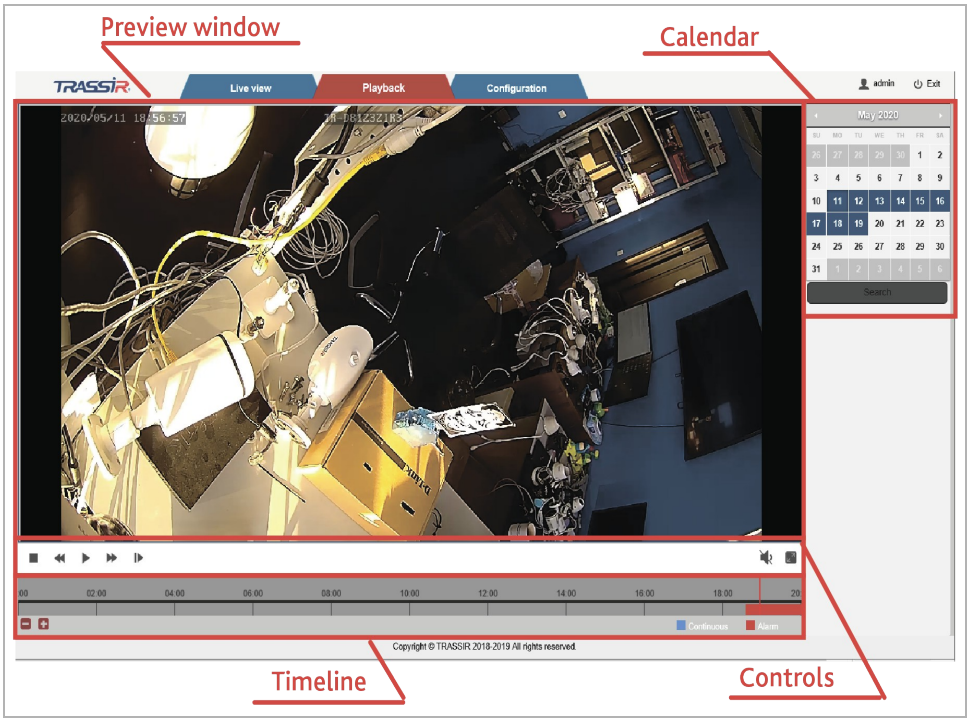
- Saturation — Saturation of the image. The higher the value is, the more saturated is the transmitted image.
- Brightness — Brightness of the image. The higher the value is, the brighter is the image.
- Sharpness — Image sharpness. The higher the value is, the sharper is the transmitted image.
- Contrast — Image contrast. The higher the value is, the sharper is the transmiited image.

Read more about image settings in section 3.4.4.5.

3.3 Archive menu

This menu lets you recorded video archive.

Press Playback to open the menu.

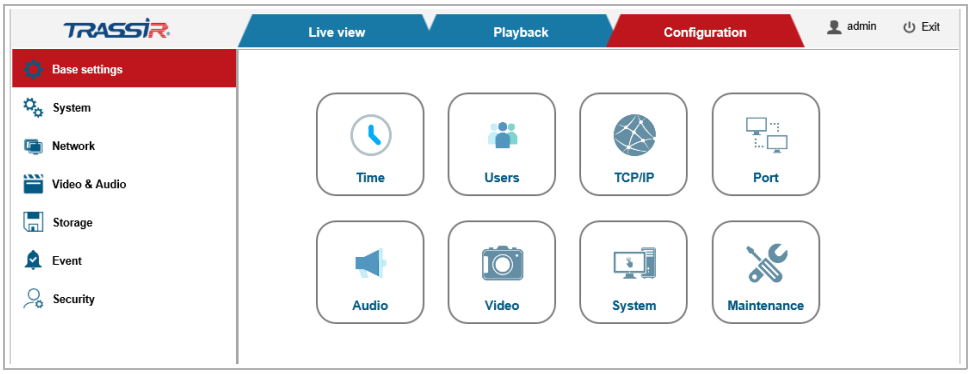


Setting	Description
Preview window	Lets you view your video.
Calendar	The highlighted dates in the calendar indicate that these days the video was recorded to the archive. Select the required date and press Search. The fragments with the recorded videos will be displayed on the timescale.
Timeline	The red color on a timeline indicates the alarm events record (see 3.4.6), the blue color indicates permanent record to the archive. Read more about archive recording setting in section 3.4.5. Hold down the left mouse button to move the timeline. Press to zoom in and out the timeline.

Setting	Description
Controls	Video playback controls:
	Start playback
	Pause playback
	Stop playback
	Proceed to the next recorded fragment
	Back to the previous fragment
	Frame by frame playback
	Fullscreen
	Sound on/off

3.4 Configuration menu

3.4.1 Base settings menu



Press Configuration to open the menu. You will see the Base Settings section.

This menu contains shortcuts to the main IP camera parameters and features:

- Time —date and time settings on IP camera (see 3.4.2.2);
- Users —configure IP camera access parameters (see 3.4.7.1);
- TCP/IP —configure IP camera network interface parameters (see 3.4.3.1);
- Port —select IP camera network ports (see 3.4.3.2);
- Audio —configure audio stream (see 3.4.4.1);
- Video Stream —configure video stream (see 3.4.4.2);
- System —check IP camera system status (see 3.4.2.4);
- Maintenance —perform IP camera system maintenance (see 3.4.2.6).

3.4.2 "System" menu

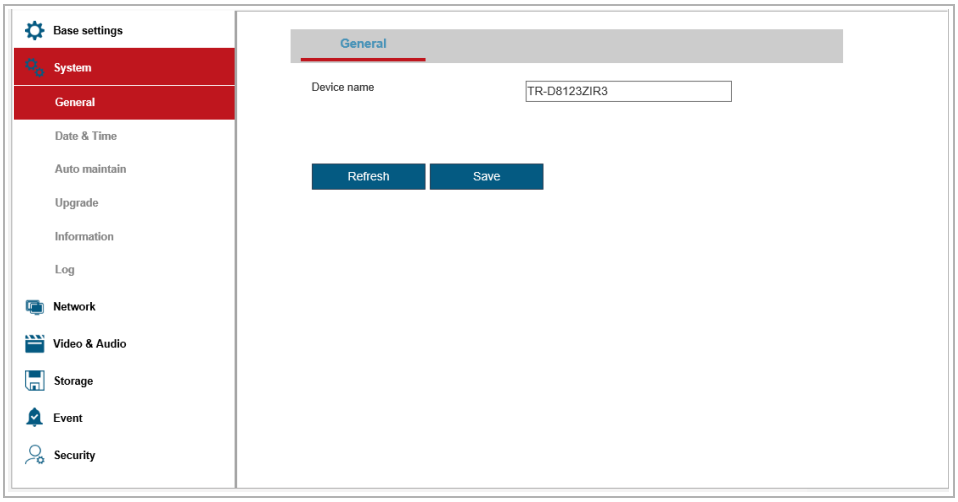
Click System to open the menu.

The menu consists of sections which allow to:

- General —change the device name (see section 3.4.2.6);
- Date & Time —configure date and time on IP camera (see section 3.4.2.2);
- Auto Maintain —configure automatic task management on IP camera (see section 3.4.2.3);
- Upgrade —upgrade IP camera hardware (see section 3.4.2.4);
- Information —check system information (see section 3.4.2.6);
- Log —check and save system log (see section 3.4.2.7).

3.4.2.1 “General” menu

Open General section in the System menu.



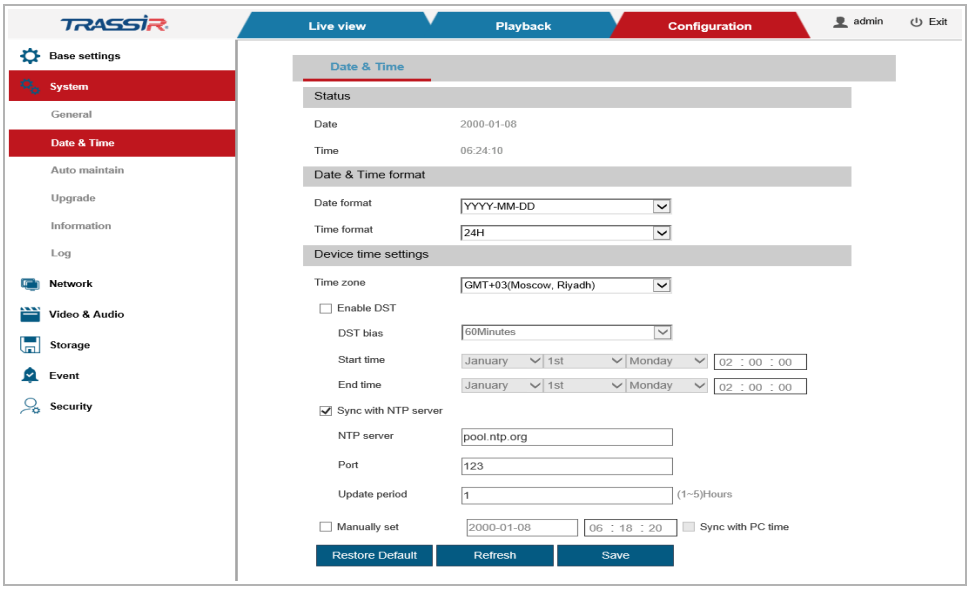
You can specify the name of the device which will be displayed when it is detected in local network in the Device name field.

Press Refresh to return to the current settings.

Press Save to save the changes.

3.4.2.2 "Date & time" menu

Open the Date & Time tab in the System settings menu to set up date and time on IP camera.



The Status block displays date and time set on IP camera.

The Date & Time format block lets you configure IP camera date and time format.

Configure values in the Time zone setting in Device Time Settings block to set up the time zone of the IP camera.

The IP camera also features daylight saving time. In order to activate it, set Enable DST flag.

NOTE.

Daylight saving time is not used in Russian Federation.

There are three ways to set up date and time on IP camera:

- Sync with NTP Server Time
  Specify data to connect to NTP server in NTP Server and Port fields. Select the time period, in hours, after which the time will synchronize on IP camera in the Update period field.
- Manual Set
  Enter current date and time into the Date and Time fields.
- Sync with PC Time

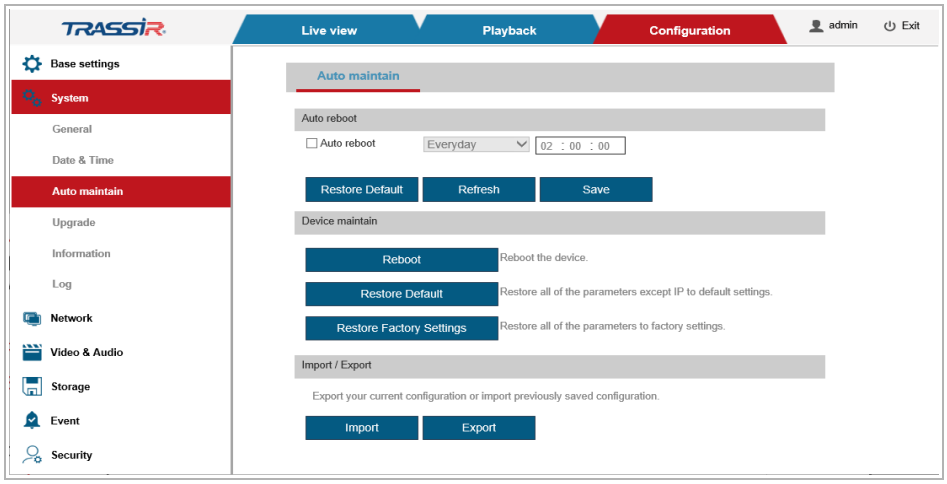
  The data from the PC on which the IP camera is configured will be downloaded into the Date and Time fields.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.2.3 "Auto maintain" menu

Open the Auto maintain section in the System settings menu.



The Auto reboot you can configure and schedule the device reboot. To do this, check the corresponding flag and select the day in the drop down list and the time in the adjacent field when the device will be rebooted.

Press Restore default to restore the default settings.

Press Save to save the changes.

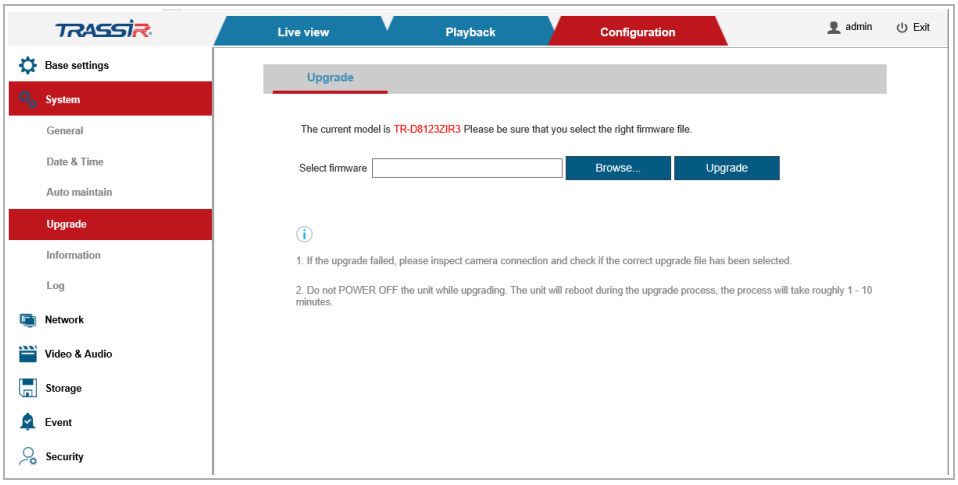
Press the corresponding button in the Device maintain block to:

- Reboot —reboot IP camera;
- Restore Default —reset all IP camera settings, except for network to default values (see 3.4.3.1);
- Restore Factory Settings —reset all IP camera settings to factory default, including network settings.

Use corresponding buttons in Import / Export block to save current settings configuration to a file or upload a previously saved configuration.

3.4.2.4 “Upgrade” menu

In order to update the IP camera firmware open the Upgrade section in the System settings menu.



Press the Browse button in Upgrade block and locate the firmware file. Press Upgrade to start uploading the file.

WARNING!

Using unofficial software to update the camera may result in a denial of warranty service.

WARNING!

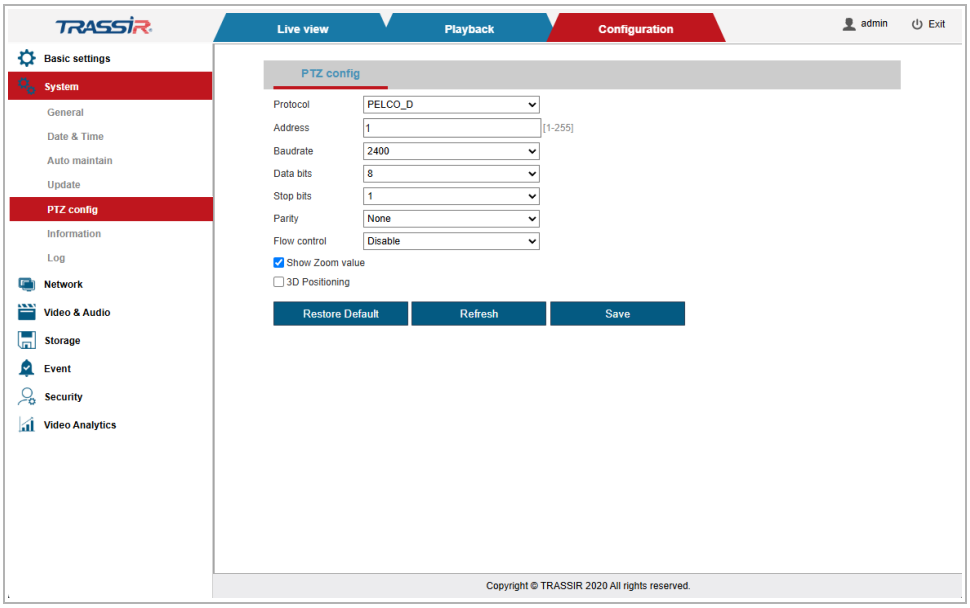
Update the camera software only if absolutely necessary.

WARNING!

The update may take several minutes.
Do not turn off the power or reboot the device during the update process.

3.4.2.5 "PTZ" menu

In order to setup PTZ of the IP camera open the PTZ in the System settings menu.



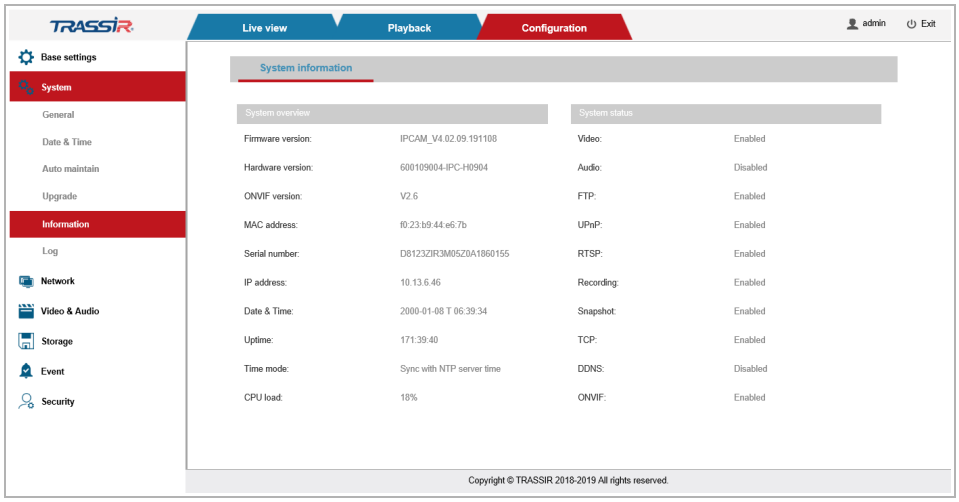
- Protocol: PTZ control protocol.
- Address: Camera ID on the network. Each PTZ device must have a unique ID to connect to one control device, such as a DVR or controller.
- Baudrate: Sets the data transfer rate between the camera and the control device using the PELCO protocol.
- Data bits: The number of data bits in one information packet for the PELCO protocol.
- Stop bits: The number of stop bits that signal the end of the information packet transmission.
- Parity: Sets the parity bit in PELCO serial protocols.
- Flow control: Additional flow control.

Check Show Zoom value to display the current zoom level of the camera.

Check 3D Positioning to specify the location for camera rotation on the video stream via the WEB interface (Live view tab).

3.4.2.6 “Information” menu

Open IP camera maintenance menu on Information tab in the System settings menu.



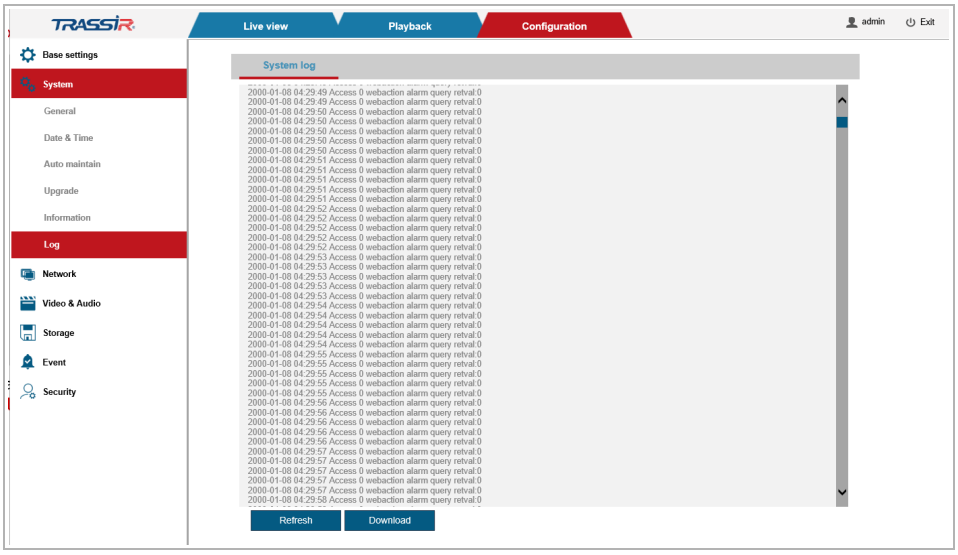
The System overview block provides the following information:

Setting	Description
Firmware version	IP camera firmware version
Hardware version	IP camera hardware version
Onvif version	ONVIF protocol version
MAC address	IP camera mac address
Serial Number	IP camera serial number
IP address	Device IP address
Date & Time	Date and time set on device
Uptime	Duration of the last continuous authorization of the current user
Time mode	The time synchronization method selected on the IP camera (see 3.4.2.2)
CPU load	CPU load level

The System status block contains info on the current status of some IP camera functions.

3.4.2.7 "Log" menu

The Log section of the System settings menu contains the system log.



You can download the system log in .txt or .html formats, if necessary. To do this, press Download, specify the name and the required file format and press Save.

3.4.3 "Network" menu

Press Network to open the menu.

The menu consists of the following sections which allow to:

- TCP/IP —check and configure camera network interface parameters (see section 3.4.3.1);
- Port —select network ports used by IP camera (see section 3.4.3.2);
- WIFI —configure IP camera wireless network connection parameters (see section 3.4.3.3);
- PPPoE — configure connection with IP camera on PPPoE protocol (see section 3.4.3.4);
- SMTP —configure parameters for sending IP messages by email (see section 3.4.3.5);
- UPnP —configure UpnP service parameters and IP camera network port forwarding (see section 3.4.3.6);
- DDNS —configure connection to DDNS server (see section 3.4.3.7);
- RTSP —configure RTSP data transfer (see section 3.4.3.8);
- RTMP — configure RTMP parameters (see section 3.4.3.9);
- VoIP — configure VoIP data transfer settings (see section 3.4.3.10);
- SNMP — configure camera management via SNMP(see section 3.4.3.11);
- IEEE 802.1x - (see section 3.4.3.12);
- Trassir Cloud —configure camera connection to TRASSIR Cloud cloud service (see section 3.4.3.13).
- HTTPS —configure data transfer via HTTPS for secure communication (see section 3.4.3.14).

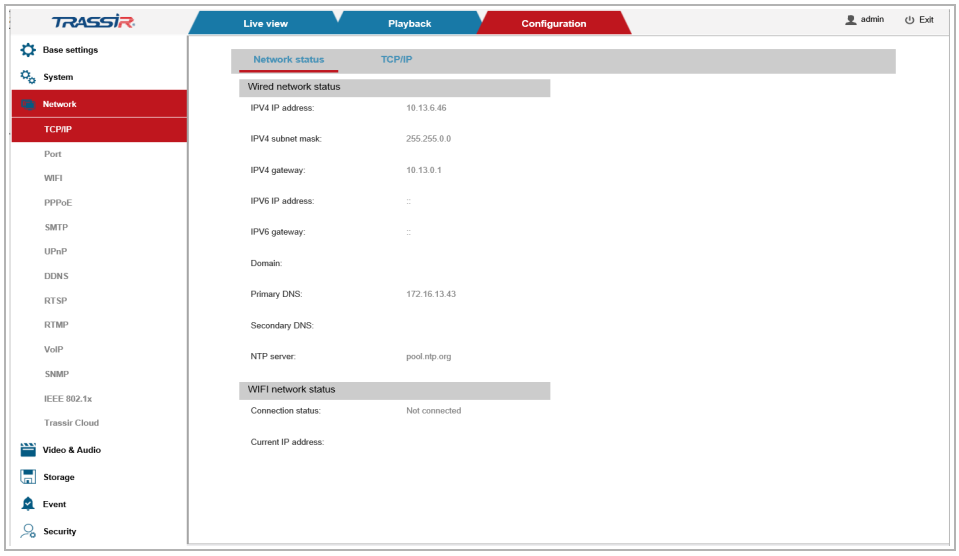
3.4.3.1 "TCP/IP" menu

The menu consists of the additional tabs which allow to:

- Network Status — check statuses of IP camera current network interfaces (see 3.4.3.1.1);
- TCP/IP — configure parameters of the network interfaces (see 3.4.3.1.2).

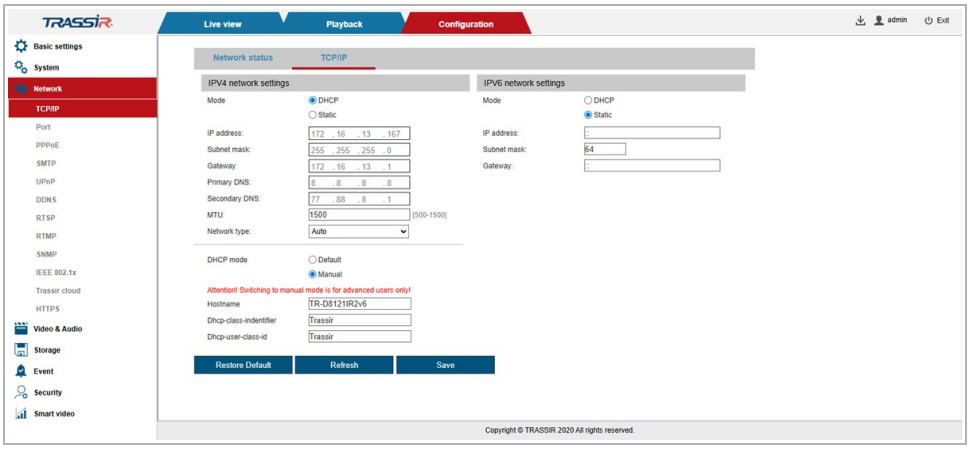
3.4.3.1.1 "Network status" tab

Open the Network status tab to check current status of the IP camera network interfaces.



3.4.3.1.2 "TCP/IP" tab

Open TCP/IP tab in the Network settings menu to change current network settings.



Before starting the configuration, select which version of the protocol will be configured.: IPv4 or IPv6.

Setting	Description
Mode	Select network interface configuration type: ◆ DHCP —Configure network interface using DHCP server; ◆ Use Static IP — Configure network interface manually. Other parameters are specified for the selected configuration type.
IP address	The IP address that will be used when accessing the IP camera.
Subnet mask	Mask of the subnet to which the IP camera is connected.
Gateway	The IP address of the proxy server if a gateway is used to connect to another network (for example, the Internet).
Primary DNS	Main DNS server address.
Secondary DNS	Alternate DNS server IP address.
MTU	Network card value. The default value is 1500.
Network type	Network card speed value.
DHCP mode	Select the DHCP mode: Default or Manual. For Manual mode, enter the parameters Hostname, Dhcp-class-identifier, Dhcp-user-class-id.

WARNING!

We strongly recommend to change the camera IP address on the first connection to the IP camera web interface.

WARNING!

Be cautious when using a DHCP server to configure IP camera network settings. Since the DHCP server assigns the camera the first free IP address.

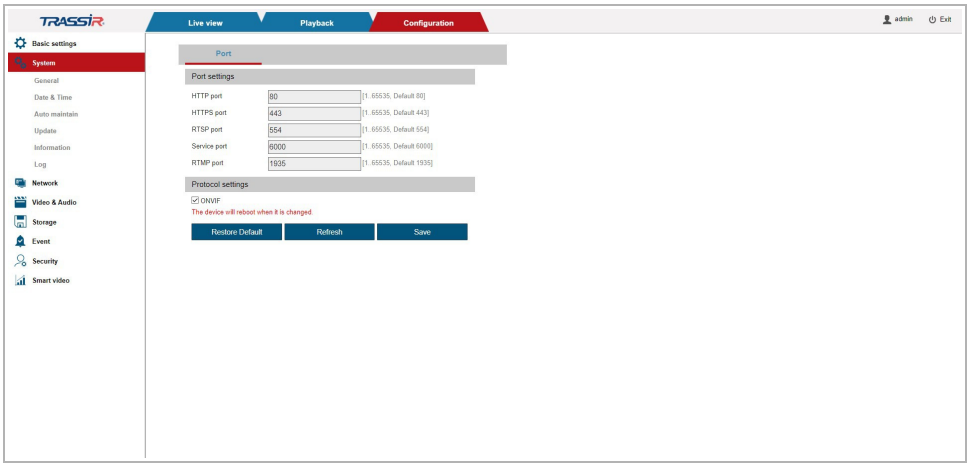
If there is no DHCP server in the local network, the camera will be assigned an IP address of the following type:169.254.x.x.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.3.2 "Port" menu

In order to configure networks ports used to access IP cameras features open the Port section.



Setting	Description
HTTP Port	The number of the port used to connect to IP camera web interface via web browser. Default value: 80 Available values range: from 1 to 65535 or 80.
RTSP Port	The number of port on which the data from IP camera will be transferred on RTSP protocol. Default value: 554 Available values range: from 1 to 65535 or 554.
RTSP Port	The number of port used for IP camera management. Default value: 6000 Available values range: from 1 to 65535 or 6000.
Service port	The number of port used for IP camera management. Default value: 6000 Available values range: from 1 to 65535 or 6000.
RTMP Port	The number of port used for IP camera management. Default value: 1935 Available values range: from 1 to 65535 or 1935.

WARNING!

Network port numbers should not match.

To use ONVIF connection set the flag in the Protocol settings block.

NOTE.

Use the following requests to connect an IP camera and transmit video on RTSP:

Main stream: rtsp://[login]:[password]@[IP address]:[rtsp port]/live/main

Sub stream: rtsp://[login]:[password]@[IP address]:[rtsp port]/live/sub

Third stream: rtsp://[login]:[password]@[IP address]:[rtsp port]/live/mobile

Example rtsp://admin:12345@192.168.25.32:554/live/main

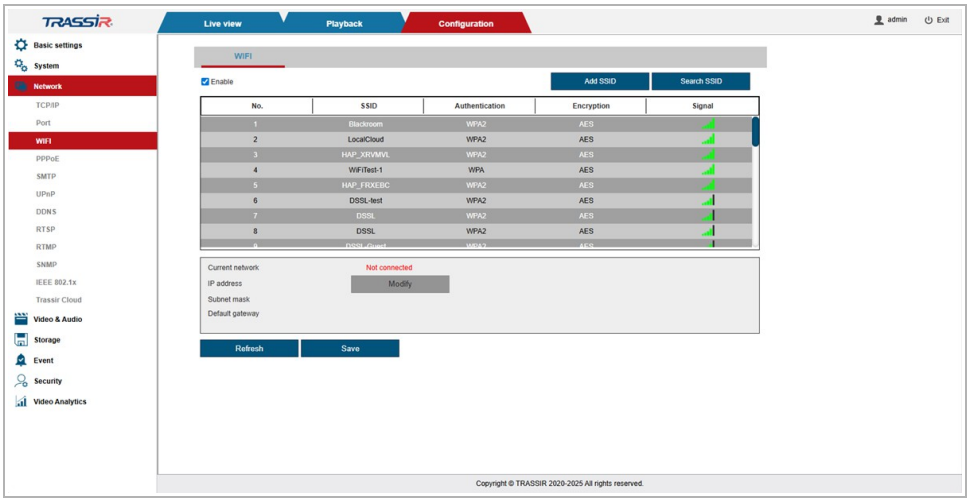
Read more about connecting an IP camera on RTSP in "SUPPLEMENT D. Operation on RTSP and ONVIF".

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.3.3 “WIFI” menu

To connect your camera to a wireless local network, open WIFI section of the Network settings menu.



Press the Search SSID button to display all available wireless networks in the table.

To connect manually, click the Add SSID button and enter the network name, encryption type, and password in the window that opens.

If necessary, you can change the camera's IP address on the network by clicking the Modify button.

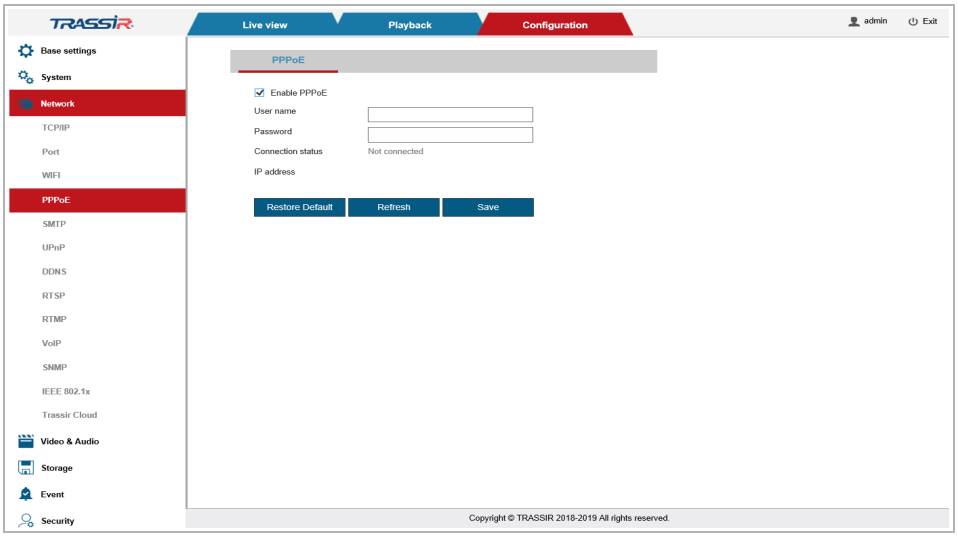
Press Save to save the changes.

WARNING!

Simultaneous use of Analytics, WIFI, TRASSIR Cloud and HTTPS can lead to unstable operation of the following camera models: TR-D2121CL3W, TR-D2121IR3Wv3, TR-D2121IR3Wv3, TR-D3121IR2Wv3, TR-D7121IR1Wv3, TR-D8121IR2Wv3.

3.4.3.4 “PPPoE” menu

Go to the PPPoE section of the Network settings menu to open the menu.



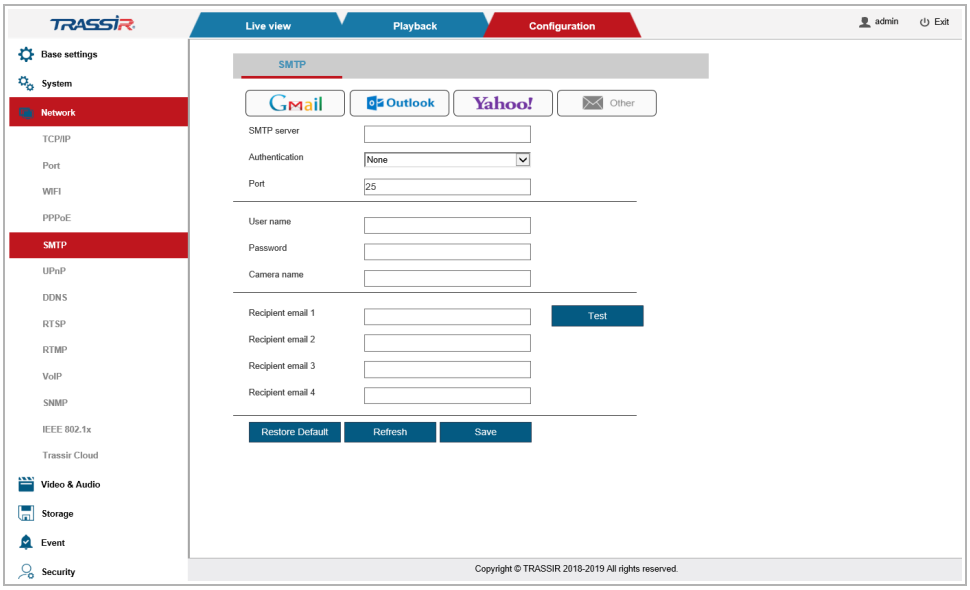
Setting	Description
Enable PPPoE	Set the flag to use PPPoE protocol.
User name	Enter user name.
Password	Enter password.
Connection status	Connection status on PPPoE protocol.
IP address	Device IP address.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.3.5 "SMTP" menu

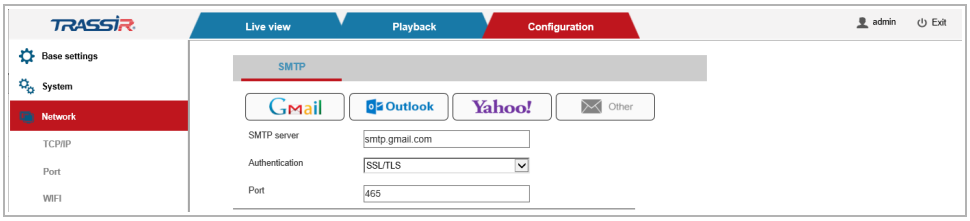
In order to configure sending messages from IP camera by email open SMTP section of the Network settings menu.



Specify SMTP server parameters in SMTP block:

Setting	Description
SMTP server	The name or IP address of the main SMTP server.
Authentication	Secure data transfer protocol: ◆ None; ◆ SSL\TLS; ◆ STARTILS.
Port	Access port number to main SMTP server.
User name	Main SMTP server user name.
Password	Authorization password on main SMTP server.
Sender	Email address rom which the messages will be sent.
Recipient email 1-4	Input up to 4 email addresses to which messages will be sent.

You can also set the default SMTP server, authentication and port by clicking the corresponding buttons at the top of the settings window:



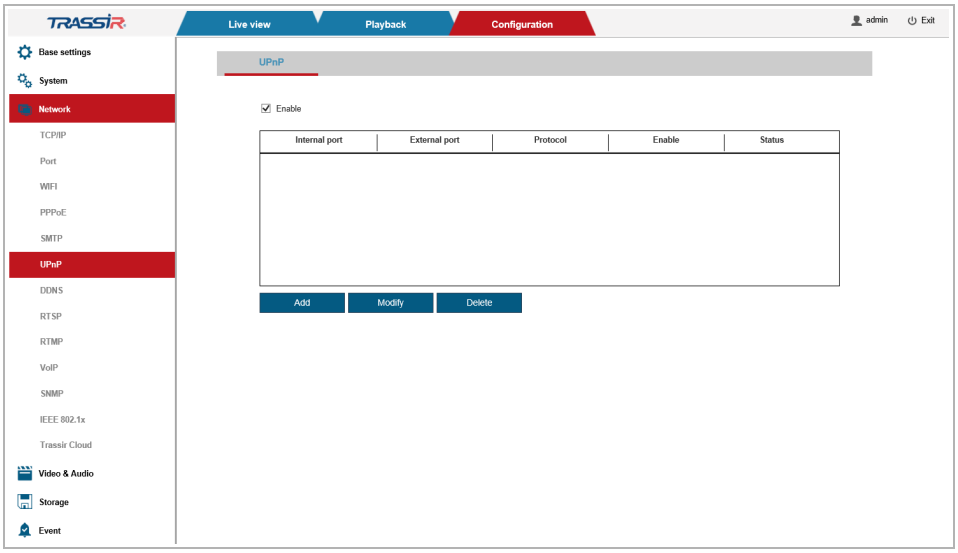
Check the correctness of the configured settings by clicking Test, if necessary. If the settings are correct, the email address, specified in the Recipient email will receive a message. Otherwise an error message will be received.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.3.6 "UpnP" menu

Open UpnP tab to configure automatic camera detection service in local network.



The **Universal Plug&Play(UPnP)** feature is intended to search for an IP camera in local network by intelligent video surveillance systems.

WARNING!

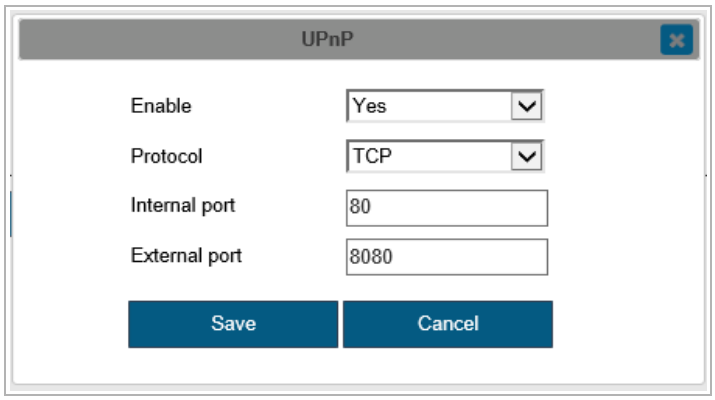
As a rule, UpnP is required for the first IP camera detection in local network. That's why we strongly recommend to disable it after the use in order to prevent unauthorized IP camera access.

This menu also allows configuring IP camera network port forwarding. Network port forwarding is usually used to access and IP camera when it is in another local network.

Press Add to create a new rule.

Press Modify to edit the existing rule.

Press Delete to delete the rule.



Setting	Description
Enable	Use UpnP conversion: Yes / No.
Protocol	Data transfer protocol: TCP / UDP.
Internal Port	Data transfer port, configured on IP camera. Available values range: from 1 to 99999.
External Port	The port on which the IP camera will be accessed from another network. Available values range: from 1 to 99999.

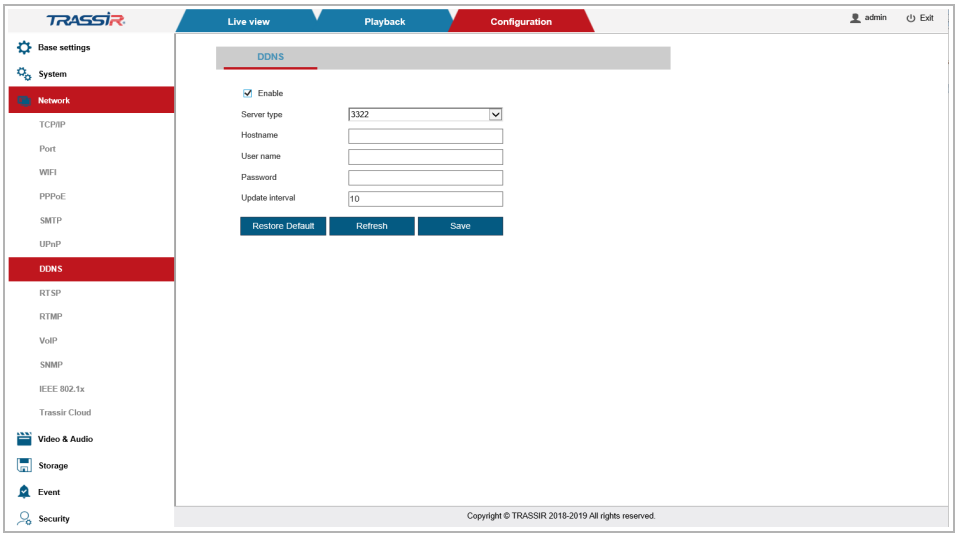
Press Save to save the changes.

3.4.3.7 "DDNS" menu

Go to the DDNS section of the Network settings menu to open the menu.

NOTE.

Prior to the configuration you should register on DDNS service providing web site ang receive all required parameters.



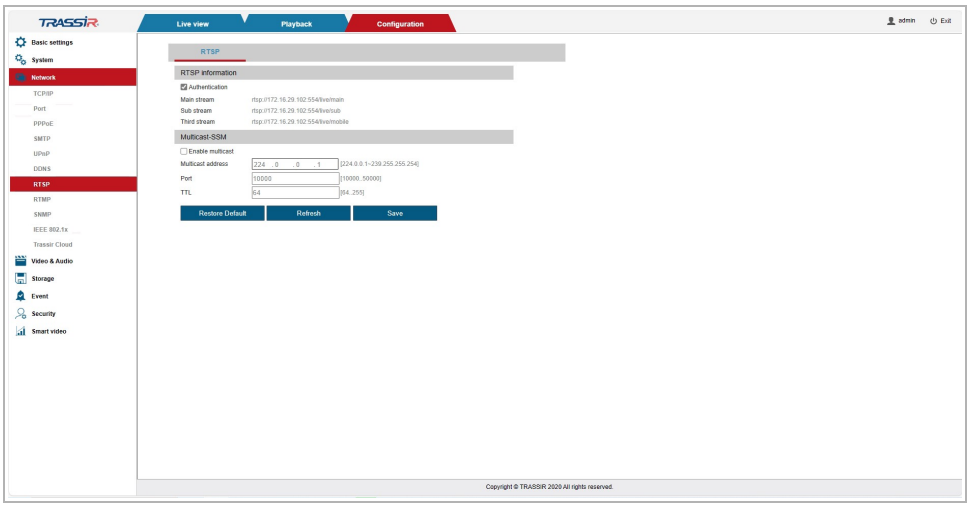
Setting	Description
Enable	Set the flag to use DDNS.
Server type	Select the server type. The following DDNS servers are supported: ◆ 3322; ◆ Oray; ◆ Dyndns; ◆ NO-IP.
Hostname	The IP address of the network device to which the broadcast this IP camera will broadcast.
User name	User name registered on DDNS server.
Password	Password received on DDNS server.
Update interval	Connection update interval, from 0 to 99.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.3.8 "RTSP" menu

In order to configure IP camera streaming open RTSP section of the Network settings menu.



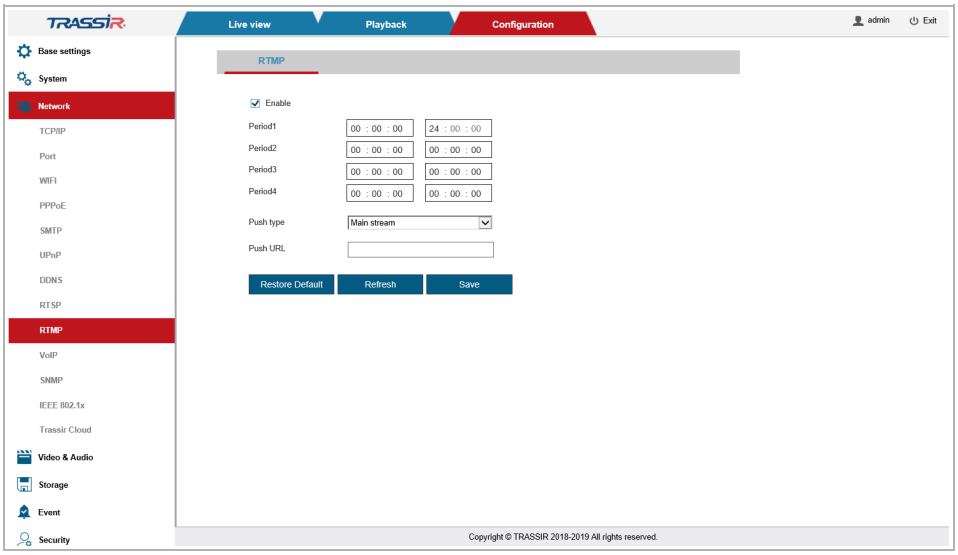
Setting	Description
Authentication	Set the flag to transmit IP camera sound stream on RTSP.
Main stream	Main stream RTSP link.
Sub stream	Sub stream RTSP link.
Third stream	Third stream RTSP link.
Enable Multicast	Set the flag for streaming from an IP camera to a remote network device.
Multicast address	The IP address of the network device to which this IP camera will broadcast
Port	Remote device port.
TTL	TTL value, from 65 to 255.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.3.9 “RTMP” menu

Go to RTMP section of the Network settings menu to open the menu.



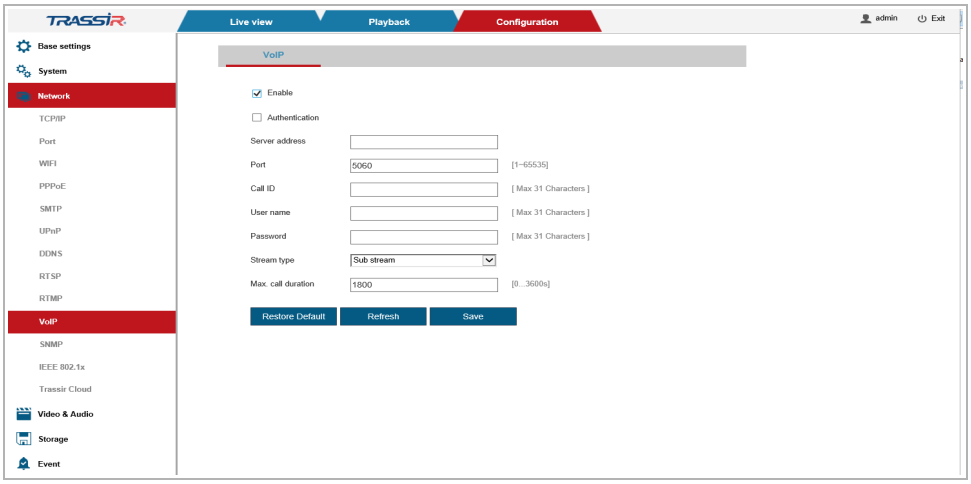
Setting	Description
Enable	Set the flag to use the setting.
Period 1-4	You can schedule the broadcasts and create up to 4 periods.
Push type	Select the stream: Main stream or Sub stream.
Push URL	Stream RTMP address.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.3.10 “VoIP” menu

Open the VoIP section in the Network settings menu.



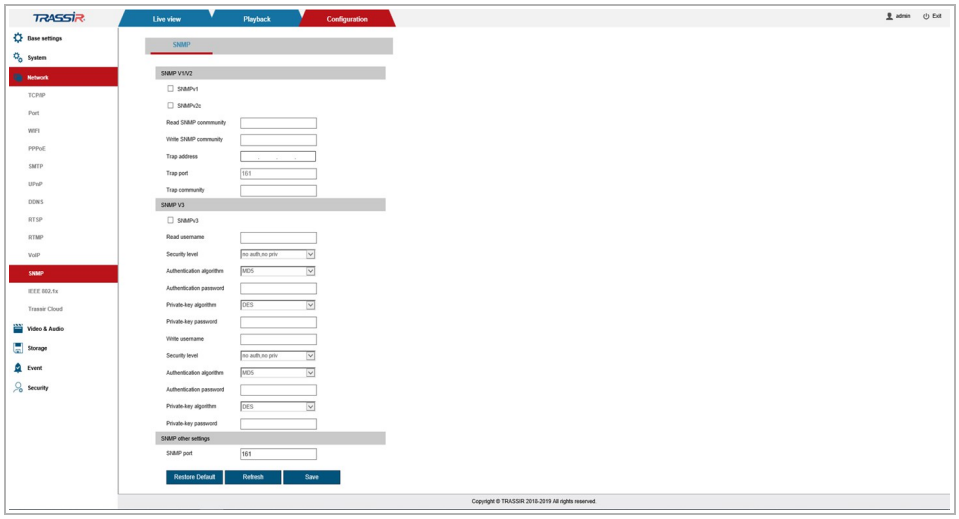
Setting	Description
Enable	Set the flag to use the setting.
Authentication	Set the flag to enable authentication.
Server address	IP address or name of the server.
Port	Server network port.
Call ID	Unique call ID
User name	User name.
Password	Password.
Stream type	Data transfer stream: Main stream or Sub stream.
Max.call duration	Maximal call duration, from 0 to 3600 s.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.3.11 "SNMP" menu

Go to the SNMP section of the Network settings menu.



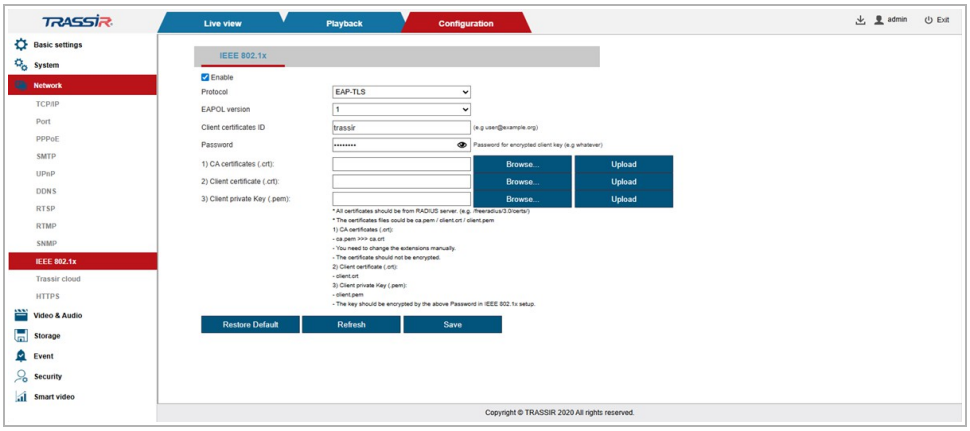
Set the flag of corresponding SNMP version to activate the option (SNMPv1, SNMPv2 or SNMPv3) and configure parameters used by the protocol.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.3.12 “IEEE 802.1x” menu

Go to the IEEE 802.1x section of the Network settings menu to open the menu.



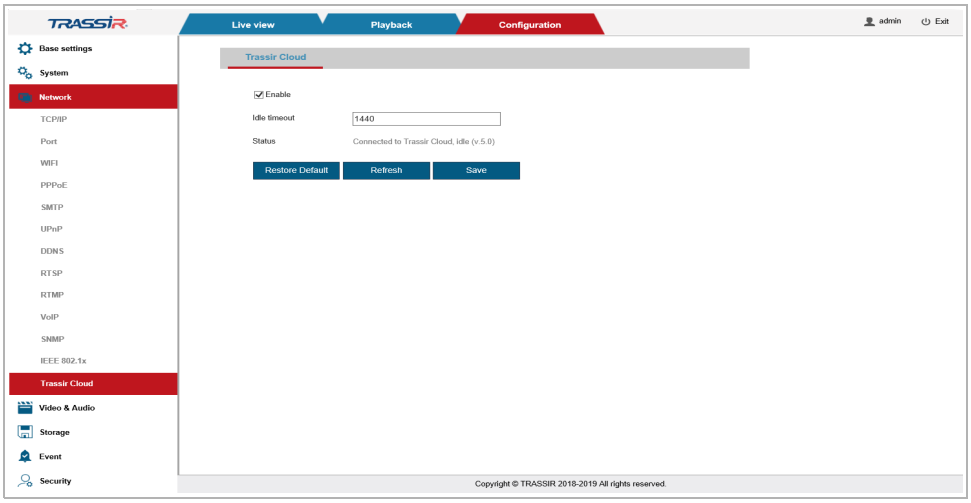
Setting	Description
Enable	Set the flag to activate EEE 802.1x.
Protocol	Data transfer protocol.
EAPOL version	EAPOL protocol version.
User name	User name.
Password	Password.
CA certificate (.crt)	To configure the EAP-TLS protocol, select a CA certificate by clicking the Browse button and add it by clicking the Upload button.
Client certificate (.crt)	To configure the EAP-TLS protocol, select a Client certificate by clicking the Browse button and add it by clicking the Upload button.
Client private key (.pem)	To configure the EAP-TLS protocol, select a Client private key by clicking the Browse button and add it by clicking the Upload button.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.3.13 "Trassir Cloud" menu

Open the Trassir Cloud tab to connect the IP camera to TRASSIR Cloud cloud service.



Setting	Description
Enable	Set the flag to activate the connection service.
Idle Timeout	Set the time period during which the camera available for cloud connection. **Upon the set time period expiration, the service will stop. You need to reboot your IP camera to restart the service.**
Status	Camera cloud service connection status: ◆ Unknown Status — service is not activated. ◆ Connected to Trassir Cloud, idle — TRASSIR Cloud is established, connect your camera in the cloud. ◆ No connection to Trassir Cloud — no connection to TRASSIR Cloud. ◆ Connected to Trassir Cloud, working — camera is connected, the video is being streamed to the cloud. ◆ "Idle Timeout" reached, service stopped — the time period required to connect the camera to the cloud is expired.

Press Restore default to restore the default settings.

Press Save to save the changes.

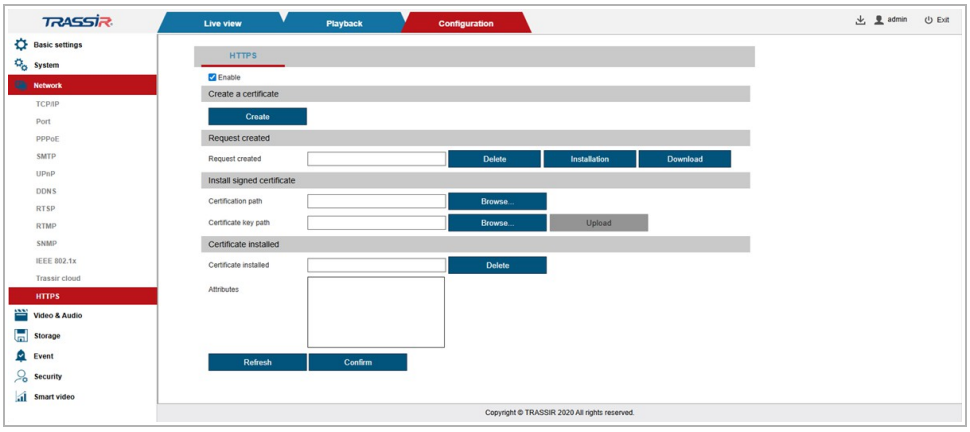
WARNING!

The final step of IP camera connection is performed directly in TRASSIR Cloud.

Simultaneous use of Analytics, WIFI, TRASSIR Cloud and HTTPS can lead to unstable operation of the following camera models: TR-D2121CL3W, TR-D2121IR3Wv3, TR-D2121IR3Wv3, TR-D3121IR2Wv3, TR-D7121IR1Wv3, TR-D8121IR2Wv3.

3.4.3.14 “HTTPS” menu

To configure the secure data transfer, go to the HTTPS section.



Setting	Description
Enable	Check to enable HTTPS.
Create a certificate	Click Create and enter the required information in the window that opens: ◆ Country — two-letter country code, for example RU. ◆ IP/domain name — a required field. ◆ Expiration date — the certificate expiration period in days. ◆ Province — the province name. ◆ Position — geographical location. ◆ Organization — name of the organization. ◆ Organizational Unit — name of the organizational unit. ◆ Mail — Email address. Click Create to create a certificate or Cancel to cancel your action.
Request created	The created request is displayed in the Request created field. Use Delete, Installation and Download buttons to manage it.
Install signed certificate	Click Browse to select the Certification path and Certificate key path, and click Upload.
Certificate installed	The installed certificate is displayed in the Certificate installed field and its information in the Attributes field. To delete the certificate, click Delete.

WARNING!

Simultaneous use of Analytics, WIFI, TRASSIR Cloud and HTTPS can lead to unstable operation of the following camera models: TR-D2121CL3W, TR-D2121IR3Wv3, TR-D2121IR3Wv3, TR-D3121IR2Wv3, TR-D7121IR1Wv3, TR-D8121IR2Wv3.

3.4.4 "Video & Audio" menu

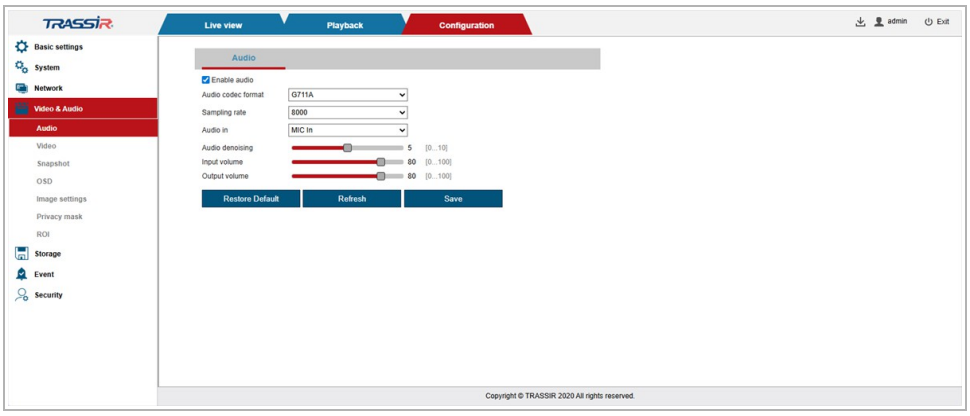
Press Video & Audio to open the menu.

The menu consists of the sections which allow to:

- Audio —configure audio stream (see section 3.4.4.1);
- Video Stream —configure video stream (see section 3.4.4.2);
- Snapshot - configure snapshot saving (see section 3.4.4.3);
- OSD - configure OSD menu display on video (see section 3.4.4.4);
- Image Settings —configure transmitted image parameters (see section 3.4.4.5);
- Privacy Mask —set up mask zones (see section 3.4.4.5.2);
- ROI —set up zones of interest (see section 3.4.4.7).

3.4.4.1 "Audio" menu

Go to the Audio section to set up IP camera audio stream.



Setting	Description
Enable audio	Set the flag to use the setting.
Audio Codec Format	Audio stream compression algorithm: G.711A, G.711U, AAC, G.726 or PCM.
Sampling rate	Audio sampling, 8000, 16000 or 24000.
Audio In	IP camera sound stream audio input: Line-in or MIC In. **Set up depending on the camera model.**
Audio denoising	Noise canceling level, from 0 to 10.
Input volume	Input audio volume level, from 0 to 100.
Output volume	Output audio volume level, from 0 to 100.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.4.2 "Video" menu

The menu consists of the additional tabs which allow you to:

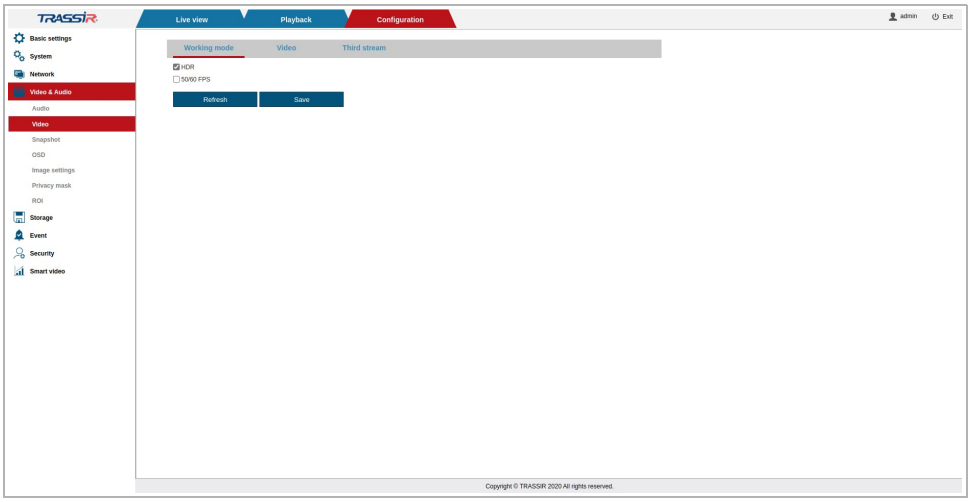
- Working mode —enable HDR (see section 3.4.4.2.1);
- Video —configure video stream (see section 3.4.4.2.2);
- Third stream —configure third (see section 3.4.4.2.3).

3.4.4.2.1 "Working mode" tab

Got to the Working mode tab in the Video settings menu.

NOTE.

Prior to the configuration activate WDR in the Image settings menu(see section 3.4.4.5.1).



Check **HDR** to enable RealWDR in the image settings.

Check **Clear HDR** to enable RealWDR in the image settings and reduce movement blurring in the frame (the RealWDR effect will be weaker).

Check **50/60 FPS** to enable the ability to increase the frame rate of streams to 50/60 fps (depending on the video standard value set in the image settings).

WARNING.

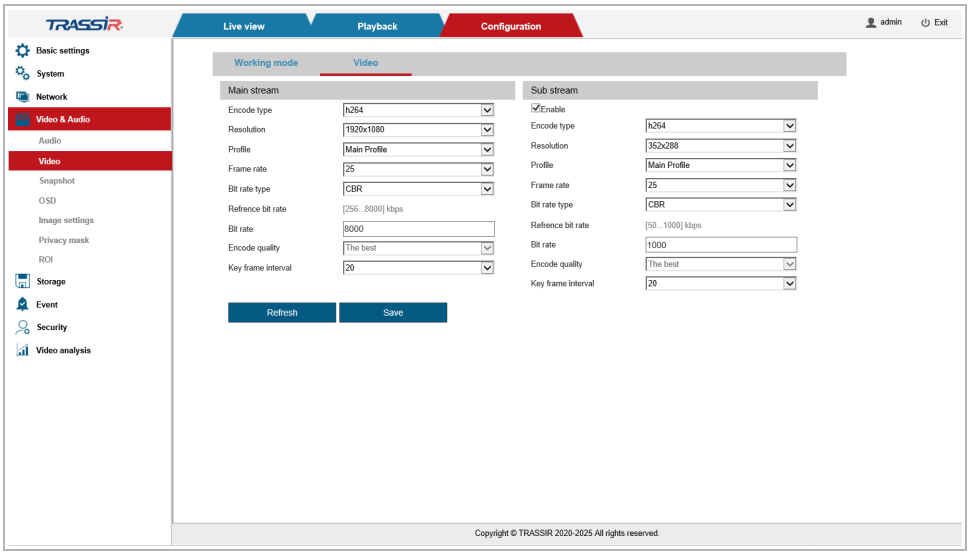
RealWDR and 50/60 fps can't be activated at the same time.

Press Save to save the changes.

3.4.4.2.2 "Video" tab

Go to the Video tab in the Video settings menu to set up IP camera video stream.

Set the Enable flag in the Sub stream block in order to activate sub stream settings.



You can configure the following parameters for each stream:

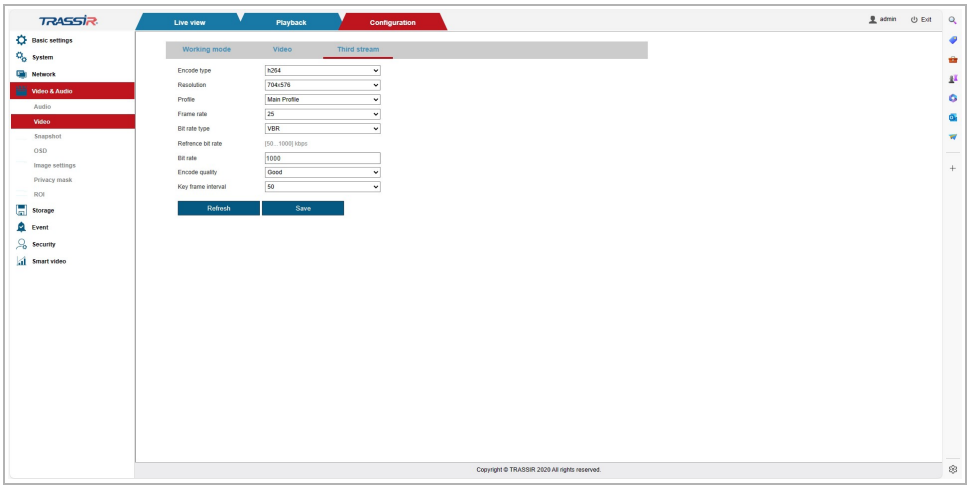
Setting	Description
Encode type	Video stream compression standard: H264 or H265.
Resolution	Video stream resolution. Main stream: 1280x720, 1280x960, 1920x1080. Sub stream: 352x288, 640x360, 640x480 or 704x576. Third stream: 352x288, 640x360, 640x480 or 704x576. **Available resolutions may vary depending on camera model.**
Profile	Select a video compression profile: Baseline, Main Profile, High Profile. Profiles allow to increase the compression efficiency of a video stream in different conditions. The higher the profile value is, the higher is the clarity of video transmission.
Frame rate	The interval at which frames containing one key frame will be grouped. The lower the value is, the more often the keyframe will follow.
Bitrate type	Video stream compression type: VBR / CBR.
Reference bit rate	If CBR is selected, the setting value is used as the maximum value of the compression rate of the video stream. Main stream: from 256 kbit/s to 8000 kbit/s. Sub streams: from 50 kbit/s to 1000 kbit/s.
Bit rate	Video stream compression rate value..
Encode Quality	If VBR is selected the setting value will define the transmitted image quality: from 1 to 6. The higher the value is, the higher is the image quality.

Setting	Description
Key frame interval	Video capturing speed, the number of frames per second, captured by IP camera. The value is selected ranging from 5 fps to 100 fps, depending on selected resolution. **Maximum parameter value may vary depending on camera model.**
Enable audio	Set the flag to switch the sound on main or sub stream.

Press Save to save the changes.

3.4.4.2.3 "Third stream" tab

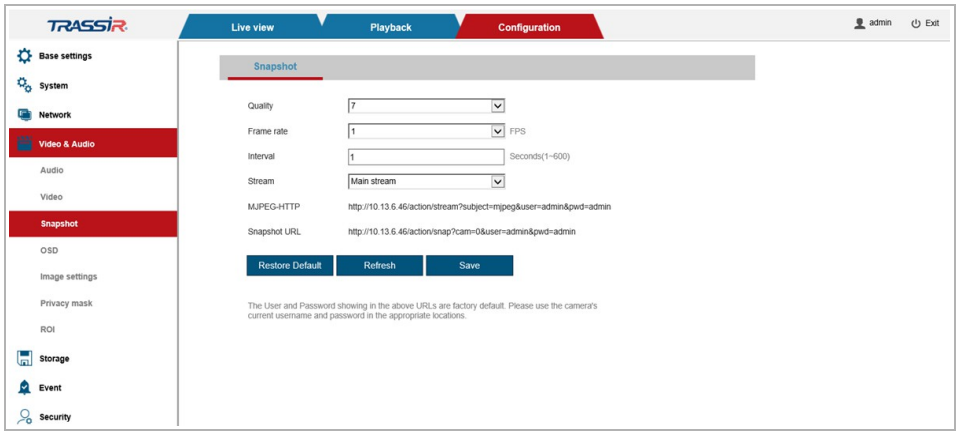
Open the Third Stream tab in order to set up the camera third stream.



The third stream is configured the same way as video stream (see section 3.4.4.2.2).

3.4.4.3 "Snapshot" menu

Go to the Snapshot section of Video & Audio settings menu to open the menu.



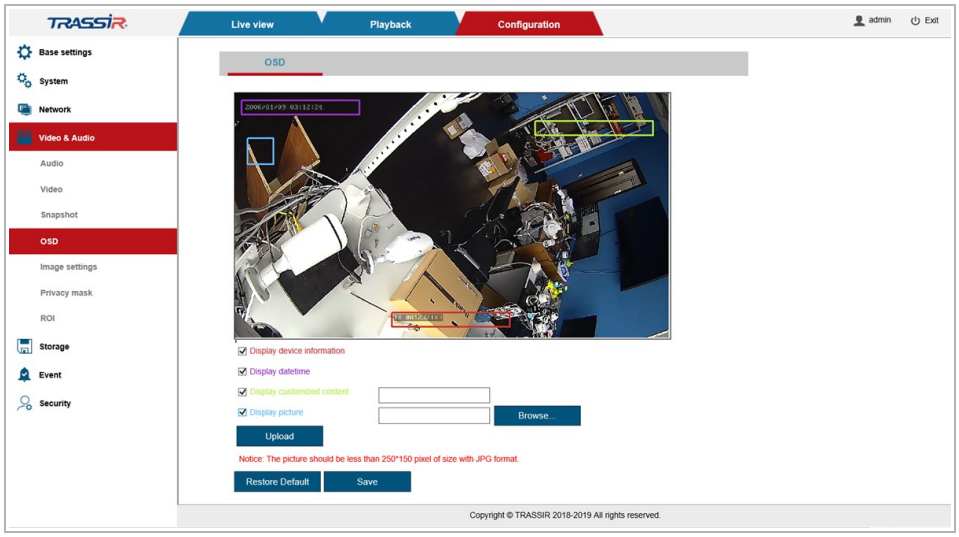
Setting	Description
Quality	The image quality: from 1 to 7. The higher the value is, the better is the image quality.
Frame rate	Video capture rate, the number of frames per second captured by the IP camera. Select values ranging from 1 fps to 5 fps depending on the selected resolution.
Snapshot interval	The interval between saved snapshots, from 1 to 600 s.
Snapshot type	Select snapshot stream: Main stream or Sub stream.
MJPEG-HTTP	RTSP video URL.
Snapshot URL	RTSP snapshot UT|RL.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.4.4 OSD menu

Go to OSD section of Video & Audio menu to open the menu.



Setting	Description
Display device information	Set the flag to display system information.
Display Datetime	Set the flag to display date and time.
Display Customized Content	Set the flag to display your text on video. Enter your text into the adjacent field.
Display picture	Set the flag to display your watermark on video. Press Browse to locate the watermark image and then press Upload.

Press Restore default to restore the default settings.

Press Save to save the changes.

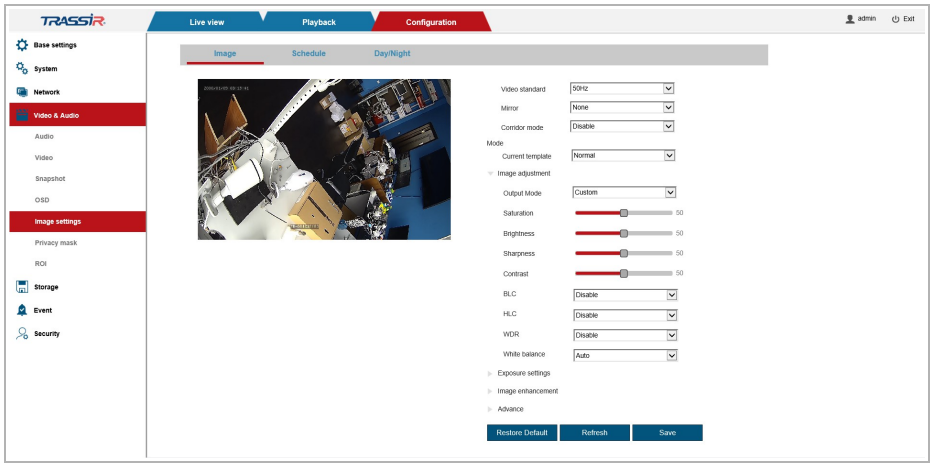
3.4.4.5 "Image settings" menu

The menu consists of the additional tabs which allow to:

- Image —configure basic image parameters (see section 3.4.4.5.1);
- Schedule —configure settings modes (see section 3.4.4.5.2);
- Day/Night —configure transition to night settings mode (see section 3.4.4.5.3).

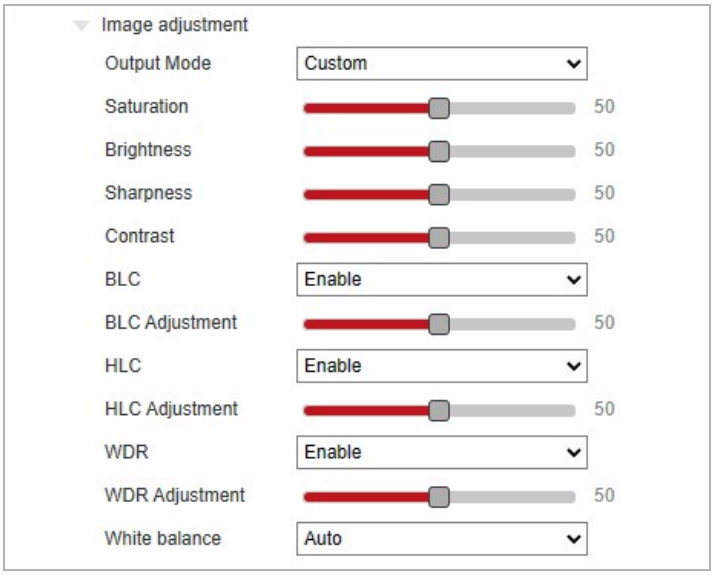
3.4.4.5.1 "Image" tab

In order to set up image transmitted by IP camera, open the Image tab in the Image settings menu.



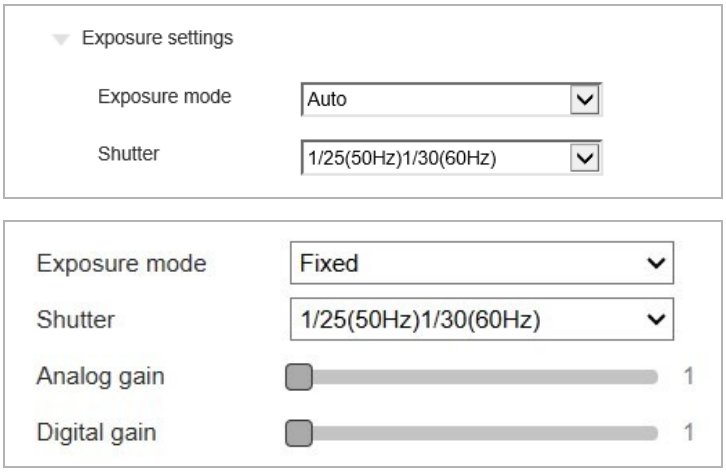
Setting	Description
Video Standard	The electricity network frequency (50Hz or 60Hz) to which the IP camera is connected.
Mirror	Image mirroring: ◆ None - disabled. ◆ Vertical —vertical axis; ◆ Horizontal —horizontal axis; ◆ Horizontal&Vertical —horizontal and vertical axes.
Corridor mode	Enable/disable corridor mode. It rotates image to 90 degrees, changing standard horizontal orientation to vertical. **Corridor mode is not compatible with Video analysis module (see section 3.4.8).**
Current template	Select template to save current settings: ◆ Normal; ◆ Day; ◆ Night. **Other settings will be applied to the selected template.**

- Image adjustment block



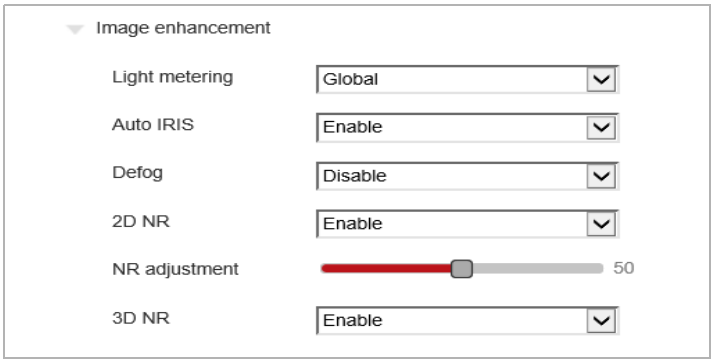
Setting	Description
Output mode	Select the coloring mode: ◆ Standard; ◆ Bright; ◆ Vivid; ◆ Gentle; ◆ Custom. Saturation, brightness, sharpness and contrast settings will be applied automatically, in accordance with the selected mode. Settings are customized manually if you select the Custom mode.
BLC	Enable/disable backlight compensation option on video. An adjustment slider appears when this option is enabled.
HLC	Enable/disable highlight compensation option on video. An adjustment slider appears when this option is enabled.
WDR	Enable/disable wide dynamic range option. An adjustment slider appears when this option is enabled. This option is effective when shooting in difficult lighting conditions when it is necessary to distinguish an object from a light source (for example, a person's face against a background of a window illuminated by sunlight).
White Balance	Customize white balance in accordance with shooting area lighting conditions: ◆ Auto — automatic selection of white balance, while the camera itself chooses a setting at which the best video stream quality will be transmitted; ◆ Out door — automatic white balance selection adapted for outdoor shooting; ◆ Indoor — automatic white balance selection adapted for outdoor shooting; ◆ Fluorescent lamp — automatic selection of white balance adapted for shooting objects lit by a fluorescent lamp; ◆ Manual — manual white balance selection.

- Exposure settings block



Setting	Description
Exposure mode	Select exposure mode: Auto/Fixed.
Shutter	Select IP camera maximum shutter value.
Analog gain	Use the slider to set the gain value for the signal from the matrix before its digitization. (only in Fixed mode)
Digital gain	Use the slider to set the gain value for the digitized signal. (only in Fixed mode)

- Image enhancement block



Setting	Description
Light metering	Exposure determination type on IP camera: Global or Middle.
Auto IRIS	Enable/disable automatic iris control.
Defog	Enable/disable antifog feature which prevents, which prevents blurring in bad weather conditions.
2D NR	Enable/disable 2D NR to reduce noise.
NR adjustment	Eliminate image noise. The higher the value is, the cleaner is the image.
3D NR	Enable/disable 3D NR to reduce image noise.

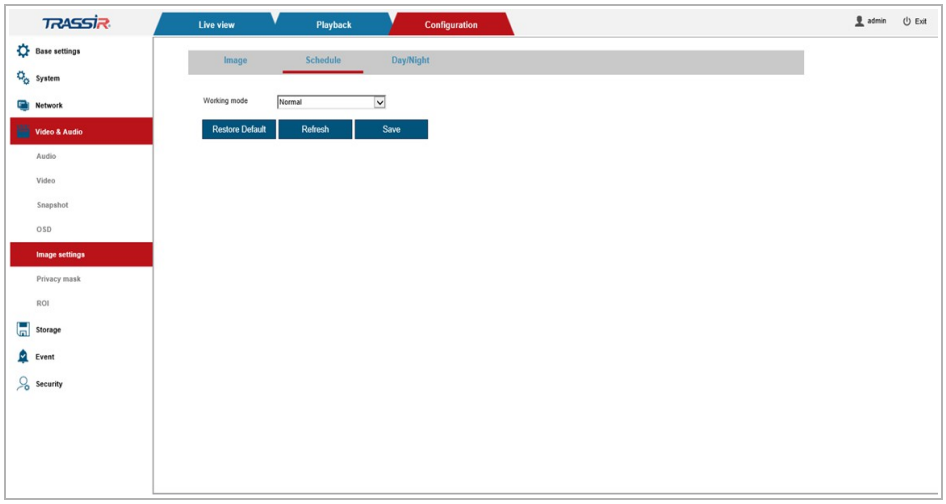
You can see the changes of the applied settings in the preview window.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.4.5.2 "Schedule" tab

To select the image modes open the Schedule tab in the Image settings menu.



Select the settings mode that will be applied to the image from the dropdown list in Working mode field:

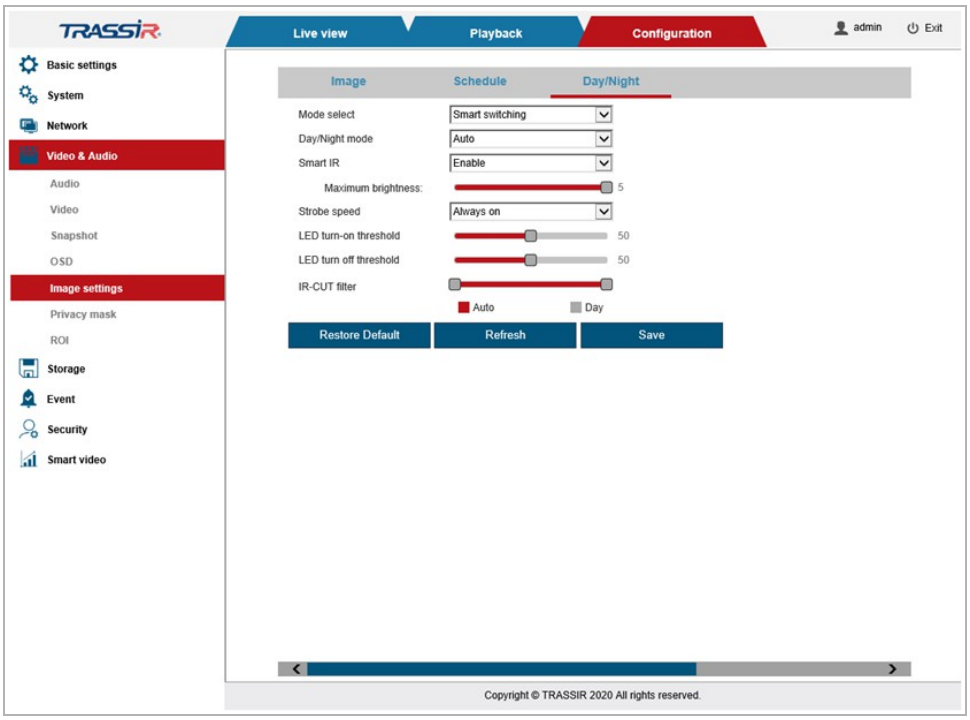
- Normal — activate standard settings mode;
- Day — activate day mode;
- Night — activate night mode;
- Timing — the day mode will be activated on schedule;
- Auto — day and night modes will replace each other according to the time of day.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.4.5.3 "Day/Night" tab

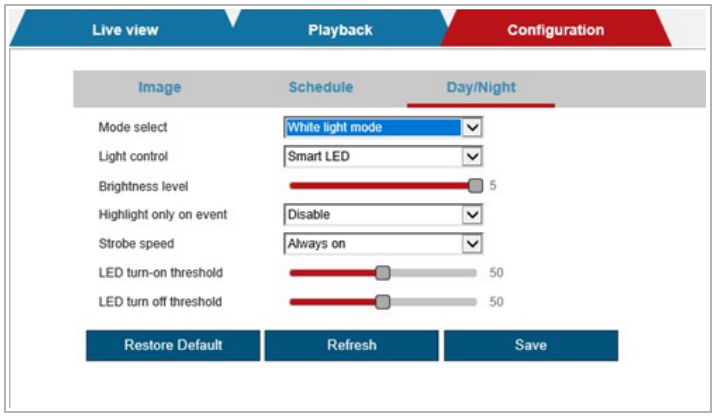
In order to set day and night mode switching, as well as turning on and adjusting the IR illumination, go to the Schedule tab in the Image settings menu.



Setting	Description
Mode select	Select the illumination operation mode: ◆ Smart switching: The IR illumination is switched on when there is insufficient light. When a person appears in the frame, it automatically changes to LED illumination. When a person leaves the frame, the LED illumination changes back to IR illumination. ◆ Infrared light mode: IR illumination. ◆ White light mode: LED illumination. ◆ Turn off the lights: The illumination is off.
Day/Night mode	Select day/night operation mode: ◆ Auto: automatic activation of B/W mode, depending on the level of illumination of the shooting area; ◆ Day: B/W mode is off / Day; ◆ Night: B/W mode is on / Night; ◆ By time: activation of the color mode on schedule Set the time period during which the color mode will be activated in the Period setting opened field; ◆ Auto(Inter sync): automatic activation of B / W mode, depending on the level of illumination of the shooting area. Set the illumination values at which color and black and white mode will switch in the THR. of day and THR. of night opened fields.
Light control	Select the operating mode of the IR illumination with the selected day and night change mode: Smart LED, Enable, Disable or LED by time.

Setting	Description
Smart IR	Enable/Disable the Smart IR function, which allows you to adjust the intensity of the camera LEDs to compensate for the distance to the object. When the function is enabled - the [Brightness level] adjustment changes to the [Maximum brightness] adjustment.
IR brightness	Use the slider to adjust the IR brightness.
LED turn on threshold	Use the slider to adjust the LED turning on threshold.
LED turn off threshold	Use the slider to adjust the LED turning off threshold.
IR-CUT Filter	Use the slider to set up the IR filter activation time.

The cameras with LED backlighting do not have infrared sensors and use LEDs when working in low-light conditions or in the dark. The LEDs can also be used to highlight alarm events.



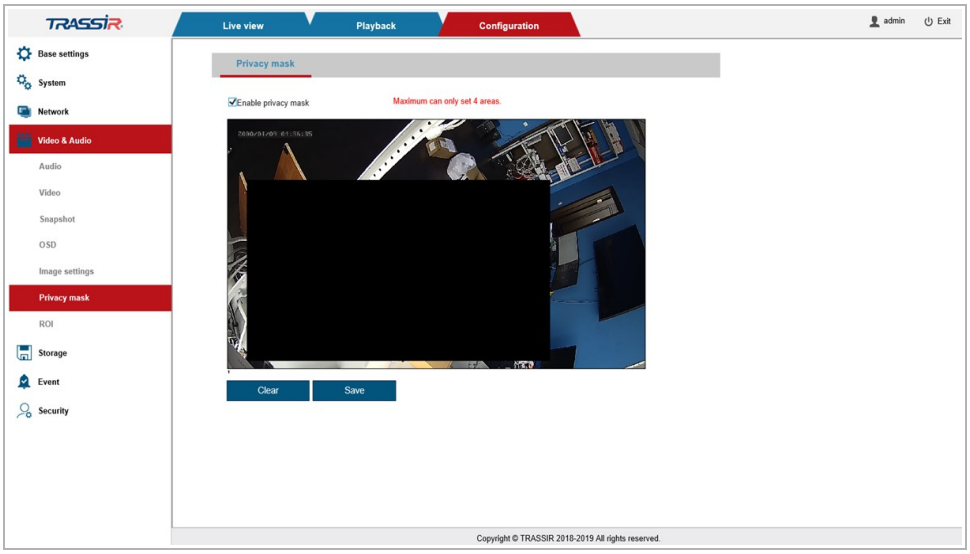
Setting	Description
Light Control	**Available only for cameras featuring LED lighting.** Select LED lighting mode: ◆ Smart LED: automatic control of lighting intensity depending on the distance to the object. ◆ Enable: LED lighting is on; ◆ Disable: LED lighting is off; ◆ LED by time: LED lighting turns on and off depending on the period selected by the sliders.
Brightness level	Manual LED illumination brightness adjustment.
Highlight only on event	Turn the illumination on/off when an alarm event is detected.
Strobe speed	Choose the frequency at which the strobe will operate.
LED turn-on threshold	Select the lighting level at which the LED will automatically turn on.
LED turn off threshold	Select the lighting level at which the LED will automatically turn off.

Press Restore Default to restore the default settings.

Press Save to save the changes.

3.4.4.6 “Privacy mask” menu

Open Privacy Mask section to set up masking zones on you IP camera.



Select an area on video that you want to hide, and use the left mouse button to draw a masking zone. Ue masking zones to hide some areas on video, for example, the dial pad of the combination lock.

NOTE.

You can customize up to 4 masking zones.

WARNING!

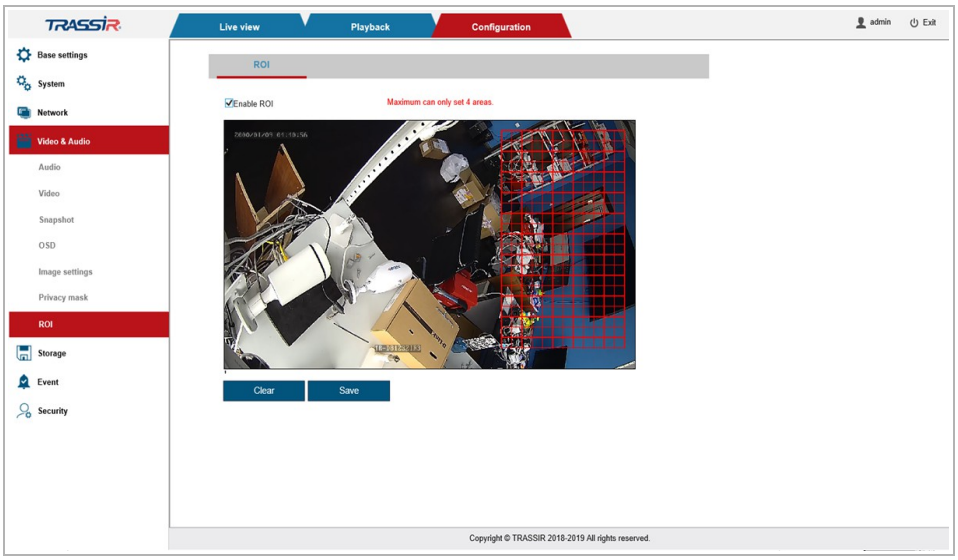
Masking zones are superimposed on the transmitted video stream, that is, they are recorded in the archive and superimposed on the image snapshots. The image hidden under such zones will be impossible to view even after disabling masking zones.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.4.7 "ROI" menu

Open ROI section in order to customize zones of interest.



ROI zones or zones of interest allow you to highlight areas of the image that will be recorded with improved image quality settings. In this case, the areas outside the zones will be saved with poorer image quality parameters.

NOTE.

You can create up to 4 zones of interest.

To define the zones, left click on image and select one or several zones of interest.

Press Clear to reset the settings.

Press Save to save the changes.

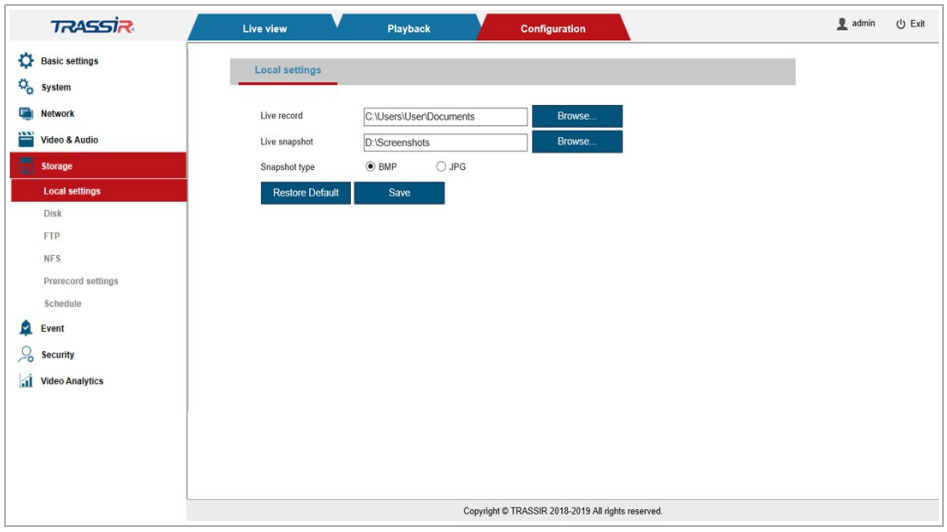
3.4.5 "Storage" menu

The menu consists of the sections which allow to:

- Local settings —set up local archive recording (see section 3.4.5.1);
- Disk —check the archive state and configure archive recording to disk (see section 3.4.5.2);
- FTP —set up archive recording to FTP server (see section 3.4.5.3);
- NFS —set up archive recording to NFS server (see section 3.4.5.4);
- Prerecord settings —configure a time period before the event detection to record (see section 3.4.5.5);
- Schedule —schedule data recording to the archive (see section 3.4.5.6).

3.4.5.1 "Local settings" menu

Go to the Local settings section of the Storage menu to open.



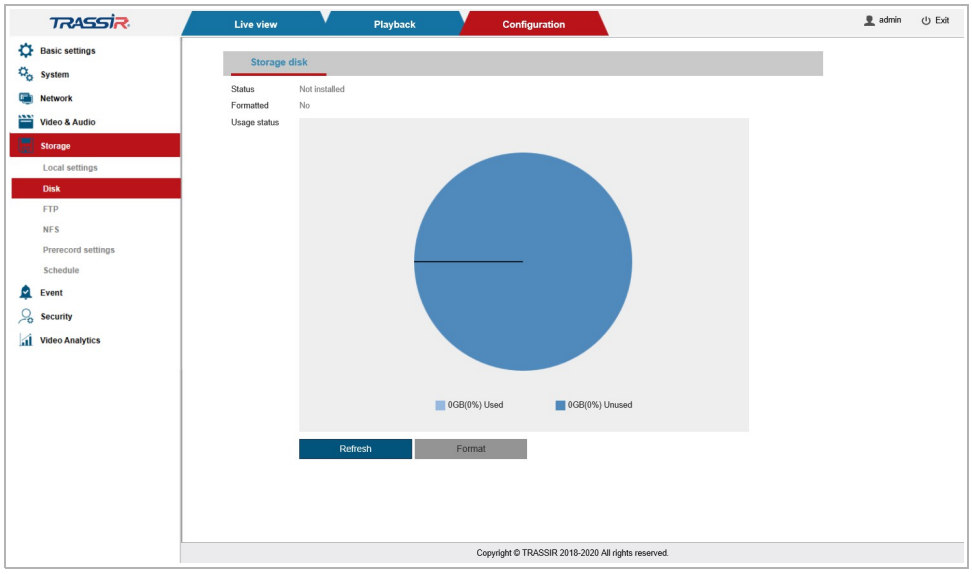
Click Browse...to set video and snapshot saving path.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.5.2 “Disk” menu

Open the Storage disk tab in the Disk settings menu.



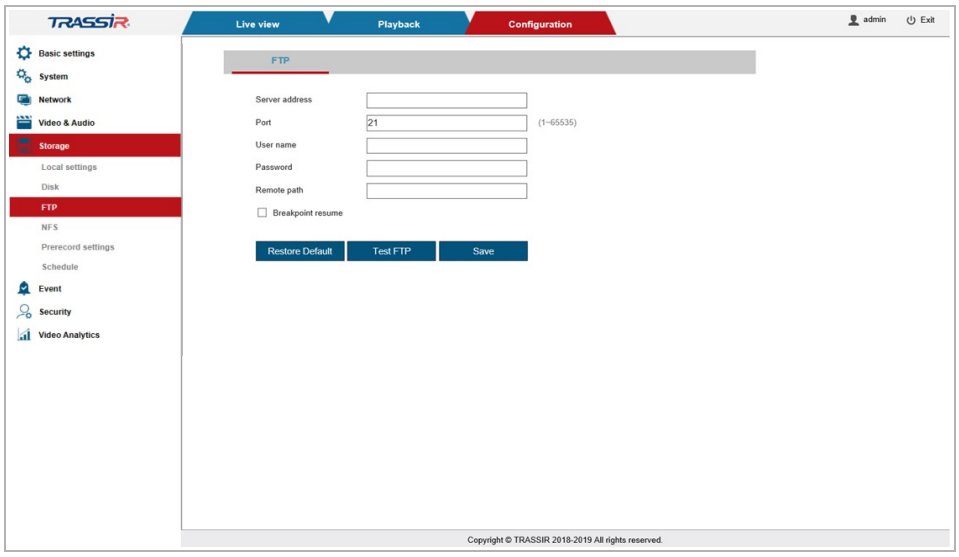
This menu lets you check status of the built-in archive and the amount of free space on it, as well as format the built-in archive to use IP camera.

NOTE.

Format built-in storage upon the first connection of memory card or USBHDD by pressing Format.

3.4.5.3 "FTP" menu

Go the FTP section of the Storage settings menu to open the menu.



Setting	Description
Server Address	Name or IP address of FTP server.
Server Port	FTP server access port number.
Username	User name to authorize on FTP server.
Password	Password to authorize on FTP server
Remote Path	The directory where messages from the camera will be saved. The default one is: FTP server root directory.
Breakpoint Resume	Set the flag to resume uploading the file to FTP server in case of disconnection.

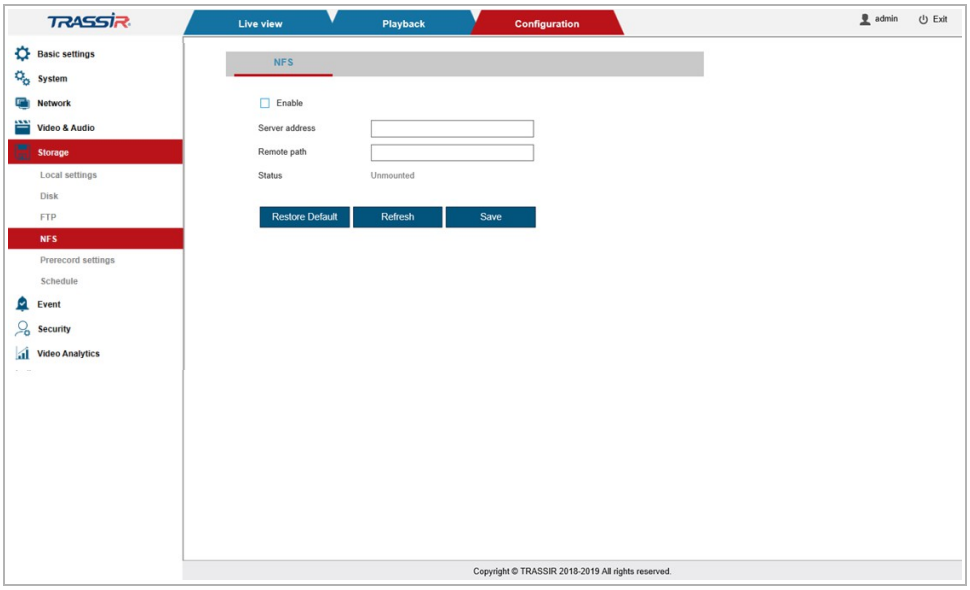
Upon configuration completion click Test FTP to establish test connection.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.5.4 "NFS" menu

Go to the NFS section of the Storage settings menu to open the menu.



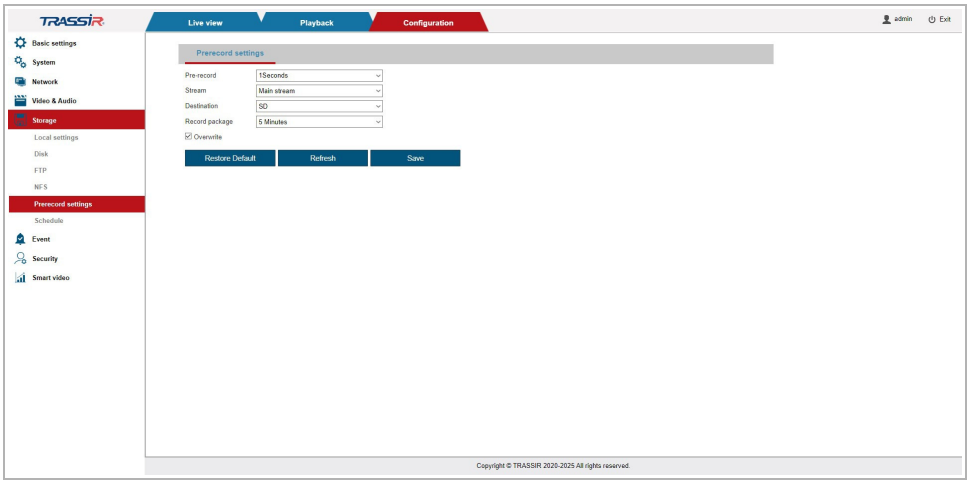
Setting	Description
Enable	Set the flag to activate the setting.
Server address	Remote server address.
Remote path	Archive saving path.
Status	Server connection status.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.5.5 "Prerecord settings" menu

This menu allows you to configure the time period before the event detection that will be recorded to the archive.



Setting	Description
Pre-record	The time period from 0 to 3 s before the event triggering during which the video will be triggering.
Stream	Select stream to record to the archive:Main stream or Sub stream.
Destination	Specify the archive saving path: SD or NFS.
Overwrite	Set the flag to overwrite the built-in storage in case of overflow. In this case, older files will be overwritten with new ones.
Record package	Maximal size of the recorded file: 3min, 5min or 10min.

Press Save to save the changes.

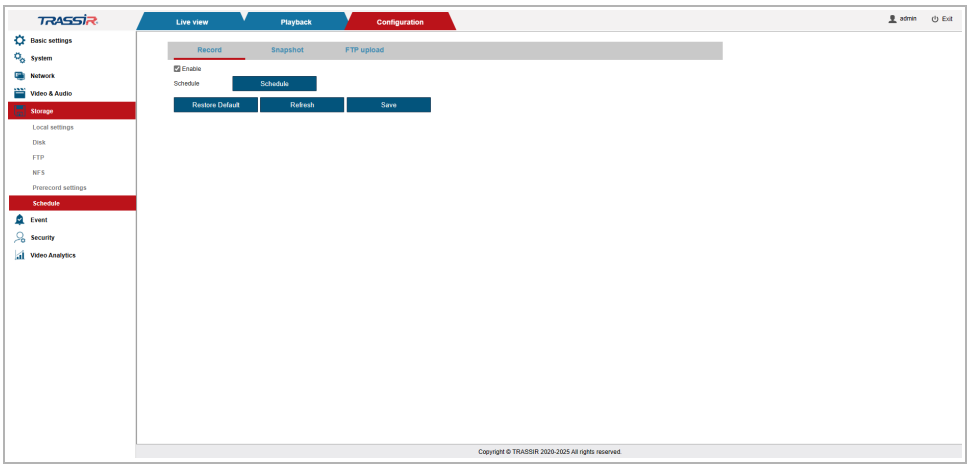
3.4.5.6 "Schedule" menu

The menu consists of the additional tabs which allow to:

- Record —configure video record to the archive (see section 3.4.5.6.1);
- Snapshot —configure snapshot saving (see section 3.4.5.6.2);
- FTP upload —configure archive uploading to FTP (see section 3.4.5.6.3).

3.4.5.6.1 "Record" tab

In order to schedule data recording to the archive open the Record tab in the Schedule settings menu.

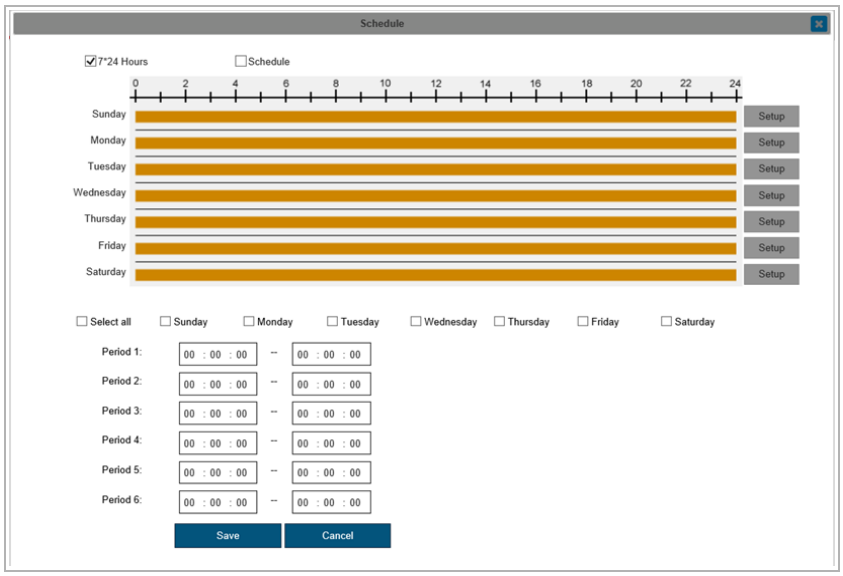


Set the Enable flag to activate the setting.

Click the Schedule button to set the schedule for recording video to the archive.

In the opened window select how the recording will be carried out by putting flags in the corresponding fields:

- 7*24 Hours — there will be permanent record to the archive;
- Schedule —recordings will be carried out on the selected dates and time periods.



In order to set the time intervals, click Setup opposite to the desired day of the week and set up to six time intervals, indicating the start and end times.

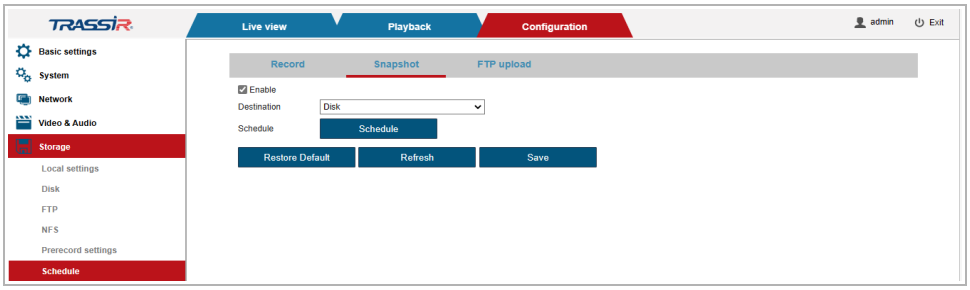
Set the flags in front of the required days of the week or set the Select all flag in order to copy aettings to the other days.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.5.6.2 "Snapshot" tab

Go to the Snapshot tab in the Schedule settings menu to open the menu.



Set the Enable flag to activate the setting.

Set snapshot saving path in the Destination field:

- SD — save to SD card;
- NFS — save to NFS server.

The snapshot saving schedule is configured the same way as on the Record tab (see section 3.4.5.6.1).

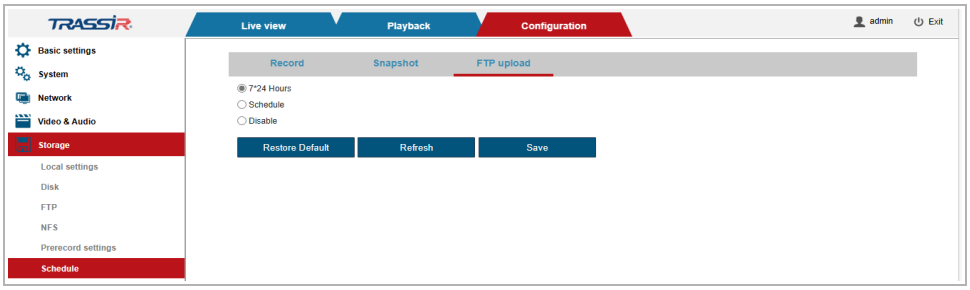
NOTE.

If the Snapshot flag is set in the event settings(see section 3.4.6) the snaphot will be saved regardless of the schedule settings.

You can set up the interval between the saved snapshots in the Snapshot section(see 3.4.4.3).

3.4.5.6.3 "FTP Upload" tab

Open FTP Upload in the Schedule settings menu to set up archive upload to FTP.



Configure FTP upload settings:

- 7*24 Hours —upload will be performed permanently;
- Schedule — upload will be performed on schedule;
- Disable — FTP upload will not be performed.

NOTE.

The snapshot FTP upload schedule is configured the same way as on the Record and Snapshot tabs (see sections 3.4.5.6.1 and 3.4.5.6.2).

NOTE.

If the FTP upload flag is set in the event settings (see section 3.4.6) the upload will be performed regardless of the schedule settings.

3.4.6 "Event" menu

Open the Event menu.

The menu consists of the following sections which allow to:

- Motion Detection —set up motion detector (see section 3.4.6.1);
- I/O alarm —set up alarm inputs/outputs (see section 3.4.6.2);
- PIR —configure PIR (see section 3.4.6.3);
- Abnormality — set up reactions in case of the camera malfunctions (see section 3.4.6.4).

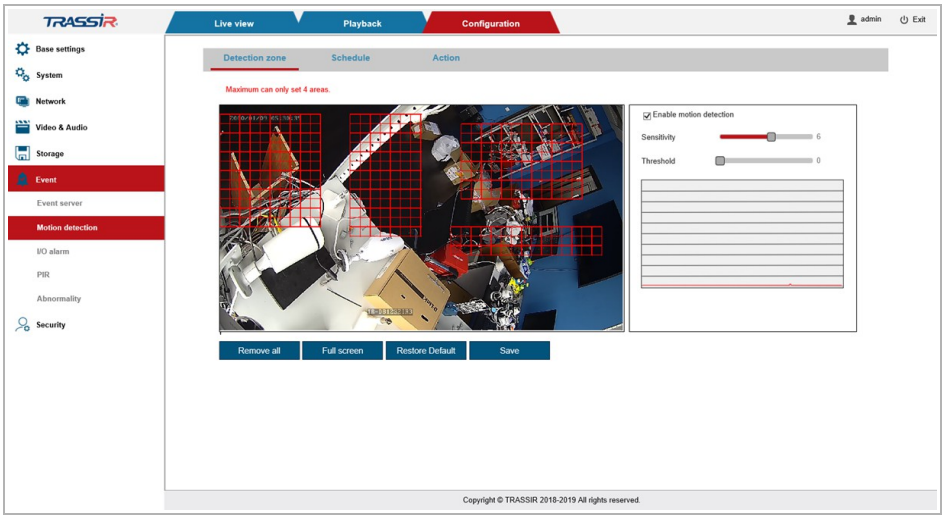
3.4.6.1 "Motion detector" menu

The menu consists of the following sections which allow to:

- Detection zone — set up motion detector zones (see section 3.4.6.1.1);
- Schedule —set up motion detector schedule (see section 3.4.6.1.2);
- Action —set up reactions for motion detector triggering (see section 3.4.6.1.3).

3.4.6.1.1 "Detection zone" tab

In order to set up shooting areas in which the reaction will trigger upon motion detection, got to the Detection zone in the Motion Detection settings menu.



NOTE.

You can create up to 4 detection zones.

In order to define the motion detector zones, left click on the image and highlight the zones in which motion detection is required.

Use Sensitivity parameter to customize motion detector sensitivity in all created zones. The higher the value is, the more sensitive is the detector.

Set the detector confidence level from 0 to 100 in the Threshold parameter. The higher the value is, the lower is the probability of false triggerings, especially when working outdoors.

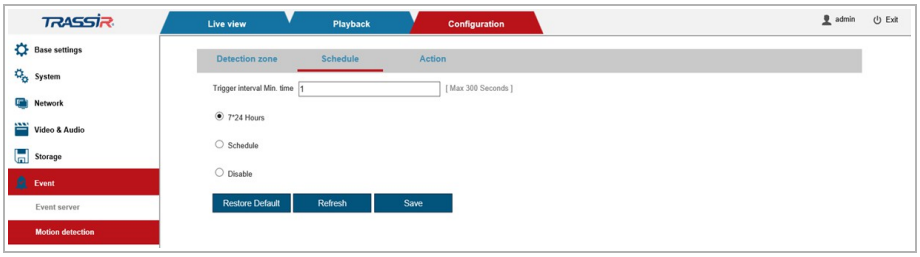
Press Full screen, to select the entire shooting area as the detection zone.

Press Remove all to remove all created zones.

Press Save to save the changes.

3.4.6.1.2 "Schedule" tab

Go to the Schedule tab to open the menu.



Specify time which will define the event occurrence from 0 to 300 s in the Trigger Interval Min. time field. If an alarm event lasts less than the specified time, it is considered not to have occurred.

In the lower block select schedule for recording to the built-in storage (see section3.4.5.1):

- 7*24 hours Record —the record will be performed permanently;
- Schedule Record —the video stream will be recorded on schedule;
- Disable —disable option.

NOTE.

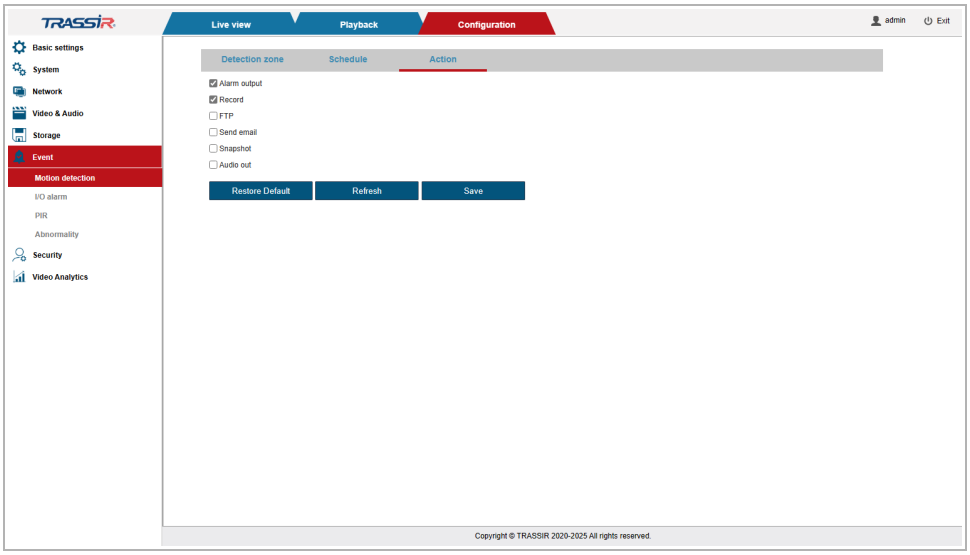
If the Record flag is set in the event settings (see section 3.4.6) the record will be performed regardless of the schedule settings.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.6.1.3 "Action" tab

In order to set up reaction on motion detector triggering go to the Action tab in Motion detection settings menu.



Select one or several actions that the IP camera will perform upon motion detection:

- Alarm output —close alarm output.(see section. 3.4.6.2).
- Record —record video to the archive. See description of the schedule settings in 3.4.6.1.2.
- FTP — upload video file or image to FTP server. See description of FTP server settings in 3.4.5.3.
- To send email. Email settings are described in 3.4.3.5.
- Snapshot —save snapshot to the archive (see section 3.4.4.3).
- Audio. Audio settings are described in 3.4.4.1.

Press Restore default to restore the default settings.

Press Save to save the changes.

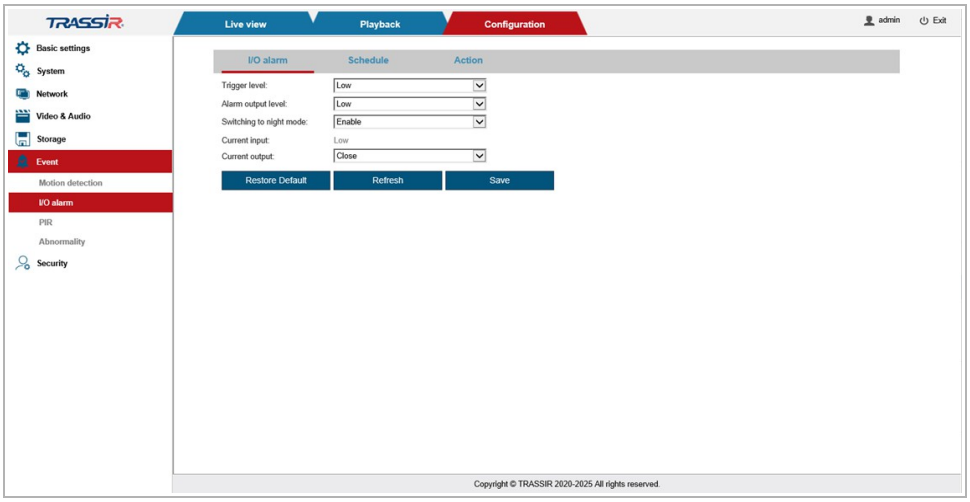
3.4.6.2 "I/O Alarm" menu

The menu consists of the additional tabs which allow to:

- I/O Alarm —configure alarm inputs and outputs (see section 3.4.6.2.1);
- Schedule —set up schedule of alarm inputs and outputs operation (see section 3.4.6.2.2);
- Action —set up reactions to the alarm input and output triggering (see section 3.4.6.2.3).

3.4.6.2.1 "I/O Alarm" tab

Go to the I/O Alarm tab to open the menu.



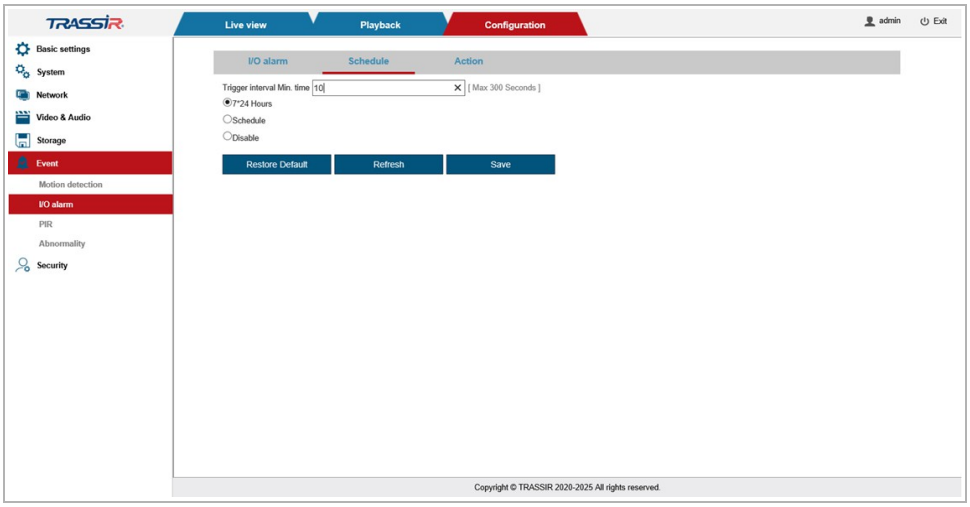
Setting	Description
Trigger level	High —an alarm event will occur **when 5V voltage appears on the contacts of the alarm input.** Low —an alarm event will occur **when the 5V voltage on the contacts of the alarm input disappears.**
Alarm output level	High —when an alarm event occurs, **up to 5V voltage will be applied to the contacts of the alarm output**. Low —when an alarm event occurs, the alarm output contacts **will be de-energized**.
Switching to the night mode	Select Enable to let the camera automatically switch to black and white mode when the status of the alarm input changes.
Current input	Current alarm input state.
Current output	Select the camera alarm output state that corresponds to the alarm event occurence: • Low; • High; • Schedule - The alarm input will operate according to the schedule; • Close - The alarm input is turned off.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.6.2.2 "Schedule" tab

Go to the Schedule tab in the I/O Alarm settings menu to set up alarm inputs and outputs schedule.

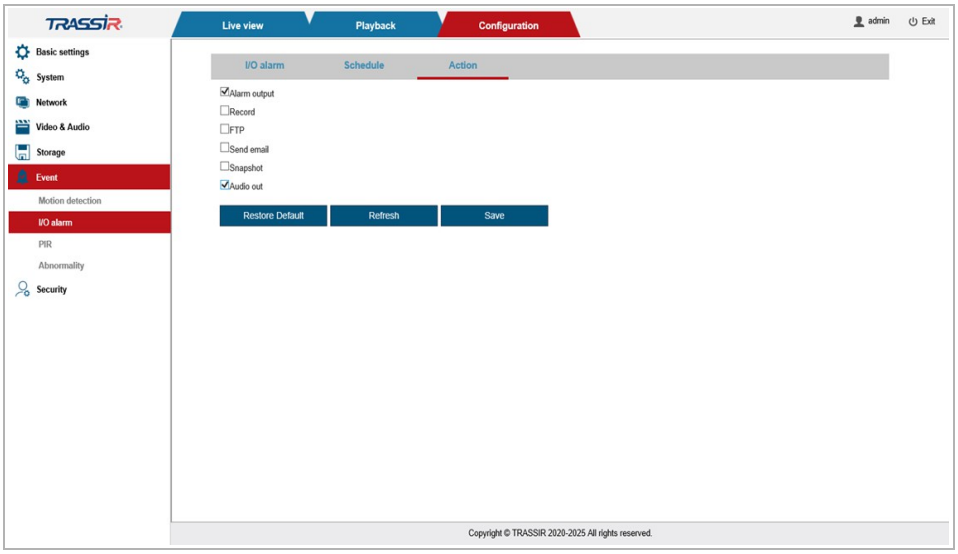


NOTE.

Alarm inputs and outputs operation schedule is configured the same way as in Motion detection section (see section 3.4.6.1.2).

3.4.6.2.3 "Action" tab

Go to the Action tab in the I/O Alarm settings menu in order to set up reactions on alam inputs and outputs triggering.



NOTE.

The reactions on alarm inputs and outputs triggering are configured the same way as in Motion detection section (see 3.4.6.2.3).

3.4.6.3 "PIR" menu

WARNING!

Not supported on these devices.

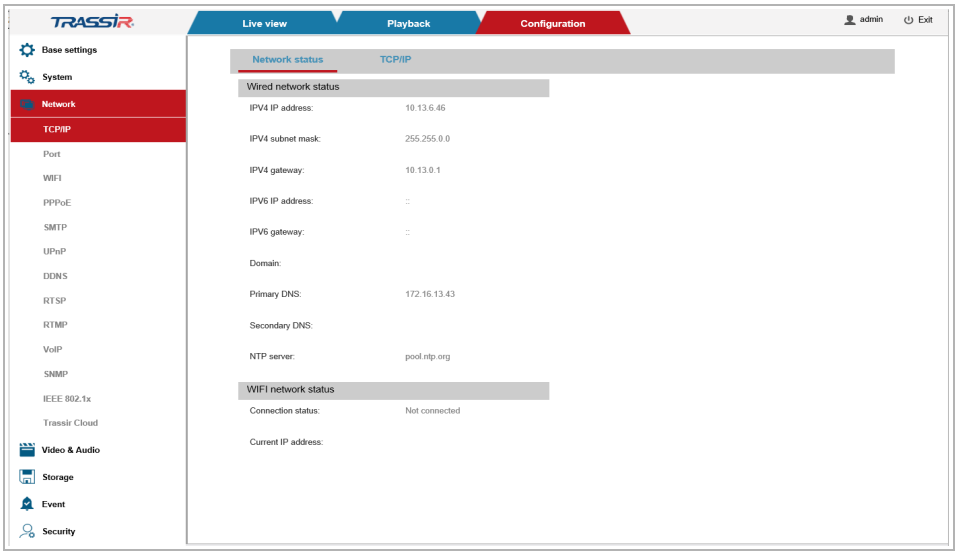
3.4.6.4 "Abnormality" menu

The menu consists of the additional tabs which allow to:

- Network disconnection —configure actions in case of network disconnection (see section 3.4.6.4.1);
- Device startup — configure action on the device start (see section 3.4.6.4.2).

3.4.6.4.1 "Network disconnection" tab

In order to set up reactions in case of device connection loss, go to the Network disconnection tab in the Abnormality settings menu.



Set the Enable flag to activate the setting.

Specify time which will determine the event occurrence, from 0 to 300 seconds in the Trigger Interval Min. time field. If an alarm event lasts less than the specified time, then it is considered not to have occurred.

Select one or several reactions on camera connection loss by checking the corresponding boxes:

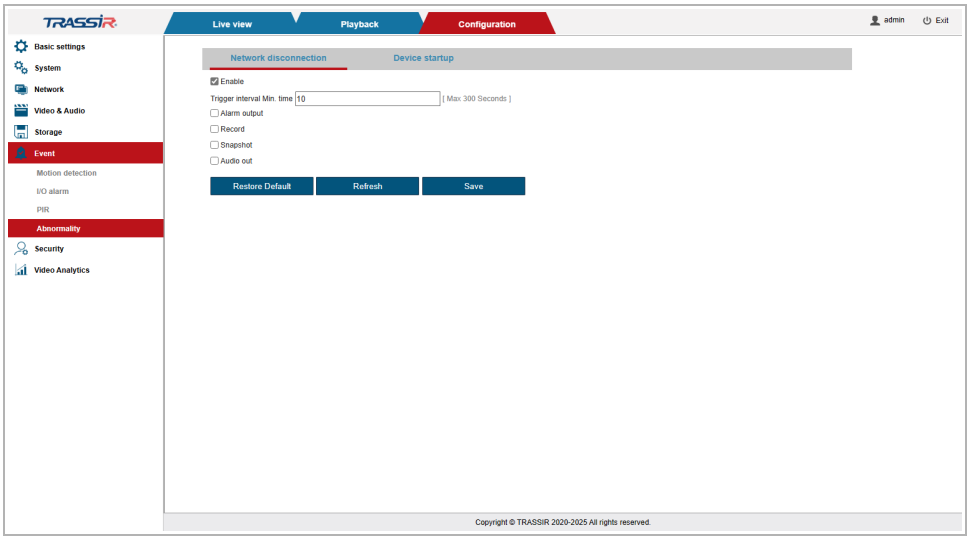
- Alarm output —close alarm output (see 3.4.6.2).
- Record —record video to the archive. You can see record settings description in 3.4.6.1.2.
- Snapshot —save snapshot to the archive (see 3.4.4.3).
- Audio out —Enable alarm sound. You can see audio settings description in 3.4.4.1.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.6.4.2 "Device startup" tab

In order to set up reactions on device startup go to the Device startup tab in the Abnormality settings menu.



Set the Enable flag to activate the setting.

Select one or several reactions on the camera startup by checking the corresponding boxes

NOTE.

The reactions are configured the same way as in Motion detection section (see 3.4.6.2.3).

3.4.7 "Security" menu

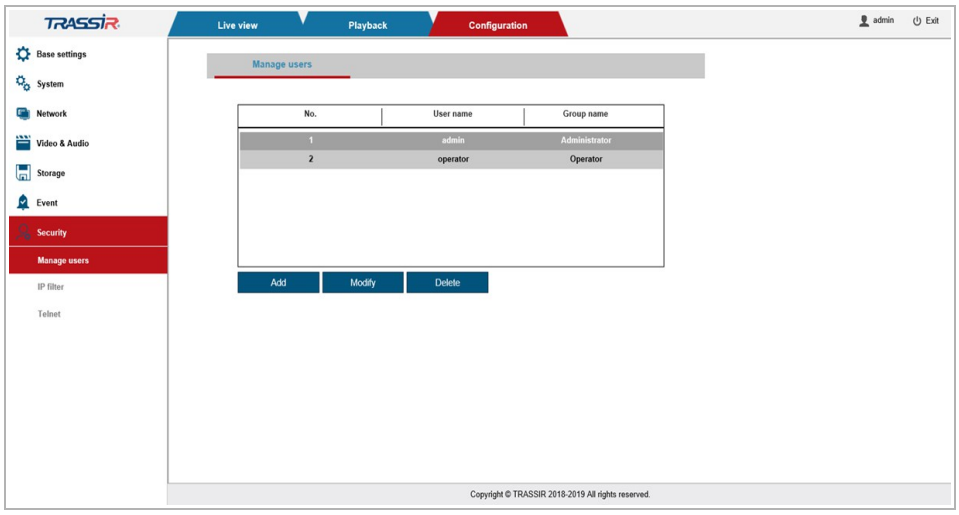
Open the Security menu.

The menu consists of the following sections which allow to:

- Manage Users —configure IP camera access parameters (see section 3.4.7.1);
- IP Filter —restrict access to the IP camera from one or several network devices (see section 3.4.7.2);
- Telnet —set up Telnet connection (see section 3.4.7.3).

3.4.7.1 "Manage users" menu

Go to the Manage Users section in the Security settings menu.



This group of settings lets you create a new user, set up access password and customize user access to the IP camera settings.

In order to modify user settings or delete a user select it from the list and press Modify or Delete correspondingly.

NOTE.

There is already a user with the Administrator rights in the IP camera settings by default.

WARNING!

We strongly recommend to change the Administrator rights upon first connection to the IP camera web interface.

Press Add to create a new user.

Setting	Description
Username	User name to authorize.
Password	Password to the IP camera web interface.
Confirm Password	Enter IP camera web interface password again.
User Group	User group to which current user belongs to: ◆ Administrator — full user; ◆ Operator — user with operator rights; ◆ Viewer — user with the rights to view log only.
Authority list	Set the corresponding flags to set up user rights.

Uncheck the corresponding boxes to change the current user authority list.

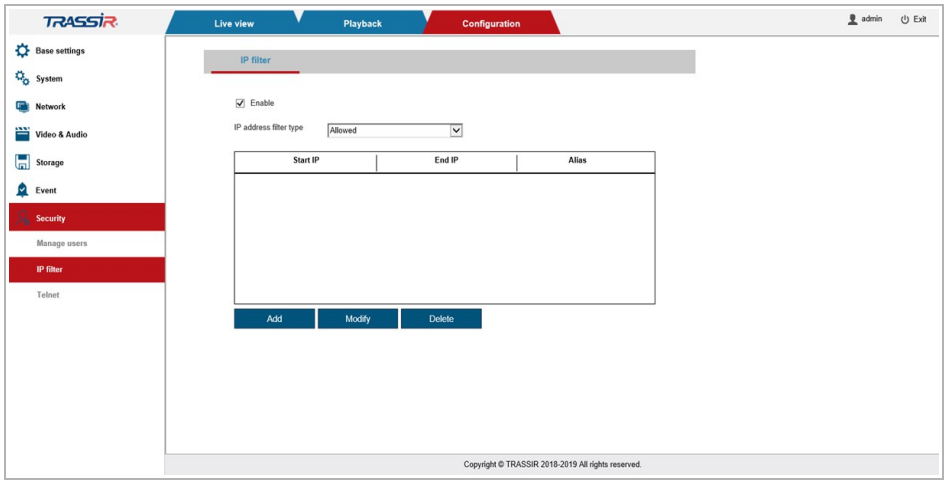
Press Save to save the changes.

3.4.7.2 “IP filter” menu

WARNING!

Before starting to configure IP filtering make sure the IP address of the PC where the IP camera is being set up is in the address white list. Otherwise access to the further IP camera settings will be blocked.

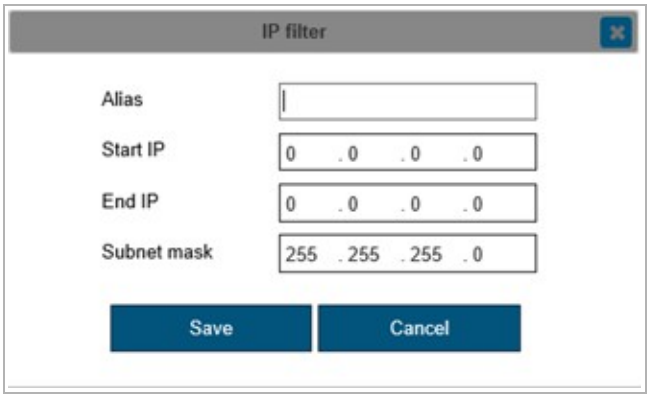
Go to the IP Filter section in the Security settings menu to open the menu.



Use IP filtering settings to restrict access to the IP camera from one or several network devices.

Select Enable IP Filtering to activate the setting.

In order to add the IP address to the allowed or forbidden addresses list select Allowed or Forbidden, respectively, in the IP address filter type block and press Add.



The IP Filter window will open. Enter the Start IP and End IP of the range into the corresponding fields. Enter the name of the IP address range in the Alias field.

Press Save to save the changes.

In order to modify or delete the created filter select it from the list and press Modify or Delete correspondingly.

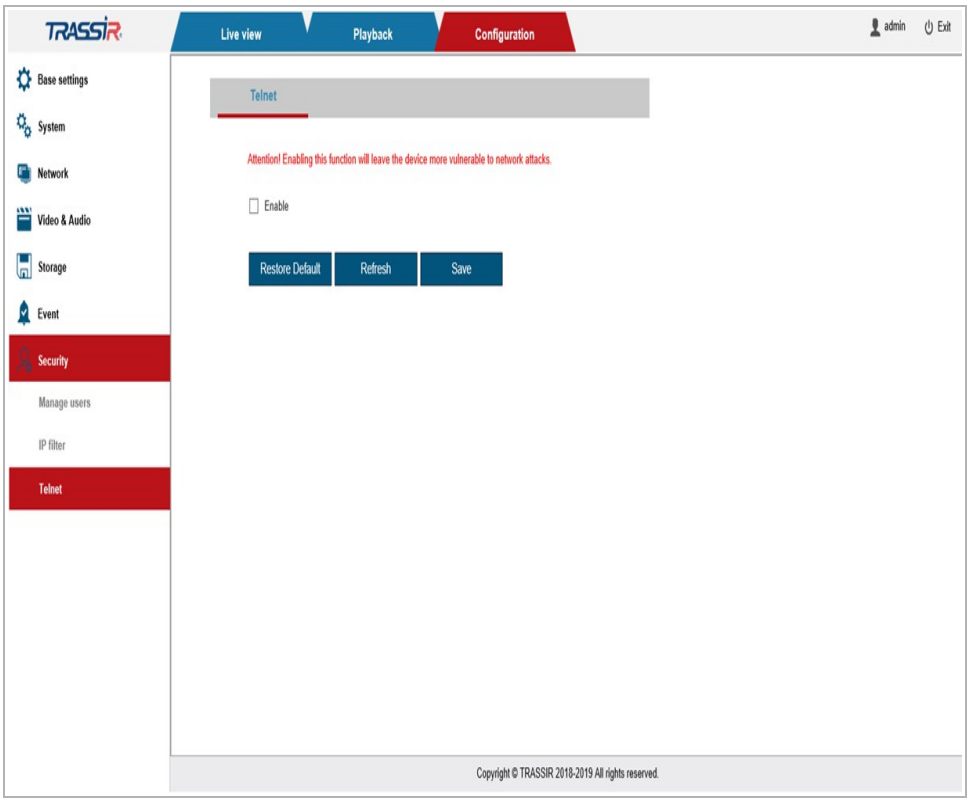
3.4.7.3 “Telnet” menu

WARNING!

It is recommended to enable this feature only in case of emergency, since when it is turned on, the device may not be protected from attacks from the network.

The Telnet feature may be necessary to remotely connect to the camera through the service console.

Open the Telnet section in the Security settings menu to configure connection via Telnet.



Set the Enable flag to allow remote connection to the camera.

Press Restore default to restore the default settings.

Press Save to save the changes.

3.4.8 "Video analytics" menu

Open Video analysis menu. It consists of the following sections which allow to:

- Facial detection —configure main facial detection parameters (see section 3.4.8.1);
- People Counting —set up counting the number of people crossing the board in one of the preset directions (see section 3.4.8.2);
- Human Detection —configure human detection (see section 3.4.8.3);
- Vehicle Detection —set up vehicle detection (see section 3.4.8.4);
- Line-crossing Detection —configure detection of people crossing the line in one of the preset directions (see section 3.4.8.5);
- Intrusion Detection —configure detection of intrusion to the preset area (see section 3.4.8.6);
- Loitering —set up detection of loitering people in the preset area (see section 3.4.8.7).

WARNING!

Simultaneous use of Video analytics, WIFI, TRASSIR Cloud and HTTPS can lead to unstable operation of the following camera models: TR-D2121CL3W, TR-D2121IR3Wv3, TR-D2121IR3Wv3, TR-D3121IR2Wv3, TR-D7121IR1Wv3, TR-D8121IR2Wv3.

3.4.8.1 "Facial detection" menu

This menu allows configuring main facial detection and recognition parameters.

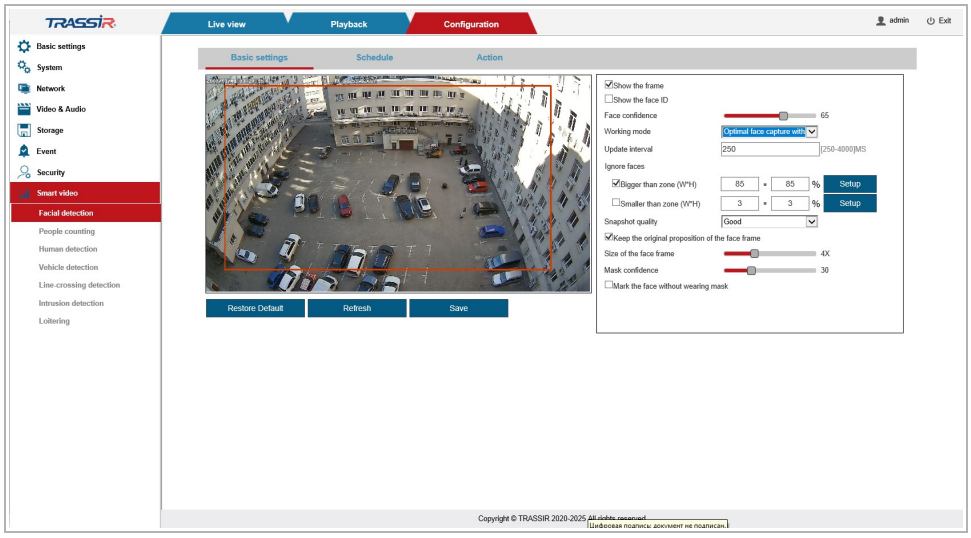
Go to Facial Detection section in the Video analysis to open.

The menu consists of additional tabs which allows to:

- Basic settings —configure basic facial detection parameters (see 3.4.8.1.1);
- Schedule —set up detector schedule (see 3.4.8.1.2);
- Action —set up actions upon facial detection (see 3.4.8.1.3).

3.4.8.1.1 "Basic settings" tab

Open the Basic settings tab in the Facial detection settings menu in order to set up basic detection parameters.



Setting	Description
Show the frame	Set the flag to highlight recognized people on video with a frame.
Show the face ID	Set the flag to display unique ID on a recognized person on video.
Face confidence	Configure detector confidence threshold. The higher the value is, the lesser is the probability of false positives.
Working mode	Detector working mode: • Optimal face capture with specified time intervals —the detector will search for faces within a set period of time. • Optimal face capture in a specified area —the detector will search for faces in a specified zone.
Update interval	The time period, after which the detector restarts searching for faces in the frame, in seconds, for Optimal face capture with specified time intervals working mode.
Min stay time	Set the minimal time of a person in the frame, in seconds, after which the detector will be triggered, for Optimal face capture in a specified area working mode.
Capture delay time	The time period, recorded upon the detector triggering, for Optimal face capture in a specified area working mode.
Ignore faces	Set the flag for detector to ignore the objects of specified size: Bigger than zone W*H or Smaller than zone W*H. Press Setup to save changes.
Snapshot quality	Select the snapshot quality.
Keep the original proposition of the face frame	Set the flag to keep the proportions of the recognized face when you increase the size of the frame.
Size of the face frame	Set the frame size in relation to the recognized face.

Setting	Description
Mask confidence	Set the threshold of confidence that there is a protective mask on a recognized face. The higher the value is, the lower is the probability of false alarms.
Mark the face without wearing mask	Set the flag for the detector to detect and highlight faces without protective mask on video.

Press Restore Default to restore the default settings.

Press Save to save the changes.

3.4.8.1.2 "Schedule" tab

Open the Schedule tab in the Facial Detection settings menu to set up facial detection schedule.

NOTE.

The facial detection schedule is configured the same way as on the Schedule tab in Motion detection section (see section 3.4.6.1.2).

3.4.8.1.3 "Action" tab

In order to set up reactions on human detection open the Action tab in the Facial detection settings menu.

NOTE.

The reactions upon the detector triggering are configured the same way as on the Action tab in the Motion detection settings menu (see section 3.4.6.1.3).

3.4.8.2 "People counting" menu

This menu allows configuring the counting of the amount of people crossing the border in one of the preset direction.

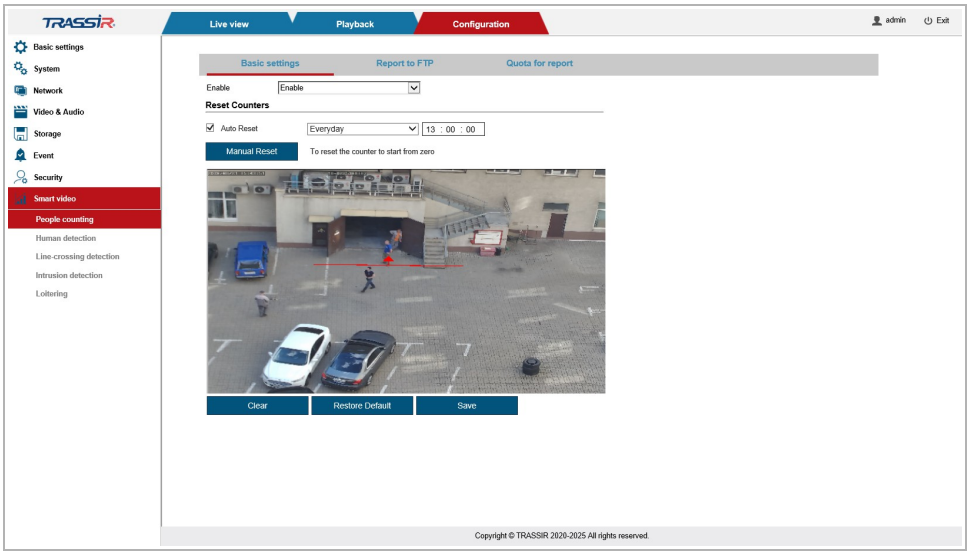
Go to the People Counting section in the Video analysis menu to open.

The section consists of the following tabs which allow to:

- Basic settings —set up border for people counting (see section 3.4.8.2.1);
- Report to FTP —configure report to FTP sending (see section 3.4.8.2.2);
- Quota for report —check the statistics of the reports sent (see section 3.4.8.2.3).

3.4.8.2.1 "Basic settings" tab

In order to set up border for counting people open the Basic settings tab in the People Counting settings menu.



Select Enable from the dropdown menu in order to activate the setting.

Left-click on the preview window and draw the border. Only one border can be drawn.

Upon the border crossing the amount of crossings in both directions will be displayed on the preview window and the alarm signal will blink, as well (see section 3.2).

There is a Reset counters field that lets you select the way to reset the border crossing counter:

Setting	Description
Auto Reset	Set the flag for automatic reset. Set the day and time of the reset in the adjacent fields.
Manual reset	Press the button to reset the counter manually.

Press Clear to remove the border.

Press Restore Default to restore the default settings.

Press Save to save the changes.

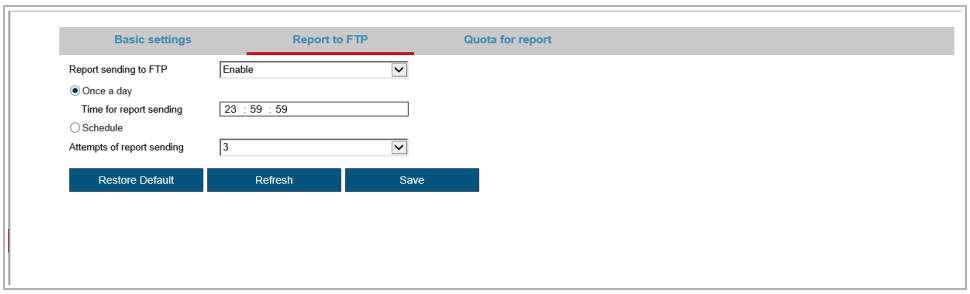
3.4.8.2.2 "Report to FTP" tab

NOTE.

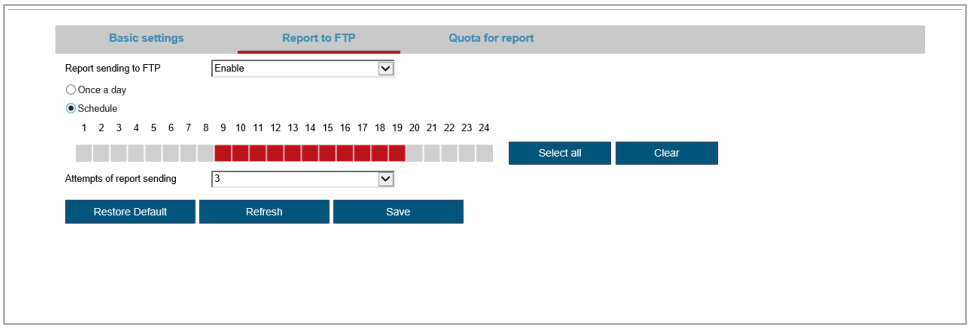
You can read about FTP settings in section 3.4.5.3.

Open the Report to FTP tab in the People Counting settings menu in order to configure people counting report settings.

Set the Enable value in the Report to FTP dropdown list, in order to use the setting, and select the wae to send the report:



Setting	Description
Once a day	Set the flag to send the report once a day and select the time of sending in the box below.
Time for report sending	Set up time of report sending.
Attempts of report sending	Set up number of attempts of the report sending, from 1 to 5.



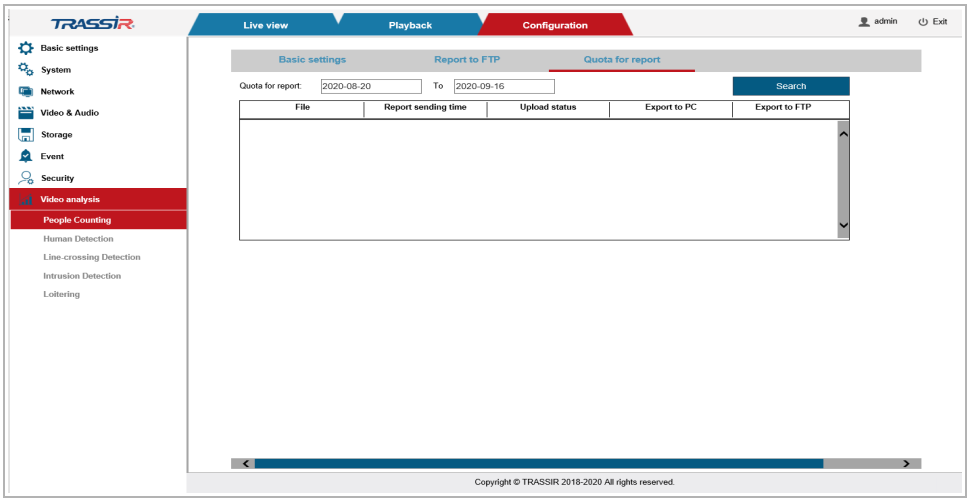
Setting	Description
Schedule	Set the flag to send the report by schedule. Set the sending time period in the opened menu.
Attempts of report sending	Set up number of attempts of the report sending, from 1 to 5.

Press Restore Default to restore the default settings.

Press Save to save the changes.

3.4.8.2.3 "Quota for Report" tab

In order to check the status of the sent reports open the Quota for report tab in the People Counting settings menu.



Set the time range for which you would like to check the reports in the Quota for report and To fields.

The information will be presented as the list of files. You can save the report to your PC or FTP by pressing Export.

3.4.8.3 “Human Detection” menu

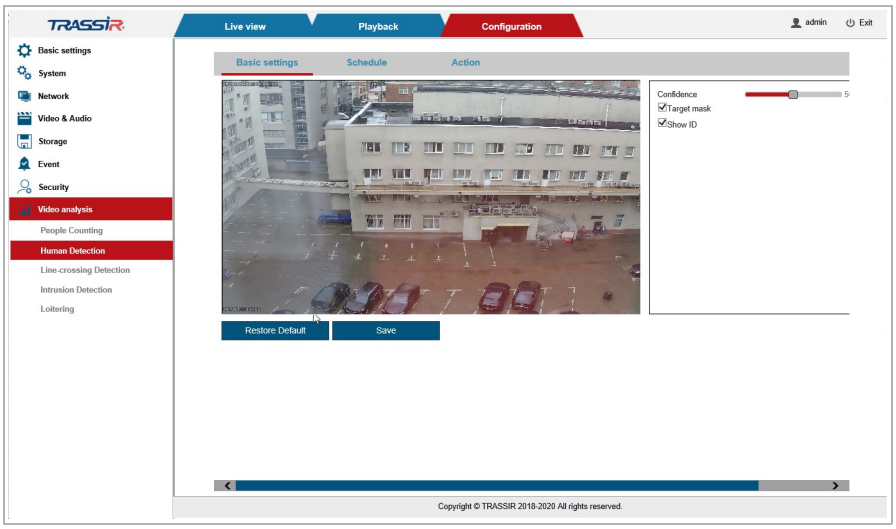
This menu allows you to set up human detection. Go to the Human Detection in the Video analysis menu to open.

The menu consists of the additional tab which allow to:

- Basic settings —configure basic detector settings (see section 3.4.8.3.1);
- Schedule —set up detector schedule (see section 3.4.8.3.2);
- Action —configure actions on human detection (see section 3.4.8.3.3).

3.4.8.3.1 "Basic settings" tab

Open the Basic settings tab in the Human Detection settings menu to set up human detector.



Setting	Description
Confidence	Configure detector confidence threshold. The higher the value is, the lesser is the probability of false positives.
Target mask	Set the flag to highlight the recognized people on video with a frame.
Show ID	Set the flag to display a unique identifier above each recognized person.

Press Restore Default to restore the default settings.

Press Save to save the changes.

3.4.8.3.2 "Schedule" tab

Open the Schedule tab in the Human Detection settings menu to set up human detection schedule.

NOTE.

The human detector schedule is configured the same way as on the Schedule tab in Motion detection section (see section 3.4.6.1.2).

3.4.8.3.3 "Action" tab

In order to set up reactions on human detection open the Action tab in the Human detection settings menu.

NOTE.

The reactions upon the detector triggering are configured the same way as on the Action в tab in the Motion detection settings menu (see section 3.4.6.1.3).

3.4.8.4 "Vehicle detection" menu

The menu allows you to set up vehicle detection.

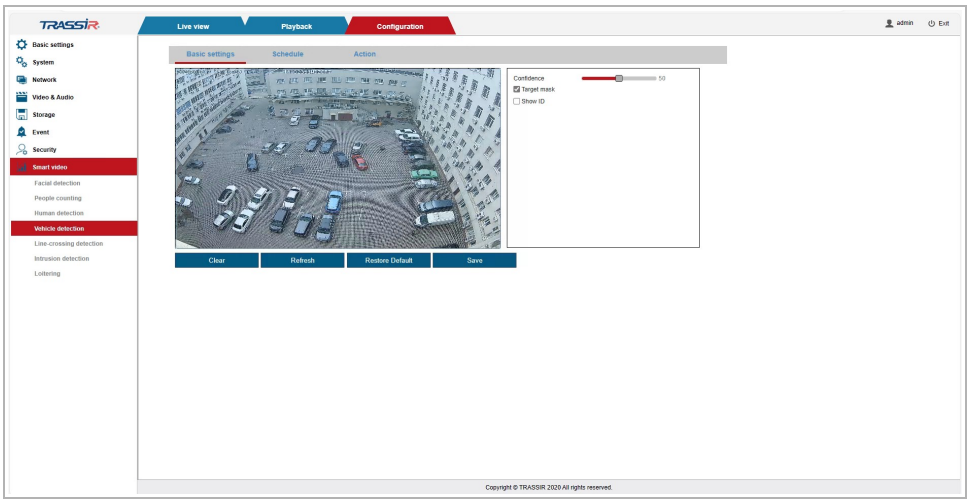
Go to Vehicle Detection of the Video analysis menu to open.

The menu consists of the additional tabs which allows you to:

- Basic settings —configure basic detector settings (see 3.4.8.4.1);
- Schedule —configure detector schedule (see 3.4.8.4.2);
- Action —set up actions upon vehicle detection (see 3.4.8.4.3).

3.4.8.4.1 "Basic settings" tab

Open the Basic settings tab in the Vehicle Detection settings menu to set up vehicle detector.



Use left mouse button to define a detection zone on video. You can use the entire area as a zone, to do this press Full screen.

Setting	Description
Confidence	Configure detector confidence threshold. The higher the value is, the lesser is the probability of false positives.
Target mask	Set the flag to highlight the recognized vehicle on video with a frame.
Show ID	Set the flag to display a unique identifier above each recognized vehicle on video.

Press Restore Default to restore the default settings.

Press Save to save the changes.

3.4.8.4.2 "Schedule" tab

Open the Schedule tab in the Vehicle Detection settings menu to set up human detection schedule.

NOTE.

The vehicle detector schedule is configured the same way as on the Schedule tab in Motion detection section (see section 3.4.6.1.2).

3.4.8.4.3 "Action" tab

In order to set up reactions on human detection open the Action tab in the Vehicle detection settings menu.

NOTE.

The reactions upon the detector triggering are configured the same way as on the Action в tab in the Motion detection settings menu (see section 3.4.6.1.3).

3.4.8.5 "Line Crossing" menu

The menu allows to set up detection of the line crossing in one of the preset directions.

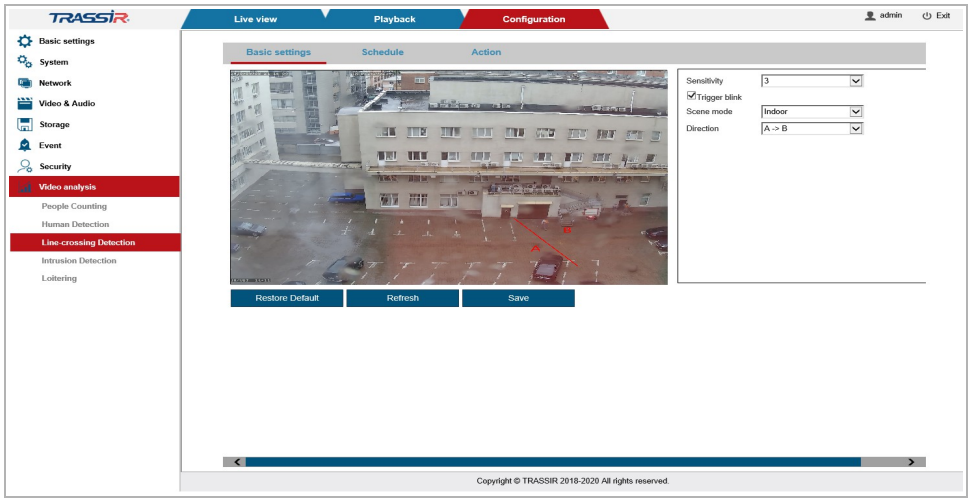
Go to the Line crossing section in Video analysis settings menu to open.

The menu consists of the additional tabs which allow to:

- Basic settings — set up basic parameters of line crossing detector (see section 3.4.8.5.1);
- Schedule —set up detector schedule (see section 3.4.8.5.2);
- Action —select actions upon the configured line crossing (see section 3.4.8.5.3).

3.4.8.5.1 "Basic settings" tab

To set up line crossing detector go to the Basic settings tab in Line Crossing settings menu.



Left-click on the preview window to draw the line. You can draw only one line and customize the following parameters:

Setting	Description
Sensitivity	Set up the detector sensitivity threshold, from 1 to 4. The higher the value is, the lesser is the probability of false positives.
Trigger blink	Set the flag to activate frame blinking upon the line crossing.
Scene mode	Select the detector scene mode: Outdoor or Indoor.
Direction	Select line crossing direction: ◆ A<->B — both ways; ◆ A->B — left to right; ◆ B->A — right to left.

Press Restore Default to restore the default settings.

Press Save to save the changes.

3.4.8.5.2 "Schedule" tab

Open the Schedule tab in the Line Crossing settings menu to set up line crossing detector schedule.

NOTE.

The line crossing detector schedule is configured the same way as on the Schedule tab in Motion detection section (see section 3.4.6.1.2).

3.4.8.5.3 "Action" tab

In order to set up reactions on line crossing open the Action tab in the Line Crossing settings menu.

NOTE.

The reactions upon the detector triggering are configured the same way as on the Action в tab in the Motion detection settings menu (see section 3.4.6.1.3).

3.4.8.6 “Intrusion Detection” menu

The menu allows to set up detection of unauthorized intrusion to a specific territory.

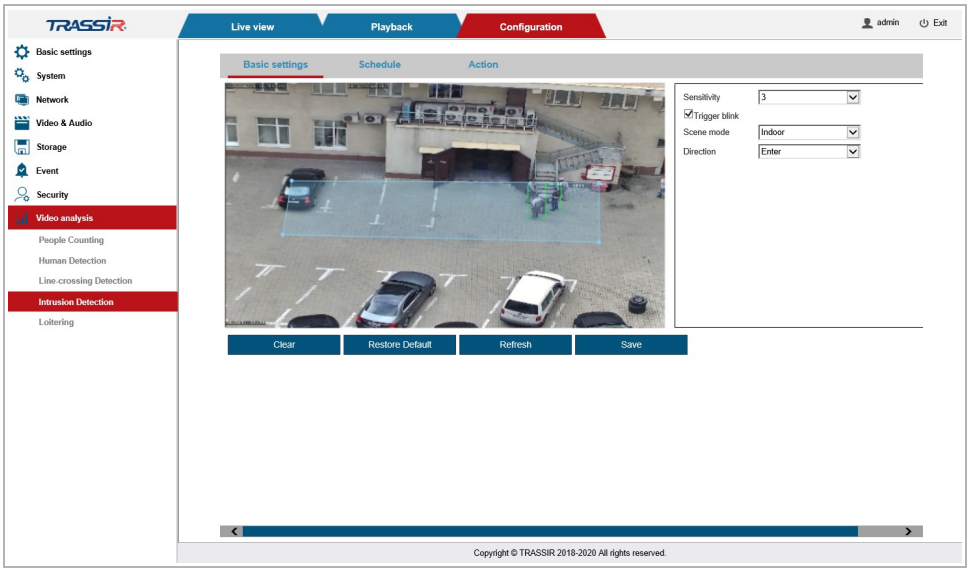
Go to the Intrusion Detection section in the Video analysis settings menu to open.

The menu consists of the additional tabs which allow to:

- Basic settings —configure basic detector parameters (see section 3.4.8.6.1);
- Schedule —set up detector schedule (see section 3.4.8.6.2);
- Action —select actions on intrusion detection (see section 3.4.8.6.3).

3.4.8.6.1 "Basic settings" tab

In order to configure the detector's settings open the Basic settings tab in the Intrusion detection settings menu.



Left-click on the preview window to specify the area which will be monitored. Set up the following parameters for this area:

Setting	Description
Sensitivity]	Set up the detector sensitivity threshold, from 1 to 4. The higher the value is, the lesser is the probability of false positives.
Trigger blink	Set the flag to activate frame blinking upon the specified area intrusion detection.
Scene mode	Select the detector scene mode: Outdoor or Indoor.
Direction	Select the zone intrusion direction: ◆ Left; ◆ Enter; ◆ Both.

Press Restore Default to restore the default settings.

Press Save to save the changes.

3.4.8.6.2 "Schedule" tab

Open the Schedule tab in the Intrusion Detection settings menu to set up line crossing detector schedule.

NOTE.

The intrusion detector schedule is configured the same way as on the Schedule tab in Motion detection section (see section 3.4.6.1.2).

3.4.8.6.3 "Action" tab

In order to set up reactions on line crossing open the Action tab in the Intrusion Detection settings menu.

NOTE.

The reactions upon the detector triggering are configured the same way as on the Action в tab in the Motion detection settings menu (see section 3.4.6.1.3).

3.4.8.7 "Loitering" Menu

The menu allows to configure the detection of loitering people on a specified area.

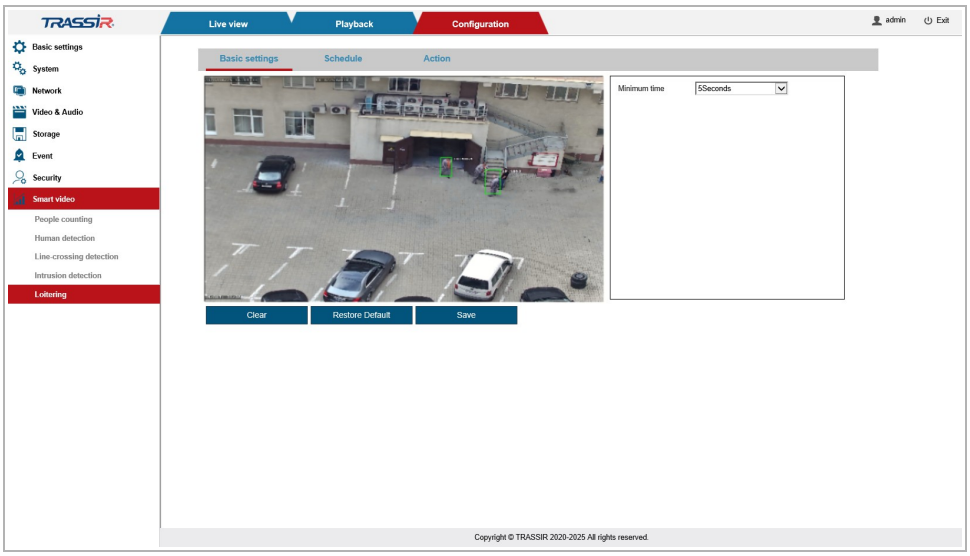
Go to the Loitering section in the Video analysis settings menu to open.

The menu consists of the additional tabs which allow to:

- Basic settings —configure basic detector parameters (see section 3.4.8.7.1);
- Schedule —set up detector schedule (see section 3.4.8.7.2);
- Action —select actions on intrusion detection (see section 3.4.8.7.3).

3.4.8.7.1 "Basic settings" tab

In order to set up basic parameters of the loitering detector open the Basic settings tab in the Loitering settings menu.



Left-click to create loitering people detection zone on video preview. Set the time allowed on the specific territory in the Minimum time field - 5, 10 or 15 s. Upon the expiration of this time the detector will trigger.

Press Restore Default to restore the default settings.

Press Save to save the changes.

3.4.8.7.2 "Schedule" tab

Open the Schedule tab in the Loitering settings menu to set up line crossing detector schedule.

NOTE.

The intrusion detector schedule is configured the same way as on the Schedule tab in Motion detection section (see section 3.4.6.1.2).

3.4.8.7.3 "Action" tab

In order to set up reactions on line crossing open the Action tab in the Loitering settings menu.

NOTE.

The reactions upon the detector triggering are configured the same way as on the Action в tab in the Motion detection settings menu (see section 3.4.6.1.3).

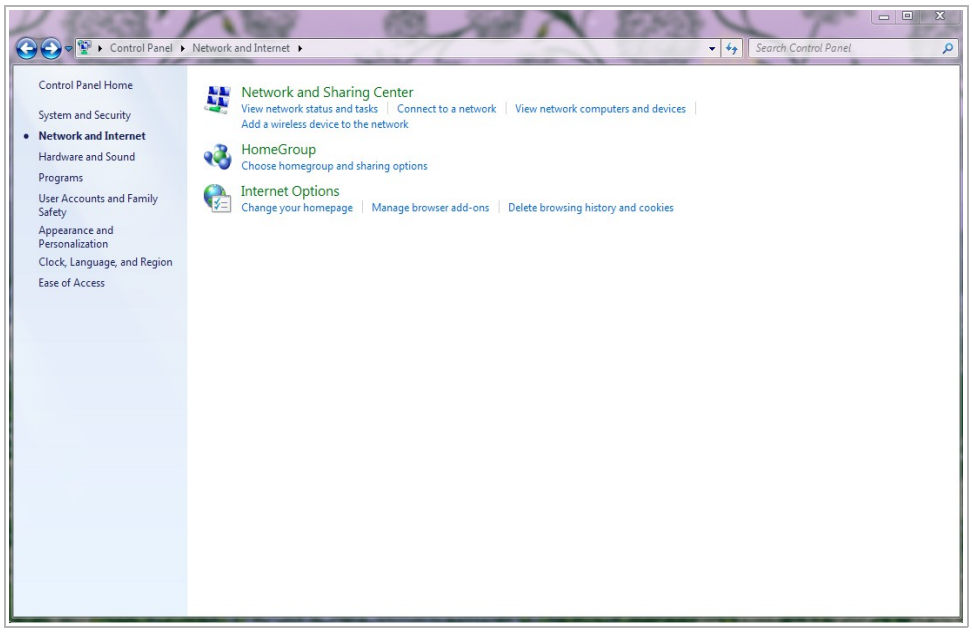
SUPPLEMENT A. CONFIGURING NETWORK SETTINGS ON PC

NOTE.

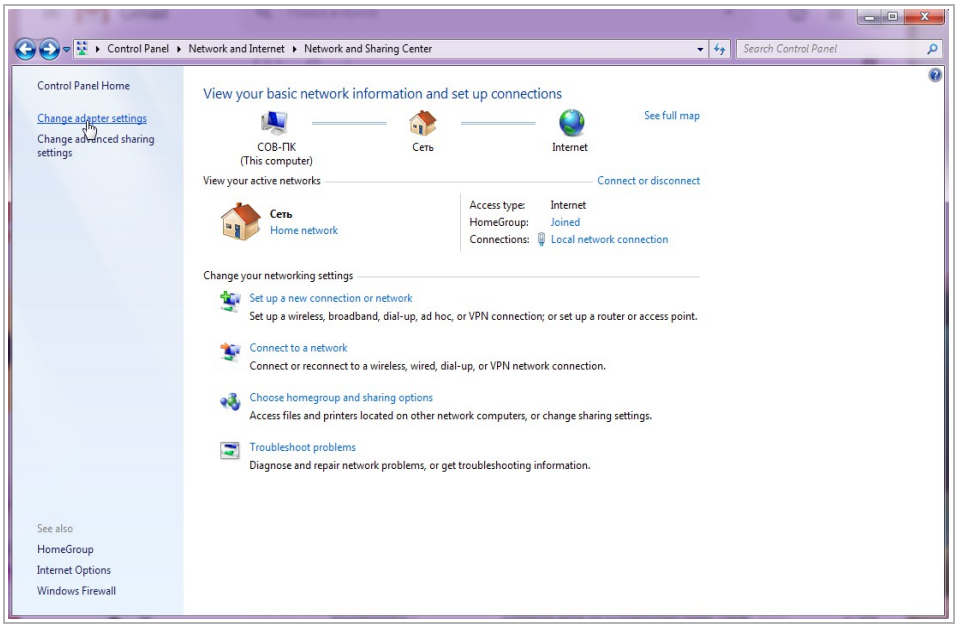
Description of network settings is presented on the example of Windows 7 operating system.

In order to access an IP camera, it is necessary that the PC and the camera are connected to the same subnet and have the corresponding IP addresses

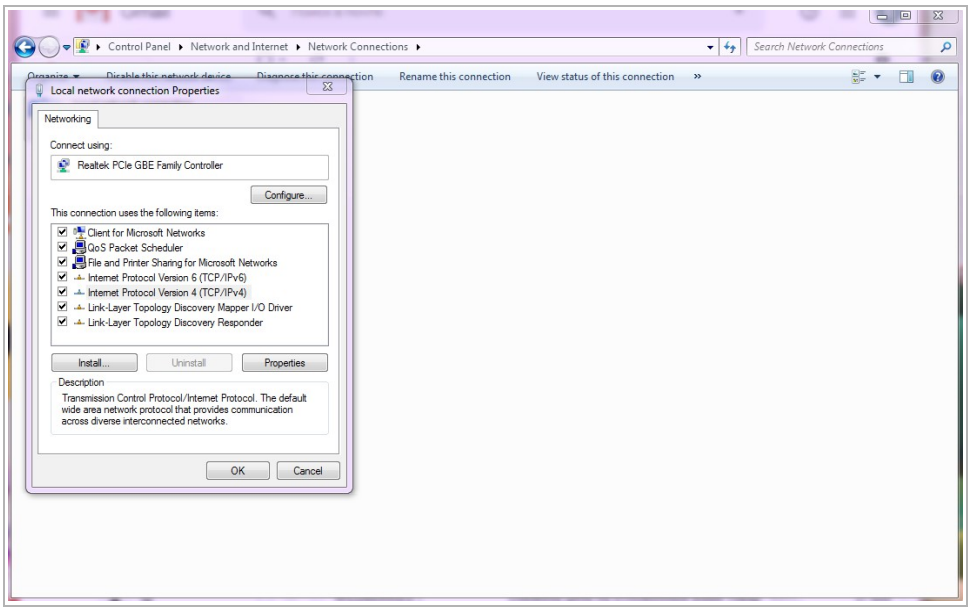
To do this, open Control panel (Start →Control panel) and run Network and Internet:



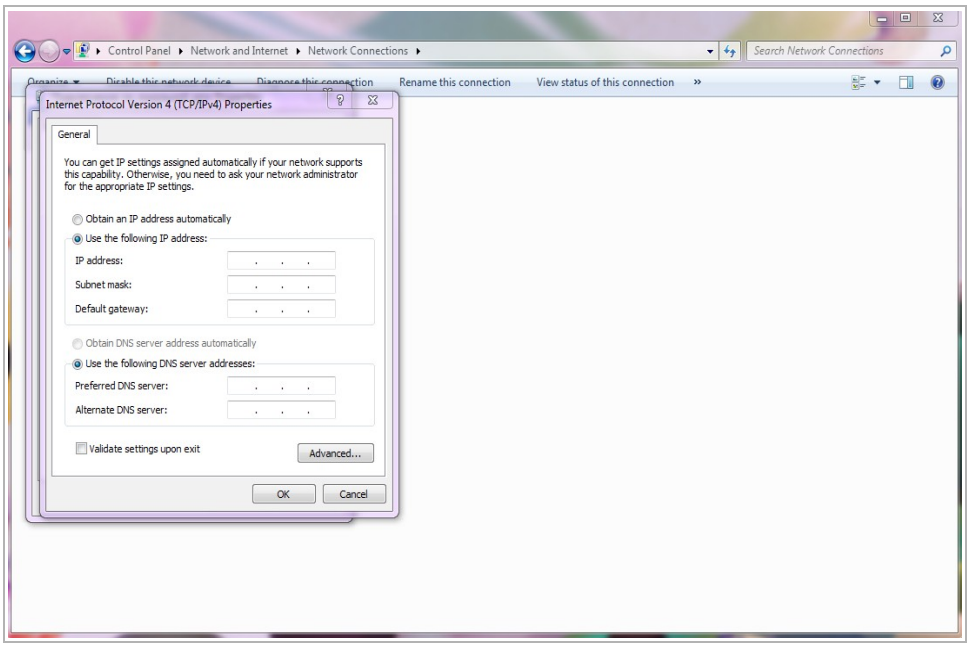
Go to the Change adapter settings menu:



Right click on adapter and press Properties:



In the opened window select Internet Protocol Version 4 (TCP/IPv4) and press Properties:

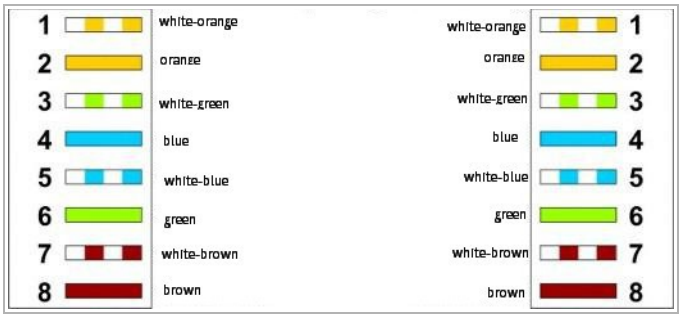


Select Use the following IP address and specify the required network settings (e.g. displayed on screenshot above).

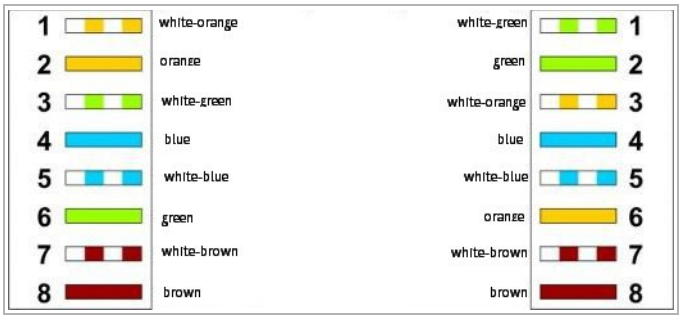
Press OK in all opened windows to save the settings.

SUPPLEMENT B. UTP CABLING

The IP camera is connected to the commutator (switch or router) using a «direct» cable with the following wiring:



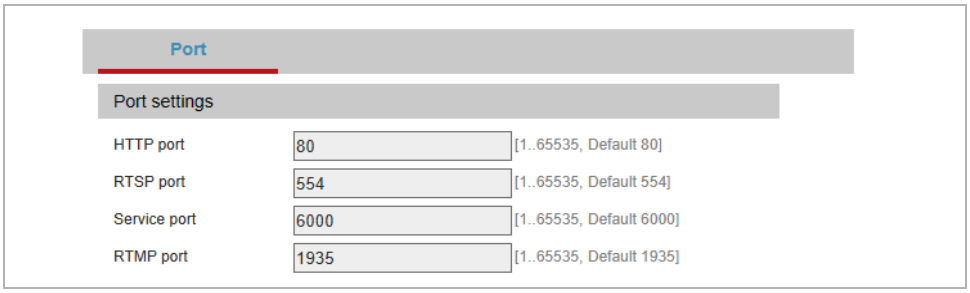
The IP camera is connected to the PC directly using «cross» cable with the following wiring:



SUPPLEMENT C. ROUTER SETTINGS

If the IP camera and the computer from which the connection is established are located in different local networks (e.g., the connection is via the Internet), in order to gain access to the IP camera it is necessary to configure the forwarding of network ports on the NAT server or router.

The IP camera uses the following network ports by default:



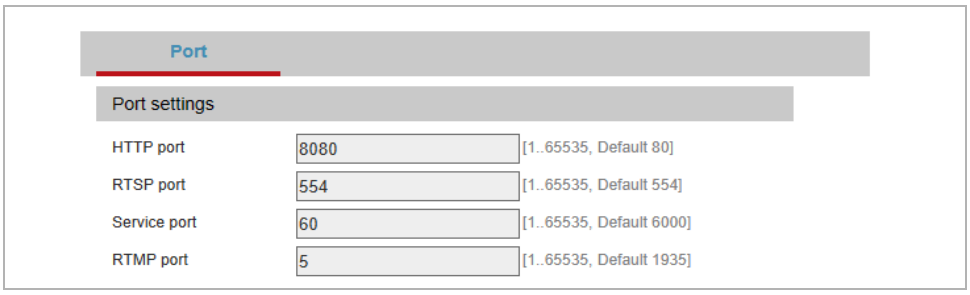
We will consider the configuration of port forwarding on the example of ZTE ZXHN F680 router.

Specify IP camera port random values. The port values for each IP camera should be unique and can't be used on the router for other services.

NOTE.

See description of the network ports in 3.4.3.2.

For example, you can set the following values:

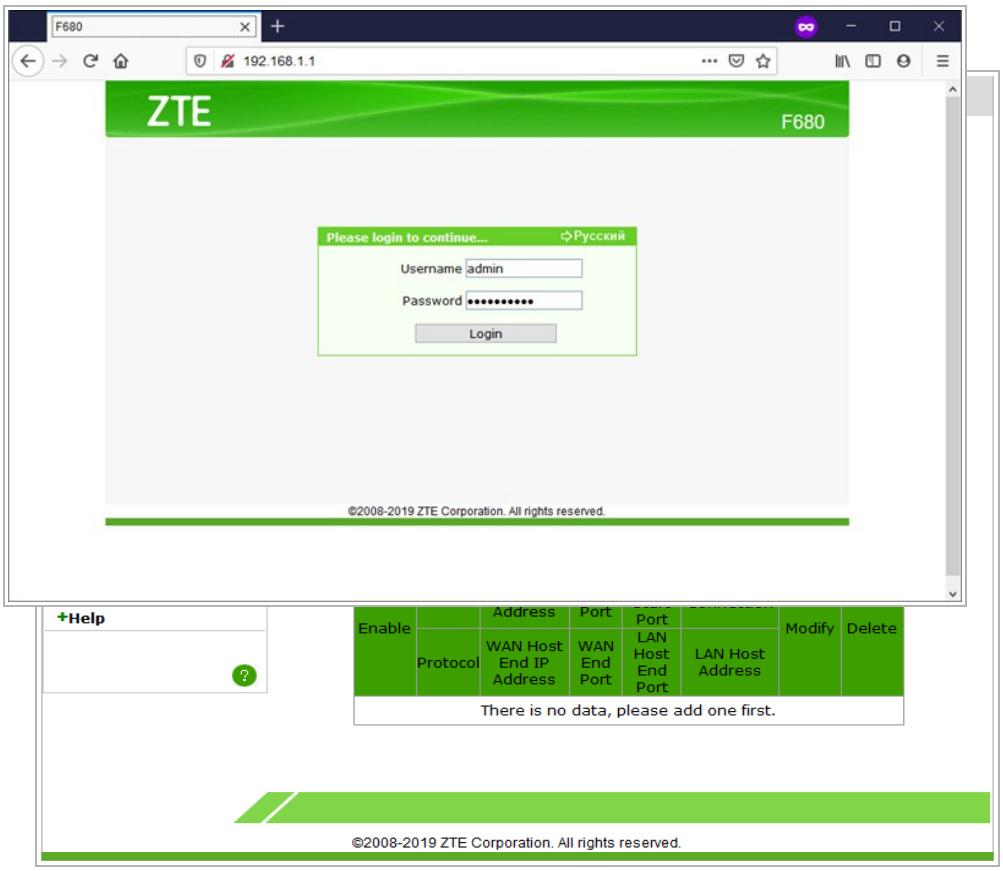


After that proceed to the router configuration.

NOTE.

Your router settings may differ from the description below.

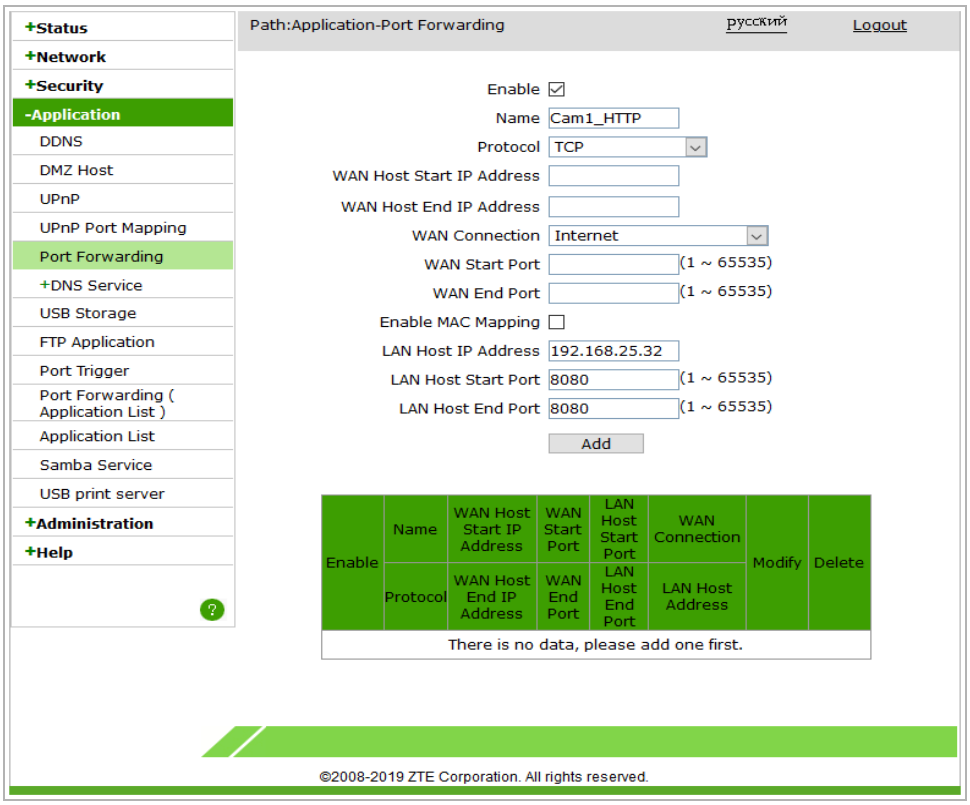
Start your web browser and enter the router IP address to access router administrator menu. As a result, the authorization window should appear:



Enter administrator login and password and press Login.

Go to the «Port forwarding» in the router settings menu (Application →Port forwarding):

As a result, a window for adding a forwarding port will open:



Enter a random forwarding name into the Name field.

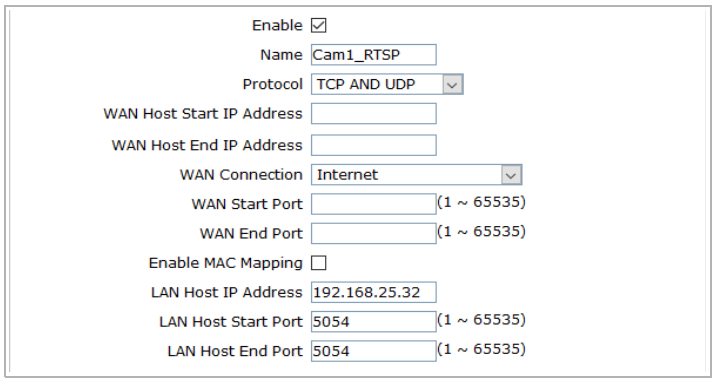
Select TCP/UDP or TCP data transfer protocol in the Protocol field.

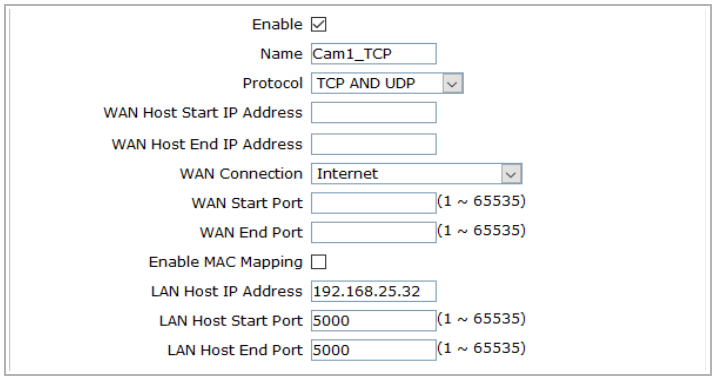
Specify http port to connect to the camera web interface which should be forwarded in the WAN Start Port and WAN End Port fields.

Specify camera internal IP address in the IP address field.

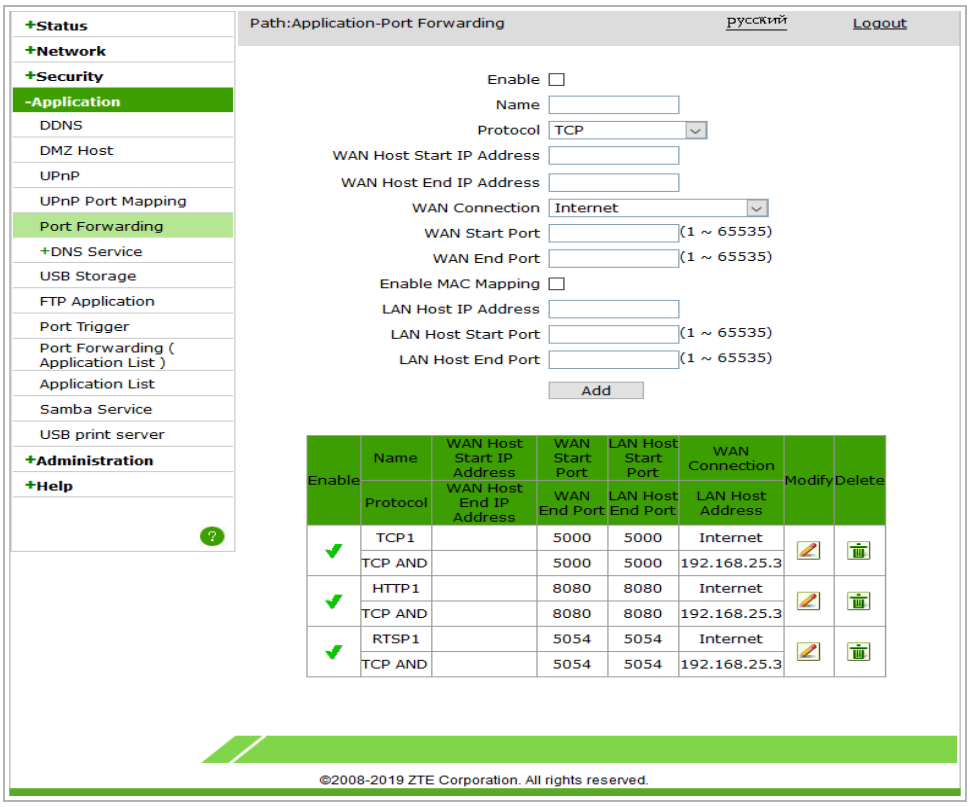
Press Add to save the forwarding rule.

Configure other port forwarding rules the same way:





As a result you should see the following:



In order to access IP camera from the Internet, enter <external router IP address>:<camera web interface connection port>.

Example: http://88.100.20.44:8080

NOTE.

You can also configure control and alarm ports forwarding.

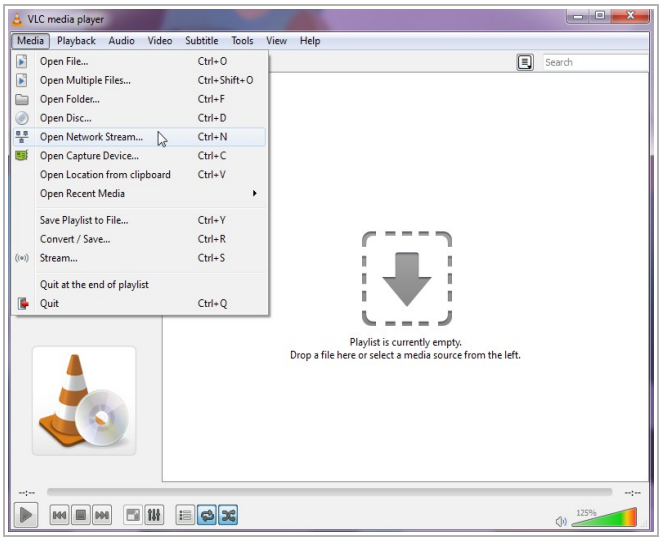
SUPPLEMENT D. OPERATION ON RTSP AND ONVIF

Connecting on RTSP protocol

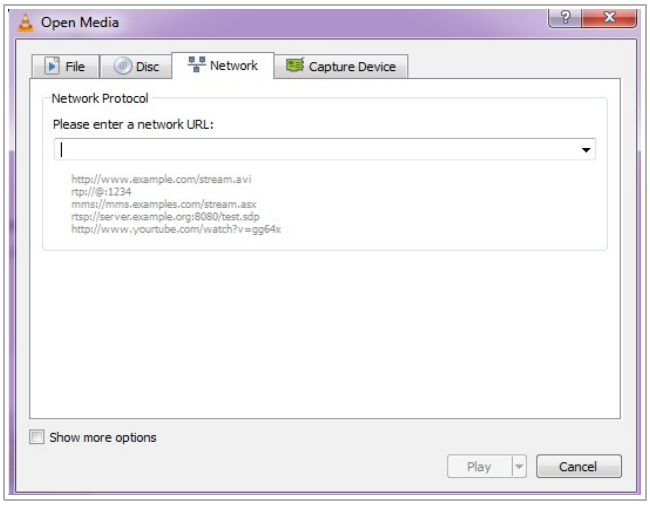
NOTE.

VLC media player (http://www.videolan.org/vlc/) will be used as an example for connection of an IP camera via RTSP. You can use any other media player with an option of video streaming.

Start media player and select network as a source. To do this select Media →Open network stream....



Enter RTSP request to the IP camera on the Network tab and press Play:



RTSP request to the IP camera should be in the following format:

main stream:
rtsp://[login]:[password]@[ip address]:[rtsp port]/live/main

sub stream:
rtsp://[login]:password]@[ip address]:[rtsp port]/live/sub

third stream:

rtsp://[login]:password]@[ip address]:[rtsp port]/live/mobile

where

[ip address] — camera ip address (see section 3.4.3.1 or 3.4.3.3);

[rtsp port] — IP camera rtsp port, which streams video (see section 3.4.3.2);

[login] and [password] — user name and password (see section 3.1);

/live/main, /live/sub, live/mobile — video stream request commands.

Example:

main stream:
rtsp://admin:12345@192.168.25.32:554/live/main

sub stream:
rtsp://admin:12345@192.168.25.32:554/live/sub

third stream:

rtsp://admin:12345@192.168.25.32:554/live/mobile

Getting a snapshot from IP camera

In order to get snapshot from IP camera enter the following request in to the browser:

rtsp://[ip address]:[port]/action/snap?cam=0&user=[login]&pwd=[password]

where

[ip address] — camera ip address (see section 3.4.3.1 or 3.4.3.3);

[port] — http port used to connect to the IP camera (see section 3.4.3.2);

[login] and [password] — user name and password (see section 3.1);

/action/snap?cam=0 — snapshot request command.

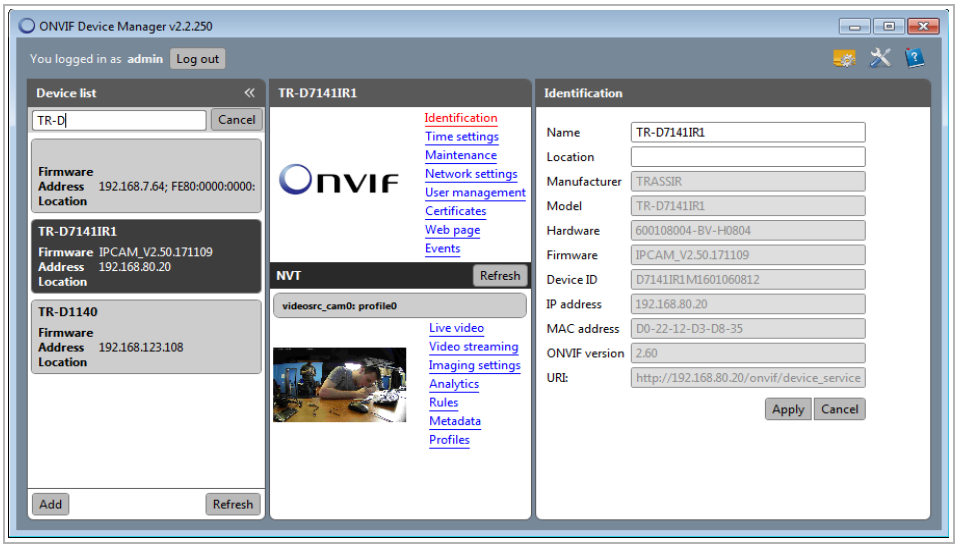
Connecting on ONVIF standard

In order to connect an IP camera on ONVIF standard, the following data is required:

- Camera IP address (see section 3.4.3.1 or 3.4.3.3);
- video streaming port (see section 3.4.3.2);
- user name and password, having access to the IP camera (see section 3.4.7.1).

NOTE.

You can also use «ONVIF Device Manager» (http://sourceforge.net/projects/onvifdm/) utility to connect to IP camera on ONVIF standard.



SUPPLEMENT E. IP CAMERA PLACEMENT

The correct IP camera placement is essential for proper video analysis module operation.

The camera installation parameters may vary depending on the focal length (more focal length - more distance of the camera from the detection zone).

The following requirements should be met in order to get the most accurate video information and increase the viewing angle:

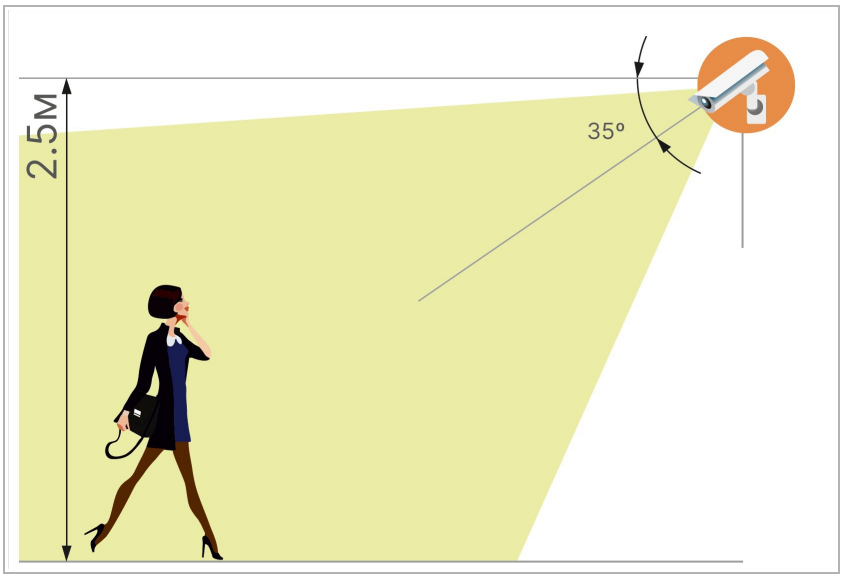
NOTE.

The following installation parameters are recommended for cameras with focal length of 2.8 mm.

Placement:

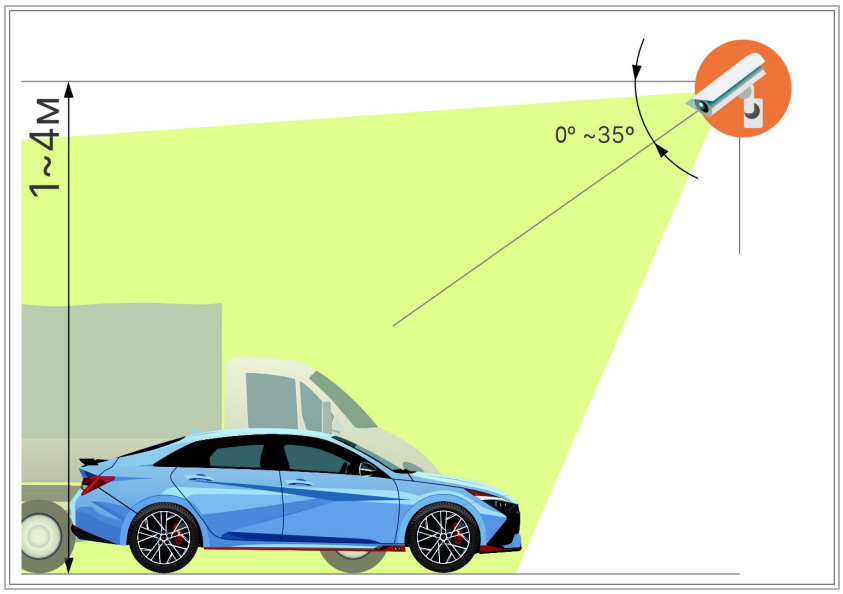
Line crossing

- The height is not less than 2,5 meters from the detected object;
- The tilt angle towards the detected object should not exceed 35% and should be adjusted depending on the installation height.



Vehicle detector

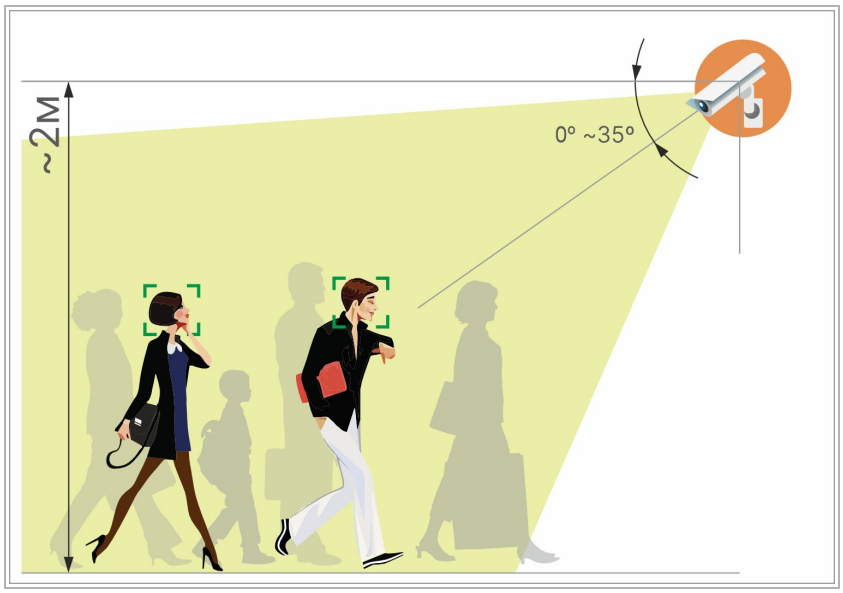
- Installation height 1-4m;



- The tilt angle towards the detected object should not exceed 35% and should be adjusted depending on the installation height.

Face detection

- Installation height 1-2 meters, tilt angle can be adjusted according to the installation height;
- It is recommended that the tilt angle towards the ceiling should not exceed 35 degrees.



Shooting area and objects:

- There should be enough free space in the intended detection area;
- The shooting area should have moderate lighting, without too bright or flickering light;
- The detected objects should be located at the sufficient distance which is not too far or too close to the camera;
- The detected objects should not move too quickly or change too often.

When installing the camera, you should take into account the external factors that can negatively affect the operation of the detectors or cause false alarms:

- Incorrect camera placement, when the objects of detection are located too close or too far from the camera;
- There are too many foreign objects in the intended detection area;
- There are too many fast moving objects in a frame;
- The lighting in the shooting area is too bright, or, on the contrary, is not sufficient;
- There are harsh shadows against bright sunlight when the camera is located outdoors;
- The unfavorable weather conditions such as gusts of wind or raindrops when the camera is located outdoors.

NOTE.

In order to decrease the amount of the false alarms, change the detectors' sensitivity or decrease the size of the detection zones. Read more in 3.4.6.1,3.4.8.2, 3.4.8.3, 3.4.8.5, 3.4.8.6, 3.4.8.7.

SUPPLEMENT F. IPC MANAGER

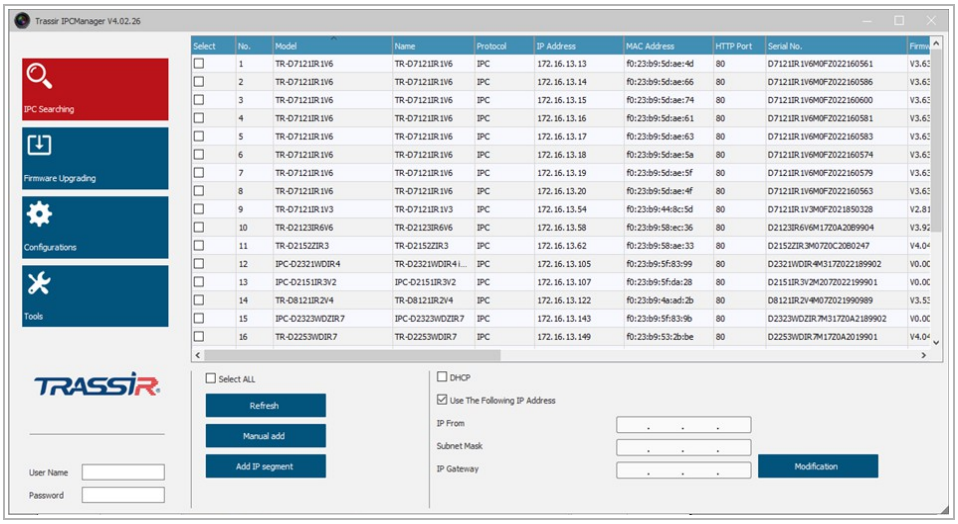
Searching for IP-camera using TRASSIR IPCManager app

Use TRASSIR IPCManager utility to find the camera if the IP address is unknown.

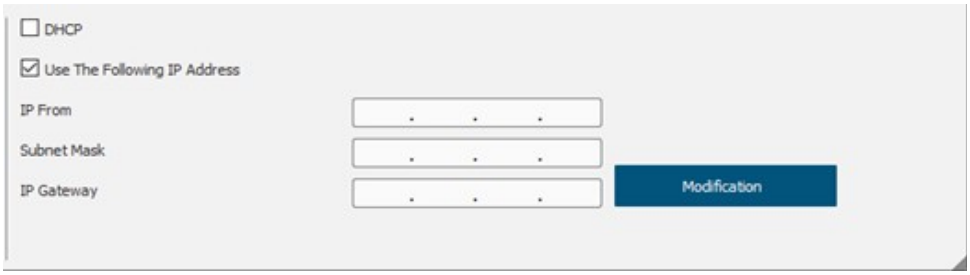
NOTE.

You can download TRASSIR IPCManager utility on www.dssl.ru.

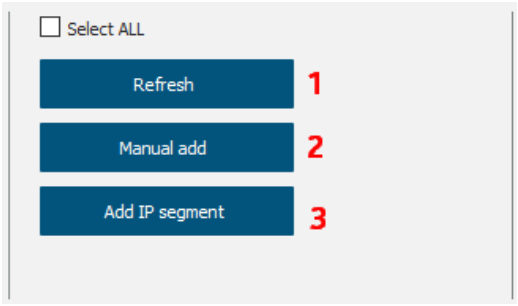
Upon the start the utility will search for IP cameras in local network automatically.



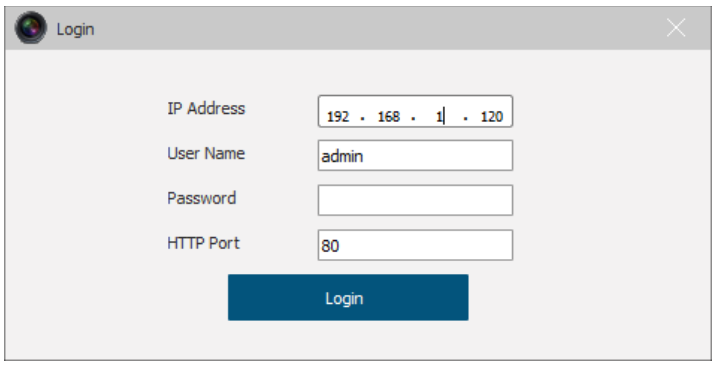
Find the IP camera in the displayed list, select and enter your user name and password in the lower left corner. Configure device basic network settings.This will allow you to access the IP camera's web interface.



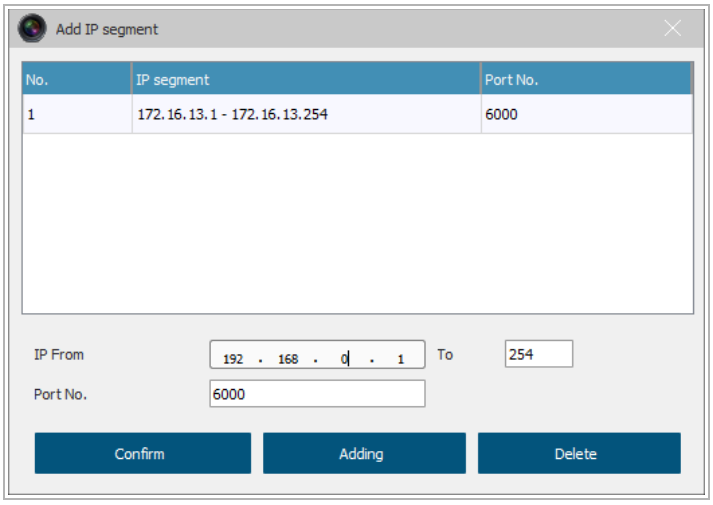
You can also:



1. Refresh the device list
2. Manual add — add camera manually. In the window that opens enter the camera data.

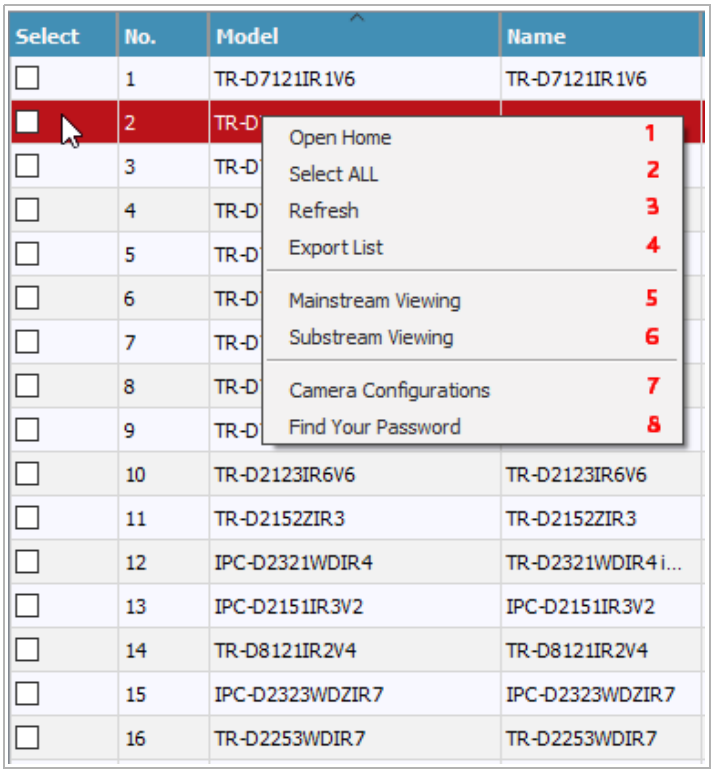


3. Add IP segment — add a network segment.



Additional menu for managing IP camera

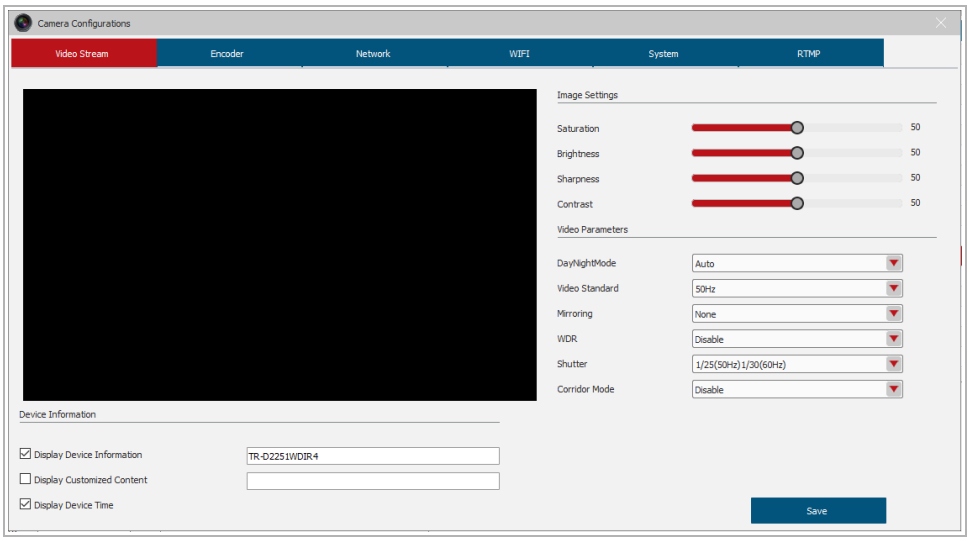
Select the camera in the list and right-click.



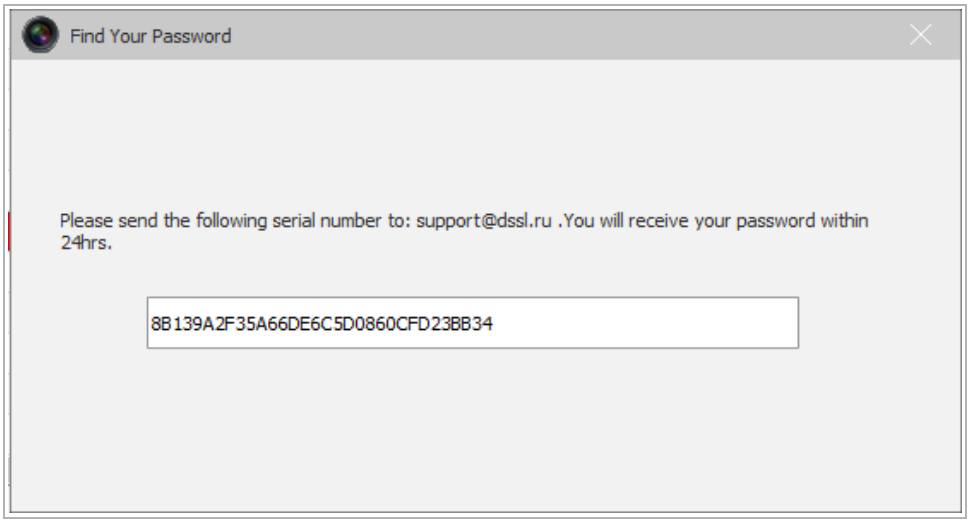
An additional menu will open, which allows you to:

1. Open home — open IP-camera web interface;
2. Select all — select all devices in the list;
3. Refresh — refresh the list of devices;
4. Export list — export list of the discovered devices;
5. Mainstream Viewing — open the camera main stream;
6. Substream Viewing — open the camera sub stream;

7. Camera configurations — open the IP-camera basic settings menu;

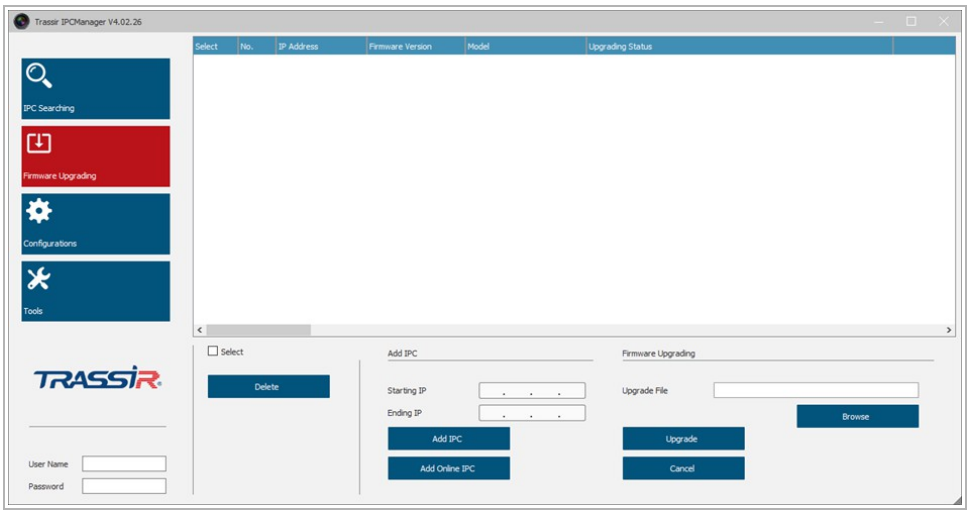


8. Find your password — IP camera password reset menu.



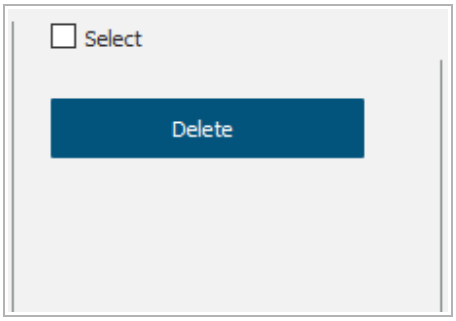
Upgrading camera with IPC Manager

The IPC Manager utility lets you update the device firmware. To do this, open the Firmware Upgrading menu.

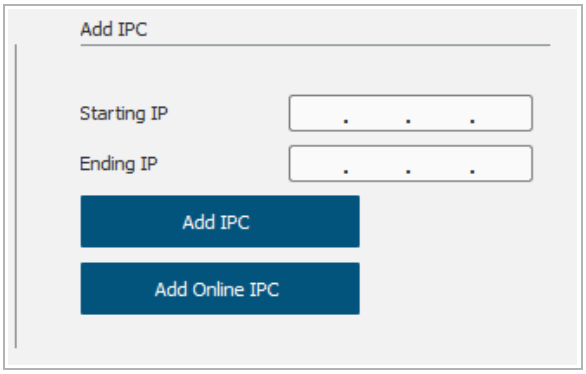


This menu lets you:

- Select all devices / Delete a device

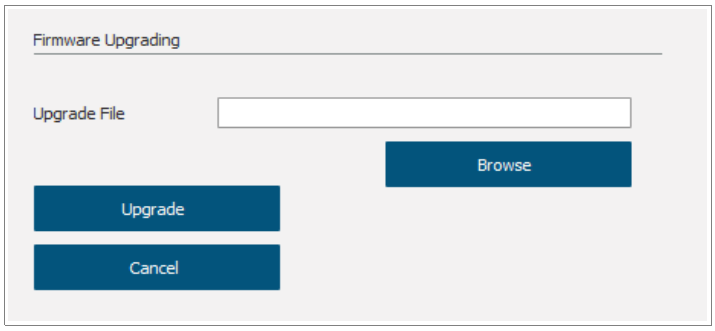


- Set a range of IP addresses for update.



If you specify a starting IP address and click Add IPC button - only the specified IP address will be added. If you specify a start and end IP addresses - the whole range of IP addresses will be added.

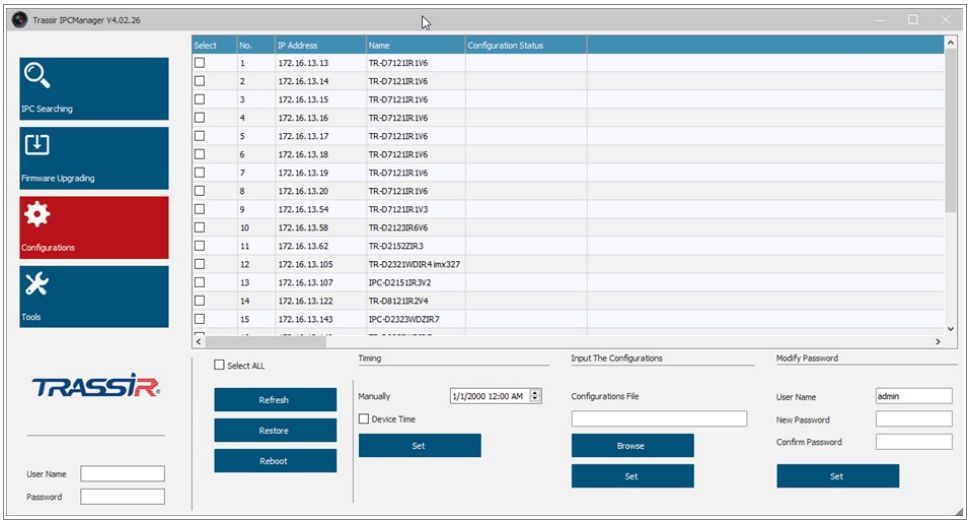
- Upgrade device firmware



Press Browse to locate the firmware file and then press Upgrade to start the upgrading process.

"Configurations" menu

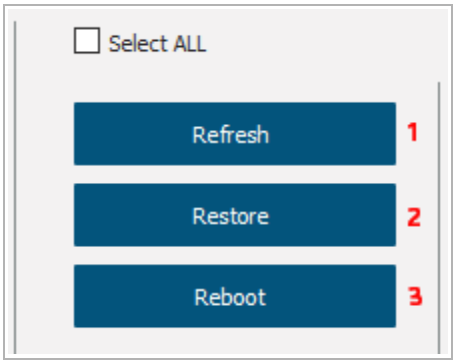
Open the Configurations menu.



This menu lets you additional parameters of IP-camera:

- Set up date and time;
- Import the configurations files for the selected device;
- Change IP-camera password;
- Save the camera configurations file.

You can also:

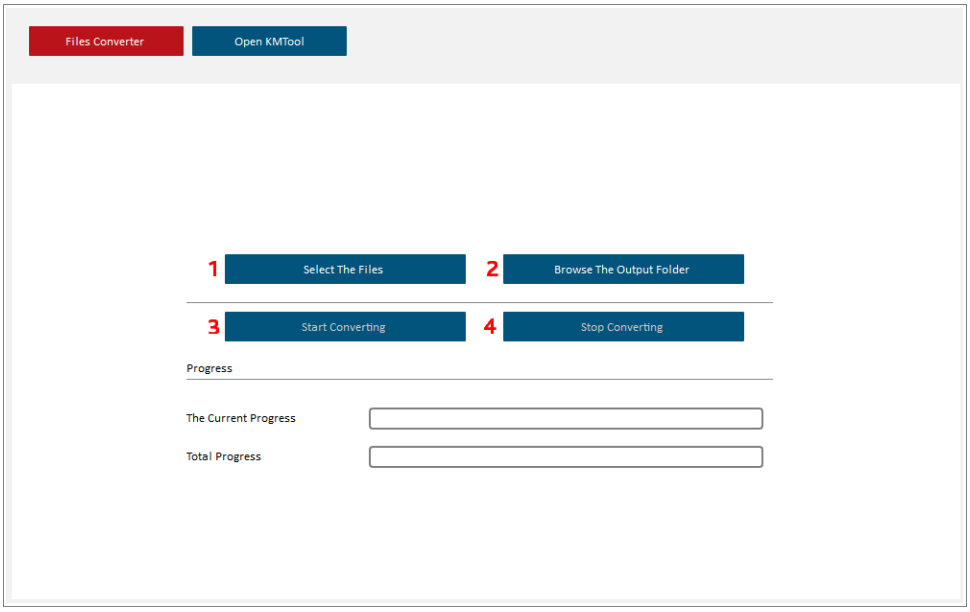


1. Refresh — refresh the device list;
2. Restore — restore the camera settings to defaults;
3. Reboot — reboot IP-camera.

"Tools" menu

Open the Tools menu.

The File Converter lets you convert video files from IP-camera SD card to MP4.



1. Select The Files — open path to source files.
2. Browse The Output Folder — open path to the converted files.
3. Start Converting.
4. Stop Converting — stop the converting process.

The KMTool tab lets you activate analytics license.

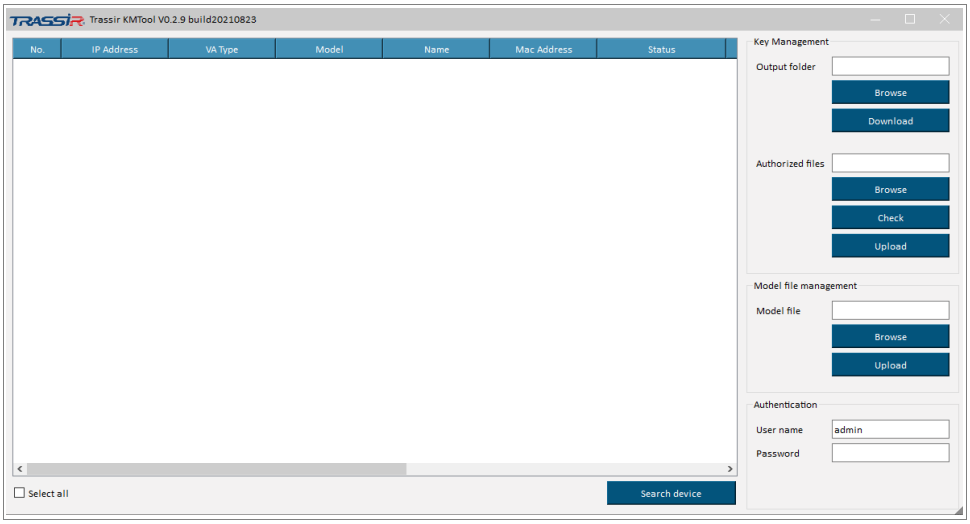
NOTE.

A license file is required for activation. To request a license file for analytics on cameras, you need to contact your manager.

There are three steps involved in activating the analytics license: collecting the necessary information about the camera, transmitting this information, and loading the license.

1st step: Collecting the necessary information on camera:

1. Start IPC Manage and go to Tools section to Open KMTool tab.
2. In the opened window in Authorization block enter login and password to access the camera.



3. The KMTool will search for devices in the local network. You can also search for devices manually, by pressing Search device.
4. You can check the device state in the Status column:activated or deactivated. Select one or several deices to activate, by checking the corresponding flags.

5. Click Browse to specify the desired folder to save the device certificate file (the file name must contain the MAC address in the following format **aa:bb:cc:dd:ee:ff.dat**). Then click Download in Output folder block to save the device certificate file in the selected folder.

2nd step: Providing information to technical support:

1. Send the folder archive/device certificate file to your manager.
2. You will receive an email with a license file attached. It takes an average of 2-3 business days to process your request. In case of any difficulties, or long absence of response, please contact technical support.

3rd step: Uploading license for camera:

1. Click Browse in the Authorized Files block in Open KMTool tab.
2. Click the Upload button. After that the tool will automatically find the necessary files on the devices and download them to the corresponding cameras.
3. Make sure that the license file was successfully added. Click Check: if the license file is correct, the Status column will display Activated. If the Status column still shows Authorization Error, contact the technical support.